



Exam : 642-821

Title : Building Cisco Remote Access Networks
(BCRAN)

Ver : 09-25-07

QUESTION 1:

A bank called CK Savings and Trust is expanding and needs to connect a new branch to their head office on the other side of town. The new branch has twelve employees and each of them require constant access to the bank's central accounting system throughout all hours of the workday. What kinds of network connections are most suitable for the bank's needs? (Choose two)

- A. ISDN BRI
- B. Dedicated lease line
- C. Asynchronous
- D. Frame Relay
- E. Time Delay

Answer: B, D

Explanation:

A remote site, or branch office, is a small-site connection to a campus over a WAN. A remote site typically has fewer users than the central site and therefore needs a smaller-size WAN connection. Remote sites connect to the central site and to some other remote site offices. Telecommuters may also require access to the remote site. A remote site can use the same connection type or different media. Remote site traffic can vary, but is typically sporadic. The network designer must determine whether it is more cost effective to offer a permanent or dialup solution. The remote site must have a variety of equipment, but not as much as the central site requires. Typical WAN solutions a remote site uses to connect to the central site follow:

1. Leased line
2. Frame relay
3. X.25
4. ISDN
5. ATM

The keywords here are: "Constant Access". We don't need and dialup solution (ISDN or Asynchronous) as it would be too costly to keep the line up the entire day.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 2-25

QUESTION 2:

DRAG DROP

Match the WAN protocols on the bottom to their proper descriptions:

642-821

Description	Place WAN protocols here
point-to-point serial IP connections	place here
ITU-T standard protocol with error-corrections	place here
standard-based, host to network over aynch/sync connections	place here
proprietary router-to-router corrections	place here
international standard cell switching protocol	place here
high performance, packet switched protocol	place here

Select from these	
X25	Point-to-Point Protocol (PPP)
High Level Data Link (HDLC)	Serial Link Internet Protocol (SLIP)
Frame Relay	Asynchronous Transfer Mode

Answer:

Description	Place WAN protocols here
point-to-point serial IP connections	Serial Link Internet Protocol (SLIP)
ITU-T standard protocol with error-corrections	X25
standard-based, host to network over aynch/sync connections	High Level Data Link (HDLC)
proprietary router-to-router corrections	High Level Data Link (HDLC)
international standard cell switching protocol	Asynchronous Transfer Mode
high performance, packet switched protocol	Frame Relay

Select from these

Explanation:

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 2-12 & 2-13

QUESTION 3:

A Certkiller remote user is getting Internet access from the local cable provider. When an individual is connected to the Internet by way of a CATV cable service, what kind of traffic is considered upstream traffic?

- A. Traffic going from the user's home traveling to the headend.
- B. Broadcast traffic, including the cable TV signals.
- C. Traffic between the headend and the TV signal.
- D. Traffic between the headend and the supplier antenna.
- E. Traffic from outside the local cable segment serving the user's home.
- F. All of the above can be considered upstream

Answer: A

Explanation:

In the CATV space, the downstream channels in a cable plant (cable head-end to subscribers) is a point-to-multipoint channel. This does have very similar characteristics to transmitting over an Ethernet segment where one transmitter is being listened to by many receivers. The major difference is that base-band modulation has been replaced by a more densely modulated RF carrier with very sophisticated adaptive signal processing and forward error correction (FEC).

In the upstream direction (subscriber cable modems transmitting towards the head-end) the environment is many transmitters and one receiver. This introduces the need for precise scheduling of packet transmissions to achieve high utilization and precise power control so as to not overdrive the receiver or other amplifier electronics in the cable system. Since the upstream direction is like a single receiver with many antennas, the channels are much more susceptible to interfering noise products. In the cable industry, we generally call this ingress noise. As ingress noise is an inherent part of CATV plants, the observable impact is an unfortunate rise in the average noise floor in the upstream channel. To overcome this noise jungle, upstream modulation is not as dense as in the downstream and we have to use more effective FEC as used in the downstream.

Reference:

http://www.cisco.com/warp/public/759/ipj_1-3/ipj_1-3_catv.html

QUESTION 4:

Which of the following synchronous serial standards are supported by Cisco routers using a serial interface? (Choose all that apply.)

- A. V.45
- B. V.35
- C. V.90
- D. EIA-530
- E. EIA/TIA-232
- F. All of the above

Answer: B, D, E

Explanation:

The five-in-one synchronous serial WAN module gets its name from the five types of signaling it supports, which include all of the following:

- EIA/TIA-232
 - EIA/TIA-449
 - V.35
 - X.21
 - EIA-530
-

QUESTION 5:

Which of the following remote-access network types are classified as circuit switched networks? (Choose two)

- A. Frame Relay
- B. ISDN
- C. Asynchronous dial-up
- D. X.25
- E. ATM

Answer: B, C

Explanation:

Circuit switching is a WAN switching method in which a dedicated physical circuit through a carrier network is established, maintained, and terminated for each communication session. Initial signaling at the setup stage determines the endpoints and the connection between the two endpoints. Typical circuit-switched connections are:

- * Asynchronous serial
- * ISDN BRI & ISDN PRI

Switched circuits allow data connections that can be initiated when needed and terminated when communication is complete. This works much like a normal telephone line works for voice communication. Integrated Services Digital Network (ISDN) is a good example of circuit switching. When a router has data for a remote site, the switched circuit is initiated with the circuit number of the remote network. In the case of ISDN circuits, the device actually places a call to the telephone number of the remote ISDN circuit.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 2-7
http://www.cisco.com/en/US/netsol/ns339/ns392/ns399/ns400/networking_solutions_white_paper0900aecd800d

Incorrect Answers:

A, D, E: These are packet switching technologies, not circuit switching. Packet switching is a WAN technology in which users share common carrier resources. Because this allows the carrier to make more efficient use of its infrastructure, the cost to the customer is generally much better than with point-to-point lines. In a packet switching setup, networks have connections into the carrier's network, and many customers share the carrier's network. The carrier can then create virtual circuits between customers' sites by which packets of data are delivered from one to the other through the network. The section of the carrier's network that is shared is often referred to as a cloud. Some examples of packet-switching networks include Asynchronous Transfer Mode (ATM), Frame Relay, Switched Multimegabit Data Services (SMDS), and X.25.

QUESTION 6:

Wireless technology has advanced over the years and fixed point-to-point microwave systems are now using higher frequencies. What is true about systems employing higher frequencies?

- A. Less spectrum range is available for broadband applications.

- B. Costs can be cut with the use of smaller antennas that can be deployed.
- C. The larger wavelengths require more sophisticated equipment.
- D. Propagation distances and weather are normally not much of a factor that has to be taken into consideration.

Answer: C

Explanation:

The principle advantage of higher frequencies is that there is more of a spectrum available for broadband applications.

Fixed-wireless systems use frequencies allocated for such use from about 900 MHz to 40 GHz. The number of different bands can be overwhelming, with multiple frequency bands assigned for private use and multiple bands assigned for carrier use. In addition, some bands are designated for licensed use while others can be used without a license. Should you care what frequency is used? Yes, but only in a general sense. Higher frequencies have some advantages over lower frequencies, but also suffer some drawbacks. The principle advantage of higher frequencies is that there is more of a spectrum available for broadband applications. The majority of higher bandwidth systems use frequencies above 5 GHz. Antennas at these frequencies are smaller due to the smaller wavelengths, making systems easier to deploy. But with higher frequency, components demand more sophisticated technology, so systems cost more. Also, propagation distance for reliable communications decreases and the signal is more susceptible to weather conditions like rain and fog. Higher frequency systems, those above about 30 GHz, are sometimes referred to as millimeter wave because the wavelength of these signals is on the order of 1 millimeter. Both private and carrier systems have a choice of using licensed or unlicensed spectrum.

Reference:

<http://www.fixedwirelessone.com/Overview%20of%20Fixed%20Wireless.htm>

QUESTION 7:

Which of the following network services would you find to be appropriate for a group of mobile Certkiller salespeople who need the versatility of accessing their e-mail on the road?

- A. Digital service
- B. High-Speed Serial (HSS) interface
- C. Asynchronous service
- D. Multi-mode service
- E. Leased Line
- F. All of the above

Answer: C

Explanation:

As WAN technologies improve, allowing many employees to do their jobs almost

anywhere, the growth in the number of telecommuter and small company sites has taken on new proportions. Like that of central and remote sites, the telecommuter site must determine its WAN solution by weighing cost and bandwidth requirements.

An asynchronous dialup solution using the existing telephony network and an analog modem is often the solution for telecommuters because it is easy to set up and the telephone facilities are already installed. As usage and bandwidth requirements increase, other remote access technologies should be considered.

The non-stationary characteristics of a mobile user make an asynchronous dialup connection the remote solution. Employees on the road can use their PCs with modems and the existing telephone network to connect to the company. Typical WAN connections employed at telecommuter sites are:

- A) asynchronous dialup solutions using modems
- B) ISDN BRI
- C) Frame Relay (pending the user utilizes the line for an extended time frame)
- D) ADSL

Typical considerations for a remote site WAN connection follow:

1. Cost
2. Authentication
3. Availability

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 2-27

QUESTION 8:

Which of the following WAN technologies are often employed at telecommuter sites, such as the end-users home office? Select all that apply.

- A. ADSL
- B. ISDN BRI
- C. HDSL
- D. Leased lines
- E. Cable modems
- F. Asynchronous dial-up

Answer: A, B, E, F

Explanation:

As WAN technologies improve, allowing many employees to do their jobs almost anywhere, the growth in the number of telecommuter and small company sites has exploded. Like that of central and remote sites, the telecommuter site must determine its WAN solution by weighing cost and bandwidth requirements.

An asynchronous dialup solution using the existing telephony network and an analog modem is often the solution for telecommuters because it is easy to set up and the telephone facilities are already installed. As usage and bandwidth requirements increase, other remote access technologies should be considered.

The non-stationary characteristics of a mobile user make an asynchronous dialup

connection the remote solution. Employees on the road can use their PCs with modems and the existing telephone network to connect to the company. Typical WAN connections employed at telecommuter sites are:

1. Asynchronous dialup
2. ISDN BRI
3. Frame Relay (pending the user utilizes the line for an extended time frame)
4. ADSL
5. Cable Modem
6. Wireless access

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 2-27

QUESTION 9:

A new cable modem was shipped to the home of a Certkiller user, where it is being installed for the first time. When a DOCSIS 1.1 compliant cable modem first initializes, (boots up) what does it do?

- A. Establishes IP connectivity (DHCP).
- B. Determines the time of day.
- C. Requests a DOCSIS configuration file from a TFTP server.
- D. Scan for a downstream channel and the establishment of timing synchronization with the CMTS.
- E. None of the above.

Answer: D

Explanation:

According to the DOCSIS (Data-over-Cable Service Interface Specifications) when you first power up a cable modem it starts scanning (starting at a low frequency) for a cable signal. When it 'hears' a cable modem stream it listens for a broadcast (from the service provider) which contains information (ie. frequency) needed to talk back with the head end. It then 'talks back' and if it communicates the right authentication information, it is allowed to proceed.

References: Page 225 of the CCNP Self-Study BCRA (642-821) ISBN: 1-58720-084-8

http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide_chapter09186a008019b57f.htm

QUESTION 10:

You are building a small network at your home and you intend on connecting your cable modem to a Cisco router. Which router interface would you connect the modem to?

- A. Synchronous serial
- B. Asynchronous serial

- C. Ethernet
- D. auxiliary
- E. BRI

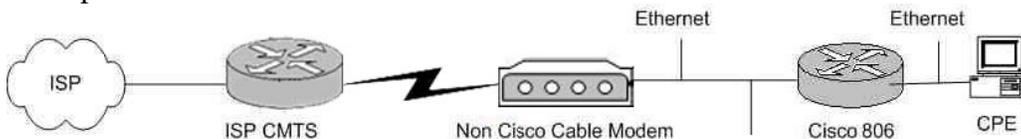
Answer: C

Explanation:

In certain environments where a non Cisco Cable Modem (CM) is used, and the CM is only capable of bridging, a Cisco router such as the Cisco 806 can be connected to the Cable Modem via the Ethernet interface. The routing can then be performed by the Cisco router behind the Cable Modem and the Client PC or Customer Premises Equipment (CPE) will be connected to the Cisco router. Network Address Translation (NAT) can then be configured on the Cisco router.

When the Cisco router is connected behind the Cable Modem the first problem that might be encountered is not obtaining an IP address dynamically on the Cisco router's Ethernet interface. Most Internet Service Providers (ISPs) allow only one host or PC behind the Cable Modem. Some ISPs assign an IP address to the PC based on the host name. Therefore, if you have a Cisco router behind the Cable Modem, then the host name for the router configured using the hostname command should be the same host name given by the ISP.

Example:



QUESTION 11:

Company XYZ is established in New York City but is establishing a new office in Miami, FL. To connect these offices, you need a cost effective solution that will allow the Miami office to securely transfer files back and forth at T1 speeds. What kind of network would you recommend for this?

- A. DSL
- B. ATM
- C. Leased line
- D. Frame Relay
- E. ISDN

Answer: D

Explanation:

Frame Relay - Medium control, shared bandwidth, medium-cost enterprise backbones. It uses the services of many different Physical layer facilities at speeds that typically range from 56 Kbps up to 2 Mbps.

To have secure file transfers it would be wise to implement a VPN-2-VPN connection on the frame relay.

WAN Connection Summary	
Connection Type	Applications
Leased lines	High control, full bandwidth, high-cost enterprise networks, and last-mile access
Frame Relay	Medium control, shared bandwidth, medium-cost enterprise backbones; branch sites
ISDN	Low control, shared bandwidth, more bandwidth than dialup
Asynchronous dialup	Low control, shared bandwidth, variable cost, cost-effective for limited-use connections like DDR
X.25	Low control, shared bandwidth, variable cost, cost-effective for limited-use connections, high reliability

Incorrect Answers:

A: DSL alone will not provide for a secure connection between the two offices, as additional hardware will be needed to create a VPN. DSL speeds do not typically come in T1 speeds.

B, C: Although both of these are options, they are less cost effective than frame relay. Leased line T1's are priced based on the distance between the endpoints, so a connection between New York and Miami may become cost prohibitive.

E. Although ISDN can indeed come in T1 speeds (PRI), in this example we want a dedicated connection, and not a usage based, dial solution such as ISDN.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 2-20

QUESTION 12:

You are an independent network designer and a client inquires about connecting together his two offices with a leased line. When would a leased line be cost effective? (Choose two)

- A. When there are long connection times.
- B. When there are short distances.
- C. When little control over the WAN is needed.
- D. When there are short connection times.

Answer: A, B

Explanation:

A point-to-point dedicated link provides a single, pre-established WAN communications path from the customer premises, straight through a carrier network (the telephone company), to a remote network. Dedicated lines are also known as leased lines. The established path is permanent and fixed for each remote network reached through the carrier facilities. Point-to-point links are reserved full-time by the carrier company for the

customer's private use. Point-to-point links are available full-time in all Cisco products. The private nature of a dedicated leased line connection allows a corporation to maximize its control over the WAN connection. Leased lines also offer high speeds up to T3/E3 levels. They are ideal for high-volume environments with steady-rate traffic patterns. However, because the line is not shared, they tend to be more costly. As a general rule, leased line connections are most cost-effective in the following situations:

1. Long connect times
2. Short distances

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 2-5

QUESTION 13:

A local Internet Service Provider is going to start offering ADSL with 640 kbps upload speed and 4Mbps download speeds. They have retained you to help in their advertisement campaign to help them find their target market. What groups of users should you target your marketing efforts to? (Choose two)

- A. Central data processing facilities receiving simultaneous uploads of data from remote offices.
- B. Support organizations providing ftp services for software distribution and documentation.
- C. Small home offices requiring 24 hour connection to the Internet for email and web communication.
- D. Web services companies providing dynamic web content serving, including video-on-demand.

Answer: A, C

Explanation:

Based on the expanding number of options currently and coming soon for the broadband market, competition for home and remote user dollars has reached a frenzied state. The deployment of broadband and similar technologies has involved quite a large amount of trial and error. The competition has seen the emergence of two primary services for widespread deployment. These are Cable and DSL.

Loosely defined, DSL is a technology that exploits unused frequencies on copper telephone lines to transmit traffic, typically at multimegabit speeds. DSL uses existing telephone wiring, without requiring any additional cabling resources. It has the capability to allow voice and high-speed data to be sent simultaneously over the same copper pair. The service is always available, so the user does not have to dial in or wait for call setup. DSL technologies can be broken down into two fundamental classifications: asymmetric (ADSL) and symmetric (SDSL). As the name implies, ADSL uses higher downstream rates and lower upstream rates. In contrast, SDSL uses the same downstream and upstream rates. ADSL is the most commonly deployed DSL technology, and is the primary focus of the DSL portion of the CCNP Remote Access Exam.

Incorrect Answers:

B: In order to maximize the use of an FTP server, you would want a greater upload speed, since the majority of users will be downloading files from the FTP server.

D: Again, we would want to ensure that the upload speed was as large as possible, due to the fact that the majority of the bandwidth will be consumed as uploads to the end users.

Reference:

Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)

Page 245 to 247

QUESTION 14:

What's true about the G.Lite (G.922) ADSL ITU standard?

- A. It offers equal bandwidth for upstream and downstream data traffic.
- B. It has limited operating range of less than 4,500 feet.
- C. It was developed specifically for the consumer market segment requiring higher download speeds.
- D. Signals cannot be carried on the same wire as POTS signals.
- E. All of the above

Answer: C

Explanation:

G.Lite is the informal name for what is now a standard way to install Asymmetric Digital Subscriber Line (ADSL) service. Also known as Universal ADSL, G.Lite makes it possible to have Internet connections to home and business computers at up to 1.5 Mbps (millions of bits per second) over regular phone lines. Even at the lowest downstream rate generally offered of 384 Kbps (thousands of bits per second), G.Lite is about seven times faster than regular phone service with a V.90 modem and three times faster than an Integrated Services Digital Network (ISDN) connection. Upstream speeds from the computer are at up to 128 Kbps. (Theoretical speeds for ADSL are much higher, but the data rates given here are what is realistically expected.)

With G.Lite, your computer's analog-to-digital modem is replaced with an "ADSL modem." and the transmission from the phone company is digital rather than the analog transmission of "plain old telephone service." G.Lite is also known as "splitterless DSL" because, unlike other DSL technologies, it does not require that a technician come to install a splitter, a device that separates voice from data signals, at the home or business (sometimes referred to as "the truck roll").

The G.Lite standard is officially known as G.992.2.

DSL technologies can be broken down into two fundamental classifications: asymmetric (ADSL) and symmetric (SDSL). As the name implies, ADSL uses higher downstream rates and lower upstream rates. In contrast, SDSL uses the same downstream and upstream rates. ADSL is the most commonly deployed DSL technology, and is the primary focus of the DSL portion of the CCNP Remote Access Exam.

DSL is a highly distance-sensitive technology. As the distance from the CO increases, the signal quality and connection speeds decrease. ADSL service is limited to a maximum

distance of 18,000 feet (5460 m) between the DSL CPE and the DSLAM, although many ADSL providers place an even lower limit on the distance to ensure quality.

References:

Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)

Page 245 to 247

http://whatis.techtarget.com/definition/0,,sid9_gci212198,00.html

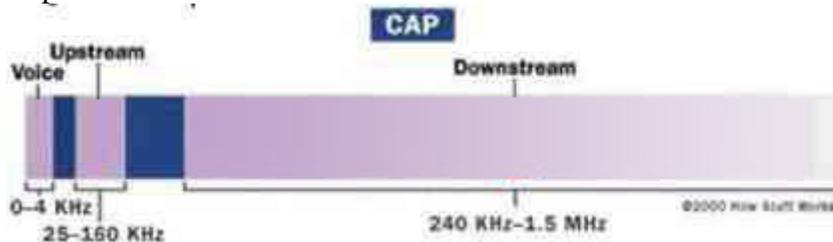
QUESTION 15:

Which proprietary DSL encapsulation type has the potential of dividing telephone lines into three widely separated, distinct channels for the sake of minimizing interference between voice, upstream and downstream data flows?

- A. G.Lite
- B. CAP
- C. DMT
- D. Half-rate DMT

Answer: B

Explanation:



CAP operates by dividing the signals on the telephone line into three distinct bands: Voice conversations are carried in the 0 to 4 KHz (kilohertz) band, as they are in all POTS circuits. The upstream channel (from the user back to the server) is carried in a band between 25 and 160 KHz. The downstream channel (from the server to the user) begins at 240 KHz and goes up to a point that varies depending on a number of conditions (line length, line noise, number of users in a particular telephone company switch) but has a maximum of about 1.5 MHz (megahertz). This system, with the three channels widely separated, minimizes the possibility of interference between the channels on one line, or between the signals on different lines.

References:

Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)

Page 248 & 249

http://www.esi-websolutions.com/technology_ADSL.htm

QUESTION 16:

Over which of the following DSL services is the foundation that Cisco's Long Reach Ethernet (LRE) is based on?

- A. ADSL
- B. HDSL
- C. IDSL
- D. VDSL

Answer: D

Explanation:

Cisco Long Range Ethernet (LRE) solution leverages Very High Data Rate Digital Subscriber Line (VDSL) technology to dramatically extend Ethernet services over existing Category 1/2/3 twisted pair wiring at speeds from 5 to 15 Mbps (full duplex) and distances up to 5,000 feet. The Cisco LRE technology delivers broadband service on the same lines as Plain Old Telephone Service (POTS), digital telephone, and ISDN traffic. In addition, Cisco LRE supports modes compatible with Asymmetric Digital Subscriber Line (ADSL) technologies, allowing service providers to provision LRE to buildings where broadband services already exist

Reference:

Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)
Page 251

QUESTION 17:

Which ADSL modulation type:

1. is prominent in residential applications
2. has 120 subchannels
3. doesn't need a splitter
4. has a 1.5 Mbps maximum downstream speed?

- A. CAP
- B. DMT
- C. G.Lite
- D. PPPoA
- E. PPPoE

Answer: C

Explanation:

ITU GLITE (ITU G.992.2) describes splitterless Asymmetric Digital Subscriber Line (ADSL) Transceivers on a metallic twisted pair that allows high-speed data transmission between the Central Office (ATU-C) and the customer end remote terminal (ATU-R). G.LITE can provide ADSL transmission simultaneously on the same pair with voice (band) service, ADSL transmission simultaneously on the same pair with ISDN services (G.961 Appendix I or II); or ADSL transmission on the same pair with voice band transmission and with TCM-ISDN (G.961 Appendix III) in an adjacent pair. G.992.2 supports a maximum 1.536 Mbps downstream and 512 kbps upstream net data rate. G.LITE uses discrete Multitone (DMT) line code. DMT is based in the use of the IFFT to

generate a set of sub-channels, and transmit information in each sub-channel independently. Figure 1 shows the G.LITE spectrum with indication of the POTS, upstream pilot tone, downstream pilot tone, subcarrier spacing, and number of subcarriers for the upstream and downstream direction. Dividing the available bandwidth into a set of independent, orthogonal subchannels are the key to DMT performance. By measuring the SNR of each subchannel and then assigning a number of bits based on its quality, DMT transmits data on subcarriers with good SNRs and avoids regions of the frequency spectrum that are too noisy or severely attenuated. The underlying modulation technique is based on quadrature amplitude modulation (QAM). Each subchannel is 4.3125 kHz wide and is capable of carrying up to 15 bits. The downstream is up to 552 kHz, offering 122 subchannels, and the upstream from 26 to 138 kHz, offering 25 upstream subchannels.

Reference: http://www.vocal.com/data_sheets/full/glite.pdf

QUESTION 18:

Certain physical factors are capable of severely limiting the maximum speed available on a DSL connection. Which of the following describe the factors that are capable of it? (Choose all that apply)

- A. Number of telephones attached to the local loop.
- B. Gauge of wire used on the local loop.
- C. Distance between the CPE and the DSLAM.
- D. Bridge taps in the local loop.
- E. Loading coils in the subscriber's line.

Answer: B, C

Explanation:

DSL is a highly distance-sensitive technology. As the distance from the CO increases, the signal quality and connection speeds decrease. ADSL service is limited to a maximum distance of 18,000 feet (5460 m) between the DSL CPE and the DSLAM, although many ADSL providers place an even lower limit on the distance to ensure quality. The 18,000-foot distance limitation for DSL is not a limitation for voice telephone calls, but for data transmission. The telco uses small amplifiers, called loading coils, to boost voice signals. Loading coils have a nasty tendency to disrupt DSL data signals. This means that if there are loading coils in the loop between the CPE and CO, you probably are not within an area that can receive DSL service.

Reference:

Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)
Page 247

QUESTION 19:

When designing an ADSL network; if you want minimal local loop impairments,

what should be the maximum distance of your lines?

- A. 1000 feet (0.3 km)
- B. 4000 feet (1,5 km)
- C. 12,000 feet (3.65 km)
- D. 18,000 feet (5,5 km)
- E. 28,000 feet (8.52 km)

Answer: D

Explanation:

DSL is a highly distance-sensitive technology. As the distance from the CO increases, the signal quality and connection speeds decrease. ADSL service is limited to a maximum distance of 18,000 feet (5460 m) between the DSL CPE and the DSLAM, although many ADSL providers place an even lower limit on the distance to ensure quality. The 18,000-foot distance limitation for DSL is not a limitation for voice telephone calls, but for data transmission. The telco uses small amplifiers, called loading coils, to boost voice signals. Loading coils have a nasty tendency to disrupt DSL data signals. This means that if there are loading coils in the loop between the CPE and CO, you probably are not within an area that can receive DSL service.

Reference:

Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)
Page 247

QUESTION 20:

What default encapsulation type does Cisco set on their routers serial interfaces?

- A. PPP
- B. HDLC
- C. Frame Relay
- D. LAPB

Answer: B

Explanation:

By default, a serial interface on a Cisco router is set to their proprietary HDLC encapsulation. More information on the various encapsulation types for a serial interface is displayed below:

Frame Relay - High-performance WAN protocol that operates at the physical and data-link layers of the OSI reference model. Frame Relay was designed originally for use across ISDN interfaces. Today, it is used over a variety of other network interfaces as well. Frame Relay is an example of a packet-switched technology; it is often described as a streamlined version of X.25, offering fewer of the robust capabilities that are offered in X.25, such as windowing and retransmission of lost data. This is because Frame Relay typically operates over WAN facilities that offer more reliable connection services and a

higher degree of reliability than the facilities available during the late 1970s and early 1980s that served as the common platforms for X.25 WANs. As mentioned above, Frame Relay is strictly a Layer 2 protocol suite, whereas X.25 provides services at Layer 3 (the network layer) as well. This enables Frame Relay to offer higher performance and greater transmission efficiency than X.25 and makes Frame Relay suitable for current WAN applications, such as LAN interconnection.

High-Level Data Link Control (HDLC) - HDLC is the default encapsulation type on point-to-point, dedicated links. It is used typically when communicating between two Cisco devices. It is a bit-oriented synchronous data-link layer protocol. HDLC specifies a data encapsulation method on synchronous serial links using frame characters and checksums. If communicating with a non-Cisco device, synchronous PPP is a more viable option.

Point-to-Point Protocol (PPP) -

PPP originally emerged as an encapsulation protocol for transporting IP traffic over point-to-point links. PPP also established a standard for the assignment and management of IP addresses, asynchronous (start/stop) and bit-oriented synchronous encapsulation, network protocol multiplexing, link configuration, link quality testing, error detection, and option negotiation for such capabilities as network-layer address negotiation and data-compression negotiation. PPP supports these functions by providing an extensible Link Control Protocol (LCP) and a family of Network Control Protocols (NCPs) to negotiate optional configuration parameters and facilities. In addition to IP, PPP supports other protocols, including Novell's Internetwork Packet Exchange (IPX) and DECnet.

Link Access Procedure, Balanced-Terminal Adapter - (LAPB-TA) performs that function. (LAPB is sometimes referred to as "X.75," because LAPB is the link layer specified in the ITU-T X.75 recommendation for carrying asynchronous traffic over ISDN.) LAPB-TA allows a system with an ISDN terminal adapter supporting asynchronous traffic over LAPB to call into a router and establish an asynchronous Point to Point Protocol (PPP) session. LAPB supports both local Challenge Handshake Authentication Protocol (CHAP) authentication and external RADIUS authorization on the Authentication, Authorization and Accounting (AAA) server.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 2-12

http://www.cisco.com/en/US/products/sw/iosswrel/ps1830/products_feature_guide09186a0080087992.html

QUESTION 21:

When a cable modem is being provisioned to operate with a host system for Internet services, which two options must occur before Layer 1 and 2 connectivity can occur? (Choose two)

- A. The cable modem must request an IP address and core configuration information from a Dynamic Host Configuration Protocol (DHCP) server.
- B. The cable modem powering up must scan and lock on the RF data channel in the downstream path.
- C. The modem must request a DOCSIS configuration file from a TFTP server.
- D. The cable modem must register with the CMTS.

E. The modem must read specific maintenance messages in the downstream path.

Answer: B, E

Explanation:

According to the DOCSIS (Data-over-Cable Service Interface Specifications) when you first power up a cable modem it starts scanning (starting at a low frequency) for a cable signal. When it 'hears' a cable modem stream it listens for a broadcast (from the service provider) which contains information (ie. frequency) needed to talk back with the head end. It then 'talks back' and if it communicates the right authentication information, it is allowed to proceed. Once these steps are completed, layers 1 and 2 will be operational.

QUESTION 22:

A new ADSL line is being installed in the home office of the Certkiller administrator. What best describes ADSL?

- A. Equal upload and downloads speeds.
- B. Slow upload, fast download speeds.
- C. An ISDN line with no D channel.
- D. Used as a T-1 replacement.

Answer: B

Explanation:

The variation called ADSL (Asymmetric Digital Subscriber Line) is the form of DSL that will become most familiar to home and small business users. ADSL is called "asymmetric" because most of its two-way or duplex bandwidth is devoted to the downstream direction, sending data to the user. Only a small portion of bandwidth is available for upstream or user-interaction messages. However, most Internet and especially graphics- or multi-media intensive Web data need lots of downstream bandwidth, but user requests and responses are small and require little upstream bandwidth. Using ADSL, up to 6.1 megabits per second of data can be sent downstream and up to 640 Kbps upstream. The high downstream bandwidth means that your telephone line will be able to bring motion video, audio, and 3-D images to your computer or hooked-in TV set. In addition, a small portion of the downstream bandwidth can be devoted to voice rather data, and you can hold phone conversations without requiring a separate line.

Reference:

http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci213915,00.html

QUESTION 23:

Router CK1 is configured as shown below:

```
interface ATM0/0
no ip address
```

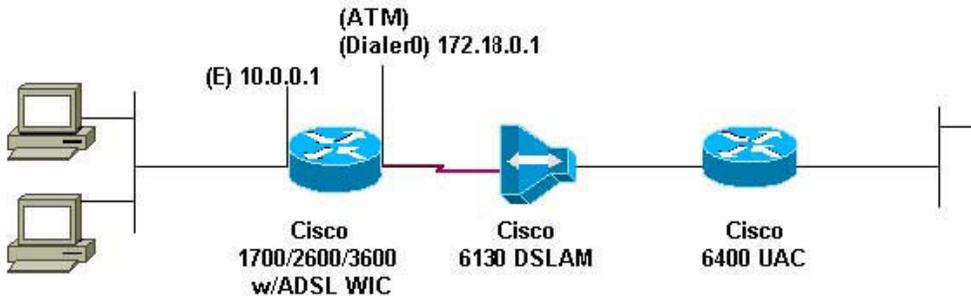
```
pvc 8/35
encapsulation aal5mux ppp dialer
dialer pool-member 1
!
interface dialer 0
ip address negotiated
encapsulation ppp
dialer pool 1
no cdp enable
ppp chap hostname Certkiller
ppp chap password Certkiller
Given the above configuration, which statement is true?
```

- A. This device is configured as a PPPoE client.
- B. This device is configured as a PPPoA client.
- C. This device is configured as RFC 1483/2684 bridge.
- D. This device is configured as an aggregation router.

Answer: B

Explanation:

This following is an example of configuring a Cisco router as a PPPoA client. The command "encapsulation aal5mux ppp dialer" placed under the ATM interface is the indication that it is using PPPoA.



Cisco ADSL WIC

```
!version 12.1
service timestamps debug datetime msec
service timestamps datetime msec
hostname R1
ip subnet-zero
ip dhcp excluded-address 10.0.0.1
!--- the DHCP pool does not lease this address;!---
!--- it is used by interface FastEthernet0
ip dhcp pool poolname
network 10.0.0.0 255.0.0.0
default-router 10.0.0.1
!--- default gateway is assigned to local devices
interface FastEthernet0
ip address 10.0.0.1 255.0.0.0
no ip directed-broadcast
no ip mroute-cache
interface ATM0
no ip address
no ip directed-broadcast
no atm ilmi-keepalive
pvc 1/150
encapsulation aal5mux ppp dialer
dialer pool-member 1
! hold-queue 224 in
interface Dialer0
ip address 172.18.0.1 255.255.0.0
ip nat outside
no ip directed-broadcast
encapsulation ppp
dialer pool 1
dialer-group 2
ppp pap sent-username username password password
ip nat inside source list 1 interface Dialer0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer0
no ip http server
access-list 1 permit 10.0.0.0 0.255.255.255
dialer-list 2 protocol ip permit
end
```

Reference:

http://www.cisco.com/en/US/tech/CK175/CK15/technologies_configuration_example09186a0080093e60.shtml

QUESTION 24:

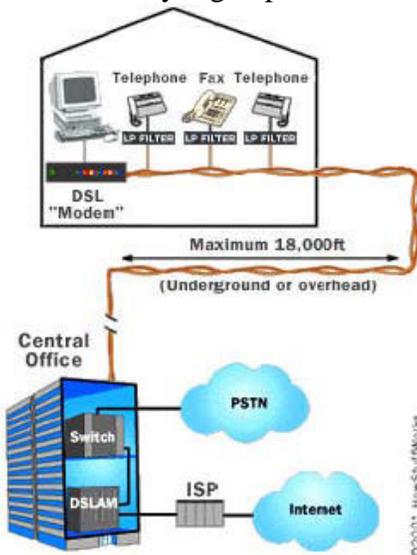
Which two statements are true about DSL? (Choose two)

- A. SDSL and POTS can work together.
- B. It uses the unused bandwidth of your existing phone line.
- C. Bandwidth is shared among users in the same geographical area.
- D. It has a maximum distance limitation of 18,000 feet from the CO.

Answer: B, D

Explanation:

DSL is a very high-speed connection that uses the same wires as a regular telephone line.



Precisely how much benefit you see will greatly depend on how far you are from the central office of the company providing the ADSL service. ADSL is a distance-sensitive technology: As the connection's length increases, the signal quality decreases and the connection speed goes down. The limit for ADSL service is 18,000 feet (5,460 meters) from the central office, though for speed and quality of service reasons many ADSL providers place a lower limit on the distances for the service. At the extremes of the distance limits, ADSL customers may see speeds far below the promised maximums, while customers nearer the central office have faster connections and may see extremely high speeds in the future. ADSL technology can provide maximum downstream (Internet to customer) speeds of up to 8 megabits per second (Mbps) at a distance of about 6,000 feet (1,820 meters), and upstream speeds of up to 640 kilobits per second (Kbps). In practice, the best speeds widely offered today are 1.5 Mbps downstream, with upstream speeds varying between 64 and 640 Kbps.

QUESTION 25:

The configuration of the 827 ADSL router depends on the encapsulation method used for the ADSL connection.

What are the three common encapsulation methods? (Choose three)

- A. PPPoE
- B. PPPoA
- C. HDLC over ATM
- D. DOCSIS
- E. RFC 1483 Bridged
- F. IP over ATM

Answer: A, B, E

Explanation:

Before you can successfully configure your Cisco DSL Router with Asymmetric Digital Subscriber Line (ADSL) service, you need specific information from your Internet Service Provider (ISP). If your ISP is unsure, unable, or unwilling to provide answers to the questions outlined below, you may not be able to correctly configure your Cisco DSL Router.

The most fundamental piece of information you will need is the type of DSL service. The following lists the type of DSL services that are available and can be configured on the Cisco 827 ADSL router:

1. Point-to-Point Protocol over Ethernet (PPPoE)
2. Point-to-Point Protocol over ATM (PPPoA)
3. RFC1483 Bridging
4. RFC1483 Routing

QUESTION 26:

Which of the following is true concerning the characteristics of a packet switching network? (Choose all that apply)

- A. It is more efficient than circuit switching
- B. Bandwidth is dedicated
- C. Bandwidth is shared
- D. It is less costly than a leased line

Answer: A, C, D

Explanation:

Wide Area Networks (WAN) refers to the technologies used to connect offices at remote locations. The size of a network is limited due to size and distance constraints. However networks may be connected over a high speed communications link (called a WAN link) to link them together and thus become a WAN. WAN links are usually:

1. Dial up connection
 2. Dedicated connection - It is a permanent full time connection. When a dedicated connection is used, the cable is leased rather than a part of the cable bandwidth and the user has exclusive use.
 3. Switched network - Several users share the same line or the bandwidth of the line. There are two types of switched networks:
 4. 1. Circuit switching - This is a temporary connection between two points such as dial-up or ISDN.
 2. Packet switching - This is a connection between multiple points. It breaks data down into small packets to be sent across the network. A virtual circuit can improve performance by establishing a set path for data transmission. This will shave some overhead of a packet switching network. A variant of packet switching is called cell-switching where the data is broken into small cells with a fixed length. Packet switching is more efficient than circuit switching. In a packet switching network, the available bandwidth is shared with other subscribers.
- Generally, leased line connections are more expensive than switched networks.

QUESTION 27:

A new ISDN line is being installed at a new Certkiller remote office in New York. At this location, which of the following ISDN functional groups is provided by the end user device?

- A. NT1
- B. NT3
- C. TE2
- D. TE3
- E. LE2
- F. TA
- G. LE

Answer: A

Explanation:

Beyond the TE1 and TE2 devices, the next connection point in the ISDN network is the network termination type 1 (NT1) or network termination type 2 (NT2) device. These are network-termination devices that connect the four-wire subscriber wiring to the conventional two-wire local loop. In North America, the NT1 is a customer premises equipment (CPE) device. In most other parts of the world, the NT1 is part of the network provided by the carrier. The NT2 is a more complicated device that typically is found in digital private branch exchanges (PBXs) and that performs Layer 2 and 3 protocol functions and concentration services. An NT1/2 device also exists as a single device that combines the functions of an NT1 and an NT2.

QUESTION 28:

You are a Cisco Certified Engineer. You are configuring a remote access solution. Your company wants to connect its US office's T1 frame relay network to its European Headquarters. Which of the following types of line should be ordered for the European office?

- A. STM-0
- B. E1
- C. OC-1
- D. DS2
- E. STM-1
- F. T3
- G. STM-2
- H. T1

Answer: B

Explanation:

Similar to the North American T-1, E1 is the European format for digital transmission. E1 carries signals at 2 Mbps (32 channels at 64Kbps), versus the T1, which carries signals at 1.544 Mbps (24 channels at 64Kbps). E1 and T1 lines may be interconnected for international use.

QUESTION 29:

The Certkiller remote access network uses multiple protocols. Which of the following are routed protocols can be used in dial-up networking?

- A. TCP / IP
- B. NetBeui
- C. OSPF
- D. IPX / SPX
- E. IGRP

Answer: A, D

Explanation:

With dial up networking, a number of routed protocols are supported, including TCP/IP and IPX /SPX.

Incorrect Answers:

B: NetBeui is not routable.

C, E: OSPF and IGRP are routing protocols, not routed protocols.

QUESTION 30:

Which of the following are situations ideal for deploying dedicated leased lines, if cost is a concern? (Choose all that apply)

- A. Long distances
- B. Multi sites
- C. Long connect times
- D. Short distances

Answer: C, D

Explanation:

With long connect times, data can be lost, calls are generally longer, and other problems can exist that would make dedicated leased lines a more inexpensive, viable solution. The longer the distance the higher the cost of the line, so for locations near each other, a dedicated T1 or DS3 circuit between the offices will be relatively inexpensive. For multi-site configurations you should use a packet switching service such as frame relay or VPN instead.

QUESTION 31:

Many telecommuters utilize the Certkiller network. Which of the following is true concerning the nature of a Telecommuter location? (Choose all that apply)

- A. Tends to have many users
- B. Needs dedicated connection services most of the time
- C. Needs only dialup services most of the time
- D. Tends to have few numbers of users

Answer: C, D

Explanation:

Telecommuting enables the workforce of an organization to become mobile. Telecommuters generally consist of individual traveling workers or the home based worker. These users typically require only network access on a periodic, as needed basis, and they often utilize dialup services.

QUESTION 32:

DDR over serial lines requires dialing devices that support what industry standard?

- A. V.32a
- B. ITU-T 5
- C. X.121
- D. V.25bis
- E. LAPD
- F. V.26bis

Answer: D

Explanation:

According to the technical documentation at CCO:

DDR over serial lines requires the use of dialing devices that support V.25bis. V.25bis is an International Telecommunication Union Telecommunication (ITU-T) Standardization Sector standard for in-band signaling to bit synchronous data communications equipment (DCE) devices. A variety of devices support V.25bis, including analog V.32 modems, ISDN terminal adapters, and inverse multiplexers. Cisco's implementation of V.25bis supports devices that use the 1984 version of V.25bis (which requires the use of odd parity), as well as devices that use the 1988 version of V.25bis (which does not use parity).

QUESTION 33:

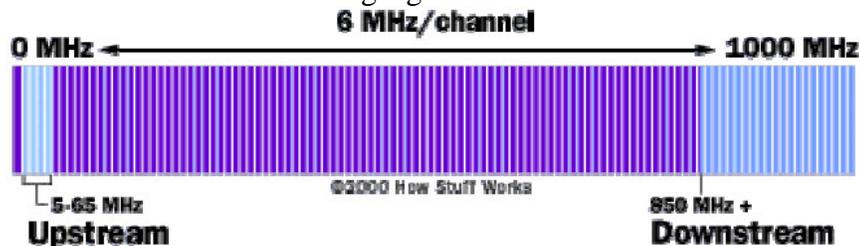
How is cable broadband technology able to transmit downstream and upstream data while at the same time delivering television content?

- A. The cable operator uses the VHF hyperband to transmit and receive data signals.
- B. The cable operator assigns any available spectrum to data, depending on how its own television spectrum is being used.
- C. The cable operator uses specific bandwidths for data signals specified by DOCSIS.
- D. The cable operator places its data signals into clean areas where there is no interference from noise or other signals.

Answer: C

Explanation:

Developed by CableLabs and approved by the ITU in March 1998, Data Over Cable Service Interface Specification (DOCSIS) defines interface standards for cable modems and supporting equipment. In a cable TV system, signals from the various channels are each given a 6-MHz slice of the cable's available bandwidth and then sent down the cable to your house. In some systems, coaxial cable is the only medium used for distributing signals.



When a cable company offers Internet access over the cable, Internet information can use the same cables because the cable modem system puts downstream data -- data sent from the Internet to an individual computer -- into a 6-MHz channel. On the cable, the data looks just like a TV channel. So Internet downstream data takes up the same amount of cable space as any single channel of programming. Upstream data -- information sent from an individual back to the Internet -- requires even less of the cable's bandwidth, just

2 MHz, since the assumption is that most people download far more information than they upload.

QUESTION 34:

DRAG DROP

Drag the correct ISDN reference point to the appropriate description.

S/T	Defines the two-wire interface between the NT-1 and the ISDN cloud	Place here
TA	Defines the interface between the TA and the attached non ISDN device	Place here
U	Defines the four-wire interface between the TE1 or terminal adapter (TA) and an NT	Place here
R		
Q		

Answer:

	Defines the two-wire interface between the NT-1 and the ISDN cloud	U
TA	Defines the interface between the TA and the attached non ISDN device	R
	Defines the four-wire interface between the TE1 or terminal adapter (TA) and an NT	S/T
Q		

QUESTION 35:

What are the drawbacks to using RFC 1482/2684 bridging with ADSL? (Choose three)

- A. Bridging is inherently insecure and requires a trusted environment.
- B. Bridging depends heavily on broadcasts in order to establish connectivity.
- C. Bridging requires expensive routing equipment because of the extensive Layer 3 overhead.
- D. Bridging architecture may allow IP address hijacking.
- E. Bridging, because of its ATM WAN configuration, can require considerable effort during initial troubleshooting.
- F. Bridging architecture can be complex to install and maintain.

Answer: A, B, D

Explanation:

Advantages and Disadvantages of RFC1483 Bridging

Following is a summary of the advantages and disadvantages of the RFC1483 bridging architecture. This architecture has some important disadvantages, most of which are inherent in the bridging model. Some of the disadvantages were noticed during ADSL deployments at customer sites.

Advantages

1. Simple to understand.

Bridging is very simple to understand and implement because there are no complex issues such as routing or authentication requirements for users.

1. Minimal configuration of the CPE.

The service provider considers this important because it no longer requires a large number of truck rolls and no longer needs to invest heavily in personnel for the support of higher level protocols. The CPE in bridge mode acts as a very simple device. Minimal troubleshooting is involved at the CPE because everything that comes in from the Ethernet passes directly to the WAN side.

1. Easy to install.

Bridging architecture is easy to install because of its simplistic nature. After end-to-end permanent virtual circuits (PVCs) are established, activities such as IP at the upper layer protocols become transparent.

1. Multiprotocol support for the subscriber.

When the CPE is in bridging mode, it is not concerned with which upper layer protocol is being encapsulated.

1. Ideal for Internet access in a single user environment.

Because the CPE acts as a set-top box, complex troubleshooting is not required for upper layer protocols. The end PCs do not require additional client installation.

Disadvantages

1. Bridging depends heavily on broadcasts to establish connectivity.

Broadcasts between thousands of users are inherently unscalable. The reasons for this are that the broadcast consumes bandwidth across the users' xDSL loop, and the broadcast requires resources at the head-end router to replicate packets for the broadcast over point-to-point (ATM PVC) media.

1. Bridging is inherently insecure and requires a trusted environment.

The Address Resolution Protocol (ARP) replies can be spoofed and a network address hijacked. Additionally, broadcast attacks can be initiated on the local subnet, thus denying service to all members of the local subnet.

1. IP address hijacking is possible.

Reference:

http://www.cisco.com/en/US/tech/CK175/CK15/technologies_white_paper09186a0080093bd0.shtml#topic3-2

QUESTION 36:

DRAG DROP

Drag the queuing characteristics on the right next to the corresponding queuing method:

Queuing method	Description	Use these
Custom Queuing	place here	prioritizes interactive traffic over file transfers
Weighted Fair Queuing	place here	transmits traffic of a specified protocol or type
Basic Queuing	place here	establishes bandwidth allocations for each type of traffic
Priority Queuing	place here	

Answer:

Queuing method	Description	Use these
Custom Queuing	establishes bandwidth allocations for each type of traffic	
Weighted Fair Queuing	prioritizes interactive traffic over file transfers	
Basic Queuing	place here	
Priority Queuing	transmits traffic of a specified protocol or type	

Explanation:

Traffic arriving at a router interface is handled by a protocol-dependent switching process. The switching process includes delivery of traffic to an outgoing interface buffer. First-in, first-out (FIFO) queuing is the classic algorithm for packet transmission. With FIFO, transmission occurs in the same order as messages are received. Until recently, FIFO queuing was the default for all router interfaces. If users require traffic to be reordered, the department or company must establish a queuing policy other than FIFO queuing.

Cisco IOS software offers three alternative queuing options:

1. Weighted fair queuing (WFQ) prioritizes interactive traffic over file transfers in order to ensure satisfactory response time for common user applications.
2. Priority queuing ensures timely delivery of a specific protocol or type of traffic because that traffic is transmitted before all others.
3. Custom queuing establishes bandwidth allocations for each different type of traffic. Basic Queuing does not exist in Cisco terms.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 13-4

QUESTION 37:

DRAG DROP

Drag the queuing mechanisms on the left to its matching feature on the right hand side:

Flow-Based WFQ	Place here	Four queues; packet starvation possible
Priority Queuing	Place here	Designed to prioritize VoIP traffic; priority and weighted classes
Custom Queuing	Place here	Up to 64 classes; no priority queue(s)
Class-Based WFQ	Place here	Round robin service; user defined bandwidth allocation
Low Latency Queuing	Place here	Interactive traffic gets priority; no classes

Answer:

Priority Queuing	Four queues; packet starvation possible
Low Latency Queuing	Designed to prioritize VoIP traffic; priority and weighted classes
Class-Based WFQ	Up to 64 classes; no priority queue(s)
Custom Queuing	Round robin service; user defined bandwidth allocation
Flow-Based WFQ	Interactive traffic gets priority; no classes

QUESTION 38:

What is the maximum percentage of bandwidth that class-based weighted fair queuing (CBWFQ) allocates by default for all classes of traffic?

- A. 50%
- B. 66.6%
- C. 75%
- D. 90%
- E. 100%
- F. None of the above

Answer: C

Explanation:

For class-based weighted fair queuing (CBWFQ) you can specify traffic classes based on importance. You can give more priority to business critical traffic like VoIP and less priority to music and movie downloads.

CBWFQ Bandwidth Allocation

The sum of all bandwidth allocation on an interface cannot exceed 75 percent of the total available interface bandwidth. The remaining 25 percent is used for other overhead,

including Layer2 overhead, routing traffic, and best-effort traffic. Bandwidth for the CBWFQ class-default class, for instance, is taken from the remaining 25 percent. However, under aggressive circumstances in which you want to configure more than 75 percent of the interface bandwidth to classes, you can override the 75percent maximum sum allocated to all classes or flows using the max-reserved-bandwidth command. If you want to override the default 75 percent, exercise caution and ensure that you allow enough remaining bandwidth to support best-effort and control traffic, and Layer 2 overhead.

Reference: Congestion Management Overview

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/fqcprt2/qcfconmg.htm

QUESTION 39:

You are tasked with determining the best queuing method to use in the Certkiller network. Which queuing methods would be best to use if you had to give strict priority to delay sensitive applications? (Choose all that apply.)

- A. PQ
- B. Flow Base Queuing
- C. Class Base Queuing
- D. LLQ
- E. CQ

Answer: A, D

Explanation:

PQ (priority queuing) and LLQ (low latency queuing) are the queuing methods of choice for voice applications. Priority queuing is the obvious choice, because it allows the administrator to manually configure different priority levels to different types of traffic. LLQ is a newer technology, designed for IPsec.

Low Latency Queueing (LLQ) for IPsec encryption engines helps reduce packet latency by introducing the concept of queueing before crypto engines. Prior to this, the crypto processing engine gave data traffic and voice traffic equal status. Administrators now designate voice traffic as priority. Data packets arriving at a router interface are directed into a data packet inbound queue for crypto engine processing. This queue is called the best effort queue. Voice packets arriving on a router interface are directed into a priority packet inbound queue for crypto engine processing. This queue is called the priority queue. The crypto engine undertakes packet processing in a favorable ratio for voice packets. Voice packets are guaranteed a minimum processing bandwidth on the crypto engine.

BenefitsThe Low Latency Queueing (LLQ) for IPsec encryption engines feature guarantees a certain level of crypto engine processing time for priority designated traffic. Better Voice PerformanceVoice packets can be identified as priority, allowing the crypto engine to guarantee a certain percentage of processing bandwidth. This feature impacts the end user experience by assuring voice quality if voice traffic is directed onto a congested network.

Improved Latency and Jitters Predictability is a critical component of network performance. The Low Latency Queueing (LLQ) for IPSec encryption engines feature delivers network traffic predictability relating to VPN. With this feature disabled, an end user employing an IP phone over VPN might experience jitter or latency, both symptoms of overall network latency and congestion. With this feature enabled, these undesirable characteristics are dissipated.

Reference:

Building Cisco Remote Access Network Student Guide version2, page 9-49

http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a008013489a.html

QUESTION 40:

You are tasked with determining the best queuing method to use in the Certkiller network. In regards to traffic control; which queuing method gives preferential service to low-volume traffic streams?

- A. FIFO Queuing
- B. Priority Queuing
- C. Custom Queuing
- D. Weighted Fair Queuing
- E. Low Latency Queuing
- F. None of the above

Answer: D

Explanation:

In WFQ, traffic is sorted by high- and low-volume conversations. The traffic in a session is kept within one conversation (session), and the records are handled FIFO within a particular conversation. The lower volume interactive traffic is given a priority and flows first. The necessary bandwidth is allocated to the interactive traffic, and the high volume conversations equally share whatever band width is left over.

Reference: CCNP Remote Access Exam Certification Guide, page 298, Brian Morgan & Craig Dennis, Cisco Press 2001, ISBN 1-58720-003-1

QUESTION 41:

Which answer correctly describes the effectiveness of the Weighted Random Early Detection (WRED) mechanism that is being used on the Certkiller network?

- A. It is effective on UDP packets and will not allow tail drops.
- B. It is effective on UDP packets and will allow tail drops.
- C. It is effective on TCP packets and will not allow tail drops.
- D. It is effective on TCP packets and will allow tail drops.
- E. None of the above

Answer: D

Explanation:

Weighted Random Early Detection provides quality of service, by randomly sacrificing some TCP packets when the line's on the verge of congestion to prevent transmission failure. When TCP realizes that its packets are being dropped, it slows down its transmission rate from the source. Since TCP 'guarantees' that packets do arrive and they do arrive in order, the randomly dropped packet will eventually get resent.

Reference: Byte-Based Weighted Random Early Detection

http://www.cisco.com/en/US/products/sw/iosswrel/ps1829/products_feature_guide09186a00801b240a.html

QUESTION 42:

You are tasked with determining the best queuing method to use in the Certkiller network. Which one of the following queuing method dynamically sorts traffic into messages that make up conversations?

- A. Priority
- B. WFQ
- C. Custom
- D. FIFO

Answer: B

Explanation:

WFQ does not require configuration of access lists to determine the preferred traffic on a serial interface. Rather, the fair queue algorithm dynamically sorts traffic into messages that are part of a conversation.

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_configuration_guide_chapter09186a00800c

QUESTION 43:

Which queuing strategies will you find already enabled by default on a Cisco WAN router? (Choose all that apply)

- A. FIFO
- B. Custom
- C. Priority
- D. Weighted Fair
- E. LLQ
- F. LIFO

Answer: A, D

Explanation:

Traffic arriving at a router interface is handled by a protocol-dependent switching process. The switching process includes delivery of traffic to an outgoing interface buffer. First-in, first-out (FIFO) queuing is the classic algorithm for packet transmission. With FIFO, transmission occurs in the same order as messages are received. Until recently, FIFO queuing was the default for all router interfaces. If users require traffic to be reordered, the department or company must establish a queuing policy other than FIFO queuing.

QUEUING COMPARISON		
Weighted Fair Queuing	Priority Queuing	Custom Queuing
No queue lists	4 queues	16 queues
Low volume given priority	High queue serviced first	Round-robin service
Conversation dispatching	Packet dispatching	Threshold dispatching
Interactive traffic prioritized	Critical traffic prioritized	Allocation of available bandwidth
File transfers have balanced access	Designed for low-bandwidth links	Designed for higher speed, low-bandwidth links
Enabled by default	Must be configured	Must be configured

By default, FIFO is used as the queuing method for links greater than T1, while WFQ is used for all links T1 and below.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 13-35

QUESTION 44:

On a Frame Relay interface operating at T1 speed; what is the default factory set queuing method used?

- A. First in, first out queuing (FIFO)
- B. Class-based weighted fair queuing (CBWFQ)
- C. Weighted fair queuing (WFQ)
- D. Priority queuing (PQ)
- E. Low-latency queuing (LLQ)

Answer: C

Explanation:

By default, FIFO is used as the queuing method for links greater than T1, while WFQ is used for all links T1 and below.

QUEUING COMPARISON		
Weighted Fair Queuing	Priority Queuing	Custom Queuing
No queue lists	4 queues	16 queues
Low volume given priority	High queue serviced first	Round-robin service
Conversation dispatching	Packet dispatching	Threshold dispatching
Interactive traffic prioritized	Critical traffic prioritized	Allocation of available bandwidth
File transfers have balanced access	Designed for low-bandwidth links	Designed for higher speed, low-bandwidth links
Enabled by default	Must be configured	Must be configured

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 13-35

QUESTION 45:

On a remote Certkiller router, the following command was issued:

```
Router# show traffic-shape
Interface Se1.1
  Access Target  Bytes  Sustain  Access  Interval  Increment  Adapt
  VC   List  Rate  Limit  bits/int  bits/int  (ms)      (bytes)   Active
  202          100000 2000   8000   8000    80       1000     BECN
```

Given the above output, what is the current CIR for this VC?

- A. 1000
- B. 2000
- C. 8000
- D. 100000

Answer: D

Explanation:

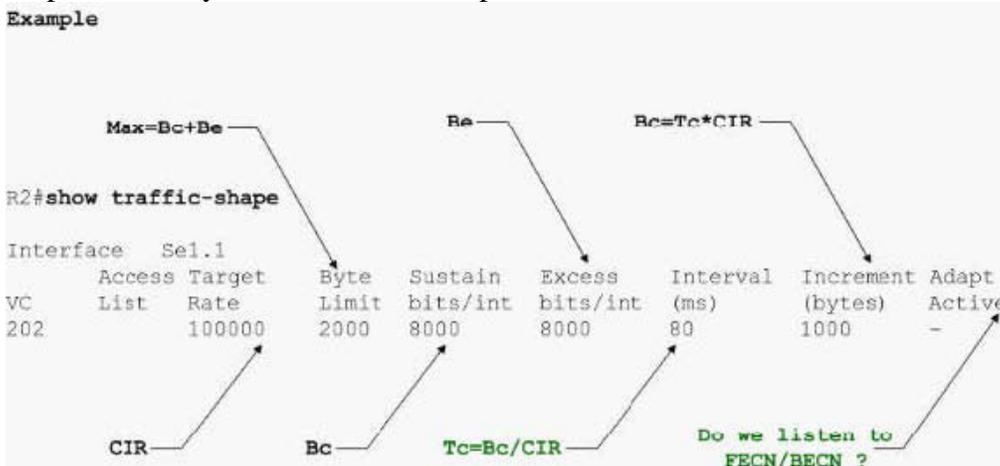
Use the show traffic-shape EXEC command to display the current traffic-shaping configuration. The command output contains the following fields.

Field	Description
Target Rate	Rate that traffic is shaped to in bps.
Byte Limit	Maximum number of bytes transmitted
	per internal interval.
Sustain bits/int	Configured sustained bits per interval.
Excess bits/int	Configured excess bits in the first
	interval.
Interval (ms)	Interval being used internally. This interval may be smaller than the Bc divided by the CIR if the router determines that traffic flow will be

	more stable with a smaller configured interval.
Increment (bytes)	Number of bytes that are sustained per
	internal interval.
Adapt Active	Contains BECN if Frame Relay has
	BECN adaptation configured.

The following is sample output of the show traffic-shape command.

Target Rate = CIR = 100000 bits/s
Mincir = CIR/2 = 100000/2 = 50000 bits/s
Sustain = Bc = 8000 bits/int
Excess = Be = 8000 bits/int
Interval = Bc/CIR = 8000/100000 = 80 ms
Increment = Bc/8 = 8000/8 = 1000 bytes
Byte Limit = Increment + Be/8 = 1000 + 8000/8 = 2000 bytes
The diagram below maps the fields described above to some sample output shown by the show traffic-shape command:



The target rate specifies the CIR. In our example the CIR is 100000.

Reference:

http://www.cisco.com/en/US/tech/ CK7 13/ CK2 37/technologies_tech_note09186a0080093c06.shtml

QUESTION 46:

Which statement defines a feature of the frame relay Local Management Interface (LMI)?

- A. An LMI describes how different Frame Relay Service provider networks connect to another.
- B. An LMI identifies the logical virtual circuit between the CPE and the Frame Relay switch and is associated with a destination address.
- C. An LMI dynamically discovers the protocol address of the remove device associated

with a given PVC.

D. An LMI is signaling standard responsible for managing the connection and maintaining status between the CPE device and the Frame Relay switch.

E. None of the above.

Answer: D

Explanation:

The Local Management Interface (LMI) is a set of enhancements to the basic Frame Relay specification. The LMI was developed in 1990 by Cisco Systems, StrataCom, Northern Telecom, and Digital Equipment Corporation. It offers a number of features (called extensions) for managing complex internetworks. Key Frame Relay LMI extensions include global addressing, virtual circuit status messages, and multicasting. The LMI global addressing extension gives Frame Relay data-link connection identifier (DLCI) values global rather than local significance. DLCI values become DTE addresses that are unique in the Frame Relay WAN. The global addressing extension adds functionality and manageability to Frame Relay internetworks. Individual network interfaces and the end nodes attached to them, for example, can be identified by using standard address-resolution and discovery techniques. LMI is fundamentally a connection management and maintenance signal between the frame relay router at the customer's premise, and the service providers frame relay switch.

LMI virtual circuit status messages provide communication and synchronization between Frame Relay DTE and DCE devices. These messages are used to periodically report on the status of PVCs, which prevents data from being sent into black holes (that is, over PVCs that no longer exist).

QUESTION 47:

FRTS is being configured on router CK1 . In Frame Relay traffic shaping, what does the term committed burst (Bc) refer to?

- A. The rate, in bits per second, at which the Frame Relay switch agrees to transfer data.
- B. The maximum number of bits that the switch agrees to transfer during any Tc.
- C. The maximum number of uncommitted bits that the Frame Relay switch attempts to transfer beyond the CIR for the first time interval only.
- D. The number of bits, during any Tc, over the CIR that can be transmitted but will be marked DE.

Answer: B

Explanation:

In Frame Relay Traffic Shaping, the following terms are used:

CIR (Committed Information Rate) - The average rate at which you want to transmit.

This is generally not the same as the CIR provided by the telco. This is the rate at which you want to send in periods of noncongestion.

Bc (Committed Burst) - The maximum amount of data to send in each Tc interval.

Be (Excessive Burst) -

The amount of excess data allowed to be sent during the first interval once credit is built up. Transmission credit is built up during periods of nontransmission. The credit is the burst size. Full credit is typically CIR / 8.

Tc (Committed Rate Measurement Interval) - The Bc / CIR time interval. The time interval shouldn't exceed 125 ms (almost always 125 ms).

QUESTION 48:

When using a Cisco router, how are routing updates and hellos processed when using custom queuing?

- A. They do not need to be queued.
- B. They are automatically placed in queue 0.
- C. They must manually be placed in a high priority queue.
- D. They must be part of a policy map to ensure that they have guaranteed bandwidth.

Answer: B

Explanation:

The following frequently asked question is posted within the Cisco forum:

Q: If custom queuing has been configured, do routing protocol updates such as Link-State Advertisements (LSAs) for Open Shortest Path First (OSPF) and broadcasts for Routing Information Protocol (RIP) and Interior Gateway Routing Protocol (IGRP) get queued in the special system queue 0, or do they get queued in the IP queue?

A: In addition to low level keepalives, some protocols -- whose traffic is originated by the router -- use queue 0 for their time critical packets. Specifically:

ISO IGRP hellos

ESIS hellos

ISIS hellos

DECnet hellos

SLARP address resolution

EIGRP hellos

OSPF hellos

Router syslog messages

Spanning tree keepalives

Reference:

http://www.cisco.com/en/US/tech/CK543/CK544/technologies_tech_note09186a0080093f90.shtml

QUESTION 49:

The following output was seen on a Certkiller router:

```
CK1#show policy-map
Policy Map POLICY-1
Class VoIP
  Bandwidth 64 (kbps)
  exponential weight 9
  class min-threshold max-threshold mark-probability
  -----
  0 - - 1/10
  1 - - 1/10
  2 - - 1/10
  3 - - 1/10
  4 - - 1/10
  5 - - 1/10
  6 - - 1/10
  7 - - 1/10
  rsvp - - 1/10

Policy Map POLICY-2
Class VoIP
  Bandwidth 48 (kbps) Max Threshold 256 (packets)

Policy Map POLICY-4
Class VOICE-TRAFFIC
  Bandwidth 64 (kbps) Max Threshold 64 (packets)
Class VOICE-SIGNALING
  Bandwidth 64 (kbps) Max Threshold 64 (packets)
CK1#
```

Based on the above information and assuming a 64K link, which policy-map configuration will best ensure that packets classified as voice are not dropped in favor of other network traffic?

- A. POLICY-1
- B. POLICY-2
- C. POLICY-3
- D. POLICY-4

Answer: B

Explanation:

When configuring QoS service policies to support voice and video, you need to ensure that adequate bandwidth exists for all required applications. Start your configuration by adding up the minimum bandwidth requirements for each major application, such as the voice media streams, video streams, voice control protocols, and all data traffic. This sum represents the minimum bandwidth requirement for any given link and should consume no more than 75% of the total bandwidth available on that link. Importantly, this 75% rule leaves bandwidth for two types of overhead traffic:

1. Routing protocol updates and layer-2 keepalives.
2. Additional applications such as e-mail, HTTP traffic, and other data traffic that is not so easily measured.

In addition, the 75% rule reserves bandwidth for two sets of layer-2 overhead:

1. Layer-2 overhead in traffic classes that you define. On ATM Permanent Virtual Circuits (PVCs), the bandwidth parameter specified in the bandwidth and priority

commands does not count or include the padding to make the last cell an even multiple of 48 bytes or the five bytes of each cell's header.

2. Layer-2 overhead of packets that match to the class-default class in a QoS service policy.

Only policy map 2 will accommodate for the overhead traffic, using 48 kbps of the available 64 kbps bandwidth, which is 75%.

QUESTION 50:

Which statement is true concerning compression?

- A. MNP-5 and V.42bis modem compression specifications are compatible.
- B. MNP-5 modem compression can be used in conjunction with payload compression.
- C. Layer 3 encryption can be used in conjunction with link compression.
- D. Payload compression uses more memory than link compression.

Answer: D

Explanation:

Compressing the data payload can result in more data throughput than what is possible using link compression alone. However, payload compression may not always be appropriate, and can be affected by the following things:

1. No Standards: Although Cisco IOS software supports several compression algorithms, they are proprietary and not necessarily interoperable.

Note: Both ends of a compression transaction must support the same algorithms.

1. Data Type: The same compression algorithm yields different compression ratios depending upon the type of data undergoing compression. Certain data types are inherently less compressible than others, which can realize up to a 6:1 compression ratio. Cisco conservatively averages Cisco IOS compression ratios at 2:1.

2. Already Compressed Data: Trying to compress already compressed data, such as JPEG or MPEG files can take longer than transferring the data without any compression at all.

3. Processor Usage: Software compression solutions consume valuable processor cycles in the router. Routers must also support other functions such as management, security, and protocol translations; compressing large amounts of data can slow down router performance and cause network latency. Performing payload compression can consume a great deal of memory and be CPU processor intensive.

The highest compression ratio is usually reached with highly compressible text files.

Compressing data can cause performance degradation because it is software, not hardware compression. While configuring compression, use caution with smaller systems that have less memory and slower CPUs.

QUESTION 51:

An interface on a Certkiller router is experiencing problems where the high priority traffic is successfully passing through but the lower priority traffic is not moving through at all. Which queuing method is most likely contributing to this problem?

- A. WFQ
- B. Priority
- C. Custom
- D. FIFO
- E. All of the above

Answer: B

Explanation:

PQ ensures that important traffic gets the fastest handling at each point where it is used.

It was designed to give strict priority to important traffic.

PQ guarantees strict priority in that it ensures that one type of traffic will be transmitted, possibly at the expense of all others. For PQ, a low priority queue can be detrimentally affected, and, in the worst case, never allowed to transmit its packets if there is a limited amount of available bandwidth or if the transmission frequency of critical traffic is high.

The following table compares some of the different queueing options:

	WFQ	CQ	PQ
Number of Queues	1. Configurable	1. 16 user queues	1. 4 queues
	number of queues	(256	
	user queues, by		
	default)		
Kind of Service	1. Ensures fairness among all traffic based on weights	1. Round-robin service 2. Proportional allocation of bandwidth for different classes	1. High priority queues serviced first 2. Absolute priority
Configuration	1. No configuration	1. Requires	1. Requires
	required	configuration	configuration

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_configuration_guide_chapter09186a00800c

QUESTION 52:

Your absent minded junior administrator has enabled AAA authentication on the Certkiller network, but forgot to set the authentication. What will happen when a user try's to login?

- A. Disallow a user from access to all resources after login.
- B. Allow any user to login without checking the authentication data.
- C. Record all access of resources and how long the user accessed each resource.
- D. Allow a user to access all resources after login.
- E. Not to record any access of resources after login.
- F. Disallow any user from logging in with or without a valid username and password.

Answer: F

Explanation:

The three parts of AAA are defined as follows:

Authentication: Authentication determines the identity of users and whether they should be allowed access to the network. Authentication allows network managers to bar intruders from their networks.

Authorization: Authorization allows network managers to limit the network services available to each user. Authorization also helps restrict the exposure of the internal network to outside callers. Authorization allows mobile users to connect to the closest local connection and still have the same access privileges as if they were directly connected to their local networks. You can also use authorization to specify which commands a new system administrator can issue on specific network devices.

Accounting: System administrators might need to bill departments or customers for connection time or resources used on the network (for example, bytes transferred).

Accounting tracks this kind of information. You can also use the accounting syslog to track suspicious connection attempts into the network and trace malicious activity.

To enable AAA on a router we would type:

```
Router(config)#aaa new-model
```

If authentication is not specifically set for a line, the default is to deny access and no authentication is performed. To set the AAA authentication we must use the following command:

```
Router(config)#aaa authentication [login | enable | arap |  
ppp | nasi] method
```

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 15-11

QUESTION 53:

What six types of accounting information does a TACACS+ / RADIUS server record?

- A. Connection, protocol, system, network, command, and resource
- B. Resource, interface, connection, system, command, and network
- C. Command, system, exec, network, connection, and resource

- D. Network, interface, exec, protocol, system, and resource
- E. Crypto, system, network, protocol, command, and resource
- F. None of the above

Answer: C

Explanation:

AAA Accounting - AAA accounting can supply information concerning user activity back to the database. This concept was especially helpful in the early days of Internet service when many ISPs offered 20 or 40 hours per week at a fixed cost and hourly or minute charges in excess of the specified timeframe. Today it is much more common for the ISP charge to be set for an unlimited access time. This does not, however, minimize the power of accounting to enable the administrator to track unauthorized attempts and proactively create security for system resources. In addition, accounting can be used to track resource usage to better allocate system usage.

Accounting is generally used for billing and auditing purposes and is simply turned on for those events that are to be tracked. The commands follow this general syntax:

```
aaa accounting what-to-track how-to-track where-to-send-the-information
```

The what-to-track arguments are as follows:

network - With this argument, network accounting logs the information, on a user basis, for PPP, SLIP, or ARAP sessions. The accounting information provides the time of access and the network resource usage in packet and byte counts.

connection - With this argument, connection accounting logs the information about outbound connections made from the router or RAS device, including Telnet and rlogin sessions. The key word is outbound; it enables the tracking of connections made from the RAS device and where those connections were established.

exec - With this argument, EXEC accounting logs the information about when a user creates an EXEC terminal session on the router. The information includes the IP address and telephone number, if it is a dial-in user, and the time and date of the access. This information can be particularly useful for tracking unauthorized access to the RAS device.

system - With this argument, system accounting logs the information about system-level events. System-level events include AAA configuration changes and reloads for the device. Again, this information would be useful to track unauthorized access or tampering with the router.

command - With this argument, command accounting logs information regarding which commands are being executed on the router. The accounting record contains a list of commands executed for the duration of the EXEC session, along with the time and date information.

resource - Before AAA resource failure stop accounting, there was no method of providing accounting records for calls that failed to reach the user authentication stage of a call setup sequence. Such records are necessary for users employing accounting records to manage and monitor their networks and their wholesale customers.

This command was introduced in Cisco IOS Software Release 12.1(3)T.

Reference:

QUESTION 54:

AN IPSec secure tunnel is being built between routers CK1 and CK2 . In IPSec, what are the common services provided by Authentication Header (AH) and Encapsulation Security Payload (ESP)?

- A. Data origin authentication, confidentiality, and anti-replay service
- B. Confidentiality, data integrity, and anti-replay service
- C. Data integrity, data origin authentication, and anti-replay service
- D. Confidentiality, data integrity, and data origin authentication
- E. Confidentiality, data integrity and authorization.

Answer: C

Explanation:

AH (Authentication Header) is used to provide data integrity and authentication. It does not provide any form of encryption to the payload of the packet. AH uses a keyed one-way hash function (also called an HMAC) such as MD5 or SHA-1 to guarantee the integrity and origin of the packet. Optionally, it can provide anti-replay protection.

ESP (Encapsulating Security Payload) is primarily used to provide payload encryption. With the current revisions of the RFC for ESP, it also includes the ability to provide authentication and integrity.

Because ESP can do all the services needed in a secure VPN network (including optional Ahs services), most implementations do not include any AH options. When the IPSec standard was created, its developers took into account the need for increased security. Therefore, IPSec can use different algorithms for payload encryption, such as DES to give you 56-bit encryption or 3DES to give you 168-bit encryption. As the need for stronger payload encryption arises, the standard will allow vendors to implement other algorithms.

Reference:

Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)

Page 435 & 436

QUESTION 55:

ADSL broadband connections using the PPPoE access method typically uses which type of user authentication method?

- A. AAA authentication
- B. DNIS authentication
- C. Caller-ID authentication
- D. PPP CHAP authentication
- E. IPSec authentication

F. L2TP authentication

Answer: D

Explanation:

Once the DSL device is installed and configured for PPPoE the encapsulation of all traffic with PPPoE/PPP headers is performed. The default authentication mechanism for PPPoE is Password Authentication Protocol (PAP). The user has the option to configure Challenge Handshake Authentication Protocol (CHAP) or MS-CHAP manually. Generally, the CHAP method is preferred and is normally used to overcome the security limitations of PAP.

QUESTION 56:

PPP authentication is being configured on router CK1 . What can PPP use to authenticate callers? (Choose all that apply.)

- A. Authentication key
- B. Message digest key
- C. CHAP
- D. PAP
- E. IPSec

Answer: C, D

Explanation:

Authentication, using either PAP or CHAP, is used as a security measure with PPP and PPP callback. Authentication allows the dial-up target to identify that any given dial-up client is a valid client with a pre-assigned username and password. If you have decided to use an authentication protocol, it will likely be PAP or CHAP. PAP is a one-way authentication between a host and a router, or a two-way authentication between routers. For PAP this process provides an insecure authentication method. If you put a protocol analyzer on the line the password will be revealed in clear text. There is no protection from "playback," which means that if you have a sniffer connected to the line and you capture the packet, you could use the packet to authenticate your way directly into the network by "playing back" the captured packet.

For more secure access control, you should use CHAP rather than PAP as the authentication method. Only use PAP if that is the only method of authentication the remote station supports.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 5-13

QUESTION 57:

Multilink PPP is being configured on router CK1 in order to bond together 2 T1's together. What is true about multilink PPP? (Choose all that apply.)

- A. MLP can identify bundles only through the authenticated name.
- B. MLP can be applied to any link type utilizing PPP encapsulation.
- C. MLP is a negotiated option only during the LCP phase of PPP.
- D. For MLP to bind links, configuring AAA authentication is a required.
- E. None of the above.

Answer: A, B

Explanation:

Multilink PPP takes advantage of multiple bearer channels to improve throughput. Datagram's are split, sequenced, transmitted across multiple links, and then recombined at the destination. The multiple links together are called a bundle.

Multilink PPP (MLP) provides load balancing over dialer interfaces, including ISDN, synchronous, and asynchronous interfaces. MLP can improve throughput and reduce latency between systems by splitting packets and sending the fragments over parallel circuits. Prior to MLP, two or more ISDN B channels could not be used in a standardized way while ensuring sequencing. MLP is most effective when used with ISDN.

MLP solves several problems related to load balancing across multiple WAN links, including the following:

1. Multivendor interoperability, as specified by RFC 1990, which replaces RFC 1717
2. Packet fragmentation, improving latency of each packet (supports RFC 1990 fragmentation and packet sequencing specifications)
3. Packet sequence and load calculation

This feature negotiates the Maximum Received Reconstructed Unit (MRRU) option during the PPP LCP negotiation to indicate to its peer that it can combine multiple physical links into a bundle.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 5-34 to 5-36

QUESTION 58:

MLPPP is being used on interface BRI0 of router CK1 . What is true about Multilink PPP when it's used on an ISDN BRI link?

- A. The D channel can be activated when outbound traffic exceeds the dialer load threshold.
- B. The second channel remains active for the remainder of the call, regardless of bandwidth demands.
- C. The second active channel can only be used for outbound traffic.
- D. Both outbound and inbound loads can be used to determine when to activate the second channel.
- E. Only inbound loads can be used to determine when to activate a second channel.

Answer: D

Explanation:

Multilink PPP is a specification that enables the bandwidth aggregation of multiple links into one logical pipe. Its mission is comparable to that of Cisco's BoD. More specifically, the Multilink PPP feature provides load-balancing functionality over multiple WAN links, while providing multi-vendor interoperability, packet fragmentation and proper sequencing, and load calculation on both inbound and outbound traffic. The "load" IOS configuration command is used to specify the load that must be exceeded on the first BRI B channel before the second B channel is utilized.

Reference:

Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)

Page 179

QUESTION 59:

Multilink PPP is being configured on all of the Certkiller ISDN routers. Which of the following correctly describe the features of Multilink PPP? (Choose all that apply)

- A. Multilink PPP has multi-vendor interoperability, as specified by RFC 1990.
- B. Multilink PPP uses packet sequence and load calculation.
- C. Multilink PPP compresses the 20 byte IP header to a 2 or 4 byte header to reduce overhead.
- D. Multilink PPP implements an indexing system that predicts character sequences.

Answer: A, B

Explanation:

Multilink PPP (MLP) provides load balancing over dialer interfaces, including ISDN, synchronous, and asynchronous interfaces. MLP can improve throughput and reduce latency between systems by splitting packets and sending the fragments over parallel circuits. Prior to MLP, two or more ISDN B channels could not be used in a standardized way while ensuring sequencing. MLP is most effective when used with ISDN. MLP solves several problems related to load balancing across multiple WAN links, including the following:

1. Multi-vendor interoperability, as specified by RFC 1990, which replaces RFC 1717
2. Packet fragmentation, improving latency of each packet (supports RFC 1990 fragmentation and packet sequencing specifications)
3. Packet sequence and load calculation

This feature negotiates the Maximum Received Reconstructed Unit (MRRU) option during the PPP LCP negotiation to indicate to its peer that it can combine multiple physical links into a bundle.

Prior to the adoption of RFC 1990, there was no standardized way to use both of the B channels and ensure proper sequencing. MLP is interoperable between Cisco routers running Cisco IOS software and

Cisco 700 series routers, and with most routers that conform to RFC 1990.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 5-34

QUESTION 60:

In a PPP connection; what purpose is served by LCP (link control protocol)?

- A. It negotiates the IP address.
- B. It negotiates the frequency on the link.
- C. It negotiates the error correction.
- D. It negotiates the modulo size.
- E. All of the above

Answer: C

Explanation:

The PPP LCP (Link Control Protocol) provides a method of establishing, configuring, maintaining, and terminating a point-to-point connection. The four PPP LCP options are Authentication, Callback, Compression, and Multilink. With LCP, the link is maintained via the use of error correcting mechanisms.

Note: To establish communications over an ISDN link, each end of the PPP link must first send Link Control Protocol (LCP) packets to configure and test the data link.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 5-11

QUESTION 61:

Which tunneling protocol connects the user to an access concentrator, which then tunnels individual PPP frames to a network access server (NAS) for processing away from the location of the circuit termination?

- A. GRE
- B. IPSEC
- C. L2TP
- D. MPLS VPN
- E. IPSec
- F. None of the above

Answer: C

Explanation:

L2TP extends the PPP model by allowing the L2 and PPP endpoints to reside on different devices interconnected by a packet-switched network. With L2TP, a user has an L2 connection to an access concentrator (e.g., modem bank, ADSL DSLAM, etc.), and the concentrator then tunnels individual PPP frames to the NAS. This allows the actual processing of PPP packets to be divorced from the termination of the L2 circuit.

L2TP uses packet-switched network connections to make it possible for the endpoints to be located on different machines. The user has an L2 connection to an access concentrator, which then tunnels individual PPP frames to the NAS, so that the packets can be processed separately from the location of the circuit termination. This means that the connection can terminate at a local circuit concentrator, eliminating possible long-distance charges, among other benefits. From the user's point of view, there is no difference in the operation.

References: http://whatis.techtarget.com/definition/0,289893,sid9_gci493383,00.html
<http://www.faqs.org/rfcs/rfc2661.html>

QUESTION 62:

Multilink PPP is being utilized on the Certkiller network. What are some of the virtues of the multilink PPP protocol (MLPPP)? (Choose all that apply)

- A. MLP splits packets and sends fragments over multiple links.
- B. MLP is effective with ISDN.
- C. Timing is critical because MLP does not support sequencing.
- D. MLP uses a round-robin algorithm to send unfragmented individual packets across multiple lines.
- E. None of the above.

Answer: A, B

Explanation:

Multilink PPP takes advantage of multiple bearer channels to improve throughput. Datagrams are split, sequenced, transmitted across multiple links, and then recombined at the destination. The multiple links together are called a bundle.

Multilink PPP (MLP) provides load balancing over dialer interfaces, including ISDN, synchronous, and asynchronous interfaces. MLP can improve throughput and reduce latency between systems by splitting packets and sending the fragments over parallel circuits. Prior to MLP, two or more ISDN B channels could not be used in a standardized way while ensuring sequencing. MLP is most effective when used with ISDN.

MLP solves several problems related to load balancing across multiple WAN links, including the following:

1. Multivendor interoperability, as specified by RFC 1990, which replaces RFC 1717
2. Packet fragmentation, improving latency of each packet (supports RFC 1990 fragmentation and packet sequencing specifications)
3. Packet sequence and load calculation

This feature negotiates the Maximum Received Reconstructed Unit (MRRU) option during the PPP LCP negotiation to indicate to its peer that it can combine multiple physical links into a bundle.

Incorrect Answers:

C: MLPPP does indeed support sequencing. This function is needed for packet re-assembly.

D: MLPPP works by first fragmenting the data and then sending it across the link.

Although round robin load balancing (packet by packet) is supported, load balancing is done on a per session basis by default.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 5-34 to 5-36

QUESTION 63:

The Link Control Protocol (LCP) is used within PPP. What four PPP options are negotiated with LCP? (Choose four)

- A. Multilink
- B. Callback
- C. Rate adaptation
- D. Authentication
- E. Accounting
- F. Compression
- G. Authorization
- H. Load Balancing

Answer: A, B, D, F

Explanation:

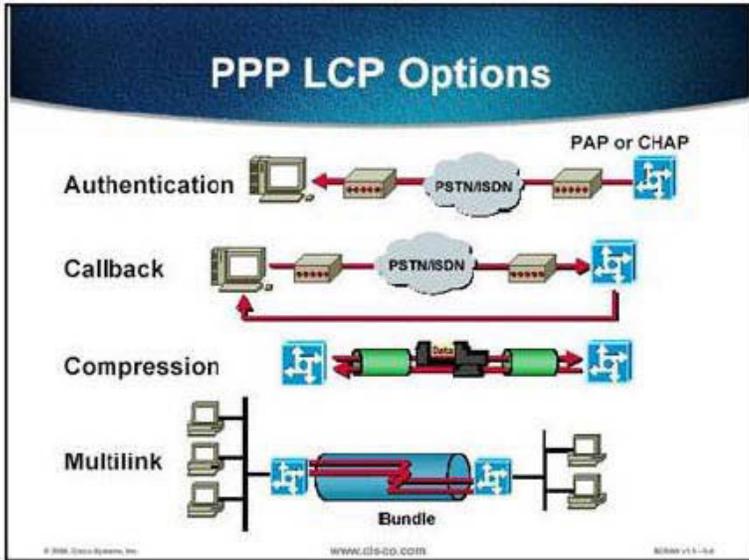
* Authentication using either PAP or CHAP is used as a security measure with PPP and PPP callback. Authentication allows the dialup target to identify that any given dialup client is a valid client with a pre-assigned username and password.

* Callback is a PPP option used to provide call and dialup billing consolidation. PPP callback was first supported in Cisco IOS(r) Release 11.0(3).

* Compression is used to improve throughput across existing lines. PPP compression was first supported in Cisco IOS Release 10.3.

* Multilink PPP takes advantage of multiple bearer channels to improve throughput.

Datagrams are split, sequenced, transmitted across multiple links, and then recombined at the destination. The multiple links together are called a bundle. Multilink PPP was first supported in Cisco IOS Release 11.0(3).



Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 5-11

QUESTION 64:

Which of the following commands will configure PPP authentication to work for a dialer profile?

- A. dialer remote-name
- B. dialer pool-member
- C. dialer string
- D. dialer map
- E. dialer idle-timeout

Answer: A

Explanation:

To specify the authentication name of the remote router on the destination subnetwork for a dialer interface, use the dialer remote-name command in interface configuration mode. To remove the specified name, use the no form of this command.

Incorrect Answers:

B: This command specifies the dialer pool that the individual interface should belong to, and does not deal with the authentication of remote routers.

C: This command deals with the number to dial to connect the ISDN call.

D: This is not related to authentication.

E: This specifies the timeout value used to drop the ISDN call. If no interesting traffic is seen during this time, the call is dropped.

QUESTION 65:

To enable PPP on an asynchronous line 2; what two commands would you use?

- A. Certkiller A(config-if)#encapsulation ppp
- B. Certkiller A(config-if)#physical-layer async
- C. Certkiller A(config)#interface async 2
- D. Certkiller A(config-if)#async 2
- E. Certkiller A(config-if)#ppp encapsulation

Answer: A, C

Explanation:

There is often confusion between the interface async and line commands. The major difference is that the interface async command lets you configure the protocol (logical) aspects of an asynchronous port, while the line command lets you configure the physical aspects of the same port. The async commands can be thought of as internal, while the line commands configure external characteristics of the configuration.

For example, you configure the basic modem-related parameters on an access server using the line command, but you configure the protocol encapsulation and authentication schemes with the interface async command.

physical-layer async - Sets the serial interface to asynchronous mode.

async 2 - Is not a valid IOS command.

encapsulation ppp - Enables the PPP encapsulation. The "ppp encapsulation" command is not valid. The correct syntax is "encapsulation ppp"

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Chapter 5

QUESTION 66:

Link compression needs to be configured on all of the Certkiller routers. Which of the following command lines would you see if you had to configure software compression for: LAPB, PPP, or HDLC on a link?

- A. Router(config-if)#ip rtp header-compression [passive]
- B. Router(config-if)#ip tcp header-compression [passive]
- C. Router(config-if)#frame-relay payload-compress
- D. Router(config-if)#compress [predictor|stac|mppc]

Answer: D

Explanation:

To configure compression, there are several commands. Most are technology-specific and fairly intuitive. The compress configuration command is used at the interface level (normally a slow serial interface) to select the link-compression algorithm. Remember to configure the same compression type on both ends of the point-to-point link.

Data compression reduces the size of data frames to be transmitted over a network link. Reducing the size of a frame reduces the time required to transmit the frame across the network. Data compression provides a coding scheme at each end of a transmission link

that allows characters to be removed from the frames of data at the sending side of the link and then replaced correctly at the receiving side. Because the condensed frames take up less bandwidth, we can transmit greater volumes at a time.

QUESTION 67:

Which of the IOS commands below would you use to map a phone number to an IP address so the remote host name can be identified for PAP or CHAP authentication during an ISDN call?

- A. dialer pool-member
- B. dialer map
- C. dialer string
- D. dialer remote-name

Answer: B

Explanation:

The only way to specify a layer 3 (IP address) to lower layer ISDN information, such as the dial string, is via the "dialer map" command:

```
dialer map protocol next-hop-address [name hostname] [speed  
56|64] [broadcast]  
[dial-string[:isdn-subaddress]]
```

This command configures a serial interface or ISDN interface to call one or multiple sites. The name parameter refers to the name of the remote system. The speed parameter is the line speed in kilobits per second to use. The broadcast parameter indicates that broadcasts should be forwarded to this address. The dial-string[:isdn-subaddress] is the number to dial to reach the destination and the optional ISDN subaddress.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 7-32

QUESTION 68:

To configure a PPP connection at the server side of the Certkiller network you need to use PPP callback so that the server side will call back to the client side. Which of the following PPP callback commands would you configure from the server side of the PPP connection?

- A. ppp callback accept
- B. ppp callback request
- C. ppp callback server
- D. callback server accept ppp

Answer: A

Explanation:

Lets say that Certkiller -1 is the PPP Callback server and Certkiller -2 the Callback Client, then the configs would see something like :

For Callback Server :

```
Certkiller -1(config)#interface bri 0
Certkiller -1(config-if)#ip address 10.120.1.1 255.255.255.0
Certkiller -1(config-if)#encapsulation ppp
Certkiller -1(config-if)#dialer callback-secure
Certkiller -1(config-if)#dialer map ip 10.120.1.2 name Certkiller -2
class dial1 4085552222
Certkiller -1(config-if)#dialer-group1
Certkiller -1(config-if)#ppp callback accept
Certkiller -1(config-if)#ppp authentication chap
!
Certkiller -1(config)#map-class dialer dial1
Certkiller -1(config-map-class)#dialer callback-server username
```

For Callback Client :

```
Certkiller -2(config)#interface bri 0
Certkiller -2 (config-if)#ip address 10.120.1.2 255.255.255.0
Certkiller -2 (config-if)#encapsulation ppp
Certkiller -2 (config-if)#dialer map ip 10.120.1.1 name Certkiller -1
4085551111
Certkiller -2 (config-if)#dialer-group 1
Certkiller -2 (config-if)#ppp callback request
Certkiller -2 (config-if)#ppp authentication chap
```

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 7-32

QUESTION 69:

You need to configure link authentication on router CK1 . Which of the following commands would you use to configure CHAP authentication on an interface?

- A. chap authentication
- B. ppp chap authentication
- C. authentication chap
- D. ppp authentication chap
- E. pap authentication

Answer: D

Explanation:

Using CHAP authentication, after the PPP link is established, the access server sends a "challenge" message to the remote node. The remote node responds with a value calculated using a one-way hash function (typically Message Digest 5 [MD5]). The access server checks the response against its own calculation of the expected hash value. If the values match, the authentication is acknowledged. Otherwise, the connection is

terminated immediately.

CHAP provides protection against playback attack through the use of a variable challenge value that is unique and unpredictable. The use of repeated challenges every two minutes during any CHAP session is intended to limit the time of exposure to any single attack. The access server (or authentication server such as TACACS+) controls the frequency and timing of the challenges. A major advantage of the constantly changing challenge string is that the line cannot be sniffed and played back later to gain unauthorized access to the network.

You enable the use of CHAP authentication with the ppp authentication CHAP command.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Chapter 5-15

QUESTION 70:

DRAG DROP

Drag the authentication characteristics to its correct authentication protocol.

An access server is in control
Passwords are sent in hash form
It should always be configured with asynchronous lines
The remote host is in control of login requests
it is used as a security measure with PPP and MLP
Passwords are set as clear text
PAP
Place here
Place here
CHAP
Place here
Place here
PAP or CHAP
Place here
Place here

Answer:

PAP

Passwords are set as clear text

The remote host is in control of login requests

CHAP

Passwords are sent in hash form

An access server is in control

PAP or CHAP

It is used as a security measure with PPP and MLP

It should always be configured with asynchronous lines

Authentication Protocol	Controls Authentication Attempt(s)	Handshake Method	Password	Protection from Playback or Repeated Attacks?
PAP	Remote office router (remote node)	Two-way. Remote office router sends username/password pair until corporate office router accepts.	Uses clear text password.	No.
CHAP	Corporate office router (local node)	Three-way. Corporate office router sends challenge to remote office router. Remote office router responds. Corporate office router accepts or rejects authentication.	Uses variable, unique, and unpredictable challenge value.	Yes, through the challenge variable and repeated challenges after the link has been established.

Explanation:

PAP

To understand how PAP works, imagine a network topology where a remote office router (Cisco 805 router) is connected to a corporate office router (such as a Cisco 3600 router). After the PPP link is established, the remote office router repeatedly sends a configured username and password until the corporate office router accepts the authentication.

PAP has the following characteristics:

The password portion of the authentication is sent across the link in clear text (not scrambled or encrypted).

PAP provides no protection from playback or repeated trial-and-error attacks.

The remote office router controls the frequency and timing of the authentication attempts.

CHAP

To understand how CHAP works, imagine a network topology where a remote office router (Cisco 805 router) is connected to a corporate office router (such as a Cisco 3600 router). After the PPP link is established, the corporate office router sends a challenge message to the remote office router. The remote office router responds with a variable value. The corporate office router checks the response against its own calculation of the value. If the values match, the corporate office router accepts the authentication. The

authentication process can be repeated any time after the link is established.

CHAP has the following characteristics:

1. The authentication process uses a variable challenge value rather than a password.
2. CHAP provides protection against playback attack through the use of the variable challenge value, which is unique and unpredictable. Repeated challenges limit the time of exposure to any single attack.

The corporate office router controls the frequency and timing of the authentication attempts.

QUESTION 71:

When a PPP connection is being established, which three configuration features are negotiated through the LCP? (Choose three)

- A. Callback
- B. Multilink
- C. Encryption
- D. Compression
- E. Protocol multiplexing

Answer: A, B, D

Explanation:

PPP LCP CONFIGURATION OPTION TYPES

The Point-to-Point Protocol (PPP) Link Control Protocol (LCP) specifies a number of Configuration Options [146] which are distinguished by an 8 bit Type field. These Types are assigned as follows:

Type Configuration Option

-
- 1 Maximum-Receive-Unit
 - 2 Async-Control-Character-Map
 - 3 Authentication-Protocol
 - 4 Quality-Protocol
 - 5 Magic-Number
 - 6 RESERVED
 - 7 Protocol-Field-Compression
 - 8 Address-and-Control-Field-Compression
 - 9 FCS-Alternatives
 - 10 Self-Describing-Pad
 - 11 Numbered-Mode
 - 12 Multi-Link-Procedure
 - 13 Callback
 - 14 Connect-Time
 - 15 Compound-Frames
 - 16 Nominal-Data-Encapsulation
 - 17 Multilink-MRRU

- 18 Multilink-Short-Sequence-Number-Header
 - 19 Multilink-Endpoint-Discriminator
 - 20 Proprietary
 - 21 DCE-Identifier
 - 22 Multi-Link-Plus-Procedure
 - 23 Link Discriminator for BACP
- Reference: <http://www.freesoft.org/CIE/RFC/1700/34.htm>

QUESTION 72:

DRAG DROP

Drag the PPP authentication process action to its descriptions.

disconnect	
Determine authentication method	
Local database	
Incoming PPP negotiation	
Continue with PPP negotiation	
Security server database	
Start of PPP authentication process	Place here
Second step if authentication is configured	Place here
Checks using username and password	Place here
Queries this with TACAS+ or RADIUS	Place here
Does this if authentication fails	Place here
Does this if authentication passes	Place here

Answer:

Start of PPP authentication process	Incoming PPP negotiation
Second step if authentication is configured	Determine authentication method
Checks using username and password	Local database
Queries this with TACAS+ or RADIUS	Security server database
Does this if authentication fails	disconnect
Does this if authentication passes	Continue with PPP negotiation

QUESTION 73:

Which field is defined in the PPP format that allows PPP to dynamically negotiate link options?

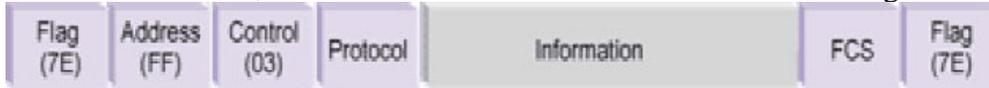
- A. Address

- B. Control
- C. Protocol
- D. Flag
- E. None of the above

Answer: C

Explanation:

There are three formats of a PPP frame, depending on whether it is carrying data or control information, as illustrated on the PPP Information Frame Diagram.



PPP Information Frame

Flag (1 byte)--Used for synchronizing the bit stream '7E'

Address (1 byte)--Usually 'FF'

Control (1 byte)--Set to '03'

Protocol field (2 bytes)--The field that contains addressing for the higher layers and is used to dynamically negotiate the PPP link options. This field is similar (but not identical) to the Ethernet Type field (Ethertype). Some common ones are:

-0021H--TCP/IP

-0023H--OSI

-0027H--DEC

-002BH--Novell

-002DH--Van Jacobson Compressed TCP/IP

-003DH--Multilink

Information field (variable)--Contains data that may be preceded by Network Layer headers, such as IP.

FCS (2 bytes)--Used to ensure data integrity

Flag (1 byte)--Signals end of frame, and possibly the start of the next frame

Reference:

<http://www.webclasses.net/Courses/Protocols/7.0/DemoBuild/units/unit02/sec05a.html>

QUESTION 74:

You are configuring the PPP encapsulation type on one of the interfaces on router CK1 . You may configure PPP on which of the following types of physical interfaces (Choose all that apply):

- A. Synchronous serial
- B. HSSI
- C. Asynchronous serial
- D. ISDN BRI/PRI

Answer: A, B, C, D

Explanation:

PPP, described in RFC 1661, encapsulates network layer protocol information over point-to-point links. You can configure PPP on the following types of physical interfaces:

Asynchronous serial

HSSI

ISDN

Synchronous serial

By enabling PPP encapsulation on physical interfaces, PPP can also be in effect on calls placed by the dialer interfaces that use the physical interfaces.

QUESTION 75:

On router CK1 , you want all calls that are being placed to use the PPP encapsulation. Router CK1 is configured with dialer interfaces and you need them to use PPP also. How can you have PPP be used on these logical dialer interfaces?

- A. By disabling PPP encapsulation on physical interfaces
- B. By enabling PPP encapsulation on virtual interfaces
- C. By enabling PPP encapsulation on physical interfaces
- D. By disabling PPP encapsulation on virtual interfaces

Answer: C

Explanation:

You can configure PPP on the following types of physical interfaces:

Asynchronous serial

HSSI

ISDN

Synchronous serial

By enabling PPP encapsulation on physical interfaces, PPP can also be in effect on calls placed by the dialer interfaces that use the physical interfaces, as the physical and data link layer attributes of the physical interface is used on the logical interfaces.

QUESTION 76:

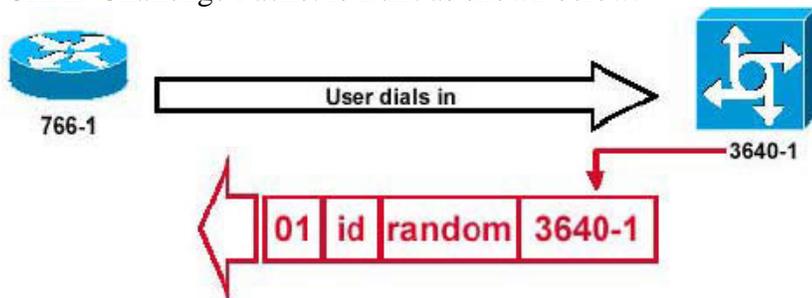
Generally, CHAP is preferred over PAP for PPP authentications. Which of the following are parts of the CHAP challenge packet? (Choose all that apply)

- A. Host name of the remote router
- B. Random number
- C. ID
- D. Host name of the local router
- E. None of the above

Answer: B, C, D

Explanation:

A CHAP Challenge Packet is Built as shown below:



The figure above illustrates these steps in the CHAP authentication between the two routers:

1. A CHAP challenge packet is built with these characteristics:
2. 1. 01 = challenge packet type identifier.
2. ID = sequential number that identifies the challenge.
3. random = a reasonably random number generated by the router.
4. 3640-1 = the authentication name of the challenger.
5. The ID and random values are kept on the called router. This is the local router, not the remote router.
6. The challenge packet is sent to the calling router. A list of outstanding challenges is maintained

Reference:

http://www.cisco.com/en/US/tech/CK713/CK507/technologies_tech_note09186a00800b4131.shtml

QUESTION 77:

Router CK1 is configured for Multilink PPP (MLPPP). Cisco multi-link PPP is compatible with and supports which of the following? (Choose all that apply)

- A. Most routers conforming to RFC1997
- B. Synchronous dialer interfaces
- C. Asynchronous dialer interfaces
- D. Cisco700 series routers
- E. A multiple-LAN interface
- F. RFC1917

Answer: B, C

Explanation:

The Multilink PPP feature provides load balancing functionality over multiple WAN links, while providing multivendor interoperability, packet fragmentation and proper sequencing, and load calculation on both inbound and outbound traffic. The Cisco implementation of MLP supports the fragmentation and packet sequencing specifications in RFC 1990. Additionally, you can change the default endpoint discriminator value that is supplied as part of user authentication. Refer to RFC 1990 for more information about the endpoint discriminator.

