Cisco 350-029

CCIE SP Written Exam, V3.0

Version: 14.0

Topic 1, I&O&T Core IP Technologies

QUESTION NO: 1

Which three modes are the operating of HDLC? (Choose three)

A. asynchronous balanced mode (ABM)
B. normal response mode (NRM)
C. normal peer mode (NPM)
D. asynchronous client mode (ACM)
E. asynchronous response mode (ARM)

Answer: A,B,E

Explanation: Normal response mode allows operation over half-duplex communication links, as long as the primary is aware that it may not transmit when it has given permission to a secondary. Asynchronous response mode is an HDLC addition[1] for use over full-duplex links. While retaining the primary/secondary distinction, it allows the secondary to transmit at any time. Asynchronous balanced mode added the concept of a combined terminal which can act as both a primary and a secondary. There are some subtleties about this mode of operation; while many features of the protocol do not care whether they are in a command or response frame, some do, and the address field of a received frame must be examined to determine whether it contains a command (the address received is ours) or a response (the address received is that of the other terminal).

QUESTION NO: 2

IP over DWDM management models (Choose two.)

A. Segmented Management
B. Integrated Management
C. Virtual Transponder
D. Traffic Management

Answer: A,B

Explanation: 1.2. IP over DWDM IPoDWDM supports 2 network management models:

1. Segmented Management:

- Retain existing operational model for certain SPs.

- Respect boundaries between IP/Transport groups.

2. Integrated Management:

- End to end provisioning.

- Better troubleshooting.

- 1 Management system, 1 database.

- Unified look & feel.

- Lower OPEX.

Lay the Foundation for Network Convergence

IP over dense wavelength-division multiplexing (IPoDWDM) is a technology pioneered by Cisco that delivers superior service flexibility, scalability, and resiliency. It allows carriers to capitalize on increasingly bandwidth intensive and complex applications for next-generation Internet innovations and collaborative business services.

Enhance Your IP Transport Through Innovation

IPoDWDM collapses network layers by tightly integrating DWDM interfaces with the routing platform. This increases efficiency, simplifies management, and accelerates service delivery. Combined with industry-leading omnidirectional and colorless reconfigurable optical add/drop multiplexer (ROADM) technology, IPoDWDM educes service truck rolls, power consumption, and space and cooling requirements. Numerous providers now use the power of IPoDWDM to distribute video content rapidly and efficiently over an all-IP network. They can provision additional network capacity instantly as demand increases for any-play consumer and managed business services. The Cisco IPoDWDM solution reduces transport elements, while supporting advanced multilayer features such as proactive protection and control plane interaction, dramatically reducing operating expenses and capital costs.

Benefit from Valuable Product Enhancements

The Cisco IPoDWDM solution features:

Ultra long haul 100 Gb IPoDWDM capability, using the Cisco CRS 1-Port 100 Gigabit Ethernet Coherent

DWDM Interface Module

100 Gb coherent regeneration using the single-slot, 100 Gb trunk card on the ONS 15454 Multiservice

Transport Platform (MSTP), fully compatible with proactive protection.

Proactive protection on the Cisco ASR 9000 Series 2-Port and 1-Port 100 Gigabit Ethernet Line Cards

Industry-leading 10 Gb IPoDWDM density on the ASR 9000 Series 36-Port and 24-Port 10 Gigabit Ethernet

Line Cards

Complete Generalized Multiprotocol Label Switching (GMPLS) interoperability between the CRS-3, ASR 9000, and ONS 15454 MSTP

QUESTION NO: 3

Which three of these are optical channel data unit (ODU) overhead fields? (Choose three)

A. general communication channel 0 (GCC0)
B. section monitoring
C. reserved (RES)
D. general communication channels 1 and 2 (GCC1 GCC2)
E. tandem connection monitoring activation deactivation (TCM ACT)

Answer: C,D,E
Explanation: Optical Data Unit (ODU)
The ODU overhead is broken into several fields: RES, PM, TCMi, TCM ACT, FTFL, EXP, GCC1/GCC2 and APS/PCC. The reserved (RES) bytes are undefined and are set aside for future applications.

The path monitoring (PM) field is similar to the SM field described above. It contains the TTI, BIP-8, BEI, BDI and Status (STAT) sub-fields.

There are six tandem connection monitoring (TCMi) fields that define the ODU TCM sub-layer, each containing TTI, BIP-8, BEI/BIAE, BDI and STAT sub-fields associated to each TCM level (i=1 to 6). The STAT sub-field is used in the PM and TCMi fields to provide an indication of the presence or absence of maintenance signals.

The tandem connection monitoring activation/deactivation (TCM ACT) field is currently undefined in the standards. The fault type and fault location reporting communication channel (FTFL) field is used to create a message spread over a 256-byte multiframe. It provides the ability to send forward and backward path-level fault indications.

The experimental (EXP) field is a field that is not subject to standards and is available for network operator applications.

General communication channels 1 and 2 (GCC1/GCC2) fields are very similar to the GCC0 field except that each channel is available in the ODU.
The automatic protection switching and protection communication channel (APS/PCC) supports up to eight levels of nested APS/PCC signals, which are associated to a dedicated-connection monitoring level depending on the value of the multiframe.

QUESTION NO: 4

What is one of the primary overhead fields associated with the Optical Payload Unit (OPU)?

A. path monitoring
B. tandem connection monitoring activation deactivation (TCM ACT)
C. Payload Structure Identifier (PSI)
D. multiframe alignment signal (MFAS)
E. section monitoring

Answer: C
Explanation: Optical Payload Unit (OPU)
In order to begin describing the OTN as defined by the ITU G.709 standard, we must first enumerate its critical elements, their termination points, and the way they relate to one another in terms of hierarchy and function.

The primary overhead field associated with the OPU is the payload structure identifier (PSI). This is a 256-byte multiframe whose first byte is defined as the payload type (PT). The remaining 255 bytes are currently reserved. The other fields in the OPU overhead are dependent on the mapping capabilities associated to the OPU. For an asynchronous mapping (the client signal and OPU clock are different) justification control (JC) bytes are available to Application Note 153Telecom Test and Measurement compensate for clock rate differences. For a purely synchronous mapping (client source and OPU clock are the same), the JC bytes become reserved. Further details on mapping are available in ITU G.709.

QUESTION NO: 5

In optical channel transport unit overhead (OTU OH), what are general communication channels 1 and 2 (GCC1/GCC2) used for?

A. for trail trace identification
B. as the backward defect indicator
C. to transmit information between OTU termination points
D. to extend command and management functions over several frames
E. General communication channels 1 and 2 (GCC1/GCC2) do not belong to OTU OH.

Answer: E
Explanation: OTU overhead:
The OTU overhead consists of three bytes for section monitoring (SM), a two-byte general communications channel (GCC0), and two bytes reserved for future international standardization.

QUESTION NO: 6

What is the minimum hardware configuration of the multishelf Cisco CRS-1 system?

A. One route processor (RP) card and one modular services card (MSC)
B. One distributed route processor (DRP) and one S13 fabric card (SFC)
C. One line card chassis (LCC) and one fabric card chassis (FCC)
D. One route processor (RP) and one fabric card chassis (FCC)
E. One line card chassis (LCC) and one S13 fabric card (SFC)

Answer: C
Explanation: 1.4. SP high end product
A minimum of one LCC and one FCC are required to configure a multishelf system.

QUESTION NO: 7

Cisco IOS XR software is partitioned into three planes: control, data, and management. Which three of these belong to the data plane? (Choose three.)

A. XML
B. RIB
C. FIB
D. QoS
E. PFI

Answer: C,D,E
Explanation: (FIB, QoS, PFI). RIB is part of control plane
1.4. SP high end product
Cisco IOS XR Software is partitioned into three planes:
Control: Distributes routing tasks and management of the routing information base (RIB) to participating RPs; different routing processes can be running on different physical units.
DatA. Maintains the forwarding information base (FIB) changes across the participating nodes, letting the router perform as a single forwarding entity.
Management: Controls the operation of the router as a single networking element.

QUESTION NO: 8

Which statement about Software Maintenance Upgrade is true?

A. CRS-1 SMU can be applied to a different platform, and vice versa.
B. SMU is an executable code for running a process or libraries that are shared between the different processes.
C. SMUs for each release are individually downloadable from Cisco.com and come in the form of a tar ball.
D. SMUs provide software fixes for critical network down and qualification blocking issues. Therefore, every software defect has a corresponding SMU.
E. SMUs are release-specific. If an issue affects multiple platforms or releases, an SMU is built separately for each release and each platform.

Answer: E

Explanation: 1.4. SP high end product

SMUs for each release are individually downloadable from Cisco.com, whereas the bootable files and optional PIEs come in the form of a tarball.

SMUs are release specific. If an issue affects multiple platforms or releases, an SMU will be separately built for each release and each platform depending on the mission-critical need.

A CRS-1 SMU cannot be applied to a different platform, and vice versa.

SMUs provide software fixes for critical network-down and qualification-blocking issues. Therefore, every software defect will not have a corresponding SMU.

QUESTION NO: 9

Cisco IOS XR has implemented a nonstop routing feature so that when RP failover occurs, the routing information can be recovered locally. Which protocol does not support the NSR feature?

A. OSPF
B. LDP
C. BGP
D. IS-IS
E. RSVP

Answer: E
Explanation:

QUESTION NO: 10

Which three components are included in the Cisco IOS XR infrastructure? (Choose three.)

A. modular line cards
B. shelf controllers
C. route processors
D. service processors
E. distributed service cards

Answer: B,C,D

Explanation: 1.4. SP high end product

1.4.01. IOS-XR structure

Distributed Infrastructure

The kernel is replicated across the router infrastructure. The services and client applications can be distributed across the router infrastructure. The infrastructure includes route processors (RPs), distributed route processors (DRPs), service processors (SPs), shelf controllers (SCs), modular service cards (MSCs), and line cards (LCs).

QUESTION NO: 11

All secure domain routers (SDRs) have shared attribute and resources. Which three resources are shared all SDRs? (Choose three.)

A. privilege-level configuration
B. fabric cards
C. SNMP traps
D. admin-level configuration
E. exec-level configuration

Answer: B,C,D

Explanation: 1.4. SP high end product

There are shared attributes and resources common to all SDRs. It is important to note that the shared resources are critical to the system's overall operation. Some examples of shared resources that are common to SDR are:

- Environmental resources.
- Power supplies.
- Fan trays.
- Fan controllers.
- Fabric cards.

Software related:

* Exec-level configuration. Configuration in admin mode can affect all SDRs.

* Admin-level configuration. Admin-level command can impact owner SDR and non-owner SDRs.

* Process instances. A few processes are shared, systemwide processes such as LRd (SDR Deamon).

Management:

* SNMP traps. For example, shared power, fans, and fabric-related traps.

* SNMP polling. Shared for power, fans, and fabric-related MIBS.

* Syslogs. Some non-owner SDRs are logged to the owner SDR.

* Shared environment variables.

QUESTION NO: 12

Which three statements about the secure domain router are true? (Choose three.)

A. The logical router can span across chassis.
B. The fabric and system controller module are shared by all logical routers.
C. Each logical router has a distinct fabric and system controller module
D. The logical router can share a route processor
E. The logical router cannot share a route processor.

Answer: A,B,E
Explanation:
1.4. SP high end product
1.4.04. Secure domain router (SDR)

QUESTION NO: 13

There are two cabling schemes to choose from when implementing a Cisco CRS-1 multi shelf system: single module cabling and multi module cabling. What is the maximum capacity of the LCCs that are supported in multi module cabling?

A. 9 LCCs
B. 7 LCCs
C. 10 LCCs
D. 6 LCCs
E. 8 LCCs

Answer: A
Explanation:
1.4. SP high end product
A single card or multiple cards can be grouped as a fabric plane. Single-module cabling requires eight S2 cards in the fabric card chassis. In this mode, each S2 is dedicated to a plane number and cabled to the appropriate line card chassis plane. If your network requires more than three LCC in the multi shelf system, this is achieved using the multi module configuration. Multi module configuration provides capacity to add up to nine LCCs.

QUESTION NO: 14

Process-level redundancy is implemented by a system manager process that creates the standby process. What two functions are provided by the system-level process called Qnet Symlink Manager (QSM)? (Choose two.)

A. backing up the information for the broken connections
B. provides common information for connecting processes and services
C. detection of a failed connection
D. provides an abstract name for a process or service
E. distribution of symbolic link information

Answer: D,E
Explanation:
1.4. SP high end product
1.4.01. IOS-XR structure
Process-Level Redundancy
Process-level redundancy is implemented by a system manager process creating the standby process.
Because the active process created the standby process, the active process has all the information that it needs to communicate with the standby process. The active process uses a checkpoint database to share running state with the standby process. Symbolic links and abstract names are used to identify the processes.
Clients do not see the standby process until the active goes away. If a process fails and it has created a standby process, a system-level process called QNet Symlink Manager (QSM) and a library called Event Connection Manager (ECM) are used to re-establish links from the clients to the processes.

QSM provides:
Distribution of symbolic link information

Abstract name for a process or service

ECM provides:

Common information for connecting processes and services

Detection of broken connections

Only processes considered essential by development engineers are designated to support process-level redundancy. This is not a user-configurable option.

Clients have to reconnect to the "new" active process (the "original" standby process) when they detect that the active process has failed. Clients can connect to it using the symbolic links and abstract names. The new active process creates a new standby process.

The general steps in process redundancy are:

The active process dies.

The standby process becomes the active process.

A new standby process starts.

The new active process begins sending updates to the new standby process.

Clients begin using the new active process through the symbolic links and abstract names.

QUESTION NO: 15

When will the primary processor core dump run in case of a switchover?

A. never takes place
B. periodically
C. during switchover
D. after switchover
E. before switchover

Answer: D
Explanation:

In networking devices with redundant processors, the Post-Switchover Core Dump feature uses better software communication techniques between redundant processors to allow the switchover to occur before dumping core information. Not having to wait for dump operations effectively decreases the switchover time between processors. The newly active primary processor runs the core dump operation after switchover ReferencE.

http://www.cisco.com/en/US/docs/ios/12_0st/12_0st18/feature/guide/coredump.html

QUESTION NO: 16 DRAG DROP

Perform an IOS-XR Upgrade. Select the correct order

deactivate

remove

add

commit

activate

install

install

install

install

install

Answer:

Perform an IOS-XR Upgrade. Select the correct order

deactivate

remove

add

commit

activate

deactivate

remove

add

activate

commit

Explanation:

Perform an IOS-XR Upgrade. Select the correct order

deactivate

remove

add

activate

commit

QUESTION NO: 17

CRS-1 single shelf maximum capacities?

A. 320 Gbit/s
B. 640 Gbit/s
C. 1.2 Tbit/s
D. 92 Tbit/s

Answer: C
Explanation:
1.4. SP high end product
1.4.05. CRS-1/3 structure

QUESTION NO: 18

Which of the following processes in IOS XR run exclusively on the Route Processor? (Choose

two.)

A. wdsysmon
B. mpls_idp
C. sysmgr
D. gsp
E. bgp

Answer: B,E
Explanation:

QUESTION NO: 19

Refer to the exhibit.

```
Router-44# show isis database router-11.00-00 detail
IS-IS Level-1 LSP router-11.00-00
LSPID                   LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
router-11.00-00         0x00000079   0xBAB5        822           0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  Code:    137 Length: 8
  IP Address:  172.16.1.1
  Metric: 10 IP 172.16.126.0 255.255.255.0
  Metric: 10 IP 172.16.1.0 255.255.255.0
  Metric: 10 IS router-33.01
  Metric: 10 IS router-44.00

Router-44# show isis database router-22.00-00 detail
IS-IS Level-1 LSP router-22.00-00
LSPID                   LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
router-22.00-00         0x00000072   0x4FE3        791           0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  Code:    137 Length: 8
  IP Address:  172.16.126.2
  Metric: 10 IP 172.16.126.0 255.255.255.0
  Metric: 10 IS router-33.01

Router-44# show isis database router-33.01-00 detail
IS-IS Level-1 LSP router-33.01-00
LSPID                   LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
router-33.01-00         0x0000006D   0x65CF        759           0/0/0
  Metric: 0  IS router-33.00
  Metric: 0  IS router-22.00
  Metric: 0  IS router-11.00

Router-44# show isis database router-44.00-00 detail
IS-IS Level-1 LSP router-44.00-00
LSPID                   LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
router-44.00-00*        0x00000072   0xF71E        554           0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:  172.16.1.8
  Metric: 10 IP 172.16.1.0 255.255.255.0
  Metric: 10 IS router-11.00
  Metric: 0  ES router-88
```

Which router is the DIS?

A. router-22
B. router-44
C. router-33 and router-44
D. router-11
E. router-33

Answer: E
Explanation:

QUESTION NO: 20

What three major tasks are performed by a Designated Intermediate System in an ISIS pseudonode environment? (Choose three.)

A. updating the pseudonode LSP
B. maintaining pseudonode link-state information
C. creating the pseudonode LSP
D. flooding LSPs over the LAN
E. election of the pseudonode

Answer: A,C,D
Explanation: Two major tasks are performed by the DIS:
· Creating and updating pseudonode LSP for reporting links to all systems on the broadcast subnetwork. See the Pseudenode LSP section for more information.
· Flooding LSPs over the LAN.
Flooding over the LAN means that the DIS sends periodic complete sequence number protocol data units (CSNPs) (default setting of 10 seconds) summarizing the following information:
LSP ID

Sequence Number
Checksum
Remaining Lifetime
The DIS is responsible for flooding. It creates and floods a new pseudonode LSP for each routing level in which it is participating (Level 1 or Level 2) and for each LAN to which it is connected. A router can be the DIS for all connected LANs or a subset of connected LANs, depending on the IS-IS priority or the Layer 2 address.

The DIS will also create and flood a new pseudonode LSP when a neighbor adjacency is established, torn down, or the refresh interval timer expires. The DIS mechanism reduces the amount of flooding on LANs.

QUESTION NO: 21

What bit should be set in the link state PDUs in an IS-IS level-1-2 router to indicate that they are a potential exit point out of the area?

A. ATT (Attached) bit
B. ABR (Area Border Rorter) bit
C. PN (Pseudonode) bit
D. P (Partition) bit
E. Down bit
**F.** IS-Type bit

Answer: A
Explanation:

QUESTION NO: 22

The Attribute field within the IS-IS LSP header contains which of the following flags? (Choose four)

A. IS-Type
B. Overload (LSPDBOL)
C. Pseudonode (PN)
D. Attached (ATT)
E. Fragment (Frag-Nr)
F. Partition (P)

Answer: A,B,D,F
Explanation:

IS-IS LAN Hello PDU

IS-IS Point-to-Point Hello PDU

IS-IS Link-State PDU (LSP)

IS-IS Complete Sequence Number PDU (CSNP)

IS-IS Partial Sequence Number PDU (PSNP)
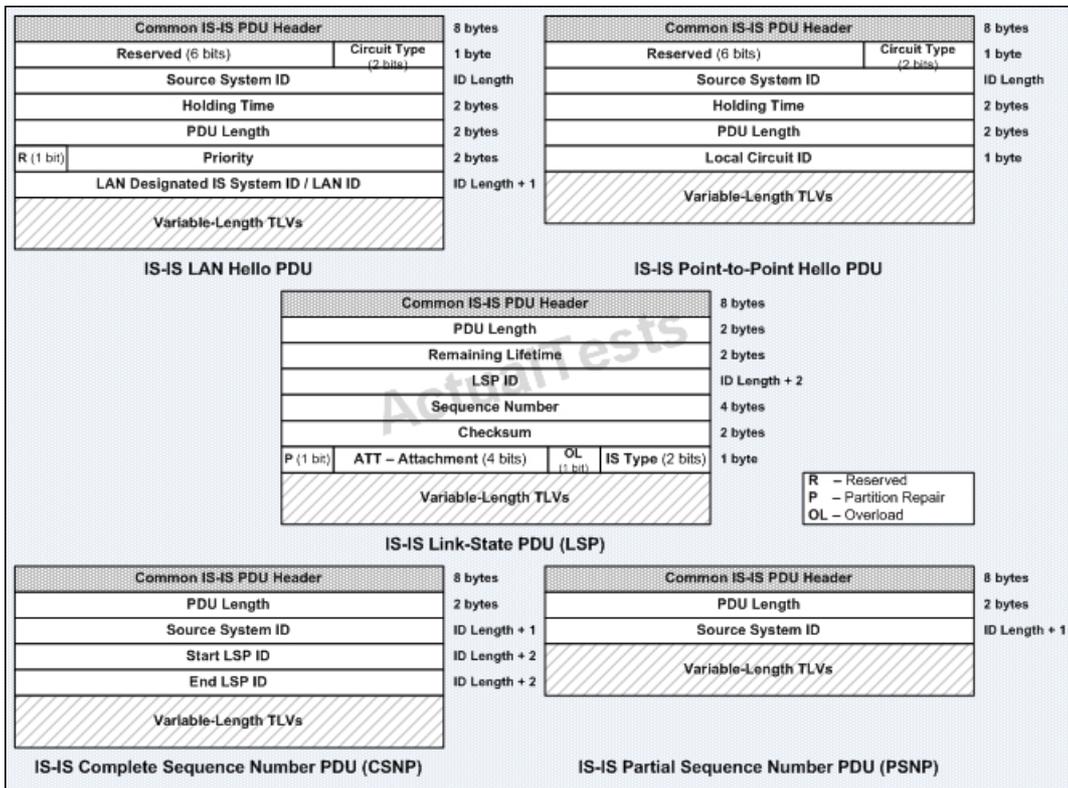
Partition Repair (P): Although this bit exists in both L1 and L2 LSPs, it is relevant only in L2 LSPs. When this bit is set to 1, it indicates that the originating router supports the automatic repair of area partitions. Cisco IOS does not support this feature; it always originates LSPs with the P bit set to 0.

Attachment (ATT): A 4-bit field indicating whether the originating router is attached to one or more areas.

Although this bit exists in both L1 and L2 LSPs, it is relevant only in L1 LSPs originated by L1/L2 routers to indicate that it is also a L2 router, which is a potential exit to reach other areas. Reading from left to right (bits 7 – 4), the bits indicate the Error metric, the Expense metric, the Delay metric, and the Default metric. Cisco IOSsupports only the default metric, so bits 5 – 7 are always 0.

Overload (OL): The Link-State Database Overload bit. This bit is often set to 0. A router set this bit on its LSPs when unable to store the entire LSDB. Routers receiving an LSP with the OL bit set will not use the originating router as a transit router as its routing table is incomplete, which may result in suboptimal routing and even routing loops; but they will still forward packets destined to the directly connected networks or interfaces of the originating router.

IS Type A 2-bit field indicating whether the originating router is an L1 or L2 IS.

01 – L1; 11 – L2; 00 and 10 are unused values.

An L1/L2 router sets the bits accordingly upon its L1 and L2 LSPs.

QUESTION NO: 23

Refer to the exhibit. Your customer has enabled IPv6 and IPv4 on routers R1 and R2, both running ISIS routing protocol, and they can no longer reach R3 network 172.26.15.0/24 (R3 does not enable IPv6, enables IPv4 only). Which two steps should be taken to restore reach ability to R3? (Choose two.)
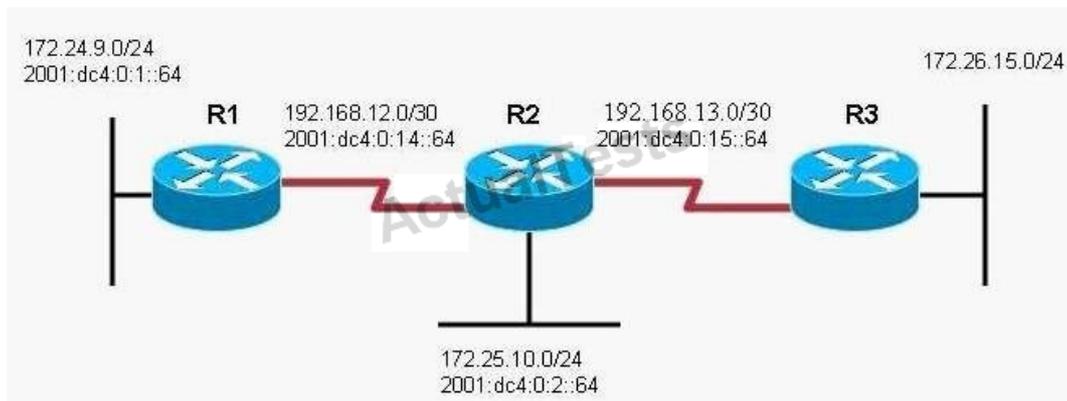
A. Enable OSPFv3 to support IPv4 and IPv6 simultaneously.
B. Configure static routes to all unreachable networks and redistribute to IS-IS.
C. Create an IPv6 tunnel from R2 to R3.
D. Transition to IS-IS Multiple Topology Mode on R3.
E. Enable wide metrics.
F. Transition to IS-IS Multiple Topology Mode on R1 and R2.

Answer: E,F
Explanation:

QUESTION NO: 24

What ISIS TLVs are used to support MPLS Traffic Engineering? (Choose three).

A. Extended IS neighbor TLV #22
B. Extended IS name TLV #137
C. Extended IS resource TLV #138
D. Extended IS reachability TLV #135
E. Router ID TLV #134

Answer: A,D,E

Explanation:

TLV Name Description

1 Area Address Includes the Area Addresses to which the Intermediate System is connected.

2 IIS Neighbors Includes all the IS-ISs running interfaces to which the router is connected.

8 Padding Primarily used in the IS-IS Hello (IIH) packets to detect the maximum transmission unit (MTU) inconsistencies. By default, IIH packets are padded to the fullest MTU of the interface.

10 Authentication The information that is used to authenticate the PDU, 22 TE IIS Neighbors Increases the maximum metric to three bytes (24 bits). Known as the Extended IS Reachability TLV, this TLV addresses a TLV 2 metric limitation. TLV 2 has a maximum metric of 63, but only six out of eight bits are used.

128 IP Int. Reachability Provides all the known IP addresses that the given router knows about via one or more internally-originated interfaces. This information may appear multiple times.

129 Protocols Supported Carries the Network Layer Protocol Identifiers (NLPID) for Network Layer protocols that the IS (Intermediate System) is capable. It refers to the Data Protocols that are supported. For example, IPv4 NLPID value 0xCC, CLNS NLPID value 0x81, and/or IPv6 NLPID value 0x8E will be advertised in this NLPID TLV.

130 IP Ext. Address Provides all the known IP addresses that the given router knows about via one or more externally-originated interfaces. This information may appear multiple times.

132 IP Int. Address The IP interface address that is used to reach the next-hop address.

134 TE Router ID This is the Multi-Protocol Label Switching (MPLS) traffic engineering router ID.

135 TE IP Reachability Provides a 32 bit metric and adds a bit for the "up/down" resulting from the routeleaking of L2->L1. Known as the Extended IP Reachability TLV, this TLV addresses the issues with both TLV 128 and TLV 130.

137 Dynamic Hostname Identifies the symbolic name of the router originating the link-state packet (LSP).

10 and 133 TLV 10 should be used for Authentication; not the TLV 133. If TLV 133 is received, it is ignored on receipt, like any other unknown TLVs. TLV 10 should be accepted for authentication only.

QUESTION NO: 25

How do routers in an IS-IS Level-1 domain exit to reach other Level-1 domains? (Choose two.)

A. Level-1 routers use default routes announced by Level-2 routers in Level-1 domain

B. Level-1 routers use default routes installed based on ATT bit (Attach Bit) in announcements from Level-1-2 router

C. Level-1 routers use specific routes, for other Level-1 domain, announced by Level-1-2 router by route leaking feature of Cisco IOS

D. Level-1 routers use specific routes, for other Level-1 domain, announced by Level-2 router by route-leaking feature of Cisco IOS

Answer: B,C

Explanation:

QUESTION NO: 26

In the IS-IS Designated Intermediate System (DIS) election process, which criteria is used for DIS selection?

A. highest router ID first, then highest priority
B. highest MAC address first, then highest priority
C. highest router ID first, then highest MAC address
D. highest priority first, then highest router ID
E. highest priority first, then highest MAC address

Answer: E

Explanation:

QUESTION NO: 27

What is periodically multicasted (every 10 seconds) by the DIS on a LAN to ensure IS-IS Link State Database accuracy?

A. IIH
B. LSP
C. CSNP
D. ISH
E. PSNP

Answer: C

Explanation:

On broadcast networks, designated routers send complete sequence number PDU (CSNP) packets to maintain database synchronization. The CSNP interval timer is the number of seconds between transmissions of CNSP packets from this interface.

QUESTION NO: 28

Which two statements regarding the IS-IS DIS election process are true? (Choose two.)

A. L1 routers on a broadcast network only establish adjacencies with the DIS.
B. If the DIS becomes unavailable the backup DIS is promoted to DIS.
C. Adding a router with a higher priority than the current DIS will result in the new router becoming DIS.
D. Separate L1 and L2 election processes are held on a brodcast network.
E. A priority of 0 will prevent a router from becoming a DIS.
F. If there is a tie based on priority, the router whose attached interface has the lowest MAC address becomes the DIS.

Answer: C,D

Explanation:

Election of the DIS

On a LAN, one of the routers elects itself the DIS, based on interface priority (the default is 64). If all interface priorities are the same, the router with the highest subnetwork point of attachment (SNPA) is selected. The SNPA is the MAC address on a LAN, and the local data link connection identifier (DLCI) on a Frame Relay network. If the SNPA is a DLCI and is the same at both sides of a link, the router with the higher system ID becomes the DIS. Every IS-IS router interface is assigned both a L1 priority and a L2 priority in the range from 0 to 127.

The DIS election is preemptive (unlike OSPF). If a new router boots on the LAN with a higher interface priority, the new router becomes the DIS. It purges the old pseudonode LSP and floods a new set of LSPs.

QUESTION NO: 29 DRAG DROP

Drag the ISIS packet types to correct type definition.

Discover neighbors to establish the adjacency with them.	IIH
Link state packet, four types.	PSNP
Contains a list of all LSPs from the current database.	CSNP
Used to request an LSP and acknowledge receipt of an LSP.	LSP

Answer:

Discover neighbors to establish the adjacency with them.	Discover neighbors to establish the adjacency with them.
Link state packet, four types.	Used to request an LSP and acknowledge receipt of an LSP.
	Contains a list of all LSPs from the current database.
Contains a list of all LSPs from the current database.	Link state packet, four types.
Used to request an LSP and acknowledge receipt of an LSP.	

Explanation:

Discover neighbors to establish the adjacency with them.

Used to request an LSP and acknowledge receipt of an LSP.

Contains a list of all LSPs from the current database.

Link state packet, four types.

There are four general types of packets, and each type can be Level 1 or Level 2.
•Intermediate System-to-Intermediate System Hello (IIH)—Used by routers to detect neighbors and form adjacencies. In addition to the IIH, which is an IS-IS protocol data unit (PDU), there is an ISH and an ESH, which are End System-to-Intermediate System (ES-IS) PDUs.

•Link-state packet (LSP)—There are four types of LSPs: Level 1 pseudonode, Level 1 nonpseudonode, Level 2
pseudonode, and Level 2 nonpseudonode.
•Complete sequence number PDU (CSNP)—CSNPs contain a list of all LSPs from the current database.
CSNPs are used to inform other routers of LSPs that may be outdated or missing from their own database.
This ensures that all routers have the same information and are synchronized. The packets are similar to an OSPF database description packet.
•Partial sequence number PDU (PSNP)—PSNPs are used to request an LSP (or LSPs) and

acknowledge receipt of an LSP (or LSPs).

QUESTION NO: 30

What is the importance of using Virtual Output Queues on ingress Line Cards in a high-end router?

A. Increases forwarding performance
B. Simplifies configuration
C. Prevents head-of-line blocking
D. Uses less memory

Answer: C
Explanation:

QUESTION NO: 31

What is the default SPF throttle timer in OSPF?

A. 5s
B. 10ms
C. 0ms
D. 30s
E. 1s
F. 500ms

Answer: A
Explanation:

QUESTION NO: 32

Which OSPF LSA is used to support MPLS Traffic-Engineering?

A. NSSA LSA (Type 7)
B. Opaque LSA (Type 11)
C. Opaque LSA (Type 9)
D. Opaque LSA (Type 10)

E. External LSA (Type 5)

Answer: D

Explanation:

Type 10 - an area-local "opaque" LSA as defined by RFC2370. Opaque LSAs contain information which should be flooded by other routers even if the router is not able to understand the extended information itself.

Typically type 10 LSAs are used for traffic engineering extensions to OSPF, flooding extra information about links beyond just their metric, such as link bandwidth and color.

QUESTION NO: 33

If two routers, both reachable from one another, originate functionally equivalent type 2 external LSAs (i.e. same destination, cost and non-zero forwarding address). Which of the following statements would apply?

A. Only the LSA generated by the lowest RID ASBR will exist in the network
B. Two LSAs will exist in the network for this destination, but only the one generated by the highest RID ASBR will be used
C. Two LSAs will exist in the network for this destination, and both will be used
D. Only the LSA generated by the highest RID ASBR will exist in the network

Answer: D

Explanation:

QUESTION NO: 34

The show ip ospf database external command displays information about which OSPF LSA type?

A. LSA type 1
B. LSA type 2
C. LSA type 7
D. LSA type 3
E. LSA type 9
F. LSA type 5

Answer: F

Explanation:

QUESTION NO: 35

Routes redistributed into an OSPF ASBR are which LSA type?

