

## Part 3

---

### QUESTION 201

After completing the line configuration commands for one of the Certkiller routers, you need to get back into global configuration mode. What command do you use to exit line configuration mode and return to global configuration mode? (Type in answer below)

Answer: exit

Explanation:

To exit line configuration mode and return to global configuration mode, use the exit command. To exit line configuration mode and return to privileged EXEC mode, enter the end command, or press Ctrl-Z.

---

### QUESTION 202

A new modem is being attached to router CK1 . On this connection, what prevents the speed between the modem and the DTE from being varied?

- A. The modem attribute syn DTE
- B. The modem attribute static DTE
- C. The modem attribute lock DTE
- D. The modem attribute fixed DTE

Answer: C

Explanation:

The lock DTE speed command, which might also be referred to as port rate adjust or buffered mode, is often related to the way in which the modem handles error correction. This command varies widely from one modem to another. Locking the modem speed ensures that the modem always communicates with the Cisco access server or router at the speed configured on the Cisco auxiliary port. If this command is not used, the modem reverts to the speed of the data link (the telephone line), instead of communicating at the speed configured on the access server.

---

### QUESTION 203

What signal is used by DTE to indicate that it is willing to accept a call, according to the RS232 standard?

- A. RTS
- B. DTR
- C. CTS
- D. ETA
- E. DSR
- F. DCD
- G. FTS

Answer: B

Explanation:

RS232C is a communications port standard

RS232C separates equipment into Data Terminal Equipment (DTE) and Data Communication Equipment (Modems) (DCE). This is rather simplistic, as it always assumes that you will connect a modem to a terminal, however the use of the serial connection has extended somewhat since those days.

It defines the meanings of the signals, but not the type of connector, nor the pins on which each signal appears. Despite that, the 25 pin (and 9 pin) D connectors on an IBM compatible personal computer are generally accepted as a sort of standard for the pins, so I'll use these as examples.

The popular names of the lines tend to be as follows:

D25 D9 Name

PG 1 Protective Ground

SG 7 Signal Ground

TxD 2 (DTE) Data transmitted by DTE to DCE

RxD 3 (DCE) Data received by DCE

RTS 4 (DTE) "Request to Send" Start transmitter

CTS 5 (DCE) "Clear to Send" Have started transmitter

DSR 6 (DCE) "Data Set Ready" Modem ready to work

DCD 8 (DCE) "Data Carrier Detect" Remote transmitter is active

DTR 20 (DTE) "Data Terminal Ready" DTE indicates DCE may go off-hook

RI 22 (DCE) "Ring Indicator" DCE says a remote DCE has called

DTE uses the RTS output signal to indicate if it can receive characters into the Rx input buffer. The DCE should not send data to the DTE when DTR input is low (no RTS).

Reference: <http://www.ericlindsay.com/computer/rs232.htm>

---

**QUESTION** 204

Which of the following is true concerning the nature of hardware flow control (Choose all that apply)?

- A. It uses CTS for Clear To Stop
- B. It uses RTS for Request To Send
- C. It uses RTS for Request To Stop
- D. It uses CTS for Clear To Send

Answer: B, D

Explanation:

The popular names of the lines and their meanings are as follows:

RTS: Request to Send - Start transmitter - DTE

CTS: Clear to Send - Have started transmitter - DCE

DSR: Data Set Ready - Modem ready to work - DCE

DCD: Data Carrier Detect - Remote transmitter is active - DCE

DTR: Data Terminal Ready - DTE

RI: Ring Indicator - DCE

---

**QUESTION 205**

Your colleague at Certkiller Inc. is trying to setup an ISDN line to use as a backup for his Frame Relay correction. What is true about his configuration shown below?

```
interface serial0
ip address 192.168.10.1 255.255.255.0
backup interface bri0
backup delay 5 10
interface bri0
ip address 192.168.11.2 255.255.255.0
dialer idle-timeout 900
dialer-group 1
dialer-group 1 protocol ip permit
```

- A. The ISDN BRI line will be in "standby" mode after 900 seconds once the serial interface activates again.
- B. The ISDN BRI line will be in "standby" mode after 10 seconds but will be in "up/ip" mode after 900 seconds once the serial interface activates again.
- C. The ISDN BRI line will be in "standby" mode after 10 seconds and will be in "standby" mode after 900 seconds once the serial interface activates again.
- D. The ISDN BRI line will be in "standby" mode after 10 seconds once the serial interface activates again.

Answer: C

Explanation:

The specific commands used in this configuration are explained below:

backup interface bri0 = backup interface interface-type number

backup delay 5 10 = backup delay {enable-delay | never} {disabledelay | never}

enable-delay = Number of seconds that elapse after the primary line goes down before the Cisco IOS software activates the secondary line.

disable-delay = Number of seconds that elapse after the primary line comes up before the Cisco IOS software deactivates the secondary line.

never prevents the secondary line from being activated or deactivated.

dialer idle-timeout 900 = dialer idle-timeout seconds

Specifies the time that the line can remain idle before it is disconnected, with the default time is 120 seconds. In this case, when the serial interface again becomes active, the ISDN call will be dropped after 900 seconds.

## Activating Dial Backup for Line Failures

```
Router(config-if)#backup interface interface-type number
```

- Specifies the backup interface

```
Router(config-if)#backup delay {enable-delay | never} {disable-delay | never}
```

- Designates when to activate the backup line if a primary line fails

© 2001, Cisco Systems, Inc. www.cisco.com IOSAM v.1-04

Reference:

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

---

### QUESTION 206

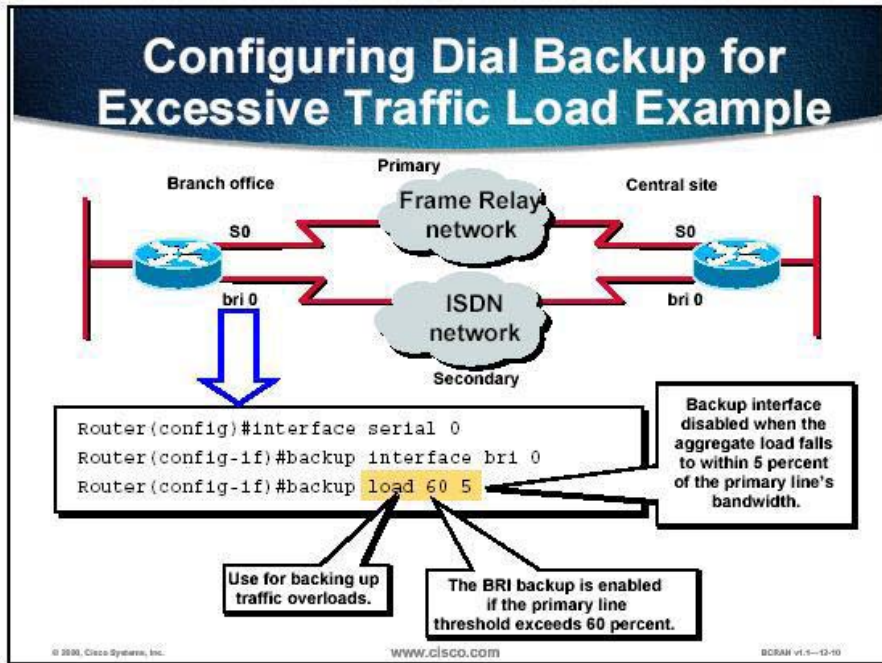
An administrator has just issued the command "backup load 60 5" on one of the Certkiller ISDN routers. What is the result of this configuration command? (Choose all that apply)

- A. The backup link activates when the primary link exceeds 60 percent of bandwidth.
- B. The backup link deactivates when the combined load falls to 4 kbps.
- C. The backup link deactivates when the primary link falls to 5 percent bandwidth.
- D. The backup link deactivates when the combined load falls to 5 percent bandwidth.
- E. The backup link activates when the primary link exceeds 60 kbps.

Answer: A, D

Explanation:

The backup load 60 5 command sets the traffic threshold to 60 percent of the primary line serial 0. When the load is exceeded, the secondary line is activated, and will not be deactivated until the combined load is less than 5 percent of the primary bandwidth.



Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Chapter 12-13

### QUESTION 207

Which command would you use to configure your backup interface to activate itself and 'kick in' when bandwidth utilization reaches 75% of the maximum bandwidth on the primary link?

- A. backup load 75 5
- B. backup delay load 3/4
- C. backup delay 75 0
- D. bandwidth demand .75%
- E. demand 75
- F. None of the above

Answer: A

Explanation:

The backup load 75 5 command specifies that the router should monitor the load on the primary interface and bring the link up when the load across the primary link is particularly heavy. The numbers represent the load on the interface, as shown by the show interface s0 command.

The load on an interface is represented by a number between 1 and 255. In the backup load 75 5 command, 75 is the percentage load at which the backup link is activated (in this case, 191/255).

The second number (in this case, 5%) is a measurement of aggregate load. Once the backup link has been initialized, the router continues to monitor the load. Once the load of both interfaces combined reaches a value of 13/255, the secondary link is terminated. So, although

dial backup was designed for link redundancy to partially compensate for primary link failure, it can also provide load-sharing capabilities to alleviate congestion on the WAN link.

Reference:

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

Page 319

---

**QUESTION 208**

What kind of terminals can you connect an ISDN line to? (Choose all that apply.)

- A. NU1
- B. TE2/TA
- C. TE1
- D. TO2
- E. NT0
- F. None of the above

Answer: B, C

Explanation:

Terminal equipment 1 (TE1) - Designates a device that is compatible with the ISDN network. A TE1 connects to a network termination of either type 1 or type 2 (NT1 or NT2).

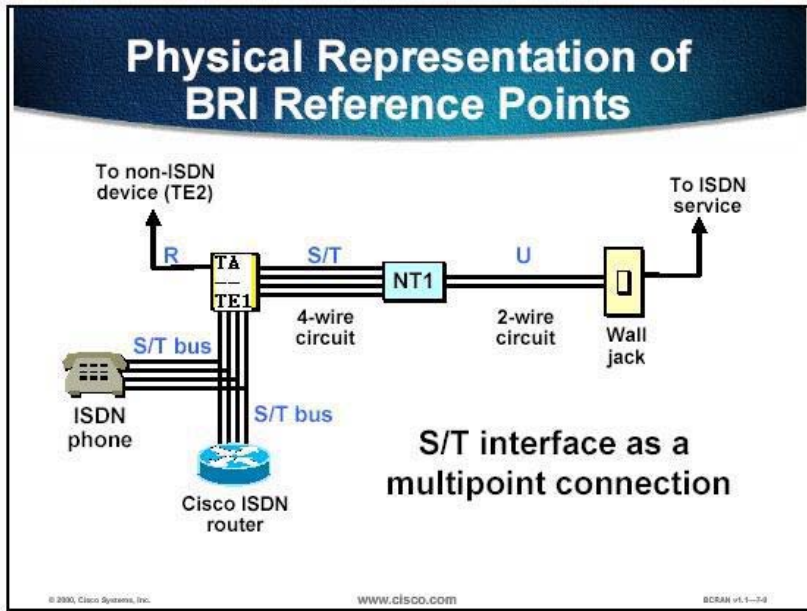
For example:

- Digital telephone
- Router with ISDN interface
- Digital facsimile equipment

Terminal equipment 2 (TE2) - Designates a device that is not compatible with ISDN and requires a terminal adapter. For example:

- Terminals with X.21, Electronic Industries Association/ Telecommunications Industry Association (EIA/TIA)-232, or X.25 interfaces
- Router without ISDN interface (AGS+ and so on)

Terminal adapter (TA) - Converts standard electrical signals into the form used by ISDN so that non-ISDN devices can connect to the ISDN network. For example: to convert V.35 or EIA/TIA-232 to ISDN (analog to ISDN).



Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 7-12

### QUESTION 209

Under which of the following circumstances would an ISDN BRI circuit be considered as a viable remote access solution?

- A. A branch office needs to connect to a mobile user.
- B. A mobile user that needs access to the central site while traveling.
- C. A remote site with sporadic traffic needs to connect to central site.
- D. A branch office requires at least 300kbps bandwidth to the central site.
- E. A mobile user that needs access at the branch office.

Answer: C

Explanation:

Basic Rate Interface (BRI) is an Integrated Systems Digital Network (ISDN) interface, and it consists of two B channels (B1 and B2) and one D channel. The B channels are used to transfer data, voice, and video. The D channel controls the B channels.

ISDN uses the D channel to carry signal information. ISDN can also use the D channel in a BRI to carry X.25 packets. The D channel has a capacity of 16 kbps, and the X.25 over D channel can utilize up to 9.6 kbps.

When this feature is configured, a separate X.25-over-D-channel logical interface is created. You can set its parameters without disrupting the original ISDN interface configuration. The original BRI interface will continue to represent the D, B1, and B2 channels.

Because some end-user equipment uses static terminal endpoint identifiers (TEIs) to access this feature, static TEIs are supported. The dialer understands the X.25-over-D-channel calls and initiates them on a new interface.

X.25 traffic over the D channel can be used as a primary interface where low-volume, sporadic interactive traffic is the normal mode of operation. Supported traffic includes IPX,

AppleTalk, transparent bridging, XNS, DECnet, and IP. This feature is not available on the ISDN Primary Rate Interface (PRI).

Reference:

[http://www.cisco.com/en/US/products/sw/iosswrel/ps1826/products\\_configuration\\_guide\\_chapter09186a00800d9b8a.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps1826/products_configuration_guide_chapter09186a00800d9b8a.html)

**QUESTION 210**

One of the Certkiller locations is using ISDN to backup their primary frame relay link. In an ISDN BRI network, what term is used to describe the device where the local loop terminated at?

- A. LE
- B. TA
- C. TE2
- D. NT1
- E. None of the above

Answer: D

Explanation:

In ISDN, the NT1 where your local loop terminates and the telephone company's loop begins.

"One important piece of equipment in any ISDN BRI installation is an NT1. The NT1 is a device similar to a channel service unit/data service unit (CSU/DSU), which is used in serial connections. The NT1 terminates the local loop....."

The NT1 has at least two interfaces: an S/T interface jack and a U interface. The S/T interface is attached to the router's BRI interface. The U interface is attached to the telco jack....."

Reference: CCNP Remote Access Exam Certification Guide, page 132, Brian Morgan & Craig Dennis, Cisco Press 2001, ISBN 1-58720-003-1

**QUESTION 211**

Match the T1/E1 PRI module LED meanings, to the correct warning indications on the right.

Select from these	Place here	
<input type="checkbox"/> LA	<input type="checkbox"/>	Alarm indicating loss of signal, loss of frame, or unavailability because of excessive errors.
<input type="checkbox"/> CD	<input type="checkbox"/>	Controller local loopback.
<input type="checkbox"/> LP	<input type="checkbox"/>	Carrier received on telco link.
<input type="checkbox"/> AL	<input type="checkbox"/>	Local alarm at remote end of connection
<input type="checkbox"/> RA	<input type="checkbox"/>	Loss of signal, loss of frame, or unavailability because of excessive errors.

Certkiller.com



Answer:

Select from these

Place here

AL

Alarm indicating loss of signal, loss of frame, or unavailability because of excessive errors.

LP

Controller local loopback.

CD

Carrier received on telco link.

RA

Local alarm at remote end of connection

LA

Loss of signal, loss of frame, or unavailability because of excessive errors.

### QUESTION 212

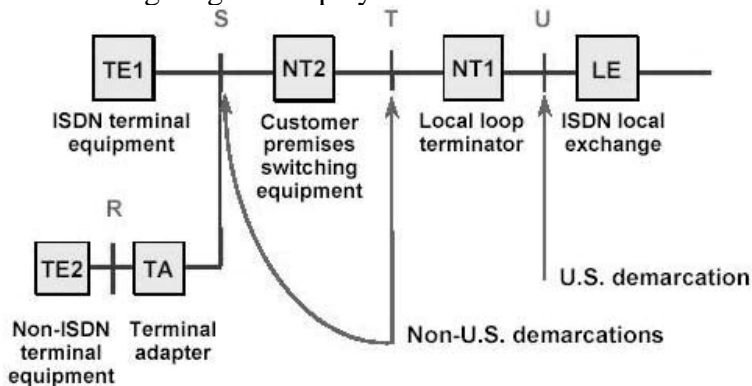
In a North American ISDN network, which reference point refers to the demarcation between the CPE and service provider?

