Exam : 642-821

Title : Building Cisco Remote Access Networks (BCRAN)

Ver : 06.20.05

Part 1

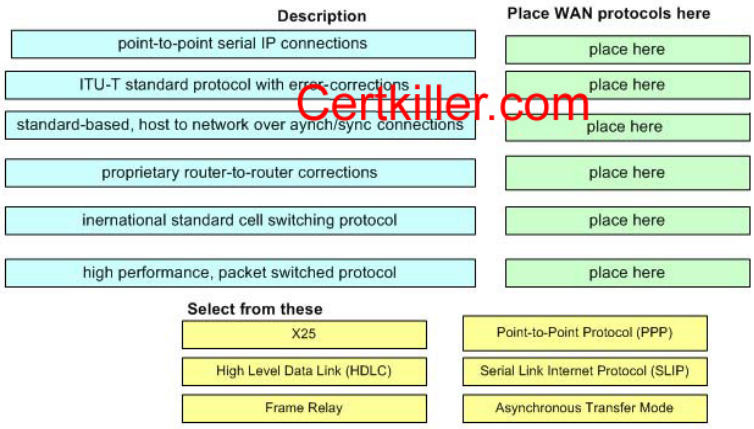
QUESTION 1
A bank called CK Savings and Trust is expanding and needs to connect a new branch to their head office on the other side of town. The new branch has twelve employees and each of them require constant access to the bank's central accounting system throughout all hours of the workday. What kinds 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

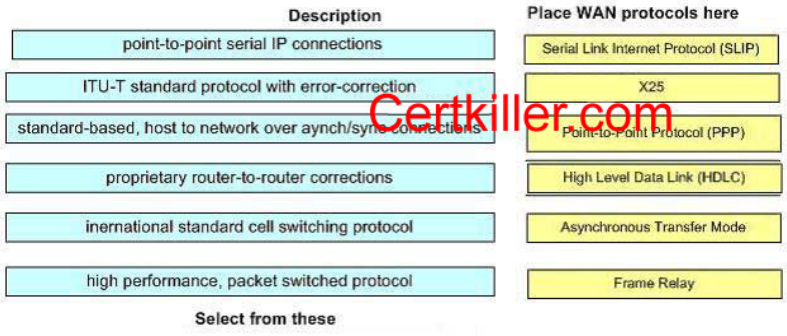
Answer: B, D

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:
• Leased line
• Frame relay
• X.25
• ISDN
• 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
Match the WAN protocols on the bottom to their proper descriptions:



Answer:



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_paper0900aecd800df195.shtml
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:
• Cost
• Authentication
• Availability
Reference:
Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 2-27

QUESTION 8
Three of the following WAN technologies are often employed at telecommuter sites, such as the end-users home office. Which three are they?

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

Answer: A, B, 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 BCRAN (642-821) ISBN: 1-58720-084-8
http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide_chapter09186a008019b57f.html

---

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

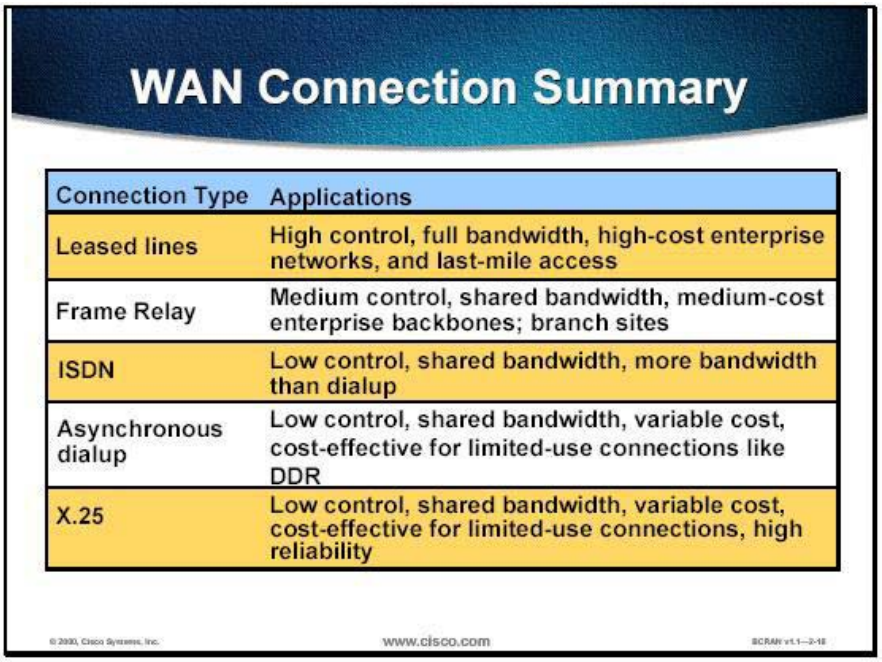
encountered is not obtaining an IP address dynamically on the Cisco router's Ethernet interface. Most Internet Service Providers (ISPs) allow only one host or PC behind the Cable Modem. Some ISPs assign an IP address to the PC based on the host name. Therefore, if you have a Cisco router behind the Cable 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.



