Part 2

QUESTION 101

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

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

Answer: D

Explanation:
Cisco routers do not accept incoming network connections to asynchronous ports (TTY lines) by default. You have to specify an incoming transport protocol, or specify transport input all before the line will accept incoming connections
Use the transport preferred command to specify which transport protocol is used on connections. Use the transport input and transport output commands to explicitly specify the protocols allowed on individual lines for both incoming and outgoing connections.
The protocol options that can be specified are:
all | lat | mop | nasi | none | pad | rlogin | ssh | telnet | v120
Reference:
http://cisco.com/en/US/products/sw/iosswrel/ps1828/products_configuration_guide_chapter0
9186a0080087329.html#25574

QUESTION 102

On one of the Certkiller routers the following configuration commands were entered:
router(config)#interface group-async 1
router(config)#group-range 1 7
What are the resulting consequences of these commands?

A. Assigns asynchronous interfaces 1 through 7 to a single master interface
B. Assign dialer privileges to interfaces async 1 through 7
C. Creates virtual asynchronous interfaces 1 through 7
D. Creates virtual TTY interfaces 1 through 7
E. Trunks asynchronous interfaces to increase modem bandwidth
F. Creates a modem pool on interfaces 1 through 7

Answer: A

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

interface group-async unit-number
no interface group-async unit-number
Using the interface group-async command, you create a single asynchronous interface to which other interfaces are associated as members using the group-range command. This one-to-many configuration allows you to configure all associated member interfaces by entering one command on the group master interface, rather than entering this command on each individual interface. You can create multiple group masters on a device; however, each member interface can be associated only with one group.
Example:
The following example defines asynchronous group master interface 0:
Router(config)# interface group-async 0
Related Commands

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

Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a00800874b0.html#1017445

QUESTION 103
Router CK1 has a modem attached to it, but you are unsure what type of modem it is. What command would you issue if you wanted the router to automatically discover the modem type, as well as automatically configure the settings?

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

Answer: A

Explanation:
Modem autoconfiguration is a Cisco IOS software feature that enables the router to issue the modem configuration commands, which frees the administrator from creating and maintaining scripts for each modem. The general syntax for modem autoconfiguration is as follows:
modem autoconfigure [discovery | type modemcap-entry-name]
The two command options for the modem autoconfigure command are as follows:
• type - This option con.gures modems without using modem commands, or so it is implied. The type argument declares the modem type that is defined in the modem capabilities database so that the administrator does not have to create the modem commands.

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

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

Reference:
Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8) Page 99

QUESTION 104
After completing your CCNP designation, your boss promoted you to the position of Vice President of Asynchronous Communications. Your first assignment is to configure the company's router to accept asynchronous connections, to allow for out of band management for the router.

Your project is to:
• Configure S0/1 for Asynchronous communication
• Set the line speed to 56K
• Set the flow control to hardware.
• Set the stop bits to one.
• Set the line password to "Budweiser".
• Configure the line to allow for both incoming and outgoing calls.
• Allow all protocols for incoming connections on the line.
• Set the loopback address to 192.168.0.1/32.

Once you complete your task, you have to check your work:
• Reverse telnet to the modem.
• Issue an AT command to login to modem configuration (modem should respond with OK)

What configuration commands will accomplish these tasks?

Answer:
Certkiller >
Certkiller 1> enable
Certkiller 1# Configure terminal
Certkiller 1(config)# Interface serial0/1

Certkiller 1(config-if)# Physical-layer async
Certkiller 1(config-if)# Exit
Certkiller 1(config)# Line 2
Certkiller 1(config-line)# Flowcontrol hardware
Certkiller 1(config-line)# Stopbits 1
Certkiller 1(config-line)# Password Budweiser
Certkiller 1(config-line)# Login
Certkiller 1(config-line)# Transport input all
Certkiller 1(config-line)# Speed 56000
Certkiller 1(config-line)# Modem inout
Certkiller 1(config-line)# Exit
Certkiller 1(config)# Interface loopback1
Certkiller 1(config-if)# Ip address 192.168.0.1 255.255.255.255
Certkiller 1(config-if)# Exit
Certkiller 1(config)# ip host modem 2002 192.168.0.01
Certkiller 1(config)# Exit
Certkiller 1# Copy run start
Certkiller 1# end
Certkiller 1> telnet 192.168.0.1 2002
at
Reference:
This configuration was verified in the Certkiller lab.

QUESTION 105
You are supervising an apprentice network technician, and he enters the following
commands on router Certkiller 1:
Certkiller 1#configure terminal
Certkiller 1(config)#line 10
Certkiller 1(config-line)#transport input all
Certkiller 1(config-line)#modem inout
What will be the resulting actions of these commands?

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

Answer: D

Explanation:
Cisco access servers support both incoming asynchronous line connections (forward
connections) and outgoing asynchronous line connections (reverse connections). For
example, a remote terminal user dialing into the access server through an asynchronous line
makes a forward connection; a user connects through an access server (reverse connection) to
an attached modem to configure the modem.
A host can make reverse Telnet connections to various types of devices attached to a Cisco

access server. Different port numbers (20xx, 40xx, and 60xx) are used because different data type and protocol negotiations will take place for different types of devices attached to the access server.

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

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

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

Each of these command options can also be specified individually.

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

Reference:

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

QUESTION 106

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

ip host remote 2007 157.23.23.96

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

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

Answer: B, E

Explanation:

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

Use the ip host configuration command to simplify reverse Telnet sessions with modems.

The ip host command maps an IP address of a port to a device name.

Reference:

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

QUESTION 107

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

A. async mode interactive

B. encapsulation ppp
C. speed 115200
D. modem inout
E. flowcontrol hardware
F. None of the above

Answer: C, D, E

Explanation:
The various line configuration options with their descriptions are displayed below:
(config-line)#exec - Allows the EXEC process on this line.
(config-line)#login - Sets a login password on this line. Without the password, no connection is allowed.
(config-line)#password - password Sets the password to be used when logging in to this line.
(config-line)#flowcontrol hardware - Uses RTS/CTS for flow control.
(config-line)#speed 115200 - Sets the maximum speed (in bits per second) between the modem and the access server. The speed command sets both the transmit and receive speed.
(config-line)#transport input all - Allows all protocols to be passed to the access server through this line.
(config-line)#stopbits - Sets the number of stop bits transmitted per byte.
(config-line)#modem inout - Uses the modem for both incoming and outgoing calls.
(config-line)#modem dialin - Uses the modem for incoming calls only (the default).
Incorrect Answers:
A: To return a line that has been placed into dedicated asynchronous network mode to interactive mode, thereby enabling the slip and ppp EXEC commands, use the async mode interactive interface configuration command. This command is used in Async interface mode, not in line mode.
B: PPP encapsulation is an interface configuration option.
Reference:
Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 4-25 & 4-26

QUESTION 108
If you were to set up a reverse Telnet session (from your router to an individual modem) what port range would you use?

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

Answer: B

Explanation:
A host can make reverse Telnet connections to various types of devices attached to a Cisco

access server. Different port numbers (20xx, 40xx, and 60xx) are used because different data type and protocol negotiations will take place for different types of devices attached to the access server.

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

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

References:
Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 4-18
Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)
Page 91

QUESTION 109
You are connected to router CK1 via line 0. Which of the following line types is associated with the line number zero on this router?

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

Answer: C

Explanation:
Cisco devices have the line numbers assigned in the following manner:
Console line (CON): Assigned line number 0
Asynchronous lines (TTY): Assigned line number n, where n represents the first physical line after the Console line. For example, TTY line 4 is assigned line number 4.
Auxiliary line (AUX): The auxiliary line is assigned the last TTY (async) line + 1. For example, if there can be n TTY lines, the Auxiliary line is assigned n+1. Note that the TTY lines are as recognized by Cisco IOS and not necessarily be present physically.

QUESTION 110
The Certkiller network administrator has connected a modem to the console port of a router. What is a reason for this type of connection? (Select all that apply)

A. Passwords can be recovered remotely.
B. Reverse Telnet has been configured.

C. Dial-on-demand routing has been configured.
D. The router needs to be accessible remotely.
E. None of the above.

Answer: A, D

Explanation:
Console Port Issues
There are several advantages to connecting a modem to the console port of a router instead of the AUX port; however, the disadvantages are significant.
Advantages of connecting a modem on the console port:
• You can recover passwords remotely. You may still need someone on-site with the router to toggle the power, but aside from that, it is identical to being there with the router.
• It is a convenient way to attach a second modem to a router without async ports. This is beneficial if you need to access the router for configuration or management and leave the AUX port free for dial-on-demand routing (DDR).
• Some routers (for example, Cisco 1600s) do not have AUX ports. If you want to connect a modem to the router and leave the serial port(s) free for other connections, the console is the only option.
Disadvantages of connecting a modem on the console port:
• The console port does not support RS232 modem control (data set ready/Data Carrier Detect (DSR/DCD), data terminal ready (DTR)). Therefore, when the EXEC session terminates (logout), the modem connection does not drop automatically; the user needs to manually disconnect the session.
• More seriously, if the modem connection should drop, the EXEC session does not automatically reset. This can present a security hole, in that a subsequent call into that modem will be able to access the console without entering a password. You can make the hole smaller by setting a tight exec-timeout on the line. However, if security is important, use a modem that can provide a password prompt.
• Unlike other async lines, the console port does not support hardware (Clear to Send/Ready to Send (CTS/RTS) flow control. It is recommended to use no flow control. If data overruns are encountered, however, you can enable software (XON/XOFF) flow control.
• The console ports on most systems only support speeds of up to 9600 bps.
• The console port lacks reverse telnet capability. If the modem loses its stored initialization string, the only remedy is to physically disconnect the modem from the router and attach it to another device (such as an AUX port or a PC) to reinitialize. If a modem on an AUX port loses its initialization string, you can use reverse telnet remotely to correct the problem.
• You cannot use a console port for dial-on-demand routing; it has no corresponding async interface.

QUESTION 111
You are logged in to router CK1 and need to change the configuration of the line ports used for modems. Which of the following parameters are set using the line command?

(Choose all that apply)

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

Answer: A, E

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

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

Reference:
http://www.cisco.com/en/US/tech/ CK8 01/ CK3 6/technologies_tech_note09186a008009428b.sht ml

---

QUESTION 112
Which of the following are valid functions that chat scripts perform? (Choose all that apply)

A. Modem configuration
B. Dialing and remote login
C. Failure detection
D. Incoming call filtering

Answer: A, B, C

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

QUESTION 113
You are running commands on modemcap. You use the following command on router CK1 :
modemcap entry
What is this command used for?

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

Answer: C

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

modem-type	Type of supported modemcap entry

Modemcaps are displayed within the configuration file and can be edited using the modemcap edit command. The modemcap entry command does not display values that are not set in the modem.
Use the modemcap entry command with the show modemcap command to interpret the capability of the specified modem.

QUESTION 114
You are configuring a new Cisco router to operate with a modem attached to the aux port. Which of the following are valid functions of the lock DTE modem attribute that can be used on this router?

A. Disable UART.
B. Enable UART.
C. Locks the data speed between the computer motherboard and the RS232 port.

D. Locks the data speed between the modem and the DTE device.

Answer: D

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

QUESTION 115
Your boss requires you to use the modem for both incoming and outgoing calls. What configuration command will enable this?

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

Answer: A

Explanation:
To configure a line for both incoming and outgoing calls, use the modem inout line configuration command.
Default
No modem control.
Command Mode
Line configuration.
Usage Guidelines
This command applies to the auxiliary port only.

QUESTION 116
On an asynchronous modem line, which of the following are NOT functions that chat scripts perform? (Choose all that apply)

A. Logging into a remote system.
B. Sending messages from one telnet session to another.
C. Instructing the modem to dial out.
D. Filtering incoming calls.
E. Initializing the directly-attached modem.

Answer: B, D

Explanation:
Chat scripts are strings of text used to send commands for modem dialing, logging in to remote systems, and initializing asynchronous devices connected to an asynchronous line. On

a router, chat scripts can be configured on the auxiliary port only. A chat script must be configured to dial out on asynchronous lines. You also can configure chat scripts so that they can be executed automatically for other specific events on a line, or so that they are executed manually.

QUESTION 117
With regards to the dialer pool, what optional keyword command can you use to resolve potential contention problems on this dialer pool? (Type in answer below)

Answer: priority

Explanation:
Dialer pool - Each interface references a dialer pool, which is a group of physical interfaces associated with a dialer profile. A physical interface can belong to multiple dialer pools. Contention for a specific physical interface is resolved by configuring the optional priority command.

QUESTION 118
In an ISDN BRI circuit; what range of values are assigned for Valid Dynamic TEI (Terminal Endpoint Identifier)?

A. 128-256
B. 25-62
C. 64-126
D. 1-24

Answer: C

Explanation:
A terminal endpoint can be any ISDN-capable device attached to an ISDN network. The TEI is a number between 0 and 127, where 0-63 is used for static TEI assignment, 64-126 are used for dynamic assignment, and 127 is used for group assignments. (0 is used only for PRI.) The TEI provides the physical identifier, and the Service Access Point Identifier (SAPI) carries the logical identifier.
The process of assigning TEIs differs slightly between North America and Europe. In North America, Layer 1 and Layer 2 are activated at all times. In Europe, the activation does not occur until the call setup is sent (known as "first call"). This delay conserves switch resources. In Germany and Italy, and in other parts of the world, the procedure for TEI assignment can change according to local practices.
In other countries, another key piece of information to obtain is the bus type. Supported types are point-to-point or point-to-multipoint connection styles. In Europe, if you are not sure which is supported, specify a point-to-multipoint connection, which will enable dynamic TEI addressing. This is important if BRI connections are necessary, because Cisco does not support BRI using TEI 0, which is reserved for PRI TEI address 0. If you see a TEI of 0 on a BRI, it means that a dynamic assignment has not yet occurred, and the BRI may not be talking to the switch. In the United States, a BRI data line is implemented only in a point-topoint

configuration.
Reference:
Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)
Page 151

QUESTION 119
Which T1 controller command would you use when configuring the timeslots on an
ISDN PRI interface on router CK1 , which is using a T1 ISDN line?

A. linecode
B. framing
C. pri-group
D. isdn switch-type
E. barcode

Answer: C

Explanation:
To specify an ISDN PRI group on a channelized T1 or E1 controller, and to release the ISDN
PRI signaling time slot, use the pri-group timeslots command in controller configuration
mode.
pri-group timeslots timeslot-range [nfas_d {backup | none | primary {nfas_int number |
nfas_group number | rlm-group number}} | service]
Syntax Description

timeslot-range	A value or range of values for time slots on a T1 or E1 controller that consists of an ISDN PRI group. Use a hyphen to indicate a range. Note Groups of time slot ranges separated by commas (1-4,8-23 for example) are also accepted.
nfas_d {backup	none	primary}	(Optional) Configures the operation of the ISDN PRI D channel. • backup—The D-channel time slot is used as the Non-Facility Associated Signaling (NFAS) D backup. • none—The D-channel time slot is used as an additional B channel. • primary—The D-channel time slot is used as the NFAS D primary. The primary keyword requires further interface and group configuration:

primary {nfas_int number nfas_group number| rlm-group number}		– nfas_int *number*—Specifies the provisioned NFAS interface as a value; value is a number from 0 to 8. – nfas_group *number*— Specifies the NFAS group. – rlm-group *number*—Specifies the Redundant Link Manager (RLM) group and release the ISDN PRI signaling channel.
service		(Optional) Configures service type mgcp for Media Gateway Control Protocol service.

Defaults:
No ISDN PRI group is configured. The switch type is automatically set to the National ISDN switch type (primary-ni keyword) when the pri-group timeslots command is configured with the rlm-group subkeyword.
Incorrect Answers:
D: This command is used to specify the central office switch type on the ISDN interface, or to configure the Cisco PRI interface to support QSIG signaling. This command is done in the interface configuration mode. Furthermore, we believe this question to be trying to identify the difference between T1 and E1 in regards to the timeslot assignments.

QUESTION 120
A new T1 line is being provisioned for the Certkiller network. What are your configuration options when configuring T1/E1 line-codes? (Choose all that apply.)

A. AMI
B. ESF
C. B8ZS
D. SF
E. CRC4

Answer: A, C

Explanation:
The valid line-code options for T1/E1 are: AMI, B8ZS, and HDB3.
Use the linecode command to identify the physical layer signaling method to satisfy the ones density requirement on the provider's digital facility. Without a sufficient number of ones in the digital bit stream, the switches and multiplexers in a WAN can lose their synchronization for transmitting signals.
* AMI Alternate Mark Inversion. Used for T1 configurations.
* B8ZS Binary 8-zero substitution. Use for T1 PRI configurations.
* HDB3 High Density Bipolar 3. Use for E1 PRI configurations.
Binary 8-zero substitution (B8ZS) accommodates the ones density requirements for T1

carrier facilities using special bipolar signals encoded over the digital transmission link. It allows 64 kbps (clear channel) for ISDN channels. Settings for these two Cisco IOS software controller commands on the router must match the framing and line-code types used at the T1/E1 WAN provider's CO switch.
Incorrect Answers:
A, C: SF, ESF, and CRC4 are valid framing types, not line coding options.
Reference:
Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 2-12 ; 2-13 & 7-68

QUESTION 121
A new T1 circuit is being provisioned for a new remote Certkiller location. Which of the following framing types are associated with T1/E1 lines? (Choose all that apply.)

A. AMI
B. ESF
C. B8ZS
D. SF
E. CRC4

Answer: B, D, E

Explanation:
The valid framing types on a T1 controller are Super Frame (SF) and Extended Super Frame (ESF). CRC4 is a framing option used on E1 lines.
Incorrect Answers:
A, C: AMI and B8ZS are valid line coding types, not framing types.
Reference:
Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 7-68

QUESTION 122
Router CK1 uses an ISDN line as a backup connection to the primary frame relay link.
On this router you enter the following command:
backup load 60 5
What effect will this change make? (Choose two)

A. The backup link activates when the primary link exceeds 60 percent of bandwidth.
B. The backup link activates when the primary link exceeds 60 kbps.
C. The backup link deactivates when the primary link falls to 5 percent bandwidth.
D. The backup link deactivates when the combined load falls to 5 percent bandwidth.
E. The backup link deactivates when the combined load falls to 5 kbps.