MLP allows packets to be fragmented and the fragments to be sent at the same time over multiple point-to-point links to the same remote address. The multiple links come up in response to a defined dialer load threshold. The load can be calculated on inbound traffic, outbound traffic, or on either, as needed for the traffic between the specific sites. MLP provides bandwidth on demand and reduces transmission latency across WAN links.

MLP is designed to work over synchronous and asynchronous serial and BRI and PRI types of single or multiple interfaces that have been configured to support both dial-on-demand rotary groups and PPP encapsulation.

QUESTION 78:

A Certkiller router is being configured as a PPP callback server. Which of the following commands can be used on the server side of a PPP callback configuration?

- A. PPP callback accept
- B. PPP callback servers
- C. PPP callback server accept PPP
- D. PPP callback request
- E. PPP callback

Answer: A

Explanation:

PPP callback provides a client-server relationship between the end points of a point-to-point connection. PPP callback allows a router to request that a dial-up peer router call back. The callback feature can be used to control access and toll costs between the routers. When PPP callback is configured on the participating routers, the calling router (the callback client) passes authentication information to the remote router (the callback server), which uses the host name and dial string authentication information to determine whether to place a return call. If the authentication is successful, the callback server disconnects and then places a return call. The remote username of the return call is used to associate it with the initial call so that packets can be transmitted.

ppp callback

To enable a dialer interface that is not a data terminal ready (DTR) interface to function either as a callback client that requests callback or as a callback server that accepts callback requests, use the ppp callback interface configuration command.

`ppp callback {accept | request}`

Syntax Description

accept	Enables this dialer interface to accept
	PPP callback requests (and function as

	the PPP callback server).
--	---------------------------

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_command_reference_chapter09186a00800c

QUESTION 79:

From the following choices, which are LCP options that are supported by PPP?

(Select three)

- A. Authentication
- B. Multilink
- C. Protocol multiplexing
- D. Compression
- E. Dynamic address allocation
- F. Dynamic address translation

Answer: A, B, D

Explanation:

The PPP LCP (Link Control Protocol) provides a method of establishing, configuring, maintaining, and terminating a point-to-point connection. The four PPP LCP options are Authentication, Callback, Compression, and Multilink. With LCP, the link is maintained via the use of error correcting mechanisms.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 5-11

QUESTION 80:

Within the Certkiller PPP environment, what does protocol multiplexing refer to?

- A. The ability to provide load balancing functionality over multiple WAN links
- B. The capability to build up and tear down multiple Layer 3 protocol sessions over a single data link
- C. The ability to allow link partners to dynamically negotiate link options, including authentication and compression
- D. The ability to reduce the size of data frames being transmitted over network links
- E. All of the above

Answer: B

Explanation:

The Point-to-Point Protocol (PPP) originally emerged as an encapsulation protocol for

transporting IP traffic over point-to-point links. PPP also established a standard for the assignment and management of IP addresses, asynchronous (start/stop) and bit-oriented synchronous encapsulation, network protocol multiplexing, link configuration, link quality testing, error detection, and option negotiation for such capabilities as network layer address negotiation and data-compression negotiation. PPP supports these functions by providing an extensible Link Control Protocol (LCP) and a family of Network Control Protocols (NCPs) to negotiate optional configuration parameters and facilities.

PPP provides a method for transmitting datagrams over serial point-to-point links. PPP contains three main components:

A method for encapsulating datagrams over serial links. PPP uses the High-Level Data Link Control (HDLC) protocol as a basis for encapsulating datagrams over point-to-point links. (See Chapter 16, "Synchronous Data Link Control and Derivatives," for more information on HDLC.)

An extensible LCP to establish, configure, and test the data link connection.

A family of NCPs for establishing and configuring different network layer protocols. PPP is designed to allow the simultaneous use of multiple network layer protocols.

Reference: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ppp.htm

QUESTION 81:

While debugging a point to point link within the Certkiller network, you notice a large number of LCP messages. LCP is responsible for the negotiation of which function?

- A. IP address
- B. Modulo size
- C. Error correction
- D. Frequency on the link
- E. Noneof the above

Answer: C

Explanation:

The PPP LCP provides a method of establishing, configuring, maintaining, and terminating the point-to-point connection. LCP goes through four distinct phases. First, link establishment and configuration negotiation occur. Before any network layer datagrams (for example, IP) can be exchanged, LCP first must open the connection and negotiate configuration parameters. This phase is complete when a configuration-acknowledgment frame has been both sent and received.

This is followed by link quality determination. LCP allows an optional link quality determination phase following the link-establishment and configuration-negotiation phase. In this phase, the link is tested to determine whether the link quality is sufficient to bring up network layer protocols. This phase is optional. LCP can delay transmission of network layer protocol information until this phase is complete.

At this point, network layer protocol configuration negotiation occurs. After LCP has

finished the link quality determination phase, network layer protocols can be configured separately by the appropriate NCP and can be brought up and taken down at any time. If LCP closes the link, it informs the network layer protocols so that they can take appropriate action.

Finally, link termination occurs. LCP can terminate the link at any time. This usually is done at the request of a user but can happen because of a physical event, such as the loss of carrier or the expiration of an idle-period timer.

QUESTION 82:

When comparing the differences between PPP and HDLC, which additional field differentiates the PPP frame from an HDLC frame format?

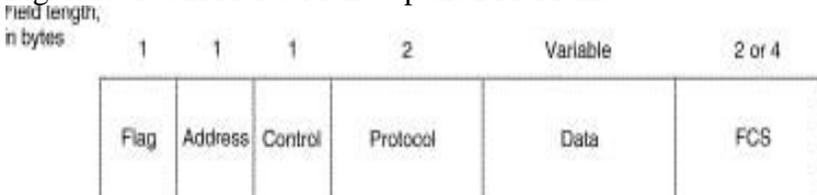
- A. Protocol
- B. Control and address-family identifier (AFI) fields
- C. LCP and control fields
- D. Next hop address and address-family identifier (AFI) fields
- E. Flag and next-hop address fields
- F. None of the above

Answer: A

Explanation:

When comparing the PPP frame to an HDLC frame, the only major change is the addition of a new field to specify the protocol of the encapsulated data.

Figure 13-1: Six Fields Make Up the PPP Frame



The following descriptions summarize the PPP frame fields illustrated in Figure 13-1:

1. Flag-A single byte that indicates the beginning or end of a frame. The flag field consists of the binary sequence 01111110.
2. Address-A single byte that contains the binary sequence 11111111, the standard broadcast address. PPP does not assign individual station addresses.
3. Control-A single byte that contains the binary sequence 00000011, which calls for transmission of user data in an unsequenced frame. A connectionless link service similar to that of Logical Link Control (LLC) Type 1 is provided. (For more information about LLC types and frame types, refer to Chapter 16.)
4. Protocol-Two bytes that identify the protocol encapsulated in the information field of the frame. The most up-to-date values of the protocol field are specified in the most recent Assigned Numbers Request For Comments (RFC).
- 5.
6. Data-Zero or more bytes that contain the datagram for the protocol specified in the protocol field. The end of the information field is found by locating the closing flag

sequence and allowing 2 bytes for the FCS field. The default maximum length of the information field is 1,500 bytes. By prior agreement, consenting PPP implementations can use other values for the maximum information field length.

7. Frame check sequence (FCS)-Normally 16 bits (2 bytes). By prior agreement, consenting PPP implementations can use a 32-bit (4-byte) FCS for improved error detection.

The HDLC frame format is omits the Protocol field.

QUESTION 83:

Compression was configured on router Certkiller A as shown below:

```
CertkillerA# show compress
Serial2
uncompressed bytes xmt/rcv 120000/120500
 1 min avg ratio xmt/rcv   0.789/0.837
 5 min avg ratio xmt/rcv   0.789/0.837
10 min avg ratio xmt/rcv   0.789/0.837
no bufs xmt 0 no bufs rcv 0
restarts
Additional Store State
Transmit bytes: Uncompressed = 40000 Compressed = 40000
Received bytes: Compressed = 50000 Uncompressed = 0
```

Given the output shown above, which three statements are true about PPP compression? (Choose three)

- A. The interface is configured with TCP header compression.
- B. The interface is configured with STAC compression.
- C. The interface is configured with Predictor compression.
- D. The actual data throughput of the router is less than what it would be if compression were not being applied.
- E. The total amount of data to be transmitted before applying compression is 160,000.
- F. The total amount of data to be transmitted after applying compression is 40,000.

Answer: B, D, E

Explanation:

Sample Output:

Here is a sample output of the show compress command:

```
CK1 #show compress
Serial2
Software compression enabled
uncompressed bytes xmt/rcv 81951/85500
compressed bytes xmt/rcv 0/0
 1 min avg ratio xmt/rcv 0.789/0.837
 5 min avg ratio xmt/rcv 0.789/0.837
10 min avg ratio xmt/rcv 0.789/0.837
no bufs xmt 0 no bufs rcv 0
```

restarts 0

Additional Stacker Stats:

Transmit bytes: Uncompressed = 28049 Compressed = 65745

Received bytes: Compressed = 74738 Uncompressed = 0

These sections explain this sample output.

Software Compression

After the serial number, the first line in the output displays "Software compression enabled".

This line indicates that compression is configured. The "additional stacker stats" output tells us that STAC compression was configured.

Uncompressed Bytes

uncompressed bytes xmt/rcv 81951/85500

This line in the output provides a count of uncompressed bytes of the compressed data. It does not include packets that cannot be compressed.

Compressed Bytes

compressed bytes xmt/rcv 0/0

This line gives the total number of already compressed bytes that are sent or received.

Throughput Ratio

The next section of output indicates a ratio of the data throughput gained or lost in the compression routine. Any number less than one indicates that the compression actually slows down data throughput. It does not reflect how compressible the data is.

1 min avg ratio xmt/rcv 0.789/0.837

5 min avg ratio xmt/rcv 0.789/0.837

10 min avg ratio xmt/rcv 0.789/0.837

Here are the common causes of poor compression ratios:

1. High CPU utilization.
2. A high percentage of small packets.
3. Data that is not very redundant (for instance, if it has already been compressed).

Bytes Transmitted

Transmit bytes: Uncompressed = 28049 Compressed= 65745

Here:

1. The uncompressed value is the amount of data that cannot be compressed, and has been sent in uncompressed format.

2. The compressed value represents the byte-count of the data after it is compressed.

The sum of these two values represents the actual number bytes transmitted on the interface, minus the layer two encapsulation overhead.

Bytes Received

Received bytes: Compressed = 74738 Uncompressed= 0

Here:

1. The compressed value is the byte-count of the compressed data received.

2. The uncompressed value is the amount of data that was received in uncompressed format.

The sum of these two values represents the actual byte count received on the interface, minus the layer two encapsulation overhead.

Reference:

http://www.cisco.com/en/US/tech/CK7_13/CK8_02/technologies_tech_note09186a008035b8c5.shtml

QUESTION 84:

Certkiller works from home via a Virtual Private Network connection. From her remote Internet connection she enters an ISP's login page. Once logged in, the ISP's owned device creates a secure tunnel straight to the main offices enterprise network. What kind of VPN is this?

- A. An intranet VPN
- B. An extranet VPN
- C. A client initiated VPN
- D. A Network Access Server initiated VPN

Answer: D

Explanation:

Although the service described above is initiated by a client, and it does occur on the Internet; it's known as a Network Access Server initiated VPN.

Client-initiated access VPNs allow for remote users to use clients to establish an encrypted IP tunnel across the Internet service provider's (ISP) shared network to the enterprise customer's network. The main advantage of client-initiated access VPNs over NAS-initiated access VPNs is that they use IPsec tunnel mode to secure the connection between the client and the ISP over the PSTN.

Incorrect Answers:

A: Intranet VPNs connect corporate headquarters, remote offices, and branch offices over a shared infrastructure using dedicated connections.

B: Extranet VPNs link customers, suppliers, partners, or communities of interest to a corporate intranet over a shared infrastructure using dedicated connections.

C: Client initiated VPN's are initiated by the client using VPN software, such as the Cisco VPN client.

Reference: Cisco Secure VPN Client Solutions Guide

http://www.cisco.com/en/US/products/sw/secursw/ps2138/products_maintenance_guide_chapter09186a008007d

QUESTION 85:

The Certkiller network is using VPNs to allow access to the corporate network. How is a Virtual Private Network (VPN) connection better than a conventional point-to-point T1 connection? (Choose only one answer)

- A. VPNs can provide reserved bandwidth for the individual user.
- B. VPN users are not tied to a specific fixed location.
- C. VPNs offer more local control of the quality of service.
- D. VPNs offer better queuing mechanisms than T1 connections.
- E. None of the above.

Answer: B

Explanation:

VPN client-A client might also create a connection to a site, which can generally be done from anywhere that an Internet connection can be made. This is especially true when connections between sites do not use dedicated connections or circuits (leased lines, Frame Relay virtual circuits, ISDN, and asynchronous calls).

When a site is connected to the Internet with a DSL or cable-modem connection, or is dialed into an Internet service provider (ISP) with an analog modem, a secure connection must be established from individual workstations to a branch or corporate office. VPN client software on a PC, such as Cisco VPN Client, can create an encrypted tunnel from the PC to the site where the necessary resources are located.

Normally, such a VPN tunnel terminates on a router or a VPN concentrator.

Reference:

Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)

Page 42

QUESTION 86:

The Certkiller network is using VPNs to allow access to the corporate network.

What is true about VPNs (virtual private networks)? (Choose all that apply)

- A. All messages require a 56-bit encryption key when sent over VPN.
- B. VPNs can make use of public and private-key technology to establish a secure tunnel for each client connection.
- C. VPNs can make use of a certification authority (CA) to digitally sign each transmitted message.
- D. All devices between the VPN client and the VPN server must be VPN enabled.
- E. None of the above

Answer: B, C

Explanation:

Both of these answer choices correctly describe the different options for establishing a secure VPN connections.

With IPsec, data can be transmitted across a public network without fear of observation, modification, or spoofing. As part of its security functions, the PIX Firewall provides IPsec standards-based VPN capability. VPNs maintain the same security and management policies as a private network. With a VPN, customers, business partners, and remote users, such as telecommuters, can access enterprise computing resources securely.

The component technologies implemented for use by IKE include:

DES-Data Encryption Standard (DES) is used to encrypt packet data. IKE implements the 56-bit DES-CBC with Explicit IV standard. See "CBC."

Triple DES (3DES)-A variant of DES, which iterates three times with three separate keys, effectively doubling the strength of DES.

CBC-Cipher Block Chaining (CBC) requires an initialization vector (IV) to start encryption. The IV is explicitly given in the IPSec packet.

Diffie-Hellman-A public-key cryptography protocol which allows two parties to establish a shared secret over an unsecure communications channel. Diffie-Hellman is used within IKE to establish session keys. 768-bit and 1024-bit Diffie-Hellman groups are supported. MD5 (HMAC variant)-MD5 (Message Digest 5) is a hash algorithm used to authenticate packet data. HMAC is a variant which provides an additional level of hashing.

SHA (HMAC variant)-SHA (Secure Hash Algorithm) is a hash algorithm used to authenticate packet data. HMAC is a variant which provides an additional level of hashing.

RSA signatures-RSA is the public key cryptographic system developed by Ron Rivest, Adi Shamir, and Leonard Adleman. RSA signatures provides non-repudiation.

Incorrect Answers:

A: Although single DES uses 56 bit encryption, many VPNs use 3DES technology or AES. 3DES uses a 168 bit encryption key.

D: Only the VPN endpoints need to be enabled for VPN/IPSec technology. The devices in between (IP routers, switches) are ignorant of the VPN connection. To these devices, only IP traffic is seen and processed like all other IP traffic.

Reference:

http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_user_guide_chapter09186a0080089917.htm

QUESTION 87:

DRAG DROP

Match the IPSec VPN terms on the left to the position in the center that correctly matches the characteristics on the right:

authentication	place here	The receiver can verify that the data was not altered during transmit.
data integrity	place here	Only entities permitted to see the data will have the capability to view the data.
data confidentiality	place here	The receiver can determine the source of the packet and certifying the source.
replay protection	place here	The receiver can verify the correct sequence of packets as they arrive.

Answer:

data integrity	The receiver can verify that the data was not altered during transmit.
data confidentiality	Only entities permitted to see the data will have the capability to view the data.
authentication	The receiver can determine the source of the packet and certifying the source.
replay protection	The receiver can verify the correct sequence of packets as they arrive.

Explanation:

Data integrity: Data integrity mechanisms, through the use of secret-key based or public-key based algorithms, which allow the recipient of a piece of protected data to verify that the data has not been modified in transit.

Data Confidentiality - This is perhaps the most important service provided by any VPN implementation. Since your private data is traveling over a public network, data confidentiality is vital and can be attained by encrypting the data. This is the process of taking all the data that one computer is sending to another and encoding it into a form that only the other computer will be able to decode.

Data Origin Authentication - It is extremely important to verify the identity of the source of the data being sent. This is necessary to guard against a number of attacks that depend on spoofing the identity of the sender. This service requires a data integrity service plus a key distribution mechanism, where a secret key is shared only between the sender and receiver.

Replay-detection: A security service where the receiver can reject old or duplicate packets in order to defeat replay attacks (replay attacks rely on the attacker sending out older or duplicate packets to the receiver and the receiver thinking that the bogus traffic is legitimate). Replay-detection is done by using sequence numbers combined with authentication, and is a standard feature of IPSec (doing so helps prevent spoofing).

References:

http://www.cisco.com/en/US/tech/ CK5 83/ CK3 72/technologies_tech_note09186a0080094865.shtml

http://www.cisco.com/en/US/tech/ CK5 83/ CK3 72/technologies_tech_note09186a0080094203.shtml

QUESTION 88:

IPSec is being used for the Certkiller VPN. In the IPSec protocol; what are the responsibilities of the Internet Key Exchange (IKE)? (Choose all that apply)

- A. Negotiating protocol parameters
- B. Integrity checking user hashes
- C. Authenticating both sides of a connection
- D. Implementing tunnel mode
- E. Exchanging public keys
- F. Packet encryption

Answer: A, C, E

Explanation:

Internet Key Exchange (IKE) is used to establish all the information needed for a VPN tunnel. Within IKE, you negotiate your security policies, establish your SAs, and create and exchange your keys that will be used by other algorithms such as DES. IKE is broken down into two phases, described next.

Phase One of IKE

Phase one is used to negotiate policy sets, authenticate peers, and create a secure channel between peers. IKE phase one can happen in one of two modes, main mode or aggressive mode. The major difference is that in main mode, three different and distinct exchanges take place to add to the security of the tunnel, whereas in aggressive mode everything is sent in a single exchange.

Phase Two of IKE

IKE phase two is used to negotiate the IPSec security parameters (such as the IPSec transform sets), establish SAs, and optionally perform additional Diffie-Hellman exchanges. IKE phase two has only one mode, called quick mode, which happens only after IKE phase one has completed.

Reference:

Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)
Page 438 to 439

QUESTION 89:

An IPSec datagram is depicted in the following diagram:

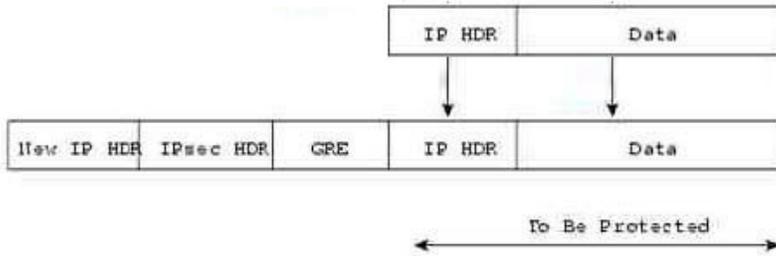


In this datagram, what is the name of the header that is marked with a 2? (Hint: It provides data authentication and confidentiality)

- A. AH header
- B. ESP header
- C. SA header
- D. MPLS VPN header

Answer: B

Explanation:



IPsec defines a new set of headers to be added to IP datagrams. These new headers are placed after the outer IP header. These new headers provide information for securing the payload of the IP packet as follows:

Authentication Header (AH)-This header, when added to an IP datagram, ensures the integrity and authenticity of the data, including the invariant fields in the outer IP header. It does not provide confidentiality protection. AH uses a keyed-hash function rather than digital signatures, because digital signature technology is slow and would greatly reduce network throughput.

Encapsulating Security Payload (ESP)-This header, when added to an IP datagram, protects the confidentiality, integrity, and authenticity of the data. If ESP is used to validate data integrity, it does not include the invariant fields in the IP header.

Reference: http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/depip_wp.htm

QUESTION 90:

Cisco developed the Cisco Encryption Technology (CET) as an encryption scheme. Which of the following are true when comparing the differences between IPsec and Cisco Encryption Technology (CET)?

- A. IPsec encrypts IP-only packets, whereas CET deciphers non-IP packets.
- B. IPsec supports AH, ESP and Anti-Replay which are not available with CET.
- C. CET supports AH, ESP and Anti-Replay which are not available with IPsec.
- D. CET is the implementation of IPsec in the Cisco Secure Services package.
- E. IPsec is used to encrypt IP-only packets, whereas CET is used to encrypt only non-IP packets.

Answer: B

Explanation:

Cisco Encryption Technology (CET) is a proprietary security solution introduced in Cisco IOS Release 11.2. It provides network data encryption at the IP packet level and implements the following standards:

- * Digital Signature Standard (DSS)
- * Diffie-Hellman (DH) public key algorithm
- * Data Encryption Standard (DES)

IPsec is a framework of open standards developed by the Internet Engineering Task Force (IETF) that provides security for transmission of sensitive information over

unprotected networks such as the Internet. It acts at the network level and implements the following standards:

- * IPSec
- * Internet Key Exchange (IKE)
- * Data Encryption Standard (DES)
- * MD5 (HMAC variant)
- * SHA (HMAC variant)
- * Authentication Header (AH)
- * Encapsulating Security Payload (ESP)

IPSec services provide a robust security solution that is standards-based. IPSec also provides data authentication and anti-replay services in addition to data confidentiality services, while CET provides only data confidentiality services.

If you require only Cisco router-to-Cisco router encryption, then you could run CET, which is a more mature, higher-speed solution. If you require a standards-based solution that provides multivendor interoperability or remote client connections, then you should implement IPSec. Also, if you want to implement data authentication with or without privacy (encryption), then IPSec is the right choice.

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a00800d

QUESTION 91:

IPSec is being used for the Certkiller VPN. Which of the IPSEC protocols is capable of negotiating security associations?

- A. AH
- B. ESP
- C. IKE
- D. SSH
- E. MD5
- F. None of the above

Answer: C

Explanation:

IKE is a key management protocol standard that is used in conjunction with the IPSec standard.

IPSec can be configured without IKE, but IKE enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard.

IKE is a hybrid protocol, which implements the Oakley key exchange and Skeme key exchange inside the ISAKMP framework. (ISAKMP, Oakley, and Skeme are security protocols implemented by IKE.) IKE automatically negotiates IPSEC security associations and enables IPSEC secure communications without manual preconfiguration.

Specifically, IKE provides the following benefits:

- * Eliminates the need to manually specify all the IPSec security parameters in the crypto maps at both peers.
- * Allows you to specify a lifetime for the IPSec security association.
- * Allows encryption keys to change during IPSec sessions.
- * Allows IPSec to provide anti-replay services.
- * Permits CA support for a manageable, scalable IPSec implementation.
- * Allows dynamic authentication of peers.

QUESTION 92:

IPSec is being used for the Certkiller VPN. Which of the phrases below are true about IPSec IKE Phase 2? (Choose all that apply.)

- A. It determines the key distribution method
- B. It identifies IPSec peer details
- C. It selects manual or IKE-initiated SAs
- D. It determines the authentication method
- E. It negotiates ISAKMP policies for peers
- F. It selects the IPSec algorithms and parameters for optimal security and performance

Answer: C, E, F

Explanation:

IKE Phase 1

The basic purpose of IKE phase 1 is to authenticate the IPSec peers and to set up a secure channel between the peers to enable IKE exchanges.

IKE phase 1 performs the following functions:

- * Authenticates and protects the identities of the IPSec peers
- * Negotiates a matching IKE SA policy between peers to protect the IKE exchange
- * Performs an authenticated Diffie-Hellman exchange with the end result of having matching shared secret keys
- * Sets up a secure tunnel to negotiate IKE phase 2 parameters

IKE Phase 2

The purpose of IKE phase 2 is to negotiate IPSec SAs to set up the IPSec tunnel. IKE phase 2 performs the following functions:

- * Negotiates IPSec SA parameters protected by an existing IKE SA
- * Establishes IPSec security associations
- * Periodically renegotiates IPSec SAs to ensure security
- * Optionally performs an additional Diffie-Hellman exchange

QUESTION 93:

IPSec is being used for the Certkiller network between routers CK1 and CK2 . During the ISAKMP negotiation process in IKE Phase 1 mode (where ISAKMP

looks for a policy that is the same on both peers) which peer would be responsible for matching the policies?

- A. The peer that initiates the negotiation sends all its policies to the remote peer, and the remote peer tries to find a match with its policy.
- B. The remote peer sends all its policies to the initiating peer, and the initiating peer tries to find a match with its policies.
- C. Both peers send all their policies to the other peer, and each peer tries to find a match with its policies.
- D. Both peers send all their policies to the other peer, but just the initiating peer tries to find a match with its policies.

Answer: A

Explanation:

When the IKE negotiation begins, IKE looks for an IKE policy that is the same on both peers. The peer that initiates the negotiation will send all its policies to the remote peer, and the remote peer will try to find a match. The remote peer looks for a match by comparing its own highest priority policy against the other peer's received policies. The remote peer checks each of its policies in order of its priority (highest priority first) until a match is found.

A match is made when both policies from the two peers contain the same encryption, hash, authentication, and Diffie-Hellman parameter values, and when the remote peer's policy specifies a lifetime less than or equal to the lifetime in the policy being compared. (If the lifetimes are not identical, the shorter lifetime-from the remote peer's policy-will be used.)

If no acceptable match is found, IKE refuses negotiation and IPSec will not be established.

If a match is found, IKE will complete negotiation, and IPSec security associations will be created.

QUESTION 94:

IPSec is being used for the Certkiller VPN. What is true about the security protocol ESP (Encapsulation Security Payload) in IPSec? (Choose three)

- A. IP packet is expanded by transport mode: 37 bytes (3DES) or 63 bytes (AES); tunnel mode: 57bytes (3DES) or 83 bytes (AES).
- B. IP packet is expanded by: transport mode 56 bytes: tunnel mode 128 bytes.
- C. Authentication is mandatory and the whole packet as well as the header is authenticated.
- D. Authentication is optional and the outer header is not authenticated.
- E. The ESP security protocol provides data confidentiality.
- F. The ESP security protocol provides no data confidentiality.

Answer: A, C, E

Explanation:

ESP is the Encapsulating Security Payload: A security protocol which provides data privacy services and optional data authentication, and anti-replay services. ESP encapsulates the data to be protected.

Both the older RFC 1829 ESP and the updated ESP protocol are implemented. The updated ESP protocol is per the latest version of the "IP Encapsulating Security Payload" Internet Draft (draft-ietf-ipsec-esp-v2-xx.txt).

RFC 1829 specifies DES-CBC as the encryption algorithm; it does not provide data authentication or anti-replay services. The updated ESP protocol allows for the use of various cipher algorithms and (optionally) various authentication algorithms. Cisco IOS implements the mandatory 56-bit DES-CBC with Explicit IV as the encryption algorithm, and MD5 or SHA (HMAC variants) as the authentication algorithms. The updated ESP protocol provides anti-replay services.

Reference: IPSec Network Security

http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_3/ipsec.htm

QUESTION 95:

What is true about the security protocol AH (Authentication Header) used in a secure IPSec tunnel? (Choose three)

- A. Authentication is mandatory.
- B. Authentication is optional.
- C. The IP packet is expanded by transport mode 37 bytes(3DES) or 63 bytes(AES); tunnel mode 57 bytes(3DES) or 83 bytes(AES).
- D. The IP packet is expanded by transport mode 56 bytes; tunnel mode 128 bytes.
- E. The IPSec AH security protocol does provide data confidentiality.
- F. The IPSec AH security protocol does not provide data confidentiality.

Answer: A, C, F

Explanation:

Authentication Header: A security protocol which provides data authentication and optional anti-replay services. AH is embedded in the data to be protected (a full IP datagram).

Both the older RFC 1828 AH and the updated AH protocol are implemented. The updated AH protocol is per the latest version of the "IP Authentication Header" Internet Draft (draft-ietf-ipsec-auth-header-xx.txt).

RFC 1828 specifies the Keyed MD5 authentication algorithm; it does not provide anti-replay services. The updated AH protocol allows for the use of various authentication algorithms; CiscoIOS has implemented the mandatory MD5 and SHA (HMAC variants) authentication algorithms. The updated AH protocol provides anti-replay services.

Reference: IPSec Network Security

http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_3/ipsec.htm

QUESTION 96:**DRAG DROP**

Match the IPSec terms on the left with their corresponding descriptions on the right.

authentication	The receiver can verify that the data was not altered during transit	Place here
data integrity	Only entities permitted to see the data will have the capability to view the data.	Place here
data confidentiality	The receiver can determine the source of the packet, guaranteeing and certifying the source.	Place here
replay protection	The receiver can verify the correct sequence of packets as they arrive.	Place here

Answer:

The receiver can verify that the data was not altered during transit	data integrity
Only entities permitted to see the data will have the capability to view the data.	data confidentiality
The receiver can determine the source of the packet, guaranteeing and certifying the source.	authentication
The receiver can verify the correct sequence of packets as they arrive.	replay protection

QUESTION 97:

Which of the following statements is true about IPSec security associations (SAs)?

- A. SAs contain unidirectional specifications only.
- B. SAs describe the mechanics of implementing a key exchange protocol.
- C. A single SA can be used for both AH and ESP encapsulation protocols.
- D. A single SA is negotiated by peers requesting secure communication.
- E. Active SAs are stored in a local database called the IPSec database.

Answer: A

Explanation:

An SA is a set of security parameters used by a tunnel for authentication and encryption. Key management tunnels use one SA for both directions of traffic; data management tunnels use at least one SA for each direction of traffic. Each endpoint assigns a unique identifier, called a security parameter index (SPI), to each SA.

A set of SAs is needed for a protected data pipe, one per direction per protocol. For example, if you have a pipe that supports Encapsulating Security Protocol (ESP) between peers, one ESP SA is required for each direction. SAs are uniquely identified by destination (IPSec endpoint) address, security protocol (AH or ESP), and SPI.

Note the following regarding SAs:

IP Security (IPSec) SAs are unidirectional and are unique in each security protocol. An Internet Key Exchange (IKE) SA is used by IKE only, and unlike the IPSec SA, it is bidirectional.

IKE negotiates and establishes SAs on behalf of IPSec.

A user can also establish IPSec SAs manually.

Reference:

http://www.cisco.com/en/US/products/sw/cscowork/ps4565/products_user_guide_chapter09186a008043bd31.html

QUESTION 98:

On router CK1 the following NAT configuration is being used:

```
ip nat pool test 192.168.1.33 192.168.1.42 netmask  
255.255.255.224
```

```
ip nat inside source list 7 pool test
```

Based on the information above, how many addresses should be available for dynamic NAT translation?

- A. 7
- B. 9
- C. 10
- D. 30
- E. 32
- F. 254
- G. 255

Answer: C

Explanation:

The correct NAT configuration syntax is displayed below:

```
ip nat pool pool-name start-ip end-ip { netmask netmask | prefix-length prefix-length }
```

Syntax explanation:

pool-name is the name of the pool

start-ip is the starting IP address for the range of addresses in the address pool;

end-ip is the ending IP address for the range of addresses in the address pool

The start-IP (first one used) is 192.168.1.33

The end-IP(last IP used) is 192.168.1.42

The IP addresses are allowed within the subnet mask with a network address of

192.168.1.32. So we have 10 usable IP addresses at our disposal.

Note: Additional information regarding the configuration of NAT is displayed below:

ip nat pool Command	Description
<i>pool-name</i>	Name of the pool.
<i>start-ip</i>	Starting IP address that defines the range of addresses in the address pool.
<i>end-ip</i>	Ending IP address that defines the range of addresses in the address pool.
netmask <i>netmask</i>	Network mask that indicates which address bits belong to the network and subnetwork fields, and which bits belong to the host field. Specify the netmask of the network to which the address pool belongs.
prefix-length <i>prefix-length</i>	Number that indicates how many bits of the netmask are 1s (how many bits of the address indicate the network). Specify the netmask of the network to which the pool addresses belong.
type <i>rotary</i>	(Optional) Indicates that the range of addresses in the address pool identifies real, inside hosts among which TCP load distribution will occur.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 14-16

QUESTION 99:

Although NAT (Network Address Translation) has many uses, there can be disadvantages associated with its use. Which of the following describe disadvantages of using NAT? (Select all that apply)

- A. It does not allow overlapping IP addressing schemes.
- B. It prevents IP routing address summarization.
- C. It results in loss of end-to-end traceability.
- D. It limits internal IP addressing schemes to private addresses.
- E. NAT has no disadvantages.
- F. It introduces switching path delays.

Answer: C, F

Explanation:

The original inside local addresses are replaced so traceability is impossible. IP address overlapping refers to the situation where two locations that want to inter-connect are both using the same IP address scheme. This is not an unusual occurrence, and will often happen when companies merge or are acquired. Without special support, the two locations will not be able to connect and establish sessions. The overlapped IP addresses can be public addresses assigned to other companies, private addresses assigned to other companies already, or from the range of private addresses as defined in RFC 1918. Private IP addresses are un-routable and require NAT translations to allow for connections to the outside world.

NAT conserves registered public addresses, maximizing its use. It also reduces address overlap and eliminates the need to renumber networks when they merge. It also increases flexibility when connecting to the Internet.

NAT Implementation Considerations

Advantages	Disadvantages
Conserves legally registered addresses	Translation introduces switching path delays
Reduces address overlap occurrence	Loss of end-to-end IP traceability
Increases flexibility when connecting to Internet	Certain applications will not function with NAT enabled
Eliminates address renumbering as network changes	

However, NAT introduces switching path delays and Loss of end-to-end traceability. Some applications will also not function when NAT is enabled.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 14-6

QUESTION 100:

Router CK1 is configured for NAT so that the Certkiller network can take advantage of the benefits of using NAT. Which of the following describe the advantages of using NAT? (Choose three)

- A. It translates IPX to IP for Internet access.
- B. It maximizes the use of registered addresses.
- C. It accommodates for the use of private address overlapping conflicts.
- D. It eliminates address renumbering when networks merge.

Answer: B, C, D

Explanation:

NAT conserves registered public addresses, maximizing its use. It also reduces address overlap and eliminates the need to renumber networks when they merge. It also increases flexibility when connecting to the Internet.

Incorrect Answers:

A: NAT is only useful for IP applications. No other routed protocols are supported with NAT.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1, Page 14-6

QUESTION 101:

On the Certkiller network, you want traffic to the Internet servers to be load balanced. The Internet router is configured with Network Address Translation (NAT). Which two actions enable load sharing through NAT? (Choose two)

- A. Enable TCP load distribution.
- B. Map the protocol ports that will be used.
- C. Create DNS entries for the inside addresses.
- D. Map an outside address to a group of inside addresses.
- E. Configure each server with the group of inside addresses.

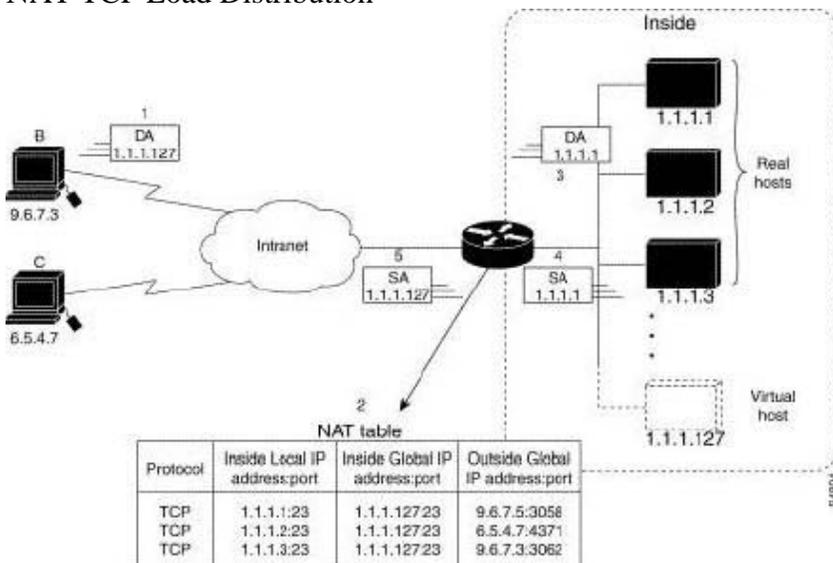
Answer: A, D

Explanation:

Providing TCP Load Distribution

Another use of NAT is unrelated to Internet addresses. Your organization may have multiple hosts that must communicate with a heavily used host. Using NAT, you can establish a virtual host on the inside network that coordinates load sharing among real hosts. Destination addresses that match an access list are replaced with addresses from a rotary pool. Allocation is done on a round-robin basis, and only when a new connection is opened from the outside to the inside. Non-TCP traffic is passed untranslated (unless other translations are in effect).

NAT TCP Load Distribution



The router performs the following process when translating rotary addresses:

1. The user on Host B (9.6.7.3) opens a connection to virtual host at 1.1.1.127.
2. The router receives the connection request and creates a new translation, allocating the next real host (1.1.1.1) for the inside local IP address.
3. The router replaces the destination address with the selected real host address and forwards the packet.

4. Host 1.1.1.1 receives the packet and responds.

5. The router receives the packet, performs a NAT table lookup using the inside local address and port number, and the outside address and port number as the key. The router then translates the source address to the address of the virtual host and forwards the packet.

The next connection request will cause the router to allocate 1.1.1.2 for the inside local address.

TCP Load Distribution Example:

In the following example, the goal is to define a virtual address, connections to which are distributed among a set of real hosts. The pool defines the addresses of the real hosts. The access list defines the virtual address. If a translation does not already exist, TCP packets from serial 0 (the outside interface) whose destination matches the access list are translated to an address from the pool.

```
ipnatpoolreal-hosts192.168.15.2192.168.15.15prefix-length28typertotary
```

```
ipnatinsidedestinationlist2poolreal-hosts
```

```
!
```

```
interfaceserial0
```

```
ipaddress192.168.15.129255.255.255.240
```

```
ipnatoutside
```

```
!
```

```
interfaceethernet0
```

```
ipaddress192.168.15.17255.255.255.240
```

```
ipnatinside
```

```
!
```

```
access-list2permit192.168.15.1
```

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a00800c

QUESTION 102:

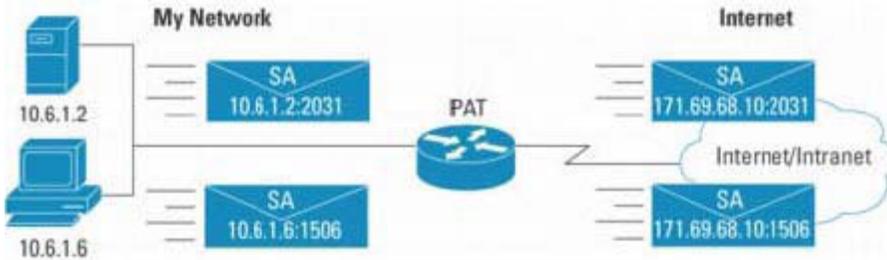
PAT, or many to one NAT, is being configured on router CK1 . Which port does PAT use to keep track of individual conversations going through this router?

- A. Inside Source
- B. Outside Source
- C. Inside Destination
- D. Outside Destination

Answer: A

Explanation:

The basic concepts of PAT (NAT overload) is displayed below:



Port Address Translation (PAT) extends NAT from "1 to 1" to "many-to-1" by associating the source port with each flow

Unique Source Port per Translation Entry

Pro	Inside Global	Inside Local	Outside Local	Outside Global
tcp	171.69.68.5:1405	10.6.15.2:1405	204.71.200.69:80	204.71.200.69:80

PAT (Port Address Translation) includes ports in addition to IP addresses

Many-to-one translation

Maps multiple IP addresses to 1 or a few IP addresses

Unique source port number identifies each session

Conserves registered IP addresses

Also called NAPT in IETF documents

Several internal addresses can be NATed to only one or a few external addresses by using a feature called Port Address Translation (PAT) which is also referred to as "overload", a subset of NAT functionality.

PAT uses unique source port numbers on the Inside Global IP address to distinguish between translations. Because the port number is encoded in 16 bits, the total number could theoretically be as high as 65,536 per IP address. PAT will attempt to preserve the original source port, if this source port is already allocated PAT will attempt to find the first available port number starting from the beginning of the appropriate port group 0-5111, 512-1023 or 1024-65535. If there is still no port available from the appropriate group and more than one IP address is configured, PAT will move to the next IP address and try to allocate the original source port again. This continues until it runs out of available ports and IP addresses.

Reference:

http://www.cisco.com/en/US/tech/CK648/CK361/technologies_white_paper09186a0080091cb9.shtml

QUESTION 103:

Which router command could you use to establish a reverse telnet session to a local modem connected to line 8?

- A. telnet 192.168.1.1 1008
- B. telnet 192.168.1.1 2008
- C. telnet 192.168.1.1 8
- D. telnet 8 192.168.1.1

Answer: B

To establish a reverse Telnet session to a modem, determine the IP address of your LAN

(Ethernet) interface, then enter a Telnet command to port 2000 + n on the access server, where n is the line number to which the modem is connected. For example, to connect to the modem attached to line 8, enter the following command from an EXEC session on the access server:

```
router# telnet 192.168.1.1 2008
Trying 192.168.1.1, 2008 ... Open
```

QUESTION 104:

Router CK1 is configured as shown below:
modemcap entry micro_LL_orig:AA=s0=0&L2

```
!  
line 74  
no exec  
modem InOut  
modem autoconfigure type micro_LL_orig  
transport input all
```

On two occasions the phrase "micro_LL_orig" appears. What does it refer to?

- A. A modem-type name descriptor.
- B. A Cisco IOS defined modemcap.
- C. An entry for modem autodiscovery.
- D. The modem Auto Answer descriptor.

Answer: A

Explanation:

For the modemcap entry command, one of the pre-defined modem-types may be used or a completely user-defined modemcap may be created. For leased-line, no new modem-type was added. Users may create their own modemcaps for leased-line functionality.

To configure the modem for leased line operation, use the modemcap entry command.

For each connection, each modem must be configured as an originator or answerer.

In the examples, "micro_LL_ans" and "micro_LL_orig" are arbitrary text descriptions for the modem type. The Cisco IOS available modem entries are displayed in the following table:

Modemcap Entries for Supported Modems

Modem Type	Output
hayes_optima	FD=&F:AA=S0=1:DTR=&D2:CD=&C1:TPL=default.
codex_3260	FD=&F:AA=S0=1:CD=&C1:DTR=&D2:HFL=*FL3:SPD=*SC1:BER
usr_courier	HFL=&H1&R2:SPD=&B1:BER=&M4:BCP=&K1:NER=&M0:NCP=&
usr_sportster	TPL=usr_courier.
hayes_optima	

viva
HFL=&K3:BER=&Q5:BCP=&Q9:NER=&Q0:NCP=&Q0:TPL=default
telebit_t3000
HFL=&K3:BER=&Q5:BCP=%C1:NER=&Q6:NCP=%C0:TPL=default
HFL=S58=2:BER=S180=3:BCP=S190=1:NER=S180=0:NCP=S190=0

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1834/products_feature_guide09186a00800803d6.html

QUESTION 105:

Why would the Certkiller administrator want to issue the "flowcontrol hardware" configuration command on an asynchronous line?

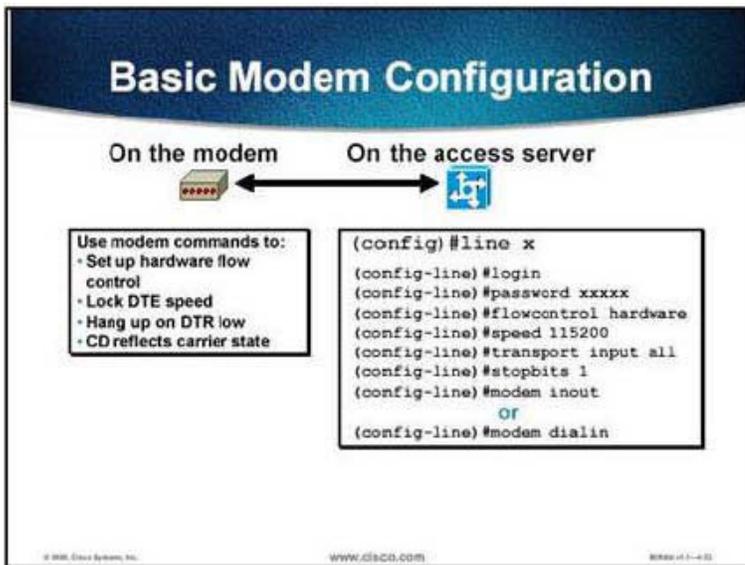
- A. It sets the modem to handle flow control instead of the router.
- B. It sets the line to use CTS/RTS flow control.
- C. It sets the modem to use MNP4 firmware.
- D. It sets RAM aside to buffer incoming and outgoing data.

Answer: B

Explanation:

Using hardware flow control (RTS/CTS), the async port drops Request To Send (RTS) when it wants the modem to disconnect, and the modem must drop Clear To Send (CTS) if it wants flowcontrol on the AUX port.

flowcontrol hardware - Uses RTS/CTS for flow control.

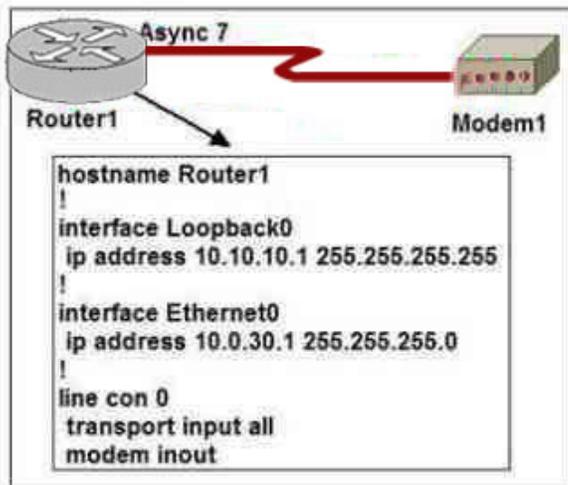


Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 4-25

QUESTION 106:

The partial configuration file of one of the Certkiller routers is shown below:



Based on this information, which of the following commands would you use to connect to Modem 1 from Router 1?

- A. telnet 10.0.30.1:7
- B. telnet 10.10.10.1 2007
- C. telnet 10.10.10.1:7
- D. reverse telnet 10.0.30.1

Answer: B

Explanation:

Since you have to go from the router to the modem you need to establish a reverse telnet session. You use the command telnet (not reverse telnet), the IP address of the modem (10.10.10.1 not, 10.0.30.1 which is the router's interface address) and a 2000 series number for the port (2000 + the number of the line console). Since the above diagram has the key phrase async 7 we can deduce that we are to connect to line 7, therefore use the port number 2007.

QUESTION 107:

You have a fixed chassis 8-port asynchronous access server. What commands can you use to view new entries on the modem capability database? (Choose all that apply)

- A. show modem entry
- B. show running-config
- C. modem entry
- D. show modemcap
- E. show entry modemcap
- F. None of the above.

Answer: B, D

Explanation:

The command show modemcap shows the modemcap database; including the values set for your current modem and the modems that the router has entries for. If there are additional details for a certain entry in the modem capabilities database, an argument is entered adjoining the entry so you can view more information. To see how the modem port options for the router are configured, use the "show running-config" command.

Reference: CCNP Remote Access Exam Certification Guide, pages 83-84, Brian Morgan & Craig Dennis, Cisco Press 2001, ISBN 1-58720-003-1

QUESTION 108:

What command could a network technician use to enable an antiquated asynchronous dialup connection on a serial interface?

- A. modem inout
- B. physical-mode async
- C. physical-layer async
- D. dialer-group layer async
- E. None of the above

Answer: C

Explanation:

Router interfaces that are synchronous only cannot be used for modem or asynchronous communication. On the router models with A/S ports (ports that can be used in the synchronous or asynchronous mode), the serial ports default to synchronous, and the interface must be declared for asynchronous usage using the physical-layer async command.

Reference:

Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)
Page 95

QUESTION 109:

On router CK1 the following command was successfully issued:

```
telnet 10.10.30.4 2009
```

What has occurred as a result of this command? (Choose all that apply.)

- A. A connection to a modem that is on line 9 is made.
- B. It specified a BRI connection to be used for Telnet.
- C. It is used to reverse Telnet connection.
- D. It is used to Telnet to port 2009 on a specific computer.

Answer: A, C

Explanation:

Line Types Line Numbering

con line = 0

tty n line = n

aux line = last_tty + 1

vty m line = last_tty + 2 + m

In the table, m refers to the number of the vty line, for example, the vty 4 line corresponds to line 14 on a router with 8 TTY ports. TTY lines correspond to asynchronous interfaces on a one-to-one basis, and vty

lines are virtual lines dynamically assigned to the synchronous interfaces.

Usually vty lines are associated with incoming Telnet sessions.

Connections to an individual line are most useful when a dial-out modem, parallel printer, or serial printer is attached to that access server line. To connect to an individual line, the remote host or terminal must specify a particular Transmission Control Protocol (TCP) port on the access server. If the Telnet protocol is used, that port is 2000 plus the line number, for example:

```
telnet 10.10.30.4 2009
```

This command initiates a reverse Telnet connection to line 9 (2000 + 9).

The following line types are used:

- * CON - Console port (available on all Cisco routers)
- * TTY - Asynchronous port
- * AUX - Auxiliary port (available on most Cisco routers)
- * VTY - Virtual terminal (for incoming Telnet, LAT, or X.25 PAD connections)

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 4-21

QUESTION 110:

Router CK1 is a Cisco router equipped with a synchronous serial interface. Which of the following standards does this interface comply with? (Choose all that apply)

- A. V.45
- B. EIA-530
- C. V.90
- D. V.35
- E. EIA/TIA-232
- F. None of the above

Answer: B, D, E

Explanation:

Dedicated leased lines typically require synchronous serial connections. The dedicated connections are made using the router's synchronous serial ports with bandwidth use of up to 34 Mbps on an E3 and 45 Mbps on a T3, available through the use of a channel service unit/data service unit (CSU/DSU). Different encapsulation methods at the data-link layer provide flexibility and reliability for user traffic. Typical connections on a dedicated network employ 56 kbps, 64 kbps, T1, E1, T3, and E3 technologies.

The following synchronous serial standards are supported on Cisco routers:

- * Electronic Industries Association/Telecommunications Industry Association (EIA/TIA)-232
- * EIA/TIA-449
- * V.35
- * X.21, X.25
- * EIA-530

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 2-6

QUESTION 111:

Before a Cisco router can accept an incoming connection through an asynchronous port, one must use an enabling command to specify which protocols are allowed through this port. Which of the following is it?

- A. modem inout
- B. async-group in
- C. access-group async
- D. transport input

Answer: D

Explanation:

Cisco routers do not accept incoming network connections to asynchronous ports (TTY lines) by default. You have to specify an incoming transport protocol, or specify transport input all before the line will accept incoming connections

Use the transport preferred command to specify which transport protocol is used on connections. Use the transport input and transport output commands to explicitly specify the protocols allowed on individual lines for both incoming and outgoing connections.

The protocol options that can be specified are:

all | lat | mop | nasi | none | pad | rlogin | ssh | telnet | v120

Reference:

http://cisco.com/en/US/products/sw/iosswrel/ps1828/products_configuration_guide_chapter09186a0080087329

QUESTION 112:

On one of the Certkiller routers the following configuration commands were entered:

```
router(config)#interface group-async 1
router(config)#group-range 1 7
```

What are the resulting consequences of these commands?

- A. Assigns asynchronous interfaces 1 through 7 to a single master interface
- B. Assign dialer privileges to interfaces async 1 through 7

- C. Creates virtual asynchronous interfaces 1 through 7
- D. Creates virtual TTY interfaces 1 through 7
- E. Trunks asynchronous interfaces to increase modem bandwidth
- F. Creates a modem pool on interfaces 1 through 7

Answer: A

Explanation:

To create a group interface to serve as master to which asynchronous interfaces can be associated as members, use the interface group-async command in global configuration mode. To restore the default, use the no form of this command.

```
interface group-async unit-number  
no interface group-async unit-number
```

Using the interface group-async command, you create a single asynchronous interface to which other interfaces are associated as members using the group-range command. This one-to-many configuration allows you to configure all associated member interfaces by entering one command on the group master interface, rather than entering this command on each individual interface. You can create multiple group masters on a device; however, each member interface can be associated only with one group.

Example:

The following example defines asynchronous group master interface 0:

```
Router(config)#interfacegroup-async0
```

Related Commands

Command Description

Command	Description
group-range	Creates a list of member asynchronous interfaces (associated with a group interface).
member	Alters the configuration of an asynchronous interface that is a member of a group.

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a008008

QUESTION 113:

Router CK1 has a modem attached to it, but you are unsure what type of modem it is. What command would you issue if you wanted the router to automatically

discover the modem type, as well as automatically configure the settings?

- A. modem autoconfigure discovery
- B. modem autoconfigure type discovery
- C. modem discovery autoconfigure
- D. modem discovery type autoconfigure
- E. None of the above

Answer: A

Explanation:

Modem autoconfiguration is a Cisco IOS software feature that enables the router to issue the modem configuration commands, which frees the administrator from creating and maintaining scripts for each modem. The general syntax for modem autoconfiguration is as follows:

```
modem autoconfigure [discovery | type modemcap-entry-name]
```

The two command options for the modem autoconfigure command are as follows:

* type - This option configures modems without using modem commands, or so it is implied. The type argument declares the modem type that is defined in the modem capabilities database so that the administrator does not have to create the modem commands.

* discovery - Autodiscover modem also uses the modem capabilities database, but in the case of discover, it tries each modem type in the database as it looks for the proper response to its query.

As you can see, the modem autoconfigure command relies on the modem capabilities database, also known as the modemcap database. The modemcap database has a listing of modems and a generic initialization string for the modem type. The discovery of a modem using the autoconfigure feature uses the initialization strings from each modem in the modemcap database. If the modem is not in the database, it fails, and the administrator has to manually add the modem to the database.

Reference:

Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)

Page 99

QUESTION 114:

SIMULATION

After completing your CCNP designation, your boss promoted you to the position of Vice President of Asynchronous Communications. Your first assignment is to configure the company's router to accept asynchronous connections, to allow for out of band management for the router.

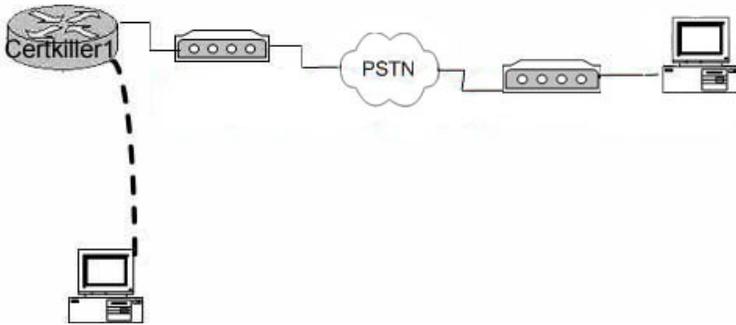
Your project is to:

- * Configure S0/1 for Asynchronous communication
- * Set the line speed to 56K
- * Set the flow control to hardware.
- * Set the stop bits to one.

- * Set the line password to "Budweiser".
- * Configure the line to allow for both incoming and outgoing calls.
- * Allow all protocols for incoming connections on the line.
- * Set the loopback address to 192.168.0.1/32.

Once you complete your task, you have to check your work:

- * Reverse telnet to the modem.
- * Issue an AT command to login to modem configuration (modem should respond with OK)



What configuration commands will accomplish these tasks?

Answer:

```
Certkiller >
Certkiller 1> enable
Certkiller 1# Configure terminal
Certkiller 1(config)# Interface serial0/1
Certkiller 1(config-if)# Physical-layer async
Certkiller 1(config-if)# Exit
Certkiller 1(config)# Line 2
Certkiller 1(config-line)# Flowcontrol hardware
Certkiller 1(config-line)# Stopbits 1
Certkiller 1(config-line)# Password Budweiser
Certkiller 1(config-line)# Login
Certkiller 1(config-line)# Transport input all
Certkiller 1(config-line)# Speed 56000
Certkiller 1(config-line)# Modem inout
Certkiller 1(config-line)# Exit
Certkiller 1(config)# Interface loopback1
Certkiller 1(config-if)# Ip address 192.168.0.1 255.255.255.255
Certkiller 1(config-if)# Exit
Certkiller 1(config)# ip host modem 2002 192.168.0.01
Certkiller 1(config)# Exit
Certkiller 1# Copy run start
Certkiller 1# end
Certkiller 1> telnet 192.168.0.1 2002
```

Reference:

This configuration was verified in the Certkiller lab.

QUESTION 115:

You are supervising an apprentice network technician, and he enters the following commands on router Certkiller 1:

```
Certkiller 1#configure terminal
```

```
Certkiller 1(config)#line 10
```

```
Certkiller 1(config-line)#transport input all
```

```
Certkiller 1(config-line)#modem inout
```

What will be the resulting actions of these commands?

- A. One-way IP traffic will be enabled.
- B. One-way Telnet from the modem to the router will be enabled.
- C. Telnet will be enabled on TCP port 10.
- D. Telnet will be enabled on TCP port 2010.

Answer: D

Explanation:

Cisco access servers support both incoming asynchronous line connections (forward connections) and outgoing asynchronous line connections (reverse connections). For example, a remote terminal user dialing into the access server through an asynchronous line makes a forward connection; a user connects through an access server (reverse connection) to an attached modem to configure the modem.

A host can make reverse Telnet connections to various types of devices attached to a Cisco access server. Different port numbers (20xx, 40xx, and 60xx) are used because different data type and protocol negotiations will take place for different types of devices attached to the access server.

The remote host must specify a particular TCP port on the router to connect with individual lines or to a rotary group. In the first line of the preceding example, the remote host makes a reverse Telnet connection to the modem using port address 2007. Note that TCP port number 2007 specifies a Telnet protocol connection (TCP port 2000) to line 7. The individual line number is added to the end of the port number type.

Connection Service	Reserved Port Range for Individual Ports	Reserved Port Range for Rotary Groups
Telnet (character mode)	2000–2xxx	3000–3xxx
TCP (line mode)	4000–4xxx	5000–5xxx
Telnet (binary mode)	6000–6xxx	7000–7xxx
Xremote	9000–9xxx	10000–10xxx

The transport input protocol command to specify which protocol to allow for connections. For example, transport input all allows all of the following protocols to be used for the connection:

```
lat | mop | nasi | none | pad | rlogin | telnet | v120
```

Each of these command options can also be specified individually.

modem inout - Uses the modem for both incoming and outgoing calls.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Chapter 4

QUESTION 116:

You're a supervisor at Certkiller and you're peaking into a trainee's workstation and you notice him enter this command.

```
ip host remote 2007 157.23.23.96
```

What's the result of this command? (Choose all that apply.)

- A. The command uses the Xremote protocol.
- B. The configuration applies to a modem attached to line 7
- C. The configuration applies to a modem attached to line 2007.
- D. 2007 is the dialer group.
- E. The command facilitates a reverse Telnet connection.

Answer: B, E

Explanation:

The configuration command "ip host name number address" defines a name and associates it to a port and/or address for Telnet. (Use a 2xxx number for the line.) This command allows a reverse Telnet connection to line 97. The name (we chose "remote") can be any you choose.

Use the ip host configuration command to simplify reverse Telnet sessions with modems. The ip host command maps an IP address of a port to a device name.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 4-47

QUESTION 117:

Which of these commands are configured from the line configuration mode?
(Choose three)

- A. async mode interactive
- B. encapsulation ppp
- C. speed 115200
- D. modem inout
- E. flowcontrol hardware
- F. None of the above

Answer: C, D, E

Explanation:

The various line configuration options with their descriptions are displayed below:

(config-line)#exec - Allows the EXEC process on this line.

(config-line)#login - Sets a login password on this line. Without the password, no

connection is allowed.

(config-line)#password - password Sets the password to be used when logging in to this line.

(config-line)#flowcontrol hardware - Uses RTS/CTS for flow control.

(config-line)#speed 115200 - Sets the maximum speed (in bits per second) between the modem and the access server. The speed command sets both the transmit and receive speed.

(config-line)#transport input all - Allows all protocols to be passed to the access server through this line.

(config-line)#stopbits - Sets the number of stop bits transmitted per byte.

(config-line)#modem inout - Uses the modem for both incoming and outgoing calls.

(config-line)#modem dialin - Uses the modem for incoming calls only (the default).

Incorrect Answers:

A: To return a line that has been placed into dedicated asynchronous network mode to interactive mode, thereby enabling the slip and ppp EXEC commands, use the async mode interactive interface configuration command. This command is used in Async interface mode, not in line mode.

B: PPP encapsulation is an interface configuration option.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 4-25 & 4-26

QUESTION 118:

If you were to set up a reverse Telnet session (from your router to an individual modem) what port range would you use?

- A. 0 to 1099
- B. 2000 to 2099
- C. 3000 to 3099
- D. 4000 to 4099
- E. 5000 to 5099

Answer: B

Explanation:

A host can make reverse Telnet connections to various types of devices attached to a Cisco access server. Different port numbers (20xx, 40xx, and 60xx) are used because different data type and protocol negotiations will take place for different types of devices attached to the access server.

The remote host must specify a particular TCP port on the router to connect with individual lines or to a rotary group. In the first line of the preceding example, the remote host makes a reverse Telnet connection to the modem using port address 2007. Note that TCP port number 2007 specifies a Telnet protocol connection (TCP port 2000) to line 7. The individual line number is added to the end of the port number type.

References:

QUESTION 119:

You are connected to router CK1 via line 0. Which of the following line types is associated with the line number zero on this router?

- A. Asynchronous line
- B. Auxiliary line
- C. Console line
- D. Virtual terminal line
- E. All of the above

Answer: C

Explanation:

Cisco devices have the line numbers assigned in the following manner:

Console line (CON): Assigned line number 0

Asynchronous lines (TTY): Assigned line number n, where n represents the first physical line after the Console line. For example, TTY line 4 is assigned line number 4.

Auxiliary line (AUX): The auxiliary line is assigned the last TTY (async) line + 1. For example, if there can be n TTY lines, the Auxiliary line is assigned n+1. Note that the TTY lines are as recognized by Cisco IOS and not necessarily be present physically.

QUESTION 120:

The Certkiller network administrator has connected a modem to the console port of a router. What is a reason for this type of connection? (Select all that apply)

- A. Passwords can be recovered remotely.
- B. Reverse Telnet has been configured.
- C. Dial-on-demand routing has been configured.
- D. The router needs to be accessible remotely.
- E. None of the above.

Answer: A, D

Explanation:

ConsolePortIssues

There are several advantages to connecting a modem to the console port of a router instead of the AUX port; however, the disadvantages are significant.

Advantages of connecting a modem on the console port:

You can recover passwords remotely. You may still need someone on-site with the router to toggle the power, but aside from that, it is identical to being there with the router.

It is a convenient way to attach a second modem to a router without async ports. This is beneficial if you need to access the router for configuration or management and leave the AUX port free for dial-on-demand routing (DDR).

Some routers (for example, Cisco 1600s) do not have AUX ports. If you want to connect a modem to the router and leave the serial port(s) free for other connections, the console is the only option.

Disadvantages of connecting a modem on the console port:

The console port does not support RS232 modem control (data set ready/Data Carrier Detect (DSR/DCD), data terminal ready (DTR)). Therefore, when the EXEC session terminates (logout), the modem connection does not drop automatically; the user needs to manually disconnect the session.

More seriously, if the modem connection should drop, the EXEC session does not automatically reset. This can present a security hole, in that a subsequent call into that modem will be able to access the console without entering a password. You can make the hole smaller by setting a tight exec-timeout on the line. However, if security is important, use a modem that can provide a password prompt.

Unlike other async lines, the console port does not support hardware (Clear to Send/Ready to Send (CTS/RTS) flow control. It is recommended to use no flow control. If data overruns are encountered, however, you can enable software (XON/XOFF) flow control.

The console ports on most systems only support speeds of up to 9600 bps.

The console port lacks reverse telnet capability. If the modem loses its stored initialization string, the only remedy is to physically disconnect the modem from the router and attach it to another device (such as an AUX port or a PC) to reinitialize.

If a modem on an AUX port loses its initialization string, you can use reverse telnet remotely to correct the problem.

You cannot use a console port for dial-on-demand routing; it has no corresponding async interface.

QUESTION 121:

You are logged in to router CK1 and need to change the configuration of the line ports used for modems. Which of the following parameters are set using the line command? (Choose all that apply)

- A. Speed
- B. Encapsulation protocol
- C. Compression ratio
- D. Authentication method
- E. Flow control
- F. IP address
- G. Speed units

Answer: A, E

Explanation:

642-821

Line configuration commands modify the operation of a terminal line. Line configuration commands always follow a line command, which defines a line number. These commands are used to change terminal parameter settings line-by-line or a range of lines. In general, the following line configuration works best for modem connections:

line "x"	TTY #. AUX port is line 1 on the router, last_tty+1 on the access server, line 65 on the Cisco 2600s and 3620, and line 129 on the Cisco 3640.
speed "xxxxx"	Set to the highest speed in common between the modem and the port. This value is usually 115200 baud, but see the Bitrate Information.
stopbits 1	Improve throughput by reducing async framing overhead (default is stopbits 2).
flowcontrol hardware	RTS/CTS flow control.
modem inout	Drop connection on loss of DCD (DSR). Cycle DTR for connection close. This command also allows outbound connections to the modem.
transport input all telnet	Allow outbound connections to this line. Needed in order to allow reverse telnet to the modem.

Reference:

http://www.cisco.com/en/US/tech/CK801/CK36/technologies_tech_note09186a008009428b.shtml

QUESTION 122:

Which of the following are valid functions that chat scripts perform? (Choose all that apply)

- A. Modem configuration
- B. Dialing and remote login

- C. Failure detection
- D. Incoming call filtering

Answer: A, B, C

Explanation:

Chat scripts are strings of text used to send commands for modem dialing, logging onto remote systems, and initializing asynchronous devices connected to an asynchronous line. On a router, chat scripts can be configured on the auxiliary port only. A chat script must be configured to dial out on asynchronous lines. You also can configure chat scripts so that they are executed automatically for other specific events on a line, or so that they are executed manually. Each chat script is defined for a different event.

QUESTION 123:

You are running commands on modemcap. You use the following command on router CK1 :

modemcap entry

What is this command used for?

- A. Adds new entry or edit current entry
- B. Views a particular modemcap entry.
- C. Displays current capabilities
- D. Deletes an entry

Answer: C

Explanation:

To store and compress information about the capability of a specified modem, use the modemcap entry command in global configuration mode.

Syntax Description

modem-type Type of supported modemcap entry

Modemcaps are displayed within the configuration file and can be edited using the modemcap edit command. The modemcap entry command does not display values that are not set in the modem.

Use the modemcap entry command with the show modemcap command to interpret the capability of the specified modem.

QUESTION 124:

You are configuring a new Cisco router to operate with a modem attached to the aux port. Which of the following are valid functions of the lock DTE modem attribute that can be used on this router?

- A. Disable UART.
- B. Enable UART.

- C. Locks the data speed between the computer motherboard and the RS232 port.
- D. Locks the data speed between the modem and the DTE device.

Answer: D

Explanation:

The lock DTE speed command is often related to the way the modem handles error correction. This command varies widely from one modem to another. Locking the modem speed ensures that the modem always communicates with the Cisco access server or router at the speed configured on the Cisco auxiliary port.

QUESTION 125:

Your boss requires you to use the modem for both incoming and outgoing calls. What configuration command will enable this?

- A. modem inout
- B. en modem inout
- C. modem inout enable
- D. en modem in out

Answer: A

Explanation:

To configure a line for both incoming and outgoing calls, use the modem inout line configuration command.

Default

No modem control.

Command Mode

Line configuration.

Usage Guidelines

This command applies to the auxiliary port only.

QUESTION 126:

On an asynchronous modem line, which of the following are NOT functions that chat scripts perform? (Choose all that apply)

- A. Logging into a remote system.
- B. Sending messages from one telnet session to another.
- C. Instructing the modem to dial out.
- D. Filtering incoming calls.
- E. Initializing the directly-attached modem.

Answer: B, D

Explanation:

Chat scripts are strings of text used to send commands for modem dialing, logging in to remote systems, and initializing asynchronous devices connected to an asynchronous line. On a router, chat scripts can be configured on the auxiliary port only. A chat script must be configured to dial out on asynchronous lines. You also can configure chat scripts so that they can be executed automatically for other specific events on a line, or so that they are executed manually.

QUESTION 127:

With regards to the dialer pool, what optional keyword command can you use to resolve potential contention problems on this dialer pool? (Type in answer below)

Answer: priority

Explanation:

Dialer pool - Each interface references a dialer pool, which is a group of physical interfaces associated with a dialer profile. A physical interface can belong to multiple dialer pools. Contention for a specific physical interface is resolved by configuring the optional priority command.

QUESTION 128:

A network administrator needs to provide telecommuters with access to corporate network services. For security reasons, the asynchronous interface should be configured to provide an in-band PPP connection only and not allow an EXEC connection. What must the administrator configure to accomplish this?

- A. Router(config-if)# async mode dedicated
- B. Router(config-if)# async mode interactive
- C. Router(config-if)# async dynamic address
- D. Router(config-line)# autoselect ppp during-login

Answer: A

Explanation:

With dedicated asynchronous network mode, the interface will use either SLIP or PPP encapsulation, depending on which encapsulation method is configured for the interface. An EXEC prompt does not appear, and the router is not available for normal interactive use.

If you configure a line for dedicated mode, you will not be able to use the async dynamic address command, because there is no user prompt.

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_command_reference_chapter09186a00800c

QUESTION 129:

In an ISDN BRI circuit; what range of values are assigned for Valid Dynamic TEI (Terminal Endpoint Identifier)?

- A. 128-256
- B. 25-62
- C. 64-126
- D. 1-24

Answer: C

Explanation:

A terminal endpoint can be any ISDN-capable device attached to an ISDN network. The TEI is a number between 0 and 127, where 0-63 is used for static TEI assignment, 64-126 are used for dynamic assignment, and 127 is used for group assignments. (0 is used only for PRI.) The TEI provides the physical identifier, and the Service Access Point Identifier (SAPI) carries the logical identifier.

The process of assigning TEIs differs slightly between North America and Europe. In North America, Layer 1 and Layer 2 are activated at all times. In Europe, the activation does not occur until the call setup is sent (known as "first call"). This delay conserves switch resources. In Germany and Italy, and in other parts of the world, the procedure for TEI assignment can change according to local practices.

In other countries, another key piece of information to obtain is the bus type. Supported types are point-to-point or point-to-multipoint connection styles. In Europe, if you are not sure which is supported, specify a point-to-multipoint connection, which will enable dynamic TEI addressing. This is important if BRI connections are necessary, because Cisco does not support BRI using TEI 0, which is reserved for PRI TEI address 0. If you see a TEI of 0 on a BRI, it means that a dynamic assignment has not yet occurred, and the BRI may not be talking to the switch. In the United States, a BRI data line is implemented only in a point-to-point configuration.

Reference:

Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)
Page 151

QUESTION 130:

Which T1 controller command would you use when configuring the timeslots on an ISDN PRI interface on router CK1 , which is using a T1 ISDN line?

- A. linecode
- B. framing
- C. pri-group
- D. isdn switch-type
- E. barcode

Answer: C

Explanation:

To specify an ISDN PRI group on a channelized T1 or E1 controller, and to release the ISDN PRI signaling time slot, use the pri-group timeslots command in controller configuration mode.

```
pri-group timeslots timeslot-range [nfas_d { backup | none | primary { nfas_int  
number | nfas_group number | rlm-group number } } | service]
```

Syntax Description

timeslot-range A value or range of values for time slots on a T1 or E1 controller that consists of an ISDN PRI group. Use a hyphen to indicate a range.

Note

Groups of time slot ranges separated by commas (1-4,8-23 for example) are also accepted.

nfas_d { backup | none | primary } (Optional) Configures the operation of the ISDN PRI D channel.

backup-The D-channel time slot is used as the Non-Facility Associated Signaling (NFAS) D backup.

none-The D-channel time slot is used as an additional B channel.

primary-The D-channel time slot is used as the NFAS D primary. The primary keyword requires further interface and group configuration:

```
primary { nfas_int number | nfas_group number | rlm-group number } -
```

nfas_int number-Specifies the provisioned NFAS interface as a value; value is a number from 0 to 8.

nfas_group number-Specifies the NFAS group.

rlm-group number-Specifies the Redundant Link Manager (RLM) group and release the ISDN PRI signaling channel.

service (Optional) Configures service type mgcp for Media Gateway Control Protocol service.

Defaults:

No ISDN PRI group is configured. The switch type is automatically set to the National ISDN switch type (primary-ni keyword) when the pri-group timeslots command is configured with the rlm-group subkeyword.

Incorrect Answers:

D: This command is used to specify the central office switch type on the ISDN interface, or to configure the Cisco PRI interface to support QSIG signaling. This command is done in the interface configuration mode. Furthermore, we believe this question to be trying to identify the difference between T1 and E1 in regards to the timeslot assignments.

QUESTION 131:

A new T1 line is being provisioned for the Certkiller network. What are your configuration options when configuring T1/E1 line-codes? (Choose all that apply.)

- A. AMI
- B. ESF

- C. B8ZS
- D. SF
- E. CRC4

Answer: A, C

Explanation:

The valid line-code options for T1/E1 are: AMI, B8ZS, and HDB3.

Use the linecode command to identify the physical layer signaling method to satisfy the ones density requirement on the provider's digital facility. Without a sufficient number of ones in the digital bit stream, the switches and multiplexers in a WAN can lose their synchronization for transmitting signals.

* AMI Alternate Mark Inversion. Used for T1 configurations.

* B8ZS Binary 8-zero substitution. Use for T1 PRI configurations.

* HDB3 High Density Bipolar 3. Use for E1 PRI configurations.

Binary 8-zero substitution (B8ZS) accommodates the ones density requirements for T1 carrier facilities using special bipolar signals encoded over the digital transmission link. It allows 64 kbps (clear channel) for ISDN channels. Settings for these two Cisco IOS software controller commands on the router must match the framing and line-code types used at the T1/E1 WAN provider's CO switch.

Incorrect Answers:

A, C: SF, ESF, and CRC4 are valid framing types, not line coding options.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 2-12 ; 2-13 & 7-68

QUESTION 132:

A new T1 circuit is being provisioned for a new remote Certkiller location. Which of the following framing types are associated with T1/E1 lines? (Choose all that apply.)

- A. AMI
- B. ESF
- C. B8ZS
- D. SF
- E. CRC4

Answer: B, D, E

Explanation:

The valid framing types on a T1 controller are Super Frame (SF) and Extended Super Frame (ESF). CRC4 is a framing option used on E1 lines.

Incorrect Answers:

A, C: AMI and B8ZS are valid line coding types, not framing types.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 7-68

QUESTION 133:

Router CK1 uses an ISDN line as a backup connection to the primary frame relay link. On this router you enter the following command:

```
backup load 60 5
```

What effect will this change make? (Choose two)

- A. The backup link activates when the primary link exceeds 60 percent of bandwidth.
- B. The backup link activates when the primary link exceeds 60 kbps.
- C. The backup link deactivates when the primary link falls to 5 percent bandwidth.
- D. The backup link deactivates when the combined load falls to 5 percent bandwidth.
- E. The backup link deactivates when the combined load falls to 5 kbps.

Answer: A, D

Explanation:

The commands backup load & no backup load are used to add and remove backup links based on traffic congestion. The command has two number variables which are percentage functions. The first one is the enable threshold and the second one is the disable load variable. So in the above example when the primary link exceeds 60% of its maximum bandwidth the backup link activates. The backup link will continue to be activated until the combined load on both links drops to 5% of maximum bandwidth (as network usage peaks tend to spike high periodically).

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_command_reference_chapter09186a00800c

QUESTION 134:

The Certkiller network has offices in Costa Rica and Brazil that communicate with the head office in Los Angeles by way of ISDN. Since each remote office is located in a different country they have unique dial requirements. Which commands would you enter on the central router to allow multiple physical interfaces to be shared by the multiple remote sites while still allowing them to keep their unique dial requirements? (Choose two)

- A. The dialer pool command
- B. The dialer-list command
- C. The dialer pool-member command
- D. The dialer-group command
- E. The dialer hunt-group command

Answer: A, C

Explanation:

A: Dialer-pool is a command which assigns a dialer interface to a specific dialer-pool.

C: Dialer pool-member makes a physical interface a member of a dialer pool, which consists of different logical interfaces with specific configurations.

Incorrect Answers:

B, D: Dialer-list and dialer-group are commands to specify an interesting traffic for the interface. When interesting traffic is seen by the router, an ISDN connection is made. If it is already established, the dialer idle timeout value is set to the maximum value.

E: Dialer hunt-group - there is no such command in Cisco IOS.

QUESTION 135:

What configuration command would you execute to define a rotary group?

- A. The dialer pool command
- B. The rotary-group command
- C. The interface rotary command
- D. The interface dialer command
- E. The dialer rotary-group command

Answer: D

Explanation:

Dialer rotary groups allow you to apply a single logical interface configuration to a set of physical interfaces. Dialer rotary groups are useful in environments that have multiple calling destinations. A dialer rotary group is defined by specifying a dialer interface. Physical interfaces are assigned to the dialer rotary group and inherit all of the dialer interface configuration parameters. When many destinations are configured, any of the physical interfaces in a rotary group can be used for outgoing calls.

interface dialer group-number - Defines a dialer rotary group. The group number ranges from 0 through 255.

Incorrect Answers:

A: Dialer pool - is for dialer profiles not for rotary groups.

B, C: There are no such commands in Cisco IOS.

E: This assigns an interface to an already specified rotary-group.

QUESTION 136:

A new ISDN circuit is being provisioned for a Certkiller location.

When is it necessary to configure the SPID on an ISDN BRI interface?

- A. When you want to use both B channels.
- B. When you want to use the D channel for low-speed data.
- C. When required by your service provider.
- D. When you want to use an ISDN BRI interface for outgoing calls.

Answer: C

Explanation:

A SPID is the Service profile identifier, which is a number that some service providers use to define the services to which an ISDN device subscribes. The ISDN device uses the SPID when accessing the switch that initializes the connection to a service provider. SPIDS are normally used to identify the ISDN circuit to the ISDN switch by many service providers, but not all. Contact your ISP for details on whether or not this information needs to be programmed into your equipment.

Reference:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t3/brivicfm.pdf>

QUESTION 137:

Which of the following commands is capable of configuring an interface for PRI and specifying the number of fixed timeslots on that circuit?

- A. pri-group
- B. interface serial
- C. dialer-group
- D. isdn switch-type
- E. None of the above

Answer: A

Explanation:

You can configure the PRI group to include all available time slots, or you can configure a select group.....

pri-group [timeslots range]

no pri-group

To specify ISDN Primary Rate Interface (PRI) on a channelized T1 card on the Cisco 7000 series, use the pri-group controller configuration command. Use the no pri-group command to remove the ISDN PRI.

timeslots range (Optional) Specifies a single range of values from 1 to 23.

When configuring NFAS for channelized T1 controllers configured for ISDN, you use an extended version of the ISDN pri-group command to specify the following:

Range of PRI timeslots to be under the control of the D channel (timeslot 24)

Function to be performed by timeslot 24 (primary D channel, backup, or none); the latter specifies its use as a B channel

Group identifier number for the interface under control of this D channel

References:

http://www.prz.tu-berlin.de/docs/misc/ciscodoc/data/doc/software/10_3/rpcs/78791.htm

http://www.cisco.com/en/US/products/hw/univgate/ps501/products_configuration_guide_chapter09186a008007d

QUESTION 138:

When configuring an ISDN interface; what purpose does the command pri-group fulfill?

- A. Configures serial interfaces created on a channelized E1 or T1 controller for ISDN PRI signaling.
- B. Configured the central office switch type for the ISDN PRI interfaces.
- C. Specifies which timeslots are allocated on the digital facility of the provider.
- D. Configured ISDN B-channel interfaces for VoIP applications that require release of the ISDN PRI signaling time slots.
- E. None of the above.

Answer: C

Explanation:

Router(config-if)#pri-group [timeslots range]

This command configures the PRI group for either T1 or E1 to carry voice traffic. For T1, available time slots are from 1 through 23; for E1, available time slots are from 1 through 31. You can configure the PRI group to include all available time slots, or you can configure a select group of time slots for the PRI group.

References: "Q.931 User-Side and Network-Side Switch Support"

http://www.cisco.com/en/US/products/sw/iosswrel/ps1834/products_feature_guide09186a00800e9764.html
Page 213 Building Cisco Remote Access Networks ISBN#1-57870-091-4

QUESTION 139:

Router CK1 is configured for ISDN as displayed below:

```
Interface BRI0
ip address 172.20.10.2 255.255.255.0
encapsulation ppp
dialer idle-timeout 30
dialer watch-disable 15
dialer load-threshold 1 outbound
dialer map ip 172.20.10.1 name RouterCK broadcast 5551111
dialer map ip 172.22.53.0 name RouterCK broadcast 5551111
dialer watch-group 8
dialer-group 8
isdn switch-type basic-ni
isdn spid1 51255526220101 5552222
isdn spid2 51255528230101 5552223
ppp authentication chap
ppp multilink
!
dialer watch-list 8 ip 172.22.53.0 255.255.255.0
access-list 101 remark Define Interesting Traffic
```

```
access-list 101 deny ospf any any  
access-list 101 permit ip any any  
dialer-list 8 protocol ip list 101
```

What is the result of the command "dialer watch-group 8"?

- A. Any IP traffic, except OSPF traffic, will cause interface BRI0 to dial RouterCK.
- B. When the watched route, 172.22.53.0/24, is removed from the routing table and there is no other valid route, dialer watch then initiates a call to RouterCK.
- C. When the watched route, 172.22.53.0/24, is removed from the routing table, regardless of whether there is another valid route pointing to an interface other than interface BRI0, dialer watch initiates the call to RouterCK.
- D. When the load threshold is met and any IP traffic, except OSPF traffic, is destined for 172.22.53.0/24 network, the dialer watch will initiate the call to RouterCK.

Answer: B

Explanation:

Dialer Watch is a backup feature that integrates dial backup with routing capabilities.

Prior dial backup implementations used the following conditions to trigger backup:

1. Interesting packets were defined at central and remote routers using Dial on Demand routing (DDR).
2. Connection loss occurred on a primary interface using a back up interface with floating static routes.
3. Traffic thresholds were exceeded using a dialer load threshold.

Prior backup implementations may not have supplied optimum performance on some networks, such as those using Frame Relay multipoint subinterfaces or Frame Relay connections that do not support end-to-end PVC status updates.

Dialer Watch provides reliable connectivity without relying solely on defining interesting traffic to trigger outgoing calls at the central router. Dialer Watch uses the convergence times and characteristics of dynamic routing protocols. Integrating backup and routing features enables Dialer Watch to monitor every deleted route. By configuring a set of watched routes that define the primary interface, you are able to monitor and track the status of the primary interface as watched routes are added and deleted. Monitoring the watched routes is done in the following sequence:

1. Whenever a watched route is deleted, Dialer Watch checks to see if there is at least one valid route for any of the defined watched IP addresses.
2. If no valid route exists, the primary line is considered down and unusable.
3. If a valid route exists for at least one of the defined IP addresses, and if the route is pointing to an interface other than the backup interface configured for Dialer Watch, the primary link is considered up.
4. If the primary link goes down, Dialer Watch is immediately notified by the routing protocol and the secondary link is brought up.
5. Once the secondary link is up, at the expiration of each idle timeout, the primary link is rechecked.
6. If the primary link remains down, the idle timer is indefinitely reset.
7. If the primary link is up, the secondary backup link is disconnected. Additionally, you

can set a disable timer to create a delay for the secondary link to disconnect, after the primary link is reestablished.

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1826/products_feature_guide09186a0080080ebf.html

QUESTION 140:

One of the Certkiller routers is configured for ISDN as shown below:

```
Interface serial0
ip address 192.168.10.1 255.255.255.0
Backup interface bri0
Backup delay 5 10
Interface bri0
ip address 192.168.11.2 255.255.255.0
dialer idle-timeout 900
dialer-group 1
```

Based on this information, what is true about the above configuration?

- A. The ISDN BRI line will go to "standby" mode 900 seconds after the serial interface reactivates.
- B. The ISDN BRI line will go to "standby" mode 10 seconds after the serial interface reactivates.
- C. The ISDN BRI line will deactivate the primary line reaches 10% utilization.
- D. The ISDN BRI line will go to standby after 900 seconds, but will reactivate if the primary line reaches 10% utilization.

Answer: B

Explanation:

If you look at carefully at this portion of command:

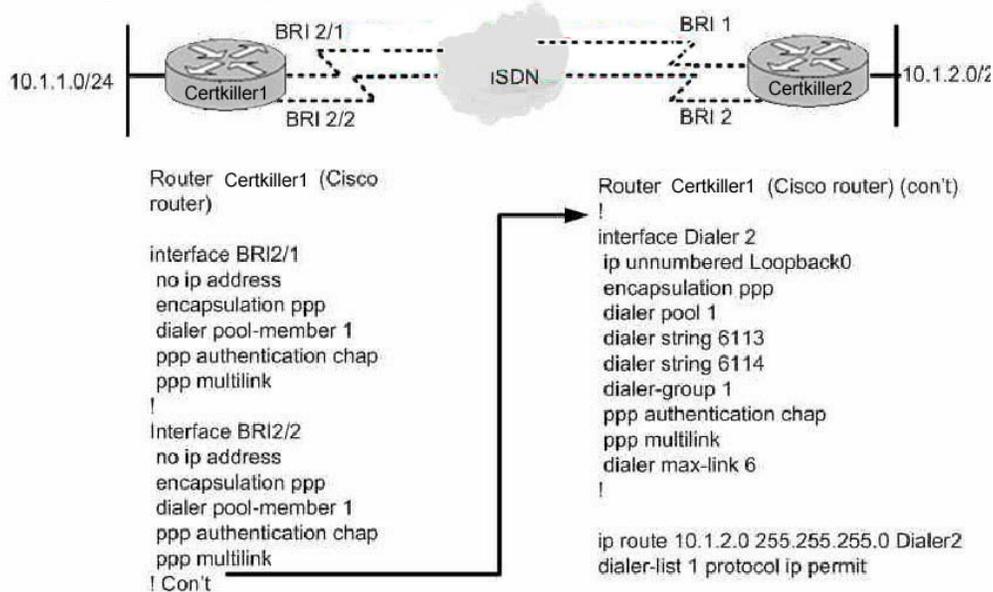
```
Interface serial0
ip address 192.168.10.1 255.255.255.0
Backup interface bri0
Backup delay 5 10
```

You'll notice that the serial interface (serial0) is backed up by the BRI interface (BR0). The commandBackup delay 5 10 has two number variables. The first number (5) commands that if serial0 were to be compromised, BRI0 is to take over after 5 seconds. The second number (10) states that if serial0 were to somehow reactivate, BRI0 will continue to remain active for 10 seconds until going into standby mode. Having a backup system wait a few seconds before kicking in is a smart feature because many times an interface may only fail for a few seconds, and five seconds is a typical length of a user's patience. The longer reactivation time is good, because the original line has to prove that it's capable of staying active for 10 seconds before earning its credibility again.

QUESTION 141:

642-821

Two Certkiller routers are set up for ISDN as shown in the diagram below, along with the partial configuration of router Certkiller 1:



Assuming that there are only two BRI interfaces on Router Certkiller 1; how many B channels will end up forming the multilink PPP bundle between routers Certkiller 1 and Certkiller 2?

- A. Four ISDN B channels will form the Multilink PPP bundle.
- B. No Multilink PPP bundle will be formed because the dialer interface is not associated with the physical interfaces.
- C. Two ISDN B channels will form the Multilink PPP bundle.
- D. No Multilink PPP bundle will be formed due to there being no load threshold configured.

Answer: D

Explanation:

To configure bandwidth on demand by setting the maximum load before the dialer places another call to a destination, use the dialer load-threshold command in interface configuration mode.

When the cumulative load of all UP links (a number n) exceeds the load threshold the dialer adds an extra link and when the cumulative load of all UP links minus one (n - 1) is at or below load threshold then the dialer can bring down that one link. The dialer will make additional calls or drop links as necessary but will never interrupt an existing call to another destination.

The load argument is the calculated weighted average load value for the interface; 1 is unloaded and 255 is fully loaded. The load is calculated by the system dynamically, based on bandwidth. You can set the bandwidth for an interface in kilobits per second, using the bandwidth command.

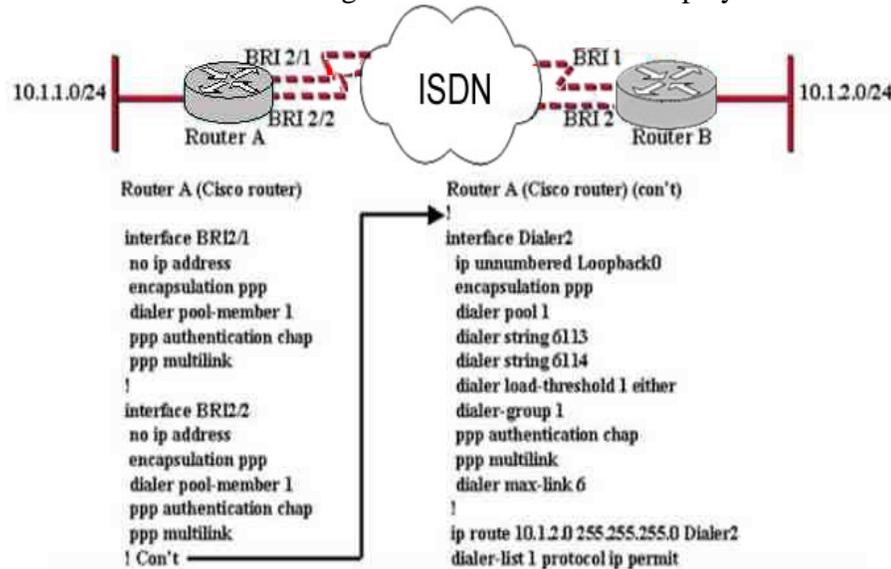
The load calculation determines how much of the total bandwidth you are using. A load value of 255 means that you are using one hundred percent of the bandwidth. The load

number is required.

The PPP multilink bundle is activated only if dialer load-threshold is in the router configuration.

QUESTION 142:

The Certkiller ISDN configuration of Router A is displayed below:



Assuming that there are only two BRI interfaces on Router Certkiller 1; how many B channels will end up forming the multilink PPP bundle between routers A & B when the total load threshold continuously remains greater than 50%?

- A. 1
- B. 2
- C. 3
- D. 4
- E. 5
- F. 6

Answer: D

Explanation:

When the cumulative load of all UP links (a number n) exceeds the load threshold the dialer adds an extra link and when the cumulative load of all UP links minus one (n - 1) is at or below load threshold then the dialer can bring down that one link. The dialer will make additional calls or drop links as necessary but will never interrupt an existing call to another destination.

The load argument is the calculated weighted average load value for the interface; 1 is unloaded and 255 is fully loaded. The load is calculated by the system dynamically, based on bandwidth. You can set the bandwidth for an interface in kilobits per second, using the bandwidth command.

The load calculation determines how much of the total bandwidth you are using. A load

value of 255 means that you are using one hundred percent of the bandwidth. The load number is required.

In this example, since the load is set to only 1 (either incoming or outgoing) the maximum number of BRI links will be bonded in the bundle. Since there are 2 data channels per BRI interface, all 4 of them will be utilized.

QUESTION 143:

You are a network technician at Certkiller and you've just finished entering these commands:

```
Certkiller A(config)#ip route 172.16.1.0 255.255.255.0 bri0
Certkiller A(config)#interface bri0
Certkiller A(config-if)#dialer map ip 10.1.1.1 name Certkiller B
5551111
Certkiller A(config-if)#dialer map ip 10.1.1.2 name Certkiller C
5552222
Certkiller A(config-if)#dialer map ip 10.1.1.3 name Certkiller D
5553333
```

As a result of your configuration; what will happen when traffic destined to host 172.16.1.1 is noticed by router Certkiller A?

- A. The packets destined for the 172.16.1.0 network will be dropped.
- B. The packets destined for the 172.16.1.0 network will be sent to the default route.
- C. A DDR call will be placed first to router Certkiller B, and if it is busy, then to Certkiller C and Certkiller D.
- D. A DDR call will be placed to router Certkiller B and the packets routed to 10.1.1.1.

Answer: C

Explanation:

The command `dialer map protocol next-hop-address [name hostname] [speed 56|64] [broadcast] [dial-string[:isdn-subaddress]]` configures a serial interface or ISDN interface to call one or multiple sites. The name parameter refers to the name of the remote system. The speed parameter is the line speed in kilobits per second to use. The broadcast parameter indicates that broadcasts should be forwarded to this address. The `dial-string[:isdn-subaddress]` is the number to dial to reach the destination and the optional ISDN subaddress. In this case, since there are 3 separate dialer maps, the BRI interface will attempt to dial out to the remote offices until a call can be made and the BRI interface comes up.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 7-32

QUESTION 144:

Two Certkiller routers are connected via an ISDN network as displayed below:



Which dialer map command would you use to configure Certkiller -1 to successfully connect to Certkiller -2?

- A. dialer map ip 10.120.1.2 name Certkiller -2 4085551111
- B. dialer map ip 10.120.1.2 name Certkiller -1 4085551111
- C. dialer map ip 10.120.1.2 name Certkiller -2 4085552222
- D. dialer map ip 10.120.1.1 name Certkiller -1 4085552222
- E. dialer map ip 10.120.1.1 name Certkiller -2 4085552222

Answer: C

Explanation:

The correct configuration syntax for both routers is displayed below:

Certkiller -1:

```
Certkiller -1(config)#interface bri 0
Certkiller -1(config-if)#ip address 10.120.1.1 255.255.255.0
Certkiller -1(config-if)#encapsulation ppp
Certkiller -1(config-if)#dialer map ip 10.120.1.2 name Certkiller -2
4085552222
```

Certkiller -2:

```
Certkiller -2(config)#interface bri 0
Certkiller -2 (config-if)#ip address 10.120.1.2 255.255.255.0
Certkiller -2 (config-if)#encapsulation ppp
Certkiller -2 (config-if)#dialer map ip 10.120.1.1 name Certkiller -1
4085551111
```

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 7-32

QUESTION 145:

Which command would you use if you had a high traffic ISDN line and you wanted to timeout an idle connection for the sake of freeing up the line so it can be used to call a second location?

- A. dialer idle-timeout
- B. dialer fast-idle
- C. dialer wait-for-carrier-time
- D. dialer in-band
- E. None of the above

Answer: B

Explanation:

dialer fast-idle seconds - Specifies the amount of time that a connected line remains idle before it is disconnected to allow a second call destined for a second location over this same line to be placed. This command, used on lines for which there is contention, applies to inbound and outbound calls. The line is considered idle when no interesting packets are being sent across it. If the line becomes idle for the configured length of time, the current call is disconnected immediately and the line is available for new calls. The default

fast-idle time is 20 seconds. This is an inactivity timer for contended interfaces.

Incorrect Answers:

A: dialer idle-timeout seconds - Specifies the idle time (in seconds) before the line is disconnected. The default is 120 seconds. This command, which is used on lines for which there is no contention, applies to inbound and outbound calls. This is an inactivity timer.

C: dialer wait-for carrier-time seconds - Specifies how long (in seconds) to wait for carrier tone. On asynchronous interfaces, this command sets the total time allowed for the chat script to run. The default time is 30 seconds. For asynchronous lines, it is better to increase the value of this parameter to 60 seconds to compensate for the possible delay in the telephone network.

D: dialer in-band - Enables DDR on an asynchronous interface.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 8-7 and 8-8

QUESTION 146:

Router CK1 is configured as a PPP callback server.

What must be configured on CK1 to ensure that improperly configured callback clients are disconnected?

- A. ppp authentication chap
- B. pp authentication pap
- C. dialer callback-secure
- D. ppp callback request
- E. callback forcedwait 15

Answer: C

Explanation:

To enable callback security, use the dialer callback-secure interface configuration command. This command affects those users that are not authorized to be called back with the dialer callback-server command. If the username (hostname in the dialer map command) is not authorized for callback, the call will be disconnected if the dialer callback-secure command is configured. If the dialer callback-secure command is not configured, the call will not be disconnected. In either case, callback has not occurred.

The following partial example configures BRI0 with the commands required to make it function as the callback server on the shared network. Callback security is enabled on BRI0, such that any user other than atlanta will be disconnected and not called back:

```
interface BRI0
ip address 172.16.1.9 255.255.255.0
encapsulation ppp
dialer callback-secure
dialer enable-timeout 2
dialer map ip 172.16.1.8 name atlanta class dial1 81012345678901
dialer-group 1
ppp callback accept
ppp authentication chap
!
map-class dialer dial1
dialer callback-server username
```

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_command_reference_chapter09186a00800c

QUESTION 147:

Which configuration will allow an ISDN link to come up 5 seconds after detecting a primary link failure and then disable the ISDN link 10 seconds after the primary link returns?

- A. RouterA(config)# interface serial 0/0
RouterA(config-if)#backup interface bri0/0
RouterA(config-if)#backup load 5 10
- B. RouterA(config)#interface serial 0/0
RouterA(config-if)#backup interface serial 0/0
RouterA(config-if)#backup load 10 5
- C. RouterA(config)#interface serial0/0
RouterA(config-if)#backup interface bri 0/0
RouterA(config-if)#backup delay 5 10
- D. RouterA(config)#interface serial 0/0
RouterA(config-if)#backup interface bri 0/0
RouterA(config-if)#backup delay 10 5

Answer: C

Explanation:

The command Backup delay 5 10 has two number variables. The first number (5) specifies that if the line protocol on the main interface goes down, The ISDN link is to take over after 5 seconds. The second number (10) states that if serial0 were to reactivate, BRI0 will continue to remain active for 10 seconds until going back into standby mode. Having a backup system wait a few

seconds before kicking in is a smart feature because many times an interface may only fail for a few seconds, and an ISDN call would not want to be initiated every time a 1 second outage happened. The longer reactivation time is also a good feature, because the original line has to prove that it's capable of staying active for 10 seconds before it will be considered to be reliable again.

QUESTION 148:

The configuration file for one of the Certkiller ISDN routers is displayed below:

```
Interface dialer0
ip unnumbered loopback 0
encapsulation ppp
dialer remote-name rta
dialer pool 0
dialer string 5551212
dialer-group 1
ppp multilink
dialer idle-timeout 30
!
Interface dialer1
ip unnumbered loopback 0
encapsulation ppp
dialer remote-name rtb
dialer pool 1
dialer string 5551234
dialer-group 1
ppp multilink
dialer idle-timeout 30
!
Interface bri0/0
encapsulation ppp
dialer pool-member 0 priority 250
dialer pool-member 1 priority 200
ppp authentication chap
ppp multilink
dialer idle-timeout 100
!
Interface bri0/1
encapsulation ppp
dialer pool-member 1 priority 100
ppp authentication chap
ppp multilink
dialer idle-timeout 100
!
Interface serial 0
ip unnumbered loopback 0
backup interface dialer 0
backup delay 5 10
!
Interface serial 1
ip unnumbered loopback 0
backup interface dialer 1
backup delay 5 10
```

Based on the information above, which three of the following statements are true? (Choose three)

- A. Dialer pool 0 will have a higher priority when using interface bri 0/0.
- B. The dialer and serial interfaces share a common IP address.
- C. Interface BRI 0/0 will be selected first when attempting to reach router rtb.
- D. The timeout value is set to 100 seconds for BRI 0/0
- E. The timeout value is set to 30 seconds for BRI 0/1.

Answer: B, C, E

Explanation:

B: Both the serial interfaces and the dialer interfaces are configured with the "ip

unnumbered loopback 0" command, so all interfaces will share the IP address that is configured on interface loopback 0.

C: Each dialer interface uses a dialer pool, a pool of physical interfaces ordered on the basis of the priority assigned to each physical interface. A physical interface can belong to multiple dialer pools, contention being resolved by priority. The dialer-pool member priority is higher for interface BRI0/0, so it will be selected first for all calls.

E: The time specified in the logical dialer interface overrides the value specified in the physical BRI interface, so even though the idle timeout is configured for 100 seconds on the BRI interfaces, the value of 30 seconds specified on the dialer interfaces will be used.

