Troy Technologies USA

CCNA
STUDY GUIDE

Exam 640-407

Edition 2

Congratulations!!

You have purchased a *Troy Technologies USA* Study Guide.

This study guide is a selection of questions and answers similar to the ones you will find on the official exam. Study and memorize the following concepts, questions and answers for approximately 15 to 20 hours and you will be prepared to take the exams. We guarantee it!

Remember, average study time is 15 to 20 hours and then you are ready!!!

GOOD LUCK!

DISCLAIMER

This study guide and/or material is not sponsored by, endorsed by or affiliated with Cisco Systems, Inc. Cisco®, Cisco Systems®, CCDA™, CCNA™, CCDP™, CCNP™, CCIE™, CCSI™, the Cisco Systems logo and the CCIE logo are trademarks or registered trademarks of Cisco Systems, Inc. in the United States and certain other countries. All other trademarks are trademarks of their respective owners.

Guarantee

If you use this study guide correctly and still fail the exam, send your official score notice and mailing address to:

Troy Technologies USA
8200 Pat Booker Rd. #368
San Antonio, TX 78233

We will gladly refund the cost of this study guide. However, you will not need this guarantee if you follow the above instructions.

It is important that you read and study the “”CCNA Concepts” portion of this study guide. We have identified important “KEYPOINTS” in this section. Please ensure that you absolutely know and understand these. You will find them in double lined boxes throughout the text.

CCNA Concepts

OSI Reference

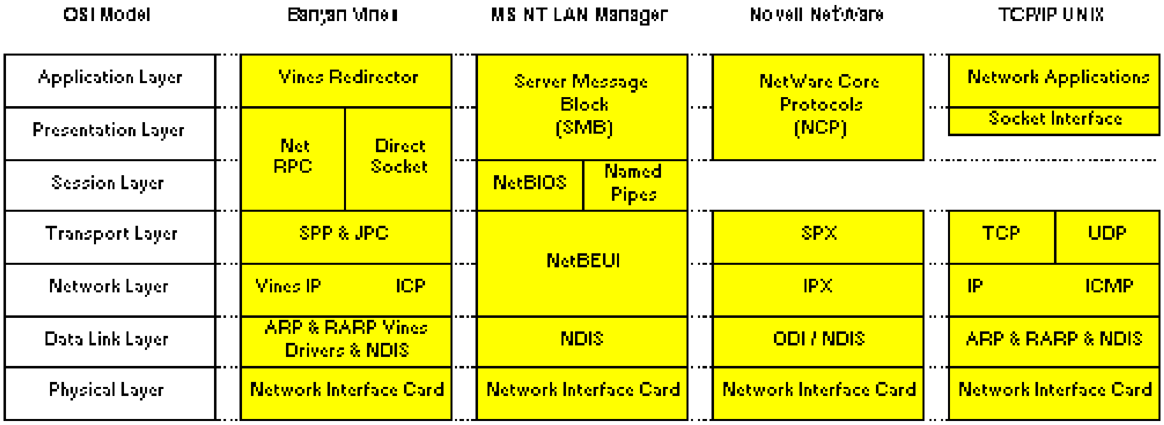
The OSI Model is the most important concept in the entire study guide, memorize it!! Many of the test questions will probably be based upon your knowledge about what happens at the different layers.

OSI MODEL

Layer	Name	Function
7	Application Layer	Provides network services to user applications. Establishes program-to-program communication. Identifies and establishes the availability of the intended communication partner, and determines if sufficient resources exist for the communication.
6	Presentation Layer	Manages data conversion, compression, decompression, encryption, and decryption. Provides a common representation of application data while the data is in transit between systems. Standards include MPEG, MIDI, PICT,TIFF, JPEG, ASCII, and EBCDIC.
5	Session Layer	Responsible for establishing and maintaining communication sessions between applications. In practice, this layer is often combined with the Transport Layer. Organizes the communication through simplex, half and full duplex modes. Protocols include NFS, SQL, RPC, Appletalk Session Protocol (ASP) and XWindows.
4	Transport Layer	Responsible for end-to-end integrity of data transmission. Hides details of network dependent info from the higher layers by providing transparent data transfer. The “window” works at this level to control how much information is transferred before an acknowledgement is required. This layer segments and reassembles data for upper level applications into a data stream. Port numbers are used to keep track for different conversations crossing the network at the same time. Uses both connection-oriented and connectionless protocols. Supports TCP, UDP and SPX.
3	Network Layer	Routes data from one node to another. Sends data from the source network to the destination network. This level uses a 2 part address to establish and manages addressing, track device locations, and determines the best path to use for moving data on the internetwork. Responsible for maintaining routing tables. Routers operate at this level.
2	Data Link Layer	Responsible for physically transmission of data from one node to another. Handles error notification, network topology, flow control. Translates messages from the upper layers into data frames and adds customized headers containing the hardware destination and source address. Bridges and switches operate at this layer. **Logical Link Control Sublayer** – Acts as a managing buffer between the upper layers and the lower layers. Uses Source Service Access Points (SSAPs) and Destination Service Access Points (DSAPs) to help the lower layers talk to the Network layer.

		Responsible for timing, and flow control. **Media Access Control Sublayer** – Builds frames from the 1's and 0's that the Physical layer picks up from the wire as a digital signal, and runs Cyclic Redundancy Checksum (CRC) to assure that nothing was damaged in transit.
1	Physical Layer	Manages putting data onto the network media and taking the data off. Sends and receives bits. Communicates directly with communication media. Provides electrical and mechanical transmission capability.

Keypoints: Know the above OSI model definitions backward and forward.



OSI Model	Banyan Vines	MS NT LAN Manager	Novell NetWare	TCP/IP UNIX
Application Layer	Vines Redirector	Server Message Block (SMB)	NetWare Core Protocols (NCP)	Network Applications Socket Interface
Presentation Layer	Net RPC Direct Socket			
Session Layer		NetBIOS Named Pipes		
Transport Layer	SPP & JPC	NetBEUI	SPX	TCP UDP
Network Layer	Vines IP ICP		IPX	IP ICMP
Data Link Layer	ARP & RARP Vines Drivers & NDIS	NDIS	ODI / NDIS	ARP & RARP & NDIS
Physical Layer	Network Interface Card	Network Interface Card	Network Interface Card	Network Interface Card

Connection-oriented vs. Connectionless Communication

Connection-orientated

Connection oriented communication is supported by TCP on port 6. It is reliable because a session is guaranteed, and acknowledgements are issued and received at the transport layer. This is accomplished via a process known as Positive Acknowledgement. When the sender transmits a packet a timer is set. If the sender does not receive an acknowledgement before the timer expires, the packet is retransmitted.

Connection-oriented service involves three phases:

Connection establishment - During the connection establishment phase, a single path between the source and destination systems is determined. Network resources are typically reserved at this time to ensure a consistent grade of service (such as a guaranteed throughput rate).

Data transfer - During the data transfer phase, data is transmitted sequentially over the path that has been established. Data always arrives at the destination system in the order it was sent.

Connection termination - During the connection termination phase, an established connection that is no longer needed is terminated. Further communication between the source and destination systems requires a new connection to be established.

Connection-oriented service has two significant disadvantages as compared to a connectionless network service:

Static path selection - Because all traffic must travel along the same static path, a failure anywhere along the path causes the connection to fail.

Static reservation of network resources - A guaranteed rate of throughput requires the commitment of resources that cannot be shared by other network users. Unless full, uninterrupted throughput is required for the communication, bandwidth is not used efficiently.

Connection-oriented services are useful for transmitting data from applications that are intolerant of delays and packet re-sequencing. Voice and video applications are typically based on connection-oriented services.

Keypoints: Positive acknowledgement requires packets to be retransmitted if an acknowledgement is not received by the time a timer expires.

Connectionless-orientated

Connectionless communication is supported by UDP on port 17. It is not guaranteed and acknowledgements are NOT sent or received. It is faster than connection orientated. It is up to the application or higher layers to check that the data was received.

Connectionless network service does not predetermine the path from the source to the destination system, nor are packet sequencing, data throughput, and other network resources guaranteed. Each packet must be completely addressed because different paths through the network might be selected for different packets, based on a variety of influences. Each packet is transmitted independently by the source system and is handled independently by intermediate network devices. Connectionless service offers two important advantages over connection-oriented service:

Dynamic path selection - Because paths are selected on a packet-by-packet basis, traffic can be routed around network failures.

Dynamic bandwidth allocation - Bandwidth is used more efficiently because network resources are not allocated bandwidth that they are not going to use. Also, since packets are not acknowledged, overhead is reduced.

Connectionless services are useful for transmitting data from applications that can tolerate some delay and re-sequencing. Data-based applications are typically based on connectionless service.

Keypoints: Bandwidth requirement is reduced because packets are not acknowledged in a connectionless environment.

Data Link and Network Addressing

MAC addresses - Uniquely identifies devices on the same medium. Addresses are 48 bits in length and are expressed as 12 hexadecimal digits. The first 6 digits specify the manufacturer and the remaining 6 are unique to the host. No two MAC addresses are the same in the world. Ultimately all communication is made to the MAC address of the card. Protocols such as ARP and RARP are used to determine the IP to MAC address relationship. MAC addresses are copied to RAM when a network card is intialized.

Data Link addresses - Addresses that operate at the data link layer. A MAC address is a data link layer address and these are built in by the manufacturer and cannot usually be changed. They can be virtualized for Adapter Fault Tolerance or HSRP. Switches and Bridges operate at the Data Link layer and use Data Link addresses to switch/bridge.

Network addresses - Addresses that operate at the Network Layer. These are IP addresses or IPX addresses that are used by Routers to route packets. Network addresses are made up of two parts, the Network ID and the Host ID. IP addresses are 32 bit dotted decimal numbers. IPX addresses are 80 bit dotted hexadecimal numbers. Network addresses are host specific and one must be bound to each interface for every protocol loaded on the machine. There is no fixed relationship between the host and the Network Address. For example, a router with three interfaces, each running IPX, TCP/IP, and AppleTalk, must have three network layer addresses for each interface. The router therefore has nine network layer addresses.

Keypoints: MAC addresses uniquely identify devices on the same medium.
MAC addresses consist of 48 bit hexadecimal numbers.
IP addresses are 32 bit dotted decimal numbers.
MAC addresses are copied into RAM when the network card initializes.

Why a Layered Model?

Standardizing hardware and software to follow the 7 layers of the OSI Model has several major benefits:

1) It reduces complexity
2) Allows for standardization of interfaces
3) Facilitates modular engineering
4) Ensures interoperability
5) Accelerates evolution
6) Simplifies teaching and learning

Data Encapsulation

Data encapsulation is the process in which the information in a protocol is wrapped, or contained, in the data section of another protocol. In the OSI model each layer encapsulates the layer immediately above it as the data flows down the protocol stack. The encapsulation process can be broken down into 5 steps.