Answer: A, D

Explanation:
The commands backup load & no backup load are used to add and remove backup links

based on traffic congestion. The command has two number variables which are percentage functions. The first one is the enable threshold and the second one is the disable load variable. So in the above example when the primary link exceeds 60% of its maximum bandwidth the backup link activates. The backup link will continue to be activated until the combined load on both links drops to 5% of maximum bandwidth (as network usage peaks tend to spike high periodically).
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_command_reference_chapter09186a00800ca527.html

QUESTION 123
The Certkiller network has offices in Costa Rica and Brazil that communicate with the head office in Los Angeles by way of ISDN. Since each remote office is located in a different country they have unique dial requirements. Which commands would you enter on the central router to allow multiple physical interfaces to be shared by the multiple remote sites while still allowing them to keep their unique dial requirements? (Choose two)

A. The dialer pool command
B. The dialer-list command
C. The dialer pool-member command
D. The dialer-group command
E. The dialer hunt-group command

Answer: A, C

Explanation:
A: Dialer-pool is a command which assigns a dialer interface to a specific dialer-pool.
C: Dialer pool-member makes a physical interface a member of a dialer pool, which consists of different logical interfaces with specific configurations.
Incorrect Answers:
B, D: Dialer-list and dialer-group are commands to specify an interesting traffic for the interface. When interesting traffic is seen by the router, an ISDN connection is made. If it is already established, the dialer idle timeout value is set to the maximum value.
E: Dialer hunt-group - there is no such command in Cisco IOS.

QUESTION 124
What configuration command would you execute to define a rotary group?

A. The dialer pool command
B. The rotary-group command
C. The interface rotary command
D. The interface dialer command
E. The dialer rotary-group command

Answer: D

Explanation:
Dialer rotary groups allow you to apply a single logical interface configuration to a set of physical interfaces. Dialer rotary groups are useful in environments that have multiple calling destinations. A dialer rotary group is defined by specifying a dialer interface. Physical interfaces are assigned to the dialer rotary group and inherit all of the dialer interface configuration parameters. When many destinations are configured, any of the physical interfaces in a rotary group can be used for outgoing calls.
interface dialer group-number - Defines a dialer rotary group. The group number ranges from 0 through 255.
Incorrect Answers:
A: Dialer pool - is for dialer profiles not for rotary groups.
B, C: There are no such commands in Cisco IOS.
E: This assigns an interface to an already specified rotary-group.

QUESTION 125
A new ISDN circuit is being provisioned for a Certkiller location. When is it necessary to configure the SPID on an ISDN BRI interface?

A. When you want to use both B channels.
B. When you want to use the D channel for low-speed data.
C. When required by your service provider.
D. When you want to use an ISDN BRI interface for outgoing calls.

Answer: C

Explanation:
A SPID is the Service profile identifier, which is a number that some service providers use to define the services to which an ISDN device subscribes. The ISDN device uses the SPID when accessing the switch that initializes the connection to a service provider. SPIDS are normally used to identify the ISDN circuit to the ISDN switch by many service providers, but not all. Contact your ISP for details on whether or not this information needs to be programmed into your equipment.
Reference:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t3/brivi cfm.pdf

---

QUESTION 126
Which of the following commands is capable of configuring an interface for PRI and specifying the number of fixed timeslots on that circuit?

A. pri-group
B. interface serial
C. dialer-group
D. isdn switch-type
E. None of the above

Answer: A

Explanation:
You can configure the PRI group to include all available time slots, or you can configure a select group.....
pri-group [timeslots range]
no pri-group
To specify ISDN Primary Rate Interface (PRI) on a channelized T1 card on the Cisco 7000 series, use the pri-group controller configuration command. Use the no pri-group command to remove the ISDN PRI.
timeslots range (Optional) Specifies a single range of values from 1 to 23.
When configuring NFAS for channelized T1 controllers configured for ISDN, you use an extended version of the ISDN pri-group command to specify the following:
• Range of PRI timeslots to be under the control of the D channel (timeslot 24)
• Function to be performed by timeslot 24 (primary D channel, backup, or none); the latter specifies its use as a B channel
• Group identifier number for the interface under control of this D channel
References:
http://www.prz.tu-berlin.de/docs/misc/ciscodoc/data/doc/software/10_3/rpcs/78791.htm
http://www.cisco.com/en/US/products/hw/univgate/ps501/products_configuration_guide_cha
pter09186a008007df5b.html

QUESTION 127
When configuring an ISDN interface; what purpose does the command pri-group fulfill?

A. Configures serial interfaces created on a channelized E1 or T1 controller for ISDN PRI signaling.
B. Configured the central office switch type for the ISDN PRI interfaces.
C. Specifies which timeslots are allocated on the digital facility of the provider.
D. Configured ISDN B-channel interfaces for VoIP applications that require release of the ISDN PRI signaling time slots.
E. None of the above.

Answer: C

Explanation:
Router(config-if)# pri-group [timeslots range]
This command configures the PRI group for either T1 or E1 to carry voice traffic. For T1, available time slots are from 1 through 23; for E1, available time slots are from 1 through 31.
You can configure the PRI group to include all available time slots, or you can configure a select group of time slots for the PRI group.
References: "Q.931 User-Side and Network-Side Switch Support"
http://www.cisco.com/en/US/products/sw/iosswrel/ps1834/products_feature_guide09186a00

QUESTION 128
Router CK1 is configured for ISDN as displayed below:
Interface BRI0
ip address 172.20.10.2 255.255.255.0
encapsulation ppp
dialer idle-timeout 30
dialer watch-disable 15
dialer load-threshold 1 outbound
dialer map ip 172.20.10.1 name RouterTK broadcast 5551111
dialer map ip 172.22.53.0 name RouterTK broadcast 5551111
dialer watch-group 8
dialer-group 8
isdn switch-type basic-ni
isdn spid1 51255526220101 5552222
isdn spid2 51255528230101 5552223
ppp authentication chap
ppp multilink
!
dialer watch-list 8 ip 172.22.53.0 255.255.255.0
access-list 101 remark Define Interesting Traffic
access-list 101 deny ospf any any
access-list 101 permit ip any any
dialer-list 8 protocol ip list 101
What is the result of the command "dialer watch-group"?

A. Any IP traffic, except OSPF traffic, will cause interface BRI0 to dial RouterTK.
B. When the watched route, 172.22.53.0/24, is removed from the routing table and there
is no other valid route, dialer watch then initiates a call to RouterTK.
C. When the watched route, 172.22.53.0/24, is removed from the routing table,
regardless of whether there is another valid route pointing to an interface other than
interface BRI0, dialer watch initiates the call to RouterTK.
D. When the load threshold is met and any IP traffic, except OSPF traffic, is destined for
172.22.53.0/24 network, the dialer watch will initiate the call to RouterTK.

Answer: B

Explanation:
Dialer Watch is a backup feature that integrates dial backup with routing capabilities. Prior
dial backup implementations used the following conditions to trigger backup:
• Interesting packets were defined at central and remote routers using Dial on Demand
routing (DDR).
• Connection loss occurred on a primary interface using a back up interface with
floating static routes.

• Traffic thresholds were exceeded using a dialer load threshold.

Prior backup implementations may not have supplied optimum performance on some networks, such as those using Frame Relay multipoint subinterfaces or Frame Relay connections that do not support end-to-end PVC status updates.

Dialer Watch provides reliable connectivity without relying solely on defining interesting traffic to trigger outgoing calls at the central router. Dialer Watch uses the convergence times and characteristics of dynamic routing protocols. Integrating backup and routing features enables Dialer Watch to monitor every deleted route. By configuring a set of watched routes that define the primary interface, you are able to monitor and track the status of the primary interface as watched routes are added and deleted. Monitoring the watched routes is done in the following sequence:

1. Whenever a watched route is deleted, Dialer Watch checks to see if there is at least one valid route for any of the defined watched IP addresses.

2. If no valid route exists, the primary line is considered down and unusable.

3. If a valid route exists for at least one of the defined IP addresses, and if the route is pointing to an interface other than the backup interface configured for Dialer Watch, the primary link is considered up.

4. If the primary link goes down, Dialer Watch is immediately notified by the routing protocol and the secondary link is brought up.

5. Once the secondary link is up, at the expiration of each idle timeout, the primary link is rechecked.

6. If the primary link remains down, the idle timer is indefinitely reset.

7. If the primary link is up, the secondary backup link is disconnected. Additionally, you can set a disable timer to create a delay for the secondary link to disconnect, after the primary link is reestablished.

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1826/products_feature_guide09186a00 80080ebf.html

---

QUESTION 129

One of the Certkiller routers is configured for ISDN as shown below:

Interface serial0
ip address 192.168.10.1 255.255.255.0
Backup interface bri0
Backup delay 5 10
Interface bri0
ip address 192.168.11.2 255.255.255.0
dialer idle-timeout 900
dialer-group 1
Based on this information, what is true about the above configuration?

A. The ISDN BRI line will go to "standby" mode 900 seconds after the serial interface reactivates.

B. The ISDN BRI line will go to "standby" mode 10 seconds after the serial interface reactivates.

C. The ISDN BRI line will deactivate the primary line reaches 10% utilization.

D. The ISDN BRI line will go to standby after 900 seconds, but will reactivate if the primary line reaches 10% utilization.

Answer: B

Explanation:
If you look at carefully at this portion of command:
Interface serial0
ip address 192.168.10.1 255.255.255.0
Backup interface bri0
Backup delay 5 10
You'll notice that the serial interface (serial0) is backed up by the BRI interface (BR0). The command Backup delay 5 10 has two number variables. The first number (5) commands that if serial0 were to be compromised, BRI0 is to take over after 5 seconds. The second number (10) states that if serial0 were to somehow reactivate, BRI0 will continue to remain active for 10 seconds until going into standby mode. Having a backup system wait a few seconds before kicking in is a smart feature because many times an interface may only fail for a few seconds, and five seconds is a typical length of a user's patience. The longer reactivation time is good, because the original line has to prove that it's capable of staying active for 10 seconds before earning its credibility again.

QUESTION 130
Two Certkiller routers are set up for ISDN as shown in the diagram below, along with the partial configuration of router Certkiller 1:
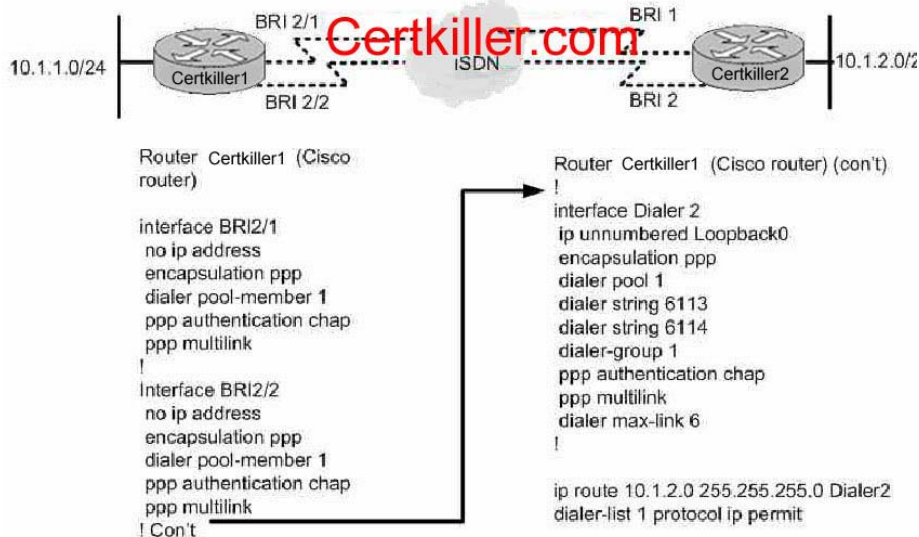
Assuming that there are only two BRI interfaces on Router Certkiller 1; how many B channels will end up forming the multilink PPP bundle between routers Certkiller 1 and Certkiller 2?

A. Four ISDN B channels will form the Multilink PPP bundle.
B. No Multilink PPP bundle will be formed because the dialer interface is not associated with the physical interfaces.

C. Two ISDN B channels will form the Multilink PPP bundle.
D. No Multilink PPP bundle will be formed due to there being no load threshold configured.

Answer: D

Explanation:
To configure bandwidth on demand by setting the maximum load before the dialer places another call to a destination, use the dialer load-threshold command in interface configuration mode.
When the cumulative load of all UP links (a number n) exceeds the load threshold the dialer adds an extra link and when the cumulative load of all UP links minus one (n - 1) is at or below load threshold then the dialer can bring down that one link. The dialer will make additional calls or drop links as necessary but will never interrupt an existing call to another destination.
The load argument is the calculated weighted average load value for the interface; 1 is unloaded and 255 is fully loaded. The load is calculated by the system dynamically, based on bandwidth. You can set the bandwidth for an interface in kilobits per second, using the bandwidth command.
The load calculation determines how much of the total bandwidth you are using. A load value of 255 means that you are using one hundred percent of the bandwidth. The load number is required.
The PPP multilink bundle is activated only if dialer load-threshold is in the router configuration.

QUESTION 131
The Certkiller ISDN configuration of Router A is displayed below:
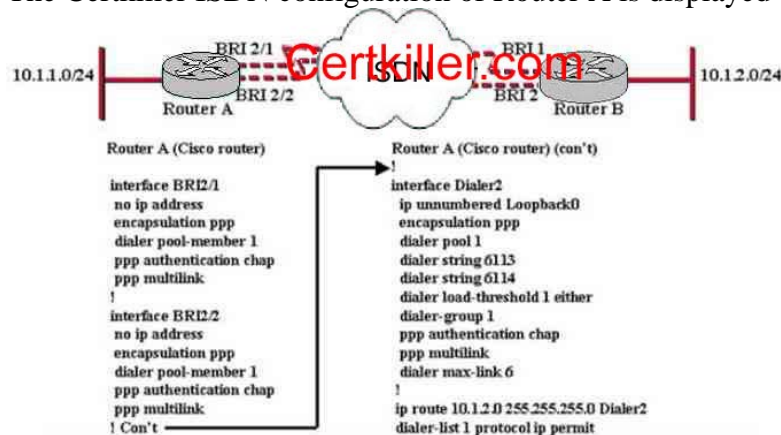
Assuming that there are only two BRI interfaces on Router Certkiller 1; how many B channels will end up forming the multilink PPP bundle between routers A & B when the total load threshold continuously remains greater then 50%?

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

E. 5
F. 6

Answer: D

Explanation:
When the cumulative load of all UP links (a number n) exceeds the load threshold the dialer adds an extra link and when the cumulative load of all UP links minus one (n - 1) is at or below load threshold then the dialer can bring down that one link. The dialer will make additional calls or drop links as necessary but will never interrupt an existing call to another destination.
The load argument is the calculated weighted average load value for the interface; 1 is unloaded and 255 is fully loaded. The load is calculated by the system dynamically, based on bandwidth. You can set the bandwidth for an interface in kilobits per second, using the bandwidth command.
The load calculation determines how much of the total bandwidth you are using. A load value of 255 means that you are using one hundred percent of the bandwidth. The load number is required.
In this example, since the load is set to only 1 (either incoming or outgoing) the maximum number of BRI links will be bonded in the bundle. Since there are 2 data channels per BRI interface, all 4 of them will be utilized.

QUESTION 132
You are a network technician at Certkiller and you've just finished entering these commands:
Certkiller A(config)#ip route 172.16.1.0 255.255.255.0 bri0
Certkiller A(config)#interface bri0
Certkiller A(config-if)#dialer map ip 10.1.1.1 name Certkiller B 5551111
Certkiller A(config-if)#dialer map ip 10.1.1.2 name Certkiller C 5552222
Certkiller A(config-if)#dialer map ip 10.1.1.3 name Certkiller D 5553333
As a result of your configuration; what will happen when traffic destned to host 172.16.1.1 is noticed by router Certkiller A?

A. The packets destined for the 172.16.1.0 network will be dropped.
B. The packets destined for the 172.16.1.0 network will be sent to the default route.
C. A DDR call will be placed first to router Certkiller B, and if it is busy, then to Certkiller C and Certkiller D.
D. A DDR call will be placed to router Certkiller B and the packets routed to 10.1.1.1.

Answer: C

Explanation:
The command dialer map protocol next-hop-address [name hostname]
[speed 56|64] [broadcast]
[dial-string[:isdn-subaddress]
configures a serial interface or ISDN interface to call one or multiple sites. The name

parameter refers to the name of the remote system. The speed parameter is the line speed in kilobits per second to use. The broadcast parameter indicates that broadcasts should be forwarded to this address. The dial-string[:isdn-subaddress] is the number to dial to reach the destination and the optional ISDN subaddress. In this case, since there are 3 separate dialer maps, the BRI interface will attempt to dial out to the remote offices until a call can be made and the BRI interface comes up.
Reference:
Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 7-32

QUESTION 133
Two Certkiller routers are connected via an ISDN network as displayed below:

Which dialer map command would you use to configure Certkiller -1 to successfully connect to Certkiller -2?

A. dialer map ip 10.120.1.2 name Certkiller -2 4085551111
B. dialer map ip 10.120.1.2 name Certkiller -1 4085551111
C. dialer map ip 10.120.1.2 name Certkiller -2 4085552222
D. dialer map ip 10.120.1.1 name Certkiller -1 4085552222
E. dialer map ip 10.120.1.1 name Certkiller -2 4085552222

Answer: C

Explanation:
The correct configuration syntax for both routers is displayed below:
Certkiller -1:
Certkiller -1(config)#interface bri 0
Certkiller -1(config-if)#ip address 10.120.1.1 255.255.255.0
Certkiller -1(config-if)#encapsulation ppp
Certkiller -1(config-if)#dialer map ip 10.120.1.2 name Certkiller -2
4085552222
Certkiller -2:
Certkiller -2(config)#interface bri 0
Certkiller -2 (config-if)#ip address 10.120.1.2 255.255.255.0
Certkiller -2 (config-if)#encapsulation ppp
Certkiller -2 (config-if)#dialer map ip 10.120.1.1 name Certkiller -1
4085551111
Reference:
Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 7-32

QUESTION 134
Which command would you use if you had a high traffic ISDN line and you wanted to timeout an idle connection for the sake of freeing up the line so it can be used to call a

second location?