A. LSA type 6
B. LSA type 1
C. LSA type 2
D. LSA type 5
E. LSA type 3
F. LSA type 4

Answer: D
Explanation:

QUESTION NO: 36

When the Cisco IOS OSPF command ip ospf dead-interval minimal hello-multiplier 5 is configured, which two statements are true? (Choose two.)

A. OSPF hello interval is 5 seconds
B. OSPF hello interval is 1 second
C. OSPF dead interval is 1 second
D. OSPF dead interval is 5 seconds
E. OSPF dead interval is 20 seconds
F. OSPF hello interval is 0.2 second

Answer: C,F
Explanation:

QUESTION NO: 37

Which three statements about OSPF partial SPF are true? (Choose three)

A. If it is triggered by Type 4, all Type 4 LSAs that announce a certain ASBR and all Type 5 and 7 LSAs are processed
B. If it is triggered by Types 5 and 7, all Type 5 and 7 LSAs that contribute to a certain destination are processed.
C. If it is triggered by Type 2, all Type 2 LSAs that contribute to a certain destination are

processed.
D. It is triggered by the change of Type 3, 4, 5, and 7 LSAs.
E. It is triggered by the change of Type 2, 3, 5, and 7 LSAs

Answer: A,B,D

Explanation: Executed on a change in a type-3/4/5/7 LSA (as per sections 16.5 and 16.6 of RFC2328)

If there is a change in a type-1 or type-2 LSA, it affects the topology of the area and so a full SPF must be run

QUESTION NO: 38

Which statement about OSPF ASBR summary LSA is true?

A. It is generated by an ASBR and indicates the reachability to an ABR located in another area.
B. It is generated by ABR and indicates the reachability to an ASBR located in another AS.
C. It is generated by ABR and indicates reachability to itself.
D. It is generated by ABR and indicates the reachability to an ASBR located in another area.
E. It is generated by an ASBR and indicates the reachability to an ABR.

Answer: D
Explanation:

QUESTION NO: 39

Which two statements about OSPF IPv6 routing are true? (Choose two)

A. It requires OSPF version 3.
B. automatically detects neighbors over NHMA interfaces
C. It supports encryption using
D. It uses LSA type 9
E. It uses LSA type 8

Answer: A,E
Explanation:

QUESTION NO: 40

Which statement about OSPF authentication is true?

A. To enable OSPF authentication in a network, OSPF area 0 authentication must be enabled first.
B. The payload of OSPFv3 packets contains no authentication information.
C. OSPFv3 supports Advanced Encryption Standard
D. OSPFv3 uses router ID as a key to encrypt OSPF hello packets.
E. OSPF MD5 authentication uses TCP, and Plan Test authentication uses UDP.

Answer: B
Explanation:

QUESTION NO: 41

Which information is carried in the OSPFv3 intra-area Prefix LSA?

A. All link-local addresses
B. All IPv6 prefix and topology information that OSPFv2 included in Router LSA and Network LSA
C. List of options associated with the link to all other routers attached to the link
D. All prefix-specific information that OSPFv2 included in Router LSA and Network LSA

Answer: D
Explanation:

OSPFv3's new LSA, the Intra-area Prefix LSA (type 9), handles intra-area network information that was previously included in OSPFv2 type 2 LSAs. It is used in order to advertise one or more IPv6 prefixes. The prefixes are associated with router segment, stub network segment or transit network segment. Intra-area prefix LSAs (type 9) & Inter-Area-Prefix-LSA (type 3) carry all IPv6 prefix information, which, in IPv4, is included in router LSAs and network LSAs.

QUESTION NO: 42

The OSPF External LSA for prefix x.x.x.x exists in the OSPF database, but the prefix is not installed in the routing table. Which are possible explanations? (Choose three)

A. ASBR originating the LSA is not reachable.
B. Route to the Forwarding Address is an internal OSPF route.
C. Inbound distribute-list is configured under the ospf process and it is denying x.x.x.x
D. Route to the ASBR does not follow the same path as the one to the Forwarding Address.

E. Route to the Forwarding Address is not an internal OSPF route.

Answer: A,C,E
Explanation:

QUESTION NO: 43

Select two valid administratively scoped multicast addresses in networks running Interior Gateway protocols like EIGRP and OSPF (Choose two).

A. 239.255.255.255
B. 224.0.0.10
C. 239.0.0.1
D. 224.0.0.5

Answer: A,C
Explanation:

QUESTION NO: 44

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

A. EIGRP supports VLSM, route summarization, and routing update authentication.
B. If the feasible successor has a higher advertised distance than the successor route, it becomes the primary route.
C. Passive routes are in the process of being calculated by DUAL.
D. EIGRP exchanges full routing table information with neighboring routers with every update.
E. A query process is used to discover a replacement for a failed route if a feasible successor is not identified from the current routing information.

Answer: A,E
Explanation:

QUESTION NO: 45

With EIGRP DUAL, a feasible successor is considered loop-free if which condition is true?

A. Its AD is equal to the metric of the successor

B. Its AD is less than the successor's FD

C. Its AD is equal to the successor's FD

D. Its AD is greater than the successor's FD

E. Its FD is equal to the metric of the successor

Answer: B

Explanation:

QUESTION NO: 46

Regarding to EIGRP protocol, a "successor" is:

A. A neighbor that has met the feasibility condition

B. A neighbor that has met the feasibility condition and has the lowest cost path towards the destination

C. Any neighbor that is in the path towards the destination.

D. Any neighbor that is in the path towards the destination and whose reported distance equals the feasible distance.

Answer: B

Explanation:

QUESTION NO: 47

RIPv2 differs from RIPv1 in which three things? (Choose three).

A. it uses multicast address 224.0.0.10, instead of broadcast.

B. it uses multicast address 224.0.0.9, instead of broadcast.

C. it can use either multicast or broadcast addresses,instead of just broadcast.

D. it sends incremental updates,instead of periodic updates.

E. it is classless, instead of classfull

F. it supports authentication, and RIPv1 does not

Answer: B,E,F

Explanation:

QUESTION NO: 48

What does RPL stand for?

A. routing primary language
B. routing policy language
C. routing police language
D. routing program language
E. routing protocol language

Answer: B
Explanation:
1.5. IGP routing
1.5.40. IOS-XR routing policy language (RPL)

QUESTION NO: 49

In a frame, the MPLS label is imposed where?

A. Before the layer 2 header
B. Within the Layer 3 header
C. After the Layer3 header and before Layer2 header
D. After the Layer2 header and before Layer3 header

Answer: D
Explanation:
Where will the label be imposed in a packet?

A. The label is imposed between the data link layer (Layer 2) header and network layer (Layer 3) header. The top of the label stack appears first in the packet, and the bottom appears last. The network layer packet immediately follows the last label in the label stack.

QUESTION NO: 50

What is the action of "pop" in the context of MPLS switching?

A. It replaces the top label in the MPLS label stack with a set of labels.
B. It replaces the top label in the MPLS label stack with another value.
C. It adds a top label in MPLS label stack.
D. It removes the top label in the MPLS label stack.

Answer: D

Explanation:

Q. What is a label? What is the structure of the label?

A. A label is a short, four-byte, fixed-length, locally-significant identifier which is used to identify a Forwarding Equivalence Class (FEC). The label which is put on a particular packet represents the FEC to which that packet is assigned.

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|
|              Label              | Exp |S|      TTL           |
|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|
```
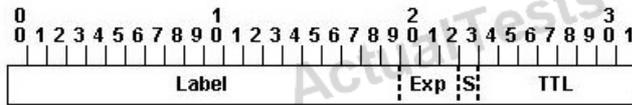
- **Label**—Label Value (Unstructured), 20 bits

- **Exp**—Experimental Use, 3 bits; currently used as a Class of Service (CoS) field.

- **S**—Bottom of Stack, 1 bit

- **TTL**—Time to Live, 8 bits

QUESTION NO: 51

Which four of these are MPLS label header fields? (Choose four.)

A. Label
B. VPI VCI
C. EXP
D. TTL
E. FCS
F. S flag

Answer: A,C,D,F
Explanation:

QUESTION NO: 52

Based on the following output in a router A running LDP, which statement is true?

ROUTER-A#show mpls ldp bindings 50.0.0.1 32

lib entry: 50.0.0.1/32, rev 5

local bindinG. label: imp-null

remote bindinG. lsr: 50.0.0.4:0, label: 16

A. None of the above.

B. The IP address 50.0.0.1/32 is assigned to the non-directly connected LDP neighbor, 50.0.0.4.

C. The IP address 50.0.0.1/32 is assigned to one of its own interfaces.

D. The IP address 50.0.0.1/32 is assigned to its directly connected LDP neighbor, 50.0.0.4.

Answer: C

Explanation:

QUESTION NO: 53

Which three statements about MPLS Label Distribution Protocol (LDP) are valid?

A. LDP hello packets are sent to UDP port 646

B. LDP hello packets are sent to TCP port 711

C. LDP sessions are TCP sessions to port 646

D. LDP sessions are TCP sessions to port 711

E. LDP establishes a peer relationship with another router that must be directly attached.

F. LDP can establishes a peer relationship with another router that is not directly attached

Answer: A,C,F

Explanation:

QUESTION NO: 54

Which option describes the incorrect usage of the Label Distribution method?

A. MP-BGP is used for label distribution for VPN customer routes.

B. LDP is primarily used in internal networks of MPLS-VPN providers.

C. MP-BGP is used for label distribution in MPLS Traffic Engineered networks.

D. Directed LDP is used for label distribution in L2-VPN Attachement Circuits.

Answer: C

Explanation:

QUESTION NO: 55

Which four services use the inner labels of an MPLS label stack? (Choose four)

A. MPLS VPN
B. switching path in MPLS core
C. Cisco MPLS Traffic Engineering and Fast Reroute
D. MPLS over ATM
E. VPN over Traffic Engineering core
F. any transport over MPLS

Answer: A,C,E,F

Explanation:

QUESTION NO: 56

Which 4 statements regarding MPLS Label Stack Encoding is true?

A. A value of 4 represents the "Implicit NULL Label."
B. A value of 0 represents the "IPv4 Explicit NULL Label."
C. A value of 1 represents the "Router Alert Label".
D. A value of 2 represents the "IPv6 Explicit NULL Label"
E. A value of 1 represents the "IPv1 Explicit NULL Label"
F. A value of 3 represents the "Implicit NULL Label"

Answer: B,C,D,F

Explanation:

A value of 0 represents the "IPv4 Explicit NULL Label". This label indicates that the label stack must be popped, and the packet forwarding must be based on the IPv4 header. This helps to keep Exp bits safe until the egress router. It is used in MPLS based QoS.

A value of 1 represents the "Router Alert Label". When a received packet contains this label value at the top of the label stack, it is delivered to a local software module for processing. The actual packet forwarding is determined by the label beneath it in the stack. However, if the packet is forwarded further, the Router Alert Label should be pushed back onto the label stack before forwarding. The use of this label is analogous to the use of the "Router Alert Option" in IP packets (for example, ping with record route option)

A value of 2 represents the "IPv6 Explicit NULL Label". It indicates that the label stack must be popped, and the packet forwarding must be based on the IPv6 header.

A value of 3 represents the "Implicit NULL Label". This is a label that an LSR can assign and distribute.

However, it never actually appears in the encapsulation. It indicates that the LSR pops the top label from the stack and forwards the rest of the packet (labeled or unlabeled) through the outgoing interface (as per the entry in Lfib). Although this value might never appear in the encapsulation, it needs to be specified in the Label Distribution Protocol, so a value is reserved.

QUESTION NO: 57   34

The mechanisms for distributing LDP are:

A. CEF and the FIB table
B. UDP and IP
C. A and B
D. RSVP and CEF
E. LDP and RSVP

Answer: E
Explanation:

QUESTION NO: 58

Based on the following output in R1, which statement is truE.

R1#show mpls forwarding-table 50.0.0.3 detail

Local Outgoing Prefix Bytes Label Outgoing Next Hop

Label Label or Tunnel Id Switched interface

19 17 50.0.0.3/32 0 Et0/0 192.168.0.14

A. If a labeled packet arrives with the topmost label of 17, all the labels will be removed and a clear IP packet is sent to Next Hop 192.168.0.14 on Ethernet 0/0.
B. If a labeled packet arrives with the topmost label of 17, the label is replaced with label 19 and the packet is sent out on the Ethernet 0/0 interface.
C. If a labeled packet arrives with the topmost label of 19, the label is replaced with label 17 and the packet is sent out on the Ethernet 0/1 interface.
D. If a labeled packet arrives with the topmost label of 19, the label is replaced with label 17 and the packet is sent out on the Ethernet 0/0 interface.

Answer: D
Explanation:

QUESTION NO: 59

What is the encapsulation mode for MPLS running on Ethernet?

A. Transparent mode.
B. Frame mode
C. Channel mode
D. Packet mode.
E. Tunnel mode.

Answer: B
Explanation:

QUESTION NO: 60

What IOS commands display MPLS label mapping on an LSR?

A. Show mpls ldp parameters
B. Show mpls ldp bindings
C. Show mpls forwading-table
D. Show mpls ldp discovery
E. Show mpls ldp neighbor detail

Answer: B
Explanation:

QUESTION NO: 61

Forwarding Equivalence Class (FEC) corresponds to which four of these? (Choose four).

A. Layer 2 circuits (ATM, FR, PPP, HDLC, Ethernet
B. Groups of addresses/sites-VPN
C. IPSEC Encryption Algorithm
D. A bridge/switch instance-VSI
E. Tunnel interface-traffic engineering

Answer: A,B,D,E
Explanation:

QUESTION NO: 62

Which two statements about forwarding equivalence class (FEC) are true? (Choose two)

A. FEC might correspond to a destination IP subnet, but it might also correspond to any traffic class that the edge LSR considers significant.
B. FEC is a group of IP packets that is forwarded over a different path, but with the same forwarding treatment.
C. FEC is a group of IP packets that is forwarded over the same path, and with the same forwarding treatment.
D. FEC is a group of IP packets that is forwarded over a different path, but with the different forwarding treatment.
E. FEC is a group of IP packets that is forwarded over the same path, but with a different forwarding treatment.

Answer: A,C
Explanation:

QUESTION NO: 63

What is the role of Forwarding Equivalence Class (FEC) in MPLS?

A. FEC determines how to establish an LSP path.
B. FEC determines how IP packets are forwarded in MPLS LSP.
C. FEC determines how MPLS labels are stacked in LSP.
D. FEC determines how a group of IP packets are mapped to an LSP.

Answer: D
Explanation:

QUESTION NO: 64

In MPLS traffic engineering, which one of the following protocols is used for Path Setup?

A. BGP
B. OSPF
C. ISIS
D. RSVP

Answer: D
Explanation:

QUESTION NO: 65

In the diagram, R1 is the head-end of a TE tunnel that terminates on R5. The red line indicates the protected link, and the gold line indicates the backup tunnel. Which router is the Point of Local Repair?
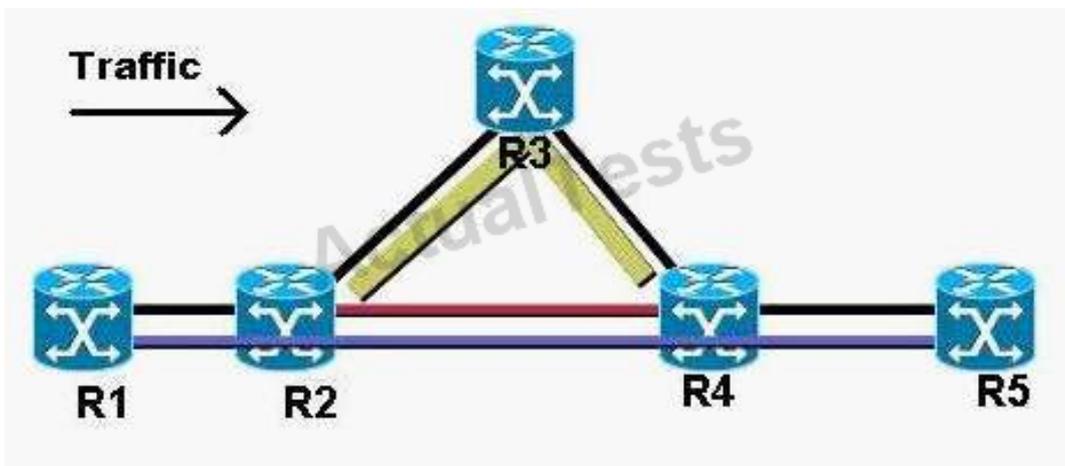
A. R2
B. R5
C. R3
D. R1
E. R4

Answer: A
Explanation:

QUESTION NO: 66

Which methods would enable traffic to be forwarded along an MPLS TE tunnel (Choose 4.)

A. MP-BGP routing
B. Static routing
C. Policy routing
D. Autoroute
E. Forwarding adjacency

Answer: B,C,D,E
Explanation:

QUESTION NO: 67

In the context of MPLS Traffic engineering, TE path calculation is conducted by:

A. TE middle point
B. TE tail end
C. Independent server
D. All TE nodes along the path
E. TE head end

Answer: E
Explanation:

QUESTION NO: 68

Which two routing protocols support MPLS traffic engineering link information distribution?
(Choose two)

A. OSPF
B. BGP
C. RIP version 2
D. IS-IS
E. EIGRP

Answer: A,D
Explanation:

QUESTION NO: 69

Which statements are correct for forwarding traffic into MPLS TE tunnels? (Choose 3)

A. Autoroute causes the tunnel to be treated as a directly connected link to the head-end.
B. Autoroute causes the TE head-end to establish IGP adjacency with the tail-end over the tunnel.
C. Forwarding adjacency makes the TE head-end node advertise the Tunnel LSP into the IGP.
D. Forwarding adjacency supports unequal cost load balancing over multiple TE tunnels.

Answer: A,C,D

Explanation:

QUESTION NO: 70

Which three statements about MPLS traffic engineering (MPLS TE) are true? (Choose three)

A. MPLS TE supports admission control
B. MPLS TE tunnel traffic is a link attribute to compute the TE tunnel path
C. MPLS TE uses BGP extension to advertise link attributes
D. MPLS TE provides protection capability
E. MPLS TE uses RSVP to establish LSP

Answer: A,D,E

Explanation:

QUESTION NO: 71

Which of these is not a component of MPLS traffic engineering?

A. trunk admission control
B. forwarding traffic to tunnel
C. information distribution
D. path selection, calculation, and setup
E. traffic patterns prediction

Answer: E

Explanation:

QUESTION NO: 72

Which two statements about MPLS point-to-multipoint traffic engineering (P2MP TE) are true? (Choose two)

A. P2MP TE uses an OSPF extension that is different from the OSPF extension that is used in P2P TE.
B. Loose path is not supported in P2MP TE.
C. Multiple IP multicast groups can map to one P2MP tunnel.

D. Affinity is not supported in P2MP TE.
E. P2MP TE uses Constrained Shortest Path First (CSPF) to calculate paths.

Answer: C,E

Explanation:

QUESTION NO: 73

Where are MPLS point-to-multipoint traffic engineering packets replicated?

A. head-end router
B. branch-point router
C. midpoint router
D. leaf-point router
E. tail-end router

Answer: B

Explanation:

ReferencE. http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_te_p2mp.pdf

1.7. MPLS Traffic Engineering

QUESTION NO: 74

Which statement about MPLS Traffic Engineering class-based tunnel selection (CBTS) is not true?

A. Local mechanism is at the middle-point router.
B. EXP selection is between multiple tunnels to the same destination
C. Bundle members are configured with EXP values to carry.
D. The tunnel selection is configured on the tunnel master.
E. The tunnel master bundles the tunnel members

Answer: A

Explanation:

1.7. MPLS Traffic Engineering

QUESTION NO: 75

Which statement about MPLS Traffic Engineering policy-based tunnel selection (PBTS) is not true?

A. The tunnel that is not configured with the policy-class command acts as the default.
B. EXP selection is between multiple tunnels to the same destination
C. There is no requirement for IGP extensions
D. Tunnels are configured using the policy-class command and carry multiple EXP values.
E. It supports VRF traffic, IP-to-MPLS switching, and MPLS-to-MPLS switching

Answer: D

Explanation:

1.7. MPLS Traffic Engineering

QUESTION NO: 76

Which two models are the models of DiffServ-Aware Traffic Engineering? (Choose two)

A. Policy-based Model
B. Class based Model
C. Russian Doll Model
D. Global Tunnel Model
E. Maximum Allocation Model

Answer: C,E

Explanation:

Therefore in practice, a Network Administrator might prefer to use:

•the Maximum Allocation Model when s/he needs to ensure isolation across all Class Types without having to use pre-emption, and s/he can afford to risk some QoS degradation of Class Types other than the Premium Class.

•the Russian Dolls Model when s/he needs to prevent QoS degradation of all Class Types and can impose preemption.

QUESTION NO: 77

Which three statements about the Cisco MPLS TE Fast Reroute (FRR) process are true? (Choose three.)

A. TE tunnels that are configured with the FRR option cannot be used as backup tunnels.
B. TE tunnels that are configured with the FRR option can be used as backup tunnels.
C. The backup tunnel that is used to protect a physical interface must have a valid IP address configured.
D. Interfaces must use MPLS global label allocation.
E. The source IP address of use backup tunnel and the merge point (MP) should not be reachable.

Answer: A,C,D

Explanation:

Restrictions for MPLS Traffic Engineering—Fast Reroute Link and Node Protection

•Interfaces must use MPLS Global Label Allocation.

•Backup tunnel headend and tailend routers must implement FRR as described in draft-pan-rsvp-fastreroute-00.txt.

•Backup tunnels are not protected. If an LSP is actively using a backup tunnel and the backup tunnel fails, the LSP is torn down.

•LSPs that are actively using backup tunnels are not considered for promotion. If an LSP is actively using a backup tunnel and a better backup tunnel becomes available, the active LSP is not switched to the better backup tunnel.

•You cannot enable FRR Hellos on a router that also has Resource Reservation Protocol (RSVP) Graceful Restart enabled.

•(Applicable only to Release 12.2.) You cannot enable primary one-hop autotunnels, backup autotunnels, or autotunnel mesh groups on a router that is also configured with stateful switchover (SSO) redundancy. This restriction does not prevent an MPLS TE tunnel that is automatically configured by TE autotunnel from being successfully recovered by any midpoint router along the LSP's path if the router experiences an SSO switchover.

•MPLS TE LSPs that are fast reroutable cannot be successfully recovered if the LSPs are FRR active and the Point of Local Repair (PLR) router experiences an SSO.

•When SSO (stateful switchover) occurs on a router, the switchover process must complete before FRR (fast reroute) can complete successfully. In a testing environment, allow approximately 2 minutes for TE SSO recovery to complete before manually triggering FRR. To check the TE SSO status, use the show ip rsvp high availability summary command. Note the status of the HA state field.

–When SSO is in the process of completing, this field will display 'Recovering'.

–When the SSO process has completed, this field will display 'Active'.

QUESTION NO: 78

Which statement about MPLS TE Fast Reroute (FRR) link protection operation is not true?

A. It requires a next-hop backup tunnel.

B. The backup tunnel terminates on the same tail-end router as the primary tunnel.

C. The point of local repair (PLR) swaps the label and pushes the backup label.

D. The restoration time is expected to be under 50 ms.

E. The backup tunnel can have associated bandwidth capacity

Answer: B

Explanation:

1.7. MPLS Traffic Engineering

The backup tunnel terminates on the merge point (MP) where traffic rejoins the primary tunnel.

QUESTION NO: 79

Which statement about MPLS TE Fast Reroute (FRR) node protection operation is not correct?

A. It requires a next-next hop backup tunnel.

B. Point of local repair (PLR) swaps the next hop label and pushes the backup label.

C. The backup tunnel terminates on the merge point (MP) where traffic rejoins the primary tunnel.

D. The backup tunnel can have associated bandwidth capacity.

**E.** Restoration time is expected under 50 ms.

Answer: E

Explanation:

1.7. MPLS Traffic Engineering

Restoration time depends on failure detection time.

QUESTION NO: 80

With the BGP peerings shown, which 3 solutions are most correct? (Choose three.)
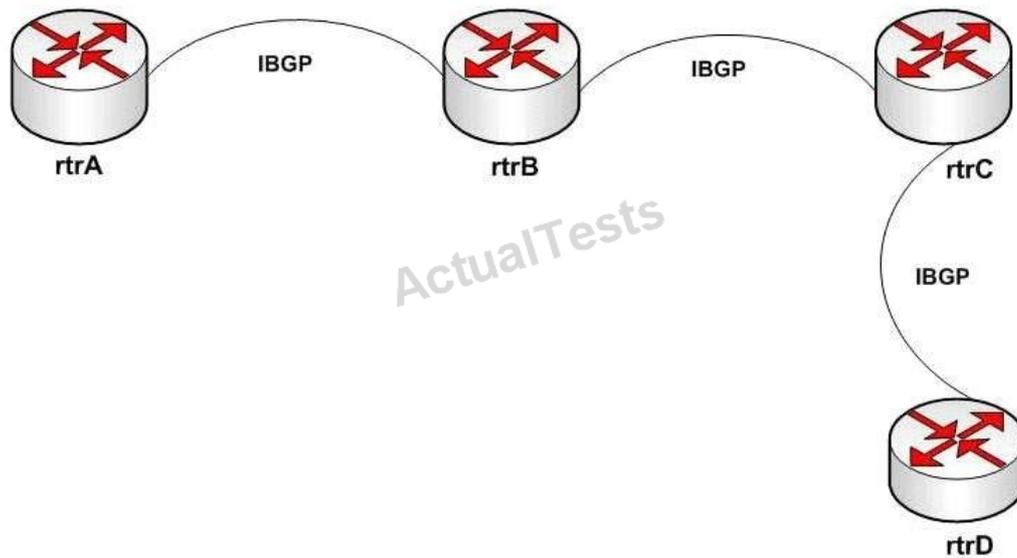
A. rtrA and rtrD are route-reflector-clients; rtrB and rtrC are route reflectors part of the same cluster.

B. rtrA and rtrD are route-reflector-clients; rtrB and rtrC are route reflectors part of the different cluster.

C. rtrA, rtrB and rtrC are part of a confederation sub-AS and rtrD is part of a different confederation sub-AS

D. rtrA, rtrB are part of one confederation sub-AS and rtrC, rtrD are part of a different confederation sub-AS

E. rtrA, rtrB and rtrC are part of a confederation sub-AS where rtrB is a route reflector and rtrA, rtrC are routereflector-clients.

Answer: B,D,E

Explanation:

QUESTION NO: 81

Referring to the exhibit, what could be preventing the R1 router from receiving any prefixes from the R2 BGP neighbor?

```
R1#show ip bgp summary
BGP router identifier 199.199.199.199, local AS number 20
BGP table version is 45, main routing table version 45
44 network entries using 4444 bytes of memory
81 path entries using 3888 bytes of memory
13 BGP path attribute entries using 780 bytes of memory
11 BGP AS-PATH entries using 264 bytes of memory
4 BGP route-map cache entries using 64 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 9440 total bytes of memory
BGP activity 88/44 prefixes, 191/110 paths, scan interval 5 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down   State/PfxRcd
192.168.1.17    4     1    1628    2693       45    0    0 00:42:22         31
192.168.20.22   4    22      70      73       45    0    0 00:42:26         31
192.168.31.1    4 65002     172     274        0    0    0 00:00:13 Idle

R1#telnet 192.168.31.1
Trying 192.168.31.1 ... Open


User Access Verification

Password: cisco

R2#sh run | begin bgp
router bgp 65002
 bgp confederation identifier 1
 bgp confederation peers 65001
 network 10.0.0.0
 neighbor 192.168.31.2 remote-as 20
```

A. The neighbor 192.168.31.2 next-hop-self command is missing on R2

B. R1 is using the wrong remote AS number in its neighbor 192.168.31.1 remote-as configuration

C. There is a TCP session establishment problem between R1 and R2

D. The no sync command is missing on R1

E. The no sync command is missing on R2

F. There is a BGP version mismatch between R1 and R2

Answer: B

Explanation:

QUESTION NO: 82

Which BGP community is used to prevent the advertisement of the BGP prefix to other BGP peers?

A. no-advertise

B. additive

C. no-export

D. local-as

E. none

Answer: A

Explanation:

QUESTION NO: 83

What statement about Transit AS is true?

A. Traffic and prefixes originating from Transit AS are carried across a Stub AS to their Source AS.
B. None of the above.
C. Traffic and prefixes originating from Source AS are carried across a Transit AS to reach their destination AS.
D. Traffic and prefixes originating from Transit AS are carried across a Stub AS to their destination AS.

Answer: C
Explanation:

QUESTION NO: 84

In which state can BGP peers exchange Update messages?

A. OpenConfirm
B. OpenSent
C. Active
D. Idle
E. Established

Answer: E
Explanation:

QUESTION NO: 85

BGP best route selection process is based on what?

A. path attributes
B. lowest cost
C. highest bandwidth
D. lowest delay

E. lowest hop-count

Answer: A
Explanation:

QUESTION NO: 86

What is the default BGP scanner time?

A. 10 minutes
B. 5 minutes
C. 120 seconds
D. 60 seconds
E. 30 minutes

Answer: D
Explanation: The scanning interval of BGP routing information.
Valid values are from 15 to 60 seconds. The default is 60 seconds.

QUESTION NO: 87

R3 and R4 are Route-Reflectors and there is an iBGP session between them, there is NO iBGP session between R1 and R2. For an External Route from CE-2 in R2 to reach R1, which two statements are true?
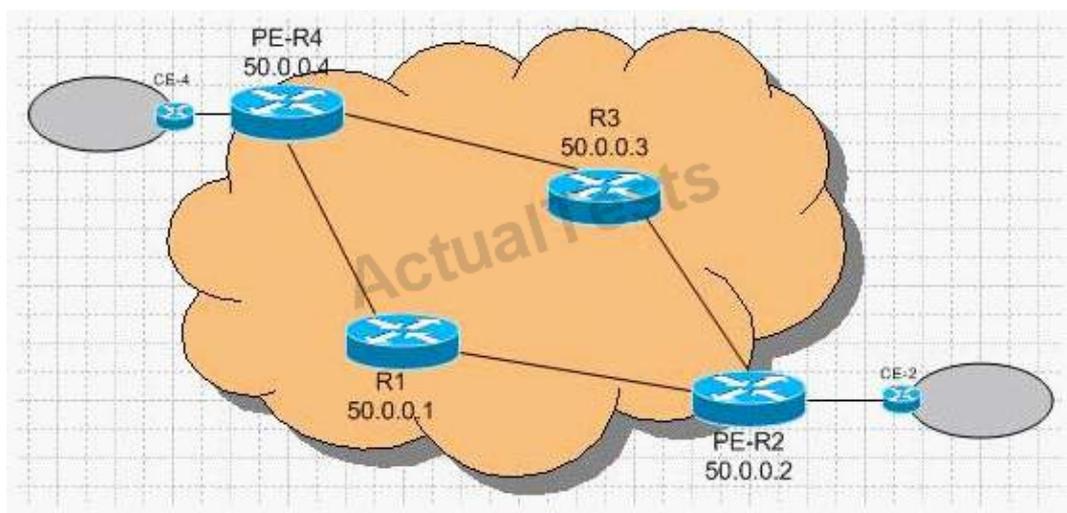
A. R1, R3 and R4 establish full mesh iBGP sessions, R2, R3 and R4 establish full mesh iBGP

sessions.

B. R1 acts as a Route-Reflector client to R3, R2 acts as a Route-Reflector client to R4.

C. R1 acts as a Route-Reflector client to R4, R4 acts as a Route-Reflector client to R3, R2 acts as a Route-Reflector client to R3.

D. CE-2 establishes multi-hop E-BGP sessions with R3 and R4.

Answer: B,C

Explanation:

QUESTION NO: 88

Which three choices are BGP Extended communities used in MPLS-VPN deployment? (Choose three).

A. Site of Origin SOO
B. Route-Distinguisher
C. Route-Target
D. Domain Identifier

Answer: A,C,D

Explanation:

BGP Extended Communities for OSPF PE/CE routing:

A Domain Identifier (Domain ID) is defined as BGP Extended Community which is carried with VPNv4 routes between PE routers. This Domain ID is used to identify the OSPF instance from which it was redistributed into BGP.

QUESTION NO: 89

What is the BGP synchronization rule?

A. BGP should not advertise a route until that route has been learned via an IGP.
B. Routing information received through an EBGP session is not forwarding to another EBGP neighbor, only to IBGP neighbors.
C. BGP neighbor peering are established and synchronized using TCP.
D. BGP should not advertise a route when that route has been learned via an IGP
E. Routing information received through an IBGP session is not forwarding to another IBGP neighbor, only to EBGP neighbors.

Answer: A

Explanation:

QUESTION NO: 90

router bgp 1

neighbor 1.1.1.1 remote-as 2

The above bgp configuration has what effect on the configured router?

A. Allows incoming TCP connections from 1.1.1.1 that are sourced from port 179
B. Allows incoming TCP connections from 1.1.1.1 that are destined to port 179
C. Allows incoming TCP connections sourced from port 179
D. Allows incoming TCP connections from 1.1.1.1 and destined to or sourced from port 179
E. Allows incoming TCP connections destined to port 179

Answer: B
Explanation:

QUESTION NO: 91

Refer to the exhibit. Which three statements describe r RIB-Failure in the show ip bgp command output? (Choose three.)