At a transmitting device, the data encapsulation method is as follows;

	Action	OSI Model	Keyword
1	Alphanumeric input of user is converted to data.	Application/Presentation/Session	DATA
2	Data is converted to segments.	Transport	SEGMENTS
3	Segments are converted to Packets or Datagrams and network header information is added.	Network	PACKETS
4	Packets or Datagrams are built into Frames.	Data Link	FRAMES
5	Frames are converted to 1s and 0s (bits) for transmission.	Physical	BITS

Keypoints: Encapsulation is the process of adding header information to data. Be very familiar with the above 5 steps of data encapsulation and the order in which they occur.

Flow Control

Flow control is a function that prevents network congestion by ensuring that transmitting devices do not overwhelm receiving devices with data.

There are a number of possible causes of network congestion. Usually it is because a high-speed computer generates data faster than the network can transfer it, or faster than the destination device can receive and process it.

There are three commonly used methods for handling network congestion:

- Buffering
- Source Quench Messages
- Windowing

Buffering - Buffering is used by network devices to temporarily store bursts of excess data in memory until they can be processed. Occasional data bursts are easily handled by buffering. However, buffers can overflow if data continues at high speeds.

Source Quench Messages - Source quench messages are used by receiving devices to help prevent their buffers from overflowing. The receiving device sends a source quench message to request that the source reduce its current rate of data transmission.

Windowing - Windowing is a flow-control method in which the source device requires an acknowledgement from the destination after a certain number of packets have been transmitted.

1. The source device sends a few packets to the destination device.
2. After receiving the packets, the destination device sends an acknowledgment to the source.
3. The source receives the acknowledgment and sends the same amount of packets.
4. If the destination does not receive one or more of the packets for some reason (such as overflowing buffers), it does not send an acknowledgment. The source will then retransmits the packets at a reduced transmission rate.

Windowing is very reliable because it uses positive acknowledgement. Positive acknowledgement requires the recipient device to communicate with the sending device, sending back an acknowledgement when it receives data. If the sending device does not receive an acknowledgement it knows to retransmit the packets at a reduced transmission rate. It the receiving device sends a packet with a zero window size, it means it's buffers are full and it cannot receive any more data. Transmission is resumed when the receiving device sends a packet with a window size higher than zero.

Keypoints: Data arriving faster than the device can handle are stored in memory.
Flow control is maintained by the receiving device sending Receive ready/not ready messages to the transmitting device.
Know that a zero window size means to stop transmitting packets.
If a sending device does not receive any acknowledgement at all, it will retransmit the last packets at a reduce rate.
Positive acknowledgement requires a recipient to communicate with the sending device by returning an acknowledgement.

CISCO IOS

The CISCO Internetwork Operating System (IOS) is the operating system software that comes with all CISCO routers.

IOS Router Modes

The IOS interface provides for 6 basic modes of operation.

MODE	Description	Access	Command Prompt
User EXEC Mode	Provides for limited examination of router information.	Default mode at login	**Router>**
Privileged EXEC Mode	Provides detailed examination, testing, debugging and file manipulation	Type **enable** at command prompt	**Router#**
Global Configuration Mode	Allows you to change high level router configuration	Type **config t** at Priv mode prompt	**Router(config)#**
ROM Monitor Mode	Automatic if the IOS does not exist or the boot sequence is interrupted	N/A	**> or rommon>**
Setup Mode	Prompted dialog that helps you setup router configuration	Type **setup** at Priv mode prompt	**Will display a series of questions.**
RXBoot Mode	Helper software that helps the router boot when it cannot find the IOS image in FLASH	N/A	**Router<boot>**

Global Configuration Mode

The Global configuration mode also allows you access to more specific router configuration modes. The 2 primary ones you should know about are the Interface and Subinterface modes.

Router(config-if)# - The Interface configuration mode is entered by typing the word **Interface** at the Global configuration prompt.

Router(config)# interface <interface type and number>

Router(config-subif)# - is a variation on the Interface command and can be access as shown below. This lets you divide any interface into smaller virtual interfaces.

Router(config)# interface <interface type and number>.<subinterface-number>

Logging in

When you first log into a router you are prompted with:

Router>

This is called User EXEC mode and only contains a limited feature set.

When in User mode, entering the command **enable** and the password, will put you in Privileged EXEC Mode. This will give you the following prompt:

Router#

From this mode you can now use all of the available commands and enter Global Configuration Mode.

Keypoints: Typing “enable” at the user mode prompt will let you enter Privileged EXEC mode.

Context Sensitive Help

The IOS has a built in Context-sensitive help. The main tool is the **?** symbol. If you are unsure of what a command or the entire syntax for a command should be, type in a partial command followed by a **?** and the help facility will provide you with the available options.

To list all commands available for a particular command mode:

Router> ?

To list a command's associated arguments:

Router> command ?

To list a keyword's associated arguments:

Router> command argument ?

Keypoints: To find out the complete syntax for a particular command, you would enter the first few characters of a command and followed immediately by a ? with no space. Example would be "cl?". This would return a list of all commands that start with "cl".

If you want to find out the arguments that can be used with a command, then you would type the command followed by a space and a ?. Example would be "clock ?". This would yield all the arguments that can be used with the "clock" command.

Command History

The IOS user interface provides a history or record of commands that you have entered. This feature is particularly useful for recalling long or complex command entries. By default, the system records the 10 most recent command lines in its history buffer.

To display the entries in the history buffer:

show history

To change the number of command lines recorded during the current terminal session use the following command:

terminal history <size number-of-command lines>

To configure the number of command lines the system records by default, enter the following command line in configuration mode:

history <size number-of-command lines>

Keypoints: To display the contents of the history buffer, you would use the "show history" command.

Editing Commands

Ctrl-W - Erases a word
Ctrl-U – Erases a line
Ctrl-A – Moves the cursor to the beginning of the current line

Ctrl-E – Moves the cursor to the end of the current line
Ctrl-F (or right arrow) – Move forward one character
Ctrl-B (or left arrow) – Move back one character
Ctrl-P (or up arrow) – Recall commands in the history buffer starting with the most recent command.
Ctrl-N (or down arrow) – Return to more recent commands in the history buffer after recalling commands with Crtl-P or the up arrow key.
ESC+B – Move backward one word
ESC+F – Move forward one word
Ctrl-Z – Ends Configuration Mode and returns to the Privileged EXEC Mode.
TAB Key – Finished a partial command

Keypoints: Know the above listed editing keystrokes and what they do. Especially the common ones like Ctrl+Z and Ctrl+A.

Router Elements

RAM

This is the working area for the Router. It contains Routing Tables, ARP Cache, IOS, etc. It also holds the Routers Running-Config file. The contents of RAM are lost when you power down.

show version — To view info about IOS in RAM
show processes — To view info about programs in RAM
show running-configuration — To view the active configuration file
show memory / show stacks / show buffers — To view tables and buffers

NVRAM

Non-Volatile RAM stores the routers startup-config file. NVRAM contents are retained when you power down or reload.

show startup-configuration - To view the contents

FLASH

Flash is an EPROM. Flash memory holds the operating system image (IOS). Having Flash allows you to update software without removing or adding chips. Flash content is retained when you power down or reload. Multiple copies of IOS can be stored in Flash memory.

show flash - To view the contents

ROM

ROM contains the power on diagnostics, a bootstrap program and operating system software. To perform upgrades the physical chips must be removed and replaced.

CDP

Cisco Discovery Protocol is a proprietary protocol to allow you to access configuration information on other routers and switches with a single command. It uses SNAP at the Data-Link Layer. By default CDP sends out a broadcast every 60 seconds and it holds this information for 180 seconds. CDP is enabled by default.

CDP is enabled globally by entering global config mode and typing:

```
Router(config)# cdp run
```

CDP is disabled on a specific interface by entering the interface configuration mode and typing:

```
Router(config-if)# no cdp enable
```

At the Interface config mode you can only enable or disable CDP. At the global config mode you can also set the holdtime and timer. For Example:

```
Router(config)# cdp timer 30
Router(config)# cdp holdtime 120
```

When CDP is enabled you can view details of other Cisco devices by typing:

```
show cdp neighbors
```

This displays the following information about neighboring router's:

1) router's hostname
2) hardware platform
3) port identifiers
4) capabilities list
5) version information
6) up to one address for each protocol supported.

To delete the CDP table of information about neighbors type:

```
clear cdp table
```

***Keypoints: Know the 6 pieces of information that are provided by CDP.**
CDP can be disabled on an interface by using the "no cdp enable" command.*

Managing Configuration Files

Router configuration information can be generated by several means. From privileged EXEC mode you can enter the configure command to configure the running configuration from either a Terminal (Console), Memory (NVRAM), or Network (TFTP)

config term – Allows you to configure manually from the console terminal.
config mem – Loads the configuration file from NVRAM, same as copy startup running.
config net – Loads the configuration from a TFTP server, same as copy TFTP startup

You can also use the copy command:

copy running-config startup-config — Copies the running config (RAM) to the Startup config (NVRAM). Used after real time changes via config term have been made that require to be saved.

copy startup-config running-config — Copies startup configuration from NVRAM into RAM where it becomes the running configuration.

copy running-config tftp — Makes a backup of the running config file to a TFTP server.
copy tftp running-config — Loads configuration information from a TFTP server.
copy tftp startup-config — Copies the config file from the TFTP server into NVRAM.

Keypoint: Know what the above 5 copy commands do.

To use a TFTP server you must specify the TFTP server's hostname or IP address and the name of the file.

To view the configuration in NVRAM:

```
show startup-config
```

To view the current running configuration:

```
show running-config
```

To re-execute the configuration commands located in NVRAM:

```
configure memory
```

To erase the contents of NVRAM:

```
erase startup-config
```

Keypoints: If NVRAM is erased or corrupted and a new IOS is reloaded, the router will start in setup mode.

Passwords, Identification, and Banners

Passwords

There are five different password that can be used when securing your Cisco Router; Enable Secret, Enable Password, Virtual Terminal Password, Auxiliary Password, and Console Password.

Enable Secret - This is a cryptographic password which has precedence over the *enable password* when it exists. Can be set up during setup mode or from global config.

```
Router(config)# enable secret <password>
```

This is the Password required to enter Priv EXEC mode.

Enable Password - Used when there is no Enable Secret or when you are using older software. Can be set up during setup mode or from global config.

```
enable password <password>
```

The enable and enable secret password cannot be the same.