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-topoint 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 highvolume 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 costeffective in the following situations:
• Long connect times
• 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-ondemand.

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 tranmission 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:
• is prominent in residential applications
• has 120 subchannels
• doesn't need a splitter
• 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 pointto-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) peforms 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_guide09186a00 80087992.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 userinteraction 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

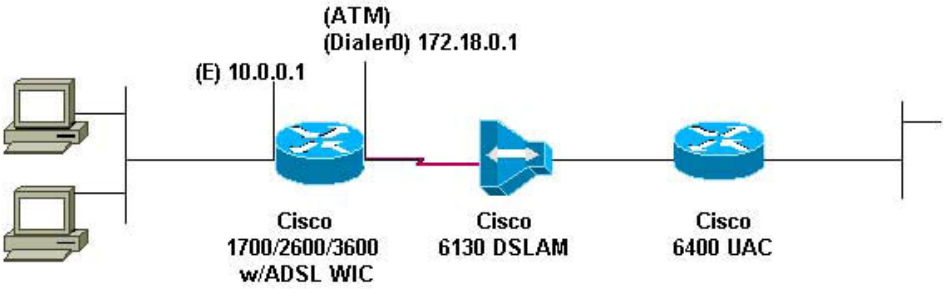
---

QUESTION 23
Router CK1 is configured as shown below:
interface ATM0/0
no ip address
pvc 8/35
encapsulation aaa15mux 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 an an aggregation router.

Answer: B

Explanation:
This following is an example of configuring a Cisco router as a PPPoA client. The command "encapsulation aal5muxppp 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 ip mroute-cache
 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/ CK1 75/ CK1 5/technologies_configuration_example09186a00 80093e60.shtml

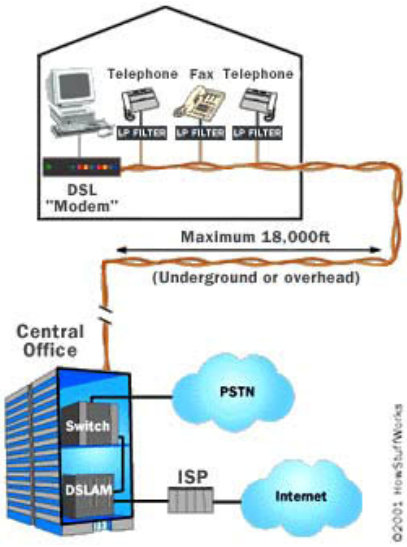
---

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 tbe 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:
• Dial up connection
• 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.
• Switched network - Several users share the same line or the bandwidth of the line.
There are two types of switched networks:
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, B, D

Explanation:
With dial up networking, a number of routed protocols are supported, including TCP/IP, NetBeui, IPX, and Appletalk.
Incorrect Answers:
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).

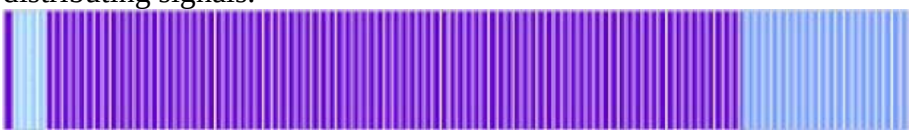
QUESTION 33
How is cable broadband technology able to transmit downstream and upstream data while at the same time delivering television content?