- A. R reference point
- B. S reference point
- C. T reference point
- D. U reference point
- E. None of the above

Answer: D

Explanation:

The following diagram displays the different ISDN reference points:



Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 7-10

### QUESTION 213

In a leased T1 circuit WAN, what role does the CSU/DSU serve?

- A. It is responsible for the provision of encryption and compression for the security of

transmitted data.

- B. It is responsible for multiplexing individual 64K channels into a single circuit.
- C. It is responsible for channelizing the leased T1 line into multiple 65K circuits.
- D. It is responsible for the provision of signal timing for communications and interfaces to the digital transmission facility.
- E. It is responsible for converting the analog T1 signals into digital signals for the router interface.

Answer: B

Explanation:

T1/E1 is one of the most popular forms of data transmission today. It has been around for many years. Originally, T1 was solely a Telco transmission mechanism tool to reduce the number of wires being installed between central offices. One T1 circuit can provide 24 channels of digitized voice or data.

T1 is based on 24 voice channels of 64 Kbps. If you multiply that out (24 x 64K) you get 1.536 Mbps and not 1.544 Mbps.

The basic building blocks of a T1 network are the CSU/DSU, multiplexer and a bridge or router. Depending on the type of T1 network being created, not all of these components need to be used. The CSU/DSU (channel service unit/data service unit) is the actual connection point for the T1 wires. It provides line diagnostics and keep-alive functions for the line. In a leased line T1, the primary function of the CSU/DSU is to multiplex the individual channels into one single T1 circuit.

---

**QUESTION 214**

Which one of the following dial backup provides for the following IOS features?

- Is triggered by a lost IGP route
- Provides reliable connectivity
- Does not rely on interesting traffic to trigger an outgoing call to a remote router

- A. Floating static routes.
- B. Dialer backup.
- C. Dialer watch.
- D. Static routes.
- E. Dialer route.

Answer: C

Explanation:

Dialer Watch provides reliable connectivity without relying solely on defining interesting traffic to trigger outgoing calls at the central router. Dialer Watch uses the convergence times and characteristics of dynamic routing protocols. By configuring a set of watched routes that define the primary interface, you are able to monitor and track the status of the primary interface as watched routes are added and deleted.

---

**QUESTION 215**

Which of the following devices are classified as DTE (Data Terminal Equipment) devices? (Choose all that apply.)

- A. Router
- B. Modem
- C. Mainframe computer
- D. Terminal
- E. CSU/DSU

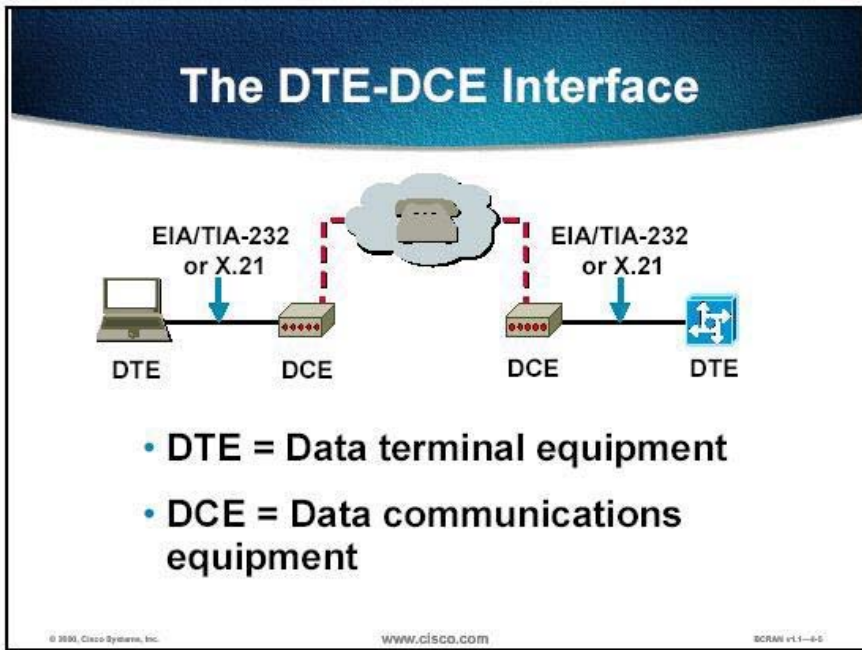
Answer: A, C, D

Explanation:

Data terminal equipment (DTE) includes end devices such as PCs, Routers, workstations, and mainframe computers. End devices communicate with each other through data communications equipment (DCE) such as modems, channel service units (CSUs), and data service units (DSUs). DCE can also be expanded to mean data circuit-terminating equipment which is the International Telecommunication Union-Telecommunications Standards Sector (ITU-TSS, or simply ITU-T; formerly known as CCITT (ITU-T/CCITT) definition. The data communications equipment, expansion of DCE is the Electronic Industries Association (EIA) definition.

The EIA/TIA-232 standard defines the interface between DTE and DCE. TIA stands for Telecommunications Industry Association. The end-to-end communication path between two DTEs consists of three segments (as illustrated in the figure): DTE-DCE, DCE-DCE, and DCE-DTE.

You must administer a set of cabling and configuration elements for each segment.



Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 4-5

**QUESTION 216**

Drag and drop the ISDN terms on the right side, next to the corresponding target on the left hand side:

Term	ISDN options	Use these
U interface	place here	four wires
TE1	place here	two wires
R interface	place here	non-ISDN device
S/T interface	place here	TE2 to TA
TE2	place here	native ISDN device

Answer:

Term	ISDN options	Use these
U interface	place here	four wires
TE1	place here	two wires
R interface	place here	non-ISDN device
S/T interface	place here	TE2 to TA
TE2	place here	native ISDN device

Explanation:

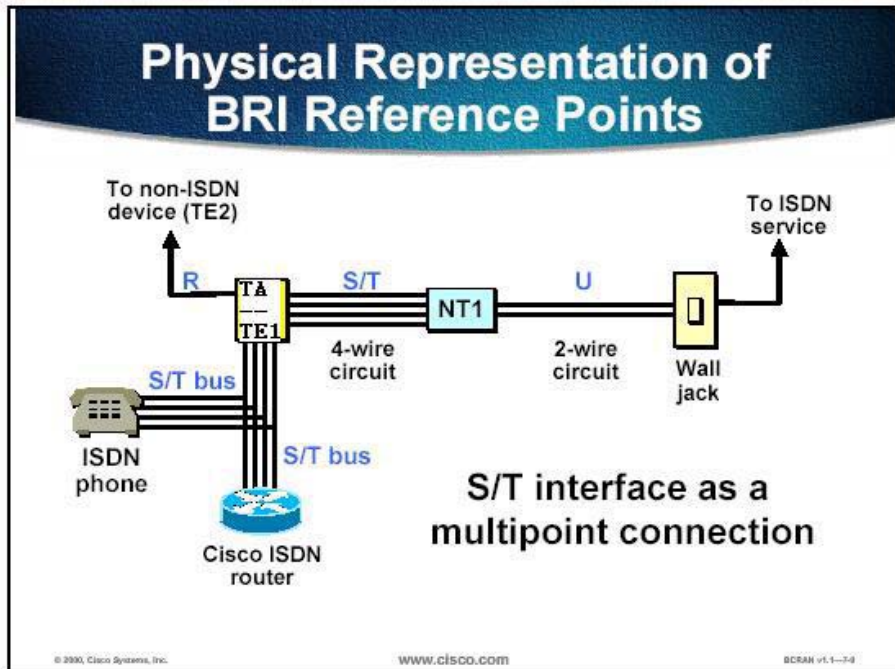
U interface - defines the two-wire interface between the NT and the ISDN cloud.

TE1 - designates a device that is compatible with the ISDN network.

R interface - defines the interface between the TA and an attached non-ISDN device (TE2).

S/T interface - is a four-wire interface (TX and RX).

TE2 - designates a device that is not compatible with ISDN and requires a terminal adapter.



Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 7-12

### QUESTION 217

In a DDR environment, it takes a certain amount of time for a line to come up. In the meantime, packets can accumulate. What command could you use to adjust the number packets that are held by the router while the DDR call is made?

- A. Use the hold-queue command.
- B. Use the no fair-queue command.
- C. Use the dialer hold-queue command.
- D. Use the dialer wait-for-carrier-time command.
- E. None of the above

Answer: C

Explanation:

Usually, when dialing is in progress the outgoing packets are dropped, since the connection is not yet made. To hold the interesting traffic to be held in a queue, to be sent out as soon as the connection is made use the command

Router(config-if)# dialer hold-queue <number>, where number is number of packets, range 0-100.

holds unto 100 packets of the interesting outgoing traffic in a queue, while the dialing takes place.

### QUESTION 218

In a dial on demand (DDR) routing environment, what variable does the dialer fast-idle command account for?

- A. The amount of idle time before dropping link on a line with contention.
- B. The amount of idle time before dropping link on a line without contention.
- C. The amount of idle time before dropping link on a line with no interesting packets sent.
- D. The amount of idle time before dropping link on a line with no interesting packets received.

Answer: A

Explanation:

The fast-idle timer is defined as the time to wait before dropping the link if there is no interesting traffic and the line is waiting to make another connection (contention).

---

**QUESTION 219**

Which of the following IOS entities are used to separate logical configurations from the physical interfaces that make or receive calls?

- A. dialer pool
- B. dialer map-class
- C. dialer profile
- D. dialer physical interface
- E. None of the above

Answer: C

Explanation:

Dialer profile is a type of configuring DDR, when the physical configuration is separated from logical interface-type profiles.

Incorrect Answers:

D: no such command

A,B: These commands are not used to create separated logical dialer entities.

---

**QUESTION 220**

You're setting up an ISDN WAN, and are in the midst of configuring your router to initiate a DDR call. In doing this, what purpose does the dialer-list command serve?

- A. It defines call destination parameters.
- B. It defines what constitutes interesting traffic.
- C. It provides for optional call parameters.
- D. It assigns a dialer-group to an interface.

Answer: B

Explanation:

The entire configuration DDR depends on how the traffic types that cause a call setup to occur are triggered. This traffic is known as interesting traffic.

Cisco's implementation of DDR allows for as much or as little specificity of interesting traffic as is deemed necessary; interesting traffic is defined by the creation of dialer-lists that can specify that an entire protocol suite, no matter the level of traffic, can trigger a call setup. Dialer-lists can be associated with standard or extended access lists to be specific to various traffic types. Rather than associating an access list with an interface, it is associated with a dialer list...."

Reference: CCNP Remote Access Exam Certification Guide, page 143, Brian Morgan & Craig Dennis, Cisco Press 2001, ISBN 1-58720-003-1

---

**QUESTION 221**

When DDR is implemented; a router will use a dialer profile to check if a dialer is connected to the desired remote destination. If the connection is there, the traffic can be sent. Every time an interesting packet crosses the dialer, a timer gets reset to the maximum configured value. What is the name of this particular timer?

- A. The wait for carrier timer
- B. The in-band timer
- C. The idle timer
- D. The fast-idle timer

Answer: C

In the above scenario the idle timer is used. The idle timer is used with the dialer idle-timeout command.

The purpose of DDR is to bring down the ISDN link when the traffic volume is low or idle. However, at times, the traffic volume can simply be in a short lull. Indeed, LAN traffic is bursty - quiet at times followed by an explosion of traffic.

To avoid the link coming down when traffic flow ceases and then being forced to redial, use the dialer idle-timeout command. Executing this command dictates that when traffic defined as interesting has ceased to flow across the link for the specified period of time (in seconds), go ahead and bring down the link. For instance, if the command dialer idle-timeout 180 is used at the interface configuration mode, the link comes down three minutes after the last piece of interesting traffic has traversed the link. Note that only interesting traffic resets the timer. Any non-interesting traffic goes across, but does not contribute to keeping the link up.

Reference: CCNP Remote Access Exam Certification Guide, page 148, Brian Morgan & Craig Dennis, Cisco Press 2001, ISBN 1-58720-003-1

---

**QUESTION 222**

What command line specifies the parameters for disconnecting an idle DDR call, when the line is needed for a new DDR call to a different destination?

- A. The time specified by dialer idle-timeout.
- B. The time specified by dialer fast-idle.
- C. The value configured by dialer load-threshold.
- D. The presence of interesting traffic (designated for a different destination) will force an

immediate disconnect.

Answer: B

Explanation:

dialer fast-idle (map-class dialer)

To specify the fast idle timer value to use when placing a call to any telephone number associated with a specified class, use the dialer fast-idle map-class dialer configuration command.

The following example specifies a dialer fast idle time of 10 seconds:

```
dialer string 4156884540 class Eng
```

```
! This mapclass
```

```
ensures that these calls use an ISDN speed of 56 kbps and a
```

```
! fast-idle time of 10 seconds.
```

```
map-class dialer Eng
```

```
isdn speed 56
```

```
dialer fast-idle 10
```

```
dialer wait-for-carrier-time 30
```

Reference:

[http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products\\_command\\_reference\\_chapter09186a00800ca525.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_command_reference_chapter09186a00800ca525.html)

---

### **QUESTION 223**

What happens to uninteresting traffic when it's carried over a DDR link?

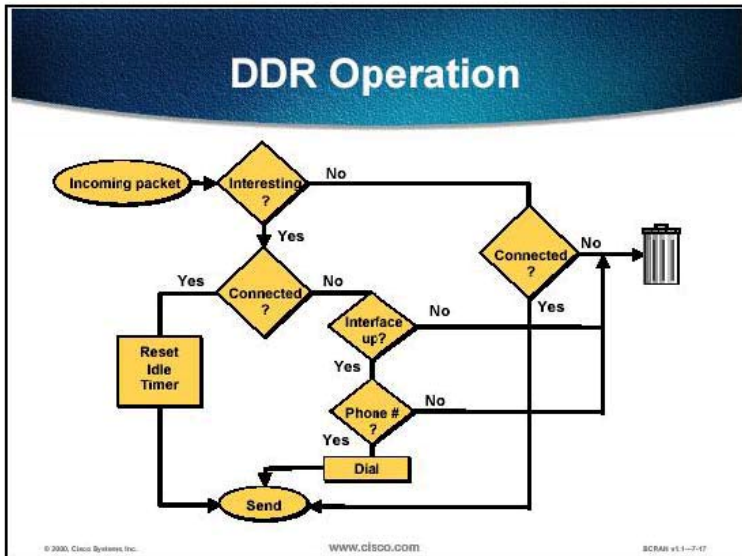
- A. Uninteresting traffic will be routed over an established DDR call, but at a lower priority than interesting traffic.
- B. Uninteresting traffic will keep DDR call established, even if no more interesting traffic is being routed over the link.
- C. Uninteresting traffic will not be routed over an established DDR call.
- D. Uninteresting traffic will be routed over an established DDR call, as long as there is enough interesting traffic to keep the call connected.

Answer: D

Explanation:

With Dial-on-Demand Routing (DDR), all traffic is classified as either interesting or uninteresting. If the traffic is interesting, then the router connects to the peer. If the traffic is not interesting then the call is not connected. However, for connections that are already connected, interesting traffic has a different purpose. It is used to reset the idle timeout back to the maximum value (configured with the dialer idle-timeout command). The moment a connection is made, the idle-timer starts to decrease. Once the router receives a packet that matches the interesting traffic definition, the idle-timer is reset back to the maximum value. Therefore, if a connection is up, it will send packets that are defined as uninteresting.





Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 7-20

### QUESTION 224

If you wanted to cache the routes learned by distance vector dynamic routing protocols so you can use them over a DDR connection and keep line usage costs down; what strategy would you use?

- A. Route redistribution
- B. DDR route maps
- C. Snapshot routing
- D. Passive interfaces
- E. Dynamic static routes

Answer: C

Explanation:

In ISDN dial-on-demand routing (DDR) environments, distance vector routing protocol periodic updates can unnecessarily keep an idle DDR link up, resulting in high usage bills. Snapshot Routing can be implemented to overcome this limitation. Distance vector protocols such as IP Routing Information Protocol (RIP), Internetwork Packet Exchange (IPX) RIP, and Interior Gateway Routing Protocol (IGRP) send a full routing table at a fixed interval of time as described below:

- The IP RIP routing protocol sends an update, by default, every 30 seconds.
- The IPX RIP routing protocol sends an update every 60 seconds, per its default interval.
- The IGRP routing protocol sends a routing table update, by default, every 90 seconds.