Virtual Terminal Password - Used for Telnet sessions to the Router. Must be specified or you will not be able to log in to the router. Can be set up during setup mode or from global config.

```
line vty 0 4
login
password <password>
```

Sets the telnet login password. Line vty 0 4 specifies the number of Telnet sessions allowed in the router.

Auxiliary Password - Used for connections via the Aux port on the Router**.**

```
line aux 0
login
password <password>
```

Console Password - Used for connections via the console port on the Router.

```
line con 0
login
password <password>
```

Keypoints: Know the 5 types of passwords that control access to a Cisco router.

Router Identification

The Router can be assigned a name by entering the following command at the global config prompt:

```
Router(config)# hostname <router name>
```

If no name is entered, the default name ”Router” will be used.

You can give each interface a description to help identify the interface. This is done in interface configuration mode by typing.

```
Router(config-if)# description <description name>
```

This will label the interface with the string you enter.

Banners

You can configure a message of the day (MOTD) banner on your router to be displayed on all connecting terminals. This done by entering the *banner motd* command in the global configuration mode.

```
Router(config)# banner motd #< message>#
```

The # sign is any delimiting character you choose to use. The message part of the command must begin and end with the same delimiting character.

To specify a banner used when you have an incoming connection to a line from a host on the network, use the *banner incoming* global configuration command. The no form of this command deletes the incoming connection banner.

```
Router(config)# banner incoming #< message>#
Router(config)# no banner incoming
```

An incoming connection is one initiated from the network side of the router. Incoming connections are also called reverse Telnet sessions. These sessions can display MOTD banners and INCOMING banners. Use the no motd-banner line configuration command to disable the MOTD banner for reverse Telnet sessions on asynchronous lines.

Keypoints: Message of the day banners are displayed at login.

IOS Startup Commands

Upon boot the Router runs a POST check on the Hardware, finds and loads the IOS software, finds and loads the startup-config file. If no valid startup-config file exists the router enters setup mode.

EXEC command:

```
Router> reload                          (reboot Cisco)
```

ROM monitor commands:

```
rommon> boot                            (boots from ROM - usual default)
rommon> boot flash                      (boots from flash)
rommon> boot filename ip address  (boots via tftp)
```

Global Configuration commands:

```
Router(config)# boot system flash                       (boots from flash)
Router(config)# boot system rom                         (boots from ROM - usual default)
Router(config)# boot system tftp < filename> <IP address> (boots via tftp)
```

Keypoints: To have the router obtain its boot image from the TFTP Server, you would use the "boot system tftp" command.
To load the boot image from ROM, you would use "boot system ROM".

Setup Command

The setup mode is either manually started by entering **Router# setup** or by booting a server with no valid startup-config file in NVRAM. Basically, setup mode asks you questions to set up the router, such as hostname, passwords and IP addresses for interfaces. You are presented with the script at the end before it is applied. It is then copied to NVRAM and becomes the startup-config and running-config file on the Router.

The Command Line Interface (CLI) allows you to make very detailed changes to your configurations. However, some major configuration changes do not require the detail provided by CLI. In these cases, you can use the setup command facility to make major enhancements to your overall configuration. Additionally, if you are not familiar with Cisco products and CLI, the setup command facility is a particularly valuable tool because it asks you the questions required to make configuration changes.

When you enter the setup command facility after first-time startup, an interactive dialog called the System

Configuration Dialog appears on the system console screen. The System Configuration Dialog guides you through the configuration process. It prompts you first for global parameters and then for interface parameters. The values shown in brackets next to each prompt are the default values last set using either the setup command facility or the configure command. The prompts and the order in which they appear on the screen vary depending on the platform and the interfaces installed on the device.

You must run through the entire System Configuration Dialog until you come to the item that you intend to change. To accept default settings for items that you do not want to change, press the Return key.

To return to the privileged EXEC prompt without making changes and without running through the entire System Configuration Dialog, press Ctrl-C.

WAN Protocols

Connection Terms

Customer Premises Equipment (CPE) - Devices physically located at the WAN subscribers premises. Includes both owned and leased devices.

Central Office (CO) - A switching facility the provides the nearest point of presence for a providers WAN service.

Demarcation (Demarc) - The point at which the CPE ends and the local loop portion of the service begins. Usually the telecommunications closet at the subscriber’s location.

Local Loop - Cabling that extends from the Demarc to the CO.

Data Terminal Equipment (DTE) - Usually the router where the packet switching application resides.

Date Circuit-terminating Equipment (DCE) - The device used to convert the user data from the DTE into an acceptable WAN protocol. This usually consists of a DSU/CSU device, modem, or NT1 device.

Keypoints: Know the definitions of the connection terms listed above.

Frame Relay

Frame relay is a fast WAN protocol that operates at the Physical and Data Link layers (mostly Data Link layer) of the OSI model. Works between DTE and DCE devices. Uses Packet Switching. DTE consists of terminals, PC’s, routers and bridges, all of which are customer owned end node devices. DCE devices such as packet switchers are owned by the service provider. Frame Relay uses Permanent Virtual Circuits (PVCs). The connection is identified by a Data Link Connection Identifier (DLCI).

Frame Relay offers a speeds between 56kbps and 2,078Mbps. However, the default setting for a serial DCE interface is T1. Frame Relay uses a CRC, bad packets are discarded and the receiving station requests re-transmission of any missing frames.

Data Link Connection Identifiers (DLCI) - Used to identify the virtual circuits. DLCIs can be set to a number between 16 and 1007.

Local Management Interfaces (LMI) - Provide information about the DLCI values and the status of virtual circuits. The default is Cisco but there are 3 possible settings:

- Cisco (Default)
- Ansi
- Q933a

To set up frame relay on an interface just set the encapsulation to frame-relay. Frame relay encapsulation can either be Cisco (Default) or IETF. You must use Cisco encapsulation to connect two Cisco routers or IETF if a third party router is involved. Frame Relay configuration is done in the interface configuration mode.

```
Router(config-if)# encapsulation frame-relay <cisco or ietf>
```

To assign a DLCI to an interface you would type.

```
Router(config-if)# frame-relay interface-dlci <number 16-1007>
```

To set the LMI type you enter:

```
Router(config-if)# frame-relay lmi-type <cisco/ansi/q933a>
```

A keepalive interval must be set to enable LMI on an interface. This is 10 seconds by default and can be set by typing:

```
Router(config-if)# frame-relay keepalive <number of seconds>
```

The Frame Relay Map tells the network protocol how to get from a specific protocol and address pair to the correct DLCI. There are two ways to make this happen, you can use the frame-relay map command or you can use the inverse-arp function. The “frame-relay map” command can be used to show which routers are reachable.

```
Router(config-if)# frame-relay inverse-arp <protocol> <dlci>
Router(config-if)# frame-relay map <protocol> <protocol address> <dlci> broadcast <cisco or ietf>
```

With frame-relay you can use subinterfaces to allow multiple virtual circuits on a single serial interface and each subinterface can be treated as a separate interface. You use the interface s0.interface number command:

```
Router(config-if)# interface s0.<subinterface number> <point-to-point or multipoint>
```

You can configure subinterfaces to support the following connection types:

Point-to-point - A single subinterface is used to establish one PVC connection to another physical interface on a remote router. Each interface would be on the same subnet and have a single DLCI. Each point-to-point connection is its own subnet and act like a leased line.

Multipoint - A single subinterface is used to establish multiple PVC connections to multiple physical interfaces on a remote router. All participating interfaces are in the same subnet and each interface would have it’s own DLCI. The subinterface acts like a NBMA network and broadcasts are subject to split horizon rules.

It is worthwhile creating a subinterface with a number that matches the DLCI identifier.

Keypoints: DLCIs are used to distinguish between PVCs.
Frame Relay operates at the Data Link and Physical layers.
You can use the "show interface" command to display the LMIs and DLCIs on a frame relay enabled interface.
The default bandwidth setting for a serial DCE interface is T1 (1.544Mbps).
Know what command is used to configure a subinterface.
Know that multipoint specifies that a frame relay subinterface is configured as a single subnet.

Monitoring Frame Relay

show frame-relay ip	- Shows frame relay ip statistics
show frame-relay lmi	- Shows LMI statistics
show frame-relay map	- Shows map table
show frame-relay pvc	- Shows PVC Statistics Also DLCI Info
show frame-relay route	- Shows frame relay routes
show frame-relay traffic	- Shows protocol statistics

The *Show Interface* command also shows Frame Relay information on a specific interface. The *show ip route* command will also show which routers are reachable.

Keypoints: The "show frame-relay map" command and the "show ip route" command can be used to show which routers are reachable.

ISDN

Integrated Services Digital Network (ISDN) is a digital service designed to run over existing telephone networks. ISDN can support both data and voice simultaneously. ISDN encompasses the OSI Physical, Data Link, and Network Layers.

ISDN networking can provide up to 128Kbps with a PPP Multilink connection to corporate networks or the Internet. A Basic Rate Interface (BRI) connection can also be used as a backup line in case the primary link goes down. In this case you have to set the desirability of the ISDN link to be very low. In other words only use if there is no other way.

ISDN has the following benefits over standard telephone connections:

1) Data transfer is faster than typical modems
2) Call setup is faster
3) ISDN can carry voice, video, and data traffic

ISDN Protocols

These protocols deal with ISDN issues:

- **E** – Specifies ISDN on the existing telephone network.
- **I** – Specifies Concepts, terminology, and Services.
- **Q** – Specifies switching and signaling.

ISDN Function Groups

Devices connected to the ISDN network are known as terminals and have the following types:

- **TE1** – Terminal Equipment type 1 understands ISDN standards. Like a BRI Interface on a router.
- **TE2** – Terminal Equipment type 2 predates ISDN standards. To use a TE2, you must have a Terminal Adapter (TA).

ISDN Reference Points

ISDN uses four different reference points to define logical interfaces. They are as follows:

- **R** – Defines the reference point between non ISDN equipment and a TA
- **S** – Defines the reference point between user terminals and an NT2
- **T** – Defines the reference point between NT1 and NT2 devices
- **U** – Defines the reference point between NT1 devices and Line Termination Equipment. (North America Only)

> ***Keypoints: Your router will always be connected by the U interface into NT1.***
> ***The BRI interface on your router is considered Terminal Equipment type 1 (TE1).***
> ***Know the 3 benefits of ISDN over standard telephone service.***

ISDN Channels

ISDN can either be Basic Rate ISDN (BRI) or Primary Rate ISDN (PRI).

BRI is 2 64Kbps B Channels for data and one 16Kbps D Channel for link management and connects to NT1 for 4-wire connection.
PRI is 23 B Channels and 1 D Channel in the US or 30 B Channel and 1 D Channel in Europe.