QUESTION 149:

Which command binds a logical dialer interface to a dialer pool?

- A. dialer pool-member number
- B. dialer-group number
- C. dialer-list number
- D. dialer poolnumber

Answer: D

Explanation:

To specify, for a logical dialer interface, which dialing pool to use to connect to a specific destination subnetwork, use the dialer pool interface configuration command. The following example shows a dialer interface configuration that is linked to the physical interface configuration shown for BRI 1 in the dialer pool-member command section. Dialer interface 1 uses dialer pool 3, of which BRI 1 is a member.

!Thisisadialerprofileforreachingremotesubnetwork1.1.1.1.

```
interfaceDialer1
ipaddress1.1.1.1255.255.255.0
encapsulationppp
dialerremote-nameSmalluser
dialerstring4540
dialerpool3
dialer-group1
```

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_command_reference_chapter09186a00800c

QUESTION 150:

You need to configure router CK1 for ISDN DDR routing. What command do you use to define interesting packets? (Type in answer below)

Answer: dialer-list

Explanation:

Dial-on-Demand Routing (DDR) addresses the need for intermittent network connections over circuit-switched WANs. With DDR, all traffic is classified as either interesting or uninteresting. If traffic is interesting, the packet is passed to the interface, and the router then connects to the remote router (if not currently connected). The router defines interesting packets with the dialer-list command. DDR is implemented in two ways: DDR with dialer profiles and legacy DDR.

QUESTION 151:

You are a Cisco Certified Engineer configuring a DDR remote access solution. Which of the following components of a dialer profile is entirely optional (Choose all that apply)?

- A. Dialer map-class
- B. Dialer interfaces
- C. Dialer pool
- D. Physical interfaces

Answer: A

Explanation:

The components of a dialer profile include: Dialer interfaces - logical entities that use a per-destination dialer profile. Any number of dialer interfaces can be created in a router. All configuration settings specific to the destination go in the dialer interface configuration. Each dialer interface uses a dialer pool, which is a pool of physical interfaces (ISDN BRI and PRI, asynchronous-modem, and synchronous serial). Dialer pool - Each interface references a dialer pool, which is a group of physical interfaces associated with a dialer profile. A physical interface can belong to multiple dialer pools. Contention for a specific physical interface is resolved by configuring the optional priority command. Physical interfaces - Interfaces in a dialer pool are configured for encapsulation parameters. The interfaces are also configured to identify the dialer pools to which the interface belongs. Dialer profiles support PPP and High-Level Data Link Control (HDLC) encapsulation.

Dialer map-class (optional) - Supply configuration parameters to dialer interfaces (for example, ISDN speed, dialer timers parameters, and so on). A map-class can be referenced from multiple dialer interfaces.

QUESTION 152:

To add physical ISDN links to a multilink bundle dynamically on an as needed basis, what command should be used?

- A. ppp multilink
- B. Enable chap
- C. Multilink ppp

- D. Enable multilink
- E. dialer load-threshold

Answer: E

Explanation:

To configure bandwidth on demand by setting the maximum load before the dialer places another call to a destination, use the dialer load-threshold command in interface configuration mode.

When the cumulative load of all UP links (a number n) exceeds the load threshold the dialer adds an extra link and when the cumulative load of all UP links minus one (n - 1) is at or below load threshold then the dialer can bring down that one link. The dialer will make additional calls or drop links as necessary but will never interrupt an existing call to another destination.

The load argument is the calculated weighted average load value for the interface; 1 is unloaded and 255 is fully loaded. The load is calculated by the system dynamically, based on bandwidth. You can set the bandwidth for an interface in kilobits per second, using the bandwidth command.

The load calculation determines how much of the total bandwidth you are using. A load value of 255 means that you are using one hundred percent of the bandwidth. The load number is required.

QUESTION 153:

What option can be used as a means for configuring DDR? (Choose all that apply)

- A. Set the route calling cost
- B. Set the route priority
- C. Use a floating static route
- D. Set up the static route to make it less desirable than the dynamic route

Answer: C, D

Explanation:

The router uses one of three methods to monitor the primary connection and initiate the backup connection when needed, as listed below:

Backup Interface - This is an interface that stays in standby until the primary interface line protocol is detected as down and then is brought up.

Floating Static Route - This backup route has an administrative distance greater than the administrative distance of the primary connection route and therefore would not be in the routing table until the primary interface goes down.

Dialer Watches - Dialer watch is a backup feature that integrates dial backup with routing capabilities.

QUESTION 154:

You work as a network technician for Certkiller .com. An ISDN BRI interface has been configured as a backup interface and is currently in standby mode. You then attempt to use the BRI interface to connect to a different site but are unsuccessful. What solution would enable the BRI interface to support the backup requirements and still be available for other DDR operations?

- A. Configure PPP multilink.
- B. Configure legacy DDR.
- C. Split the B channels, one for backup and the other for DDR operations.
- D. Configure the D channel.
- E. Configure dialer profiles.
- F. Configure standby-suppress mode.

Answer: E

Explanation:

Dialer profiles separate logical configurations from the physical interfaces that receive or make calls. Because of this separation, multiple dialer profile configurations can share interfaces such as ISDN, asynchronous modems, or synchronous serial connections. Dialer profiles allow you to bind logical and physical configurations together dynamically on a per call basis. This allows physical interfaces to take on different characteristics based on incoming or outgoing call requirements. Dialer profiles can define encapsulation, access control lists, minimum or maximum calls, and toggle features on or off. Dialer profiles are particularly useful where multiple ISDN B channels are to be used to connect to multiple remote destinations simultaneously. In such a case, one dialer profile can be bound to one set of B channels while another dialer profile can be bound to another set of B channels. This allows the same physical interface to connect to multiple remote destinations simultaneously.

Reference:

http://www.cisco.com/en/US/tech/CK801/CK133/technologies_configuration_example09186a0080093c2e.shtml

QUESTION 155:

The "dialer fast-idle" configuration command was issued on router CK1 . What does the dialer fast-idle command specify in a DDR environment?

- A. The termination of the call if no interesting traffic has been transmitted for the specified time.
- B. Disconnect time if there is another call waiting for the same interface and the interface is idle.
- C. The length of idle time to wait for a carrier when dialing out before abandoning the call
- D. The length of idle time to wait for keepalives before assuming inactive and disconnecting the call

Answer: B

Explanation:

The dialer fast-idle configuration command is described below:

Command Description

Command	Description
dialer fast-idle (interface configuration)	Specifies the amount of time that a line for
	which there is contention will stay idle before it
	is disconnected and the competing call is
	placed.

QUESTION 156:

Part of the configuration file for router Certkiller 1 is displayed below:

```
hostname Certkiller1
!
username Certkiller2 password 0certkiller
!
interface BRI0/0
 ip address 1.1.1.1 255.255.255.0
 encapsulation ppp
 isdn switch-type basic-ni
 isdn spid1 555121200001
 isdn spid2 555121200002
```

You work as a network engineer at Certkiller . You must configure Certkiller 1 so that it accepts ISDN calls from Certkiller 2 but does not dial Certkiller 2. Give the partial configuration, what must you do to complete the configuration and meet these requirements?

- A. Certkiller 1(config)# dialer-list 1 protocol ip permit
Certkiller 1(config)# interface bri0/0
Certkiller 1(config-if)# dialer map ip 1.1.1.2 name Certkiller 2 broadcast 5551212
Certkiller 1(config-if)# dialer-group 1
Certkiller 1(config-if)# ppp authentication chap callin
- B. Certkiller 1(config)# dialer-list 1 protocol ip permit
Certkiller 1(config)# interface bri0/0
Certkiller 1(config-if)# dialer map ip 1.1.1.2 name Certkiller 2 broadcast
Certkiller 1(config-if)# dialer-group 1

```
Certkiller 1(config-if)# ppp authentication chap
C. Certkiller 1(config)# dialer-list 1 protocol ip deny
Certkiller 1(config)# interface bri0/0
Certkiller 1(config-if)# dialer map ip 1.1.1.2
Certkiller 1(config-if)# dialer-group 1
Certkiller 1(config-if)# ppp authentication chap callin
D. Certkiller 1(config)# interface bri0/0
Certkiller 1(config-if)# dialer map ip 1.1.1.2 name Certkiller 2 broadcast 5551212
Certkiller 1(config-if)# ppp authentication chap
```

Answer: D

Explanation:

Since there is no dialer-list associated with this choice, no interesting traffic will be seen by the router, so a call can not be initiated by Certkiller 1. However, it has been correctly configured to accept calls from Certkiller 2. It is important to remember that traffic defined as "interesting" is only used for initiating the ISDN call, and not for defining the traffic that can traverse an ISDN call. Once the ISDN connection is made, all traffic will be allowed through the ISDN line until no interesting traffic is seen and the idle timer expires.

QUESTION 157:

While troubleshooting an ISDN connectivity issue, the following was shown via debugging:

```
BR0:1 CHAP: I CHALLENGE id 17 len 33 from "Certkiller13"
BR0:1 CHAP: Username maui-soho-01 not found
BR0:1 CHAP: Unable to authenticate for peer
BR0:1 ppp: phase is TERMINATING
```

Give the output in the exhibit, which two statements are true? (Select two)

- A. The local router username is Certkiller 13
- B. The username supplied by the remote router is not configured locally.
- C. The username supplied by the local router is not configured on the remote router.
- D. The command username CertK Bill13 password password must be configured on the local router.
- E. The command username Certkiller 13 password password must be configured on the remote router.
- F. The remote router is not configured for CHAP authentication.

Answer: B, D

Explanation:

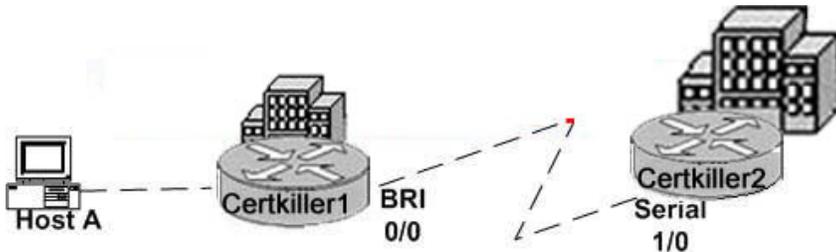
In this example, the remote router is issuing the CHAP challenge to the remote router, which is "Certkiller 13." This username is not configured locally so it is not found. To

remedy this, you should issue the "username Certkiller 13 password" command on the local router.

QUESTION 158:

SIMULATION

The following information will be used to configure router Certkiller 1 in this simulation:



Certkiller .com is configuring ISDN links to provide connectivity to their central site from branch locations. As the network administrator at the Certkiller 1 location it is your job to configure connectivity to the central site at the Certkiller 2 location. Using a Cisco 1700 series with a BRI interface, you will configure connectivity to a Cisco 2600 series router with a PRI interface already configured at the central site. Your task is to configure the BRI interface for ISDN and use PPP encapsulation with CHAP authentication. Any IP traffic destined for the central site should initiate an ISDN connection. An idle timeout of 60 seconds should be configured for the line to drop in the absence of interesting traffic. A dialer map is to be used to facilitate the connectivity. As you are the branch location, only a static default route is to be configured for routing to the central site. The telco requires you to use the National ISDN switch type for your interface. Use the topology in the exhibit for reference. Further necessary information is as follows:

Privileged Mode password is Certkiller

Password to be used for CHAP authentication: Certkiller

Central site hostname: Certkiller 2

Local IP address 192.168.233.2/30

Central IP address 192.168.233.1/30

The telecommunications company has provided the following information for each BRI B channel:

SPID1 51044422163712; LDN 5552216

SPID2 51044422163712; LDN 5552217

Central Site LDN: 515553216

Start the simulation by click the host icon.

Answer:

Router >

Router >enable

Router #config t

Router(config)# hostname Certkiller 1

Certkiller 1(config)#isdn switch-type basic-ni

Certkiller 1(config)#username Certkiller 2 password Certkiller

```
Certkiller 1(config)#interface bri0
Certkiller 1(config_int)#ip address 192.168.233.2 255.255.255.252
Certkiller 1(config_int)#no shut
Certkiller 1(config_int)#encapsulation ppp
Certkiller 1(config_int)#ppp authentication chap
Certkiller 1(config_int)#dialer idle-timeout 60
Certkiller 1(config_int)#isdn spid1 51044422163712 5552216
Certkiller 1(config_int)#isdn spid2 51044422163712 5552217
Certkiller 1(config_int)#dialer map ip 192.168.233.1 name Certkiller 2 5155553216
Certkiller 1(config_int)#dialer-group 1
Certkiller 1(config_int)#exit
Certkiller 1(config)#dialer-list 1 protocol ip permit
Certkiller 1(config)#ip route 0.0.0.0 0.0.0.0 192.168.233.1
Certkiller 1(config)#exit
```

QUESTION 159:

You are configuring the ISDN interfaces that connect to router CK1 . Which two commands assign multiple ISDN BRI interfaces to a single hunt group? (Choose two)

- A. dialer-group
- B. multilink ppp
- C. interface dialer
- D. dialer hunt-group
- E. dialer rotary-group

Answer: C, E

Explanation:

Dialer Rotary Group Example

The following example configures BRI interfaces to connect into a rotary group (dialer-group) and then configures a dialer interface for that dialer-group. In this example, 5 different ISDN BRI circuits form one trunk group, as specified by the logical dialer interface.

```
Hostname CK1
interface bri 0
description connected into a rotary group
encapsulation ppp
dialer rotary-group 1
!
interface bri 1
no ip address
encapsulation ppp
dialer rotary-group 1
!
```

```
interface bri 2
encapsulation ppp
dialer rotary-group 1
!
interface bri 3
no ip address
encapsulation ppp
dialer rotary-group 1
!
interface bri 4
encapsulation ppp
dialer rotary-group 1
!
```

```
interface Dialer 1
description Dialer group controlling the BRIs
ip address 88.88.1.1 255.255.255.0
encapsulation ppp
```

Based on this configuration example, the "dialer rotary-group" is used to specify the BRI interfaces to be placed in the hunt group, and the "interface dialer" is used to configure the parameters of the hunt group.

QUESTION 160:

You are setting up ISWDM backup on one of the Certkiller routers. Which dial feature provides reliable connectivity, does not rely on defined interesting traffic to trigger outgoing calls to the remote router, and is triggered by a lost route?

- A. dialer backup
- B. floating static routes
- C. dialer watch
- D. dialer route
- E. All of the above

Answer: C

Explanation:

Dialer Watch is a backup feature that integrates dial backup with routing capabilities. Dialer Watch provides reliable connectivity without relying solely on defining interesting traffic to trigger outgoing calls at the central router. Hence, dialer watch also can be considered regular DDR with no requirement for interesting traffic, just lost routes. By configuring a set of watched routes that define the primary interface, you are able to monitor and track the status of the primary interface as watched routes are added and deleted.

QUESTION 161:

One of the Certkiller routers was configured as shown below:

```
Router CK1 (config-controller)# pri-group timeslots 1-8, 24
```

Based on the configuration above, what does the number 24 represent in the T1 PRI configuration?

- A. The number of B channel time slots available.
- B. The number of B channel time slots used.
- C. The starting point of the B channel time slots.
- D. The D channel time slot.

Answer: D

Explanation:

To configure the isdn switch-type and pri-group:

```
bru-nas-03#configure terminal
```

```
bru-nas-03(config)#isdn switch-type primary-net5
```

```
bru-nas-03(config)#controller e1 0
```

```
bru-nas-03(config-controller)#pri-group timeslots 1-31
```

Note: In some countries, service providers offer Fractional PRI lines. This means that fewer than 30 B-channels may be used for ISDN connections. For fractional PRI lines, the timeslots range must include the operational B-channels, plus the D-channel (this is fixed on timeslot 16). For example:

1. Pri-group timeslots 1-10, 16 for the first ten B-channels.

Reference: http://www.cisco.com/warp/public/116/E1_error.html

QUESTION 162:

The partial configuration of router CK1 is displayed below:

```
<partial running configuration>
!
hostname CK1
!
username CK2 password 0 cisco
!
isdn switch-type basic-ni
!
interface Ethernet0
ip address 172.16.1.1 255.255.255.0
!
interface Serial0
ip address 192.168.10.2 255.255.255.252
encapsulation ppp
ppp authentication chap
!
interface BRI0
ip address 172.20.10.2 255.255.255.0
encapsulation ppp
dialer idle-timeout 30
dialer map ip 172.20.10.1 name CK2 broadcast 5551111
dialer watch-group 8
dialer-group 1
isdn switch-type basic-ni
isdn spid1 51255522220101 5552222
isdn spid2 51255522230101 5552223
ppp authentication chap
!
router ospf 5
log-adjacency-changes
network 172.16.1.0 0.0.0.255 area 0
network 172.17.1.0 0.0.0.255 area 0
network 172.20.10.0 0.0.0.255 area 0
network 192.168.10.0 0.0.0.3 area 0
!
dialer watch-list 8 ip 172.22.53.0 255.255.255.0
!
access-list 101 deny ospf any any
access-list 101 permit ip any any
!
dialer-list 1 protocol ip list 101
```

Based on the information shown above, what is required to make this a valid "dialer watch" configuration?

- A. The CK1 backup interface must be configured with the dialer watch-disable 30 command.
- B. The CK1 dialer watch must be configured for group 1, not group 8.
- C. The CK1 OSPF configuration must have a network statement for 172.22.53.0.
- D. The BRI of CK1 must be configured with an additional dialer map statement referencing the "watched" network.

Answer: D

Explanation:

Below is a properly configured router using dialer watch, along with inserted comments. The additional map statement that is required is in bold.

```
interface BRI0
ip address 172.20.10.2 255.255.255.0
!IP address for the BRI interface (backup link).
encapsulation ppp
```

```
dialer idle-timeout 30
!Idle timeout(in seconds)for this backup link.
!Dialer watch checks the status of the primary link every time the
!idle-timeout expires.
dialer watch-disable 15
!Delays disconnecting the backup interface for 15 seconds after the
!primary interface is found to be up.
dialer map ip 172.20.10.1 name maui-nas-05 broadcast 5551111
!Dialer map for the BRI interface of the remote router.
dialer map ip 172.22.53.0 name CK1 broadcast 5551111
!Map statement for the route/network being watched by the
!dialer watch-list command.
!This address must exactly match the network configured with the
!dialer watch-list command.
!When the watched route disappears, this dials the specified phone
number.
dialer watch-group 8
!Enable Dialer Watch on this backup interface.
!Watch the route specified with dialer watch-list 8.
dialer-group 1
!Apply interesting traffic defined in dialer-list 1.
isdn switch-type basic-ni
isdn spid1 51255522220101 5552222
isdn spid2 51255522230101 5552223
ppp authentication chap
!Use chap authentication.
!
router ospf 5
log-adjacency-changes
network 172.16.1.0 0.0.0.255 area 0
network 172.17.1.0 0.0.0.255 area 0
network 172.20.10.0 0.0.0.255 area 0
network 192.168.10.0 0.0.0.3 area 0
!
ip classless
no ip http server
!
dialer watch-list 8 ip 172.22.53.0 255.255.255.0
!This defines the route(s) to be watched.
!This exact route(including subnet mask) must exist in the routing
table.
!Use the dialer watch-group 8 command to apply this list to the backup
interface.
access-list 101 remark Define Interesting Traffic
access-list 101 deny ospf any any
!Mark OSPF as uninteresting.
```

!This will prevent OSPF hellos from keeping the link up.

```
Access-list 101 permit ip any any
```

```
dialer-list 1 protocol ip list 101
```

!Interesting traffic is defined by access-list 101.

!This is applied to BRI0 using dialer-group 1.

```
!
```

```
end
```

Incorrect Answers:

A. This task is optional. Under some conditions, you may want to implement a delay before the backup interface is dropped once the primary interface recovers. This delay can ensure stability, especially for flapping interfaces or interfaces experiencing frequent route changes.

B. The number needs to only match what is being used on the dialer watch list statement, which is 8.

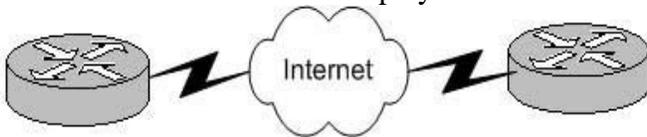
C. Only the networks that are normally placed in the OSPF process need to be added, which are the networks locally attached on the router.

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800d

QUESTION 163:

The Certkiller ISDN network is displayed below:



```
hostname ck1
|
username ck2 password 0 certkiller
|
interface BRI0/0
ip address 20.1.1.1 255.255.255.0
no ip directed-broadcast
encapsulation ppp
dialer map ip 20.1.1.2 name ck2 broadcast 5772222
dialer-group 1
isdn switch-type basic-5ess
ppp authentication chap callin
ppp chap hostname alias-ck1
|
access-list 101 permit ip any any
dialer-list 1 protocol ip list 101
|

hostname ck2
|
username alias-ck1 password 0 certkiller
|
interface BRI0/0
ip address 20.1.1.2 255.255.255.0
no ip directed-broadcast
encapsulation ppp
dialer map ip 20.1.1.1 name alias- broadcast 5771111
dialer-group 1
isdn switch-type basic-5ess
ppp authentication chap
|
access-list 101 permit ip any any
dialer-list 1 protocol ip list 101
|
```

Which two things will occur when CK1 initiates a call to CK2 and attempts to make a connection? (Choose two)

- A. Both routers will send a challenge.
- B. Only CK2 will send a challenge.
- C. Only CK1 will send a challenge.
- D. The CK2 router will generate a hash value and send it to CK1 .
- E. The PPP connection establishment will succeed.
- F. The PPP connection establishment will fail.

Answer: B, E

Explanation:

If Router 1 initiates a call to Router 2, Router 2 would challenge Router 1, but Router 1 would not challenge Router 2. This occurs because the ppp authentication chap callin command is configured on Router 1. This is an example of a unidirectional authentication.

In this setup, the ppp chap hostname alias-r1 command is configured on Router 1. Router 1 uses "alias-r1" as its hostname for CHAP authentication instead of "r1." The Router 2 dialer map name should match Router 1's ppp chap hostname; otherwise, two B channels are established, one for each direction.



Configurations

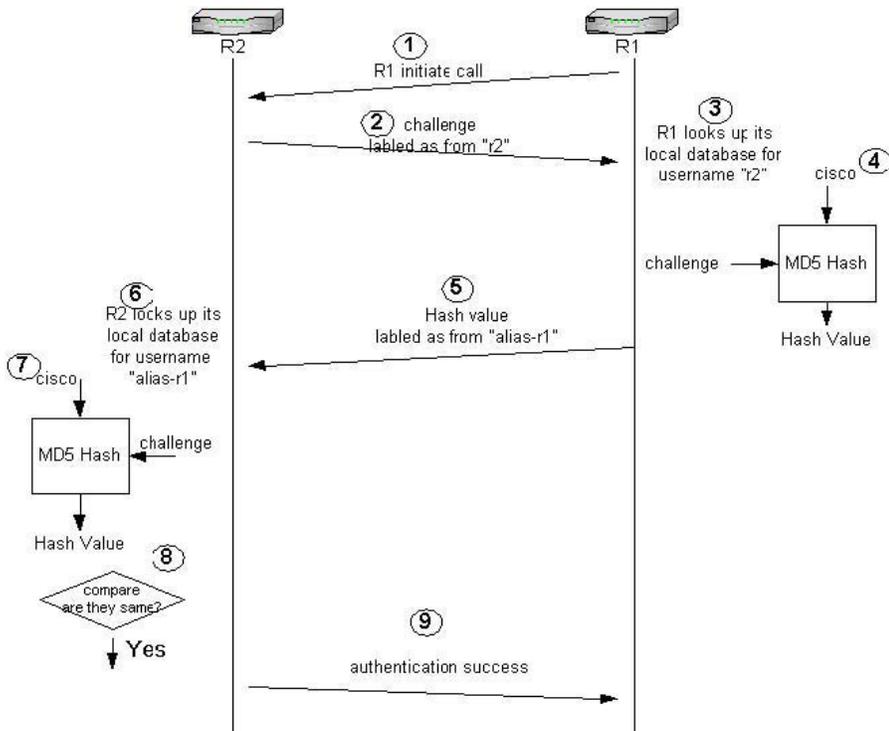
Router 1

```
!  
isdn switch-type basic-5ess  
!  
hostname r1  
!  
username r2 password 0 cisco  
!-- Hostname of other router and shared secret  
!  
interface BRI0/0  
ip address 20.1.1.1 255.255.255.0  
no ip directed-broadcast  
encapsulation ppp  
dialer map ip 20.1.1.2 name r2 broadcast 5772222  
dialer-group 1  
isdn switch-type basic-5ess  
ppp authentication chap callin  
!-- Authentication on incoming calls only  
ppp chap hostname alias-r1  
!-- Alternate CHAP hostname  
!  
access-list 101 permit ip any any
```

```
dialer-list 1 protocol ip list 101
!  
Router 2  
!  
isdn switch-type basic-5ess  
!  
hostname r2  
!  
username alias-r1 password 0 cisco  
! -- Alternate CHAP hostname and shared secret.  
! -- The username must match the one in the ppp chap hostname  
! -- command on the remote router.  
!  
interface BRI0/0  
ip address 20.1.1.2 255.255.255.0  
no ip directed-broadcast  
encapsulation ppp  
dialer map ip 20.1.1.1 name  
alias-r1 broadcast 5771111  
! -- Dialer map name matches alternate hostname "alias-r1".  
dialer-group 1  
isdn switch-type basic-5ess  
ppp authentication chap  
!  
access-list 101 permit ip any any  
dialer-list 1 protocol ip list 101  
!
```

Configuration Explanation

Please refer to the numbers below this graphic for explanations:



1. In this example, Router 1 initiates the call. Since Router 1 is configured with the ppp authentication chap callin command, it does not challenge the calling party, which is Router 2.

2. When Router 2 receives the call, it challenges Router 1 for authentication. By default for this authentication, the hostname of the router is used to identify itself. If the ppp chap hostname name command is configured, a router uses the name in place of the hostname to identify itself. In this example, the challenge is labeled as it is coming from "r2."

3. Router 1 receives Router 2's challenge and looks in its local database for username "r2."

4. Router 1 finds the "r2" password, which is "cisco." Router 1 uses this password and the challenge from Router 2 as input parameters of the MD5 hash function. The hash value is generated.

5. Router 1 sends the hash output value to Router 2. Here, since the ppp chap hostname command is configured as "alias-r1," the reply is labeled as coming from "alias-r1."

6. Router 2 receives the reply and looks for the "alias-r1" username in its local database for the password.

7. Router 2 finds that the password for "alias-r1" is "cisco." Router 2 uses the password and the challenge sent out earlier to Router 1 as input parameters for the MD5 hash function. The hash function generates a hash value.

8. Router 2 compares the hash value it generated and the one it receives from Router 1.

9. Since the input parameters (challenge and password) are identical, the hash value is same resulting in a successful authentication.

Reference:

[http://www.cisco.com/en/US/tech/ CK7 13/ CK5 07/technologies_configuration_example09186a0080094333.shtml#c](http://www.cisco.com/en/US/tech/CK7_13/CK5_07/technologies_configuration_example09186a0080094333.shtml#c)

QUESTION 164:

What is a feature of Multilink PPP on ISDN BRI links?

- A. The D channel can be activated when outbound traffic exceeds the dialer load threshold.
- B. The second active channel can only be used for outbound traffic.
- C. The second channel remains active for the remainder of the call, regardless of bandwidth demands.
- D. Both outbound and inbound traffic loads can be used to determine when to activate the second channel

Answer: D

Explanation:

Using the "dialer load-threshold" command, the second B channel can be configured to come up based on the inbound or outbound loads, or both.

To configure bandwidth on demand by setting the maximum load before the dialer places another call to a destination, use the dialer load-threshold command in interface configuration mode. To disable the setting, use the no form of this command.

dialer load-threshold load [outbound | inbound | either]

no dialer load-threshold

Syntax Description

load	Interface load used to determine whether to initiate another call or to drop a link to the destination. This argument represents a utilization percentage; it is a number between 1 and 255, where 255 is 100 percent.
outbound	(Optional) Calculates the actual load using outbound data only.
inbound	(Optional) Calculates the actual load using inbound data only.
either	(Optional) Sets the maximum calculated load as the larger of the outbound and inbound loads.

When the cumulative load of all UP links (a number n) exceeds the load threshold the dialer adds an extra link and when the cumulative load of all UP links minus one (n - 1) is at or below load threshold then the dialer can bring down that one link. The dialer will make additional calls or drop links as necessary but will never interrupt an existing call to another destination.

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a008008

QUESTION 165:

You need to adjust the WFQ settings on router CK1 . Which of the following commands could you use to correctly configure Weighted Fair Queuing (WFQ)?

- A. router(config)# bandwidth 56
- B. router(config)# fair-queue 64
- C. router(config-if)# fair-queue 128
- D. router(config-if)# priority-fair 16
- E. router(config)# priority fair 8

Answer: C

Explanation:

To enable weighted fair queuing (WFQ) for an interface, use the fair-queue interface configuration command. This command is done on an interface level.

```
fair-queue [congestive-discard-threshold [dynamic-queues [reservable-queues]]]  
no fair-queue
```

Syntax Description

congestive-discard-threshold	(Optional) Number of messages allowed in each queue. The default is 64 messages, and a new threshold must be a power of 2 in the range from 16to 4096. When a conversation reaches this threshold, new message packets are discarded.
------------------------------	---

dynamic-queues	(Optional) Number of dynamic queues used for best-effort conversations (that is, a normal conversation not requiring any special network services). Values are 16, 32, 64, 128, 256, 512, 1024, 2048, and 4096. See Table 4 and Table 5 in the fair-queue (class-default) command for the default number of dynamic queues.
reservable-queues	(Optional) Number of reservable queues used for reserved conversations in the range 0 to 1000. The default is 0. Reservable queues are used for interfaces configured for features such as Resource Reservation Protocol (RSVP).

Defaults

Fair queuing is enabled by default for physical interfaces whose bandwidth is less than or equal to 2.048Mbps and that do not use the following:

1. X.25 and Synchronous Data Link Control (SDLC) encapsulations
2. Link Access Procedure, Balanced (LAPB)
3. Tunnels
4. Loopbacks
5. Dialer
6. Bridges
7. Virtual interfaces

Fair queuing is not an option for the protocols listed above. However, if custom queuing or priority queuing is enabled for a qualifying link, it overrides fair queuing, effectively disabling it. Additionally, fair queuing is automatically disabled if you enable the autonomous or silicon switching engine mechanisms.

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_r/qrfcmd1.htm#1098249

QUESTION 166:

The following configuration command was applied to a Certkiller router:

```
policy-map Policy1
class Class1
priority 10
class Class2
bandwidth 20
queue-limit 45
```

```
class Class3  
bandwidth 30  
random-detect
```

From the information above, what is true about this configuration?

- A. WRED is used in Class1 and Class2.
Traffic not matching any classes will be dropped.
- B. WRED is used in Class3.
Traffic not matching any classes will be handled by the class-default class.
- C. WRED is used in Class1 and Class3.
Traffic not matching any classes will be best effort by default class.
- D. WRED is used in Class3.
Traffic not matching any classes will be dropped.

Answer: B

Explanation:

To enable WRED with its default configuration parameters use the random-detect command as shown in the last line of the command interface below the Class3 configuration parameters.

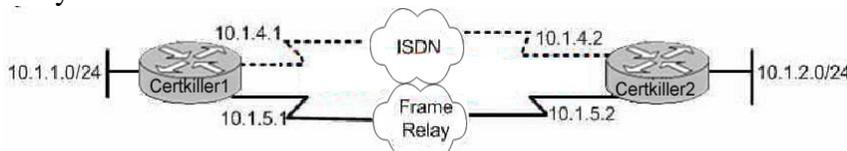
In a policy-map, if traffic doesn't match a class it gets handled by what's defined in the default class.

Reference:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgr/qos_c/qcprt3/qcdwred.htm

QUESTION 167:

Study the exhibit below:



1. In the graphic, all interfaces are up and correctly configured.
2. The bandwidth of the Frame Relay interface is 256k
3. The bandwidth of the ISDN interface is 128k
4. On Certkiller 1, the local best EIGRP metric (feasible distance) is 150 for the Frame Relay link and 300 for the ISDN link.
5. However the reported distance for both routes is 100.
6. The router Certkiller 1 has been configured like this:
router eigrp 1
network 10.0.0.0
variance 3
traffic-share balanced
!
ip route 10.1.2.0 255.255.255.0 10.1.4.2 99

If a host on network 10.1.1.0 sends data to a host on network 10.1.2.0, which route

will Router Certkiller 1 choose?

- A. Traffic will be routed over the Frame Relay link.
 - B. Traffic will be routed over the ISDN link.
 - C. Traffic will be load balanced between the Frame Relay and ISDN links.
 - D. Traffic will be load balanced between the Frame Relay and ISDN links.
- The Frame Relay link, however, will transport twice the traffic as the ISDN link.

Answer: D

The routing protocol of this scenario is EIGRP. EIGRP has a administrative distance of 90 and the floating static route has a configured administrative distance of 99. Therefore the static route is not taken (the lowest administrative distance is the best), we see only EIGRP route in the routing table. EIGRP use frame-relay and ISDN connection because the variance 3 and the traffic-share balanced permit the balancing of the load on the both connection. The answer is D.

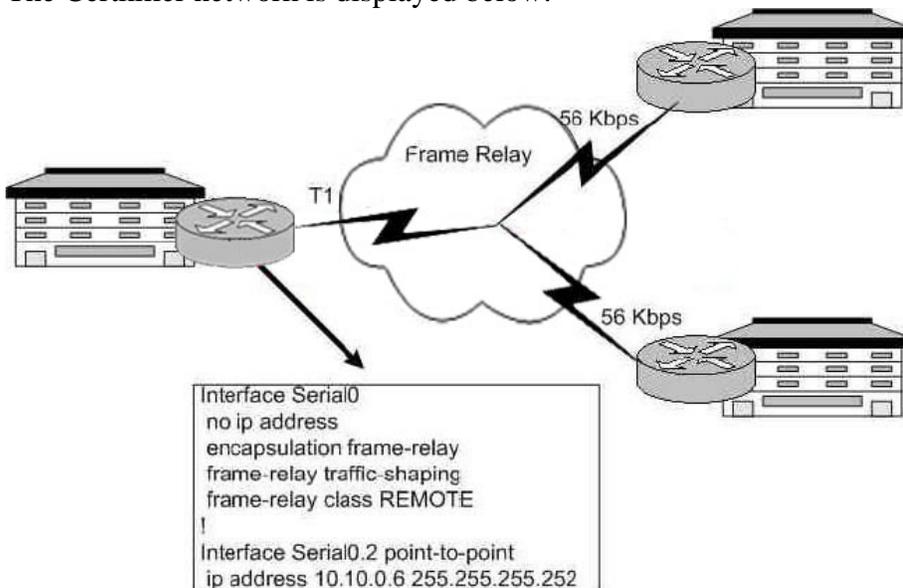
Note: More information on EIGRP load balancing can be found here:

http://www.cisco.com/en/US/tech/CK365/technologies_tech_note09186a008009437d.shtml

Every routing protocol supports equal cost path load balancing. In addition to that, IGRP and EIGRP also support unequal cost path load balancing. Use the variance command to instruct the router to include routes with a metric less than n times the minimum metric route for that destination, where n is the number specified by the variance command.. The variable n can take a value between 1 and 128, with the default being 1, which means equal cost load balancing. Traffic is also distributed among the links with unequal costs, proportionately, with respect to the metric.

QUESTION 168:

The Certkiller network is displayed below:



What will be the result if the command "frame-relay traffic rate 56000 128000" was applied on the indicated router?

- A. It enables the average and peak rate for traffic received on the interface.
- B. It will have no effect until the REMOTE class is assigned to a sub-interface.
- C. It enables the average and peak rate for traffic sent out a virtual circuit.
- D. It configured the interface default bandwidth and peak rate for traffic sent.
- E. None of the above

Answer: C

Explanation:

In the command `frame-relay traffic rate 56000 128000` there are two number variables. The first number variable (56 000) is for the average traffic rate (in bits per second) and the second number is the peak rate (128 000) of the virtual circuit.

Once the `map-class` commands been entered, the prompt changes. At this point, it is time to define the traffic parameters. The average and peak transmission rates can be configured at this point along with defining whether the router should respond to BECN requests. It is also possible to define queues to prioritize PVCs. The command structure for defining peak and average rates is as follows (the peak rate is optional):

```
RouterA (config-map-class)#frame-relay traffic-rate average  
[peak]
```

Reference: CCNP Remote Access Exam Certification Guide, page 272, Brian Morgan & Craig Dennis, Cisco Press 2001, ISBN 1-58720-003-1

QUESTION 169:

The HQ Certkiller router is using subinterfaces on the frame relay interface. What's true about configuring Frame Relay subinterfaces? (Choose all that apply.)

- A. The configuration must be added to the D channel.
- B. The physical interface and subinterface can each be configured with IP addresses.
- C. Subinterface is configured either multipoint or point-to-point.
- D. Any IP address must be removed from the subinterface.
- E. None of the above.

Answer: C, D

Explanation: The answer should be C and D, not B and C. This is because the Layer 3 address should be removed from the major interface, this allows the subints to have there own address applied.

Note:

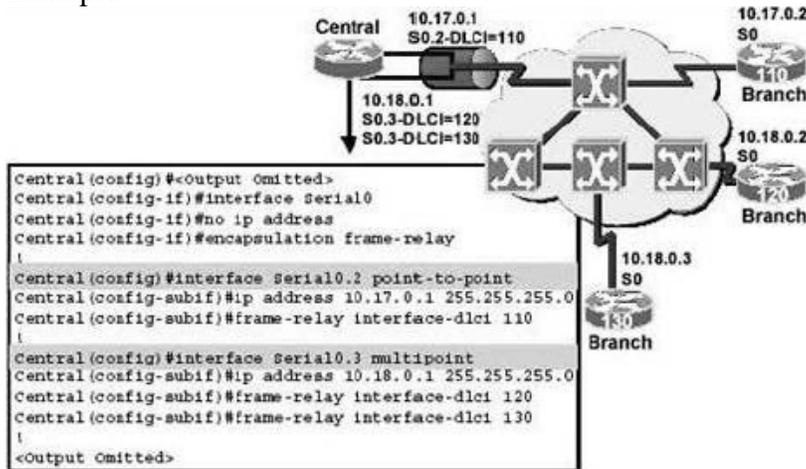
To enable the forwarding of broadcast routing updates in a Frame Relay network, you can configure the router with logically assigned interfaces called subinterfaces. Subinterfaces are logical subdivisions of a physical interface. In split horizon routing environments, routing updates received on one subinterface can be sent out another subinterface. In subinterface configuration, each virtual circuit can be configured as a point-to-point connection, which allows the subinterface to act similar to a leased line.

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 or subinterface on a remote router. In this case, the interfaces would be in the same subnet and each interface would have a single DLCI. Each point-to-point connection is its own subnet. In this environment, broadcasts are not a problem because the routers are point-to-point and act like a leased line.

Multipoint - A single subinterface is used to establish multiple PVC connections to multiple physical or subinterfaces on remote routers. In this case, all the participating interfaces would be in the same subnet and each interface would have its own local DLCI. In this environment, because the subinterface is acting like a regular NBMA Frame Relay network, broadcast traffic is subject to the split horizon rule.

Example:



As this example shows, you should remove any network-layer address assigned to the physical interface. If the physical interface has an address, frames will not be received by the local subinterfaces.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 11-19

QUESTION 170:

Which of the following Frame Relay encapsulation command would you use if you were going to connect an interface on a Cisco router to an interface on a Juniper router?

- A. Router(config-if)#encapsulation frame-relay ansi
- B. Router(config-if)#encapsulation frame-relay cisco
- C. Router(config-if)#encapsulation frame-relay ietf
- D. Router(config-if)#encapsulation frame-relay q933i

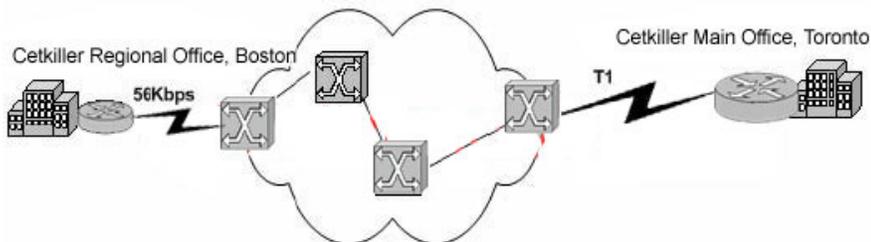
Answer: C

Explanation: The correct configuration syntax is:Router(config-if)# encapsulation frame-relay [cisco | ietf]This command select the encapsulation type to encapsulate

the frame relay data traffic end-to-end. The Cisco proprietary encapsulation is the default type. Use IETF encapsulation if connecting to a non-Cisco router.

QUESTION 171:

The Certkiller WAN is displayed below:



Certkiller's regional offices are connected together by way of a Frame Relay connection. Which command would you use to allow the Toronto router to dynamically adjust the rate at which it sends packets to the Boston router, during periods of network congestion?

- A. frame-relay traffic-rate adaptive
- B. frame-relay traffic-rate dynamic
- C. frame-relay adaptive-shaping becn
- D. frame-relay adaptive-shaping fecn

Answer: C

Explanation:

Specify that the router dynamically fluctuate the rate at which it sends packets depending on the BECNs (Backward Explicit Congestion Notifications) it receives if you want the sending router to adjust its transmission rate based on the BECNs received. To select BECN as the mechanism to which traffic shaping will adapt, use the frame-relay adaptive-shaping becn command.

The frame-relay adaptive-shaping command configures a router to adjust virtual circuit (VC) sending rates in response to BECN backward congestion notification messages or interface congestion.

Include this command in a map-class definition and apply the map class either to the main interface or to a subinterface.

Adaptive traffic shaping for interface congestion can be configured along with BECN.

When adaptive shaping for interface congestion is used with BECN, if interface congestion exceeds the queue-depth, then the PVC send rate is reduced to minCIR. When interface congestion drops below the queue-depth, then the send rate is adjusted in response to BECN.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 11-30

QUESTION 172:

You are the network administrator at Certkiller .com. If you enable Frame Relay

642-821

traffic shaping and were to configure a CIR of 64kbps using 125ms time interval, what will be the value of the committed burst (Bc)?

- A. 24000 bits
- B. 32000 bits
- C. 16000 bits
- D. 8000 bits
- E. 48000 bits
- F. 64000 bits

Answer: D

Explanation:

To understand the concepts of traffic shaping, it is important to have a firm grasp of the various traffic parameters in the Frame Relay network. In particular, you should know that some (such as committed information rate [CIR] and excessive burst [Be]) are commonly used but misunderstood.

CIR (Committed Information Rate) - The average rate at which you want to transmit.

This is generally not the same as the CIR provided by the telco. This is the rate at which you want to send in periods of noncongestion.

Bc (Committed Burst) - The amount of data to send in each Tc interval.

Be (Excessive Burst) - The amount of excess data allowed to be sent during the first interval once credit is built up. Transmission credit is built up during periods of nontransmission. The credit is the burst size. Full credit is typically CIR / 8.

Tc (Committed Rate Measurement Interval) - The Bc / CIR time interval. The time interval shouldn't exceed 125 ms (almost always 125 ms).

MinCIR (Minimum CIR) - The minimum amount of data to send during periods of congestion. This is usually what you get from the telco.

MinCIR - defaults to one-half of CIR.

PIR (Peak Information Rate) - The highest possible rate of transmission on any given interface.

MIR (Minimum Information Rate) - The slowest rate of transmission on any given interface.

Interval - Bc / CIR. The maximum is 125 ms, or 1/8 second.

Byte Increment - Bc / 8. This value must be greater than 125.

Limit - Byte Increment + Be / 8 (in bytes).

The calculation is $TC = Bc / CIR$

$125ms (tc) = 8000bits (Bc) / 64kbps (CIR)$

Reference:

Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)

Page 300 & 301

QUESTION 173:

At the HQ location of your frame relay network, your Cisco router connects numerous sites via PVCs. One of the remote routers is using a non-Cisco router.

Which of the following Frame Relay commands could you use to change the encapsulation on any single PVC?

- A. no frame-relay encapsulation ietf
- B. encapsulation frame-relay ietf
- C. no frame-relay encapsulation cisco
- D. frame-relay map ip 10.160.2.1 100 broadcast ietf

Answer: D

Explanation:

The default encapsulation, which is Cisco, is applied to all the VCs available on that serial interface. If most destinations use the Cisco encapsulation, but one destination requires the IETF, you would specify, under the interface, the general encapsulation to be used by most destinations. Because the default encapsulation is Cisco, you would specify the exception using the frame-relay map command.

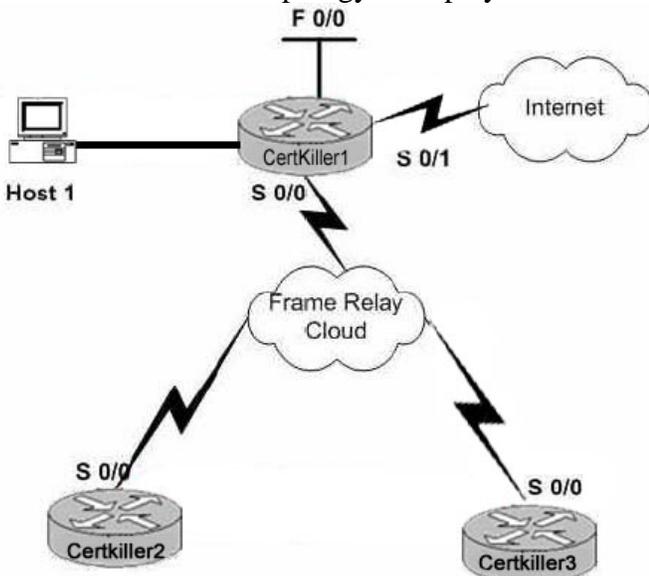
Reference:

Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)
Page 277

QUESTION 174:

SIMULATION

The Certkiller network topology is displayed below:



Certkiller's Spanish test division is finally upgrading its ISDN BRI links to Frame Relay and they've invited you to contribute to this project.

There are three locations, each location has one Cisco 2600 series router.

- 1) Central Office (Madrid) - Certkiller 1
- 2) Regional Office #A (Barcelona) - Certkiller 2
- 3) Regional Office #B (Gibraltar) - Certkiller 3

The support staff at the Barcelona and Gibraltar offices have completed their end of

the configuraton; but since the staff at the Madrid office have all gone to Ibeza for vacation you've been left with the Madrid office to configure.

Your assignment is to:

1. enable Frame Relay on the Serial 0/0 interface
2. configure two sub-interfaces with the appropriate IP address and DLCI under Serial 0/0 using the DLCI number as the sub-interface name
3. build static routes to the Barcelona and Gibraltar branch office LANs.

Network information:

Router: Certkiller 1

F0/0: 10.10.241.1/24

S0/0: DLCI286 - 192.168.233.1/30

DLCI287 - 192.168.233.5/30

S0/1: 172.16.0.6/30

Router: Certkiller 2

F0/0: 10.10.242.1/24

S0/0: 192.168.233.2/30

Router: Certkiller 3

F0/0: 10.10.243.1/24

S0/0: 192.168.233.6/30

On the Madrid router the following DLCIs and IP addresses are to be assigned:

To router Certkiller 2 - DLCI 286 and IP address 192.168.233.1/30

To router Certkiller 3 - DLCI 287 and IP address 192.168.233.5/30

Route to destination network at Certkiller 2 is 10.10.242.0/24

Route to destination network at Certkiller 3 is 10.10.243.0/24

Configure the Madrid router to satisfy the above requirements.

Answer:

Explanaton:

```
Certkiller 1(config)#int s0/0
```

```
Certkiller 1(config-if)#encapsulation frame-relay
```

```
Certkiller 1(config-if)#no shut
```

```
Certkiller 1(config-subif)#int s0/0.286 point-to-point
```

```
Certkiller 1(config-subif)#ip address 192.168.233.1
```

```
255.255.255.252
```

```
Certkiller 1(config-subif)#frame-relay interface-dlci 286
```

```
Certkiller 1(config-fr-dlci)#exit
```

```
Certkiller 1(config-subif)#exit
```

```
Certkiller 1(config)#int s0/0
```

```
Certkiller 1(config-if)#int s0/0.287 point-to-point
```

```
Certkiller 1(config-subif)#ip address 192.168.233.5
```

```
255.255.255.252
```

```
Certkiller 1(config-subif)#frame-relay interface-dlci 287
```

```
Certkiller 1(config-fr-dlci)#exit
```

```
Certkiller 1(config-subif)#exit
```

```
Certkiller 1(config)#ip route 10.10.242.0 255.255.255.0
```

```
192.168.233.2
```

```
Certkiller 1(config)#ip route 10.10.242.0 255.255.255.0
192.168.233.6
Certkiller 1(config)#exit
Certkiller 1# copy run start
You can check your configuration with:
Certkiller 1#show frame-relay pvc
Certkiller 1#show frame-relay map
Certkiller 1(config-subif)#
```

QUESTION 175:

You issue the following command on one of your Cisco routers:

```
frame-relay map ip 192.168.166.21 100
```

What will be the end result of this command? (Choose all that apply)

- A. Split horizon is disabled.
- B. IP address 192.168.166.21 is statically mapped to DLCI 100.
- C. IP address 192.168.166.21 is dynamically mapped to DLCI 100.
- D. Inverse ARP is enabled.
- E. Split horizon is enabled
- F. Inverse ARP is disabled.

Answer: B, F

Explanation:

A DLCI number is a data link connection identifier. Permanent virtual circuits (PVCs) and switched virtual circuits (SVCs) are identified by a DLCI number. The DLCI number defines a single virtual connection through the WAN and is the Frame Relay equivalent to a hardware address.

Periodically, through the exchange of signaling messages, a network may announce a new virtual circuit with its corresponding DLCI number. However, protocol addressing is not included in the announcement. The station receiving such an indication will learn of the new connection, but will not be able to address the other side. Without a new configuration or mechanism for discovering the protocol address of the other side, this new virtual circuit is unusable. For this reason, Inverse Address Resolution Protocol (Inverse ARP) was developed. Inverse ARP allows a Frame Relay network to discover the protocol address associated with the virtual circuit, and ARP is more flexible than relying on static configuration. So if you use dynamic address mapping, Frame Relay Inverse ARP provides a given DLCI and requests next-hop protocol addresses for a specific connection. The router then updates its mapping table and uses the information in the table to route outgoing traffic. Dynamic address mapping is enabled by default for all protocols on a physical interface. If you use the static mapping, you must use the frame-relay map command to statically map destination network protocol addresses to a designated DLCI.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Chapter 11

QUESTION 176:

You are a senior network administrator and you're checking up on your trainee. You look into his monitor and notice the following configuration:

```
interface Serial0/0
no ip address
encapsulation frame-relay
no fair-queue
frame-relay traffic-shaping
bandwidth 1536
!
interface Serial0/0.100 point-to-point
ip address 10.1.1.1 255.255.255.0
frame-relay interface-dlci 100
frame-relay class cisco
!
interface Serial0/0.200 point-to-point
ip address 10.1.2.1 255.255.255.0
frame-relay interface-dlci 200
frame-relay class cisco
!
interface Serial0/0.300 point-to-point
ip address 10.1.3.1 255.255.255.0
frame-relay interface-dlci 300
!!
map-class frame-relay cisco
frame-relay cir 128000
frame-relay adaptive-shaping becn
```

According to the above configuration, what is the CIR of interface Serial0/0.300?

- A. 56 kbps
- B. 128 kbps
- C. 64 kbps
- D. 1536 kbps
- E. 896 kbps

Answer: A

Explanation:

frame-relay traffic-shaping - This command enables FRTS for the interface. Every DLCI under this interface is traffic shaped with either user-defined or default traffic shaping parameters. User-defined parameters can be specified in two ways:

- E. Using the command class class_name under the frame-relay interface-dlci configuration or
- F. Using the command frame-relay class under the serial interface.

1. The following output displays the default FRTS parameters.

```
ms3810-3c#show traffic-shape
```

```
Access Target Byte Sustain Excess Interval Increment Adat
```

```
I/F List Rate Limit bits/int bits/int (ms) (bytes) Acte
```

```
Se1 56000 875 56000 0 125 875 -
```

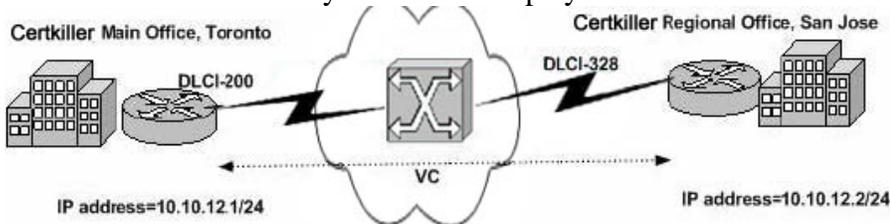
Note: The CIR defaults to a value of 56 Kbps. Hence, PVCs that inherit these default FRTS attributes are forced. In this example, the frame-relay class cisco was not defined on interface serial 0/0.300, so the default value of 56000 is used.

Reference:

http://www.cisco.com/en/US/tech/CK652/CK698/technologies_tech_note09186a00800d6788.shtml

QUESTION 177:

The Certkiller frame relay network is displayed below:



Which Frame Relay map command would you use to configure static address mapping from Certkiller's main office in Toronto to the regional office in San Jose?

- A. frame-relay map ip 10.10.12.2 328 broadcast ietf
- B. frame-relay map ip 10.10.12.1 200 broadcast cisco
- C. frame-relay map ip 10.10.12.2 200 broadcast cisco
- D. frame-relay map ip 10.10.12.1 328 broadcast ietf
- E. None of the above

Answer: C

Explanation:

The answer should be C not

A. In option A, the frame-relay map command is stating the next hop IP address AND the NEXT HOP DLCI number. This is incorrect. The frame-relay map command consists of the next hop IP address and the LOCAL DLCI number.

QUESTION 178:

When configuring Frame Relay traffic shaping on one of the Certkiller routers, what command would you use to associate a subinterface with a map class?

- A. frame-relay map
- B. frame-relay class
- C. map-class frame-relay

- D. frame-relay map-class
- E. map frame-relay class

Answer: C

How to configure Frame Relay traffic Shaping :

Step 1: Specify a map class to be defined with the map-class frame-relay map classname command.

Step 2: Define the map class. When you define a map class for Frame Relay, you can:

1. Define the average and peak rates (in bits per second) allowed on virtual circuits associated with the map class.
2. Specify that the router dynamically fluctuate the rate at which it sends packets depending on the BECNs it receives.
3. Specify either a custom queue list or a priority queue group to use on virtual circuits associated with the map class.
4. Once you have defined a map class with queuing and traffic shaping parameters, enter interface configuration mode and enable Frame Relay encapsulation on an interface with the encapsulation frame relay command, discussed earlier in this chapter.

Step 4: Enable Frame Relay traffic shaping on an interface with the frame-relay trafficshaping command. Enabling Frame Relay traffic shaping on an interface enables both traffic shaping and per-virtual circuit queuing on all the PVCs and SVCs on the interface. Traffic shaping enables the router to control the circuit's output rate and react to congestion notification information if also configured.

Step 5: Map a map class to all virtual circuits on the interface with the frame-relay class map class-name command. The map class-name argument must match the map class-name of the map class you configured.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Chapter 11

QUESTION 179:

What configuration step must you perform before traffic shaping parameters can be applied to a Frame Relay interface?

- A. Define a map class.
- B. Disable any queuing mechanism currently assigned to the interface.
- C. Specify a queuing technique to be used on a Frame Relay connection.
- D. Specify the use of BECN or FECN for traffic adaptation.
- E. None of the above.

Answer: A

Explanation:

Frame Relay traffic shaping is accomplished through the creation of a map class. After the map class is defined the configuration of Frame Relay Traffic Shaping parameters can take place. When you define a map class for Frame Relay, you can:

1. Define the average and peak rates (in bits per second) allowed on virtual circuits

associated with the map class.

2. Specify that the router dynamically fluctuate the rate at which it sends packets, depending on the BECNs it receives.

3. Specify either a custom queue list or a priority queue group to use on virtual circuits associated with the map class.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 11-29

QUESTION 180:

The "show interface serial 10/0 was issued on router CK1 as shown below:

```
Serial10/0 is up, line protocol is up
Hardware is HD64570
Internet address is 172.16.81.1/24
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
  reliability 255/255, txload 1/255, rxload 1/255
Encapsulation FRAME-RELAY, loopback not set
Keepalive set (10 sec)
LMI enq sent 15617, LMI stat recvd 15598, LMI upd recvd 0, DTE LMI up
LMI enq recvd 17, LMI stat sent 0, LMI upd sent 0
LMI DLCI 0 LMI type is ANSI Annex D frame relay DTE
FR SVC disabled, LAPF state down
Broadcast queue 0/64, broadcasts sent/dropped 3/0, interface broadcasts 0
Last input 00:00:12, output 00:00:02, output hang never
Last clearing of "show interface" counters 1d19h
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/1/256 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
Available Bandwidth 1158 kilobits/sec
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
15647 packets input, 226474 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
15653 packets output, 205398 bytes, 0 underruns
0 output errors, 0 collisions, 5 interface resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=down
```

What type of Frame Relay encapsulation is used on this interface?

- A. ANSI
- B. IETF
- C. CISCO
- D. Q933
- E. None of the above

Answer: C

Explanation:

The default encapsulation on an interface is Cisco. When the serial interface of a Cisco router is configured for frame relay displays "encapsulation frame-relay" as shown on line 6 of the output above, the default encapsulation type is used.

Incorrect Answers:

A: This is the configured LMI type, not the encapsulation type for the interface.

B: Although IETF is an encapsulation option, this was not used here. If it was, the output

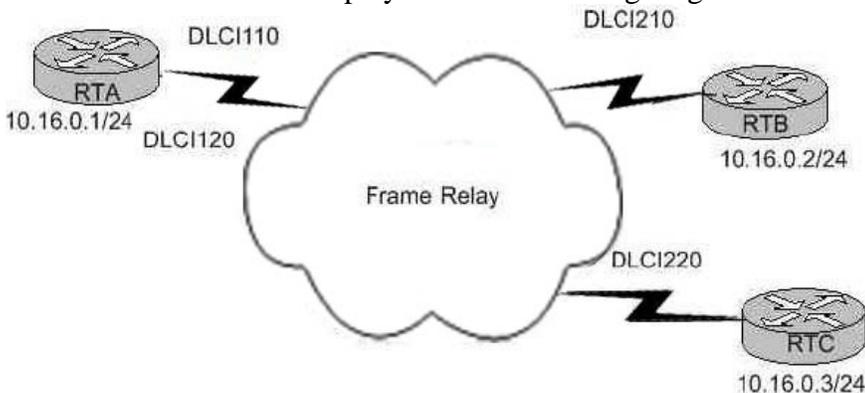
would have stated "encapsulation frame-relay ietf" as shown in the following example:

```
router# show interface serial0
Serial0 is up, line protocol is up
Hardware is PQUICC Serial
MTU 5000 bytes, BW 1544 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation FRAME-RELAY IETF, crc 16, loopback not set
Keepalive set (10 sec)
```

D: This is not a valid Cisco frame relay encapsulation option. The only options are Cisco, which is the default Cisco proprietary method; and IETF, which is the industry standard.

QUESTION 181:

The Certkiller WAN is displayed in the following diagram:



RTA is connected across a hub-and-spoke Frame Relay network to RTB and to RTC. RTC is a non-Cisco router.

Which two static map entries must the administrator configure to allow RTA to communicate with RTB and RTC?

- A. frame-relay map ip 10.16.0.2 110 ietf
frame-relay map ip 10.16.0.3 120
- B. frame-relay map ip 10.16.0.2 210
frame-relay map ip 10.16.0.3 220
- C. frame-relay map ip 10.16.0.2.110 broadcast
frame-relay map ip 10.16.0.3 120 broadcast ietf
- D. frame-relay map ip 10.16.0.2 210 broadcast
frame-relay map ip 10.16.0.3 220 broadcast ietf

Answer: C

Explanation:

The "frame relay map" command is used to statically map an IP address to a DLCI instead of relying on inverse ARP. The DLCI and IP address of the remote locations should be specified. By default, Cisco uses the Cisco proprietary frame relay encapsulation. When connecting to a non-Cisco router, the industry standard IETF frame relay encapsulation should be specified. In this case, since only RTC is a non-Cisco

router, the 'IETF' keyword should be placed only on the frame relay map pointing to this router.

Not D: Because the DLCIs identified (210, 220) are not local to router RT

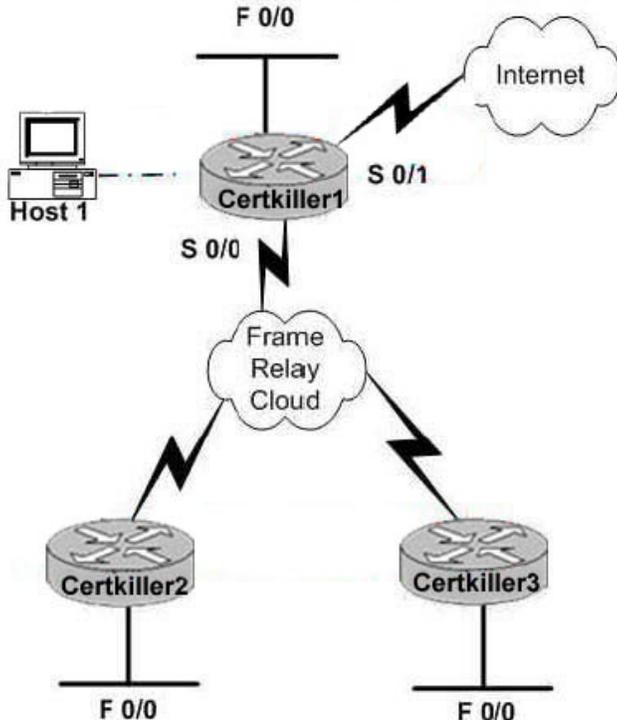
A. The

correct answer is 'C'.

QUESTION 182:

SIMULATION

The Certkiller network is displayed in the following diagram:



You work as network technician at the Beograd office of Certkiller .com. Certkiller .com is transitioning from ISDN BRI links to a Frame Relay solution for the benefits provided by permanent connections. It is your job to coordinate this transition. The network support specialist at each branch location has completed their configuration, and each is awaiting the completion of the central router configuration to test connectivity. All three locations are using Cisco 2600 series routers. Your tasks are to enable Frame Relay on the Serial 0/0 interface, configure two sub-interfaces with the appropriate IP address and DLCI under Serial 0/0 using the DLCI number as the sub-interface name, and build static routes to the branch sites' LAN. Use the topology in the graphic for reference. Further necessary information is as follows:

DLCIs and IP addresses to be assigned on Central Router Certkiller 1:

To router Certkiller 2 - DLCI 68 and IP address 192.168.152.1/30

To router Certkiller 3 - DLCI 69 and IP address 192.168.152.5/30

Route to destination network at R2 is 10.10.15.0/24

Route to destination network at R3 is 10.10.16.0/24

Router Certkiller 1

F0/0: 10.10.14.1/24
S0/0: DLCI68 - 192.168.152.1/30
DLCI69 - 192.168.152.5/30
Router Certkiller 2
F0/0: 10.10.15.1/24
S0/0: 192.168.152.2/30
Router Certkiller 3
F0/0: 10.10.15.1/24
S0/0: 192.168.152.6/30
Configure R1 to accomplish these tasks.

Answer:

```
R1>en
Password:
R1#conf t
Enter configuration commands, one per line. End with END.
R1(config)#int s 0,1
R1(config-if)#no ip add Certkiller.com
R1(config-if)#encap fr
R1(config-if)#int s0/0.676 point-to-po
R1(config-subif)#ip add 192.168.53.1 255.255.255.252
R1(config-subif)#frame-relay interface-dlci 676
R1(config-fr-dlci)#
R1(config-subif)#int s0/0.677 point-to-p
R1(config-subif)#ip add 192.168.53.5 255.255.255.252
R1(config-subif)#frame-relay interface-dlci 677
R1(config-fr-dlci)#ex1
R1(config-subif)#ex1
R1(config)#ip route 10.10.99.0 255.255.255.0 192.168.53.2
R1 (config) tex1
00:00:00:00 sys-1 CONFIG_t Configured from console by console
R1#conf t
Enter configuration commands, one per line. End with END.
R1(config)#no ip route 10.10.99.0 255.255.255.0 192.168.53.2
R1(config)#ip route 10.10.98.0 255.255.255.0 192.168.53.2
R1(config)#ip route 10.10.99.0 255.255.255.0 192.168.53.6
R1 (config) tex1
00:00:00:00 sys-1 CONFIG_t Configured from console by console
R1#cop ru s
Destination filename [startup-config]?
Building configuration...
```

QUESTION 183:

On a subinterface of router CK1 , the following configuration command was issued:

frame-relay interface-dlci

What is this command used for?

- A. To remove an interface
- B. To specify a loopback interface
- C. To define a local DLCI number
- D. To define a remote DLCI number
- E. To select an interface

Answer: C

Explanation:

For point-to-point subinterfaces, the destination is presumed to be known and is identified or implied in the frame-relay interface-dlci command.

If you specified a point-to-point subinterface in the configuration, you must perform the following task in interface configuration mode:

Task	Command
Associate the selected point-to-point subinterface with a DLCI	<code>frame-relay interface-dlci dlci [option]</code>

This statically maps the interface to a DLCI.

If you define a subinterface for point-to-point communication, you cannot reassign the same subinterface number to be used for multipoint communication without first rebooting the router. Instead, you can simply avoid using that subinterface number and use a different subinterface number instead.

QUESTION 184:

Serial 0/0 of router CK1 is being used for a frame relay link. Under the Serial 0/0 interface of router CK1, the "ip unnumbered ethernet 0/0" command was issued. Which of the following correctly describe the IP un-numbered Ethernet 0/0 command when it is issued in configuration mode for a serial interface?

- A. The IP address of the Ethernet interface is used by the serial interface.
- B. There is no effect at all
- C. DHCP traffic received on the serial interface is forwarded to the Ethernet interface.
- D. ARP traffic received on the serial interface is forwarded to the Ethernet interface.

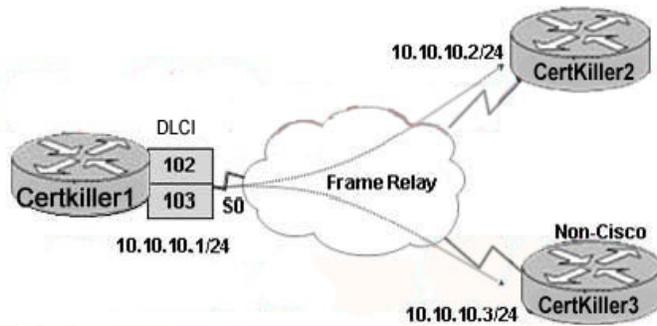
Answer: A

Explanation:

The ip unnumbered configuration command allows you to enable IP processing on a serial interface without assigning it an explicit IP address. The ip unnumbered interface can "borrow" the IP address of another interface already configured on the router, thereby conserving network and address space. In this case, it will use the IP address that is already assigned to the ethernet interface.

QUESTION 185:

The Certkiller frame relay network is displayed below:



```
hostname CertKiller2
!
interface s0
ip address 10.10.10.2 255.255.255.0
encapsulation frame-relay
frame-relay map ip 10.10.10.1 201 broadcast
```

```
hostname CertKiller3
!
interface s0
ip address 10.10.10.3 255.255.255.0
encapsulation frame-relay
frame-relay map ip 10.10.10.1 301 broadcast
```

```
CertKiller3# debug frame-relay packets
```

```
CertKiller3# ping 10.10.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.2, timeout is 2 seconds:
```

```
00:27:51: Serial0:Encaps failed--no map entry link 7(IP).
00:27:53: Serial0:Encaps failed--no map entry link 7(IP).
00:27:53: Serial0:Encaps failed--no map entry link 7(IP).
00:27:57: Serial0:Encaps failed--no map entry link 7(IP).
00:27:59: Serial0:Encaps failed--no map entry link 7(IP).
Success rate is 0 percent (0/5)
```

In this network, Certkiller 1 is connected over a Frame Relay cloud to Certkiller 2 and a non-Cisco device, Certkiller 3. What must be configured on the Certkiller 1 S0 interface to achieve full connectivity with the spoke routers?

- A. encapsulation frame-relay
frame-relay map ip 10.10.10.2 102 broadcast
frame-relay map ip 10.10.10.3 103 broadcast
- B. encapsulation frame-relay ietf
frame-relay map ip 10.10.10.2 102 broadcast
frame-relay map ip 10.10.10.3 103 broadcast
- C. encapsulation frame-relay
frame-relay map ip 10.10.10.2 102 broadcast ietf
frame-relay map ip 10.10.10.3 103 broadcast
- D. encapsulation frame-relay
frame-relay map ip 10.10.10.2 102 broadcast
frame-relay map ip 10.10.10.3 103 broadcast ietf
- E. encapsulation frame-relay
frame-relay map ip 10.10.10.2 102 broadcast cisco
frame-relay map ip 10.10.10.3 103 broadcast

Answer: D

Explanation:

By default, Cisco routers use the Cisco proprietary encapsulation for frame relay connections. This is recommended when connecting together Cisco routers. When connecting a Cisco router to a non-Cisco router, the IETF standard encapsulation type must be used. In this case, router Certkiller 3 is not a Cisco router, so the connection to it must be used with the IETF keyword, while the connection to the other Cisco router (Certkiller 2) remains using the Cisco encapsulation.

QUESTION 186:

What is the correct syntax to configure software compression for LAPB, PPP, and HDLC for a link?

- A. Router(config-if)#frame-relay payload-compress
- B. Router(config-if)#ip rtp header-compression [passive]
- C. Router(config-if)#ip tcp header-compression [passive]
- D. Router(config-if)#compress [predictor|stac|mppc]

Answer: D

Explanation:

To configure software compression for Link Access Procedure, Balanced (LAPB), PPP, and High-Level Data Link Control (HDLC) encapsulations, use the compress command in interface configuration mode. The correct syntax is:

compress [predictor | stac | mppc]

Syntax Description

predictor	Specifies that a predictor (RAND) compression algorithm will be used on LAPB and PPP encapsulation. Compression is implemented in the software installed in the router's main processor.
stac	<p>Specifies that a Stacker (LZS) compression algorithm will be used on LAPB, HDLC, and PPP encapsulation. For all platforms except Cisco 7200 series and platforms that support the VIP2, compression is implemented in the software installed in the router's main processor.</p> <p>On Cisco 7200 series, and on VIP2s in Cisco 7500 series, specifying the compress stac command with no options causes the router to use the fastest available compression method for PPP encapsulation only:</p> <ul style="list-style-type: none">▪ If the router contains a compression service adapter (CSA), compression is performed in the CSA hardware (hardware compression).▪ If the CSA is not available, compression is performed in the software installed on the VIP2 (distributed compression).▪ If the VIP2 is not available, compression is performed in the router's main processor (software compression).
mppc	(Optional) Specifies that the MPPC compression algorithm will be used.

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a008008

QUESTION 187:

An administrator wants to run OSPF over the point-to-multipoint Frame Relay network. What configuration command would specify the Frame Relay network type that will not require additional configuration for OSPF neighbors?

- A. frame-relay map ip 192.168.1.1 110
- B. frame-relay map ip 192.168.1.1 110 broadcast
- C. frame-relay map ip 192.168.1.1 110 ietf
- D. frame-relay map ip.192.168.1.1 110 cisco

Answer: B

Explanation:

The "broadcast" keyword is required to send broadcast and multicast traffic across the frame relay network. This is needed to transport most IP routing protocol traffic, including OSPF traffic for building neighbor adjacencies. By default, the "broadcast" feature is not enabled.

Example:

```
interface Serial2  
ip address 1.1.1.2 255.255.255.0
```

```
encapsulation frame-relay  
ip ospf network point-to-multipoint  
no keepalive  
frame-relay map ip 1.1.1.1 16 broadcast
```

QUESTION 188:

On one of the Certkiller routers the following configuration command was issued:
Certkiller A(config)#aaa authentication login default group tacacs+
none

What is this command used for?

- A. It uses the list of servers specified in group "TACACS+", if none are available, then no access is permitted.
- B. It uses the list of TACACS+ servers for authentication, if TACACS+ fails then uses no authentication.
- C. It uses the list of TACACS+ servers for authentication, if TACACS+ fails then no access is permitted.
- D. No authentication is required to login.
- E.

It uses a subset of TACACS+ servers named "group" for authentication as defined by the aaa group servers tacacs+ command.

F. TACACS+ is the first default authentication method.

Answer: B

Explanation:

Once AAA has been enabled on the router, the administrator must declare the methods by which authentication can take place. The aaa authentication login command answers this question: How do I authenticate the login dialog?

The declaration of default tells the router what to do if no listname has been declared on the interface. If a listname has been declared, that listname controls the login. In this statement the listname group is defined, It declares that listname group use TACACS+ by default, and if that fails no authentication is required because the none command has been entered at the end.

Additional methods for the aaa authentication command are:

- * enable - Uses the enable password for authentication.
- * line - Uses the line password for authentication.
- * local - Uses the local username/password database for authentication.
- * none - Uses no authentication.
- * tacacs+ - Uses the TACACS+ authentication method.
- * radius - Uses the RADIUS authentication method.
- * guest - Allows guest logins without passwords. This option applies only to ARAP operations.
- * auth-guest - Allows guest logins only if the user has already logged in to EXEC. This option only applies to ARAP operations.

* if-needed - Stops further authentication if the user has already been authenticated. This option only applies to PPP operations.

* krb5 - Uses Kerberos 5 for authentication, this option only applies to PPP operations.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 15-12

Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)

Page 409 & 410

QUESTION 189:

You are tasked with configuring authentication on one of the Certkiller routers. Which of the following authentication protocols exchanges information between the client and the server using UDP?

- A. AAA
- B. RADIUS
- C. LCP
- D. TACACS+
- E. All of the above

Answer: B

Explanation:

RADIUS is a client/server-based network security protocol. It uses UDP for a transport protocol.

The RADIUS server is typically run on a computer. The clients are any type of device that is responsible for passing user information to designated RADIUS servers and then acting on the response that is returned. Transactions between the client and RADIUS server are authenticated through the use of a shared secret, which is never sent over the network. Some of the advantages of RADIUS are the following:

1. RADIUS has less packet overhead because it uses UDP.
2. With source code format distribution, RADIUS is a fully open protocol format. The user can modify it to work with any security system currently available on the market.
3. RADIUS offers enhanced accounting functionality.

Reference:

Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)

Page 403

QUESTION 190:

Listed below are a number of router IOS commands. To define 'interesting' traffic for a single host with DDR you'll need a set of three commands. Which ones are they? (Choose three)

- A. Certkiller A(config)#dialer-list 1 protocol ip permit 10.1.1.1
- B. Certkiller A(config-if)#dialer-group 1

- C. Certkiller A(config)#dialer-list 1 protocol ip list 2
- D. Certkiller A(config)#dialer-group 2
- E. Certkiller A(config)#access-list 2 permit host 192.168.1.21
- F. Certkiller A(config-if)#dialer-list 2 protocol ip permit

Answer: B, C, E

Explanation:

The dialer-list command is used to configure dial-on-demand calls that will initiate a connection. The simple form of the command specifies whether a whole protocol suite, such as IP or Internetwork Packet Exchange (IPX(r)), will be permitted or denied to trigger a call. The more complex form references an access list that will allow finer control of the definition of interesting traffic. The syntax for this command is:

```
Router(config)#dialer-list group-number protocol protocol {permit | deny}
```

list access-list-number

The dialer-group interface command applies the dialer list specifications to an interface.

The syntax for this command is:

```
Router(config-if)#dialer-group group-number
```

The access-list command gives more control over interesting traffic. It uses standard or extended access lists. The syntax for this command is:

```
Router(config)#access-list access-list-number {permit | deny}
{protocol | protocol-keyword} {source source-wildcard | any}
{destination destination-wildcard | any} [protocol-options] [log]
```

By knowing this we can generate the router commands:

```
Certkiller A (config)#dialer-list 1 protocol ip list 2
Certkiller A(config)#access-list 2 permit host 192.168.1.21
Certkiller A(config-if)#dialer-group 1
```

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 7-30 & 7-31

QUESTION 191:

While you were on your lunch break your apprentice trainee was busy configuring access lists. When you return to your workstation you find the following configuration:

```
access-list 101 permit ip any any
access-list 101 deny tcp any any eq ftp
dialer-list 2 protocol ip list 101
```

What is true about the configuration that your trainee entered? (Choose all that apply)

- A. FTP traffic will be forwarded.
- B. Since FTP uses two sockets, both must be defined to prevent packet forwarding.
- C. FTP will cause the line to come up.

D. FTP traffic will not be forwarded.

Answer: A C

Explanation:

The logic that IOS uses with a multiple-entry Access Control List can be summarized as follows:

1. The matching parameters of the access-list statement are compared to the packet.
2. If a match is made, the action defined in this access-list statement (permit or deny) is performed.
3. If a match is not made in Step 2, repeat Steps 1 and 2 using each successive statement in the ACL until a match is made.
4. If no match is made with an entry in the access list, the deny action is performed.

The access-list 101 permit ip any any command is used and the result is that every packet will be permitted. So the second command "access-list 101 deny tcp any any eq ftp" is never read by the IOS since all IP traffic (including FTP) will match the first line.

The dialer-list 2 protocol ip list 101 command binds the Access Control List to the dialer list. Therefore the FTP traffic will be forwarded and it will bring up the line.

Reference:

Cisco Press - ICND - 640-811 - Exam Certification Study Guide 2004 (ISBN 1-58720-083-x) Page 430

QUESTION 192:

The following command was issues on router CK1 , which has been configured for PPP call back:

```
dialer hold-queue 100 timeout 10
```

From this information, when will CK1 place outbound interesting packets in queue?

- A. While a dial connection is established.
- B. While higher priority traffic is sent over a dial connection.
- C. During network congestion on a dial connection.
- D. For 10 seconds after a source quench message is received.
- E. For 10 seconds for 10 consecutive quench messages.

Answer: A

Explanation:

The dialer hold-queue timeout determines how long to wait before the client can make another call to the same destination. The server must make the return call before the client hold-queue timer expires to prevent the client from trying again and possibly preventing the return call from being connected.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 5-24

QUESTION 193:

You have just received a brand new Cisco router and need to configure auditing on it. What command would you use to enable auditing of the privileged mode access commands?

- A. aaa accounting enable 15
- B. ip audit enable
- C. aaa accounting command 15
- D. aaa accounting enable priv

Answer: C

Explanation:

AAA accounting can supply information concerning user activity back to the database. This concept was especially helpful in the early days of Internet service when many ISPs offered 20 or 40 hours per week at a fixed cost and hourly or minute charges in excess of the specified timeframe. Today it is much more common for the ISP charge to be set for an unlimited access time. This does not, however, minimize the power of accounting to enable the administrator to track unauthorized attempts and proactively create security for system resources. In addition, accounting can be used to track resource usage to better allocate system usage.

Accounting is generally used for billing and auditing purposes and is simply turned on for those events that are to be tracked.

Syntax:

```
aaa accounting {system | network | exec | connection | commands level} {default | list-name} {start-stop | stop-only | none} method1 [method2...]
```

Commands - Runs accounting for all commands at the specified privilege level.

Level - Specific command level to track for accounting. Valid entries are 0 through 15.

Command - With this argument, command accounting logs information regarding which commands are being executed on the router. The accounting record contains a list of commands executed for the duration of the EXEC session, along with the time and date information.

Reference:

Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)
Page 416.

QUESTION 194:

Which command should you use to audit SLIP, PPP, and ARAP network service requests on your Cisco router?

- A. ip audit services enable
- B. aaa accounting network
- C. aaa accounting services enable
- D. ip aaa audit network

E. ip audit enable

Answer: B

Explanation:

Accounting enables the administrator to collect information such as start and stop times for user access, executed commands, traffic statistics, and resource usage and then store that information in the relational database management system (RDBMS). In other words, accounting enables the tracking of services and resources that are accessed by the user. Use the aaa accounting command in global configuration mode for auditing and billing purposes, as follows:

command level - Audits all commands at the specified privilege level (0-15).

connection - Audits all outbound connections such as Telnet, rlogin.

exec - Audits the EXEC process.

network - Audits all network service requests, such as SLIP, PPP, and ARAP.

system - Audits all system-level events, such as reload.

start-stop - Sends a start accounting notice at the beginning of a process and a stop accounting notice at the end of a process. The start accounting record is sent in the background. The requested user process begins regardless of whether the start accounting notice was received by the accounting server.

stop-only - Sends a stop accounting notice at the end of the requested user process.

wait-start - As in start-stop, sends both a start and a stop accounting notice to the accounting server. With the wait-start keyword, the requested user service does not begin until the start accounting notice is acknowledged. A stop accounting notice is also sent.

{tacacs+ | radius} - Uses TACACS+ for accounting, or enables RADIUS-style accounting.

Reference:

Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)

Page 401

QUESTION 195:

Some of the Certkiller locations are still using AppleTalk. What is true about RADIUS and TACACS+ compatibility with the AppleTalk Remote Access (ARA) protocol? (Choose all that apply.)

- A. RADIUS server is incapable of supporting AppleTalk Remote Access (ARA) protocol.
- B. TACACS+ server is incapable of supporting AppleTalk Remote Access (ARA) protocol.
- C. RADIUS server is capable of supporting AppleTalk Remote Access (ARA) protocol.
- D. TACACS+ server is capable of supporting AppleTalk Remote Access (ARA) protocol.
- E. Neither TACACS+ or RADIUS servers is capable of supporting AppleTalk Remote Access (ARA) protocol.

F. All of the above.

Answer: A, D

Explanation:

RADIUS does not support the following protocols:

1. AppleTalk Remote Access (ARA) protocol
2. Net BIOS Frame Protocol Control protocol
3. Novell Asynchronous Services Interface (NASI)
4. X.25 PAD connection

The TACACS+ protocol forwards many types of username password information. This information is encrypted over the network with MD5, an encryption algorithm.

TACACS+ can forward the password types for ARA, SLIP, PAP, CHAP, and standard Telnet. This allows clients to use the same username password for different protocols.

References:

http://www.gazi.edu.tr/tacacs/docs/tac_rad_comp.html

<http://www.cisco.com/warp/public/614/7.html>

QUESTION 196:

Which IOS command would you use on your router to specify a RADIUS server to take responsibility for authenticating dial-up clients?

- A. aaa radius server
- B. radius-server host
- C. ip aaa radius host
- D. aaa authentication radius-server

Answer: B

Explanation:

To specify a RADIUS server host, use the radius-server host configuration command.

Use the no form of this command to delete the specified RADIUS host.

```
radius-server host {hostname | ip-address} [auth-portport-number]
[acct-portport-number]
[timeoutseconds] [retransmitretries] [keystring]
no radius-server host {hostname | ip-address}
```

<i>hostname</i>	DNS name of the RADIUS server host.
<i>ip-address</i>	IP address of the RADIUS server host.
auth-port	(Optional) Specifies the UDP destination port for authentication requests.
<i>port-number</i>	(Optional) Port number for authentication requests; the host is not used for authentication if set to 0. The default authorization port number is 1645.
acct-port	(Optional) Specifies the UDP destination port for accounting requests.
<i>port-number</i>	(Optional) Port number for accounting requests; the host is not used for accounting if set to 0. The default accounting port number is 1646.
timeout	(Optional) The time interval (in seconds) that the router waits for the RADIUS server to reply before retransmitting. This setting overrides the global value of the radius-server timeout command. If no timeout value is specified, the global value is used. Enter a value in the range 1 to 1000.
<i>seconds</i>	(Optional) Specifies the timeout value. Enter a value in the range 1 to 1000. If no timeout value is specified, the global value is used.
retransmit	(Optional) The number of times a RADIUS request is resent to a server, if that server is not responding or responding slowly. This setting overrides the global setting of the radius-server retransmit command.
<i>retries</i>	(Optional) Specifies the retransmit value. Enter a value in the range 1 to 100. If no retransmit value is specified, the global value is used.
key	(Optional) Specifies the authentication and encryption key used between the router and the RADIUS daemon running on this RADIUS server. This key overrides the global setting of the radius-server key command. If no key string is specified, the global value is used. The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the radius-server host command syntax. This is because the leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.
<i>string</i>	(Optional) Specifies the authentication and encryption key for all RADIUS communications between the router and the RADIUS server. This key must match the encryption used on the RADIUS daemon. All leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1826/products_feature_guide09186a0080087cdc.html#xtoc

QUESTION 197:

What's a major problem an administrator faces when using symmetric encryption to secure their IP networks?

- A. Slow calculation to encrypt and decrypt cipher
- B. Key management
- C. Based on complex mathematical operations
- D. Best used for small (low volume) encryption tasks

Answer: B

Explanation:

The problem with symmetric encryption is with the key. There's a shared secret key at both ends, so the probability of a hacker finding the key is exponentially greater. Therefore there's great difficulty and responsibility in managing the keys. They need to be secured during service and distribution. They need to be changed often, and since humans are involved in each task, there's always doubt to the integrity of the security.

QUESTION 198:

An ISDN PRI controller for the ISDN T1 on one of the Certkiller routers is configured as shown below:

```
controller t1 1
channel-group 0 timeslot 1-6
channel-group 1 timeslot 7
channel-group 2 timeslot 8
channel-group 3 timeslot 9-11
pri-group timeslot 12-24
```

What is true about the partial configuration above?

- A. This is an incorrect configuration because more than one timeslot must be in a channel group.
- B. This is a correct configuration and a corresponding serial interface named interface serial 0:23 for the D channel will automatically be created.
- C. This is an incorrect configuration because channel groups and a primary group can not be configured on the same controller interface.
- D. This is an incorrect configuration and the user must create corresponding serial interface for each of the data bearing timeslots 12-23

Answer: B

Explanation:

Once the controller is defined and configured, the last available channel will automatically be used by the Cisco IOS to be used as the ISDN D channel. In this case, serial 0/0:23 is the last available channel in an ISDN T1 (serial 0/0:0 is the first) so this will be created automatically.

Reference: CCNP Remote Access Exam Certification Guide, page 173-174, Brian Morgan & Craig Dennis, Cisco Press 2001, ISBN 1-58720-003-1

QUESTION 199:

The Certkiller Italian WAN is displayed in the following diagram:



```
hostname Rome
!  
username Paris password 0 Certkiller  
isdn switch-type basic-net3  
!!  
interface BRI0  
no ip address  
encapsulation ppp  
dialer pool-member 1  
!  
interface Dialer1  
ip address 10.10.0.1 255.255.255.252  
encapsulation ppp  
dialer remote-name Paris  
dialer idle-timeout 30  
dialer string 6115  
dialer pool 1  
ppp authentication chap  
!  
router rip  
network 10.0.0.0  
!  
dialer-list 1 protocol ip permit
```

Assuming that Rome is the client (initiating the call) and Paris is the server (receiving the call) what is true?

- A. Rome will initiate the call whenever any IP traffic is routed towards the Paris router.
- B. Rome will initiate the call whenever any IP traffic is routed towards the Paris router however the call will last 30 seconds at maximum.
- C. Rome will never initiate the call because the dialer remote-name is incorrectly configured on the Rome router.
- D. Rome will never initiate the call because the dialer interface is not associated with any interesting traffic.

Answer: D

Explanation:

In order to associate an access list or a dialer list to an ISDN interface, the "dialer-group" command must be used on the BRI or Dialer interface. In this example, the "dialer-list 1" was created, which permits all IP traffic. The problem is that this dialer list was not tied to the dialer interface. The correct configuration syntax should have been:

```
interface Dialer1
```

```
ip address 10.10.0.1 255.255.255.252
encapsulation ppp
dialer remote-name Paris
dialer-group 1
dialer idle-timeout 30
dialer string 6115
dialer pool 1
ppp authentication chap
```

Reference: CCNP Remote Access Exam Certification Guide, page 143, Brian Morgan & Craig Dennis, Cisco Press 2001, ISBN 1-58720-003-1

QUESTION 200:

You are a senior network administrator and your junior administrator didn't arrive to work because he claimed he was sick. So you give him an assignment to do from home via Telnet. So from his home; he logged onto the companies router and entered the following command:

```
Router(config)#aaa new-model
```

Before entering anything else, the lazy junior administrator (with the intention of being cautious) thought it would be safe to save the configuration to NVRAM, log off from telnet and take a break for a few hours. Assuming that no local username or password exists on the router database, what will happen when the administrator tries to immediately establish another telnet session? (Choose two)

- A. The session asks for a username that may not exist.
- B. The router requires a reboot so the administrator can login.
- C. The administrator must access the router through the console port to login.
- D. The administrator can log in without using a password.

Answer: A, C

Explanation:

Once AAA has been enabled on the router, the administrator must declare the methods by which authentication can take place. The key issue is to ensure that the administrator has a way to gain access to the router if the AAA server is down. Failure to provide a backdoor interface can result in lost communications to the router and the necessity to break in through the console port. Care should be taken to always configure a local access method during any implementation of AAA.

References:

Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)
Page 408

CCNP Remote Access Exam Certification Guide, page 374, Brian Morgan & Craig Dennis, Cisco Press 2001, ISBN 1-58720-003-1

QUESTION 201:

When radius authentication is being configured on a router, which commands will allow a user to telnet successfully into the router?

```
Router(config)# radius-server host 192.168.1.23
```

```
Router(config)# radius-server key Certkiller
```

```
Router(config)# aaa new-model
```

A. Router(config)# aaa authentication login AAA group radius local none

```
Router(config)# line vty 0 4
```

```
Router(config-line)# login authentication AAA
```

B. Router(config)# aaa authentication login AAA group radius local none

```
Router(config)# line vty 0 4
```

```
Router(config-line)# login authentication Certkiller
```

C. Router(config)# aaa authentication login default group radius local none

```
Router(config) line vty 0 4
```

```
Router(config-line) login authentication AAA
```

D. Router(config)# aaa authentication login AAA group radius local none

```
Router(config)# line vty 0 4
```

```
Router(config-line)# login authentication default
```

Answer: A

Explanation:

The answer should be A not C. In option C, the aaa authentication command is using the default group, then under the line interface it points to a configured list called AAA (login authentication AAA). This is incorrect, with this answer the configured login list AAA doesn't exist therefore the line authentication method wouldn't work.

In option A, the authentication list AAA is configured AND under the line configuration, points to this configured list. This is the only option that is correct.

QUESTION 202:

Given the following configuration, which two statements about the router are true?

(Choose two.)

```
router(config)# aaa authentication login default group tacacs+ none
```

A. No authentication is required to login.

B. It uses TACACS+ as the first default authentication method.

C. It uses the default local database for authentication. If authentication fails, then no access is permitted.

D. It uses the list of servers specified in group "TACACS+". If none are available, then no access is permitted.

E. It uses the list of TACACS+ servers for authentication. If the TACACS+ authentication servers are unavailable, then the router uses no authentication.

F. It uses a subset of TACACS+ servers named "group" for authentication as defined by the aaa group server tacacs+ command.

Answer: B, E

Explanation:

The Cisco IOS software uses the first method listed to authenticate users. If that method fails to respond (indicated by an ERROR), the Cisco IOS software selects the next authentication method listed in the method list. This process continues until there is successful communication with a listed authentication method, or all methods defined in the method list are exhausted. From the configuration file shown above, the order of operation is to first check the tacacs+ server, and should that fail do not use any authentication method.

QUESTION 203:

When comparing the differences between PPPoA and PPPoE, which of the following statements are true?

- A. PPPoE does not support session authentication with an aggregation router.
- B. PPPoE provides simple bridged connections for a limited number of hosts.
- C. PPPoA relies on client software to provide connectivity and authentication.
- D. PPPoA is routed end-to-end over ATM from the user's PC to the aggregation router.
- E. None of the above

Answer: D

Explanation:

Some key advantages of PPPoE and how they differ from PPPoA include:

- * Per session authentication based on Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP). This is the greatest advantage of PPPoE as authentication overcomes the security hole in a bridging architecture.
- * Per session accounting is possible, which allows the service provider to charge the subscriber based on session time for various services offered. The service provider may also require a minimal access charge.
- * PPPoE can be used on existing CPE installations that cannot be upgraded to PPP or that do not have the ability to run PPPoA, extending the PPP session over the bridged Ethernet LAN to the PC.
- * PPPoE preserves the point-to-point session used by Internet Service Providers (ISPs) in the current dialup model. PPPoE is the only protocol capable of running point-to-point over Ethernet without requiring an intermediate IP stack.
- * The Network Access Provider (NAP) or Network Service Provider (NSP) can provide secure access to a corporate gateway without managing end-to-end permanent virtual circuits (PVCs) and making use of Layer 3 routing and/or Layer 2 Tunneling Protocol (L2TP) tunnels. This makes the business model of selling wholesale services and virtual private networks (VPNs) scalable.
- * PPPoE can provide a host (PC) access to multiple destinations at a given time. There can be multiple PPPoE sessions per PVC.
- * The NSP can oversubscribe by deploying idle and session time-outs using an industry

standard Remote Authentication Dial-In User Service (RADIUS) server for each subscriber.

* PPP can be used with the service selection gateway (SSG) feature.

Some key disadvantages of PPPoE and how they differ from PPPoA include:

* PPPoE client software must be installed on all hosts (PCs) connected to the Ethernet segment. This means that the access provider must maintain the CPE and the client software on the PC.

* Because PPPoE implementation uses RFC1483 bridging, it is susceptible to broadcast storms and possible denial-of-service attacks.

Reference:

http://www.cisco.com/warp/public/794/pppoe_arch.html

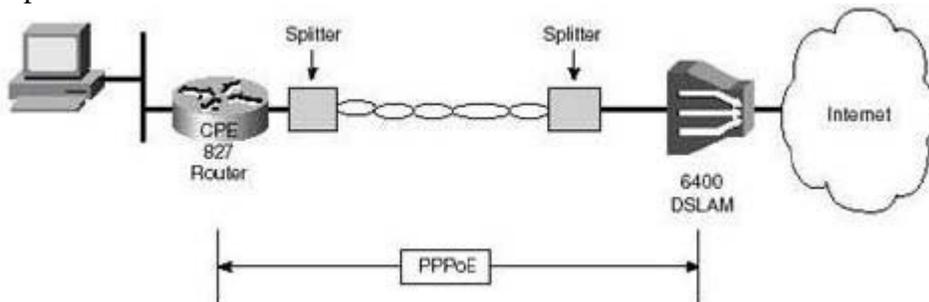
QUESTION 204:

DSL connections commonly use PPP over Ethernet (PPoE). What process does a Certkiller host have to perform to establish a PPoE SESSION_ID?

- A. A DHCP request process to request and IP address and session ID.
- B. A Discovery process to identify a PPPoE server and request a session ID.
- C. A RARP request process to request a MAC address and session ID.
- D. A BOOTP process to request a configuration and session ID.
- E. None of the above

Answer: B

Explanation:



When a router wants to initiate a PPPoE session, it must first perform Discovery to identify the Ethernet MAC address of the peering device and establish a PPPoE SESSION_ID. Discovery is inherently a client/server relationship. During Discovery, a router discovers the provider DSLAM. Discovery allows the CPE router to discover all available DSLAMs, and then select one. When Discovery completes successfully, both the CPE router and the selected DSLAM have the information they will use to build their point-to-point connection over Ethernet.

Reference:

Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)

Page 253

QUESTION 205:

Many Certkiller remote offices use DSL for their connectivity. Which four features are usually required for an 827 ADSL router to support a home ADSL broadband Internet connection with multiple end-user PCs? (Choose four)

- A. IPSec
- B. Bridging (IRB or RBE)
- C. PPPoE client
- D. PAT
- E. DHCP server
- F. Static default route

Answer: C, D, E, F

Explanation:

In Cisco IOS(r) Software Release 12.1(3)XG, a PPP over Ethernet (PPPoE) client feature was introduced for the Cisco 827 router. This feature allows the PPPoE functionality to be moved to the router. Multiple PCs can be installed behind the Cisco 827. Before their traffic is sent to the PPPoE session, it can be encrypted, filtered, and so forth. Also, Network Address Translation (NAT) can run.

PAT is needed to be able to translate multiple internal IP addresses into one single IP address. Since the majority of DSL connections provide only IP address, this is necessary.

A DHCP server is normally required, so that IP addresses can be dynamically assigned to the PC's sharing the DSL connection.

Finally, a static default route needs to be configured on the 827 DSL router pointing out the DSL interface, so that all traffic destined for the Internet will be forwarded out to the DSL network.

QUESTION 206:

Router CK1 is configured as shown below:

```
interface ATM0/0
no ip address
dialer pool-member 1
pvc 1/32
encapsulation aal5mux ppp dialer
```

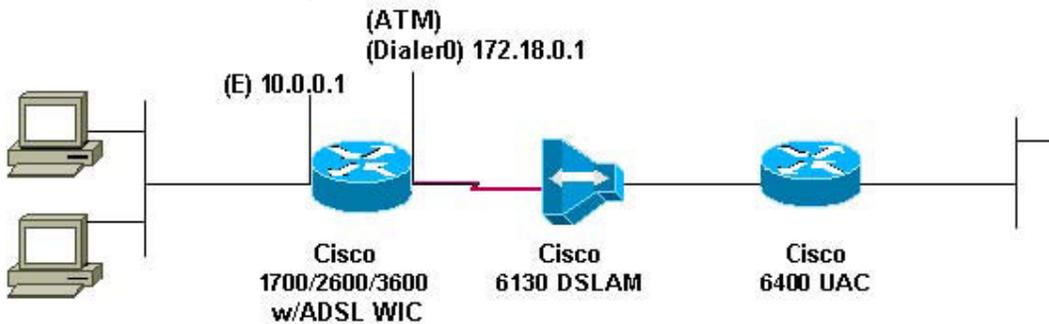
Given the above configuration, which statement is true?

- A. This device is configured as a PPPoE client.
- B. This device is configured as a PPPoA client.
- C. This device is configured as RFC 1483/2684 bridge.
- D. This device is configured as an aggregation router.
- E. None of the above.

Answer: B

Explanation:

This following is an example of configuring a Cisco router as a PPPoA client. The command "encapsulation aal5mux ppp dialer" placed under the ATM interface is the indication that it is using PPPoA.



Partial sample config for a PPPoA client.

```
hostname CK1
!!interface ATM0
no ip address
no ip directed-broadcast
no ip mroute-cache
no atm ilmi-keepalive
pvc 1/150
encapsulation aal5mux ppp dialer
dialer pool-member 1
!!interface Dialer0
ip address 172.18.0.1 255.255.0.0
ip nat outside
no ip directed-broadcast
encapsulation ppp
dialer pool 1
dialer-group 2
ppp pap sent-username
username password password
```

Reference:

[http://www.cisco.com/en/US/tech/ CK1 75/ CK1](http://www.cisco.com/en/US/tech/CK175/CK15/technologies_configuration_example09186a0080093e60.shtml)

[5/technologies_configuration_example09186a0080093e60.shtml](http://www.cisco.com/en/US/tech/CK175/CK15/technologies_configuration_example09186a0080093e60.shtml)

QUESTION 207:

The following was issued on a Certkiller DSL router:

```
CertKillerADSL#show dsl int atm 0
Modem Status:          ATU-R (DS)          ATU-C (US)
DSL Mode:              Showtime (DMTDSL_SHOWTIME)
ITU STD NUM:          ITU G.992.1 (G.DMT)
Vendor ID:            0x01                0x01
Vendor Specific:     'ALCB'              'ANDV'
Vendor Country:      0x0000              0x0000
Capacity Used:       6%                  14%
Noise Margin:        31.0 dB              27.0 dB
Output Power:        18.0 dBm             12.0 dBm
<output omitted>
```

```
Speed (kbps):          Interleave      Fast      Interleave      Fast
<output omitted>
```

Observe the output from the show dsl int atm 0 command shown above. What does the display of the upstream and downstream speed indicate?

- A. Layer 1 connectivity has been established
- B. Layer 2 connectivity has been established
- C. Layer 1 and 2 connectivity has been established
- D. Layer 3 connectivity has been established
- E. Layer 2 and 3 connectivity has been established

Answer: C

Explanation:

The output in this example shown above displays the normal operation of a DSL router that is fully functioning. If the modem state changes from "0x8" to "SHOWTIME," it means that the Cisco 827 has successfully trained with the DSLAM. This verifies connectivity at layer 1. Layer 2 connectivity can be verified via the speed of the connections both upstream and downstream. For a complete overview of the output from the "show dsl interface atm" command, see the link provided below:

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_command_reference_chapter09186a008017

QUESTION 208:

Which two statements are true when an IPSec-protected path is configured for transport mode? (Choose two)

- A. The payload of the packet is protected but the original IP address exposed.
- B. The application endpoints must also be the IPSec endpoints.
- C. IPSec gateways provide IPSec services to hosts.
- D. Security is provided for the transport layer and above only.
- E. Encrypted packets are encapsulated in another IP packet for routing.