```
R1> show ip bgp
BGP table version is 5, local router ID is 2.100.200.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
            r RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
r> 6.6.6.0/24       10.10.13.3               0    130      0 30 i
*> 7.7.7.0/24       10.10.13.3               0    125      0 30 i
```

A. It is a redundancy route.
B. It is a route with a better administrative distance already present in IGP.
C. The number of routes in VRF exceeds the route limit that is configured under the VRF instance.
D. It is a rerouting entry
E. It indicates memory failure

Answer: B,C,E
Explanation:

QUESTION NO: 92

What best explains the BGP route-reflector function?

A. None of the above.
B. BGP route-reflector does not have to be in the forwarding path of data coming from its clients.
C. BGP route-reflector will stop reflecting the routes if they're not directly-connected clients.
D. BGP route-reflector should be in forwarding path of data coming from its clients.

Answer: B

Explanation:

Q. What does `r RIB-Failure` mean in the show ip bgp command output?

```
R1> show ip bgp
BGP table version is 5, local router ID is 200.200.200.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
r> 6.6.6.0/24       10.10.13.3             0    130      0 30 i
*> 7.7.7.0/24       10.10.13.3             0    125      0 30 i
```

A. When BGP tries to install the bestpath prefix into Routing Information Base (RIB) (for example, the IP Routing table), RIB might reject the BGP route due to any of these reasons:

- Route with better administrative distance already present in IGP. For example, if a static route already exists in IP Routing table.

- Memory failure.

- The number of routes in VPN routing/forwarding (VRF) exceeds the route-limit configured under the VRF instance.

In such cases, the prefixes that are rejected for these reasons are identified by `r RIB Failure` in the **show ip bgp** command output and are not advertised to the peers. This feature was first made available in Cisco IOS Software Release 12.2(08.05)T.

QUESTION NO: 93

What is the order of preference for these commands when all of them are applied to one neighbor in the BGP inbound filter direction?

A. prefix-list/distribute-list, filter-list, route-map
B. route-map, filter-list, prefix-list/distribute-list
C. route-map, prefix-list/distribute-list, filter-list
D. filter-list, prefix-list/distribute-list, route-map
E. prefix-list/distribute-list, route-map, filter-list

Answer: B

Explanation:

Q. What is the order of preference of attributes when some or all are applied to one neighbor in

BGP?

A. The order of preference varies based on whether the attributes are applied for inbound updates or outbound updates.

For inbound updates the order of preference is:

route-map

filter-list

prefix-list, distribute-list

For outbound updates the order of preference is:

prefix-list, distribute-list

filter-list

route-map

NotE. The attributes prefix-list and distribute-list are mutually exclusive, and only one command (neighbor

prefix-list or neighbor distribute-list) can be applied to each inbound or outbound direction for a particular neighbor.

QUESTION NO: 94

Which two statements about the bgp deterministic-med and bgp always-compare-med commands are true? (Choose two)

A. The bgp deterministic-med command is used to influence the BGP route selection process to cause the

MED attribute to have higher precedence over the AS path length

B. The bgp always-compare command is used to influence the BGP route selection process to cause the MED attribute to have higher precedence over the AS path system.

C. Enabling the bgp deterministic-med command ensures the comparison of the MED variable when choosing routes advertised by different peers in the same autonomous system.

D. Enabling the bgp always-compare-med command ensures the comparison of the MED variable for paths from neighbors in different autonomous systems.

E. The bgp deterministic-med and bgp always-compare-med commands are enabled by defult.

Answer: C,D

Explanation:

Enabling the bgp deterministic-med command ensures the comparison of the MED variable when choosing routes advertised by different peers in the same autonomous system. Enabling the bgp always-compare-med command ensures the comparison of the MED for paths from neighbors in different autonomous systems.

NotE. The bgp deterministic-med and bgp always-compare-med commands are not enabled by default. Also, the two commands are separate; enabling one does not automatically enable the other.

QUESTION NO: 95

What is the requirement of Remote Triggered Black Hole (RTBH) filtering?

A. ISIS updates exchange between trigger router and black hole router
B. EBGP updates exchange between trigger router and black hole router
C. None of above
D. OSPF updates exchange between trigger router and black hole router
E. IBGP updates exchange between trigger router and black hole router

Answer: E
Explanation:

QUESTION NO: 96

Which of the following are steps to configure destination-based Remote Triggered Black Hole (RTBH) filtering? (Choose three.)

A. Configure BGP between trigger and black hole routers.
B. Configure OSPF between trigger router and black hole routes
C. Configure all edge routers with static (reserved) host route to Null0
D. Configure on trigger router to advertise victim host route with community
E. Activate black hole by redistributing route for victim into BGP with next-hop set to the static (reserved) hostroute configured on edge routers.

Answer: A,C,E
Explanation:

The three steps in destination-based black hole filtering are summarized below.
Step 1. The setup (preparation)
A trigger is a special device that is installed at the NOC exclusively for the purpose of triggering a black hole.
The trigger must have an iBGP peering relationship with all the edge routers, or, if using route reflectors, it must have an iBGP relationship with the route reflectors in every cluster. The trigger is

also configured to redistribute static routes to its iBGP peers. It sends the static route by means of an iBGP routing update.

Step 2. The trigger
An administrator adds a static route to the trigger, which redistributes the route by sending a BGP update to all its iBGP peers, setting the next hop to the target destination address under attack as 192.0.2.1 in the current example. The PEs receive their iBGP update and set their next hop to the target to the unused IP address space 192.0.2.1. The route to this address is set to null0 in the PE, using a static routing entry in the router configuration. The next hop entry in the forwarding information base (FIB) for the destination IP (target) is now updated to null0. All traffic to the target will now be forwarded to Null0 at the edge and dropped.

Step 3. The withdrawal
Once the trigger is in place, all traffic to the target destination is dropped at the PEs. When the threat no longer exists, the administrator must manually remove the static route from the trigger, which sends a BGP route withdrawal to its iBGP peers. This prompts the edge routers to remove the existing route for the target that ispointed to 192.0.2.1 and to install a new route based on the IGP routing information base (RIB).

QUESTION NO: 97

Which statement about Remotely Triggered Black Hole (RTBH) is true?

A. Route tagging is one of the techniques used by RTBH
B. It is used for BGP authentication
C. It cannot work with static routes
D. It uses extended ACLs for blocking attacks by creating a black hole
E. Before configuring RTBH. LDP must be enabled on the interface

Answer: A
Explanation:

QUESTION NO: 98

Refer to the exhibit.
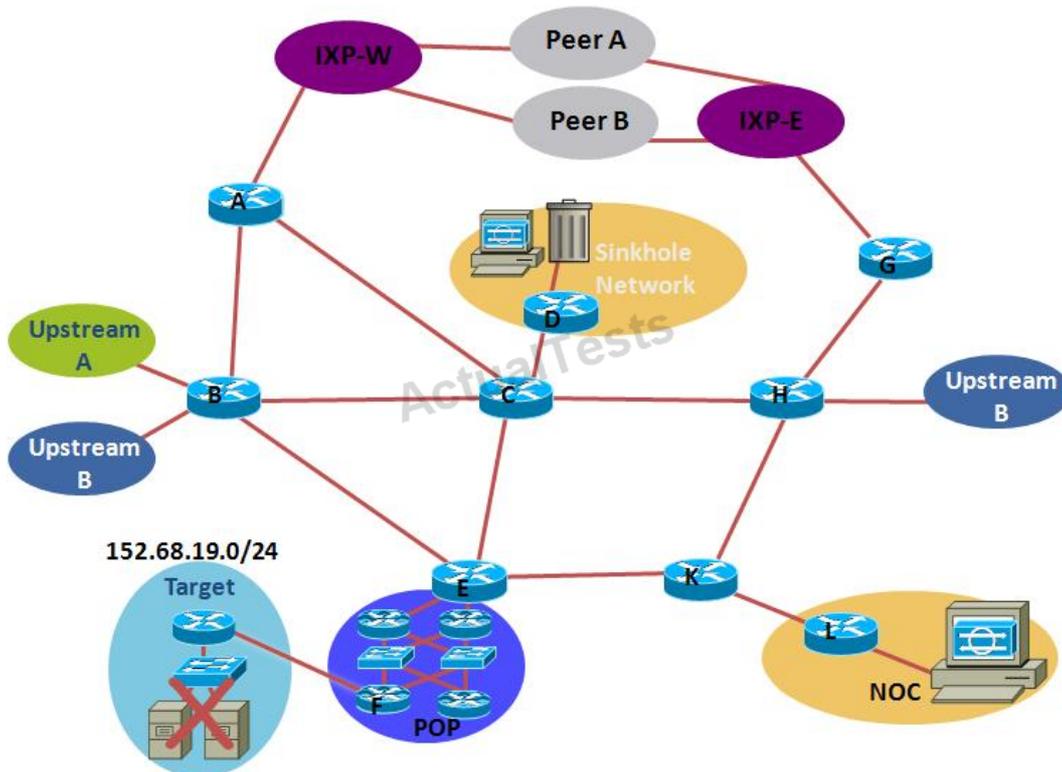
The SP network is configuring Remote Filtering to protect hosts on network 152.68.19.0/24. Which routers should be configured to the sinkhole router?

A. L and K
B. A, B, F, G, and H
C. C and D
D. A, B, G, and H
E. A, D, F, G, and L

Answer: A
Explanation:

QUESTION NO: 99

Refer to the exhibit.
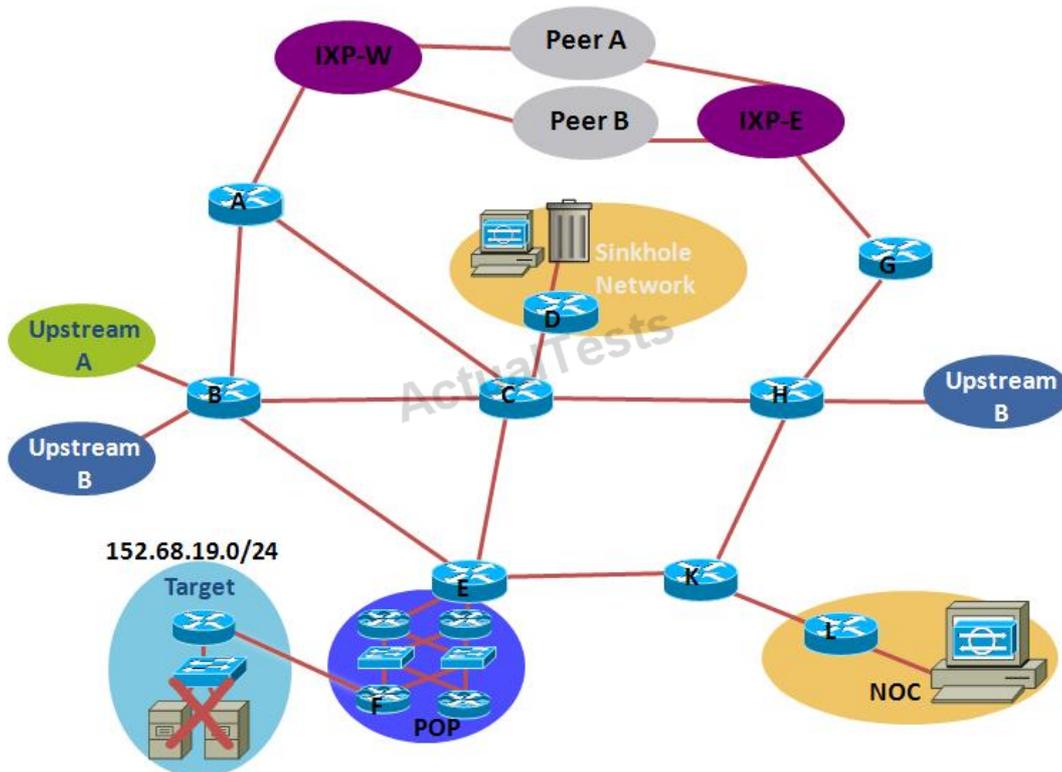
If the SP network is configuring RTBH filtering to protect hosts on the 152.68.19.0/24 network, which router should be configured as the black hole activating router?

A. F
B. C
C. D
D. L
E. A
F. K

Answer: A

Explanation:

1.13. Security in core

1.13.15. Remote triggered black hole (RTBH)

QUESTION NO: 100

Which three protocols use TLVs to carry attributes? (Choose three.)

A. Cisco Discovery Protocol
B. Label Discovery Protocol
C. Border Gateway Protocol

D. OSPF
E. RIP version 2

Answer: A,B,C
Explanation:

QUESTION NO: 101

Which three statements about BGP confederation and route reflectors are true? (Choose three)

A. Clusters are used in confederation schemes to avoid loops.
B. BGP network can have a confederation within a route reflector area.
C. An internal BGP network cannot have a route reflector within a confederation.
D. An internal BGP network can have a route reflector within a confederation.
E. Clusters are used in route reflector schemes to avoid loops.
F. BGP network cannot have a confederation within a route reflector area.

Answer: D,E,F
Explanation:

QUESTION NO: 102

Which three BGP attributes are carried by TLV? (Choose three)

A. Local Preference
B. Weight
C. Origin
D. Network Layer Reachability Information (NLRI)
E. Multiple Exit Discriminator (MED)

Answer: A,D,E
Explanation:
http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080094bbd.shtml#backinf

oBGP uses TLVs to carry attributes such as Network Layer Reachability Information (NLRI),
Multiple Exit Discriminator (MED), and local preference.
Several routing protocols use TLVs to carry a variety of attributes. Cisco Discovery Protocol
(CDP), Label Discovery Protocol (LDP), and Border Gateway Protocol (BGP) are examples of
protocols that use TLVs. BGP uses TLVs to carry attributes such as Network Layer Reachability

Information (NLRI), Multiple Exit Discriminator (MED), and local preference.

QUESTION NO: 103

Which three statements about the BGP next-hop attribute are true? (Choose three.)

A. EBGP sessions between confederation sub ASs do not modify the next-hop attribute.
B. By default, iBGP sessions change the next-hop attribute learned from eBGP peers to self address.
C. By default, the next-hop attribute is not changed when a prefix is reflected by the route reflector
D. EBGP sessions between confederation sub ASs change the next-hop attribute to peer address.
E. By default, iBGP sessions preserve the next-hop attribute learned from eBGP peers.

Answer: A,C,E
Explanation:

QUESTION NO: 104 DRAG DROP

Drag the Subsequent Address Family Identifiers number on the left to the correct protocol on the right.	
1	Network Layer Reachability Information with MPLS labels
2	MPLS-labeled VPN address
4	BGP MDT SAFI
65	Network Layer Reachability Information used for multicast forwarding
66	Network Layer Reachability Information used for unicast forwarding
128	Virtual Private LAN Service

Answer:

Drag the Subsequent Address Family Identifiers number on the left to the correct protocol on the right.	
1	4
2	128
4	66
65	2
66	1
128	65

Explanation:

4
128
66
2
1
65

1 – Network Layer Reachability Information used for unicast forwarding

2 – Network Layer Reachability Information used for multicast forwarding

4 – Network Layer Reachability Information with MPLS Labels

65 – Virtual Private LAN Service

66 – BGP MGT SAFI

128 – MPLS-labeled VPN address

ReferencE. http://www.iana.org/assignments/safi-namespace/safi-namespace.xhtml

QUESTION NO: 105

Which two statements are true about SAFI & AFI?

A. Subsequent Address Family identifier (SAFI) provides additional information about the type of the Network
Layer ports carried in the BGP update
B. Address Family identifier (AFI) field carries the identity of the Network Layer ports for which the BGP speaker intends to advertise multiple paths
C. Subsequent Address Family identifier (SAFI) provides additional information about the type of

the Network Layer Reachability Information carried in the attribute
D. Address Family identifier (AFI) carries the identity of the Network Layer protocol for which the BGP speaker intends to advertise multiple paths

Answer: C,D

Explanation:

QUESTION NO: 106

What are the Address Family Identifier (AFI) and Subsequent Address Family Identifier (SAFI) values for VPNv6?

A. AFI is 2, SAFI is 96
B. AFI is 2, SAFI is 64
C. AFI is 1, SAFI is 64
D. AFI is 1, SAFI is 128
E. AFI is 2, SAFI is 128

Answer: E

Explanation:

Table 1 SAFIs supported by Cisco IOS software

SAFI field value	Description	Reference
1	NLRI used for unicast forwarding.	RFC 2858
2	NLRI used for multicast forwarding.	RFC 2858
3	NLRI used for both unicast and multicast forwarding.	RFC 2858
4	NLRI with MPLS labels.	RFC 3107
64	Tunnel SAFI.	draft-nalawade-kapoor-tunnel-safi-01.txt
65	Virtual Private LAN Service (VPLS).	—
66	BGP MDT SAFI	draft-nalawade-idr-mdt-safi-00.txt
128	MPLS-labeled VPN address	RFC-ietf-l3vpn-rfc2547bis-03.txt

QUESTION NO: 107

In which two ways does the BGP graceful capability preserve prefix information during a restart? (Choose two)

A. The peer router immediately removes the BGP routers that it learned from the restarting router

from its BGP routing tables.

B. The router establishes BGP sessions with other routers and relearns the BGP routes from others that are also capable of graceful restart. The restarting router waits to receive updates from the neighboring routers.

C. The peer router sends an end-of-RIB message to the restarting router.

D. The restarting router removes any stale prefixes after the timer for stale entries expires.

E. The restarting router does not remove any stale prefixes after the timer for stale entries expires.

Answer: B,D

Explanation:

BGP Graceful Restart for NSF

When an NSF-capable router begins a BGP session with a BGP peer, it sends an OPEN message to the peer.

Included in the message is a declaration that the NSF-capable or NSF-aware router has graceful restart capability. Graceful restart is the mechanism by which BGP routing peers avoid a routing flap following a switchover. If the BGP peer has received this capability, it is aware that the device sending the message is NSF-capable. Both the NSF-capable router and its BGP peer(s) (NSF-aware peers) need to exchange the graceful restart capability in their OPEN messages, at the time of session establishment. If both the peers do not exchange the graceful restart capability, the session will not be graceful restart capable.

If the BGP session is lost during the RP switchover, the NSF-aware BGP peer marks all the routes associated with the NSF-capable router as stale; however, it continues to use these routes to make forwarding decisions for a set period of time. This functionality means that no packets are lost while the newly active RP is waiting for convergence of the routing information with the BGP peers.

After an RP switchover occurs, the NSF-capable router reestablishes the session with the BGP peer. In establishing the new session, it sends a new graceful restart message that identifies the NSF-capable router as having restarted.

At this point, the routing information is exchanged between the two BGP peers. Once this exchange is complete, the NSF-capable device uses the routing information to update the RIB and the FIB with the new forwarding information. The NSF-aware device uses the network information to remove stale routes from its BGP table. Following that, the BGP protocol is fully converged.

If a BGP peer does not support the graceful restart capability, it will ignore the graceful restart capability in an

OPEN message but will establish a BGP session with the NSF-capable device. This functionality will allow interoperability with non-NSF-aware BGP peers (and without NSF functionality), but the BGP session with non-NSF-aware BGP peers will not be graceful restart capable.

QUESTION NO: 108

What are the two benefits of graceful restart? (Choose two)

A. Graceful restart allows session information recovery without disruption to the network.
B. A node can perform a graceful restart to help a neighbor recover its state. The label bindings are kept on state information, which helps the failed node recover faster and does not affect the current forward traffic.
C. Graceful restart allows a node to recover state from its neighbor when there is no RP or before the device undergoes SSO.
D. Graceful restart does not allow session information recovery.
E. During a graceful restart, the router removes any stale prefixes after a timer for stale entries expires

Answer: A,B
Explanation:

QUESTION NO: 109

Which BGP attribute can be used to influence inbound traffic flow?

A. cluster ID
B. Weight
C. MED
D. local preference
E. aggregate

Answer: C
Explanation:

QUESTION NO: 110

Which description of BGP authentication is true?

A. MD5 has been used by BGP to encrypt BGP update packets.
B. BGP uses a message-digest algorithm to authenticate BGP peers
C. A plain-text password authentication is an option of BGP authentication
D. EBGP peers authentication is faster than IBGP peers authentication
E. BGP uses public key and private key to authenticate BGP peers.

Answer: B

Explanation:

BGP Authentication

BGP supports MD5 authentication between neighbors, using a shared password. It is configured under BGP router configuration mode with the command neighbor {ip-address | peer-group-name} password password.

When authentication is configured, BGP authenticates every TCP segment from its peer and checks the source of each routing update. Most ISPs require authentication for their EBGP peers.

QUESTION NO: 111

In which of the following BGP-related events is an End-of-RIB (EOR) message sent? (Choose two.)

A. Following a link flap in the BGP speaker's AS
B. During initial convergence.
C. Following a Route Processor Switchover.
D. Just before sending a CEASE message to tear down the session.
E. During capability negotiation

Answer: B,C

Explanation:

The Peer Router must signal the completion of the initial routing update by sending the End-of-RIB marker (discussed below)

While continuing to forward packets, the Peer Router refreshes the Restarting Router with any relevant BGP updates. The Peer Router indicates completion of this process by sending an End-of-RIB (EOR) marker. The EOR marker for IPv4 is a BGP update message that is of the minimum length—23 bytes. The EOR does not contain any routes to be added or withdrawn. Essentially, it is an "empty" update, whose sole purpose is to indicate that all available routes have been sent. The EOR marker helps speed convergence, because it allows the router to begin best-path selection as quickly as possible, without waiting for the timer to expire.

Once the Restarting Router has received all available routes from each peer, it can conduct best-path selection, and send any updates to its Peer Routers. The Restarting Router will also use the EOR to indicate the completion of this process.

QUESTION NO: 112

What method of streaming live video is the least taxing on bandwidth in a large enterprise environment?

A. TCP
B. UDP
C. HTTP
D. Multicast

Answer: D
Explanation:

QUESTION NO: 113

Which three statements about anycast RP are true? (Choose three.)

A. MSDP is running between anycast RPs.
B. Anycast RP provides redundancy and load-sharing capabilities
C. Multicast BGP is running between anycast RPs.
D. In anycast RP, two or more RPs are configured with the same multicast IP address on loopback interfaces
E. In anycast RP, two or more RPs are configured with the same unicast IP address on loopback interfaces

Answer: A,B,E
Explanation:

QUESTION NO: 114

Which are correct descriptions and configurations of Anycast RP? (Choose three).

A. In Anycast RP, two or more RPs are configured with the same IP address on loopback interfaces.
B. Anycast RP provides redundancy and load-sharing capabilities.
C. Routers with Anycast RP can be configured statically (loopback 1.1.1.1) with the command ip pim rpaddress 1.1.1.1
D. Routers with Anycast RP can be configured statically (loopback 1.1.1.1) with the command ip rp-address pim 1.1.1.1
E. Routers with Anycast RP can be configured statically (loopback 1.1.1.1) with the command ip anycast-rp pim 1.1.1.1

Answer: A,B,C

Explanation:

QUESTION NO: 115

What is the Cisco IOS default behavior for switching from the shared tree to the shortest path tree in PIM-SM operations?

A. immediately after receiving the first packet on the shared tree for a given (S, G)
B. after receiving over 1 kb/s traffic on the shared tree for a given (S, G)
C. 10 seconds after receiving the first packet on the shared tree for a given (S, G)
D. 30 seconds after receiving the first packet on the shared tree for a given (S, G)
E. after receiving over 10 kb/s traffic on the shared tree for a given (S, G)

Answer: A

Explanation:

QUESTION NO: 116

Cisco IOS XR Software Multicast Routing Implementation, which three features are supported in IPv6 on Cisco CRS router? (Choose three.)

A. PIM-SSM
B. Aggregation multicast
C. PIM-Bidirectional
D. OOR handling
E. Integrated multicast
F. Multicast NSF

Answer: A,C,F

Explanation:

Table 1: Supported Features for IPv4 and IPv6 on Cisco CRS Routers

Feature	IPv4 Support	IPv6 Support
Dynamic host registration	Yes (IGMP v1/2/3)	Yes (MLD v1/2)
Explicit tracking of hosts, groups, and channels	Yes (IGMP v3)	Yes (MLD v2)
PIM-SM[1]	Yes	Yes
PIM-SSM[2]	Yes	Yes
PIM-Bidir[3]	Yes	Yes
Auto-RP	Yes	No
Multicast VPN	Yes	Yes[4]
BSR[5]	Yes	Yes
MSDP[6]	Yes	No
BGP[7]	Yes	Yes
Multicast NSF[8]	Yes	Yes
OOR handling[9]	Yes	No

QUESTION NO: 117

Which of the following statements is correct regarding PIM Sparse Mode operations?

A. Receivers are "registered" with RP by their first-hop router
B. It supports shared trees only assuming all hosts want the multicast traffic
C. From the RP, traffic flows down a Source Tree to each receiver
D. It does not support all underlying unicast routing protocols like BGP