A. dialer idle-timeout
B. dialer fast-idle
C. dialer wait-for-carrier-time
D. dialer in-band
E. None of the above

Answer: B

Explanation:
dialer fast-idle seconds - Specifies the amount of time that a connected line remains idle before it is disconnected to allow a second call destined for a second location over this same line to be placed. This command, used on lines for which there is contention, applies to inbound and outbound calls. The line is considered idle when no interesting packets are being sent across it. If the line becomes idle for the configured length of time, the current call is disconnected immediately and the line is available for new calls. The default fast-idle time is 20 seconds. This is an inactivity timer for contended interfaces.
Incorrect Answers:
A: dialer idle-timeout seconds - Specifies the idle time (in seconds) before the line is disconnected. The default is 120 seconds. This command, which is used on lines for which there is no contention, applies to inbound and outbound calls. This is an inactivity timer.
C: dialer wait-for carrier-time seconds - Specifies how long (in seconds) to wait for carrier tone. On asynchronous interfaces, this command sets the total time allowed for the chat script to run. The default time is 30 seconds. For asynchronous lines, it is better to increase the value of this parameter to 60 seconds to compensate for the possible delay in the telephone network.
D: dialer in-band - Enables DDR on an asynchronous interface.
Reference:
Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 8-7 and 8-8

QUESTION 135
Router CK1 is configured as a PPP callback server.
What must be configured on CK1 to ensure that improperly configured callback clients are disconnected?

A. ppp authentication chap
B. pp authentication pap
C. dialer callback-secure
D. ppp callback request
E. callback forcedwait 15

Answer: C

Explanation:
To enable callback security, use the dialer callback-secure interface configuration command.

This command affects those users that are not authorized to be called back with the dialer callback-server command. If the username (hostname in the dialer map command) is not authorized for callback, the call will be disconnected if the dialer callback-secure command is configured. If the dialer callback-secure command is not configured, the call will not be disconnected. In either case, callback has not occurred.

The following partial example configures BRI0 with the commands required to make it function as the callback server on the shared network. Callback security is enabled on BRI0, such that any user other than atlanta will be disconnected and not called back:

interface BRI0
ip address 172.16.1.9 255.255.255.0
encapsulation ppp
dialer callback-secure
dialer enable-timeout 2
dialer map ip 172.16.1.8 name atlanta class dial1 81012345678901
dialer-group 1
ppp callback accept
ppp authentication chap
!
map-class dialer dial1
dialer callback-server username
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_command_reference_ch
apter09186a00800ca532.html#4557

QUESTION 136
Which configuration will allow an ISDN link to come up 5 seconds after detecting a primary link failure and then disable the ISDN link 10 seconds after the primary link returns?

A. RouterA(config)# interface serial 0/0
RouterA(config-if)#backup interface bri0/0
RouterA(config-if)#backup load 5 10
B. RouterA(config)#interface serial 0/0
RouterA(config-if)#backup interface serial 0/0
RouterA(config-if)#backup load 10 5
C. RouterA(config)#interface serial0/0
RouterA(config-if)#backup interface bri 0/0
RouterA(config-if)#backup delay 5 10
D. RouterA(config)#interface serial 0/0
RouterA(config-if)#backup interface bri 0/0
RouterA(config-if)#backup delay 10 5

Answer: C

Explanation:
The command Backup delay 5 10 has two number variables. The first number (5)

specifies that if the line protocol on the main interface goes down, The ISDN link is to take over after 5 seconds. The second number (10) states that if serial0 were to reactivate, BRI0 will continue to remain active for 10 seconds until going back into standby mode. Having a backup system wait a few seconds before kicking in is a smart feature because many times an interface may only fail for a few seconds, and an ISDN call would not want to be initiated every time a 1 second outage happened. The longer reactivation time is also a good feature, because the original line has to prove that it's capable of staying active for 10 seconds before it will be considered to be reliable again.

QUESTION 137
The configuration file for one of the Certkiller ISDN routers is displayed below:

```
Interface dialer0
    ip unnumbered loopback 0
    encapsulation ppp
    dialer remote-name rta
    dialer pool 0
    dialer string 5551212
    dialer-group 1
    ppp multilink
    dialer idle-timeout 30
!
Interface dialer1
    ip unnumbered loopback 0
    encapsulation ppp
    dialer remote-name rtb
    dialer pool 1
    dialer string 5551234
    dialer-group 1
    ppp multilink
    dialer idle-timeout 30

Interface bri0/0
    encapsulation ppp
    dialer pool-member 0 priority 250
    dialer pool-member 1 priority 200
    ppp authentication chap
    ppp multilink
    dialer idle-timeout 100
!
Interface bri0/1
    encapsulation ppp
    dialer pool-member 1 priority 100
    ppp authentication chap
    ppp multilink
    dialer idle-timeout 100
!
Interface serial 0
    ip unnumbered loopback 0
    backup interface dialer 0
    backup delay 5 10
!
Interface serial 1
    ip unnumbered loopback 0
    backup interface dialer 1
    backup delay 5 10
```

Based on the information above, which three of the following statements are true?
(Choose three)

A. Dialer pool 0 will have a higher priority when using interface bri 0/0.
B. The dialer and serial interfaces share a common IP address.
C. Interface BRI 0/0 will be selected first when attempting to reach router rtb.
D. The timeout value is set to 100 seconds for BRI 0/0
E. The timeout value is set to 30 seconds for BRI 0/1.

Answer: B, C, E

Explanation:
B: Both the serial interfaces and the dialer interfaces are configured with the "ip unnumbered loopback 0" command, so all interfaces will share the IP address that is

configured on interface loopback 0.
C: Each dialer interface uses a dialer pool, a pool of physical interfaces ordered on the basis
of the priority assigned to each physical interface. A physical interface can belong to multiple
dialer pools, contention being resolved by priority. The dialer-pool member priority is higher
for interface BRI0/0, so it will be selected first for all calls.
E: The time specified in the logical dialer interface overrides the value specified in the
physical BRI interface, so even though the idle timeout is configured for 100 seconds on the
BRI interfaces, the value of 30 seconds specified on the dialer interfaces will be used.

QUESTION 138
Which command binds a logical dialer interface to a dialer pool?

A. dialer pool-member number
B. dialer-group number
C. dialer-list number
D. dialer pool number

Answer: D

Explanation:
To specify, for a logical dialer interface, which dialing pool to use to connect to a specific
destination subnetwork, use the dialer pool interface configuration command.
The following example shows a dialer interface configuration that is linked to the physical
interface configuration shown for BRI 1 in the dialer pool-member command section. Dialer
interface 1 uses dialer pool 3, of which BRI 1 is a member.
! This is a dialer profile for reaching remote subnetwork 1.1.1.1.
interface Dialer1
ip address 1.1.1.1 255.255.255.0
encapsulation ppp
dialer remote-name Smalluser
dialer string 4540
dialer pool 3
dialer-group 1
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_command_reference_ch
apter09186a00800ca525.html

QUESTION 139
You need to configure router CK1 for ISDN DDR routing. What command do you use
to define interesting packets? (Type in answer below)

Answer: dialer-list

Explanation:
Dial-on-Demand Routing (DDR) addresses the need for intermittent network connections
over circuit-switched WANs. With DDR, all traffic is classified as either interesting or

uninteresting. If traffic is interesting, the packet is passed to the interface, and the router then connects to the remote router (if not currently connected). The router defines interesting packets with the dialer-list command. DDR is implemented in two ways: DDR with dialer profiles and legacy DDR.

QUESTION 140

You are a Cisco Certified Engineer configuring a DDR remote access solution. Which of the following components of a dialer profile is entirely optional (Choose all that apply)?

A. Dialer map-class
B. Dialer interfaces
C. Dialer pool
D. Physical interfaces

Answer: A

Explanation:
The components of a dialer profile include: Dialer interfaces - logical entities that use a perdestination dialer profile. Any number of dialer interfaces can be created in a router. All configuration settings specific to the destination go in the dialer interface configuration. Each dialer interface uses a dialer pool, which is a pool of physical interfaces (ISDN BRI and PRI, asynchronous-modem, and synchronous serial). Dialer pool - Each interface references a dialer pool, which is a group of physical interfaces associated with a dialer profile. A physical interface can belong to multiple dialer pools. Contention for a specific physical interface is resolved by configuring the optional priority command. Physical interfaces - Interfaces in a dialer pool are configured for encapsulation parameters. The interfaces are also configured to identify the dialer pools to which the interface belongs. Dialer profiles support PPP and High-Level Data Link Control (HDLC) encapsulation.
Dialer map-class (optional) - Supply configuration parameters to dialer interfaces (for example, ISDN speed, dialer timers parameters, and so on). A map-class can be referenced from multiple dialer interfaces.

QUESTION 141

To add physical ISDN links to a multilink bundle dynamically on an as needed basis, what command should be used?

A. ppp multilink
B. Enable chap
C. Multilink ppp
D. Enable multilink
E. dialer load-threshold

Answer: E

Explanation:
To configure bandwidth on demand by setting the maximum load before the dialer places

another call to a destination, use the dialer load-threshold command in interface configuration mode.

When the cumulative load of all UP links (a number n) exceeds the load threshold the dialer adds an extra link and when the cumulative load of all UP links minus one (n - 1) is at or below load threshold then the dialer can bring down that one link. The dialer will make additional calls or drop links as necessary but will never interrupt an existing call to another destination.

The load argument is the calculated weighted average load value for the interface; 1 is unloaded and 255 is fully loaded. The load is calculated by the system dynamically, based on bandwidth. You can set the bandwidth for an interface in kilobits per second, using the bandwidth command.

The load calculation determines how much of the total bandwidth you are using. A load value of 255 means that you are using one hundred percent of the bandwidth. The load number is required.

QUESTION 142

What option can be used as a means for configuring DDR? (Choose all that apply)

A. Set the route calling cost
B. Set the route priority
C. Use a floating static route
D. Set up the static route to make it less desirable than the dynamic route

Answer: C, D

Explanation:
The router uses one of three methods to monitor the primary connection and initiate the backup connection when needed, as listed below:
• Backup Interface - This is an interface that stays in standby until the primary interface line protocol is detected as down and then is brought up.
• Floating Static Route - This backup route has an administrative distance greater than the administrative distance of the primary connection route and therefore would not be in the routing table until the primary interface goes down.
• Dialer Watches - Dialer watch is a backup feature that integrates dial backup with routing capabilities.

QUESTION 143

You work as a network technician for Certkiller .com. An ISDN BRI interface has been configured as a backup interface and is currently in standby mode. You then attempt to use the BRI interface to connect to a different site but are unsuccessful.
What solution would enable the BRI interface to support the backup requirements and still be available for other DDR operations?

A. Configure PPP multilink.
B. Configure legacy DDR.
C. Split the B channels, one for backup and the other for DDR operations.

D. Configure the D channel.
E. Configure dialer profiles.
F. Configure standby-suppress mode.

Answer: E

Explanation:
Dialer profiles separate logical configurations from the physical interfaces that receive or make calls. Because of this separation, multiple dialer profile configurations can share interfaces such as ISDN, asynchronous modems, or synchronous serial connections. Dialer profiles allow you to bind logical and physical configurations together dynamically on a per call basis. This allows physical interfaces to take on different characteristics based on incoming or outgoing call requirements. Dialer profiles can define encapsulation, access control lists, minimum or maximum calls, and toggle features on or off. Dialer profiles are particularly useful where multiple ISDN B channels are to be used to connect to multiple remote destinations simultaneously. In such a case, one dialer profile can be bound to one set of B channels while another dialer profile can be bound to another set of B channels. This allows the same physical interface to connect to multiple remote destinations simultaneously.
Reference:
http://www.cisco.com/en/US/tech/ CK8 01/ CK1 33/technologies_configuration_example09186a0 080093c2e.shtml

QUESTION 144
The "dialer fast-idle" configuration command was issued on router CK1 . What does the dialer fast-idle command specify in a DDR environment?

A. The termination of the call if no interesting traffic has been transmitted for the specified time.
B. Disconnect time if there is another call waiting for the same interface and the interface is idle.
C. The length of idle time to wait for a carrier when dialing out before abandoning the call
D. The length of idle time to wait for keepalives before assuming inactive and disconnecting the call

Answer: B

Explanation:
The dialer fast-idle configuration command is described below:

Command	Description
dialer fast-idle (interface configuration)	Specifies the amount of time that a line for which there is contention will stay idle before it is disconnected and the competing call is placed.

QUESTION 145
Part of the configuration file for router Certkiller 1 is displayed below:
You work as a network engineer at Certkiller . You must configure Certkiller 1 so that it accepts ISDN calls from Certkiller 2 but does not dial Certkiller 2. Give the partial configuration, what must you do to complete the configuration and meet these requirements?

A. Certkiller 1(config)# dialer-list 1 protocol ip permit
Certkiller 1(config)# interface bri0/0
Certkiller 1(config-if)# dialer map ip 1.1.1.2 name Certkiller 2 broadcast 5551212
Certkiller 1(config-if)# dialer-group 1
Certkiller 1(config-if)# ppp authentication chap callin
B. Certkiller 1(config)# dialer-list 1 protocol ip permit
Certkiller 1(config)# interface bri0/0
Certkiller 1(config-if)# dialer map ip 1.1.1.2 name Certkiller 2 broadcast
Certkiller 1(config-if)# dialer-group 1
Certkiller 1(config-if)# ppp authentication chap
C. Certkiller 1(config)# dialer-list 1 protocol ip deny
Certkiller 1(config)# interface bri0/0
Certkiller 1(config-if)# dialer map ip 1.1.1.2
Certkiller 1(config-if)# dialer-group 1
Certkiller 1(config-if)# ppp authentication chap callin
D. Certkiller 1(config)# interface bri0/0
Certkiller 1(config-if)# dialer map ip 1.1.1.2 name Certkiller 2 broadcast 5551212
Certkiller 1(config-if)# ppp authentication chap

Answer: D

Explanation:
Since there is no dialer-list associated with this choice, no interesting traffic will be seen by the router, so a call can not be initiated by Certkiller 1. However, it has been correctly configured to accept calls from Certkiller 2. It is important to remember that traffic defined as "interesting" is only used for initiating the ISDN call, and not for defining the traffic that can traverse an ISDN call. Once the ISDN connection is made, all traffic will be allowed through the ISDN line until no interesting traffic is seen and the idle timer expires.

QUESTION 146
While troubleshooting an ISDN connectivity issue, the following was shown via debugging:

```
BR0:1 CHAP: I CHALLENGE id 17 len 33 from "Certkiller13"
BR0:1 CHAP: Username maui-soho-01 not found
BR0:1 CHAP: Unable to authenticate for peer
BR0:1 PPP: Phase is TERMINATING
```

Give the output in the exhibit, which two statements are true? (Select two)

A. The local router username is Certkiller 13

B. The username supplied by the remote router is not configured locally.
C. The username supplied by the local router is not configured on the remote router.
D. The command username CertK Kng13 password password must be configured on the local router.
E. The command username Certkiller 13 password password must be configured on the remote router.
F. The remote router is not configured for CHAP authentication.

Answer: B, D

Explanation:
In this example, the remote router is issuing the CHAP challenge to the remote router, which is " Certkiller 13." This username is not configured locally so it is not found. To remedy this, you should issue the "username Certkiller 13 password" command on the local router.

QUESTION 147
Simulation
The following information will be used to configure router Certkiller 1 in this simulation:

Certkiller .com is configuring ISDN links to provide connectivity to their central site from branch locations. As the network administrator at the Certkiller 1 location it is your job to configure connectivity to the central site at the Certkiller 2 location. Using a Cisco 1700 series with a BRI interface, you will configure connectivity to a Cisco 2600 series router with a PRI interface already configured at the central site. Your task is to configure the BRI interface for ISDN and use PPP encapsulation with CHAP authentication. Any IP traffic designed for the central site should initiate an ISDN connection. An idle timeout of 60 seconds should be configured for the line to drop in the absence of interesting traffic. A dialer map is to be used to facilitate the connectivity. As you are the branch location, only a static default route is to be configured for routing to the central site. The telco requires you to use the National ISDN switch type for your interface. Use the topology in the exhibit for reference.
Further necessary information is as follows:
Privileged Mode password is Certkiller
Password to be used for CHAP authentication: Certkiller
Central site hostname: Certkiller 2
Local IP address 192.168.233.2/30
Central IP address 192.168.233.1/30
The telecommunications company has provided the following information for each BRI B channel:
SPID1 51044422163712; LDN 5552216
SPID2 51044422163712; LDN 5552217

Central Site LDN: 5155553216
Start the simulation by click the host icon.

Answer:
Router >
Router >enable
Router #config t
Router(config)# hostname Certkiller 1
Certkiller 1(config)#isdn switch-type basic-ni
Certkiller 1(config)#username Certkiller 2 password Certkiller
Certkiller 1(config)#interface bri0
Certkiller 1(config_int)#ip address 192.168.233.2 255.255.255.252
Certkiller 1(config_int)#no shut
Certkiller 1(config_int)#encapsulation ppp
Certkiller 1(config_int)#ppp authentication chap
Certkiller 1(config_int)#dialer idle-timeout 60
Certkiller 1(config_int)#isdn spid1 51044422163712 5552216
Certkiller 1(config_int)#isdn spid2 51044422163712 5552217
Certkiller 1(config_int)#dialer map ip 192.168.233.1 name Certkiller 2 5155553216
Certkiller 1(config_int)#dialer-group 1
Certkiller 1(config_int)#exit
Certkiller 1(config)#dialer-list 1 protocol ip permit
Certkiller 1(config)#ip route 0.0.0.0 0.0.0.0 192.168.233.1
Certkiller 1(config)#exit

QUESTION 148
You need to adjust the WFQ settings on router CK1 . Which of the following
commands could you use to correctly configure Weighted Fair Queuing (WFQ)?