Answer: B, E

Explanation:

IPSec can operate in one of two separate modes: transport mode and tunnel mode. These modes refer to how data is sent and secured throughout the network. In transport mode, IPSec protection is provided all the way from the source to the destination. In this way, transport mode is said to provide end-to-end transmission security.

Tunnel mode secures data only between tunnel points or gateways. Tunnel mode provides gateway-to-gateway transmission security. When data is in transmission between the client and the server, it remains unprotected until it reaches the gateway. Once at the gateway, it is secured with IPSec until it reaches the destination gateway. At this point, data packets are decrypted and verified. The data is then sent to the receiving host unprotected. Tunnel mode is often employed when data must leave the secure confines of a local LAN or WAN and travel between hosts over a public network such as the Internet.

Transport mode is a host-to-host connection involving only two machines. In tunnel mode, the IPSec machines act as gateways and traffic for any number of client machines may be carried.

Host machines (as opposed to security gateways) with IPSec implementations may also support transport mode. In this mode, the host does its own IPSec processing and routes some packets via IPSec.

In Transport-mode ESP, the ESP header is inserted into the IP datagram immediately prior to the transport-layer protocol header (e.g., TCP, UDP, or ICMP). In this mode, bandwidth is conserved because there are no encrypted IP headers or IP options.

QUESTION 209:

Router CK1 is a Cisco 827 ADSL router configured as a PPPoE client. Part of the configuration of router CK1 is displayed below:

```
Interface Dialer0
ip address negotiated
ip nat outside
encapsulation ppp
dialer pool 1
ppp chap hostname 827-x@Certkiller.com
ppp chap password Certkiller
```

What is missing under the Interface Dialer0 configuration of CK1 ?

- A. Request-dialin
- B. Request-dialout
- C. IP mtu 1492
- D. IP mtu 1500
- E. DSL operating-mode auto
- F. Protocol pppoe

Answer: C

Explanation:

When a host (usually a PC) initiates a TCP session with a server, it negotiates the IP segment size by using the MSS option field in the TCP SYN packet. The value of the MSS field is determined by the maximum transmission unit (MTU) configuration on the host. The default MSS value for a PC is 1500 bytes. The PPP over Ethernet (PPPoE) standard supports a MTU of only 1492 bytes. The disparity between the host and PPPoE MTU size can cause the router in between the host and the server to drop 1500-byte packets and terminate TCP sessions over the PPPoE network. Even if the path MTU (which detects the correct MTU across the path) is enabled on the host, sessions may be dropped because system administrators sometimes disable the ICMP error messages that must be relayed from the host in order for path MTU to work.

The "ip tcp adjust-mss" command helps prevent TCP sessions from being dropped by adjusting the MSS value of the TCP SYN packets.

The "ip tcp adjust-mss" command is effective only for TCP connections passing through the router.

In most cases, the optimum value for the max-segment-size argument is 1452 bytes. This value plus the 20-byte IP header, the 20-byte TCP header, and the 8-byte PPPoE header add up to a 1500-byte packet that matches the MTU size for the Ethernet link.

If you are configuring the ip mtu command on the same interface as the ip tcp adjust-mss command, it is recommended that you use the following commands and values:

```
ip tcp adjust-mss 1452
```

```
ip mtu 1492
```

The ip tcp adjust-mss command does not work on subinterfaces or GRE tunnels.

Example:

The following example shows the configuration of a PPPoE client with the MTU value set to 1492:

```
vpdn enable no vpdn logging! vpdn-group 1 request-dialin protocol pppoe! interface
Ethernet0 ip address 192.168.100.1 255.255.255.0 ip tcp adjust-mss 1452 ip nat inside!
interface ATM0 no ip address no atm ilmi-keepalive pvc 8/35 pppoe client
dial-pool-number 1! dsl equipment-type CPE dsl operating-mode GSHDSL symmetric
annex B dsl linerate AUTO! interface Dialer1 ip address negotiated ip mtu 1492 ip nat
outside encapsulation ppp dialer pool 1 dialer-group 1 ppp authentication pap callin ppp
pap sent-username sohodyn password 7 141B1309000528! ip nat inside source list 101
Dialer1 overload ip route 0.0.0.0 0.0.0.0 Dialer1 access-list permit ip
192.168.100.0 0.0.0.0 255 any
```

QUESTION 210:

Certkiller .com would like to provide VPN security between its remote sites. After reviewing the Certkiller .com requirements, you recommend that the Certkiller should protect the entire original IP packet by encrypting it and encapsulating it inside a new, unencrypted IP header. The unencrypted header will be used to route the packet through the Internet.

Which mode will accomplish this?

- A. IPSec Mode
- B. Transport Mode
- C. Channel Mode
- D. Tunnel Mode
- E. Host-to-host Mode
- F. Protect Mode

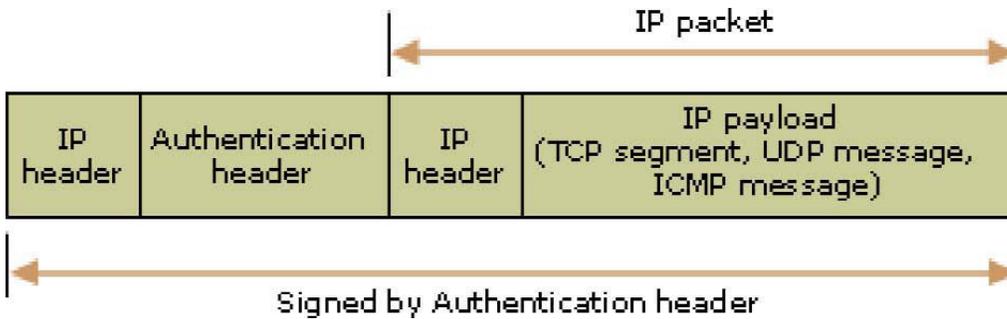
Answer: D

Explanation:

Tunnel mode provides the protection of an entire IP packet by treating it as an AH or ESP payload. With tunnel mode, an entire IP packet is encapsulated with an AH or ESP header and an additional IP header. The IP addresses of the outer IP header are the tunnel endpoints, and the IP addresses of the encapsulated IP header are the ultimate source and destination addresses.

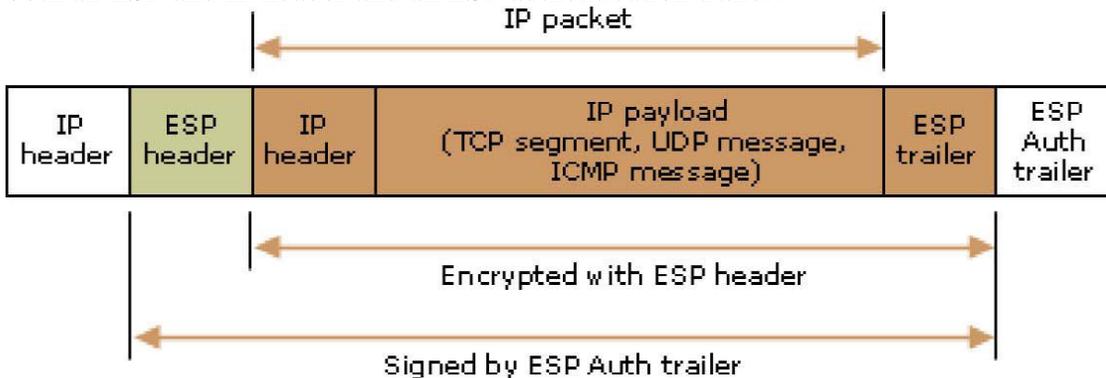
AH tunnel mode

As shown in the following illustration, AH tunnel mode encapsulates an IP packet with an AH and IP header and signs the entire packet for integrity and authentication.



ESP tunnel mode

As shown in the following illustration, ESP tunnel mode encapsulates an IP packet with both an ESP and IP header and an ESP authentication trailer.



The signed portion of the packet indicates where the packet has been signed for integrity and authentication. The encrypted portion of the packet indicates what information is protected with confidentiality.

Because a new header for tunneling is added to the packet, everything that comes after the ESP header is signed (except for the ESP authentication trailer) because it is now encapsulated in the tunneled packet. The original header is placed after the ESP header. The entire packet is appended with an ESP trailer before encryption occurs. Everything that follows the ESP header, except for the ESP authentication trailer, is encrypted. This includes the original header which is now considered to be part of the data portion of the packet.

Reference:

http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sag_ipsec_und11.msp

QUESTION 211:

What happens to the NAT translation table entries when the command "clear ip nat trans *" is entered on one of the Certkiller routers?

- A. It clears static NAT translation entries and NAT resumes.
- B. It clears dynamic NAT translation table entries and NAT resumes.
- C. It clears all existing NAT translation table entries and NAT is suspended.
- D. It clears all inactive NAT translation entries and NAT is suspended.
- E. None of the above

Answer: B

Explanation:

The following describes the various NAT clearing commands and their uses:

clear ip nat trans* - Clears all dynamic translation entries.

clear ip nat trans inside global-ip local-ip [outside local-ip global-ip] - Clears a simple translation entry containing an inside translation, or both an inside and outside translation.

clear ip nat trans outside local-ip global-ip - Clears a simple translation entry containing an outside translation.

clear ip nat trans protocol inside global-ip global-port local-ip local-port [outside local-ip local-port global-ip globalport] - Clears an extended entry (in its various forms).

Clearing NAT Translation Entries

```

Router#sh ip nat trans
Pro Inside global      Inside local      Outside local      Outside global
tcp 192.168.2.1:11003  10.1.1.1:11003   172.16.2.2:23     172.16.2.2:23
tcp 192.168.2.1:1067   10.1.1.1:1067   172.16.2.3:23     172.16.2.3:23
Router#clear ip nat trans *
Router#
Router#show ip nat trans

```

→ All entries are cleared.

```

Router#show ip nat transPro Inside global      Inaide local      Outside
local      Outside global
udp 192.168.2.2:1220  10.1.1.2:1120   171.69.2.132:53   171.69.1.132:53
tcp 192.168.2.1:11003  10.1.1.1:11003  172.16.2.2:23     172.16.2.2:23
tcp 192.168.2.1:1067  10.1.1.1:1067  172.16.2.3:23     172.16.2.3:23
Router#clear ip nat trans udp inside 192.168.2.2 10.1.1.2 1220
171.69.2.132 53 171.69.1.132 53
Router#show ip nat trans
Pro Inside global      Inside local      Outside local      Outside global
tcp 192.168.2.1:11003  10.1.1.1:11003   172.16.2.2:23     172.16.2.2:23
tcp 192.168.2.1:1067  10.1.1.1:1067   172.16.2.3:23     172.16.2.3:23

```

→ 192.168.2.2 is cleared.

© 2006, Cisco Systems, Inc. www.cisco.com SCRAA v1.1-16-10

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 14-23

QUESTION 212:

The NAT table of one of the Certkiller routers is displayed below:

```

CertkillerRouter#sh ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
tcp  78.37.71.213:1249  192.168.1.105:1249  80.15.249.113:80  80.15.249.113:80
tcp  78.37.71.213:2898  192.168.1.104:2898  205.188.228.17:554  205.188.228.17:554
udp  78.37.71.213:500    192.168.1.103:500   171.70.192.90:500  171.70.192.90:500
tcp  78.37.71.213:1161  192.168.1.105:1161  143.1.78.83.22:80  143.1.78.83.22:80
tcp  78.37.71.213:1252  192.168.1.104:1252  63.208.194.103:443  63.208.194.103:443
udp  78.37.71.213:10000  192.168.1.103:10000  171.70.192.90:10000  171.70.192.90:10000
tcp  78.37.71.213:1064  192.168.1.105:1064  206.65.183.95:80   206.65.183.95:80
udp  78.37.71.213:5060  192.168.1.15:5060   12.144.47.27:5060  12.144.47.27:5060
tcp  78.37.71.213:1142  192.168.1.105:1142  143.1.78.224.27:80  143.1.78.224.27:80
tcp  78.37.71.213:1146  192.168.1.105:1146  143.1.78.224.27:80  143.1.78.224.27:80

```

Based on this information, what is true about the command output above?

- A. It reflects basic IP address translation.
- B. It reflects how one inside host is seen as four different hosts to the outside world.
- C. It reflects IP address translation with overloading.
- D. It reflects no active translations.
- E. None of the above.

Answer: C

Explanation:

Cisco defines these terms as follows:

Inside local address - The IP address assigned to a host on the inside network. This is the address configured as a parameter of the computer's OS or received via dynamic address allocation protocols such as DHCP. The address is likely not a legitimate IP address assigned by the Network Information Center (NIC) or service provider.

Inside global address - A legitimate IP address assigned by the NIC or service provider that represents one or more inside local IP addresses to the outside world.

Outside local address - The IP address of an outside host as it appears to the inside network. Not necessarily a legitimate address, it is allocated from an address space routable on the inside.

Outside global address - The IP address assigned to a host on the outside network by the host's owner. The address is allocated from a globally routable address or network space. In this example, we can see that the IP address used for translating the inside hosts to the outside is the "inside global" address. This NAT table displays port information, and multiple entries with only the single IP address 78.37.71.213 being used. Because of this, PAT, or many to one, NAT is being used, which means that NAT with the keyword "overload" was configured.

References: CCNP Remote Access Exam Certification Guide, pages 350-351, Brian Morgan & Craig Dennis, Cisco Press 2001, ISBN 1-58720-003-1

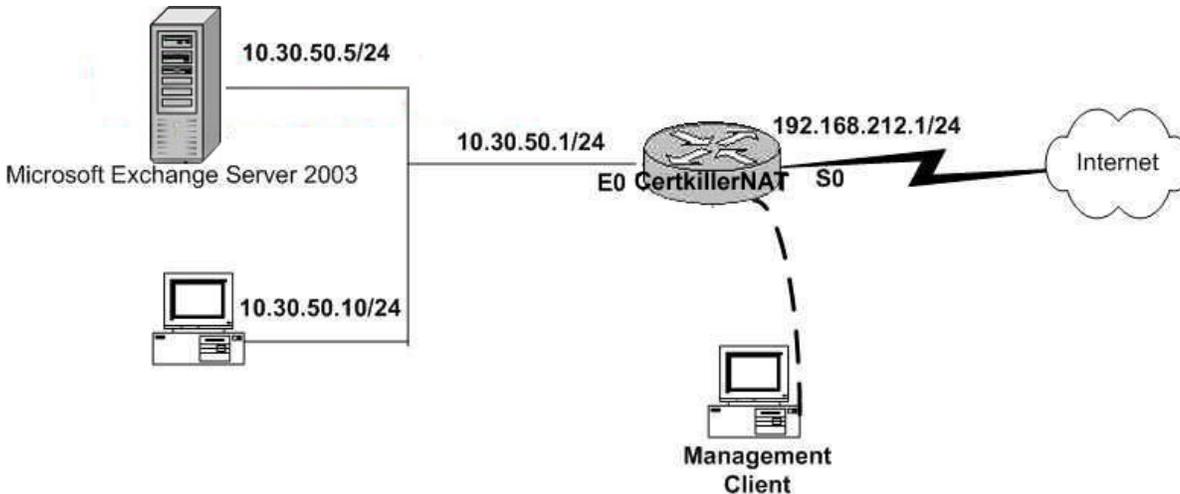
http://www.cisco.com/en/US/tech/CK648/CK361/technologies_tech_note09186a0080094837.shtml

QUESTION 213:

SIMULATION

The Certkiller network is displayed below:

642-821



Certkiller .com is in the process of updating their network. They're going to change their internet service provider, install a local E-mail server, and install Microsoft Exchange Server 2003. The new ISP has allocated Certkiller .com a new Class C address range. However, the addresses of the internal routers and servers are to be kept intact. So you are to configure the router for NAT so the internal clients can use a single external IP address assigned to the public router interface. Finally you want Microsoft Exchange Server 2003 to be Internet accessible, so you have to provide a static translation for it.

Your task is to configure the router for this using the following information:

Certkiller NAT

S0: 192.168.212.1/24

E0: 10.30.50.1/24

Secret password: Certkiller

Answer:

```
Certkiller NAT#config t
```

```
Certkiller NAT(config)#access-list 5 permit 10.30.50.0 0.0.0.255
```

```
Certkiller NAT(config)# ip nat inside source list5 interface s0 overload
```

```
Certkiller NAT(config)#ip nat inside source static 10.30.50.5 192.168.212.5
```

```
Certkiller NAT(config)#int s 0
```

```
Certkiller NAT(config-if)#ip nat outside
```

```
Certkiller NAT(config-if)#exit
```

```
Certkiller NAT(config)#int e 0
```

```
Certkiller NAT(config-if)#ip nat inside
```

```
Certkiller NAT(config-if)#<Ctrl-Z>
```

```
Certkiller NAT#copy running start
```

```
Certkiller NAT#
```

Incorrect Answer:

```
Certkiller NAT#config t
```

```
Certkiller NAT(config)#access-list 5 permit 10.30.50.0 0.0.0.255
```

```
Certkiller NAT(config)#ip nat pool lan 192.168.212.1 192.168.212.1 netmask 255.255.255.0
```

```
Certkiller NAT(config)#ip nat inside source list 5 pool lan overload
```

```
Certkiller NAT(config)#ip nat inside source static 10.30.50.5 192.168.212.5
Certkiller NAT(config)#int s 0
Certkiller NAT(config-if)#ip nat outside
Certkiller NAT(config-if)#exit
Certkiller NAT(config)#int e 0
Certkiller NAT(config-if)#ip nat inside
Certkiller NAT(config-if)#<Ctrl-Z>
Certkiller NAT#copy running start
Certkiller NAT#
```

QUESTION 214:

You need to configure NAT on the interfaces of the CK1 router. Which router interface command would you use to enable NAT on an inside interface?

- A. ip nat inside
- B. ip nat map inside
- C. ip nat permit inside
- D. ip address inside

Answer: A

Explanation:

When you are configuring NAT, NAT should be enabled on at least one inside and one outside interface. The command for enabling NAT on inside interface is:

```
R(config-if)# ip nat inside
```

The command for enabling NAT on the outside interface is:

```
R(config-if)# ip nat outside
```

Remember to enter into appropriate configuration modes before entering the commands. Usually, the inside NAT will be configured on an Ethernet interface, whereas the outside NAT is configured on a serial interface. The command `ip nat inside source static <local ip> <global ip>` configures address translation for static NAT. The command `ip nat inside source list <access-list-number> pool <name>` is used to map the access-list to the IP NAT pool during the configuration of Dynamic NAT.

QUESTION 215:

What do network administrators often fail to consider when implementing NAT TCP load distribution?

- A. It is enabled with the type rotary parameter on the ip nat pool command.
- B. It is enabled by mapping multiple outside addresses to an inside address.
- C. It is configured with the overload parameter on the ip nat inside command.
- D. It requires an access list that permits an outside address to a group of inside local addresses.
- E. All of the above.

Answer: D

Explanation:

TCP load distribution - A dynamic form of destination translation can be configured for some outside-to-inside traffic. When a mapping scheme is established, destination addresses matching an access list are replaced with an address from a rotary pool.

Allocation is done on a round-robin basis, and only when a new connection is opened from the outside to the inside. All non-TCP traffic is passed un-translated (unless other translations are in effect).

NAT requires an access-list that permits the outside address to the pool of inside local addresses. NST uses a single outside IP address, not multiple outside IP addresses. Furthermore, this single outside IP address can be translated to a pool of internal IP addresses. The ip nat pool command defines a pool of IP addresses for NAT. It does not enable NAT. The ip nat inside command enables NAT of the inside destination address. NAT is not configured by this command.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 14-19

[QUESTION 216:](#)

A Certkiller ADSL router is configured as shown below:

```
hostname 827-x
|
vpdn enable
|
vpdn-group pppoe
request-dialin
protocol pppoe
|
interface Ethernet0
ip address 10.0.0.1 255.0.0.0
ip nat inside
|
Interface ATM0
no ip address
no atm ilmi-keepalive
pvc 3/34
pppoe-client dial-pool-number 1
|
bundle-enable
dsl operating-mode auto
|
Interface Dialer0
ip address negotiated
ip mtu 1492
encapsulation ppp
dialer pool 1
ppp chap hostname 827-x@cisco.com
ppp chap password cisco
|
ip route 0.0.0.0 0.0.0.0 Dialer0
|
ip nat inside source list 101 interface Dialer0 overload
access-list 101 permit ip 10.0.0.0 0.255.255.255 any
```

Refer to the display configuration.

The 827 ADSL router is supposed to be setup as a PPPoE client. The user PCs behind the 827 are having Internet connectivity issues.

What could be the cause of the problem?

- A. The vpdn-group pppoe configuration is not correct.
- B. The port address translation (PAT) configuration is not correct.
- C. The access-list 101 configuration is not correct.
- D. For interface Dialer0, the IP MTU size should be 1500.
- E. The default static route should be pointing to the ATM0 interface.

Answer: B

Explanation:

In the above configuration, the problem is the fact that a NAT statement is missing.

Under the Dialer 0 interface, the command "ip nat outside" should have been configured.

For NAT to operate properly, one or more interfaces must be configured for the inside (or trusted side, in the case) and one or more interfaces need to be specified as outside (untrusted side on this DSL connection).

QUESTION 217:

Under PAT, packets destined for the outside world have their private IP address plus port number translated to the router's external IP address _____ the IP packet is forwarded to the WAN.

- A. None of the choices.
- B. Port number should not be included in the equation
- C. Port number should not be included in the translation, but should be forwarded
- D. Before
- E. After

Answer: D

Explanation:

Packets destined for an external address have their private IP address plus port number translated to the router's external IP address before the IP packet is forwarded to the WAN. IP packets returning to the router have their external IP addresses (plus port number) translated back to the private IP addresses, and the packets are forwarded to the LAN.

QUESTION 218:

In a North American commercial network environment; what kind of interface will you use to connect an asynchronous serial modem to a router or an end station?

- A. HSSI (High Speed Serial Interface)
- B. X.21
- C. RS-449
- D. EIA/TIA-232-C

Answer: D

Explanation:

The RS-232-C interface is a recommended standard (RS) interface established by the Electronic Industries Association (EIA). (Also known as EIA/TIA-232)

The standard defines the specific electrical, functional, and mechanical characteristics used in asynchronous transmissions between a computer (data terminal equipment, or DTE) and a peripheral device (data communications equipment, or DCE). RS is the abbreviation for recommended standard, and the C denotes the third revision of that standard. RS-232-C is compatible with the CCITT V.24 and V.28 standards, as well as ISO IS2110.

RS-232-C uses a 25-pin or 9-pin DB connector. The accompanying illustration shows the pinouts used in a DB-25 male connector. It is used for serial communications between a computer and a peripheral device, such as a printer, modem, or mouse. The maximum cable limit of 15.25 meters (50 feet) can be extended by using high-quality cable, line

drivers to boost the signal, or short-haul modems.

Reference: <http://www.warknite.com/books/dictionary/Terms/2461HTML-2483.html>

QUESTION 219:

In an asynchronous interface, what purpose do chat scripts serve?

- A. Informing the router as to which modem type is attached to the asynchronous interface.
- B. Send messages from one Telnet session to another.
- C. Synchronize the serial DDR.
- D. Initialize the directly attached modem.

Answer: A

Explanation:

A chat script is a one-line command that is used on an asynchronous interface to send commands for modem dialing and for logging on to remote systems. Chat scripts indicate the possible responses to expect and the information to send in each case. You can create a different chat script for each type of modem in use on the router and for each system the router might need to log in to.

Chat scripts are required for dialing out on the asynchronous interface on the router's auxiliary port, but are also used on other asynchronous interfaces on access servers.

Chat scripts are strings of text used to send commands for modem dialing, logging onto remote systems, and initializing asynchronous devices connected to an asynchronous line. On a router, chat scripts can be configured on the auxiliary port only. A chat script must be configured to dial out on asynchronous lines. You also can configure chat scripts so that they are executed automatically for other specific events on a line, or so that they are executed manually. Each chat script is defined for a different event. These events can include the following:

Line activation

Incoming connection initiation

Asynchronous dial-on-demand routing

Line resets

Startup

References:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgr/dial_c/dcasddr.htm

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgr/dial_c/dcmodem.htm#5148

QUESTION 220:

You're at a computer supply warehouse and you find an EIA/TIA-232 null modem cable with a DB25 connector. Ordinarily, two of the pins are cross connected on this cable. Which two are they? (Choose two)

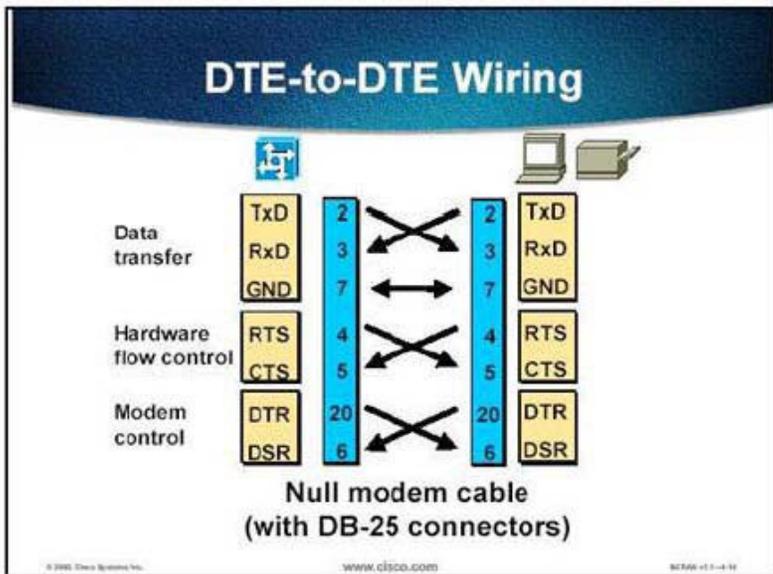
- A. Pin 2

- B. Pin 3
- C. Pin 4
- D. Pin 5
- E. Pin 7
- F. Pin 8

Answer: A, B

Explanation:

When two DTE devices (for example, an access server and a terminal) are near each other, it makes sense to connect them directly without going through a telephone network and two modems. An ordinary EIA/TIA-232 cable will not work in this case because both DTE devices transmit on the TxD lead (pin 2), and both expect input on the RxD lead (pin 3). A "null modem cable" is required for the DTE-to-DTE connection. Null modems crisscross DB-25 pins 2 and 3 and other corresponding pins (as shown in the figure) so that the two DTE devices can communicate. Some devices can be configured to operate either like a DTE or a DCE. Configuring a device as a DCE usually means that it receives data on pin 2 and transmits data on pin 3. For example, many serial printers are configured as DCE devices so they can be connected directly to a DTE (for example, a PC or a terminal server) with an ordinary EIA/TIA-232 cable, eliminating the need for a null modem connection.



Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 4-10

QUESTION 221:

Which of the following modem standards includes the 'quick connect' and 'modem on hold' specifications?

- A. V.92
- B. V.32bis

- C. V.22
- D. V.90
- E. V.34
- F. None of the above

Answer: A

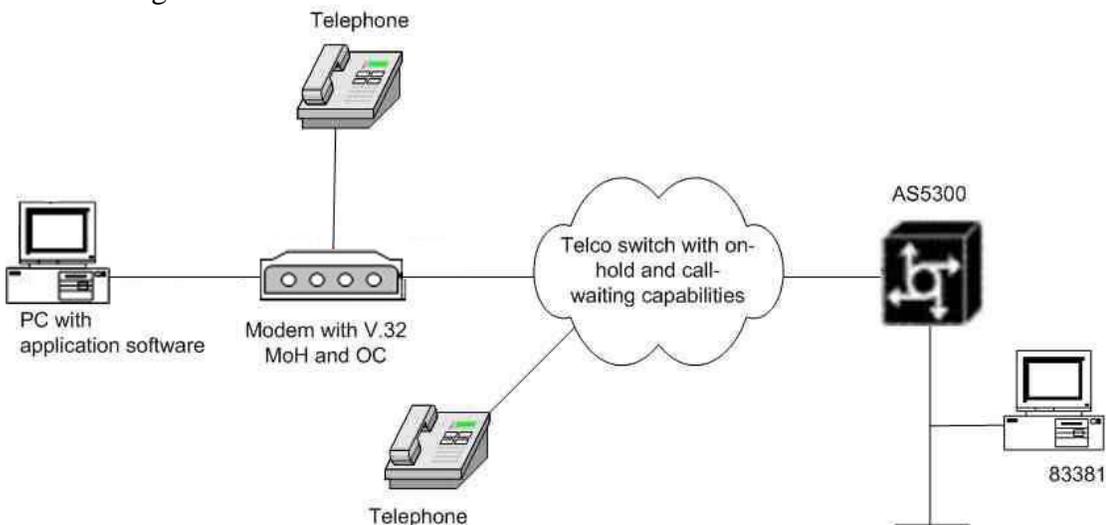
Explanation:

What V.92 is supposed to offer?

Increased upstream rates - up to 48k by using a PCM stream through an a/d conversion. [Still, only 1 a/d conversion is required: if you have trouble getting 56k rates with V.90, there will be no improvement.] As of September, 2003, most server-side modems do not support PCM upstream at all, and those that do - 3Com & Patton - support a maximum upstream rate of 33.3kbps - less than the maximum V.34 upstream! Modem on Hold-V.92 Modem on Hold allows a dial-in customer to suspend a modem session to answer an incoming voice call or to place an outgoing call while engaged in a modem session. When the dial-in customer uses Modem on Hold to suspend an active modem session to engage in an incoming voice call, the Internet service provider (ISP) modem listens to the original modem connection and waits for the dial-in customer's modem to resume the connection. When the voice call ends, the modem signals the telephone system to end the second call and return to the original modem connection, then the modem signals the ISP modem that it is ready to resume the modem call. Both modems renegotiate the connection, and the original exchange of data continues.

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ft92mmh1.htm#10228>

Quick Connect - The time to establish a connection may be reduced with faster handshaking.V.92 Quick Connect speeds up the client-to-server startup negotiation, reducing the overall connect time up to 30 percent. The client modem retains line condition information and characteristics of the connection to the Internet service provider (ISP), which reduces connect time by avoiding some of the initial signal handshaking.



http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xa/122xa_2/ft92m

QUESTION 222:

In an asynchronous remote access network; the end devices are known as data terminal equipment (DTE) and they communicate through data circuit-terminating equipment (DCE). What kind of modem signal does a DCE use to transmit data?

- A. RTS
- B. RD
- C. CTR
- D. TD
- E. All of the above

Answer: B

Explanation:

With a 25-pin connector (DB-25), only 8 pins are actually used for connecting a DTE (for example, an access server) to a DCE (for example, a modem). The other 17 signals are not "interesting" and are ignored. The eight interesting signals can be grouped into three categories by their functionality: data transfer, hardware flow control, and modem control. The figure shows the data transfer group, as follows:

1. TxD-Transmit Data. The DTE transmits data to the DCE.
2. RxD-Receive Data. The DTE receives data from the DCE.
3. GRD (pin 7)-Ground. Provides the ground reference for voltage measurements.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 4-7

QUESTION 223:

When a modem is powered up, what does it do to notify the connected computer that the DCE is ready to use?

- A. The modem sets DTE pin 4.
- B. The modem sets DTR pin 20.
- C. The modem sets DSR pin 6.
- D. The modem sets DCE pin 5.
- E. The modem sets DTR pin 3.
- F. None of the above

Answer: C

Explanation:

Modem control consists of several signals between the DTE and DCE that are used to initiate, terminate, and monitor the status of the connection. This figure shows the remaining two groups of interesting signals between a DTE device and a DCE device, as follows:

Hardware flow control:

1. RTS - Request To Send. The DTE has buffers available to receive from the DCE.
2. CTS - Clear To Send. The DCE has buffers available to take data from the DTE.

Modem control:

1. DTR - Data Terminal Ready. The DTE indicates to the DCE that it can accept an incoming call.
2. CD - Carrier Detect (also referred to as Data Carrier Detect [DCD]). The DCE has established a carrier signal with the remote DCE.
3. DSR (pin 6) - Data Set Ready. The DCE is ready for use. This pin is not used on modem connections.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 4-7

QUESTION 224:

You're teaching a lesson on asynchronous modems at the CertKiller academy, and you're explaining how the DCE and DTE signal between each other. Suddenly one of your students stands up and asks what happens when the signal on the DTR is lost. What is the correct answer?

- A. The CD tells the DTE that a DCE-to-DCE connection has been established.
- B. The DTE applies voltage on pin 20 to alert the DCE that it is connected and available to receive data.
- C. The DCE terminates its connection with the remote modem.
- D. The DTE issues a RTS to the DCE enabling communication.

Answer: C

Explanation:

Either the DTE device or the DCE device may signal for the connection to be terminated. The signals that are used for this function are DTR from the DTE or the modem recognizing the loss of the CD signal.

Modem Control Example

Two ways to terminate an existing connection:

- **DTE-initiated** 
 - Access server drops DTR
 - Modem must be programmed to terminate connection on loss of DTR and restore to saved settings in its NVRAM
- **DCE-initiated** 
 - Access server detects Carrier Detect (CD) low and terminates connection
 - Modem must be programmed so that CD reflects the state of the carrier

© 1995, Cisco Systems, Inc. www.cisco.com SCRAP v1.1-44

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 4-8

QUESTION 225:

CORRECT TEXT

After completing the line configuration commands for one of the Certkiller routers, you need to get back into global configuration mode. What command do you use to exit line configuration mode and return to global configuration mode? (Type in answer below)

Answer: exit

Explanation:

To exit line configuration mode and return to global configuration mode, use the exit command. To exit line configuration mode and return to privileged EXEC mode, enter the end command, or press Ctrl-Z.

QUESTION 226:

A new modem is being attached to router CK1 . On this connection, what prevents the speed between the modem and the DTE from being varied?

- A. The modem attribute syn DTE
- B. The modem attribute static DTE
- C. The modem attribute lock DTE
- D. The modem attribute fixed DTE

Answer: C

Explanation:

The lock DTE speed command, which might also be referred to as port rate adjust or buffered mode, is often related to the way in which the modem handles error correction. This command varies widely from one modem to another. Locking the modem speed ensures that the modem always communicates with the Cisco access server or router at the speed configured on the Cisco auxiliary port. If this command is not used, the modem reverts to the speed of the data link (the telephone line), instead of communicating at the speed configured on the access server.

QUESTION 227:

What signal is used by DTE to indicate that it is willing to accept a call, according to the RS232 standard?

- A. RTS
- B. DTR
- C. CTS
- D. ETA
- E. DSR
- F. DCD
- G. FTS

Answer: B

Explanation:

RS232C is a communications port standard

RS232C separates equipment into Data Terminal Equipment (DTE) and Data Communication Equipment (Modems) (DCE). This is rather simplistic, as it always assumes that you will connect a modem to a terminal, however the use of the serial connection has extended somewhat since those days.

It defines the meanings of the signals, but not the type of connector, nor the pins on which each signal appears. Despite that, the 25 pin (and 9 pin) D connectors on an IBM compatible personal computer are generally accepted as a sort of standard for the pins, so I'll use these as examples.

The popular names of the lines tend to be as follows:

D25 D9 Name

PG 1 Protective Ground

SG 7 Signal Ground

TxD 2 (DTE) Data transmitted by DTE to DCE

RxD 3 (DCE) Data received by DCE

RTS 4 (DTE) "Request to Send" Start transmitter

CTS 5 (DCE) "Clear to Send" Have started transmitter

DSR 6 (DCE) "Data Set Ready" Modem ready to work

DCD 8 (DCE) "Data Carrier Detect" Remote transmitter is active

DTR 20 (DTE) "Data Terminal Ready" DTE indicates DCE may go off-hook
RI 22 (DCE) "Ring Indicator" DCE says a remote DCE has called
DTE uses the RTS output signal to indicate if it can receive characters into the Rx input buffer. The DCE should not send data to the DTE when DTR input is low (no RTS).
Reference: <http://www.ericlindsay.com/computer/rs232.htm>

QUESTION 228:

Which of the following is true concerning the nature of hardware flow control (Choose all that apply)?

- A. It uses CTS for Clear To Stop
- B. It uses RTS for Request To Send
- C. It uses RTS for Request To Stop
- D. It uses CTS for Clear To Send

Answer: B, D

Explanation:

The popular names of the lines and their meanings are as follows:

RTS: Request to Send - Start transmitter - DTE

CTS: Clear to Send - Have started transmitter - DCE

DSR: Data Set Ready - Modem ready to work - DCE

DCD: Data Carrier Detect - Remote transmitter is active - DCE

DTR: Data Terminal Ready - DTE

RI: Ring Indicator - DCE

QUESTION 229:

Your colleague at Certkiller Inc. is trying to setup an ISDN line to use as a backup for his Frame Relay correction. What is true about his configuration shown below?

```
interface serial0
ip address 192.168.10.1 255.255.255.0
backup interface bri0
backup delay 5 10
interface bri0
ip address 192.168.11.2 255.255.255.0
dialer idle-timeout 900
dialer-group 1
dialer-group 1 protocol ip permit
```

- A. The ISDN BRI line will be in "standby" mode after 900 seconds once the serial interface activates again.
- B. The ISDN BRI line will be in "standby" mode after 10 seconds but will be in "up/ip" mode after 900 seconds once the serial interface activates again.
- C. The ISDN BRI line will be in "standby" mode after 10 seconds and will be in

"standby" mode after 900 seconds once the serial interface activates again.
D. The ISDN BRI line will be in "standby" mode after 10 seconds once the serial interface activates again.

Answer: C

Explanation:

The specific commands used in this configuration are explained below:

backup interface bri0 = backup interface interface-type number

backup delay 5 10 = backup delay {enable-delay | never}
{disable-delay | never}

enable-delay = Number of seconds that elapse after the primary line goes down before the Cisco IOS software activates the secondary line.

disable-delay = Number of seconds that elapse after the primary line comes up before the Cisco IOS software deactivates the secondary line.

never prevents the secondary line from being activated or deactivated.

dialer idle-timeout 900 = dialer idle-timeout seconds

Specifies the time that the line can remain idle before it is disconnected, with the default time is 120 seconds. In this case, when the serial interface again becomes active, the ISDN call will be dropped after 900 seconds.

Activating Dial Backup for Line Failures

```
Router(config-if)#backup interface interface-type number
```

- Specifies the backup interface

```
Router(config-if)#backup delay {enable-delay | never}  
{disable-delay | never}
```

- Designates when to activate the backup line if a primary line fails

© 1998 Cisco Systems, Inc. www.cisco.com B0844 v1.1-02

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 4-21

QUESTION 230:

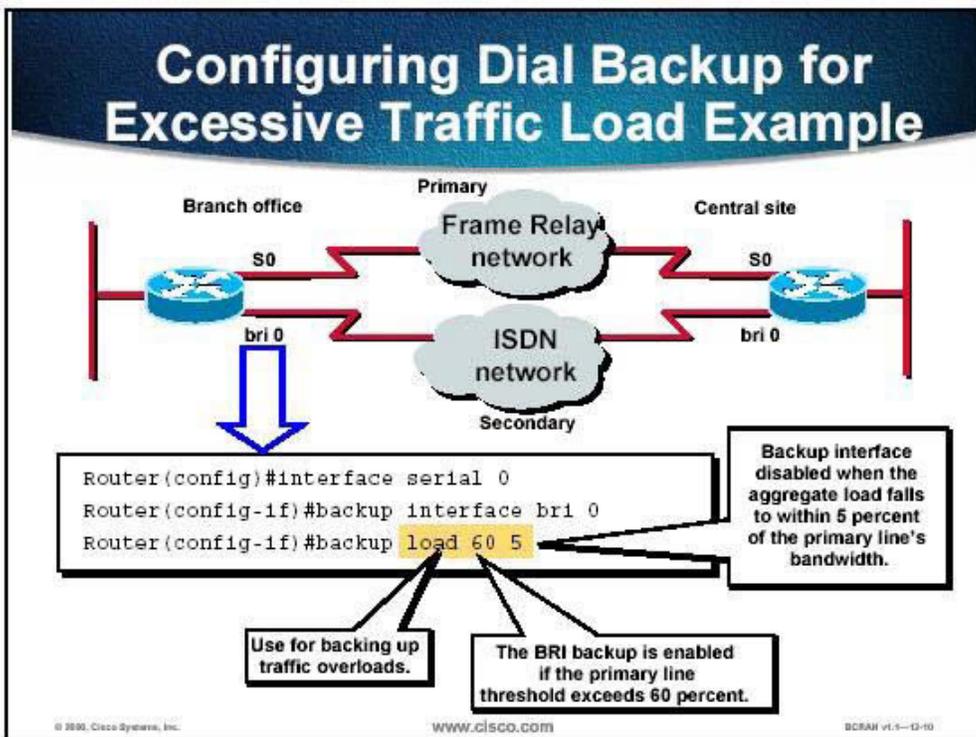
An administrator has just issued the command "backup load 60 5" on one of the Certkiller ISDN routers. What is the result of this configuration command? (Choose all that apply)

- A. The backup link activates when the primary link exceeds 60 percent of bandwidth.
- B. The backup link deactivates when the combined load falls to 4 kbps.
- C. The backup link deactivates when the primary link falls to 5 percent bandwidth.
- D. The backup link deactivates when the combined load falls to 5 percent bandwidth.
- E. The backup link activates when the primary link exceeds 60 kbps.

Answer: A, D

Explanation:

The backup load 60 5 command sets the traffic threshold to 60 percent of the primary line serial 0. When the load is exceeded, the secondary line is activated, and will not be deactivated until the combined load is less than 5 percent of the primary bandwidth.



Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Chapter 12-13

QUESTION 231:

Which command would you use to configure your backup interface to activate itself and 'kick in' when bandwidth utilization reaches 75% of the maximum bandwidth on the primary link?

- A. backup load 75 5
- B. backup delay load 3/4
- C. backup delay 75 0

- D. bandwidth demand .75%
- E. demand 75
- F. None of the above

Answer: A

Explanation:

The backup load 75 5 command specifies that the router should monitor the load on the primary interface and bring the link up when the load across the primary link is particularly heavy. The numbers represent the load on the interface, as shown by the show interface s0 command.

The load on an interface is represented by a number between 1 and 255. In the backup load 75 5 command, 75 is the percentage load at which the backup link is activated (in this case, 191/255).

The second number (in this case, 5%) is a measurement of aggregate load. Once the backup link has been initialized, the router continues to monitor the load. Once the load of both interfaces combined reaches a value of 13/255, the secondary link is terminated. So, although dial backup was designed for link redundancy to partially compensate for primary link failure, it can also provide load-sharing capabilities to alleviate congestion on the WAN link.

Reference:

Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)
Page 319

QUESTION 232:

What kind of terminals can you connect an ISDN line to? (Choose all that apply.)

- A. NU1
- B. TE2/TA
- C. TE1
- D. TO2
- E. NT0
- F. None of the above

Answer: B, C

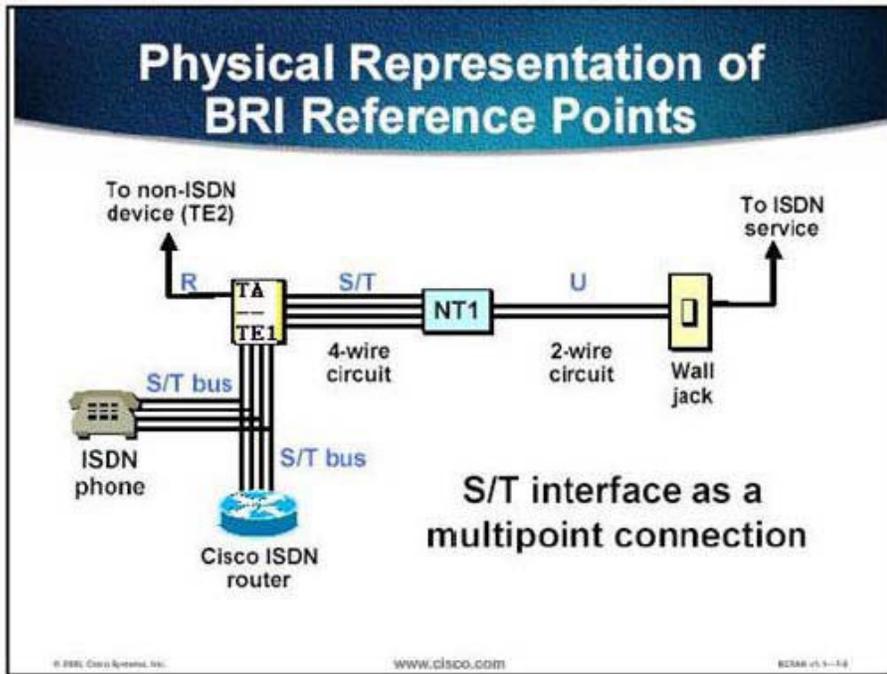
Explanation:

Terminal equipment 1 (TE1) - Designates a device that is compatible with the ISDN network. A TE1 connects to a network termination of either type 1 or type 2 (NT1 or NT2). For example:

1. Digital telephone
2. Router with ISDN interface
3. Digital facsimile equipment

Terminal equipment 2 (TE2) - Designates a device that is not compatible with ISDN and requires a terminal adapter. For example:

1. Terminals with X.21, Electronic Industries Association/ Telecommunications Industry Association (EIA/TIA)-232, or X.25 interfaces
 2. Router without ISDN interface (AGS+ and so on)
- Terminal adapter (TA) - Converts standard electrical signals into the form used by ISDN so that non-ISDN devices can connect to the ISDN network. For example: to convert V.35 or EIA/TIA-232 to ISDN (analog to ISDN).



Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 7-12

QUESTION 233:

Under which of the following circumstances would an ISDN BRI circuit be considered as a viable remote access solution?

- A. A branch office needs to connect to a mobile user.
- B. A mobile user that needs access to the central site while traveling.
- C. A remote site with sporadic traffic needs to connect to central site.
- D. A branch office requires at least 300kbps bandwidth to the central site.
- E. A mobile user that needs access at the branch office.

Answer: C

Explanation:

Basic Rate Interface (BRI) is an Integrated Systems Digital Network (ISDN) interface, and it consists of two B channels (B1 and B2) and one D channel. The B channels are used to transfer data, voice, and video. The D channel controls the B channels. ISDN uses the D channel to carry signal information. ISDN can also use the D channel in a BRI to carry X.25 packets. The D channel has a capacity of 16 kbps, and the X.25 over

D channel can utilize up to 9.6 kbps.

When this feature is configured, a separate X.25-over-D-channel logical interface is created. You can set its parameters without disrupting the original ISDN interface configuration. The original BRI interface will continue to represent the D, B1, and B2 channels.

Because some end-user equipment uses static terminal endpoint identifiers (TEIs) to access this feature, static TEIs are supported. The dialer understands the X.25-over-D-channel calls and initiates them on a new interface.

X.25 traffic over the D channel can be used as a primary interface where low-volume, sporadic interactive traffic is the normal mode of operation. Supported traffic includes IPX, AppleTalk, transparent bridging, XNS, DECnet, and IP. This feature is not available on the ISDN Primary Rate Interface (PRI).

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1826/products_configuration_guide_chapter09186a00800d

QUESTION 234:

One of the Certkiller locations is using ISDN to backup their primary frame relay link. In an ISDN BRI network, what term is used to describe the device where the local loop terminated at?

- A. LE
- B. TA
- C. TE2
- D. NT1
- E. None of the above

Answer: D

Explanation:

In ISDN, the NT1 where your local loop terminates and the telephone company's loop begins.

"One important piece of equipment in any ISDN BRI installation is an NT1. The NT1 is a device similar to a channel service unit/data service unit (CSU/DSU), which is used in serial connections. The NT1 terminates the local loop....."

The NT1 has at least two interfaces: an S/T interface jack and a U interface. The S/T interface is attached to the router's BRI interface. The U interface is attached to the telco jack....."

Reference: CCNP Remote Access Exam Certification Guide, page 132, Brian Morgan & Craig Dennis, Cisco Press 2001, ISBN 1-58720-003-1

QUESTION 235:

DRAG DROP

Match the T1/E1 PRI module LED meanings, to the correct warning indications on

the right.

Select from these

LA

CD

LP

AL

RA

Place here

Alarm indicating loss of signal, loss of frame, or unavailability because of excessive errors.

Controller local loopback.

Carrier received on telco link.

Local alarm at remote end of connection

Loss of signal, loss of frame, or unavailability because of excessive errors.

Answer:

Select from these

Place here

AL

Alarm indicating loss of signal, loss of frame, or unavailability because of excessive errors.

LP

Controller local loopback.

CD

Carrier received on telco link.

RA

Local alarm at remote end of connection

LA

Loss of signal, loss of frame, or unavailability because of excessive errors.

QUESTION 236:

In a North American ISDN network, which reference point refers to the demarcation between the CPE and service provider?

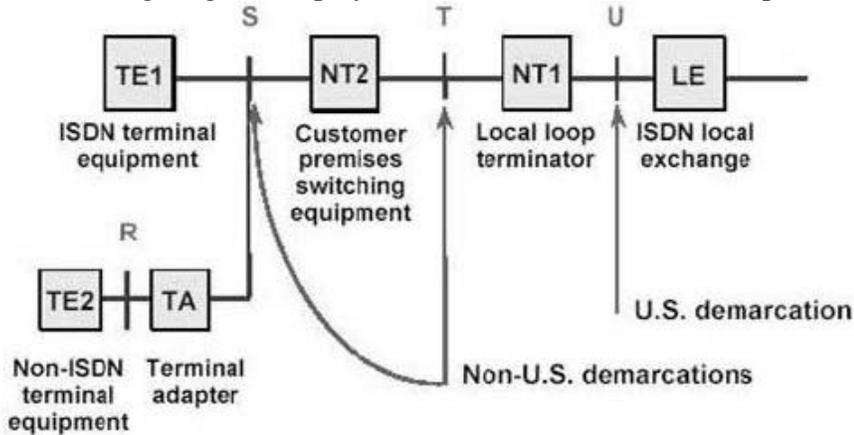
- A. R reference point
- B. S reference point
- C. T reference point
- D. U reference point

E. None of the above

Answer: D

Explanation:

The following diagram displays the different ISDN reference points:



Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 7-10

QUESTION 237:

In a leased T1 circuit WAN, what role does the CSU/DSU serve?

- A. It is responsible for the provision of encryption and compression for the security of transmitted data.
- B. It is responsible for multiplexing individual 64K channels into a single circuit.
- C. It is responsible for channelizing the leased T1 line into multiple 65K circuits.
- D. It is responsible for the provision of signal timing for communications and interfaces to the digital transmission facility.
- E. It is responsible for converting the analog T1 signals into digital signals for the router interface.

Answer: B

Explanation:

T1/E1 is one of the most popular forms of data transmission today. It has been around for many years. Originally, T1 was solely a Telco transmission mechanism tool to reduce the number of wires being installed between central offices. One T1 circuit can provide 24 channels of digitized voice or data.

T1 is based on 24 voice channels of 64 Kbps. If you multiply that out (24 x 64K) you get 1.536 Mbps and not 1.544 Mbps.

The basic building blocks of a T1 network are the CSU/DSU, multiplexer and a bridge or router. Depending on the type of T1 network being created, not all of these components need to be used. The CSU/DSU (channel service unit/data service unit) is the actual

connection point for the T1 wires. It provides line diagnostics and keep-alive functions for the line. In a leased line T1, the primary function of the CSU/DSU is to multiplex the individual channels into one single T1 circuit.

QUESTION 238:

Which one of the following dial backup provides for the following IOS features?

1. Is triggered by a lost IGP route
2. Provides reliable connectivity
3. Does not rely on interesting traffic to trigger an outgoing call to a remote router

- A. Floating static routes.
- B. Dialer backup.
- C. Dialer watch.
- D. Static routes.
- E. Dialer route.

Answer: C

Explanation:

Dialer Watch provides reliable connectivity without relying solely on defining interesting traffic to trigger outgoing calls at the central router. Dialer Watch uses the convergence times and characteristics of dynamic routing protocols. By configuring a set of watched routes that define the primary interface, you are able to monitor and track the status of the primary interface as watched routes are added and deleted.

QUESTION 239:

Which of the following devices are classified as DTE (Data Terminal Equipment) devices? (Choose all that apply.)

- A. Router
- B. Modem
- C. Mainframe computer
- D. Terminal
- E. CSU/DSU

Answer: A, C, D

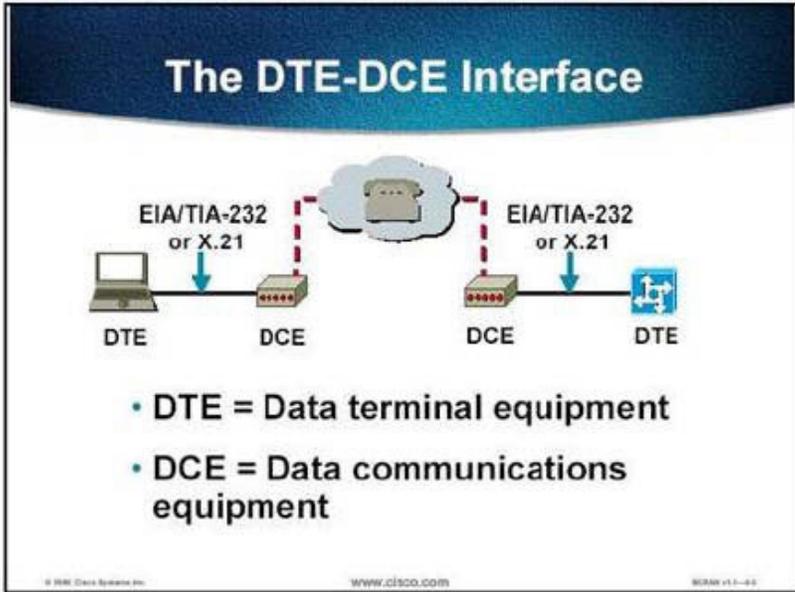
Explanation:

Data terminal equipment (DTE) includes end devices such as PCs, Routers, workstations, and mainframe computers. End devices communicate with each other through data communications equipment (DCE) such as modems, channel service units (CSUs), and data service units (DSUs). DCE can also be expanded to mean data circuit-terminating equipment which is the International Telecommunication Union-Telecommunications Standards Sector (ITU-TSS, or simply ITU-T; formerly known as CCITT

(ITU-T/CCITT) definition. The data communications equipment, expansion of DCE is the Electronic Industries Association (EIA) definition.

The EIA/TIA-232 standard defines the interface between DTE and DCE. TIA stands for Telecommunications Industry Association. The end-to-end communication path between two DTEs consists of three segments (as illustrated in the figure): DTE-DCE, DCE-DCE, and DCE-DTE.

You must administer a set of cabling and configuration elements for each segment.



Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 4-5

QUESTION 240:

DRAG DROP

Drag and drop the ISDN terms on the right side, next to the corresponding target on the left hand side:

Term	ISDN options	Use these
U interface	place here	four wires
TE1	place here	two wires
R interface	place here	non-ISDN device
S/T interface	place here	TE2 to TA
TE2	place here	native ISDN device

Answer:

Term	ISDN options	Use these
U interface	two wires	
TE1	native ISDN device	
R interface	TE2 to TA	
S/T interface	four wires	
TE2	non-ISDN device	

Explanation:

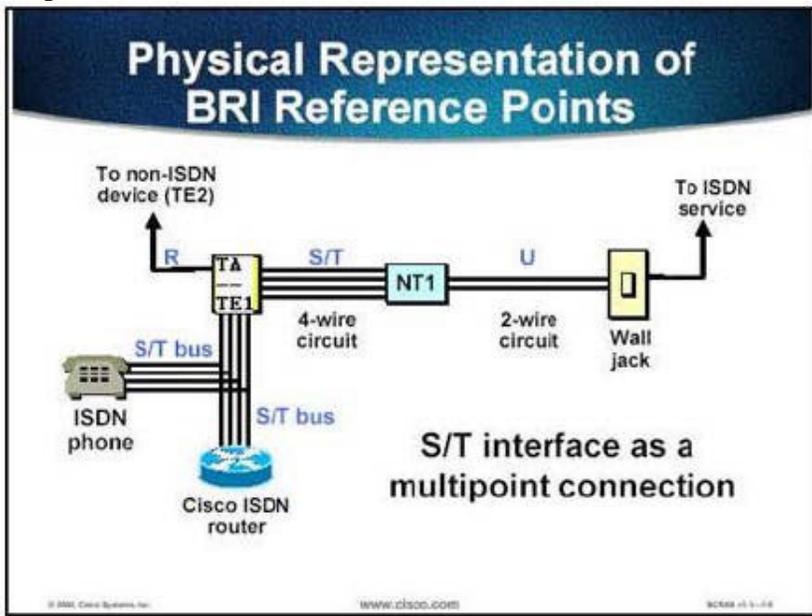
U interface - defines the two-wire interface between the NT and the ISDN cloud.

TE1 - designates a device that is compatible with the ISDN network.

R interface - defines the interface between the TA and an attached non-ISDN device (TE2).

S/T interface - is a four-wire interface (TX and RX).

TE2 - designates a device that is not compatible with ISDN and requires a terminal adapter.



Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 7-12

QUESTION 241:

In a DDR environment, it takes a certain amount of time for a line to come up. In the meantime, packets can accumulate. What command could you use to adjust the number packets that are held by the router while the DDR call is made?

A. Use the hold-queue command.

- B. Use the no fair-queue command.
- C. Use the dialer hold-queue command.
- D. Use the dialer wait-for-carrier-time command.
- E. None of the above

Answer: C

Explanation:

Usually, when dialing is in progress the outgoing packets are dropped, since the connection is not yet made. To hold the interesting traffic to be held in a queue, to be sent out as soon as the connection is made use the command

Router(config-if)# dialer hold-queue <number>, where number is number of packets, range 0-100.

holds upto 100 packets of the interesting outgoing traffic in a queue, while the dialing takes place.

QUESTION 242:

In a dial on demand (DDR) routing environment, what variable does the dialer fast-idle command account for?

- A. The amount of idle time before dropping link on a line with contention.
- B. The amount of idle time before dropping link on a line without contention.
- C. The amount of idle time before dropping link on a line with no interesting packets sent.
- D. The amount of idle time before dropping link on a line with no interesting packets received.

Answer: A

Explanation:

The fast-idle timer is defined as the time to wait before dropping the link if there is no interesting traffic and the line is waiting to make another connection (contention).

QUESTION 243:

Which of the following IOS entities are used to separate logical configurations from the physical interfaces that make or receive calls?

- A. dialer pool
- B. dialer map-class
- C. dialer profile
- D. dialer physical interface
- E. None of the above

Answer: C

Explanation:

Dialer profile is a type of configuring DDR, when the physical configuration is separated from logical interface-type profiles.

Incorrect Answers:

D: no such command

A,B: These commands are not used to create separated logical dialer entities.

QUESTION 244:

You're setting up an ISDN WAN, and are in the midst of configuring your router to initiate a DDR call. In doing this, what purpose does the dialer-list command serve?

- A. It defines call destination parameters.
- B. It defines what constitutes interesting traffic.
- C. It provides for optional call parameters.
- D. It assigns a dialer-group to an interface.

Answer: B

Explanation:

The entire configuration DDR depends on how the traffic types that cause a call setup to occur are triggered. This traffic is known as interesting traffic.

Cisco's implementation of DDR allows for as much or as little specificity of interesting traffic as is deemed necessary; interesting traffic is defined by the creation of dialer-lists that can specify that an entire protocol suite, no matter the level of traffic, can trigger a call setup.

Dialer-lists can be associated with standard or extended access lists to be specific to various traffic types. Rather than associating an access list with an interface, it is associated with a dialer list..."

Reference: CCNP Remote Access Exam Certification Guide, page 143, Brian Morgan & Craig Dennis, Cisco Press 2001, ISBN 1-58720-003-1

QUESTION 245:

When DDR is implemented; a router will use a dialer profile to check if a dialer is connected to the desired remote destination. If the connection is there, the traffic can be sent. Every time an interesting packet crosses the dialer, a timer gets reset to the maximum configured value. What is the name of this particular timer?

- A. The wait for carrier timer
- B. The in-band timer
- C. The idle timer
- D. The fast-idle timer

Answer: C

Explanation:

In the above scenario the idle timer is used. The idle timer is used with the dialer idle-timeout command.

The purpose of DDR is to bring down the ISDN link when the traffic volume is low or idle. However, at times, the traffic volume can simply be in a short lull. Indeed, LAN traffic is bursty - quiet at times followed by an explosion of traffic.

To avoid the link coming down when traffic flow ceases and then being forced to redial, use the dialer idle-timeout command. Executing this command dictates that when traffic defined as interesting has ceased to flow across the link for the specified period of time (in seconds), go ahead and bring down the link. For instance, if the command dialer idle-timeout 180 is used at the interface configuration mode, the link comes down three minutes after the last piece of interesting traffic has traversed the link. Note that only interesting traffic resets the timer. Any non-interesting traffic goes across, but does not contribute to keeping the link up.

Reference: CCNP Remote Access Exam Certification Guide, page 148, Brian Morgan & Craig Dennis, Cisco Press 2001, ISBN 1-58720-003-1

QUESTION 246:

What command line specifies the parameters for disconnecting an idle DDR call, when the line is needed for a new DDR call to a different destination?

- A. The time specified by dialer idle-timeout.
- B. The time specified by dialer fast-idle.
- C. The value configured by dialer load-threshold.
- D. The presence of interesting traffic (designated for a different destination) will force an immediate disconnect.

Answer: B

Explanation:

dialer fast-idle (map-class dialer)

To specify the fast idle timer value to use when placing a call to any telephone number associated with a specified class, use the dialer fast-idle map-class dialer configuration command.

The following example specifies a dialer fast idle time of 10 seconds:

```
dialerstring4156884540classEng
!Thismap-classensureshatthesecallsuseanISDNspeedof56kbpsanda
!fast-idletimeof10seconds.
map-classdialerEng
isdnspeed56
dialerfast-idle10
dialerwait-for-carrier-time30
```

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_command_reference_chapter09186a00800c

QUESTION 247:

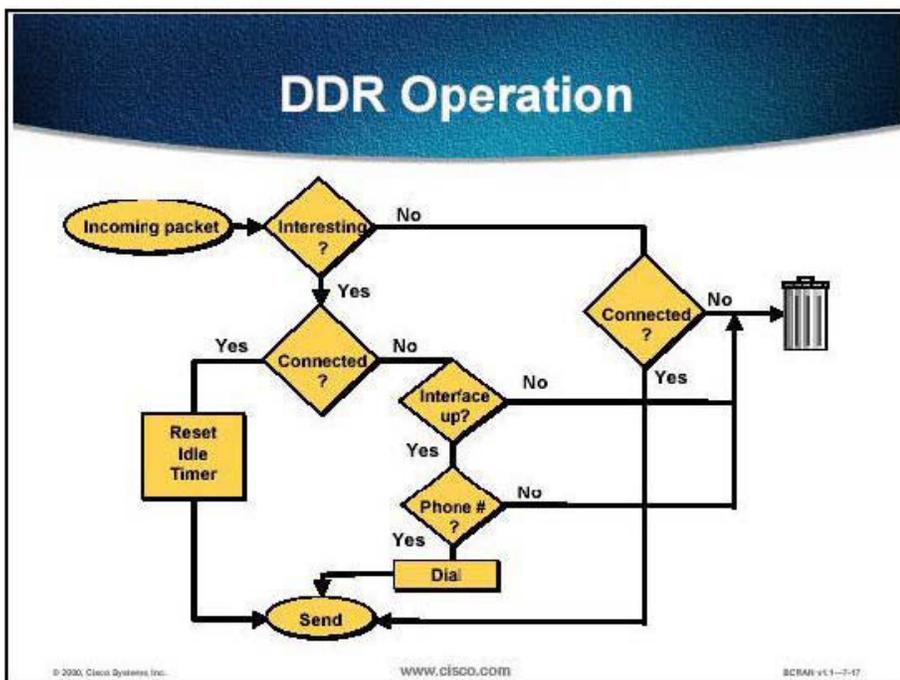
What happens to uninteresting traffic when it's carried over a DDR link?

- A. Uninteresting traffic will be routed over an established DDR call, but at a lower priority than interesting traffic.
- B. Uninteresting traffic will keep DDR call established, even if no more interesting traffic is being routed over the link.
- C. Uninteresting traffic will not be routed over an established DDR call.
- D. Uninteresting traffic will be routed over an established DDR call, as long as there is enough interesting traffic to keep the call connected.

Answer: D

Explanation:

With Dial-on-Demand Routing (DDR), all traffic is classified as either interesting or uninteresting. If the traffic is interesting, then the router connects to the peer. If the traffic is not interesting then the call is not connected. However, for connections that are already connected, interesting traffic has a different purpose. It is used to reset the idle timeout back to the maximum value (configured with the dialer idle-timeout command). The moment a connection is made, the idle-timer starts to decrease. Once the router receives a packet that matches the interesting traffic definition, the idle-timer is reset back to the maximum value. Therefore, if a connection is up, it will send packets that are defined as uninteresting.



Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 7-20

QUESTION 248:

If you wanted to cache the routes learned by distance vector dynamic routing protocols so you can use them over a DDR connection and keep line usage costs down; what strategy would you use?

- A. Route redistribution
- B. DDR route maps
- C. Snapshot routing
- D. Passive interfaces
- E. Dynamic static routes

Answer: C

Explanation:

In ISDN dial-on-demand routing (DDR) environments, distance vector routing protocol periodic updates can unnecessarily keep an idle DDR link up, resulting in high usage bills. Snapshot Routing can be implemented to overcome this limitation. Distance vector protocols such as IP Routing Information Protocol (RIP), Internetwork Packet Exchange (IPX) RIP, and Interior Gateway Routing Protocol (IGRP) send a full routing table at a fixed interval of time as described below:

1. The IP RIP routing protocol sends an update, by default, every 30 seconds.
 2. The IPX RIP routing protocol sends an update every 60 seconds, per its default interval.
 3. The IGRP routing protocol sends a routing table update, by default, every 90 seconds.
- If you dialed the central site for each of these updates, this periodic traffic would keep an ISDN line up indefinitely and result in a high usage bill. If you do not dial the central site for these updates, dynamic routes (learned from the routing protocol) would be removed from the routing table. Snapshot routing forces the router to keep the routing table intact when the DDR link is down and controls when to dial for periodic routing protocol updates.

Snapshot routing provides the remedy for the constant periodic updates generated by the distance vector routing protocols. Snapshot routing operates by defining a routing protocol update active period and quiet period. The router may exchange a snapshot of the routing table during the active period. After the active period expires, a quiet period is maintained where routing updates are suppressed and the snapshot of the routing table is kept intact. Snapshot routing can be applied to IPX/RIP and AppleTalk Routing Table Maintenance Protocol (RTMP) as well.

QUESTION 249:

On a DDR link; which feature maintains dynamic routing tables by controlling dial up connections for the sake of receiving periodic routing updates?

- A. Dial Backup
- B. Snapshot Routing
- C. Dialer Maps
- D. Route Redistribution

Answer: B

Explanation:

Snapshot routing was developed to save bandwidth utilization across dialup interfaces. With snapshot routing, the routing table is placed in an update-restricted (that is, frozen) state. This implementation of DDR utilizes a quiet period and an active period. The routing table is not updated during the quiet period, which is the length of time that the routing table remains frozen. When the quiet period expires, a dialer interface initiates a call to a remote router. The active period is the length of time the call remains up in order for the two routers to exchange routing updates.

Reference:

Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)
Page 187

QUESTION 250:

Snapshot routing was designed to conserve bandwidth in dialup interfaces. Which of the following routing protocols are supported by Snapshot routing? (Choose two)

- A. RIP
- B. OSPF
- C. BGP
- D. IGRP
- E. EIGRP

Answer: A, D

Explanation:

It is important to note that snapshot routing is designed for use only with distance vector routing protocols. Distance vector routing Snapshot allows the use of all "distance vector" routing protocols over DDR lines are :

1. RIP & IGRP for IP
2. RTMP for Appletalk
3. RIP and SAP for IPX
4. RTP for Vines

In addition, you can configure the router to exchange routing updates each time the line protocol goes from "down" to "up" or from "dialer spoofing" to "fully up."

References:

Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)

QUESTION 251:

You are the CTO of Certkiller Inc. and management has given you the order to reduce costs. So instead of purchasing dedicated router ports you decide to allow the last available physic BRI interface on your central router to dial out to the remote branch offices. Which two commands would your administrators have to enter to provide this capability? (Choose all that apply.)

- A. The dialer-group command
- B. The multilink ppp command
- C. The backup interface dialer command
- D. The dialer hunt-group command
- E. The dialer rotary-group command

Answer: C, E

Explanation:

Configuring Interfaces to Use a Backup Interface

To configure one or more interfaces to use a backup interface, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# interface type number	Specifies the interface to be backed up and begins interface configuration mode.
Step 2	Router(config-if)# ip unnumbered loopback0	Specifies IP unnumbered loopback.
Step 3	Router(config-if)# backup interface dialer number	Specifies the backup interface and begins interface configuration mode.
Step 4	Router(config-if)# backup delay enable-delay disable-delay	Specifies delay between the physical interface going down and the backup being enabled, and between the physical interface coming back up and the backup being disabled.

Dialer rotary group - ISDN rotary groups are similar to dialer pools. One primary differences, however, is the lack of map class capabilities in rotary groups. Configuring rotary groups involves the creation of logical dialer interfaces (as is done in dialer pool configurations), the interface designation of which is an important detail.

Reference: CCNP Remote Access Exam Certification Guide, page 160, Brian Morgan & Craig Dennis, Cisco Press 2001, ISBN 1-58720-003-1

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fdial_c/fnsprt6/dcdbakdp.htm

QUESTION 252:

How can an ISDN interface be used as a backup link for a primary interface and still use DDR to communicate with other sites?

- A. By using dialer profiles.
- B. An ISDN interface cannot be both.
- C. With the command backup interface serial 0/0 on the bri0/0 interface along with normal DDR commands.
- D. With the command backup interface bri 0/0 on the physical interface and normal DDR commands on the bri0/0 interface.

Answer: A

Explanation:

Dialer profiles separate logical configurations from the physical interfaces that receive or make calls. Because of this separation, multiple dialer profile configurations can share interfaces such as ISDN, asynchronous modems, or synchronous serial connections. Dialer profiles allow you to bind logical and physical configurations together dynamically on a per call basis. This allows physical interfaces to take on different characteristics based on incoming or outgoing call requirements. Dialer profiles can define encapsulation, access control lists, minimum or maximum calls, and toggle features on or off. Dialer profiles are particularly useful where multiple ISDN B channels are to be used to connect to multiple remote destinations simultaneously. In such a case, one dialer profile can be bound to one set of B channels while another dialer profile can be bound to another set of B channels. This allows the same physical interface to connect to multiple remote destinations simultaneously.

Reference:

http://www.cisco.com/en/US/tech/CK801/CK133/technologies_configuration_example09186a0080093c2e.shtml

QUESTION 253:

DRAG DROP

Drag the channelized T1/E1 PRI Network Module LED abbreviation to the correct meaning.

642-821

EN	Local alarm at remote end of connection	Place here
RA	Carrier received on telco link	Place here
LA	The module has passed self-tests and is available to the router	Place here
LP	Controller local loopback	Place here
CD	Loss of signal, loss of frame, or unavailability because of excessive errors	Place here

Answer:

Local alarm at remote end of connection	RA
Carrier received on telco link	CD
The module has passed self-tests and is available to the router	EN
Controller local loopback	LP
Loss of signal, loss of frame, or unavailability because of excessive errors	LA

Explanation:

PRI Module LEDs

All network modules have an enable (EN) LED. This LED indicates that the module has passed its self-tests and is available to the router.

All PRI modules display four additional LEDs for each port. These LEDs are described in the following table:

LED	Meaning
RA	Local alarm at remote end of connection
LA	Loss of signal, loss of frame, or unavailability because of excessive errors
LP	Controller local loopback
CD	Carrier received on telco link

Reference:

http://www.cisco.com/en/US/products/hw/modules/ps2797/products_module_installation_guide_chapter09186a0

QUESTION 254:

What is the purpose of the dialer hold-queue command?

[642-821](#)

- A. To allow interesting outgoing packets to be queued until a modem connection is established.
- B. To allow any outgoing packets to be queued until a modem connection is established.
- C. To allow interesting outgoing packets to be queued when a source quench message is received.
- D. To allow any outgoing packets to be queued during network congestion.

Answer: A

Explanation:

Sometimes packets destined for a remote router are discarded because no connection exists. Establishing a connection using an analog modem can take time, during which packets are discarded. However, configuring a dialer hold queue will allow interesting outgoing packets to be queued and sent as soon as the modem connection is established. A dialer hold queue can be configured on any type of dialer, including in-band synchronous, asynchronous, DTR, and ISDN dialers. Also, hunt group leaders can be configured with a dialer hold queue. If a hunt group leader (of a rotary dialing group) is configured with a hold queue, all members of the group will be configured with a dialer hold queue and no individual member's hold queue can be altered. To establish a dialer hold queue, use the following command in interface configuration mode:

Command	Purpose
<code>dialer hold-queue packets</code>	Create a dialer hold queue and specify the number of packets to be held in it.

As many as 100 packets can be held in an outgoing dialer hold queue.

QUESTION 255:

The following debug output was seen on RTA within the Certkiller network:

```
RTA# debug ppp negotiation
PPP protocol negotiation debugging is on
RTA#
*Mar 1 00:06:36.645: %LINK-3-UPDOWN: Interface BR10/1 changed state to up
*Mar 1 00:06:36.661: BR0/1 PPP: Treating connection as a callin
*Mar 1 00:06:36.665: BR0/1 PPP: Phase is ESTABLISHING. Passive Open [0 sess, 0 load]
*Mar 1 00:06:36.669: BR0/1 LCP: State is Listen
*Mar 1 00:06:37.034: BR0/1 LCP: I CONFREQ [Listen] id 7 len 17
*Mar 1 00:06:37.038: BR0/1 LCP: AuthProto PAP (0x0304C023)
*Mar 1 00:06:37.042: BR0/1 LCP: MagicNumber 0x507A214D (0x0506507A214D)
*Mar 1 00:06:37.046: BR0/1 LCP: Callback 0 (0x0D0300)
*Mar 1 00:06:37.054: BR0/1 LCP: O CONFREQ [Listen] id 4 len 15
*Mar 1 00:06:37.058: BR0/1 LCP: AuthProto CHAP (0x0305C22305)
*Mar 1 00:06:37.062: BR0/1 LCP: MagicNumber 0x1081E7E1 (0x05061081E7E1)
*Mar 1 00:06:37.066: BR0/1 LCP: O CONFREQ [Listen] id 7 len 7
*Mar 1 00:06:37.070: BR0/1 LCP: Callback 0 (0x0D0300)
*Mar 1 00:06:37.098: BR0/1 LCP: I CONFACK [REQsent] id 4 len 15
*Mar 1 00:06:37.102: BR0/1 LCP: AuthProto CHAP (0x0305C22305)
*Mar 1 00:06:37.106: BR0/1 LCP: MagicNumber 0x1081E7E1 (0x05061081E7E1)
*Mar 1 00:06:37.114: BR0/1 LCP: I CONFREQ [ACKrcvd] id 8 len 14
*Mar 1 00:06:37.117: BR0/1 LCP: AuthProto PAP (0x0304C023)
*Mar 1 00:06:37.121: BR0/1 LCP: MagicNumber 0x507A214D (0x0506507A214D)
*Mar 1 00:06:37.125: BR0/1 LCP: O CONFNAK [ACKrcvd] id 8 len 9
*Mar 1 00:06:37.129: BR0/1 LCP: AuthProto CHAP (0x0305C22305)
*Mar 1 00:06:37.165: BR0/1 LCP: I CONFREQ [ACKrcvd] id 9 len 15
*Mar 1 00:06:37.173: BR0/1 LCP: MagicNumber 0x507A214D (0x0506507A214D)
*Mar 1 00:06:37.177: BR0/1 LCP: O CONFACK [ACKrcvd] id 9 len 15
*Mar 1 00:06:37.181: BR0/1 LCP: AuthProto CHAP (0x0305C22305)
*Mar 1 00:06:37.185: BR0/1 LCP: MagicNumber 0x507A214D (0x0506507A214D)
*Mar 1 00:06:37.189: BR0/1 LCP: State is Open
*Mar 1 00:06:37.193: BR0/1 PPP: Phase is AUTHENTICATING. by both [0 sess, 0 load]
```

Given the above output, which two statements are true? (Choose two)

- A. The negotiated authentication protocol to be used is PAP.
- B. The negotiated authentication protocol to be used is CHAP.
- C. The two devices were not able to agree on an authentication protocol.
- D. This router is configured to accept callback requests.
- E. This router has initiated a callback request.
- F. The peer router is configured as a callback client.

Answer: B, F

Explanation:

The debug ppp negotiation command enables you to view the PPP negotiation transactions, identify the problem or stage when the error occurs, and develop a resolution.

Information regarding the output above is displayed below:

```
*Mar 1 00:06:37.058: BR0/1 LCP: AuthProto CHAP (0x0305C22305)
*Mar 1 00:06:37.062: BR0/1 LCP: MagicNumber 0x1081E7E1 (0x05061081E7E1)
!-- This router requests:
!-- Option: Authentication Protocol, Value: CHAP
*Mar 1 00:06:37.038: BR0/1 LCP: AuthProto PAP (0x0304C023)
```

*Mar 1 00:06:37.042: BR0:1 LCP: MagicNumber 0x507A214D (0x0506507A214D)

*Mar 1 00:06:37.046: BR0:1 LCP: Callback 0 (0x0D0300)

!--- The peer has requested:

!--- Option: Authentication Protocol, Value: PAP

!--- Option: MagicNumber (This is used to detect loopbacks and is always sent.)

!--- Option: Callback, Value: 0 (This is for PPP Callback; MS Callback uses 6.)

Reference:

For information regarding the use of the "debug PPP negotiation" command, see the following link:

http://www.cisco.com/en/US/tech/CK7_13/CK5_07/technologies_tech_note09186a00800ae945.shtml

QUESTION 256:

The following configuration was placed on a Certkiller router named RTA:

```
rtar(config)# interface bri0
rtar(config-if)# ip address 192.168.12.3 255.255.255.240
rtar(config-if)# encapsulation ppp
rtar(config-if)# dialer map ip 192.168.12.1 name ROUTER1 5554321
rtar(config-if)# dialer-group 1
rtar(config-if)# ppp authentication chap
rtar(config-if)# isdn spid1 40855512120000 5551212
rtar(config-if)# isdn spid2 40855512340000 5551234
rtar(config-if)# ppp multilink
rtar(config-if)# dialer load-threshold 128 either
```

Given the configuration commands in the exhibit, when will additional B channels be added to the multilink PPP bundle?

- A. When the total load of outbound traffic reaches 128 k
- B. When the total load of inbound traffic reaches 128 k
- C. When the maximum calculated load as the larger of the outbound and inbound loads reaches 128 k
- D. When the total load of inbound traffic reaches 50 percent of bandwidth utilization.
- E. When the total load of outbound traffic reaches 50 percent of bandwidth utilization
- F. When the load of the inbound or outbound traffic reaches 50% utilization.
- G. When the load reaches 128 percent

Answer: F

Explanation:

To configure bandwidth on demand by setting the maximum load before the dialer places another call to a destination, use the dialer load-threshold interface command.

Syntax:

```
dialer load-threshold load[outbound | inbound | either]
```

<i>load</i>	Interface load used to determine whether to initiate another call or to drop a link to the destination. This argument represents a utilization percentage; it is a number between 1 and 255, where 255 is 100%.
outbound	(Optional) Calculates the actual load using outbound data only.
inbound	(Optional) Calculates the actual load using inbound data only.
either	(Optional) Sets the maximum calculated load as the larger of the outbound and inbound loads.

In this example, the dialer load-threshold is set to 128, and 128/255 is approximately 50%. Since the keyword "either" was used, the larger of the two loads (inbound and outbound) will be used.

QUESTION 257:

Fill in the following blanks to make the statement below correct:

An ISDN PRI in Australia provides _____ B channels plus _____ D channels.

- A. 15, 1
- B. 24, 1
- C. 32, 1
- D. 30, 1
- E. 24, 2

Answer: D

Explanation:

ISDN Primary Rate Interface (PRI) service offers 23 B channels and 1 D channel in North America and Japan, yielding a total bit rate of 1.544 Mbps (the PRI D channel runs at 64 kbps). ISDN PRI in Europe, Australia, and other parts of the world provides 30 B channels plus one 64-kbps D channel and a total interface rate of 2.048 Mbps. The PRI physical layer specification is ITU-T I.431.

QUESTION 258:

You are a Cisco Certified Engineer. You are configuring an ISDN remote access solution. With ISDN, non-ISDN terminals are referred to as:

- A. LE
- B. NT1
- C. TE1
- D. LE2
- E. LA
- F. TE2

Answer: F

Explanation:

ISDN components include terminals, terminal adapters (TAs), network-termination devices, line-termination equipment, and exchange-termination equipment. ISDN terminals come in two types. Specialized ISDN terminals are referred to as terminal equipment type 1 (TE1). Non-ISDN terminals, such as DTE, that predate the ISDN standards are referred to as terminal equipment type 2 (TE2). TE1s connect to the ISDN network through a four-wire, twisted-pair digital link. TE2s connect to the ISDN network through a T

A. The ISDN TA can be either a standalone device or a board inside the TE2.

If the TE2 is implemented as a standalone device, it connects to the TA via a standard physical-layer interface. Examples include EIA/TIA-232-C (formerly RS-232-C), V.24, and V.35.

QUESTION 259:

Is the following statement True or False?

By directly connecting to the ISDN NT1 device, the router has more control over ISDN parameters in Europe.

- A. True
- B. False
- C. True only for BRI
- D. None of the choices.
- E. True only for PRI

Answer: B

Explanation:

The native ISDN interface on the Cisco 2503 router allows the router to be directly connected to an ISDN NT1 device. In many countries, the NT1 is provided by the telephone company. In the United States, however, the NT1 is customer-owned equipment. By directly connecting to the ISDN network, the router has more direct control over ISDN parameters and has access to ISDN information. In Europe, the ISDN providers retain more control over the ISDN parameters.

QUESTION 260:

A new ISDN circuit is being provisioned for a remote Certkiller location. With ISDN, specialized ISDN terminals are referred to as which of the following?

- A. LE
- B. NT1
- C. TA
- D. TE1

- E. TE3
- F. LA

Answer: D

Explanation:

ISDN components include terminals, terminal adapters (TAs), network-termination devices, line-termination equipment, and exchange-termination equipment. ISDN terminals come in two types. Specialized ISDN terminals are referred to as terminal equipment type 1 (TE1). Non-ISDN terminals, such as DTE, that predate the ISDN standards are referred to as terminal equipment type 2 (TE2). TE1s connect to the ISDN network through a four-wire, twisted-pair digital link. TE2s connect to the ISDN network through a T

A. The ISDN TA can be either a standalone device or a board inside the TE2.

If the TE2 is implemented as a standalone device, it connects to the TA via a standard physical-layer interface. Examples include EIA/TIA-232-C (formerly RS-232-C), V.24, and V.35.

QUESTION 261:

A new ISDN circuit is being provisioned for a remote Testing office. In ISDN, ITU-T I.450 belongs to which layer?

- A. Layer 1
- B. Layer 4
- C. Layer 3
- D. Layer 2

Answer: C

Explanation:

Two Layer 3 specifications are used for ISDN signaling: ITU-T (formerly CCITT) I.450 (also known as ITU-T Q.930) and ITU-T I.451 (also known as ITU-T Q.931). Together, these protocols support user-to-user, circuit-switched, and packet-switched connections. A variety of call-establishment, call-termination, information, and miscellaneous messages are specified, including SETUP, CONNECT, RELEASE, USER INFORMATION, CANCEL, STATUS, and DISCONNECT. These messages are functionally similar to those provided by the X.25 protocol.

QUESTION 262:

New ISDN links are being provisioned for the Certkiller North American remote office branches. Which of the following ISDN reference points are relevant only in North America?

- A. R

- B. U
- C. S
- D. T
- E. None of the above
- F. All of the above

Answer: B

Explanation:

ISDN specifies a number of reference points that define logical interfaces between functional groups, such as TAs and NT1s. ISDN reference points include the following:

R - The reference point between non-ISDN equipment and a TA.

S - The reference point between user terminals and the NT2.

T - The reference point between NT1 and NT2 devices.

U - The reference point between NT1 devices and line-termination equipment in the carrier network. The U reference point is relevant only in North America, where the NT1 function is not provided by the carrier network.

QUESTION 263:

In the Certkiller network, you will be responsible for provisioning, configuring, and maintaining all of their ISDN connections. At ISDN layer 3, which of the following messages are NOT included? (Choose all that apply)

- A. PAUSE
- B. DISCONNECT
- C. CONNECT
- D. STATUS
- E. USER INFORMATION
- F. RELEASE
- G. SETUP
- H. CANCEL

Answer: A

Explanation:

According to Cisco: Two Layer 3 specifications are used for ISDN signaling: ITU-T (formerly CCITT) I.450 (also known as ITU-T Q.930) and ITU-T I.451 (also known as ITU-T Q.931). Together, these protocols support user-to-user, circuit-switched, and packet-switched connections. A variety of call-establishment, call-termination, information, and miscellaneous messages are specified, including SETUP, CONNECT, RELEASE, USER INFORMATION, CANCEL, STATUS, and DISCONNECT. These messages are functionally similar to those provided by the X.25 protocol.

QUESTION 264:

ISDN is used throughout the Certkiller network. In ISDN, the ITU-T Q.931 standard belongs to which layer?

- A. Layer 1
- B. Layer 4
- C. Layer 3
- D. Layer 2

Answer: C

Explanation:

Two Layer 3 specifications are used for ISDN signaling: ITU-T (formerly CCITT) I.450 (also known as ITU-T Q.930) and ITU-T I.451 (also known as ITU-T Q.931). Together, these protocols support user-to-user, circuit-switched, and packet-switched connections. A variety of call-establishment, call-termination, information, and miscellaneous messages are specified, including SETUP, CONNECT, RELEASE, USER INFORMATION, CANCEL, STATUS, and DISCONNECT. These messages are functionally similar to those provided by the X.25 protocol.

QUESTION 265:

Link Access Procedure, Balanced (LAPD) is an important aspect of any ISDN connection. In ISDN, LAPD belongs to which layer?

- A. Layer 2
- B. Layer 3
- C. Layer 1
- D. Layer 4

Answer: A

Explanation:

Layer 2 of the ISDN signaling protocol is Link Access Procedure, D channel (LAPD). LAPD is similar to High-Level Data Link Control (HDLC) and Link Access Procedure, Balanced (LAPB). As the expansion of the LAPD acronym indicates, this layer it is used across the D channel to ensure that control and signaling information flows and is received properly.

QUESTION 266:

How many Layer 3 specifications exist for ISDN signaling?

- A. 0
- B. 1
- C. 2
- D. 3

E. 4

Answer: C

Explanation:

According to the technical documentation at CCO:

Two Layer 3 specifications are used for ISDN signaling: ITU-T (formerly CCITT) I.450 (also known as ITU-T Q.930) and ITU-T I.451 (also known as ITU-T Q.931). Together, these protocols support user-to-user, circuit-switched, and packet-switched connections.

A variety of call-establishment, call-termination, information, and miscellaneous messages are specified, including SETUP, CONNECT, RELEASE, USER INFORMATION, CANCEL, STATUS, and DISCONNECT.

QUESTION 267:

IN the Certkiller network, multiple ISDN routers are connected to a variety of different ISDN carrier switches. Which feature would you use if a single router needed to connect to multiple ISDN switch types?

- A. Multilink PPP
- B. Multilink Switches
- C. Multilink ISDN Channel aggregation
- D. Multiple ISDN Switch Types
- E. None of the above

Answer: D

Explanation:

The Multiple ISDN Switch Types feature allows you to configure more than one ISDN switch type per router. You can apply an ISDN switch type on a per interface basis, thus extending the existing global isdn switch-type command to the interface level. This allows Basic Rate Interfaces (BRI) and Primary Rate Interfaces (PRI) to run simultaneously on platforms that support both interface types.

QUESTION 268:

At the Certkiller network, you are responsible for provisioning and setting up new ISDN connections. A new ISDN PRI is being installed at a remote location and you want to configure the router. What T1 controller command can you use to configure the controller for ISDN PRI operation? (Type in answer below)

Answer: ISDN Switch-type

Explanation:

To configure an ISDN switch type for BRI and PRI interfaces using new switch type keywords, perform the following tasks beginning in global configuration mode. Step 2 is

optional.

Task	Command
Step 1 Configure the global ISDN switch type.	<code>isdn-switch type switch-type</code>
Step 2 Configure the interface level ISDN switch type (optional).	<code>isdn-switch type switch-type</code>

National ISDN Switch Types for Basic Rate and Primary Rate Interfaces provides the following benefits: Unlike previous custom implementations, such as basic-5ess, basic-dms100, primary-5ess, and primary-dms100, the National ISDN specification is designed to be switch independent. This increases flexibility in adapting to evolving standards and future enhancements. The ability to select PRI B channel order election for outgoing calls allows extended flexibility and compatibility with a variety of ISDN switch type service implementations. Additionally, this ability reduces ISDN switch misconfigurations, which can delay initial service activation.

QUESTION 269:

A new ISDN circuit is being installed at a remote Certkiller location. Which of the following are network-termination devices, in addition to NT1, that can connect the four-wire subscriber wiring to the conventional two-wire local loop?

- A. NT3
- B. TA2
- C. LE
- D. NT2
- E. TA
- F. LE2

Answer: D

Explanation:

Beyond the TE1 and TE2 devices, the next connection point in the ISDN network is the network termination type 1 (NT1) or network termination type 2 (NT2) device. These are network-termination devices that connect the four-wire subscriber wiring to the conventional two-wire local loop. In North America, the NT1 is a customer premises equipment (CPE) device. In most other parts of the world, the NT1 is part of the network provided by the carrier. The NT2 is a more complicated device that typically is found in digital private branch exchanges (PBXs) and that performs Layer 2 and 3 protocol functions and concentration services. An NT1/2 device also exists as a single device that combines the functions of an NT1 and an NT2.

QUESTION 270:

In general, multiple ISDN Switch Types support which of the following ISDN interfaces?

- A. None of the choices.
- B. Both BRI and PRI
- C. BRI only
- D. PRI only
- E. This feature is no longer supported

Answer: B

Explanation:

The Multiple ISDN Switch Types feature allows you to configure more than one ISDN switch type per router. You can apply an ISDN switch type on a per interface basis, thus extending the existing global isdn switch-type command to the interface level. This allows Basic Rate Interfaces (BRI) and Primary Rate Interfaces (PRI) to run simultaneously on platforms that support both interface types.

QUESTION 271:

Which of the following statements about the ISDN switch type is NOT true?
(Choose all that apply)

- A. It selects the PRI controller line code.
- B. It defines the type of signaling used by the ISDN service provider switch.
- C. It is a set of US only standard
- D. It is proprietary
- E. It is both a global and an interface command.
- F. It is a PRI controller command.
- G. None of the above.

Answer: A, C, D, F

Explanation:

To configure the switch type, use the command `isdn switch-type switch-type` in the global or interface configuration mode.

The ISDN switch type can be verified using the command `show isdn status`. The Telco should explicitly indicate the switchtype that needs to be configured. Occasionally (especially in North America) the Telco may indicate the switchtype is "custom" or "national". In such cases, use the following guidelines to determine the switchtype configuration:

Custom: If the Telco indicates that their switch-type is Custom, then configure the switch type on the router as `basic-5ess` (for BRI with 5ess switch), `primary-5ess` (for PRI with 5ess), `basic-dms` (for BRI with DMS switch), or `primary-dms` (for PRI with DMS).

National: switch type conforming to the NI-1 standard for BRI and NI-2 standard for PRI (there is no NI-1 standard for PRIs). If the Telco informs you that the switch type is National, then the Cisco router configuration should be `basic-ni` (for BRI) or `primary-ni` (for PRI).

Incorrect Answers:

B.: This statement is true. This describes the purpose of defining the switch type, so that the router can effectively communicate with the ISDN switch.

E: With support for the multiple ISDN switch types, this statement is also correct.

QUESTION 272:

The Certkiller Company currently uses an ISDN BRI in standby mode to back up the primary serial connection. How can the BRI interface be configured to allow dialup operation as well as backup services?

- A. Configure the BRI as a standard DDR connection and configure the serial port to use BRI as the backup.
- B. Configure one B channel of the BRI as Standby Backup and two B channels as DDR.
- C. Configure one B channel of the BRI as Standby Backup and the other B channel as DDR.
- D. Configure two B channels of the BRI as Standby Backup and the other B channel as DDR.
- E. Use the dialer profile as a backup and configure the BRI as a member of the dialer pool.
- F. Configure one B channel of the BRI as Standby Backup and nothing else.

Answer: E

Explanation:

A backup interface is an interface that stays idle until certain circumstances occur, then it is activated. The backup interface can be a physical interface such as a Basic Rate Interface (BRI), or an assigned backup dialer interface to be used in a dialer pool. While the primary line is up, the backup interface is placed in standby mode. Once in standby, the backup interface is effectively shutdown until enabled. Any route associated with the backup interface will not appear in the routing table.

QUESTION 273:

According to ISDN standards, the ITU-T Q.931 is the protocol that works for:

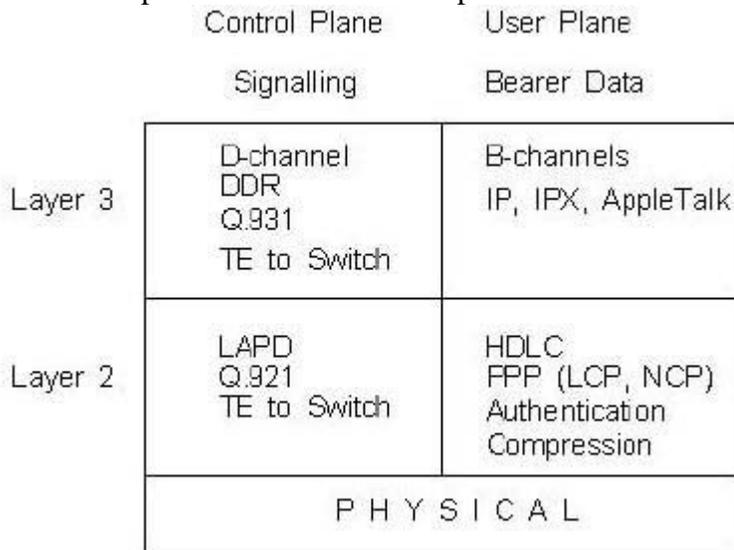
- A. Layer3; D channel
- B. Layer1, D channel
- C. Layer5; B channel
- D. Layer2; B channel
- E. Layer4; B channel
- F. Layer2; D channel

Answer: A

Explanation:

642-821

The ISDN protocol model can be represented in the following diagram:



Everything that is important occurs in the Control Plane on the D-Channel.

Additional Info:

Layer 3 ISDN signalling is specified in Q.930 (ITU-T I.450) and Q.931 (ITU-T I.451) and operate locally between the router and the switch. Different switch vendors have different bit interpretations hence why the switch type is important. Like Q.921, Q.931 is only concerned with the terminal to local switch, and it deals with making and tearing down the call via the D channel. Within the ISDN network itself SS7 Internal Signalling Utility Protocol (ISUP) is used. The fields for Q.931 are shown below:

Bits 8 4 4 1 7 1 7 8

Protocol Discriminator	0's	Call Reference Length	Flag	Call Reference	0	Message Type	Information Elements
------------------------	-----	-----------------------	------	----------------	---	--------------	----------------------

Reference: <http://www.rhyshaden.com/isdn.htm>

QUESTION 274:

You are setting up router CK1 for a backup link using the "backup interface" command. Which statement is true concerning the backup interface?

- A. The backup interface can be configured to active based upon the load of the primary interface or the link condition of the primary interface, but not both simultaneously.
- B. Load sharing via the "backup load" command is not supported if the backup interface is configured on a subinterface.
- C. The default interval time for monitoring load is 60 seconds.
- D. On the backup interface, the command backup interface interface should be used.
- E. All of the above

Answer: B

Explanation:

Although a subinterface can be configured as a backup interface, you can not specify the load of a subinterface when configuring the backup using the backup load command. The following is a configuration example using the backup load:

```
interface serial 0  
backup interface serial 1  
backup load 75 5
```

In this case, the secondary line (which is serial1) will not be activated when the primary (srial 0) goes down. The secondary line will be activated when the load on the primary line is greater than 75 percent of the primary's bandwidth. The secondary line will then be brought down when the aggregate load between the primary and secondary lines fits within 5 percent of the primary bandwidth.

However, the link specified to back up must be a physical link, and not a sub-interface. Incorrect Answers:

A: Using the backup load command, the three keyword options are inbound, outbound, or either. Either takes into account the load of both directions simultaneously.

C: Using backup load, the IOS software monitors the traffic load and computes a 5-minute moving average.

D. This configuration statement should be placed under the primary interface, or the interface to be backed up, and not on ht backup interface itself.

QUESTION 275:

Interface Serial 1 of a Certkiller router is being configured to use backup interface. Which two statements are true about the application of the backup interfacecommand? (Choose two.)

- A. The backup interface is in standby mode until activated.
- B. A Fast Ethernet interface can be used as a backup interface.
- C. The backup interface can be used to load balance.
- D. Both primary and backup routes appear in the route table. The backup route, however, has a higher administrative distance.
- E. Each primary interface can have up to three backup interfaces.

Answer: A, C

Explanation:

The "backup interface" command places the interface into standby mode until such time as the primary interface goes down. When you issue a "show interface" command, the backup interface will display as "interface X is in standby mode, line protocol is down." Using the "backup load" feature, a link can be brought up temporarily in order to balance traffic when the primary link becomes overly congested. When the transmitted or received load on the primary line is greater than the value assigned to the enable-threshold argument, the secondary line is enabled.

The secondary line is then disabled when one of the following conditions occurs:

The transmitted load on the primary line plus the transmitted load on the secondary line is less than the value entered for the disable-load argument.

The received load on the primary line plus the received load on the secondary line is less than the value entered for the disable-load argument.

QUESTION 276:

Which two statements are true about the use of the backup load 65 10 command that was configured on one of the Certkiller routers? (Choose two)

- A. The secondary line will terminate when the load of the primary line drops to 10% of the bandwidth of the primary line.
- B. The secondary line will terminate when the aggregated load of the primary and backup lines drops to 10% of the primary line bandwidth.
- C. The secondary line will come up 10 seconds after traffic on the primary line reaches 65% of the bandwidth of the primary line.
- D. The secondary line will come up when the traffic on the primary line reaches 65% of the bandwidth of the primary line.
- E. The backup interface will come up 65 seconds after the primary link goes down.
- F. The secondary interface will terminate the connection 10 seconds after the primary link comes up.

Answer: B, D

Explanation:

To set a traffic load threshold for dial backup service, use the backup load interface configuration command. To return to the default value, use the no form of this command. The full syntax is as follows:

```
backup load {enable-threshold | never} {disable-load | never}
```

Syntax Description

<i>enable-threshold</i>	Percentage of the primary line's available bandwidth that the traffic load must exceed to enable dial backup.
<i>disable-load</i>	Percentage of the primary line's available bandwidth that the traffic load must be less than to disable dial backup.
never	Sets the secondary line never to be activated due to traffic load.

When the transmitted or received load on the primary line is greater than the value assigned to the enable-threshold argument, the secondary line is enabled.

The secondary line is disabled when one of the following conditions occurs:

1. The transmitted load on the primary line plus the transmitted load on the secondary line is less than the value entered for the disable-load argument.
2. The received load on the primary line plus the received load on the secondary line is less than the value entered for the disable-load argument.

If the never keyword is used instead of an enable-threshold value, the secondary line is never activated because of traffic load. If the never keyword is used instead of a disable-load argument, the secondary line is never activated because of traffic load.

Example:

The following example sets the traffic load threshold to 60 percent of the primary line serial 0. When that load is exceeded, the secondary line is activated, and will not be deactivated until the combined load is less than 5 percent of the primary bandwidth.

```
interface serial 0  
backup load 60 5  
backup interface serial 1
```

Reference:

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1828/products_command_reference_chapter09186a

QUESTION 277:

A company has unique dial requirements for each branch site that communicates with a central router. Which two commands permit multiple physical interfaces on a central router to be shared by multiple remote sites while retaining their unique site requirements? (Choose two.)

- A. dialer pool
- B. dialer-list
- C. dialer-group
- D. dialer hunt-group
- E. dialer pool-member

Answer: A, E

Explanation:

Dialer interfaces can be configured to use a specific dialing pool; in turn physical interfaces can be configured to belong to the same dialing pool. Using dialer pools allows for multiple physical interfaces to be shared by a logical pool.