Occasionally when configuring ISDN you will need to configure a Service Profile ID (SPID). A SPID is a series of characters which can look like phone numbers. These numbers will identify your connection to the Switch at the CO. The SPIDs are processed during each call setup operation.

> ***Keypoints: Total bandwidth for a BRI connection is 144 Kbps (64+64+16) and connects to NT1 for 4-wire connection.***
> ***A SPID is a series of characters that identifies you to a switch at the CO.***

Cisco's ISDN Implementation

Cisco implements BRI using a BRI RJ45 interface on a router enabled as a TE1 device.

HDLC

The High Level Data Link Control Protocol is a link layer protocol that is the standard encapsulation type for Cisco Serial interfaces. It is a bit-oriented synchronous data link layer protocol developed by ISO. Derived from SDLC, HDLC specifies a data encapsulation method on synchronous serial links using frame characters and checksums.

PPP

Point-to-Point Protocol. A successor to SLIP, PPP provides router-to-router and host-to-network connections over synchronous and asynchronous circuits. This data link protocol can be used over either asynchronous (dial-up) or synchronous (ISDN) media. It uses the Link Control protocol (LCP) to maintain the data link. It has a number of features, including Authentication using either PAP or CHAP and compression.

PPP is enabled at the Interface configuration mode by typing:

```
Router(config-if)# encapsulation ppp
```

There are then several sub PPP commands such as authentication, multilink, compression, and callback.

The *Show Interface* command lists the encapsulation method on an interface. Also *Show Running-Config* displays the PPP commands allocated to an interface.

***Keypoints: PPP compression is handled by the Link Control Protocol (LCP).**

Network Protocols

Network Addresses

There are two parts to every Network address. These are the Network ID and the Host ID. In TCP/IP, this is decided by the address class and the subnet mask. In IPX/SPX, the first 8 hex digits represent the network ID and the remaining 12 hex digits represent the host ID (the MAC address).

Routers and other internetworking devices require one network layer address per physical network connection for each network layer protocol supported. For example, a router with three interfaces, each running AppleTalk, TCP/IP, and IPX, must have three network layer addresses for each interface. The router therefore has nine network layer addresses.

TCP/IP

IP Addressing Fundamentals

A host or node is a computer or device on a TCP/IP network. Every TCP/IP host is uniquely identified by its IP address. An IP address consists of a network ID and a host ID. If two different hosts belong to the same network, they have the same network ID. The two hosts will have different host ID's and can communicate with each other locally without going through a router. If two hosts have different network ID's, they belong to different segments on the network. They must communicate with each other remotely through a router or default gateway.

An IP address consists of 32 binary bits, where each bit is either a 0 or 1. We write the 32 bits into four 8-bit numbers (octets) separated by a periods.

For Example: 11000001 . 00001010 . 00011110 . 00000010 (IP address in binary form)

To convert the IP address from binary to decimal form, we convert each of the four 8-bit numbers in each octet according to the following table:

Decimal Value	128	64	32	16	8	4	2	1
Octet Value	x	x	x	x	x	x	x	x

So the first octet in the above binary number would be translated as:

Decimal Value	128	64	32	16	8	4	2	1
Octet Value	1	1	0	0	0	0	0	1

Everywhere a 1 appears in the table, the decimal value in that column is added to determine the decimal value of the entire octet.

or 128 + 64 + 1 = 193

Using the same table to translate the other three octets would give us the following result.

00001010 = 8 + 2 = 10

00011110 = 16 + 8 + 4 + 2 = 30

00000010 = 2

So in decimal form, the above IP address is: 193 . 10 . 30 . 2

Address Classes

An IP address consists of two parts, one identifying the network and one identifying the host. The Class of the address determines which part is the network address and which part is the host address.

There are 5 different address classes. Classes can be distinguished by the decimal notation of the very first octet. The following Address Class table illustrates how you can determine to which class and address belongs.

CLASS	FIRST OCTET	NETWORK ID	DEFAULT SUBNET MASK	AVAILABILITY
A	1-126	First Octet	255.0.0.0	AVAILABLE
B	128-191	First 2 Octets	255.255.0.0	AVAILABLE
C	192-223	First 3 Octets	255.255.255.0	AVAILABLE
D	224-239	N/A	N/A	RESERVEDFOR MULTICASTING
E	240-255	N/A	N/A	RESERVED

Note: 127 is reserved for loopback (127.0.0.1) and is used for internal testing on the local machine.

Using this table we can see the IP address in our above example is a Class C address. We can also see which part of that IP address is the Network ID and which is the Host ID.

Network ID: (First 3 Octets) = 193.10.30
Host ID: (However many Octets are left) = 2

Whenever you want to refer to your entire network with an IP address, the host section is set to all 0's (binary=00000000) = 0. For example 193.10.30.0 specifies the network for the above address. When the host section is set to all 1’s (binary=11111111) = 255, it specifies a broadcast that is sent to all hosts on a network. 193.10.30.255 specifies a broadcast address for our example IP address.

Keypoints: Know the range of IP address classes and their default subnet mask.
Class A IP addresses allow the most number of hosts.
Class C IP addresses allow the fewest number of hosts.

Subnetting

Subnetting is the process used to divide the total available IP addressed (hosts) for your Network into smaller subnetworks (subnets). For example, the Network ID we used in the discussion above (193.10.30.0). This network would consist of 256 possible IP addresses (193.10.30.0 - 193.10.30.255). We know this because in a Class C address, only the last octet is available for host IDs (0000000 - 11111111) or (0-255). Since 0 is used to identify the whole network and 255 is reserved for broadcasts, that leaves us with 254 possible hosts (193.10.30.1 - 193.10.30.254).

Suppose we wanted to divide those 254 addresses up into 6 smaller subnets. This can be done by using what is referred to as a Subnet Mask. By looking at the above table we can see Class C addresses all have a default subnet mask of 255.255.255.0. Since the last octet of the subnet mask is 0, it means that the host IDs have not been subdivide into smaller subnets. However, if we choose to divide our network into a few smaller segments (subnets), then we would change the default subnet mask by replacing the last octet with one of the valid subnet masks.

On the exam you will be asked to calculate subnet masks, valid ranges within a subnet, number of subnets possible and number of hosts possible. If you memorize the 2 tables below, you should have no problem answering any of these questions.

Class B Addresses

# of bits	Subnet mask	Subnets	Hosts	Range
2	255.255.192.0	2	16,382	64
3	255.255.224.0	6	8190	32
4	255.255.240.0	14	4094	16
5	255.255.248.0	30	2046	8
6	255.255.252.0	62	1022	4
7	255.255.254.0	126	510	2
8	255.255.255.0	254	254	1
9	255.255.255.128	510	126	128
10	255.255.255.192	1022	62	64
11	255.255.255.224	2046	30	32
12	255.255.255.240	4094	14	16
13	255.255.255.248	8190	6	8
14	255.255.255.252	16,382	2	4

Class C Addresses

# of bits	Subnet mask	Subnets	Hosts	Range
2	255.255.255.192	2	62	64

3	255.255.255.224	6	30	32
4	255.255.255.240	14	14	16
5	255.255.255.248	30	6	8
6	255.255.255.252	62	2	4

Here’s how it works.

QUESTION: If you have a class B IP network with a 10-bit subnet mask, how many subnets and hosts can you have?

ANSWER: 1022 subnets with 62 hosts (*just look on the table for this answer)*

QUESTION: You have an IP address of 172.16.13.5 with a subnet mask of 255.255.255.128. What is your network ID and what range is the range of addresses in this subnet.

ANSWER: Network ID is 172.16.13.0, range is 172.16.13.1 - 172.16.13.126

(Since you are subnetting all 8-bits in the 3rd octet, the number in the 3rd octet becomes part of your network ID. By looking at the table you see you have 126 hosts in each subnet. You also see the address range for each subnet is 128. Since the 0 is you network address and 127 is your broadcast address, the valid range of hosts addresses in this subnet is 172.16.13.1 - 172.16.13.126 = 126).

QUESTION: You have a subnet mask of 255.255.255.248 in a class B network. How many subnets and hosts do you have?

ANSWER: 8190 subnets, each with 6 hosts.

QUESTION: If you have a Class C network with a 6-bit subnet mask, how many subnets and hosts do you have?

ANSWER: 62 subnets, each with 2 hosts.

QUESTION: You have an IP address of 172.16.3.57 with an 11-bit subnet mask. What is the Network ID, range of subnet addresses, and Broadcast address for this subnet?

ANSWER: Network ID = 172.16.3.32 = 1
Host Ids = 172.16.3.33 - 172.16.3.62 = 30
Broadcast Address = 172.16.3.63 = 1
32

By looking at the table above, you can see that a class B address with an 11 bit subnet mask has a RANGE of 32 with 30 HOSTS. Since this is a class B address we know that the first 2 octets are the original Network ID (172.16.0.0). Since we are subnetting all 8-bits of the 3rd octet, then the 3rd octet automatically becomes part of our Subnetwork ID (172.16.3). We know by the table that an 11-bit subnet mask will have 30 hosts and 32 addresses in each range. Since we are subnetting more than 8-bits, the four octet of our subnet will always begin with 0. So the first 32 Ip address available to us in 172.16.3 are 172.16.3.0 - 172.16.3.31. Our given IP address (172.16.3.57) is not in this range. The next range of 32 IP addresses is 172.16.2.32 - 172.16.3.63. Bingo…..This is the subnet we are looking for. We know that the first address in the subnet range is always the Network ID (172.16.3.32). The next 30 are all valid hosts (172.16.3.33 - 172.16.3.62). The remaining address (172.16.3.63) is our broadcast address.

QUESTION: You have a class C network address of 192.158.17.0. You need the largest possible number of subnets with up to 12 hosts on each. Which subnet mask would you use?

ANSWER: 255.255.255.240 (*look at the table)*

QUESTION: You have a Network ID of 172.191.0.0. with 8 subnets. You need to allow for the largest possible number of hosts per subnet. Which subnet mask would you use?

ANSWER: 255.255.240.0 *(look at the table)*

Keypoints: We highly recommend you quickly draw the above IP tables when you first enter the testing room. Your are going to have to know this information. For the Class B table, the key is to memorize the first two columns (# of bits and subnet mask. For the 3rd column (Subnets) you just have to memorize the "2" in the first row. After that you can just use the formula (previous number x 2 + 2 = next entry). For example, the next row would be 2 x 2 + 2 = 6. The fourth column is easy, it is just the inverse or opposite of the 3rd column. Turn the 3rd column upside down and you have the forth column. The fifth column (Range) is pretty easy also. Just remember that the first row is "64". Then as you go down the column use the formula (previous number divided by 2) until you get to the "1". Then start over again with "128" and divide by 2 again as you go down the column.