A. router(config)# bandwidth 56
B. router(config)# fair-queue 64
C. router(config-if)# fair-queue 128
D. router(config-if)# priority-fair 16
E. router(config)# priority fair 8

Answer: C

Explanation:
To enable weighted fair queuing (WFQ) for an interface, use the fair-queue interface
configuration command. This command is done on an interface level.
fair-queue [congestive-discard-threshold [dynamic-queues [reservable-queues]]]
no fair-queue
Syntax Description

congestive-discard-threshold	(Optional) Number of messages allowed in each queue. The default is 64 messages, and a new threshold must be a power of 2 in the range from 16 to 4096. When a conversation reaches this threshold, new message packets are discarded.
dynamic-queues	(Optional) Number of dynamic queues used for best-effort conversations (that is, a normal conversation not requiring any special network services). Values are **16,32,64,128,256,512,1024,2048**, and **4096**. See Table 4 and Table 5 in the **fair-queue** (class-default) command for the default number of dynamic queues.
reservable-queues	(Optional) Number of reservable queues used for reserved conversations in the range 0 to 1000. The default is 0. Reservable queues are used for interfaces configured for features such as Resource Reservation Protocol (RSVP).

Defaults
Fair queuing is enabled by default for physical interfaces whose bandwidth is less than or equal to 2.048 Mbps and that do not use the following:
• X.25 and Synchronous Data Link Control (SDLC) encapsulations
• Link Access Procedure, Balanced (LAPB)
• Tunnels
• Loopbacks
• Dialer
• Bridges
• Virtual interfaces
Fair queuing is not an option for the protocols listed above. However, if custom queuing or priority queuing is enabled for a qualifying link, it overrides fair queuing, effectively disabling it. Additionally, fair queuing is automatically disabled if you enable the autonomous or silicon switching engine mechanisms.
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_r/qrfcmd1.htm#1098249

QUESTION 149
The following configuration command was applied to a Certkiller router:
policy-map-Policy1
class Class1
priority 10

class Class2
bandwidth 20
queue-limit 45
class Class3
bandwidth 30
random-detect
From the information above, what is true about this configuration?

A. WRED is used in Class1 and Class2.
Traffic not matching any classes will be dropped.
B. WRED is used in Class3.
Traffic not matching any classes will be handled by the class-default class.
C. WRED is used in Class1 and Class3.
Traffic not matching any classes will be best effort by default class.
D. WRED is used in Class3.
Traffic not matching any classes will be dropped.

Answer: B

Explanation:
To enable WRED with its default configuration parameters use the random-detect command
as shown in the last line of the command interface below the Class3 configuration
parameters.
In a policy-map, if traffic doesn't match a class it gets handled by what's defined in the
default class.
Reference:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/qos_c/qcprt3/qcd
wred.htm

QUESTION 150
Study the exhibit below:

• In the graphic, all interfaces are up and correctly configured.
• The bandwidth of the Frame Relay interface is 256k
• The bandwidth of the ISDN interface is 128k
• On Certkiller 1, the local best EIGRP metric (feasible distance) is 150 for the
Frame Relay link and 300 for the ISDN link.
• However the reported distance for both routes is 100.
• The router Certkiller 1 has been configured like this:
router eigrp 1
network 10.0.0.0
variance 3
traffic-share balanced

!
ip route 10.1.2.0 255.255.255.0 10.1.4.2 99
If a host on network 10.1.1.0 sends data to a host on network 10.1.2.0, which route will
Router Certkiller 1 choose?

A. Traffic will be routed over the Frame Relay link.
B. Traffic will be routed over the ISDN link.
C. Traffic will be load balanced between the Frame Relay and ISDN links.
D. Traffic will be load balanced between the Frame Relay and ISDN links.
The Frame Relay link, however, will transport twice the traffic as the ISDN link.

Answer: D
The routing protocol of this scenario is EIGRP. EIGRP has a administrative distance of 90
and the floating static route has a configured administrative distance of 99. Therefore the
static route is not taken (the lowest administrative distance is the best), we see only EIGRP
route in the routing table. EIGRP use frame-relay and ISDN connection because the variance
3 and the traffic-share balanced permit the balancing of the load on the both connection. The
answer is D.
Note: More information on EIGRP load balancing can be found here:
http://www.cisco.com/en/US/tech/ CK3 65/technologies_tech_note09186a008009437d.shtml
Every routing protocol supports equal cost path load balancing. In addition to that, IGRP and
EIGRP also support unequal cost path load balancing. Use the variance command to instruct
the router to include routes with a metric less than n times the minimum metric route for that
destination, where n is the number specified by the variance command.. The variable n can
take a value between 1 and 128, with the default being 1, which means equal cost load
balancing. Traffic is also distributed among the links with unequal costs, proportionately,
with respect to the metric.

QUESTION 151
The Certkiller network is displayed below:
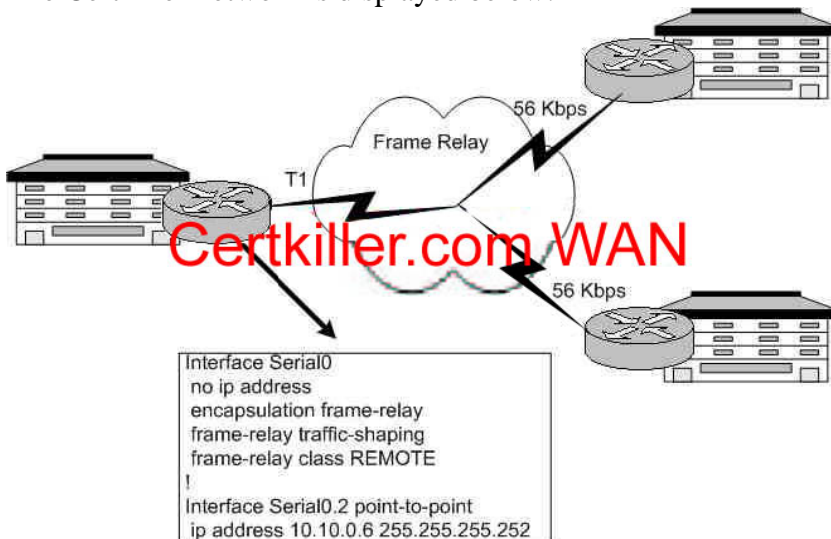
What will be the result if the command "frame-relay traffic rate 56000
128000" was applied on the indicated router?

A. It enables the average and peak rate for traffic received on the interface.
B. It will have no effect until the REMOTE class is assigned to a sub-interface.
C. It enables the average and peak rate for traffic sent out a virtual circuit.
D. It configured the interface default bandwidth and peak rate for traffic sent.
E. None of the above

Answer: C

Explanation:
In the command frame-relay traffic rate 56000 128000 there are two number variables. The
first number variable (56 000) is for the average traffic rate (in bits per second) and the
second number is the peak rate (128 000) of the virtual circuit.
Once the map-class commands been entered, the prompt changes. At this point, it is time to
define the traffic parameters. The average and peak transmission rates can be configured at
this point along with defining whether the router should respond to BECN requests. It is also
possible to define queues to prioritize PVCs. The command structure for defining peak and
average rates is as follows (the peak rate is optional):
RouterA (config-map-class)#frame-relay traffic-rate average
[peak]
Reference: CCNP Remote Access Exam Certification Guide, page 272, Brian Morgan &
Craig Dennis, Cisco Press 2001, ISBN 1-58720-003-1

QUESTION 152
The HQ Certkiller router is using subinterfaces on the frame relay interface. What's
true about configuring Frame Relay subinterfaces? (Choose all that apply.)

A. The configuration must be added to the D channel.
B. The physical interface and subinterface can each be configured with IP addresses.
C. Subinterface is configured either multipoint or point-to-point.
D. Any IP address must be removed from the subinterface.
E. None of the above.

Answer: B, C

Explanation:
To enable the forwarding of broadcast routing updates in a Frame Relay network, you can
configure the router with logically assigned interfaces called subinterfaces. Subinterfaces are
logical subdivisions of a physical interface. In split horizon routing environments, routing
updates received on one subinterface can be sent out another subinterface. In subinterface
configuration, each virtual circuit can be configured as a point-to-point connection, which
allows the subinterface to act similar to a leased line.
You can configure subinterfaces to support the following connection types:
Point-to-point - A single subinterface is used to establish one PVC connection to another
physical or subinterface on a remote router. In this case, the interfaces would be in the same
subnet and each interface would have a single DLCI. Each point-to-point connection is its

own subnet. In this environment, broadcasts are not a problem because the routers are pointto-point and act like a leased line.

Multipoint - A single subinterface is used to establish multiple PVC connections to multiple physical or subinterfaces on remote routers. In this case, all the participating interfaces would be in the same subnet and each interface would have its own local DLCI. In this environment, because the subinterface is acting like a regular NBMA Frame Relay network, broadcast traffic is subject to the split horizon rule.

Example:
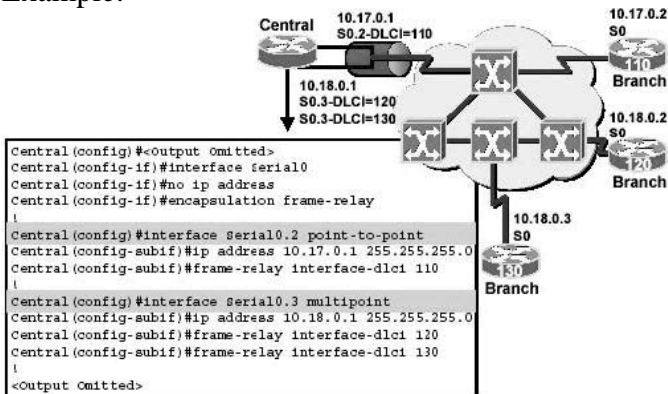
As this example shows, you should remove any network-layer address assigned to the physical interface. If the physical interface has an address, frames will not be received by the local subinterfaces. Although using layer 3 addresses on the main interface is not recommended, it is indeed possible to do this, therefore, B is correct in addition to C.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 11-19

QUESTION 153

Which of the following Frame Relay encapsulation command would you use if you were going to connect an interface on a Cisco router to an interface on a Juniper router?

A. Router(config-if)#encapsulation frame-relay ansi
B. Router(config-if)#encapsulation frame-relay cisco
C. Router(config-if)#encapsulation frame-relay ietf
D. Router(config-if)#encapsulation frame-relay q933i

Answer: C

Explanation:

The correct configuration syntax is:

Router(config-if)# encapsulation frame-relay [cisco | ietf]

This command select the encapsulation type to encapsulate the frame relay data traffic endto-end. The Cisco proprietary encapsulation is the default type. Use IETF encapuslation if connecting to a non-Cisco router.

QUESTION 154

The Certkiller WAN is displayed below:

Certkiller 's regional offices are connected together by way of a Frame Relay connection. Which command would you use to allow the Toronto router to dynamically adjust the rate at which it sends packets to the Boston router, during periods of network congestion?

A. frame-relay traffic-rate adaptive
B. frame-relay traffic-rate dynamic
C. frame-relay adaptive-shaping becn
D. frame-relay adaptive-shaping fecn

Answer: C

Explanation:
Specify that the router dynamically fluctuate the rate at which it sends packets depending on the BECNs (Backward Explicit Congestion Notifications) it receives if you want the sending router to adjust its transmission rate based on the BECNs received. To select BECN as the mechanism to which traffic shaping will adapt, use the frame-relay adaptive-shaping becn command.
The frame-relay adaptive-shaping command configures a router to adjust virtual circuit (VC) sending rates in response to BECN backward congestion notification messages or interface congestion.
Include this command in a map-class definition and apply the map class either to the main interface or to a subinterface.
Adaptive traffic shaping for interface congestion can be configured along with BECN. When adaptive shaping for interface congestion is used with BECN, if interface congestion exceeds the queue-depth, then the PVC send rate is reduced to minCIR. When interface congestion drops below the queue-depth, then the send rate is adjusted in response to BECN.
Reference:
Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 11-30

QUESTION 155
You are the network administrator at Certkiller .com. If you enable Frame Relay traffic shaping and were to configure a CIR of 64kbps using 125ms time interval, what will be the value of the committed burst (Bc)?

A. 24000 bits
B. 32000 bits
C. 16000 bits
D. 8000 bits

E. 48000 bits
F. 64000 bits

Answer: D

Explanation:
To understand the concepts of traffic shaping, it is important to have a firm grasp of the various traffic parameters in the Frame Relay network. In particular, you should know that some (such as committed information rate [CIR] and excessive burst [Be]) are commonly used but misunderstood.
CIR (Committed Information Rate) - The average rate at which you want to transmit. This is generally not the same as the CIR provided by the telco. This is the rate at which you want to send in periods of noncongestion.
Bc (Committed Burst) - The amount of data to send in each Tc interval.
Be (Excessive Burst) - The amount of excess data allowed to be sent during the first interval once credit is built up. Transmission credit is built up during periods of nontransmission. The credit is the burst size. Full credit is typically CIR / 8.
Tc (Committed Rate Measurement Interval) - The Bc / CIR time interval. The time interval shouldn't exceed 125 ms (almost always 125 ms).
MinCIR (Minimum CIR) - The minimum amount of data to send during periods of congestion. This is usually what you get from the telco.
MinCIR - defaults to one-half of CIR.
PIR (Peak Information Rate) - The highest possible rate of transmission on any given interface.
MIR (Minimum Information Rate) - The slowest rate of transmission on any given interface.
Interval - Bc / CIR. The maximum is 125 ms, or 1/8 second.
Byte Increment - Bc / 8. This value must be greater than 125.
Limit - Byte Increment + Be / 8 (in bytes).
The calculation is TC = Bc/CIR
125ms (tc) = 8000bits (Bc)/64kbps (CIR)
Reference:
Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)
Page 300 & 301

QUESTION 156
At the HQ location of your frame relay network, your Cisco router connects numerous sites via PVCs. One of the remote routers is using a non-Cisco router. Which of the following Frame Relay commands could you use to change the encapsulation on any single PVC?

A. no frame-relay encapsulation ietf
B. encapsulation frame-relay ietf
C. no frame-relay encapsulation cisco
D. frame-relay map ip 10.160.2.1 100 broadcast ietf

Answer: D

Explanation:
The default encapsulation, which is Cisco, is applied to all the VCs available on that serial interface. If most destinations use the Cisco encapsulation, but one destination requires the IETF, you would specify, under the interface, the general encapsulation to be used by most destinations. Because the default encapsulation is Cisco, you would specify the exception using the frame-relay map command.
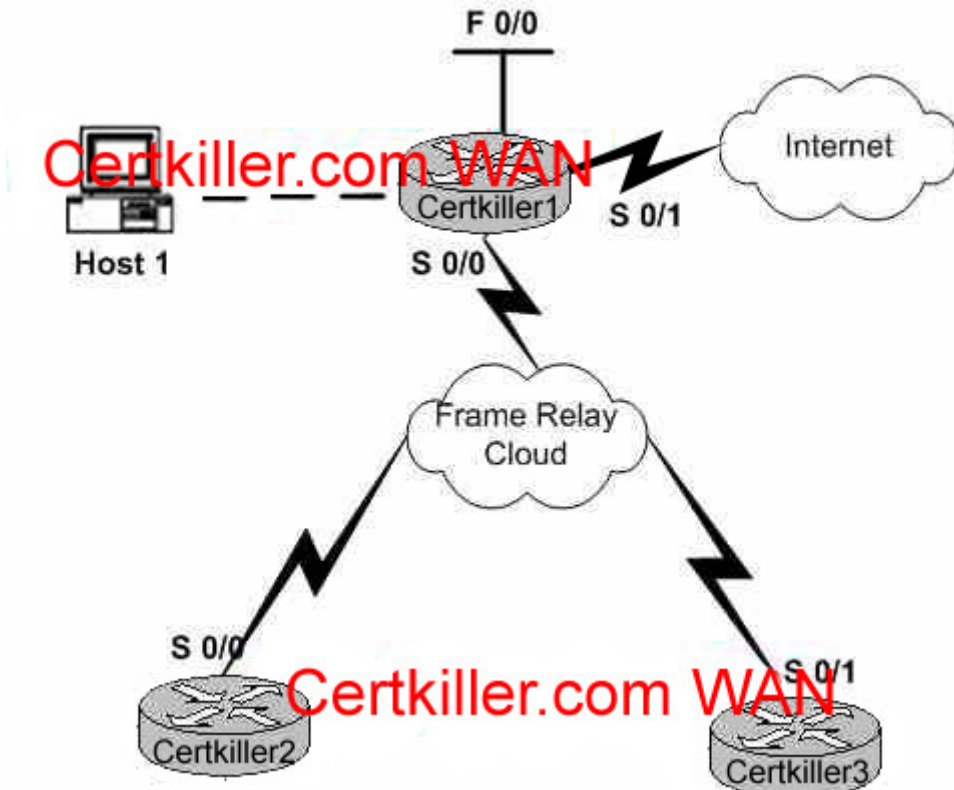Reference:
Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)
Page 277

QUESTION 157
The Certkiller network topology is displayed below:

Certkiller 's Spanish test division is finally upgradings its ISDN BRI links to Frame Relay and they've invited you to contribute to this project.
There are three locations, each location has one Cisco 2600 series router.
1) Central Office (Madrid) - Certkiller 1
2) Regional Office #A (Barcelona) - Certkiller 2
3) Regional Office #B (Gibraltar) - Certkiller 3
The support staff at the Barcelona and Gibraler offices have completed their end of the configuraton; but since the staff at the Madrid office have all gone to Ibeza for vacation you've been left with the Madrid office to configure.
Your assignment is to:
• enable Frame Relay on the Serial 0/0 interface

• configure two sub-interaces with the appropriate IP address and DLCI under
Serial 0/0 using the DLCI number as the sub-interface name
• build static routes to the Barcelona and Gibraltar branch office LANs.
Network information:
Router: Certkiller 1
F0/0: 10.10.241.1.24
S0/0: DLCI286 - 192.168.233.1/30
DLCI287 - 192.168.233.5/30
S0/1: 172.16.0.6/30
Router: Certkiller 2
F0/0: 10.10.242.1/24
S0/0: 192.168.233.2/30
Router: Certkiller 3
F0/0: 10.10.243.1/24
S0/0: 192.168.233.6/30
On the Madrid router the following DLCIs and IP addresses are to be assigned:
To router Certkiller 2 - DLCI 286 and IP address 192.168.233.1/30
To router Certkiller 3 - DLCI 287 and IP address 192.168.233.5/30
Route to destination network at Certkiller 2 is 10.10.242.0/24
Route to destination network at Certkiller 3 is 10.10.243.0/24
Configure the Madrid router to satisfy the above requirements.