E. Receivers are "joined" to the Shared Tree (rooted the rp) by their local Designated Router (DR)

Answer: E
Explanation:

QUESTION NO: 118

Which two statements about RPF checks in Multicast Source Discovery Protocol (MSDP) are true? (Choose two)

A. RPF check should be done against the route to the source of the corresponding PIM-SM domain.

B. Checking session advertisement (SA) messages causes messages looping.

C. The RPF check ensures that there is a working redundancy for anycast RPs.

D. RPF check should be done against the route to the RP of the PIM-SM domain that originated the SA.

E. It prevents message looping, and session advertisement (SA) messages must be RPF checked.

Answer: D,E

Explanation:

SA Message Receipt

SA messages are only accepted from the MSDP RPF peer that is in the best path back toward the originator.

The same SA message arriving from other MSDP peers must be ignored or SA loops can occur. Deterministically selecting the MSDP RPF peer for an arriving SA message requires knowledge of the MSDP topology. However, MSDP does not distribute topology information in the form of routing updates. MSDP infers this information by using (M)BGP routing data as the best approximation of the MSDP topology for the SA RPF check mechanism. An MSDP topology, therefore, must follow the same general topology as the BGP peer topology. Besides a few exceptions (such as default MSDP peers and MSDP peers in MSDP mesh groups), MSDP peers, in general should also be (M)BGP peers.

Rule 1 of RPF checking in MSDP is applied when the sending MSDP peer is also an i(M)BGP peer. When Rule 1 is applied, the RPF check proceeds as follows:

The peer searches the BGP Multicast Routing Information Base (MRIB) for the best path to the RP that originated the SA message. If a path is not found in the MRIB, the peer then searches the Unicast Routing Information Base (URIB). If a path is still not found, the RPF check fails.

If the previous search succeeds (that is, the best path is found), the peer then determines the address of the BGP neighbor for this best path, which will be the address of the BGP neighbor that sent the peer the path in BGP update messages.

QUESTION NO: 119

What type of IPv6 address is this address FF05::2:260:8FF:FE52:F9D8?

A. multicast temporary node local

B. multicast temporary site local

C. unicast permanent link local

D. multicast permanent node link local

E. multicast permanent site local

F. unicast temporary link local

Answer: E

Explanation:

Permanent IPv6 Multicast addresses are assigned by IANA while the temporary IPv6 Multicast addresses can be used in pre-deployment Multicast testing. The Flag field may contain one of two possible values, as illustrated and described in the Table below:

Type of Multicast Address Binary Representation Hexadecimal Value

Permanent 0000 0

Temporary 0001 1

Multicast scope

The scope field indicates the scope of the IPv6 internetwork for which the multicast traffic is intended. The size of this field is 4 bits. In addition to information provided by multicast routing protocols, routers use multicast scope to determine whether multicast traffic can be forwarded. For multicast addresses there are 14 possible scopes (some are still unassigned), ranging from interface-local to global (including both link-local and sitelocal).

The following table lists the defined values for the scope field:

Table 3. Multicast scope field values

Value Scope

0 Reserved

1 Interface-local scope (same node)

2 Link-local scope (same link)

3 Subnet-local scope

4 Admin-local scope

5 Site-local scope (same site)

8 Organization-local scope

E Global scope

F Reserved

All other scope field values are currently undefined.

For example, traffic with the multicast address of FF02::2 has a link-local scope. An IPv6 router never forwards this type of traffic beyond the local link.

QUESTION NO: 120

In PIM-SM operations, the first router connected to the multicast source sends the Register message to which device?

A. Designated Router (DR)
B. Multicast source
C. Multicast receiver
D. RP mapping agent
E. RP

Answer: E

Explanation:

A multicast data sender just starts sending data destined for a multicast group. The sender's local router (DR) takes those data packets, unicast-encapsulates them, and sends them directly to the RP. The RP receives these encapsulated data packets, decapsulates them, and forwards them onto the shared tree. The packets then follow the (*,G) multicast tree state in the routers on the RP Tree, being replicated wherever the RP Tree branches, and eventually reaching all the receivers for that multicast group. The process of encapsulating data packets to the RP is called registering, and the encapsulation packets are known as PIM Register packets.

QUESTION NO: 121

Which three statements about bidirectional PIM are true? (Choose three)

A. Traffic for a bidirectional group flows along the one shared tree and simultaneously utilizes multiple paths in a redundant network topology.
B. It does not require any traffic signaling in the protocol
C. Membership to a bidirectional group is signaled using explicit Join messages.
D. It maintains source-specific forwarding state.
E. It reduces memory, bandwidth, and CPU requirements

Answer: B,C,E

Explanation:

ReferencE. http://www.cisco.com/en/US/docs/ios/12_1t/12_1t2/feature/guide/dtbipim.html

QUESTION NO: 122

Which of the following technologies can improve convergence time following a link failure in a service provider network? (Choose two.)

A. RSVP
B. MPLS TE FR

C. MPLS VPN
D. SNMP
E. BFD
F. VPLS

Answer: B,E
Explanation:

QUESTION NO: 123

You are about to design a very fast convergence time on a SP network. Which feature would you utilize to declare a link failure within less than two seconds of the fault on a link?

A. fast convergence SFP
B. MTU discovery
C. redundancy links
D. keepalive
E. carrier delay

Answer: E
Explanation:
1.11. Convergence

QUESTION NO: 124

Select the two answers that best describe the IP Event Dampening featurE.

A. The IP Event Dampening uses exponential decay mechanism to suppress the effects of excessive interface flapping
B. BGP Operators use IP Event Dampening to suppress the effect of unstable internet Routes
C. The IP Event Dampening works with routing protocols by stopping the announcement of dampened
Interface subnets in their updates
D. When IP Event Dampened internet routes reach their re-use limit, BGP installs them in the Routing Table and announces them to other BGP speakers

Answer: A,C
Explanation:
1.10. High Availability

QUESTION NO: 125

Refer to the exhibit.
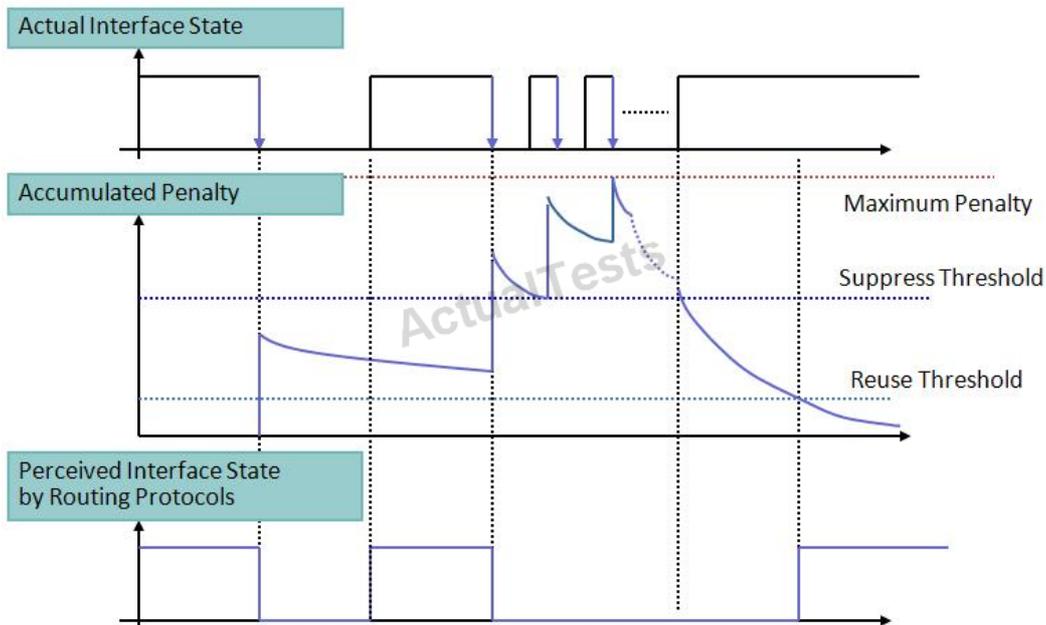
Which Cisco IOS feature does this algorithm illustrate?

A. OSPF exponential back-off
B. IP event dampening
C. partial SPF
D. EIGRP DUAL
E. the Cisco MPLS traffic engineering path recalculation

Answer: B
Explanation:
1.10. High Availability
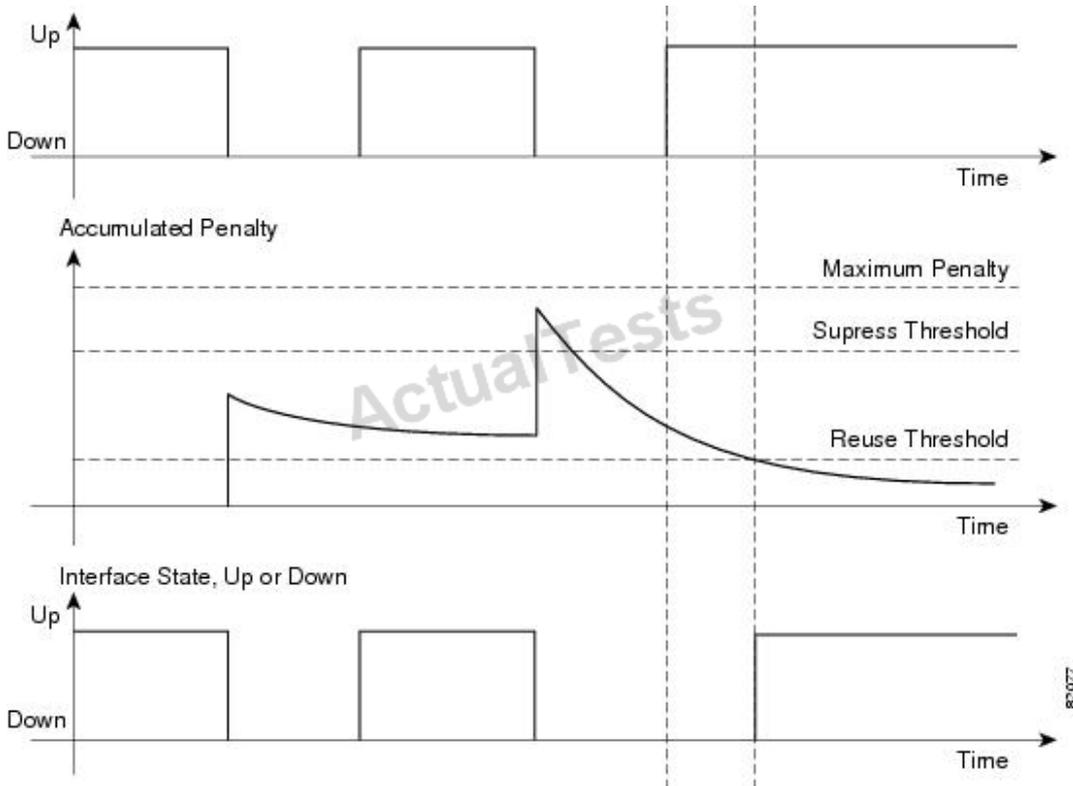
QUESTION NO: 126

Which of the following events can NOT be tuned via router configuration to provide for faster convergence following a link failure?

A. Failure detection
B. IGP LSP/LSA origination
C. Per-hop flooding time of new link state
D. Number of hops that need to be notified of new link state
E. Failure reporting

Answer: D
Explanation:

QUESTION NO: 127

Which configuration prevents traffic that is sourced from the unique local address scope to be sent out of the link to the upstream service provider?

A. interface ethernet0/0
ipv6 traffic-filter NoULA out
!
ipv6 access-list NoULA
deny ipv6 FC00::/8 any
permit ipv6 any any
B. interface ethernet0/0
ipv6 traffic-filter NoULA out
!
ipv6 access-list NoULA
deny ipv6 FC00::/7 any
permit ipv6 any any
C. interface ethernet0/0
ipv6 access-group NoULA out
!
ipv6 access-list NoULA
deny ipv6 FC00::/8 any
permit ipv6 any any
D. interface ethernet0/0
ipv6 access-group NoULA out
!
ipv6 access-list NoULA
deny ipv6 FC00::/7 any
permit ipv6 any any

Answer: B
Explanation:

A unique local address (ULA) is an IPv6 address in the block fc00::/7, defined in RFC 4193. It is
the approximate IPv6 counterpart of the IPv4 private address. Unique local addresses are
available for use in private networks, e.g. inside a single site or organization or spanning a limited
number of sites or organizations.

They are not routable in the global IPv6 Internet.
With our IPv6 ACL completed, we just need to apply it to an interface. There is a minor difference
in syntax herE. instead of using the command ip access-group to apply our IPv6 ACL, we use the
more aptly named command ipv6 traffic-filter, followed by the ACL name and a direction (in this
case, "out").

QUESTION NO: 128

The IPv6 address FE80::656:78FF:FE9A:BCDE is what type of address?

A. Site-local
B. Link-local
C. Multicast
D. None of the above

Answer: B
Explanation:

A link-local address is an IPv6 unicast address that can be automatically configured on any interface using the link-local prefix FE80::/10 (1111 1110 10) and the interface identifier in the modified EUI-64 format. Link-local addresses are not necessarily bound to the MAC address (configured in a EUI-64 format). Link-local addresses can also be manually configured in the FE80::/10 format using the ipv6 address link-local command.

QUESTION NO: 129

Which option is not a valid method to assign the lowest-order 64-bit field of an IPv6 unicast address?

A. ARP
B. manual assignment
C. DHCPv6
D. auto-configured based on the 48-bit MAC address
E. auto-generated pseudo-random number

Answer: A
Explanation: I concluded, and quickly confirmed that there's no such thing as ARP in IPv6 – so how do hosts find each other on a network? During the course of my studies, I learned that many functions like this were wrapped under the umbrella of IPv6 Neighbor Discovery, which runs on ICMPv6. The function of ARP is replaced in IPv6 by Neighbor Solicitation messages. I'd like to deep dive for a minute or two and explain exactly how this works.

QUESTION NO: 130

When IPv6 is deployed by a Service Provider to bring on an IPv6 Enterprise, which transition strategy works the best?

A. Deploy IPv6 at the Edges and tunnel Enterprise through the core
B. None of the above will work

C. Deploy IPv6 at Edges and Core at the same time for smooth transition
D. Deploy IPv6 at the core first and then move to Edges toward the end customer

Answer: A
Explanation:

QUESTION NO: 131

Which two statements about DS-Lite are true? (Choose two.)

A. IPv4 packets are carried over IPv6 tunnels to the LSN while IPv6 traffic is forwarded natively.
B. Ipv6 packets are carried over IPv4 tunnels to the LSN while IPv4 traffic is forwards natively.
C. The LSN performs NAT44 on private IPv4 source addresses.
D. DS-Lite does not perform any address translation.

Answer: A,C
Explanation:
ReferencE. "Understanding Dual-Stack Lite"
http://www.networkworld.com/community/node/46600
Dual-Stack Lite is a promising approach that takes the best of NAT464 while avoiding its
problems: It uses
IPv6-only links between the provider and the customer, but does not use NAT64 translation. When
a device in the customer network sends an IPv4 packet to an external destination, the IPv4 packet
is encapsulated in an IPv6 packet for transport into the provider network. At the LSN, the packet is
decapsulated and NAT44 isperformed.

QUESTION NO: 132

Which two are characteristics of an IPv6 multicast address? (Choose two)

A. Is allocated from the unicast address space
B. Second octet contains a 4-bit multicast scope field
C. Starts with a prefix of FE80 to FEBF in hex
D. Last 64 bit contains the modified MAC address of the Ethernet interface
E. First (most significant) octet is FF in hex
F. Starts with a prefix of FECO to FEFF in hex

Answer: B,E
Explanation:

The 12000 uses virtual output queues to eliminate the Head of Line Blocking within the switch fabric.

IPv6 [edit]

Multicast addresses in IPv6 have the prefix ff00::/8. IPv6 multicast addresses are generally formed from four bit groups, illustrated as follows:

General multicast address format

Bits	8	4	4	112
Field	prefix	flags	scope	group ID

The *prefix* holds the binary value 11111111 for any multicast address. Currently, 3 of the 4 flag bits in the *flags* field are defined;[4] the most-significant flag bit three flags are known as *R*, *P* and *T*.

Multicast address flags[5]

Bit	Flag	0	1
0 (MSB)	(Reserved)	(Reserved)	(Reserved)
1	R (Rendezvous)[6]	Rendezvous point not embedded	Rendezvous point embedded
2	P (Prefix)[7]	Without prefix information	Address based on network prefix
3 (LSB)	T (Transient)[8]	Well-known multicast address	Dynamically assigned multicast address

Similar to unicast addresses, the prefix of IPv6 multicast addresses specifies their scope, however, the set of possible scopes is different. The 4-bit *sc* (or sco indicate where the address is valid and unique.

QUESTION NO: 133

What is the importance of using Virtual Output Queues on ingress Line Cards in a high-end router?

A. Increases forwarding performance
B. Simplifies configuration
C. Prevents head-of-line blocking
D. Uses less memory

Answer: C
Explanation:

The 12000 uses virtual output queues to eliminate the Head of Line Blocking within the switch fabric.

Topic 2, I&O&T Edge/Access Technologies

QUESTION NO: 134

Which of the following is a correct arrangement of APS Action Requests in order of priority, with highest priority first?

A. Lookout of Protection, Forced Switch, SD, Manual Switch
B. SD, Lockout of Protection, Forced Switch, Manual Switch
C. Lockout of Protection, Manual Switch, SD, Forced Switch
D. Manual Switch, Forced Switch, Lockout of Protection, SD
E. Manual Switch, Lockout of Protection, Forced Switch, SD

Answer: A
Explanation:

1.1. Packet over SONET

Table 1 shows the priority requests from the highest (lockout) to the lowest (manual).

Table 1 APS Priority Request

Priority Priority Request

1 Lockout of protect port

2 Forced switch

3 Signal failure—low priority

4 Signal degradation—low priority

5 Manual switch

QUESTION NO: 135

In which of the following lists of APS Action Requests is the priority correctly arranged from lowest to highest?

A. Wait-to-Restore, Manual Switch, Forced Switch, Lockout of Protection
B. Wait-to-Restore, Forced Switch, Manual Switch, Lockout of Protection.
C. Manual Switch, Wait-to-Restore, Lockout of Protection, Forced Switch.
D. Lockout of Protection, Forced Switch, Manual Switch, Wait-to-Restore
E. Lockout of Protection, Manual Switch, Forced Switch, Wait-to-Restore
F. Wait-to-Restore, Manual Switch, Lockout of Protection, Forced Switch

Answer: A
Explanation:

1.1. Packet over SONET

Table 1 shows the priority requests from the highest (lockout) to the lowest (manual).

Table 1 APS Priority Request

Priority Priority Request

1 Lockout of protect port

2 Forced switch

3 Signal failure—low priority

4 Signal degradation—low priority

5 Manual switch

QUESTION NO: 136

SONET's three layers arE. (Choose three.)

A. DS1
B. Frame
C. Path
D. Line
E. Section

Answer: C,D,E
Explanation:
SONET Layers
SONET divides the overhead and transport functions into three layers:
•Section
•Line
•Path
These three layers are associated with both the physical equipment that segments the network and the bytes of information that flows through the network elements.

QUESTION NO: 137

For SONET ring switching, the 50ms switch time? (Choose two.)

A. Includes the detection time
B. Applies to rings smaller than 1200km
C. Applies to rings smaller than 1000km
D. Includes up to 16 nodes

Answer: B,D

Explanation:

APS protection switching has always been known for its recovery speed. SONET defines a maximum switch time of 50 milliseconds for a BLSR ring with no extra traffic and less than 1200 km of fiber. The specifications actually state 60 milliseconds, with 10 ms for discovery of the problem and 50 ms to perform the switch, but most people refer to this as just 50 ms. The maximum number of nodes on a BLSR is 16.

QUESTION NO: 138

Which three are advantages of SONET? (Choose three)

A. Allows the transportation of all forms of traffic
B. Multiplexing is easy
C. Clocks do not need to be synchronized
D. Reduces network complexity and cost
E. Padding is not necessary and not permitted

Answer: A,B,D

Explanation:

SONET Advantages

The big advantage of SONET is that it was designed to provide the following functions needed in networking at that time:

Single-step multiplexing

Access to low-level signals directly

Carry existing DS1, DS3, ATM, and packet traffic

Synchronous timing to eliminate bit stuffing

Overhead room for acceptable network management information

Allow transmission of data at higher speeds (50 Mbps+)

QUESTION NO: 139

Which statement about standard STS-1 SONET framing is true?

A. 8 rows by 64 bytes
B. 6 rows by 64 bytes
C. 10 rows by 96 bytes
D. 8 rows by 128 bytes

E. 9 rows by 90 bytes

Answer: E

Explanation: In the case of an STS-1, the frame is 810 octets in size, while the STM-1/STS-3c frame is 2,430 octets in size.

For STS-1, the frame is transmitted as three octets of overhead, followed by 87 octets of payload. This is repeated nine times, until 810 octets have been transmitted, taking 125 s. In the case of an STS-3c/STM-1, which operates three times faster than an STS-1, nine octets of overhead are transmitted, followed by 261 octets of payload. This is also repeated nine times until 2,430 octets have been transmitted, also taking 125 s.

For both SONET and SDH, this is often represented by displaying the frame graphically: as a block of 90 columns and nine rows for STS-1, and 270 columns and nine rows for STM1/STS-3c. This representation aligns all the overhead columns, so the overhead appears as a contiguous block, as does the payload.

QUESTION NO: 140

Which two statements are true about DPT/RPR?

A. DPT/RPR uses a bi-directional ring consisting of two symmetric counter rotating fibre rings.
B. DPT/RPR is defined in the IEEE 802.17 standard and it uses Token Bucket system to avoid collisions on the fiber.
C. DPT/RPR can be deployed in the Core of the SP networks where point-to-point POS links are used to make best use of the Bandwidth.
D. In DPT/RPR rings, data packets can be sent in one direction (downstream) and the corresponding control packets in the opposite direction (upstream), thus using both fibres concurrently to maximize bandwidth.

Answer: A,D

Explanation:

• SONET/SDH is the accepted transport architecture.

• The key building block is the twin optical fiber ring forming point-to-point connections that are "nailed up" between several SONET/SDH add-drop multiplexers (ADM).

• The twin fiber rings in SONET/SDH ring run in parallel, one is the working ring carrying the communication traffic. The other is the protection ring acting as a backup in the event of cable failure or failure of an ADM node.

• SONET/SDH provides good quality performance monitoring and failure protection information which also travel along the ring.

• The exclusive use of one ring for data and the other for protection means one ring is fully utilized

and the other ring is virtually redundant, awaiting the unlikely event of a failure.

This, of course, is not the most efficient use of fiber, especially given the considerable cost to lay fiber.

QUESTION NO: 141

What does FRTP stand for?

A. Frame Relay Top Pseudowire
B. Frame Relay Traffic Pseudowire
C. Frame Relay Traffic Protocol
D. Frame Relay Traffic Policing

Answer: D
Explanation:
Frame Relay Traffic Policing provides a mechanism to rate-limit packets on switched PVCs using a "leakybucket" implementation. When enabled, Traffic Policing prevents traffic congestion by discarding or setting the Discard Eligible (DE) bit on packets that exceed specified traffic parameters. Traffic Policing parameters can be specified per DCE interface, or per switched PVC, using the 'map class' mechanisms.

QUESTION NO: 142

Which two statements about spanning tree path cost are true? (Choose two.)

A. The path cost can be changed for an interface using the spanning-tree cost command.
B. The path cost can be changed for an interface using the stp path-cost command.
C. The STP default path cost depends on the interface speed.
D. The STP default path cost is similar for all interface.

Answer: A,C
Explanation:

QUESTION NO: 143

Two islands of IPv6 networks that are running ISIS (IPv6 IGP) must be connected using a tunnel over an IPv4 network. Which tunneling method can be used to achieve this goal?

A. GRE tunnels
B. automatic 6 to 4 tunnels
C. ISATAP tunnels
D. manual tunnels (RFC 2893)

Answer: A
Explanation:

GRE has a protocol field that identifies the passenger protocol. GRE tunnels allow Intermediate System-to-Intermediate System (IS-IS) or IPv6 to be specified as a passenger protocol, which allows both IS-IS and IPv6 traffic to run over the same tunnel. If GRE did not have a protocol field, it would be impossible to distinguish whether the tunnel was carrying IS-IS or IPv6 packets. The GRE protocol field is why it is desirable that you tunnel IS-IS and IPv6 inside GRE ReferencE. http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-tunnel.html

QUESTION NO: 144

What are the default values for GRE tunnel keepalive time and number of retries?

A. 5 seconds and 3 retries
B. 10 seconds and 5 retries
C. 10 seconds and 3 retries
D. 20 seconds and 5 retries
E. 5 seconds and 5 retries

Answer: C
Explanation:
This output shows the commands you use in order to configure keepalives on GRE tunnels.

Router# configure terminal

Router(config)#interface tunnel0

Router(config-if)#keepalive 5 4

!--- The syntax of this command is keepalive [seconds [retries]].

!--- Keepalives are sent every 5 seconds and 4 retries.

!--- Keepalives must be missed before the tunnel is shut down.

!--- The default values are 10 seconds for the interval and 3 retries.

QUESTION NO: 145

Refer to the exhibit.
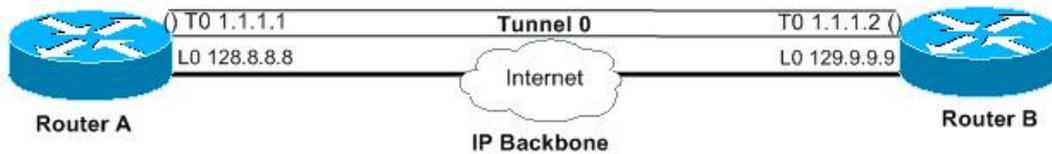