Enabling IP Routing

IP routing is enabled by default on Cisco routers. To enable IP on an interface, you have to be in the interface configuration mode:

Router(config-if)# ip address <IP address><Subnet Mask>

Add static IP routes with:

```
ip route <network> <mask> <address | interface > <admin distance>
ip default-network <network>
```

The following commands can be used to monitor you IP information:

```
show ip protocol
show ip route
show ip interfaces
```

Keypoints: IP routing is enabled by default on the Cisco routers.
Enable IP on an interface by assigning an IP address to that interface as demonstrated above.
Know how to configure an IP static route.

Configuring IP addresses

To configure an IP address you have to enter the following command at the interface config prompt:

```
        Router(config-if)# ip address <IP address> <subnet mask>
```

Verifying IP addresses

IP addresses can be verified by either using Telnet, ping, or trace.

Telnet - verifies the application-layer software between source and destination stations. This is the most complete test mechanism available.
Ping - Uses the ICMP protocol to verify the hardware connection at the logical address of the network layer.
Trace - Uses Time-To-Live (TTL) values to generate messages from each router used along the path. This is very powerful in its ability to locate failures in the path from the source to the destination.

Keypoints: Ping, Telnet and Trace can all be used to verify network connectivity. This is accomplished by typing the command followed by the complete IP address or host name.

TCP/IP transport layer protocols

TCP/IP uses the DOD Model which is :

Process Application	- Maps to Application, Presentation, Session
Host to Host	- Maps to Transport
Internet	- Maps to Network
Network Access	- Maps to Data Link and Physical

TCP/IP Transport Layer (OSI) or Host to Host (DOD) protocols use TCP and UDP.

Transmission Control Protocol - TCP is a connection oriented transport layer protocol with built in reliability. Takes large blocks of data and breaks it down into segments. It numbers and sequences each segment so the destination's TCP protocol can re-assemble back into the original order. TCP uses acknowledgement via sliding windows. Has a large overhead due to built in error checking. This protocol uses Port 6.

User Datagram Protocol - UDP is a connectionless oriented transport protocol for use when the upper layers provide error-recovery and reliability. UDP does not sequence data or re-assemble it into any order after transmission. This protocol uses Port 17.

TCP/IP network layer protocols

TCP/IP Network Layer (OSI) or Internet (DOD) protocols are IP, ARP, RARP, BOOTP, and ICMP.

Internet protocol - IP provides routing and a single interface to the upper layers. No upper layer protocol and no lower layer protocol have any functions relating to routing. IP receives segments from the transport layer and fragments them into packets including the hosts IP address.

Address Resolution Protocol - ARP is responsible for resolving IP addresses to MAC addresses. It stores these in its arp cache for later use. It does this to inform a lower layer of the destination's MAC address.

Reverse Address Resolution Protocol - RARP resolves MAC addresses to IP addresses on diskless workstations.

Boot Strap Protocol - BootP is used also for diskless workstations when it requires an IP address.

Internet Control Message Protocol - ICMP is a management protocol and messaging service provider for IP. Its messages are carried as IP datagrams. ICMP is used in to perform the following functions:

- *Destination Unreachable* **-** If a router cannot send an IP packet any further it uses an ICMP echo to send a message back to the sender notifying it that the remote node is unreachable.

- *Buffer Full* **-** If a routers memory buffer is full ICMP will send out a message to the originator.

- *Hops* **-** Each IP datagram is assigned a path. This consists of hops. If it goes through the maximum number of hops the packet is discarded and the discarding router sends an ICMP echo to the host.

- *Ping* **-** Ping uses ICMP echo messages to check connectivity.

Keypoints: Know the above 4 functions of ICMP.

Novell IPX

Enable IPX protocol

The IPX protocol uses SAP advertisements to update the network servers. IPX addresses are composed of a network number (32 bit number) and a node address (48 bit MAC address) represented by dotted triplets of 4 hexadecimal numbers. Eg. 0000004a.0000.0c00.23fe, where 4a is the network. Leading zeros are not needed. Encapsulation type is optional. The command to enable IPX on the router is:

```
Router(config)# ipx routing
```

To enable IPX on an interface you have to go to the interface configuration mode and type the following command:

```
Router(config-if)# ipx network 4a
```

This adds IPX to the interface and sets the IPX network number to 4a. You do not have to enter an IPX host address as this is assigned as the MAC address of the interface. You can also enter **encap** after the network number to set the encapsulation type. If this is not entered the default frame type for the interface is used.

Subinterfaces can be addressed using:

```
Router(config-if)# int e0.100
```

This causes subinterface number 100 on the Ethernet 0 interface to display.

```
Router(config-subif)# ipx network 4a encap sap
```

This sets the subinterface to IPX network 4a using sap encapsulation which is Ethernet_802.2.

Keypoints: An IPX address consists of a 32bit network number and a 48 bit node number (MAC Address).
IPX will support multiple logical networks on a single interface by using a unique encapsulation type.

IPX address and encapsulation types

Interface Type	IPX Frame Type	Cisco Encapsulation Type
Ethernet	Ethernet_802.3	Novell-ether (Default)
	Ethernet_802.2	Sap
	Ethernet_II	Arpa
	Ethernet_Snap	Snap
Token Ring	Token Ring	Sap (Default)
	Token Ring_Snap	Snap
FDDI	Fddi_Snap	Snap (Default)
	Fddi_802.3	Sap
	Fddi_Raw	Novell-fddi

Monitoring IPX

The following commands are used to monitor your IPX interfaces:

Ping ipx {host address}	Diagnose basic IPX network connectivity.
Show ipx interface {interface}	Displays the status of the IPX interfaces configured on the Router and the parameters configured on each interface.
Show ipx route	List the entries in the IPX routing table.
Show ipx servers	List the servers discovered through SAP advertisements.
Show ipx traffic	Display information about the IPX traffic.
Debug ipx routing activity	Displays routing update packets transmitted and received between routers

Keypoints: IPX uses SAP advertisements to perform network updates.
Know what the above IPX monitoring commands do.

Routing Protocol Types

Distance Vector Concept

Distance vector based routing algorithms pass periodic copies of a routing table from router to router. Regular updates between routers communicate topology changes. Each router receives a routing table from its direct neighbor and increments all learned routes by one.

This is the way that the algorithm learns the internetwork topology, via second hand information. Distance Vector algorithms do not allow a router to know the exact topology of an internetwork.

RIP and IGRP are Distance Vector Routing Protocols.

Distance Vector Topology Changes

When the topology in a distance vector network changes, routing table updates must occur. As with the network discovery process, topology change notification must occur router to router.

Distance Vector protocols call for each router to send its entire routing table to each of its adjacent neighbors. When a router receives an update from a neighboring router, it compares the update to its own routing table. If it learns about a better route (smaller hop count) to a network from its neighbor, the router updates its own routing table.

Problems with Distance Vector

Distance Vector routing protocols are prone to Routing Loops and counting to infinity. Routing loops can occur if the internetwork's slow convergence on a new configuration causes inconsistent routing entries. Counting to infinity continuously loops packets around the network, despite the fundamental fact that the destination network is down.

To over come these you can implement several different options:

- **Defining a maximum number of hops -** Specify a maximum distance vector metric as infinity. 16 with RIP and 256 with IGRP.

- **Split Horizon -** If you learn a protocol's route on an interface, do not send information about that route back out that interface.

- **Route Poisoning -** Information past out on an interface is marked as unreachable by setting the hop count to 16 for RIP

- **Hold Down Timers -** Routers ignore network update information for some period of time.

Keypoints: Know the 4 ways to reduce routing loops (listed above) and what they mean.

Link State Concepts

The Link State Routing algorithm maintains a more complex table of topology information. Routers using a link state routing protocol have a complete understanding and view of the entire network. The Link State algorithm uses Link State Packets (LSP) to inform other routers of distant links. All routers exchange LSP to build a total view of the network. OSPF is a Link State Routing Protocol.

When the topology changes, the first routers to find out sends LSP to all other routers on the internetwork. All routers then re-calculate the best path to any affected route. Link State routing protocols are more intensive in terms of power, memory, and bandwidth required.

Differences between Distance Vector and Link State

- Distance Vector gets all its information second hand or gossip whereas link state routing obtains a total topology of the internetwork.
- Distance Vector determines the best path by counting hops. Links State uses a complex bandwidth analysis.
- Distance Vector updates topology changes every 30 seconds as default which causes a slow convergence time. Link State can be triggered by topology changes resulting in faster convergence times.

Problems with Link State

Link-state (OSPF) needs lots of processing power to rebuild the routing database (tree). Network bandwidth, is another problem. Link-state info can flood the network.

Keypoints: Routers can learn hops dynamically by receiving periodic updates from other routers, or by default routes.

Routing Protocols

Routers can be used to segment networks by routing between two or more interfaces. Broadcasts will be filtered and the packets will be routed based upon the destination network address (IP or IPX). ***Routing*** protocols such as RIP, IGRP, OSPF, etc. are used to route information between routers. These differ from ***Routed*** protocols such as TCP/IP, IPX, AppleTalk, etc.

Multiprotocol Routing

There are 2 types of multiprotocol routing:

Separate - A multiprotocol routing environment in which each protocol is not aware of the other protocols on the same router. RIP and OSPF are separate routing protocols.

Integrated - A multiprotocol routing environment where each protocol is aware of the other protocols and they share the results of the routing algorithm. EIGRP is an integrated routing protocol that integrates support for IP, AppleTalk and IPX using a distance vector algorithm based on IGRP.

RIP

RIP is a distance vector routing protocol that uses hop count as its metric. The maximum hop count is 15 so 16 hops is deemed unreachable. RIP updates are broadcast every 30 seconds by default. RIP is enabled by typing:

```
Router# router rip
```

This puts you in router configuration mode. You then have to associate attached networks with the RIP process. You only associate directly attached networks.

```
Router(config-router)# network <network id>
```

****Keypoints: The "network" command is used in router configuration mode to enable directly connected networks to be used by RIP.***

IGRP

IGRP is a distance vector routing protocol designed by Cisco. The maximum hop count is 255 and it uses a combination of variables to determine a composite metric.

- Bandwidth
- Delay
- Load
- Reliability
- Maximum Transmission Unit (MTU)

IGRP is enabled by typing:

```
        Router# router igrp 12
```

Where 12 is the autonomous system number. You then have to associate directly connected networks in the same way as you did with RIP.

```
network <network id>
```

Keypoints: Enable IGRP routing by using the "router igrp <autonomous system #>" command.

Network Security

Access Lists

Access lists are a list of conditions that control access to a router's interface.