If you dialed the central site for each of these updates, this periodic traffic would keep an ISDN line up indefinitely and result in a high usage bill. If you do not dial the central site for these updates, dynamic routes (learned from the routing protocol) would be removed from the routing table. Snapshot routing forces the router to keep the routing table intact when the

DDR link is down and controls when to dial for periodic routing protocol updates. Snapshot routing provides the remedy for the constant periodic updates generated by the distance vector routing protocols. Snapshot routing operates by defining a routing protocol update active period and quiet period. The router may exchange a snapshot of the routing table during the active period. After the active period expires, a quiet period is maintained where routing updates are suppressed and the snapshot of the routing table is kept intact. Snapshot routing can be applied to IPX/RIP and AppleTalk Routing Table Maintenance Protocol (RTMP) as well.

---

**QUESTION 225**

On a DDR link; which feature maintains dynamic routing tables by controlling dial up connections for the sake of receiving periodic routing updates?

- A. Dial Backup
- B. Snapshot Routing
- C. Dialer Maps
- D. Route Redistribution

Answer: B

Explanation:

Snapshot routing was developed to save bandwidth utilization across dialup interfaces. With snapshot routing, the routing table is placed in an update-restricted (that is, frozen) state. This implementation of DDR utilizes a quiet period and an active period. The routing table is not updated during the quiet period, which is the length of time that the routing table remains frozen. When the quiet period expires, a dialer interface initiates a call to a remote router. The active period is the length of time the call remains up in order for the two routers to exchange routing updates.

Reference:

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

Page 187

---

**QUESTION 226**

Snapshot routing was designed to conserve bandwidth in dialup interfaces. Which of the following routing protocols are supported by Snapshot routing? (Choose two)

- A. RIP
- B. OSPF
- C. BGP
- D. IGRP
- E. EIGRP

Answer: A, D

Explanation:

It is important to note that snapshot routing is designed for use only with distance vector

routing protocols. Distance vector routing Snapshot allows the use of all "distance vector" routing protocols over DDR lines are :

- RIP & IGRP for IP
- RTMP for Appletalk
- RIP and SAP for IPX
- RTP for Vines

In addition, you can configure the router to exchange routing updates each time the line protocol goes from "down" to "up" or from "dialer spoofing" to "fully up."

References:

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

Page 187

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgr/dial\\_c/dcsnap.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgr/dial_c/dcsnap.htm)

---

**QUESTION 227**

You are the CTO of Certkiller Inc. and management has given you the order to reduce costs. So instead of purchasing dedicated router ports you decide to allow the last available physic BRI interface on your central router to dial out to the remote branch offices. Which two commands would your administrators have to enter to provide this capability? (Choose all that apply.)

- A. The dialer-group command
- B. The multilink ppp command
- C. The backup interface dialer command
- D. The dialer hunt-group command
- E. The dialer rotary-group command

Answer: C, E

Explanation:

Configuring Interfaces to Use a Backup Interface

To configure one or more interfaces to use a backup interface, use the following commands beginning in global configuration mode:

	<b>Command</b>	<b>Purpose</b>
<b>Step 1</b>	Router(config)# <b>interface</b> <i>type number</i>	Specifies the interface to be backed up and begins interface configuration mode.
<b>Step 2</b> <b>Step 3</b>	Router(config-if)# <b>unnumbered loopback0ip</b> Router(config-if)# <b>backup interface dialer</b> <i>number</i>	Specifies IP unnumbered loopback. Specifies the backup interface and begins interface configuration mode.
<b>Step 4</b>	Router(config-if)# <b>backup delay</b> <i>enable-delay disable-delay</i>	Specifies delay between the physical interface going down and the backup being enabled, and between the physical interface coming back up and the backup being disabled.

Dialer rotary group - ISDN rotary groups are similar to dialer pools. One primary differences, however, is the lack of map class capabilities in rotary groups. Configuring rotary groups involves the creation of logical dialer interfaces (as is done in dialer pool configurations), the interface designation of which is an important detail.

Reference: CCNP Remote Access Exam Certification Guide, page 160, Brian Morgan & Craig Dennis, Cisco Press 2001, ISBN 1-58720-003-1

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fdial\\_c/fnsprt6/dc\\_dbakdp.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fdial_c/fnsprt6/dc_dbakdp.htm)

---

**QUESTION 228**

How can an ISDN interface be used as a backup link for a primary interface and still use DDR to communicate with other sites?

- A. By using dialer profiles.
- B. An ISDN interface cannot be both.
- C. With the command backup interface serial 0/0 on the bri0/0 interface along with normal DDR commands.
- D. With the command backup interface bri 0/0 on the physical interface and normal DDR commands on the bri0/0 interface.

Answer: A

Explanation:

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

Reference:

[http://www.cisco.com/en/US/tech/CK8\\_01/CK1\\_33/technologies\\_configuration\\_example09186a0080093c2e.shtml](http://www.cisco.com/en/US/tech/CK8_01/CK1_33/technologies_configuration_example09186a0080093c2e.shtml)

---

**QUESTION 229**

Drag the channelized T1/E1 PRI Network Module LED abbreviation to the correct meaning.

EN	Local alarm at remote end of connection	Place here
RA	Carrier received on telco link	Place here
LA	The module has passed self-tests and is available to the router	Place here
LP	Controller local loopback	Place here
CD	Loss of signal, loss of frame, or unavailability because of excessive errors	Place here

Answer:

Local alarm at remote end of connection	RA
Carrier received on telco link	CD
The module has passed self-tests and is available to the router	EN
Controller local loopback	LP
Loss of signal, loss of frame, or unavailability because of excessive errors	LA

Explanation:

PRI Module LEDs

All network modules have an enable (EN) LED. This LED indicates that the module has passed its self-tests and is available to the router.

All PRI modules display four additional LEDs for each port. These LEDs are described in the following table:

ISDN PRI Network Module LEDs	
LED	Meaning
RA	Local alarm at remote end of connection
LA	Loss of signal, loss of frame, or unavailability because of excessive errors
LP	Controller local loopback
CD	Carrier received on telco link

Reference:

[http://www.cisco.com/en/US/products/hw/modules/ps2797/products\\_module\\_installation\\_guide\\_chapter09186a008007c8d2.html#wp1024462](http://www.cisco.com/en/US/products/hw/modules/ps2797/products_module_installation_guide_chapter09186a008007c8d2.html#wp1024462)

### QUESTION 230

What is the purpose of the dialer hold-queue command?

A. To allow interesting outgoing packets to be queued until a modem connection is

642-821

established.

- B. To allow any outgoing packets to be queued until a modem connection is established.
- C. To allow interesting outgoing packets to be queued when a source quench message is received.
- D. To allow any outgoing packets to be queued during network congestion.

Answer: A

Explanation:

Sometimes packets destined for a remote router are discarded because no connection exists. Establishing a connection using an analog modem can take time, during which packets are discarded. However, configuring a dialer hold queue will allow interesting outgoing packets to be queued and sent as soon as the modem connection is established.

A dialer hold queue can be configured on any type of dialer, including in-band synchronous, asynchronous, DTR, and ISDN dialers. Also, hunt group leaders can be configured with a dialer hold queue. If a hunt group leader (of a rotary dialing group) is configured with a hold queue, all members of the group will be configured with a dialer hold queue and no individual member's hold queue can be altered.

To establish a dialer hold queue, use the following command in interface configuration mode:

Command	Purpose
<b>dialer hold-queue</b> <i>packets</i>	Create a dialer hold queue and specify the number of packets to be held in it.

As many as 100 packets can be held in an outgoing dialer hold queue.

---

**QUESTION 231**

The following debug output was seen on RTA within the Certkiller network:

```

RTA# debug ppp negotiation
PPP protocol negotiation debugging is on
RTA#
*Mar 1 00:06:36.645: %LINK-3-UPDOWN: Interface BR10/1 changed state to up
*Mar 1 00:06:36.661: BR0:1 PPP: Treating connection as a callin
*Mar 1 00:06:36.665: BR0:1 PPP: Phase is ESTABLISHING. Passive Open [0 sess, 0 load]
*Mar 1 00:06:36.669: BR0:1 LCP: State is Listen
*Mar 1 00:06:37.034: BR0:1 LCP: I CONFREQ [Listen] id 7 len 17
*Mar 1 00:06:37.038: BR0:1 LCP: AuthProto PAP (0x0304C023)
*Mar 1 00:06:37.042: BR0:1 LCP: MagicNumber 0x507A214D (0x0506507A214D)
*Mar 1 00:06:37.046: BR0:1 LCP: Callback 0 (0x0D0300)
*Mar 1 00:06:37.054: BR0:1 LCP: O CONFREQ [Listen] id 4 len 15
*Mar 1 00:06:37.058: BR0:1 LCP: AuthProto CHAP (0x0305C22305)
*Mar 1 00:06:37.062: BR0:1 LCP: MagicNumber 0x1081E7E1 (0x05061081E7E1)
*Mar 1 00:06:37.066: BR0:1 LCP: O CONFREQ [Listen] id 7 len 7
*Mar 1 00:06:37.070: BR0:1 LCP: Callback 0 (0x0D0300)
*Mar 1 00:06:37.098: BR0:1 LCP: I CONFACK [REQsent] id 4 len 15
*Mar 1 00:06:37.102: BR0:1 LCP: AuthProto CHAP (0x0305C22305)
*Mar 1 00:06:37.106: BR0:1 LCP: MagicNumber 0x1081E7E1 (0x05061081E7E1)
*Mar 1 00:06:37.114: BR0:1 LCP: I CONFREQ [ACKrcvd] id 8 len 14
*Mar 1 00:06:37.117: BR0:1 LCP: AuthProto PAP (0x0304C023)
*Mar 1 00:06:37.121: BR0:1 LCP: MagicNumber 0x507A214D (0x0506507A214D)
*Mar 1 00:06:37.125: BR0:1 LCP: O CONFNAK [ACKrcvd] id 8 len 9
*Mar 1 00:06:37.129: BR0:1 LCP: AuthProto CHAP (0x0305C22305)
*Mar 1 00:06:37.165: BR0:1 LCP: I CONFREQ [ACKrcvd] id 9 len 15
*Mar 1 00:06:37.173: BR0:1 LCP: MagicNumber 0x507A214D (0x0506507A214D)
*Mar 1 00:06:37.177: BR0:1 LCP: O CONFACK [ACKrcvd] id 9 len 15
*Mar 1 00:06:37.181: BR0:1 LCP: AuthProto CHAP (0x0305C22305)
*Mar 1 00:06:37.185: BR0:1 LCP: MagicNumber 0x507A214D (0x0506507A214D)
*Mar 1 00:06:37.189: BR0:1 LCP: State is Open
*Mar 1 00:06:37.193: BR0:1 PPP: Phase is AUTHENTICATING. by both [0 sess, 0 load]

```

Given the above output, which two statements are true? (Choose two)

- A. The negotiated authentication protocol to be used is PAP.
- B. The negotiated authentication protocol to be used is CHAP.
- C. The two devices were not able to agree on an authentication protocol.
- D. This router is configured to accept callback requests.
- E. This router has initiated a callback request.
- F. The peer router is configured as a callback client.

Answer: B, F

#### Explanation:

The debug ppp negotiation command enables you to view the PPP negotiation transactions, identify the problem or stage when the error occurs, and develop a resolution.

Information regarding the output above is displayed below:

```
*Mar 1 00:06:37.058: BR0:1 LCP: AuthProto CHAP (0x0305C22305)
```

```
*Mar 1 00:06:37.062: BR0:1 LCP: MagicNumber 0x1081E7E1
(0x05061081E7E1)
```

!--- This router requests:

```
!--- Option: Authentication Protocol, Value: CHAP
```

```
*Mar 1 00:06:37.038: BR0:1 LCP: AuthProto PAP (0x0304C023)
```

```
*Mar 1 00:06:37.042: BR0:1 LCP: MagicNumber 0x507A214D
(0x0506507A214D)
```

```
*Mar 1 00:06:37.046: BR0:1 LCP: Callback 0 (0x0D0300)
```

!--- The peer has requested:

```
!--- Option: Authentication Protocol, Value: PAP
```

!--- Option: MagicNumber (This is used to detect loopbacks and is always sent.)

!--- Option: Callback, Value: 0 (This is for PPP Callback; MS Callback uses 6.)

Reference:

For information regarding the use of the "debug PPP negotiation" command, see the following link:

[http://www.cisco.com/en/US/tech/CK7\\_13/CK5\\_07/technologies\\_tech\\_note09186a00800ae945.shtml](http://www.cisco.com/en/US/tech/CK7_13/CK5_07/technologies_tech_note09186a00800ae945.shtml)

---

### QUESTION 232

The following configuration was placed on a Certkiller router named RTA:

```
rta(config)# interface bri0
rta(config-if)# ip address 192.168.12.3 255.255.255.240
rta(config-if)# encapsulation ppp
rta(config-if)# dialer map ip 192.168.12.1 name ROUTER1 5554321
rta(config-if)# dialer-group 1
rta(config-if)# ppp authentication chap
rta(config-if)# isdn spid1 40855512120000 5551212
rta(config-if)# isdn spid2 40855512340000 5551234
rta(config-if)# ppp multilink
rta(config-if)# dialer load-threshold 128 either
```

Given the configuration commands in the exhibit, when will additional B channels be added to the multilink PPP bundle?

- A. When the total load of outbound traffic reaches 128 k
- B. When the total load of inbound traffic reaches 128 k
- C. When the maximum calculated load as the larger of the outbound and inbound loads reaches 128 k
- D. When the total load of inbound traffic reaches 50 percent of bandwidth utilization.
- E. When the total load of outbound traffic reaches 50 percent of bandwidth utilization
- F. When the load of the inbound or outbound traffic reaches 50% utilization.
- G. When the load reaches 128 percent

Answer: F

Explanation:

To configure bandwidth on demand by setting the maximum load before the dialer places another call to a destination, use the dialer load-threshold interface command.

Syntax:

```
dialer load-threshold load [outbound | inbound | either]
```

load Interface load used to determine whether to initiate another call or to drop a link to the destination.

This argument represents a utilization percentage; it is a number between 1 and 255, where 255 is 100%.

outbound (Optional) Calculates the actual load using outbound data only.

inbound (Optional) Calculates the actual load using inbound data only.

either (Optional) Sets the maximum calculated load as the larger of the outbound and inbound loads.

In this example, the dialer load-threshold is set to 128, and 128/255 is approximately 50%.



Since the keyword "either" was used, the larger of the two loads (inbound and outbound) will be used.

---

**QUESTION 233**

Fill in the following blanks to make the statement below correct:

An ISDN PRI in Australia provides \_\_\_\_ B channels plus \_\_\_\_\_ D channels.

- A. 15, 1
- B. 24, 1
- C. 32, 1
- D. 30, 1
- E. 24, 2

Answer: D

Explanation:

ISDN Primary Rate Interface (PRI) service offers 23 B channels and 1 D channel in North America and Japan, yielding a total bit rate of 1.544 Mbps (the PRI D channel runs at 64 kbps). ISDN PRI in Europe, Australia, and other parts of the world provides 30 B channels plus one 64-kbps D channel and a total interface rate of 2.048 Mbps. The PRI physical layer specification is ITU-T I.431.

---

**QUESTION 234**

You are a Cisco Certified Engineer. You are configuring an ISDN remote access solution. With ISDN, non-ISDN terminals are referred to as:

- A. LE
- B. NT1
- C. TE1
- D. LE2
- E. LA
- F. TE2

Answer: F

Explanation:

ISDN components include terminals, terminal adapters (TAs), network-termination devices, line-termination equipment, and exchange-termination equipment. ISDN terminals come in two types. Specialized ISDN terminals are referred to as terminal equipment type 1 (TE1). Non-ISDN terminals, such as DTE, that predate the ISDN standards are referred to as terminal equipment type 2 (TE2). TE1s connect to the ISDN network through a four-wire, twisted-pair digital link. TE2s connect to the ISDN network through a T

A. The ISDN TA can

be either a standalone device or a board inside the TE2. If the TE2 is implemented as a standalone device, it connects to the TA via a standard physical-layer interface. Examples include EIA/TIA-232-C (formerly RS-232-C), V.24, and V.35.