```
Router A

interface tunnel 0
ip address 1.1.1.1 255.255.255.240
tunnel source 128.8.8.8
tunnel destination 129.9.9.9
keepalive 5 4
interface loopback 0
Ip address 128.8.8.8 255.255.255.255

Router B

interface tunnel 0
ip address 1.1.1.2 255.255.255.240
tunnel source 129.9.9.9
tunnel destination 128.8.8.8
keepalive 5 4
interface loopback 0
ip address 129.9.9.9 255.255.255.255
```

Which two configurations are shown? (Choose two)

A. L2TP tunnel configuration
B. GRE tunnel configuration
C. IPsec tunnel configuration
D. tunnel keepalive mechanism configuration

Answer: B,D
Explanation:

QUESTION NO: 146

An architecture that utilizes PPPoE deals with IP address allocation by what type of negotiation?

A. NIS
B. IPCP
C. RADIUS
D. LDAP

Answer: B
Explanation:

QUESTION NO: 147

Which three are the ATM cell header fields? (Choose three.)

A. Cell loss priority (CLP)
B. Discard eligibility (DE)
C. Head error control (HEC)
D. Generic flow control (GFC)
E. Forward explicit congestion notification (FECN)

Answer: A,C,D
Explanation:
The ATM cell header consists of the following fields: generic flow control (GFC), virtual path identifier (VPI), virtual channel identifier (VCI), payload type (PT), cell loss priority (CLP) and header error control (HEC).

QUESTION NO: 148

Pick the 4 valid ATM Cell Header fields:

A. GFC-4 bits of generic flow control
B. Forward-explicit congestion notification(FECN)
C. VCI-16 bits of virtual channel identifier
D. CLP-1 bit of congestion loss
E. HEC-8 bit of header error control
F. ATM Discard Eligibility(DE) bit

Answer: A,C,D,E
Explanation:

The ATM cell header consists of the following fields: generic flow control (GFC), virtual path

identifier (VPI), virtual channel identifier (VCI), payload type (PT), cell loss priority (CLP) and header error control (HEC).

QUESTION NO: 149

What is the default maximum transmission unit on the Cisco router ATM interface?

A. 4470 bytes
B. 1516 bytes
C. 9288 bytes
D. 1500 bytes
E. 1492 bytes

Answer: A
Explanation:
Why are MTUs 4470 Bytes?
Most Cisco ATM router interfaces use a default MTU size of 4470 bytes. This number was chosen to match exactly Fiber Distributed Data Interface (FDDI) and High-Speed Serial Interface (HSSI) interfaces for autonomous switching.

QUESTION NO: 150

Which statement about ATM AAL5 over MPLS is true?

A. It supports ATM signaling.
B. It supports traffic shaping of packets in MPLS to the ATM path.
C. It supports ATM switched virtual circuits
D. It supports fragmentation and reassembly.
E. It supports AAL5 SDU switching.

Answer: E
Explanation:
ReferencE. http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsaal22.html#wp1015337
Restrictions
The following restriction apply to AAL5 over MPLS:
•The AAL5 over MPLS feature supports only AAL5 SDU switching.
•The following services are not supported with the AAL5 over MPLS feature:

–ATM switched virtual circuits (SVCs)

–ATM signaling

–Fragmentation and reassembly

–Traffic shaping of packets in the MPLS-to-ATM path

•The instructions for configuring AAL5 over MPLS in this feature module apply only to the Cisco 12000 series router for 12.0(21)ST. Avoid using these instructions for any other platform or release.

QUESTION NO: 151

Which type of AAL does ATM utilize to deliver CBR traffic?

A. AAL2
B. AAL4
C. AAL5
D. AAL1
E. AAL3

Answer: D

Explanation:

An ATM Adaptation layer 1 or AAL1 is used for transmitting Class A traffic, that is, real-time, constant bit rate, connection oriented traffic (example- uncompressed audio and video). Bits are fed in by the application at constant rate and must be delivered to other end with minimum delay, jitter or overhead. The input is stream of bits without message boundaries. For this traffic, error detection protocols cannot be used since timeouts and retransmission causes delay but the missing cells are reported to the application, that must take its own action to recover from them.

QUESTION NO: 152

What are three common reasons for ATM CRC errors? (Choose three.)

A. Incorrect VPI and VCI configuration
B. Noise, gain hits, or other transmission problems on the data link equipment
C. ATM cells are dropped due to incorrect ATM routing in the service provider.
D. A faulty or failing ATM interface.
E. Cells are dropped due to traffic policing in the ATM cloud on one or more virtual circuits

attached to the ATM interface.

Answer: B,D,E
Explanation:

Reasons for ATM CRC Errors

The following are some potential reasons for ATM CRC errors:

Dropped cells due to traffic policing in the ATM cloud on one or more VCs attached to the ATM interface.

Noise, gain hits, or other transmission problems on the data-link equipment.

A faulty or failing ATM interface.

The show interfaces command output displays the CRC error count. These errors suggest that when the SAR reassembles the packet and checks the CRC, the calculated CRC value does not match the value in the assembled packet's CRC field.

QUESTION NO: 153

Select the three best answers which best describe Private Network-to Network Interface (PNNI) in an ATM network (Choose three.)

A. It is the Routing protocol used between ATM switches
B. PNNI uses the same Dijsktra algorithm for SPF calculation
C. PNNI and OSPF use the same Database to make cohesive decision for packet forwarding
D. PNNI measures line capacities and delays in addition to simple cost metrics

Answer: A,B,D
Explanation:

The Private Network-to-Network Interface (PNNI) is a link-state routing protocol used in ATM networks. PNNI is similar to the open shortest path first (OSPF) used for IP routing.

PNNI is a suite of network protocols that can be used to discover an ATM network topology, create a database of topology information, and route calls over the discovered topology. PNNI is a link-state routing protocol, which means that the protocol collects information about the current state of links and nodes in the network to build a network database. The PNNI network database can be used to determine the network structure and the current state of network components. To build the PNNI network database, each PNNI node must receive topology information from all the other devices in the network. To keep the database current, the node must receive regular updates from other nodes.

QUESTION NO: 154

What is the label for MPLS over ATM?

A. VPI 16
B. DLCI
C. VPI and VCI
D. circuit number
E. PVC and SVC

Answer: C
Explanation:

QUESTION NO: 155

What is used as label in cell-based MPLS?

A. VPI and VCI
B. None of above
C. VCI
D. Specific 4 bytes label
E. VPI

Answer: A
Explanation:

QUESTION NO: 156

When should traffic shaping be implemented on Frame Relay PVCs? (Choose two)

A. When you want to drop excess traffic above the CIR
B. When there is a speed mismatch between the central site and the remote site.
C. When using Frame Relay SVCs
D. When over-subscribing the central site link
E. When LLQ is implemented on the Frame Relay PVC.
F. When Multilink PPP LFI is implemented on the Frame Relay PVC.

Answer: B,D
Explanation:

QUESTION NO: 157

Which statement about Frame Relay is not true?

A. Static mapping is used when the remote router does not support Inverse ARP.
B. Frame Relay Inverse ARP requires LMI capability to construct an address to the DLCI mapping table on the router.
C. Frame Relay Inverse ARP is disabled by default in Cisco IOS Software for all protocols that are enabled on the physical interface.
D. Inverse ARP does not work when LMI is disabled.
E. Frame Relay provides forward and backward congestion notification messages.

Answer: C
Explanation:

QUESTION NO: 158

Which three are optional extensions of the Frame Relay Local Management Interface specification? (Choose three)

A. Switched virtual circuit
B. Virtual circuit status
C. Simple flow control
D. Multicasting
E. Permanent virtual circuit

Answer: B,C,D
Explanation: Optional LMI Extensions:

The LMI specification also defines several optional extensions:

* Global addressing convention

* Multicast capability

* A simple flow control mechanism

* Ability for the network to communicate a PVC's CIR to the subscriber in a Status message

* A new message type that allows the network to announce PVC status changes without

prompting from the subscriber Implementors may build any, all, or none of these features into their

networks.

QUESTION NO: 159

Select the three valid LMI extension:

A. Multicasting
B. Global addressing
C. Forward-explicit congestion notification (FECN)
D. Virtual circuit status messages.
E. Backward-explicit congestion notification (BECN)

Answer: A,B,D

Explanation:

Optional LMI Extensions:

The LMI specification also defines several optional extensions:

* Global addressing convention

* Multicast capability

* A simple flow control mechanism

* Ability for the network to communicate a PVC's CIR to the subscriber in a Status message

* A new message type that allows the network to announce PVC status changes without prompting from the subscriber

Implementors may build any, all, or none of these features into their networks.

QUESTION NO: 160

In the Cisco Resilient Ethernet Protocol (REP), how many ports are always blocking?

A. zero
B. at least one
C. at least two
D. at least four
E. at least three

Answer: B

Explanation:

http://www.cisco.com/en/US/prod/collateral/switches/ps6568/ps6580/prod_white_paper0900aecd8 06ec6fa.pdf

Cisco REP Operation

With REP at least one port is always blocked in any given segment, that is, the alternate port.

QUESTION NO: 161

Which four statements about Ethernet virtual circuit (EVC) infrastructure are true? (Choose four.)

A. EVC infrastructure is a Layer 3 platform-independent routing architecture that supports IP over Ethernet services.
B. Ethernet flow point (EFP) is configured on the main interface.
C. Feature commands like MQC-based QoS policies can be specified.
D. EVC infrastructure is a Layer 2 platform-independent bridging architecture that supports Ethernet services.
E. Each Ethernet flow point (EFP) matches a predefined VLAN tag-based criteria.
F. Ethernet flow point (EFP) is configured on the VLAN interface.

Answer: B,C,D,E
Explanation:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/ethernet_virtual_connection.html#wp1050309
http://www.cisco.com/en/US/docs/switches/metro/me3600x

QUESTION NO: 162

Which three of these are types of Ethernet Virtual Connections (EVCs) in the MEF concept? (Choose three)

A. rooted multipoint EVC (E-Tree)
B. point-to-point EVC (E-Line)
C. point-to-multipoint EVC (E-Tree)
D. hub spoke EVC (E-Tree)
E. multipoint-to-multipoint EVC (E-LAN)

Answer: A,B,E
Explanation:
MEF Service
Ethernet Service Types can be used to create a broad range of Subscriber services. The service types are characterized by their required connectivity [10]. The following service types have been defined to date:
Ethernet Line Service (E-Line Service) uses a Point-to-Point EVC. The Ethernet LAN Service (E-LAN Service) uses a Multipoint-to-Multipoint EVC. The Ethernet Tree Service (E-TREE Service)

uses a Rooted-Multipoint EVC.

QUESTION NO: 163

Which two statements about 10 Gigabit Ethernet (10GE) are true? (Choose two.)

A. 10 Gigabit Ethernet does not support VLAN definition
B. 10 Gigabit Ethernet supports full duplex links, but does not support half duplex links.
C. 10 Gigabit Ethernet supports unshielded or shielded twisted-pair cable connections
D. 10 Gigabit Ethernet supports Carrier Sense Multiple Access with Collision Detection (CSMA/CD).
E. 10 Gigabit Ethernet supports optical fiber connections in single mode only. Multi mode is not supported.

Answer: B,C
Explanation:

QUESTION NO: 164

What does the protocol field inside the PPP frame indicate?

A. the protocol used to determine the authentication method
B. the protocol used to identify the data in the Information field
C. the protocol used to carry the PPP frame
D. the protocol used to decode the FCS field
E. the protocol used to detect the number of padding bytes

Answer: B
Explanation:
The Protocol field indicates the type of payload packet (e.g. LCP, NCP, IP, IPX, AppleTalk, etc.). The Information field contains the PPP payload; it has a variable length with a negotiated maximum called the Maximum Transmission Unit. By default, the maximum is 1500 octets. It might be padded on transmission; if the information for a particular protocol can be padded, that protocol must allow information to be distinguished from padding.

QUESTION NO: 165

Which statement about the Link Control Protocol (LCP) is true?

A. LCP is used for basic PPP link setup and operation.
B. LCP is used for PPP CHAP authentication.
C. LCP is used for PPP over ATM (PPPoA) setup.
D. LCP is used for PPP over Ethernet (PPPoE) setup.
E. LCP is used for PPP over Frame Relay (PPPoFR) setup.

Answer: A

Explanation:

The LCP protocol:

Checks the identity of the linked device and either accepts or rejects the device determines the acceptable packet size for transmission searches for errors in configuration can terminate the link if requirements exceed the parameters.

QUESTION NO: 166

Which four of these statements are restrictions for Frame Relay PVC bundles with QoS support for IP and MPLS? (Choose four)

A. A PVC bundle will not come up unless all the precedence, DSCP, and EXP levels are configured in the bundle.
B. A PVC bundle can perform precedence and DSCP matching at the same time
C. A PVC bundle may contain no more than sixteen PVCs
D. A PVC can be in only one PVC bundle
E. A PVC bundle cannot perform precedence and DSCP matching at the same time.
F. A PVC bundle may contain no more than eight PVCs.

Answer: A,D,E,F
Explanation:
Reference:

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ft_frbnd.html#wp1027175

Restrictions for Frame Relay PVC Bundles with QoS Support for

IP and MPLS

• A PVC can be a part of one and only one PVC bundle.

• A PVC bundle may contain no more than eight PVCs.

• A PVC that is a bundle member cannot be used in any other capacity, For example a PVC bundle member cannot be configured in a map statement.

• A PVC bundle cannot perform precedence and DSCP matching at the same time. If the wrong matching scheme is configured, unpredictable behavior will result.

• A PVC bundle will not come up unless all the precedence, DSCP, or EXP levels are configured in the bundle.

• Voice over Frame Relay (VoFR) is not supported on PVC-bundle members.

• Fast switching over Frame Relay PVC bundles is not supported.

QUESTION NO: 167

What is the purpose of Dual Ring Interconnect with D C for SDH rings?

A. Protects signals when a ring switch fails
B. Protects signals when multiple span switches fail
C. Protects pre-emptible traffic from being dropped when a ring switch occurs
D. Protects signals against any combination of link failure in each ring

Answer: D
Explanation:

QUESTION NO: 168

What is the function of the AJB bits on DS1 using Extended Super Frame (ESF)?

A. It is used for signaling on-hook and off-hook status.
B. It carries CRC information for error detection.
C. It is used for a control and performance information.
D. It is used for a frame's synchronization and alignment.

Answer: A
Explanation:
DS1 frame synchronization[edit source | edit]

See also: Synchronization in telecommunications

Frame synchronization is necessary to identify the timeslots within each 24-channel frame.

Synchronization takes place by allocating a framing, or 193rd, bit. This results in 8 kbit/s of framing

data, for each DS1.

Because this 8-kbit/s channel is used by the transmitting equipment as overhead, only 1.536 Mbit/s is actually passed on to the user. Two types of framing schemes are Super Frame (SF) and Extended Super Frame (ESF). A Super Frame consists of twelve consecutive 193-bit frames, whereas an Extended Super Frame consists of twenty-four consecutive 193-bit frames of data. Due to the unique bit sequences exchanged, the framing schemes are not compatible with each other. These two types of framing (SF, and ESF) use their 8 kbit/s framing channel in different ways.

QUESTION NO: 169

Which statement is FALSE concerning Concatenation?

A. It allows ITCM to send multiple upstream packets in one single large burst.
B. It reduces upstream data throughput.
C. It can be enabled/disabled from CMTS on per upstream port basis if desired
D. Concatenation activity on an interface can be checked by the show controller counters command

Answer: B
Explanation:

QUESTION NO: 170

What features set is most frequently used to prevent hackers from flooding a port with MAC-addresses?

A. BPDU Guard
B. 802.x
C. Port Security
D. Storm Control

Answer: C
Explanation:

QUESTION NO: 171

What does UDLD stand for?

A. UniDirectional Loop Detection
B. Unspecified Distribution Label Detection
C. Unified Distribution Label Direction
D. UniDirectional Link Detection

Answer: D
Explanation:

QUESTION NO: 172

What is the statistical reserve?

A. Bandwidth that is reserved for SVCs to route over a trunk
B. Bandwidth that is reserved on a trunk so that ABR connections can burst
C. Bandwidth on a trunk that is reserved for control traffic and cannot be used by connections
D. Bandwidth that cannot be allocated to connections but can be used to accommodate statistical variations in the traffic

Answer: D
Explanation:

QUESTION NO: 173

Which of the following is reported in the LMI regular status polling? (Choose three.)

A. Addition or Deletion of PVC.
B. PVC status (active or inactive).
C. Link integrity.
D. None of the other alternatives apply.

Answer: A,B,C
Explanation:

QUESTION NO: 174

ATM carries IP and PPP information with ATM cells. What ATM adaptation Layer is used when an

ATM cell carries IP packets and PPP frames?

A. AAU2
B. AAL3
C. AAL4
D. AAL5

Answer: D
Explanation:

QUESTION NO: 175

Which two of the following are designated fields for MAC tunneling protocol (802.1ah)?

A. Control Word
B. Tunnel Label
C. 802.1q VLAN TAG
D. ISL
E. Service Ethertype
F. PseudoLAN TAG

Answer: E,F
Explanation:

QUESTION NO: 176

Assume two routers on the same subnet, R1 and R2, both configured for HSRP. R1 has a priority of 120. Which of the following HSRP interface configurations will always result in the R2 becoming the primary? (Choose two.)

A. standby 1 priority 120
B. standby 1 priority 130 preempt
C. standby 1 priority 130
D. standby 1 priority 120 preempt
E. standby 1 priority 110 preempt
F. standby 1 priority 110

Answer: B,C
Explanation:

QUESTION NO: 177

Select the 3 best answers describing operation and configuration of Frame-Relay Inverse ARP.

A. Dynamic address mapping uses Frame Relay Inverse ARP to request the next-hop protocol address for a specific connection on its known DLCI.
B. Responses to Inverse ARP requests are entered in an address-to-DLCI mapping table on the router or access server which is used to supply the next-hop protoco address or the DLCI for outgoing traffic.
C. Inverse ARP is enabled by default for all protocols enabled on the physical interface.
D. Inverse ARP is configured using the following command under the Interface configuration 'frame-relay mapdlci (dlci number) protocol protocol-address'.
E. Inverse ARP in Frame-Relay is synonymous of ARP in Ethernet.

Answer: A,B,C
Explanation:

QUESTION NO: 178

What are the benefits of using TCAM technology in high-end routing products? (Choose two.)

A. Simplified configuration
B. Lower maintenance cost
C. Deterministic performance
D. Longer uptime
E. Lower power consumption

Answer: C,D
Explanation:

QUESTION NO: 179

Which two statements best describe EtherChannel? (Choose two).

A. EtherChannel technology helps aggregate traffic grouping multiple, full-duplex point-to-point links together
B. EtherChannel technology is based on the 802.1 IEEE stand
C. EtherChannel can aggregate up to 800 Mbps,8 Gbps,or 80Gbps of aggregate bandwidth for a

Fast EtherChannel, Gigabit EtherChannel,or 10 Gigabit EtherChannel connection respectively.

D. EtherChannel is defined for Rapid Spanning Tree for faster convergence.

Answer: A,C

Explanation:

QUESTION NO: 180

Which two things are correct about QinQ technology? (Choose two.)

A. The Outer.1Q tag represents customer VLAN ID and inner.1Q tag represents Service Provider VLAN (PVLAN)

B. It is an effective way to achieve VLAN transparency between Provider and enterprise customer by tunneling one ser of VLAN tags inside a second VLAN tag

C. The Outer.1Q tag represents Service Provider VLAN (PVLAN) and inner.1Q tag represents customer VLAN

D. QinQ is a way to hide native VLAN which can conflict with Provider native VLAN

Answer: B,C

Explanation:

IEEE 802.1ad[note 1] is an Ethernet networking standard informally known as IEEE 802.1QinQ[by whom?] and is an amendment to IEEE standard IEEE 802.1Q-1998. The technique is also known as provider bridging, Stacked VLANs, or simply QinQ or Q-in-Q. "Q-in-Q" can for supported devices apply to C-tag stacking on Ctag (Ethernet Type = 0x8100) but this has limited application in the modern methodology of network routing.

The original 802.1Q specification allows a single Virtual Local Area Network (VLAN) header to be inserted into an Ethernet frame. QinQ allows multiple VLAN headers to be inserted into a single frame, an essential capability for implementing Metro Ethernet network topologies. Just as QinQ extends 802.1Q, QinQ itself is extended by other Metro Ethernet protocols.[specify]

In a multiple VLAN header context, out of convenience the term "VLAN tag" or just "tag" for short is often used in place of "802.1Q VLAN header". QinQ allows multiple VLAN tags in an Ethernet frame; together these tags constitute a tag stack. When used in the context of an Ethernet frame, a QinQ frame is a frame that has 2 VLAN 802.1Q headers (double-tagged).

There is a mild confusion regarding the naming because the 802.1ad standard was grown out of the 802.1QinQ[citation needed] protocol (which was developed based the trademarked method 802.1Q, with capital "Q" as a distinction instead of the 802.1q as the standardised protocol) which originally used 0x8100 as ethernet type instead of 0x88a8. While the network industry usually mix the naming, the proper, standardized name is 802.1ad which sometimes gets appended by the other alternative names mentioned above; the plain "802.1QinQ"[citation needed] name usually refers to the old standard which is now[when?] considered obsolete.

QUESTION NO: 181

In the context of GMPLS, LMP stands for:

A. Load Management Protocol
B. Label Management Protocol
C. Loop Management Protocol
D. Link Management Protocol

Answer: D
Explanation:

The Generalized Multi-Protocol Label Switching (GMPLS)[1] is a protocol suite extending MPLS to manage further classes of interfaces and switching technologies other than packet interfaces and switching, such as time division multiplex, layer-2 switch, wavelength switch and fiber-switch. GMPLS is composed of three main protocols:
Resource Reservation Protocol with Traffic Engineering extensions (RSVP-TE) signaling protocol.[5][6]Open Shortest Path First with Traffic Engineering extensions (OSPF-TE) routing protocol.[7][8] Link Management Protocol (LMP).[9]

QUESTION NO: 182

GMPLS is based upon:

A. VPI/VCI-based switching devices
B. Non-Packet-based devices
C. Packet-based switching devices
D. None of the above

Answer: B
Explanation:
The Generalized Multi-Protocol Label Switching (GMPLS)[1] is a protocol suite extending MPLS to manage further classes of interfaces and switching technologies other than packet interfaces and switching, such as time division multiplex, layer-2 switch, wavelength switch and fiber-switch.

GMPLS is composed of three main protocols:

Resource Reservation Protocol with Traffic Engineering extensions (RSVP-TE) signaling protocol.[5][6]

Open Shortest Path First with Traffic Engineering extensions (OSPF-TE) routing protocol.[7][8]

Link Management Protocol (LMP).[9]

QUESTION NO: 183

The layer 2 protocol used by POS technology offers a standardized way for mapping IP packets into SONET/ SDH payloads. Select the correct sequence of POS operation:

1) Data is scrambled and synchronous mapping takes place by octet into the SONET/SDH frame.

2) Encapsulated via Point-to-Point Protocol (PPP) takes place framing information is added with High-level

Data Link Control (HDLC).

3) Gaps between frames are filled with flags, set to value 7E.

4) Octet stuffing occurs if any flags or resultant escape characters (of value 7D) are found in the data.

5) Data is segmented into an IP datagram with its 20-byte IP header.

A. 1, 3, 4, 5, 2
B. 5, 2, 3, 1, 4
C. 2, 3, 5, 4, 1
D. 5, 2, 3, 4, 1
E. 1, 2, 3, 4, 5

Answer: D
Explanation:

The proper order of operation of PoS is:
When transmitting:
IP -> PPP -> FCS generation -> Byte stuffing -> Scrambling -> SONET/SDH framing
When receiving:
SONET/SDH framing -> Descrambling -> Byte destuffing -> FCS detection -> PPP -> IP
Remote

Topic 3, D&I&O&T Remote Access Technologies

QUESTION NO: 184

Which two routers support cable access? (Choose two.)

A. ME3000
B. uBR10000
C. ASR9000
D. CRS-1
E. ME3600
F. uBR7200

Answer: B,F
Explanation:
Cisco uBR10000 Series Universal Broadband Routers
Cisco uBR7200 Series Universal Broadband Routers

QUESTION NO: 185

In PPPoA architecture, which two methods are most commonly deployed? (Choose two)

A. Terminating PPP sessions at the service provider
B. PPP framing
C. PPP multiplexing
D. GRE tunneling
E. L2TP tunneling

Answer: A,E
Explanation:
Reference:

http://www.cisco.com/en/US/tech/tk175/tk819/technologies_white_paper09186a0080093bd2.shtml

In PPPoA architectures, the service destination can be reached in different ways. Some of the most commonly deployed methods are:

Terminating PPP sessions at the service provider

L2TP Tunneling

Using SSG

QUESTION NO: 186

Which are three advantages of PPPoA implementation? (Choose three)

A. NAP and NSP provide secure access to corporate gateways without managing end-to-end PVCs. NAP and NSP use Layer 3 routing, Layer 2 Forwarding, or Layer 2 Tunneling Protocol tunnels. Hence, they can scale their business models for selling wholesale service.
B. The NSP can oversubscribe by deploying idle and session timeouts using an industry standard RADIUS server for each subscriber.
C. Only a single session per CPE on one virtual channel (VC). The username and password are configured on the CPE, so all users behind the CPE for that particular VC can access only one set of services. Users cannot select different sets of services, although using multiple VCs and establishing different PPP session on different VCs is possible.
D. If a single IP address is provided to the CPE, and NAT or PAT is implemented, certain pplications such as IPTV, which embed IP information in the payload, well not work. Additionally, if an IP subnet feature is used, an IP address also has to be reserved for the CPE.
E. PPPoA can use the features on the Cisco Service Selection Gateway (SSG)

Answer: A,B,E
Explanation:
Advantages:
Per session authentication based on Password Authentication Protocol (PAP) or Challenge Handshake
Authentication Protocol (CHAP). This is the greatest advantage of PPPoA as authentication overcomes the security hole in a bridging architecture.
Per session accounting is possible, which allows the service provider to charge the subscriber based on session time for various services offered. Per session accounting enables a service provider to offer a minimum access level for minimal charge and then charge subscribers for additional services used.
IP address conservation at the CPE. This allows the service provider to assign only one IP address for a CPE, with the CPE configured for network address translation (NAT). All users behind one CPE can use a single IP address to reach different destinations. IP management overhead for the Network Access Provider/Network Services Provider (NAP/NSP) for each individual user is reduced while conserving IP addresses. Additionally, the service provider can provide a small subnet of IP addresses to overcome the limitations of port address translation (PAT) and NAT.
NAPs/NSPs provide secure access to corporate gateways without managing end-to-end PVCs

and using Layer 3 routing or Layer 2 Forwarding/Layer 2 Tunneling Protocol (L2F/L2TP) tunnels. Hence, they can scale their business models for selling wholesale services.

Troubleshooting individual subscribers. The NSP can easily identify which subscribers are on or off based on active PPP sessions, rather than troubleshooting entire groups as is the case with bridging architecture. The NSP can oversubscribe by deploying idle and session timeouts using an industry standard Remote Authentication Dial-In User Service (RADIUS) server for each subscriber. Highly scalable as we can terminate a very high number of PPP sessions on an aggregation router. Authentication, authorization, and accounting can be handled for each user using external RADIUS servers. Optimal use of features on the Service Selection Gateway (SSG).

Disadvantages:

Only a single session per CPE on one virtual channel (VC). Since the username and password are configured on the CPE, all users behind the CPE for that particular VC can access only one set of services. Users cannot select different sets of services, although using multiple VCs and establishing different PPP sessions on different VCs is possible.

Increased complexity of the CPE setup. Help desk personnel at the service provider need to be more knowledgeable. Since the username and password are configured on the CPE, the subscriber or the CPE vendor will need to make setup changes. Using multiple VCs increases configuration complexity. This, however, can be overcome by an autoconfiguration feature which is not yet released.

The service provider needs to maintain a database of usernames and passwords for all subscribers. If tunnels or proxy services are used, then the authentication can be done on the basis of the domain name and the user authentication is done at the corporate gateway. This reduces the size of the database that the service provider has to maintain.

If a single IP address is provided to the CPE and NAT/PAT is implemented, certain applications such as IPTV, which embed IP information in the payload, will not work. Additionally, if an IP subnet feature is used, an IP address also has to be reserved for the CPE.

QUESTION NO: 187

Which four of these key points should be considered during implementation of PPPoA architecture? (Choose four)

A. The number of subscribers that will be serviced currently and in the future because this affects the number of required PPPoA sessions
B. The types of applications that the NSP offers to the end subscriber

C. The capacity of ATM and Frame Relay interworking on the NSP

D. In the case of more than one user, whether all users need to reach the same final destination or service, or they all have different service destinations

E. Whether the service provider or the final service destination is providing the IP address to the CPE of the subscriber

Answer: A,B,D,E

Explanation:

Implementation Considerations for PPPoA Architecture

The number of subscribers that will be serviced currently and in the future, as this affects the number of required PPP sessions.

Whether the PPP sessions are being terminated at the service provider aggregation router or forwarded to other corporate gateways or Internet Service Providers (ISPs).

Whether the service provider or the final service destination is providing the IP address to the subscriber's CPE.

Whether the IP addresses provided are legal public or private. Is the CPE going to do NAT/PAT or will NAT be performed at the termination destination?