Answer:
Certkiller 1(config)#int s0/0
Certkiller 1(config-if)#encapsulation frame-relay
Certkiller 1(config-if)#no shut
Certkiller 1(config-subif)#int s0/0.286 point-to-point
Certkiller 1(config-subif)#ip address 192.168.233.1
255.255.255.252
Certkiller 1(config-subif)#frame-relay interface-dlci 286
Certkiller 1(config-fr-dlci)#exit
Certkiller 1(config-subif)#exit
Certkiller 1(config)#int s0/0
Certkiller 1(config-if)#int s0/0.287 point-to-point
Certkiller 1(config-subif)#ip address 192.168.233.5
255.255.255.252
Certkiller 1(config-subif)#frame-relay interface-dlci 287
Certkiller 1(config-fr-dlci)#exit
Certkiller 1(config-subif)#exit
Certkiller 1(config)#ip route 10.10.242.0 255.255.255.0
192.168.233.2
Certkiller 1(config)#ip route 10.10.242.0 255.255.255.0
192.168.233.6
Certkiller 1(config)#exit
Certkiller 1# copy run start
You can check your configuration with:

Certkiller 1#show frame-relay pvc
Certkiller 1#show frame-relay map
Certkiller 1(config-subif)#

QUESTION 158
You issue the following command on one of your Cisco routers:
frame-relay map ip 192.168.166.21 100
What will be the end result of this command? (Choose all that apply)

A. Split horizon is disabled.
B. IP address 192.168.166.21 is statically mapped to DLCI 100.
C. IP address 192.168.166.21 is dynamically mapped to DLCI 100.
D. Inverse ARP is enabled.
E. Split horizon is enabled
F. Inverse ARP is disabled.

Answer: B, F

Explanation:
A DLCI number is a data link connection identifier. Permanent virtual circuits (PVCs) and switched virtual circuits (SVCs) are identified by a DLCI number. The DLCI number defines a single virtual connection through the WAN and is the Frame Relay equivalent to a hardware address.
Periodically, through the exchange of signaling messages, a network may announce a new virtual circuit with its corresponding DLCI number. However, protocol addressing is not included in the announcement. The station receiving such an indication will learn of the new connection, but will not be able to address the other side. Without a new configuration or mechanism for discovering the protocol address of the other side, this new virtual circuit is unusable. For this reason, Inverse Address Resolution Protocol (Inverse ARP) was developed. Inverse ARP allows a Frame Relay network to discover the protocol address associated with the virtual circuit, and ARP is more flexible than relying on static configuration. So if you use dynamic address mapping, Frame Relay Inverse ARP provides a given DLCI and requests next-hop protocol addresses for a specific connection. The router then updates its mapping table and uses the information in the table to route outgoing traffic. Dynamic address mapping is enabled by default for all protocols on a physical interface. If you use the static mapping, you must use the frame-relay map command to statically map destination network protocol addresses to a designated DLCI.
Reference:
Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Chapter 11

QUESTION 159
You are a senior network administrator and you're checking up on your trainee. You look into his monitor and notice the following configuration:
interface Serial0/0
no ip address
encapsulation frame-relay

no fair-queue
frame-relay traffic-shaping
bandwidth 1536
!
interface Serial0/0.100 point-to-point
ip address 10.1.1.1 255.255.255.0
frame-relay interface-dlci 100
frame-relay class cisco
!
interface Serial0/0.200 point-to-point
ip address 10.1.2.1 255.255.255.0
frame-relay interface-dlci 200
frame-relay class cisco
!
interface Serial0/0.300 point-to-point
ip address 10.1.3.1 255.255.255.0
frame-relay interface-dlci 300
!
!
map-class frame-relay cisco
frame-relay cir 128000
frame-relay adaptive-shaping becn
According to the above configuration, what is the CIR of interface Serial0/0.300?

A. 56 kbps
B. 128 kbps
C. 64 kbps
D. 1536 kbps
E. 896 kbps

Answer: A

Explanation:
frame-relay traffic-shaping - This command enables FRTS for the interface. Every DLCI
under this interface is traffic shaped with either user-defined or default traffic shaping
parameters. User-defined parameters can be specified in two ways:
o Using the command class class_name under the frame-relay interface-dlci
configuration or
o Using the command frame-relay class under the serial interface.
• The following output displays the default FRTS parameters.

ms3810-3c#**show traffic-shape**

      Access Target Byte Sustain Excess
Interval Increment Adat
I/F   List Rate   Limit bits/int bits/int (ms)
(bytes) Acte

| Se1 | 56000 | 875 | 56000 | 0 | 125 |
| 875 | - | | | | |

Note: The CIR defaults to a value of 56 Kbps. Hence, PVCs that inherit these default FRTS attributes are forced. In this example, the frame-relay class cisco was not defined on interface serial 0/0.300, so the default value of 56000 is used.
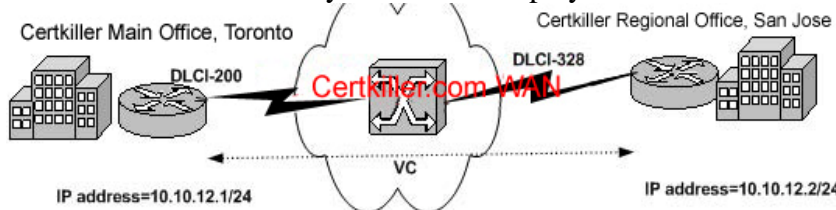Reference:
http://www.cisco.com/en/US/tech/ CK6 52/ CK6 98/technologies_tech_note09186a00800d6788.sh tml

---

QUESTION 160
The Certkiller frame relay network is displayed below:

Which Frame Relay map command would you use to configure static address mapping from Certkiller s main office in Toronto to the regional office in San Jose?

A. frame-relay map ip 10.10.12.2 328 broadcast ietf
B. frame-relay map ip 10.10.12.1 200 broadcast cisco
C. frame-relay map ip 10.10.12.2 200 broadcast cisco
D. frame-relay map ip 10.10.12.1 328 broadcast ietf
E. None of the above

Answer: A

Explanation:
Only choice A specifies the coorect DLCI, which is 328 for San Jose, to the correct IP address of the San Jose end, which is 10.10.12.2. The entire configuration file for Toronto is shown below:
Certkiller Router (config) #interface Serial1
Certkiller Router (config-if) #ip address 10.10.12.1
255.255.255.0
Certkiller Router (config-if) #encapsulation frame-relay
Certkiller Router (config-if) #bandwidth 56
Certkiller Router (config-if) #frame-relay map ip
10.16.12.2 328 broadcast ietf
Note: The encapsulation type defaults to Cisco for frame relay PVCs, but the IETF encapsulation type can always be used. Because the cisco encapsulation is Cisco-proprietary, the IETF value must always be used when connecting to a non-Cisco router.

QUESTION 161
When configuring Frame Relay traffic shaping on one of the Certkiller routers, what command would you use to associate a subinterface with a map class?

A. frame-relay map
B. frame-relay class
C. map-class frame-relay
D. frame-relay map-class
E. map frame-relay class

Answer: C
How to configure Frame Relay traffic Shaping :
Step 1: Specify a map class to be defined with the map-class frame-relay map classname command.
Step 2: Define the map class. When you define a map class for Frame Relay, you can:
• Define the average and peak rates (in bits per second) allowed on virtual circuits associated with the map class.
• Specify that the router dynamically fluctuate the rate at which it sends packets depending on the BECNs it receives.
• Specify either a custom queue list or a priority queue group to use on virtual circuits associated with the map class.
• Once you have defined a map class with queuing and traffic shaping parameters, enter interface configuration mode and enable Frame Relay encapsulation on an interface with the encapsulation frame relay command, discussed earlier in this chapter.
Step 4: Enable Frame Relay traffic shaping on an interface with the frame-relay trafficshaping command. Enabling Frame Relay traffic shaping on an interface enables both traffic shaping and per-virtual circuit queuing on all the PVCs and SVCs on the interface. Traffic shaping enables the router to control the circuit's output rate and react to congestion notification information if also configured.
Step 5: Map a map class to all virtual circuits on the interface with the frame-relay class map class-name command. The map class-name argument must match the map class-name of the map class you configured.
Reference:
Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Chapter 11

QUESTION 162
What configuration step must you perform before traffic shaping parameters can be applied to a Frame Relay interface?

A. Define a map class.
B. Disable any queuing mechanism currently assigned to the interface.
C. Specify a queuing technique to be used on a Frame Relay connection.
D. Specify the use of BECN or FECN for traffic adaptation.
E. None of the above.

Answer: A

Explanation:
Frame Relay traffic shaping is accomplished through the creation of a map class. After the map class is defined the configuration of Frame Relay Traffic Shaping parameters can take place. When you define a map class for Frame Relay, you can:
• Define the average and peak rates (in bits per second) allowed on virtual circuits associated with the map class.
• Specify that the router dynamically fluctuate the rate at which it sends packets, depending on the BECNs it receives.
• Specify either a custom queue list or a priority queue group to use on virtual circuits associated with the map class.
Reference:
Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 11-29

QUESTION 163
The "show interface serial 10/0 was issued on router CK1 as shown below:

```
Serial10/0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 172.16.81.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY, loopback not set
  Keepalive set (10 sec)
  LMI enq sent  15617, LMI stat recvd 15598, LMI upd recvd 0, DTE LMI up
  LMI enq recvd 17, LMI stat sent  0, LMI upd sent  0
  LMI DLCI 0  LMI type is ANSI Annex D  frame relay DTE
  FR SVC disabled, LAPF state down
  Broadcast queue 0/64, broadcasts sent/dropped 3/0, interface broadcasts 0
  Last input 00:00:12, output 00:00:02, output hang never
  Last clearing of "show interface" counters 1d19h
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
    Conversations  0/1/256 (active/max active/max total)
    Reserved Conversations 0/0 (allocated/max allocated)
    Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    15647 packets input, 226474 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    15653 packets output, 205398 bytes, 0 underruns
    0 output errors, 0 collisions, 5 interface resets
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions
    DCD=up  DSR=up  DTR=up  RTS=up  CTS=down
```

What type of Frame Relay encapsulation is used on this interface?

A. ANSI
B. IETF
C. CISCO
D. Q933
E. None of the above

Answer: C

Explanation:
The default encapsulation on an interface is Cisco. When the serial interface of a Cisco router is configured for frame relay displays "encapsulation frame-relay" as shown on line 6 of the output above, the default encapsulation type is used.
Incorrect Answers:
A: This is the configured LMI type, not the encapsulation type for the interface.
B: Although IETF is an encapsulation option, this was not used here. If it was, the output

would have stated "encapsulation frame-relay ietf" as shown in the following example:
router# show interface serial0
Serial0 is up, line protocol is up
Hardware is PQUICC Serial
MTU 5000 bytes, BW 1544 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation FRAME-RELAY IETF, crc 16, loopback not set
Keepalive set (10 sec)
D: This is not a valid Cisco frame relay encapsulation option. The only options are Cisco,
which is the default Cisco proprietary method; and IETF, which is the industry standard.

QUESTION 164
The Certkiller WAN is displayed in the following diagram:
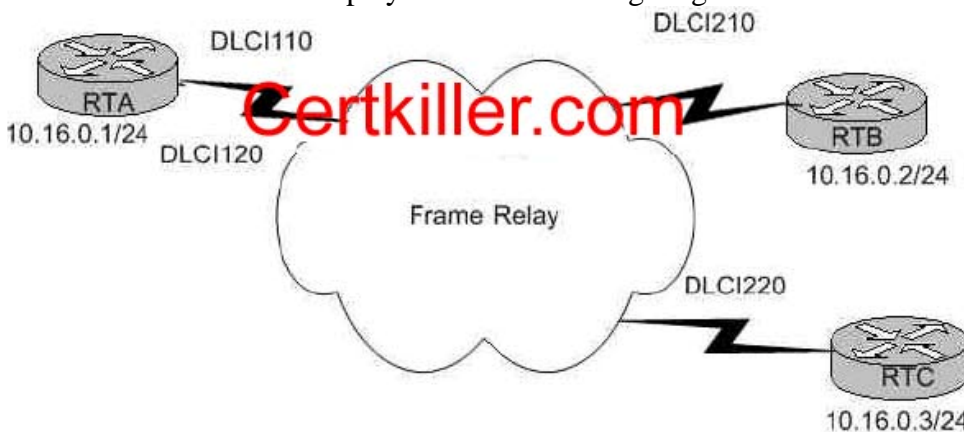
RTA is connected across a hub-and-spoke Frame Relay network to RTB and to RTC.
RTC is a non-Cisco router.
Which two static map entries must the administrator configure to allow RTA to
communicate with RTB and RTC?

A. frame-relay map ip 10.16.0.2 110 ietf
frame-relay map ip 10.16.0.3 120
B. frame-relay map ip 10.16.0.2 210
frame-relay map ip 10.16.0.3 220
C. frame-relay map ip 10.16.0.2.110 broadcast
frame-relay map ip 10.16.0.3 120 broadcast ietf
D. frame-relay map ip 10.16.0.2 210 broadcast
frame-relay map ip 10.16.0.3 220 broadcast ietf

Answer: D

Explanation:
The "frame relay map" command is used to statically map an IP address to a DLCI instead of
relying on inverse ARP. The DLCI and IP address of the remote locations should be
specified. By default, Cisco uses the Cisco proprietary frame relay encapsulation. When
connecting to a non-Cisco router, the industry standard IETF frame relay encapsulation

642-821

should be specified. In this case, since only RTC is a non-Cisco router, the 'IETF" keyword should be placed only on the frame relay map pointing to this router.

QUESTION 165
The Certkiller network is displayed in the following diagram:
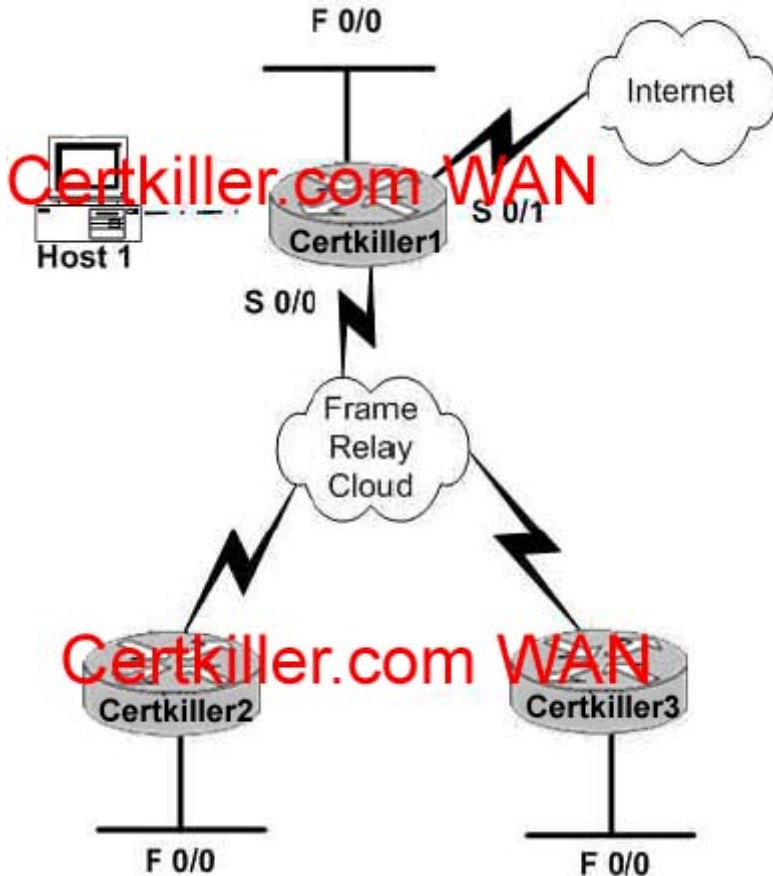
You work as network technician at the Beograd office of Certkiller .com. Certkiller .com is transitioning from ISDN BRI links to a Frame Relay solution for the benefits provided by permanent connections. It is your job to coordinate this transition. The network support specialist at each branch location has completed their configuration, and each is awaiting the completion of the central router configuration to test connectivity. All three locations are using Cisco 2600 series routers. Your tasks are to enable Frame Relay on the Serial 0/0 interface, configure two sub-interfaces with the appropriate IP address and DLCI under Serial 0/0 using the DLCI number as the subinterface name, and build static routes to the branch sites' LAN. Use the topology in the graphic for reference. Further necessary information is as follows:
DLCIs and IP addresses to be assigned on Central Router Certkiller 1:
To router Certkiller 2 - DLCI 68 and IP address 192.168.152.1/30
To router Certkiller 3 - DLCI 69 and IP address 192.168.152.5/30
Route to destination network at R2 is 10.10.15.0/24
Route to destination network at R3 is 10.10.16.0/24
Router Certkiller 1
F0/0: 10.10.14.1/24

Actualtests.com - The Power of Knowing

S0/0: DLCI68 - 192.168.152.1/30
DLCI69 - 192.168.152.5/30
Router Certkiller 2
F0/0: 10.10.15.1/24
S0/0: 192.168.152.2/30
Router Certkiller 3
F0/0: 10.10.15.1/24
S0/0: 192.168.152.6/30
Configure R1 to accomplish these tasks.