**QUESTION 235**

Is the following statement True or False?

By directly connecting to the ISDN NT1 device, the router has more control over ISDN parameters in Europe.

- A. True
- B. False
- C. True only for BRI
- D. None of the choices.
- E. True only for PRI

Answer: B

Explanation:

The native ISDN interface on the Cisco 2503 router allows the router to be directly connected to an ISDN NT1 device. In many countries, the NT1 is provided by the telephone company. In the United States, however, the NT1 is customer-owned equipment. By directly connecting to the ISDN network, the router has more direct control over ISDN parameters and has access to ISDN information. In Europe, the ISDN providers retain more control over the ISDN parameters.

---

**QUESTION 236**

A new ISDN circuit is being provisioned for a remote Certkiller location. With ISDN, specialized ISDN terminals are referred to as which of the following?

- A. LE
- B. NT1
- C. TA
- D. TE1
- E. TE3
- F. LA

Answer: D

Explanation:

ISDN components include terminals, terminal adapters (TAs), network-termination devices, line-termination equipment, and exchange-termination equipment. ISDN terminals come in two types. Specialized ISDN terminals are referred to as terminal equipment type 1 (TE1). Non-ISDN terminals, such as DTE, that predate the ISDN standards are referred to as terminal equipment type 2 (TE2). TE1s connect to the ISDN network through a four-wire, twisted-pair digital link. TE2s connect to the ISDN network through a T

A. The ISDN TA can

be either a standalone device or a board inside the TE2. If the TE2 is implemented as a standalone device, it connects to the TA via a standard physical-layer interface. Examples include EIA/TIA-232-C (formerly RS-232-C), V.24, and V.35.

**QUESTION 237**

A new ISDN circuit is being provisioned for a remote Testing office. In ISDN, ITU-T I.450 belongs to which layer?

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

Answer: C

Explanation:

Two Layer 3 specifications are used for ISDN signaling: ITU-T (formerly CCITT) I.450 (also known as ITU-T Q.930) and ITU-T I.451 (also known as ITU-T Q.931). Together, these protocols support user-to-user, circuit-switched, and packet-switched connections. A variety of call-establishment, call-termination, information, and miscellaneous messages are specified, including SETUP, CONNECT, RELEASE, USER INFORMATION, CANCEL, STATUS, and DISCONNECT. These messages are functionally similar to those provided by the X.25 protocol.

---

**QUESTION 238**

New ISDN links are being provisioned for the Certkiller North American remote office branches. Which of the following ISDN reference points are relevant only in North America? (Choose all that apply)

- A. R
- B. U
- C. S
- D. T
- E. None of the above
- F. All of the above

Answer: B

Explanation:

ISDN specifies a number of reference points that define logical interfaces between functional groups, such as TAs and NT1s. ISDN reference points include the following:

R - The reference point between non-ISDN equipment and a TA.

S - The reference point between user terminals and the NT2.

T - The reference point between NT1 and NT2 devices.

U - The reference point between NT1 devices and line-termination equipment in the carrier network. The U reference point is relevant only in North America, where the NT1 function is not provided by the carrier network.

---

**QUESTION 239**

In the Certkiller network, you will be responsible for provisioning, configuring, and maintaining all of their ISDN connections. At ISDN layer 3, which of the following messages are NOT included? (Choose all that apply)

- A. PAUSE
- B. DISCONNECT
- C. CONNECT
- D. STATUS
- E. USER INFORMATION
- F. RELEASE
- G. SETUP
- H. CANCEL

Answer: A

Explanation:

According to Cisco: Two Layer 3 specifications are used for ISDN signaling: ITU-T (formerly CCITT) I.450 (also known as ITU-T Q.930) and ITU-T I.451 (also known as ITUT Q.931). Together, these protocols support user-to-user, circuit-switched, and packet-switched connections. A variety of call-establishment, call-termination, information, and miscellaneous messages are specified, including SETUP, CONNECT, RELEASE, USER INFORMATION, CANCEL, STATUS, and DISCONNECT. These messages are functionally similar to those provided by the X.25 protocol.

---

**QUESTION 240**

ISDN is used throughout the Certkiller network. In ISDN, the ITU-T Q.931 standard belongs to which layer?

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

Answer: C

Explanation:

Two Layer 3 specifications are used for ISDN signaling: ITU-T (formerly CCITT) I.450 (also known as ITU-T Q.930) and ITU-T I.451 (also known as ITU-T Q.931). Together, these protocols support user-to-user, circuit-switched, and packet-switched connections. A variety of call-establishment, call-termination, information, and miscellaneous messages are specified, including SETUP, CONNECT, RELEASE, USER INFORMATION, CANCEL, STATUS, and DISCONNECT. These messages are functionally similar to those provided by the X.25 protocol.

---

**QUESTION 241**

Link Access Procedure, Balanced (LAPD) is an important aspect of any ISDN connection. In ISDN, LAPD belongs to which layer?

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

Answer: A

Explanation:

Layer 2 of the ISDN signaling protocol is Link Access Procedure, D channel (LAPD). LAPD is similar to High-Level Data Link Control (HDLC) and Link Access Procedure, Balanced (LAPB). As the expansion of the LAPD acronym indicates, this layer it is used across the D channel to ensure that control and signaling information flows and is received properly.

---

**QUESTION 242**

How many Layer 3 specifications exist for ISDN signaling?

- A. 0
- B. 1
- C. 2
- D. 3
- E. 4

Answer: C

Explanation:

According to the technical documentation at CCO:

Two Layer 3 specifications are used for ISDN signaling: ITU-T (formerly CCITT) I.450 (also known as ITU-T Q.930) and ITU-T I.451 (also known as ITU-T Q.931). Together, these protocols support user-to-user, circuit-switched, and packet-switched connections. A variety of call-establishment, call-termination, information, and miscellaneous messages are specified, including SETUP, CONNECT, RELEASE, USER INFORMATION, CANCEL, STATUS, and DISCONNECT.

---

**QUESTION 243**

IN the Certkiller network, multiple ISDN routers are connected to a variety of different ISDN carrier switches. Which feature would you use if a single router needed to connect to multiple ISDN switch types?

- A. Multilink PPP
- B. Multilink Switches
- C. Multilink ISDN Channel aggregation
- D. Multiple ISDN Switch Types

E. None of the above

Answer: D

Explanation:

The Multiple ISDN Switch Types feature allows you to configure more than one ISDN switch type per router. You can apply an ISDN switch type on a per interface basis, thus extending the existing global isdn switch-type command to the interface level. This allows Basic Rate Interfaces (BRI) and Primary Rate Interfaces (PRI) to run simultaneously on platforms that support both interface types.

---

**QUESTION 244**

At the Certkiller network, you are responsible for provisioning and setting up new ISDN connections. A new ISDN PRI is being installed at a remote location and you want to configure the router. What T1 controller command can you use to configure the controller for ISDN PRI operation? (Type in answer below)

Answer: ISDN Switch-type

Explanation:

To configure an ISDN switch type for BRI and PRI interfaces using new switch type keywords, perform the following tasks beginning in global configuration mode. Step 2 is optional.

<b>Task</b>	<b>Command</b>
<b>Step 1</b> Configure the global ISDN switch type.	<b>isdn-switch type</b> <i>switch-type</i>
<b>Step 2</b> Configure the interface level ISDN switch type (optional).	<b>isdn-switch type</b> <i>switch-type</i>

National ISDN Switch Types for Basic Rate and Primary Rate Interfaces provides the following benefits: Unlike previous custom implementations, such as basic-5ess, basicdms100, primary-5ess, and primary-dms100, the National ISDN specification is designed to be switch independent. This increases flexibility in adapting to evolving standards and future enhancements. The ability to select PRI B channel order election for outgoing calls allows extended flexibility and compatibility with a variety of ISDN switch type service implementations. Additionally, this ability reduces ISDN switch misconfigurations, which can delay initial service activation.

---

**QUESTION 245**

A new ISDN circuit is being installed at a remote Certkiller location. Which of the following are network-termination devices, in addition to NT1, that can connect the four-wire subscriber wiring to the conventional two-wire local loop (Choose all that apply)?

A. NT3

- B. TA2
- C. LE
- D. NT2
- E. TA
- F. LE2

Answer: D

Explanation:

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

---

**QUESTION 246**

In general, multiple ISDN Switch Types support which of the following ISDN interfaces?

- A. None of the choices.
- B. Both BRI and PRI
- C. BRI only
- D. PRI only
- E. This feature is no longer supported

Answer: B

Explanation:

The Multiple ISDN Switch Types feature allows you to configure more than one ISDN switch type per router. You can apply an ISDN switch type on a per interface basis, thus extending the existing global isdn switch-type command to the interface level. This allows Basic Rate Interfaces (BRI) and Primary Rate Interfaces (PRI) to run simultaneously on platforms that support both interface types.

---

**QUESTION 247**

Which of the following statements about the ISDN switch type is NOT true? (Choose all that apply)

- A. It selects the PRI controller line code.
- B. It defines the type of signaling used by the ISDN service provider switch.
- C. It is a set of US only standard
- D. It is proprietary

- E. It is both a global and an interface command.
- F. It is a PRI controller command.
- G. None of the above.

Answer: A, C, D, F

Explanation:

To configure the switch type, use the command `isdn switch-type switch-type` in the global or interface configuration mode.

The ISDN switch type can be verified using the command `show isdn status`. The Telco should explicitly indicate the switchtype that needs to be configured. Occasionally (especially in North America) the Telco may indicate the switchtype is "custom" or "national". In such cases, use the following guidelines to determine the switchtype configuration:

Custom: If the Telco indicates that their switch-type is Custom, then configure the switch type on the router as `basic-5ess` (for BRI with 5ess switch), `primary-5ess` (for PRI with 5ess), `basic-dms` (for BRI with DMS switch), or `primary-dms` (for PRI with DMS).

National: switch type conforming to the NI-1 standard for BRI and NI-2 standard for PRI (there is no NI-1 standard for PRIs). If the Telco informs you that the switch type is National, then the Cisco router configuration should be `basic-ni` (for BRI) or `primary-ni` (for PRI).

Incorrect Answers:

B.: This statement is true. This describes the purpose of defining the switch type, so that the router can effectively communicate with the ISDN switch.

E: With support for the multiple ISDN switch types, this statement is also correct.

---

**QUESTION 248**

The Certkiller Company currently uses an ISDN BRI in standby mode to back up the primary serial connection. How can the BRI interface be configured to allow dialup operation as well as backup services?

- A. Configure the BRI as a standard DDR connection and configure the serial port to use BRI as the backup.
- B. Configure one B channel of the BRI as Standby Backup and two B channels as DDR.
- C. Configure one B channel of the BRI as Standby Backup and the other B channel as DDR.
- D. Configure two B channels of the BRI as Standby Backup and the other B channel as DDR.
- E. Use the dialer profile as a backup and configure the BRI as a member of the dialer pool.
- F. Configure one B channel of the BRI as Standby Backup and nothing else.

Answer: E

Explanation:



A backup interface is an interface that stays idle until certain circumstances occur, then it is activated. The backup interface can be a physical interface such as a Basic Rate Interface (BRI), or an assigned backup dialer interface to be used in a dialer pool. While the primary line is up, the backup interface is placed in standby mode. Once in standby, the backup interface is effectively shutdown until enabled. Any route associated with the backup interface will not appear in the routing table.

---

**QUESTION 249**

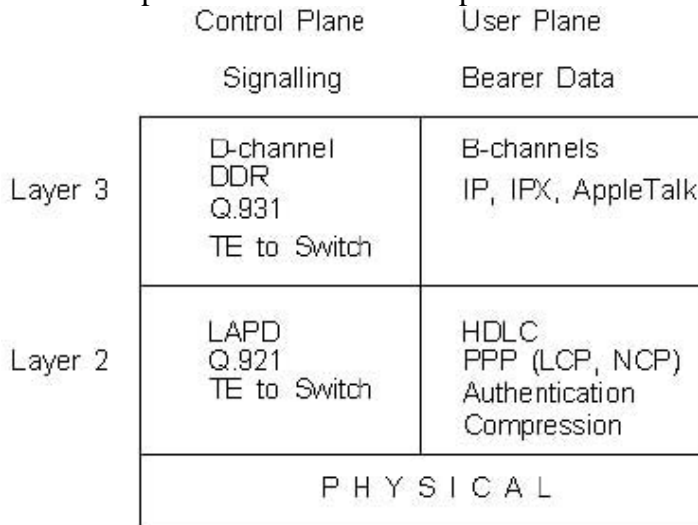
According to ISDN standards, the ITU-T Q.931 is the protocol that works for:

- A. Layer3; D channel
- B. Layer1, D channel
- C. Layer5; B channel
- D. Layer2; B channel
- E. Layer4; B channel
- F. Layer2; D channel

Answer: A

Explanation:

The ISDN protocol model can be represented in the following diagram:



Everything that is important occurs in the Control Plane on the D-Channel.

Additional Info:

Layer 3 ISDN signalling is specified in Q.930 (ITU-T I.450) and Q.931 (ITU-T I.451) and operate locally between the router and the switch. Different switch vendors have different bit interpretations hence why the switch type is important. Like Q.921, Q.931 is only concerned with the terminal to local switch, and it deals with making and tearing down the call via the D channel. Within the ISDN network itself SS7 Internal Signalling Utility Protocol (ISUP) is used. The fields for Q.931 are shown below:

Bits 8 4 4 1 7 1 7 8

Protocol Discriminator	0's	Call Reference Length	Flag	Call Reference	0	Message Type	Information Elements
------------------------	-----	-----------------------	------	----------------	---	--------------	----------------------

Reference: <http://www.rhyshaden.com/isdn.htm>

---

**QUESTION 250**

You are designing a Frame Relay network with a hub & spoke topology. What interface configuration combination would you use if you wanted inverse ARP to resolve addresses? (Choose two)

- A. Main interface at the hub router.  
Point-to-point subinterface at the spoke routers.
- B. Point-to-point subinterface at the hub router.  
Multipoint subinterface at the spoke routers.
- C. Point-to-point subinterface at the hub router.  
Main interface at the spoke routers.
- D. Multipoint subinterface at the hub router.  
Point-to-point subinterface at the spoke routers.

Answer: B, C

Explanation:

Frame Relay supports two types of interfaces: point-to-point and multipoint. The one you choose determines whether you need to use the configuration commands that ensure IP address to data-link connection identifier (DLCI) mappings. After configuring the PVC itself, you must tell the router which PVC to use in order to reach a specific destination. Let's look at these options:

- Point-to-point subinterface - With point-to-point subinterfaces, each pair of routers has its own subnet. If you put the PVC on a point-to-point subinterface, the router assumes that there is only one point-to-point PVC configured on the subinterface. Therefore, any IP packets with a destination IP address in the same subnet are forwarded on this VC. This is the simplest way to configure the mapping and is therefore the recommended method. Use the frame-relay interface-dlci command to assign a DLCI to a specified Frame Relay subinterface.
- Multipoint networks - Multipoint networks have three or more routers in the same subnet. If you put the PVC in a point-to-multipoint subinterface or in the main interface (which is multipoint by default), you need to either configure a static mapping or enable inverse Address Resolution Protocol (ARP) for dynamic mapping. In order to ensure that Inverse ARP resolves addresses across a hub and spoke topology, it is best to use single point to point subinterfaces for each PVC at the hub site.

Reference:

[http://www.cisco.com/en/US/tech/CK4\\_82/CK6\\_07/technologies\\_configuration\\_example09186a0080094a7a.shtml](http://www.cisco.com/en/US/tech/CK4_82/CK6_07/technologies_configuration_example09186a0080094a7a.shtml)

---

**QUESTION 251**

The Certkiller WAN consists of a hub and spoke frame relay network. In a multipoint

Frame Relay architecture; what is true about reachability issues? (Choose all that apply.)

- A. Split horizon can cause problems in NBMA environments.
- B. Subinterfaces can resolve split horizon issues.
- C. Split horizon is not an issue with multipoint subinterfaces.
- D. Subinterfaces do not apply in Frame Relay networks.
- E. Split horizon is an issue with point-to-point subinterfaces.
- F. A single physical interface can be configured to simulate multiple logical interfaces.
- G. All of the above.