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.

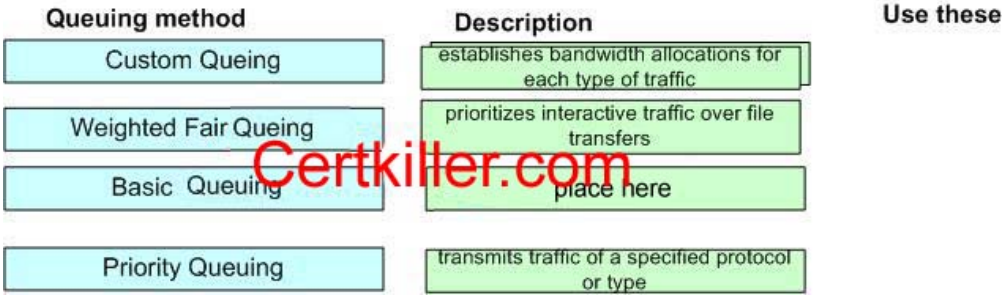


When a cable company offers Internet access over the cable, Internet information can use the same cables because the cable modem system puts downstream data -- data sent from the Internet to an individual computer -- into a 6-MHz channel. On the cable, the data looks just like a TV channel. So Internet 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 the queuing characteristics on the right next to the corresponding queuing method:

Answer:



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:

• Weighted fair queuing (WFQ) prioritizes interactive traffic over file transfers in order to ensure satisfactory response time for common user applications.

• Priority queuing ensures timely delivery of a specific protocol or type of traffic because that traffic is transmitted before all others.

• 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 35
Drag the queuing mechanisms on the left to its matching feature on the right hand side:

Answer:

QUESTION 36
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 Layer 2 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 75 percent 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 37
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.
Benefits
The Low Latency Queueing (LLQ) for IPSec encryption engines feature guarantees a certain level of crypto engine processing time for priority designated traffic.

Better Voice Performance
Voice 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 38
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 39
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 40
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_chapter09186a00800ca595.html

---

QUESTION 41
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 42
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 43
On a remote Certkiller router, the following command was issued:

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

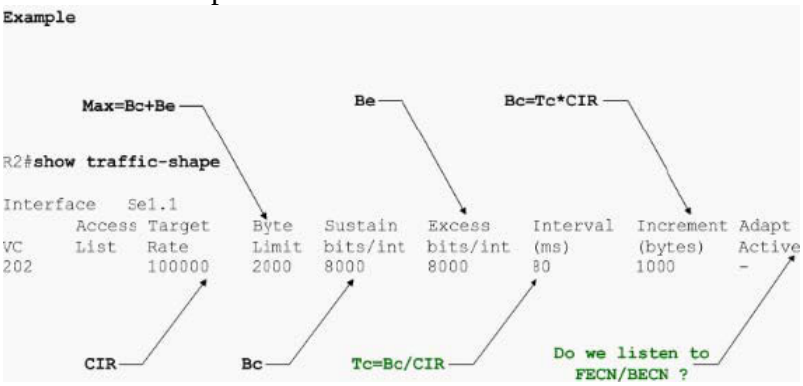
A. 1000
B. 2000
C. 8000
D. 100000

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 44
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 45
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 46
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:
Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 2-12
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfacct.htm#1014024

QUESTION 47
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 48
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 49
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 50
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:
• Multivendor interoperability, as specified by RFC 1990, which replaces RFC 1717
• Packet fragmentation, improving latency of each packet (supports RFC 1990 fragmentation and packet sequencing specifications)

• 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 51
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 52
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:
• Multi-vendor interoperability, as specified by RFC 1990, which replaces RFC 1717
• Packet fragmentation, improving latency of each packet (supports RFC 1990 fragmentation and packet sequencing specifications)
• 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 53
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 54
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 55
Multilink PPP is being utilized on the Certkiller network. What are some of the virtues of the multilink PPP protocol (MLP)? (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