Dialer Profile for ISDN BRI Backing Up Two Leased Lines Example:

The following example shows the configuration of a site that backs up two leased lines using one BRI. Two dialer interfaces are defined. Each serial (leased line) interface is configured to use one of the dialer interfaces as a backup. Both of the dialer interfaces use dialer pool 1, which has physical interface BRI 0 as a member. Thus, physical interface BRI 0 can back up two different serial interfaces and can make calls to two different sites.

```
interface dialer0  
ip unnumbered loopback0  
encapsulation ppp  
dialer remote-name Remote0  
dialer pool 1  
dialer string 5551212  
dialer-group 1  
interface dialer1  
ip unnumbered loopback0
```

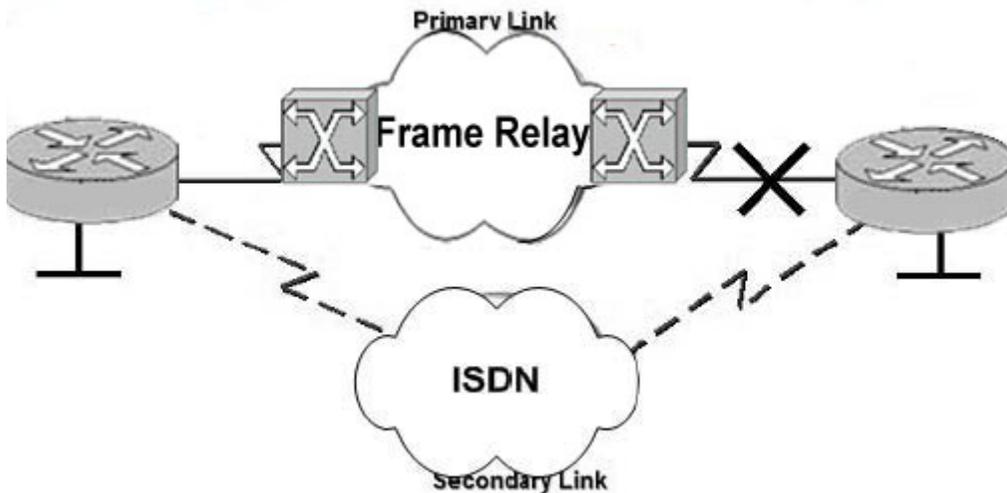
```
encapsulation ppp
dialer remote-name Remote1
dialer pool 1
dialer string 5551234
dialer-group 1
interface bri 0
encapsulation PPP
dialer pool-member 1
ppp authentication chap
interface serial 0
ip unnumbered loopback0
backup interface dialer 0
backup delay 5 10
interface serial 1
ip unnumbered loopback0
backup interface dialer1
backup delay 5 10
```

Reference:

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1826/products_configuration_guide_chapter09186a

QUESTION 278:

The Certkiller WAN is displayed in the diagram below:



For fault tolerance, Certkiller 1 is backing up its primary Frame Relay link with a secondary ISDN link. However, the link between Certkiller 2 and the service provider has failed, yet Certkiller 1 has remained in an up/up state because it is still exchanging LMIs with its FR switch. What two solutions would correct this situation? (Choose two.)

- A. Frame Relay end-to-end keepalive.
- B. Configure the load-interval feature.
- C. Configure dialer profiles.

- D. Configure the PVC monitor feature.
- E. Change the encapsulation to Frame Relay IETF.
- F. Configure point-to-point subinterfaces.

Answer: A, F

Explanation:

Frame Relay devices connect with each other through virtual circuits. Each virtual circuit is uniquely identified by a Data Link Connection Identifier (DLCI). In environments in which permanent virtual circuits (PVCs) are used, information regarding added or deleted PVCs and information about availability or unavailability of PVCs is carried through a Local Management Interface (LMI) with the use of status bits.

The Frame Relay switch within the local PVC segment deduces the status of the remote PVC segment through a Network-to-Network interface (NNI) and reports the status to the local router. If local management support within the switch is not end-to-end, the keepalive feature is the only source of information about the remote router. Frame Relay end-to-end keepalives provide status to verify that end-to-end communications are working and that traffic is getting through.

Benefits:

1. Enables monitoring of PVC status for network monitoring or backup applications
2. Bi-directional communication of PVC status
3. Configurable on a per PVC basis with configurable timers

Using this feature would fix the problem associated with the problem in this question.

Alternatively, using subinterfaces would work because the subinterface would go down, while the physical interface remained up. As long as the logical subinterface was not up, the ISDN link could be triggered to make the backup connection.

Reference:

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1830/products_feature_guide09186a0080087a58.html

QUESTION 279:

You are designing a Frame Relay network with a hub & spoke topology. What interface configuration combination would you use if you wanted inverse ARP to resolve addresses? (Choose two)

- A. Main interface at the hub router.
Point-to-point subinterface at the spoke routers.
- B. Point-to-point subinterface at the hub router.
Multipoint subinterface at the spoke routers.
- C. Point-to-point subinterface at the hub router.
Main interface at the spoke routers.
- D. Multipoint subinterface at the hub router.
Point-to-point subinterface at the spoke routers.

Answer: B, C

Explanation:

Frame Relay supports two types of interfaces: point-to-point and multipoint. The one you choose determines whether you need to use the configuration commands that ensure IP address to data-link connection identifier (DLCI) mappings. After configuring the PVC itself, you must tell the router which PVC to use in order to reach a specific destination.

Let's look at these options:

1. Point-to-point subinterface - With point-to-point subinterfaces, each pair of routers has its own subnet. If you put the PVC on a point-to-point subinterface, the router assumes that there is only one point-to-point PVC configured on the subinterface. Therefore, any IP packets with a destination IP address in the same subnet are forwarded on this VC. This is the simplest way to configure the mapping and is therefore the recommended method. Use the frame-relay interface-dlci command to assign a DLCI to a specified Frame Relay subinterface.

2. Multipoint networks - Multipoint networks have three or more routers in the same subnet. If you put the PVC in a point-to-multipoint subinterface or in the main interface (which is multipoint by default), you need to either configure a static mapping or enable inverse Address Resolution Protocol (ARP) for dynamic mapping.

In order to ensure that Inverse ARP resolves addresses across a hub and spoke topology, it is best to use single point to point subinterfaces for each PVC at the hub site.

Reference:

http://www.cisco.com/en/US/tech/CK4_82/CK6_07/technologies_configuration_example09186a0080094a7a.shtml

QUESTION 280:

The Certkiller WAN consists of a hub and spoke frame relay network. In a multipoint Frame Relay architecture; what is true about reachability issues? (Choose all that apply.)

- A. Split horizon can cause problems in NBMA environments.
- B. Subinterfaces can resolve split horizon issues.
- C. Split horizon is not an issue with multipoint subinterfaces.
- D. Subinterfaces do not apply in Frame Relay networks.
- E. Split horizon is an issue with point-to-point subinterfaces.
- F. A single physical interface can be configured to simulate multiple logical interfaces.
- G. All of the above.

Answer: A, B, F

Explanation:

The concept of sub interfaces was originally created in order to better handle issues caused by split-horizon over Non-Broadcast Multiple Access (NBMA) networks (e.g. frame relay, X.25) and distance-vector based routing protocols (e.g. IPX RIP/SAP, AppleTalk). Split-horizon dictates that a routing update received on an interface cannot be retransmitted out onto the same interface.

Multipoint interfaces/subinterfaces are still subject to the split-horizon limitations as discussed above. All nodes attached to a multipoint subinterface belong to the same network number. Typically, multipoint subinterfaces are used in conjunction with point-to-point interfaces in cases where an existing multipoint frame relay cloud is migrating to a subinterfaced point-to-point network design. A multipoint subinterface is used to keep remote sites on a single network number while slowly migrating remote sites to their own point-to-point subinterface network.

Configuring Frame Relay subinterfaces ensures that a single physical interface is treated as multiple virtual interfaces. This capability allows you to overcome split horizon rules so packets received on one virtual interface can be forwarded to another virtual interface, even if they are configured on the same physical interface.

References:

http://www.alliancedatacom.com/manufacturers/cisco-systems/framerelay_design/subinterfaces.asp

http://www.cisco.com/warp/public/116/fr_faq.html#21

QUESTION 281:

The performance and capabilities of Frame Relay is comparable to dedicated leased lines. What advantages does a Frame Relay connection have over a leased line?

(Choose all that apply.)

- A. Lower cost.
- B. Better suited multiple branch locations.
- C. Full guaranteed bandwidth.
- D. More control over the connection.
- E. None of the above

Answer: A, B

Explanation:

Frame Relay provides virtual circuit connectivity for enterprise networks that require 56 kbps up to T1/E1 speeds. It costs less than leased lines because it uses statistical multiplexing of packets to gain efficiencies within the network, at the cost of a less-stringent bandwidth and latency guarantee. Frame Relay is being widely deployed in enterprise networks to connect regional and branch offices into the enterprise backbone.

WAN Connection Summary	
Connection Type	Applications
Leased lines	High control, full bandwidth, high-cost enterprise networks, and last-mile access
Frame Relay	Medium control, shared bandwidth, medium-cost enterprise backbones; branch sites
ISDN	Low control, shared bandwidth, more bandwidth than dialup
Asynchronous dialup	Low control, shared bandwidth, variable cost, cost-effective for limited-use connections like DDR
X.25	Low control, shared bandwidth, variable cost, cost-effective for limited-use connections, high reliability

Reference:

http://www.cisco.com/en/US/products/hw/modules/ps2033/products_white_paper09186a0080091ca9.shtml

QUESTION 282:

Which of the following represent characteristics of a Frame Relay connection (Choose two)

- A. Branch site connectivity
- B. Circuit-switched
- C. High reliability
- D. Medium cost

Answer: A, D

Explanation:

Frame Relay provides virtual circuit connectivity for enterprise networks that require 56 kbps up to T1/E1 speeds. It costs less than leased lines because it uses statistical multiplexing of packets to gain efficiencies within the network, at the cost of a less-stringent bandwidth and latency guarantee. Frame Relay is being widely deployed in enterprise networks to connect regional and branch offices into the enterprise backbone.

WAN Connection Summary	
Connection Type	Applications
Leased lines	High control, full bandwidth, high-cost enterprise networks, and last-mile access
Frame Relay	Medium control, shared bandwidth, medium-cost enterprise backbones; branch sites
ISDN	Low control, shared bandwidth, more bandwidth than dialup
Asynchronous dialup	Low control, shared bandwidth, variable cost, cost-effective for limited-use connections like DDR
X.25	Low control, shared bandwidth, variable cost, cost-effective for limited-use connections, high reliability

Reference:

http://www.cisco.com/en/US/products/hw/modules/ps2033/products_white_paper09186a0080091ca9.shtml

QUESTION 283:

One of the Certkiller remote locations is connected to the HQ site via a frame relay link. A Frame Relay connection is essentially an interconnection process between which types of equipment? (Choose all that apply.)

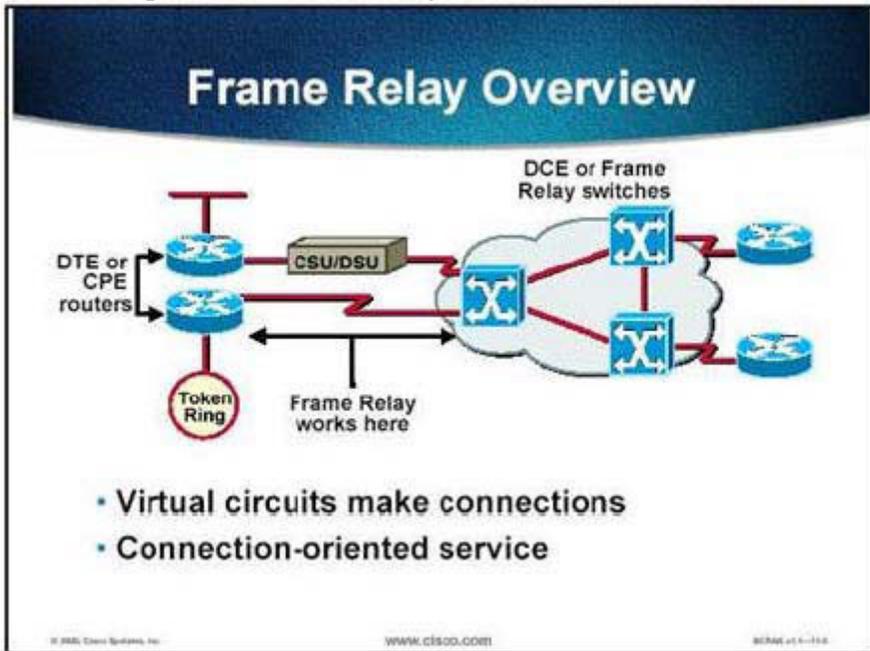
- A. DCE
- B. DTE
- C. PSTN
- D. PDN
- E. DSLAM
- F. None of the above

Answer: A, B

Explanation:

Frame Relay is an International Telecommunication Union Telecommunication Standardization Sector (ITU-T) and American National Standards Institute (ANSI) standard that defines the process for sending data over a public data network (PDN). It is a next-generation protocol to X.25 and is a connection oriented data-link technology that is streamlined to provide high performance and efficiency. It relies on upper-layer protocols for error correction and today's more dependable fiber and digital networks. Note that Frame Relay defines the interconnection process between your customer premises equipment (CPE) (also known as data terminal equipment [DTE]), such as a

router, and the service provider's local access switching equipment (known as data communications equipment [DCE]). It does not define how the data is transmitted within the service provider's Frame Relay cloud.



Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 11-4

QUESTION 284:

Switch CK1 is used as a frame relay switch. When this Frame Relay switch becomes locally congested, the header of a frame (moving towards the destination device) is changed to a 1. Which frame header bit is it?

- A. BECN
- B. MIR
- C. CIR
- D. FECN
- E. PIR
- F. None of the above

Answer: D

Explanation:

If a frame handler (i.e. Frame Relay router) suffers from congestion, it will notify the corresponding access nodes by FECN (C/R=0) and BECN (C/R=1) bits set to one. The access nodes won't accept frames that exceed the CIR any longer unless the congestion alarm has stopped (FECN=0, BECN=0).

When the congestion queue thresholds configured at the interface or class level of the PE router are exceeded, PE router does the following:

1. Sets the FECN bit to 1 on the outgoing packets.

2. Sets the BECN bit to 1 for all traffic destined for the originating CE router, which decreases its traffic based on the number of BECN packets it received.

FECN and BECN each is controlled by a single bit contained in the Frame Relay frame header. The Frame Relay frame header also contains a Discard Eligibility (DE) bit, which is used to identify less important traffic that can be dropped during periods of congestion. The FECN bit is part of the Address field in the Frame Relay frame header. The FECN mechanism is initiated when a DTE device sends Frame Relay frames into the network. If the network is congested, DCE devices (switches) set the value of the frames' FECN bit to 1. When the frames reach the destination DTE device, the Address field (with the FECN bit set) indicates that the frame experienced congestion in the path from source to destination. The DTE device can relay this information to a higher-layer protocol for processing. Depending on the implementation, flow control may be initiated, or the indication may be ignored.

The BECN bit is part of the Address field in the Frame Relay frame header. DCE devices set the value of the BECN bit to 1 in frames traveling in the opposite direction of frames with their FECN bit set. This informs the receiving DTE device that a particular path through the network is congested. The DTE device then can relay this information to a higher-layer protocol for processing. Depending on the implementation, flow-control may be initiated, or the indication may be ignored.

Reference: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/frame.htm

QUESTION 285:

It is possible to support multiple logical Frame Relay virtual circuits over the same physical serial connection. How does this happen?

- A. The DCE provides multiple time slots in which to send specific VC data streams.
- B. The DTE encapsulates packets with a header containing an identifier for each VC.
- C. The Frame Relay switch uses inverse ARP to map the Layer 3 address to a DLCI for each VC.
- D. The DTE channelizes the bandwidth into multiple 64K circuits, each supporting a separate VC.
- E. None of the above

Answer: B

Explanation:

Frame Relay provides a means for statistically multiplexing many logical data conversations (referred to as virtual circuits) over a single physical transmission link by assigning connection identifiers to each pair of DTE devices. The service provider's switching equipment constructs a table that maps connection identifiers to outbound ports. When a frame is received, the switching device analyzes the connection identifier and delivers the frame to the pre-established, associated outbound port.

The virtual circuits can be either permanent virtual circuits (PVCs) or switched virtual circuits (SVCs). PVCs are permanently established connections that are used when there is frequent and consistent data transfer between DTE devices across a Frame Relay

network.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Chapter 11-5

QUESTION 286:

Within the Certkiller network, multiple frame PVC's are used to connect all of the locations. In which three states can a Frame Relay permanent virtual circuit (PVC) occur? (Select three)

- A. Down
- B. Deleted
- C. Init
- D. Inactive
- E. Active
- F. Operational

Answer: B, D, E

Explanation:

The show frame-relay pvc command displays the status of each configured connection as well as traffic statistics. This command is also useful for viewing the number of backward explicit congestion notification (BECN) and forward explicit congestion notification (FECN) packets received by the router. The PVC STATUS can be active, inactive, or deleted.

If you enter show frame-relay pvc, you will see the status of all the PVCs configured on the router. If you specify a specific PVC, you will only see the status of that PVC. In the figure, the show frame-relay pvc 110 command only displays the status of PVC 110.

Verifying Frame Relay Operation (cont.)

```
Router#show frame-relay pvc 110
PVC Statistics for interface Serial0 (Frame Relay DTE)
DLCI = 110, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0
input pkts 14055 output pkts 32795 in bytes 1096228
out bytes 6216155 dropped pkts 0 in FECN pkts 0
in BECN pkts 0 out FECN pkts 0 out BECN pkts 0
in DE pkts 0 out DE pkts 0
out broadcast pkts 32795 out broadcast bytes 6216155
<Output Omitted>
```

- Displays PVC traffic statistics

© 2000, Cisco Systems, Inc. www.cisco.com BCRN v1.1-11-11

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 11-12

QUESTION 287:

Router CK1 is configured for frame relay and has the LMI auto-sensing feature enabled. What's true about LMI auto-sensing? (Choose all that apply)

- A. It involves sending full status requests to the Frame Relay switch.
- B. It is used to automatically detect the Frame Relay CIR of each PVC.
- C. It is used to tell the router about LMI type.
- D. It only works if the Frame Relay LMI type is cisco.

Answer: A,C

Explanation:

Local Management Interface (LMI) is a signaling standard between the CPE device and the Frame Relay switch that is responsible for managing the connection and maintaining status between the devices. LMIs include support for a keepalive mechanism, which verifies that data is flowing; a multicast mechanism, which provides the network server with its local DLCI; the multicast addressing, which gives DLCIs global rather than local significance in Frame Relay networks; and a status mechanism, which provides an ongoing status on the DLCIs known to the switch.

Although the LMI is configurable, beginning in Release 11.2, the Cisco router tries to autosense which LMI type the Frame Relay switch is using by sending one or more full status requests to the Frame Relay switch. The Frame Relay switch responds with one or more LMI types. The router configures itself with the last LMI type received. Three

types of LMIs are supported:

1. cisco - LMI type defined jointly by Cisco, StrataCom, Northern Telecom, and Digital Equipment Corporation, nicknamed "the gang of four"
2. ansi - Annex D, defined by the ANSI standard T1.617
3. q933a - ITU-T Q.933 Annex A

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 11-7

QUESTION 288:

While troubleshooting a Frame Relay connection, you discover that the PVC status is being reported as deleted. What is most likely causing this problem?

- A. The PVC is not configured on the CSU/DSU.
- B. The PVC is not configured on the remote router.
- C. The PVC is not configured on the local router.
- D. The PVC is not configured on the Frame Relay switch.
- E. All of the above could cause this

Answer: C

Explanation:

If an LMI status report indicates that a PVC is not active, then it is marked as inactive. A PVC is marked as deleted if it is not listed in a periodic LMI status message.

When the interface is configured as a DCE and the DLCI usage is SWITCHED, the value displayed in the PVC STATUS field is determined by the status of outgoing interfaces (up or down) and status of the outgoing PVC.

The status of the outgoing PVC is updated in the local management interface (LMI) message exchange. PVCs terminated on a DCE interface use the status of the interface to set the PVC STATUS.

If the outgoing interface is a tunnel, the PVC status is determined by what is learned from the tunnel. If an LMI status report indicates that a PVC is not active, then it is marked as inactive. A PVC is marked as deleted if it is not listed in a periodic LMI status message, such as when the remote frame switch is configured for a specific PVC while the router is not.

QUESTION 289:

What is true about a Frame Relay data-link connection identifier (DLCI)? (Choose all that apply)

- A. DLCI is assigned by the customer and applied to their CPE.
- B. DLCI is assigned by the Frame Relay service provider.
- C. DLCI must be identical on all DTE devices.
- D. DLCI has a local significance only.
- E. DLCI has remote significance only.

F. None of the above

Answer: B, D

Explanation:

The DLCI is a number that is tagged to the virtual circuit of the service provider. Since the number is determined on a 'per-leg' basis during data transmission, so it's only locally significant. The number only has to be agreed upon by the two frame relay devices directly connected to each other. Although a specific DLCI number can be requested from the customer, the DLCI is assigned from the frame relay provider.

QUESTION 290:

Which of the following terms describes the committed average rate that a Frame Relay switch transfers data at during periods of non-congestion?

- A. Committed burst rate
- B. Excess burst rate
- C. Local access rate
- D. CIR
- E. MIR
- F. PIR
- G. BCR

Answer: D

Explanation:

The CIR (committed information rate) is the rate that an administrator would want to transmit at during times when the network isn't congested. The CIR that you want isn't necessarily the same as the CIR of the service provider. CIR rates are purchased from the provider. When the data rates exceed the CIR, the frames are marked as Discard Eligible (DE) and are not guaranteed to be delivered across the frame relay network.

Reference: CCNP Remote Access Exam Certification Guide, page 270, Brian Morgan & Craig Dennis, Cisco Press 2001, ISBN 1-58720-003-1

QUESTION 291:

You are tasked with the IP address assignment of the Certkiller frame relay network. With regards to network layer address assignment, which of the following are true regarding the effects of using frame relay sub interfaces on a physical interface?

- A. The network layer address of each sub interface must be in the same subnet as the physical interface address.
- B. The network layer address of each sub interface must be approved by IANA
- C. The network layer address must be removed from the physical interface.

- D. The network layer address of each sub interface must be the same as the physical interface address.
- E. The sub interfaces should be assigned the network broadcast address of the physical interface.
- F. None of the above.

Answer: C

Explanation:

Frame Relay subinterfaces provide a mechanism for supporting partially meshed Frame Relay networks. Most protocols assume transitivity on a logical network; that is, if station A can talk to station B, and station B can talk to station C, then station A should be able to talk to station C directly. Transitivity is true on LANs, but not on Frame Relay networks unless A is directly connected to C. Additionally, certain protocols such as AppleTalk and transparent bridging cannot be supported on partially meshed networks because they require "split horizon," in which a packet received on an interface cannot be sent from the same interface even if received and transmitted on different VCs.

Configuring Frame Relay subinterfaces ensure that a single physical interface is treated as multiple virtual interfaces, which allows you to overcome split horizon rules. Packets received on one virtual interface can be forwarded to another virtual interface, even if they are configured on the same physical interface. Subinterfaces address the limitations of Frame Relay networks by providing a way to subdivide a partially meshed Frame Relay network into a number of smaller, fully meshed (or point-to-point) subnetworks. Each subnetwork is assigned its own network number and appears to the protocols as if it is reachable through a separate interface. (Note that point-to-point subinterfaces can be unnumbered for use with IP, reducing the addressing burden that might otherwise result.)

QUESTION 292:

Which of the following components make up the Frame Relay frame (Choose all that apply)?

- A. The parity portion
- B. Header and address area
- C. Frame check sequence
- D. Security bit
- E. User-data portion

Answer: B, C, E

Explanation:

Flags indicate the beginning and end of the frame. Three primary components make up the Frame Relay frame: the header and address area, the user-data portion, and the frame check sequence (FCS). The address area, which is 2 bytes in length, is comprised of 10 bits representing the actual circuit identifier and 6 bits of fields related to congestion

management. This identifier commonly is referred to as the data-link connection identifier (DLCI).

QUESTION 293:

Which of the following LMI extensions are considered to be optional? (Choose all that apply)

- A. Multicasting
- B. Simple flow control
- C. Virtual circuit status messages
- D. Global addressing

Answer: A, B, D

Explanation:

In addition to the basic Frame Relay protocol functions for transferring data, the consortium Frame Relay specification includes LMI extensions that make supporting large, complex internetworks easier. Some LMI extensions are referred to as "common" and are expected to be implemented by everyone who adopts the specification. Other LMI functions are referred to as "optional." A summary of the LMI extensions follows: Virtual circuit status messages (common)-Provide communication and synchronization between the network and the user device, periodically reporting the existence of new PVCs and the deletion of already existing PVCs, and generally provide information about PVC integrity. Virtual circuit status messages prevent the sending of data into black holes-that is, over PVCs that no longer exist.

Multicasting (optional)-Allows a sender to transmit a single frame but have it delivered by the network to multiple recipients. Thus, multicasting supports the efficient conveyance of routing protocol messages and address resolution procedures that typically must be sent to many destinations simultaneously.

Global addressing (optional)-Gives connection identifiers global rather than local significance, allowing them to be used to identify a specific interface to the Frame Relay network. Global addressing makes the Frame Relay network resemble a local-area network (LAN) in terms of addressing; Address Resolution Protocols, therefore, perform over Frame Relay exactly as they do over a LAN.

Simple flow control (optional)-Provides for an XON/XOFF flow control mechanism that applies to the entire Frame Relay interface. It is intended for devices whose higher layers cannot use the congestion notification bits and that need some level of flow control.

QUESTION 294:

With Frame Relay, a communication session across an SVC consists of how many operational states?

- A. Four
- B. Five

- C. One
- D. Three
- E. Two

Answer: A

Explanation:

Switched virtual circuits (SVCs) are temporary connections used in situations requiring only sporadic data transfer between DTE devices across the Frame Relay network. A communication session across an SVC consists of the following four operational states:

Call setup-The virtual circuit between two Frame Relay DTE devices is established.

Data transfer-Data is transmitted between the DTE devices over the virtual circuit.

Idle-The connection between DTE devices is still active, but no data is transferred. If an SVC remains in an idle state for a defined period of time, the call can be terminated.

Call termination-The virtual circuit between DTE devices is terminated.

QUESTION 295:

Is the following statement true or false?

The primary benefit of the use of the FECN and BECN fields in Frame Relay is for the purpose of congestion indications.

- A. False
- B. True
- C. True only for IOS V11 or above
- D. True only for IOS V12 or above

Answer: B

Explanation:

Forward-explicit congestion notification (FECN) is a single-bit field that can be set to a value of 1 by a switch to indicate to an end DTE device, such as a router, that congestion was experienced in the direction of the frame transmission from source to destination.

The primary benefit of the use of the FECN and BECN fields is the capability of higher-layer protocols to react intelligently to these congestion indicators. Today, DECnet and OSI are the only higher-layer protocols that implement these capabilities.

Backward-explicit congestion notification (BECN) is a single-bit field that, when set to a value of 1 by a switch, indicates that congestion was experienced in the network in the direction opposite of the frame transmission from source to destination.

QUESTION 296:

In Frame Relay, what bit is used to indicate that a frame has lower importance than other frames?

- A. DA

- B. DT
- C. DE
- D. DL
- E. C bit

Answer: C

Explanation:

The Discard Eligibility (DE) bit is used to indicate that a frame has lower importance than other frames. The DE bit is part of the Address field in the Frame Relay frame header.

DTE devices can set the value of the DE bit of a frame to 1 to indicate that the frame has lower importance than other frames. When the network becomes congested, DCE devices will discard frames with the DE bit set before discarding those that do not. This reduces the likelihood of critical data being dropped by Frame Relay DCE devices during periods of congestion.

QUESTION 297:

In the Certkiller frame relay network, the LMI signaling multicast mechanism is intended for which of the following?

- A. Providing outgoing status on known DLCIs
- B. Providing network server with its remote DLCI
- C. Providing network server with its local DLCI
- D. Verifying data flow
- E. None of the above

Answer: C

Explanation:

The Cisco implementation of frame relay provides support for a keepalive mechanism, a multicast group, and a status message, as follows:

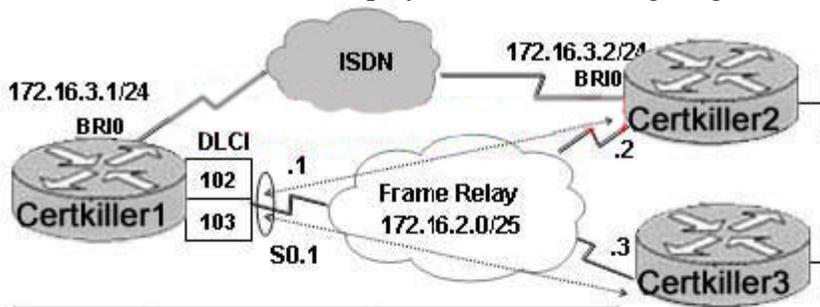
1. The keepalive mechanism provides an exchange of information between the network server and the switch to verify that data is flowing.
2. The multicast mechanism provides the network server with its local data link connection identifier (DLCI) and the multicast DLCI. This feature is specific to the Cisco implementation of the Frame Relay joint specification.
3. The status mechanism provides an ongoing status report on the DLCIs known by the switch.

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products_configuration_guide_chapter09186a008008

QUESTION 298:

The Certkiller network is displayed in the following diagram.



```

Certkiller1# show running-config
!
interface Serial0
encapsulation frame-relay
!
interface Serial0.1
backup interface bri0
ip address 172.16.2.1 255.255.255.128
frame-relay map ip 172.16.2.2 102 broadcast
frame-relay map ip 172.16.2.3 103 broadcast
!
interface BRI0
ip address 172.16.3.1 255.255.255.0
encapsulation ppp
dialer map ip 172.16.3.2 name R2 broadcast 5552000
dialer-group 1
!
router eigrp 4
network 172.16.0.0
!
access-list 100 deny eigrp any any
access-list 100 permit ip any any
!
dialer-list 1 protocol ip list 100

```

Certkiller 1 is connected with a multipoint subinterface over the Frame Relay to the spoke routers Certkiller 2 and Certkiller 3. The ISDN interface is configured to provide a back-up link should the primary connection to Certkiller 2 fail. However, when the PVC to Certkiller 2 drops, the BRI interface remains in "standby" mode and does not bring up the back-up link. Based on the information and the configuration file shown above, what could the problem be?

- A. The EIGRP updates are configured as noninteresting traffic.
- B. The backup command is configured under the S0.1 multipoint interface of Certkiller 1.
- C. The CertKiller1 S0 interface remains up because of the active PVC between Certkiller 1 and Certkiller 3.
- D. The CertKiller1 S0.1 interface remains up because of the active PVC between Certkiller 1 and Certkiller 3.

Answer: D

Explanation:

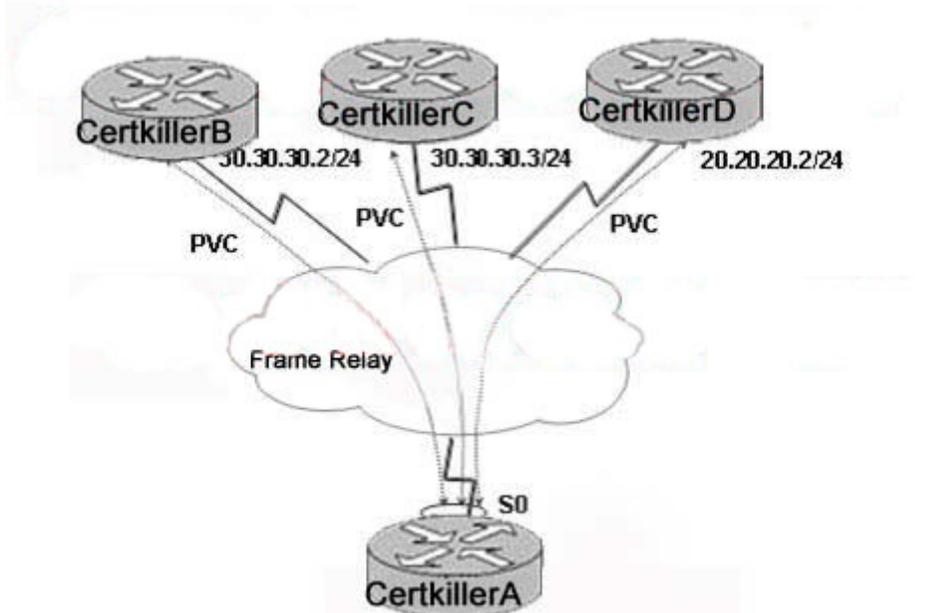
Using the backup interface in this configuration tells the router to initiate an ISDN call on

interface BRI0 when the line protocol on sub-interface serial 0.1 goes down. However, since there are two separate frame relay maps configured the sub-interface will remain up as long as at least one of the PVC's is operational.

Note: Placing the "backup interface" command under interface serial 0 would not help in this situation, since all sub-interfaces must be down in order for the physical interface to go down. The best way to accomplish the goal of this network is to create a separate subinterface for the connection to Certkiller 2 and place the "backup interface" command there.

QUESTION 299:

The Certkiller frame relay network is displayed in the following diagram:



Which subinterface configuration options will allow for full IP connectivity between Certkiller A and the spoke routers?

- A. Certkiller A(config)# interface S0.1 point-to-point
Certkiller A(config)# interface S0.2 point-to-point
Certkiller A(config)# interface S0.3 point-to-point
- B. Certkiller A(config)# interface S0.1 multipoint
Certkiller A(config)# interface S0.2 multipoint
Certkiller A(config)# interface S0.3 multipoint
- C. Certkiller A(config)# interface S0.1 multipoint
Certkiller A(config)# interface S0.2 point-to-point
Certkiller A(config)# interface S0.3 point-to-point
- D. Certkiller A(config)# interface S0.1 multipoint
Certkiller A(config)# interface S0.2 point-to-point
Certkiller A(config)# interface S0.3 point-to-point
- E. Certkiller A(config)# interface S0.1 multipoint
Certkiller A(config)# interface S0.2 multipoint
Certkiller A(config)# interface S0.3 point-to-point

Answer: C

Explanation:

Since routers Certkiller B and Certkiller C both belong to the same IP subnet on the WAN, a single multipoint subinterface would be sufficient to provide for connectivity to them from the hub router Certkiller

A. After this is done, only a single point to point subinterface needs to be created to router Certkiller D. This subinterface needs to be created because Certkiller D resides in a separate IP subnet than the other 2 routers. With choice C, interface s0.1 will be configured with an IP address in the 30.30.30.0/24 range, and interface s0.2 will be configured with an IP address in the 20.20.20.0/24 range.

QUESTION 300:

Which statement best describes a digital certificate, which is being implemented in the Certkiller network as a VPN technology?

- A. A digital identification mechanism which establishes credentials issued by a certification authority.
- B. A network service that issues and manages security credentials and public keys for e-mail encryption.
- C. An digital signature that can authenticate the identity of the sender of a message or the signer of a document.
- D. An algorithm provided by a designated authority used as an encryption key.

Answer: A

Explanation:

While IPSec provides the core technology for VPNs, integrating digital certificates ensures scalability and the highest possible security.

Authentication in IPSec can be provided through the use of digital certificates or shared secrets. These two approaches differ in security, in conceptual complexity, in the level of control they allow over communications, and in the amount of additional equipment required to use them.

Authentication that depends on shared secrets, although easy to implement, is practical only in small VPNs and where the trust within a domain is uniform. For two nodes to communicate securely through the public network using shared secrets, they must be configured with identical shared secrets. The distribution of the shared secret in the first place can only be carried out in a separate out-of-band secure channel. The management of the shared secrets becomes more difficult as the number of nodes involved in the communication becomes large ($[N \cdot \sup{2}]$ problem), because new secrets are typically distributed manually on a pairwise unique basis. Therefore, it is difficult to scale a shared secret-based VPN.

Digital certificates, on the other hand, use a trusted third-party authentication system,

which scales linearly when the number of involved parties becomes Large. A CA (certification authority) is an entity trusted by all the certificate users or that has been granted power to issue digital certificates and vouch for the binding between data items contained in a certificate. The CA manages the life cycle of certificates and, depending on the type of certificate and the certification practice statement that applies, may be responsible for the life cycle of key pairs associated with the certificates.

In a digital world, a digital certificate is like a passport, only more secure: The digital signature of the issuing CA guarantees the certificate's authenticity. It is impossible to forge a digital signature unless one knows the signing private key.

Reference: http://www.findarticles.com/p/articles/mi_m0TLC/is_8_34/ai_65142156

QUESTION 301:

In some applications TACACS+ and RADIUS are NOT suitable for authentication, so a technician will implement Kerberos instead. What kind of circumstances would dictate the use of Kerberos?

- A. The usage of various router functions needs to be accounted for by user name.
- B. Multiple level of authorization need to be applied to various router commands.
- C. DES encrypted authentication is required.
- D. Authentication, authorization and accounting need to use a single database.
- E. The utilization of authentication functions needs to be authorized by user names and passwords.

Answer: C

Explanation:

The Kerberos protocol uses strong cryptography so that a client can prove its identity to a server (and vice versa) across an insecure network connection. After a client and server has used Kerberos to prove their identity, they can also encrypt all of their communications to assure privacy and data integrity as they go about their business.

Kerberos is a network authentication protocol developed by MIT. Kerberos can provide authentication only. It doesn't have the capability to perform authorization. Some sites with existing Kerberos servers use Kerberos for authentication, while using TACACS+ or RADIUS for authorization.

Encryption in Kerberos is based on DES, the Data Encryption Standard. The encryption library implements those routines. Several methods of encryption are provided, with tradeoffs between speed and security. An extension to the DES Cypher Block Chaining (CBC) mode, called the Propagating CBC mode, is also provided. In CBC, an error is propagated only through the current block of the cipher, whereas in PCBC, the error is propagated throughout the message. This renders the entire message useless if an error occurs, rather than just a portion of it. The encryption library is an independent module, and may be replaced with other DES implementations or a different encryption library.

References:

<http://web.mit.edu/kerberos/www/>

http://www.cisco.com/en/US/tech/CK5_83/CK3_85/technologies_white_paper09186a00800941b2.shtml

QUESTION 302:

You are a network design consultant and you've just been contracted by a human resource company to explain to them the benefits of a remote access server; more specifically, what kind of workers could benefit the most from them. How would you respond?

- A. Mobile sales force requiring dial-in access.
- B. Corporate staff requiring access to web-bases applications.
- C. Mobile sales force requiring dedicated connection.
- D. Corporate staff requiring access to applications on corporate systems.
- E. None of the above

Answer: A

Explanation:

A router acts as an access server, which is a concentration point for dial-in and dial-out calls. Mobile users, for example, can call into an access server at a central site to access their e-mail messages. The biggest users of remote access servers are mobile employees that need occasional, temporary connections into the network.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 2-8

QUESTION 303:

You are an administrator of a rapidly expanding company and your network is based on a Cisco 2511 access server. All 16 of its asynchronous interfaces have been configured to permit simultaneous remote access, leaving only one AUX port available for remote administration via modem. What line number must you use to configure this remote administration aux port for the modem?

- A. Line 0
- B. Line 17
- C. Line 1
- D. Line 18
- E. Line 7

Answer: B

Explanation:

The following lines are used in Cisco IOS:

0 is specified for the console line

TTY lines 1-16 are used for the asynchronous lines.

Line 17 is reserved for the aux port.

QUESTION 304:

Identify two characteristics of the RADIUS protocol when associated with AAA.
(Choose two)

- A. Uses TCP
- B. Fully encrypts the body of the packet.
- C. Based upon open standards.
- D. Allows router commands to be grouped on a per-user or per-group basis.
- E. Combines the functions of authorization and authentication.

Answer: C, E

Explanation:

Cisco Systems uses a strategy known as authentication, authorization, and accounting (AAA) for verifying the identity of, granting access to, and tracking the actions of remote users. In today's networks, the Terminal Access Controller Access Control System plus (TACACS+) and Remote Access Dial-In User Service (RADIUS) protocols are commonly used to provide AAA solutions.

The RADIUS protocol was developed by Livingston Enterprises, Inc., as an access server authentication and accounting protocol. Implemented by several vendors of network access servers, RADIUS has gained support among a wide customer base, including Internet service providers (ISPs). The RADIUS authentication protocol is documented separately from the accounting protocol, but the two can be used together for a comprehensive solution.

The RADIUS protocol combines the processes of authentication and authorization. The Access-Accept packets sent by the RADIUS server to the client contain all the authorization information, making separation of the authentication and authorization functions difficult. The use of RADIUS is most appropriate when simple, single-step authentication and authorization is required, as with most service provider networks. In June 1996, draft 5 of the RADIUS protocol specification was submitted to the Internet Engineering Task Force (IETF). The RADIUS specification (RFC 2058) and RADIUS accounting standard (RFC 2059) are now proposed standard protocols. The text of the IETF proposed standards can be found at the following URLs:

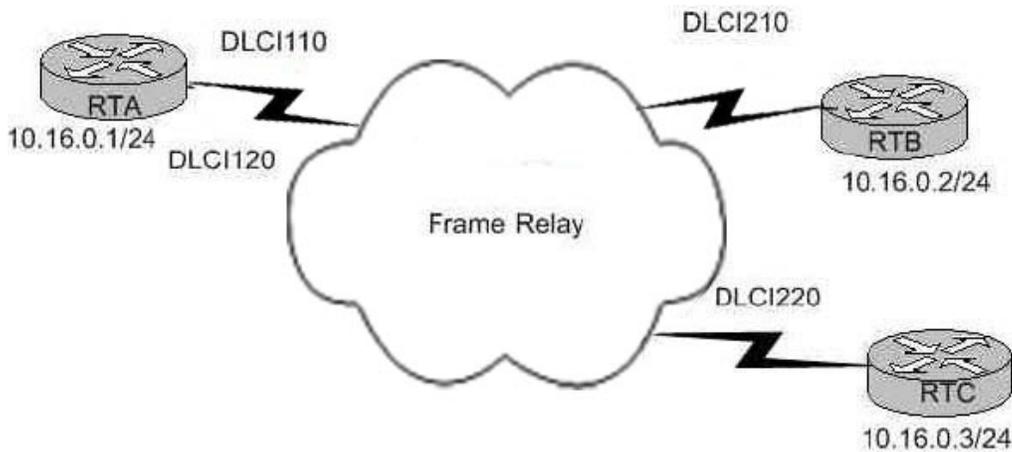
<ftp://ds.internic.net/rfc/rfc2058.txt>

Reference:

http://www.cisco.com/en/US/tech/CK59/technologies_white_paper09186a00800a3c92.shtml

QUESTION 305:

The Certkiller network is displayed in the following diagram:



RTA is the hub router, with RTB and RTC configured as spokes. Currently no spoke router can ping any other spoke router, but all spoke routers can ping the hub. There are no routing protocols configured and Inverse ARP is enabled. What must the administrator do to correct the problem?

- A. Configure static map commands on the hub router.
- B. Configure static map commands on all spoke routers.
- C. Configure subinterfaces on the hub router.
- D. Configure subinterfaces on all spoke routers.
- E. Enable split horizon on the hub router.
- F. Disable split horizon on all spoke routers.

Answer: B

Explanation:

Frame Relay supports two types of interfaces: point-to-point and multipoint. The one you choose determines whether you need to use the configuration commands that ensure IP address to data-link connection identifier (DLCI) mappings. After configuring the PVC itself, you must tell the router which PVC to use in order to reach a specific destination. Let's look at these options:

1. Point-to-point subinterface - With point-to-point subinterfaces, each pair of routers has its own subnet. If you put the PVC on a point-to-point subinterface, the router assumes that there is only one point-to-point PVC configured on the subinterface. Therefore, any IP packets with a destination IP address in the same subnet are forwarded on this VC. This is the simplest way to configure the mapping and is therefore the recommended method. Use the frame-relay interface-dlci command to assign a DLCI to a specified Frame Relay subinterface.

2. Multipoint networks - Multipoint networks have three or more routers in the same subnet. If you put the PVC in a point-to-multipoint subinterface or in the main interface (which is multipoint by default), you need to either configure a static mapping or enable inverse Address Resolution Protocol (ARP) for dynamic mapping.

In order to ensure that Inverse ARP resolves addresses across a hub and spoke topology, it is best to use single point to point subinterfaces for each PVC at the hub site.

Alternatively, use static map entries on the spoke routers. Since the remote spoke routers can already ping the hub site, there is no need to add static entries on the hub router.

QUESTION 306:

Which two encapsulation methods require that an 827 ADSL router be configured with a PPP username and CHAP password? (Choose two)

- A. PPPoE with the 827 configured as a bridge.
- B. PPPoE with the 827 configured as the PPPoE client.
- C. PPPoA
- D. RFC 1483 Bridged with the 827 configured as the PPPoE client.
- E. RFC 1482 Bridged with the 827 configured as a bridge.

Answer: B, C

Explanation:

When using the Point to Point Protocol over Ethernet (PPPoE) or the Point to Point Protocol over ATM (PPPoA), you must configure a PPP username and password to match the settings configured from the Internet Service Provider. This is required for both PPPoE and PPPoA in order to overcome some of the security concerns of these two Internet access methods.

QUESTION 307:

What command should you use to specify RADIUS as the method of user authentication when no other method list has been defined? (Type in answer below)

Answer: aaa authentication ppp default radius

Explanation:

Use the aaa authentication ppp command with the radius method keyword to specify RADIUS as the authentication method for use on interfaces running PPP. Before you can use RADIUS as the authentication method, you need to enable communication with the RADIUS security server.

QUESTION 308:

TO better accommodate for the growing number of remote access users, Certkiller is implementing CiscoSecure. Which of the following are the three major components of Cisco Secure (Choose all that apply)?

- A. L2TP
- B. RDBMS
- C. Packet filter firewall
- D. Netscape Fast Track Server

- E. AAA Server
- F. Track Server

Answer: B, D, E

Explanation:

RDBMS synchronization import definitions are a listing of the action codes allowable in an accountActions table. The RDBMS Synchronization feature of CiscoSecure AccessControlServer (ACS) for WindowsServer uses a table named "accountActions" as input for automated or manual updates of the CiscoSecure user database.

CiscoSecure supports both Cisco network access servers (such as the Cisco 2509, 2511, 3620, 3640, and AS5200) and the PIX firewall. It is a basic access control server (ACS) for Windows NT Server Version 4.0. CiscoSecure uses the Terminal Access Controller Access Control System (TACACS)+ protocol to provide Authentication, Authorization, and Accounting (AAA) to ensure a secure environment. This enables you to control access to your network from a central location.

QUESTION 309:

CORRECT TEXT

What command should you use so that your access server will attempt to authenticate all incoming calls that start a PPP session with CHAP, and will use PAP only if the remote device does not support CHAP? (Type in answer below)

Answer: ppp authentication chap pap

Explanation:

If the remote device does not support chap then use pap. So chap must be first mentioned before pap in the command. With this configuration, PAP will be used only should the remote device not support CHAP.

Note:

If you configure ppp authentication chap on an interface, all incoming calls on that interface that initiate a PPP connection will have to be authenticated using CHAP; likewise, if you configure ppp authentication pap, all incoming calls that start a PPP connection will have to be authenticated via PAP. If you configure ppp authentication chap pap, the access server will attempt to authenticate all incoming calls that start a PPP session with CHAP. If the remote device does not support CHAP, the access server will try to authenticate the call using PAP. If the remote device doesn't support either CHAP or PAP, authentication will fail and the call will be dropped. If you configure ppp authentication pap chap, the access server will attempt to authenticate all incoming calls that start a PPP session with PAP. If the remote device does not support PAP, the access server will try to authenticate the call using CHAP. If the remote device doesn't support either protocols, authentication will fail and the call will be dropped. If you configure the ppp authentication command with the callin keyword, the access server will only authenticate the remote device if the remote device initiated the call.

QUESTION 310:

CORRECT TEXT

What command should you use to enable AAA authentication regardless of the supported login authentication methods to use? (Type in answer below)

Answer: aaa authentication login

Explanation:

The AAA security services facilitate a variety of login authentication methods. Use the "aaa authentication login" command to enable AAA authentication no matter which of the supported login authentication methods you decide to use. With the "aaa authentication login" command, you create one or more lists of authentication methods that are tried at login. These lists are applied using the login authentication line configuration command.

QUESTION 311:

What AAA command should you use to specify the local username database as the authentication method for use on lines running PPP when no other method list has been defined? (Type in answer below)

Answer: aaa authentication ppp default local

Explanation:

Use the "aaa authentication ppp" command with the method keyword local to specify that the Cisco router or access server will use the local username database for authentication. For example, to specify the local username database as the method of authentication for use on lines running PPP when no other method list has been defined, enter:
aaa authentication ppp default local

QUESTION 312:

On router CK1 , you need to specify the location of a new CiscoSecure server that was just installed. Which of the following indicates the address of the CiscoSecure server in your network?

- A. en tacacs-server host
- B. server host tacacs
- C. tacacs-server en
- D. tacacs-server host
- E. None of the above

Answer: D

Explanation:

The tacacs-server host command allows you to specify the names of the IP host or hosts maintaining a TACACS server. Because the TACACS software searches for the hosts in the order specified, this feature can be useful for setting up a list of preferred servers. To specify a TACACS+ host, use the tacacs-server host command in global configuration mode. Use the no form of this command to delete the specified name or address.
tacacs-server host hostname [single-connection] [port integer] [timeout integer] [key string]

Syntax Description

<i>hostname</i>	Name or IP address of the host.
<i>single-connection</i>	(Optional) Specify that the router maintain a single open connection for confirmation from a AAA/TACACS+ server (CiscoSecure Release 1.0.1 or later). This command contains no autodetect and fails if the specified host is not running a CiscoSecure daemon.
<i>port</i>	(Optional) Specify a server port number. This option overrides the default, which is port 49.
<i>integer</i>	(Optional) Port number of the server. Valid port numbers range from 1 to 65535.
<i>timeout</i>	(Optional) Specify a timeout value. This overrides the global timeout value set with the tacacs-server timeout command for this server only.
<i>integer</i>	(Optional) Integer value, in seconds, of the timeout interval.
<i>key</i>	(Optional) Specify an authentication and encryption key. This must match the key used by the TACACS+ daemon. Specifying this key overrides the key set by the global command tacacs-server key for this server only.
<i>string</i>	(Optional) Character string specifying authentication and encryption key.

QUESTION 313:

CORRECT TEXT

What keyword of the aaa authentication login command do you use to specify the line password as the login authentication method? (Type in answer below)

Answer: line

Explanation:

According to the technical documentation at CCO: Use the aaa authentication login command with the line method keyword to specify the line password as the login authentication method. For example, to specify the line password as the method of user authentication at login when no other method list has been defined, enter the following:
aaa authentication login default line

QUESTION 314:

You need to have what type of connection to connect an AAA server to the Certkiller network?

- A. Serial interface
- B. Synchronous call
- C. T1
- D. Ethernet
- E. Asynchronous call
- F. ISDN PRI
- G. T3

Answer: D

Explanation:

Like other network servers, the only connections that can be used to connect to the network is via the Ethernet Network Interface Card (NIC) or ethernet interface on the server.

QUESTION 315:

A new CiscoSecure ACS is being installed in the Certkiller network. Which of the following are components of the CiscoSecure ACS server? (Choose all that apply)

- A. AAA server
- B. Netscape Fastrack server
- C. RDBMS
- D. RADIUS Interface

Answer: A, B, C

Explanation:

The CiscoSecure ACS consists of several interrelated software modules that carry out different communication, profile data retrieval, profile data storage, administrative, and performance-enhancement functions. Understanding the interaction of these modules is useful for troubleshooting or fine tuning CiscoSecure ACS performance.

The CiscoSecure ACS components include:

1. The AAA Server
2. The DBServer
3. The relational database management system (RDBMS)
4. The two web server modules: Netscape FastTrack and Acme FastAdmin
5. The optional Distributed Sessions Manager (DSM)
6. The command-line interface (CLI) module

Reference:

http://www.cisco.com/en/US/products/sw/secursw/ps4911/products_user_guide_chapter09186a00800eca43.htm

QUESTION 316:

Which of the following networks would be the most suitable candidates for traffic prioritization? (Choose all that apply)

- A. A Frame Relay connection experiences utilization from 10 to 40%.
- B. A bursty WAN link that experiences only temporary congestion.
- C. A DDR connection is always connected and runs at 70 to 100% utilization most of the day.
- D. Low-speed data links that are not experiencing congestion problems.
- E. A connection that has multiple protocols sharing a single data path.

Answer: B, C, E

Explanation:

Traffic prioritization is used so that critical traffic gets through, even at the expense of lesser traffic.

B: The temporary congestion for high priority traffic can be avoided with traffic prioritization.

C: Some protocols can be assigned higher priorities.

E: On high utilization links it could be useful to prioritize important traffic.

Incorrect Answers:

A: If there is no congestion there is no need to use traffic prioritization.

D: With low utilization and no congestion there is no need to use traffic prioritization.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1

QUESTION 317:

Which Quality of Service method should an administrator configure if they want to give business essential traffic like VOIP and email strict priority over less essential traffic like internet surfing and file downloads?

- A. Weighted round robin
- B. Weighted fair queuing
- C. Random early detect
- D. Priority queuing
- E. All of the above would accomplish this

Answer: D

Explanation:

The Cisco IOS contains numerous traffic prioritization and congestion avoidance

mechanisms and options. Some of them are described in the following table:

QUEUEING COMPARISON		
Weighted Fair Queueing	Priority Queueing	Custom Queueing
No queue lists	4 queues	16 queues
Low volume given priority	High queue serviced first	Round-robin service
Conversation dispatching	Packet dispatching	Threshold dispatching
Interactive traffic prioritized	Critical traffic prioritized	Allocation of available bandwidth
File transfers have balanced access	Designed for low-bandwidth links	Designed for higher speed, low-bandwidth links
Enabled by default	Must be configured	Must be configured

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 13-35

QUESTION 318:

On router Certkiller 1 the following configuration command was entered:

```
queue-list 1 protocol ip 2 tcp 20
```

What is the result of this command?

- A. It assigns IP data traffic to priority queue 2.
- B. It assigns FTP data traffic to custom queue 2.
- C. It assigns IP traffic that matches IP access list 20 to priority queue 2.
- D. It assigns FTP traffic that matches IP access list 2 to custom queue 1.

Answer: B

Explanation:

According to the above command; FTP data traffic (TCP port #20) is assigned to custom queue 2.

Queue's can be assigned by: size, protocol, interface, or by default values.

```
Certkiller (config)#queue-list list number protocol  
protocol-name queue-number queue-keyword keyword-value
```

This example assigns Telnet packets to queue number 2:

```
queue-list 4 protocol ip 2 tcp 23
```

Note: FTP uses TCP ports 20 and 21.

Reference: CCNP Remote Access Exam Certification Guide, page 308-311, Brian

Morgan & Craig Dennis, Cisco Press 2001, ISBN 1-58720-003-1

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/qos_c/qcpart2/qccq.htm

QUESTION 319:

On your network, you wish to implement a Quality of Service method that treats all traffic as fairly as possible. You want to ensure that large data sessions do not unfairly consume all of the bandwidth while small data sessions that could be handled quickly are forced to wait in line. Which queuing method would you use to dynamically provide you with fair bandwidth allocation for every traffic type in the network?

- A. Priority
- B. WFQ
- C. Custom
- D. FIFO

Answer: B

Explanation:

Weighted Fair Queuing (WFQ)-This is the default method of queuing on links that are T1/E1 speeds or less. It offers fair access to the available bandwidth for each traffic flow. WFQ is one of Cisco's premier queuing techniques. It is a flow-based queuing algorithm that does two things simultaneously: It schedules interactive traffic to the front of the queue to reduce response time, and it fairly shares the remaining bandwidth between high bandwidth flows.

QUEUING COMPARISON		
Weighted Fair Queuing	Priority Queuing	Custom Queuing
No queue lists	4 queues	16 queues
Low volume given priority	High queue serviced first	Round-robin service
Conversation dispatching	Packet dispatching	Threshold dispatching
Interactive traffic prioritized	Critical traffic prioritized	Allocation of available bandwidth
File transfers have balanced access	Designed for low-bandwidth links	Designed for higher speed, low-bandwidth links
Enabled by default	Must be configured	Must be configured

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 13-35

QUESTION 320:

Link compression supports which of the following compression algorithms? (Choose all that apply.)

- A. Van Jacobson
- B. Stac
- C. MNP5
- D. Predictor
- E. Huffman

Answer: B, D

We refer to the data compression schemes used in internetworking devices as lossless compression algorithms. These schemes reproduce the original bit streams exactly, with no degradation or loss. This feature is required by routers and other devices to transport data across the network. The two most commonly used compression algorithms on internetworking devices are the Stacker compression and the Predictor data compression algorithms.

Stacker Compression

Stacker compression is based on the Lempel-Ziv compression algorithm. The Stacker algorithm uses an encoded dictionary that replaces a continuous stream of characters with codes. This stores the symbols represented by the codes in memory in a dictionary-style list. Because the relationship between a code and the original symbol varies as the data varies, this approach is more responsive to the variations in the data. This flexibility is particularly important for LAN data, because many different applications can be transmitting over the WAN at any one time. In addition, as the data varies, the dictionary changes to accommodate and adapt to the varying needs of the traffic. Stacker compression is more CPU-intensive and less memory-intensive.

Predictor Compression

The Predictor compression algorithm tries to predict the next sequence of characters in a data stream by using an index to look up a sequence in the compression dictionary. It then examines the next sequence in the data stream to see if it matches. If it does, that sequence replaces the looked-up sequence in the dictionary. If there is no match, the algorithm locates the next character sequence in the index and the process begins again. The index updates itself by hashing a few of the most recent character sequences from the input stream. No time is spent trying to compress already compressed data. The compression ratio obtained using predictor is not as good as other compression algorithms, but it remains one of the fastest algorithms available. Predictor is more memory-intensive and less CPU-intensive.

Incorrect Answers:

A: Van Jacobson is another name for tcp header-compression

C: MNP5 relates to modem compression.

E: This algorithm is not supported by Cisco at all.

QUESTION 321:

What FRTS (Frame Relay Traffic Shaping) term specifies the maximum number of uncommitted bits that the Frame Relay switch attempts to transfer beyond the CIR?

- A. Local access rate
- B. Oversubscription rate
- C. Committed burst
- D. Excess burst
- E. Excess information rate

Answer: D

Explanation:

FRTS provides parameters that are useful for managing network traffic congestion on frame relay networks. FRTS eliminates bottlenecks in Frame Relay networks with high-speed connections to the central site and low-speed connections to the branch sites. You can configure rate enforcement values to limit the rate at which data is sent from the virtual circuit (VC) at the central site.

The following definitions are important to FRTS:

Committed Information Rate (CIR)	Rate (bits per second) the frame relay provider guarantees for data transfer. CIR values are set by the Frame Relay service provider and configured by the user on the router. Note: The port / interface access rate can be higher than CIR. The rate is averaged over a Tc period of time.
Committed Burst (Bc)	Maximum number of bits the frame relay network commits to transfer over a Committed Rate Measurement Interval (Tc). $Tc = Bc / CIR$.
Excess Burst (Be)	Maximum number of uncommitted bits the frame relay switch attempts to transfer beyond the CIR over the Committed Rate Measurement Interval (Tc).
Committed Rate Measurement Interval (Tc)	Time interval over which Bc or (Bc + Be) bits are transmitted. Tc is calculated as $Tc = Bc / CIR$. The Tc value is not directly configured on Cisco routers. It is calculated after the Bc and CIR values are configured. Tc cannot exceed 125 ms.
Backwards Explicit Congestion Notification (BECN)	A bit in the Frame Relay frame header that indicates congestion in the network. When a Frame Relay switch recognizes congestion, it sets the BECN bit on frames destined for the source router, instructing the router to reduce the transmission rate.

Reference:

http://www.cisco.com/en/US/tech/CK652/CK698/technologies_tech_note09186a00800d6788.shtml

QUESTION 322:

The Certkiller network is using VOIP to make intra-office calls. What is the recommended queuing strategy for these voice packets?

- A. CBWFQ
- B. FIFO
- C. WFQ
- D. LLQ
- E. WRED

Answer: D

Explanation:

The Low Latency Queuing feature brings strict priority queuing to Class-Based Weighted Fair Queuing (CBWFQ). Strict priority queuing allows delay-sensitive data such as voice to be dequeued and sent first (before packets in other queues are dequeued), giving delay-sensitive data preferential treatment over other traffic.

Without Low Latency Queuing, CBWFQ provides weighted fair queuing based on defined classes with no strict priority queue available for real-time traffic. CBWFQ allows you to define traffic classes and then assign characteristics to that class. For example, you can designate the minimum bandwidth delivered to the class during congestion.

For CBWFQ, the weight for a packet belonging to a specific class is derived from the bandwidth you assigned to the class when you configured it. Therefore, the bandwidth assigned to the packets of a class determines the order in which packets are sent. All packets are serviced fairly based on weight; no class of packets may be granted strict priority. This scheme poses problems for voice traffic that is largely intolerant of delay, especially variation in delay. For voice traffic, variations in delay introduce irregularities of transmission manifesting as jitter in the heard conversation.

The Low Latency Queuing feature provides strict priority queuing for CBWFQ, reducing jitter in voice conversations. Because of this, it is the recommended queuing strategy when using VOIP.

QUESTION 323:

If CBWFQ is being used, which three commands can be configured within each traffic class? (Choose three)

- A. bandwidth
- B. service-policy
- C. queue-limit
- D. priority
- E. random-detect

Answer: A, C, D

Explanation:

CBWFQ extends the standard WFQ functionality to provide support for user-defined traffic classes. For CBWFQ, you define traffic classes based on match criteria including protocols, access control lists (ACLs), and input interfaces. Packets satisfying the match criteria for a class constitute the traffic for that class. A FIFO queue is reserved for each class, and traffic belonging to a class is directed to the queue for that class.

Once a class has been defined according to its match criteria, you can assign it characteristics. To characterize a class, you assign it bandwidth, weight, and maximum packet limit. The bandwidth assigned to a class is the guaranteed bandwidth delivered to the class during congestion.

To configure CBWFQ, perform the tasks in the following sections. The first three

sections are required; the remaining sections are optional.

1. Defining Class Maps (Required)
2. Configuring Class Policy in the Policy Map (Required)
3. Attaching the Service Policy and Enabling CBWFQ (Required)
4. Modifying the Bandwidth for an Existing Policy Map Class (Optional)
5. Modifying the Queue Limit for an Existing Policy Map Class (Optional)
6. Configuring the Bandwidth Limiting Factor
7. Deleting Classes (Optional)
8. Deleting Policy Maps (Optional)
9. Verifying Configuration of Policy Maps and Their Classes (Optional)

To configure a policy map and create class policies that make up the service policy, use the first command in global configuration mode to specify the policy map name, then use the following commands in policy-map class configuration mode to configure policy for a standard class.

The following example first defines a CBWFQ configuration and then reserves a strict priority queue:

```
!Thefollowingcommandsdefineaclassmap:
router(config)#class-mapclass1
router(config-cmap)#matchaccess-group101
router(config-cmap)#exit
!Thefollowingcommandscreateandattachapolicymap:
router(config)#policy-mappolicy1
router(config-pmap)#classclass1
router(config-pmap-c)#bandwidth3000
router(config-pmap-c)#queue-limit30
router(config-pmap-c)#random-detect
router(config-pmap-c)#random-detectprecedence032256100
router(config-pmap-c)#exit
router(config)#interfaceSerial1
router(config-if)#service-policyoutputpolicy1
```

QUESTION 324:

Router CK1 had the following configuration command added to interface Serial 0

```
Router(config-if)# ip tcp header-compression passive
```

Which two statements are true about the command entered in the display? (Choose two)

- A. The router will compress all traffic.
- B. The router will only compress outgoing TCP packets if incoming TCP packets on the same interface are compressed.
- C. The router will accept incoming compressed TCP packets but will not compress any outgoing TCP packets.
- D. The Layer 2 header will be compressed and therefore cannot be used for WAN switching networks such as Frame Relay.
- E. The Layer 2 header will be left intact and therefore can be used for WAN switching

networks such as Frame Relay.

F. For crossing point-to-point connections, the Layer 2 header will be encapsulated by another link layer such as LAPB.

Answer: B, D

Explanation:

ip tcp header-compression

To enable TCP header compression, use the ip tcp header-compression command in interface configuration mode.

ip tcp header-compression [passive]

Syntax Description

passive	(Optional) Compresses outgoing TCP packets only if incoming TCP packets on the same interface are compressed. If you do not specify the passive keyword, the Cisco IOS software compresses all traffic.
----------------	--

You can compress the headers of your TCP/IP packets to reduce their size and thereby increase performance. Header compression is particularly useful on networks with a large percentage of small packets, such as those supporting many Telnet connections. This feature only compresses the TCP header, so it has no effect on UDP packets or other protocol headers. The TCP header compression technique, described fully in RFC 1144, is supported on serial lines using HDLC or PPP encapsulation. You must enable compression on both ends of a serial connection.

Note: This compression command is only supported on PPP or HDLC links.

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_configuration_guide_chapter09186a008008

QUESTION 325:

Router CK1 is configured for WRED. With WRED, what will happen to the priority queue if the queue is full and more priority queue traffic is matched?

- A. Priority traffic will be restrained to its allocated queue size, and packets will be dropped.
- B. WRED will start dropping packets from other queues.
- C. Priority queue packets will be placed in the class-default queue.
- D. WRED will start dropping packets from the priority queue.

Answer: B

Explanation:

Weighted RED (WRED) generally drops packets selectively based on IP precedence. Packets with a higher IP precedence are less likely to be dropped than packets with a lower precedence. Thus, higher priority traffic is delivered with a higher probability than lower priority traffic. However, you can also configure WRED to ignore IP precedence

when making drop decisions so that non-weighted RED behavior is achieved. In contrast to RED, WRED can be configured to give preference to certain traffic types. This way, the lower priority traffic will be more likely to be dropped than traffic in the priority queue.

QUESTION 326:

One of the Certkiller Cisco 1700 series routers was configured for CBWFQ as shown below:

```
Router (config)#policy-map policy1
Router (config-pmap)#class class1
Router (config-pmap-c)#bandwidth 3000
Router (config-pmap-c)#queue-limit 30
Router (config-pmap-c)#exit
Router (config-pmap)#class class2
Router (config-pmap-c)#bandwidth 2000
Router (config-pmap-c)#exit
```

From the CBWFQ configuration referenced in the display, what is the queue-limit for class2?

- A. No limit
- B. 16
- C. 32
- D. 64
- E. 128

Answer: D

Explanation:

To specify or modify the maximum number of packets the queue can hold for a class policy configured in a policy map, use the queue-limit policy-map class configuration command.

queue-limit number-of-packets

<i>number-of-packets</i>	A number in the range from 1 to 64 specifying the maximum number of packets that the queue for this class can accumulate.
--------------------------	---

Defaults

On the Versatile Interface Processor (VIP)-based platforms, the default value is chosen as a function of the bandwidth assigned to the traffic class. The default value is also based on available buffer memory. If sufficient buffer memory is available, the default queue-limit value is equal to the number of 250-byte packets that would lead to a latency of 500 milliseconds(ms) when the packets are delivered at the configured rate. For example, if two 250-byte packets are required to lead to a latency of 500 ms, the default number-of-packets value would be 2.

On all other platforms, the default is 64.

In this example, since the queue was not explicitly configured, the standard default value of 64 would be used.

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a008008

QUESTION 327:

Router CK1 is configured with Class Based Weighted Fair Queuing (CBWFQ). By default, what is the maximum percentage of bandwidth CBWFQ allocated for all classes of traffic?

- A. 25
- B. 50
- C. 75
- D. 90
- E. 100

Answer: C

Explanation:

You can attach a single policy map to one or more interfaces or one or more VCs to specify the service policy for those interfaces or VCs.

Currently a service policy specifies class-based weighted fair queuing (CBWFQ). The class policies comprising the policy map are then applied to packets that satisfy the class map match criteria for the class.

To successfully attach a policy map to an interface or a VC, the aggregate of the configured minimum bandwidths of the classes comprising the policy map must be less than or equal to 75 percent of the interface bandwidth or the bandwidth allocated to the VC.

The default maximum reservable bandwidth value of 75 percent is designed to leave sufficient bandwidth for overhead traffic, such as routing protocol updates and Layer 2 keepalives. It also covers Layer 2 overhead for packets matching defined traffic classes or the class-default class.

QUESTION 328:

Which three conditions would suggest using weighted random early detection as an alternative to tail drops when configuring class-based weighted fair queuing?

(Choose three)

- A. Your network is designed for a more passive rather than active strategy in discarding packets.
- B. You want to enable TCP global synchronization to avoid congestion.
- C. You would like to use IP Precedence or DSCP values to make early dropping decisions.
- D. The bulk of your traffic is TCP traffic.
- E. You would like a chance to decide which packets will be dropped when it becomes

necessary.

Answer: C, D, E

Explanation:

WRED provides separate thresholds and weights for different IP precedences, allowing you to provide different qualities of service for different traffic. Standard traffic may be dropped more frequently than premium traffic during periods of congestion.

WRED has the following restrictions:

WRED is only useful when the bulk of the traffic is TCP/IP traffic. With TCP, dropped packets indicate congestion, so the packet source will reduce its transmission rate. With other protocols, packet sources may not respond or may resend dropped packets at the same rate. Thus, dropping packets does not decrease congestion.

WRED treats non-IP traffic as precedence 0, the lowest precedence. Non-IP traffic will be dropped more often than IP traffic.

WRED is only available on a per-interface basis. You cannot configure WRED on a subinterface.

Incorrect Answers:

A: WRED takes a proactive approach in congestion management by selectively discarding packets before problems arise.

B: WRED avoids the globalization problems that occur when tail drop is used as the congestion avoidance mechanism on the router. Global synchronization occurs as waves of congestion crest only to be followed by troughs during which the transmission link is not fully utilized. Global synchronization of Transmission Control Protocol (TCP) hosts, for example, can occur because packets are dropped all at once. Global synchronization manifests when multiple TCP hosts reduce their transmission rates in response to packet dropping, then increase their transmission rates once again when the congestion is reduced.

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1824/products_feature_guide09186a0080087ae4.html

QUESTION 329:

When configuring a strict priority queue using LLQ, Cisco recommends that you only send which type of static to this queue?

- A. DNS and DHCP
- B. VoIP
- C. Streaming video
- D. Routing protocol traffic
- E. VoIP call signaling

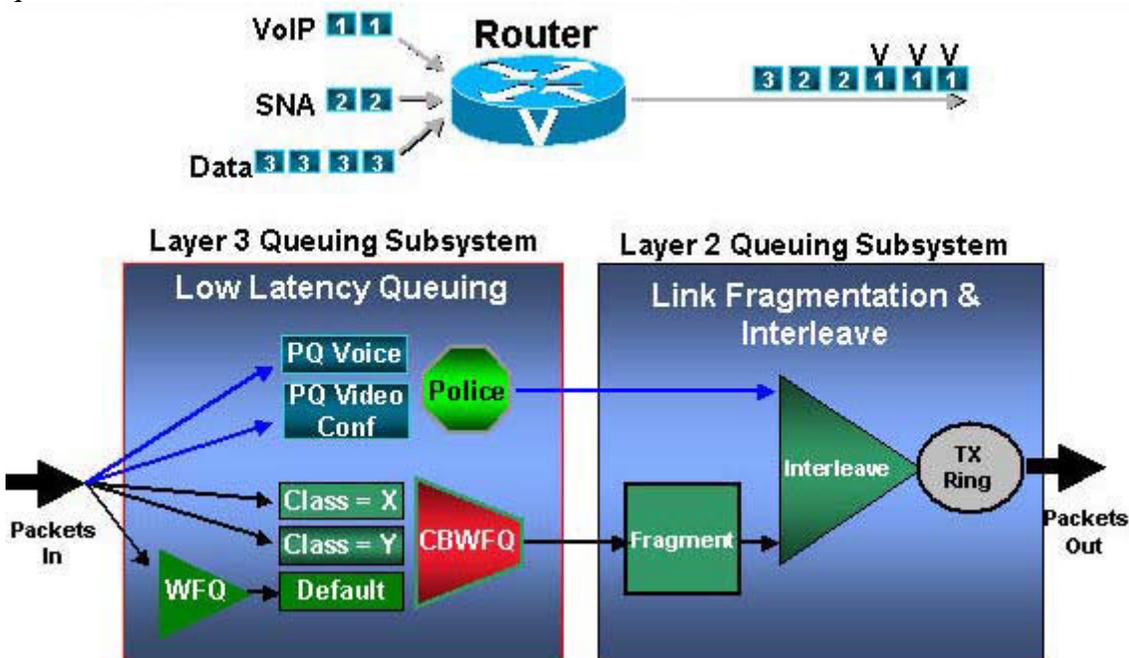
Answer: B

Explanation:

LLQ is a feature that provides a strict PQ to Class-Based Weighted Fair Queuing

(CBWFQ). LLQ enables a single strict PQ within CBWFQ at the class level. With LLQ, delay-sensitive data (in the PQ) is dequeued and sent first. In a VoIP with LLQ implementation, voice traffic is placed in the strict PQ.

The PQ is policed to ensure that the fair queues are not starved of bandwidth. When you configure the PQ, you specify in Kbps the maximum amount of bandwidth available to the PQ. When the interface is congested, the PQ is serviced until the load reaches the configured Kbps value in the priority statement. Excess traffic is then dropped to avoid the problem with Cisco's legacy priority-group feature of starving the lower priority queues.



This method is more complex and flexible than IP RTP Priority. The choice between the methods should be based on the patterns of traffic in your real network and your actual needs.

Reference:

http://www.cisco.com/en/US/tech/CK652/CK698/technologies_tech_note09186a0080094660.shtml

QUESTION 330:

Certkiller .com is currently running a Frame Relay network in a hub and spoke topology. To ease the WAN bandwidth bottleneck, Certkiller would like to configure compression in an effort to optimize WAN links. Certkiller does use multiple protocols and other applications that require that the layer 2 header remains intact. Which type of compression should Certkiller use?

- A. Link compression
- B. Payload compression
- C. TCP/IP header compression
- D. MPPC

Answer: B

Explanation:

Frame Relay Payload Compression

Layer 2 payload compression involves the compression of the payload of a Layer 2 WAN protocol, such as PPP, Frame Relay, High-Level Data Link Control (HDLC), X.25, and Link Access Procedure, Balanced (LAPB). The Layer 2 header is untouched by the act of compression. However, the entire contents of the payload (that include higher-layer protocol headers) are compressed.

QUESTION 331:

You need a strict priority queuing mechanism to support the VOIP used in the Certkiller network. Which two queuing methods allow for strict priority queuing of delay sensitive applications? (Choose two)

- A. Flow-based WFQ
- B. Class-based WFQ
- C. LLQ
- D. CQ
- E. PQ

Answer: C, E

Explanation:

LLQ:

LLQ is a feature that provides a strict PQ to Class-Based Weighted Fair Queuing (CBWFQ). LLQ enables a single strict PQ within CBWFQ at the class level. With LLQ, delay-sensitive data (in the PQ) is dequeued and sent first. In a VoIP with LLQ implementation, voice traffic is placed in the strict PQ.

Priority Queueing:

Priority Queueing strictly gives priority queues absolute preferential treatment over low priority queues. Important traffic, given the highest priority, always takes precedence over less important traffic.

QUESTION 332:

Certkiller .com's network policy states that voice traffic should be serviced before other non-essential application traffic such as http and ftp. Non-essential traffic starvation is not an issue.

Which quality of service method should Certkiller employ?

- A. Random early detect
- B. Weighted fair queuing
- C. Weighted round robin
- D. Priority queuing

Answer: D

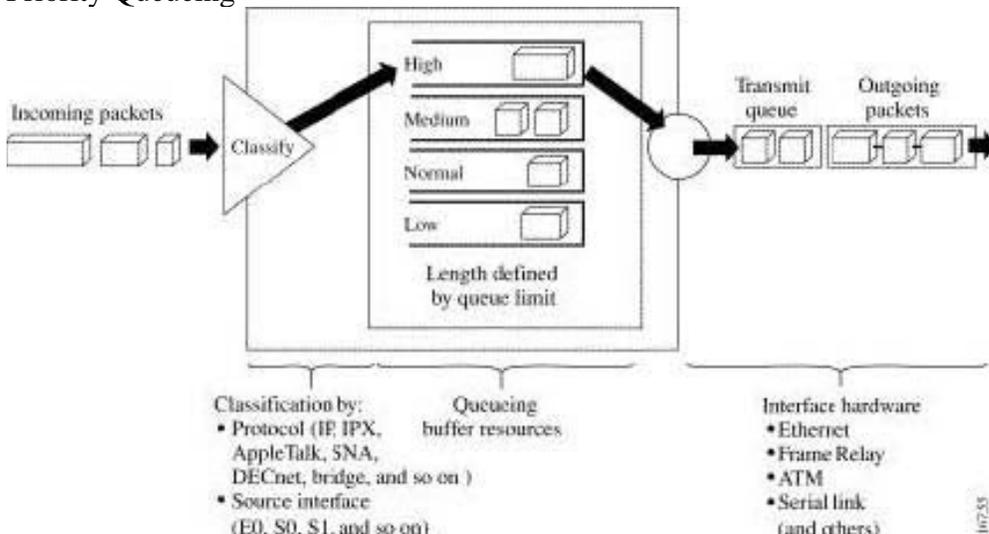
Explanation:

Priority Queueing:

PQ allows you to define how traffic is prioritized in the network. You configure four traffic priorities. You can define a series of filters based on packet characteristics to cause the router to place traffic into these four queues; the queue with the highest priority is serviced first until it is empty, then the lower queues are serviced in sequence.

During transmission, PQ strictly gives priority queues absolute preferential treatment over low priority queues; important traffic, given the highest priority, always takes precedence over less important traffic. Packets are classified based on user-specified criteria and placed into one of the four output queues-high, medium, normal, and low-based on the assigned priority.

Priority Queueing



When a packet is to be sent out an interface, the priority queues on that interface are scanned for packets in descending order of priority. The high priority queue is scanned first, then the medium priority queue, and so on. The packet at the head of the highest queue is chosen for transmission. This procedure is repeated every time a packet is to be sent.

QUESTION 333:

A Certkiller router was configured as shown below:

```
Router(config)#policy-map policy1
Router(config-pmap)#class class1
Router(config-pmap-c)#bandwidth 3000
Router(config-pmap-c)#_queue-limit 30
Router(config-pmap-c)#exit
Router(config-pmap)#class class2
Router(config-pmap-c)#bandwidth 2000
Router(config-pmap-c)#exit
```

Examine the configuration.

When using CBWFQ, what will happen to UDP packets if their destination queue is full?

- A. The router will send a BECN message to the host.
- B. The packet will be sent to the class-default queue.
- C. The host will resend the packet if it does not receive an ACK message.
- D. Tail dropping will occur.

Answer: D

Explanation:

In CBWFQ, after a queue has reached its configured queue limit, enqueueing of additional packets to the class causes tail drop or packet drop to take effect, depending on how class policy is configured.

Tail drop is used for CBWFQ classes unless you explicitly configure policy for a class to use WRED to drop packets as a means of avoiding congestion. Note that if you use WRED packet drop instead of tail drop for one or more classes comprising a policy map, you must ensure that WRED is not configured for the interface to which you attach that service policy.

QUESTION 334:

You need to configure Custom Queuing on one of the Certkiller routers. Which two items are required when configuring custom queuing? (Choose all that apply)

- A. Define the custom queue.
- B. Specify the maximum size of the queues.
- C. Define the available bandwidth to each queue.
- D. Create a default queue.
- E. Assign packets to the queue.

Answer: A, B, E

Explanation:

You must follow certain required, basic steps to enable custom queueing for your network. In addition, you can choose to assign packets to custom queues based on protocol type, interface where the packets enter the router, or other criteria you specify.

The following sections outline these minimum configuration tasks:

1. Define the Custom Queue List
2. Specify the Maximum Size of the Custom Queues
3. Assign Packets to Custom Queues

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_configuration_guide_chapter09186a00800c

QUESTION 335:

What is the default queuing method used on Cisco router interfaces running at or below 2 Mbps?

- A. CBWFQ
- B. LLQ
- C. WFQ
- D. FIFO
- E. PQ

Answer: C

Explanation:

The default queuing method for all interfaces that are E1/T1 (2 Mbps) or below is Weighted Fair Queuing. For all interfaces above 2 Mbps, the default queuing mechanism is First In, First Out, (FIFO).

QUESTION 336:

When CBWFQ is being used, what is 25 percent of the total available bandwidth reserved for?

- A. The highest priority class
- B. Routing traffic
- C. Low volume traffic
- D. High volume traffic
- E. Delay sensitive traffic
- F. None of the above

Answer: B

Explanation:

With CBWFQ, You can configure class policies for as many classes as are defined on the router, up to the maximum of 64. However, the total amount of bandwidth allocated for all classes included in a policy map to be attached to a VC must not exceed 75 percent of the available bandwidth of the VC. The remaining 25 percent of available bandwidth is used for encapsulation, such the layer 2 encapsulations, routing and best-effort traffic, and other functions that assume overhead.

QUESTION 337:

The Certkiller network needs to implement Quality of Service Traffic Shaping across their WAN in order to prioritize their important traffic. Which of the following are QoS Traffic shaping tools provided by Cisco (Choose 2)?

- A. BECN
- B. RSVP
- C. FECN
- D. GTS
- E. FRTS
- F. DE

Answer: D, E

Explanation:

Cisco's QoS software solutions include two traffic shaping tools -- generic traffic shaping (GTS) and Frame Relay traffic shaping (FRTS) -- to manage traffic and congestion on the network. GTS provides a mechanism to control the traffic flow on a particular interface. It reduces outbound traffic flow to avoid congestion by constraining specified traffic to a particular bit rate (also known as the token bucket approach), while queuing bursts of the specified traffic. FRTS provides parameters that are useful for managing network traffic congestion. These include committed information rate (CIR), FECN and BECN, and the DE bit. For some time, Cisco has provided support for FECN for DECnet, BECN for SNA traffic using direct LLC2 encapsulation via RFC 1490, and DE bit support. The FRTS feature builds on this Frame Relay support with additional capabilities that improve the scalability and performance of a Frame Relay network, increasing the density of virtual circuits and improving response time. More information can be found at: [this site](#)

QUESTION 338:

In the Certkiller frame relay network, traffic shaping needs to be configured on one of the routers. Which of the following is the first configuration step necessary to enable frame relay traffic shaping?

- A. Specify the FECN for traffic adaptation.
- B. Specify a queuing technique to be used on a connection.
- C. Specify the BECN for traffic adaptation.
- D. Specify and define map class.

Answer: D

Explanation:

The following steps are needed to properly configure Frame Relay Traffic Shaping:

Step 1: Specify a map class to be defined with the map-class frame-relay map classname command.

Step 2: Define the map class. When you define a map class for Frame Relay, you can:

1. Define the average and peak rates (in bits per second) allowed on virtual circuits associated with the map class.
2. Specify that the router dynamically fluctuate the rate at which it sends packets depending on the BECNs it receives.

3. Specify either a custom queue list or a priority queue group to use on virtual circuits associated with the map class.
4. Once you have defined a map class with queuing and traffic shaping parameters, enter interface configuration mode and enable Frame Relay encapsulation on an interface with the encapsulation frame-relay command, discussed earlier in this chapter.
Step 4: Enable Frame Relay traffic shaping on an interface with the frame-relay trafficshaping command. Enabling Frame Relay traffic shaping on an interface enables both traffic shaping and per-virtual circuit queuing on all the PVCs and SVCs on the interface. Traffic shaping enables the router to control the circuit's output rate and react to congestion notification information if also configured.
Step 5: Map a map class to all virtual circuits on the interface with the frame-relay class map class-name command. The map class-name argument must match the map class-name of the map class you configured.

QUESTION 339:

You want to increase the throughput of your slow speed lines through the use of hardware compression. By using Cisco hardware compression adapters, what compression options can be supported? (Choose all that apply)

- A. IPX advanced compression
- B. IP payload compression V8
- C. frame relay FRF.9 stacker compression
- D. PPP stacker compression

Answer: C, D

Explanation:

There are no industry-standard compression specifications, but Cisco IOS(r) software supports several third-party compression algorithms, including Hi/fn Stac Limpel Zif Stac (LZS), Predictor, and Microsoft Point-to-Point Compression (MPPC). These compress data on a per-connection basis or at the network trunk level.

Compression can take place on an entire-packet, header-only, or payload-only basis. The success of these solutions are easy to measure via compression ratio and platform latency.

Cisco IOS software supports the following data compression products:

1. FRF.9, for Frame Relay compression
2. Link Access Procedure, Balanced (LAPB) payload compression using using LZS or Predictor High-Level Data Link Control (HDLC) using LZS
3. X.25 payload compression of encapsulated traffic
4. Point-to-Point Protocol (PPP) using LZS (Stacker), Predictor, and Microsoft Point-to-Point Compression (MPPC).

Reference:

Understanding Data Compression

http://www.cisco.com/en/US/tech/CK7_13/CK8_02/technologies_tech_note09186a00801b3b86.shtml

QUESTION 340:

You want to increase the throughput of your slow speed lines through the use of TCP compression on router CK1 . To enable TCP header compression on this router, what command should be used?

- A. compress lapd set
- B. frame-relay payload-compress
- C. ppp compress
- D. compress
- E. ip tcp header-compression
- F. compress all

Answer: E

Explanation:

You can compress the headers of your TCP/IP packets in order to reduce the size of your packets. TCP header compression is supported on serial lines using Frame Relay, HDLC, or PPP encapsulation. You must enable compression on both ends of a serial connection. RFC 1144 specifies the compression process. Compressing the TCP header can speed up Telnet connections dramatically. In general, TCP header compression is advantageous when your traffic consists of many small packets, not for traffic that consists of large packets. Transaction processing (usually using terminals) tends to use small packets and file transfers use large packets. This feature only compresses the TCP header, so it has no effect on UDP packets or other protocol headers.

When compression is enabled, fast switching is disabled. This condition means that fast interfaces like T1 can overload the router. Consider the traffic characteristics of your network before using this command.

To enable TCP header compression, "use the ip tcp header-compression" command in interface configuration mode.

QUESTION 341:

You want router CK1 to prioritize low volume traffic over large data transfer session. Which traffic queuing method give a low-volume stream preferential service?

- A. FIDO
- B. Priority
- C. Custom
- D. Weighted Fair
- E. Low Latency

Answer: D

Explanation:

WFQ is an automated scheduling method that provides fair bandwidth allocation to all network traffic. WFQ applies priority, or weights, to identified traffic to classify traffic into conversations and determine how much bandwidth each conversation is allowed relative to other conversations. WFQ is a flow-based algorithm that simultaneously schedules interactive traffic to the front of a queue to reduce response time and fairly shares the remaining bandwidth among high-bandwidth flows. In other words, WFQ allows you to give low-volume traffic, such as Telnet sessions, priority over high-volume traffic, such as FTP sessions. WFQ gives concurrent file transfers balanced use of link capacity; that is, when multiple file transfers occur, the transfers are given comparable bandwidth.

QUESTION 342:

Payload Compression is being done on the Certkiller network to increase the overall data throughput. What statement is true about payload compression?

- A. Payload compression can be used in conjunction with TCP/IP header compression.
- B. The payload compression algorithm uses Predictor or STAC to compress traffic into another data link layer such as PPP.
- C. Payload compression is appropriate for virtual network services such as Frame Relay and ATM.
- D. With payload compression the complete packet is compressed and the switching information in the header is not available.

Answer: C

Explanation:

Layer 2 payload compression involves the compression of the payload of a Layer 2 WAN protocol, such as PPP, Frame Relay, High-Level Data Link Control (HDLC), X.25, and Link Access Procedure, Balanced (LAPB). The Layer 2 header is untouched by the act of compression, making it a good fit for layer 2 virtual network technologies such as frame relay and ATM. However, the entire contents of the payload (that include higher-layer protocol headers) are compressed.

Incorrect Answers:

A: You do not implement both Layer 2 payload compression and TCP/IP header compression concurrently because:

1. It is redundant and wasteful.
2. Often, the link does not come up or does not pass IP traffic.

Use only Layer 2 payload compression, rather than both Layer 2 payload compression and TCP/IP header compression.

B: Although Payload Compression is compressed by either a form of the "stacker" algorithm (based on the industry standard Lempel Ziv algorithm or the "predictor" algorithm, it is not used to compress traffic into a separate data link layer.

D: The Layer 2 header is untouched by the act of compression.

QUESTION 343:

Which policy map configuration command can be used to mitigate the problem of the TCP global synchronization?

- A. random-detect
- B. queue-limit 10
- C. compression header ip tcp
- D. priority 24

Answer: A

Explanation:

Weighted Random Early Discard (WRED) avoids the globalization problems that occur when tail drop is used as the congestion avoidance mechanism on the router. Global synchronization occurs as waves of congestion crest only to be followed by troughs during which the transmission link is not fully utilized. Global synchronization of Transmission Control Protocol (TCP) hosts, for example, can occur because packets are dropped all at once. Global synchronization manifests when multiple TCP hosts reduce their transmission rates in response to packet dropping, then increase their transmission rates once again when the congestion is reduced.

RED is used to drop packets before congestion issues occur. To configure WRED, use the "random-detect" configuration command. This can be done in either interface configuration mode or in policy map mode.

QUESTION 344:

Which of the following symptoms suggest congestion on a serial line? (Choose three)

- A. The connectivity is intermittent.
- B. The hardware in the serial link failed
- C. The connection fails at a particular time of day.
- D. The connection fails as load increases.
- E. The connection has never worked.

Answer: A, C, D

Explanation:

With regard to general serial link symptoms, intermittent connectivity can indicate a faulty router interface card or cable, a faulty CSU/DSU, a timing problem, or a congested serial line.

A connection that fails as load increases can indicate a dirty or congested serial line, while a connection that fails at a particular time of day is almost certainly due to an overused/congested serial line.

A connection that fails after some period of normal operation can indicate any of the following:

1. a cable running too close to EMI sources
2. a hardware failure in the serial link
3. incorrect routing tables
4. software problems such as buffer misses

If a connection has never worked, it may indicate that the serial facility is not actually provided or has failed.

Symptoms and problems specific to Frame Relay can usually be attributed to either Frame Relay being misconfigured on the router or a misconfigured Frame Relay switch. You should also check for a faulty interface card or cable.

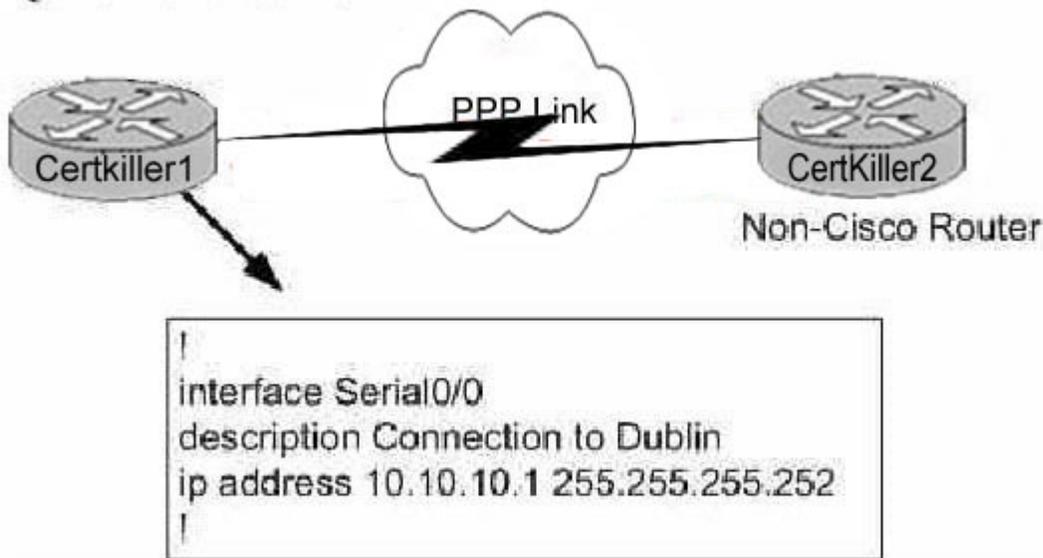
Incorrect Answers:

B: If there is a hardware problem, the issue would be a physical layer problem most likely causing a hard outage. This is not related to a congestions issue.

C: If the connection has never worked from the beginning, then it means that traffic isn't going through, so there can't be any congestion because there's no traffic congesting the lines.

QUESTION 345:

Certkiller A is connected via a Point to Point link to a Juniper router as displayed below:



Router Certkiller A is a Cisco router and it can't ping the Juniper router across the PPP link. You enter this command to Router A:

```
RTR Certkiller A#show interface s0/0
```

This is what you notice in the command output:

```
serial 0/0 is up, line protocol is down
```

What is the most likely reason for the line protocol being down?

- A. The IP addresses are not in the same subnet.
- B. The IP address is a non routable private address.
- C. There is a bad cable connecting the two routers.

D. The encapsulation type on RTR A Serial0/0 interface is incorrect.

Answer: D

Explanation:

The default encapsulation type on a Cisco serial interface is HDLC, which is Cisco proprietary and only good for a Cisco device. If no other encapsulation command is configured (none is shown in the above information) for the PPP link, it stays on HDLC by default, and the line protocol doesn't work for a non Cisco device. When connecting a private line (point to point) connection to a non-Cisco router, always use PPP encapsulation.

QUESTION 346:

What commands would you execute to troubleshoot and verify a PPP session?
(Choose two)

- A. The show interfaces command
- B. The debug PPP session command
- C. The show PPP command
- D. The debug PPP negotiation command
- E. The debug ppp dialer command

Answer: A, D

Explanation:

The command show interfaces will show you detailed statistics for all interfaces configured.

The command debug PPP negotiation will show you real time PPP negotiations.

References: CCNP Remote Access Exam Certification Guide, page 112, Brian Morgan & Craig Dennis, Cisco Press 2001, ISBN 1-58720-003-1

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgr/inter_r/irshowin.htm#1017387

QUESTION 347:

A Certkiller Cisco router running IOS Version 12.0 is installed. Which debug command would you use to troubleshoot an unsuccessful CHAP authentication on this router?

- A. debug ppp errors
- B. debug ppp negotiation
- C. debug authentication chap
- D. debug ppp tasks

Answer: B

Explanation:

The debug ppp negotiation and debug ppp authentication commands are useful in enabling the administrator to view the real-time communication between PPP configured devices. They are mentioned together because they are often implemented simultaneously. The "debug ppp negotiation" command was added after IOS version 12.0. Prior to that, only the "debug ppp authentication" command was supported.

Incorrect Answers:

A, C, D: These are all invalid Cisco IOS commands.

Reference: CCNP Remote Access Exam Certification Guide, page 112, Brian Morgan & Craig Dennis, Cisco Press 2001, ISBN 1-58720-003-1

QUESTION 348:

You are working on a problem with a Certkiller ISDN connection. To verify that the ISN line is working correctly, you perform a "show isdn status" command on the router. Which state will Layer 2 display if the line is up and active?

- A. TEI_ASSIGNED
- B. ASSIGN_AWAITING_TEI
- C. MULTIPLE_FRAME_ESTABLISHED
- D. TEI_UNASSIGNED

Answer: C

Explanation:

Table: Show ISDN Status Field Descriptions

Layer 2 Status	
TEI= 109, state = MULTIPLE_FRAME_ESTABLISHED TEI = 110, state = MULTIPLE_FRAME_ESTABLISHED	<p>Status of ISDN Layer 2 with Terminal Endpoint Identifier (TEI) number and multiframe structure state. The valid TEI number range is 64 to 126. The most often seen Layer 2 states are MULTIPLE_FRAME_ESTABLISHED and TEI_ASSIGNED.</p> <p>A</p> <p>state=MULTIPLE_FRAME_ESTABLISHED indicates there is data link connectivity to the telco ISDN switch. This is the state that you should see under normal operations. Any other state usually indicates a problem on the circuit.</p> <p>A state=TEI_ASSIGNED indicates that the router has lost connectivity to the switch. This is normal if the telco (commonly in Europe) deactivates Layers 1 and 2 when there are no active calls. If this is not the case, proceed to Troubleshooting BRI Layer 2 for more information on Layer 2 issues.</p> <p>Refer to Annex B in the ITU Q.921 specifications for more information on all the other possible Layer 2 states such as:</p> <ul style="list-style-type: none">• TEI_UNASSIGNED• ASSIGN_AWAITING_TEI• ESTABLISH_AWAITING_TEI• AWAITING_ESTABLISHMENT• AWAITING_RELEASE• TIMER_RECOVERY <p>The above states are often temporary. Use the command clear interface bri number to reestablish Layer 2 connectivity. If those states persist for extended periods use the debug isdn q921 command for further troubleshooting.</p>

Reference:

http://www.cisco.com/en/US/tech/CK8_01/CK3_79/technologies_tech_note09186a0080094b78.shtml

QUESTION 349:

You are setting up link authentication on router CK1 and want to verify that it is working properly. Which command will enable you to observe the authentication process of a connection being set up?

- A. debug modem
- B. show dialer
- C. debug ppp chap
- D. debug ppp authentication

Answer: D

Explanation:

To determine if the router is performing CHAP or PAP authentication, look for the following lines in the debug ppp negotiation and debug ppp authentication output: Look for CHAP in the AUTHENTICATING phase.

*Mar 7 21:16:29.468: BR0:1 PPP: Phase is AUTHENTICATING, by this end

*Mar 7 21:16:29.468: BR0:1 CHAP: O CHALLENGE id 5 len 33 from "maui-soho-03"
PAP

Look for PAP in the AUTHENTICATING phase.

*Mar 7 21:24:11.980: BR0:1 PPP: Phase is AUTHENTICATING, by both

*Mar 7 21:24:12.084: BR0:1 PAP: I AUTH-REQ id 1 len 23 from "maui-soho-01"

Reference:

http://www.cisco.com/warp/public/471/ppp_authen_ts_fl.html#5

QUESTION 350:

While logged into router CK1 , you are curious to see the Dial on Demand Routing (DDR) events that are taking place. Which of the following commands will you use to display these events in real time?

- A. show dialer
- B. debug dialer events
- C. debug ppp dialer
- D. debug dialer negotiation

Answer: B

Explanation:

Whenever you're asked a question with the key words 'real-time' then chances are it's a debug command. The debug dialer command is to see in real time what's attempting to cross the ISDN link. The EXEC command:

debug dialer events shows real time information about packets as they are received on a dialer interface. When DDR is enabled, information concerning the cause of the call (interface name, source and destination address of packets) is included as well.

QUESTION 351:

DRAG DROP

Drag 3 of the ISDN troubleshooting commands from the left, to their matching descriptions on the right:

Debug isdn q931	Place here	Determine PAP or CHAP authentication
Show dailer	Place here	Display layer 2 access procedures on the D channel
Debug isdn q911	Place here	Display call setup and teardown information
Debug isdn q921		

Answer:

-----	Show dailer	Determine PAP or CHAP authentication
	Show dailer	Display layer 2 access procedures on the D channel
Debug isdn q911	Debug isdn q911	Display call setup and teardown information

Explanation:

Use the debug isdn q921 EXEC command to display data link layer (Layer 2) access procedures that are taking place at the router on the D channel (LAPD) of its Integrated Services Digital Network (ISDN) interface.

debug isdn q931

Use the debug isdn q931 EXEC command to display information about call setup and teardown of ISDN network connections (Layer 3) between the local router (user side) and the network

Reference:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12supdoc/debug_r/dipx.pdf

QUESTION 352:

Which of the following commands would be the most useful when troubleshooting a Frame Relay network? (Choose two)

- A. show frame-relay map
- B. show ip route
- C. debug neighbors
- D. debug frame-relay topology
- E. All of the above.

Answer: A, B

Explanation:

Use this command to determine if frame-relay inverse-arp resolved a remote IP address to a local DLCI. This command is not enabled for point-to-point subinterfaces. It is only useful for multipoint interfaces and subinterfaces. Sample output is shown below:

RouterA#show frame-relay map

Serial0 (up): ip 157.147.3.65 dlci 980(0x3D4,0xF440),
dynamic,

broadcast,, status defined, active

The "show ip route command can also be a usefull troubleshooting tool in nearly every topology, since it will display all of the routes known in the routing table, how those routes were learned, and from which neighbors.

Incorrect Answers:

C, D: These are invalid IOS commands.

http://www.cisco.com/en/US/tech/ CK7 13/ CK2 37/technologies_tech_note09186a008014f8a7.shtml#topic20

QUESTION 353:

Which show command can you use in a Frame Relay network to verify line configuration, protocol, and LMI status on the serial interface of a Certkiller router?