- Each packet is compared with each line of the access list in sequential order.
- Once a match is made it is acted upon and no further comparisons take place.
- There is an implicit deny at the end of each access list.

Access List Numbers to Know

1-99	- IP Standard Access Lists
100-199	- IP Extended Access Lists
800-899	- IPX Standard Access Lists
900-999	- IPX Extended Access Lists
1000-1099	- IPX SAP Access List

Keypoints: Know what numbers apply to which type of access lists.

Standard IP Access List

A standard IP access list analyses the source address of the packet and matches it against the access list. To create an access list in global configuration mode:

```
Router(config)# access-list <number 1-99>  <permit or deny> <source address> <wildcard mask>
```

Wildcard Mask

A wildcard mask is 32 bit, 4 octet, address that can be used on a router to allow you to apply an access list to a specific IP address or a specific range of IP addresses. Here is how it works:

Let say you want to apply an access list 100 to all hosts in the 172.30.0.0 network. Your input on the router would look like this:

```
Router(config)# access-list 100 permit 172.30.0.0  0.0.255.255
```

The wildcard mask will be converted to binary 00000000.00000000.11111111.11111111. A "0" bit tells the router to compare that position of the packets IP address to the source address 172.30.0.0 to see if it matches. If all the "0" bits match, it will apply the access list. If it doesn't, the access list will not be applied to this packet. A "1" bit in the wildcard mask tells the router to ignore this bit of the packets IP address. So all 8 bits of octet 1 (172) and all 8 bits of octet 2 (30) will be compared to any incoming packet. The last 2 octets of the packet are ignored. Therefore any packet beginning with 172.30 will have the access list applied.

Now if you wanted to check only IP addresses in subnets 172.30.16.0 to 172.30.31.0, you would have to manipulate the bits in the wildcard mask to only check the bits unique to those subnets.

To check for only a specific address, you would enter a wildcard mask of 0.0.0.0. This means that every bit of the IP address will be compared to the source IP address you entered for the access list.

Ex: access-list 100 permit 172.30.16.100 0.0.0.0

This will only apply to packets from host 172.30.16.100.

You apply the access list to an interface by entering the interface configuration mode and typing.

Router(config-if)# <protocol> access-group <list number> <out/in>

This applies the access list to all traffic on the selected interface. **Out** means packets leaving the interface and **in** means packets entering the interface.

Extended IP Access Lists

Extended IP access lists operate the same as standard IP access lists but they use the number from 100-199 instead of 1-99. Also more options are available instead of only checking the source address.
You can now specify:

- Source Address
- Destination Address
- IP Protocol (TCP, UDP, ICMP etc…)
- Port Information (www, DNS, ftp, etc..)

Access-list <number 100-199> <permit or deny> <protocol> <source address> <destination address> <operator> <port>

EX: access-list 100 deny tcp 172.18.16.0 0.0.0.255 any eq ftp

The above example will deny any ftp traffic from 172.18.16.x to any destination address.

ANY can be used to specify any source or destination address which is the same as 0.0.0.0 255.255.255.255
HOST can be used to specify a host. Host 172.18.16.2 is the same as 172.18.16.2 255.255.255.255

Extended IP access lists are applied to an interface in the same way as standard IP access lists.

show access-lists - Displays all access lists running on the router.
show ip access-lists - Displays all IP access lists running on the router.
show ip int - Shows the IP interface information and indicates any Outbound or inbound access lists.
sh run - Shows the running config and any access lists that are globally set up and to which interfaces.

****Keypoints: To display the contents of a particular access list, you would use the “show access-list <list #>” command.***

Standard IPX Access Lists

Standard IPX access lists permit or deny packets based upon the source and destination IPX addresses. This differs from IP where it only looks at the source address.

There are no wildcard masks with IPX and you can use either the Node Address or Network Address.

```
Router(config)# access-list 810 permit 4b 5c
```

The above line will only allow packets from network 4b to reach network 5c. These are applied in a similar way to IP from the interface config mode:

```
Router(config-if)# ipx access-group 810 out
```

Extended IPX Access Lists

Extended IPX Access Lists can filter based upon:

- Source Network/Node
- Destination Network/Node
- IPX Protocol (SAP, SPX etc)
- IPX Socket

access-list <number 900-999> <permit/deny> <protocol> <source address> <socket> <destination address> <socket>

Keypoints: If you do not enter the argument "in" or "out" at the end of the access-group command, then "out" is assumed.
You can use the "show interface" command to see if an access list has been enabled on a particular interface.

IPX SAP Filters

IPX Sap Filters are used to filter out SAP broadcasts. They use the number range 1000-1099.

Access-list <number 1000-1099> <permit/deny> <source address> <service type>

```
access-list 1020 permit 3a.0000.0000.0001 0
int e0
ipx input-sap-filter 1020
```

This would allow only the server on IPX network 3a.0000.0000.0001 to be seen by the outside world.
The service type of 0 matches all services.

Local Area Networks (LANs)

Full-Duplex Ethernet – can provide double the bandwidth of traditional ethernet, but requires a single workstation on a single switch port, and the NIC must support it. Collision free because there are separate send and receive wires, and only one workstation is on the segment.

Half-Duplex - must provide for collision detection, therefore can only use 50% of bandwidth available.

Ethernet networks generally operate using broadcasts. This caused problems in older bus networks due to broadcast storms reducing each client's bandwidth. The CSMA/CD contention method also states that only one node can transmit at the same time so the more nodes the lower the actual effective bandwidth for each node.

LAN Segmentation

Bridges - segment LAN's by learning the MAC address of the nodes on each directly connected interface. This helps segment LAN's because the Bridge looks up the destination MAC address in its address table and forwards the frame to the correct interface. Bridges act to increase the number of collision domains. The downside is that frames with unrecognized MAC addresses are forwarded to every interface. Bridges work at the data-link layer or layer 2.

Routers - can be used to segment LAN's via routing between two or more Ethernet interfaces. Broadcasts will be filtered and the packets will be routed based upon the destination network address (IP or IPX). Separates broadcasts and possibly protocols. Each segment is a broadcast domain of it's own and does not pass broadcasts to the adjacent segments. Routers can connect networks that use different media and it works at the network layer or layer 3.

Switches - are advanced multiport bridges that can either segment LAN's or provide total end to end non-contentious bandwidth to clients. They support Full Duplex. VLAN's can be used. Switches work on the MAC address (Data Link Address) in the same way as Bridges but they switch at the hardware level (Wire Speed), whereas a bridge uses software. As a result, switches are much faster layer 2 devices. Switches use either store-and-forward switching or cut-through switching for LAN switching (forwarding) traffic.

Repeaters & Hubs - are both devices that operate at the physical layer of the OSI model. They simply pass data without performing any type of address recognition functionality.

***Keypoints: Routers use IP addresses to forward packets.**
Know which layers of the OSI model the above devices operate in.
Bridges increase the number of collision domains, thus reducing the number of collisions.
Bridges lookup MAC addresses in their address table and forwards the data toward the destination device.

Store-and-Forward Switching

With Store and Forward switching, the switch copies the entire frame into its buffer and computes the CRC. The frame is discarded if a CRC error is detected or if the frame is a runt (less than 64 bytes including the CRC) or a giant (more than 1518 bytes including the CRC). The LAN switch then looks up the destination address in its switching table and determines the outgoing interface. The frame is then sent to the interface. Store-and-Forward switching is standard on Cisco Catalyst 5000 switches.

Latency using Store and Forward switching is dependant upon the frame size and is slower than Cut-through switching.

Cut-Through Switching

With Cut-Through switching, the switch copies only the Destination Address which is the first 6 bytes after the frame preamble into its buffer. The LAN switch then looks up the destination address in its switching table and determines the outgoing interface. The frame is then sent to the interface. A cut-through switch provides reduced latency because it begins to forward the frame as soon as it reads the destination address and determines the outgoing interface.

Keypoints: Know the difference between "Store and Forward" and "Cut-Through" switching.

Fast Ethernet

Fast Ethernet is based on the Ethernet's CSMA/CD contention method but is ten times faster. Because of the slot time used in CSMS/CD networks the total segment distance must also be reduced.

Fast Ethernet Specifications

- **100BaseTX -** 100BaseTX uses a two-pair Category 5 UTP cable with an RJ45 connector and the same pin out as in 10BaseT. 100BaseTX supports full duplex operation. For 100BaseTX using Cat5 UTP with a max distance is 100 Meters

- **100BaseFX -** 100BaseFX uses a two strand fiber cable of which one strand transmits and the other receives. Supports full duplex operation. The max distance is 412 Meters Half Duplex or 2 Kilometers Full Duplex.

- **100BaseT4 -** 100BaseT4 uses four-pair Cat 3, 4, or 5 UTP cabling and RJ45. Allows the use of voice grade cabling to run at 100Mbps.

Fast Ethernet has its advantages due to being ten times faster than 10BaseT and can be used on existing Cat5 cabling using existing Ethernet contention methods. It protects the investment in current cabling and experience.

Spanning Tree Protocol

Spanning-Tree Protocol is a link management protocol that provides path redundancy while preventing undesirable loops in the network. For an Ethernet network to function properly, only one active path can exist between two stations. Multiple active paths between stations cause loops in the network. If a loop exists in the network topology, the potential exists for duplication of messages. When loops occur, some switches see the same stations appearing on both sides of the switch. This condition confuses the forwarding algorithm and allows duplicate frames to be forwarded.

To provide path redundancy, Spanning-Tree Protocol defines a tree that spans all switches in an extended network. Spanning-Tree Protocol forces certain redundant data paths into a standby (blocked) state. If one network segment in the Spanning-Tree Protocol becomes unreachable, or if Spanning-Tree Protocol costs change, the spanning-tree algorithm reconfigures the spanning-tree topology and reestablishes the link by activating the standby path.

Virtual LANs

A VLAN (Virtual Local Area Network) is a switched network that is logically segmented by communities of interest without regard to the physical location of users. Each port on the Switch can belong to a VLAN. Ports in a VLAN share broadcasts. Ports that do not belong to that VLAN do not share these broadcasts thus improving the overall performance of the network. VLANs remove the physical constraints of workgroup communications. Layer 3 routing provides communications between VLANs. In other words users can be in totally different physical locations and still be on the same VLAN. Likewise users in the same physical location can be on different VLANs.

VLANs provide the following benefits:

- **Reduced administration costs from solving problems associated with moves and changes -** As users physically move they just have to be re-patched and enabled into their existing VLAN

- **Workgroup and network security -** You can restrict the number of users in a VLAN and also prevent another user from joining a VLAN without prior approval from the VLAN network management application.

- **Controlled Broadcast activity -** Broadcasts are only propagated within the VLAN. This offers segmentation based on logical constraints.