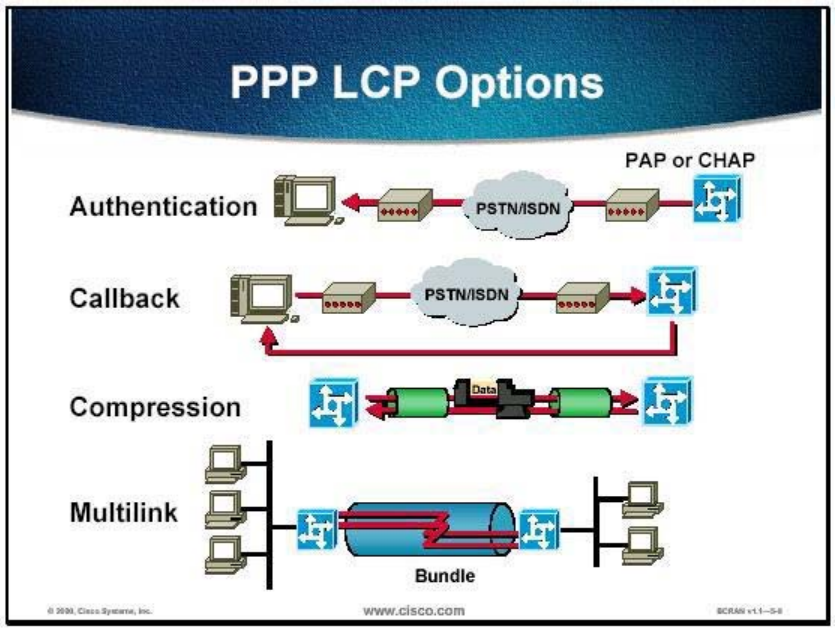
ensuring sequencing. MLP is most effective when used with ISDN.
MLP solves several problems related to load balancing across multiple WAN links, including the following:
• Multivendor interoperability, as specified by RFC 1990, which replaces RFC 1717
• Packet fragmentation, improving latency of each packet (supports RFC 1990 fragmentation and packet sequencing specifications)
• 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 56
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 57
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 58
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 59
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 60
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 61
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 62
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 63
Drag the authentication characteristics to its correct authentication protocol.

Answer:

Explanation:

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.

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:
• The authentication process uses a variable challenge value rather than a password.
• 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 64
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

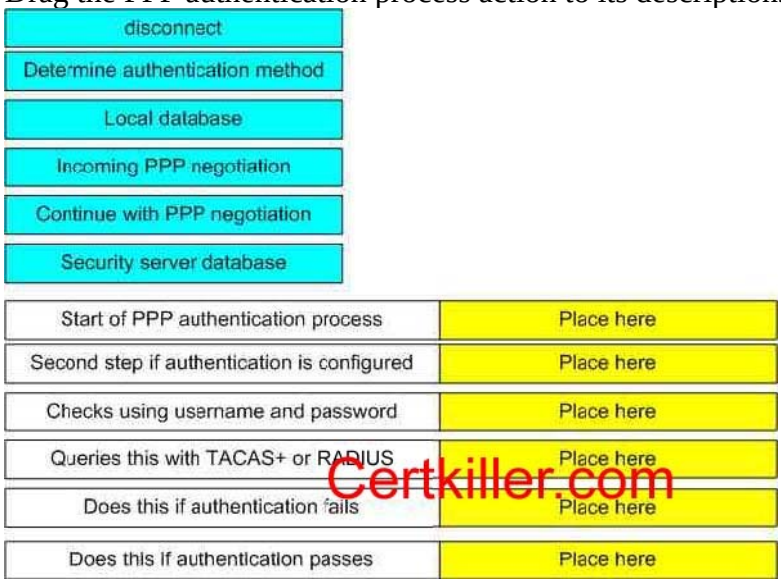
Answer: A, B, D

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:

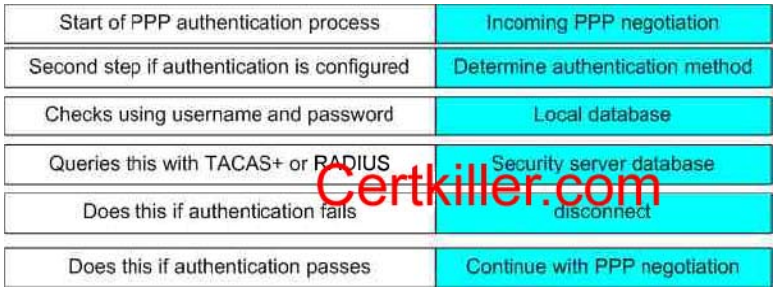
Type	Configuration Option
1	Maximum-Receive-Unit
2	Async-Control-Character-Map
3	Authentication-Protocol
4	Quality-Protocol
5	Magic-Number
6	RESERVED
7	Protocol-Field-Compression
8	Address-and-Control-Field-Compression
9	FCS-Alternatives
10	Self-Describing-Pad
11	Numbered-Mode
12	Multi-Link-Procedure
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 65
Drag the PPP authentication process action to its descriptions.



Answer:



QUESTION 66
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:
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 67
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-topoint 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 68
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

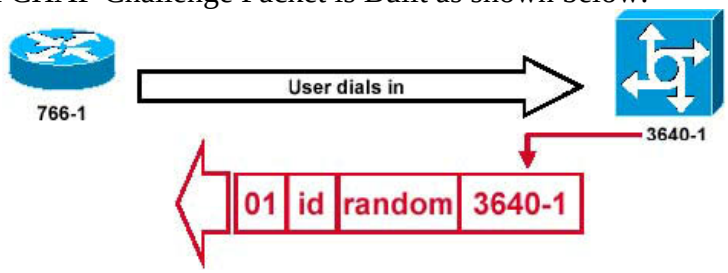
Explanation:
You can configure PPP on the following types of physical interfaces:
Asynchronous serial
HSSI
ISDN
Synchronous serial
By enabling PPP encapsulation on physical interfaces, PPP can also be in effect on calls placed by the dialer interfaces that use the physical interfaces, as the physical and data link layer attributes of the physical interface is used on the logical interfaces.

QUESTION 69
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:
o 01 = challenge packet type identifier.
o ID = sequential number that identifies the challenge.
o random = a reasonably random number generated by the router.
o 3640-1 = the authentication name of the challenger.
2. The ID and random values are kept on the called router. This is the local router, not the remote router.
3. The challenge packet is sent to the calling router. A list of outstanding challenges is maintained
Reference:

http://www.cisco.com/en/US/tech/ CK7 13/ CK5 07/technologies_tech_note09186a00800b4131.sh
tml

QUESTION 70
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 confirming 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 71
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_chapter09186a00800ca532.html#4676

QUESTION 72
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 73
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 74
Tess King 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_chapter09186a008007da0d.html

---

QUESTION 75
The Certkiller network is using VPNs to allow access to the corporate network. How is a Virtual Private Network (VPN) connection better then 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:

QUESTION 76
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.html

---

QUESTION 77
Match the IPSec VPN terms on the left to the position in the center that correctly matches the characteristics on the right:

Answer:

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

QUESTION 78
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 Difie-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

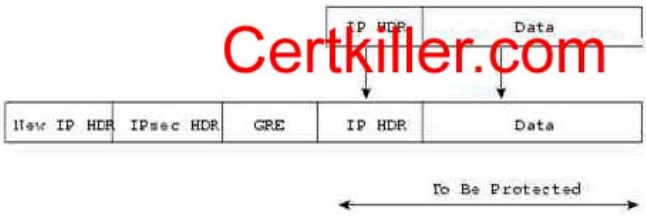
QUESTION 79
An IPSec datagram is depicted in the following diagram:

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 80
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_chapter09186a00800d981b.html#77018

QUESTION 81
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 82
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 83
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 end all their policies to the other peer, and each peer tries to find a match with its policies.
D. Both peers end 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 84
IPSec is being used for the Certkiller VPN. What is true about the security protocol ESP (Encapsualtion 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 85
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.

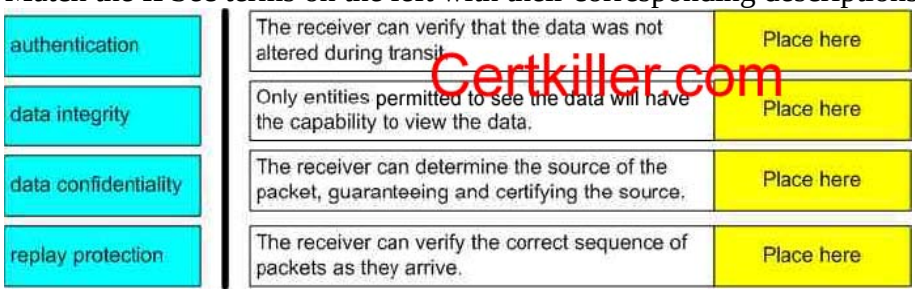
Answer: A, C, F

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 (draftietf-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; Cisco IOS 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 86
Match the IPSec terms on the left with their corresponding descriptions on the right.