- A. show interface
- B. show frame relay lmi
- C. show frame-relay pvc
- D. show frame-relay status
- E. show frame-relay interface
- F. show frame-relay map

Answer: C

Explanation:

To display statistics about permanent virtual circuits (PVCs) for Frame Relay interfaces, use the show frame-relay pvc command in privileged EXEC mode.

```
RouterA# show frame-relay pvc
```

```
PVC Statistics for interface Serial0 (Frame Relay DTE)
```

```
DLCI = 666, DLCI USAGE = UNUSED, PVC STATUS = DELETED, INTERFACE = Serial0
```

```
input pkts 0 output pkts 0 in bytes 0
```

```
out bytes 0 dropped pkts 0 in FECN pkts 0
```

```
in BECN pkts 0 out FECN pkts 0 out BECN pkts 0
```

```
in DE pkts 0 out DE pkts 0
```

```
pvc create time 0:03:18 last time pvc status changed 0:02:27
```

```
Num Pkts Switched 0
```

```
DLCI = 980, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0
```

```
input pkts 19 output pkts 87 in bytes 2787
```

```
out bytes 21005 dropped pkts 0 in FECN pkts 0
```

```
in BECN pkts 0 out FECN pkts 0 out BECN pkts 0
```

```
in DE pkts 0 out DE pkts 0
```

```
pvc create time 1:17:47 last time pvc status changed 0:58:27
```

The PVC can have four possible states. These are shown by the PVC STATUS field as follows:

ACTIVE - PVC is up and functioning normally.

INACTIVE - PVC is not up end-to-end. This may be because either there is no mapping (or incorrect mapping) for the local DLCI in the frame-relay cloud or the remote end of the PVC is deleted.

DELETED - Either the Local Management Interface (LMI) is not exchanged between the router and the local switch, or the switch does not have DLCI configured on the local switch.

STATIC - no keepalive configured on the frame-relay interface of the router.

QUESTION 354:

Which one of the following show commands would you use to view a permanent virtual circuit (PVC) associated with the Certkiller network?

- A. show ip route
- B. show frame-relay lmi
- C. show frame-relay pvc
- D. show frame-relay map
- E. show frame-relay status

Answer: C

Explanation:

From the Cisco Press book, pg. 291..."The show frame-relay map command is used to view the DLCI mappings that have been created. The question refers to permanent virtual circuits (PVC) not mappings. On pg. 288 of the same book, ..."the show frame-relay pvc command. This command is useful for viewing the status of statically or dynamically defined PVCs."

QUESTION 355:

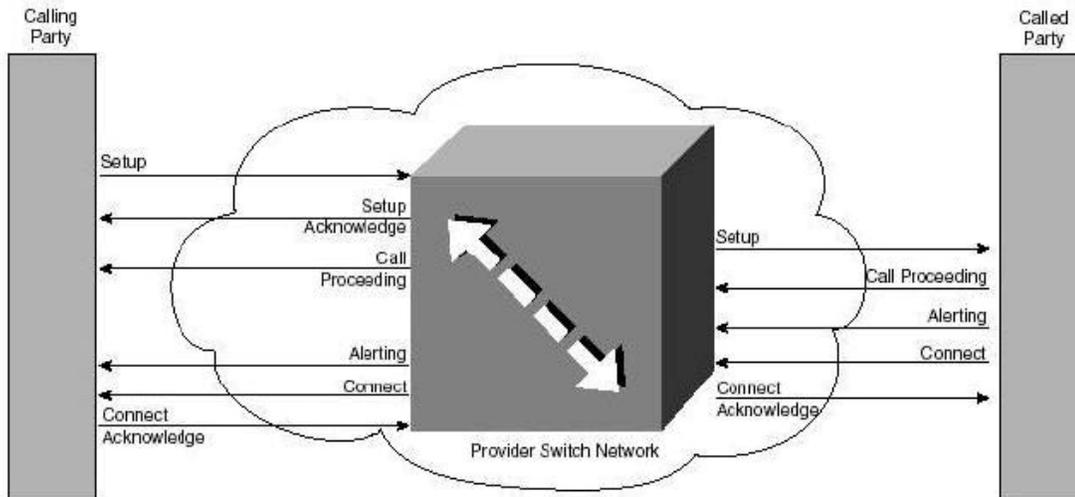
Your junior administrator has been trying to connect his Cisco router to the internet via an ISDN BRI. He's receiving ISDN SETUP messages but he isn't getting a CONNECT message, so he asks you for help. What is the most likely cause of his problem? (Choose all that apply.)

- A. The ISDN BRI line is not working at Layer 1.
- B. The ISDN BRI line is not working at Layer 2.
- C. The ISDN BRI line may not be configured correctly to handle the call.
- D. The ISDN BRI line is not working at Layer 3.
- E. The ISDN BRI line is working at layer 2 but not at layer 1.

Answer: C, D

Explanation:

The setup procedure for ISDN calls is very similar to that of other circuit-switched technologies. It begins with a request, which is acknowledged. The acknowledging switch then forwards the setup request to the next switch in the line, and so on. Once the called party is reached, a connect message is sent, which also must be acknowledged.



ITU-T Q.931 is specified as the protocol for Layer 3 of the D channel. The protocol messages and their rules for exchange are derived from the DSS1 protocol suite. And if you have the problem mentioned, you have probably configured the BRI settings wrong.

Reference:

Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)

Page 154 & 155

QUESTION 356:

You are tasked with troubleshooting a problem with the Frame Relay connection at one of your sites. Upon arrival at a remote location, you start your diagnostics and it comes to your attention that the Frame Relay PVC is in an inactive state on the router. What do you suspect is the cause of this problem?

- A. PVC is in DOWN state on the remote router.
- B. PVC is not configured on local router.
- C. PVC is not configured on the Frame Relay switch.
- D. PVC is in a DELETED state on the remote router.

Answer: C

Explanation:

Not D: How can that be, the question states that the router is in the "INACTIVE" state, how can the router be in the DELETED state.

It can only be one of three states INACTIVE, ACTIVE or DELETED.

INACTIVE state: Indicates that the local router connection to the FR switch is working, but the remote router connection to the FR switch is not working.

ACTIVE state: Indicates that the connection is active, routers are exchanging data.

DELETED state: Indicates not LMI is being sent from the FR switch the DLCI

has been removed from the FR switch, or there is no service between the CPE router and the FR switch.

QUESTION 357:

The following output was seen while troubleshooting a frame relay issue:

```
R8#debug frame-relay packet
Frame Relay packet debugging is on
R8#
R8#ping 172.16.81.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.81.3, timeout is 2 seconds:
Serial8/0:Encaps failed--no map entry link 7(IP)
Success rate is 0 percent (0/5)
```

Based on the information above, what is the underlying cause of this problem?

- A. Missing routing table entry.
- B. Frame Relay encapsulation mismatch.
- C. Missing MAC address
- D. Missing inverse ARP entry.
- E. Frame Relay LMI type mismatch.

Answer: D

Explanation:

You are not able to ping your own IP address on a multipoint Frame Relay interface. This is because Frame Relay multipoint (sub)interfaces are non-broadcast, (unlike Ethernet and point-to-point interfaces High-Level Data Link Control [HDLC]), and Frame Relay point-to-point sub-interfaces.

Furthermore, you are not able to ping from one spoke to another spoke in a hub and spoke configuration. This is because there is no mapping for your own IP address (and none were learned via Inverse ARP). But if you configure a static map (using the frame-relay map command) for your own IP address (or one for the remote spoke) to use the local DLCI, you can then ping your devices.

Reference:

http://www.cisco.com/en/US/tech/CK713/CK237/technologies_tech_note09186a008014f8a7.shtml

QUESTION 358:

Study the partial output of the configuration file for router CK1 below interface BRI0

```
description connected to ntt 81019998887654
ip address 10.12.15.5 255.255.255.0
encapsulation ppp
dialer idle-timeout 30
```

```
dialer load-threshold 40 either
dialer map ip 10.12.15.8 name Certkiller B 81019998888901
dialer map ip 10.12.15.9 name Certkiller C 81019998881234
dialer map ip 10.12.15.4 name Certkiller D 81019998881122
dialer-group 1
ppp authentication pap
ppp multilink
```

What's true about the type of dial-on demand routing being implemented?

- A. By configuring legacy DDR on interface BRI0, calls made to all three sites will use the same communication parameters.
- B. Calls made using BRI0 will attempt to use the authentication configured for the dial rotary, and if unsuccessful, will use pap authentication.
- C. By configuring BRI0 as a member of a dial-group 1, communications parameters assigned to the group will override those configured on the interface.
- D. The dialer profile communication parameters will override those configured directly on interface BRI0.

Answer: A

Explanation:

```
dialer map protocol next-hop-address [name hostname] [speed
56|64] [broadcast]
[dial-string[:isdn-subaddress]
```

Dialer map - Configures a serial interface or ISDN interface to call one or multiple sites. The name parameter refers to the name of the remote system. The speed parameter is the line speed in kilobits per second to use. The broadcast parameter indicates that broadcasts should be forwarded to this address. The dial-string [:isdn-subaddress] is the number to dial to reach the destination and the optional ISDN subaddress.

Incorrect Answers:

B: Although PAP authentication has been configured, there is no dialer interface or dialer rotary to use.

C, D: Dialer profiles and dialer groups are not configured.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 7-32

QUESTION 359:

Which of the following commands are useful in verifying and troubleshooting PPP sessions? (Choose two)

- A. debug PPP negotiation
- B. debug PPP session
- C. show interfaces
- D. show PPP

Answer: A, C

Explanation:

1. Use the show interfaces command to display status and counter information about an interface.

1. The debug ppp negotiation command is a great tool for troubleshooting the PPP Link Control protocol activities such as authentication, compression, and multilink.

* show PPP and debug PPP session commands do not exist

Reference:

Cisco Press - CiscoPedia v3.0

QUESTION 360:

Which of the following debug commands could you use to troubleshoot Layer 3 ISDN information? (Choose two)

- A. debug isdn q931
- B. debug isdn q921
- C. debug isdn network
- D. debug isdn event
- E. debug isdn layer 3

Answer: A, D

Explanation:

Use the debug isdn q931 EXEC command to display information about call setup and teardown of ISDN network connections (Layer 3) between the local router (user side) and the network. The ISDN network layer interface provided by the access router conforms to the user interface specification defined by ITU-T recommendation Q.931, supplemented by other specifications such as for switch types VN2 and VN3. The router tracks only activities that occur on the user side, not the network side, of the network connection.

The debug isdn q931 command output is limited to commands and responses exchanged during peer-to-peer communication carried over the D channel. This debug information does not include data transmitted over the B channels. The peers (network layers) communicate with each other via an ISDN switch over the D channel.

The debug isdn events command also displays information that is useful for monitoring and troubleshooting Multilink PPP.

Use the

debug isdn q921 EXEC command to display data-link layer (Layer 2) access procedures that are taking place at the access router on the D channel (LAPD) of its ISDN interface. This command is useful when you want to observe signaling events between the access router and the ISDN switch. The ISDN data-link layer interface provided by the access router conforms to the user interface specification defined by ITU-T recommendation Q.921.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 7-65

QUESTION 361:

You're a senior network technician at CertKiller and its Friday afternoon and all of your junior administrators have left work early. While inspecting their workstations you realize that one of your junior administrators has left a debug command running. On inspection of his monitor you see the following command output:

```
1d16h: %LINK-3-UPDPDOWN: Interface Serial3/0, changed state to up
*Mar 2 16:52:15.297: Se3/0 PPP: Treating connection as a
dedicated line
*Mar 2 16:52:15.441: Se3/0 PPP: Phase is AUTHENTICATING, by this
end
*Mar 2 16:52:15.445: Se3/0 CHAP: O CHALLENGE id 7 len 29 from
"NAS1"
```

With reference to the above output, which two statements are true? (Choose all that apply.)

- A. The client is attempting to setup a Serial Line Internet Protocol connection
- B. This is a connection attempt to an async port.
- C. The connection is established on serial interface 3/0.
- D. The user is authenticating with the privileged mode password "NAS1".
- E. The user is authenticating using CHAP.

Answer: C E

Explanation:

1. A CHAP challenge packet is built with the following characteristics:

01 = challenge packet type identifier

id = sequential number that identifies the challenge

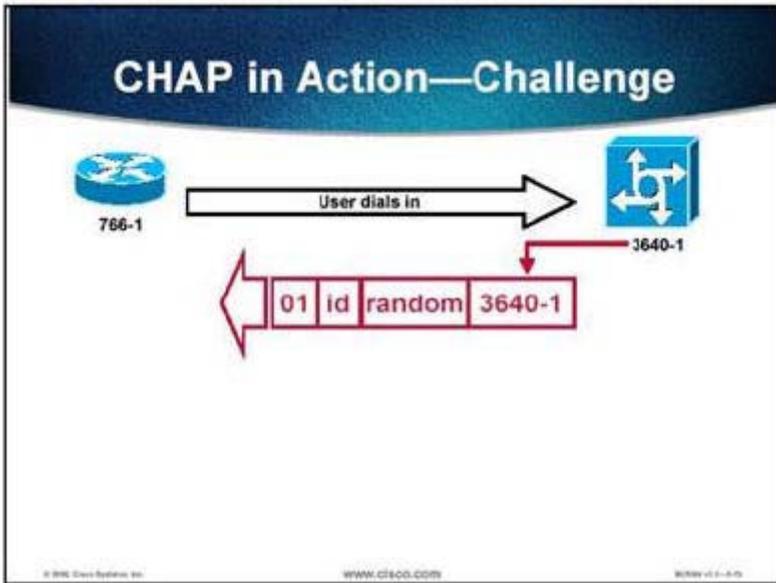
random = a reasonably random number

3640-1 = the authentication name of the challenger

2. The id and random values are kept on the access server.

3. The challenge packet is sent to the caller. A list of outstanding challenges is maintained.

When using Chap authentication, the access server sends a challenge message to the remote node after the PPP link is established. The remote node responds with a value calculated by using a one-way hash function. The access server (NAS1) checks the response against its own calculation of the expected hash value.



Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 5-17

QUESTION 362:

What command could a network analyst use if they wanted to analyze DDR events in real time?

- A. debug ppp dialer
- B. debug dialer
- C. show dialer
- D. debug dialer negotiation

Answer: B

Explanation:

There are many more commands and command outputs that are useful in troubleshooting the dial process in general. For instance, the debug dialer command is one of the best tools to use to figure out which traffic is attempting to traverse the ISDN link.

Troubleshooting Multilink PPP

```
BranchF#debug dialer
BranchF#ping 10.115.0.135

Type escape sequence to abcr.
Sending 5, 100-byte ICMP Echos to 10.115.0.135, timeout is 2 seconds:

BRI0: Dialing cause ip (s=10.155.0.1, d=10.115.0.135)
BRI0: Attempting to dial 6000
%LINK-3-UPDOWN: Interface ERI0:2, changed state to up
dialer Protocol up for BR0:2.
%LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0:2, changed state to
up!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 32/34/36 ms
BranchF#
BRI0: rotary group to 6000 overloaded (1)
BRI0: Attempting to dial 6000
%ISDN-6-CONNECT: Interface BRI0:2 is now connected to 6000 CentralF
```

Incorrect Answers:

A, D: These are invalid Cisco IOS commands.

C: TO see events in real time, use the debug command, not the show command.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 7-63

QUESTION 363:

You're a specialized frame-relay contractor and you've just finished configuring a network. What command would you use to verify the frame-relay traffic-shaping parameters?

- A. show frame-relay pvc
- B. show frame-relay interface
- C. show frame-relay status
- D. show frame-relay map-class
- E. None of the above

Answer: A

Explanation:

The show frame-relay pvc command includes the parameters used in traffic shaping, if enabled, and the queuing algorithm in use.

```

CentralA#sh frame-relay pvc
PVC Statistics for interface Serial3/1 (Frame Relay DTE)
DLCI = 110, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial3/1.1

  input pkts 35           output pkts 40           in bytes 4324
  out bytes 6684         dropped pkts 0           in FECN pkts 0
  in BECN pkts 0        out FECN pkts 0         out BECN pkts 0
  in DE pkts 0          out DE pkts 0
  out bcst pkts 25      out bcst bytes 5124
  Shaping adapts to BECN
  pvc create time 00:12:55, last time pvc status changed 00:12:55

```

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 11-39

QUESTION 364:

You want to analyze the number of total BECN and FECN packet statistics on the serial interface of Certkiller 's main router. Which of the following commands would you use?

- A. show frame-relay map
- B. show frame-relay pvc
- C. show frame-relay lmi
- D. show interfaces

Answer: B

Explanation:

The show frame-relay pvc command displays the status of each configured connection as well as traffic statistics. This command is also useful for viewing the number of backward explicit congestion notification (BECN) and forward explicit congestion notification (FECN) packets received by the router. The PVC STATUS can be active, inactive, or deleted.

If you enter show frame-relay pvc, you will see the status of all the PVCs configured on the router. If you specify a specific PVC, you will only see the status of that PVC. In the figure, the show frame-relay pvc 110 command only displays the status of PVC 110.

Verifying Frame Relay Operation (cont.)

```
Router#show frame-relay pvc 110
PVC Statistics for interface Serial0 (Frame Relay DTE)
DLCI = 110, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0

input pkts 14055 output pkts 32795 in bytes 1096228
out bytes 6216155 dropped pkts 0 in FECN pkts 0
in BECN pkts 0 out FECN pkts 0 out BECN pkts 0
in DE pkts 0 out DE pkts 0
out beas pkts 32795 out beas bytes 6216155

<Output Omitted>
```

- Displays PVC traffic statistics

© 2000, Cisco Systems, Inc. www.cisco.com BCR66 v1.1-01-11

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 11-12

QUESTION 365:

Which of the following commands could a network technician use to view source and destination IP addresses of a DDR connection on an ISDN? (Choose all that apply.)

- A. show dialer state
- B. debug dialer
- C. show spid
- D. show dialer interface
- E. None of the above

Answer: B, D

Explanation:

The "show dialer interface" command shows status and connection information regarding each B channel and the number to which the channel is connected. It also shows successful and failed calls.

The following examples are used to illustrate this:

```
BranchF#debug dialer
BranchF#ping 10.115.0.135

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.115.0.135, timeout is 2 seconds:

BRI0: Dialing cause ip (s=10.155.0.1, d=10.115.0.135)
BRI0: Attempting to dial 6000
%LINK-3-UPDOWN: Interface BRI0:2, changed state to up
dialer Protocol up for BR0:2.
%LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0:2, changed state to
up!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 32/34/36 ms
BranchF#
BRI0: rotary group to 6000 overloaded (1)
BRI0: Attempting to dial 6000
%ISDN-6-CONNECT: Interface BRI0:2 is now connected to 6000 CentralF
```

```
NASX#show dialer interface bri0
BRI0 - dialer type = ISDN

Dial String      Successes      Failures      Last called      Last status
5553972          6              0             19 secs         Successful
0 incoming call(s) have been screened.
BRI0: B-Channel 1
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is data link layer up
Dial reason: ip (s=10.1.1.8, d=10.1.1.1)

Interface bound to profile Dialer0

Time until disconnect 102 secs
Current call connected 00:00:19
Connected to 5553972 (system1)

BRI0: B-Channel 2
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle
```

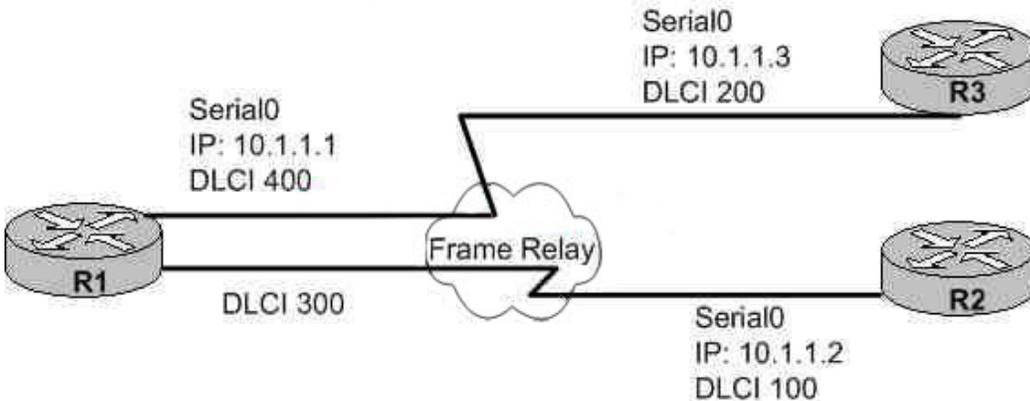
Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 7-63

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 8-21

QUESTION 366:

The Certkiller network is displayed in the following diagram:



Router R2 is can successfully ping Router R1, but it can't ping Router 3. What is the set of frame-relay map ip commands can you use on router R2 to fix the problem?

- A. frame-relay map ip 10.1.1.3 200
frame-relay map ip 10.1.1.1 400
- B. frame-relay map ip 10.1.1.3 100
frame-relay map ip 10.1.1.1 100
- C. frame-relay map ip 10.1.1.3 100
frame-relay map ip 10.1.1.1 400
- D. frame-relay map ip 10.1.1.3 200
frame-relay map ip 10.1.1.1 300

Answer: B

Explanation:

. In the frame-relay map ip <ip address> dlci command, the dlci is the local number, not the local number of the dlci on the other routers.

Not D: DLCIs 200 & 300 are not local to R2. They are the DLCI for their own router for that interface.

QUESTION 367:

You are a network administrator at Certkiller and you've just entered the command "debug frame-relay lmi." From this, you see the following:

```
Serial10/0(in): Status, myseq 72
RT IE 1, length 1, type 0
KA IE 3, length 2, yourseq 73, myseq 72
PVC IE 0x7 , length 0x3 , dlci 100, status 0x0
PVC IE 0x7 , length 0x3 , dlci 200, status 0x2
Serial10/0(out): StEng, myseq 73, yourseen 73, DTE up
datagramstart = 0x1346F34, datagramsize = 14
FR encap = 0x00010308
00 75 95 01 01 01 03 02 49 49
```

Considering the above output; what is the status of DLCI 100?

- A. active
- B. init
- C. inactive
- D. down
- E. deleted

Answer: C

Explanation:

The possible values of the status field are explained below:

1. 0x0-Added/inactive means that the switch has this DLCI programmed but for some reason (such as the other end of this PVC is down), it is not usable.
2. 0x2-Added/active means the Frame Relay switch has the DLCI and everything is

operational. You can start sending it traffic with this DLCI in the header.

3. 0x3-0x3 is a combination of an active status (0x2) and the RNR (or r-bit) that is set (0x1). This means that the switch - or a particular queue on the switch - for this PVC is backed up, and you stop transmitting in case frames are spilled.

4. 0x4-Deleted means that the Frame Relay switch doesn't have this DLCI programmed for the router. But it was programmed at some point in the past. This could also be caused by the DLCIs being reversed on the router, or by the PVC being deleted by the telco in the Frame Relay cloud. Configuring a DLCI (that the switch doesn't have) will show up as a 0x4.

Since the status for DLCI 100 is 0x0, the PVC is inactive.

Reference:

http://www.cisco.com/en/US/tech/CK7_13/CK2_37/technologies_tech_note09186a008014f8a7.shtml#topic20

QUESTION 368:

If you wanted to view the state of ISDN interface BRI 0's first B channel on router CK1 , which IOS command would you use?

- A. show interface BRI 0 1
- B. show interface BRI 0 2
- C. show dialer interface BRI 0
- D. show dialer interface BRI 0.0
- E. None of the above

Answer: A

Explanation:

```
Router# show interfaces bri 0 1
```

```
BRI0:1 is down, line protocol is down
```

```
Hardware is BRI
```

```
MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
```

```
Encapsulation PPP, loopback not set, keepalive not set
```

```
LCP Closed
```

```
Closed: IPCP
```

```
Last input never, output never, output hang never
```

```
Last clearing of "show interface" counters never
```

```
Queuing strategy: fifo
```

```
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
```

```
5 minute input rate 0 bits/sec, 0 packets/sec
```

```
5 minute output rate 0 bits/sec, 0 packets/sec
```

```
0 packets input, 0 bytes, 0 no buffer
```

```
Received 0 broadcasts, 0 runts, 0 giants
```

```
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
```

```
0 packets output, 0 bytes, 0 underruns
```

```
0 output errors, 0 collisions, 7 interface resets
```

```
0 output buffer failures, 0 output buffers swapped out
```

0 carrier transitions

Reference:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/dial_r/drdshoil.pdf

QUESTION 369:

Which one of the following show commands would you use to display what 'interesting traffic' triggered a DDR call on ISDN BRI 0 of one of the Certkiller routers?

- A. show interface bri0
- B. show dialer interface bri0
- C. show interface dialer
- D. show ip route connected

Answer: B

Explanation:

Enter the show dialer interface EXEC command with the interface type and number to display statistics on the physical interface bound to the dialer interface. Output includes the configured timers. The "Idle timer (never)" and "Dial reason:" lines indicate that persistent dialing is configured.

```
Router# show dialer interface dialer 1
Di1 - dialer type = DIALER PROFILE
Idle timer (never), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is data link layer up
Number of active calls = 1
Dial String Successes Failures Last DNIS Last status
7135551234 4 0 00:00:06 successful Default
BRI1/0 - dialer type = ISDN
Dial String Successes Failures Last DNIS Last status
0 incoming call(s) have been screened.
0 incoming call(s) rejected for callback.
BRI1/0:2 - dialer type = ISDN
Idle timer (never), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is data link layer up
Dial reason: Dialing on persistent Dialer Profile
Interface bound to profile Di1
Time until disconnect never
Current call connected 00:00:06
Connected to 7135551234 (7135551234)
```

Reference:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t111/ftdperst.htm>

QUESTION 370:

You have an ISDN BRI connection. You need to check the Layer 3 sessions; more specifically the call-type and B channel utilized. Which of the following commands would you use?

- A. debug dialer
- B. show isdn status
- C. show dialer-group
- D. show dialer interface

Answer: B

Explanation:

Understanding the show isdn status Output

The show isdn status output shown below is an example of a properly functioning BRI circuit. In the following example, Layer 1 is MULTIPLE_FRAME_ESTABLISHED, the Terminal Endpoint Identifiers (TEIs) have been successfully negotiated, and ISDN Layer 3 (end-to-end) is ready to make or receive calls. The items you should pay attention to are linked to each corresponding field in the table shown below.

CK1 # show isdn status

The current ISDN Switchtype

= basic-ni1

ISDN BRI0 interface

Layer 1

Status:

ACTIVE

Layer 2

Status:

TEI = 109, State = MULTIPLE_FRAME_ESTABLISHED

TEI = 110, State = MULTIPLE_FRAME_ESTABLISHED

Spid Status

TEI 109, ces = 1, state = 8(established)

spid1 configured, spid1 sent, spid1 valid

Endpoint ID Info: epsf = 0, usid = 1, tid = 1

TEI 110, ces = 2, state = 8(established)

spid2 configured, spid2 sent, spid2 valid

Endpoint ID Info: epsf = 0, usid = 3, tid = 1

Layer 3 Status

0 Active Layer 3 Call(s)

Activated dsl 0 CCBs = 0

Total Allocated ISDN CCBs = 0

References:

Building Cisco Remote Access Networks page 203 ISBN#1-57870-091-4

http://www.cisco.com/en/US/tech/CK8_01/CK3_79/technologies_tech_note09186a0080094b78.shtml

QUESTION 371:

You have just been hired by CertKiller consulting branch to troubleshoot a clients Frame Relay network.

You enter the command:

```
show interface serial0
```

The output from the command contains the lines:

```
Serial0 is up, line protocol is down
```

So you ask the resident administrator what the encapsulation type is, and he answers:

```
"Serial 0 is configured with frame relay encapsulation."
```

From the above two facts, what is most likely the source of the problem?

- A. IP subnet mismatch
- B. No carrier signal
- C. No IP address configured
- D. LMI type mismatch
- E. LAPF state, down

Answer: D

Explanation:

"Serial0 is up, line protocol is down" indicates that the router is getting a carrier signal from the CSU/DSU or modem. Check to make sure the Frame Relay provider has activated their port and that your Local Management Interface (LMI) settings match. Generally, the Frame Relay switch ignores the data terminal equipment (DTE) unless it sees the correct LMI (use Cisco's default "cisco" LMI). Check to make sure the Cisco router is transmitting data. You will most likely need to check the line integrity using loop tests at various locations beginning with the local CSU and working your way out until you get to the provider's Frame Relay switch.

Reference:

http://www.cisco.com/en/US/tech/CK7_13/CK2

[37/technologies_tech_note09186a008014f8a7.shtml#serialupdown](http://www.cisco.com/en/US/tech/CK7_13/CK2_37/technologies_tech_note09186a008014f8a7.shtml#serialupdown)

QUESTION 372:

You are a network administrator at T & K bicycle wheel works and by coincidence the network uses a hub and spoke Frame Relay architecture. Sadly, no spoke routers can ping any other spoke routers, yet all the spoke routers are able to ping the hub router. What is most likely the cause of this mishap?

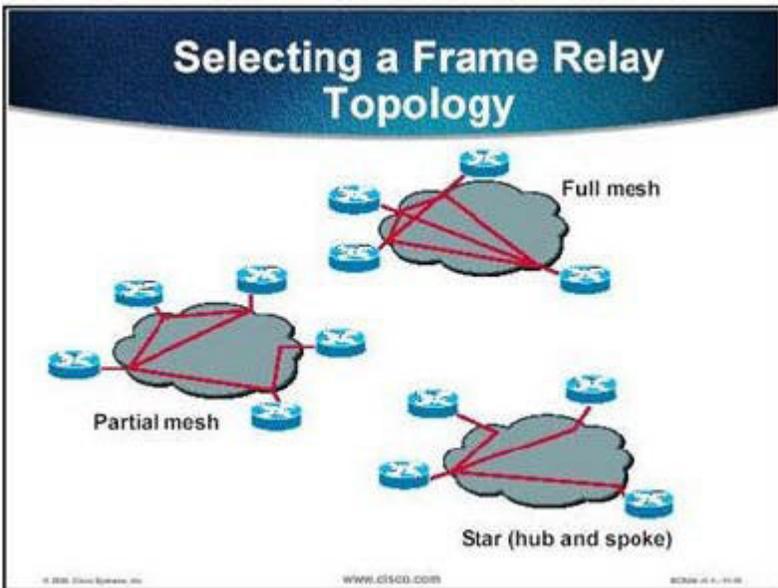
- A. Disabled split horizon
- B. Spanning-tree loop
- C. Inverse ARP issue
- D. Poison reverse issue

Answer: C

Explanation:

A star topology, also known as a hub-and-spoke configuration, is the most popular Frame Relay network topology. In this topology, remote sites are connected to a central site that generally provides a service or application. This is the least expensive topology because it requires the least number of PVCs. In this scenario, the central router provides a multipoint connection because it is typically using a single interface to interconnect multiple PVCs.

You cannot ping from one spoke to another spoke in a hub and spoke configuration using multipoint interfaces because there is no mapping for the other spokes' IP addresses. Only the hub's address is learned via the Inverse Address Resolution Protocol (IARP). If you configure a static map using the frame-relay map command for the IP address of a remote spoke to use the local data link connection identifier (DLCI), you can ping the addresses of other spokes.



Incorrect Answers:

A: Disabling the split horizon feature would actually fix this issue in many frame relay networks where the hub site is using the main serial interface (not using sub-interfaces).

B: This is a layer 2 bridging/switching mechanism and has no relevance in layer 3 pings being successful on a network.

D: This is not likely at all, since all remote locations are unable to ping each other, but they can ping the main site.

Reference:

http://www.cisco.com/en/US/tech/CK713/CK237/technologies_tech_note09186a008014f8a7.shtml#topic2

QUESTION 373:

What command could you use if you wanted to find out the number of successful and failed calls?

- A. show interface
- B. show isdn q931
- C. show dialer
- D. show isdn active call
- E. All of the above
- F. None of the above

Answer: C

Explanation:

The show dialer command displays: status, connection information, and the number connected to for each B channel; as well as a list of successful and failed calls.

QUESTION 374:

The "show isdn status" command was issued on a Certkiller router as displayed below:

```
Router CK1 #show isdn status
Global ISDN Switchtype = basic-ni
ISDN BRI0 interface dsl 0, interface ISDN
Switchtype = basic-ni
Layer 1 Status:
ACTIVE
Layer2 Status:
TEI = 73, Ces = 2, SAPI = 0, State = TEI_ASSIGNED
TEI = 74, Ces = 1, SAPI = 0, State = TEI_ASSIGNED
Layer 3 Status :
0 Active Layer 3 Call(s)
```

What is true about the router in the command output above?

- A. Layer 1, 2, and 3 status is active.
- B. Layer 1 status is active but Layer 2 status indicates lost connectivity.
- C. TEI values assigned are not a valid numbers.
- D. Layers 1 and 2 status is active but Layer 3 status indicates lost connectivity.

Answer: B

Explanation:

The show isdn status output shown below is an example of a properly functioning BRI circuit. In the following example, Layer 1 is MULTIPLE_FRAME_ESTABLISHED, the Terminal Endpoint Identifiers (TEIs) have been successfully negotiated, and ISDN Layer 3 (end-to-end) is ready to make or receive calls. The items you should pay attention to are linked to each corresponding field in the table shown below.

```
maui-nas-01# show isdn status
ISDN Switchtype
= basic-ni1
```

ISDN BRI0 interface

Layer 1

Status:

ACTIVE

Layer 2

Status:

TEI = 109, State = MULTIPLE_FRAME_ESTABLISHED

TEI = 110, State = MULTIPLE_FRAME_ESTABLISHED

Spid Status

:

Endpoint ID Info: epsf = 0, usid = 3, tid = 1

TEI 109, ces = 1, state = 8(established)

spid1 configured, spid1 sent, spid1 valid

Endpoint ID Info: epsf = 0, usid = 1, tid = 1

TEI 110, ces = 2, state = 8(established)

spid2 configured, spid2 sent, spid2 valid

Layer 3 Status

:

0 Active Layer 3 Call(s)

Activated dsl 0 CCBs = 0

Total Allocated ISDN CCBs = 0

QUESTION 375:

The "show line" command was issued on the Certkiller terminal server as displayed below:

Certkiller TermsSrv#show line

Tty	Typ	Tx/Rx	A	Modem	Roty	AccO	AccI	Uses	Noise	Overruns
0	CTY		-	-	-	-	-	0	0	0/0
1	TTY	9600/9600	-	-	-	-	-	0	136	0/0
2	TTY	9600/9600	-	-	-	-	-	0	73	0/0
3	TTY	9600/9600	-	-	-	-	-	0	69	0/0
4	TTY	9600/9600	-	-	-	-	-	0	82	0/0
5	TTY	9600/9600	-	-	-	-	-	0	26	0/0
6	TTY	9600/9600	-	-	-	-	-	0	0	0/0
7	TTY	9600/9600	-	-	-	-	-	0	21	0/0
8	TTY	9600/9600	-	-	-	-	-	0	21	0/0
9	AUX	9600/9600	-	-	-	-	-	0	0	0/0
10	VTY		-	-	-	-	-	2	0	0/0
11	VTY		-	-	-	-	-	0	0	0/0
12	VTY		-	-	-	-	-	0	0	0/0
13	VTY		-	-	-	-	-	0	0	0/0
14	VTY		-	-	-	-	-	0	0	0/0
15	VTY		-	-	-	-	-	0	0	0/0
16	VTY		-	-	-	-	-	0	0	0/0
17	VTY		-	-	-	-	-	0	0	0/0
18	VTY		-	-	-	-	-	0	0	0/0
19	VTY		-	-	-	-	-	0	0	0/0

Based on the information above, how is the router being accessed?

- A. console port 0
- B. asynchronous port 0
- C. asynchronous port 7
- D. auxiliary port 0
- E. virtual terminal port 0

F. virtual terminal port 10

Answer: F

Explanation:

If you look carefully at the command output, and pay attention to the left column you should notice an asterisk right before the phrase '10 VTY'; this shows that virtual terminal number 10 is being accessed. The asterisk shows the means by which the local session is being used when accessing the device.

QUESTION 376:

Which of the following statements best describes the term spoofing in the following output?

Router Certkiller 1#show interface dialer1

Dialer1 is up, line protocol is up (spoofing)

- A. The router is allowed to act as a proxy Domain Name System (DNS) server.
- B. The router is protected from accepting traffic from outside the network which is pretending to be from inside the network.
- C. The dialer is allowed to masquerade as "up" so that upper level protocols will continue to operate as expected.
- D. Prevents full periodic routing updates from being passed on the line and only allows routing updates on network changes.

Answer: C

Explanation:

Interfaces - up/up (spoofing)

In order for packets to be routed to and through an interface, that interface must be up/up as seen in a show interfaces output:

Montecito# show interfaces ethernet 0

Ethernet0 is up, line protocol is up

Hardware is Lance, address is . . .

What happens to a dialer interface that is not connected? If protocol is not up and running on the interface, the implication is that the interface itself will not be up. Routes which rely on that interface will be flushed from the routing table, and traffic will not be routed to that interface. The result is that no calls would be initiated by the interface.

The solution to counter this possibility is to allow the state up/up (spoofing) for dialer interfaces. Any interface can be configured as a dialer interface. For example, a Serial or Async interface could be made into a dialer by adding the command dialer in-band or dialer dtr to the interface's configuration. These lines are unnecessary for interfaces that are by nature a dialer interface (BRIs and PRIs). The output for a show interface will look like this:

Montecito# show interfaces bri 0

BRI0 is up, line protocol is up (spoofing)

Hardware is BRI

Internet address is . . .

In other words, the interface "pretends" to be up/up so that associated routes will remain in force and so that packets can be routed to the interface.

QUESTION 377:

Study the command output below:

kickin load 60% kickout load 40%

Which of the following commands is capable of producing the above output?

- A. show load
- B. show primary
- C. show dialer-profile
- D. show interface
- E. show backup

Answer: D

Explanation:

Use the show interfaces command to display status and counter information about an interface. The following example illustrates this:

```
----->
CK1 # show interfaces s0/1
Serial0/1 is up, line protocol is up
Hardware is PowerQUICC Serial
Description: connects to X.25 switch
Internet address is 10.10.0.30/24
Backup interface Serial0/0, failure delay 0 sec, secondary
disable delay 0 sec,
kickin load not set, kickout load not set
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation X25, loopback not set
X.25 DCE, address 3034, state R1, modulo 8, timer 0
----->
```

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080110d07.html

QUESTION 378:

An 806 router E1 interface is connected to a cable modem. The end-user PC is connected to the 806 router E0 interface. The end-user PC is having Internet connectivity issues but the 806 router is able to ping the different Internet sites. Which two errors could be causing the problem? (Choose two)

- A. The 806 is configured as the DHCP server, but the end-user PC is not setup for DHCP.
- B. The static default route is not configured correctly on the 806 router.
- C. Port Address Translation (PAT) is not configured correctly on the 806 router.
- D. The 806 router is not properly configured to act as the PPPoE client.
- E. The 806 router is not properly configured for PPP CHAP authentication.

Answer: A, C

Explanation:

If the Cisco is configured as the DHCP server but the PC is configured with a static IP address, the PC will not obtain an IP address dynamically from the server. This could explain why the PC is having Internet connectivity issues.

Another explanation is that the Cisco is not correctly configured for PAT. Port address translation is used to allow multiple inside hosts to share a single IP address so that the hosts can appear to the Internet to have a registered IP address.

All of the other answer choices are incorrect. If they were true, then the Cisco router itself would not be able to access the Internet.

QUESTION 379:

CORRECT TEXT

While logged into one of the Certkiller ISDN routers, you wish to see the active calls. What command will display the number of active calls? (Type in answer below)

Answer: show isdn status

Explanation:

The "show isdn status" command ensures that the router is properly communicating with the ISDN switch. In the output, verify that Layer 1 Status is ACTIVE, and that the Layer 2 Status state = MULTIPLE_FRAME_ESTABLISHED appears. This command also displays the number of active calls.

QUESTION 380:

Within the Certkiller network, you have multiple ISDN user devices physically attached to one circuit. Which of the following can happen as a result of this? (Choose all that apply)

- A. Compression
- B. Collisions
- C. Encryption
- D. Contention
- E. None of the above

Answer: B, D

Explanation:

Multiple ISDN user devices can be physically attached to one circuit. In this configuration, collisions can result if two terminals transmit simultaneously. ISDN therefore provides features to determine link contention. When an NT receives a D bit from the TE, it echoes back the bit in the next E-bit position. The TE expects the next E bit to be the same as its last transmitted D bit.

QUESTION 381:

CORRECT TEXT

While troubleshooting a router issue, you suspect that the CPU may be becoming over-utilized. What command do you use to check the CPU utilization of the router? (Type in answer below)

Answer: show process cpu

Explanation:

Software compression is available in all router platforms. Software compression is performed by the main processor in the router. Compression is performed in software and might significantly affect system performance. We recommend that you disable compression if the router CPU load exceeds 65 percent. To display the CPU load, use the "show process cpu" EXEC command.

QUESTION 382:

CORRECT TEXT

You are a Cisco Certified Engineer and have been assigned the task of configuring a DDR remote access solution. What command may be used to show the general diagnostic information for interfaces configured? (Type in answer below)

Answer: show dialer

Explanation:

The show dialer [interface type number] command displays general diagnostic information for interfaces configured for DDR. If the dialer came up properly, the Dialer state is data link layer up message should appear. If physical layer up appears, then the line protocol came up, but the Network Control Protocol (NCP) did not. The source and destination addresses of the packet that initiated the dialing are shown in the Dial reason line. This show command also displays the timer's configuration and the time before the connection times out.

QUESTION 383:

Router CK1 is configured as an access server. The following command was issued on router CK1 :

```
ip host corpX 1098 157.11.11.96
```

From this command, which of the following is true?

- A. 157.11.11.96 is NOT a valid IANA approved IP address.
- B. 157.11.11.96 is the IP address of the remote host.
- C. The command allows a reverse telnet connection.
- D. The configuration applies in 1098 seconds.
- E. 1098 is the dialer group ID.

Answer: B

Explanation:

The access server maintains a table of host names and their corresponding addresses, also called host name-to-address mapping. Higher-layer protocols such as Telnet use host names to identify network devices (hosts). The access server and other network devices must be able to associate host names with IP addresses to communicate with other IP devices. Host names and IP addresses can be associated with one another through static or dynamic means.

Manually assigning host names to addresses is useful when dynamic mapping is not available.

To assign host names to addresses, perform the following task in global configuration mode:

Task	Command
Statically associate host names with IP addresses.	<pre>ip host <i>hostname</i> [<i>tcp-port-number</i>] <i>address1</i> [<i>address2...address8</i>]</pre>

In this example, the name corpX is being statically mapped to 157.11.11.96 using TCP port 1098.

QUESTION 384:

Router CK1 is configured as shown below:

```
interface serial 1  
ip address 128.10.200.65 255.255.255.192  
dialer in-band  
!  
ip route 0.0.0.0 0.0.0.0 128.10.200.66
```

Which of the following is true?

- A. This configuration is for an outgoing call only configuration
- B. This configuration is for an answer and outgoing call configuration
- C. This configuration is for an answer only configuration
- D. This configuration is not valid

Answer: C

Explanation:

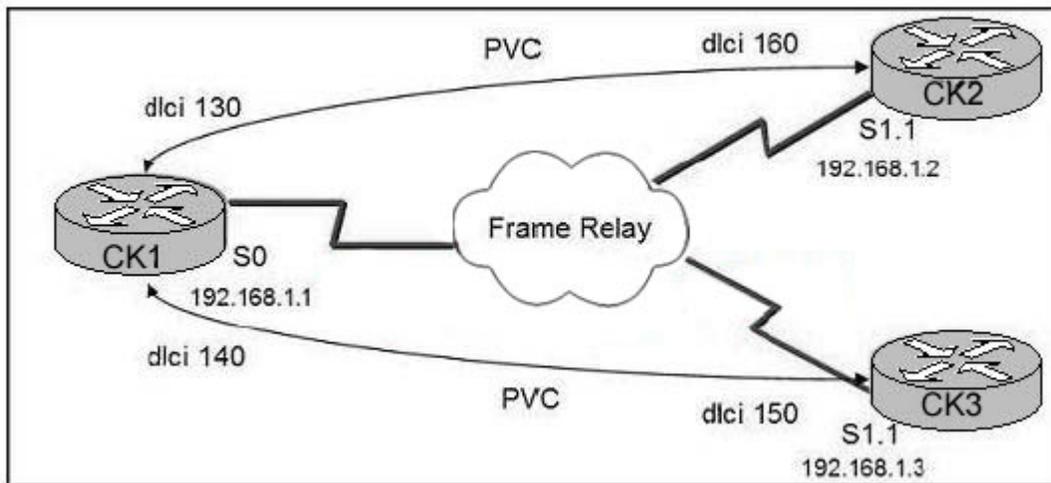
The dialer in-band command specifies that chat scripts will be used on asynchronous interfaces and V.25bis will be used on synchronous interfaces. The parity keywords do not apply to asynchronous interfaces.

The parity setting applies to the dialer string that is sent out to the modem. If you do not specify a parity value, or if you specify no parity, no parity is applied to the output number. If odd parity is configured, the dialed number will have odd parity (7-bit ASCII characters with the eighth bit as the parity bit.)

If an interface only accepts calls and does not place calls, the dialer-in-band interface configuration command is the only command needed to configure it. If an interface is configured in this manner, with no dialer rotary groups, the idle timer never disconnects the line. It is up to the remote end (the end that placed the call) to disconnect the line based on idle time.

QUESTION 385:

Three Certkiller routers are connected as shown in the diagram below:



Refer to the exhibit. An administrator is not able to ping from CK2 to CK3 in the Frame Relay network. A show running-config command partial output displays the following:

```
CK2 # show running-config
!
interface Serial1
no ip address
encapsulation frame-relay
!
interface Serial1.1
ip address 192.168.1.2 255.255.255.0
frame-relay map ip 192.168.1.1 160
```

What command could be used on the CK2 multipoint serial 1.1 subinterface to complete a successful ping to CK3 ?

- A. CK2 (config-if)# frame-relay map ip 192.168.1.1 160
- B. CK2 (config-if)#frame-relay map ip 192.168.1.3 150
- C. CK3 (config-if)#frame-relay map ip 192.168.1.3 160
- D. CK2 (config-if)#frame-relay map ip 192.168.1.1 30
- E. CK2 (config-if)#frame-relay map ip 192.168.1.2 160
- F. CK2 (config-if)#frame-relay map ip 192.168.1.2 150

Answer: C

Explanation:

In order to be able to ping across a frame relay NBMA network, you need to either specify a separate sub-interface used for each PVC, or use frame-relay map statements used to specify the remote router. In this multi-point network, the spoke routers (CK2 and CK3) only have a single PVC to the hub CK1 location. So, for CK2 to be able to ping another remote router, a map must be made specifying the remote routers IP address, as well as the DLCI used to reach it. Since the only DLCI value it can use is 160 (to CK1) choice C is correct.

QUESTION 386:

You are verifying ISDN connectivity between two Certkiller routers. Which two commands will verify an ISDN circuit operation end to end? (Choose two)

- A. show isdn status
- B. debug isdn q931
- C. debug dialer
- D. debug isdn q921
- E. debug serial interface

Answer: B, C

Explanation:

The "debug dialer" and "debug isdn q931" can both be used to verify ISDN call setup and completion. When DDR is enabled on the interface, information concerning the cause of any call (called the Dialing cause) is displayed using the "debug dialer" command. The following line of output for an IP packet lists the name of the DDR interface and the source and destination addresses of the packet:

Dialing cause: Serial0: ip (s=172.16.1.111 d=172.16.2.22)

Here is a sample output of the debug isdn q931 command. The output indicates the disconnect cause code for a failed ISDN call:

Calling#ping 10.10.10.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.10.10.2, timeout is 2 seconds:

20:52:14: ISDN BR0: TX -> SETUP pd = 8 callref = 0x2E

20:52:14: Bearer Capability i = 0x8890

20:52:14: Channel ID i = 0x83 20:52:14: Keypad Facility i = '5551111'

20:52:15: ISDN BR0: RX <- CALL_PROC pd = 8 callref = 0xAE
20:52:15: Channel ID i = 0x89
20:52:16: ISDN BR0: RX <- PROGRESS pd = 8 callref = 0xAE
20:52:16: Progress Ind i = 0x8A81 - Call not end-to-end ISDN,
may have in-band info
20:52:16: Signal i = 0x01 - Ring back tone on
20:52:34: ISDN BR0: RX <- DISCONNECT pd = 8 callref = 0xAE
20:52:34: Cause i = 0x829F08 - Normal, unspecified or Special intercept,
call blocked group restriction
20:52:34: ISDN BR0: TX -> RELEASE pd = 8 callref = 0x2E
20:52:34: ISDN BR0: RX <- RELEASE_COMP pd = 8 callref = 0xAE

QUESTION 387:

A new ISDN connection has just been added to router CK1 . Which command will allow an administrator to observe signaling events between this router and the ISDN switch in real time?

- A. debug isdn q921
- B. debug isdn q931
- C. show isdn status
- D. show interface bri #
- E. None of the above

Answer: A

Explanation:

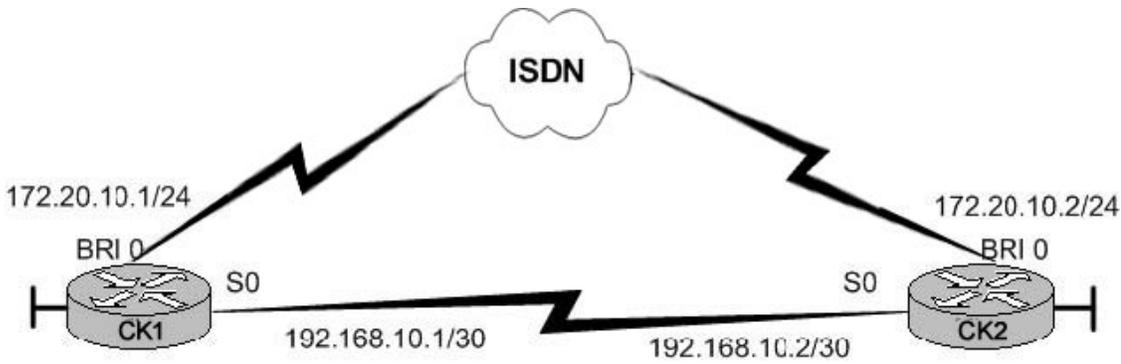
Use the debug isdn q921 privileged EXEC command to display data link layer (layer 2) access procedures that are taking place at the router on the D channel (LAPD) of its Integrated Services Digital Network (ISDN) interface.

The ISDN data link layer interface provided by the router conforms to the user interface specification defined by ITU-T recommendation Q.921. The debug isdn q921 command output is limited to commands and responses exchanged during peer-to-peer communication carried over the D channel. This debug information does not include data transmitted over the B channels that are also part of the router's ISDN interface. The peers (data link layer entities and layer management entities on the routers) communicate with each other via an ISDN switch over the D channel. The ISDN switch provides the network interface defined by Q.921.

QUESTION 388:

ISDN is being used as a backup link between two Certkiller locations as shown below:

642-821



```
CK1#show running-config
!
isdn switch-type basic-ni
!
interface Serial0
 backup delay 10 30
 backup interface BRI0
 ip address 192.168.10.1 255.255.255.252
 encapsulation ppp
!
interface BRI0
 ip address 172.20.10.1 255.255.255.0
 encapsulation ppp
 dialer map ip 172.20.10.2 name R2 broadcast 5551111
 dialer map ip 172.20.10.2 name R2 broadcast 5551112
 isdn spid1 51299699380101 9969938
 isdn spid2 51299699460101 9969946
 dialer-group 1
!
router ospf 1
 network 192.168.10.0 0.0.0.3 area 0
!
access-list 101 permit ip any any
!
dialer-list 1 protocol ip list 101
```

Refer to the exhibit above. The BRI 0 interface on CK1 is configured as a backup interface for the serial connection. The ISDN backup link was tested and was able to connect to the remote site CK2 . However, when CK1 loses the connectivity over the serial link, the backup link does not come up. What could the problem be?

- A. The OSPF hello packets are not considered as interesting traffic to dial the backup link.
- B. The ISDN backup interface network is not included in the OSPF routing protocol.
- C. The PPP authentication is not included in then backup interface configuration.
- D. The enable-timer, specified by the backup delay command, has expired before the backup interface comes up.

Answer: B

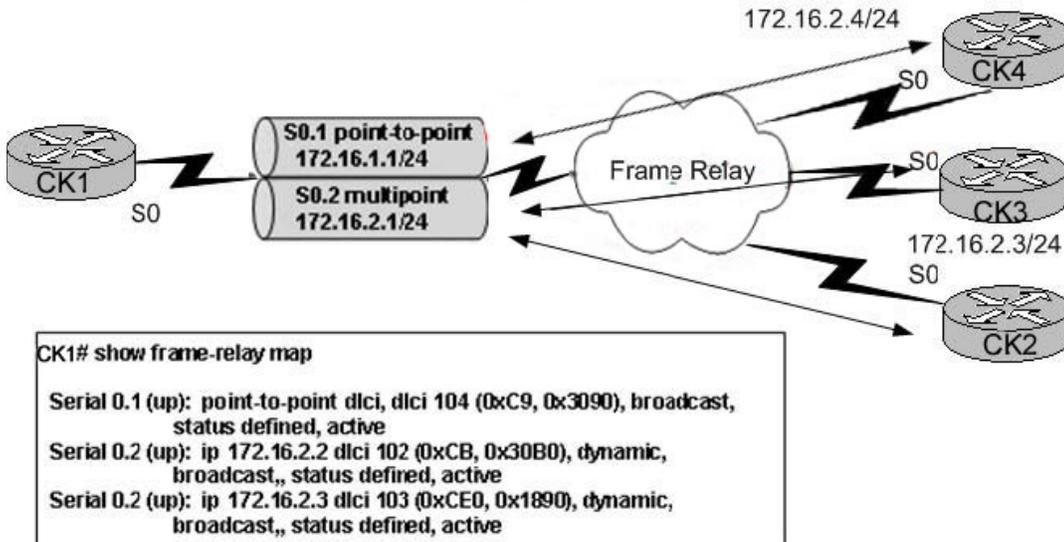
Explanation:

Since the IP subnet used for the ISDN link (172.20.10.0/24) is not included under the OSPF process, no OSPF traffic will trigger this link to come up.

Note: If this network was added under the OSPF process, then the OSPF hello packets will always keep this link up, potentially resulting in a costly situation. To truly set up the ISDN link correctly, it would need some additional configuration statements to ensure that the link only came up in a backup situation. Some of the options available here is a floating static router, using the "backup interface" command, or by making the ISDN link and OSPF demand circuit.

QUESTION 389:

The Certkiller frame relay network is depicted below:



In the exhibit, the hub router CK1 Serial0 is configured with one point-to-point and one multipoint subinterface to connect to the spoke routers. The show frame-relay map command on CK1 depicts the active status of all Frame Relay PVCs. However, the ping from CK1 to CK4 failed. What should be done to fix the problem?

- A. The CK1 subinterface and the serial interfaces all spoke routers must be on the same subnet.
- B. The CK1 subinterface must have a designated subnet for each spoke router.
- C. The CK1 point-to-point subinterface and the CK4 serial interface must be on the same subnet.
- D. All spoke routers must be on their own subnet.

Answer: C

Explanation:

As with all layer 2 network connections, the link connecting the router devices must be part of the same IP subnet. This is true for any data link level connections between routers.

QUESTION 390:

The "show ISDN status" command was issued on router CK1 as shown below:

```
CK1# show isdn status
Global ISDN Switchtype = basic-ni
ISDN BRI0 interface
dsl 0, interface ISDN Switchtype = basic-ni
Layer 1 Status:
ACTIVE
Layer 2 Status:
Layer 2 NOT Activated
TEI Not Assigned, ces = 1, state = 3(await establishment)
spid1 configured, spid1 NOT sent, spid1 NOT valid
TEI Not Assigned, ces = 2, state = 1(terminal down)
spid2 configured, spid2 NOT sent, spid2 NOT valid
Layer 3 Status:
TWAIT timer active
0 Active Layer 3 Call(s)
Activated dsl 0 CCBs = 0
The Free Channel Mask: 0x80000003
Total Allocated ISDN CCBs = 0
```

Based on the command output shown, which statement mostly likely describes the problem?

- A. The wrong spids were configured-
- B. The wrong ISDN switch was configured.
- C. The BRI 0 interface is administratively down.
- D. The IP address on the interface was incorrectly configured.
- E. There is nothing wrong with the ISDN configuration.

Answer: A

Explanation:

The show isdn status output shown below is an example of a properly functioning BRI circuit. In the following example, Layer 1 is `MULTIPLE_FRAME_ESTABLISHED`, the Terminal Endpoint Identifiers (TEIs) have been successfully negotiated, and ISDN Layer 3 (end-to-end) is ready to make or receive calls. The items you should pay attention to are linked to each corresponding field in the table shown below.

maui-nas-01#show isdn status

The current

ISDN Switchtype

= basic-ni1

ISDN BRI0 interface

Layer 1

Status:

ACTIVE

Layer 2

Status:

TEI = 109, State = `MULTIPLE_FRAME_ESTABLISHED`

TEI = 110, State = `MULTIPLE_FRAME_ESTABLISHED`

Spid Status

:
TEI 109, ces = 1, state = 8(established)
spid1 configured, spid1 sent, spid1 valid
Endpoint ID Info: epsf = 0, usid = 1, tid = 1
TEI 110, ces = 2, state = 8(established)
spid2 configured, spid2 sent, spid2 valid
Endpoint ID Info: epsf = 0, usid = 3, tid = 1
Layer 3 Status

:
0 Active Layer 3 Call(s)
Activated dsl 0 CCBs = 0
Total Allocated ISDN CCBs = 0

In our example, the layer 1 information is working properly, so the correct switch type was specified. However, the layer 2 information regarding the SPIDs is not, most likely due to incorrectly configured SPID values.

QUESTION 391:

The following output was displayed on one of the Certkiller frame relay routers:

```
PVC Statistics for interface Serial0/0 (Frame Relay DTE)

Local      Active    Inactive  Deleted   Static
Switched   0         0         0         0
Unused     0         0         0         0

DLCI = 19, DLCI USAGE = LOCAL, PVC STATUS = DELETED, INTERFACE = Serial0/0.19
...
DLCI = 18, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0.18
...
DLCI = 17, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0.17
...
DLCI = 16, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0.16
```

A hub router is connecting four sites using Frame Relay point-to-point subinterfaces. An administrator troubleshooting the issue enters the command show frame-relay pvc on the hub router. Given the above output, which statement is correct?

- B. The router is configured for a DLCI that is not detected on the other end of the PVC.
- C. The router has dynamically found a DLCI that is not intended for its network.
- D. The router is configured for Inverse ARP on the subinterfaces.
- E. The router is configured for a DLCI that the switch does not recognize.

Answer: D

Explanation:

The PVC can have four possible states. These are shown by the PVC STATUS field as follows:

ACTIVE - PVC is up and functioning normally.

INACTIVE - PVC is not up end-to-end. This may be because either there is no mapping (or incorrect mapping) for the local DLCI in the frame-relay cloud or the remote end of the PVC is deleted.

DELETED - Either the Local Management Interface (LMI) is not exchanged between the router and the local switch, or the switch does not have DLCI configured on the local switch.

STATIC - no keepalive configured on the frame-relay interface of the router.

In our example, the first DLCI (DLCI 19) is shown as deleted, most likely due to it being configured locally on the router, but not on the frame relay switch.

QUESTION 392:

The following was displayed on a Certkiller ISDN router.

```
ISDN Serial1:23 interface
  dsl 1, interface ISDN Switchtype = primary-5ess
Layer 1 Status:
  Active
Layer 2 Status:
  TEI = 0, ces = 1, SAPI = 0, State = TEI_ASSIGNED
Layer 3 Status:
  0 Active Layer 3 Call(s)
Activated dsl 1 CCBs = 0
The Free Channel Mask: 0x807FFFFF
Total Allocated ISDN CCBs = 5
```

Observe the exhibited output from a show isdn status command. Which statement is true?

- A. There were five attempts to make calls.
- B. Layer 1 is not operational.
- C. Layer 2 is operational.
- D. The router is not exchanging frames with the ISDN switch.

Answer: D

Explanation:

A state=TEI_ASSIGNED indicates that the router has lost connectivity to the switch. This is normal if the telco (commonly in Europe) deactivates Layers 1 and 2 when there are no active calls.

A fully functioning ISDN link to the switch would result in a state of MULTIPLE_FRAME_ESTABLISHED in the layer 2 portion. This is the state that you should see under normal operations. Any other state usually indicates a problem on the circuit.

Reference:

http://www.cisco.com/en/US/tech/CK8_01/CK3_79/technologies_tech_note09186a0080094b78.shtml#layer2

QUESTION 393:

You are tasked with determining the cause of the PAP problems on the Certkiller ISDN network. Which two debugs should you use to find the cause of an unsuccessful PAP negotiation? (Choose two)

- A. debug ppp pap
- B. debug ppp negotiation
- C. debug authentication chap
- D. debug ppp authentication

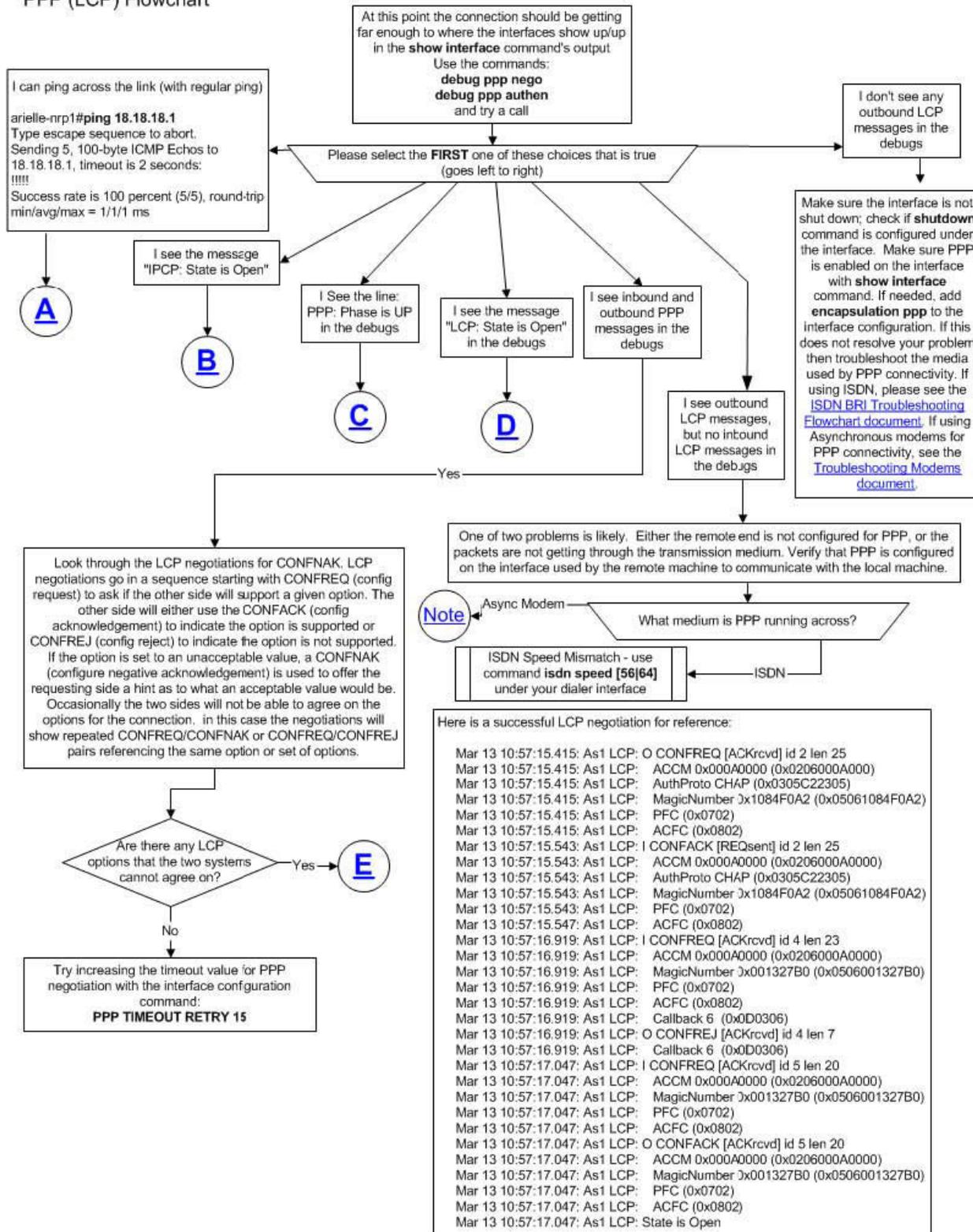
Answer: B, D

Explanation:

Troubleshooting Flowcharts

The following flow chart lists the steps in troubleshooting PPP authentication issues. Notice the two recommended debug commands are "debug PPP authentication" and "debug PPP negotiation".

PPP (LCP) Flowchart



Reference:

http://www.cisco.com/en/US/tech/CK7_13/CK5_07/technologies_tech_note09186a008019cfa7.shtml

QUESTION 394:

Which Cisco IOS command displays active Layer 3 sessions on an ISDN PRI connection, showing the call-type and B channel used?

- A. debug dialer
- B. show isdn status
- C. show dialer-group
- D. show dialer interface

Answer: B

Explanation:

The following is an example output from the "show ISDN status" command.

```
CK1 #show isdn status
```

```
The current
```

```
ISDN Switchtype
```

```
= basic-ni1
```

```
ISDN BRI0 interface
```

```
Layer 1
```

```
Status:
```

```
ACTIVE
```

```
Layer 2
```

```
Status:
```

```
TEI = 109, State = MULTIPLE_FRAME_ESTABLISHED
```

```
TEI = 110, State = MULTIPLE_FRAME_ESTABLISHED
```

```
Spid Status
```

```
:
```

```
TEI 109, ces = 1, state = 8(established)
```

```
spid1 configured, spid1 sent, spid1 valid
```

```
Endpoint ID Info: epsf = 0, usid = 1, tid = 1
```

```
TEI 110, ces = 2, state = 8(established)
```

```
spid2 configured, spid2 sent, spid2 valid
```

```
Endpoint ID Info: epsf = 0, usid = 3, tid = 1
```

```
Layer 3 Status
```

```
:
```

```
0 Active Layer 3 Call(s)
```

```
Activated dsl 0 CCBs = 0
```

```
Total Allocated ISDN CCBs = 0
```

For a complete description of the fields above and their meaning, see the link provided below.

Reference:

http://www.cisco.com/en/US/tech/CK8_01/CK3_79/technologies_tech_note09186a0080094b78.shtml

QUESTION 395:

Router Certkiller 3 is configured as shown below:

```
hostname Certkiller3
!
ip dhcp excluded-address 10.10.10.1
!
ip dhcp pool CLIENT
import all
network 10.10.10.0 255.255.255.0
default-router 10.10.10.1

interface Ethernet0
ip address dhcp
ip nat inside
no shut
!
interface Ethernet1
ip address 10.10.10.1 255.255.255.0
ip nat outside
no shut

ip route 0.0.0.0 0.0.0.0 Ethernet1
!
ip nat inside source list 102 interface Ethernet1 overload
!
access-list 102 permit ip 10.10.10.0 0.0.0.255 any
```

The Certkiller 3 router E1 interface is connected to a cable modem and the E0 interface is connected to an end-user PC. The end-user PC is having internet connectivity issues. What could be the cause of the problem?

- A. The IRB configuration is missing.
- B. The port address translation (PAT) configuration is not correct.
- C. The access-list 102 configuration is not correct.
- D. The DHCP server configuration is not correct.
- E. The IP address command on the E0 and E1 interface is wrong.

Answer: E

Explanation:

Based on the configuration above, the inside network is Ethernet 0 while the outside (Internet facing) interface is Ethernet 1. However, interface Ethernet 1 was configured with an IP address of the inside network's default gateway, while Ethernet 0 was configured with no IP address at all. If we remove the 10.10.10.1 IP address on Ethernet 1, and put this address on Ethernet 0, everything will work.

QUESTION 396:

Study the exhibit regarding RouterA in the Certkiller network below:

```
RouterA# show crypto isakmp policy
Protection suite priority 15
  encryption algorithm: DES - Data Encryption Standard (56 bit keys)
  hash algorithm:      Message Digest 5
  authentication method: Rivest-Shamir-Adleman Signature
  Diffie-Hellman Group: #2 (1024 bit)
  lifetime:            5000 seconds, no volume limit
Protection suite priority 20
  encryption algorithm: DES - Data Encryption Standard (56 bit keys)
  hash algorithm:      Secure Hash Standard
  authentication method: preshared Key
  Diffie-Hellman Group: #1 (768 bit)
  lifetime:            10000 seconds, no volume limit
Protection suite of priority 110
  encryption algorithm: DES - Data Encryption Standard (56 bit keys).
  hash algorithm:      Message Digest 5
  authentication method: Rivest-Shamir-Adleman Encryption
  Diffie-Hellman group: #1 (768 bit)
  lifetime:            86400 seconds, no volume limit
Default protection suite
  encryption algorithm: DES - Data Encryption Standard (56 bit keys).
  hash algorithm:      Secure Hash Standard
  authentication method: Rivest-Shamir-Adleman Signature
```

How many IKE policies were administratively defined above?

- A. 0
- B. 1
- C. 2
- D. 3
- E. 4

Answer: D

Explanation:

There are three policies in the exhibit (using priority 15, 20 and 110, respectively) which were manually configured on this router. The default policy is not explicitly defined, and is included as the default IKE parameters on Cisco IP Sec routers.

QUESTION 397:

Two Certkiller locations are trying to connect to each other over a VPN, but the connection is failing. Which common problem causes an IPSEC VPN to fail?

- A. ACLs configured in the IPSEC traffic path blocking ISAKMP, ESP, and AH traffic.
- B. Multiple transform sets configured but only one transform set is specified in the crypto map entry.
- C. Crypto ACL configuration errors where permit is used to specify that matching packets must be encrypted.
- D. Multiple interfaces sharing the same crypto map set.

Answer: A

Explanation:

By default, IPSec and all packets that traverse the PIX Firewall are subjected to blocking as specified by inbound conduit, outbound list or interface access-list. To enable IPSec packets to traverse the PIX Firewall, ensure that you have statements in conduits,

outbound lists or interface access-lists that permit the packets. The same holds true for IPSec routers that have access lists configured.

IKE uses UDP port 500. The IPSec ESP and AH protocols use protocol numbers 50 and 51.

Ensure your access lists are configured so that protocol 50, 51 and UDP port 500 traffic is not blocked at interfaces used by IPSec. In some cases you may be required to add a statement to your access lists to explicitly permit this traffic.

QUESTION 398:

An IPSec tunnel has just been created on the Certkiller network, and you wish to verify it. Which command will display the configured IKE policies?

- A. show crypto isakmp policy
- B. show crypto ipsec
- C. show crypto isakmp
- D. show crypto map

Answer: A

Explanation:

To display the parameters for each Internet Key Exchange (IKE) policy, use the show crypto isakmp policy command in EXEC mode.

The following is sample output from the show crypto isakmp policy command after two IKE policies have been configured (with priorities 15 and 20, respectively):

```
CK1 # show crypto isakmp policy
```

```
Protection suite priority 15
```

```
encryption algorithm: DES - Data Encryption Standard (56 bit keys)
```

```
hash algorithm: Message Digest 5
```

```
authentication method: Rivest-Shamir-Adleman Signature
```

```
Diffie-Hellman Group: #2 (1024 bit)
```

```
lifetime: 5000 seconds, no volume limit
```

```
Protection suite priority 20
```

```
encryption algorithm: DES - Data Encryption Standard (56 bit keys)
```

```
hash algorithm: Secure Hash Standard
```

```
authentication method: preshared Key
```

```
Diffie-Hellman Group: #1 (768 bit)
```

```
lifetime: 10000 seconds, no volume limit
```

```
Default protection suite
```

```
encryption algorithm: DES - Data Encryption Standard (56 bit keys)
```

```
hash algorithm: Secure Hash Standard
```

```
authentication method: Rivest-Shamir-Adleman Signature
```

```
Diffie-Hellman Group: #1 (768 bit)
```

```
lifetime: 86400 seconds, no volume limit
```

QUESTION 399:

While troubleshooting an IPsec VPN, the following was seen on router R1:

```
R1#debug crypto isakmp
00:02:58: ISAKMP: received ke message (1/1)
00:02:58: ISAKMP (0:0): SA request profile is (NULL)
00:02:58: ISAKMP: local port 500, remote port 500
00:02:58: ISAKMP: set new node 0 to QM_IDLE
00:02:58: ISAKMP: insert sa successfully sa = 82AF88B8
00:02:58: ISAKMP (0:1): Can not start Aggressive mode, trying Main mode.
00:02:58: ISAKMP: Looking for a matching key for 10.1.1.1 in default : success
00:02:58: ISAKMP (0:1): found peer pre-shared key matching 10.1.1.1
00:02:58: ISAKMP (0:1): constructed NAT-T vendor-07 ID
00:02:58: ISAKMP (0:1): constructed NAT-T vendor-03 ID
00:02:58: ISAKMP (0:1): constructed NAT-T vendor-02 ID
00:02:58: ISAKMP (0:1): Input = IKE_MSG_FROM_IPSEC, IKE_SA_REQ_MM
00:02:58: ISAKMP (0:1): Old State = IKE_READY New State = IKE_I_MM1

00:02:58: ISAKMP (0:1): beginning Main mode xchange
00:02:58: ISAKMP (0:1): sending packet to 10.1.1.1 my_port 500 peer_port 500 (I) MM_NO_STATE
00:02:58: ISAKMP (0:1): received packet from 10.1.1.1 dport 500 sport 500 Global (I) MM_NO_STATE
00:02:58: ISAKMP (0:1): Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
00:02:58: ISAKMP (0:1): Old State = IKE_I_MM1 New State = IKE_I_MM2

00:02:58: ISAKMP (0:1): processing SA payload. message ID = 0
00:02:58: ISAKMP (0:1): processing vendor id payload
00:02:58: ISAKMP (0:1): vendor ID seems Unity/DPD but major 245 mismatch
00:02:58: ISAKMP (0:1): vendor ID is NAT-T v7
00:02:58: ISAKMP: Looking for a matching key for 10.1.1.1 in default : success
00:02:58: ISAKMP (0:1): found peer pre-shared key matching 10.1.1.1
00:02:58: ISAKMP (0:1) local preshared key found
00:02:58: ISAKMP : Scanning profiles for xauth ...
00:02:58: ISAKMP (0:1): Checking ISAKMP transform 1 against priority 100 policy
```

Refer to the graphic. Which configuration statements match the debug output shown above?

- A. crypto isakmp policy 100
encr aes
authentication rsa-encr
group 5
- B. crypto isakmp policy 100
encr 3des
authentication pre-share
group 2
- C. crypto isakmp policy 100
hash md5
authentication rsa-sig
- D. crypto isakmp policu 100
encr des
lifetime 7200
- E. crypto isakmp policy 100
hash md5
group 1
lifetime 7200

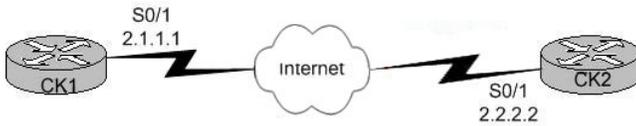
Answer: B

Explanation:

The answer lies near the bottom of the output, where it states "found peer pre-shared key matching 10.1.1.1" and "local preshared key found." Choice B is the only choice that is configured for using pre-shared key authentication.

QUESTION 400:

Exhibit:



```
CK1#show crypto isakmp sa
dst      src      state   conn-id slot
2.1.1.1  2.2.2.2  QM_IDLE 3      0
```

Refer to the exhibit. A network administrator is verifying a site-to-site IPsec VPN configuration. Based on the output shown, what must be true about CK1 and CK2 ?

- A. CK1 and CK2 have not completed IKE Phase 1.
- B. CK1 and CK2 have not completed IKE Phase 2.
- C. CK1 and CK2 are authenticated IKE peers.
- D. CK1 and CK2 maintain unidirectional IPsec SAs with each other.
- E. CK1 and CK2 have timed out their IPsec SAs.

Answer: C

Explanation:

The QM idle is the normal operating state of the security association (SA).

The following is sample output from the show crypto isakmp sa command after IKE negotiations have been successfully completed between two peers:

```
Router# show crypto isakmp saf_vrf/i_vrf dst src state conn-id slot
/vpn2 172.21.114.123 10.1.1.1 QM_IDLE 13 0
```

Table 29 through Table 32 show the various states that may be displayed in the output of the show crypto isakmp sa command. When an Internet Security Association and Key Management Protocol (ISAKMP) SA exists, it will most likely be in its quiescent state (QM_IDLE). For long exchanges, some of the MM_xxx states may be observed.

Table 29 States in Main Mode Exchange

State	Explanation
MM_NO_STATE	The ISAKMP SA has been created, but nothing else has happened yet. It is "larval" at this stage—there is no state.
MM_SA_SETUP	The peers have agreed on parameters for the ISAKMP SA.
MM_KEY_EXCH	The peers have exchanged Diffie-Hellman public keys and have generated a shared secret. The ISAKMP SA remains unauthenticated.
MM_KEY_AUTH	The ISAKMP SA has been authenticated. If the router initiated this exchange, this state transitions immediately to QM_IDLE, and a Quick Mode exchange begins.

Table 30 States in Aggressive Mode Exchange

State	Explanation
AG_NO_STATE	The ISAKMP SA has been created, but nothing else has happened yet. It is "lava" at this stage—there is no state.
AG_INIT_EXCH	The peers have done the first exchange in aggressive mode, but the SA is not authenticated.
AG_AUTH	The ISAKMP SA has been authenticated. If the router initiated this exchange, this state transitions immediately to QM_IDLE, and a quick mode exchange begins.

Table 31 States in Quick Mode Exchange

State	Explanation
QM_IDLE	The ISAKMP SA is idle. It remains authenticated with its peer and may be used for subsequent quick mode exchanges. It is in a quiescent state.

Table 32 show crypto isakmp sa Field Descriptions

Field	Description
f_vrf/i_vrf	The front door virtual routing and forwarding (FVRF) and the inside VRF (IVRF) of the IKE SA. If the FVRF is global, the output shows f_vrf as an empty field.

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_command_reference_chapter09186a008017

QUESTION 401:

You've come to a job site to check the traffic flow on a Frame Relay connection. A hub router has its DE set to 1 when receiving frames. Meanwhile a remote router is receiving frames with the DE bit set to 0. What does this indicate about traffic?

- A. CIR exceeded in both directions.
- B. CIR exceeded from remote route to hub router.
- C. CIR exceeded from hub router to remote router.
- D. CIR exceeded in neither direction.

Answer: B

Explanation:

Frame Relay service provider's use a parameter called committed information rate (CIR) to provision network resources to a Frame Relay user and regulate usage according to the assigned parameters. A mechanism written for the Frame Relay protocol exists for letting Frame Relay users know that congestion has been encountered within the Frame Relay network. This mechanism relies on the FECN/BECN bits in the Q.922 header of the frame. The network or the user can selectively set the discard eligible (DE) bit in the

frames and drop these frames when congestion is encountered. When the DE bit is set to 1, this means that the frame is Discard Eligible, and that it has exceeded the CIR.

Frames transmitted in excess of CIR	The number of frames transmitted to the attached equipment which have one of the following conditions: <ul style="list-style-type: none">• Were determined at ingress to exceed the configured Committed Information Rate (CIR) for the PVC, or,• Were received at ingress with DE = 1 and the Discard Eligible (DE) feature is enabled, or,• Were received at ingress when the virtual circuit (VC) queue exceeded the configured DE threshold and the DE feature is enabled.
-------------------------------------	--

Reference:

Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)

Page 302

QUESTION 402:

You're a Frame Relay specialist, and you've been called in to assist in a troubleshooting job. The local administrator tells you that the router is receiving frames with the BECN bit set (at 60 second intervals) but it IS NOT receiving frames with the FECN bit set. From the information he's just given, you're certain that there's too much traffic congestion on the Frame Relay switch. In which direction is there too much traffic?

- A. Too much traffic in both directions.
- B. Too much traffic within the local network.
- C. Too much traffic from remote router to local router.
- D. Too much traffic from local router to remote router.

Answer: D

Explanation:

In a frame relay network, FECN (forward explicit congestion notification) is a header bit transmitted by the source (sending) terminal requesting that the destination (receiving) terminal slow down its requests for data. BECN (backward explicit congestion notification) is a header bit transmitted by the destination terminal requesting that the source terminal send data more slowly. FECN and BECN are intended to minimize the possibility that packets will be discarded (and thus have to be resent) when more packets arrive than can be handled.

If the source terminal in a communications circuit generates frequent FECN bits, it indicates that the available network bandwidth (at that time) is not as great as can be supported by the destination terminal. Likewise, if the destination generates frequent BECN bits, it means the available network bandwidth (at that time) is not as great as can be supported by the source. In either case, the root cause is lack of available bandwidth at the times during which FECN or BECN bits are generated. This can occur because of outdated or inadequate network infrastructure, heavy network traffic, high levels of line noise, or portions of the system going down. Identifying and resolving these issues can improve overall network performance, especially when the system is called upon to carry

a large volume of traffic.

Reference:

http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci787381,00.html

QUESTION 403:

On RTA, the "show compress" command was issued as shown below:

```
RTA# show compress:
Serial2
uncompressed bytes xmt/rcv 120000/120500
1 min avg ratio xmt/rcv 0.789/0.837
5 min avg ratio xmt/rcv 0.789/0.837
10 min avg ratio xmt/rcv 0.789/0.837
no bufs xmt 0 no bufs rcv 0
restarts 0
Additional Stacker Stats
Transmit bytes: Uncompressed = 40000 Compressed = 40000
Received bytes: Compressed = 50000 Uncompressed = 0
```

Given the above output, which two statements are true concerning PPP compression? (Choose two)

- A. The interface is configured with TCP header compression.
- B. The interface is configured with STAC compression.
- C. The interface is configured with predictor compression.
- D. The overall data compression ratio is 2:1.
- E. The total amount of data to be transmitted before applying compression is 120,000.
- F. The total amount of data to be transmitted after applying compression is 40,000.

Answer: B, D

Explanation:

Compression is a link efficiency mechanism, which can be used to reduce the size of the payload and packet headers. This creates more bandwidth on a given link. You can perform compression either in software, or through hardware compression modules. Cisco IOS supports Stacker, Predictor and MPPC algorithms at link layer for payload compression. Each algorithm differs in the utilization of router resources required, and in their compression efficiency.

Sample Output:

Here is a sample output of the show compress command:

```
router1#show compress
Serial2
Software compression enabled
uncompressed bytes xmt/rcv 81951/85500
compressed bytes xmt/rcv 0/0
1 min avg ratio xmt/rcv 0.789/0.837
5 min avg ratio xmt/rcv 0.789/0.837
10 min avg ratio xmt/rcv 0.789/0.837
no bufs xmt 0 no bufs rcv 0
```

restarts 0

Additional Stacker Stats:

Transmit bytes: Uncompressed = 28049 Compressed = 65745

Received bytes: Compressed = 74738 Uncompressed = 0

These sections explain this sample output.

Software Compression

After the serial number, the first line in the output displays "Software compression enabled".

This line indicates that compression is configured.

Note: Software compression makes heavy demands on the processor of the router. The maximum compressed serial line rate depends on the type of Cisco router you use, and the compression algorithm you specify.

Uncompressed Bytes

uncompressed bytes xmt/rcv 81951/85500

This line in the output provides a count of uncompressed bytes of the compressed data. It does not include packets that cannot be compressed.

Compressed Bytes

compressed bytes xmt/rcv 0/0

This line gives the total number of already compressed bytes that are sent or received.

Throughput Ratio

The next section of output indicates a ratio of the data throughput gained or lost in the compression routine. Any number less than one indicates that the compression actually slows down data throughput. It does not reflect how compressible the data is.

1 min avg ratio xmt/rcv 0.789/0.837

5 min avg ratio xmt/rcv 0.789/0.837

10 min avg ratio xmt/rcv 0.789/0.837

Here are the common causes of poor compression ratios:

1. High CPU utilization.
2. A high percentage of small packets.
3. Data that is not very redundant (for instance, if it has already been compressed).

Buffer Allocation

no bufs xmt 0 no bufs rcv 0

This line indicates the number of times the compression routine was not able to allocate a buffer to compress or decompress a packet.

Restarts

restarts 0

This represents the number of times the compression routine detected that the dictionaries were out of sync and restarted to build a dictionary. Line errors are a common cause of restarts.

Bytes Transmitted

Transmit bytes: Uncompressed = 28049 Compressed = 65745

Here:

The uncompressed value is the amount of data that cannot be compressed, and has been sent in uncompressed format.

The compressed value represents the byte-count of the data after it is compressed.

The sum of these two values represents the actual number bytes transmitted on the

interface, minus the layer two encapsulation overhead.

Bytes Received

Received bytes: Compressed = 74738 Uncompressed= 0

Here:

The compressed value is the byte-count of the compressed data received.

The uncompressed value is the amount of data that was received in uncompressed format.

The sum of these two values represents the actual byte count received on the interface, minus the layer two encapsulation overhead.

Interpret the show compress Output:

From this output, you can calculate:

1. The total amount of data to be transmitted before you apply the compression routine:

$$81951 + 28049 = 110000$$

1. The total amount of data to be transmitted after you compress it:

$$28049 + 65745 = 93794$$

1. The overall data compression:

$$110000 / 93794 = 1.17$$

1. The compression ratio of the compressed packets:

$$81951 / 65745 = 1.24$$

In the example for our question here:

1. The total amount of data to be transmitted before you apply the compression routine:

$$120000 + 40000 = 160000$$

1. The total amount of data to be transmitted after you compress it:

$$40000 + 40000 = 80000$$

1. The compression ratio of the compressed packets:

$$160000/80000 = 2 \text{ to } 1, \text{ making choice D correct.}$$

Reference:

http://www.cisco.com/en/US/tech/ CK7 13/ CK8 02/technologies_tech_note09186a008035b8c5.shtml#topic1d

QUESTION 404:

The following command was issued on router CK1 :

```
CK1 # show frame-relay pvc
```

```
PVC Statistics for interface Serial1 (Frame Relay DTE)
```

```
DLCI = 100M DLCI USAGE = LOCAL
```

```
PVC STATUS = INACTIVE INTERFACE = Serial1
```

```
input pkts 0 output pkts 0 in bytes 0
```

```
out bytes 0 dropped pkts 0 in FECN pkts 0
```

```
in BECN pkts 0 out FECN pkts 0 out BECN pkts 0
```

```
in DE pkts 0 out DE pkts 0
```

```
outcast pkts 0 outcast bytes 0
```

Given the above output, which statement is true?

- A. An LMI is not being received from the Frame Relay switch.
- B. The DLCI has been removed from the Frame Relay switch.
- C. The remote router connection to the Frame Relay switch is not functioning.
- D. The router is configured to be a Frame Relay switch

Answer: C

Explanation:

The PVC can have four possible states. These are shown by the PVC STATUS field as follows:

ACTIVE - PVC is up and functioning normally.

INACTIVE - PVC is not up end-to-end. This may be because either there is no mapping (or incorrect mapping) for the local DLCI in the frame-relay cloud or the remote end of the PVC is deleted.

DELETED - Either the Local Management Interface (LMI) is not exchanged between the router and the local switch, or the switch does not have DLCI configured on the local switch.

STATIC - no keepalive configured on the frame-relay interface of the router.

Since this PVC is inactive and appears to have a local DLCI usage assigned, the remote router's connection to the frame relay network must not be functioning correctly.

QUESTION 405:

A Frame Relay PVC status is reported as "Deleted" on the local router. Which statement is true about the PVC configuration?

- A. The PVC is not configured on the CSU/DSU.
- B. The PVC is not configured on the local router.
- C. The PVC is not configured on the remote router.
- D. The PVC is not configured on the Frame Relay switch.

Answer: D

Explanation:

A frame relay PVC can have four possible states. These are shown by the PVC STATUS field as follows:

ACTIVE - PVC is up and functioning normally.

INACTIVE - PVC is not up end-to-end. This may be because either there is no mapping (or incorrect mapping) for the local DLCI in the frame-relay cloud or the remote end of the PVC is deleted.

DELETED - Either the Local Management Interface (LMI) is not exchanged between the router and the local switch, or the switch does not have the DLCI configured on the local frame relay switch.

STATIC - no keepalive configured on the frame-relay interface of the router.

QUESTION 406:

A Frame Relay switch informs a router that there are five PVCs available. The DLCIs assigned to these PVCs are 17, 18, 19, 20, and 21.

Router CK1 is configured with 5 point to point subinterfaces for these DLCI's. How

does the router know which DLCI to use with each subinterface?

- A. Each subinterface must manually be associated with the correct DLCI.
- B. Each subinterface learns the correct DLCI from the Frame Relay switch.
- C. Each subinterface learns the correct DLCI from the routing protocol.
- D. Each subinterface automatically accepts the first available DLCI.
- E. Each subinterface is dynamically associated with the correct DLCI via Inverse ARP.

Answer: A

Explanation:

For point-to-point subinterfaces, the destination is presumed to be known and is identified or implied in the frame-relay interface-dlci command. For multipoint subinterfaces, the destinations can be dynamically resolved through the use of Frame Relay Inverse ARP or can be statically mapped through the use of the frame-relay map command.

If you specified a point-to-point subinterface in the configuration, you must perform the following task in interface configuration mode:

Task	Command
Associate the selected point-to-point subinterface with a DLCI.	frame-relay interface-dlci [option]

This statically maps the interface to a DLCI.

If you define a subinterface for point-to-point communication, you cannot reassign the same subinterface number to be used for multipoint communication without first rebooting the router. Instead, you can simply avoid using that subinterface number and use a different subinterface number instead.

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products_configuration_guide_chapter09186a008008

QUESTION 407:

While troubleshooting a frame relay issue with the Certkiller network, the following command was issued:

```
Router1# debug frame-relay lmi
Serial0(in): Status, myseq 18
RT IE 1, length 1, type 0
KA IE 3, length 2, yourseq 20, myseq 18
PVC IE 0x7, length 0x6, dlci 101, status 0x2, bw 0
Serial0(out): StEnq, myseq 20, yourseen 18, DTE up
datagramstart = 0x400053C datagramsize = 13
FR encap = 0xFCF10309
00 75 01 01 00 03 02 19 17
```

Given the above output, which statement is true?

- A. DLCI 101 is currently added/inactive.
- B. DLCI 101 is currently added/active.
- C. DLCI 101 is currently deleted.
- D. DLCI 101 is not yet established.

Answer: B

Explanation:

The possible values of the status field are explained below:

0x0-Added/inactive means that the switch has this DLCI programmed but for some reason (such as the other end of this PVC is down), it is not usable.

0x2-Added/active means the Frame Relay switch has the DLCI and everything is operational. You can start sending it traffic with this DLCI in the header.

0x3-0x3 is a combination of an active status (0x2) and the RNR (or r-bit) that is set (0x1). This means that the switch - or a particular queue on the switch - for this PVC is backed up, and you stop transmitting in case frames are spilled.

0x4

-Deleted means that the Frame Relay switch doesn't have this DLCI programmed for the router. But it was programmed at some point in the past. This could also be caused by the DLCIs being reversed on the router, or by the PVC being deleted by the telco in the Frame Relay cloud. Configuring a DLCI (that the switch doesn't have) will show up as a 0x4.

In this example, the status field of DLCI 101 is 0x2, so it is added/active.

QUESTION 408:

Which command displays the remote network address associated with each PVC?

- A. show ip route
- B. show frame-relay lmi
- C. show frame-relay map
- D. show frame-relay pvc
- E. show frame-relay status

Answer: C

Explanation:

To display the current map entries and information about the connections, use the show frame-relay map EXEC command.

The following is sample output from the show frame-relay map command:

```
CK1 # show frame-relay map
Serial 1 (administratively down): ip 10.108.177.177
dlci 177 (0xB1,0x2C10), static,
broadcast,
CISCO
TCP/IP Header Compression (inherited), passive (inherited)
```

Table of "show frame-relay map" Field Descriptions	
Field	Description
Serial 1 (administratively down)	Identifies a Frame Relay interface and its status (up or down).
ip 131.108.177.177	Destination IP address (Remote Network Address)
dlci 177 (0xB1,0x2C10)	DLCI that identifies the logical connection being used to reach this interface. This value is displayed in three ways: its decimal value (177), its hexadecimal value (0xB1), and its value as it would appear on the wire (0x2C10).
static	Indicates whether this is a static or dynamic entry.
CISCO	Indicates the encapsulation type for this map; either CISCO or IETF.

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a00800c

QUESTION 409:

The following output was seen on a Certkiller DSL router:

```
Certkiller3# show dsl interface atm 0

Modem Status:      ATU-R (DS)          ATU-C(US)
DSL Mode:          Showtime (DMTDSL_SHOWTIME)
ITU STD NUM:       ITU G.992.1 (G.DMT)
Vendor ID:         0x01          0x1
Vendor Specific:   'ALCB'          'GSPN'
Vendor Country:    0x0000          0x0002
Capacity Used:     97%          100%
Noise Margin:      5.0 dB          5.0 dB
Output Power:      9.5 dBm          12.0 dBm
<output omitted>

Speed (kbps):      Interleave      Fast  Interleave  Fast
                   7616          0    896          0
<output omitted>
```

You work as a network engineer at Certkiller .com. You are troubleshooting a DSL connectivity issue. You have issued the show dsl interface command and received

the above output. Given this information, what could be the problem?

- A. An incorrect power supply is being used.
- B. The service provider is not providing DSL service to this wall jack.
- C. Incorrect VPI/VCI values are configured on the router.
- D. The service provider is using a DSLAM that does not support the Alcatel DSL chipset.

Answer: C

Explanation:

If you experience trouble with the ADSL connection, make sure to verify the following:
That the ADSL line is connected and is using pins 3 and 4. For more information on the ADSL connection, see the hardware guide for your router.

That the ADSL CD LED is on. If it is not on, the router may not be connected to the digital subscriber line access multiplexer (DSLAM). For more information on the ADSL LEDs, see the hardware installation guide specific to your router.

That you are using the correct Asynchronous Transfer Mode (ATM) variable path identifier/variable circuit identifier (VPI/VCI).

That the DSLAM supports discrete multi-tone (DMT) Issue 2.

Incorrect Answers:

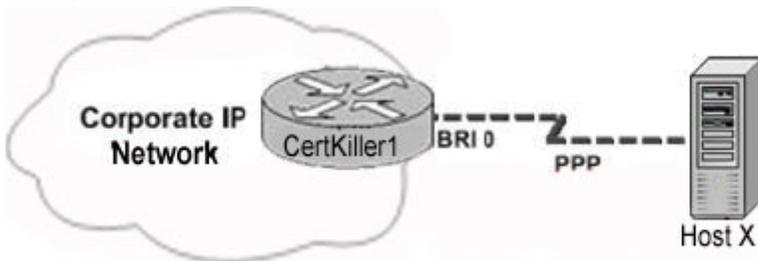
A: The power outputs shown are normal

B: This is incorrect, due to the operational status of the modem as displayed by the "showtime" keyword.

D: In this example, the Alcatel chipset is configured, with the Globespan chipset configured as the secondary chipset. If this was not supported, the modem status would not read "showtime."

QUESTION 410:

Exhibit:



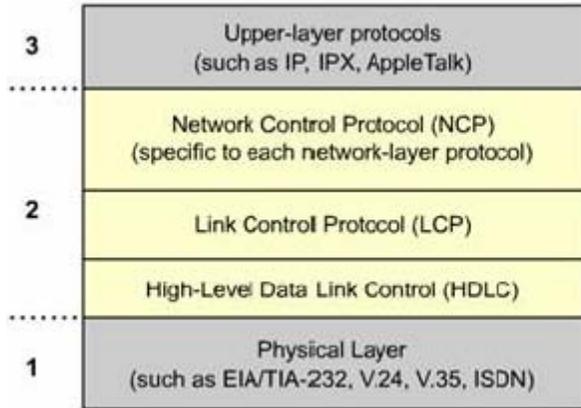
Refer to the exhibit. Host X is unable to access the network using PPP. Debug output on Certkiller 1 shows errors during NCP negotiation. If NCP negotiation fails, which IPCP options could be affected on Host X? (Choose three.)

- A. IP address
- B. multilink
- C. TCP header compression
- D. WINS and DNS server address

- E. bandwidth on demand
- F. callback

Answer: A, C, D

Explanation:



Once the LCP establishes the Layer 2 connection, the Network Control Protocol (NCP) takes over. Link partners exchange NCP packets to establish and configure different network-layer protocols including IP, IPX, and AppleTalk. Each Layer 3 protocol has its own NCP. For example, IP's NCP is IPCP. IPX's NCP is IPXCP and Appletalk's NCP is ATALKCP.

The NCP can build up and tear down multiple Layer 3 protocol sessions over a single data link. This capability is called protocol multiplexing. When a host requests that the connection be terminated, the NCP tears down the Layer 3 sessions and then the LCP tears down the data link. When Error occurred in NCP, TCP negotiation will fail so unable to IP Address, TCP header compression and unable to negotiate with WINS or DNS server.

QUESTION 411:

Exhibit:

```

Mar 13 10:57:15.415: As1 LCP: O CONFREQ [ACKrcvd] id 2 len 25
Mar 13 10:57:15.415: As1 LCP: ACCM 0x000A0000 (0x0206000A0000)
Mar 13 10:57:15.415: As1 LCP: AuthProto CHAP (0x0305C22305)
Mar 13 10:57:15.415: As1 LCP: MagicNumber 0x1084F0A2 (0x05061084F0A2)
Mar 13 10:57:15.415: As1 LCP: PFC (0x0702)
Mar 13 10:57:15.415: As1 LCP: ACFC (0x0802)
Mar 13 10:57:15.543: As1 LCP: I CONFACK [REQsent] id 2 len 25
Mar 13 10:57:15.543: As1 LCP: ACCM 0x000A0000 (0x0206000A0000)
Mar 13 10:57:15.543: As1 LCP: AuthProto CHAP (0x0305C22305)
Mar 13 10:57:15.543: As1 LCP: MagicNumber 0x1084F0A2 (0x05061084F0A2)
Mar 13 10:57:15.543: As1 LCP: PFC (0x0702)
Mar 13 10:57:15.547: As1 LCP: ACFC (0x0802)
Mar 13 10:57:16.919: As1 LCP: I CONFREQ [ACKrcvd] id 4 len 23
Mar 13 10:57:16.919: As1 LCP: ACCM 0x000A0000 (0x0206000A0000)
Mar 13 10:57:16.919: As1 LCP: MagicNumber 0x001327B0 (0x0506001327B0)
Mar 13 10:57:16.919: As1 LCP: PFC (0x0702)
Mar 13 10:57:16.919: As1 LCP: ACFC (0x0802)
Mar 13 10:57:16.919: As1 LCP: Callback 6 (0x0D0306)
Mar 13 10:57:16.919: As1 LCP: O CONFREQ [ACKrcvd] id 4 len 7
Mar 13 10:57:16.919: As1 LCP: Callback 6 (0x0D0306)
Mar 13 10:57:17.047: As1 LCP: I CONFREQ [ACKrcvd] id 5 len 20
Mar 13 10:57:17.047: As1 LCP: ACCM 0x000A0000 (0x0206000A0000)
Mar 13 10:57:17.047: As1 LCP: MagicNumber 0x001327B0 (0x0506001327B0)
Mar 13 10:57:17.047: As1 LCP: PFC (0x0702)
Mar 13 10:57:17.047: As1 LCP: ACFC (0x0802)
Mar 13 10:57:17.047: As1 LCP: O CONFACK [ACKrcvd] id 5 len 20
Mar 13 10:57:17.047: As1 LCP: ACCM 0x000A0000 (0x0206000A0000)
Mar 13 10:57:17.047: As1 LCP: MagicNumber 0x001327B0 (0x0506001327B0)
Mar 13 10:57:17.047: As1 LCP: PFC (0x0702)
Mar 13 10:57:17.047: As1 LCP: ACFC (0x0802)
Mar 13 10:57:17.047: As1 LCP: State is Open

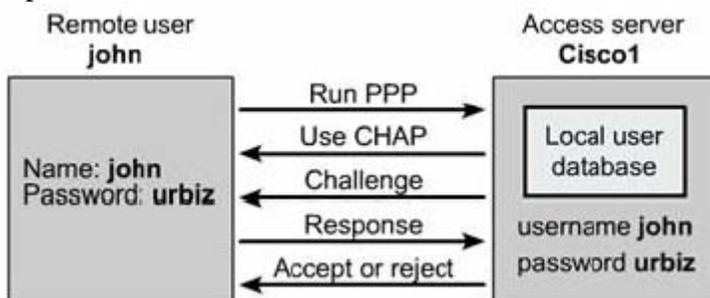
```

Which statement is true about the exhibited output from a debug ppp negotiation command?