Answer: A, B, F

Explanation:

The concept of sub interfaces was originally created in order to better handle issues caused by split-horizon over Non-Broadcast Multiple Access (NBMA) networks (e.g. frame relay, X.25) and distance-vector based routing protocols (e.g. IPX RIP/SAP, AppleTalk). Splithorizon dictates that a routing update received on an interface cannot be retransmitted out onto the same interface.

Multipoint interfaces/subinterfaces are still subject to the split-horizon limitations as discussed above. All nodes attached to a multipoint subinterface belong to the same network number. Typically, multipoint subinterfaces are used in conjunction with point-to-point interfaces in cases where an existing multipoint frame relay cloud is migrating to a subinterfaced point-to-point network design. A multipoint subinterface is used to keep remote sites on a single network number while slowly migrating remote sites to their own point-to-point subinterface network.

Configuring Frame Relay subinterfaces ensures that a single physical interface is treated as multiple virtual interfaces. This capability allows you to overcome split horizon rules so packets received on one virtual interface can be forwarded to another virtual interface, even if they are configured on the same physical interface.

References:

[http://www.alliancedatacom.com/manufacturers/cisco-systems/framerelay\\_design/subinterfaces.asp](http://www.alliancedatacom.com/manufacturers/cisco-systems/framerelay_design/subinterfaces.asp)

[http://www.cisco.com/warp/public/116/fr\\_faq.html#21](http://www.cisco.com/warp/public/116/fr_faq.html#21)

---

**QUESTION 252**

The performance and capabilities of Frame Relay is comparable to dedicated leased lines. What advantages does a Frame Relay connection have over a leased line? (Choose all that apply.)

- A. Lower cost.
- B. Better suited multiple branch locations.
- C. Full guaranteed bandwidth.
- D. More control over the connection.
- E. None of the above

Answer: A, B

Explanation:

Frame Relay provides virtual circuit connectivity for enterprise networks that require 56 kbps up to T1/E1 speeds. It costs less than leased lines because it uses statistical multiplexing of packets to gain efficiencies within the network, at the cost of a less-stringent bandwidth and latency guarantee. Frame Relay is being widely deployed in enterprise networks to connect regional and branch offices into the enterprise backbone.

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

© 2003 Cisco Systems, Inc. www.cisco.com BCRAN v1.1-2-10

Reference:

[http://www.cisco.com/en/US/products/hw/modules/ps2033/products\\_white\\_paper09186a0080091ca9.shtml](http://www.cisco.com/en/US/products/hw/modules/ps2033/products_white_paper09186a0080091ca9.shtml)

### QUESTION 253

Which of the following represent characteristics of a Frame Relay connection (Choose two)

- A. Branch site connectivity
- B. Circuit-switched
- C. High reliability
- D. Medium cost

Answer: A, D

Explanation:

Frame Relay provides virtual circuit connectivity for enterprise networks that require 56 kbps up to T1/E1 speeds. It costs less than leased lines because it uses statistical multiplexing of packets to gain efficiencies within the network, at the cost of a less-stringent bandwidth and latency guarantee. Frame Relay is being widely deployed in enterprise networks to connect regional and branch offices into the enterprise backbone.

## WAN Connection Summary

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

© 2000, Cisco Systems, Inc.

WWW.CISCO.COM

#CRAN v1.1-2-1E

Reference:

[http://www.cisco.com/en/US/products/hw/modules/ps2033/products\\_white\\_paper09186a0080091ca9.shtml](http://www.cisco.com/en/US/products/hw/modules/ps2033/products_white_paper09186a0080091ca9.shtml)

### QUESTION 254

One of the Certkiller remote locations is connected to the HQ site via a frame relay link. A Frame Relay connection is essentially an interconnection process between which types of equipment? (Choose all that apply.)

- A. DCE
- B. DTE
- C. PSTN
- D. PDN
- E. DSLAM
- F. None of the above

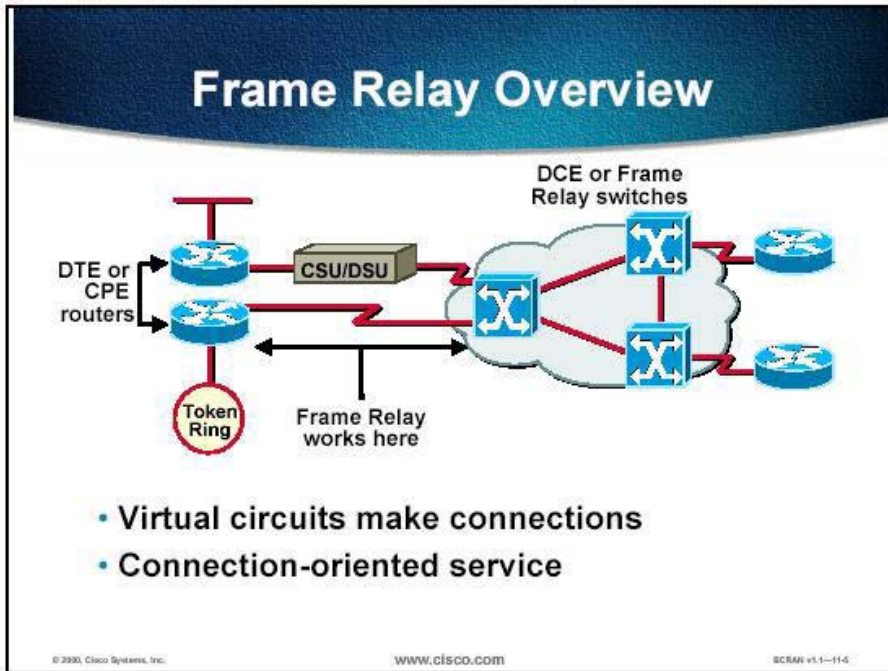
Answer: A, B

Explanation:

Frame Relay is an International Telecommunication Union Telecommunication Standardization Sector (ITU-T) and American National Standards Institute (ANSI) standard that defines the process for sending data over a public data network (PDN). It is a nextgeneration protocol to X.25 and is a connection oriented data-link technology that is streamlined to provide high performance and efficiency. It relies on upper-layer protocols for error correction and today's more dependable fiber and digital networks.

Note that Frame Relay defines the interconnection process between your customer premises equipment (CPE) (also known as data terminal equipment [DTE]), such as a router, and the service provider's local access switching equipment (known as data communications

equipment [DCE]). It does not define how the data is transmitted within the service provider's Frame Relay cloud.



Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 11-4

#### QUESTION 255

Switch CK1 is used as a frame relay switch. When this Frame Relay switch becomes locally congested, the header of a frame (moving towards the destination device) is changed to a 1. Which frame header bit is it?

- A. BECN
- B. MIR
- C. CIR
- D. FECN
- E. PIR
- F. None of the above

Answer: D

Explanation:

If a frame handler (i.e. Frame Relay router) suffers from congestion, it will notify the corresponding access nodes by FECN (C/R=0) and BECN (C/R=1) bits set to one. The access nodes won't accept frames that exceed the CIR any longer unless the congestion alarm has stopped (FECN=0, BECN=0).

When the congestion queue thresholds configured at the interface or class level of the PE router are exceeded, PE router does the following:

- Sets the FECN bit to 1 on the outgoing packets.
- Sets the BECN bit to 1 for all traffic destined for the originating CE router, which

decreases its traffic based on the number of BECN packets it received.

FECN and BECN each is controlled by a single bit contained in the Frame Relay frame header. The Frame Relay frame header also contains a Discard Eligibility (DE) bit, which is used to identify less important traffic that can be dropped during periods of congestion. The FECN bit is part of the Address field in the Frame Relay frame header. The FECN mechanism is initiated when a DTE device sends Frame Relay frames into the network. If the network is congested, DCE devices (switches) set the value of the frames' FECN bit to 1. When the frames reach the destination DTE device, the Address field (with the FECN bit set) indicates that the frame experienced congestion in the path from source to destination. The DTE device can relay this information to a higher-layer protocol for processing. Depending on the implementation, flow control may be initiated, or the indication may be ignored. The BECN bit is part of the Address field in the Frame Relay frame header. DCE devices set the value of the BECN bit to 1 in frames traveling in the opposite direction of frames with their FECN bit set. This informs the receiving DTE device that a particular path through the network is congested. The DTE device then can relay this information to a higher-layer protocol for processing. Depending on the implementation, flow-control may be initiated, or the indication may be ignored.

Reference: [http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/frame.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/frame.htm)

---

**QUESTION 256**

It is possible to support multiple logical Frame Relay virtual circuits over the same physical serial connection. How does this happen?

- A. The DCE provides multiple time slots in which to send specific VC data streams.
- B. The DTE encapsulates packets with a header containing an identifier for each VC.
- C. The Frame Relay switch uses inverse ARP to map the Layer 3 address to a DLCI for each VC.
- D. The DTE channelizes the bandwidth into multiple 64K circuits, each supporting a separate VC.
- E. None of the above

Answer: B

Explanation:

Frame Relay provides a means for statistically multiplexing many logical data conversations (referred to as virtual circuits) over a single physical transmission link by assigning connection identifiers to each pair of DTE devices. The service provider's switching equipment constructs a table that maps connection identifiers to outbound ports. When a frame is received, the switching device analyzes the connection identifier and delivers the frame to the pre-established, associated outbound port.

The virtual circuits can be either permanent virtual circuits (PVCs) or switched virtual circuits (SVCs). PVCs are permanently established connections that are used when there is frequent and consistent data transfer between DTE devices across a Frame Relay network.

Reference:

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

---

**QUESTION 257**

Within the Certkiller network, multiple frame PVC's are used to connect all of the locations. In which three states can a Frame Relay permanent virtual circuit (PVC) occur? (Select three)

- A. Down
- B. Deleted
- C. Init
- D. Inactive
- E. Active
- F. Operational

Answer: B, D, E

Explanation:

The show frame-relay pvc command displays the status of each configured connection as well as traffic statistics. This command is also useful for viewing the number of backward explicit congestion notification (BECN) and forward explicit congestion notification (FECN) packets received by the router. The PVC STATUS can be active, inactive, or deleted.

If you enter show frame-relay pvc, you will see the status of all the PVCs configured on the router. If you specify a specific PVC, you will only see the status of that PVC. In the figure, the show frame-relay pvc 110 command only displays the status of PVC 110.

**Verifying Frame Relay Operation (cont.)**

```
Router#show frame-relay pvc 110
PVC Statistics for interface Serial0 (Frame Relay DTE)
DLCI = 110, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0

  input pkts 14055 output pkts 32795 in bytes 1096228
  out bytes 6216155 dropped pkts 0 in FECN pkts 0
  in BECN pkts 0 out FECN pkts 0 out BECN pkts 0
  in DE pkts 0 out DE pkts 0
  out bcst pkts 32795 out bcst bytes 6216155

<Output Omitted>
```

- Displays PVC traffic statistics

© 2000, Cisco Systems, Inc. www.cisco.com BCRAG v1.1--11-11

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 11-12



**QUESTION 258**

Router CK1 is configured for frame relay and has the LMI auto-sensing feature enabled. What's true about LMI auto-sensing? (Choose all that apply)

- A. It involves sending full status requests to the Frame Relay switch.
- B. It is used to automatically detect the Frame Relay CIR of each PVC.
- C. It is used to tell the router about LMI type.
- D. It only works if the Frame Relay LMI type is cisco.

Answer: A,C

Explanation:

Local Management Interface (LMI) is a signaling standard between the CPE device and the Frame Relay switch that is responsible for managing the connection and maintaining status between the devices. LMIs include support for a keepalive mechanism, which verifies that data is flowing; a multicast mechanism, which provides the network server with its local DLCI; the multicast addressing, which gives DLCIs global rather than local significance in Frame Relay networks; and a status mechanism, which provides an ongoing status on the DLCIs known to the switch.

Although the LMI is configurable, beginning in Release 11.2, the Cisco router tries to autosense which LMI type the Frame Relay switch is using by sending one or more full status requests to the Frame Relay switch. The Frame Relay switch responds with one or more LMI types. The router configures itself with the last LMI type received. Three types of LMIs are supported:

- cisco - LMI type defined jointly by Cisco, StrataCom, Northern Telecom, and Digital Equipment Corporation, nicknamed "the gang of four"
- ansi - Annex D, defined by the ANSI standard T1.617
- q933a - ITU-T Q.933 Annex A

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 11-7

---

**QUESTION 259**

While troubleshooting a Frame Relay connection, you discover that the PVC status is being reported as deleted. What is most likely causing this problem?

- A. The PVC is not configured on the CSU/DSU.
- B. The PVC is not configured on the remote router.
- C. The PVC is not configured on the local router.
- D. The PVC is not configured on the Frame Relay switch.
- E. All of the above could cause this

Answer: C

Explanation:

If an LMI status report indicates that a PVC is not active, then it is marked as inactive. A PVC is marked as deleted if it is not listed in a periodic LMI status message.

When the interface is configured as a DCE and the DLCI usage is SWITCHED, the value displayed in the PVC STATUS field is determined by the status of outgoing interfaces (up or down) and status of the outgoing PVC.

The status of the outgoing PVC is updated in the local management interface (LMI) message exchange. PVCs terminated on a DCE interface use the status of the interface to set the PVC STATUS.

If the outgoing interface is a tunnel, the PVC status is determined by what is learned from the tunnel. If an LMI status report indicates that a PVC is not active, then it is marked as inactive. A PVC is marked as deleted if it is not listed in a periodic LMI status message, such as when the remote frame switch is configured for a specific PVC while the router is not.

---

**QUESTION 260**

What is true about a Frame Relay data-link connection identifier (DLCI)? (Choose all that apply)

- A. DLCI is assigned by the customer and applied to their CPE.
- B. DLCI is assigned by the Frame Relay service provider.
- C. DLCI must be identical on all DTE devices.
- D. DLCI has a local significance only.
- E. DLCI has remote significance only.
- F. None of the above

Answer: B, D

Explanation:

The DLCI is a number that is tagged to the virtual circuit of the service provider. Since the number is determined on a 'per-leg' basis during data transmission, so it's only locally significant. The number only has to be agreed upon by the two frame relay devices directly connected to each other. Although a specific DLCI number can be requested from the customer, the DLCI is assigned from the frame relay provider.

---

**QUESTION 261**

Which of the following terms describes the committed average rate that a Frame Relay switch transfers data at during periods of non-congestion?

- A. Committed burst rate
- B. Excess burst rate
- C. Local access rate
- D. CIR
- E. MIR
- F. PIR
- G. BCR

Answer: D

Explanation:

The CIR (committed information rate) is the rate that an administrator would want to transmit at during times when the network isn't congested. The CIR that you want isn't necessarily the same as the CIR of the service provider. CIR rates are purchased from the provider. When the data rates exceed the CIR, the frames are marked as Discard Eligible (DE) and are not guaranteed to be delivered across the frame relay network.

Reference: CCNP Remote Access Exam Certification Guide, page 270, Brian Morgan & Craig Dennis, Cisco Press 2001, ISBN 1-58720-003-1

---

**QUESTION 262**

You are tasked with the IP address assignment of the Certkiller frame relay network. With regards to network layer address assignment, which of the following are true regarding the effects of using frame relay sub interfaces on a physical interface?

- A. The network layer address of each sub interface must be in the same subnet as the physical interface address.
- B. The network layer address of each sub interface must be approved by IANA
- C. The network layer address must be removed from the physical interface.
- D. The network layer address of each sub interface must be the same as the physical interface address.
- E. The sub interfaces should be assigned the network broadcast address of the physical interface.
- F. None of the above.

Answer: C

Explanation:

Frame Relay subinterfaces provide a mechanism for supporting partially meshed Frame Relay networks. Most protocols assume transitivity on a logical network; that is, if station A can talk to station B, and station B can talk to station C, then station A should be able to talk to station C directly. Transitivity is true on LANs, but not on Frame Relay networks unless A is directly connected to C. Additionally, certain protocols such as AppleTalk and transparent bridging cannot be supported on partially meshed networks because they require "split horizon," in which a packet received on an interface cannot be sent from the same interface even if received and transmitted on different VCs. Configuring Frame Relay subinterfaces ensure that a single physical interface is treated as multiple virtual interfaces, which allows you to overcome split horizon rules. Packets received on one virtual interface can be forwarded to another virtual interface, even if they are configured on the same physical interface. Subinterfaces address the limitations of Frame Relay networks by providing a way to subdivide a partially meshed Frame Relay network into a number of smaller, fully meshed (or point-to-point) subnetworks. Each subnetwork is assigned its own network number and appears to the protocols as if it is reachable through a separate interface. (Note that point-to-point subinterfaces can be unnumbered for use with IP, reducing the addressing burden that might otherwise result.)