Answer:

QUESTION 87
Which of the following statements is true about IPSec security associations (SAs)?

A. SAs contain unidirectional specifications only.
B. SAs describe the mechanics if implementing a key exchange protocol.
C. A single SA ca 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 88
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
pool-name	Name of the pool.
start-ip	Starting IP address that defines the range of addresses in the address pool.
end-ip	Ending IP address that defines the range of addresses in the address pool.
netmask *netmask*	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 *prefix-length*	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 rotary	(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 89
Although NAT (Network Address Translation) hant color=red size=3>QUESTION 89
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.

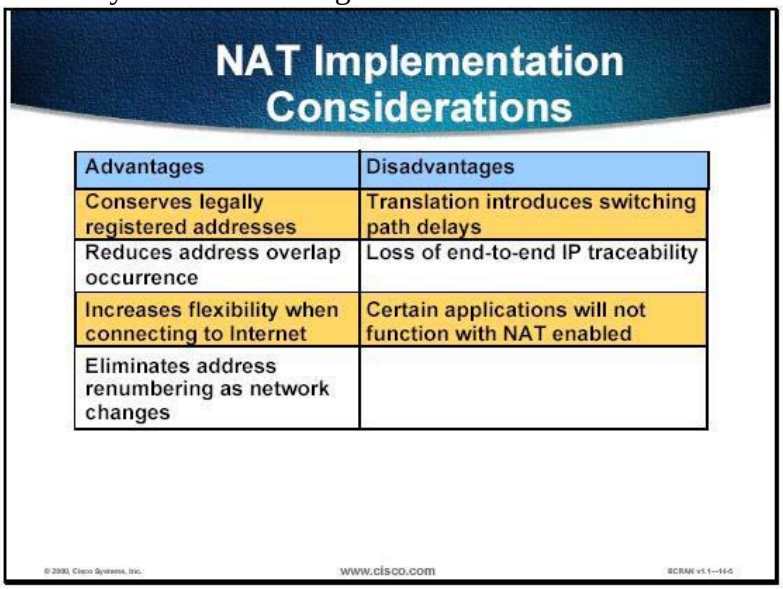
However, NAT introduces switching path delays and Loss of end-to-end traceability. Some applications will also not function when NAT is enabled.
Reference:
Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 14-6

QUESTION 90
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.



a

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

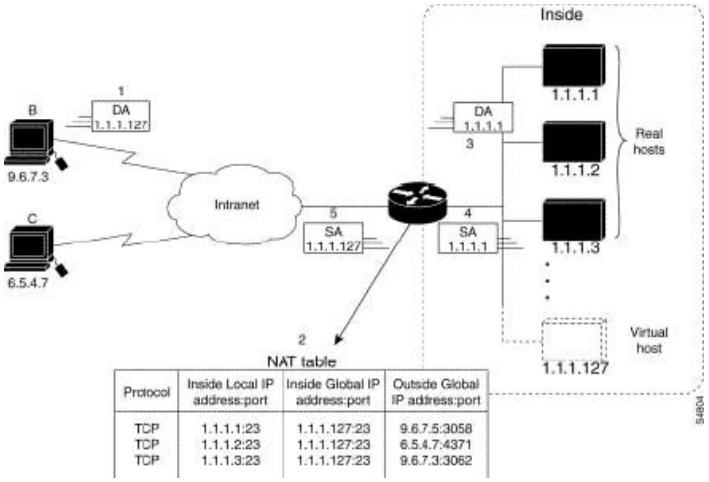
QUESTION 91
On the Certkiller network, you want traffic to the Internet servers to be load balanced. The Internet router is configured with Network Address Translation (NAT). Which