- A. The negotiation was unsuccessful.
- B. This router received the initial request to establish a connection.
- C. Router As1 requested callback.
- D. CHAP was rejected by the neighboring router as the authentication protocol.

Answer: C

Explanation:



When using CHAP authentication, the access server sends a challenge message to the remote node after the PPP link is established, Figure. The remote node responds with a value calculated by using a one-way hash function, typically Message Digest 5 (MD5). The access server checks the response against its own calculation of the expected hash value. If the values match, the authentication is acknowledged. Otherwise, the connection is immediately terminated. Thus, the actual username and password themselves are not actually sent over the media.

When we observe the output of debug ppp negotiation, we will get different types of packets. CONFREQ → To Open a connection to the peer, the device transmits this message along

with the configuration options and values the sender wishes the peer to support. All options and values are negotiated simultaneously. If the peer responds with a CONFREJ or CONFNACK message, then the router sends another CONFREQ with another set of options or values.

CONFREJ → If some configuration option received in the CONFREQ message is not acceptable or not recognizable, the router responds with CONFREJ message.

CONFNACK → If the received configuration option is recognizable and acceptable, but some value is not acceptable, the router transmits a CONFNACK message. The router appends the option and value that it can accept in the CONFNACK message so that the peer can include that option in the next CONFREQ message.

CONFACK → If all options in the CONFREQ message are recognizable and all values are acceptable, then the router transmits a CONFACK message.

TERMREQ → This message is used to initiate an LCP close.

TERMACK → This message is transmitted in response to the TERMREQ message.

In Exhibit, CONFREJ packets are showing, that means peer rejecting the request of the router.

Sample debug ppp negotiation Output

This is an annotated description of debug ppp negotiation command output:

```
maui-soho-01#debug ppp negotiation PPP protocol negotiation debugging is
onmaui-soho-01#*Mar 1 00:06:36.645: %LINK-3-UPDOWN: Interface BRI0:1, changed
state to up!-- The Physical Layer (BRI Interface) is up. Only now can PPP!--
negotiation begin.*Mar 1 00:06:36.661: BR0:1 PPP: Treating connection as a callin*Mar
1 00:06:36.665: BR0:1 PPP: Phase is ESTABLISHING, Passive Open[0 sess, 0 load]!--
The PPP Phase is ESTABLISHING. LCP negotiation now occurs.*Mar 1 00:06:36.669:
BR0:1 LCP: State is Listen*Mar 1 00:06:37.034: BR0:1 LCP: I CONFREQ [Listen] id 7
len 17!-- This is the incoming CONFREQ. The ID field is 7.*Mar 1 00:06:37.038:
BR0:1 LCP: AuthProto PAP (0x0304C023)*Mar 1 00:06:37.042: BR0:1 LCP:
MagicNumber 0x507A214D (0x0506507A214D)*Mar 1 00:06:37.046: BR0:1 LCP:
Callback 0 (0x0D0300)!-- The peer has requested!-- Option: Authentication Protocol,
Value: PAP!-- Option: MagicNumber (This is used to detect loopbacks and is always
sent.)!-- Option: Callback, Value: 0 (This is for PPP Callback; MS Callback uses
6.)*Mar 1 00:06:37.054: BR0:1 LCP: O CONFREQ [Listen] id 4 len 15!-- This is an
outgoing CONFREQ, with parameters for the peer to implement!-- Note that the ID
Field is 4, so this is not related to the previous!-- CONFREQ message.*Mar 1
00:06:37.058: BR0:1 LCP: AuthProto CHAP (0x0305C22305)*Mar 1 00:06:37.062:
BR0:1 LCP: MagicNumber 0x1081E7E1 (0x05061081E7E1)!-- This router requests!--
Option: Authentication Protocol, Value: CHAP!-- Option: MagicNumber (This is used
to detect loopbacks and is always sent.)*Mar 1 00:06:37.066: BR0:1 LCP: O CONFREJ
[Listen] id 7 len 7!-- This is an outgoing CONFREJ for message with Field ID 7!--
This is the response to the CONFREQ received first.*Mar 1 00:06:37.070: BR0:1 LCP:
Callback 0 (0x0D0300)!-- The option that this router rejects is Callback!-- If the router
wanted to do MS Callback rather than PPP Callback, it!-- would have sent a CONFNACK
message instead.*Mar 1 00:06:37.098: BR0:1 LCP: I CONFACK [REQsent] id 4 len
15!-- This is an incoming CONFACK for a message with Field ID 4.*Mar 1
00:06:37.102: BR0:1 LCP: AuthProto CHAP (0x0305C22305)*Mar 1 00:06:37.106:
BR0:1 LCP: MagicNumber 0x1081E7E1 (0x05061081E7E1)!-- The peer can support all
```

requested parameters.*Mar 1 00:06:37.114: BR0:1 LCP: I CONFREQ [ACKrcvd] id 8 len 14!--- This is an incoming CONFREQ message; the ID field is 8.!--- This is a new CONFREQ message from the peer in response to the CONFREQ id:7.*Mar 1 00:06:37.117: BR0:1 LCP: AuthProto PAP (0x0304C023)*Mar 1 00:06:37.121: BR0:1 LCP: MagicNumber 0x507A214D (0x0506507A214D)!--- The peer has requested!--- Option: Authentication Protocol, Value: PAP!--- Option: MagicNumber (This is used to detect loopbacks and is always sent.)*Mar 1 00:06:37.125: BR0:1 LCP: O CONFNAK [ACKrcvd] id 8 len 9!--- This is an outgoing CONFNAK for a message with Field ID 8.*Mar 1 00:06:37.129: BR0:1 LCP: AuthProto CHAP (0x0305C22305)!--- This router recognizes the option Authentication Protocol,!--- but does not accept the value PAP. In the CONFNAK message,!--- it suggests CHAP instead.*Mar 1 00:06:37.165: BR0:1 LCP: I CONFREQ [ACKrcvd] id 9 len 15!--- This is an incoming CONFREQ message with Field ID 9.*Mar 1 00:06:37.169: BR0:1 LCP: AuthProto CHAP (0x0305C22305)*Mar 1 00:06:37.173: BR0:1 LCP: MagicNumber 0x507A214D (0x0506507A214D)!--- CHAP authentication is requested.*Mar 1 00:06:37.177: BR0:1 LCP: O CONFACK [ACKrcvd] id 9 len 15!--- This is an outgoing CONFACK for a message with Field ID 9.*Mar 1 00:06:37.181: BR0:1 LCP: AuthProto CHAP (0x0305C22305)*Mar 1 00:06:37.185: BR0:1 LCP: MagicNumber 0x507A214D (0x0506507A214D)*Mar 1 00:06:37.189: BR0:1 LCP: State is Open!--- This indicates the LCP is Open.*Mar 1 00:06:37.193: BR0:1 PPP Ph i

QUESTION 412:

Exhibit:

```
ipsec1# show crypto ipsec sa
interface: FastEthernet0
  Crypto map tag: aesmap, local addr. 10.48.66.147

protected vrf:
local ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0)
current_peer: 10.48.66.146:500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 30, #pkts encrypt: 30, #pkts digest 30
#pkts decaps: 30, #pkts decrypt: 30, #pkts verify 30
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors: 0, #recv errors: 0

local crypto endpt:10.48.66.147. remove crypt endpt:10.48.66.146
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
current outbound spi: 2EB0BA1A

inbound esp sas:
spi: 0xFECA28BC(4274661564)
  transform: esp-256-aes esp-sha-hmac ,
  in use settings ={Tunnel,}
  slot: 0, conn id: 2000, flow_id: 1, crypto map: aesmap
  sa timing: remaining key lifetime (k/sec): (4554237/2895)
  IV size: 16 bytes
  replay detection support: Y

inbound ah sas:

outbound pcp sas:
ipsec1#
```

Refer to the exhibit. A network engineer is troubleshooting a traffic flow problem. Specifically, the LAN of router ipsec1 is not reaching hosts on the LAN of router ipsec2. Given the output in the exhibit, what is the problem?

- A. The IPsec SA is not fully established.
- B. The remote router did not accept any proposed transform sets.
- C. The local router did not accept any proposed transform sets.
- D. The crypto access lists are incorrect.

Answer: D

Explanation:

The crypto ACLs identify the traffic flows that will be protected. Extended IP ACLs select IP traffic to encrypt by protocol, IP address, network, subnet, and port. Although the ACL syntax is unchanged from extended IP ACLs, the meanings are slightly different for crypto ACLs. When using crypto ACLs, permit specifies that matching packets must be encrypted and deny specifies that matching packets do not need to be encrypted. Crypto ACLs behave similar to an extended IP ACL applied to the outbound traffic on an interface.

See the command reference for a complete description of this command. The command syntax for the basic form of extended IP access lists is as follows:

```
access-list access-list-number { permit | deny } protocol source  
source-wildcard destination destination-wildcard[precedence precedence]  
[tos tos] [log]
```

Any unprotected inbound traffic that matches a permit entry in the crypto ACL for a crypto map entry flagged as IPsec will be dropped, because this traffic was expected to be protected by IPsec.

If certain traffic only requires authentication for IPsec protection, and other traffic should receive both authentication and encryption, create two different crypto ACLs to define the two different types of traffic. These different ACLs are then used in different crypto map entries that specify different IPsec policies.

Warning: Cisco recommends avoiding the use of the any keyword to specify source or destination addresses. The permit any statement is strongly discouraged, as this will cause all outbound traffic to be protected and send all protected traffic to the peer specified in the corresponding crypto map entry. This statement will also cause all inbound traffic to require protection. Then, all inbound packets that lack IPsec protection will be silently dropped, including packets for routing protocols, NTP, echo, and echo response.

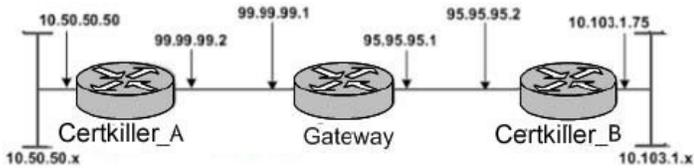
Try to be as restrictive as possible when defining which packets to protect in a crypto ACL. If the any keyword must be used in a permit statement, the statement must be prefaced with a series of deny statements to filter out any traffic that should not be protected.

In a later step, a crypto ACL will be associated a crypto map, which is then assigned to a specific interface.

In Output ACL is misconfigured.

QUESTION 413:

Exhibit:



Certkiller_B# show run

```
<output omitted>
crypto isakmp policy 1
  crypto isakmp key cisco123 address 99.99.99.2
  |
crypto ipsec transform-set rtpset esp-des esp-md5-hmac
  |
crypto map rtp 1 ipsec-isakmp
  set peer 99.99.99.2
  set transform-set rtpset
  match address 115
  |
Interface FastEthernet0/0
  ip address 95.95.95.2 255.255.255.0
  crypto map rtp
<output omitted>
|
access-list 115 permit ip 10.50.50.0 0.0.0.255 10.103.1.0 0.0.0.255
<output omitted>
```

Refer to the exhibit. The administrator wants the router to be used for IPsec with preshared authentication. Which configuration command is needed to complete the setup?

- A. authentication pre-shared
- B. crypto isakmp enable
- C. crypto isakmp identity address
- D. crypto ipsec security-association lifetime

Answer: A

Explanation: Here is the sample Configuration for authentication

```
RouterA(config)#crypto isakmp policy 110
RouterA(config-isakmp)#authentication pre-share
RouterA(config-isakmp)#encryption des
RouterA(config-isakmp)#group1
RouterA(config-isakmp)#hash md5
RouterA(config-isakmp)#lifetime 86400
```

QUESTION 414:

Exhibit:

```
Router# show dialer
BRI0/0 - dialer type - ISDN
Dial String    Successes    Failures    Last DNIS    Last Status
5551235        0           0           never        -
5551234        21          0           00:00:31    successful
0 incoming call (s) have been screened
0 incoming call (s) rejected for callback.

BRI0/1 - dialer type - ISDN
Idle timer (60 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is multilink member
Dial reason: Multilink bundle overload
Connected to 5551234 (SanJose1)

BRI0/2 - dialer type - ISDN
Idle timer (60 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is multilink member
Dial reason: ip (s=192.168.1.2, d=192.168.0.1)
Connected to 5551234 (SanJose1)
```

Given the above output, which statement is true?

- A. BRI/0:1 is the first link in this MP bundle.
- B. BRI/0:1 triggered a call due to interesting traffic.
- C. BRI/0:1 is currently utilizing dial string 5551235 to connect to SanJose1.
- D. BRI/0:2 dialed a connection to 192.168.1.2.
- E. BRI/0:2 exceeded the dialer load-threshold set for that interface.

Answer: E

Explanation:

dialer load-threshold

To configure bandwidth on demand by setting the maximum load before the dialer places another call to a destination, use the dialer load-threshold command in interface configuration mode. To disable the setting, use the no form of this command.

dialer load-threshold load [outbound | inbound | either]

no dialer load-threshold

Syntax Description

<i>load</i>	Interface load used to determine whether to initiate another call or to drop a link to the destination. This argument represents a utilization percentage; it is a number between 1 and 255, where 255 is 100 percent.
<i>Outbound</i>	(Optional) Calculates the actual load using outbound data only.
<i>inbound</i>	(Optional) Calculates the actual load using inbound data only.
<i>either</i>	(Optional) Sets the maximum calculated load as the larger of the outbound and inbound loads.

Defaults

No maximum load is predefined.

When the cumulative load of all UP links (a number n) exceeds the load threshold the dialer adds an extra link and when the cumulative load of all UP links minus one (n - 1) is at or below load threshold then the dialer can bring down that one link.

The dialer will make additional calls or drop links as necessary but will never

interrupt an existing call to another destination.

The load argument is the calculated weighted average load value for the interface; 1 is unloaded and 255 is fully loaded. The load is calculated by the system dynamically, based on bandwidth. You can set the bandwidth for an interface in kilobits per second, using the bandwidth command.

The load calculation determines how much of the total bandwidth you are using. A load value of 255 means that you are using one hundred percent of the bandwidth. The load number is required.

See the description of the bandwidth command earlier in this guide for more information.

When multilink PPP is configured, the dialer load-threshold 1 command no longer keeps a multilink bundle of n links connected indefinitely and the dialer-load threshold 2 command no longer keeps a multilink bundle of 2 links connected indefinitely. If you want a multilink bundle to be connected indefinitely, you must set a high idle timer or make all traffic interesting.

When two connected routers are configured to dial out, only one router should have the dialer max-call or dialer pool-member max-links command configured.

Otherwise, if both routers dial simultaneously, each will reject the incoming call when it exceeds the setting for the max-links argument. If the maximum number of calls configured is one and dialing out is synchronized, no connection will come up or it will take many retries before the connection stays up. To prevent this problem, one of the following configurations is recommended:

Use the dialer max-call command to restrict the number of connections, rather than the dialer pool-member max-links command. The result is the same and the dialer max-call command is easier to understand and configure.

When two systems will dial each other and a maximum of one link is desired, configure the dialer max-calls command on only one side of the connection, not on both sides.

Configure the dialer load-threshold command on only one side of the connection, either the local or remote router, and configure the dialer max-call command on the interface where the dialer load-threshold command is configured.

Examples

In the following example, if the load to a particular destination on an interface in dialer rotary group5 exceeds interface load 200, the dialer will initiate another call to the destination:

```
interface dialer 5dialer load-threshold 200
```

In Exhibit, you can see that dialed reason to multiple destination.

QUESTION 415:

Exhibit:

```
Router(config-if)# ip tcp header-compression passive
```

Given the configuration command shown in the exhibit, which statement is true?

A. All incoming TCP packets will be compressed.

- B. All outgoing TCP packets will be compressed.
- C. Incoming TCP packets will be compressed only if outgoing TCP packets on the same interface is compressed.
- D. Outgoing TCP packets will be compressed only if incoming TCP packets on the same interface is compressed.
- E. All incoming and outgoing TCP packets will be compressed.

Answer: D

Explanation:

Configure TCP header compression using the command:

```
ip tcp header-compression
```

Optionally, the `ip tcp header-compression passive` command specifies that TCP header compression is not required, but will be used if the router receives compressed headers from its link partner.

QUESTION 416:

Which three items are correct about the IPSec ESP security protocol? (Chose three.)

- A. Authentication is mandatory and the whole packet including the header is authenticated.
- B. Authentication is optional and the outer header is not authenticated.
- C. IP packet is expanded by transport mode: 37 bytes(3DES) or 63 bytes(AES); tunnel mode 57 bytes(3DES) or 83 bytes(AES)
- D. IP packet is expanded by: transport mode 24 bytes; tunnel mode 44 bytes
- E. The ESP security protocol provides data confidentiality.
- F. The ESP security protocol provides no data confidentiality.

Answer: B, C, E

Explanation:

Encapsulating Security Payload

The ESP header is inserted after the IP header, and before the upper layer protocol header in transport mode or before an encapsulated IP header in tunnel mode.

ESP is used to provide the following services:

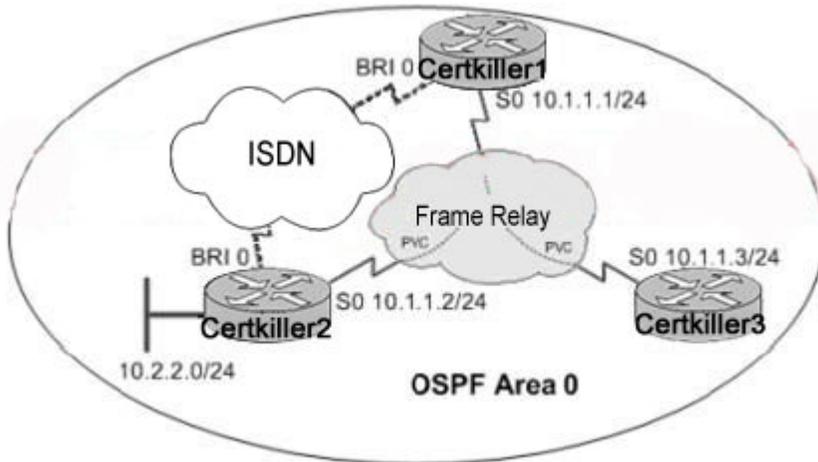
1. Confidentiality
2. Data origin authentication
3. Connectionless integrity
4. Anti-replay service, a form of partial sequence integrity
5. Limited traffic flow confidentiality, by defeating traffic flow analysis

The set of services provided depends on options selected at the time of security association establishment and on the placement of the implementation. Confidentiality may be selected independently of all other services. However, use of confidentiality without integrity/authentication, either in ESP or separately in AH, may make certain traffic

vulnerable to certain forms of active attacks that could undermine the confidentiality service.

QUESTION 417:

Exhibit:



Refer to the diagram. A network administrator has configured a floating static route to 10.2.2.0/24 so that Certkiller 1 will use its ISDN link to Certkiller 2 in the event the primary link fails. During testing, the administrator notices that when the Certkiller 2 serial connection goes down, Certkiller 1 does not install the floating static route and use the backup link as planned.

Which approach will ensure that Certkiller 1 uses the ISDN link to 10.2.2.0/24 when the Certkiller 2 serial connection fails?

- Configure a static host route for the Certkiller 2 BRI, using an administrative distance of 2.
- Configure dial backup on Certkiller 2 using the interface backup command.
- Configure Dialer Watch on Certkiller 1 using watch-list statements for Certkiller 2 networks.
- Configure the Certkiller 1 Frame Relay map for Certkiller 2 with the keyword broadcast.
- Configure the Certkiller 1 BRI with the no peer neighbor-route command.

Answer: C

Explanation: dialer watch-list <group-number> delay route-check initial <seconds>
This command enables the router to check whether the primary route is up after the initial startup of the router is complete and the timer expires. Without this command, dialer watch is only triggered when the primary route is removed from the routing table. If the primary link fails to come up during initial startup of the router, the route is never added to the routing table and hence cannot be watched. Therefore, with this command, dialer watch dials the backup link in the event of a primary link failure during the initial startup of the router.

QUESTION 418:

Which IPSEC protocol negotiates security associations?

- A. AH
- B. ESP
- C. IKE
- D. SSH

Answer: C

Explanation:

Internet Key Exchange (IKE) enhances IPsec by providing additional features, flexibility, and ease of configuration for the IPsec standard. IKE is a hybrid protocol that implements the Oakley key exchange and Skeme key exchange inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. ISAKMP, Oakley, and Skeme are security protocols implemented by IKE. IKE provides authentication of the IPsec peers, negotiates IPsec keys, and negotiates IPsec security associations.

The IKE tunnel protects the SA negotiations. After the SAs are in place, IPsec protects the data that A and B exchange.

IKE Mode configuration allows a gateway to download an IP address (and other network-level configuration) to the client as part of an IKE negotiation. Using this exchange, the gateway gives IP addresses to the IKE client to be used as an "inner" IP address encapsulated under IPsec. This provides a known IP address for the client, which can be matched against IPsec policy.

This feature implements IKE Mode Configuration into existing Cisco IOS IPsec software images. Using IKE Mode Configuration, a Cisco access server can be configured to download an IP address to a client as part of an IKE transaction. IKE automatically negotiates IPsec SAs and enables IPsec secure communications without costly manual preconfiguration.

IKE provides these benefits:

1. Eliminates the need to manually specify all the IPsec security parameters in the crypto maps at both peers.
2. Allows the user to specify a lifetime for the IPsec security association.
3. Allows encryption keys to change during IPsec sessions.
4. Allows IPsec to provide anti-replay services.
5. Permits certification authority (CA) support for a manageable, scalable IPsec implementation.
6. Allows dynamic authentication of peers.

QUESTION 419:

Which set of commands will accomplish the tasks below?

- Make bri0/0 a backup interface to serial0/0
- Activate the backup interface 5 seconds after the primary link fails and deactivates the backup interface 10 seconds after the primary link is re-established.

- A. Router(config)#interface bri 0/0
Router(config-if)#backup interface serial 0/0
Router(config-if)#backup delay 5 10
- B. Router(config)#interface serial 0/0
Router(config-if)#backup interface bri 0/0
Router(config-if)#backup delay 5 10
- C. Router(config)#interface bri 0/0
Router(config-if)#backup interface serial 0/0
Router(config-if)#backup delay 10 5
- D. Router(config)#interface serial 0/0
Router(config-if)#backup interface bri 0/0
Router(config-if)#backup delay 10 5

Answer: B

Explanation:

The backup interface bri 0/0 command assigns BRI0/0 as the backup interface. The backup delay 5 10 command configures the backup link to activate if the primary interface is down for 5 seconds. The secondary line will deactivate 10 seconds after the primary line is re-enabled. The primary interface must also be configured for the desired protocol, DDR, Frame Relay, and encapsulation type.

QUESTION 420:

Which three statements about ISDN dialer profiles are true? (Choose three.)

- A. A dialer profile consists of a physical interface, a map class, a dialer pool, and an optional dialer interface.
- B. An advantage of dialer profiles is to set different DDR parameters for each call on an ISDN interface.
- C. An ISDN BRI interface can only belong to a single dialer pool at a time.
- D. Dialer profiles allow a backup interface to be nondedicated and usable when the primary interface is operational.
- E. Dialer profiles allow physical interface to take on different characteristics that are based on incoming or outgoing call requirements.
- F. Dialer profiles do not support PPP Password Authentication Protocol (PAP)

Answer: B, D, E

Explanation:

DDR with dialer profiles is a newer, more scalable alternative to configuring DDR. Dialer profiles separate the logical configurations from the interface that receives or makes calls. Examples of logical configurations are the network layer, encapsulation, and dialer parameters. Dialer profiles can define encapsulation and access control lists (ACLs), as well as turn features on or off. With dialer profiles, the logical and physical configurations are dynamically bound to each other on

a per-call basis. This allows physical interfaces to dynamically assume different characteristics based on incoming or outgoing calls.

Dialer profiles allow the creation of different configuration parameters for ISDN B-channels on PRI and BRI interfaces. Unlike the restrictions found with a dialer rotary group, a physical interface can be used by multiple dialer interfaces.

A dialer interface is basically a dialer profile that can be bound to any member of the dialer pool. A dialer profile can be configured for each remote user or router establishing a call. When the access server needs to place a call, it looks for the appropriate dialer profile. Once it identifies the correct profile, the access server attempts to find an available physical interface that belongs to the appropriate dialer pool. If a physical interface is available, the access server temporarily binds the dialer profile to that interface and makes the call.

QUESTION 421:

Exhibit:

```
Router(config)# interface serial 1/1
Router(config-if)# backup interface bri0/0
Router(config-if)# backup load 80 10
```

Based on the above configuration, which statement is true?

- A. The backup interface will be used when traffic reaches 80 kbps on the primary interface.
- B. The backup interface will be disabled when the combined load on the primary and backup interface is less than 10%.
- C. The backup interface will be disabled when the combined load on the primary and backup interface is less than 80 kbps.
- D. The backup interface will be disabled when the load on the primary interface is less than 10%.
- E. The backup interface will be disabled when the load on the primary interface is less than 80 kbps.

Answer: B

Explanation:

A backup interface can be configured to activate the secondary link based on the traffic load on the primary link. The IOS monitors the traffic load and computes the percentage of utilization on the link. This calculation is based on a five-minute average, and it is computed every 5 seconds

To configure a backup for when the primary line reaches or exceeds a certain threshold, perform the following steps on one side of the connection only:

1. Select the primary interface:

```
Router(config)#interface interface-type slot/port
```

2. Use the following command on the primary interface to specify the backup to be used if a dial backup is needed:

```
Router(config-if)#backup interface interface-type slot/port
```

or

Router(config-if)#backup interface dialer number

3. To set the traffic load threshold for dial backup service, use the following command syntax:

```
Router(config-if)#backup load {enable-threshold | never} {disable-load | never}
```

The secondary line is brought down when one of the following conditions occur:

1. The transmitted load on the primary line plus the transmitted load on the secondary line is less than the value entered for the disable-load argument.

2. The received load on the primary line plus the received load on the secondary line is less than the value entered for the disable-load argument.

QUESTION 422:

Exhibit:

```
policy-map MYPOLICY
class class-default
bandwidth 256
```

Refer to the partial configuration shown. For CBWFQ, what will the queuing strategy be for the class-default in the policy map, MYPOLICY?

- A. FIFO
- B. WFQ
- C. Best-effort treatment
- D. Priority
- E. custom

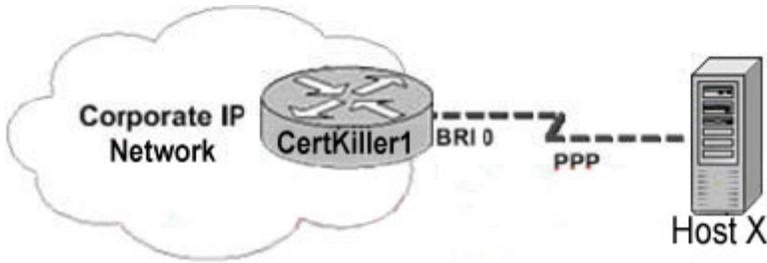
Answer: A

Explanation:

Class-based weighted fair queuing (CBWFQ) extends the standard WFQ functionality to provide support for user-defined traffic classes. By using CBWFQ, network managers can define traffic classes based on several match criteria, including protocols, access control lists (ACLs), and input interfaces. A FIFO queue is reserved for each class, and traffic belonging to a class is directed to the queue for that class. More than one IP flow, or "conversation", can belong to a class.

QUESTION 423:

Exhibit:



Refer to the diagram. Host X is unable to establish an ISDN connection with Certkiller 1 using PPP. Which commands can be used on Certkiller 1 to troubleshoot the LCP and NCP negotiation between these two hosts? (Choose two.)

- A. debug ppp negotiation
- B. debug ppp authentication
- C. debug dialer
- D. debug isdn q931
- E. debug isdn q921

Answer: A, B

Explanation:

The debug ppp negotiation command is an excellent tool for troubleshooting the PPP LCP activities such as authentication, compression, and MLP. When the LCP is in OPEN state, the NCP negotiation takes place. LCP options must be negotiated before any NCP activities take place for PPP to work. The debug ppp negotiation command allows the following negotiation to be observed:

1. CHAP authentication
2. Compression Control Protocol (CCP)
3. NCP protocols IPCP, IPXCP, ATCP, and so on.

When specifically debugging CHAP or PAP authentication, the debug ppp authentication command can be used in place of debug ppp negotiation. The debug ppp authentication command gives you the same output as debug ppp negotiation, but that output is limited to CHAP and PAP authentication events.

QUESTION 424:

Exhibit:

```
Certkiller8# sh dsl int atm 0
Line not activated: displaying cached data from last activation
Log file of training sequence:
<output omitted>
```

While troubleshooting a DSL connectivity issue, the administrator issued the show dsl interface command and received the output shown in the exhibit. Additionally, issuing the show interface command showed that the ATM interface was down and the line protocol was down. Given this information, what could be the problem?

- A. An incorrect power supply is being utilized.
- B. Incorrect VPN/VCI values are configured on the router.
- C. PPP negotiation with the remote router failed.
- D. DHCP service failed to assign a valid IP.

Answer: A

Explanation: When dsl interface atm0 working it shows following outout:

```
ADSL-router#show dsl int atm 0 ATU-R (DS) ATU-C (US)Modem Status:
Showtime (DMTDSL_SHOWTIME)DSL Mode: ITU G.992.1 (G.DMT)ITU STD
NUM: 0x01 0x01Vendor ID: 'ALCB' 'ANDV'Vendor Specific: 0x0000
0x0000Vendor Country: 0x00 0x00Capacity Used: 7% 32%Noise Margin: 30.0 dB
23.0 dBOutput Power: 18.0 dBm 12.0 dBmAttenuation: 1.0 dB 7.0 dBDefect Status:
None NoneLast Fail Code: NoneSelftest Result: 0x49Subfunction: 0x02Interrupts:
50011 (1 spurious)Activations: 50Init FW: embeddedOperartion FW: embeddedSW
Version: 3.8129FW Version: 0x1A04 Interleave Fast Interleave FastSpeed (kbps):
576 0 128 0Reed-Solomon EC: 0 0 0 0CRC Errors: 0 0 0 0Header Errors: 0 0 0 0Bit
Errors: 0 0BER Valid sec: 0 0BER Invalid sec: 0 0<skip>So possible cause of output
is due to incorrect power supply.
```

QUESTION 425:

Exhibit:

```
hostname R1
!
username R2 secret 5 $1$cGzE$uZBVvrel3DNveOfLc5CO/
!
interface BRI0/0
 ip address 172.20.1.1 255.255.255.0
 encapsulation ppp
 dialer idle-timeout 60
 dialer fast-idle 60
 dialer map ip 172.20.1.2 name R2 broadcast 5552222
 dialer map ip 172.20.1.2 name R2 broadcast 5552223
 dialer load-threshold 95 either
 dialer-group 6
 isdp switch-type basic-ni
 isdn spid1 51255522220101
 isdn spid2 51255522230101
 ppp authentication chap pap
 ppp pap sent-username R1 password 0 cisco
 ppp multilink
!
 ip route 10.0.0.0 255.0.0.0 172.20.1.2
!
 access-list 2000 permit tcp any any eq telnet
 access-list 2000 permit tcp any any eq smtp
 dialer watch-list 6 ip 10.0.0.0 255.255.255.0
 dialer-list 1 protocol ip permit
 dialer-list 6 protocol ip list 2000
```

Refer to the output shown in the exhibit. Which three statements are true about this configuration? (Choose three.)

- A. R1 will not bring up a second B-channel to R2 until either the inbound or outbound load reaches 95%.
- B. R1 will attempt to authenticate R2 using first CHAP, then PAP.
- C. R1 will treat all IP traffic destined for 10.0.0.0/8 as "interesting".
- D. If R1 pings 172.20.1.2 at least once every 59 seconds, the DDR link will stay up.
- E. As configured, the BRI0/0 of R1 can only be used to connect with R2.
- F. If the ISDN link is not already up, traffic destined for a Telnet server at 10.1.1.1 will cause R1 to dial R2.

Answer: B, E, F

Explanation:

ppp authentication chap pap tries to authenticate using chap first then only use pap to authenticate. Dialer map is mapping to remote R2 router only so R1 can connect to R2. Telnet connection is permitted so, if the ISDN link is not already up, traffic destined for the telnet server will cause R1 to dial R2.

QUESTION 426:

An administrator is attempting to configure TACACS+ AAA authentication for privileged EXEC mode access. The current configuration is as follows:

```
Certkiller B(config)# tacacs-server host 192.168.1.23
```

```
Certkiller B(config)# tacacs-server key CISCO
```

```
Certkiller B(config)# aaa new.model
```

```
Certkiller B(config)# aaa authentication enable AAA group tacacs+ enable none
```

With the above configuration, what will be the result?

- A. Authentication will be successful from the TACACS+ server.
- B. Authentication will be successful from the local enable password.
- C. Because the authentication list is not applied to any lines, authentication will not be successful.
- D. Because the authentication enable command cannot be used with a named list, authentication will not be successful.

Answer: D

Explanation:

The aaa authentication login command enables AAA authentication for logins on terminal lines (TTYs), virtual terminal lines (VTYs), and the console (con 0). This command can be used to create one or more lists that are tried at login.

```
Router(config)#aaa authentication login {default | list-name} method1
```

```
[...[method4]]
```

The default list is applied to all lines. A named list must be applied to a specific line or group of lines using the aaa login authentication command.

The additional methods of authentication are used only if the previous method returns an

ERROR, not a FAIL. A typical ERROR is a failure to connect with a member of a server group due to link failure or a server-side problem.

To ensure that the user is granted access, even if all methods return an ERROR, specify none as the final method in the command line. If all defined methods end with an ERROR and none is not specified as the final method, the user will not be authenticated. If authentication is not specifically set for a line, the default is to deny access and no authentication is performed.

Depending on the security policy of the organization, none may always be configured as the final method. It may also be determined that denying access when all other methods return an ERROR is the most secure course of action.

The `aaa new-model` command enables the AAA feature. Finally, the `aaa authentication login` command defines the method list. The method list configures RTA to attempt to contact the TACACS+ servers first. If neither server is reached, this method returns an ERROR and AAA tries to use the second method, the `enable password`. If this attempt also returns an ERROR, because no `enable password` is configured on the router, the user is allowed access with no authentication.

The default list is applied to the console (con 0), all TTY lines including the auxiliary line or AUX port, and all VTY lines. To override the default method list, apply a named list to one or more of these lines.

The `aaa authentication login PASSPORT group radius local none` command creates a named method list called PASSPORT. The first method in this list is the group of RADIUS servers. If cannot contact a RADIUS server, then will try and contact the local username/password database. Finally, the `none` keyword assures that if no usernames exist in the local database, the user is granted access.

Named method lists for login authentication are applied using the `login authentication` command.

Router(config-line)#`login authentication listname`

The `login authentication` command can be used to apply the PASSPORT method list to all five VTYs.

QUESTION 427:

Exhibit:

```
interface BR10/0
no ip address
dialer rotary-group 1
isdn spid1 55512120001
isdn spid2 55512120002
!
interface Dialer0
ip address 10.1.1.1 255.255.255.0
encapsulation ppp
dialer in-band
dialer idle-timeout 100
dialer fast-idle 15
dialer map ip 10.1.1.2 name R2 broadcast 5551212
dialer map ip 10.1.1.3 name R3 class ISDN-56k broadcast 5551212
dialer-group 1
ppp authentication chap
```

Refer to the exhibit. What is true about the exhibited configuration?

- A. BRI0/0 will receive its dialer configuration from Dialer0.
- B. BRI0/0 is not configured to be a member of the rotary group defined by Dialer0.
- C. BRI0/0 must be configured for PPP before it can join the rotary group.
- D. BRI0/0 cannot join the rotary group until the dialer pool 1 command is entered on Dialer0.
- E. The dialer load-threshold command is required for BRI0/0 to bind with Dialer0.
- F. The dialer in-band command invalidates the ISDN rotary group configuration.

Answer: B

Explanation:

Dialer rotary groups apply a single interface configuration to a set of physical interfaces. Dialer rotary groups are useful in environments that have multiple callers and multiple calling destinations. A dialer rotary group is defined by configuring a dialer interface. The dialer interface is not a physical interface. It is a logical entity that allows propagation of an interface configuration to multiple interfaces. A dialer interface defined by a number, such as interface dialer 0 (zero), allows for parameter configuration of the interface. Any physical interface that is assigned to the dial rotary group inherits the dialer interface configuration parameters. If the dialer interface is configured with multiple dialer maps, any physical interface in the rotary group can be used for the outgoing call

Bri0/0 interface is not configured as a member of rotary group 0.

dialer rotary-group 0 needs to configure inside of bri0/0 configuration mode.

QUESTION 428:

Router CK1 had the following configuration command added to interface Serial 0

```
Router(config-if)# ip tcp header-compression passive
```

Which two statements are true about the command entered in the display? (Choose two)

- A. The router will compress all traffic.
- B. The router will only compress outgoing TCP packets if incoming TCP packets on the same interface are compressed.
- C. The router will accept incoming compressed TCP packets but will not compress any outgoing TCP packets.
- D. The Layer 2 header will be compressed and therefore cannot be used for WAN switching networks such as Frame Relay.
- E. The Layer 2 header will be left intact and therefore can be used for WAN switching networks such as Frame Relay.
- F. For crossing point-to-point connections, the Layer 2 header will be encapsulated by another link layer such as LAPB.

Answer: B, D

Explanation:

Configure TCP header compression using the command:

```
ip tcp header-compression
```

Optionally, the `ip tcp header-compression passive` command specifies that TCP header compression is not required, but will be used if the router receives compressed headers from its link partner. `ip tcp header-compression passive` command Layer 2 header also compressed therefore can't use for WAN switching networks such as Frame Relay.

QUESTION 429:

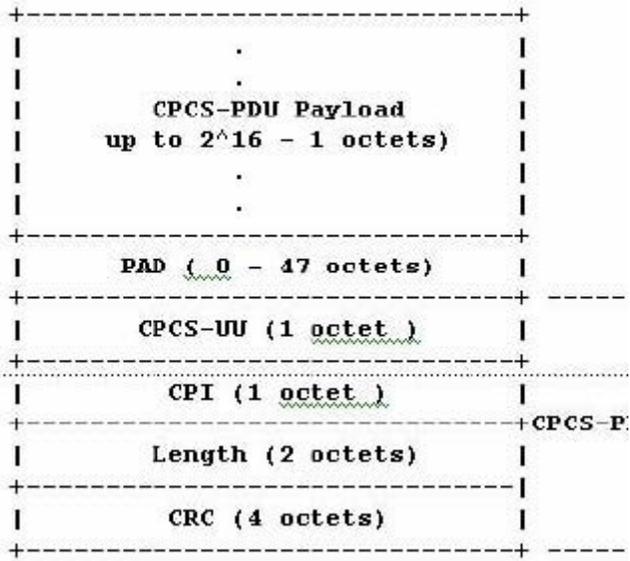
What are two advantages to the use of RFC 1483 to encapsulate IP data over ATM?
(Choose two.)

- A. multiprotocol support
- B. inherently more secure because of the Address Resolution Protocol (ARP)
- C. the CPE in bridge mode performs routing functions
- D. ideal for single-user Internet access

Answer: A, D

Explanation:

Asynchronous Transfer Mode (ATM) based networks are of increasing interest for both local and wide area applications. This memo describes two different methods for carrying connectionless network interconnect traffic, routed and bridged Protocol Data Units (PDUs), over an ATM network. The first method allows multiplexing of multiple protocols over a single ATM virtual circuit. The protocol of a carried PDU is identified by prefixing the PDU by an IEEE 802.2 Logical Link Control (LLC) header. This method is in the following called "LLC Encapsulation" and a subset of it has been earlier defined for SMDS [1]. The second method does higher-layer protocol multiplexing implicitly by ATM Virtual Circuits (VCs). It is in the following called "VC Based Multiplexing". ATM is a cell based transfer mode that requires variable length user information to be segmented and reassembled to/from short, fixed length cells. This memo doesn't specify a new Segmentation And Reassembly (SAR) method for bridged and routed PDUs. Instead, the PDUs are carried in the Payload field of Common Part Convergence Sublayer (CPCS) PDU of ATM Adaptation Layer type 5 (AAL5) [2].

AAL5 CPCS-PDU Format

The Payload field contains user information up to $2^{16} - 1$ octets. The PAD field pads the CPCS-PDU to fit exactly into the ATM cells such that the last 48 octet cell payload created by the SAR sublayer will have the CPCS-PDU Trailer right justified in the cell. The CPCS-UU (User-to-User indication) field is used to transparently transfer CPCS user to user information. The field has no function under the multiprotocol ATM encapsulation described in this memo and can be set to any value. The CPI (Common Part Indicator) field aligns the CPCS-PDU trailer to 64 bits. Possible additional functions are for further study in CCITT. When only the 64 bit alignment function is used, this field shall be coded as 0x00. The Length field indicates the length, in octets, of the Payload field. The maximum value for the Length field is 65535 octets. A Length field coded as 0x00 is used for the abort function. The CRC field protects the entire CPCS-PDU except the CRC field itself. LLC Encapsulation is needed when several protocols are carried over the same VC. In order to allow the receiver to properly process the incoming AAL5 CPCS-PDU, the Payload Field must contain information.

Reference from

<http://www.ietf.org/rfc/rfc1483.txt>

QUESTION 430:

Exhibit:

```
<output omitted>
|
interface ATM0/0/0
no ip address
no ip directed-broadcast
no atm ilmi-keepalive
atm ilmi-pvc-discovery subinterface
pvc 0/16 ilmi
|
interface ATM0/0/0.1 multipoint
no ip directed-broadcast
class-int bridge1
bridge-group 1
|
interface ATM0/0/0.4 multipoint
no ip directed-broadcast
class-int router
|
interface Ethernet0/0/1
no ip address
no ip directed-broadcast

interface Ethernet0/0/1
ip address 171.68.186.117 255.255.255.240
no ip directed-broadcast
|
<output omitted>
|
vc-class atm bridge1
encapsulation aal5snap
|
vc-class atm router
encapsulation aal5mux ppp Virtual-Template1
<output omitted>
```

Refer to the exhibit. Given the partial configuration for a Cisco 6400, which statement about the default encapsulation is true?

- A. Interface ATM 0/0/0 is using the default encapsulation.
- B. Interface ATM 0/0/0.1 is using the default encapsulation.
- C. Interface ATM 0/0/0.4 is using the default encapsulation.
- D. None of the ATM interfaces are using the default encapsulation.

Answer: C

QUESTION 431:

Which statement is true about the pri-group timeslots 1-16,24 controller command?

- A. 1024 K of total data bandwidth is available.
- B. 1088 K of total bada bandwidth is available.
- C. This command is for an E1 PRI.
- D. The interface serial 0/0:24 is automatically created.

Answer: A

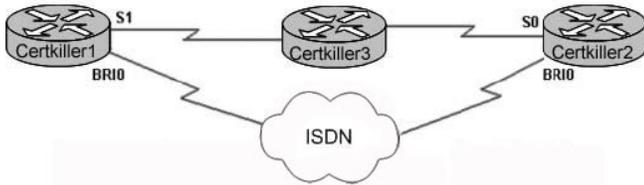
Explanation:

The pri-group command configures the specified interface for PRI operation and the number of fixed timeslots that are allocated on the provider's digital facility:

```
Router(config-controller)#pri-group [timeslots range]
```

QUESTION 432:

Exhibit:



```
Certkiller1# show int dialer 0
```

```
Dialer0 is standby mode (spoofing), line protocol is down (spoofing)
Hardware is Unknown
Internet address is 10.9.9.1/24
MTU 1500 bytes, BW 56 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, loopback not set
DTR is pulsed for 1 seconds on reset
Last input 1w6d, output never, output hang never
Last clearing of "show interface" counters 6w4d
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/1/16 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
Available Bandwidth 42 kilobits/sec
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
596 packets input, 48924 bytes
600 packets output, 49280 bytes
```

Refer to the exhibit. Router Certkiller 2 does not have a route to 10.9.9.0/24 in its routing table. What could be the cause?

- A. The primary interface on Certkiller 2 is still in use.
- B. The primary interface on Certkiller 1 is still in use.
- C. PPP negotiations are failing between Certkiller 1 and Certkiller 2.
- D. The ISDN line between Certkiller 1 and the ISDN switch is failing.

Answer: B

Explanation: Best answer is B, probably that primary interface on Certkiller 1 is still in use so not in routing table.

QUESTION 433:

Exhibit:

```
Phoenix# show running-config
--output omitted--
interface Serial0
no ip address
encapsulation frame-relay
frame-relay lmi-type ansi
frame-relay traffic-shaping
!
interface Serial0.2 point-to-point
ip address 10.128.30.17 255.255.255.248
frame-relay interface-dlci 102
class fast_vcs
!
interface Serial0.3 point-to-point
ip address 10.128.30.5 255.255.255.248
ip ospf cost 200
frame-relay interface-dlci 103
class slow_vcs
!
interface Serial3
no ip address
encapsulation frame-relay
frame-relay traffic-shaping
frame-relay class fast_vcs
!
interface Serial3.2 multipoint
ip address 100.120.20.13 255.255.255.248
frame-relay map ip 100.120.20.6 16 ietf broadcast
!
interface Serial3.3 point-to-point
ip address 100.120.10.13 255.255.255.248
frame-relay interface-dlci 101
!
map-class frame-relay slow_vcs
```

Refer to the exhibit. Which statement is true about the Frame Relay Traffic Shaping (FRTS) configuration that is shown?

- A. Interfaces Serial3.2 and Serial 3.3 are not configured for FRTS.
- B. Interfaces Serial3.2 and Serial 3.3 will inherit FRTS parameters from the Serial3 interface.
- C. Only Serial0 interfaces are properly configured for FRTS.
- D. The map class slow_vcs is configured incorrectly.
- E. The map class fast_vcs is configured incorrectly.

Answer: B

Explanation:

FRTS provides parameters that are useful for managing network traffic congestion on frame relay networks. FRTS eliminates bottlenecks in Frame Relay networks with high-speed connections to the central site and low-speed connections to the branch sites. You can configure rate enforcement values to limit the rate at which data is sent from the virtual circuit (VC) at the central site.

this diagram illustrates the network topology for the sample scenarios used in this document:



Sample Scenario: Frame Relay Traffic Shaping for Data Only

Assume this scenario: A 128Kbps frame relay circuit with a CIR PVC of 64Kbps. The user wants to burst to port speed (128Kbps) and throttle down to CIR rate (64 kbps) if BECNs are received to avoid data loss.

FRTS for Data PVCs

This is a typical FRTS configuration for data PVCs:

```
!--- Output suppressed.interface Serial1no ip addressno ip
directed-broadcastencapsulation frame-relayno fair-queueframe-relay
traffic-shaping!interface Serial1.100 point-to-pointip address 1.1.1.1
255.255.255.0no ip directed-broadcastframe-relay interface-dlci 100class
my_net!--- Output suppressed.!map-class frame-relay my_netframe-relay
adaptive-shaping becnframe-relay cir 128000frame-relay bc 8000frame-relay be
8000frame-relay mincir 64000Relevant FRTS Commands* frame-relay
traffic-shaping-This command enables FRTS for the interface. Every DLCI under
this interface is traffic shaped with either user-defined or default traffic shaping
parameters. User-defined parameters can be specified in two ways:
o Using the command class class_name under the frame-relay interface-dlci
configuration or
o Using the command frame-relay class under the serial interface.
```

In the example above, class my_net is used under the DLCI configuration.

* class class_name -Use this command to configure FRTS parameters for a specific DLCI. In the above example, the class is defined as "my_net". The class parameters are configured under the command map-class frame-relay class_name .

* map-class frame-relay class_name -Use this command to configure the FRTS parameters for a specified class. There can be multiple class-maps in a configuration. Each DLCI can have a separate class or DLCIs can share a single map class.

* frame-relay adaptive-shaping becn -This command configures the router to respond to frame relay frames that have the BECN bit set. When a frame is received on that PVC with the BECN bit set, then the router throttles traffic down on that PVC to the MINCIR value. The CIR is usually set to the port speed or a value higher than the true CIR of the PVC. The MINCIR value is then set to the true CIR of the PVC.

* frame-relay cir bps -Use this command to specify the incoming or outgoing committed information rate (CIR) for a Frame Relay virtual circuit.

* frame-relay bc bits -Use this command to specify the incoming or outgoing committed burst size (Bc) for a Frame Relay virtual circuit.

* frame-relay be bits -Use this command to specify the incoming or outgoing excess burst size (Be) for a Frame Relay virtual circuit.

* frame-relay mincir bps -Use this command to specify the minimum acceptable incoming or outgoing committed information rate (CIR) for a Frame Relay virtual circuit. This is the rate at which traffic will be throttled down to when using adaptive shaping.

Frame Relay Traffic Shaping For Voice

When configuring FRTS for voice, data performance may suffer at the expense of good voice quality. Here are some guidelines to enhance voice quality when configuring FRTS for voice:

* Do not exceed the CIR of the PVC

Most users have difficulty following this recommendation because the result is the router will no longer be able to burst to port speed. Because voice quality cannot tolerate much delay, any queueing of voice packets within the Frame Relay cloud must be minimized. When CIR is exceeded (PVC CIR, not the router configured CIR), depending on the provider and how congested the rest of the Frame Relay network is, packets may begin queue in the Frame Relay network. By the time the Frame Relay switch queues have backed up enough to trigger BECNs, the voice quality is already diminished. Because customers have many different Frame Relay providers and differing amounts of congestion across their sites, it is difficult to forecast what configuration works. Maintaining values at (or below) CIR on the PVCs that transport voice has proven to work consistently.

Some providers sell a Frame Relay service of 0 CIR. Obviously, not exceeding CIR in this case would prevent any voice from being sent across the frame link. A service of 0 CIR may be used for voice but there needs to be a Service Level Agreement (SLA) with the provider to guarantee minimal delay and jitter for a certain bandwidth across the 0 CIR PVC.

* Do not use frame relay adaptive shaping

If the configured CIR within the frame relay map class is the same as the true CIR of the PVC, there is no need to throttle down traffic due to BECNs. If CIR is not exceeded, BECNs are not generated.

* Make Bc small so that Tc (shaping interval) is small ($Tc = Bc/CIR$)

The minimum Tc value is 10 ms, which is ideal for voice. With a small Tc value, there is no risk of large packets using all the shaping credits. Large Tc values can lead to large gaps between packets sent because the traffic shaper waits an entire Tc period to build up additional credits to send the next frame. Making Bc = 1000 bits is usually a low enough value to force the router to use the minimum Tc of 10ms. This setting should not affect data throughput.

* Set Be = zero

To ensure the CIR value is not exceeded, Be is set to zero so there is no excess burst within the first shaping interval.

Reference From :

http://www.cisco.com/en/US/tech/CK652/CK698/technologies_tech_note09186a00800d6788.shtml

QUESTION 434:

A customer's network policy states that voice traffic should be serviced before all other application traffic, such as HTTP and FTP. Which quality of service methods should the customer employ?

- A. WFQ
- B. Custom queuing
- C. CBWFQ
- D. LLQ

Answer: D

Explanation:

The Low Latency Queuing (LLQ) feature provides strict priority queuing for class-based weighted fair queuing (CBWFQ), reducing jitter in voice conversations. Configured by the priority command, strict priority queuing gives delay-sensitive data, such as voice, preferential treatment over other traffic. With this feature, delay-sensitive data is sent first, before packets in other queues are treated. LLQ is also referred to as priority queuing/class-based weighted fair queuing (PQ/CBWFQ) because it is a combination of the two techniques.

For CBWFQ, the weight for a packet belonging to a specific class is derived from the bandwidth assigned to the class during configuration. Therefore, the bandwidth assigned to the packets of a class determines the order in which packets are sent. All packets are serviced equally, based on weight. No class of packets may be granted strict priority. This scheme poses problems for voice and video traffic that is largely intolerant of delay, especially variation in delay. For voice traffic, variations in delay introduce irregularities of transmission, which manifest as jitter in the conversation.

QUESTION 435:

Exhibit:

```
interface Serial1/0
  encapsulation frame-relay
  no frame-relay inverse-arp
  frame-relay lmi-type cisco

interface Serial1/0.123 multi point
  ip address 172.16.123.1 255.255.255.128
  frame-relay map ip 172.16.123.1 103
  frame-relay map ip 172.16.123.2 102 broadcast
  frame-relay map ip 172.16.123.3 103 broadcast
  no frame-relay inverse-arp
  no ip split-horizon
```

Refer to the exhibit. What is the purpose of the command frame-relay map ip 172.16.123.1 103?

- A. to allow the router to successfully ping 172.16.123.1
- B. to allow the router to form a Layer 2 frame map to another router
- C. to allow Layer 3 connectivity to another router
- D. to allow routing between the two hub routers
- E. to prevent routing between the two hub routers

Answer: A

Explanation:

When using dynamic address mapping, Inverse ARP requests a next-hop protocol address for each

active PVC. Once the requesting router receives an Inverse ARP response, it updates its DLCI-to-Layer 3 address mapping table. Dynamic address mapping is enabled by default for all protocols enabled on a physical interface. If the Frame Relay environment supports LMI autosensing and Inverse ARP, dynamic address mapping takes place automatically. Therefore, no static address mapping is required

If the environment does not support LMI autosensing and Inverse ARP, a Frame Relay map must be manually configured. Use the frame-relay map command to configure static address mapping. Once a static map for a given DLCI is configured, Inverse ARP is disabled on that DLCI.

To configure a frame-relay static map use the following syntax.
Router(config-if)#frame-relay map protocol protocol-address dlci
[broadcast] [ietf | cisco]

QUESTION 436:

Which command associates a map class with an interface or subinterface when configuring Frame Relay traffic shaping?

- A. frame-relay map
- B. frame-relay class
- C. map-class frame-relay
- D. frame-relay map-class
- E. map frame-relay class

Answer: B

Explanation:

A map class defines a set of configuration parameters that can be used by more than one interface or subinterface. Configure Frame Relay traffic shaping parameters for the map class, and then apply the map class to one or more Frame Relay interfaces. Frame Relay traffic shaping parameters cannot be configured directly on the interface.

Configure the Map Class

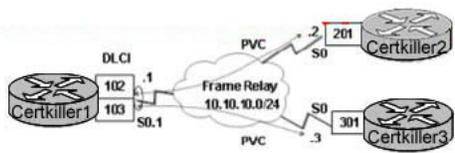
```
RTA(config)#map-class frame-relay PRIORITY-QUEUE
RTA(config-map-class)#frame-relay priority-group 3
RTA(config-map-class)#exit
RTA(config)#priority-list 3 protocol decent high
RTA(config)#priority-list 3 protocol ip normal
RTA(config)#priority-list 3 default medium
```

Apply the Map Class to a Frame Relay Interface

```
RTA(config)#interface serial 0/2
RTA(config-if)#encapsulation frame-relay
RTA(config-if)#frame-relay traffic-shaping
RTA(config-if)#frame-relay class PRIORITY-QUEUE
```

QUESTION 437:

Exhibit:



```

Hostname Certkiller2
!
interface s0
ip address 10.10.10.2 255.255.255.0
encapsulation frame-relay
frame-relay map ip 10.10.10.1 201 broadcast
!
!
!

Hostname Certkiller3
!
interface s0
ip address 10.10.10.3 255.255.255.0
encapsulation frame-relay
frame-relay map ip 10.10.10.1 301 broadcast
!
!
!

Certkiller3# debug frame-relay packets

Certkiller3# ping 10.10.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.2, timeout is 2 seconds:
00:27:51: Serial0:Encaps failed--no map entry link 7(IP).
00:27:53: Serial0:Encaps failed--no map entry link 7(IP).
00:27:55: Serial0:Encaps failed--no map entry link 7(IP).
00:27:57: Serial0:Encaps failed--no map entry link 7(IP).
00:27:59: Serial0:Encaps failed--no map entry link 7(IP).
Success rate is 0 percent (0/5)

```

Refer to the exhibit. Certkiller 1 is able to connect to both spoke sites. However, Certkiller 3 is unable to ping Certkiller 2. Which configuration will fix this problem?

- A. Certkiller 2(config-if)# encapsulation frame-relay ietf
Certkiller 3(config-if)# encapsulation frame-relay ietf
- B. Certkiller 2(config-if)# no frame-relay inverse-arp
Certkiller 3(config-if)# no frame-relay inverse-arp
- C. Certkiller 2(config-if)# frame-relay map ip 10.10.10.3 201 broadcast
Certkiller 3(config-if)# frame-relay map ip 10.10.10.2 301 broadcast
- D. Certkiller 2(config-if)# frame-relay interface-dlci 201
Certkiller 3(config-if)# frame-relay interface-dlci 301

Answer: C

Explanation:

When using dynamic address mapping, Inverse ARP requests a next-hop protocol address for each active PVC. Once the requesting router receives an Inverse ARP response, it updates its DLCI-to-Layer 3 address mapping table. Dynamic address mapping is enabled by default for all protocols enabled on a physical interface. If the Frame Relay environment supports LMI autosensing and Inverse ARP, dynamic address mapping takes place automatically. Therefore, no static address mapping is required.

If the environment does not support LMI autosensing and Inverse ARP, a Frame Relay map must be manually configured. Use the frame-relay map command to configure static address mapping. Once a static map for a given DLCI is configured, Inverse ARP is disabled on that DLCI.

To configure a frame-relay static map use the following syntax.

```
Router(config-if)#frame-relay map protocol protocol-address dlci
[broadcast] [ietf | cisco]
```

The broadcast keyword is commonly used with the frame-relay map command. The

broadcastkeyword provides two functions. First, it forwards broadcasts when multicasting is not enabled and secondly, it simplifies the configuration of OSPF for nonbroadcast networks that use Frame Relay.

The broadcastkeyword might also be required for routing protocols such as AppleTalk that depend on regular routing table updates. This is especially true when the router at the remote end is waiting for a routing update packet to arrive before adding the route.

QUESTION 438:

Which type of remote-user VPN has users dial in to an Internet service provider (ISP) where an ISP-owned device establishes a secure tunnel to the users' enterprise network?

- A. client initiated VPN
- B. network access server (NAS) initiated VPN
- C. intranet VPN
- D. extranet VPN

Answer: B

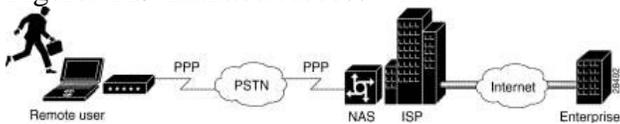
Explanation:

AS-initiated access VPNs allow for remote users to dial in to the ISP's NAS. The NAS establishes an encrypted tunnel to the enterprise's private network.

NAS-initiated VPNs allow remote users to connect to multiple networks using multiple tunnels. NAS-initiated VPNs do not encrypt the connection between the client and the ISP, but rely on the security of the PSTN.

Figure shows a NAS-initiated access VPN topology. Because the Cisco Secure VPN Client is not required for a NAS-initiated access VPN solution, it is not a component of this network. The disadvantage of NAS-initiated access VPNs is that the PSTN is not secured.

Figure NAS-Initiated Access VPN



Reference from:

http://www.cisco.com/en/US/products/sw/secursw/ps2138/products_maintenance_guide_chapter09186a008

QUESTION 439:

A central site is responsible for reaching three separate remote locations. Each of these locations uses a different location-specific profile. Which configuration command would make it possible for the central site router to use these three profiles with just a single physical interface?

- A. group-range
- B. dialer list

- C. dialer group
- D. interface dialer

Answer: D

Explanation:

The interface dialer command in global configuration mode creates a dialer rotary group:

```
Router(config)#interface dialer group-number
```

The interface dialer 1 command creates the logical interface configuration that will be shared among the members of the rotary group. Since this interface is numbered "1", a physical line participating in this rotary group must also be configured with the command dialer rotary-group 1.

QUESTION 440:

Exhibit:

<pre>Certkiller1# show running-config <output omitted> interface BRI0/0 ip address 172.16.21.1 255.255.255.128 encapsulation ppp dialer map snapshot 1 name R2R2 broadcast 5551100 dialer map ip 172.16.21.2 name R2R2 broadcast 5551200 dialer-group 1 isdn switch-type basic-ni isdn spid1 3035551000101 5551100 isdn spid2 3035551010101 5551101 no peer neighbor-route snapshot client 5 20 dialer ppp authentication chap ppp chap hostname R1R1</pre>	<pre>Certkiller2# show running-config <output omitted> interface BRI0/0 ip address 172.16.21.2 255.255.255.128 encapsulation ppp dialer map ip 172.16.21.1 name R1R1 broadcast 5551200 dialer-group 1 isdn switch-type basic-ni isdn spid1 30355512000101 5551200 isdn spid2 30355512010101 5551201 no peer neighbor-route snapshot server 5 dialer ppp authentication chap</pre>
---	---

Refer to the exhibit. Router Certkiller 1 is not able to connect to router Certkiller 2 using ISDN. What is the problem?

- A. misconfigured dialer maps
- B. authentication
- C. routing
- D. Layer 2 INACTIVE
- E. Snapshot routing

Answer: B

Explanation: In Observation of Certkiller 1 and Certkiller 2 router, both not able to connect to due to the problem of authentication.

In R2R2 router no local username and password database nor sending the username and password using ppp chap hostname command.

See the Example:

Enable PPP encapsulation and PAP authentication with the following commands:

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

Router(config-if)#ppp authentication pap

A local username/password database must also be configured, or point it to a network host that has that information, such as a TACACS+ server. Without access to a username/password database, the router will not know which combinations are authorized and will deny all login attempts. Configure a local username/password database by using the following command in global configuration mode:

Router(config)#username username password password

The username and password must match the username and password in the remote router's ppp pap sent-username command. For example, the following would add the entry for a user called Romeo in the router's local database:

Router(config)#username romeo password juliet

In some cases, the asynchronous interface of a router is configured to place calls to other access servers. If an interface is to respond to a peer's request to authenticate with PAP, the ppp pap sent-username command must be used:

Router(config-if)#ppp pap sent-username username password password

The username and password in the ppp pap sent-username command, must match the username username password password statement on the remote host or router.

QUESTION 441:

In PPP NCP, what does IPCP do? (Choose three.)

- A. negotiates IP addresses
- B. negotiates compression
- C. relays primary and backup WINS and DNS servers
- D. defines authentication protocols
- E. defines BRI virtual interface types
- F. relays primary and backup TFTP servers

Answer: A, B, C

Explanation:

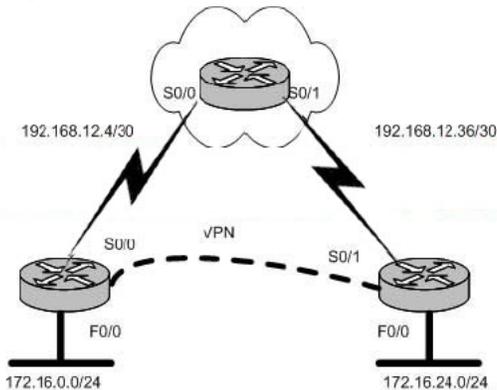
PPP defines the Link Control Protocol (LCP). The job of the LCP is to establish, configure, and test the data-link connection. When hosts negotiate a PPP connection, they exchange LCP packets. These packets allow link partners to dynamically negotiate link options, including authentication, compression, and MLP. The protocol field is used to identify various Layer 3 protocols, such as IP or IPX. The LCP field allows for the following features:

1. Authentication
2. Callback
3. Compression
4. Multilink PPP

Once the LCP establishes the Layer 2 connection, the Network Control Protocol (NCP) takes over. Link partners exchange NCP packets to establish and configure different network-layer protocols including IP, IPX, and AppleTalk. Each Layer 3 protocol has its own NCP. For example, IP's NCP is IPCP. IPX's NCP is IPXCP and Appletalk's NCP is ATALKCP.

QUESTION 442:

Exhibit:

**Show Commands:**

```

Central# show crypto isakmp policy
Protection suite of priority 110
  encryption algorithm:  DES - Data Encryption Standard (56 bit keys).
  hash algorithm:       Secure Hash Standard
  authentication method: Pre-Shared Key
  Diffie-Hellman group: #1 (768 bit)
  lifetime:             86400 seconds, no volume limit
Default protection suite
  encryption algorithm:  DES - Data Encryption Standard (56 bit keys).
  hash algorithm:       Secure Hash Standard
  authentication method: Rivest-Shamir-Adleman Signature
  Diffie-Hellman group: #1 (768 bit)
  lifetime:             86400 seconds, no volume limit

Central# show crypto isakmp key
HostName/Address      Preshared Key
192.168.12.9          ispgaes02
192.168.12.13         ispgaes03
192.168.12.17         ispgaes04
192.168.12.21         ispgaes05
192.168.12.25         ispgaes06
192.168.12.33         ispgaes08
192.168.12.37         ispgaes09
192.168.12.41         ispgaes10
192.168.12.45         ispgaes11
192.168.12.49         ispgaes12

Central# show crypto ipsec sa
interface: Serial0/0
  crypto map map: name, local addr: 192.168.12.5
  local ident [addr/mask/proto]: (172.16.0.0/255.255.0/0/0)
  remote ident [addr/mask/proto]: (172.16.24.0/255.255.0/0/0)
  current_peer: 192.168.12.7
  PROTECT, flags:(origin,!,acl)
  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
  #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

  local crypto endpt.: 192.168.12.5, remote crypto endpt.: 192.168.12.37
  path mtu 1500, ip mtu 1500, ip mtu interface Serial0/0
  current outbound spi: 0

  inbound esp sas:

  inbound ah sas:

  inbound pcp sas:

Central# show crypto ipsec transform-set
transform set GAREDS: ( esp-des )
will negotiate = ( Tunnel, )

```

Refer to the exhibits. Certkiller Incorporated is an Internet game provider. The game service network has recently added an additional facility to connect to an already configured central site. As a remote site technician you will be required to configure the VPN connection at the remote site for secure communication between the central and remote LAN segments. Using the physical topology and the show output provided from the commands show crypto isakmp policy, show crypto ipsec sa, and show crypto ipsec transform-set on the central router, answer the following question:

Which authentication method must be configured for the IKE policy on the Remote router?

- A. Remote(config-isakmp)# authentication rsa-sig
- B. Remote(config-isakmp)# authentication rsa-encr

- C. Remote(config-isakmp)# authentication pre-shared
- D. Remote(config-isakmp)# hash md5
- E. Remote(config-isakmp)# hash sha

Answer: C

Explanation:

Configuring IKE is complicated. First, determine the IKE policy details to enable the selected authentication method, and then configure it. Having a detailed plan lessens the chances of improper configuration. The following steps should be included in the plan:

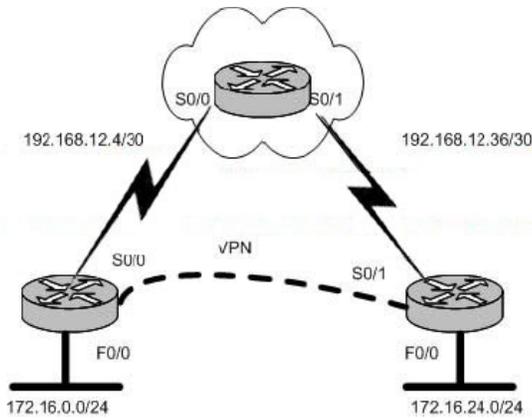
1. Determine the key distribution method- Determine the key distribution method based on the numbers and locations of IPSec peers. For a small network, keys may be distributed manually. For larger networks, use a CA server to support scalability of IPSec peers. Then, configure the Internet Security Association Key Management Protocol (ISAKMP) to support the selected key distribution method.
2. Determine the authentication method- Determine the authentication method based on the key distribution method. Cisco IOS software supports either pre-shared keys, RSA encrypted nonces, or RSA signatures to authenticate IPSec peers. This lesson focuses on using pre-shared keys.
3. Identify IPSec peer IP addresses and host names- Determine the details of all of the IPSec peers that will use ISAKMP and pre-shared keys for establishing security associations (SAs). This information will be used to configure IKE.
4. Determine ISAKMP policies for peers- An ISAKMP policy defines a combination or "suite" of security parameters to be used during the ISAKMP negotiation. Each ISAKMP negotiation begins with each peer agreeing on a common, or shared, ISAKMP policy. Determine the ISAKMP policy suites in advance of configuration. Then, configure IKE to support the policy details that have been determined. Examples of ISAKMP policy details are included in the following list:
 5. 1. Encryption algorithm
 2. Hash algorithm
 3. IKE SA lifetime

In the output of show crypto isakmp key pre-shared authentication method is displayed. In both pairs, authentication method should be same.

So Remote(config-isakmp)# authentication pre-shared should be configured in remote router.

QUESTION 443:

Exhibit:



Show Commands:

```
Central# show crypto isakmp policy
Protection suite of priority 110
  encryption algorithm:  DES - Data Encryption Standard (56 bit keys).
  hash algorithm:       Secure Hash Standard
  authentication method: Pre-Shared Key
  Diffie-Hellman group: #1 (768 bit)
  lifetime:             06400 seconds, no volume limit
Default protection suite
  encryption algorithm:  DES - Data Encryption Standard (56 bit keys).
  hash algorithm:       Secure Hash Standard
  authentication method: Rivest-Shamir-Adleman Signature
  Diffie-Hellman group: #1 (768 bit)
  lifetime:             86400 seconds, no volume limit

Central# show crypto isakmp key
Hostname/Address      Preshared Key
192.168.12.9          ispgames02
192.168.12.13         ispgames03
192.168.12.17         ispgames04
192.168.12.21         ispgames05
192.168.12.25         ispgames06
192.168.12.33         ispgames08
192.168.12.37         ispgames09
192.168.12.41         ispgames10
192.168.12.45         ispgames11
192.168.12.49         ispgames12

Central# show crypto ipsec sa

Interface: Serial0/0
Crypto map tag: GARET8, local addr: 192.168.12.5

local ident (addr/mask/prot/port): (172.16.0.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (172.16.24.0/255.255.255.0/0/0)
current_peer: 192.168.12.37
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
  #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

local crypto endpt.: 192.168.12.5, remote crypto endpt.: 192.168.12.37
path mtu 1500, ip mtu 1500, ip mtu interface Serial0/0
current outbound spi: 0

inbound esp sas:
inbound ah sas:
inbound pcp sas:

Central# show crypto ipsec transform-set
Transform set GARET8: ( esp-des )
  will negotiate = ( Tunnel, ),
```

Refer to the exhibits. Certkiller Incorporated is an Internet game provider. The game service network has recently added an additional facility to connect to an already configured central site. As a remote site technician you will be required to configure the VPN connection at the remote site for secure communication between the central and remote LAN segments. Using the physical topology and the show output provided from the commands show crypto isakmp policy, show crypto ipsec sa, and show crypto ipsec transform-set on the central router, answer the following question:

Which key and address must be identified for the IKE policy in the crypto isakmp key global configuration command on the remote router? (Choose two.)

- A. ispgames02
- B. ispgames08
- C. ispgames09

- D. 192.168.12.5
- E. 192.168.12.33
- F. 192.168.12.37

Answer: C, D

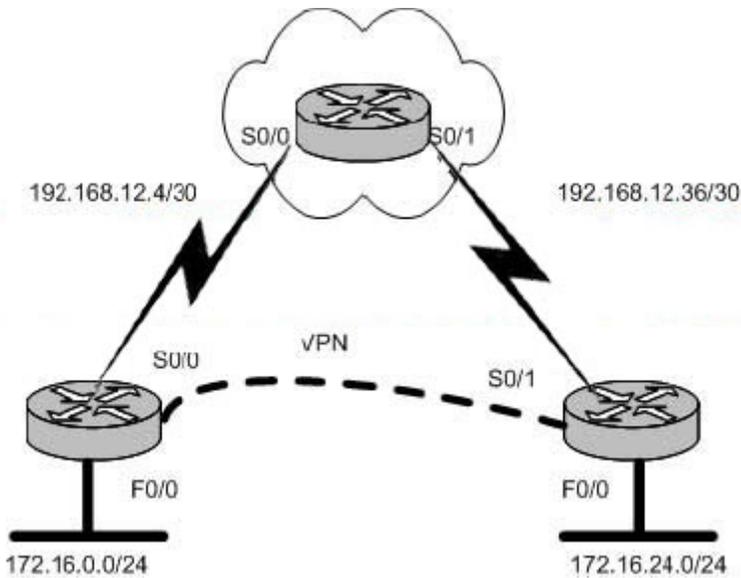
Explanation:

Configuring IKE is complicated. First, determine the IKE policy details to enable the selected authentication method, and then configure it. Having a detailed plan lessens the chances of improper configuration. The following steps should be included in the plan:

1. Determine the key distribution method- Determine the key distribution method based on the numbers and locations of IPSec peers. For a small network, keys may be distributed manually. For larger networks, use a CA server to support scalability of IPSec peers. Then, configure the Internet Security Association Key Management Protocol (ISAKMP) to support the selected key distribution method.
 2. Determine the authentication method- Determine the authentication method based on the key distribution method. Cisco IOS software supports either pre-shared keys, RSA encrypted nonces, or RSA signatures to authenticate IPSec peers. This lesson focuses on using pre-shared keys.
 3. Identify IPSec peer IP addresses and host names- Determine the details of all of the IPSec peers that will use ISAKMP and pre-shared keys for establishing security associations (SAs). This information will be used to configure IKE.
 4. Determine ISAKMP policies for peers- An ISAKMP policy defines a combination or "suite" of security parameters to be used during the ISAKMP negotiation. Each ISAKMP negotiation begins with each peer agreeing on a common, or shared, ISAKMP policy. Determine the ISAKMP policy suites in advance of configuration. Then, configure IKE to support the policy details that have been determined. Examples of ISAKMP policy details are included in the following list:
 5. 1. Encryption algorithm
 2. Hash algorithm
 3. IKE SA lifetime
- In the output Peer VPN Peer is configured between 192.168.12.5 and 192.168.12.37. The identity should be 192.168.12.5 and key must be same in both routers. So, Key configured in 192.168.12.37 is ispgames09

QUESTION 444:

Exhibit:



Show Commands:

```
Central# show crypto isakmp policy
Protection suite of priority 110
  encryption algorithm: DES - Data Encryption Standard (56 bit keys).
  hash algorithm: Secure Hash Standard
  authentication method: Pre-Shared Key
  Diffie-Hellman group: #1 (768 bit)
  lifetime: 86400 seconds, no volume limit
Default protection suite
  encryption algorithm: DES - Data Encryption Standard (56 bit keys).
  hash algorithm: Secure Hash Standard
  authentication method: Rivest-Shamir-Adleman Signature
  Diffie-Hellman group: #1 (768 bit)
  lifetime: 86400 seconds, no volume limit

Central# show crypto isakmp key
Hostname/Address      Preshared Key
192.168.12.9          ispgame02
192.168.12.13         ispgame03
192.168.12.17         ispgame04
192.168.12.21         ispgame05
192.168.12.25         ispgame06
192.168.12.33         ispgame08
192.168.12.37         ispgame09
192.168.12.41         ispgame10
192.168.12.45         ispgame11
192.168.12.49         ispgame12

Central# show crypto ipsec sa
interface: Serial0/0
  Crypto map tag: GAMEB, local addr: 192.168.12.5
  local ident [addr/mask/proto]: (172.16.0.0/255.255.255.0/0/0)
  remote ident [addr/mask/proto]: (172.16.24.0/255.255.255.0/0/0)
  current peer: 192.168.12.37
  PERMIT, flags=(origin_is_acl, )
  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
  #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

  local crypto endpt.: 192.168.12.5, remote crypto endpt.: 192.168.12.37
  path mtu 1500, ip mtu 1500, ip mtu interface Serial0/0
  current outbound spi: 0

  inbound esp sas:
  inbound ah sas:
  inbound pcp sas:

Central# show crypto ipsec transform-set
Transform set GAMEB: ( esp-des )
  will negotiate = ( Tunnel, )
```

Refer to the exhibits. Certkiller Incorporated is an Internet game provider. The game service network has recently added an additional facility to connect to an already configured central site. As a remote site technician you will be required to configure the VPN connection at the remote site for secure communication between the central and remote LAN segments. Using the physical topology and the show output provided from the commands show crypto isakmp policy, show crypto ipsec sa, and show crypto ipsec transform-set on the central router, answer the following question:

Which access-list statement would be used for identifying local and remote VPN

traffic to be encrypted at the remote site?

- A. access-list 110 permit ip 172.16.0.0 0.0.0.255 172.16.24.0 0.0.0.255
- B. access-list 110 permit ip 172.16.24.0 0.0.0.255 172.16.0.0 0.0.0.255
- C. access-list 110 permit ip 192.168.12.4 0.0.0.3 192.168.12.36 0.0.0.3
- D. access-list 110 permit ip 192.168.12.36 0.0.0.3 192.168.12.4 0.0.0.3

Answer: B

Explanation:

The crypto ACLs identify the traffic flows that will be protected. Extended IP ACLs select IP traffic to encrypt by protocol, IP address, network, subnet, and port. Although the ACL syntax is unchanged from extended IP ACLs, the meanings are slightly different for crypto ACLs. When using crypto ACLs, permit specifies that matching packets must be encrypted and deny specifies that matching packets do not need to be encrypted. Crypto ACLs behave similar to an extended IP ACL applied to the outbound traffic on an interface.

See the command reference for a complete description of this command. The command syntax for the basic form of extended IP access lists is as follows:

```
access-list access-list-number { permit | deny } protocol source  
source-wildcard destination destination-wildcard[precedence precedence]  
[tos tos] [log]
```

Any unprotected inbound traffic that matches a permit entry in the crypto ACL for a crypto map entry flagged as IPsec will be dropped, because this traffic was expected to be protected by IPsec.

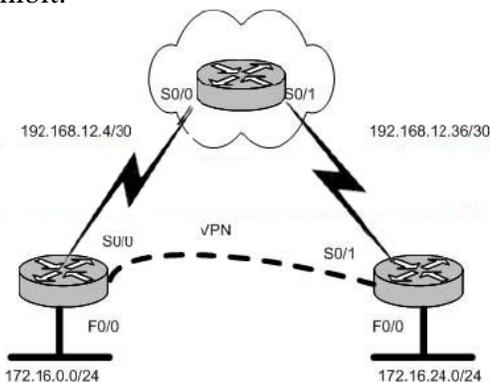
If certain traffic only requires authentication for IPsec protection, and other traffic should receive both authentication and encryption, create two different crypto ACLs to define the two different types of traffic. These different ACLs are then used in different crypto map entries that specify different IPsec policies.

VPN is configured between 172.16.0.0/24 and 172.16.24.0/24 network so it should be allow.

```
access-list 110 permit ip 172.16.24.0 0.0.0.255 172.16.0.0 0.0.0.255
```

QUESTION 445:

Exhibit:



Show Commands:

```
Central# show crypto isakmp policy
Protection suite of priority 110
  encryption algorithm:  DES - Data Encryption Standard (56 bit keys).
  hash algorithm:        Secure Hash Standard
  authentication method: Pre-Shared Key
  Diffie-Hellman group:  #1 (768 bit)
  lifetime:              86400 seconds, no volume limit
Default protection suite
  encryption algorithm:  DES - Data Encryption Standard (56 bit keys).
  hash algorithm:        Secure Hash Standard
  authentication method: Rivest-Shamir-Acleman Signature
  Diffie-Hellman group:  #1 (768 bit)
  lifetime:              86400 seconds, no volume limit

Central# show crypto isakmp key
Hostname/Address      Freshshared Key
192.168.12.9          ispgames02
192.168.12.13         ispgames03
192.168.12.17         ispgames04
192.168.12.21         ispgames05
192.168.12.25         ispgames06
192.168.12.33         ispgames08
192.168.12.37         ispgames09
192.168.12.41         ispgames10
192.168.12.45         ispgames11
192.168.12.49         ispgames12

Central# show crypto ipsec sa
interface: Serial0/0
  Crypto map tag: GAMES, local addr. 192.168.12.5
  local ident [addr/mask/proto]: (172.16.0.0/255.255.255.0/0/0)
  remote ident [addr/mask/proto]: (172.16.24.0/255.255.255.0/0/0)
  current_peer: 192.168.12.37
  PERMIT, flags=(origin_is_acl, )
  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
  #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

  local crypto endpt.: 192.168.12.5, remote crypto endpt.: 192.168.12.37
  path mtu 1500, ip mtu 1500, ip mtu interface Serial0/0
  current outbound spi: 0

  inbound esp sas:

  inbound ah sas:

  inbound pcp sas:

Central# show crypto ipsec transform-set
Transform set GAMEDB: ( esp-des )
  will negotiate = ( Tunnel, ),
```

Refer to the exhibits. Certkiller Incorporated is an Internet game provider. The game service network has recently added an additional facility to connect to an already configured central site. As a remote site technician you will be required to configure the VPN connection at the remote site for secure communication between the central and remote LAN segments. Using the physical topology and the show output provided from the commands show crypto isakmp policy, show crypto ipsec sa, and show crypto ipsec transform-set on the central router, answer the following question:

Which transform-set and peer address need to be configured within the IPSec policy on the remote router? (Choose two.)

- A. 192.168.12.5
- B. 192.168.12.37
- C. GAMES
- D. GAMEDB
- E. esp-des
- F. esp-null

Answer: A, E

Explanation:

An IPSec policy defines a combination of IPSec parameters used during the IPSec negotiation. Planning for IPSec IKE phase two is another important step that should be completed before actually configuring IPSec on a Cisco router. Policy details to determine at this stage include the following:

1. Select IPSec algorithms and parameters for optimal security and performance-

Determine the type of IPSec security to use when securing interesting traffic. A choice between high performance and stronger security will have to be made for some IPSec algorithms. Some algorithms have import and export restrictions that may delay or prevent implementation of the network.

2. Select transforms and, if necessary, transform sets- Use the IPSec algorithms and parameters previously selected to help select IPSec transforms, transform sets, and modes of operation.
3. Identify IPSec peer details- Including the IP addresses and host names of all IPSec peers that will be connected.
4. Determine IP address and applications of hosts to be protected- Decide which hosts IP addresses and applications should be protected at the local peer and remote peer.
5. Select manual or IKE-initiated SAs- Choose whether SAs are manually established or are established using IKE.

The goal of this planning step is to gather the precise data needed in later steps to minimize misconfiguration.

Transfer-Set can be

Transform	Description
esp-des	ESP transform using DES cipher (56 bits)
esp-3des	ESP transform using 3DES(EDE) cipher (168 bits)
esp-md5-hmac	ESP transform with HMAC MD5 authentication used with an esp des or esp 3des transform to provide additional integrity of ESP packet
esp-sha-hmac	ESP transform with HMAC SHA authentication used with an esp-des or des-3des transform to provide additional integrity of ESP packet
esp-null	ESP transform without a cipher. May be used in combination with esp-md5-hmac or esp-sha-hmac if one wants ESP authentication with no encryption

Transfer set also should be same between the peers. As per exhibit transfer set should be esp-des and should configured in 192.168.12.5

QUESTION 446:

Exhibit:



```

Certkiller2#show crypto ipsec sa

interface: Serial0/0
Crypto map tag: VPN-CM-4, local addr:2.2.2.2

protected vrf:
local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.252/0/0)
remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.252/0/0)
current_peer: 2.1.1.1:500
<output omitted>

inbound esp sas:
spi: 0xBFEA4FA8(3219804072)
transform: esp-256-aes esp-sha-hmac .
in use settings =(Tunnel, )
slot: 0, conn id: 2004, flow_id: 5, crypto map: VPN-CM-4
sa timing: remaining key lifetime (k/sec): (4426113/66)
IV size: 16 bytes
replay detection support: Y

inbound ah sas:

outbound esp sas:
spi: 0x1080ACDB(276868315)
transform: esp-256-aes esp-sha-hmac .
in use settings =(Tunnel, )
slot: 0, conn id: 2005, flow_id: 6, crypto map: VPN-CM-4
sa timing: remaining key lifetime (k/sec): (4426100/63)
IV size: 16 bytes
replay detection support: Y

outbound ah sas:

R2#

```

Refer to the exhibit. A network administrator is attempting to verify an IPsec VPN connection between Certkiller 1 and Certkiller 2. Which three statements are true about the VPN? (Choose three.)

- A. Traffic from Host A to Host X will be protected by IPsec.
- B. Traffic from Host B to Host X will be protected by IPsec.
- C. AH is used by Certkiller 2 to protect VPN traffic to Certkiller 1.
- D. SHA-1 is used by Certkiller 1 to protect VPN traffic to Certkiller 2.
- E. Certkiller 1 and Certkiller 2 are IKE peers.
- F. Certkiller 1 and Certkiller 2 have established a Transport Mode IPsec VPN.

Answer: A, D, E

Explanation:

A Virtual Private Network (VPN) is defined as network connectivity deployed on a shared infrastructure with the same policies and security as a private network.

A VPN can be between two end systems, or it can be between two or more networks. A VPN can be built using tunnels and encryption. VPNs can occur at any layer of the OSI protocol stack. A VPN is an alternative WAN infrastructure that replaces or augments existing private networks that use leased-line or enterprise-owned Frame Relay or ATM networks.

VPNs provide three critical functions:

1. Confidentiality (encryption)- The sender can encrypt the packets before transmitting them across a network. By doing so, no one can access the communication without permission. If intercepted, the communications cannot be read.
2. Data integrity- The receiver can verify that the data was transmitted through the Internet without being altered.
3. Origin authentication- The receiver can authenticate the source of the packet, guaranteeing and certifying the source of the information.

IPSec is configured, data will secure by IPSec.

HMAC-SHA-1- Uses a 160-bit secret key. The variable length message and the 160 bit shared secret key are combined and run through the HMAC-SHA-1 hash algorithm. The output is a 160-bit hash. The hash is appended to the original message and forwarded to the remote end.

QUESTION 447:

When AAA accounting is being configured on a Cisco router, what two accounting method types are available? (Choose two.)

- A. login
- B. group tacacs+
- C. local
- D. enable
- E. group radius

Answer: B, E

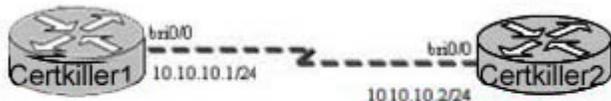
Explanation:

Access servers and other network hosts are often configured to use a security protocol. Hosts use a security protocol to communicate with a specialized security server. The security server maintains a password and username database. The security server also stores authorization configurations and accounting information. The Cisco IOS supports three key security protocols named TACACS+, RADIUS, and Kerberos. TACACS+ is a security application used with AAA that provides centralized validation of users attempting to gain access to a router or network access server. TACACS+ services are maintained in a database on a TACACS+ daemon running on a UNIX, Windows NT, or Windows 2000 workstation. TACACS+ provides for separate and modular authentication, authorization, and accounting facilities.

RADIUS is a distributed client/server system used with AAA that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server. This central server contains all user authentication and network service access information.

QUESTION 448:

Exhibit:



Which command will allow Certkiller 1 to test its legacy DDR configuration without having any dialer map statement configured?

- A. isdn test call interface bri 0 5551234 speed 56
- B. ping 10.10.10.2

- C. debug isdn q931
- D. debug isdn q921

Answer: A

Explanation:

You can use the `isdn test call interface` command to test your DDR configuration. You can also use this command to verify the dialing string and speed without having to know the IP address of the remote router or without configuring a dialer map or string.

Syntax: `isdn test call interface interface-number dialing-string[speed 56 | 64]`

QUESTION 449:

Given the configuration:

```
access-list 101 deny tcp any any eq ftp
access-list 101 permit ip any any
dialer-list 2 protocol ip list 101
```

Which two statements about the configuration are true with respect to the DDR?
(Choose two.)

- A. FTP traffic will never be forwarded.
- B. FTP traffic will only be forwarded while other interesting traffic is being forwarded.
- C. All traffic will cause the line to activate.
- D. FTP will cause the line to activate.
- E. FTP will not cause the line to activate.
- F. Since FTP uses two sockets, both must be defined to prevent packet forwarding.

Answer: B, E

Explanation:

The `dialer-list` command is used to define what type of traffic is "interesting". A router will bring up a DDR interface, if it is not up already, to route interesting traffic. Once the call is established, the router will not disconnect the call as long as it continues to receive interesting traffic to route over the DDR link. While the link is up, other "uninteresting" traffic can be routed over the link. Uninteresting traffic is traffic that is not defined by the dialer list. However, if the link is idle for a configurable period of time, the router will disconnect the call. The router considers the link idle if it is not being used to route interesting traffic. Every time interesting traffic is routed out a DDR interface, the idle timer is reset. Therefore, traffic that is uninteresting will not keep a DDR call established.

The simple form of the `dialer-list` command specifies whether a whole protocol suite, such as IP or IPX, will be permitted to trigger a call. The more complex form of the `dialer-list` command references an access list. This allows finer control of the definition of interesting traffic.

Configure a simple dialer list using the following syntax:

```
Router(config)#dialer-list dialer-group-number protocol protocol-name  
{permit | deny }
```

The following example configures a dialer-list that will trigger a call for any IP traffic:

```
RTA(config)#dialer-list 1 protocol ip permit
```

The

access-list command specifies interesting traffic that initiates a DDR call. The dialer-list command is used with the access list:

```
Router(config)#access-list access-list-number [permit | deny] {protocol  
| protocol-keyword} {source source-wildcard | any} {destination  
destination-wildcard | any} [protocol-specific-options] [log]
```

```
Router(config)#dialer-list dialer-group list access-list-number
```

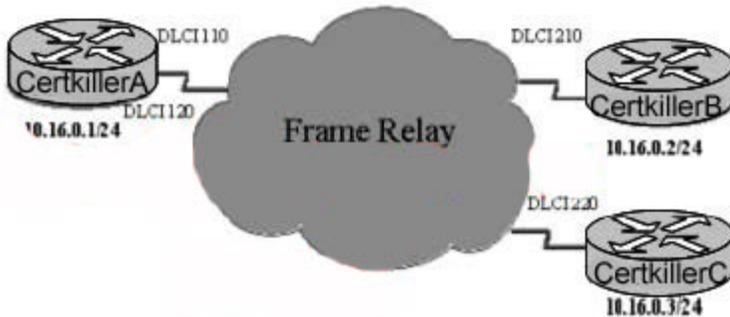
The following example configures an access list and a dialer list so that only traffic from one host is considered interesting:

```
Router(config)#access-list 24 permit host 192.168.1.2
```

```
Router(config)#dialer-list 1 list 24
```

QUESTION 450:

Exhibit:



Certkiller B is connected across a hub-and-spoke Frame Relay network to Certkiller A and a non-Cisco device, Certkiller C. Which statement is true in terms of configuring Certkiller B to communicate with Certkiller A and Certkiller C?

- A. A static map must be configured for both Certkiller A and Certkiller C.
- B. A static map must be configured for Certkiller A only.
- C. Inverse ARP can be used to map dynamically to Certkiller A, but a static map must be configured for Certkiller C.
- D. Inverse ARP can be used to map dynamically to both Certkiller A and Certkiller C.

Answer: A

Explanation:

When using dynamic address mapping, Inverse ARP requests a next-hop protocol address for each active PVC. Once the requesting router receives an Inverse ARP response, it updates its DLCI-to-Layer 3 address mapping table. Dynamic address mapping is enabled by default for all protocols enabled on a physical interface. If the Frame Relay environment supports LMI autosensing and Inverse ARP, dynamic address mapping takes place automatically. Therefore, no

static address mapping is required.

If the environment does not support LMI autosensing and Inverse ARP, a Frame Relay map must be manually configured. Use the frame-relay map command to configure static address mapping. Once a static map for a given DLCI is configured, Inverse ARP is disabled on that DLCI.

To configure a frame-relay static map use the following syntax.

```
Router(config-if)#frame-relay map protocol protocol-address dlci  
[broadcast] [ietf | cisco]
```

QUESTION 451:

Which three statements are true about the Point-to-Point Protocol (PPP) frame format? (Choose three.)

- A. Link Control Protocol (LCP) is a PPP component for establishing, configuring, and testing the data-link connection.
- B. Network Control Protocol (NCP) is a PPP component for establishing and configuring various network-layer protocols.
- C. PPP is the default encapsulation on serial interfaces of Cisco routers.
- D. The HDLC frame format is based on the PPP frame format.
- E. The NCP field supports such features as authentication, callback, compression, and MLPPP.
- F. Unlike the ISO HDLC frame, the PPP frame includes a protocol field and an LCP field.

Answer: A, B, F

Explanation:

PPP defines the Link Control Protocol (LCP). The job of the LCP is to establish, configure, and test the data-link connection. When hosts negotiate a PPP connection, they exchange LCP packets. These packets allow link partners to dynamically negotiate link options, including authentication, compression, and MLP. The protocol field is used to identify various Layer 3 protocols, such as IP or IPX. The LCP field allows for the following features:

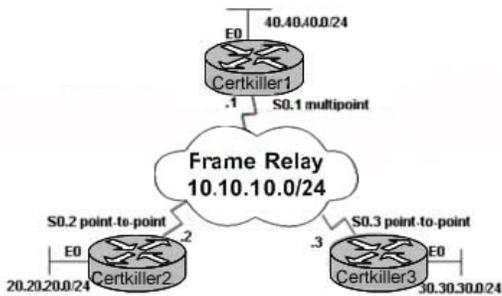
1. Authentication
2. Callback
3. Compression
4. Multilink PPP

Once the LCP establishes the Layer 2 connection, the Network Control Protocol (NCP) takes over. Link partners exchange NCP packets to establish and configure different network-layer protocols including IP, IPX, and AppleTalk. Each Layer 3 protocol has its own NCP. For example, IP's NCP is IPCP. IPX's NCP is IPXCP and Appletalk's NCP is ATALKCP.

The NCP can build up and tear down multiple Layer 3 protocol sessions over a single data link. This capability is called protocol multiplexing. When a host requests that the connection be terminated, the NCP tears down the Layer 3 sessions and then the LCP tears down the data link.

QUESTION 452:

Exhibit:



```

Certkiller2# show ip route
Gateway of last resort is not set
 20.20.20.0/24 is subnetted, 1 subnets
C    20.20.20.0 is directly connected, Ethernet0
R    40.0.0.0/8 [120/1] via 10.10.10.1, 00:00:11 Serial0.2
 10.10.10.0/24 is subnetted, 1 subnets
C    10.10.10.0 is directly connected, Serial0.2
Certkiller2#

```

Refer to the show ip route output of the exhibit. RIP is configured on Certkiller 1, Certkiller 2, and Certkiller 3. All three routers are able to ping each other. However, Certkiller 2 is not receiving the routes advertised by Certkiller 3. What can be done to resolve this problem?

- A. Configure frame-relay inverse-arp on the Certkiller 1 serial0.1 subinterface.
- B. Configure no frame-relay inverse-arp on the Certkiller 1 serial0.1 subinterface.
- C. Configure ip split-horizon on the Certkiller 1 serial0.1 subinterface.
- D. Configure no ip split-horizon on the Certkiller 1 serial0.1 subinterface.
- E. Configure ip split-horizon on the Certkiller 2 and Certkiller 3 serial0 interfaces.
- F. Configure no ip split-horizon on the Certkiller 2 and Certkiller 3 serial0 subinterfaces.

Answer: D

Explanation:

Normally, routers that are connected to broadcast-type IP networks and that use distance-vector routing protocols employ the split horizon mechanism to reduce the possibility of routing loops. Split horizon blocks information about routes from being advertised by a router out of any interface from which that information originated. This behavior usually optimizes communications among multiple routers, particularly when links are broken. However, with nonbroadcast networks (such as Frame Relay and Switched Multimegabit Digital System [SMDS]), situations can arise for which this behavior is less than ideal. For these situations, you might want to disable split horizon with IGRP and RIP.

Router(config-if)# ip split-horizon Enables split horizon.

Router(config-if)# no ip split-horizon Disables split horizon.

QUESTION 453:

Exhibit:

```
Certkiller2# sh frame-relay map
Serial0/1 (up): ip 192.168.12.1 dli 201(0xC9,0x3090), dynamic,
broadcast,, status defined, active
Certkiller2#
```

According to the show frame-relay map output provided in the exhibit, how was DLCI 201 mapped to 192.168.12.1?

- A. The mapping was created using the frame-relay map command.
- B. The mapping was created using the map-class frame-relay command.
- C. The mapping was created using the frame-relay interface-dlci command.
- D. The mapping was created via Inverse ARP.

Answer: D

LMI State can be:

The Frame Relay switch uses LMI to report the status of configured PVCs. The three possible PVC states are as follows:

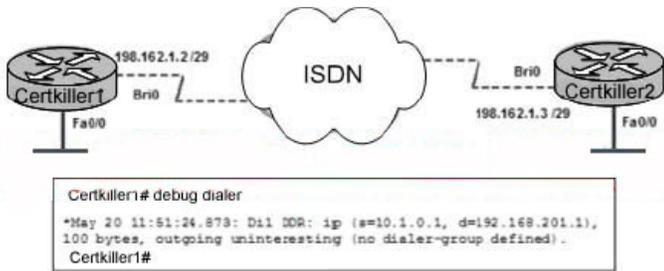
1. Active state- Indicates that the connection is active and that routers can exchange data.
2. Inactive state- Indicates that the local connection to the Frame Relay switch is working, but the remote router connection to the Frame Relay switch is not working.
3. Deleted state- Indicates that no LMI is being received from the Frame Relay switch, or that there is no service between the CPE router and Frame Relay switch.

DLCIs can be manually mapped to Layer 3 addresses on a router using the appropriate configuration commands. Building static maps can require a great deal of administrative overhead in complex networks and static maps cannot adapt to changes in the Frame Relay topology. Through the exchange of LMI, a Frame Relay switch may announce a new virtual circuit with its corresponding DLCI. Unfortunately, Layer 3 protocol addressing is not included in the announcement. The station receiving such an indication will learn of the new connection, but it will not be able to address the other side. Without a new configuration or a mechanism for discovering the protocol address of the other side, this new virtual circuit is unusable.

Inverse Address Resolution Protocol (Inverse ARP) was developed to provide a mechanism for dynamic DLCI to Layer 3 address maps. Inverse ARP works much the same way Address Resolution Protocol (ARP) works on a LAN. However, with ARP, the device knows the Layer 3 IP address and needs to know the remote data link MAC address. With Inverse ARP, the router knows the Layer 2 address which is the DLCI, but needs to know the remote Layer 3 IP address.

QUESTION 454:

Exhibit:



Refer to the exhibit. Given the output generated by the debug dialer command, what solution can be configured on Certkiller 1 to correct the problem?

- A. Configure a dialer-list in global configuration mode.
- B. Configure the dialer-group command on the dialer interface.
- C. Configure the dialer-group command on the BRI0 physical interface.
- D. Configure the dialer pool command on the dialer interface.
- E. Configure the dialer pool-member command on the dialer interface.
- F. Configure a local username entry for Certkiller 2

Answer: B

Explanation: In output, no dialer-group defined so needs to configure the dialer-group command on dialer interface.

Once the dialer list is created, it needs to be assigned to any interface responsible for initiating the call. This is accomplished by using the dialer-group command. The dialer group is referenced in the dialer-list command:

```

Router(config)#dialer-list 1 protocol ip permit
Router(config)#interface bri 0/0
Router(config-if)#dialer-group 1

```

QUESTION 455:

An administrator wants to configure authorization for any reverse Telnet connections. Which commands would complete this configuration?

```

Certkiller B(config)# radius-server host 192.168.1.23
Certkiller B(config)# radius-server key Certkiller
Certkiller B(config)# aaa new-model

```

- A. Certkiller B(config)# aaa authentication login AAA group radius local none
Certkiller B(config)# aaa authorization network AAA group radius local none
- B. Certkiller B(config)# aaa authentication login AAA group radius local none
Certkiller B(config)# aaa authorization reverse-access default group radius none
- C. Certkiller B(config)# aaa authorization reverse-access default group radius none
- D. Certkiller B(config)# aaa authentication login AAA group tacacs local none
Certkiller B(config)# aaa authorization reverse-access default group radius none

Answer: B

Explanation:

The `aaa authorization reverse-access` command configures authorization for reverse Telnet sessions. Users attempting to reverse Telnet from the router must be authorized to issue the command first by a RADIUS server.

QUESTION 456:

Which two features are enhancements that IKE provides for IPsec? (Choose two.)

- A. supports multicast traffic
- B. allows the changing of encryption keys during an IPsec session
- C. allows the SA to have a specified lifetime
- D. supports multiple protocols
- E. allows dynamic authentication of peers
- F. eliminates the need to manually specify all the IPsec security parameters in the crypto maps at both peers.

Answer: B,C

Explanation:

Internet Key Exchange (IKE) enhances IPsec by providing additional features, flexibility, and ease of configuration for the IPsec standard. IKE is a hybrid protocol that implements the Oakley key exchange and Skeme key exchange inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. ISAKMP, Oakley, and Skeme are security protocols implemented by IKE. IKE provides authentication of the IPsec peers, negotiates IPsec keys, and negotiates IPsec security associations.