---

**QUESTION 263**

Which of the following components make up the Frame Relay frame (Choose all that

apply)?

- A. The parity portion
- B. Header and address area
- C. Frame check sequence
- D. Security bit
- E. User-data portion

Answer: B, C, E

Explanation:

Flags indicate the beginning and end of the frame. Three primary components make up the Frame Relay frame: the header and address area, the user-data portion, and the frame check sequence (FCS). The address area, which is 2 bytes in length, is comprised of 10 bits representing the actual circuit identifier and 6 bits of fields related to congestion management. This identifier commonly is referred to as the data-link connection identifier (DLCI).

---

**QUESTION** 264

Which of the following LMI extensions are considered to be optional? (Choose all that apply)

- A. Multicasting
- B. Simple flow control
- C. Virtual circuit status messages
- D. Global addressing

Answer: A, B, D

Explanation:

In addition to the basic Frame Relay protocol functions for transferring data, the consortium Frame Relay specification includes LMI extensions that make supporting large, complex internetworks easier. Some LMI extensions are referred to as "common" and are expected to be implemented by everyone who adopts the specification. Other LMI functions are referred to as "optional." A summary of the LMI extensions follows:

Virtual circuit status messages (common)-Provide communication and synchronization between the network and the user device, periodically reporting the existence of new PVCs and the deletion of already existing PVCs, and generally provide information about PVC integrity. Virtual circuit status messages prevent the sending of data into black holes-that is, over PVCs that no longer exist.

Multicasting (optional)-Allows a sender to transmit a single frame but have it delivered by the network to multiple recipients. Thus, multicasting supports the efficient conveyance of routing protocol messages and address resolution procedures that typically must be sent to many destinations simultaneously.

Global addressing (optional)-Gives connection identifiers global rather than local significance, allowing them to be used to identify a specific interface to the Frame Relay

network. Global addressing makes the Frame Relay network resemble a local-area network (LAN) in terms of addressing; Address Resolution Protocols, therefore, perform over Frame Relay exactly as they do over a LAN.

Simple flow control (optional)-Provides for an XON/XOFF flow control mechanism that applies to the entire Frame Relay interface. It is intended for devices whose higher layers cannot use the congestion notification bits and that need some level of flow control.

---

**QUESTION 265**

With Frame Relay, a communication session across an SVC consists of how many operational states?

- A. Four
- B. Five
- C. One
- D. Three
- E. Two

Answer: A

Explanation:

Switched virtual circuits (SVCs) are temporary connections used in situations requiring only sporadic data transfer between DTE devices across the Frame Relay network. A

communication session across an SVC consists of the following four operational states:

Call setup-The virtual circuit between two Frame Relay DTE devices is established.

Data transfer-Data is transmitted between the DTE devices over the virtual circuit.

Idle-The connection between DTE devices is still active, but no data is transferred. If an SVC remains in an idle state for a defined period of time, the call can be terminated.

Call termination-The virtual circuit between DTE devices is terminated.

---

**QUESTION 266**

Is the following statement true or false?

The primary benefit of the use of the FECN and BECN fields in Frame Relay is for the purpose of congestion indications.

- A. False
- B. True
- C. True only for IOS V11 or above
- D. True only for IOS V12 or above

Answer: B

Explanation:

Forward-explicit congestion notification (FECN) is a single-bit field that can be set to a value of 1 by a switch to indicate to an end DTE device, such as a router, that congestion was experienced in the direction of the frame transmission from source to destination. The primary benefit of the use of the FECN and BECN fields is the capability of higher-layer

protocols to react intelligently to these congestion indicators. Today, DECnet and OSI are the only higher-layer protocols that implement these capabilities.

Backward-explicit congestion notification (BECN) is a single-bit field that, when set to a value of 1 by a switch, indicates that congestion was experienced in the network in the direction opposite of the frame transmission from source to destination.

---

**QUESTION 267**

In Frame Relay, what bit is used to indicate that a frame has lower importance than other frames?

- A. DA
- B. DT
- C. DE
- D. DL
- E. C bit

Answer: C

Explanation:

The Discard Eligibility (DE) bit is used to indicate that a frame has lower importance than other frames. The DE bit is part of the Address field in the Frame Relay frame header. DTE devices can set the value of the DE bit of a frame to 1 to indicate that the frame has lower importance than other frames. When the network becomes congested, DCE devices will discard frames with the DE bit set before discarding those that do not. This reduces the likelihood of critical data being dropped by Frame Relay DCE devices during periods of congestion.

---

**QUESTION 268**

In the Certkiller frame relay network, the LMI signaling multicast mechanism is intended for which of the following?

- A. Providing outgoing status on known DLCIs
- B. Providing network server with its remote DLCI
- C. Providing network server with its local DLCI
- D. Verifying data flow
- E. None of the above

Answer: C

Explanation:

The Cisco implementation of frame relay provides support for a keepalive mechanism, a multicast group, and a status message, as follows:

- o The keepalive mechanism provides an exchange of information between the network server and the switch to verify that data is flowing.
- o The multicast mechanism provides the network server with its local data link connection identifier (DLCI) and the multicast DLCI. This feature is specific

to the Cisco implementation of the Frame Relay joint specification.

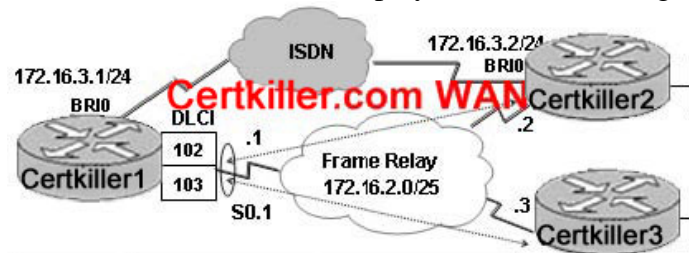
o The status mechanism provides an ongoing status report on the DLCIs known by the switch.

Reference:

[http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products\\_configuration\\_guide\\_chapter09186a00800873e0.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products_configuration_guide_chapter09186a00800873e0.html)

## QUESTION 269

The Certkiller network is displayed in the following diagram.



```

Certkiller1# show running-config
!
interface Serial0
encapsulation frame-relay
!
interface Serial0.1
backup interface bri0
ip address 172.16.2.1 255.255.255.128
frame-relay map ip 172.16.2.2 102 broadcast
frame-relay map ip 172.16.2.3 103 broadcast
!
interface BRI0
ip address 172.16.3.1 255.255.255.0
encapsulation ppp
dialer map ip 172.16.3.2 name R2 broadcast 5552000
dialer-group 1
!
router eigrp 4
network 172.16.0.0
!
access-list 100 deny eigrp any any
access-list 100 permit ip any any
!
dialer-list 1 protocol ip list 100

```

Certkiller 1 is connected with a multipoint subinterface over the Frame Relay to the spoke routers Certkiller 2 and Certkiller 3. The ISDN interface is configured to provide a back-up link should the primary connection to Certkiller 2 fail. However, when the PVC to Certkiller 2 drops, the BRI interface remains in "standby" mode and does not bring up the back-up link. Based on the information and the configuration file shown above, what could the problem be?

- A. The EIGRP updates are configured as noninteresting traffic.
- B. The backup command is configured under the S0.1 multipoint interface of Certkiller 1.
- C. The TeastKing1 S0 interface remains up because of the active PVC between Certkiller 1 and Certkiller 3.
- D. The TeastKing1 S0.1 interface remains up because of the active PVC between Certkiller 1 and Certkiller 3.

Answer: D

Explanation:

Using the backup interface in this configuration tells the router to initiate an ISDN call on interface BRI0 when the line protocol on sub-interface serial 0.1 goes down. However, since there are two separate frame relay maps configured the sub-interface will remain up as long as at least one of the PVC's is operational.

Note: Placing the "backup interface" command under interface serial 0 would not help in this situation, since all sub-interfaces must be down in order for the physical interface to go down. The best way to accomplish the goal of this network is to create a separate subinterface for the connection to Certkiller 2 and place the "backup interface" command there.

---

**QUESTION 270**

The Certkiller frame relay network is displayed in the following diagram:



Which subinterface configuration options will allow for full IP connectivity between Certkiller A and the spoke routers?

- A. Certkiller A(config)# interface S0.1 point-to-point  
Certkiller A(config)# interface S0.2 point-to-point  
Certkiller A(config)# interface S0.3 point-to-point
- B. Certkiller A(config)# interface S0.1 multipoint  
Certkiller A(config)# interface S0.2 multipoint  
Certkiller A(config)# interface S0.3 multipoint
- C. Certkiller A(config)# interface S0.1 multipoint  
Certkiller A(config)# interface S0.2 point-to-point  
Certkiller A(config)# interface S0.3 point-to-point
- D. Certkiller A(config)# interface S0.1 multipoint  
Certkiller A(config)# interface S0.2 point-to-point  
Certkiller A(config)# interface S0.3 point-to-point
- E. Certkiller A(config)# interface S0.1 multipoint  
Certkiller A(config)# interface S0.2 multipoint  
Certkiller A(config)# interface S0.3 point-to-point



Answer: C

Explanation:

Since routers Certkiller B and Certkiller C both belong to the same IP subnet on the WAN, a single multipoint subinterface would be sufficient to provide for connectivity to them from the hub router Certkiller

A. After this is done, only a single point to point subinterface needs to be created to router Certkiller D. This subinterface needs to be created because Certkiller D resides in a separate IP subnet than the other 2 routers.

With choice C, interface s0.1 will be configured with an IP address in the 30.30.30.0/24 range, and interface s0.2 will be configured with an IP address in the 20.20.20.0/24 range.

---

**QUESTION 271**

Which statement best describes a digital certificate, which is being implemented in the Certkiller network as a VPN technology?

- A. A digital identification mechanism which establishes credentials issued by a certification authority.
- B. A network service that issues and manages security credentials and public keys for email encryption.
- C. An digital signature that can authenticate the identity of the sender of a message or the signer of a document.
- D. An algorithm provided by a designated authority used as an encryption key.

Answer: A

Explanation:

While IPSec provides the core technology for VPNs, integrating digital certificates ensures scalability and the highest possible security.

Authentication in IPSec can be provided through the use of digital certificates or shared secrets. These two approaches differ in security, in conceptual complexity, in the level of control they allow over communications, and in the amount of additional equipment required to use them.

Authentication that depends on shared secrets, although easy to implement, is practical only in small VPNs and where the trust within a domain is uniform. For two nodes to communicate securely through the public network using shared secrets, they must be configured with identical shared secrets. The distribution of the shared secret in the first place can only be carried out in a separate out-of-band secure channel. The management of the shared secrets becomes more difficult as the number of nodes involved in the communication becomes large ([N.sup.2] problem), because new secrets are typically distributed manually on a pairwise unique basis. Therefore, it is difficult to scale a shared secret-based VPN.

Digital certificates, on the other hand, use a trusted third-party authentication system, which scales linearly when the number of involved parties becomes Large. A CA (certification authority) is an entity trusted by all the certificate users or that has been granted power to issue digital certificates and vouch for the binding between data items contained in a

certificate. The CA manages the life cycle of certificates and, depending on the type of certificate and the certification practice statement that applies, may be responsible for the life cycle of key pairs associated with the certificates.

In a digital world, a digital certificate is like a passport, only more secure: The digital signature of the issuing CA guarantees the certificate's authenticity. It is impossible to forge a digital signature unless one knows the signing private key.

Reference: [http://www.findarticles.com/p/articles/mi\\_m0TLC/is\\_8\\_34/ai\\_65142156](http://www.findarticles.com/p/articles/mi_m0TLC/is_8_34/ai_65142156)

---

**QUESTION 272**

In some applications TACACS+ and RADIUS are NOT suitable for authentication, so a technician will implement Kerberos instead. What kind of circumstances would dictate the use of Kerberos?

- A. The usage of various router functions needs to be accounted for by user name.
- B. Multiple level of authorization need to be applied to various router commands.
- C. DES encrypted authentication is required.
- D. Authentication, authorization and accounting need to use a single database.
- E. The utilization of authentication functions needs to be authorized by user names and passwords.

Answer: C

Explanation:

The Kerberos protocol uses strong cryptography so that a client can prove its identity to a server (and vice versa) across an insecure network connection. After a client and server has used Kerberos to prove their identity, they can also encrypt all of their communications to assure privacy and data integrity as they go about their business.

Kerberos is a network authentication protocol developed by MIT. Kerberos can provide authentication only. It doesn't have the capability to perform authorization. Some sites with existing Kerberos servers use Kerberos for authentication, while using TACACS+ or RADIUS for authorization.

Encryption in Kerberos is based on DES, the Data Encryption Standard. The encryption library implements those routines. Several methods of encryption are provided, with tradeoffs between speed and security. An extension to the DES Cypher Block Chaining (CBC) mode, called the Propagating CBC mode, is also provided. In CBC, an error is propagated only through the current block of the cipher, whereas in PCBC, the error is propagated throughout the message. This renders the entire message useless if an error occurs, rather than just a portion of it. The encryption library is an independent module, and may be replaced with other DES implementations or a different encryption library.

References:

<http://web.mit.edu/kerberos/www/>

[http://www.cisco.com/en/US/tech/CK5\\_83/CK3\\_85/technologies\\_white\\_paper09186a00800941b2.shtml](http://www.cisco.com/en/US/tech/CK5_83/CK3_85/technologies_white_paper09186a00800941b2.shtml)

---

**QUESTION 273**

You are a network design consultant and you've just been contracted by a human

resource company to explain to them the benefits of a remote access server; more specifically, what kind of workers could benefit the most from them. How would you respond?

- A. Mobile sales force requiring dial-in access.
- B. Corporate staff requiring access to web-based applications.
- C. Mobile sales force requiring dedicated connection.
- D. Corporate staff requiring access to applications on corporate systems.
- E. None of the above

Answer: A

Explanation:

A router acts as an access server, which is a concentration point for dial-in and dial-out calls. Mobile users, for example, can call into an access server at a central site to access their email messages. The biggest users of remote access servers are mobile employees that need occasional, temporary connections into the network.

Reference:

Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 2-8

---

**QUESTION 274**

You are an administrator of a rapidly expanding company and your network is based on a Cisco 2511 access server. All 16 of its asynchronous interfaces have been configured to permit simultaneous remote access, leaving only one AUX port available for remote administration via modem. What line number must you use to configure this remote administration aux port for the modem?

- A. Line 0
- B. Line 17
- C. Line 1
- D. Line 18
- E. Line 7

Answer: B

Explanation:

The following lines are used in Cisco IOS:

0 is specified for the console line

TTY lines 1-16 are used for the asynchronous lines.

Line 17 is reserved for the aux port.

---

**QUESTION 275**

Identify two characteristics of the RADIUS protocol when associated with AAA.  
(Choose two)

- A. Uses TCP

- B. Fully encrypts the body of the packet.
- C. Based upon open standards.
- D. Allows router commands to be grouped on a per-user or per-group basis.
- E. Combines the functions of authorization and authentication.

Answer: C, E

Explanation:

Cisco Systems uses a strategy known as authentication, authorization, and accounting (AAA) for verifying the identity of, granting access to, and tracking the actions of remote users. In today's networks, the Terminal Access Controller Access Control System plus (TACACS+) and Remote Access Dial-In User Service (RADIUS) protocols are commonly used to provide AAA solutions.

The RADIUS protocol was developed by Livingston Enterprises, Inc., as an access server authentication and accounting protocol. Implemented by several vendors of network access servers, RADIUS has gained support among a wide customer base, including Internet service providers (ISPs). The RADIUS authentication protocol is documented separately from the accounting protocol, but the two can be used together for a comprehensive solution.

The RADIUS protocol combines the processes of authentication and authorization. The Access-Accept packets sent by the RADIUS server to the client contain all the authorization information, making separation of the authentication and authorization functions difficult.