Answer:

```
R1>en
Password:
R1#conf t
Enter configuration commands, one per line.  End with END.
R1(config)#int s 0,J
R1(config-if)#no ip add    Certkiller.com
R1(config-if)#encap fr
R1(config-if)#int s0/0.676 point-to-po
R1(config-subif)#ip add 192.168.53.1 255.255.255.252
R1(config-subif)#frame-relay interface-dlci 676
R1(config-fr-dlci)#
R1(config-subif)#int s0/0.677 point  p
R1(config-subif)#ip add 192.168.53.5 255.255.255.252
R1(config-subif)#frame-relay interface-dlci 677
R1(config-fr-dlci)#
R1(config-subif)#exi
R1(config)#ip route 10.10.99.0 255.255.255.0 192.168.53.2
R1(config)#ip rou
00:0  config redured .  config nfigured from console by console
R1#conf t
Enter configuration commands, one per line.  End with END.
R1(config)#no ip route 10.10.99.0 255.255.255.0 192.168.53.2
R1(config)#ip route 10.10.98.0 255.255.255.0 192.168.53.2
R1(config)#ip route 10.10.99.0 255.255.255.0 192.168.53.6
R1(config)#exi
00:0  config reduce .  config nfigured from console by console
R1#cop ru st
Destination filename [startup-config]?
Building configuration...
```

QUESTION 166
On a subinterface of router CK1 , the following configuration command was issued:
frame-relay interface-dlci
What is this command used for?

A. To remove an interface
C. To specify a loopback interface
D. To define a local DLCI number
E. To define a remote DLCI number
F. To select an interface

Answer: C

Explanation:
For point-to-point subinterfaces, the destination is presumed to be known and is identified or
implied in the frame-relay interface-dlci command.

If you specified a point-to-point subinterface in the configuration, you must perform the following task in interface configuration mode:

Task	Command
Associate the selected point-to-point subinterface with a DLCI.	**frame-relay interface-dlci** *dlci* [*option*]

This statically maps the interface to a DLCI.
If you define a subinterface for point-to-point communication, you cannot reassign the same subinterface number to be used for multipoint communication without first rebooting the router. Instead, you can simply avoid using that subinterface number and use a different subinterface number instead.

QUESTION 167

Serial 0/0 of router CK1 is being used for a frame relay link. Under the Serial 0/0 interface of router CK1 , the "ip unnumbered ethernet 0/0" command was issued.
Which of the following correctly describe the IP un-numbered Ethernet 0/0 command when it is issued in configuration mode for a serial interface?

A. The IP address of the Ethernet interface is used by the serial interface.
B. There is no effect at all
C. DHCP traffic received on the serial interface is forwarded to the Ethernet interface.
D. ARP traffic received on the serial interface is forwarded to the Ethernet interface.

Answer: A

Explanation:
The ip unnumbered configuration command allows you to enable IP processing on a serial interface without assigning it an explicit IP address. The ip unnumbered interface can "borrow" the IP address of another interface already configured on the router, thereby conserving network and address space. In this case, it will use the IP address that is already assigned to the ethernet interface.

QUESTION 168

The Certkiller frame relay network is displayed below:
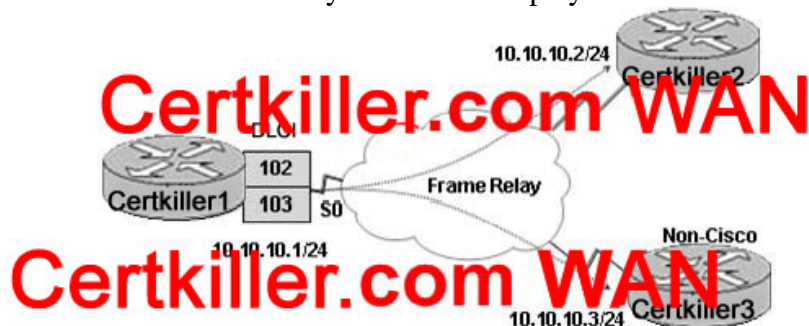
In this network, Certkiller 1 is connected over a Frame Relay cloud to Certkiller 2 and a

non-Cisco device, Certkiller 3. What must be configured on the Certkiller 1 S0 interface to achieve full connectivity with the spoke routers?

A. encapsulation frame-relay
frame-relay map ip 10.10.10.2 102 broadcast
frame-relay map ip 10.10.10.3 103 broadcast
B. encapsulation frame-relay ietf
frame-relay map ip 10.10.10.2 102 broadcast
frame-relay map ip 10.10.10.3 103 broadcast
C. encapsulation frame-relay
frame-relay map ip 10.10.10.2 102 broadcast ietf
frame-relay map ip 10.10.10.3 103 broadcast
D. encapsulation frame-relay
frame-relay map ip 10.10.10.2 102 broadcast
frame-relay map ip 10.10.10.3 103 broadcast ietf
E. encapsulation frame-relay
frame-relay map ip 10.10.10.2 102 broadcast cisco
frame-relay map ip 10.10.10.3 103 broadcast

Answer: D

Explanation:
By default, Cisco routers use the Cisco proprietary encapsulation for frame relay connections. This is recommended when connecting together Cisco routers. When connecting a Cisco router to a non-Cisco router, the IETF standard encapsulation type must be used. In this case, router Certkiller 3 is not a Cisco router, so the connection to it must be used with the IETF keyword, while the connection to the other Cisco router (Certkiller 2) remains using the Cisco encapsulation.

QUESTION 169
On one of the Certkiller routers the following configuration command was issued:
Certkiller A(config)#aaa authentication login default group tacacs+
none
What is this command used for?

A. It uses the list of servers specified in group "TACACS+", if none are available, then no access is permitted.
B. It uses the list of TACACS+ servers for authentication, if TACACS+ fails then uses no authentication.
C. It uses the list of TACACS+ servers for authentication, if TACACS+ fails then no access is permitted.
D. No authentication is required to login.
E. It uses a subset of TACACS+ servers named "group" for authentication as defined by the aaa group servers tacacs+ command.
F. TACACS+ is the first default authentication method.

Answer: B

Explanation:
Once AAA has been enabled on the router, the administrator must declare the methods by which authentication can take place. The aaa authentication login command answers this question: How do I authenticate the login dialog?
The declaration of default tells the router what to do if no listname has been declared on the interface. If a listname has been declared, that listname controls the login. In this statement the listname group is defined, It declares that listname group use TACACS+ by default, and if that fials no authentication is required because the none command has been entered at the end.
Additional methods for the aaa authentication command are:
* enable - Uses the enable password for authentication.
* line - Uses the line password for authentication.
* local - Uses the local username/password database for authentication.
* none - Uses no authentication.
* tacacs+ - Uses the TACACS+ authentication method.
* radius - Uses the RADIUS authentication method.
* guest - Allows guest logins without passwords. This option applies only to ARAP operations.
* auth-guest - Allows guest logins only if the user has already logged in to EXEC. This option only applies to ARAP operations.
* if-needed - Stops further authentication if the user has already been authenticated. This option only applies to PPP operations.
* krb5 - Uses Kerberos 5 for authentication, this option only applies to PPP operations.
Reference:
Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 15-12
Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)
Page 409 & 410

QUESTION 170
You are tasked with configuring authentication on one of the Certkiller routers. Which of the following authentication protocols exchanges information between the client and the server using UDP?

A. AAA
B. RADIUS
C. LCP
D. TACACS+
E. All of the above

Answer: B

Explanation:
RADIUS is a client/server-based network security protocol. It uses UDP for a transport protocol.

The RADIUS server is typically run on a computer. The clients are any type of device that is responsible for passing user information to designated RADIUS servers and then acting on the response that is returned. Transactions between the client and RADIUS server are authenticated through the use of a shared secret, which is never sent over the network. Some of the advantages of RADIUS are the following:
• RADIUS has less packet overhead because it uses UDP.
• With source code format distribution, RADIUS is a fully open protocol format. The user can modify it to work with any security system currently available on the market.
• RADIUS offers enhanced accounting functionality.
Reference:
Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)
Page 403

QUESTION 171
Listed below are a number of router IOS commands. To define 'interesting' traffic for a single host with DDR you'll need a set of three commands. Which ones are they?
(Choose three)

A. Certkiller A(config)#dialer-list 1 protocol ip permit 10.1.1.1
B. Certkiller A(config-if)#dialer-group 1
C. Certkiller A(config)#dialer-list 1 protocol ip list 2
D. Certkiller A(config)#dialer-group 2
E. Certkiller A(config)#access-list 2 permit host 192.168.1.21
F. Certkiller A(config-if)#dialer-list 2 protocol ip permit

Answer: B, C, E

Explanation:
The dialer-list command is used to configure dial-on-demand calls that will initiate a connection. The simple form of the command specifies whether a whole protocol suite, such as IP or Internetwork Packet Exchange (IPX(r)), will be permitted or denied to trigger a call. The more complex form references an access list that will allow finer control of the definition of interesting traffic. The syntax for this command is:
Router(config)#dialer-list group-number protocol protocol {permit | deny}
list access-list-number
The dialer-group interface command applies the dialer list specifications to an interface. The syntax for this command is:
Router(config-if)#dialer-group group-number
The access-list command gives more control over interesting traffic. It uses standard or extended access lists. The syntax for this command is:
Router(config)#access-list access-list-number {permit | deny}
{protocol | protocol-keyword} {source source-wildcard | any}
{destination destination-wildcard | any} [protocol-options] [log]
By knowing this we can generate the router commands:
Certkiller A (config)#dialer-list 1 protocol ip list 2
Certkiller A(config)#access-list 2 permit host 192.168.1.21

Certkiller A(config-if)#dialer-group 1
Reference:
Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 7-30 & 7-31

QUESTION 172
While you were on your lunch break your apprentice trainee was busy configuring
access lists. When you return to your workstation you find the following configuration:
access-list 101 permit ip any any
access-list 101 deny tcp any any eq ftp
dialer-list 2 protocol ip list 101
What is true about the configuration that your trainee entered? (Choose all that apply)

A. FTP traffic will be forwarded.
B. Since FTP uses two sockets, both must be defined to prevent packet forwarding.
C. FTP will cause the line to come up.
D. FTP traffic will not be forwarded.

Answer: A C

Explanation:
The logic that IOS uses with a multiple-entry Access Control List can be summarized as
follows:
1. The matching parameters of the access-list statement are compared to the packet.
2. If a match is made, the action defined in this access-list statement (permit or deny) is
performed.
3. If a match is not made in Step 2, repeat Steps 1 and 2 using each successive statement
in the ACL until a match is made.
4. If no match is made with an entry in the access list, the deny action is performed.
The access-list 101 permit ip any any command is used and the result is that every packet
will be permitted. So the second command "access-list 101 deny tcp any any eq ftp" is never
read by the IOS since all IP traffic (including FTP) will match the first line.
The dialer-list 2 protocol ip list 101 command binds the Access Control List to the dialer list.
Therefore the FTP traffic will be forwarded and it will bring up the line.
Reference:
Cisco Press - ICND - 640-811 - Exam Certification Study Guide 2004 (ISBN 1-58720-083-
x) Page 430

QUESTION 173
The following command was issues on router CK1 , which has been configured for PPP
call back:
dialer hold-queue 100 timeout 10
From this information, when will CK1 place outbound interesting packets in queue?

A. While a dial connection is established.
B. While higher priority traffic is sent over a dial connection.
C. During network congestion on a dial connection.

D. For 10 seconds after a source quench message is received.
E. For 10 seconds for 10 consecutive quench messages.

Answer: A

Explanation:
The dialer hold-queue timeout determines how long to wait before the client can
make another call to the same destination. The server must make the return call before the
client hold-queue timer expires to prevent the client from trying again and possibly
preventing the return call from being connected.
Reference:
Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 5-24

QUESTION 174
You have just received a brand new Cisco router and need to configure auditing on it.
What command would you use to enable auditing of the privileged mode access
commands?

A. aaa accounting enable 15
B. ip audit enable
C. aaa accounting command 15
D. aaa accounting enable priv

Answer: C

Explanation:
AAA accounting can supply information concerning user activity back to the database. This
concept was especially helpful in the early days of Internet service when many ISPs offered
20 or 40 hours per week at a fixed cost and hourly or minute charges in excess of the
specified timeframe. Today it is much more common for the ISP charge to be set for an
unlimited access time. This does not, however, minimize the power of accounting to enable
the administrator to track unauthorized attempts and proactively create security for system
resources. In addition, accounting can be used to track resource usage to better allocate
system usage.
Accounting is generally used for billing and auditing purposes and is simply turned on for
those events that are to be tracked.
Syntax:
aaa accounting {system | network | exec | connection | commands level} {default | listname}
{start-stop | stop-only | none} method1 [method2...]
Commands - Runs accounting for all commands at the specified privilege level.
Level - Specific command level to track for accounting. Valid entries are 0 through 15.
Command - With this argument, command accounting logs information regarding which
commands are being executed on the router. The accounting record contains a list of
commands executed for the duration of the EXEC session, along with the time and date
information.
Reference:

Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)
Page 416.

QUESTION 175
Which command should you use to audit SLIP, PPP, and ARAP network service
requests on your Cisco router?

A. ip audit services enable
B. aaa accounting network
C. aaa accounting services enable
D. ip aaa audit network
E. ip audit enable

Answer: B

Explanation:
Accounting enables the administrator to collect information such as start and stop times for
user access, executed commands, traffic statistics, and resource usage and then store that
information in the relational database management system (RDBMS). In other words,
accounting enables the tracking of services and resources that are accessed by the user. Use
the aaa accounting command in global configuration mode for auditing and billing
purposes, as follows:
command level - Audits all commands at the specified privilege level (0-15).
connection - Audits all outbound connections such as Telnet, rlogin.
exec - Audits the EXEC process.
network - Audits all network service requests, such as SLIP, PPP, and ARAP.
system - Audits all system-level events, such as reload.
start-stop - Sends a start accounting notice at the beginning of a process and a stop
accounting notice at the end of a process. The start accounting record is sent in the
background. The requested user process begins regardless of whether the start accounting
notice was received by the accounting server.
stop-only - Sends a stop accounting notice at the end of the requested user process.
wait-start - As in start-stop, sends both a start and a stop accounting notice to the
accounting server. With the wait-start keyword, the requested user service does not begin
until the start accounting notice is acknowledged. A stop accounting notice is also sent.
{tacacs+ | radius} - Uses TACACS+ for accounting, or enables RADIUS-style accounting.
Reference:
Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)
Page 401

QUESTION 176
Some of the Certkiller locations are still using AppleTalk. What is true about RADIUS
and TACACS+ compatibility with the AppleTalk Remote Access (ARA) protocol?
(Choose all that apply.)

A. RADIUS server is incapable of supporting AppleTalk Remote Access (ARA)

protocol.
B. TACACS+ server is incapable of supporting AppleTalk Remote Access (ARA) protocol.
C. RADIUS server is capable of supporting AppleTalk Remote Access (ARA) protocol.
D. TACACS+ server is capable of supporting AppleTalk Remote Access (ARA) protocol.
E. Neither TACACS+ or RADIUS servers is capable of supporting AppleTalk Remote Access (ARA) protocol.
F. All of the above.

Answer: A, D

Explanation:
RADIUS does not support the following protocols:
• AppleTalk Remote Access (ARA) protocol
• Net BIOS Frame Protocol Control protocol
• Novell Asynchronous Services Interface (NASI)
• X.25 PAD connection
The TACACS+ protocol forwards many types of username password information. This information is encrypted over the network with MD5, an encryption algorithm. TACACS+ can forward the password types for ARA, SLIP, PAP, CHAP, and standard Telnet. This allows clients to use the same username password for different protocols.
References:
http://www.gazi.edu.tr/tacacs/docs/tac_rad_comp.html
http://www.cisco.com/warp/public/614/7.html

QUESTION 177
Which IOS command would you use on your router to specify a RADIUS server to take responsibility for authenticating dial-up clients?

A. aaa radius server
B. radius-server host
C. ip aaa radius host
D. aaa authentication radius-server

Answer: B

Explanation:
To specify a RADIUS server host, use the radius-server host configuration command. Use the no form of this command to delete the specified RADIUS host.
radius-server host {hostname | ip-address} [auth-port port-number]
[acct-port port-number]
[timeout seconds] [retransmit retries] [key string]
no radius-server host {hostname | ip-address}
hostname DNS name of the RADIUS server host.
ip-address IP address of the RADIUS server host.

auth-port (Optional) Specifies the UDP destination port for authentication requests.
portnumber
(Optional) Port number for authentication requests; the host is not used for
authentication if set to 0. The default authorization port number is 1645.
acct-port (Optional) Specifies the UDP destination port for accounting requests.
portnumber
(Optional) Port number for accounting requests; the host is not used for
accounting if set to 0. The default accounting port number is 1646.
timeout (Optional) The time interval (in seconds) that the router waits for the RADIUS
server to reply before retransmitting. This setting overrides the global value of
the radius-server timeout command. If no timeout value is specified, the global
value is used. Enter a value in the range 1 to 1000.
seconds (Optional) Specifies the timeout value. Enter a value in the range 1 to 1000. If
no timeout value is specified, the global value is used.
retransmit (Optional) The number of times a RADIUS request is resent to a server, if that
server is not responding or responding slowly. This setting overrides the global
setting of the radius-server retransmit command.
retries (Optional) Specifies the retransmit value. Enter a value in the range 1 to 100. If
no retransmit value is specified, the global value is used.
key (Optional) Specifies the authentication and encryption key used between the
router and the RADIUS daemon running on this RADIUS server. This key
overrides the global setting of the radius-server key command. If no key string
is specified, the global value is used.
The key is a text string that must match the encryption key used on the RADIUS
server. Always configure the key as the last item in the radius-server host
command syntax. This is because the leading spaces are ignored, but spaces
within and at the end of the key are used. If you use spaces in the key, do not
enclose the key in quotation marks unless the quotation marks themselves are
part of the key.
string (Optional) Specifies the authentication and encryption key for all RADIUS
communications between the router and the RADIUS server. This key must
match the encryption used on the RADIUS daemon. All leading spaces are
ignored, but spaces within and at the end of the key are used. If you use spaces in
your key, do not enclose the key in quotation marks unless the quotation marks
themselves are part of the key
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1826/products_feature_guide09186a00
80087cdc.html#xtocid103469

QUESTION 178
What's a major problem an administrator faces when using symmetric encryption to
secure their IP networks?