IKE provides these benefits:

1. Eliminates the need to manually specify all the IPsec security parameters in the crypto maps at both peers.
 2. Allows the user to specify a lifetime for the IPsec security association.
 3. Allows encryption keys to change during IPsec sessions.
 4. Allows IPsec to provide anti-replay services.
 5. Permits certification authority (CA) support for a manageable, scalable IPsec implementation.
 6. Allows dynamic authentication of peers.
-

QUESTION 457:

Which feature describes the dialer fast-idle command?

- A. determines the amount of time an incoming call can remain idle before disconnecting
- B. determines the amount of time a DDR line can remain idle when another outgoing call needs to be placed
- C. causes an active DDR line to be disconnected immediately when idle
- D. determines the amount of time a DDR line can remain idle when another

incoming call needs to be answered

Answer: B

Explanation:

When the router is waiting to use a line to make another call, it uses a more aggressive idle timeout called fast-idle. The fast-idle time is the number of seconds that a line can remain idle before the current call is disconnected to allow another call that is waiting to use the line. The dialer fast-idle command can be used to alter this value. The default value is 20 seconds.

The following commands configure short timeout periods, which may be appropriate for expensive toll lines:

```
RTA(config-if)#dialer idle-timeout 60
```

```
RTA(config-if)#dialer fast-idle 15
```

QUESTION 458:

Exhibit:

```
7206# show policy-map interface atm 1/0.1
ATM1/0.1: VC 0/100--
  Service 100c1 output cowfg (1283)
    Class-map: A (match all) (1285/2)
      28621 packets, 7098008 bytes
      5 minute offered rate 10000 bps, drop rate 0 bps
      Match: access-group 101 (1289)
      Weighted Fair Queueing
        Output Queue: Conversation 73
        Bandwidth 500 (kbps) Max Threshold 64 (packets)
        (pkts matched/bytes matched) 28621/7098008
        (depth/total drops/no-buffer drops) 0/0/0
    Class-map: B (match-all) (1301/4)
      2058 packets, 148176 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group 103 (1305)
      Weighted Fair Queueing
        Output Queue: Conversation 75
        Bandwidth 50 (kbps) Max Threshold 64 (packets)
        (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0
    Class-map: class-default (match-any) (1309/0)
      10 packets 968 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any (1313)
```

Refer to the exhibit. In the output from the router 7206, what is the significance of the information, 28621 packets, 7098008 bytes?

- A. the number of packets that match the criteria of the class, whether the interface is congested or not congested
- B. the number of packets that match the criteria of the class when the interface was congested
- C. the number of packets using FIFO
- D. the number of packets, calculated every 30 seconds and averaged, which have been dropped in the last 5 minutes
- E. the number of packets using WRED
- F. the number of packets, calculated every 30 seconds and averaged, using LLQ

Answer: E

Explanation:

Weighted fair queuing overcomes an important limitation of FIFO queuing. Weighted fair queuing is an automated method that provides fair bandwidth allocation to all network traffic. Weighted fair queuing provides traffic priority management that dynamically sorts traffic into conversations, or flows. Weighted fair queuing then breaks up a stream of packets within each conversation to ensure that bandwidth is shared fairly between individual conversations. There are four types of weighted fair queuing: flow-based, distributed, class-based, and distributed class-based.

Weighted fair queuing (WFQ) is a flow-based algorithm that schedules delay-sensitive traffic to the front of a queue to reduce response time, and also shares the remaining bandwidth fairly among high-bandwidth flows. By breaking up packet trains, WFQ assures that low-volume traffic is transferred in a timely fashion. Weighted fair queuing gives low-volume traffic, such as Telnet sessions, priority over high-volume traffic, such as File Transfer Protocol (FTP) sessions. Weighted fair queuing gives concurrent file transfers balanced use of link capacity. Weighted fair queuing automatically adapts to changing network traffic conditions.

In Output the information, 28621 packets, 7098008 bytes is the number of WRED packets.

QUESTION 459:

Exhibit:

```
Access-6400# show atm pvc
VCD/      Peak Avg/Min Burst
Interface Name VPI VCI Type Escaps SC Kbps Kbps Cells Sts
0/0/0      2  0  16 PVC  ILMI  UBR 155000      UP
0/0/0.1    7  1  34 PVC-D SNAP UBR 155000      UP
0/0/0.4    8  4  33 PVC-D MUX  UBR 155000      UP
```

Refer to the exhibit. . Interface ATM0/0/0.4 pvc command, which statement about the configuration is true?

- A. Interface ATM0/0/0 is configured for PPP encapsulation
- B. Interface ATM0/0/0.1 is configured for PPP encapsulation.
- C. Interface ATM0/0/0.4 is configured for PPP encapsulation
- D. None of the interfaces are configured for PPP encapsulation

Answer: C

Explanation:

Here is an example of show interfaces command output:

```
Router#show interfaces atm 4/0 ATM4/0 is up, line protocol is up Hardware is
cxBus ATMInternet address is 131.108.97.165, subnet mask is 255.255.255.0MTU
4470 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255ATM E164
Auto Conversion InterfaceEncapsulation ATM, loopback not set, keepalive set (10
sec)Encapsulation(s): AAL5, PVC mode256 TX buffers, 256 RX buffers, 1024
Maximum VCs, 1 Current VCsSignalling vc = 1, vpi = 0, vci = 5ATM NSAP
```

address: BC.CDEF.01.234567.890A.BCDE.F012.3456.7890.1234.13Last input 0:00:05, output 0:00:05, output hang neverLast clearing of "show interface" counters neverOutput queue 0/40, 0 drops; input queue 0/75, 0 dropsFive minute input rate 0 bits/sec, 0 packets/secFive minute output rate 0 bits/sec, 0 packets/sec144 packets input, 31480 bytes, 0 no bufferReceived 0 broadcasts, 0 runts, 0 giants13 input errors, 12 CRC, 0 frame, 0 overrun, 1 ignored, 0 abort154 packets output, 4228 bytes, 0 underruns0 output errors, 0 collisions, 1 interface resets, 0 restartsIn Encapsulation field, encapsulation type is MUX it means ppp encapsulation. Go

http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_command_reference_chapter09186a00
more details.

QUESTION 460:

Exhibit:

```
827# show running-config
- output Omitted
interface Ethernet0
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast (default)
ip nat inside
!
interface ATM0
no ip address
no ip directed-broadcast (default)
ip nat outside
no atm ilmi-keepalive (default)
pvc 8/35
encapsulation aal5mux ppp dialer
dialer pool-member 1
!
bundle-enable
!
interface Dialer0
ip address negotiated
no ip directed-broadcast (default)
ip nat outside
encapsulation ppp
dialer pool 1
!
ip nat inside source list 1 interface Dialer0 overload
ip classless (default)
ip route 0.0.0.0 0.0.0.0 Dialer0 (default gateway)
!
access-list 1 permit 192.168.1.0 0.0.0.255
end
```

Refer to the exhibit. What is this configuration an example of?

- A. replacing a bridge or modem with an 800 series router
- B. dial backup and remote management for an 800 series rout
- C. PPP over ATM with NAT
- D. PPP over Ethernet with NAT
- E. PPP over Ethernet with NAT, using a dial-on-demand PPP-over-Ethernet connection
- F. PPP over ATM with centrally managed addressing and dial backup

Answer: E

Explanation:

ISPs often provide their customers with a DSL modem that has one Ethernet interface to connect to the customer Ethernet segment, and another interface for DSL line connectivity. In such a case, the DSL modem only acts as a bridge if the CPE is not configurable for any IP connectivity or enhanced features over DSL. This limits your connectivity to only one PPPoE Client PC. With the addition of a Cisco IOS router connected to the Ethernet of the DSL modem, you can run the PPPoE Client IOS feature on the Cisco router. This can connect multiple PCs on the Ethernet segment connected to the Cisco IOS router. With the use of the Cisco IOS router, you can enhance your DSL connectivities and all IOS features, such as Security, Network Address Translation (NAT) and Dynamic Host Configuration Protocol (DHCP) to internal hosts.

The PPPoE feature allows you to initiate a PPP session on a simple bridging Ethernet connected client. The session is transported over the ATM link via encapsulated Ethernet-bridged frames. You can terminate the session at either a local exchange carrier central office or an ISP point of presence. The given exhibit is the example of PPPOE configuration over NAT.

QUESTION 461:

Under which circumstance would use of Kerberos authentication system be required, instead of TACACS+ or RADIUS?

- A. Authentication, authorization and accounting need to use the a single database.
- B. Multiple levels of authorization need to be applied to various router commands.
- C. DES encrypted authentication is required.
- D. The usage of various router functions needs to be accounted for by user name.

Answer: C

Explanation:

Kerberos is a secret-key network authentication protocol used with AAA that uses the Data Encryption Standard (DES) cryptographic algorithm for encryption and authentication. Kerberos was designed to authenticate requests for network resources. Kerberos is based on the concept of a trusted third party that performs secure verification of users and services. The primary use of Kerberos is to verify that users and the network services they use are really who and what they claim to be. To accomplish this, a trusted Kerberos server issues tickets to users. These tickets, which have a limited lifespan, are stored in a user's credential cache. These tickets are then used in place of the standard username and password authentication mechanism.

QUESTION 462:

Which timer is reset to the maximum configured value every time an interesting packet is forwarded across the link?

- A. wait for carrier timer

- B. dialer idle timer
- C. dialer enable timer
- D. busy timer

Answer: B

Explanation:

Dialup connections are subject to an idle timer. The idle timer keeps track of how much time has elapsed since interesting traffic was routed out the interface. By default, the idle-timeout is set to 120 seconds. This value can be customized to make the timer more aggressive, or the timeout value can be increased to keep the connection up longer. To manually set the idle timeout value, use the dialer idle-timeout command.

Router(config-if)#dialer fast-idle seconds

QUESTION 463:

Which three statements are true about TCP/IP header compression? (Choose three.)

- A. It is a multiprotocol compression algorithm capable of also compressing AppleTalk and IPX/SPX headers.
- B. It keeps the Layer 2 header intact and can still travel across a WAN link.
- C. It subscribes to the Van Jacobson algorithm defined in RFC 1144.
- D. It subscribes to the Lempel-Ziv (LZ)-based compression-based algorithm defined in RFC 1149.
- E. To configure, use the compress tcp interface configuration command.
- F. To configure, use the ip tcp header-compression interface configuration command.

Answer: B, C, F

Explanation:

PPP can also maximize performance by using data compression, which may provide higher data throughput across low-speed links.

Compression is an option that is negotiated by LCP. So, if the party called is not configured for compression, no compression will take place. The best compression ratio is usually reached with text files. Some file formats, such as JPEG or MPEG, are already compressed. Also, applications such as Winzip and StuffIt can compress files before they are sent over the network. If a router applies a compression algorithm to a file that is already compressed, the result is a compression ratio of 1:1 or even less.

TCP header compression is also an option negotiated by LCP. The TCP header compression technique, often referred to by its creator's name, Van Jacobson, is described in RFC 1144. It is supported on serial lines that use HDLC, PPP, or SLIP encapsulation. TCP header compression must be entered on both ends of the connections for it to work. Only TCP headers are compressed, UDP headers are not affected. Header compression is particularly useful on networks with a large percentage of small packets, such as those supporting many Telnet connections.

Configure TCP header compression using the command:

```
ip tcp header-compression
```

Optionally, the `ip tcp header-compression passive` command specifies that TCP header compression is not required, but will be used if the router receives compressed headers from its link partner

QUESTION 464:

Which two statements are true about the use of the `backup load 65 10` command on a router? (Choose two.)

- A. The secondary line will terminate when the load of the primary line drops to 10% of the bandwidth of the primary line.
- B. The secondary line will terminate when the aggregate load of the primary and backup lines drops to 10% of the primary line bandwidth.
- C. The secondary line will come up 10 seconds after traffic on the primary line reaches 65% of the bandwidth of the primary line.
- D. The secondary line will come up when the traffic on the primary line reaches 65% of the bandwidth of the primary line.
- E. The backup interface will come up 65 seconds after the primary link goes down.
- F. The secondary interface will terminate the connection 10 seconds after the primary link comes up.

Answer: B,D

Explanation:

A backup interface can be configured to activate the secondary link based on the traffic load on the primary link. The IOS monitors the traffic load and computes the percentage of utilization on the link. This calculation is based on a five-minute average, and it is computed every 5 seconds. To configure a backup for when the primary line reaches or exceeds a certain threshold, perform the following steps on one side of the connection only:

4. Select the primary interface:

```
Router(config)#interface interface-type slot/port
```

5. Use the following command on the primary interface to specify the backup to be used if a dial backup is needed:

```
Router(config-if)#backup interface interface-type slot/port
```

or

```
Router(config-if)#backup interface dialer number
```

6. To set the traffic load threshold for dial backup service, use the following command syntax:

```
Router(config-if)#backup load {enable-threshold | never} {disable-load | never}
```

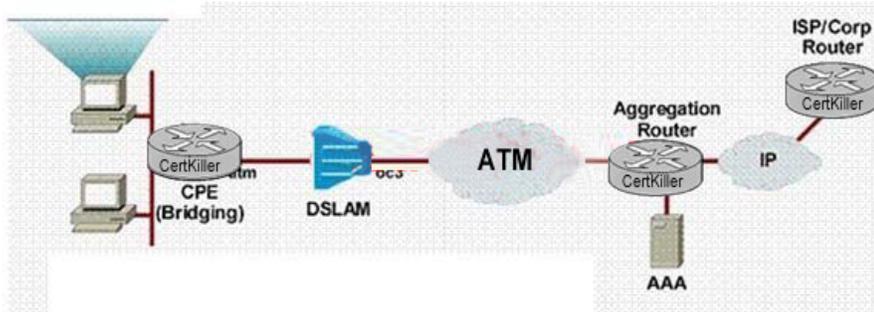
The secondary line is brought down when one of the following conditions occur:

1. The transmitted load on the primary line plus the transmitted load on the secondary line is less than the value entered for the `disable-load` argument.

The received load on the primary line plus the received load on the secondary line is less than the value entered for the `disable-load` argument.

QUESTION 465:

Exhibit:



Refer to the exhibit. Which two statements are true about the broadband technology that is depicted in the exhibit? (Choose two.)

- A. The exhibit is an example of PPPoA
- B. The exhibit is an example of PPPoE.
- C. The exhibit is an example of RFC 1483/2684 bridging.
- D. The PPP session is established between the CPE and the aggregation router.
- E. The PPP session is established between the end-user PC and the aggregation router.
- F. Because the CPE acts as a set-top box, the exhibited technology is ideal for single-user Internet access.

Answer: B,E

Explanation:

ISPs often provide their customers with a DSL modem that has one Ethernet interface to connect to the customer Ethernet segment, and another interface for DSL line connectivity. In such a case, the DSL modem only acts as a bridge if the CPE is not configurable for any IP connectivity or enhanced features over DSL. This limits your connectivity to only one PPPoE Client PC. With the addition of a Cisco IOS router connected to the Ethernet of the DSL modem, you can run the PPPoE Client IOS feature on the Cisco router. This can connect multiple PCs on the Ethernet segment connected to the Cisco IOS router. With the use of the Cisco IOS router, you can enhance your DSL connectivities and all IOS features, such as Security, Network Address Translation (NAT) and Dynamic Host Configuration Protocol (DHCP) to internal hosts.

The PPPoE feature allows you to initiate a PPP session on a simple bridging Ethernet connected client. The session is transported over the ATM link via encapsulated Ethernet-bridged frames. You can terminate the session at either a local exchange carrier central office or an ISP point of presence. The given exhibit is the example of PPPOE configuration over NAT.

QUESTION 466:

Exhibit:

```
Router# show frame relay pvc
PVC Statistics for interface is dial (Frame Relay DCE)

DLCI = 22, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial3/1:1.1
for interface is dial (Frame Relay)
input pkts 9 output pkts 300008 in bytes 2754
out bytes 161802283 dropped pkts 0 in FECN pkts 0
in BECN pkts 1 out FECN pkts 0 out BECN pkts 0
in DE pkts 0 out DE pkts 0
outbcast pkts 0 outbcast bytes 0
Shaping adapts to Foresight in Foresight signals 1304
pvc create time 1d05h, last time pvc status changed 00:11:00
```

Refer to the exhibit. Which statement is true about the show frame-relay pvc output?

- A. Traffic shaping is enabled.
- B. The remote connection is not working correctly.
- C. The local connection is not working correctly
- D. LMIs are not being received

Answer: B

Explanation: See the output and explanation

The following is sample output from the show frame-relay pvc command:

```
Router# show frame-relay pvc PVC Statistics for interface Serial (Frame Relay
DCE)DLCI = 22, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE,
INTERFACE = Serial3/1:1.1input pkts 9 output pkts 300008 in bytes 2754out
bytes 161802283 dropped pkts 0 in FECN pkts 0in BECN pkts 1 out FECN pkts
0 out BECN pkts 0in DE pkts 0 out DE pkts 0outbcast pkts 0 outbcast bytes 0
Shaping adapts to ForeSight in ForeSight signals 1304 pvc create time 1d05h, last
time pvc status changed 00:11:00If the circuit is configured for shaping to adapt to
BECN, it is indicated in the display:
```

Shaping adapts to BECNIf traffic shaping on the circuit does not adapt to either BECN or ForeSight, nothing extra shows:

```
DLCI = 100, DLCI USAGE = SWITCHED, PVC STATUS = ACTIVEinput pkts 0
output pkts 0 in bytes 0out bytes 0 dropped pkts 0 in FECN pkts 0in BECN pkts
0 out FECN pkts 0 out BECN pkts 0in DE pkts 0 out DE pkts 0outbcast pkts 0
outbcast bytes 0pvc create time 0:03:03 last time pvc status changed 0:03:03 Num
Pkts Switched 0Multipoint Subinterfaces Example
```

The following is sample output from the show frame-relay pvc command for multipoint subinterfaces. The output displays both the subinterface number and the DLCI. This display is the same whether the PVC is configured for static or dynamic addressing.

```
DLCI = 300, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE =
Serial0.103input pkts 10 output pkts 7 in bytes 6222out bytes 6034 dropped pkts
0 in FECN pkts 0in BECN pkts 0 out FECN pkts 0 out BECN pkts 0in DE pkts 0
out DE pkts 0outbcast pkts 0 outbcast bytes 0pvc create time 0:13:11 last time pvc
status changed 0:11:46DLCI = 400, DLCI USAGE = LOCAL, PVC STATUS =
ACTIVE, INTERFACE = Serial0.104input pkts 20 output pkts 8 in bytes 5624out
bytes 5222 dropped pkts 0 in FECN pkts 0in BECN pkts 0 out FECN pkts 0 out
```

BECN pkts 0 in DE pkts 0 out DE pkts 0 outcast pkts 0 outcast bytes 0 pvc create time 0:03:57 last time pvc status changed 0:03:48 Table 2 describes the fields shown in the displays.

Table 2 show frame-relay pvc Field Descriptions	
Field	Description
DLCI	One of the DLCI numbers for the PVC.
DLCI USAGE	Lists SWITCHED when the router or access server is used as a switch, or LOCAL when the router or access server is used as a DTE.
PVC STATUS	<p>Status of the PVC. The DCE device reports the status, and the DTE device receives the status. When you disable the Local Management Interface (LMI) mechanism on the interface (by using the no keepalive command), the PVC status is STATIC. Otherwise, the PVC status is exchanged using the LMI protocol:</p> <ul style="list-style-type: none"> • STATIC—LMI is disabled on the interface. • ACTIVE— The PVC is operational and can transmit packets. • INACTIVE—The PVC is configured, but down. • DELETED—The PVC is not present (DTE device only), which means that no status is received from the LMI protocol. <p>If the frame-relay end-to-end keepalive command is used, the end-to-end keepalive (EEK) status is reported in addition to the LMI status. For example:</p> <ul style="list-style-type: none"> • ACTIVE (EEK UP) —The PVC is operational according to LMI and end-to-end keepalives. • ACTIVE (EEK DOWN)—The PVC is operational according to LMI, but end-to-end keepalive has failed.
INTERFACE = Serial0.103	Specific subinterface associated with this DLCI.
input pkts	Number of packets received on this PVC.
output pkts	Number of packets sent on this PVC.

in bytes	Number of bytes received.
out bytes	Number of bytes sent.
dropped pkts	Number of packets dropped by the router at Frame Relay level because an active outbound DLCI was not found.
in FECN pkts	Number of packets received with the FECN bit set.
in BECN pkts	Number of packets received with the BECN bit set.
out FECN pkts	Number of packets sent with the FECN bit set.
out BECN pkts	Number of packets sent with the BECN bit set.
in DE pkts	Number of DE packets received.
out DE pkts	Number of DE packets sent.
outcast pkts	Number of output broadcast packets.
outcast bytes	Number of output broadcast bytes.
pvc create time	Time the PVC was created.
last time pvc status changed	Time the PVC changed status (active to inactive).
Num Pkts Switched	Number of packets switched within the router or access server; this PVC is the source PVC.

Reference from:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s12/12sfrsdg>

QUESTION 467:

Which traffic queuing method gives a low-volume traffic stream preferential service?

- A. FIFO
- B. Priority
- C. Custom
- D. Weighted Fair
- E. Low Latency

Answer: A

Explanation:

When FIFO queuing is in effect, traffic is transmitted in the order received without regard for bandwidth consumption or the associated delays. File transfers and other high-volume network

applications often generate series of packets of associated data known as packet trains. Packet trains are groups of packets that tend to move together through the network. These packet trains can consume all available bandwidth, and other traffic flows back up behind them.

Weighted fair queuing overcomes an important limitation of FIFO queuing. Weighted fair queuing is an automated method that provides fair bandwidth allocation to all network traffic. Weighted fair queuing provides traffic priority management that dynamically sorts traffic into conversations, or flows. Weighted fair queuing then breaks up a stream of packets within each conversation to ensure that bandwidth is shared fairly between individual conversations. There are four types of weighted fair queuing: flow-based, distributed, class-based, and distributed class-based.

QUESTION 468:

Which two commands will verify an ISDN circuit from end to end? (Choose two.)

- A. show isdn status
- B. debug isdn q931
- C. debug dialer
- D. debug isdn q921
- E. debug serial interface

Answer: A,B

Explanation:

At Layer 3, the B channel can carry datagrams using a variety of Layer 3 protocols, including IP, IPX, and AppleTalk. The D-channel uses the Q.931 at Layer 3. Q.931 is used to communicate between an ISDN switch of a carrier and a customer TE device such as a router.

The show isdn status command is especially useful when trying to track down the root of an ISDN connectivity problem.

The debug isdn q921 command is useful to observe signaling events between the router and the ISDN switch

QUESTION 469:

What happens when Inverse ARP creates a Frame Relay mapping and the command frame-relay map ip 10.10.1.1 201 broadcast is entered on the router?

- A. Upon a reboot, Inverse ARP is disabled for all DLCIs.
- B. Upon a reboot, the static mapping is used if Inverse ARP fails.
- C. Upon entering the static mapping, Inverse ARP will be disabled.
- D. The static mapping will only be used as a backup to Inverse ARP
- E. Upon a reboot, Inverse ARP will be disabled for DLCI 201 only.

Answer: C

Explanation:

DLCIs can be manually mapped to Layer 3 addresses on a router using the appropriate

configuration commands. Building static maps can require a great deal of administrative overhead in complex networks and static maps cannot adapt to changes in the Frame Relay topology. Through the exchange of LMI, a Frame Relay switch may announce a new virtual circuit with its corresponding DLCI. Unfortunately, Layer 3 protocol addressing is not included in the announcement. The station receiving such an indication will learn of the new connection, but it will not be able to address the other side. Without a new configuration or a mechanism for discovering the protocol address of the other side, this new virtual circuit is unusable.

Inverse Address Resolution Protocol (Inverse ARP) was developed to provide a mechanism for dynamic DLCI to Layer 3 address maps. Inverse ARP works much the same way Address Resolution Protocol (ARP) works on a LAN. However, with ARP, the device knows the Layer 3 IP address and needs to know the remote data link MAC address. With Inverse ARP, the router knows the Layer 2 address which is the DLCI, but needs to know the remote Layer 3 IP address.

When using dynamic address mapping, Inverse ARP requests a next-hop protocol address for each active PVC. Once the requesting router receives an Inverse ARP response, it updates its DLCI-to-Layer 3 address mapping table. Dynamic address mapping is enabled by default for all protocols enabled on a physical interface. If the Frame Relay environment supports LMI autosensing and Inverse ARP, dynamic address mapping takes place automatically. Therefore, no static address mapping is required.

If the environment does not support LMI autosensing and Inverse ARP, a Frame Relay map must be manually configured. Use the frame-relay map command to configure static address mapping. Once a static map for a given DLCI is configured, Inverse ARP is disabled on that DLCI.

QUESTION 470:

Exhibit:

```
CertKiller1# show crypto isakmp sa
dst          Sre          state        conn-id      slot
10.1.1.2     10.1.1.1    MM_NO_STATE  1            0
```

You are a network technician for Certkiller .com. Study the exhibit carefully. You are troubleshooting an IPsec tunnel between Certkiller 1 and Certkiller 2. You issue the command `crypto isakmap sa` command. What is the cause of the problem?

- A. Certkiller 1 is using the incorrect address as its identity
- B. Certkiller 2 is using the incorrect address as its identity
- C. Phase 1 attributes do not match between peers.
- D. Phase 2 attributes do not match between peers.
- E. The crypto map is applied to the wrong interface

Answer: E

Explanation:

Show crypto isakmp sa commands display all current Internet Key Exchange (IKE) security associations (SAs) at a peer.

States in Main Mode Exchange

State	Explanation
MM_NO_STATE	The ISAKMP SA has been created, but nothing else has happened yet. It is "larval" at this stage-there is no state.
MM_SA_SETUP	The peers have agreed on parameters for the ISAKMP SA.
MM_KEY_EXCH	The peers have exchanged Diffie-Hellman public keys and have generated a shared secret. The ISAKMP SA remains unauthenticated.
MM_KEY_AUTH	The ISAKMP SA has been authenticated. If the router initiated this exchange, this state transitions immediately to QM_IDLE, and a Quick Mode exchange begins.

QUESTION 471:

Exhibit:

```
CertKiller1# show running-config interface Serial0
!
interface Serial0
 backup delay 10 30
 backup interface Dialer1
 ip address 192.168.10.2.255.255.255.252
 encapsulation ppp
 no fair-queue
 clockrate 64000
 ppp authentication chap
```

You are a network technician for Certkiller .com. Study the exhibit carefully. Which two backup delay statements are true? Select two.

- A. Interface Dialer1 will be activated 30 seconds after interface Serial0 is restored.
- B. Interface Dialer1 will be deactivated 30 seconds after interface Serial0 is restored.
- C. Interface Dialer1 will be activated 10 seconds after interface Serial0 goes down.
- D. Interface Dialer1 will be deactivated 10 seconds after interface Serial0 goes down.

- E. Interface Dialer 1 will be activated if there is interesting traffic after 10 seconds.
- F. Interface Dialer 1 will be activated if there is no interesting traffic after 30 seconds.

Answer: B,C

Explanation:

backup delay :To define how much time should elapse before a secondary line status changes after a primary line status has changed, use the backup delay interface configuration command. To return to the default, so that as soon as the primary fails, the secondary is immediately brought up without delay, use the no form of this command.

backup delay {enable-delay | never} {disable-delay | never}
no backup delay {enable-delay | never} {disable-delay | never}
Syntax Description

enable-delay	Number of seconds that elapse after the primary line goes down before the Cisco IOS software activates the secondary line.
disable-delay	Number of seconds that elapse after the primary line comes up before the Cisco IOS software deactivates the secondary line.
Never	Prevents the secondary line from being activated or deactivated.

QUESTION 472:

Your boss at Certkiller , Mrs Certkiller, wants to define a rotary group. Which command should she use?

- A. dialer rotary-group
- B. dialer pool
- C. interface dialer
- D. interface rotary
- E. interface rotary

Answer: A

Explanation:

DDR rotary groups and dialer profiles are used to further define and optimize traffic queues. Rotary groups allow inherited configuration of physical interfaces by applying a logical interface configuration, and "this rotary group" can be used for

outgoing calls. A hunt group is a series of telephone lines that are programmed to find the next "free line" when a call is received.

Rotary groups are configured with the IOS commands interface dialer group-number and dialer rotary-group rotary-number. To troubleshoot rotary groups and dialer profiles you would use show dialer interface bri..

QUESTION 473:

Exhibit

```
interface Serial1/0
  encapsulation frame-relay
  no frame-relay inverse-arp
  frame-relay lmi-type cisco

interface Serial1/0.123 multipoint
  ip address 172.16.123.1 255.255.255.128
  frame-relay map ip 172.16.123.1 103
  frame-relay map ip 172.16.123.2 102
  frame-relay map ip 172.16.123.3 103 broadcast
  no frame-relay inverse-arp
  no ip split-horizon
```

You are a network technician for Certkiller .com. Study the exhibit carefully.

Why was the following command used?

no frame-relay inverse-arp

- A. to allow the creation of dynamic address maps
- B. to prevent the creation of dynamic address maps
- C. to prevent serial interfaces from borrowing the MAC address of each other
- D. to prevent Ethernet interfaces from borrowing the MAC address of serial interfaces
- E. to allow routing between the two hub routers
- F. to prevent routing between the two hub routers

Answer: B

Explanation:

DLCIs can be manually mapped to Layer 3 addresses on a router using the appropriate configuration commands. Building static maps can require a great deal of administrative overhead in complex networks and static maps can't adapt to changes in the Frame Relay topology.

Inverse ARP was developed to provide a mechanism for dynamic DLCI to Layer 3 address maps.

You can enable Inverse ARP using:

frame-relay inverse-arp

You can disable:
no frame-relay inverse-arp

QUESTION 474:

You are a Cisco Certified Engineer. You are configuring a remote access solution. Which of the following are the necessary interface configuration tasks for ISDN BRI (Choose all that apply)?

- A. Assign the interface type as BRI.
- B. Specify static routes to remote ISDN locations.
- C. Specify the ISDN provider's switch type.
- D. Assign the interface to a dialer group.
- E. Specify routing protocol used
- F. Specify dynamic routes to remote ISDN locations.

Answer: C, D

Explanation:

According to Cisco: To configure the dialer interface that will be used as an intermediary between a physical interface that will function as backup interface and the interfaces that will use the backup, use the following commands beginning in global configuration mode:

Step	Command	Purpose
1	interface dialer number	Create a dialer interface.
2	ip unnumbered loopback0	Specify IP unnumbered loopback.
3	encapsulation ppp	Specify PPP encapsulation.
4	dialer remote-name username	Specify the remote router's CHAP authentication name.
5	dialer string dial-string	Specify the remote destination to call.
6	dialer pool number	Specify the dialing pool to use for calls to this destination.
7	dialer-group group-number	Assign the dialer interface to a dialer group.

QUESTION 475:

ISDN PRI in Australia provides ____ B channels plus _____ D channels.

- A. 15,1
- B. 24, 1
- C. 32, 1
- D. 30, 1
- E. 24, 2

Answer: D

Explanation:

According to the technical documentation at CCO:

ISDN Primary Rate Interface (PRI) service offers 23 B channels and 1 D channel in

North America and Japan, yielding a total bit rate of 1.544 Mbps (the PRI D channel runs at 64 kbps). ISDN PRI in Europe, Australia, and other parts of the world provides 30 B channels plus one 64-kbps D channel and a total interface rate of 2.048 Mbps. The PRI physical layer specification is ITU-T I.431.

QUESTION 476:

You are a Cisco Certified Engineer. You are configuring a remote access solution. You may configure PPP on which of the following types of physical interfaces (Choose all that apply):

- A. Synchronous serial
- B. HSSI
- C. Asynchronous serial
- D. ISDN

Answer: A, B, C, D

Explanation:

According to Cisco: PPP, described in RFC 1661, encapsulates network layer protocol information over point-to-point links. You can configure PPP on the following types of physical interfaces:

- Asynchronous serial
- HSSI
- ISDN
- Synchronous serial

By enabling PPP encapsulation on physical interfaces, PPP can also be in effect on calls placed by the dialer interfaces that use the physical interfaces.

QUESTION 477:

You want your router to be able to dynamically fluctuate at the rate at which it sends packets, depending on the BECNs it receives. What command will you use for this?

- A. frame-relay shaping becn
- B. frame-relay adaptive becn
- C. frame-relay adaptive-shaping becn
- D. frame-relay becn adaptive-shaping

Answer: C

Explanation:

According to Cisco: This command replaces the frame-relay becn-response-enable command, which will be removed in a future Cisco IOS release.

QUESTION 478:

You are a Cisco Certified Engineer. You are configuring a remote access solution. Which of the following parameters are set using the line command (Choose all that apply)?

- A. Speed
- B. Encapsulation protocol
- C. Compression ratio
- D. Authentication method
- E. Flow control
- F. IP address
- G. Speed units

Answer: A, E

Explanation:

According to Cisco: Line configuration commands modify the operation of a terminal line. Line configuration commands always follow a line command, which defines a line number. These commands are used to change terminal parameter settings line-by-line or a range of lines. More information can be found at: [QUESTION](#)

QUESTION 479:

Which of the following are valid functions that chat scripts perform (Choose all that apply)?

- A. modem configuration
- B. dialing and remote login
- C. failure detection
- D. incoming call filtering

Answer: A, B, C

Explanation:

According to Cisco: Chat scripts are strings of text used to send commands for modem dialing, logging onto remote systems, and initializing asynchronous devices connected to an asynchronous line. On a router, chat scripts can be configured on the auxiliary port only. A chat script must be configured to dial out on asynchronous lines. You also can configure chat scripts so that they are executed automatically for other specific events on a line, or so that they are executed manually. Each chat script is defined for a different event.

QUESTION 480:

When configuring X.25 to use a PVC, why is it important for you to ensure that no

traffic is sent toward your remote terminal server between the time the x25 map command is issued and the time that x25 pvc command is issued?

- A. an switched virtual circuit will be produced instead
- B. all X25 traffic will be temporarily buffered in queue in a hold state
- C. a PVC will be produced but will be locked up
- D. all X25 traffic will be blocked
- E. None of the choices.

Answer: A

Explanation:

According to the technical documentation at CCO:

When configuring X.25 to use a PVC, you must ensure that no traffic is sent toward a remote terminal server between the time the x25 map command is issued and the time that x25 pvc command is issued. Otherwise, the local system will create an switched virtual circuit (SVC), and then the PVC command will not be allowed. Map entries with the broadcast attribute are particularly likely to get traffic, due to routing protocol traffic. The simplest way to ensure that no traffic is sent while configuring is to shut down the interface while configuring it for a PVC.

QUESTION 481:

You are a Cisco Certified Engineer. You are configuring an ISDN remote access solution. With ISDN, non-ISDN terminals are referred to as:

- A. LE
- B. NT1
- C. TE1
- D. LE2
- E. LA
- F. TE2

Answer: F

Explanation:

According to Cisco: ISDN components include terminals, terminal adapters (TAs), network-termination devices, line-termination equipment, and exchange-termination equipment. ISDN terminals come in two types. Specialized ISDN terminals are referred to as terminal equipment type 1 (TE1). Non-ISDN terminals, such as DTE, that predate the ISDN standards are referred to as terminal equipment type 2 (TE2). TE1s connect to the ISDN network through a four-wire, twisted-pair digital link. TE2s connect to the ISDN network through a T

A. The ISDN TA can be either a standalone device or a board inside the TE2. If the TE2 is implemented as a standalone device, it connects to the TA

via a standard physical-layer interface. Examples include EIA/TIA-232-C (formerly RS-232-C), V.24, and V.35.

QUESTION 482:

What command should you use to specify RADIUS as the method of user authentication when no other method list has been defined (fill in the blank):

Answer: aaa authentication ppp default radius

Explanation:

According to the technical documentation at CCO:

Use the aaa authentication ppp command with the radius method keyword to specify RADIUS as the authentication method for use on interfaces running PPP. Before you can use RADIUS as the authentication method, you need to enable communication with the RADIUS security server.

QUESTION 483:

By directly connecting to the ISDN NT1 device, the router has more control over ISDN parameters in Europe.

- A. True
- B. False
- C. True only for BRI
- D. None of the choices.
- E. True only for PRI

Answer: B

Explanation:

According to the technical documentation at CCO:

The native ISDN interface on the Cisco 2503 router allows the router to be directly connected to an ISDN NT1 device. In many countries, the NT1 is provided by the telephone company. In the United States, however, the NT1 is customer-owned equipment. By directly connecting to the ISDN network, the router has more direct control over ISDN parameters and has access to ISDN information.

QUESTION 484:

What command should you use to display the current X25 virtual circuit parameters and statistics (fill in the blank):

Answer: show x25 vc

Explanation:

According to the technical documentation at CCO:

The terminal server provides EXEC show commands to provide information on interface operation and virtual circuit operation. Use the EXEC command show interfaces to display interface parameters and statistics. Use the EXEC command show x25 vc to display virtual circuit parameters and statistics.

QUESTION 485:

You are a Cisco Certified Engineer. You are configuring an ISDN remote access solution. With ISDN, specialized ISDN terminals are NOT being referred to as (Choose all that apply):

- A. LE
- B. NT1
- C. TA
- D. TE1
- E. TE3
- F. LA

Answer: A, B, C, E, F

Explanation:

According to Cisco: ISDN components include terminals, terminal adapters (TAs), network-termination devices, line-termination equipment, and exchange-termination equipment. ISDN terminals come in two types. Specialized ISDN terminals are referred to as terminal equipment type 1 (TE1). Non-ISDN terminals, such as DTE, that predate the ISDN standards are referred to as terminal equipment type 2 (TE2). TE1s connect to the ISDN network through a four-wire, twisted-pair digital link. TE2s connect to the ISDN network through a T

A. The ISDN TA can be either a standalone device or a board inside the TE2. If the TE2 is implemented as a standalone device, it connects to the TA via a standard physical-layer interface. Examples include EIA/TIA-232-C (formerly RS-232-C), V.24, and V.35.

QUESTION 486:

You are a Cisco Certified Engineer. You are configuring a remote access solution. You plan to use CiscoSecure. Which of the following are the three major components of Cisco Secure (Choose all that apply)?

- A. L2TP
- B. RDBMS
- C. Packet filter firewall
- D. Netscape Fast Track Server
- E. AAA Server
- F. Track Server

Answer: B, D, E

Explanation:

RDBMS synchronization import definitions are a listing of the action codes allowable in an accountActions table. The RDBMS Synchronization feature of CiscoSecure AccessControlServer (ACS) for WindowsServer uses a table named "accountActions" as input for automated or manual updates of the CiscoSecure user database.

According to Cisco: CiscoSecure supports both Cisco network access servers (such as the Cisco 2509, 2511, 3620, 3640, and AS5200) and the PIX firewall. It is a basic access control server (ACS) for Windows NT Server Version 4.0. CiscoSecure uses the Terminal Access Controller Access Control System (TACACS)+ protocol to provide Authentication, Authorization, and Accounting (AAA) to ensure a secure environment. This enables you to control access to your network from a central location.

QUESTION 487:

Under PAT, packets destined for the outside world have their private IP address plus port number translated to the router's external IP address _____ the IP packet is forwarded to the WAN.

- A. None of the choices.
- B. port number should not be included in the equation
- C. port number should not be included in the translation, but should be forwarded
- D. before
- E. after

Answer: D

Explanation:

According to the technical documentation at CCO: Packets destined for an external address have their private IP address plus port number translated to the router's external IP address before the IP packet is forwarded to the WAN. IP packets returning to the router have their external IP addresses (plus port number) translated back to the private IP addresses, and the packets are forwarded to the LAN.

QUESTION 488:

You are a Cisco Certified Engineer. You are configuring a remote access solution. Which of the following are QoS Traffic shaping tools provided by Cisco (Choose 2)?

- A. BECN
- B. RSVP
- C. FECN
- D. GTS
- E. FRTS

F. DE

Answer: D, E

Explanation:

According to Cisco: Cisco's QoS software solutions include two traffic shaping tools---generic traffic shaping (GTS) and Frame Relay traffic shaping (FRTS)---to manage traffic and congestion on the network. GTS provides a mechanism to control the traffic flow on a particular interface. It reduces outbound traffic flow to avoid congestion by constraining specified traffic to a particular bit rate (also known as the token bucket approach), while queuing bursts of the specified traffic. FRTS provides parameters that are useful for managing network traffic congestion. These include committed information rate (CIR), FECN and BECN, and the DE bit. For some time, Cisco has provided support for FECN for DECnet, BECN for SNA traffic using direct LLC2 encapsulation via RFC 1490, and DE bit support. The FRTS feature builds on this Frame Relay support with additional capabilities that improve the scalability and performance of a Frame Relay network, increasing the density of virtual circuits and improving response time. More information can be found at: [this site](#)

QUESTION 489:

You are a Cisco Certified Engineer. You are configuring an ISDN remote access solution. In ISDN, ITU-T I.450 belongs to which layer?

- A. Layer 1
- B. Layer 4
- C. Layer 3
- D. Layer 2

Answer: C

Explanation:

According to Cisco: Two Layer 3 specifications are used for ISDN signaling: ITU-T (formerly CCITT) I.450 (also known as ITU-T Q.930) and ITU-T I.451 (also known as ITU-T Q.931). Together, these protocols support user-to-user, circuit-switched, and packet-switched connections. A variety of call-establishment, call-termination, information, and miscellaneous messages are specified, including SETUP, CONNECT, RELEASE, USER INFORMATION, CANCEL, STATUS, and DISCONNECT. These messages are functionally similar to those provided by the X.25 protocol.

QUESTION 490:

You are a Cisco Certified Engineer. You are configuring a remote access solution. Your company wants to connect its US office via ISDN to its European Headquarters. The US office uses T1. Which of the following types of line should be ordered for the European office?

- A. STM-0
- B. E1
- C. OC-1
- D. DS2
- E. STM-1
- F. T3
- G. STM-2

Answer: B

Explanation:

E1 is the European version of T1. It offers 2MB/Sec throughput. According to [webopedia.com](#): Similar to the North American T-1, E1 is the European format for digital transmission. E1 carries signals at 2 Mbps (32 channels at 64Kbps), versus the T1, which carries signals at 1.544 Mbps (24 channels at 64Kbps). E1 and T1 lines may be interconnected for international use.

QUESTION 491:

You are a Cisco Certified Engineer. You are configuring a remote access solution. In New York, which of the following ISDN functional groups is provided by the end user device?

- A. NT1
- B. NT3
- C. TE2
- D. TE3
- E. LE2
- F. TA
- G. LE

Answer: A

Explanation:

According to Cisco: Beyond the TE1 and TE2 devices, the next connection point in the ISDN network is the network termination type 1 (NT1) or network termination type 2 (NT2) device. These are network-termination devices that connect the four-wire subscriber wiring to the conventional two-wire local loop. In North America, the NT1 is a customer premises equipment (CPE) device. In most other parts of the world, the NT1 is part of the network provided by the carrier. The NT2 is a more complicated device that typically is found in digital private branch exchanges (PBXs) and that performs Layer 2 and 3 protocol functions and concentration services. An NT1/2 device also exists as a single device that combines the functions of an NT1 and an NT2.

QUESTION 492:

X.21bis is a _____ layer protocol.

- A. session
- B. network
- C. physical
- D. None of the choices.
- E. data link
- F. transport

Answer: C

Explanation:

According to the technical documentation at CCO: X.21bis is a physical layer protocol used in X.25 that defines the electrical and mechanical procedures for using the physical medium. X.21bis handles the activation and deactivation of the physical medium connecting DTE and DCE devices. It supports point-to-point connections, speeds up to 19.2 kbps, and synchronous, full-duplex transmission over four-wire media.

QUESTION 493:

Refer to the exhibit: *** MISSING ***

What type of ATM cable connector is it:

- A. SC
- B. FSD
- C. MIC
- D. ST

Answer: D

Explanation:

According to the technical documentation at CCO:

ST - round, bayonet, or twistlock coupling connector.

SC - push/pull coupling connector similar to ST connector except for a more square form.

FSD (also called MIC) - fixed shroud duplex system is specified for FDDI interface.

Because TAXI is 100 Mbps derived from the physical media FDDI, it was kept the same for ATM TAXI mode.

BNC - standard connector used to connect IEEE 802.3 10Base2 coaxial cable to a transceiver.

RJ-45 - standard 8-wire connector for IEEE 802.3 StarLAN networks. Used also as a telephone line in some cases.

QUESTION 494:

Which of the following ISDN reference points are not relevant only in North America (Choose all that apply)?

- A. R
- B. U
- C. S
- D. T

Answer: A, C, D

Explanation:

According to the technical documentation at CCO:

ISDN specifies a number of reference points that define logical interfaces between functional groups, such as TAs and NT1s. ISDN reference points include the following:

R-The reference point between non-ISDN equipment and a TA.

S-The reference point between user terminals and the NT2.

T-The reference point between NT1 and NT2 devices.

U-The reference point between NT1 devices and line-termination equipment in the carrier network. The U reference point is relevant only in North America, where the NT1 function is not provided by the carrier network.

QUESTION 495:

A user dials to the company's network. He found that he is in someone else's session. Why will this happen (Choose all that apply)?

- A. The last session was not terminated.
- B. The access server did not disconnect the session properly.
- C. The server is over utilized
- D. The server RAM is corrupted
- E. The server CPU is over utilized

Answer: A, B

Explanation:

The last user's session is still open. This is the cause of the problem.

QUESTION 496:

You are a Cisco Certified Engineer. You are configuring a remote access solution. You have a Cisco router with a physical BRI and serial interface. Can you back up the serial interface and still use the BRI interface, and how?

- A. Yes, you must configure a serial for frame relay.
- B. Yes, you must configure a sub interface.
- C. Yes, you must configure a dialer interface.

D. No, this cannot be done.

Answer: C

Explanation:

According to Cisco: A backup interface is an interface that stays idle until certain circumstances occur, then it is activated. The backup interface can be a physical interface such as a Basic Rate Interface (BRI), or an assigned backup dialer interface to be used in a dialer pool. While the primary line is up, the backup interface is placed in standby mode. Once in standby, the backup interface is effectively shutdown until enabled. Any route associated with the backup interface will not appear in the routing table. More information can be found at: [this site](#)

QUESTION 497:

You are a Cisco Certified Engineer. You are configuring an ISDN remote access solution. At ISDN layer 3, which of the following messages are NOT included (Choose all that apply)?

- A. PAUSE
- B. DISCONNECT
- C. CONNECT
- D. STATUS
- E. USER INFORMATION
- F. RELEASE
- G. SETUP
- H. CANCEL

Answer: A

Explanation:

According to Cisco: Two Layer 3 specifications are used for ISDN signaling: ITU-T (formerly CCITT) I.450 (also known as ITU-T Q.930) and ITU-T I.451 (also known as ITU-T Q.931). Together, these protocols support user-to-user, circuit-switched, and packet-switched connections. A variety of call-establishment, call-termination, information, and miscellaneous messages are specified, including SETUP, CONNECT, RELEASE, USER INFORMATION, CANCEL, STATUS, and DISCONNECT. These messages are functionally similar to those provided by the X.25 protocol.

QUESTION 498:

You are a Cisco Certified Engineer. You are configuring a remote access solution. How do you have PPP be in effect on calls placed by the dialer interfaces that use the physical interfaces?

- A. by disabling PPP encapsulation on physical interfaces

- B. by enabling PPP encapsulation on virtual interfaces
- C. by enabling PPP encapsulation on physical interfaces
- D. by disabling PPP encapsulation on virtual interfaces

Answer: C

Explanation:

According to Cisco: PPP, described in RFC 1661, encapsulates network layer protocol information over point-to-point links. You can configure PPP on the following types of physical interfaces:

Asynchronous serial

HSSI

ISDN

Synchronous serial

By enabling PPP encapsulation on physical interfaces, PPP can also be in effect on calls placed by the dialer interfaces that use the physical interfaces.

QUESTION 499:

Regarding DHCP, DHCP relay and DHCP server are mutually exclusive.

- A. None of the choices.
- B. True
- C. False only for certain IOS version
- D. False
- E. False only for IOS version below V10

Answer: B

Explanation:

According to the technical documentation at CCO:

The following are application notes for DHCP server:

DHCP relay and DHCP server are mutually exclusive.

When DHCP server is initialized, default addresses are used if no LAN or internal address exists. The Cisco 700 series router picks up the DHCP client's default gateway, netmask, and starting DHCP addresses by using the LAN IP address, if one exists. If a LAN address does not exist, the router uses the internal IP address. If neither exists, it uses the default settings: 10.0.0.1 as the LAN IP address (default gateway for DHCP clients), 255.0.0.0 as the subnet mask, and 10.0.0.2 as the starting DHCP client addresses. For the DHCP values to be automatically generated based on the LAN or internal IP address, each DHCP value must be set to 0.0.0.0 or none, for the new values to take effect.

QUESTION 500:

A LAPD Address field can be 1 or 2 bytes long.

- A. True
- B. False
- C. True only in the US
- D. True only in Asia
- E. True only in Europe

Answer: A

Explanation:

According to the technical documentation at CCO:

The LAPD Flag and Control fields are identical to those of HDLC. The LAPD Address field can be either 1 or 2 bytes long. If the extended address bit of the first byte is set, the address is 1 byte; if it is not set, the address is 2 bytes. The first Address-field byte contains the service access point identifier (SAPI), which identifies the portal at which LAPD services are provided to Layer 3. The C/R bit indicates whether the frame contains a command or a response. The Terminal Endpoint Identifier (TEI) field identifies either a single terminal or multiple terminals. A TEI of all ones indicates a broadcast.

QUESTION 501:

Which of the following are valid functions of the lock DTE modem attribute?

- A. Disable UART.
- B. Enable UART.
- C. Locks the data speed between the computer motherboard and the RS232 port.
- D. Locks the data speed between the modem and the DTE device.

Answer: D

Explanation:

The lock DTE speed command is often related to the way the modem handles error correction. This command varies widely from one modem to another. Locking the modem speed ensures that the modem always communicates with the Cisco access server or router at the speed configured on the Cisco auxiliary port.

QUESTION 502:

Which of the following are not the valid types of ATM addresses (Choose all that apply)?

- A. DCC
- B. GCT
- C. BSP
- D. ICD
- E. NSAP

F. AED

Answer: B, C, F

Explanation:

According to the technical documentation at CCO:

There are 3 types of private ATM addresses:

NSAP encoding format for E.164 addresses - The authority and format identifier (AFI) is 45. These addresses are used in establishing ISDN calls by public networks, and they are normally used in public telephony.

Data Country Code (DCC) AESA - The AFI is 39. These addresses are to be used in public networks. For example, the initial domain identifier (IDI) value 0x84.0f identifies the United States.

International Code Designator (ICD) AESA - The AFI is 47. These addresses are used in private organizations, and the ICD field indicates the code set or organization. Cisco uses by default ICD addresses.

QUESTION 503:

Which of the following are NOT the valid types of X.25 PLP packet fields (Choose all that apply)?

- A. User Data
- B. LCI
- C. GFI
- D. PTI
- E. None of the choices.

Answer: E

Explanation:

According to the technical documentation at CCO:

Four types of PLP packet fields exist:

General Format Identifier (GFI)-Identifies packet parameters, such as whether the packet carries user data or control information, what kind of windowing is being used, and whether delivery confirmation is required.

Logical Channel Identifier (LCI)-Identifies the virtual circuit across the local DTE/DCE interface.

Packet Type Identifier (PTI)-Identifies the packet as one of 17 different PLP packet types.

User Data-Contains encapsulated upper-layer information. This field is present only in data packets. Otherwise, additional fields containing control information are added.

QUESTION 504:

You are a Cisco Certified Engineer. You are configuring a DDR remote access

solution. What command may be used to show the general diagnostic information for interfaces configured (fill in the blank)

Answer: show dialer

Explanation:

According to Cisco: show dialer [interface type number] - Displays general diagnostic information for interfaces configured for DDR. If the dialer came up properly, the Dialer state is data link layer up message should appear. If physical layer up appears, then the line protocol came up, but the Network Control Protocol (NCP) did not. The source and destination addresses of the packet that initiated the dialing are shown in the Dial reason line. This show command also displays the timer's configuration and the time before the connection times out.

QUESTION 505:

Your boss requires you to use the modem for both incoming and outgoing calls. How do you do this?

- A. modem inout
- B. en modem inout
- C. modem inout enable
- D. en modem in out

Answer: A

Explanation:

You may configure the line for modem control using the modem inout line configuration command.

QUESTION 506:

You are a Cisco Certified Engineer. You are configuring a remote access solution. What type of commands do you use to modify the operation of the ATM interface?

- A. None of the choices.
- B. Local EXEC commands
- C. Line commands
- D. Global EXEC commands
- E. Interface configuration commands

Answer: E

Explanation:

According to Cisco: Interface configuration commands modify the operation of the ATM interface. Interface configuration commands always follow an interface global

configuration command, which defines the interface type. Use the interface type_number.subif command to access interface configuration mode. In the following example, ATM interface 1 is about to be configured. The new prompt, ATM(config-if)Q, indicates interface configuration mode.

QUESTION 507:

You are a Cisco Certified Engineer. You are configuring an ISDN remote access solution. In ISDN, ITU-T Q.931 belongs to which layer?

- A. Layer 1
- B. Layer 4
- C. Layer 3
- D. Layer 2

Answer: C

Explanation:

According to Cisco: Two Layer 3 specifications are used for ISDN signaling: ITU-T (formerly CCITT) I.450 (also known as ITU-T Q.930) and ITU-T I.451 (also known as ITU-T Q.931). Together, these protocols support user-to-user, circuit-switched, and packet-switched connections. A variety of call-establishment, call-termination, information, and miscellaneous messages are specified, including SETUP, CONNECT, RELEASE, USER INFORMATION, CANCEL, STATUS, and DISCONNECT. These messages are functionally similar to those provided by the X.25 protocol.

QUESTION 508:

You are a Cisco Certified Engineer. You are configuring an ISDN remote access solution. In ISDN, LAPD belongs to which layer?

- A. Layer 2
- B. Layer 3
- C. Layer 1
- D. Layer 4

Answer: A

Explanation:

According to Cisco: Layer 2 of the ISDN signaling protocol is Link Access Procedure, D channel (LAPD). LAPD is similar to High-Level Data Link Control (HDLC) and Link Access Procedure, Balanced (LAPB). As the expansion of the LAPD acronym indicates, this layer it is used across the D channel to ensure that control and signaling information flows and is received properly.

QUESTION 509:

You are a Cisco Certified Engineer. You are configuring a remote access solution with chat scripts. Which of the following are NOT the functions of chat scripts (Choose all that apply)?

- A. Logging into a remote system.
- B. Sending messages from one telnet session to another.
- C. Instructing the modem to dial out.
- D. Filtering incoming calls.
- E. Initializing the directly-attached modem.

Answer: B, D

Explanation:

According to Cisco: Chat scripts are strings of text used to send commands for modem dialing, logging in to remote systems, and initializing asynchronous devices connected to an asynchronous line. On a router, chat scripts can be configured on the auxiliary port only. A chat script must be configured to dial out on asynchronous lines. You also can configure chat scripts so that they can be executed automatically for other specific events on a line, or so that they are executed manually. More information can be found at: [this site](#)

QUESTION 510:

Within a LAPB Information (I) frames, what are used for performing flow control and error recovery (Choose all that apply)?

- A. P/F bit
- B. Send sequence number
- C. Receive sequence number
- D. R/C bit
- E. D/E bit

Answer: A, B, C

Explanation:

According to the technical documentation at CCO:

Information (I) frames-These frames carry upper-layer information and some control information (necessary for full-duplex operations). Send and receive sequence numbers and the poll final (P/F) bit perform flow control and error recovery. The send sequence number refers to the number of the current frame. The receive sequence number records the number of the frame to be received next. In full-duplex conversation, both the sender and the receiver keep send and receive sequence numbers. The poll bit is used to force a final bit message in response; this is used for error detection and recovery.

QUESTION 511:

You may configure PPP on the following types of physical interfaces (Choose all that apply):

- A. ISDN
- B. Asynchronous serial
- C. HSSI
- D. Synchronous serial

Answer: A, B, C, D

Explanation:

According to Cisco: PPP, described in RFC 1661, encapsulates network layer protocol information over point-to-point links. You can configure PPP on the following types of physical interfaces:

- Asynchronous serial
- HSSI
- ISDN
- Synchronous serial

By enabling PPP encapsulation on physical interfaces, PPP can also be in effect on calls placed by the dialer interfaces that use the physical interfaces.

QUESTION 512:

You are a Cisco Certified Engineer. You are configuring a remote access solution. What command allows you to verify that PAP or CHAP authentication was successful between two routers (fill in the blank):

Answer: show dialer

Explanation:

According to Cisco: show dialer [interface type number] - Displays general diagnostic information for interfaces configured for DDR. If the dialer came up properly, the Dialer state is data link layer up message should appear. If physical layer up appears, then the line protocol came up, but the Network Control Protocol (NCP) did not. The source and destination addresses of the packet that initiated the dialing are shown in the Dial reason line. This show command also displays the timer's configuration and the time before the connection times out.

QUESTION 513:

What command should you use so that your access server will attempt to authenticate all incoming calls that start a PPP session with CHAP, and will use PAP only if the remote device does not support CHAP (fill in the blank)

Answer: ppp authentication chap pap

Explanation: If the remote device does not support chap then use pap. So chap must be first mentioned before pap in the command.

Note:

According to the technical documentation at CCO:

If you configure ppp authentication chap on an interface, all incoming calls on that interface that initiate a PPP connection will have to be authenticated using CHAP; likewise, if you configure ppp authentication pap, all incoming calls that start a PPP connection will have to be authenticated via PAP. If you configure ppp authentication chap pap, the access server will attempt to authenticate all incoming calls that start a PPP session with CHAP. If the remote device does not support CHAP, the access server will try to authenticate the call using PAP. If the remote device doesn't support either CHAP or PAP, authentication will fail and the call will be dropped. If you configure ppp authentication pap chap, the access server will attempt to authenticate all incoming calls that start a PPP session with PAP. If the remote device does not support PAP, the access server will try to authenticate the call using CHAP. If the remote device doesn't support either protocols, authentication will fail and the call will be dropped. If you configure the ppp authentication command with the callin keyword, the access server will only authenticate the remote device if the remote device initiated the call.

QUESTION 514:

In X.25, LAPB maps to the _____ layer.

- A. physical
- B. transport
- C. data link
- D. network
- E. None of the choices.
- F. session

Answer: C

Explanation:

According to the technical documentation at CCO: X.25 uses the following three protocols, which map to the bottom three layers of the OSI reference model:

PLP, which maps to the network layer

LAPB, which maps to the data link layer

X.21bis, EIA/TIA-232, EIA/TIA-449, EIA-530, and G.703, which map to the physical layer

QUESTION 515:

How many Layer 3 specifications exist for ISDN signaling?

- A. three
- B. four
- C. two
- D. five
- E. one

Answer: C

Explanation:

According to the technical documentation at CCO:

Two Layer 3 specifications are used for ISDN signaling: ITU-T (formerly CCITT) I.450 (also known as ITU-T Q.930) and ITU-T I.451 (also known as ITU-T Q.931). Together, these protocols support user-to-user, circuit-switched, and packet-switched connections. A variety of call-establishment, call-termination, information, and miscellaneous messages are specified, including SETUP, CONNECT, RELEASE, USER INFORMATION, CANCEL, STATUS, and DISCONNECT.

QUESTION 516:

Which of the following is NOT true concerning the valid action to take for choosing Cisco products for use (Choose all that apply)?

- A. Use Cisco Product Pick up tool to plan for the hardware requirement.
- B. Use Cisco Product Wizard GUI to plan for the hardware requirement.
- C. Use Cisco Product Selection tool to plan for the hardware requirement.
- D. Use Cisco Intelligent Agent to plan for the hardware requirement.

Answer: A, B, D

QUESTION 517:

You are a Cisco Certified Engineer. You are configuring an ISDN remote access solution. Which of the following technologies allows you to configure multiple ISDN switch type per router?

- A. Multilink PPP
- B. Multilink Switches
- C. Multilink ISDN Channel aggregation
- D. Multiple ISDN Switch Types

Answer: D

Explanation:

According to Cisco: The Multiple ISDN Switch Types feature allows you to configure more than one ISDN switch type per router. You can apply an ISDN switch type on a per interface basis, thus extending the existing global isdn switch-type command to the

interface level. This allows Basic Rate Interfaces (BRI) and Primary Rate Interfaces (PRI) to run simultaneously on platforms that support both interface types.

QUESTION 518:

Which of the following circuit operation procedures will you use in a X.25 SVC (Choose all that apply)?

- A. call setup
- B. call clearing
- C. call fixing
- D. data compression
- E. data transfer

Answer: A, B, E

Explanation:

According to the technical documentation at CCO:

Layer 3 X.25 uses three virtual circuit operational procedures: call setup, data transfer, and call clearing. Execution of these procedures depends on the virtual circuit type being used. For a PVC, Layer 3 X.25 is always in data transfer mode because the circuit has been permanently established. If an SVC is used, all three procedures are used.

QUESTION 519:

How can you be sure if your router is properly initialized (Choose all that apply)?

- A. Check the Red Power Light
- B. Check the Enable light
- C. Passive LED
- D. Active LED

Answer: B, D

Explanation:

You should be familiar with the front panel of the router, and make sure you know the basic way of operating the router.

QUESTION 520:

You are a Cisco Certified Engineer. You are configuring a remote access solution. With regards to network layer address assignment, which of the following are NOT the effects of using frame relay sub interfaces on a physical interface (Choose all that apply)?

- A. The network layer address of each sub interface must be in the same subnet as the

physical interface address.

- B. The network layer address of each sub interface must be approved by IANA
- C. The network layer address must be removed from the physical interface.
- D. The network layer address of each sub interface must be the same as the physical interface address.
- E. The sub interfaces should be assigned the network broadcast address of the physical interface.
- F. The network layer address of each sub interface must NOT be approved by the network administrator

Answer: A, B, D, E, F

Explanation:

According to Cisco: Frame Relay subinterfaces provide a mechanism for supporting partially meshed Frame Relay networks. Most protocols assume transitivity on a logical network; that is, if station A can talk to station B, and station B can talk to station C, then station A should be able to talk to station C directly. Transitivity is true on LANs, but not on Frame Relay networks unless A is directly connected to C. Additionally, certain protocols such as AppleTalk and transparent bridging cannot be supported on partially meshed networks because they require "split horizon," in which a packet received on an interface cannot be sent from the same interface even if received and transmitted on different VCs. Configuring Frame Relay subinterfaces ensures that a single physical interface is treated as multiple virtual interfaces, which allows you to overcome split horizon rules. Packets received on one virtual interface can be forwarded to another virtual interface, even if they are configured on the same physical interface. Subinterfaces address the limitations of Frame Relay networks by providing a way to subdivide a partially meshed Frame Relay network into a number of smaller, fully meshed (or point-to-point) subnetworks. Each subnetwork is assigned its own network number and appears to the protocols as if it is reachable through a separate interface. (Note that point-to-point subinterfaces can be unnumbered for use with IP, reducing the addressing burden that might otherwise result.)

QUESTION 521:

Which of the following routed protocols can be used in dial-up networking?

- A. TCP / IP
- B. NetBeui
- C. OSPF
- D. IPX / SPX
- E. IGRP

Answer: A, B, D

Explanation:

OSPF and IGRP are routing protocols, not routed protocols

QUESTION 522:

You are a Cisco Certified Engineer. You are configuring a remote access solution. You want to compress the traffics using the router processor. Before you do so, what command do you use to check the CPU load (fill in the blank):

Answer: show process cpu

Explanation:

According to Cisco: Software compression is available in all router platforms. Software compression is performed by the main processor in the router. Compression is performed in software and might significantly affect system performance. We recommend that you disable compression if the router CPU load exceeds 65 percent. To display the CPU load, use the show process cpu EXEC command.

QUESTION 523:

What command should you use to enable AAA authentication regardless of the supported login authentication methods to use (fill in the blank):

Answer: aaa authentication login

Explanation:

According to the technical documentation at CCO:

The AAA security services facilitate a variety of login authentication methods. Use the aaa authentication login command to enable AAA authentication no matter which of the supported login authentication methods you decide to use. With the aaa authentication login command, you create one or more lists of authentication methods that are tried at login. These lists are applied using the login authentication line configuration command.

QUESTION 524:

You are a Cisco Certified Engineer. You are configuring a remote access solution. What command do you use to exit line configuration mode and return to global configuration mode (fill in the blank):

Answer: exit

Explanation:

According to Cisco: To exit line configuration mode and return to global configuration mode, use the exit command. To exit line configuration mode and return to privileged EXEC mode, enter the end command, or press Ctrl-Z.

QUESTION 525:

Which of the following components make up the Frame Relay frame (Choose all that apply)?

- A. parity portion
- B. header and address area
- C. frame check sequence
- D. security bit
- E. user-data portion

Answer: B, C, E

Explanation:

According to the technical documentation at CCO: Flags indicate the beginning and end of the frame. Three primary components make up the Frame Relay frame: the header and address area, the user-data portion, and the frame check sequence (FCS). The address area, which is 2 bytes in length, is comprised of 10 bits representing the actual circuit identifier and 6 bits of fields related to congestion management. This identifier commonly is referred to as the data-link connection identifier (DLCI).

QUESTION 526:

You are a Cisco Certified Engineer. You are configuring a remote access solution. Which of the following situations are NOT well served by an access server (Choose all that apply)?

- A. Corporate staff requiring dial-out access.
- B. Corporate staff requiring access instant application access on corporate systems.
- C. Corporate staff requiring access to FTP based files.
- D. Mobile sales force requiring dial-in access.
- E. Corporate staff requiring access to web based accounting applications.

Answer: B, C, E

Explanation:

According to Cisco: The Cisco 2500 access server series represents Cisco's low cost entry into the access server marketplace. Three new products have recently been added to this family: the dial optimized AS2509-RJ and AS2511-RJ, and the temperature hardened Cisco 2509-ET. The Cisco 2500 access server series gives users the ability to connect asynchronous devices such as dumb terminals, modems, router consoles, slot machines, and ISDN TAs into a routed network. This product family contains new features that make them easier to use than ever, and they run the same Cisco IOS software that runs the backbone of the Internet on a high-performance router engine. They also give users integrated synchronous serial ports to backhaul routed traffic through T1/E1 lines. The Cisco 2500 access server series provide a variety of models designed for small office and remote site environments. Each model is a fixed-configuration router that supports at least two interface types. Each access server comes standard with Flash EPROM

technology for simplified software maintenance. For software, the Cisco 2500 access server series offer a wide choice of feature sets, so you can select the appropriate protocol set for your network environment. These feature sets range from IP and bridging-only to a feature set containing the full array of Cisco's software functionality.

QUESTION 527:

What command should you use to specify the local username database as the authentication method for use on lines running PPP when no other method list has been defined (fill in the blank):

Answer: `aaa authentication ppp default local`

Explanation:

According to the technical documentation at CCO:

Use the `aaa authentication ppp` command with the method keyword `local` to specify that the Cisco router or access server will use the local username database for authentication. For example, to specify the local username database as the method of authentication for use on lines running PPP when no other method list has been defined, enter:

```
aaa authentication ppp default local
```

QUESTION 528:

You are a Cisco Certified Engineer. You are configuring a remote access solution. What T1 controller command can you use to configure the controller for ISDN PRI operation (fill in the blank):

Answer: `ISDN Switch-type`

Explanation:

According to Cisco: National ISDN Switch Types for Basic Rate and Primary Rate Interfaces provides the following benefits: Unlike previous custom implementations, such as `basic-5ess`, `basic-dms100`, `primary-5ess`, and `primary-dms100`, the National ISDN specification is designed to be switch independent. This increases flexibility in adapting to evolving standards and future enhancements. The ability to select PRI B channel order election for outgoing calls allows extended flexibility and compatibility with a variety of ISDN switch type service implementations. Additionally, this ability reduces ISDN switch misconfigurations, which can delay initial service activation. More information about the switch types can be found at this site

QUESTION 529:

Which of the following indicates the address of the CiscoSecure server in your network?

A. `en tacacs-server host`

- B. server host tacacs
- C. tacacs-server en
- D. tacacs-server host

Answer: D

Explanation:

According to Cisco: The tacacs-server host command allows you to specify the names of the IP host or hosts maintaining a TACACS server. Because the TACACS software searches for the hosts in the order specified, this feature can be useful for setting up a list of preferred servers.

QUESTION 530:

Which of the following LMI extensions are NOT optional (Choose all that apply)?

- A. Multicasting
- B. Simple flow control
- C. Virtual circuit status messages
- D. Global addressing

Answer: C

Explanation:

According to the technical documentation at CCO:

In addition to the basic Frame Relay protocol functions for transferring data, the consortium Frame Relay specification includes LMI extensions that make supporting large, complex internetworks easier. Some LMI extensions are referred to as "common" and are expected to be implemented by everyone who adopts the specification. Other LMI functions are referred to as "optional." A summary of the LMI extensions follows: Virtual circuit status messages (common)-Provide communication and synchronization between the network and the user device, periodically reporting the existence of new PVCs and the deletion of already existing PVCs, and generally provide information about PVC integrity. Virtual circuit status messages prevent the sending of data into black holes-that is, over PVCs that no longer exist.

Multicasting (optional)-Allows a sender to transmit a single frame but have it delivered by the network to multiple recipients. Thus, multicasting supports the efficient conveyance of routing protocol messages and address resolution procedures that typically must be sent to many destinations simultaneously.

Global addressing (optional)-Gives connection identifiers global rather than local significance, allowing them to be used to identify a specific interface to the Frame Relay network. Global addressing makes the Frame Relay network resemble a local-area network (LAN) in terms of addressing; Address Resolution Protocols, therefore, perform over Frame Relay exactly as they do over a LAN.

Simple flow control (optional)-Provides for an XON/XOFF flow control mechanism that

applies to the entire Frame Relay interface. It is intended for devices whose higher layers cannot use the congestion notification bits and that need some level of flow control.

QUESTION 531:

You are a Cisco Certified Engineer. You are configuring a remote access solution. Which of the following correctly describe the IP un-numbered Ethernet 0/0 command, when it is issued in configuration mode for a serial interface?

- A. The IP address of the Ethernet interface is used by the serial interface.
- B. There is no effect at all
- C. DHCP traffic received on the serial interface is forwarded to the Ethernet interface.
- D. ARP traffic received on the serial interface is forwarded to the Ethernet interface.

Answer: A

Explanation:

According to Cisco: The ip unnumbered configuration command allows you to enable IP processing on a serial interface without assigning it an explicit IP address. The ip unnumbered interface can "borrow" the IP address of another interface already configured on the router, thereby conserving network and address space. More information can be found at: [this site](#)

QUESTION 532:

You are a Cisco Certified Engineer. You are configuring a remote access solution. Which of the following are network-termination devices, in addition to NT1, that can connect the four-wire subscriber wiring to the conventional two-wire local loop (Choose all that apply)?

- A. NT3
- B. TA2
- C. LE
- D. NT2
- E. TA
- F. LE2

Answer: D

Explanation:

According to Cisco: Beyond the TE1 and TE2 devices, the next connection point in the ISDN network is the network termination type 1 (NT1) or network termination type 2 (NT2) device. These are network-termination devices that connect the four-wire subscriber wiring to the conventional two-wire local loop. In North America, the NT1 is a customer premises equipment (CPE) device. In most other parts of the world, the NT1 is part of the network provided by the carrier. The NT2 is a more complicated device that

typically is found in digital private branch exchanges (PBXs) and that performs Layer 2 and 3 protocol functions and concentration services. An NT1/2 device also exists as a single device that combines the functions of an NT1 and an NT2.

QUESTION 533:

You are a Cisco Certified Engineer. You are configuring a remote access solution. Cisco multi-link PPP is compatible with and supports which of the following items (Choose all that apply)?

- A. Most routers conforming to RFC1997
- B. Synchronous dialer interfaces
- C. Asynchronous dialer interfaces
- D. Cisco700 series routers
- E. A multiple-LAN interface
- F. RFC1917

Answer: B, C

Explanation:
Multilink PPP

The Multilink PPP feature provides load balancing functionality over multiple WAN links, while providing multivendor interoperability, packet fragmentation and proper sequencing, and load calculation on both inbound and outbound traffic. The Cisco implementation of MLP supports the fragmentation and packet sequencing specifications in RFC 1990.

Additionally, you can change the default endpoint discriminator value that is supplied as part of user authentication. Refer to RFC 1990 for more information about the endpoint discriminator.

MLP allows packets to be fragmented and the fragments to be sent at the same time over multiple point-to-point links to the same remote address.

The multiple links come up in response to a defined dialer load threshold. The load can be calculated on inbound traffic, outbound traffic, or on either, as needed for the traffic between the specific sites. MLP provides bandwidth on demand and reduces transmission latency across WAN links.

MLP is designed to work over synchronous and asynchronous serial and BRI and PRI types of single or multiple interfaces that have been configured to support both dial-on-demand rotary groups and PPP encapsulation.

QUESTION 534:

What keyword of the aaa authentication login command do you use to specify the line password as the login authentication method (fill in the blank):

Answer: line

Explanation:

According to the technical documentation at CCO: Use the aaa authentication login command with the line method keyword to specify the line password as the login authentication method. For example, to specify the line password as the method of user authentication at login when no other method list has been defined, enter the following:
aaa authentication login default line

QUESTION 535:

In general, multiple ISDN Switch Types supports which of the following ISDN interfaces?

- A. None of the choices.
- B. Both BRI and PRI
- C. BRI only
- D. PRI only
- E. This feature is no longer supported

Answer: B

Explanation:

According to Cisco: The Multiple ISDN Switch Types feature allows you to configure more than one ISDN switch type per router. You can apply an ISDN switch type on a per interface basis, thus extending the existing global isdn switch-type command to the interface level. This allows Basic Rate Interfaces (BRI) and Primary Rate Interfaces (PRI) to run simultaneously on platforms that support both interface types.

QUESTION 536:

You are a Cisco Certified Engineer. You are configuring a remote access solution. Which of the following statements about the ISDN switch type are NOT true (Choose all that apply)?

- A. It selects the PRI controller line code.
- B. It defines the type of signaling used by the ISDN service provider switch.
- C. It is a set of US only standard
- D. It is proprietary
- E. It is both a global and an interface command.
- F. It is a PRI controller command.

Answer: A, C, D, F

Explanation:

According to Cisco: ISDN PRI is supported on the Cisco 7200 series and 7500 series routers using T1 or E1 versions of the Multichannel Interface Processor (MIP) card, on

the Cisco 4000 series channelized E1/T1/PRI network processor module (NPM), and on the Cisco AS5200 access server. Channelized T1 ISDN PRI offers 23 B channels and 1 D channel. Channelized E1 ISDN PRI offers 30 B channels and 1 D channel. Channel 24 is the D channel for T1, and channel 16 is the D channel for E1. More information about the switch types can be found at this site

QUESTION 537:

You are a Cisco Certified Engineer. You are configuring a remote access solution with modems. What prevents the speed between the modem and the DTE from being varied?

- A. the modem attribute syn DTE
- B. the modem attribute static DTE
- C. the modem attribute lock DTE
- D. the modem attribute fixed DTE

Answer: C

Explanation:

According to Cisco: The lock DTE speed command, which might also be referred to as port rate adjust or buffered mode, is often related to the way in which the modem handles error correction. This command varies widely from one modem to another. Locking the modem speed ensures that the modem always communicates with the Cisco access server or router at the speed configured on the Cisco auxiliary port. If this command is not used, the modem reverts to the speed of the data link (the telephone line), instead of communicating at the speed configured on the access server.

QUESTION 538:

You are a Cisco Certified Engineer. You are configuring a DDR remote access solution. What command do you use to define interesting packets (fill in the blank):

Answer: dialer-list

Explanation:

According to Cisco: Dial-on-Demand Routing (DDR) addresses the need for intermittent network connections over circuit-switched WANs. With DDR, all traffic is classified as either interesting or uninteresting. If traffic is interesting, the packet is passed to the interface, and the router then connects to the remote router (if not currently connected). The router defines interesting packets with the dialer-list command. DDR is implemented in two ways: DDR with dialer profiles and legacy DDR.

QUESTION 539:

You are a Cisco Certified Engineer. You are configuring a remote access solution

with modems. Which of the following terms, in addition to port rate adjust, are associated with the modem attribute lock DTE (Choose all that apply)?

- A. buffered mode
- B. port rate prefetch
- C. port id tag changes
- D. unbuffered cache

Answer: A

Explanation:

According to Cisco: The lock DTE speed command, which might also be referred to as port rate adjust or buffered mode, is often related to the way in which the modem handles error correction. This command varies widely from one modem to another. Locking the modem speed ensures that the modem always communicates with the Cisco access server or router at the speed configured on the Cisco auxiliary port. If this command is not used, the modem reverts to the speed of the data link (the telephone line), instead of communicating at the speed configured on the access server.

QUESTION 540:

You are a Cisco Certified Engineer. You are configuring a remote access solution. Your company currently uses an ISDN BRI in standby mode to back up the primary serial connection. How can the BRI interface be configured to allow dialup operation as well as backup services?

- A. Configure the BRI as a standard DDR connection and configure the serial port to use BRI as the backup.
- B. Configure one B channel of the BRI as Standby Backup and two B channels as DDR.
- C. Configure one B channel of the BRI as Standby Backup and the other B channel as DDR.
- D. Configure two B channels of the BRI as Standby Backup and the other B channel as DDR.
- E. Use the dialer profile as a backup and configure the BRI as a member of the dialer pool.
- F. Configure one B channel of the BRI as Standby Backup and nothing else.

Answer: E

Explanation:

According to Cisco: A backup interface is an interface that stays idle until certain circumstances occur, then it is activated. The backup interface can be a physical interface such as a Basic Rate Interface (BRI), or an assigned backup dialer interface to be used in a dialer pool. While the primary line is up, the backup interface is placed in standby mode. Once in standby, the backup interface is effectively shutdown until enabled. Any

route associated with the backup interface will not appear in the routing table. More information can be found at: [this site](#)

QUESTION 541:

You are a Cisco Certified Engineer. You are configuring a remote access solution. ITU-T Q.931 is the protocol that works for:

- A. Layer3; D channel
- B. Layer1, D channel
- C. Layer5; B channel
- D. Layer2; B channel
- E. Layer4; B channel
- F. Layer2; D channel

Answer: A

Explanation:

According to Cisco: Cisco platforms support Q.931 user- and network-side switch types for ISDN call processing. User-side PRI enables the Cisco platform to provide a standard ISDN PRI user-side interface to the Public Switched Telephone Network (PSTN). Network-side PRI enables the Cisco platform to provide a standard Digital T1/E1 Packet Voice Trunk Network Modules on Cisco 2600 series and Cisco 3600 series routers. More information can be found at: [this site](#)

QUESTION 542:

You are a Cisco Certified Engineer. You are configuring a remote access solution. Which of the following commands can be used on the server side of a PPP callback configuration?

- A. PPP callback accepts
- B. PPP callback servers
- C. PPP callback server accept PPP
- D. PPP callback request
- E. PPP callb acb
- F. PPP call accept

Answer: A

Explanation:

According to Cisco: PPP callback provides a client-server relationship between the end points of a point-to-point connection. PPP callback allows a router to request that a dial-up peer router call back. The callback feature can be used to control access and toll costs between the routers. When PPP callback is configured on the participating routers, the calling router (the callback client) passes authentication information to the remote

router (the callback server), which uses the host name and dial string authentication information to determine whether to place a return call. If the authentication is successful, the callback server disconnects and then places a return call. The remote username of the return call is used to associate it with the initial call so that packets can be transmitted.

QUESTION 543:

You are a Cisco Certified Engineer. You are configuring a remote access solution. Which of the following statements will you consider as NOT true (Choose all that apply)?

- A. ITU-T Q.932 defines call control between the TE and LE.
- B. The D channel is governed by IAB.
- C. DSSI is a subset of Q.931.
- D. The D channel is governed by DDR.
- E. ITU-T Q.931 is specified as the protocol for layer2 of the ISDN D channel.

Answer: A, B, C, E

Explanation:

According to Cisco: Dial-on-Demand Routing (DDR) backup is a method of bringing up an alternate link should the primary WAN link fail. The router configured for DDR backup recognizes that the connection to the remote site has been lost, and initiates a DDR connection to the remote site using a different transmission media. More information can be found at: [this site](#)

QUESTION 544:

You are a Cisco Certified Engineer. You are configuring a remote access solution. You run the following command:
`ip host corpX 1098 157.11.11.96`
Which of the following statements are NOT true (Choose all that apply)?

- A. 157.11.11.96 is NOT a valid IANA approved IP address.
- B. 157.11.11.96 is the IP address of the remote host.
- C. The command allows a reverse telnet connection.
- D. The configuration applies in 1098 seconds.
- E. 1098 is the dialer group ID.

Answer: A, B, D, E

Explanation:

According to Cisco: Manually assigning host names to addresses is useful when you want to force a local address association and you are reasonably certain this address association will not conflict with other associations elsewhere in the internetwork. To

map IP addresses to a host name, perform the following global configuration task: Task
Command

Statically associate a host names with IP addresses. ip host name [TCP-port-number]
address1[address2...address8]

QUESTION 545:

You are a Cisco Certified Engineer. You are configuring a remote access solution.
Which of the following is the first configuration step necessary to enable frame relay
traffic shaping?

- A. Specify the FECN for traffic adaptation.
- B. Specify a queuing technique to be used on a connection.
- C. Specify the BECN for traffic adaptation.
- D. Specify and define map class.

Answer: D

Explanation:

According to Cisco: Cisco's QoS software solutions include two traffic shaping tools---generic traffic shaping (GTS) and Frame Relay traffic shaping (FRTS)---to manage traffic and congestion on the network. GTS provides a mechanism to control the traffic flow on a particular interface. It reduces outbound traffic flow to avoid congestion by constraining specified traffic to a particular bit rate (also known as the token bucket approach), while queuing bursts of the specified traffic. FRTS provides parameters that are useful for managing network traffic congestion. These include committed information rate (CIR), FECN and BECN, and the DE bit. For some time, Cisco has provided support for FECN for DECnet, BECN for SNA traffic using direct LLC2 encapsulation via RFC 1490, and DE bit support. The FRTS feature builds on this Frame Relay support with additional capabilities that improve the scalability and performance of a Frame Relay network, increasing the density of virtual circuits and improving response time. More information can be found at: [this site](#)

QUESTION 546:

You are a Cisco Certified Engineer. You are configuring a remote access solution.
To ensure that the calls configured for callback can really connect, what command
should you use (fill in the blank):

Answer: dialer callback-secure

Explanation:

According to Cisco: PPP callback provides a client-server relationship between the end points of a point-to-point connection. PPP callback allows a router to request that a dial-up peer router call back. The callback feature can be used to control access and toll costs between the routers. When PPP callback is configured on the participating routers,

the calling router (the callback client) passes authentication information to the remote router (the callback server), which uses the host name and dial string authentication information to determine whether to place a return call. If the authentication is successful, the callback server disconnects and then places a return call. The remote username of the return call is used to associate it with the initial call so that packets can be transmitted.

QUESTION 547:

You are a Cisco Certified Engineer. You are configuring a DDR remote access solution. Which of the following components of a dialer profile is entirely optional?

- A. Dialer map-class
- B. Dialer interfaces
- C. Dialer pool
- D. Physical interfaces

Answer: A

Explanation:

According to Cisco: The components of a dialer profile include: Dialer interfaces - logical entities that use a per-destination dialer profile. Any number of dialer interfaces can be created in a router. All configuration settings specific to the destination go in the dialer interface configuration. Each dialer interface uses a dialer pool, which is a pool of physical interfaces (ISDN BRI and PRI, asynchronous-modem, and synchronous serial). Dialer pool - Each interface references a dialer pool, which is a group of physical interfaces associated with a dialer profile. A physical interface can belong to multiple dialer pools. Contention for a specific physical interface is resolved by configuring the optional priority command. Physical interfaces - Interfaces in a dialer pool are configured for encapsulation parameters. The interfaces are also configured to identify the dialer pools to which the interface belong. Dialer profiles support PPP and High-Level Data Link Control (HDLC) encapsulation. Dialer map-class (optional) - Supply configuration parameters to dialer interfaces (for example, ISDN speed, dialer timers parameters, and so on). A map-class can be referenced from multiple dialer interfaces.

QUESTION 548:

Which of the following are situations ideal for deploying dedicated leased line, if cost is a concern (Choose all that apply)?

- A. long distances
- B. multi sites
- C. long connect times
- D. short distances

Answer: C, D

Explanation:

The longer the distance the higher the cost of the line. For multi-site configuration you should use Packet switching service or VPN instead.

QUESTION 549:

Which of the following frames are used by LAPB (Choose all that apply)?

- A. unnumbered
- B. numbered
- C. supervisory
- D. information

Answer: A, C, D

Explanation:

According to the technical documentation at CCO:

Layer 2 of the ISDN signaling protocol is Link Access Procedure, D channel (LAPD). LAPD is similar to High-Level Data Link Control (HDLC) and Link Access Procedure, Balanced (LAPB). As the expansion of the LAPD acronym indicates, this layer is used across the D channel to ensure that control and signaling information flows and is received properly. The LAPD frame format is very similar to that of HDLC; like HDLC, LAPD uses supervisory, information, and unnumbered frames. The LAPD protocol is formally specified in ITU-T Q.920 and ITU-T Q.921.

QUESTION 550:

You are a Cisco Certified Engineer. You are configuring a remote access solution. What signal is used by DTE to indicate that it is willing to accept a call?

- A. RTS
- B. DTR
- C. CTS
- D. ETA
- E. DSR
- F. DCD
- G. FTS

Answer: B

Explanation:

According to Cisco: DTE uses the RTS output signal to indicate if it can receive characters into the Rx input buffer. The DCE should not send data to the DTE when DTR input is low (no RTS). More information can be found at: [this site](#)

QUESTION 551:

Refer to the exhibit:

```
interface serial 1
ip address 128.10.200.65 255.255.255.192
dialer in-band
!
ip route 0.0.0.0 0.0.0.0 128.10.200.66
```

Which of the following is true?

- A. this configuration is for an outgoing call only configuration
- B. this configuration is for an answer and outgoing call configuration
- C. this configuration is for an answer only configuration
- D. this configuration is not valid

Answer: C

Explanation:

According to the technical documentation at CCO:

Cisco's dial-on-demand routing (DDR) feature allows you to use existing telephone lines to form a wide-area network (WAN). While using existing telephone lines, you can analyze traffic patterns to determine whether the installation of leased lines is appropriate. DDR provides significant cost savings over leased lines for links that are utilized for only a few hours each day or that experience low traffic flow.

DDR over serial lines requires the use of dialing devices that support V.25bis. V.25bis is an International Telecommunication Union Telecommunication (ITU-T) Standardization Sector standard for in-band signaling to bit synchronous data communications equipment (DCE) devices. A variety of devices support V.25bis, including analog V.32 modems, ISDN terminal adapters, and inverse multiplexers. Cisco's implementation of V.25bis supports devices that use the 1984 version of V.25bis (which requires the use of odd parity), as well as devices that use the 1988 version of V.25bis (which does not use parity).

QUESTION 552:

You are a Cisco Certified Engineer. You are configuring a remote access solution. In which two of the following situations would implementing a queuing policy other than FIFO be NOT beneficial? (Select two.)

- A. Time sensitive applications and server connections time out during only the most congested periods.
- B. A T1 WAN connection experiences utilization from 20% to 50% with no noticeable congestion.
- C. large graphics files transfers between the marketing office and the central printing facility are sometimes needed
- D. WAN traffic across a T1 link suffers constant congestion

Answer: B, C

Explanation:

Queuing policy will not be beneficial for B or C.

QUESTION 553:

Which of the following is true concerning the nature of a Telecommuter site (Choose all that apply)?

- A. tends to have many users
- B. needs dedicated connection services most of the time
- C. needs only dialup services most of the time
- D. tends to have few number of users

Answer: C, D

QUESTION 554:

Which of the following are parts of the CHAP challenge packet (Choose all that apply)?

- A. host name of the remote router
- B. random number
- C. ID
- D. host name of the local router

Answer: B, C, D

Explanation:

According to the technical documentation at CCO:

When CHAP is enabled on an interface and a remote device attempts to connect to it, the access server sends a CHAP packet to the remote device. The CHAP packet requests or "challenges" the remote device to respond. The challenge packet consists of an ID, a random number, and the host name of the local router.

QUESTION 555:

With Frame Relay, a communication session across an SVC consists of how many operational states?

- A. four
- B. five
- C. one
- D. three

E. two

Answer: A

Explanation:

According to the technical documentation at CCO:

Switched virtual circuits (SVCs) are temporary connections used in situations requiring only sporadic data transfer between DTE devices across the Frame Relay network. A communication session across an SVC consists of the following four operational states:

Call setup-The virtual circuit between two Frame Relay DTE devices is established.

Data transfer-Data is transmitted between the DTE devices over the virtual circuit.

Idle-The connection between DTE devices is still active, but no data is transferred. If an SVC remains in an idle state for a defined period of time, the call can be terminated.

Call termination-The virtual circuit between DTE devices is terminated.

QUESTION 556:

The primary benefit of the use of the FECN and BECN fields in Frame Relay is for the purpose of congestion indications.

A. False

B. True

C. True only for IOS V11 or above

D. True only for IOS V12 or above

Answer: B

Explanation:

According to the technical documentation at CCO:

Forward-explicit congestion notification (FECN) is a single-bit field that can be set to a value of 1 by a switch to indicate to an end DTE device, such as a router, that congestion was experienced in the direction of the frame transmission from source to destination.

The primary benefit of the use of the FECN and BECN fields is the capability of higher-layer protocols to react intelligently to these congestion indicators. Today, DECnet and OSI are the only higher-layer protocols that implement these capabilities.

Backward-explicit congestion notification (BECN) is a single-bit field that, when set to a value of 1 by a switch, indicates that congestion was experienced in the network in the direction opposite of the frame transmission from source to destination.

QUESTION 557:

You are asked to specify the interface load at which the dialer initiates another call to the destination. Which command will you use?

A. en dialer threshold

B. dialer load-threshold

- C. en dialer load-threshold
- D. dialer loadthres

Answer: B

Explanation:

You use this command to define the load level that must be exceeded on the first ISDN B channel before the router attempts to bring up a second B channel for a multilink PPP connection. The load value is between 1 and 255.

QUESTION 558:

You are a Cisco Certified Engineer. You are configuring a remote access solution. You have multiple ISDN user devices physically attached to one circuit. Which of the following can happen (Choose all that apply)?

- A. compression
- B. collisions
- C. encryption
- D. contention

Answer: B, D

Explanation:

According to Cisco: Multiple ISDN user devices can be physically attached to one circuit. In this configuration, collisions can result if two terminals transmit simultaneously. ISDN therefore provides features to determine link contention. When an NT receives a D bit from the TE, it echoes back the bit in the next E-bit position. The TE expects the next E bit to be the same as its last transmitted D bit.

QUESTION 559:

In a X25 SVC, Layer 3 X.25 is always in data transfer mode.

- A. True only for IOS V12 or above
- B. True only for IOS V10 or above
- C. True
- D. False
- E. True only for IOS V11 or above

Answer: D

Explanation:

According to the technical documentation at CCO:

Layer 3 X.25 uses three virtual circuit operational procedures: call setup, data transfer, and call clearing. Execution of these procedures depends on the virtual circuit type being

used. For a PVC, Layer 3 X.25 is always in data transfer mode because the circuit has been permanently established. If an SVC is used, all three procedures are used.

QUESTION 560:

DDR over serial lines requires dialing devices that support what standard?

- A. V.32a
- B. ITU-T 5
- C. X.121
- D. V.25bis
- E. LAPD
- F. V.26bis

Answer: D

Explanation:

According to the technical documentation at CCO:

DDR over serial lines requires the use of dialing devices that support V.25bis. V.25bis is an International Telecommunication Union Telecommunication (ITU-T) Standardization Sector standard for in-band signaling to bit synchronous data communications equipment (DCE) devices. A variety of devices support V.25bis, including analog V.32 modems, ISDN terminal adapters, and inverse multiplexers. Cisco's implementation of V.25bis supports devices that use the 1984 version of V.25bis (which requires the use of odd parity), as well as devices that use the 1988 version of V.25bis (which does not use parity).

QUESTION 561:

Which of the following correctly describe one purpose of using the dialer map command (Choose all that apply)?

- A. Configures a serial interface to call one site
- B. Configures an ISDN interface to call multiple sites
- C. Configures a serial interface to call multiple sites
- D. Configures an ISDN interface to call one site

Answer: A, B, C, D

Explanation:

According to Cisco: Typically, dialer maps are the preferred method of placing calls whereas a dialer string is reserved for scenarios in which the name of the answering router may not be known (i.e. a router pool). The dialer map command maps a protocol, a protocol address, a name for PPP authentication, and dial information to a specific remote router. It is one of the most important pieces of an ISDN configuration.

QUESTION 562:

What command should you use to double confirm that each of your interfaces supports a QSAAL PVC (fill in the blank):

Answer: show atm vc

Explanation:

According to the technical documentation at CCO: Use the show atm vc command to confirm that each interface supports a QSAAL PVC. Note how this VC cross-connects to interface ATM 2/0/0, which identifies the switch's internal management port. Since signaling messages are control messages, they must be sent to and processed by the CPU.

QUESTION 563:

In Frame Relay, what bit is used to indicate that a frame has lower importance than other frames?

- A. DA
- B. DT
- C. DE
- D. DL
- E. DC

Answer: C

Explanation:

According to the technical documentation at CCO:

The Discard Eligibility (DE) bit is used to indicate that a frame has lower importance than other frames. The DE bit is part of the Address field in the Frame Relay frame header.

DTE devices can set the value of the DE bit of a frame to 1 to indicate that the frame has lower importance than other frames. When the network becomes congested, DCE devices will discard frames with the DE bit set before discarding those that do not. This reduces the likelihood of critical data being dropped by Frame Relay DCE devices during periods of congestion.

QUESTION 564:

When will PPP callback occur (Choose all that apply)?

- A. when PPP NCP negotiation is not successful.
- B. when callback timer is started
- C. when callback timer is stopped
- D. when PPP NCP negotiation is successful

Answer: C, D

QUESTION 565:

Methods in traffic shaping do not include which of the following (Choose all that apply)?

- A. Rate enforcement on per-Byte basis
- B. Rate enforcement on per-VC basis
- C. Rate enforcement on per-MB basis
- D. Rate enforcement on per-Bit basis

Answer: A, C, D

QUESTION 566:

You need to have what type of connection to connect to an AAA server?

- A. serial interface
- B. synchronous call
- C. T1
- D. ethernet
- E. asynchronous call
- F. ISDN PRI
- G. T3

Answer: D

QUESTION 567:

To connect DTE and DCE devices, what type of connections are appropriate (Choose all that apply)?

- A. use RJ-45 to DB-25 adapter for straight-through mode
- B. use RJ-45 to DB-25 adapter for rolled mode
- C. use RJ-45 to RJ-45 cable for straight-through mode
- D. use RJ-45 to RJ-45 cable for rolled mode

Answer: B, C

QUESTION 568:

To add links to a multilink bundle, what command should be used?

- A. ppp multilink

- B. Enable chap
- C. Multilink ppp
- D. Enable multilink
- E. dialer load-threshold

Answer: E

QUESTION 569:

LMI signaling multicast mechanism is not intended for (Choose all that apply)?

- A. providing outgoing status on known DLCIs
- B. providing network server with its remote DLCI
- C. providing network server with its local DLCI
- D. verifying data flow

Answer: A, B, D

QUESTION 570:

You are a Cisco Certified Engineer. You are configuring an ISDN remote access solution. What command can you use to display all the call setup and tear down of connections (fill in the blank):

Answer: debug isdn q931

Explanation:

According to Cisco: debug isdn q931 - Shows call setup and tear down of the ISDN network connection (Layer 3). debug isdn q921 - Shows data link layer messages (Layer 2) on the D channel between the router and the ISDN switch. Use this debug if the show isdn status command does not display Layer 1 and Layer 2 up.

QUESTION 571:

Which of the following are components of the CiscoSecure ACS server (Choose all that apply)?

- A. AAA server
- B. Netscape Fastrack server
- C. RDBMS
- D. RADIUS Interface

Answer: A, B, C

QUESTION 572:

You want to define maximum calls for DDR. From the following choices which option should you use?

- A. Dialer profile
- B. Modemcap
- C. Dial Routing
- D. Dial Encap Entry

Answer: A

QUESTION 573:

When you apply the dialer list to an interface, you need to use a command. What command is this?

- A. dialer-group profile
- B. dialer-group map
- C. dialer-group
- D. dialer-group list

Answer: C

QUESTION 574:

Which of the following is true concerning QoS (Choose all that apply)?

- A. need to define QoS properties and policies on devices or device interfaces.
- B. need to run with WF QUESTION
- C. a set of capabilities allowing you to create differentiated services for network traffic
- D. need to send stop signals in 5 minutes interval

Answer: A, C

QUESTION 575:

You are a Cisco Certified Engineer. You are configuring a DDR remote access solution. With regards to the dialer pool, what command can you use to resolve potential contention problem (fill in the blank):

Answer: priority

Explanation:

According to Cisco: Dialer pool - Each interface references a dialer pool, which is a group of physical interfaces associated with a dialer profile. A physical interface can belong to multiple dialer pools. Contention for a specific physical interface is resolved by configuring the optional priority command.

QUESTION 576:

What option can be used as an alternative to DDR (Choose all that apply)?

- A. set the route calling cost
- B. set the route priority
- C. use a floating static route
- D. set up the static route to make it less desirable than the dynamic route

Answer: C, D

QUESTION 577:

What does TCP IP header exclude in its compression scheme?

- A. TCP/IP header
- B. Layer 3 header
- C. Layer 4 header
- D. Layer 2 header

Answer: B, C, D

QUESTION 578:

By using Cisco hardware compression adapters, what compression options can be supported (Choose all that apply)?

- A. IPX advanced compression
- B. IP payload compression V8
- C. frame relay FRF.9 stacker compression
- D. PPP stacker compression

Answer: C, D

QUESTION 579:

You are a Cisco Certified Engineer. You are configuring an ISDN remote access solution. What command will display the number of active calls (fill in the blank):

Answer: show isdn status

Explanation:

According to Cisco: show isdn status - Ensure that the router is properly communicating with the ISDN switch. In the output, verify that Layer 1 Status is ACTIVE, and that the

Layer 2 Status state = MULTIPLE_FRAME_ESTABLISHED appears. This command also displays the number of active calls.

QUESTION 580:

To enable TCP header compression, what command will you consider?

- A. compress lapd set
- B. frame-relay payload-compress
- C. ppp compress
- D. compress
- E. ip tcp header-compression
- F. compress all

Answer: E

QUESTION 581:

To configure an access server to communicate with a modem, you run the following command:

modem

What is this command for?

- A. Set the stop bits per byte
- B. Set RTS/CTS for hardware flow control
- C. Set login password
- D. Set maximum communication speed
- E. Set the modem for incoming call, outgoing call or both
- F. Set the protocols

Answer: E

QUESTION 582:

You are running commands on modemcap. You use the following command:

no modemcap edit

What command is it for?

- A. delete entry
- B. add new entry or edit current entry
- C. view a particular modemcap entry.
- D. displays current attributes

Answer: A

QUESTION 583:

Which of the following is true concerning the nature of hardware flow control (Choose all that apply)?

- A. uses CTS for Clear To Stop
- B. uses RTS for Request To Send
- C. uses RTS for Request To Stop
- D. uses CTS for Clear To Send

Answer: B, D

QUESTION 584:

Which of the following are layers covered by PPP (Choose all that apply)?

- A. Layer Two-High-Level Data Link Control
- B. Layer Three-Upper-Layer protocols
- C. LinkControl Protocol and Network Control Protocol
- D. Layer One-Physical
- E. LAYER Four

Answer: A, B, C, D

QUESTION 585:

To configure frame relay subinterface, you use the following command:

frame-relay interface-dlci

What is this command for?

- A. remove interface
- B. None of the answers
- C. loopback interface
- D. define local DLCI number
- E. define remote DLCI number
- F. select interface

Answer: D

QUESTION 586:

You are running commands on modemcap. You use the following command:

modemcap entry

What command is it for?

- A. add new entry or edit current entry

- B. view a particular modemcap entry.
- C. displays current attributes
- D. delete entry

Answer: B

QUESTION 587:

You like to display related statistics. What command can you use?

- A. show frame-relay set
- B. show frame-relay
- C. show frame-relay stat
- D. show frame-relay lmi

Answer: D

QUESTION 588:

Which of the following is true concerning the characteristics of a packet switching network (Choose all that apply)?

- A. more efficient than circuit switching
- B. bandwidth is dedicated
- C. bandwidth is shared
- D. Less costly than leased line

Answer: A, C, D