Profiles of end subscribers, residential users, small office home office (SOHO) customers,and telecommuters.

In the case of more than one user, whether all users need to reach the same final destination or service, or they all have different service destinations.

Is the service provider providing any value added services like voice or video? Does the service provider require all subscribers to first go to a particular network before reaching a final destination? When subscribers use SSG, are they going to use passthrough services, PPP Terminated Aggregation (PTA), a mediation device, or proxy?

How the service provider bills subscribers—based on a flat rate, per session usage, or services used.

Deployment and provisioning of CPEs, DSLAMs and aggregation points of presence (POPs).

The business model for the NAP. Does the model also include selling wholesale services like secure corporate access and value added services like voice and video? Are NAPs and NSPs the same entity?

The business model of the company. Is it comparable to an independent local exchange carrier (ILEC), a competitive local exchange carrier (CLEC) or an ISP?

The types of applications the NSP will offer to the end subscriber.

The anticipated upstream and downstream volume of data flow.

Keeping these points in mind, we will discuss how the PPPoA architecture will fit and scale to different business models for service providers and how the providers can benefit using this architecture.

QUESTION NO: 188

Which three of these statements about PPPoE are true? (Choose three.)

A. PPPoE can provide a host with access to a destination over Ethernet. You can have only one PPPoE session per PVC.
B. You must install PPPoE client software on all hosts that connect to the Ethernet segment. This means that the access provider must maintain a CPE.
C. You cannot use PPPoE with Cisco Service Selection Gateway.
D. PPPoE implementation is susceptible to broadcast storms and possible denial-of-service attacks.
E. Per-session accounting is possible, which allows the service provider to charge the subscriber based on session time for various services offered. The service provider can also require a minimum access charge.

Answer: B,D,E
Explanation:

QUESTION NO: 189

In a cable HFC plant, what is a modulator?

A. Set top box
B. Diplex filter
C. Local head end
D. Fiber node

Answer: A
Explanation:

QUESTION NO: 190

What is the effect of turning on all available downstream carrier tones in a DMT DSL transmission systems?

A. Downstream RS error correction effectiveness is reduced.
B. The downstream line rate and throughput remains unchanged, but FEC efficiency is reduced.
C. The upstream DSL bandwidth is reduced, since less carriers become available for upstream

traffic.
D. The downstream DSL bandwidth is increased.

Answer: D
Explanation:

QUESTION NO: 191

During the modem boot process, how does the modem acquire the downstream channel?

A. The modem is commanded by the CMTS to set to the specific channel.
B. The modem uses the default value in the broadcom chipset.
C. The modem tuner sets a level as defined by the DOCSIS specification.
D. The modem tuner scans the downstream spectrum until digital QAM modulated signal is encountered

Answer: D
Explanation:

QUESTION NO: 192

What is the effect of changing DMT interleaved delay from 3 milliseconds to 15 milliseconds?

A. Latency remains the same, but throughput is decreased.
B. Latency remains the same, but error correction effectives may also be reduced.
C. Latency is increased, but faster error correction occurs.
D. Fewer ATM PVCs can be provisioned on DSL line.

Answer: C
Explanation:

QUESTION NO: 193

Typical ADSL broadband Internet access requires a username and password to be entered on end-user PC connected to the ADSL modem in order for the end user to gain access to the Internet. If a Cisco ADSL router is used instead of an ADSL modem, what functionality is required on the Cisco ADSL router so the end-user connected to the Cisco ADSL router can access the Internet without entering a username and password?

A. Route Bridge Encapsulation (RBE)
B. PPPoA
C. Integrated Routing and Bridging (IRB)
D. AAA
E. PPPoE client

Answer: E
Explanation:

QUESTION NO: 194

In Ethernet Aggregation application which option is needed when the U-PE connects to an N-PE and broadband remote access servers?

A. Ethernet Multipoint Service (EMS)
B. VPLS
C. E1
D. Wire Service

Answer: A
Explanation:

Topic 4, I&O&T Layer 3 VPN

QUESTION NO: 195

Option 10C is an implementation of Inter-AS MPLS VPN. Which two statements about Option 10C are true? (Choose two.)

A. Great scalability is offered
B. Route Target Rewrite must be configured on ASBRs
C. Multihop EBGP is utilized between route reflectors
D. Multihop EBGP is utilized between ASBRs
E. The ASBRs hold VPNv4 routes

Answer: A,C
Explanation:

QUESTION NO: 196

Which four statements about the Carrier Supporting Carrier (CSC) feature are true? (Choose four.)

A. MPLS is required between the PE and CE routers that connect the backbone carrier to the customer carrier.
B. The backbone carrier must enable the PE router to check that the packets it receives from the CE router contain only the labels that the PE router advertised to the CE router.
C. Every packet that crosses the backbone carrier must be encapsulated so that the packet includes MPLS labels
D. AII PE routers that link the backbone carrier to the customer carrier must run Route Target Rewrite.
E. A routing protocol is required between the PE and CE routers that connect the backbone carrier to the customer carrier. The routing protocol enables the customer carrier to exchange IGP routing information with the backbone carrier.

Answer: A,B,C,E
Explanation:

QUESTION NO: 197

In the Carrier Supporting Carrier (CsC) feature, which two protocols run between CSC-PE and CSC-CE. (Choose two)

A. IGP and RSVP
B. EBGPv4 with a sending community
C. IGP and EBGPv4
D. IGP and LDP
E. EBGPv4 with a sending label

Answer: D,E
Explanation:

QUESTION NO: 198

Option 10A (back-to-back VRF) is an implementation of inter-AS MPLS VPN. Which of four statements about option 10A are not true? (Choose four.)

A. MPLS is required between the ASBRs.

B. ASBR must hold all routing information.

C. It is a scalable solution.

D. It is a simple solution.

E. MP-EBGP is used to exchange routes between ASBRs.

Answer: A,C,D,E

Explanation:

QUESTION NO: 199

Identify the differences of option 10A, as opposed to option 10C, for interAS vpn offerings For option 10A? (Choose three).

A. Greater scalability is offered

B. The ASBR holds VPNv4 routes

C. Relative technical simplicity is offered

D. Lower relative security is offered

E. Multihop eBGP between ASBRs is utilized

F. Better suitability for InterProvider VPNs is provided

Answer: B,C,F

Explanation:

QUESTION NO: 200

Which two features prevent routing loops between the OSPF sites of a customer when the sites are multihomed or a backdoor link is used between the sites? (Choose two.)

A. sham link

B. down bit

C. virtual link

D. Site of Origin

E. domain tag

Answer: B,E

Explanation:

If a route sent from a PE router to a CE router could then be received by another PE router from one of its own CE router, there are chances of routing loops. This situation is possible when a "backdoor link" connects two CE routers connected to two different PE routers.

To prevent this, the PE sets the DN bit in any LSA that it sends to the CE router. If the PE router receives any LSA with DN bit set, it ignores the LSA.

1) DN bit:

When a PE router sends a Type-3 LSA to a CE router, the DN bit in LSA Options field must be set. Now if the CE router sends the Type-3 LSA to other PE router(s), the PE router will not redistribute it further.

When a PE router needs to distribute a route to a CE router which comes from the outside of CE router's OSPF domain, the PE router presents itself as an ASBR and distributes the route in Type-5 LSA. The DN bit must be set in the LSA.

The Options field is present in all LSAs. The Options field is 1-byte long as follows-
DN O DC EA N/P MC E MT
2) Route Tags (Domain Tags):

In some implementations (where DN bit is not set), Domain Tags (named by Cisco) are used to ensure Type-5
LSAs generated by a PE router will be ignored by other PE routers that may receive it.
The value of Domain tag is configurable and arbitrary if not set. Hence must be distinct from other OSPF tags

QUESTION NO: 201

Which IOS features are used to avoid Routing loops when dynamic Routing protocols are used between PE and CE in MPLS-VPN networks? (Choose two)

A. BGP cost community
B. BGP feature allow-as in
C. Access-list Control in Distance Vector protocol like RIP and EIGRP.
D. SHAM links with OSPF
E. RPF Reverse Path forwarding.
F. Site Of Origin SOO.

Answer: C,F
Explanation:

QUESTION NO: 202
If the OSPF protocol is used to connect customer edge (CE) routers to service provider edge (PE)

routers in the VPN backbone, which two options best describe the use of SHAM links?

A. A sham-link is created between any two VPN sites that belong to the same OSPF area and share an OSPF backdoor link
B. A sham-link is seen as an intra-area link between PE routers, an OSPF adjacency is created and database is exchanged
C. A sham-link is created between two directly connected PE routers so that it is preferred over the low speed backdoor door
D. A sham-link is part of OSPF network of MPLS-VPN provider.

Answer: A,B
Explanation:

QUESTION NO: 203

What is the proper MP-BGP configuration between the shown PE routers to implement MPLS VPNs on PER2?
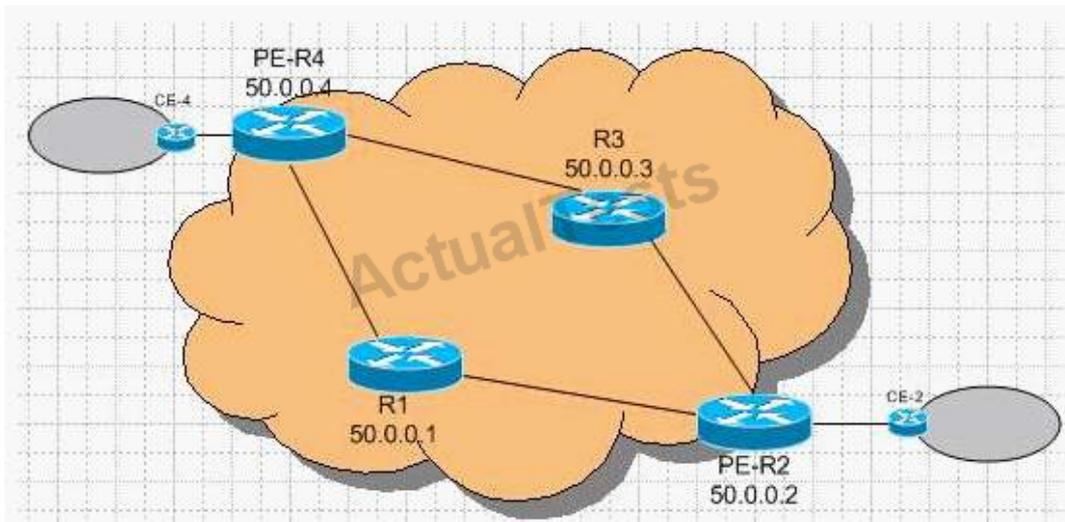
A. None of the above
B. router bgp 1
neighbor 50.0.0.4 remote-as 1
neighbor 50.0.0.4 update-source Loopback0
no auto-summary
!
address-family ipv4
neighbor 50.0.0.4 activate
neighbor 50.0.0.4 send-community extended
exit-address-family
C. router bgp 1

neighbor 50.0.0.4 remote-as 1
neighbor 50.0.0.4 update-source Loopback0
no auto-summary
!
address-family vpnv4
neighbor 50.0.0.4 activate
neighbor 50.0.0.4 send-community extended
exit-address-family
D. router bgp 1
neighbor 50.0.0.4 remote-as 1
neighbor 50.0.0.4 update-source Loopback0
no auto-summary
!
address-family vpnv4 unicast multicast
neighbor 50.0.0.4 activate
neighbor 50.0.0.4 send-community extended
exit-address-family

Answer: C
Explanation:

QUESTION NO: 204

Refer to the exhibit.
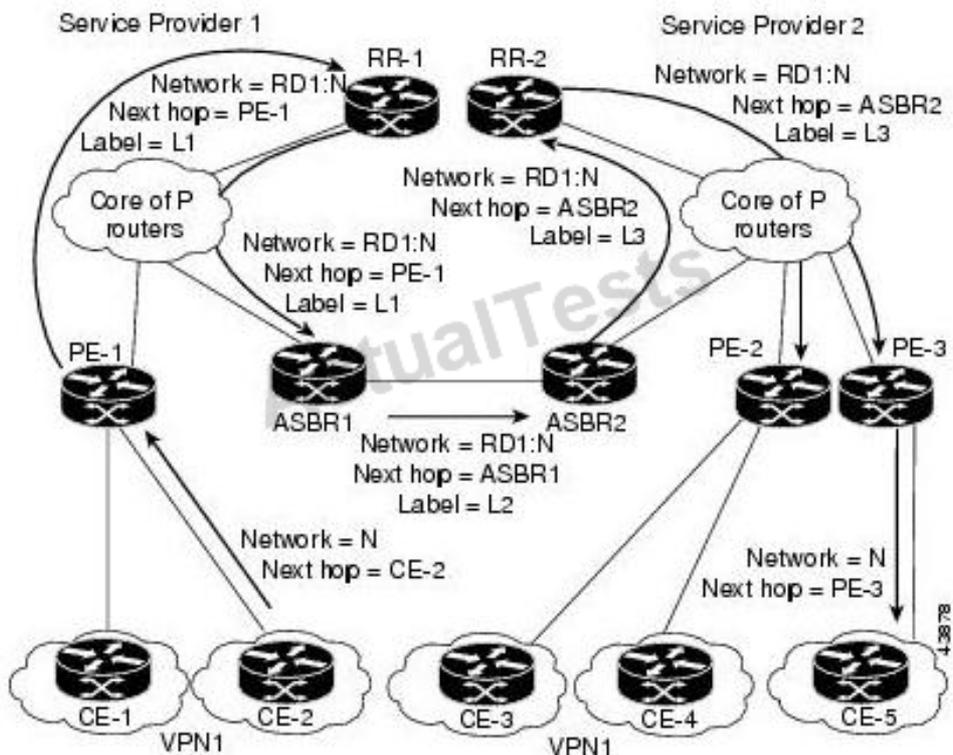
The exhibit illustrates the exchange of VPN route and label information between MPLS VPN inter-AS. The exhibit also shows ASBRs exchanging VPN-IPv4 addresses.

Which command is needed to change the next-hop address when ASBR2 is not configured?

A. Redistribute command with the BGP routing process
B. Redistribute command with connected
C. Redistribute command with the IGP routing process
D. Redistribute command with static

Answer: B

Explanation:

Figure 11-3 illustrates the exchange of VPN route and label information between autonomous systems. The only difference is that ASBR2 is configured with the redistribute connected command, which propagates the host routes to all PEs. The redistribute connected command is necessary because ASBR2 is not the configured to change the next hop address.

Figure 11-3 Host Routes Propagated to All PEs Between Two Autonomous Systems
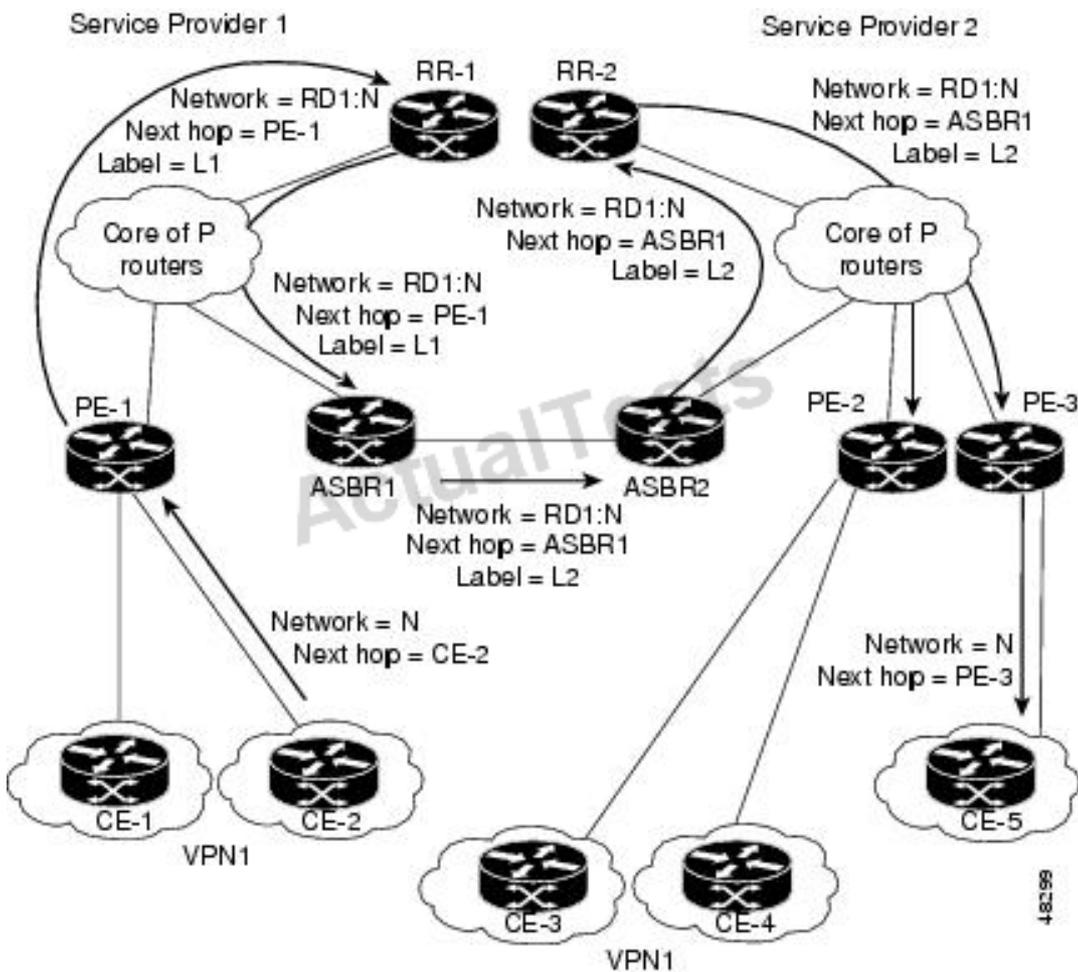
Reference:

http://www.cisco.com/en/US/docs/net_mgmt/ip_solution_center/4.0/mpls/user/guide/11_isc.html

QUESTION NO: 205

When configuring Multicast VPN (MVPN) over an MPLS core, both the Default and Data MDT is configured under which configuration mode?

A. router(config-router)#
B. router(config)#
C. router(config-router-af)#
D. router(config-if)#
E. router(config-vrf)#

Answer: E
Explanation:

QUESTION NO: 206

In Multicast VPN (MVPN) implementations, which two of the following statements are regarding the Default MDT Group? (Choose two).

A. It is used for PIM control traffic.
B. It is optionally configured for a high bandwidth multicast source to reduce multicast traffic replication to uninterested PE routers.
C. Within the VRF configuration in the PE router, multiple Default MDT groups are configured so each VRF can support multiple multicast sources.
D. There is a reduced multicast state in the MPLS core P routers.
E. When multicast traffic exceeds a certain configured threshold, traffic from the Data MDT is switched to the
Default MDT to conserve bandwidth.

Answer: A,D
Explanation:
MVPN supports two MDT types:
•Default MDT—The default MDT is a permanent channel for PIM control messages and low-bandwidth streams between all PE routers in a particular multicast domain. All multicast traffic in the default MDT is replicated to every other PE router in the domain. Each PE router is logically

seen as a PIM neighbor (one hop away) from every other PE router in the domain.

•Data MDT—Data MDTs are optional. If enabled, they are dynamically created to provide optimal paths for high-bandwidth transmissions, such as full-motion video, that do not need to be sent to every PE router. This allows for on-demand forwarding of high-bandwidth traffic between PE routers, so as to avoid flooding every PE router with every high-bandwidth stream that might be created.

QUESTION NO: 207

In relation to MPLS Multicast VPN, which three statements about multicast distribution (MDT) groups are true? (Choose three)

A. Default MDT groups are used for PIM control traffic, low-bandwidth sources, and flooding of sparse mode traffic.
B. MDTs are built in customer networks
C. Data MDT groups are used for high-bandwidth sources to reduce replication to uninterested PEs.
D. MDTs are built in provider networks
E. The number of MDTs depends on PIM modes of MDT groups.

Answer: C,D,E
Explanation:
•Default-MDT

Tree created by the MVPN configuration. The Default-MDT is used for customer Control Plane and low rate Data Plane traffic. It connects all of the PE routers with MVRFs in a particular MD and one will exist in every MD whether there is any active source in the respective customer network.

QUESTION NO: 208

Which statement about multicast VPN is true?

A. The MDT group address should be the same for both address families in the same VRF.
B. The MDT group address should be the same for both address families in the different VRFs.
C. Configuration of the MDT source on a pre-VRF basis is supported only on IPv6.
D. The MDT group address should be different for both address families in the same VRF.

Answer: A

Explanation:

Restrictions for Multicast VPN for Multicast Routing

· Configuration of the MDT source on a per-VRF basis is only supported on IPv4. · The MDT group address should be the same for both the address families in the same VRF.

Default-MDTs must have the same group address for all VRFs that comprise a MVPN. Data-MDTs may have the same group address if PIM-SSM is used. If PIM-SM is used, they must have a different group address, as providing the same one could result in the PE router receiving unwanted traffic. This is a PIM-SM protocol issue, not an implementation issue.

QUESTION NO: 209

Which statement about the use of Route Target Rewrite is true?

A. It is mainly used in Intra-AS MPLS VPN deployments and is configured at the ASBR to avoid misconfiguration of the Route Target assignment for VPN configurations.
B. It is mainly used in Inter-AS MPLS VPN deployments and is configured at the ASBR to avoid misconfiguration of the Route Target assignment for VPN configurations.
C. It is mainly used in Intra-AS MPLS VPN deployments and is configured at the Router Reflector to avoid misconfiguration in Route Target assignment for VPN configurations
D. It is mainly used in Inter-AS MPLS VPN deployments and is configured at the Router Reflector to avoid misconfiguration of the Route Target assignment for VPN configurations
E. It is mainly used in Inter-AS MPLS VPN deployments and is configured at the PE router to avoid to misconfiguration of the Route Target assignment for VPN configurations

Answer: B

Explanation:

The MPLS VPN—Route Target Rewrite feature allows the replacement of route targets on incoming and outgoing Border Gateway Protocol (BGP) updates. Typically, Autonomous System Border Routers (ASBRs) perform the replacement of route targets at autonomous system boundaries. Route Reflectors (RRs) and provider edge (PE) routers can also perform route target replacement. The main advantage of the MPLS VPN - Route Target Rewrite feature is that it keeps the administration of routing policy local to the autonomous system.

QUESTION NO: 210

Which statements about the Route Target Rewrite feature are not true? (Choose two.)

A. After the route target replacement policy is applied to the target router, the BGP session need not be refreshed manually to put the policy into operation.
B. Route Target Rewrite allows the administration of the routing policy to stay local to the AS.
C. Route target replacement is always done by the ASBR.
D. Route target rewrites are supported for VRF export maps.
E. Route target replacement can be done on incoming and outgoing BGP updates.

Answer: A,C

Explanation:

The MPLS VPN—Route Target Rewrite feature allows the replacement of route targets on incoming and outgoing Border Gateway Protocol (BGP) updates. Typically, Autonomous System Border Routers (ASBRs) perform the replacement of route targets at autonomous system boundaries. Route Reflectors (RRs) and provider edge (PE) routers can also perform route target replacement.

The main advantage of the MPLS VPN - Route Target Rewrite feature is that it keeps the administration of routing policy local to the autonomous system.

QUESTION NO: 211

Which statement about implementing the Cisco IPv6 provider Edge Router over MPLS is true?

A. 6PE feature is supported over tunnels other than RSVP-TE tunnels.
B. Core MPLS routers are supporting IPv6 only.
C. 6PE feature is not supported over tunnels other than RSVP-TE tunnels.
D. Core MPLS routers are supporting IPv4 only.

Answer: C

Explanation:

ReferencE. http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-over_mpls.pdf
The following restrictions apply when implementing the IPv6 Provider Edge Router over MPLS (6PE) feature:
Core MPLS routers are supporting MPLS and IPv4 only, so they cannot forward or create any IPv6 Internet Control Message Protocol (ICMP) messages.
Load balancing ability is not provided by Cisco 6PE between an MPLS path and an IPv6 path. If both are available, the MPLS path is always preferred. Load balancing between two MPLS paths is possible. BGP multipath is not supported for Cisco 6PE routes. If two BGP peers advertise the same prefix with an equal cost, Cisco 6PE will use the last route to cross the MPLS core.

6PE feature is not supported over tunnels other than RSVP-TE tunnels.

QUESTION NO: 212

Assume that the PEs are separated by Multiple P routers.

How many labels should the ingress PE push for 6PE functionality?

A. 1
B. None
C. 3
D. 2
E. It depends on the numbers of hops between the ingress and egress PE.

Answer: D
Explanation:

A PE device on receiving the IPv6 prefix from CE by routing protocol will assign a label and advertise through BGP to other PE devices which in turn will be advertised to remote CE devices.

This label information will be used to switch the packet through MPLS cloud. 6PE implementation will have minimum 2 labels imposed, top label being the one to identify the remote PE while bottom label to identify the IPv6 prefix.

QUESTION NO: 213

Which option describes a benefits of IPv6 VPN Provider Edge?

A. Provider support for intra-AS and CSC scenarios
B. Uses separate signaling plane, which provides more security than IPv4
C. BGP is the preferred routing protocol for connecting two SPs.
D. No requirement for a separate signaling plane

Answer: D
Explanation:

QUESTION NO: 214

Which two statements about VPNv4 address are true? (Choose two.)

A. The VPNv4 address is 128 bits long with a 128-bit long subnet mask

B. The VPNv4 address consists of an RD and an IPv4 address.

C. The VPNv4 address is 96 bits long with a 64-bit long subnet mask.

D. The VPNv4 address is 128 bits long with a 64-bit long subnet mask.

E. The VPNv4 address consists of an RT and an IPv4 address.

F. The VPNv4 address is 96 bits long with a 32-bit long subnet mask

Answer: B,F

Explanation:

QUESTION NO: 215

Which two statements about Layer 3 MPLS VPN are true? (Choose two.)

A. The virtual routing and forwarding table is separate from the global routing table that exists on PE routers.
Routes are injected into the VRF from the CE-PE routing protocols for that VRF and any MP-BGP announcements that match the defined VRF RTs.

B. Multiprotocol Border Gateway Protocol is run between PE and CE routers to exchange customer prefixes in a VPNv4 format.

C. A customer edge router peers at Layer 3 to the provider edge. The PE-CE interface runs either a dynamic routing protocol (eBGP, RIPv2, EIGRP, OSPF) or a static routing protocol (Static, Connected).

D. VPNv4 address is the combination of the RT and customer IPv4 prefix. These VPNv4 prefixes are passed in MP-BGP.

Answer: A,C

Explanation:

QUESTION NO: 216

Which Cisco IOS command displays the export VPN route target value of a VRF?

A. show ip vrf all

B. show ip vrf route-targets all

C. show ip vrf summary

D. show ip vrf interfaces

E. show ip vrf detail

F. show ip vrf

Answer: E

Explanation:

The show ip vrf [{detail | interfaces}] vrf-name command shows detailed configurations about the VRF.

Pesaro# show ip vrf detail Customer_A

VRF Customer_A; default RD 100:101

Interfaces:

Loopback101 Loopback111

Connected addresses are not in global routing table

Export VPN route-target communities

RT:100:1001

Import VPN route-target communities

RT:100:1001

No import route-map

No export route-map

Pesaro# show ip vrf interfaces

Interface IP-Address VRF Protocol

Loopback101 200.0.6.1 Customer_A up

Loopback111 200.1.6.1 Customer_A up

Loopback102 200.0.6.1 Customer_B up

QUESTION NO: 217

Refer to the exhibit.

Which IPv6 deployment feature is displayed?

A. MPLS 6PE
B. MPLS 6VPE
C. 6 to 4 Replay Service
D. native IPv6 over MPLS
E. 6 to 4 Tunnel

121

Answer: B

Explanation:

IPv6 Provider Edge Router (6PE) over MPLS
IPv6 global connectivity over and IPv4-MPLS core
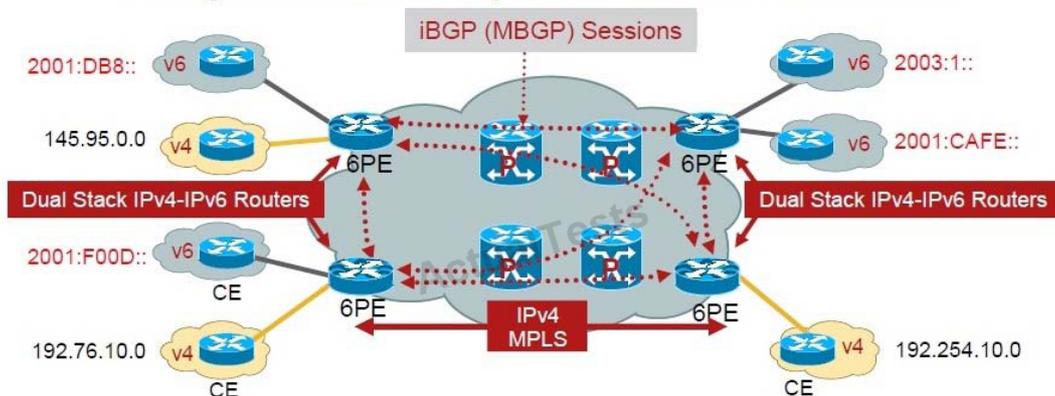
- 6PEs must support dual stack IPv4+IPv6 (6PE)
- IPv6 addresses exist in global table of PE routers only
- IPv6 reachability exchanged among 6PEs via iBGP (MP-BGP)
    - IPv6 AF (2) + Label SAFI (4) used to exchange prefixes between PEs
- IPv6 packets transported from 6PE to 6PE inside MPLS (label switching)
- Core uses IPv4 control plane (LDPv4, TEv4, IGPv4, MP-BGP)

6VPE: BGP-MPLS VPN extension for IPv6 (RFC 4659)
Layer-3 VPNs for IPv6 customers
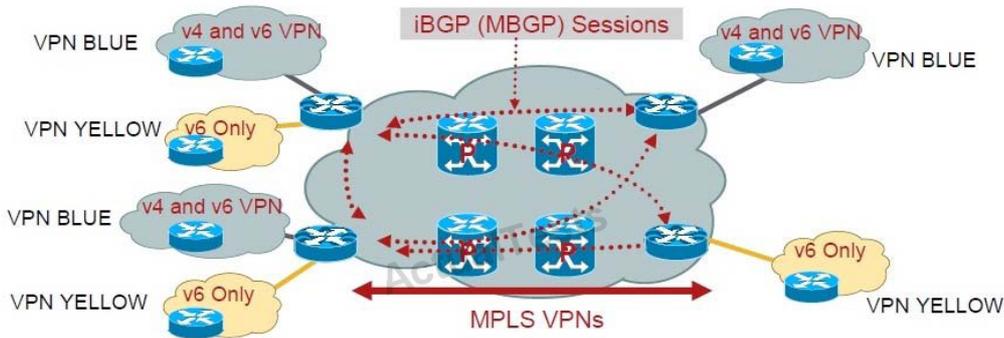
Apply all RFC4364bis mechanisms to IPv6 VPNs:
- IPv6-VPN reachability exchanged among PEs via MP-BGP
- New BGP address family: AFI=2 (IPv6"), SAFI=128 (VPN)
  - NLRI in the form of <length, VPN-IPv6-prefix, label>
  - 192bits Address (24 Byte) including the 64 bits route distinguisher (8 Bytes) and the 128 bits IPv6 address (16 Bytes)   **<RD:IPv6>**
  - Nexthop is carried as RD:v4-mapped-v6-address
- VRFs, RT, SOO, RRs,...operate exactly as with IPv4-VPN IPv6 packets

QUESTION NO: 218

Refer to the exhibit.
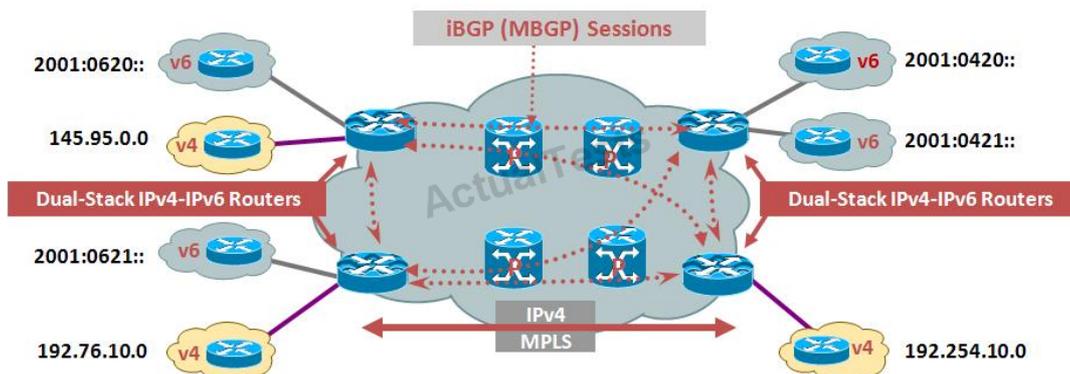
Which IPv6 deployment feature is displayed?

A. MPLS 6PE
B. MPLS 6VPE
C. 6 to 4 Replay Service
D. native IPv6 over MPLS
E. 6 to 4 Tunnel

Answer: A

Explanation:

QUESTION NO: 219

In which Cisco IOS configuration mode is the route distinguisher (RD) configured?

A. R1(config-route-at)#
B. R1(config-route-map)#
C. R1(config-it)#
D. R1(config-vrf)#
E. R1(config)#
F. R1(router)#

Answer: D

Explanation:

QUESTION NO: 220

Which three statements about the Route Distinguisher (RD) are true? (Choose three.)

A. The RD is a BGP extended community.
B. The RD prefix and a route target make the VPNv4 address unique.
C. RD, similar to the AS number, is assigned to a service provider by the Internet Assigned Numbers Authority (IANA).
D. The RD is an 8-byte field.
E. One customer may use different RDs for the same IPv4 route.

Answer: B,D,E

Explanation:

QUESTION NO: 221

Refer to the exhibit.
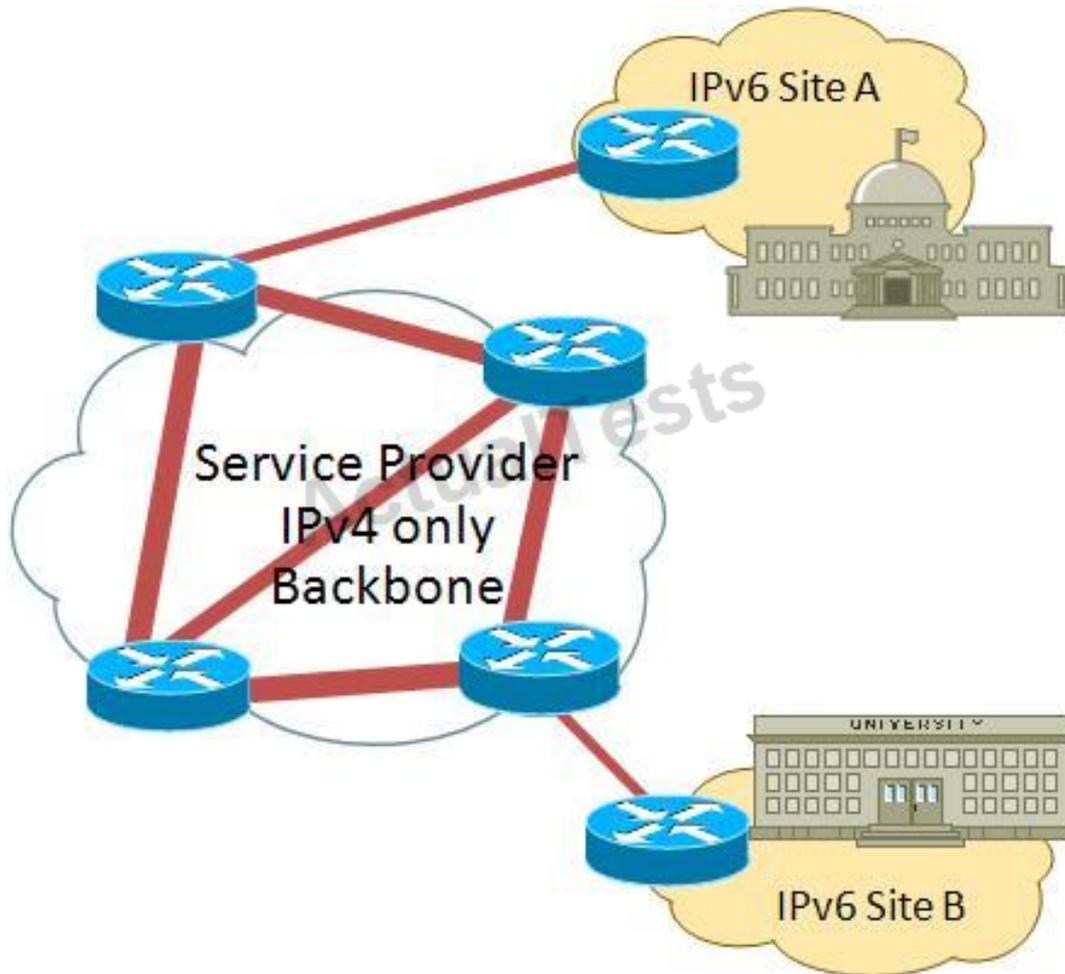
The service provider is an MPLS and IPv4 enabled network. Which two approaches can enable IPv6 tunneling between site A and site B over the backbone? (Choose two.)

A. IPv6 customer premise (6CP) over MPLS
B. IPv6 VPN provider edge (6VPE) over MPLS
C. IPv6 virtual forwarding (6VF) over MPLS
D. IPv6 forwarding instance (6FI) over MPLS
E. IPv6 provider edge router (6PE) over MPLS

Answer: B,E
Explanation:

QUESTION NO: 222

Which two requirements to deploy 6PE and 6VPE solutions are mandatory? (Choose two.)

A. MPLS is enabled on the core, distribution, and edge devices.
B. A triple stack is enabled on PE devices.

C. The network has at least six PE devices.

D. A dual stack is enabled on all the P and PE devices in a network.

Answer: A,D

Explanation:

http://www.cisco.com/en/US/docs/wireless/asr_901/Configuration/Guide/6pe_6vpe.html

QUESTION NO: 223

Which three of these are major components of an MPLS VPN network? (Choose three)

A. LDP notification

B. L2TPv3 session

C. VPN route target communities

D. Multiprotocol BGP peering of PE routers

E. MPLS forwarding

Answer: C,D,E

Explanation:

QUESTION NO: 224

Which statement about VPNv6 addresses is true?

A. The VPNv6 address is a 96-bit route distinguisher and a 128-bit IPv6 address

B. The VPNv6 address is a 64-bit route distinguisher and a 128-bit IPv6 address

C. The VPNv6 address is a 64-bit route distinguisher and a 96-bit IPv6 address

D. The VPMv6 address is a 96-bit route distinguisher and a 96-bit IPv6 address

E. The VPNv6 address is a 128-bit route distinguisher and a 128-bit IPv6 address

Answer: B

Explanation:

QUESTION NO: 225

What is the encapsulation format of an MPLS Multicast VPN (MVPN) packet?

A. IP unicast in IP unicast
B. IP multicast in IP anycast
C. IP anycast in IP anycast
D. IP multicast in IP unicast
E. IP multicast in IP multicast
F. IP unicast in IP multicast

Answer: E
Explanation:

QUESTION NO: 226

Using more than one label on a single packet is required in what context?

A. MPLS TE
B. When CEF switching and Label switching is done
C. In all the above circumstances.
D. MPLS VPN

Answer: D
Explanation:

QUESTION NO: 227

In the Inter-AS VPN deployment shown in the diagram, what is the Next Hop address of MP-IBGP Update for CE4 network received at PE-R2?
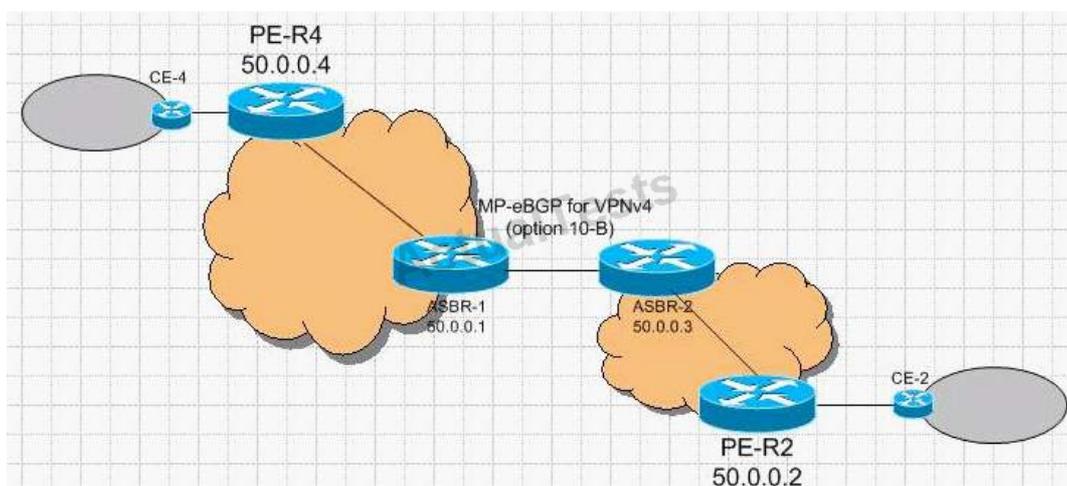
A. ASBR-2 50.0.0.3
B. PE-R2 50.0.0.2
C. PE-R4 50.0.0.4
D. ASBR-1 50.0.0.1

Answer: A

Explanation:

QUESTION NO: 228

There is MPLS VPN traffic traversing through a TE intermediate router. What is the MPLS packet label stack sequence (from outer to inner) for the VPN traffic on this router?

A. VPN label, IGP label, TE label
B. TE label, IGP label, VPN label
C. IGP label, VPN label, TE label
D. TE label, VPN label, IGP label
E. IGP label, TE label, VPN label

Answer: B

Explanation:

QUESTION NO: 229

Which three statements about the route target (RT) are true? (Choose three.)

A. The RT is a BGP extended community.
B. The RT is an 8-byte field that is prefixed to an IPv4 address to make it a unique VPNv4 address.
C. When a VPN route that is learned from a CE router is injected into BGP, one or more RTs are associated with it
D. The distribution of VPN routing information is controlled through the use of VPN RTs
E. When a VPN route that is learned from a CE router is injected into BGP, there is always one RT that is associated with it.

Answer: A,C,D

Explanation:

QUESTION NO: 230

In the context of MPLS, what is the correct action to be performed when an aggregate label is received?

A. It replaces the bottom label in the MPLS label stack with a VPN label and propagates
B. It replaces the top label in the MPLS label stack with a VPN label and propagates
C. It adds the VPN label into the top label in the MPLS label stack
D. It removes the top label in the MPLS label stack and does a Layer 3 lookup on underlying IP packets

Answer: D
Explanation:

QUESTION NO: 231

Which two statements are correct with regard to route distinguisher as defined in RFC 4364 AKA IP-VPN (MPLS-VPN)? (Choose two.)

A. The configuration to define Route-Distinguisher is ip vrf CNT rd 1:1
B. A route distinguisher can be imported and exported to and from a VRF
C. Route-Distinguisher is an 8 byte BGP attribute value used in influencing BGP best path algorithm.
D. Route-Distinguisher is an 8 byte value used in creating unique VPNv4 address.

Answer: A,D
Explanation:

Topic 5, I&O&T Layer 2 VPN

QUESTION NO: 232 DRAG DROP

Drag the command on the left to the correct step on the right to perform Frame Relay interworking with Ethernet over MPLS on a Cisco IOS router.
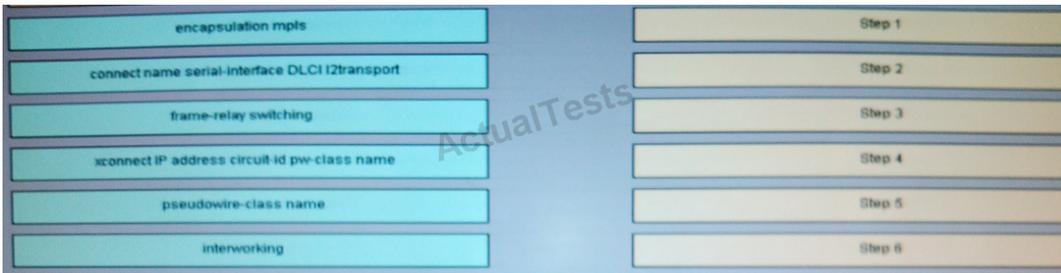
Answer:

Explanation:

Step 1 – frame-relay switching

Step 2 – pseudowire-class name

Step 3 – encapsulation mpls

Step 4 – interworking

Step 5 – connect name serial-interface DLCI l2transport

Step 6 –xconnect IP address circuit-id pw-class name

QUESTION NO: 233

Which two implementations are standard Virtual Private LAN Service (VPLS) implementations that are supported by the IETF? (Choose two)

A. VPLS uses LDP for signaling.
B. VPLS uses BGP for autodiscovery and signaling.
C. VPLS uses extended IS-IS for signaling
D. VPLS uses OSPF version 3 for auto discovery and signaling
E. VPLS uses spanning tree for signaling

Answer: A,B
Explanation:

QUESTION NO: 234

Which three things are the building blocks of the Cisco VPLS architecture? (Choose three)

A. VLAN Trunk Protocol (VTP)
B. State Synchronization Protocol (SSP)
C. L2VPN
D. Ethernet Virtual Switch Interface (VSI)
E. Label Distribution Protocol (LDP)

Answer: C,D,E
Explanation:

QUESTION NO: 235

What is the data encapsulation method for the VPLS virtual circuit (VC)?

A. MAC over MPLS
B. L2TPV3
C. 802.1 QinQ
D. Ethernet over MPLS
E. GRE

Answer: D
Explanation:

QUESTION NO: 236

With VPLS, which protocol is used for label exchange and PW signalling?

A. MP-BGP
B. LDP
C. BGP
D. MTP
E. Directed LDP
F. IGP

Answer: E
Explanation:
Using a directed LDP session, each provider edge advertises a virtual circuit label mapping that is

used as part of the label stack imposed on the Ethernet frames by the ingress provider edge during packet forwarding.

QUESTION NO: 237

Which two statements are correct?

A. A VC type 5 transports a VLAN over MPLS.
B. A VC type 4 tunnels an Ethernet port over MPLS.
C. A VC type 5 tunnels an Ethernet port over MPLS.
D. A VC type 4 transports a VLAN over MPLS.

Answer: C,D
Explanation:
VC Type 4 is used for Ethernet VLAN mode.
VC Type 5 is used for Ethernet Port mode.

QUESTION NO: 238

Which statement about VPLS is true?

A. All CE devices emulate a bridge
B. All provider devices emulate a bridge
C. Hierarchical VPLS reduces signaling overhead
D. Each PE device emulates a bridge
E. Each CE device emulates a bridge

Answer: C
Explanation:
A hierarchical model can be used to improve the scalability characteristics of VPLS. Hierarchical VPLS (HVPLS) reduces signaling overhead and packet replication requirements for the provider edge.

QUESTION NO: 239

Which two statements about VPLS are true? (Choose two.)

A. There is a full mesh of pseudo wires.
B. There is a partial mesh of pseudo wires.
C. Only L2TPv3 can be used for pseudo wire establishment.
D. There is split-horizon to avoid loops.

Answer: A,D
Explanation:

QUESTION NO: 240