A. Slow calculation to encrypt and decrypt cipher
B. Key management
C. Based on complex mathematical operations

D. Best used for small (low volume) encryption tasks

Answer: B

Explanation:
The problem with symmetric encryption is with the key. There's a shared secret key at both ends, so the probability of a hacker finding the key is exponentially greater. Therefore there's great difficulty and responsibility in managing the keys. They need to be secured during service and distribution. They need to be changed often, and since humans are involved in each task, there's always doubt to the integrity of the security.

QUESTION 179
An ISDN PRI controller for the ISDN T1 on one of the Certkiller routers is configured as shown below:
controller t1 1
channel-group 0 timeslot 1-6
channel-group 1 timeslot 7
channel-group 2 timeslot 8
channel-group 3 timeslot 9-11
pri-group timeslot 12-24
What is true about the partial configuration above?

A. This is an incorrect configuration because more than one timeslot must be in a channel group.
B. This is a correct configuration and a corresponding serial interface named interface serial 0:23 for the D channel will automatically be created.
C. This is an incorrect configuration because channel groups and a primary group can not be configured on the same controller interface.
D. This is an incorrect configuration and the user must create corresponding serial interface for each of the data bearing timeslots 12-23

Answer: B

Explanation:
Once the controller is defined and configured, the last available channel will automatically be used by the Cisco IOS to be used as the ISDN D channel. In this case, serial 0/0:23 is the last available channel in an ISDN T1 (serial 0/0:0 is the first) so this will be created automatically.
Reference: CCNP Remote Access Exam Certification Guide, page 173-174, Brian Morgan & Craig Dennis, Cisco Press 2001, ISBN 1-58720-003-1

QUESTION 180
The Certkiller Italian WAN is displayed in the following diagram:

hostname Rome
!
username Paris password 0 Certkiller
isdn switch-type basic-net3
!
!
interface BRI0
no ip address
encapsulation ppp
dialer pool-member 1
!
interface Dialer1
ip address 10.10.0.1 255.255.255.252
encapsulation ppp
dialer remote-name Paris
dialer idle-timeout 30
dialer string 6115
dialer pool 1
ppp authentication chap
!
router rip
network 10.0.0.0
!
dialer-list 1 protocol ip permit
Assuming that Rome is the client (initiating the call) and Paris is the server (receiving the call) what is true?

A. Rome will initiate the call whenever any IP traffic is routed towards the Paris router.
B. Rome will initiate the call whenever any IP traffic is routed towards the Paris router however the call will last 30 seconds at maximum.
C. Rome will never initiate the call because the dialer remote-name is incorrectly configured on the Rome router.
D. Rome will never initiate the call because the dialer interface is not associated with any interesting traffic.

Answer: D

Explanation:
In order to associate an access list or a dialer list to an ISDN interface, the "dialer-group" command must be used on the BRI or Dialer interface. In this example, the "dialer-list 1" was created, which permits all IP traffic. The problem is that this dialer list was not tied to the dialer interface. The correct configuration syntax should have been:
interface Dialer1
ip address 10.10.0.1 255.255.255.252
encapsulation ppp
dialer remote-name Paris

dialer-group 1
dialer idle-timeout 30
dialer string 6115
dialer pool 1
ppp authentication chap
Reference: CCNP Remote Access Exam Certification Guide, page 143, Brian Morgan &
Craig Dennis, Cisco Press 2001, ISBN 1-58720-003-1

QUESTION 181
You are a senior network administrator and your junior administrator didn't arrive to
work because he claimed he was sick. So you give him an assignment to do from home
via Telnet. So from his home; he logged onto the companies router and entered the
following command:
Router(config)#aaa new-model
Before entering anything else, the lazy junior administrator (with the intention of being
cautious) thought it would be safe to save the configuration to NVRAM, log off from
telnet and take a break for a few hours. Assuming that no local username or password
exists on the router database, what will happen when the administrator tries to
immediately establish another telnet session? (Choose two)

A. The session asks for a username that may not exist.
B. The router requires a reboot to so the administrator can login.
C. The administrator must access the router through the console port to login.
D. The administrator can log in without using a password.

Answer: A, C

Explanation:
Once AAA has been enabled on the router, the administrator must declare the methods by
which authentication can take place. The key issue is to ensure that the administrator has a
way to gain access to the router if the AAA server is down. Failure to provide a backdoor
interface can result in lost communications to the router and the necessity to break in through
the console port. Care should be taken to always configure a local access method during any
implementation of AAA.
References:
Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)
Page 408
CCNP Remote Access Exam Certification Guide, page 374, Brian Morgan & Craig Dennis,
Cisco Press 2001, ISBN 1-58720-003-1

QUESTION 182
When comparing the differences between PPPoA and PPPoE, which of the following
statements are true?

A. PPPoE does not support session authentication with an aggregation router.
B. PPPaE provides simple bridged connections for a limited number of hosts.

C. PPPoA relies on client software to provide connectivity and authentication.
D. PPPoA is routed end-to-end over ATM from the user's PC to the aggregation router.
E. None of the above

Answer: D

Explanation:
Some key advantages of PPPoE and how they differ from PPPoA include:
• Per session authentication based on Password Authentication Protocol (PAP) or
Challenge Handshake Authentication Protocol (CHAP). This is the greatest advantage
of PPPoE as authentication overcomes the security hole in a bridging architecture.
• Per session accounting is possible, which allows the service provider to charge the
subscriber based on session time for various services offered. The service provider
may also require a minimal access charge.
• PPPoE can be used on existing CPE installations that cannot be upgraded to PPP or
that do not have the ability to run PPPoA, extending the PPP session over the bridged
Ethernet LAN to the PC.
• PPPoE preserves the point-to-point session used by Internet Service Providers (ISPs)
in the current dialup model. PPPoE is the only protocol capable of running point-topoint
over Ethernet without requiring an intermediate IP stack.
• The Network Access Provider (NAP) or Network Service Provider (NSP) can provide
secure access to a corporate gateway without managing end-to-end permanent virtual
circuits (PVCs) and making use of Layer 3 routing and/or Layer 2 Tunneling Protocol
(L2TP) tunnels. This makes the business model of selling wholesale services and
virtual private networks (VPNs) scalable.
• PPPoE can provide a host (PC) access to multiple destinations at a given time. There
can be multiple PPPoE sessions per PVC.
• The NSP can oversubscribe by deploying idle and session time-outs using an industry
standard Remote Authentication Dial-In User Service (RADIUS) server for each
subscriber.
• PPP can be used with the service selection gateway (SSG) feature.
Some key disadvantages of PPPoE and how they differ from PPPoA include:
• PPPoE client software must be installed on all hosts (PCs) connected to the Ethernet
segment. This means that the access provider must maintain the CPE and the client
software on the PC.
• Because PPPoE implementation uses RFC1483 bridging, it is susceptible to broadcast
storms and possible denial-of-service attacks.
Reference:
http://www.cisco.com/warp/public/794/pppoe_arch.html

QUESTION 183
DSL connections commonly use PPP over Ethernet (PPoE). What process does a
Certkiller host have to perform to establish a PPoE SESSION_ID?

A. A DHCP request process to request and IP address and session ID.
B. A Discovery process to identify a PPPoE server and request a session ID.

C. A RARP request process to request a MAC address and session ID.
D. A BOOTP process to request a configuration and session ID.
E. None of the above

Answer: B

Explanation:
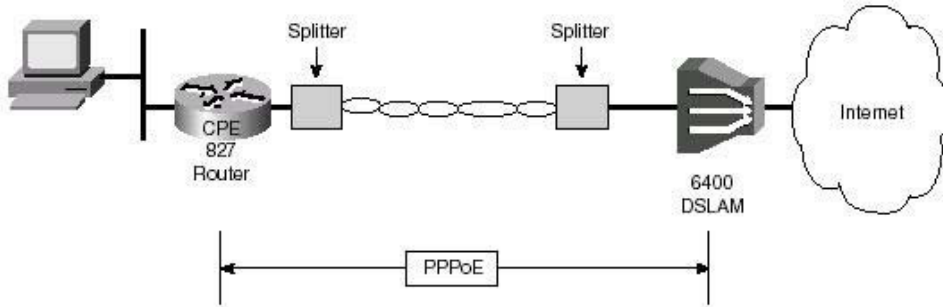
When a router wants to initiate a PPPoE session, it must first perform Discovery to identify the Ethernet MAC address of the peering device and establish a PPPoE SESSION_ID. Discovery is inherently a client/server relationship. During Discovery, a router discovers the provider DSLAM. Discovery allows the CPE router to discover all available DSLAMs, and then select one. When Discovery completes successfully, both the CPE router and the selected DSLAM have the information they will use to build their point-to-point connection over Ethernet.
Reference:
Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8) Page 253

QUESTION 184
Which two statements are true when an IPSec-protected path is configured for transport mode? (Choose two)

A. The payload of the packet is protected but the original IP address exposed.
B. The application endpoints must also be the IPSec endpoints.
C. IPSec gateways provide IPSec services to hosts.
D. Security is provided for the transport layer and above only.
E. Encrypted packets are encapsulated in another IP packet for routing.

Answer: B, E

Explanation:
IPSec can operate in one of two separate modes: transport mode and tunnel mode. These modes refer to how data is sent and secured throughout the network. In transport mode, IPSec protection is provided all the way from the source to the destination. In this way, transport mode is said to provide end-to-end transmission security.
Tunnel mode secures data only between tunnel points or gateways. Tunnel mode provides gateway-to-gateway transmission security. When data is in transmission between the client and the server, it remains unprotected until it reaches the gateway. Once at the gateway, it is

secured with IPSec until it reaches the destination gateway. At this point, data packets are decrypted and verified. The data is then sent to the receiving host unprotected. Tunnel mode is often employed when data must leave the secure confines of a local LAN or WAN and travel between hosts over a public network such as the Internet.

Transport mode is a host-to-host connection involving only two machines. In tunnel mode, the IPsec machines act as gateways and trafiic for any number of client machines may be carried.

Host machines (as opposed to security gateways) with IPsec implementations may also support transport mode. In this mode, the host does its own IPsec processing and routes some packets via IPsec.

In Transport-mode ESP, the ESP header is inserted into the IP datagram immediately prior to the transport-layer protocol header (e.g., TCP, UDP, or ICMP). In this mode, bandwidth is conserved because there are no encrypted IP headers or IP options.

QUESTION 185
Router CK1 is a Cisco 827 ADSL router configured as a PPPoE client. Part of the configuration of router CK1 is displayed below:

```
Interface Dialer0
ip address negotiated
ip nat outside
encapsulation ppp
dialer pool 1
ppp chap hostname 827-x@Certkiller.com
ppp chap password Certkiller
```
What is missing under the Interface Dialer0 configuration of CK1 ?

A. Request-dialin
B. Request-dialout
C. IP mtu 1492
D. IP mtu 1500
E. DSL operating-mode auto
F. Protocol pppoe

Answer: C

Explanation:
When a host (usually a PC) initiates a TCP session with a server, it negotiates the IP segment size by using the MSS option field in the TCP SYN packet. The value of the MSS field is determined by the maximum transmission unit (MTU) configuration on the host. The default MSS value for a PC is 1500 bytes. The PPP over Ethernet (PPPoE) standard supports a MTU of only 1492 bytes. The disparity between the host and PPPoE MTU size can cause the router in between the host and the server to drop 1500-byte packets and terminate TCP sessions over the PPPoE network. Even if the path MTU (which detects the correct MTU across the path) is enabled on the host, sessions may be dropped because system administrators sometimes disable the ICMP error messages that must be relayed from the host in order for path MTU to work.

The "ip tcp adjust-mss" command helps prevent TCP sessions from being dropped by adjusting the MSS value of the TCP SYN packets.

The "ip tcp adjust-mss" command is effective only for TCP connections passing through the router.

In most cases, the optimum value for the max-segment-size argument is 1452 bytes. This value plus the 20-byte IP header, the 20-byte TCP header, and the 8-byte PPPoE header add up to a 1500-byte packet that matches the MTU size for the Ethernet link.

If you are configuring the ip mtu command on the same interface as the ip tcp adjust-mss command, it is recommended that you use the following commands and values:

• ip tcp adjust-mss 1452
• ip mtu 1492

The ip tcp adjust-mss command does not work on subinterfaces or GRE tunnels.

Example:

The following example shows the configuration of a PPPoE client with the MTU value set to 1492:

```
vpdn enable
no vpdn logging
!
vpdn-group 1
request-dialin
protocol pppoe
!
interface Ethernet0
ip address 192.168.100.1.255.255.255.0
ip tcp adjust-mss 1452
ip nat inside
!
interface ATM0
no ip address
no atm ilmi-keepalive
pvc 8/35
pppoe client dial-pool-number 1
!
dsl equipment-type CPE
dsl operating-mode GSHDSL symmetric annex B
dsl linerate AUTO
!
interface Dialer1
ip address negotiated
ip mtu 1492
ip nat outside
encapsulation ppp
dialer pool 1
dialer-group 1
ppp authentication pap callin
ppp pap sent-username sohodyn password 7 141B1309000528
```

!
ip nat inside source list 101 Dialer1 overload
ip route 0.0.0.0.0.0.0.0 Dialer1
access-list permit ip 192.168.100.0.0.0.0.255 any

QUESTION 186
Certkiller .com would like to provide VPN security between its remote sites. After reviewing the Certkiller .com requirements, you recommend that the Certkiller should protect the entire original IP packet by encrypting it and encapsulating it inside a new, unencrypted IP header. The unencrypted header will be used to route the packet through the Internet.
Which mode will accomplish this?

A. IPSec Mode
B. Transport Mode
C. Channel Mode
D. Tunnel Mode
E. Host-to-host Mode
F. Protect Mode

Answer: D

Explanation:
Tunnel mode provides the protection of an entire IP packet by treating it as an AH or ESP payload. With tunnel mode, an entire IP packet is encapsulated with an AH or ESP header and an additional IP header. The IP addresses of the outer IP header are the tunnel endpoints, and the IP addresses of the encapsulated IP header are the ultimate source and destination addresses.
AH tunnel mode
As shown in the following illustration, AH tunnel mode encapsulates an IP packet with an AH and IP header and signs the entire packet for integrity and authentication.
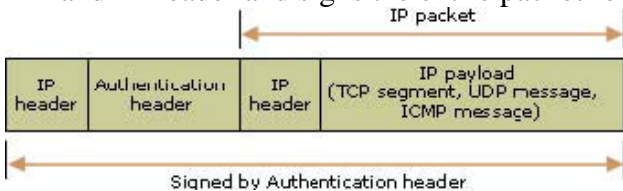
ESP tunnel mode
As shown in the following illustration, ESP tunnel mode encapsulates an IP packet with both an ESP and IP header and an ESP authentication trailer.
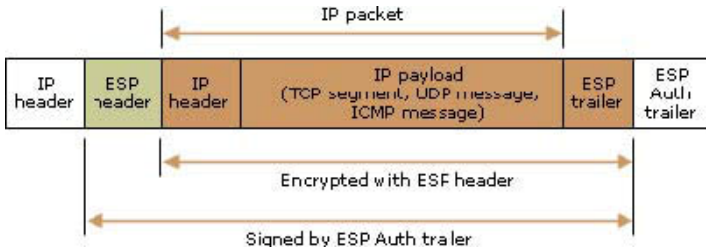
The signed portion of the packet indicates where the packet has been signed for integrity and

authentication. The encrypted portion of the packet indicates what information is protected with confidentiality.

Because a new header for tunneling is added to the packet, everything that comes after the ESP header is signed (except for the ESP authentication trailer) because it is now encapsulated in the tunneled packet. The original header is placed after the ESP header. The entire packet is appended with an ESP trailer before encryption occurs. Everything that follows the ESP header, except for the ESP authentication trailer, is encrypted. This includes the original header which is now considered to be part of the data portion of the packet.
Reference:
http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/enus/
sag_ipsec_und11.mspx

QUESTION 187
What happens to the NAT translation table entries when the command "clear ip nat trans *" is entered on one of the Certkiller routers?

A. It clears static NAT translation entries and NAT resumes.
B. It clears dynamic NAT translation table entries and NAT resumes.
C. It clears all existing NAT translation table entries and NAT is suspended.
D. It clears all inactive NAT translation entries and NAT is suspended.
E. None of the above

Answer: B

Explanation:
The following describes the various NAT clearing commands and their uses:
clear ip nat trans* - Clears all dynamic translation entries.
clear ip nat trans inside global-ip local-ip [outside local-ip
global-ip] - Clears a simple translation entry containing an inside translation, or both an inside and outside translation.
clear ip nat trans outside local-ip global-ip - Clears a simple
translation entry containing an outside translation.
clear ip nat trans protocol inside global-ip global-port
local-ip local-port [outside local-ip local-port global-ip
globalport] - Clears an extended entry (in its various forms).

Reference:
Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 14-23

QUESTION 188
The NAT table of one of the Certkiller routers is displayed below:

Based on this information, what is true about the command output above?

A. It reflects basic IP address translation.
B. It reflects how one inside host is seen as four different hosts to the outside world.
C. It reflects IP address translation with overloading.
D. It reflects no active translations.
E. None of the above.

Answer: C

Explanation:
Cisco defines these terms as follows:
• Inside local address - The IP address assigned to a host on the inside network. This is
the address configured as a parameter of the computer's OS or received via dynamic
address allocation protocols such as DHCP. The address is likely not a legitimate IP
address assigned by the Network Information Center (NIC) or service provider.
• Inside global address - A legitimate IP address assigned by the NIC or service
provider that represents one or more inside local IP addresses to the outside world.

• Outside local address - The IP address of an outside host as it appears to the inside network. Not necessarily a legitimate address, it is allocated from an address space routable on the inside.

• Outside global address - The IP address assigned to a host on the outside network by the host's owner. The address is allocated from a globally routable address or network space.

In this example, we can see that the IP address used for translating the inside hosts to the outside is the "inside global" address. This NAT table displays port information, and multiple entries with only the single IP address 78.37.71.213 being used. Because of this, PAT, or many to one, NAT is being used, which means that NAT with the keyword "overload" was configured.