- **Leveraging of existing hub investments -** Existing hubs can be plugged into a switch port and assigned a VLAN of their own. This segregates all users on the hub to one VLAN.

- **Centralized administration control -** VLANs can be centrally administrated.

PRACTICE QUESTIONS

1: What is the Network ID for the IP address 192.168.12.6, assuming default subnet mask?

A: 192.168.12.0

2: What is the Node ID for the IP address 192.168.12.6, assuming default subnet mask?

A: 0.0.0.6

3: What is the Network ID for the IPX address 2c.0000.0c56.de34?

A: 2c

4: What is the Node ID for the IPX address 2c.0000.0c56.de34?

A: 0000.0c56.de34

5: In what order do the five steps of Data Encapsulation take place?

A: 1) User information is converted to data.
2) Data is converted to segments.
3) Segments are converted to packets or datagrams.
4) Packets or datagrams are converted to frames.
5) Frames are converted to bits.

6: What kind of services are provided by the Presentation layer?

A: PICT,JPEG, MIDI, MPEG, ASCII and EBCDIC

7: What kind of services are provided by the Session layer?

A: NFS, SQL, RPC and NetBIOS

8: How do you enable a Banner on a Cisco Router?

A: Router(Config)# banner motd #

9: What are the two ways to display IPX address information on interface Ethernet1?

A: show ipx interface ethernet1
show interface ethernet1

10: Which IP-class provides the fewest numbers of Hosts?

A: Class C

11: How do you change the Console password on a router to be sharon?

A: Router(config)# line con 0
Router(config-line)# login
Router(config-line)# password sharon

12: How are the ISDN protocols defined?

A: I - stands for concepts, terminology and services
E - stands for existing telephone network
Q - stands for switching and signaling

13: Your are configuring RIP on your router. What happens when you enter the command "Router(config-router)# network 175.76.3.0"?

A: RIP has been enabled on the 175.76.3.0 network.

14: What is the command to show both source and destination addresses for IPX?

A: debug IPX routing activity

15: How do you log into User EXEC mode?

A: Press enter and enter the password if necessary.

16: What command instructs the router to load the IOS from Read Only Memory ?

A: boot system rom

17: What is the Frame Relay configuration command for the second subinterface?

A: interface s0.2 point-to-point

18: What is the command level where you enter the access list command?

A: Router(config)#

19: How are routing loops prevented? (choose 4)

A: Route Poisoning
Hold downs
Split horizon
Triggered Updates

20: What's the default subnet mask for a Class A IP address?

A: 255.0.0.0

21: What's the default subnet mask for a Class B IP address?

A: 255.255.0.0

22: What's the default subnet mask for a Class C IP address?

A: 255.255.255.0

23: What is half duplexing?

A: It is a one-way transmit connection to a receive circuit or vice-versa.

24: What are the three main method of flow control?

A: Windowing
Buffering
Source Quench Messaging

25: What are the correct encapsulation types for frame-relay?

A: Cisco & Ietf

26: In IOS editing mode, how do you return to the beginning of command line?

A: Ctrl + a

27: What type of WAN protocol uses PVCs?

A: Frame Relay

28: What is the command to assign a IP access list 10 to a router interface?

A: Router(config-if)# ip access-group 10

29: How would you backup the IOS image to a TFTP server?

A: copy flash tftp

30: What command would you use to get totally out of config mode and return to PRIV mode on the router?

A: ctrl + z

31: How does "store and forward" LAN switching method work?

A: Switch waits for the whole frame before forwarding.
Latency varies with different frame sizes.

32: You have a class B IP address with a 12 bit subnet. How many subnets and hosts are available?

A: 4096 subnets, 14 hosts

33: Match the IPX Frame Type with the correct IOS encapsulation?

*A:**IPX Frame Type***	***Cisco Encapsulation Type***
Ethernet_802.3	*Novell-ether (Default)*
Ethernet_802.2	*Sap*
Ethernet_II	*Arpa*
Ethernet_Snap	*Snap*
Token Ring	*Sap (Default)*
Token Ring_Snap	*Snap*
Fddi_Snap	*Snap (Default)*
Fddi_802.3	*Sap*
Fddi_Raw	*Novell-fddi*
HDLC	*HDLC (Default)*

34: Router configuration can be done by what three methods?

A: Memory (NVRAM)
Terminal (Console)
Network (TFTP)

35: To make a router boot from a file called FRED on the TFTP server at IP address 171.59.117.19, which command should be entered?

```
A:  Router(config)# boot system TFTP fred 171.59.117.19
```

36: How do you change the Auxiliary password to Cisco ?

```
A:  Router(config)# line aux 0
    Router(config-line)# login
    Router(config-line)# password Cisco
```

37: How do you change the Virtual Terminal password to CCIE ?

```
A:  Router(config)# line vty 0 4
    Router(config-line)# login
    Router(config-line)# password CCIE
```

38: How do you change the Enable Secret password to CCNA ?

```
A:  Router(config)# enable secret CCNA
```

39: How many access-lists are possible on an interface per protocol ?

A: There can be only one access list for in and one for out on each interface per protocol.

40: What happens to a packet which is not permitted in the access list ?

A: There is an implicit deny any at the end of an access list. So if the packet is not explicitly permitted, it will be dropped.

41: Which command is used to view the access-list on serial0 interface ?

A: show access-lists serial0

42: What are the access-list ranges for IP (standard and extended)?

A: 1-99	*IP standard access list*
100-199	*IP extended access list*

43: What does the command "cdp timer 120" do?

A: Changes the cdp update time to 120 seconds?

44: Which of the following are the frame-relay LMI types used in Cisco routers?

A: Cisco (Default)
Ansi
Q944a

45: What is LMI?

A: Management information that tells current DLCI values, global or local significance, and the status of virtual circuits.

46: What commands could you enter to monitor Frame-relay activity on cisco routers?

A: show interface s0
show frame-relay map

47: You have network 145.100.0.0 with a subnet mask of 255.255.248.0. If an access list is applied to address 145.100.8.0 with a wildcard mask of 0.0.7.255, what address range will it filter?

A: Just the 145.100.8.0 subnet

48: What are the 2 steps used to configure and access list?

A: Create the list using access-list command.
Associate the list to an interface using the access-group command.

49: What does the ipx maximum paths command do?

A: Allows you to forward IPX packets over multiple paths to improve load sharing.

50: Which of the following protocols are used to get an IP address from a known MAC address?

A: RARP – Reverse Address Resolution Protocol.

51: You have an IP address of 153.50.6.27 and a subnet mask of 255.255.255.128. What is the class, how many bits are being subnetted, and what is the broadcast address?

A: Class B, 9 bits, 153.50.6.127

52: How do you display the ipx routing updates in or out between routers?

A: sh ipx traffic

53: How do you enable IPX on a router?

A: ipx routing, int e0, IPX network 77790, encapsulation arpa

54: How do you display your configured DLCI's on a frame-relay router?

A: sh frame-relay pvc

55: A Unique ID placed in the header of each frame as it travels the switch fabric with a user-assigned ID defined in each frame is known as?

A: Frame tagging

56: Which OSI layer is responsible for putting 1s and 0s into a logical group?

A: Data Link

57: Which OSI layer is responsible for addressing devices and routing through an internetwork?

A: Network

58: Which layer is responsible for flow control, acknowledgment, and windowing?

A: Transport

59: Which layer hides details of any network-dependent information from the higher layers by providing transparent data transfer?

A: Transport

60: Which layer is responsible for coordinating communication between systems?

A: Session

61: Which layer is responsible for negotiating data transfer syntax?

A: Presentation

62: Which layer is responsible for synchronizing sending and receiving applications, identifying and establishing the availability of the intended communication partner, and determining if sufficient resources for the intended communication exists?

A: Application

63: CPE is an acronym for what?

A: Customer Premises Equipment

64: What is true about connection-oriented sessions?

A: Sessions take place at Transport Layer.
TCP is responsible for segment delivery.
Unacknowledged segments are resent.

All received data is acknowledged by the sender.
Segments are sequenced and put back into order upon arrival.

65: CSU/DSU is an acronym for which of the following?

A: Channel Service Unit - device that connects end-user equipment to the local digital telephone loop.
Data Service Unit - used to adapt the physical interface on a DTE device to a circuit like T1. DSU does the signal timing as well.

66: CO is an acronym for which of the following?

A: Central office

67: What is cut-through switching?

A: Packet switching where data is exiting the switch at the same time it is still entering the inbound port.

68: What does the Spanning-Tree Algorithm (STA) do?

A: Implemented by STP to prevent loops by creating a spanning tree.

69: Of the different switching types, which one has the lowest latency?

A: Cut-Through

70: Of the different switching types, which one has the highest latency?

A: Store and Forward

71: To specify all hosts in the class B IP network 172.16.0.0, which wildcard access list mask would you use?

A: 0.0.255.255

72: IP extended access lists use what parameters as a basis for permitting or denying packets?

A: Source Address
Destination Address
Port Number
Protocol

73: How would you specify only to check host 172.16.30.65 in an IP access list?

A: 172.16.30.65 0.0.0.0, or host 172.16.30.65

74: What is the port number used by TCP?

A: 6

75: What is the port number used by UDP?

A: 17

76: What does the acronym ARP stand for?

A: Address Resolution Protocol

77: Which protocol derives a hardware address from a known IP address?

A: ARP

78: Which protocol works at the Internet layer of the DOD model and is responsible for making routing decisions?

A: IP

79: Which port numbers are used by TCP and UDP to set up sessions with other hosts?

A: 1023 and above

80: The User Datagram Protocol works at which layer of the DOD model?

A: Host-to-Host.

81: Which protocol sends redirects back to an originating router?

A: Internet Control Message Protocol - ICMP

82: Ping uses which Internet layer protocol?

A: ICMP

83: What does the following command do?

Router(config)# router igrp 101

A: Identifies IGRP as the routing protocol on autonomous system 101.

84: Which protocols use the Transport layer?

A: TCP,UDP, and SPX.

85: Which of the following is a connectionless protocols use the Transport layer?

A: UDP

86: Which protocol is used for booting diskless workstations?

A: Bootstrap Protocol

87: What command do you use to change your enable password?

A: Router(config)# enable password <password>

88: What command can you use to copy the configuration from NVRAM into running RAM?

A: copy startup-config running-config, or copy start run

89: What is the syntax for changing the name of a Cisco router?

A: Hostname <routername>

90: To exit from privileged mode and go back to the user mode, what would you type at the privileged mode prompt?

A: disable

91: What is the auxiliary (AUX) port used for?

A: Modem connections for a console, or a dialup connection for temporary Dial on Demand Routing (DDR)

92: How do you enable the advanced editing features?