The use of RADIUS is most appropriate when simple, single-step authentication and authorization is required, as with most service provider networks.

In June 1996, draft 5 of the RADIUS protocol specification was submitted to the Internet Engineering Task Force (IETF). The RADIUS specification (RFC 2058) and RADIUS accounting standard (RFC 2059) are now proposed standard protocols. The text of the IETF proposed standards can be found at the following URLs:

<ftp://ds.internic.net/rfc/rfc2058.txt>

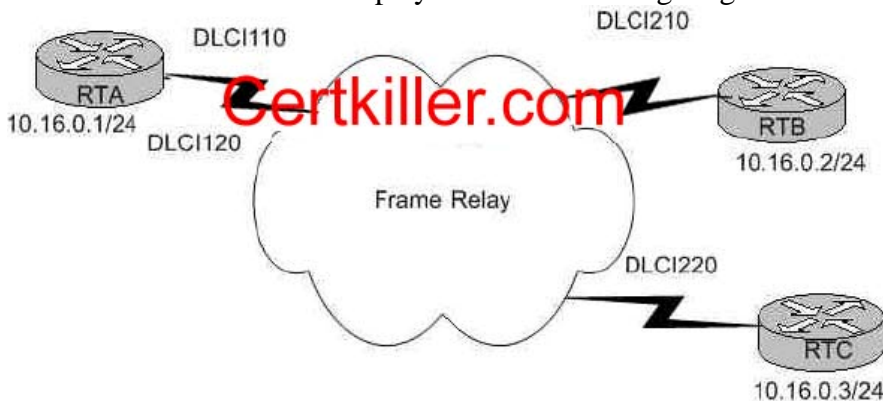
Reference:

[http://www.cisco.com/en/US/tech/CK59/technologies\\_white\\_paper09186a00800a3c92.shtml](http://www.cisco.com/en/US/tech/CK59/technologies_white_paper09186a00800a3c92.shtml)

---

### QUESTION 276

The Certkiller network is displayed in the following diagram:



RTA is the hub router, with RTB and RTC configured as spokes. Currently no spoke router can ping any other spoke router, but all spoke routers can ping the hub. There are no routing protocols configured and Inverse ARP is enabled.

What must the administrator do to correct the problem?

- A. Configure static map commands on the hub router.
- B. Configure static map commands on all spoke routers.
- C. Configure subinterfaces on the hub router.
- D. Configure subinterfaces on all spoke routers.
- E. Enable split horizon on the hub router.
- F. Disable split horizon on all spoke routers.

Answer: B

Explanation:

Frame Relay supports two types of interfaces: point-to-point and multipoint. The one you choose determines whether you need to use the configuration commands that ensure IP address to data-link connection identifier (DLCI) mappings. After configuring the PVC itself, you must tell the router which PVC to use in order to reach a specific destination. Let's look at these options:

- Point-to-point subinterface - With point-to-point subinterfaces, each pair of routers has its own subnet. If you put the PVC on a point-to-point subinterface, the router assumes that there is only one point-to-point PVC configured on the subinterface. Therefore, any IP packets with a destination IP address in the same subnet are forwarded on this VC. This is the simplest way to configure the mapping and is therefore the recommended method. Use the frame-relay interface-dlci command to assign a DLCI to a specified Frame Relay subinterface.

- Multipoint networks - Multipoint networks have three or more routers in the same subnet. If you put the PVC in a point-to-multipoint subinterface or in the main interface (which is multipoint by default), you need to either configure a static mapping or enable inverse Address Resolution Protocol (ARP) for dynamic mapping. In order to ensure that Inverse ARP resolves addresses across a hub and spoke topology, it is best to use single point to point subinterfaces for each PVC at the hub site. Alternatively, use static map entries on the spoke routers. Since the remote spoke routers can already ping the hub site, there is no need to add static entries on the hub router.

---

**QUESTION 277**

Which two encapsulation methods require that an 827 ADSL router be configured with a PPP username and CHAP password? (Choose two)

- A. PPPoE with the 827 configured as a bridge.
- B. PPPoE with the 827 configured as the PPPoE client.
- C. PPPoA
- D. RFC 1483 Bridged with the 827 configured as the PPPoE client.
- E. RFC 1482 Bridged with the 827 configured as a bridge.

Answer: B, C

Explanation:

When using the Point to Point Protocol over Ethernet (PPPoE) or the Point to Point Protocol over ATM (PPPoA), you must configure a PPP username and password to match the settings configured from the Internet Service Provider. This is required for both PPPoE and PPPoA in order to overcome some of the security concerns of these two Internet access methods.

---

**QUESTION 278**

What command should you use to specify RADIUS as the method of user authentication when no other method list has been defined? (Type in answer below)

Answer: aaa authentication ppp default radius

Explanation:

Use the aaa authentication ppp command with the radius method keyword to specify RADIUS as the authentication method for use on interfaces running PPP. Before you can use RADIUS as the authentication method, you need to enable communication with the RADIUS security server.

---

**QUESTION 279**

TO better accommodate for the growing number of remote access users, Certkiller is implementing CiscoSecure. Which of the following are the three major components of Cisco Secure (Choose all that apply)?

- A. L2TP
- B. RDBMS
- C. Packet filter firewall
- D. Netscape Fast Track Server
- E. AAA Server
- F. Track Server

Answer: B, D, E

Explanation:

RDBMS synchronization import definitions are a listing of the action codes allowable in an accountActions table. The RDBMS Synchronization feature of CiscoSecure AccessControlServer (ACS) for WindowsServer uses a table named "accountActions" as input for automated or manual updates of the CiscoSecure user database.

CiscoSecure supports both Cisco network access servers (such as the Cisco 2509, 2511, 3620, 3640, and AS5200) and the PIX firewall. It is a basic access control server (ACS) for Windows NT Server Version 4.0. CiscoSecure uses the Terminal Access Controller Access Control System (TACACS)+ protocol to provide Authentication, Authorization, and Accounting (AAA) to ensure a secure environment. This enables you to control access to your network from a central location.

---

**QUESTION 280**

What command should you use so that your access server will attempt to authenticate all incoming calls that start a PPP session with CHAP, and will use PAP only if the

remote device does not support CHAP? (Type in answer below)

Answer: ppp authentication chap pap

Explanation:

If the remote device does not support chap then use pap. So chap must be first mentioned before pap in the command. With this configuration, PAP will be used only should the remote device not support CHAP.

Note:

If you configure ppp authentication chap on an interface, all incoming calls on that interface that initiate a PPP connection will have to be authenticated using CHAP; likewise, if you configure ppp authentication pap, all incoming calls that start a PPP connection will have to be authenticated via PAP. If you configure ppp authentication chap pap, the access server will attempt to authenticate all incoming calls that start a PPP session with CHAP. If the remote device does not support CHAP, the access server will try to authenticate the call using PAP. If the remote device doesn't support either CHAP or PAP, authentication will fail and the call will be dropped. If you configure ppp authentication pap chap, the access server will attempt to authenticate all incoming calls that start a PPP session with PAP. If the remote device does not support PAP, the access server will try to authenticate the call using CHAP. If the remote device doesn't support either protocols, authentication will fail and the call will be dropped. If you configure the ppp authentication command with the callin keyword, the access server will only authenticate the remote device if the remote device initiated the call.

---

**QUESTION 281**

What command should you use to enable AAA authentication regardless of the supported login authentication methods to use? (Type in answer below)

Answer: aaa authentication login

Explanation:

The AAA security services facilitate a variety of login authentication methods. Use the "aaa authentication login" command to enable AAA authentication no matter which of the supported login authentication methods you decide to use. With the "aaa authentication login" command, you create one or more lists of authentication methods that are tried at login. These lists are applied using the login authentication line configuration command.

---

**QUESTION 282**

What AAA command should you use to specify the local username database as the authentication method for use on lines running PPP when no other method list has been defined? (Type in answer below)

Answer: aaa authentication ppp default local

Explanation:

Use the "aaa authentication ppp" command with the method keyword local to specify that the Cisco router or access server will use the local username database for authentication. For

example, to specify the local username database as the method of authentication for use on lines running PPP when no other method list has been defined, enter:

```
aaa authentication ppp default local
```

---

**QUESTION 283**

On router CK1 , you need to specify the location of a new CiscoSecure server that was just installed. Which of the following indicates the address of the CiscoSecure server in your network?

- A. en tacacs-server host
- B. server host tacacs
- C. tacacs-server en
- D. tacacs-server host
- E. None of the above

Answer: D

Explanation:

The tacacs-server host command allows you to specify the names of the IP host or hosts maintaining a TACACS server. Because the TACACS software searches for the hosts in the order specified, this feature can be useful for setting up a list of preferred servers.

To specify a TACACS+ host, use the tacacs-server host command in global configuration mode. Use the no form of this command to delete the specified name or address.

tacacs-server host hostname [single-connection] [port integer] [timeout integer] [key string]

Syntax Description

<i>hostname</i>	Name or IP address of the host.
single-connection	(Optional) Specify that the router maintain a single open connection for confirmation from a AAA/TACACS+ server (CiscoSecure Release 1.0.1 or later). This command contains no autodetect and fails if the specified host is not running a CiscoSecure daemon.
port	(Optional) Specify a server port number. This option overrides the default, which is port 49.
<i>integer</i>	(Optional) Port number of the server. Valid port numbers range from 1 to 65535.
timeout	(Optional) Specify a timeout value. This overrides the global timeout value set with the tacacs-server timeout command for this server only.



<i>integer</i>	(Optional) Integer value, in seconds, of the timeout interval.
<i>key</i>	(Optional) Specify an authentication and encryption key. This must match the key used by the TACACS+ daemon. Specifying this key overrides the key set by the global command tacacs-server key for this server only.
<i>string</i>	(Optional) Character string specifying authentication and encryption key.

---

**QUESTION 284**

What keyword of the aaa authentication login command do you use to specify the line password as the login authentication method? (Type in answer below)

Answer: line

Explanation:

According to the technical documentation at CCO: Use the aaa authentication login command with the line method keyword to specify the line password as the login authentication method. For example, to specify the line password as the method of user authentication at login when no other method list has been defined, enter the following:  
aaa authentication login default line

---

**QUESTION 285**

You need to have what type of connection to connect an AAA server to the Certkiller network?

- A. Serial interface
- B. Synchronous call
- C. T1
- D. Ethernet
- E. Asynchronous call
- F. ISDN PRI
- G. T3

Answer: D

Explanation:

Like other network servers, the only connections that can be used to connect to the network is via the Ethernet Network Interface Card (NIC) or ethernet interface on the server.

---

**QUESTION 286**

A new CiscoSecure ACS is being installed in the Certkiller network. Which of the

following are components of the CiscoSecure ACS server? (Choose all that apply)

- A. AAA server
- B. Netscape Fastrack server
- C. RDBMS
- D. RADIUS Interface

Answer: A, B, C

Explanation:

The CiscoSecure ACS consists of several interrelated software modules that carry out different communication, profile data retrieval, profile data storage, administrative, and performance-enhancement functions. Understanding the interaction of these modules is useful for troubleshooting or fine tuning CiscoSecure ACS performance.

The CiscoSecure ACS components include:

- The AAA Server
- The DBServer
- The relational database management system (RDBMS)
- The two web server modules: Netscape FastTrack and Acme FastAdmin
- The optional Distributed Sessions Manager (DSM)
- The command-line interface (CLI) module

Reference:

[http://www.cisco.com/en/US/products/sw/secursw/ps4911/products\\_user\\_guide\\_chapter09186a00800eca43.html](http://www.cisco.com/en/US/products/sw/secursw/ps4911/products_user_guide_chapter09186a00800eca43.html)

---

**QUESTION 287**

Which of the following networks would be the most suitable candidates for traffic prioritization? (Choose all that apply)

- A. A Frame Relay connection experiences utilization from 10 to 40%.
- B. A bursty WAN link that experiences only temporary congestion.
- C. A DDR connection is always connected and runs at 70 to 100% utilization most of the day.
- D. Low-speed data links that are not experiencing congestion problems.
- E. A connection that has multiple protocols sharing a single data path.

Answer: B, C, E

Explanation:

Traffic prioritization is used so that critical traffic gets through, even at the expense of lesser traffic.

B: The temporary congestion for high priority traffic can be avoided with traffic prioritization.

C: Some protocols can be assigned higher priorities.

E: On high utilization links it could be useful to prioritize important traffic.

Incorrect Answers:

A: If there is no congestion there is no need to use traffic prioritization.  
D: With low utilization and no congestion there is no need to use traffic prioritization.

Reference:

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

---

**QUESTION 288**

Which Quality of Service method should an administrator configure if they want to give business essential traffic like VOIP and email strict priority over less essential traffic like internet surfing and file downloads?

- A. Weighted round robin
- B. Weighted fair queuing
- C. Random early detect
- D. Priority queuing
- E. All of the above would accomplish this

Answer: D

Explanation:

The Cisco IOS contains numerous traffic prioritization and congestion avoidance mechanisms and options. Some of them are described in the following table:

**QUEUING COMPARISON**

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

Reference:

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

---

**QUESTION 289**

On router Certkiller 1 the following configuration command was entered:  
queue-list 1 protocol ip 2 tcp 20

What is the result of this command?

- A. It assigns IP data traffic to priority queue 2.
- B. It assigns FTP data traffic to custom queue 2.
- C. It assigns IP traffic that matches IP access list 20 to priority queue 2.
- D. It assigns FTP traffic that matches IP access list 2 to custom queue 1.

Answer: B

Explanation:

According to the above command; FTP data traffic (TCP port #20) is assigned to custom queue 2.

Queue's can be assigned by: size, protocol, interface, or by default values.

```
Certkiller (config)#queue-list list number protocol protocolname  
queue-number queue-keyword keyword-value
```

This example assigns Telnet packets to queue number 2:

```
queue-list 4 protocol ip 2 tcp 23
```

Note: FTP uses TCP ports 20 and 21.

Reference: CCNP Remote Access Exam Certification Guide, page 308-311, Brian Morgan & Craig Dennis, Cisco Press 2001, ISBN 1-58720-003-1

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/qos\\_c/qcpart2/qccq.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/qos_c/qcpart2/qccq.htm)

---

### QUESTION 290

On your network, you wish to implement a Quality of Service method that treats all traffic as fairly as possible. You want to ensure that large data sessions do not unfairly consume all of the bandwidth while small data sessions that could be handled quickly are forced to wait in line. Which queuing method would you use to dynamically provide you with fair bandwidth allocation for every traffic type in the network?

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

Answer: B

Explanation:

Weighted Fair Queuing (WFQ)-This is the default method of queuing on links that are T1/E1 speeds or less. It offers fair access to the available bandwidth for each traffic flow.

WFQ is one of Cisco's premier queuing techniques. It is a flow-based queuing algorithm that does two things simultaneously: It schedules interactive traffic to the front of the queue to reduce response time, and it fairly shares the remaining bandwidth between high bandwidth flows.

### QUEUING COMPARISON

<b>Weighted Fair</b>	<b>Priority Queuing</b>	<b>Custom Queuing</b>
----------------------	-------------------------	-----------------------

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

Reference:

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

---

**QUESTION 291**

Link compression supports which of the following compression algorithms? (Choose all that apply.)

- A. Van Jacobson
- B. Stac
- C. MNP5
- D. Predictor
- E. Huffman

Answer: B, D

We refer to the data compression schemes used in internetworking devices as lossless compression algorithms. These schemes reproduce the original bit streams exactly, with no degradation or loss. This feature is required by routers and other devices to transport data across the network. The two most commonly used compression algorithms on internetworking devices are the Stacker compression and the Predictor data compression algorithms.

**Stacker Compression**

Stacker compression is based on the Lempel-Ziv compression algorithm. The Stacker algorithm uses an encoded dictionary that replaces a continuous stream of characters with codes. This stores the symbols represented by the codes in memory in a dictionary-style list. Because the relationship between a code and the original symbol varies as the data varies, this approach is more responsive to the variations in the data. This flexibility is particularly important for LAN data, because many different applications can be transmitting over the WAN at any one time. In addition, as the data varies, the dictionary changes to accommodate and adapt to the varying needs of the traffic. Stacker compression is more CPU-intensive and

less memory-intensive.