According to RFC 3931, L2TPv3 utilizes the IANA assigned IP protocol ID of:

A. 110
B. 101
C. 121
D. 51
E. 151
F. 115

Answer: F
Explanation:
IP Protocol 115 (L2TPv3)

QUESTION NO: 241

Which two options best describe the purpose of session ID and cookie field in a L2TPv3 packet?

A. The session ID is a 32-bit locally significant field used to identify the call on the destination or egress tunnel endport. The session ID will be negotiated by the control connection or statically defined if using the L2TP v3 data plane only.
B. The cookie is a variable length (with a maximum of eight bytes),word-aligned optional field. The control connection can negotiate this as an additional level of guarantee beyond the regular session ID lookup to make sure that a data message has been directed to the correct session or that any recently reused session ID will not be misdirected.
C. The cookie is a 32-bit locally significant field used to identify the call on the destination or egress tunnel endpoint. The cookie will be negotiated by the control connection or statically defined if using the L2TPv3 data plane only

D. The session ID is a variable length (with a maximum of eight bytes), word-aligned optional field. The control connection can negotiate this as an additional level of guarantee beyond the regular cookie lookup to make sure that a data message has been directed to the correct session or that any recently reused cookie will not be misdirected.

Answer: A,B
Explanation:
Session ID:

The 32-bit nonzero session ID carried in the data message header is used to associate incoming data messages with a particular local attachment circuit. Note that one L2TPv3 session corresponds to one pseudowire.

Cookie:

Following the session ID is an optional variable length random cookie value (maximum 64 bits). This cookie value can be used in addition to the session ID and adds an extra level of assurance that the incoming data messages are correctly associated with the local attachment circuit. Furthermore, a randomly chosen cookie provides protection against blind insertion attacks. That is, an attacker would find it very difficult, if not impossible, to insert packets into a data stream (pseudowire) if the attacker is unable to sniff packets transiting the network between peer LCCEs. This is because of the difficulty of guessing the correct cookie value (0 to 264 if the cookie is 64 bits in length).

QUESTION NO: 242

In AToM, control word is an optional 4-byte field used in the pseudowire packet. The control word carries generic and Layer 2 payload-specific information to emulate L2 packets correctly. In pseudowire packet, where is this control word inserted?

A. Inserted between the MPLS label stack and the Layer 3 payload
B. Inserted between the MPLS label stack and the Layer 3 Header
C. Inserted between the MPLS label stack and the Layer 2 payload
D. Inserted between the MPLS label stack and the Layer 2 header

Answer: D
Explanation:

QUESTION NO: 243

In the case of Ethernet transport, which two types of attachment circuits does L2TPv3 support? (Choose two.)

A. port tunneling on the Ethernet subinterface
B. VLAN tunneling on the Ethernet trunk
C. port tunneling on the Ethernet interface
D. VLAN tunneling on the Ethernet VLAN subinterface
E. port tunneling on the Ethernet trunk

Answer: C,D
Explanation:
L2TPv3 can be configured on either a physical port or on a subinterface. The first is known as Port tunneling and the second as vlan tunneling.

QUESTION NO: 244

Packed Cell Relay encapsulation with AToM includes which of the following? (Choose four.)

A. Tunnel label
B. VC-label
C. 5-byte ATM header
D. Payload
E. 4 byte ATM header
F. Support for 30 packed cells.

Answer: A,B,D,E
Explanation:
Packed cell relay (cell packing). This allows the encapsulation of multiple ATM cells in each AToM data channel packet.

QUESTION NO: 245

Which three configuration options are available for configuring the l2tp-class command in L2TPv3? (Choose three)

A. TCP port
B. authentication
C. IP DF bit

D. retransmit retries
E. sequencing
F. hostname

Answer: B,D,F
Explanation:

On Cisco 7200, l2tp-class options available are;
R1(config-l2tp-class)#?
l2tp-class configuration commands:
accounting Method list to use for tunnel accounting authentication Authenticate the L2TP control
connection cookie Local cookie options default Set a command to its defaults digest Message
Digest Authentication for the L2TP control connection exit Exit from l2tp-class configuration
mode hello Set HELLO message interval hidden Hide AVPs in outgoing control messages
hostname Local hostname for control connection authentication no Negate a command or set its
defaults password Password for control connection authentication, AVP hiding receive-window
Receive window size for the control connection retransmit Control message retransmission
parameters timeout Control connection timeout parameters
R1(config-l2tp-class)#retransmit ?
initial SCCRQ message retries/timeout settings
retries Number of retries before tearing down a control connection timeout Control packet
retransmission
timeout parameters
R1#sh run | be l2tp-class
l2tp-class test
authentication
hostname TESTNODE
retransmit retries 5

QUESTION NO: 246

Which statement about L2VPN Pseudowire Switching is not true?

A. L2VPN Pseudowire Switching allows the user to extend L2VPN Pseudowires across an inter-
AS boundary
B. L2VPN Pseudowire Switching allows the user to extend L2VPN Pseudowires across two
separate MPLS networks.
C. Quality of service is not supported per Pseudowire
D. L2VPN Pseudowire Switching connects two or more contiguous Pseudowires segments to from
an end-toend

multihop Pseudowire
E. The Cisco MPLS Traffic Engineering tunnel selection is not supported

Answer: E

Explanation:

ReferencE. http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsstitch.html#wp1053770

QUESTION NO: 247

Which three statements about L2TPv3 are true? (Choose three)

A. L2TPv3 Frame Relay support includes only 32-bit DLCI addressing.
B. L2TPv3 sessions do not support Frame Relay LMI interworking.
C. Multipoint DLCI is not supported.
D. To use DCE or a Network-to-Network Interface on a Frame Relay port, you must configure the frame-relayswitching command.
E. L2TPv3 feature does not support Frame Relay extended addressing.

Answer: C,D,E

Explanation:

Frame Relay-Specific Restrictions

•Frame Relay per-DLCI forwarding and port-to-port trunking are mutually exclusive. L2TPv3 does not support the use of both on the same interface at the same time.

•The xconnect command is not supported on Frame Relay interfaces directly. For Frame Relay, the Xconnect is applied under the connect command specifying the DLCI to be used.

•Changing the encapsulation type on any interface removes any existing xconnect command applied to that interface.

•To use DCE or a Network-to-Network Interface (NNI) on a Frame Relay port, you must configure the framerelay switching command.

•The configuration of an L2TPv3 session on a Multilink Frame Relay (MLFR) bundle interface is supported only on Cisco 12000 series Two-Port Channelized OC-3/STM-1 (DS1/E1) and Six-Port Channelized T3 (T1) line cards. (For more information, see Binding L2TPv3 Sessions to Multilink Frame Relay Interfaces.) •Frame Relay policing is nondistributed on the Cisco 7500 series. By configuring Frame Relay policing, you cause traffic on the affected PVCs to be sent to the RSP for processing.

•Frame Relay support is for 10-bit DLCI addresses. Frame Relay Extended Addressing is not supported.

•Multipoint DLCI is not supported.

•The keepalive will automatically be disabled on interfaces that have an Xconnect applied to them, except for

Frame Relay encapsulation, which is a requirement for LMI.

•Static L2TPv3 sessions will not support Frame Relay LMI interworking.

QUESTION NO: 248

Which two statements best describe the signalling requirements of virtual circuit setup of VPLS and exchange of reachability information (MAC addresses)?

A. Cisco VPLS does not require the exchange of reachability (MAC addresses) information via a signaling protocol. This information is learned from the data plane using standard address learning, aging, and filtering mechanisms defined for Ethernet bridging.

B. Cisco VPLS uses directed LDP as a signalling protocol to exchange reachability (MAC addresses) information to avoid maintanance of ARP cache.

C. In Cisco VPLS the virtual circuit setup uses Multi-Protocol BGP as autodiscovery and signaling mechanism.

Using BGP allows BPDUs to be propagated across VPLS in a scaleable fashion.

D. In Cisco VPLS the virtual circuit setup uses the same LDP signaling mechanism defined for point-to-point services. Using a directed LDP session, each provider edge advertises a virtual circuit label mapping that is used as part of the label stack imposed on the Ethernet frames by the ingress provider edge during packet forwarding.

Answer: A,D
Explanation:

QUESTION NO: 249

When an MPLS Layer 2 VPN runs in the hub-and-spoke model, where is QoS implemented?

A. hub and spoke
B. PE
C. CE
D. hub
E. spoke

Answer: D
Explanation:

QUESTION NO: 250

When you design QoS on CE for an MPLS Layer 2 VPN, which three things should be considered? (Choose three.)

A. Layer 2 access link QoS design
B. enterprise-to-service-provider mapping models
C. Layer 3 link access QoS design
D. service provider service level agreements
E. Layer 2 link access load balancing

Answer: A,B,D
Explanation:

QUESTION NO: 251

Which two Any Transport over MPLS (AToM) traffic encapsulations require the use of a control word? (Choose two)

A. HDLC
B. ATM AAL5
C. PPP
D. Ethernet VLAN
E. Frame Relay

Answer: B,E
Explanation:
AToM Header
The AToM header is 4 bytes (control word). The control word is optional for Ethernet, PPP, HDLC, and cell relay transport types. However, the control word is required for Frame Relay, and ATM AAL5 transport types.

QUESTION NO: 252

Which two features must be configured to perform AToM NSF? (Choose two)

A. FRR
B. SSO
C. distribute CEF

D. switch virtual path
E. graceful restart

Answer: B,E

Explanation:

Before you configure AToM NSF, you need to configure MPLS LDP Graceful Restart. MPLS LDP GR is enabled globally. When you enable LDP GR, it has no effect on existing LDP sessions. LDP GR is enabled for new sessions that are established after the feature has been globally enabled.

How AToM NSF Works

AToM NSF improves the availability of the network of the service provider that uses AToM to provide Layer 2 VPN services. HA provides the ability to detect failures and handle them with minimal disruption to the service being provided. AToM NSF is achieved by SSO and NSF mechanisms. A standby RP provides control-plane redundancy. The control plane state and data plane provisioning information for the attachment circuits (ACs) and AToM pseudowires (PWs) are checkpointed to the standby RP to provide NSF for AToM L2VPNs.

QUESTION NO: 253

Which three attribute-value pairs (AVPs) must be present in L2TPv3 ICRQ messages? (Choose three.)

A. PW capabilities list
B. Message type
C. Assigned control connection ID
D. PW type
E. Remote session ID
F. Hostname

Answer: B,D,E

Explanation:

The ICRQ can include information such as pseudowire type, required Layer 2specific sublayer, and circuit status.
The following AVPs MUST be present in the ICRQ:
Message Type
Local Session ID
Remote Session ID
Serial Number
Pseudowire Type

Remote End ID
Circuit Status
Services

Topic 6, I&O&T Managed Services Traversing the Core

QUESTION NO: 254

Which two statements about NTP version 4 are true? (Choose two)

A. It supports fast synchronization at starting and before network failures.
B. It supports automatic server discovery.
C. It uses a fixed-point arithmetic
D. It supports the "nanokernel" kernel implementation.
E. It does not support Public-Key Cryptography

Answer: B,D
Explanation: Section: I&O&T Managed Services Traversing the Core
Explanation

4.1.9. What's new in Version 4?
According to the NTP Version 4 Release Notes found in release.htm, the new features of version four (as compared to version three) arE.

Use of floating-point arithmetic instead of fixed-point arithmetic.
Redesigned clock discipline algorithm that improves accuracy, handling of network jitter, and polling intervals.
Support for the nanokernel kernel implementation that provides nanosecond precision as well as improved algorithms.

Public-Key cryptography known as autokey that avoids having common secret keys.
Automatic server discovery (manycast mode)
Fast synchronization at startup and after network failures (burst mode)
New and revised drivers for reference clocks
Support for new platforms and operating systems

QUESTION NO: 255

Referring to the exhibit, if RTP header compression is used on the link, the header's overhead on the voice packet will be reduced by what percent?

voice packet
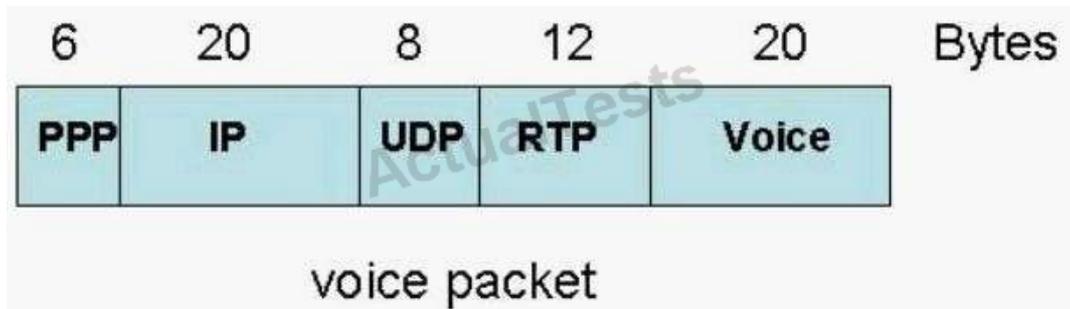
A. from 50% to 25%
B. from 50% to 20%
C. from 70% to 20%
D. from 70% to 33%

Answer: D
Explanation:

QUESTION NO: 256

What is the port number of the IPsec Authentication Header packet?

A. IP protocol 50
B. TCP port 51
C. UDP port 50
D. IP protocol 51
E. UDP port 51
F. TCP port 50

Answer: D
Explanation:

6.2. Managed Security services traversing the core

AH operates directly on top of IP, using IP protocol number 51.

ESP operates directly on top of IP, using IP protocol number 50.

QUESTION NO: 257

What is the port number of the IPsec Encapsulating Security Payload packet?

A. UDP port 50
B. IP protocol 51
C. TCP port 51
D. TCP port 50
E. IP protocol 50
F. UDP port51

Answer: E

Explanation:

6.2. Managed Security services traversing the core

AH operates directly on top of IP, using IP protocol number 51.

ESP operates directly on top of IP, using IP protocol number 50.

QUESTION NO: 258

How many messages does Internet Key Exchange (IKE) use to negotiate SA characteristics when running in aggressive mode?

A. 3 messages
B. 4 messages
C. 5 messages
D. 2 messages
E. 6 messages

Answer: A

Explanation:

The Aggressive Mode is an exchange in the first phase of IKE/ISAKMP (The ISAKMP Aggressive Exchange) is like the Main Mode, but some messages are embedded to the others. The first message proposes the policy, and passes data for key-exchange, the nonce and some information for identification. The second message is a response which authenticates the responder and concludes the policy and key-exchange. At this point all the information for encryption key for the ISAKMP SA is exchanged and last the message could be encrypted, but doesn't have to be. The last message is used for authenticating the initiator and provides a proof of participation in the exchange. The identity of the responder could not be protected, but by

encrypting the last message the identity of the initiator is protected.

QUESTION NO: 259

How many messages does Internet Key Exchange (IKE) use to negotiate SA characteristics when running in main mode?

A. 3 messages
B. 6 messages
C. 4 messages
D. 2 messages
E. 5 messages

Answer: B
Explanation:
3.1.1 Main Mode
The Main Mode is an exchange in the first phase of IKE/ISAKMP (The ISAKMP Identity Protection Exchange) the first two messages are used for negotiating the security policy for the exchange. The next two messages are used for the Diffie-Hellman keying material exchange. The last two messages are used for authenticating the peers with signatures or hashes and optional certificates. Last two authentication messages are encrypted with the previously negotiated key and the identities of the parties are protected from eavesdroppers.

QUESTION NO: 260

Which four statements about an IP service level agreement (SLA) are true? (Choose four)

A. SLA responder knows type of operation, the port used, and duration.
B. SLA responder inserts in and out timestamps in the packet payload.
C. SLA sender and responder use the IP SLA Control Protocol to communicate with each other before sending test packets.
D. SLA sender and responder communication can be encrypted.
E. SLA sender and responder communication can be authenticated with MD5.

Answer: A,B,C,E
Explanation:

QUESTION NO: 261

Which three of these statements about the IP service level agreement (SLA) sender are true?
(Choose three)

A. SLA sender target can be an IP host
B. SLA sender sends a probe packet and a response probe packet
C. SLA sender sends a probe packet
D. SLA sender target must be a router
E. SLA sender target can be an IP SLA responder

Answer: A,C,E
Explanation:

QUESTION NO: 262

R1#show ip cache flow.

Srclf	SrcIPaddress	SrcP	SrcAS	Dstlf	DstIPaddress	DstP	DstAS	Pr	Pkts	B/Pk
29	192.1.6.69	77	3042	49	194.10.6.2	1308	267	6	1	40
29	192.1.6.222	1243	3042	49	194.10.6.2	1774	267	6	1	40
29	192.1.6.108	1076	3042	49	194.10.6.2	1869	267	6	1	40
29	192.1.6.159	903	3042	49	194.10.6.2	1050	267	6	1	40
29	192.1.6.54	730	3042	49	194.10.6.2	2018	267	6	1	40
29	192.1.6.136	559	3042	49	194.10.6.2	1821	267	6	1	40
29	192.1.6.216	383	3042	49	194.10.6.2	1516	267	6	1	40
29	192.1.6.111	45	3042	49	194.10.6.2	1894	267	6	1	40
29	192.1.6.29	1209	3042	49	194.10.6.2	1600	267	6	1	40

A network administrator issues the command "show ip cache flow" and finds the shown output.
What can be concluded? (Choose two.)

A. It is normal traffic.
B. There is a potential sacrificed host located at network 192.1.6.0 generating attacks.
C. There is a potential DOS attack on device of 194.10.6.2.
D. It is multicast traffic source from 194.10.6.2
E. It is multicast traffic destined for 194.10.6.2

Answer: B,C
Explanation:

QUESTION NO: 263

Which three statements about NetFlow are true? (Choose three)

A. NetFlow records unidirectional IP traffic flow.
B. NetFlow records MPLS frame flow.
C. NetFlow export is only over TCP.
D. NetFlow records is only over UDP.
E. NetFlow records subinterface information of traffic flow.

Answer: A,B,E
Explanation:

QUESTION NO: 264

Which four statements about NetFlow are true? (Choose four.)

A. NetFlow records bidirectional IP traffic flow.
B. NetFlow export can be implemented over IPv4.
C. NetFlow export can be implemented over IPv6.
D. NetFlow records multicast IP traffic flow.
E. NetFlow records ingress traffic.
F. NetFlow records egress traffic.

Answer: B,D,E,F
Explanation:

QUESTION NO: 265

Which descriptions of Netflow is correct? (Choose three.)

A. By default,Netflow records bidirectional IP traffic flow.
B. Netflow answers questions regarding IP traffiC. who, what, where, when, and how
C. Netflow accounts for both transit traffic and traffic destined for the router.
D. Netflow returns the subinterface information in the flow records.

Answer: B,C,D
Explanation:

QUESTION NO: 266

How many bits does EXP occupy in the MPLS label header?

A. 8
B. 4
C. 3
D. 1
E. 2

Answer: C
Explanation:

QUESTION NO: 267

What is the typical marked DSCP value for a voice media packet in Voice over IP technology?

A. AF41
B. AF31
C. AF21
D. BE
E. EF

Answer: E
Explanation:

QUESTION NO: 268

What is the typical marked DSCP value for a voice signaling packet in VoIP technology?

A. BE
B. AF41
C. AF21
D. EF
E. AF31

Answer: E

Explanation:

QUESTION NO: 269

Which MQC-based output queueing method is designed to support multiple traffic classes including VoIP traffic, mission-critical traffic, bulk traffic, interactive traffic and default class traffic?

A. Custom Queueing
B. CB-WRED
C. WRR Queueing
D. LLQ
E. CBWFQ

Answer: D
Explanation:

QUESTION NO: 270

When provisioning for Interactive-Video (e.g. video conferencing traffic) which three statements depicts the correct requirements?

A. Loss should be no more than 1 percent.
B. One-way latency should be no more than 150 ms
C. Jitter should be no more than 30 ms
D. Loss should be no more than 3 percent
E. One-way latency should be no more than 75 ms
F. Jitter should be no more than 300 ms

Answer: A,B,C
Explanation:
Interactive Video

When provisioning for Interactive Video (IP Videoconferencing) traffic, the following guidelines are recommended:

•Interactive Video traffic should be marked to DSCP AF41; excess Interactive-Video traffic can be marked down by a policer to AF42 or AF43.

•Loss should be no more than 1 %.

•One-way Latency should be no more than 150 ms.

•Jitter should be no more than 30 ms.

•Overprovision Interactive Video queues by 20% to accommodate bursts

Because IP Videoconferencing (IP/VC) includes a G.711 audio codec for voice, it has the same loss, delay, and delay variation requirements as voice, but the traffic patterns of videoconferencing are radically different from voice.

QUESTION NO: 271

What is the definition of "jitter"?

A. The total end-to-end delay
B. The time it takes for the bits to transit the physical media.
C. The delay caused by placing the bits on the wire.
D. The variations of delay.

Answer: D
Explanation:

QUESTION NO: 272

DSCP value "101110" looks like which IP Precedence value to non-DiffServ compliant devices?

A. IP Precedence 6
B. IP Precedence 4
C. IP Precedence 3
D. IP Precedence 5
E. IP Precedence 2
F. IP Precedence 7

Answer: D
Explanation:

QUESTION NO: 273

With the DSCP value fo "101110", what does the "11" in bits DS1 and DS2 indicate?

A. CS (Class Selector Value)
B. Queue Depth
C. PHB (Per-Hop Behavior)

D. IP Precedence
E. Drop Probability
F. AF Class

Answer: E
Explanation:

QUESTION NO: 274

How many content definitions does CSG allow?

A. 40
B. 400
C. 4000
D. 40,000

Answer: C
Explanation:
CISCO CSG CONFIGURATION LIMITS
• 256 total virtual LANs (client and server)
• 4000 content definitions
• 1024 services
• 16,000 access control list (ACL) items
• Up to six Cisco CSGs and/or CSMs can be installed in a Cisco Catalyst 6500 Series or Cisco
7600 Series chassis

QUESTION NO: 275

What is the main difference between the information displayed on the dspload and the dsptrkutl
screens?

A. The dspload screen is for all trunks; the dsptrkutl screen is for one trunk.
B. The dspload screen shows the expected traffic; the dsptrkutl screen shows actual traffic.
C. The information on the dspload screen never changes; the dsptrkutl screen is dynamic
D. The dspload screen shows historical information; the dsptrkutl screen shows current
information.

Answer: B
Explanation:

Displays both the used and available bandwidth (both in the transmit and receive directions) for each trunk at the specified node. The "transmit" direction is from the node specified and to the node at the other end of the trunk. In the screen display, the numbers of disabled trunks appear in dim, reverse video on the screen.

dsptrkutl

Displays dynamic utilization information for a specified trunk. The trunk must be upped and added to use this command. The following lists the trunk utilization and terminated connection parameters included in the display. The parameter values are updated according to the specified or default interval and the screen remains displayed until the DEL key is depressed. Disabled trunks have their trunk number displayed in dim, reverse video on the screen.

QUESTION NO: 276

What protocol does an IP phone use to learn the voice VLAN ID it should use for voice traffic?

A. VTP
B. 802.1q
C. CDP
D. Skinny Station Protocol

Answer: C
Explanation:

QUESTION NO: 277

What is the relationship between the Domain Name System (DNS) and LDAP?

A. All the root DNS servers maintain information in a distributed LDAP tree.
B. DNS clients access DNS information by making LDAP queries to DNS servers.
C. An LDAP DN attribute is a Domain Name.
D. It is currently recommended to express DN as a sequence of Domain components

Answer: D
Explanation:

QUESTION NO: 278

What layer of the TMN (telecommunications management network) model does CTM fit into?

A. Network management layer
B. Element management layer
C. Business management layer
D. Network element layer

Answer: B
Explanation:

QUESTION NO: 279

What is TCI?

A. Tag Calling Interface
B. Tag Control Identifier
C. ToS Class Interface
D. Tag Control Information

Answer: D
Explanation:

QUESTION NO: 280

In the Apache Web Server configuration, the command KeepAlive ON is used to

A. Allow a CSS to probe the server
B. Allow a connection to be closed with a TCP RESET
C. Allow persistent connections
D. Allow the use of HTTP HEAD request

Answer: C
Explanation:

QUESTION NO: 281

How many token buckets are needed to support a multi-actions policer that meters conforming, exceeding and violating traffic?

A. 1
B. 3
C. 5
D. 2
E. 6
F. 4

Answer: D
Explanation:

QUESTION NO: 282

What are the differences between LLQ and CBWFQ? (Choose two.)

A. LLQ priority queue bandwidth is policed with a congestion aware policer.
B. With LLQ, bandwidth allocations for the priority queue and all the CBWFQ queues are configured using the priority command.
C. LLQ does not support WFQ on the default traffic class (class-default).
D. LLQ supports the addition of strict priority queuing.
E. LLQ is configured using MQC and CBWFQ is configured using the fair-queue command.

Answer: A,D
Explanation:

QUESTION NO: 283

What is used to provide read access to QoS configuration and statistics information on Cisco platforms that support Modular QoS CLI (MQC)?

A. Cisco SDM QoS Wizard
B. Cisco AutoQoS
C. CDP
D. Cisco Class-Based QoS MIB.
E. Cisco NBAR Discovery

Answer: D
Explanation:

QUESTION NO: 284

As described in RFC 3270, short-pipe mode operation, the PE to CE egress polices are based upon:

A. customer marking
B. remarked IP tos value
C. Qos groups/discard class
D. innermost label exp value
E. MDRR quantam
F. topmost label exp value

Answer: A
Explanation:

QUESTION NO: 285

Select the statement that best describes "The cure for Amplification Principle" in the Internet domain, as explained in RFC 3429 (Internet Architectural Guidelines)

A. None of the above
B. Amplification is prevented if local changes have only a local effect as opposed to system in which local change have a global effect
C. Amplification is prevented if global changes have only a local effect as opposed to systems in which global changes have a local effect
D. Internet domain does not suffer from "The Amplification Principle" as BGP takes care of misbehaving advertisers

Answer: B
Explanation:
In the Internet domain, it has been shown that increased interconnectivity results in more complex and often slower BGP routing convergence [AHUJA]. A related result is that a small amount of inter-connectivity causes the output of a routing mesh to be significantly more complex than its input [GRIFFIN]. An important method for reducing amplification is ensure that local changes have only local effect (this is as opposed to systems in which local changes have global effect). Finally, ATM provides an excellent example of an amplification effect: if you lose one cell, you destroy the entire packet (and it gets worse, as in the absence of mechanisms such as Early Packet Discard [ROMANOV], you will continue to carry the already damaged packet).

QUESTION NO: 286

A network administrator wants to detect a login attack against a router. What IOS command can make the attack recorded in syslog server?

A. Login detect login-failure log
B. none of the above
C. Logging detect fail-login
D. Login on-failure log
E. Logging login on-failure

Answer: D
Explanation:

QUESTION NO: 287

Which of the following IOS commands cause syslog messages to be stamped with time and dates?

A. logging datetime on
B. service timestamps log datetime
C. service logging datetime
D. logging timestamps on
E. logging trap datetime

Answer: B
Explanation:
Service timestamps
To configure the system to apply a time stamp to debugging messages or system logging messages, use the service timestamps command in global configuration mode. To disable this service, use the no form of this command.
Service timestamps [debug | log] [uptime | datetime [msec]] [localtime] [show-timezone] [year] no service timestamps [debug | log]

QUESTION NO: 288

Which of the following statements regarding Selective Packet Discard (SPD) is correct?

A. Selective Packet Discard (SPD) is a mechanism to drop non-routing packets instead of routing packets when the process level queue is congested.
B. Selective Packet Discard (SPD) is a mechanism to drop normal IP packets instead of VOIP packets when the link is overloaded
C. None of above.
D. Selective Packet Discard (SPD) is a mechanism to drop Frame Relay frames with the DE bit set instead of
Frame Relay frames DE bits without being set when the link is overloaded
E. Selective Packet Discard (SPD) is a mechanism to drop packets with low IP precedence instead of packets with high IP precedence when the link is overloaded

Answer: A
Explanation:

QUESTION NO: 289

In which modes does selective packet discard (SPD) operate? (Choose three.)

A. discard
B. random
C. normal
D. full
E. select

Answer: B,C,D
Explanation:

QUESTION NO: 290

Which of the following statements regarding Control Plane Policing (CoPP) is correct? (Choose three.)

A. Control Plane Policing (CoPP) addresses the need to protect the management planes, ensuring routing stability, availability, and critical packet delivery.
B. Control Plane Policing (CoPP) leverages MQC to define traffic classification criteria and to specify configurable policy actions for the classified traffic.
C. Control Plane Policing (CoPP) uses a dedicated "control-plane" command via the Modular QoS CLI (MQC) to provide filtering and rate limiting capabilities.

D. Control Plane Policing (CoPP) uses "service policy" command under relevant interfaces to filter DOS packet to protect routing packets.
E. Control Plane Policing (CoPP) protects the transit management and data traffic through the router.

Answer: A,B,C
Explanation:

QUESTION NO: 291

Which of the following comparison of Control Plane Policing (CoPP) with Receive ACL (RACL) is correct? (Choose two.)

A. CoPP protects against IP spoofing, RACL protects against DoS attacks.
B. CoPP can not use named access lists, RACL can use named access lists.
C. CoPP applies to a dedicated control plane interface, RACL applies to all interfaces.
D. CoPP needs a AAA server, RACL does not need a AAA server.
E. CoPP supports rate limits, RACL does not support rate limits.

Answer: C,E
Explanation:

QUESTION NO: 292

How would you characterize the source and type in a denial of service attack on a router?

A. By perform a show ip interface to see the type and source of the attack based upon the access-list matches
B. By setting up an access-list to permit all ICMP, TCP, and UDP traffic with the log or log-input commands, then use the show access-list and show log commands to determine the type and source of attack
C. By performing a show interface to see the transmitted load "txload" and receive load "rxload", if the interface utilization is not maxed out, there is no attack underway
D. By applying an access-list to all incoming and outgoing interfaces, turning off route-cache on all interfaces, then, when telnetting into the router perform a debug IP packet detail

Answer: B
Explanation:

QUESTION NO: 293

Which of the following descriptions about IP spoofing is correct?

A. IP destination address is forged
B. IP source address is forged
C. IP TCP destination port is forged
D. None of above
E. IP TCP source port is forged

Answer: B
Explanation:
1.13. Security in core

QUESTION NO: 294

BCP (Best Common Practices) 38/RFC 2827 Ingress and Egress Packet Filtering would help mitigate what classification of attack?

A. Denial of service attack
B. Sniffing attack
C. Spoofing attack
D. Reconnaisance attack
E. Port Scan attack

Answer: C
Explanation:

6. Summary