A: terminal editing

93: What keys do you use to view, from history, the last command that was entered into a Cisco router?

A: CTRL+P

94: What key do you press to have the Cisco IOS finish typing a command for you?

A: TAB

95: What does the erase startup-config command do?

A: Erases the startup-configuration from NVRAM

96: What is the command to set the clock rate on your DCE interfaces to 64kbps?

A: clock rate 64000

97: If you have two Cisco routers connected with DTE/DCE cables, to which router would you add the command clock rate?

A: DCE

98: What is the administrative distance used for in static routes?

A: To rate the source's trustworthiness

99: Static routes are used for which of the following?

A: Defining a path to an IP destination network.
Building routing tables to remote networks.

100: What is the command syntax to set a gateway of last resort in your Cisco router?

A: ip route 0.0.0.0 0.0.0.0 <gateway address>

101: Which Cisco IOS command can you use to see the routing table?

A: sh ip route or sh ipx route

102: What are three ways that routers learn paths to destinations?

A: Static, default or dynamic routing

103: Which protocol will send a message to routers if a network outage or congestion occurs?

A: ICMP

104: Which protocol is used to manage and monitor the network?

A: SNMP

105: Which frame has a TYPE field to identify the upper-layer protocol?

A: Ethernet_II

106: When should you use static routing instead of dynamic routing?

A: When you have only a few routers and want to save bandwidth.

107: What is the command for creating an IP static route?

A: ip route <destination_network_address> < subnet_mask> < default_gateway>

108: When looking at a routing table, what does the "S" identifier mean?

A: Statically connected

109: What is true about IP routing?

A: A device will send a frame with the hardware destination or the default gateway. The router will strip the frame and put the datagram in a new frame with the new remote destination address.

110: What static route parameter will tell a router the name of the interface to use to get to a destination network?

A: interface

111: When creating a static route, what is the gateway parameter used for?

A: Defining the next hop.

112: What is true when creating static routes?

A: Gateway is required, the administrative distance is optional.

113: When looking at a routing table, what does the "C" identifier mean?

A: Directly Connected

114: What is the routing algorithm used by RIP?

A: Distance Vector

115: What is the routing metric used by RIP?

A: Hop count

116: What is the routing algorithm used by IGRP?

A: Distance Vector

117: Which command can you type at the router prompt to verify the broadcast frequency for IGRP?

A: sh ip protocol

118: Which utility will identify the path that a packet takes as it travels to it's final destination?

A: Trace

119: What are the routing metrics used by IGRP?

A: Bandwidth, reliability, MTU, delay, and load. IGRP can also use hop counts to determine the best route to a remote network.

120: What does a metric of 16 hops represent in a RIP routing network?

A: Destination is unreachable

121: What are Hold-downs used for?

A: To prevent regular update messages from reinstating a route that has gone down.

122: What routing technique prevents the router from sending info through the same interface from which it was originally received?

A: Split Horizon

123: What routing technique sends routing updates to indicate that a network is unreachable?

A: Route poisoning

124: What are the three types of routes that IGRP advertises?

A: Interior, system and exterior routes.

125: Which of the following are distance-vector protocols?

A: RIP and IGRP

126: Which of the following routing protocols use Autonomous Systems?

A: IGRP, EIGRP, OSPF & NLSP

127: What is true about link-state networks?

A: They maintain a more complex table than distance-vector based networks.

128: What is convergence?

A: The speed and ability of a group of internetwork devices running a specific protocol to agree on the topology after a change takes place.

129: What type of routing protocols send their entire routing table every 30 seconds?

A: Distance-vector

130: What is the default administrative distance of RIP?

A: 120

131: What is the default administrative distance for IGRP?

A: 100

132: You just received an output that states the CDP hold time, hardware, port ID, and local interface of a remote router. What was the command did you enter?

A: show cdp neighbor

133: What's the default CDP hold time?

A: 180 seconds

134: What's the default CDP update broadcast rate?

A: 60 seconds

135: What frame type does CDP use to gather information about its directly connected neighbors?

A: SNAP

136: Which command can you type to view the hostnames configured in your router (choose two)?

A: show hosts
sh host

137: How would you configure it so you could type in the hostname "Randy" instead of the IP address to access the remote router named Randy?

A: Router(config)# ip host randy <ip_address>

138: If you type "copy tftp flash", what will happen?

A: You copy a file from TFTP server to router flash.

139: What command will allow you to load a Cisco router configuration that is stored on a TFTP server into working RAM?

A: config net <ip address of TFTP server>

140: What does it mean if you're running a trace and receive a "P" as a response?

A: Protocol unreachable.

141: Copy the router configuration stored in NVRAM to RAM, which command could you use?

A: config mem

142: What command should you use to have your router load the valid Cisco IOS from a TFTP server?

A: boot system tftp <file name> <ip address of tftp server>

143: Which command would you use if you want to disable DNS lookup?

A: no ip domain-lookup

144: How can you telnet into multiple routers but keep the sessions open all at the same time?

A: Ctrl + Shift+ x

145: After telneting into multiple routers simultaneously, what command can you type to see these connections?

A: sh sessions

146: How often do servers exchange SAP information unless set otherwise?

A: Every 60 seconds

147: What is the default Ethernet encapsulation on NetWare 3.11?

A: 802.3

148: Which command would you use to see if you were receiving SAP and RIP information on an interface?

A: sh ipx int

149: Which command would you use to see if the router is hearing your server SAPs?

A: sh ipx servers

150: What do IP standard access lists use as a basis for permitting or denying packets?

A: Source address

151: Which access list command will allow only WWW traffic into network 193.11.33.0?

A: Access-list 101 permit tcp any 193.11.33.0 0.0.0.255 eq www

152: Which of the following will show which ports have IP access lists applied?

A: Show ip interface, or show running-config

153: What is logged when IP access list logging is enabled?

A: Source address, source port, destination address, destination port, protocol, and access list number.

154: Which of the following can be logged by IPX extended access lists?

A: Source address, source socket, destination address, destination socket, access list number, protocol.

155: Which of the following will apply IPX SAP access list 1010 for incoming traffic?

A: ipx input-sap-filter 1010

156: What is the IP extended access list range?

A: 100-199

157: What is the extended IPX access list range?

A: 900-999

158: What would you enter in an IPX access list to signify any host or any network?

A: -1

159: What type of connection would you use to support applications requiring high-speed voice, video and data communications.

A: ISDN

160: Which protocol requires you to use IETF encapsulation if connecting to non-Cisco equipment?

A: Frame relay

161: What does the ISDN Basic Rate Interface provide?

A: Two 64-Kbps B channels and one 16 Kpbs D channel.

162: What do frame relay DLCIs identify?

A: DLCI identifies a logical connection between DTE devices.

163: What does ISDN PRI support?

A: 23 B channels and one 64 Kbps D channel

164: What is the default encapsulation on point-to-point links between two Cisco routers?

A: HDLC

165: What is true when using DDR?

A: You must use static routing.

166: Which access configuration allows only traffic from network 172.16.0.0 to enter interface serial0?

A: Router(config)# access-list 10 permit 172.16.0.0 0.0.255.255
Router(config)# int s0
Router(config-if)# ip access-group 10 in

167: If you want to capture IPX access lists being accessed, what command parameter do you add to your extended IPX access list?
A: Log

168: In an IP access list, you want to refer to host 172.16.50.1 only. What wildcard mask would you use to make the list as specific as possible?

A: 0.0.0.0

169: You want to create an access list to permit only the subnets 161.130.16.0 through 161.130.31.0. Assume the default subnet mask. What wildcard mask would you use?

A: 0.0.15.255

170: If you enter the shutdown command on a particular interface, and then enter a show interface command, what will the status line say?

A: Serial1 is administratively down, line protocol is down.

171: A switching facility the provides the nearest point of presence for a providers WAN service is called?

A: (CO) Central Office

172: What commands provide route verification?

A: Ping
Trace
Telnet

173: You are entering a static IP route and you type the following command:

ip route 172.16.1.0 255.255.255.0 172.16.2.1 110

What does the “110” at the end mean?

A: Administrative Distance

174: You are entering a static IP route and you type the following command:

ip route 172.16.1.0 255.255.255.0 172.16.2.1 120

What does the “172.16.2.1” mean?

A: Default Gateway or Next Hop

175: What is the primary characteristic of a connection-oriented (reliable) protocol?

A: Issues Acknowledgements

176: How do you set the frame relay interface s1 bandwidth to 56kbps?

A: Router(config)# interface s1
Router(config-if)# bandwidth 56

177: What do you need to support full-duplex Ethernet?

A: Full duplex NICs with Loopback and collision detection disabled.

178: What are advantages to segmenting your network with routers.

A: Manageability
Flow Control
Explicit packet lifetime control
Multiple active paths

179: Which of the following describes a full-duplex transmission?

A: Uses a point to point connection from the transmitter of the transmitting station to the receiver of the receiving station.
Simultaneous data transmission between a sending and receiving stations.

180: If a frame is received at a switch and only the destination hardware address is read before the frame is forwarded, what type of switching method are you using?

A: Cut-Through Switching

181: Which is true regarding store-and-forward switching method?

A: Latency depends on frame length.

182: What command would you enter to display the contents of access list 102?

A: show access-list 102

183: How can you turn off the advanced editing features?

A: terminal no editing

184: What is the syntax you would use to configure a port on a Catalyst 5000 switch?

A: type slot/port

185: What is an administrative distance of 0?

A: 0 is the default administrative distance for directly connected routes. The router trusts a 0 distance the most.

186: You have to recommend the cheapest device to increase bandwidth on your network. What would you recommend?

A: 100MB hub

187: If you wanted create an access list to only permit traffic to or from network 198.55.56.0 to be permit through a particular interface, what command would you use to create the access list?

A: access-list 1 permit 198.55.56.0 0.0.0.255

188: You want to create a static route to network 161.25.0.0. Your next hop address will be 161.172.1.67 and you want to use an administrative distance of 110. The new IP address uses the default subnet mask. What command would you enter in config mode?

A: ip route 161.25.0.0 255.255.0.0 161.172.1.67 110

189: How would you configure an access list to only allow traffic from network 141.75.0.0 to enter serial interface s0?

```
A:  access-list 1 permit 141.75.0.0 0.0.255.255
    interface serial 0
    ip access-group 1 in
```

190: At what layer of the OSI model does a router operate?

A: layer 3

191: What does the command "boot system ROM" do?

A: Forces the router to load the IOS from ROM.

192: If you wanted to subnet your class C network into 2 subnets, what would you use as a subnet mask?

A: 255.255.255.192

193: What do bridges use to make packet forwarding decisions?

A: MAC address

194: What do routers use to make packet forwarding decisions?

A: IP address