### Predictor Compression

The Predictor compression algorithm tries to predict the next sequence of characters in a data stream by using an index to look up a sequence in the compression dictionary. It then examines the next sequence in the data stream to see if it matches. If it does, that sequence replaces the looked-up sequence in the dictionary. If there is no match, the algorithm locates the next character sequence in the index and the process begins again. The index updates itself by hashing a few of the most recent character sequences from the input stream. No time is spent trying to compress already compressed data. The compression ratio obtained using predictor is not as good as other compression algorithms, but it remains one of the fastest algorithms available. Predictor is more memory-intensive and less CPU-intensive.

Incorrect Answers:

A: Van Jacobson is another name for tcp header-compression

C: MNP5 relates to modem compression.

E: This algorithm is not supported by Cisco at all.

---

### QUESTION 292

What FRTS (Frame Relay Traffic Shaping) term specifies the maximum number of uncommitted bits that the Frame Relay switch attempts to transfer beyond the CIR?

- A. Local access rate
- B. Oversubscription rate
- C. Committed burst
- D. Excess burst
- E. Excess information rate

Answer: D

Explanation:

FRTS provides parameters that are useful for managing network traffic congestion on frame relay networks. FRTS eliminates bottlenecks in Frame Relay networks with high-speed connections to the central site and low-speed connections to the branch sites. You can configure rate enforcement values to limit the rate at which data is sent from the virtual circuit (VC) at the central site.

The following definitions are important to FRTS:

Committed Information Rate (CIR)	Rate (bits per second) the frame relay provider guarantees for data transfer. CIR values are set by the Frame Relay service provider and configured by the user on the router. Note: The port / interface access rate can be higher than CIR. The rate is averaged over a Tc period of time.
----------------------------------	--

Committed Burst (Bc)	Maximum number of bits the frame relay network commits to transfer over a Committed Rate Measurement Interval (Tc). $Tc = Bc / CIR$ .
Excess Burst (Be)	Maximum number of uncommitted bits the frame relay switch attempts to transfer beyond the CIR over the Committed Rate Measurement Interval (Tc).
Committed Rate Measurement Interval (Tc)	Time interval over which Bc or (Bc+ Be) bits are transmitted. Tc is calculated as $Tc = Bc / CIR$ . The Tc value is not directly configured on Cisco routers. It is calculated after the Bc and
Backwards Explicit Congestion Notification (BECN)	CIR values are configured. Tc cannot exceed 125 ms. A bit in the Frame Relay frame header that indicates congestion in the network. When a Frame Relay switch recognizes congestion, it sets the BECN bit on frames destined for the source router, instructing the router to reduce the transmission rate.

Reference:

[http://www.cisco.com/en/US/tech/ CK6 52/ CK6 98/technologies\\_tech\\_note09186a00800d6788.shtml](http://www.cisco.com/en/US/tech/ CK6 52/ CK6 98/technologies_tech_note09186a00800d6788.shtml)

---

**QUESTION 293**

The Certkiller network is using VOIP to make intra-office calls. What is the recommended queuing strategy for these voice packets?

- A. CBWFQ
- B. FIFO
- C. WFQ
- D. LLQ
- E. WRED

Answer: D

Explanation:

The Low Latency Queuing feature brings strict priority queuing to Class-Based Weighted

Fair Queuing (CBWFQ). Strict priority queuing allows delay-sensitive data such as voice to be dequeued and sent first (before packets in other queues are dequeued), giving delay-sensitive data preferential treatment over other traffic.

Without Low Latency Queueing, CBWFQ provides weighted fair queuing based on defined classes with no strict priority queue available for real-time traffic. CBWFQ allows you to define traffic classes and then assign characteristics to that class. For example, you can designate the minimum bandwidth delivered to the class during congestion.

For CBWFQ, the weight for a packet belonging to a specific class is derived from the bandwidth you assigned to the class when you configured it. Therefore, the bandwidth assigned to the packets of a class determines the order in which packets are sent. All packets are serviced fairly based on weight; no class of packets may be granted strict priority. This scheme poses problems for voice traffic that is largely intolerant of delay, especially variation in delay. For voice traffic, variations in delay introduce irregularities of transmission manifesting as jitter in the heard conversation.

The Low Latency Queueing feature provides strict priority queuing for CBWFQ, reducing jitter in voice conversations. Because of this, it is the recommended queuing strategy when using VOIP.

---

**QUESTION 294**

If CBWFQ is being used, which three commands can be configured within each traffic class? (Choose three)

- A. bandwidth
- B. service-policy
- C. queue-limit
- D. priority
- E. random-detect

Answer: A, C, D

**Explanation:**

CBWFQ extends the standard WFQ functionality to provide support for user-defined traffic classes. For CBWFQ, you define traffic classes based on match criteria including protocols, access control lists (ACLs), and input interfaces. Packets satisfying the match criteria for a class constitute the traffic for that class. A FIFO queue is reserved for each class, and traffic belonging to a class is directed to the queue for that class.

Once a class has been defined according to its match criteria, you can assign it characteristics. To characterize a class, you assign it bandwidth, weight, and maximum packet limit. The bandwidth assigned to a class is the guaranteed bandwidth delivered to the class during congestion.

To configure CBWFQ, perform the tasks in the following sections. The first three sections are required; the remaining sections are optional.

- Defining Class Maps (Required)
- Configuring Class Policy in the Policy Map (Required)
- Attaching the Service Policy and Enabling CBWFQ (Required)
- Modifying the Bandwidth for an Existing Policy Map Class (Optional)



- Modifying the Queue Limit for an Existing Policy Map Class (Optional)
- Configuring the Bandwidth Limiting Factor
- Deleting Classes (Optional)
- Deleting Policy Maps (Optional)
- Verifying Configuration of Policy Maps and Their Classes (Optional)

To configure a policy map and create class policies that make up the service policy, use the first command in global configuration mode to specify the policy map name, then use the following commands in policy-map class configuration mode to configure policy for a standard class.

The following example first defines a CBWFQ configuration and then reserves a strict priority queue:

! The following commands define a class map:

```
router(config)# class-map class1
router(config-cmap)# match access-group 101
router(config-cmap)# exit
```

! The following commands create and attach a policy map:

```
router(config)# policy-map policy1
router(config-pmap)# class class1
router(config-pmap-c)# bandwidth 3000
router(config-pmap-c)# queue-limit 30
router(config-pmap-c)# random-detect
router(config-pmap-c)# random-detect precedence 0 32 256 100
router(config-pmap-c)# exit
router(config)# interface Serial1
router(config-if)# service-policy output policy1
```

---

### **QUESTION** 295

Router CK1 had the following configuration command added to interface Serial 0

```
Router(config-if)# ip tcp header-compression passive
```

Which two statements are true about the command entered in the display? (Choose two)

- A. The router will compress all traffic.
- B. The router will only compress outgoing TCP packets if incoming TCP packets on the same interface are compressed.
- C. The router will accept incoming compressed TCP packets but will not compress any outgoing TCP packets.
- D. The Layer 2 header will be compressed and therefore cannot be used for WAN switching networks such as Frame Relay.
- E. The Layer 2 header will be left intact and therefore can be used for WAN switching networks such as Frame Relay.
- F. For crossing point-to-point connections, the Layer 2 header will be encapsulated by another link layer such as LAPB.

Answer: B, D

Explanation:

ip tcp header-compression

To enable TCP header compression, use the ip tcp header-compression command in interface configuration mode.

ip tcp header-compression [passive]

Syntax Description

<b>passive</b>	(Optional) Compresses outgoing TCP packets only if incoming TCP packets on the same interface are compressed. If you do not specify the <b>passive</b> keyword, the Cisco IOS software compresses all traffic.
----------------	--

You can compress the headers of your TCP/IP packets to reduce their size and thereby increase performance. Header compression is particularly useful on networks with a large percentage of small packets, such as those supporting many Telnet connections. This feature only compresses the TCP header, so it has no effect on UDP packets or other protocol headers. The TCP header compression technique, described fully in RFC 1144, is supported on serial lines using HDLC or PPP encapsulation. You must enable compression on both ends of a serial connection.

Note: This compression command is only supported on PPP or HDLC links.

Reference:

[http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products\\_configuration\\_guide\\_chapter09186a00800872fd.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_configuration_guide_chapter09186a00800872fd.html)

---

### QUESTION 296

Router CK1 is configured for WRED. With WRED, what will happen to the priority queue if the queue is full and more priority queue traffic is matched?

- A. Priority traffic will be restrained to its allocated queue size, and packets will be dropped.
- B. WRED will start dropping packets from other queues.
- C. Priority queue packets will be placed in the class-default queue.
- D. WRED will start dropping packets from the priority queue.

Answer: B

Explanation:

Weighted RED (WRED) generally drops packets selectively based on IP precedence. Packets with a higher IP precedence are less likely to be dropped than packets with a lower precedence. Thus, higher priority traffic is delivered with a higher probability than lower priority traffic. However, you can also configure WRED to ignore IP precedence when making drop decisions so that non-weighted RED behavior is achieved.

In contrast to RED, WRED can be configured to give preference to certain traffic types. This

way, the lower priority traffic will be more likely to be dropped than traffic in the priority queue.

---

**QUESTION 297**

One of the Certkiller Cisco 1700 series routers was configured for CBWFQ as shown below:

```
Router (config)#policy-map policy1
Router (config-pmap)#class class1
Router (config-pmap-c)#bandwidth 3000
Router (config-pmap-c)#queue-limit 30
Router (config-pmap-c)#exit
Router (config-pmap)#class class2
Router (config-pmap-c)#bandwidth 2000
Router (config-pmap-c)#exit
```

From the CBWFQ configuration referenced in the display, what is the queue-limit for class2?

- A. No limit
- B. 16
- C. 32
- D. 64
- E. 128

Answer: D

Explanation:

To specify or modify the maximum number of packets the queue can hold for a class policy configured in a policy map, use the queue-limit policy-map class configuration command.

queue-limit number-of-packets  
number-ofpackets

<i>number-of-packets</i>	A number in the range from 1 to 64 specifying the maximum number of packets that the queue for this class can accumulate.
--------------------------	---

Defaults

On the Versatile Interface Processor (VIP)-based platforms, the default value is chosen as a function of the bandwidth assigned to the traffic class. The default value is also based on available buffer memory. If sufficient buffer memory is available, the default queue-limit value is equal to the number of 250-byte packets that would lead to a latency of 500 milliseconds (ms) when the packets are delivered at the configured rate. For example, if two 250-byte packets are required to lead to a latency of 500 ms, the default number-of-packets value would be 2.

On all other platforms, the default is 64.

In this example, since the queue was not explicitly configured, the standard default value of 64 would be used.

Reference:

[http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products\\_command\\_reference\\_chapter09186a0080087f22.html#wp1056065](http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a0080087f22.html#wp1056065)

**QUESTION 298**

Router CK1 is configured with Class Based Weighted Fair Queuing (CBWFQ). By default, what is the maximum percentage of bandwidth CBWFQ allocated for all classes of traffic?

- A. 25
- B. 50
- C. 75
- D. 90
- E. 100

Answer: C

Explanation:

You can attach a single policy map to one or more interfaces or one or more VCs to specify the service policy for those interfaces or VCs.

Currently a service policy specifies class-based weighted fair queuing (CBWFQ). The class policies comprising the policy map are then applied to packets that satisfy the class map match criteria for the class.

To successfully attach a policy map to an interface or a VC, the aggregate of the configured minimum bandwidths of the classes comprising the policy map must be less than or equal to 75 percent of the interface bandwidth or the bandwidth allocated to the VC.

The default maximum reservable bandwidth value of 75 percent is designed to leave sufficient bandwidth for overhead traffic, such as routing protocol updates and Layer 2 keepalives. It also covers Layer 2 overhead for packets matching defined traffic classes or the class-default class.

---

**QUESTION 299**

Which three conditions would suggest using weighted random early detection as an alternative to tail drops when configuring class-based weighted fair queuing? (Choose three)

- A. Your network is designed for a more passive rather than active strategy in discarding packets.
- B. You want to enable TCP global synchronization to avoid congestion.
- C. You would like to use IP Precedence or DSCP values to make early dropping decisions.
- D. The bulk of your traffic is TCP traffic.
- E. You would like a chance to decide which packets will be dropped when it becomes necessary.

Answer: C, D, E

Explanation:

WRED provides separate thresholds and weights for different IP precedences, allowing you

to provide different qualities of service for different traffic. Standard traffic may be dropped more frequently than premium traffic during periods of congestion.

WRED has the following restrictions:

- WRED is only useful when the bulk of the traffic is TCP/IP traffic. With TCP, dropped packets indicate congestion, so the packet source will reduce its transmission rate. With other protocols, packet sources may not respond or may resend dropped packets at the same rate. Thus, dropping packets does not decrease congestion.
- WRED treats non-IP traffic as precedence 0, the lowest precedence. Non-IP traffic will be dropped more often than IP traffic.
- WRED is only available on a per-interface basis. You cannot configure WRED on a subinterface.

Incorrect Answers:

A: WRED takes a proactive approach in congestion management by selectively discarding packets before problems arise.

B: WRED avoids the globalization problems that occur when tail drop is used as the congestion avoidance mechanism on the router. Global synchronization occurs as waves of congestion crest only to be followed by troughs during which the transmission link is not fully utilized. Global synchronization of Transmission Control Protocol (TCP) hosts, for example, can occur because packets are dropped all at once. Global synchronization manifests when multiple TCP hosts reduce their transmission rates in response to packet dropping, then increase their transmission rates once again when the congestion is reduced.

Reference:

[http://www.cisco.com/en/US/products/sw/iosswrel/ps1824/products\\_feature\\_guide09186a0080087ae4.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps1824/products_feature_guide09186a0080087ae4.html)

---

### QUESTION 300

When configuring a strict priority queue using LLQ, Cisco recommends that you only send which type of static to this queue?

- A. DNS and DHCP
- B. VoIP
- C. Streaming video
- D. Routing protocol traffic
- E. VoIP call signaling

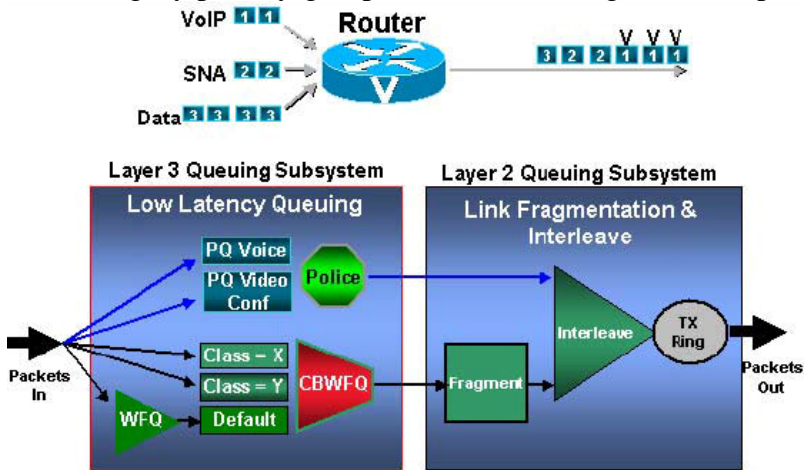
Answer: B

Explanation:

LLQ is a feature that provides a strict PQ to Class-Based Weighted Fair Queuing (CBWFQ). LLQ enables a single strict PQ within CBWFQ at the class level. With LLQ, delay-sensitive data (in the PQ) is dequeued and sent first. In a VoIP with LLQ implementation, voice traffic is placed in the strict PQ.

The PQ is policed to ensure that the fair queues are not starved of bandwidth. When you configure the PQ, you specify in Kbps the maximum amount of bandwidth available to the PQ. When the interface is congested, the PQ is serviced until the load reaches the configured Kbps value in the priority statement. Excess traffic is then dropped to avoid the problem with

Cisco's legacy priority-group feature of starving the lower priority queues.



This method is more complex and flexible than IP RTP Priority. The choice between the methods should be based on the patterns of traffic in your real network and your actual needs.

Reference:

[http://www.cisco.com/en/US/tech/CK652/CK698/technologies\\_tech\\_note09186a0080094660.shtml](http://www.cisco.com/en/US/tech/CK652/CK698/technologies_tech_note09186a0080094660.shtml)