References: CCNP Remote Access Exam Certification Guide, pages 350-351, Brian Morgan & Craig Dennis, Cisco Press 2001, ISBN 1-58720-003-1

http://www.cisco.com/en/US/tech/ CK6 48/ CK3 61/technologies_tech_note09186a0080094837.sh tml

---

QUESTION 189

The Certkiller network is displayed below:
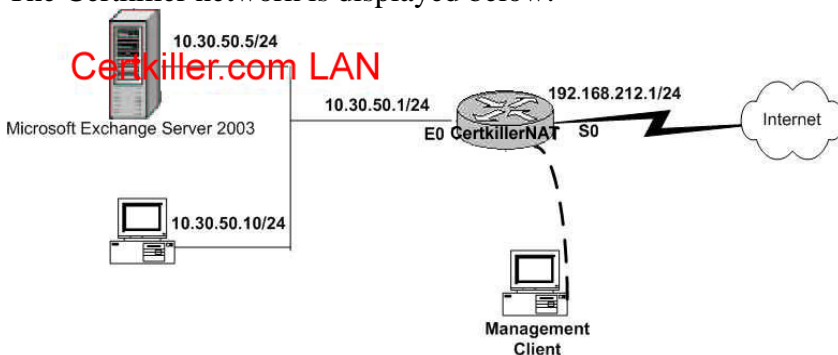
Certkiller .com is in the process of updating their network. They're going to change their internet service provider, install a local E-mail server, and install Microsoft Exchange Server 2003. The new ISP has allocated Certkiller .com a new Class C address range. However, the addresses of the internal routers and servers are to be kept intact. So you are to configure the router for NAT so the internal clients can use a single external IP address assigned to the public router interface. Finally you want Microsoft Exchange Server 2003 to be Internet accessible, so you have to provide a static translation for it. Your task is to configure the router for this using the following information:

Certkiller NAT
S0: 192.168.212.1/24
E0: 10.30.50.1/24
Secret password: Certkiller

Answer:
Certkiller NAT#config t
Certkiller NAT(config)#access-list 5 permit 10.30.50.0 0.0.0.255
Certkiller NAT(config)# ip nat inside source list 5 interface s0
overload
Certkiller NAT(config)#ip nat inside source static 10.30.50.5

192.168.212.5
Certkiller NAT(config)#int s 0
Certkiller NAT(config-if)#ip nat outside
Certkiller NAT(config-if)#exit
Certkiller NAT(config)#int e 0
Certkiller NAT(config-if)#ip nat inside
Certkiller NAT(config-if)#<Ctrl-Z>
Certkiller NAT#copy running start
Certkiller NAT#
Incorrect
Answer:
Certkiller NAT#config t
Certkiller NAT(config)#access-list 5 permit 10.30.50.0 0.0.0.255
Certkiller NAT(config)#ip nat pool lan 192.168.212.1
192.168.212.1 netmask 255.255.255.0
Certkiller NAT(config)#ip nat inside source list 5 pool lan
overload
Certkiller NAT(config)#ip nat inside source static 10.30.50.5
192.168.212.5
Certkiller NAT(config)#int s 0
Certkiller NAT(config-if)#ip nat outside
Certkiller NAT(config-if)#exit
Certkiller NAT(config)#int e 0
Certkiller NAT(config-if)#ip nat inside
Certkiller NAT(config-if)#<Ctrl-Z>
Certkiller NAT#copy running start
Certkiller NAT#

QUESTION 190
You need to configure NAT on the interfaces of the CK1 router. Which router interface
command would you use to enable NAT on an inside interface?

A. ip nat inside
B. ip nat map inside
C. ip nat permit inside
D. ip address inside

Answer: A

Explanation:
When you are configuring NAT, NAT should be enabled on at least one inside and one
outside interface. The command for enabling NAT on inside interface is:
R(config-if)# ip nat inside
The command for enabling NAT on the outside interface is:
R(config-if)# ip nat outside
Remember to enter into appropriate configuration modes before entering the commands.

Usually, the inside NAT will be configured on an Ethernet interface, whereas the outside NAT is configured on a serial interface. The command ip nat inside source static <local ip> <global ip> configures address translation for static NAT.
The command ip nat inside source list <access-list-number> pool <name> is used to map the access-list to the IP NAT pool during the configuration of Dynamic NAT.

QUESTION 191
What do network administrators often fail to consider when implementing NAT TCP load distribution?

A. It is enabled with the type rotary parameter on the ip nat pool command.
B. It is enabled by mapping multiple outside addresses to an inside address.
C. It is configured with the overload parameter on the ip nat inside command.
D. It requires an access list that permits an outside address to a group of inside local addresses.
E. All of the above.

Answer: D

Explanation:
TCP load distribution - A dynamic form of destination translation can be configured for some outside-to-inside traffic. When a mapping scheme is established, destination addresses matching an access list are replaced with an address from a rotary pool. Allocation is done on a round-robin basis, and only when a new connection is opened from the outside to the inside. All non-TCP traffic is passed un-translated (unless other translations are in effect). NAT requires an access-list that permits the outside address to the pool of inside local addresses. NST uses a single outside IP address, not multiple outside IP addresses. Furthermore, this single outside IP address can be translated to a pool of internal IP addresses. The ip nat pool command defines a pool of IP addresses for NAT. It does not enable NAT. The ip nat inside command enables NAT of the inside destination address. NAT is not configured by this command.
Reference:
Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 14-19

QUESTION 192
A Certkiller ADSL router is configured as shown below:

```
hostname 827-x
!
vpdn enable
!
vpdn-group pppoe
 request-dialin
  protocol pppoe
!
interface Ethernet0
 ip address 10.0.0.1 255.0.0.0
 ip nat inside
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
 pvc 3/34
 pppoe-client dial-pool-number 1
 !
 bundle-enable
 dsl operating-mode auto
!
interface Dialer0
 ip address negotiated
 ip mtu 1492
 encapsulation ppp
 dialer pool 1
 ppp chap hostname 827-x@cisco.com
 ppp chap password cisco
!
ip route 0.0.0.0 0.0.0.0 Dialer0
!
ip nat inside source list 101 interface Dialer0 overload
access-list 101 permit ip 10.0.0.0 0.255.255.255 any
```

Refer to the display configuration.
The 827 ADSL router is supposed to be setup as a PPPoE client. The user PCs behind the 827 are having Internet connectivity issues.
What could be the cause of the problem?

A. The vpdn-group pppoe configuration is not correct.
B. The port address translation (PAT) configuration is not correct.
C. The access-list 101 configuration is not correct.
D. For interface Dialer0, the IP MTU size should be 1500.
E. The default static route should be pointing to the ATM0 interface.

Answer: B

Explanation:
In the above configuration, the problem is the fact that a NAT statement is missing. Under the Dialer 0 interface, the command "ip nat outside" should have been configured. For ANT to operate properly, one or more interfaces must be configured for the inside (or trusted side, in the case) and one or more interfaces need to be specified as outside (untrusted side on this DSL connection).

QUESTION 193
Under PAT, packets destined for the outside world have their private IP address plus
port number translated to the router's external IP address _____ the IP packet is
forwarded to the WAN.

A. None of the choices.
B. Port number should not be included in the equation
C. Port number should not be included in the translation, but should be forwarded
D. Before
E. After

Answer: D

Explanation:
Packets destined for an external address have their private IP address plus port number
translated to the router's external IP address before the IP packet is forwarded to the WAN.
IP packets returning to the router have their external IP addresses (plus port number)
translated back to the private IP addresses, and the packets are forwarded to the LAN.

QUESTION 194
In a North American commercial network environment; what kind of interface will you
use to connect an asynchronous serial modem to a router or an end station?

A. HSSI (High Speed Serial Interface)
B. X.21
C. RS-449
D. EIA/TIA-232-C

Answer: D

Explanation:
The RS-232-C interface is a recommended standard (RS) interface established by the
Electronic Industries Association (EIA). (Also known as EIA/TIA-232)
The standard defines the specific electrical, functional, and mechanical characteristics used in
asynchronous transmissions between a computer (data terminal equipment, or DTE) and a
peripheral device (data communications equipment, or DCE). RS is the abbreviation for
recommended standard, and the C denotes the third revision of that standard. RS-232-C is
compatible with the CCITT V.24 and V.28 standards, as well as ISO IS2110.
RS-232-C uses a 25-pin or 9-pin DB connector. The accompanying illustration shows the
pinouts used in a DB-25 male connector. It is used for serial communications between a
computer and a peripheral device, such as a printer, modem, or mouse. The maximum cable
limit of 15.25 meters (50 feet) can be extended by using high-quality cable, line drivers to
boost the signal, or short-haul modems.
Reference: http://www.warknite.com/books/dictonary/Terms/2461HTML-2483.html

QUESTION 195
In an asynchronous interface, what purpose do chat scripts serve?

A. Informing the router as to which modem type is attached to the asynchronous
interface.
B. Send messages from one Telnet session to another.
C. Synchronize the serial DDR.
D. Initialize the directly attached modem.

Answer: A

Explanation:
A chat script is a one-line command that is used on an asynchronous interface to send
commands for modem dialing and for logging on to remote systems. Chat scripts indicate the
possible responses to expect and the information to send in each case. You can create a
different chat script for each type of modem in use on the router and for each system the
router might need to log in to.
Chat scripts are required for dialing out on the asynchronous interface on the router's
auxiliary port, but are also used on other asynchronous interfaces on access servers.
Chat scripts are strings of text used to send commands for modem dialing, logging onto
remote systems, and initializing asynchronous devices connected to an asynchronous line. On
a router, chat scripts can be configured on the auxiliary port only. A chat script must be
configured to dial out on asynchronous lines. You also can configure chat scripts so that they
are executed automatically for other specific events on a line, or so that they are executed
manually. Each chat script is defined for a different event. These events can include the
following:
• Line activation
• Incoming connection initiation
• Asynchronous dial-on-demand routing
• Line resets
• Startup
References:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/dial_c/dcasddr.htm
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/dial_c/dcmodem.h
tm#5148

QUESTION 196
You're at a computer supply warehouse and you find an EIA/TIA-232 null modem
cable with a DB25 connector. Ordinarily, two of the pins are cross connected on this
cable. Which two are they? (Choose two)

A. Pin 2
B. Pin 3
C. Pin 4
D. Pin 5
E. Pin 7

F. Pin 8

Answer: A, B

Explanation:
When two DTE devices (for example, an access server and a terminal) are near each other, it makes sense to connect them directly without going through a telephone network and two modems. An ordinary EIA/TIA-232 cable will not work in this case because both DTE devices transmit on the TxD lead (pin 2), and both expect input on the RxD lead (pin 3). A "null modem cable" is required for the DTE-to-DTE connection.
Null modems crisscross DB-25 pins 2 and 3 and other corresponding pins (as shown in the figure) so that the two DTE devices can communicate. Some devices can be configured to operate either like a DTE or a DCE. Configuring a device as a DCE usually means that it receives data on pin 2 and transmits data on pin 3. For example, many serial printers are configured as DCE devices so they can be connected directly to a DTE (for example, a PC or a terminal server) with an ordinary EIA/TIA-232 cable, eliminating the need for a null modem connection.
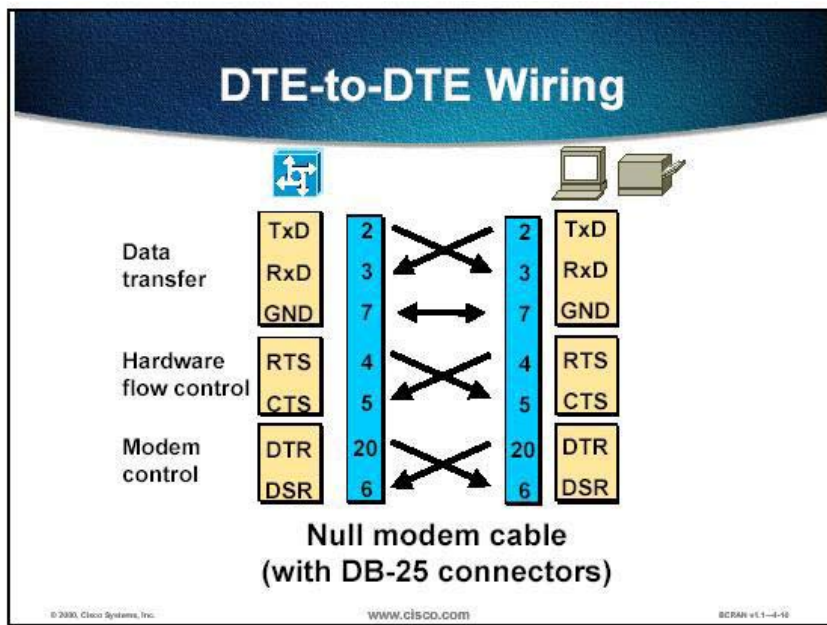
Reference:
Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 4-10

QUESTION 197
Which of the following modem standards includes the 'quick connect' and 'modem on hold' specifications?

A. V.92
B. V.32bis
C. V.22
D. V.90
E. V.34

F. None of the above

Answer: A

Explanation:
What V.92 is supposed to offer?
Increased upstream rates - up to 48k by using a PCM stream through an a/d conversion.
[Still, only 1 a/d conversion is required: if you have trouble getting 56k rates with V.90, there will be no improvement.] As of September, 2003, most server-side modems do not support PCM upstream at all, and those that do - 3Com & Patton - support a maximum upstream rate of 33.3kbps - less than the maximum V.34 upstream!
Modem on Hold-V.92 Modem on Hold allows a dial-in customer to suspend a modem session to answer an incoming voice call or to place an outgoing call while engaged in a modem session. When the dial-in customer uses Modem on Hold to suspend an active modem session to engage in an incoming voice call, the Internet service provider (ISP) modem listens to the original modem connection and waits for the dial-in customer's modem to resume the connection. When the voice call ends, the modem signals the telephone system to end the second call and return to the original modem connection, then the modem signals the ISP modem that it is ready to resume the modem call. Both modems renegotiate the connection, and the original exchange of data continues.
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ft9 2mmh1.htm#1022885
Quick Connect - The time to establish a connection may be reduced with faster handshaking.V.92 Quick Connect speeds up the client-to-server startup negotiation, reducing the overall connect time up to 30 percent. The client modem retains line condition information and characteristics of the connection to the Internet service provider (ISP), which reduces connect time by avoiding some of the initial signal handshaking.
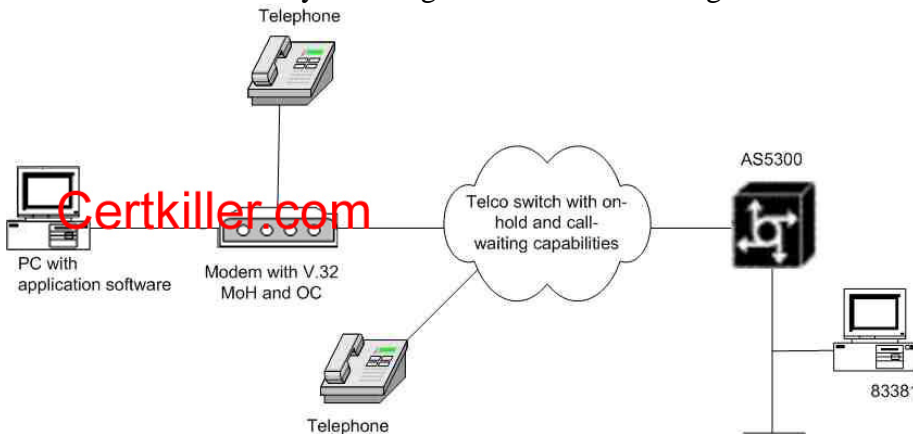
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/1 22xa/122xa_2/ft92mqc.htm#xtocid1863

QUESTION 198
In an asynchronous remote access network; the end devices are known as data terminal equipment (DTE) and they communicate through data circuit-terminating equipment (DCE). What kind of modem signal does a DCE use to transmit data?

A. RTS
B. RD
C. CTR
D. TD
E. All of the above

Answer: B

Explanation:
With a 25-pin connector (DB-25), only 8 pins are actually used for connecting a DTE (for example, an access server) to a DCE (for example, a modem). The other 17 signals are not "interesting" and are ignored. The eight interesting signals can be grouped into three categories by their functionality: data transfer, hardware flow control, and modem control. The figure shows the data transfer group, as follows:
• TxD-Transmit Data. The DTE transmits data to the DCE.
• RxD-Receive Data. The DTE receives data from the DCE.
• GRD (pin 7)-Ground. Provides the ground reference for voltage measurements.
Reference:
Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 4-7

QUESTION 199
When a modem is powered up, what does it do to notify the connected computer that the DCE is ready to use?

A. The modem sets DTE pin 4.
B. The modem sets DTR pin 20.
C. The modem sets DSR pin 6.
D. The modem sets DCE pin 5.
E. The modem sets DTR pin 3.
F. None of the above

Answer: C

Explanation:
Modem control consists of several signals between the DTE and DCE that are used to initiate, terminate, and monitor the status of the connection. This figure shows the remaining two groups of interesting signals between a DTE device and a DCE device, as follows:
Hardware flow control:
• RTS - Request To Send. The DTE has buffers available to receive from the DCE.
• CTS - Clear To Send. The DCE has buffers available to take data from the DTE.
Modem control:
• DTR - Data Terminal Ready. The DTE indicates to the DCE that it can accept an incoming call.
• CD - Carrier Detect (also referred to as Data Carrier Detect [DCD]). The DCE has established a carrier signal with the remote DCE.
• DSR (pin 6) - Data Set Ready. The DCE is ready for use. This pin is not used on

modem connections.
Reference:
Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 4-7

QUESTION 200
You're teaching a lesson on asynchronous modems at the Test-King academy, and
you're explaining how the DCE and DTE signal between each other. Suddenly one of
your students stands up and asks what happens when the signal on the DTR is lost.
What is the correct answer?

A. The CD tells the DTE that a DCE-to-DCE connection has been established.
B. The DTE applies voltage on pin 20 to alert the DCE that it is connected and available
to receive data.
C. The DCE terminates its connection with the remote modem.
D. The DTE issues a RTS to the DCE enabling communication.

Answer: C

Explanation:
Either the DTE device or the DCE device may signal for the connection to be terminated.
The signals that are used for this function are DTR from the DTE or the modem recognizing
the loss of the CD signal.

Reference:
Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 4-8