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

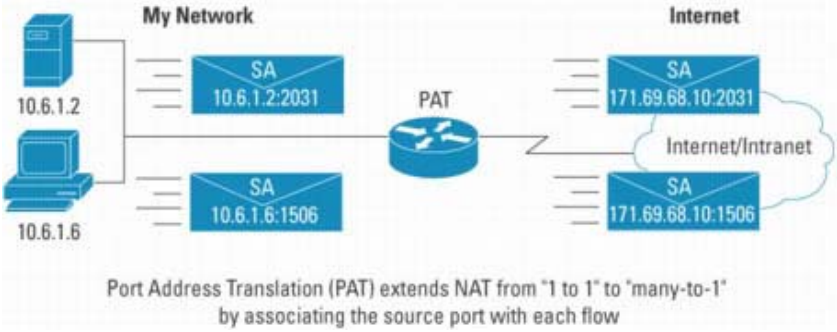
access list defines the virtual address. If a translation does not already exist, TCP packets from serial 0 (the outside interface) whose destination matches the access list are translated to an address from the pool.
ip nat pool real-hosts 192.168.15.2 192.168.15.15 prefix-length 28 type rotary
ip nat inside destination list 2 pool real-hosts
!
interface serial 0
ip address 192.168.15.129 255.255.255.240
ip nat outside
!
interface ethernet 0
ip address 192.168.15.17 255.255.255.240
ip nat inside
!
access-list 2 permit 192.168.15.1
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a00800ca6b4.html#29755

QUESTION 92
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:



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/ CK6 48/ CK3 61/technologies_white_paper09186a0080091cb9.shtml

---

QUESTION 93
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 94
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=*SM3:BCP=*DC1:NER=*SM1:NCP=*DC0:NEC=E0:NRS=Q1:CID=&S1.
usr_courier	HFL=&H1&R2:SPD=&B1:BER=&M4:BCP=&K1:NER=&M0:NCP=&K0:TPL=default.
usr_sportster	TPL=usr_courier.
hayes_optima	HFL=&K3:BER=&Q5:BCP=&Q9:NER=&Q0:NCP=&Q0:TPL=default.
viva	HFL=&K3:BER=&Q5:BCP=%C1:NER=&Q6:NCP=%C0:TPL=default.
telebit_t3000	HFL=S58=2:BER=S180=3:BCP=S190=1:NER=S180=0:NCP=S190=0:TPL=default.

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

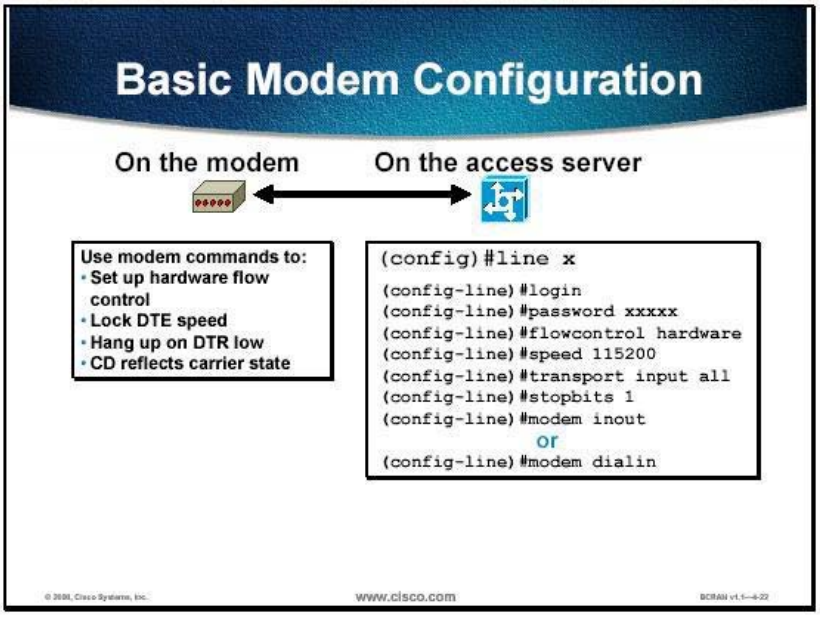
---

QUESTION 95
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 96
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 97
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 98
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 99
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 100
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