Ingress traffic filtering at the periphery of Internet connected networks will reduce the effectiveness of source address spoofing denial of service attacks. Network service providers and administrators have already begun implementing this type of filtering on periphery routers, and it is recommended that all service providers do so as soon as possible. In addition to aiding the
Internet community as a whole to defeat this attack method, it can also assist service providers in locating the source of the attack if service providers can categorically demonstrate that their network already has ingress filtering in place on customer links.
Corporate network administrators should implement filtering to ensure their corporate networks are not the source of such problems. Indeed, filtering could be used within an organization to ensure users do not cause problems by improperly attaching systems to the wrong networks.
The filtering could also, in practice, block a disgruntled employee from anonymous attacks.

It is the responsibility of all network administrators to ensure they do not become the unwitting source of an attack of this nature.

QUESTION NO: 295

What are BCP 38 (Best Common Practices 38) / RFC 2827 Ingress Packet Filtering Principles? (Choose three.)

A. Filter Smurf ICMP packets.
B. Filter as close to the core as possible
C. Filter as close to the edge as possible
D. Filter as precisely as possible
E. Filter both source and destination where possible.

Answer: C,D,E
Explanation:
1.13. Security in core

QUESTION NO: 296

Which of the following IOS commands can detect whether the SQL slammer virus propagates in your networks?

A. access-list 110 permit any any udp eq 69 log
B. access-list 100 permit any any udp eq 1434 log
C. access-list 110 permit any any udp eq 69
D. access-list 100 permit any any udp eq 1434

Answer: B
Explanation:

QUESTION NO: 297

Refer to the exhibit.
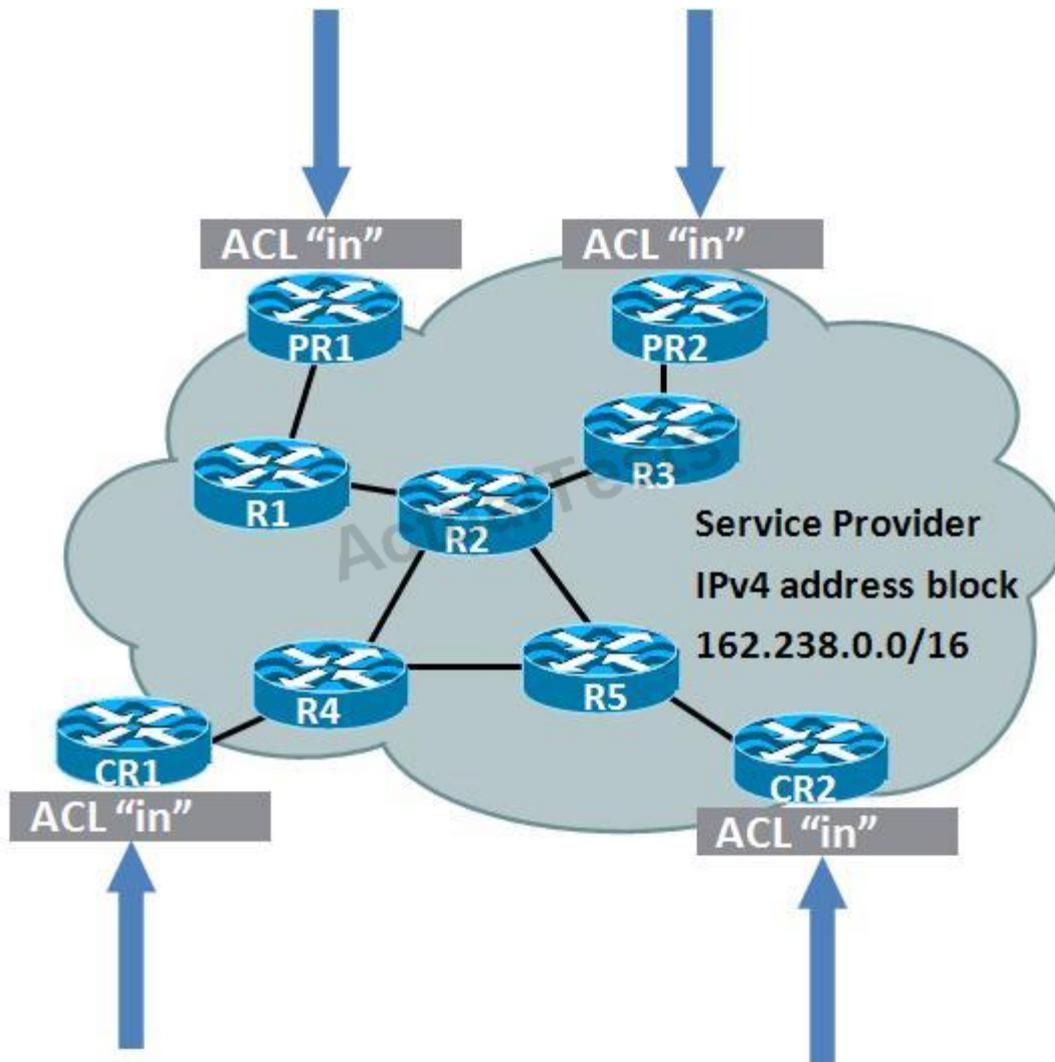
Inbound infrastructure ACLs are configured to protect the SP network. Which two types of traffic should be permitted in the infrastructure ACL? (Choose two.)

A. traffic destined for network of 172.30.0.0/16
B. traffic source from network of 172.30.0.0/16
C. traffic destined for network of 162.238.0.0/16
D. traffic source from network of 162.238.0.0/16
E. traffic destined for network of 232.16.0.0/16

Answer: C,E
Explanation:

QUESTION NO: 298

Refer to the exhibit.
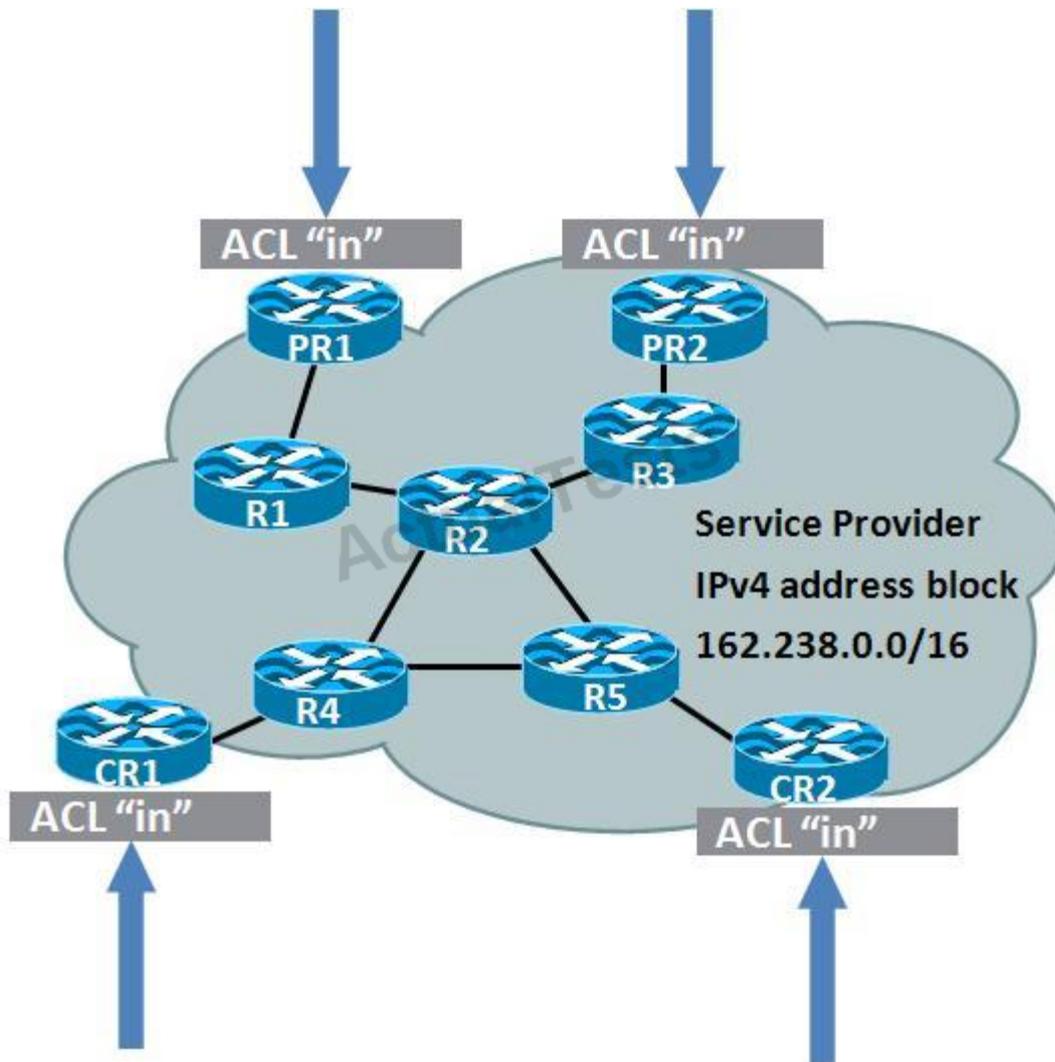
Inbound Infrastructure ACLs are configured to protect the SP network. Which three types of traffic should be filtered in the infrastructure ACLs? (Choose three.)

A. traffic from a source with an IP address that is within 239.255.0.0/16
B. FTP traffic destined for internal routers
C. IPsec traffic that at an internal router
D. traffic from a source with an IP address that is within 162.238.0.0/16
E. EBGP traffic that peers with edge routers

Answer: A,B,D

Explanation:

With the use of the protocols and addresses identified, the infrastructure ACL can be built to permit the protocols and protect the addresses. In addition to direct protection, the ACL also provides a first line of defense against certain types of invalid traffic on the Internet:

- RFC 1918 space must be denied. (RFC1918 describes a set of network ranges set aside for so-called "private" use.)

- Packets with a source address that fall under special-use address space, as defined in RFC 3330, must be denied.

- Anti-spoof filters must be applied. (Your address space must never be the source of packets from outside your AS.)

QUESTION NO: 299

What are two uRPF working modes? (Choose two.)

A. express mode
B. safe mode
C. loose mode
D. strict mode
E. tight mode

Answer: C,D
Explanation:

QUESTION NO: 300

Which of the following IOS features can prevent IP spoofing attacks?

A. Unicast Reverse Path Forwarding (uRPF)
B. MPLS traffic Engineering
C. Cisco Express Forwarding
D. PPP over Ethernet
E. IS-IS routing

Answer: A
Explanation:

QUESTION NO: 301

What is a limitation of implementing uRPF?

A. Domain name must be defined.
B. MPLS LDP must be enabled.
C. BGP routing protocol must be running.
D. Symmetrical routing is required.

E. Named access-lists must be configured.

Answer: D
Explanation:

QUESTION NO: 302

Which of the following descriptions about uRPF loose mode is correct? (Choose two).

A. It is typically used on point-to-point interfaces where the same interface is used for both directions of packet flows; if the source address has a return route in the FIB table, it is then checked against the adjacency table to ensure the same interface receiving the packet is the same interface used for the return path
B. If a packet fails the uRPF loose mode check, the packet is then transmitted and creates a log message
C. It is typically used on multipoint interfaces or on routers where asymmetrical routing is used (packets are received on one interface but the return path is not on the same interface); loose mode verifies a source address by looking in forwarding information base(FIB).
D. If a packet fails the uRPF loose mode check, the packet is then dropped

Answer: C,D
Explanation:

When administrators use Unicast RPF in strict mode, the packet must be received on the interface that the router would use to forward the return packet. Unicast RPF configured in strict mode may drop legitimate traffic that is received on an interface that was not the router's choice for sending return traffic. Dropping this legitimate traffic could occur when asymmetric routing paths are present in the network.

When administrators use Unicast RPF in loose mode, the source address must appear in the routing table.

Administrators can change this behavior using the allow-default option, which allows the use of the default route in the source verification process. Additionally, a packet that contains a source address for which the return route points to the Null 0 interface will be dropped. An access list may also be specified that permits or denies certain source addresses in Unicast RPF loose mode. Care must be taken to ensure that the appropriate Unicast RPF mode (loose or strict) is configured during the deployment of this feature because it can drop legitimate traffic. Although asymmetric traffic flows may be of concern when deploying this feature, Unicast RPF loose mode is a scalable option for networks that contain asymmetric routing paths.

QUESTION NO: 303

What Cisco IOS feature examines packets received to make sure that the source address and interface are in the routing table and match the interface that the packet was received on?

A. MPLS Traffic Engineering
B. Receive ACL
C. Unicast RPF
D. Authentication
E. Dynamic access-lists

Answer: C
Explanation:

QUESTION NO: 304

Which statement about SNMP is true?

A. SNMP version 2 uses a proxy agent to forward GetNext message to SNMP version 3.
B. SNMP version 2 supports message integrity to ensure that a packet has not been tampered with in transit.
C. Proxy agents were used only in SNMP version 1.
D. SNMP version 3 supports encryption and SNMP version 2 support authentication.
E. GetBulk messages are converted to GetNext messages by the proxy agent and are then forwarded to the SNMP version 1 agent.

Answer: E
Explanation:

Proxy agents:
A SNMPv2 agent can act as a proxy agent on behalf of SNMPv1 managed devices, as follows:
A SNMPv2 NMS issues a command intended for a SNMPv1 agent.
The NMS sends the SNMP message to the SNMPv2 proxy agent.
The proxy agent forwards Get, GetNext, and Set messages to the SNMPv1 agent unchanged.
GetBulk messages are converted by the proxy agent to GetNext messages and then are forwarded to the SNMPv1 agent.
The proxy agent maps SNMPv1 trap messages to SNMPv2 trap messages and then forwards them to the NMS.

SNMPv3 provides important security features:[11]

Confidentiality - Encryption of packets to prevent snooping by an unauthorized source.

Integrity - Message integrity to ensure that a packet has not been tampered while in transit including an optional packet replay protection mechanism.

Authentication - to verify that the message is from a valid source.

QUESTION NO: 305

Which of the following statements about MD5 Routing Updates authentication is valid? (Select two)

A. The MD5 algorithm inputs the routing updates of arbitrary length and outputs a 128-bit hash
B. The MD5 algorithm inputs the routing updates of every 64bit length and outputs an 8-bit hash
C. Multiple keys are supported
D. Routing updates packets are delivered in encrypted messages
E. Shared secret keys are delivered in encrypted messages

Answer: A,C
Explanation:

QUESTION NO: 306

RFC 3270 describes Differentiated Services (Diff-Serv) over Multi-Protocol Label Switching (MPLS) networks.

Which model alters Differentiated Services (Diff-Serv) code points set in different Differentiated Services (Diff-Serv) domain?

A. None of the above will alter Differentiated Services (Diff-Serv) code points set in different Differentiated Services (Diff-Serv) domain.
B. Uniform model
C. Pipe Model
D. Short Pipe

Answer: B
Explanation:

QUESTION NO: 307

Which ACL entry can be used to block Teredo tunnels?

A. Teredo tunnels cannot be blocked
B. deny udp any any 3544
C. deny ipv6 udp any any 3544
D. deny 41 any any

Answer: B
Explanation:

Topic 7, Mix Questions

QUESTION NO: 308

Which three of these can be a forwarding equivalence class? (Choose three)

A. IPSec tunnel
B. routing equivalence paths
C. traffic engineering tunnel
D. bridge or switch instance
E. groups of IP addresses

Answer: C,D,E
Explanation:

QUESTION NO: 309

How many messages does Internet Key Exchange use to negotiate SA characteristics when it runs in aggressive mode?

A. 3
B. 4
C. 5
D. 2
E. 6

Answer: A

Explanation:

QUESTION NO: 310

Refer to the exhibit.
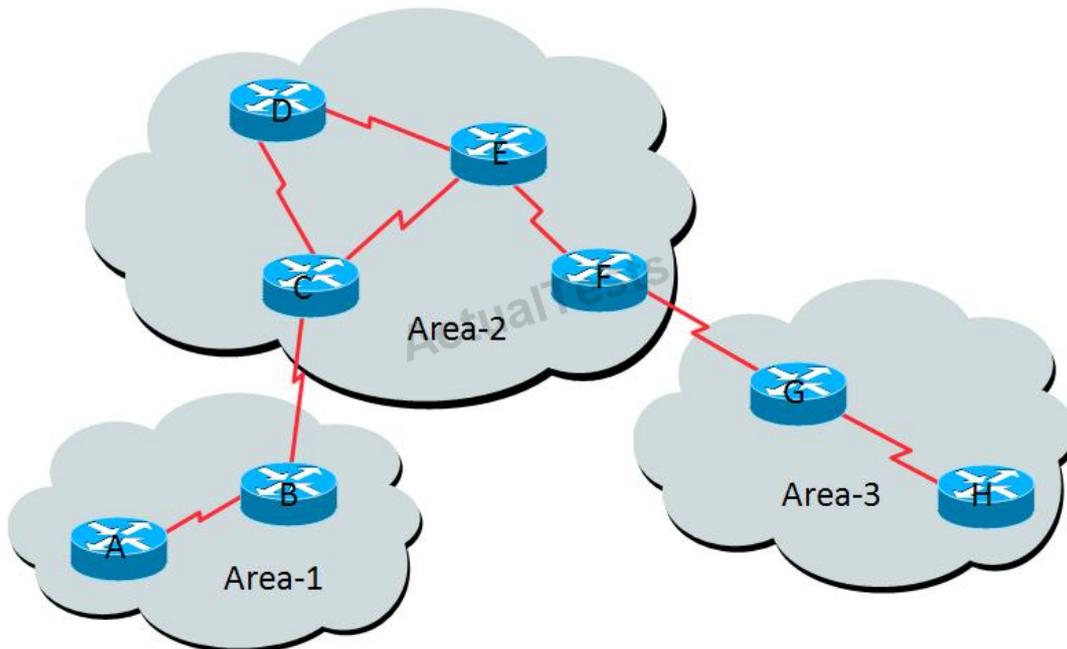
All routers are running IS-IS. Which routers must be Level 2 routers?

A. B, D, E and G
B. A, D, E, and H
C. B, C, F, and G
D. B, C, E, F, and G
E. A, B, C, D, F, G, and H

Answer: D

Explanation:

QUESTION NO: 311

In PIM-SM operations, to which device does the first router that connects with the multicast source send the register message?

A. RP
B. multicast source
C. IGMP router
D. multicast receiver
E. PIM designated router

Answer: A
Explanation:

QUESTION NO: 312

Where is the MPLS label imposed?

A. after the Layer 3 header and before the Layer 2 payload
B. after the Layer 3 header and before the Layer 4 payload
C. after the Layer 2 header and before the Layer 1 payload
D. after the Layer 1 header and before the Layer 2 payload
E. after the Layer 2 header and before the Layer 3 payload

Answer: E
Explanation:

QUESTION NO: 313

Which statement about PIM sparse mode operations is true?

A. It does not support all underlying unicast routing protocols like BGP
B. Receivers are registered with RP by their first hop router
C. From the RP, traffic flows down a source tree to each receiver.
D. It supports shared trees only, and assumes all hosts want the multicast traffic
E. Receivers are joined to the shared tree by their local designated router

Answer: E
Explanation:

QUESTION NO: 314

Which router or router combination is used to calculate the MPLS traffic engineering tunnel path?

A. head-end router and tail-end router
B. middle-point router
C. head-end router
D. tail-end router

Answer: C
Explanation:

QUESTION NO: 315

Which two statements about MPLS Label Distribution Protocol (LDP) are true? (Choose two)

A. LDP hello packets are sent to TCP 646.
B. LDP session packets are sent to TCP 646.
C. LDP session packets are sent to TCP 711.
D. LDP hello packets are sent to TCP 711.
E. LDP hello packets are sent to UDP 711.
F. LDP hello packets are sent to UDP 646.

Answer: B,F
Explanation:

QUESTION NO: 316

What best describes the usage of Route-Target rewrite?

A. Route-Target Rewrite is mainly used in Inter-AS MPLS-VPN deployments and is configured at the Route-Reflector in originating AS ASBR to avoid misconfiguration in Route-Target assignment for VPN configurations.
B. Route-Target Rewrite is mainly used in Inter-AS MPLS-VPN deployments and is configured at the ASBR to avoid misconfiguration in Route-Target assignment for VPN configurations.
C. Route-Target Rewrite is mainly used in Inter-AS MPLS-VPN deployments and is configured at the PE router in originating AS ASBR to avoid misconfiguration in Route-Target assignment for VPN configurations.
D. None of the above.

Answer: B
Explanation:

QUESTION NO: 317

Having the above BGP peerings, select the two configurations for rtrB that will fulfill the following criteria:

-Will advertise all routes from rtrA to rtrD but not to rtrC

-Will advertise the routes from rtrD to rtrC
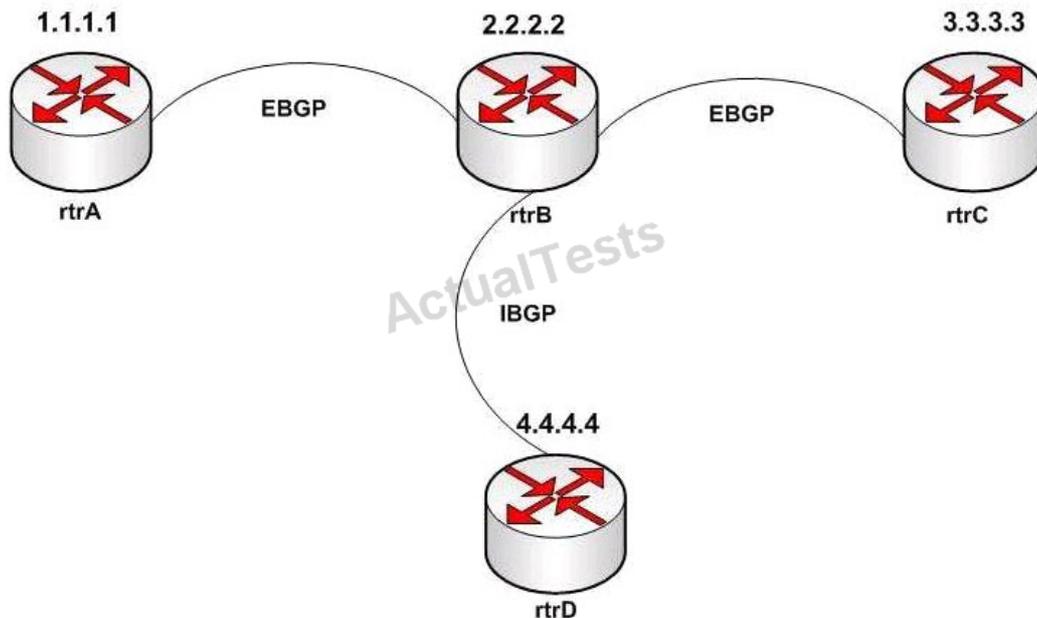
A. router bgp 2
neighbor 1.1.1.1 remote-as 1
neighbor 1.1.1.1 route-map rtrA in
!
route-map rtrA permit 10
set community no-advertise
!
B. router bgp 2
neighbor 1.1.1.1 remote-as 1
neighbor 1.1.1.1 route-map rtrA in
!
route-map rtrA permit 10
set community no-export
!
C. router bgp 2
neighbor 1.1.1.1 remote-as 1
neighbor 1.1.1.1 route-map rtrA in
neighbor 3.3.3.3 remote-as 3
neighbor 3.3.3.3 route-map rtrC out
!

route-map rtrA permit 10
set community 5
!
route-map rtrC permit 10
match community 5
!
D. router bgp 2
neighbor 1.1.1.1 remote-as 1
neighbor 1.1.1.1 route-map rtrA in
neighbor 3.3.3.3 remote-as 3
neighbor 3.3.3.3 route-map rtrC out
!
route-map rtrA permit 10
set community 5
!
route-map rtrC permit 10
match community 5
!
route-map rtrC permit 20
!

Answer: B,D
Explanation:

QUESTION NO: 318

What protocol is used for Path Setup in MPLS traffic engineering?

A. BGP
B. PIM
C. ISIS
D. OSPF
E. RSVP

Answer: E
Explanation:

QUESTION NO: 319

Which of the following comparison of Control Plane Policing (CoPP) with Receive ACL (Racl) is
correct?

A. CoPP protects against IP spoofing; Racl protects against DoS attacks.

B. CoPP can not use named access lists; Racl can use named access lists

C. CoPP applies to a dedicated control plane interface; Racl applies to all interfaces.

D. CoPP needs a AAA server, Racl does not need a AAA server

E. CoPP supports rate limits; Racl does not support rate limits

Answer: C,E

Explanation:

QUESTION NO: 320

VoIP bearer traffic is typically marked to which DSCP value?

A. af41

B. af31

C. 0 (default)

D. cs7

E. cs3

F. ef

Answer: F

Explanation:

QUESTION NO: 321

MPLS label headers for packet media consist of:

A. Version

B. Label

C. COS/EXP

D. TTL

E. S flag

Answer: B,C,D,E

Explanation:

QUESTION NO: 322

Select 3 AVPs (Attribute-Value Pair) which MUST be present in the ICRQ:

A. Called Number
B. Call Serial Number
C. Message Type
D. Calling Number
E. Assigned Session ID

Answer: B,C,E
Explanation:

QUESTION NO: 323

The ASBR-summary LSA is:

A. Generated by the ABR and describes reachabilty to the ASBR for routers in the same area with the ASBR
B. Generated by the ASBR and describes reachability to itself
C. Generated by the ABR and describes reachabilty to the ASBR for routers in a different area from the ASBR
D. Generated by the ASBR and describes reachabilty to the ABR

Answer: C
Explanation:

QUESTION NO: 324

Unicast Reverse Path Forwarding (Urpf) can work in the following modes:

A. Safe mode
B. Loose mode
C. Strict mode
D. Express mode
E. Tunnel mode

Answer: B,C
Explanation:

QUESTION NO: 325

Which command will display the MPLS label binding for IP prefix 1.1.1.0 on the router?

A. All of the above.
B. show tag-switching tdp binding 1.1.1.0/24
C. show tag-switching tdp bindings neighbor 1.1.1.0
D. A and B both will show the binding.
E. show tag-switching interface e0/0

Answer: B
Explanation:

QUESTION NO: 326

What is true regarding Autonomous Systems (AS)?

A. All of the Above
B. AS numbers are assigned by the IANA
C. AS numbers are used by BGP (Border Gateway protocol to exchange IP routing information with neighboring AS
D. In the internet, an Autonomous System (AS) is a collection of IP networks and routers under the control

Answer: A
Explanation:

QUESTION NO: 327

Which of the following processes are likely to be found in a microkernel?

A. Memory management
B. Lightweight messaging
C. Process scheduling
D. Hardware abstraction
E. Host stack
F. All of the above

Answer: F
Explanation:

QUESTION NO: 328

What statement is true?

A. Link Control Protocol (LCP) is used for denying PPP connections to unauthorized devices.
B. Link Control Protocol (LCP) is used for basic PPP link setup and operation
C. Link Control Protocol (LCP) for PPP is synonymous to ARP for Ethernet.
D. None of the above.

Answer: B
Explanation:

QUESTION NO: 329

What will significantly degrade DSL performance, regardless of DSL rate or line length? Select all that apply

A. Micro liters installed between a telephone and shared line.
B. POTS splitters at the subscriber's end of the DSL line
C. POTS splitters at the telco CO.
D. None of the other alternatives apply.

Answer: D
Explanation:

QUESTION NO: 330

What is true regarding Cisco Network Registrar in Cable networks?

A. It provides comprehensive Domain Name system
B. It provides DHCP administrative functionality
C. It provides TFTP server functionality.
D. All of the above are true.

Answer: D
Explanation:

QUESTION NO: 331

In optical transmission systems, chirped lasers are used for the purpose of:

A. Turning the laser to a specific ITU channel
B. Keeping the signal wavelength "locked" to a specific technology
C. Suppressing FWM and SBS non-linear effects
D. None ofthe above

Answer: D
Explanation:

QUESTION NO: 332

When gateways are registering with a gatekeeper, the gatekeeper can be

A. On the same subnet
B. On a remote LAN
C. In a different subnet
D. Any of the above

Answer: D
Explanation:

QUESTION NO: 333

Which two IOS commands are equivalents for putting a Cisco 7500 OC-12 RPR interface card into wrapped mode? Select all that apply

A. shutdown [a | b]
B. srp shutdown [a | b]
C. srp ips request manual-switched [a | b]

Answer: B,C
Explanation:

QUESTION NO: 334

Which statement is FALSE concerning the interleave depth value?

A. A higher interleave depth provides more protection from burst of noise on the HFC network
B. Higher interleave depth increase downstream latency.

C. Lower interleave depth cause some packet loss on typical HFC networks
D. None ofthe above

Answer: D
Explanation:

QUESTION NO: 335

MPLS label mapping on an LSR is displayed by which IOS command?

A. Show mpls ldp neighbor detail
B. Show mpls ldp bindings
C. Show mpls ldp parameters
D. Show mpls ldp discovery

Answer: B
Explanation:

QUESTION NO: 336

GMPLS is based upon Non-Packet-based devices

A. True
B. False

Answer: A
Explanation:

QUESTION NO: 337

Which three IS-IS TLVs are used to support MPLS traffic engineering? (Choose three).

A. extended TLV 22
B. extended TLV 23
C. extended TLV 134
D. extended TLV 135

E. extended TLV 136
F. extended TLV 138

Answer: A,C,D
Explanation:

QUESTION NO: 338

If the IPv6 address 2001:0DB8:0000:0000:09C0:876A:0000:130B is entered into a router, which option is displayed in the configuration?

A. 2001:db8:0:0:9C0:876A::130B
B. 2001:db8:0:0:09C0:876A:0:130B
C. 2001:db8::9C0:876A:0:130B
D. 2001:db8::9C0:876A:130B
E. 2001:0db8::9C:876A:13B

Answer: C
Explanation:

QUESTION NO: 339

How many bits are expressed by "::" in the address 2001:DB8::9C0:876A:0:130B?

A. 32 bits
B. 28 bits
C. 44 bits
D. 64 bits
E. 0 bits

Answer: A
Explanation:

QUESTION NO: 340

Which statement about OSPFv3 is true?

A. OSPFv3 runs on per subnet basis instead of per-link.

B. OSPFv3 instance ID is only locally significant.

C. OSPFv3 authentication is performed using the authentication field in the OSPFv3 packet header.

D. OSPFv3 neighbor discovery messages can be sourced only from link-local addresses.

Answer: D

Explanation:

QUESTION NO: 341

In the case of 6RD, how does the residential gateway device route the IPv6 packet received from local host?

A. It looks into the local NAT table to translate the IPv6 address into an IPv4 address.

B. It looks for the IPv6 destination in the local IPv6 routing table.

C. It sends all the IPv6 traffic to the Border Relay router.

D. It derives the IPv4 address from the IPv6 destination address.

Answer: D

Explanation:

QUESTION NO: 342

What happens when a broadcast storm is detected?

A. The traffic threshold reaches 100%.

B. CPU utilization reaches 100%.

C. The value of the TotalSuppDiscards counter increments.

D. The port goes down.

E. The switch goes down.

Answer: C

Explanation:

QUESTION NO: 343

Which statement about the requirements of eBGP multipath is true?

A. The path should be learned from an external or confederation-external neighbor.
B. The path should be learned from an internal neighbor.
C. The IGP metric to the BGP next hop should be equal to the best-path IGP metric, unless the router is configured for unequal-cost iBGP multipath.
D. The path should be learned from an IGP protocol.

Answer: A
Explanation:

QUESTION NO: 344

Which two options describe how 6RD compares to automatic 6to4 tunneling? (Choose two.)

A. 6RD provides a controlled exit point from the IPv6 Internet.
B. 6RD provides a controlled entry point to the IPv6 Internet.
C. 6RD is widely available in current OS implementations.
D. Automatic 6to4 tunneling is widely available in current OS implementations.
E. Automatic 6to4 tunneling and 6RD use a well-known IPv6 prefix.

Answer: B,D
Explanation:

QUESTION NO: 345

In Cisco IOS XR Software Multicast Routing Implementation, which three features are supported in IPv6 on Cisco CSR routers? (Choose three.)

A. Multicast NSF
B. PIM-SSM
C. OOR handling
D. Aggregation multicast
E. Integrated multicast
F. PIM-Bidirectional

Answer: A,B,F
Explanation:

QUESTION NO: 346

Which three options are EIGRP route types? (Choose three.)

A. internal routE. routes that originate within the AS
B. summary routE. routes that are summarized in the router
C. external routE. routes that are redistributed to EIGRP
D. partial routE. partial routes that are summarized in the router
E. stub routE. default route that originates in the area

Answer: A,B,C

Explanation:

QUESTION NO: 347

Which statement about provider-independent and provider-assigned address blocks is true?

A. There is no difference.
B. PI space is not globally routable and can be used as private addressing.
C. PA space is globally routable and can be obtained from IANA by all organizations.
D. PA space is assigned by the ISP and PI space is assigned by the regional registry. Both are globally routable.
E. PI and PA blocks are both assigned by the regional registry to all organizations.

Answer: D

Explanation:

QUESTION NO: 348

You applied this ACL to the interface and several people reported that they were unable to access the network.

ipv6 access-list webOnly

 permit tcp any 2001:DB8::/32

 permit udp any 2001:DB8::/32

 deny ipv6 any any

Which answer explains why they were unable to access the network?

A. The connections are stale. The users must close and restart their applications.

B. DNS queries and replies are not working.

C. The ACL is blocking the operation of the ND process.

D. DHCP requests are not reaching to the DHCP server.

Answer: C

Explanation:

QUESTION NO: 349

Which type of IPv6 address does OSPFv3 use to communicate with OSPFv3 neighbors?

A. link-local

B. site-local

C. global

D. unique local

E. anycast

Answer: A

Explanation:

QUESTION NO: 350

Which two statements about 6RD are true? (Choose two.)

A. The 6RD customer edge device forwards all packets to the 6RD border relay.

B. The 6RD customer edge device can forward packets destined to other 6RD customer edge devices outside the local 6RD domain without traversing the 6RD border relay.

C. Packets between 6RD customer edge devices in the same 6RD domain do not need to traverse the 6RD border relay.

D. Packets received from a 6RD domain can easily be identified as such on the IPv6 Internet.

E. The entry point into the local 6RD domain is deterministic.

Answer: C,E

Explanation:

QUESTION NO: 351

What is the maximum capacity of a single Cisco CRS-1?

A. 64 Tb/s
B. 78 Tb/s
C. 92 Tb/s
D. 106 Tb/s
E. 128 Tb/s

Answer: C
Explanation:

QUESTION NO: 352

Which two options describe the order of preference of attributes when some or all are applied to one neighbor in BGP? (Choose two.)

A. For inbound updates, the order of preference is route-map, filter-list, prefix-list, distribute-list.
B. For inbound updates, the order of preference is filter-list, route-map, prefix-list, distribute-list.
C. For inbound updates, the order of preference is prefix-list, route-map, filter-list, distribute-list.
D. For outbound updates, the order of preference is filter-list, prefix-list, distribute-list, route-map.
E. For outbound updates, the order of preference is prefix-list, distribute-list, filter-list, route-map.
F. For outbound updates, the order of preference is route-map, prefix-list, distribute-list, filter-list.

Answer: A,E
Explanation:

QUESTION NO: 353

R1 and R2 share the same Fast Ethernet connection. OSPFv3 is configured on each interface, but the adjacency is not being established.

Review the configuration provided. Which option explains why the OSPFv3 adjacency is not coming up?

R1

Interface fastethernet 0/0

 ipv6 address 2001:db8:1234:1::1/64

 ipv6 ospf 1 area 0 instance 2

ipv6 enable

ipv6 router ospf 1

 router-id 1.1.1.1

R2

 Interface fastethernet 0/0

 ipv6 address 2001:db8:6789:9::1/64

 ipv6 ospf 2 area 0 instance 3

ipv6 router ospf 2

 router-id 2.2.2.2

A. The two routers are not on the same subnet.
B. IPv6 is not enabled on R2 Fast Ethernet 0/0.
C. There is no reachability to 1.1.1.1 or 2.2.2.2.
D. The OSPFv3 processes do not match.
E. The instance IDs do not match.

Answer: E
Explanation:

QUESTION NO: 354

Which statement about IPv6 security is true?

A. Reconnaissance attacks are easier to do in IPv6 compared to IPv4.
B. IPv6 amplification attacks can happen using IPv6 broadcast address.
C. RA-guard feature is used to block rogue RAs.
D. ICMP policies on firewalls do not need to be changed for IPv6 because ICMP is Layer 3 agnostic.

Answer: C
Explanation:

QUESTION NO: 355

Which two network management models are supported by IPoDWDM? (Choose two.)

A. virtual transponder protocol management
B. segmented management
C. integrated management
D. traffic management
E. slow outages management

Answer: B,C
Explanation:

QUESTION NO: 356

The origin is a mandatory attribute that defines the origin of the path information.

Which three options are valid origin attributes? (Choose three.)

A. IBGP: NLRI is learned via intra-AS BGP.
B. EBGP: NLRI is learned via inter-AS BGP.
C. IGP: NLRI is interior to the AS of origination.
D. EGP: NLRI is learned via EGP.
E. INCOMPLETE. NLRI is unknown or learned some other way.

Answer: C,D,E
Explanation:

QUESTION NO: 357

Which carrier-grade IPv6 technology helps with IPv4 address depletion?

A. dual stack and NAT444
B. NAT444 and 6RD
C. NAT444 and DS-Lite
D. 6RD and DS-Lite

Answer: C
Explanation:

QUESTION NO: 358

Which mode does PPP interface use for peer authentication?

A. in-band
B. semi-in-band
C. out-band
D. semi-out-band
E. in-band and out-band

Answer: C
Explanation:

QUESTION NO: 359

In Ethernet Aggregation applications, which option is needed when the U-PE connects to an N-PE and broadband remote access server?

A. Ethernet Multipoint Service
B. E1
C. VPLS
D. DSLAM
E. wire emulation

Answer: D
Explanation:

QUESTION NO: 360

Which three options are functions of the Cisco Service Control Engine? (Choose three.)

A. intelligent inspection and control of IP packets
B. application of session-level bandwidth shaping
C. provisioning of access aggregation
D. per-subscriber bandwidth management
E. Implementation of VPN services

Answer: A,B,D

Explanation:

QUESTION NO: 361

Which statement about 6PE is true?

A. An additional address family was added to MP-BGP for the support of 6PE.
B. MP-iBGP is needed to support 6PE.
C. LDP is needed to support 6PE.
D. P routers need to be dual stack.
E. MP-eBGP is needed to support 6PE.

Answer: B

Explanation:

QUESTION NO: 362

Which three statements about 6VPE are true? (Choose three.)

A. An additional address family was added to MP-BGP to support 6VPE.
B. 6VPE routes are installed in the global routing table.
C. MP-BGP can be used to propagate routes between the PE and the CE.
D. 6VPE is functionally equivalent to VPNv4.

Answer: A,C,D

Explanation:

QUESTION NO: 363

Which three options are restrictions for MPLS VPN BGP Local Convergence? (Choose three.)

A. The MPLS VPN BGP Local Convergence feature affects only traffic that is exiting the VPN. Therefore, it cannot fully protect traffic end-to-end by itself.
B. This link protection can be initiated during a HA SSO. But links that were configured with this protection before the switchover begins remain protected after the switchover.
C. The MPLS VPN BGP Local Convergence feature for IPv4/IPV6 supports the eBGP, RIP, EIGRP,OSPF, and dynamic routing protocols.

D. Any next-hop core tunneling technology that is supported by BGP is also supported for protection, including MPLS, L2TPv3, and IP/GRE. CSC protocol between the PE and CE is also supported. Interautonomous system option A (back-to-back VRF) is supported because it is essentially the same as performing the PE-CE link protection in both autonomous systems. However, interautonomous system options B and C protection are not supported.
E. If you perform an in-service software downgrade from an image that does include this link protection to an image that does not support this feature, active protection is halted when BGP routes are refreshed.

Answer: A,D,E
Explanation:

QUESTION NO: 364

In MPLS VPN, where must MP-BGP peering be configured?

A. in all CE routers within a VPN community
B. in all CE routers across a VPN community
C. in all PE routers within a VPN community
D. in all PE routers across a VPN community
E. in all PE and CE routers within a VPN community
F. in all PE and CE routers across a VPN community

Answer: C
Explanation:

QUESTION NO: 365

One benefit of MPLS Layer 3 VPN is that migration for the end customer is simplified.

 Which statement is true?

A. There is no requirement to support MPLS on the PE router and modifications are required for a customer intranet.
B. There is no requirement to support MPLS on the PE router and no modifications are required for a customer intranet.
C. There is no requirement to support MPLS on the CE router and no modifications are required for a customer intranet.
D. There is requirement to support MPLS on the CE router and no modifications are required for a

customer intranet.

Answer: C
Explanation:

QUESTION NO: 366

Which statement describes a restriction of inter-AS MPLS VPN?

A. Allows a VPN to cross more than one service provider backbone.
B. Inter-AS functionality is available using both VPNv4 and VPNv6.
C. Inter-AS functionality is available using VPNv4 only.
D. Inter-AS functionality is available using VPNv6 only.

Answer: C
Explanation:

QUESTION NO: 367

Which option describes a benefit of IPv6 VPN Provider Edge?

A. Uses separate signaling plane, which provides more security than IPv4
B. No requirement for a separate signaling plane
C. Provides support for intra-AS and CSC scenarios
D. BGP is the preferred routing protocol for connecting two SPs.

Answer: B
Explanation:

QUESTION NO: 368

What is the port number of an IPSec Encapsulating Security Payload packet?

A. IP protocol 50
B. IP protocol 51
C. TCP port 50
D. TCP port 51
E. UDP port 50

F. UDP port 51

Answer: A
Explanation:

QUESTION NO: 369

Refer to the exhibit.
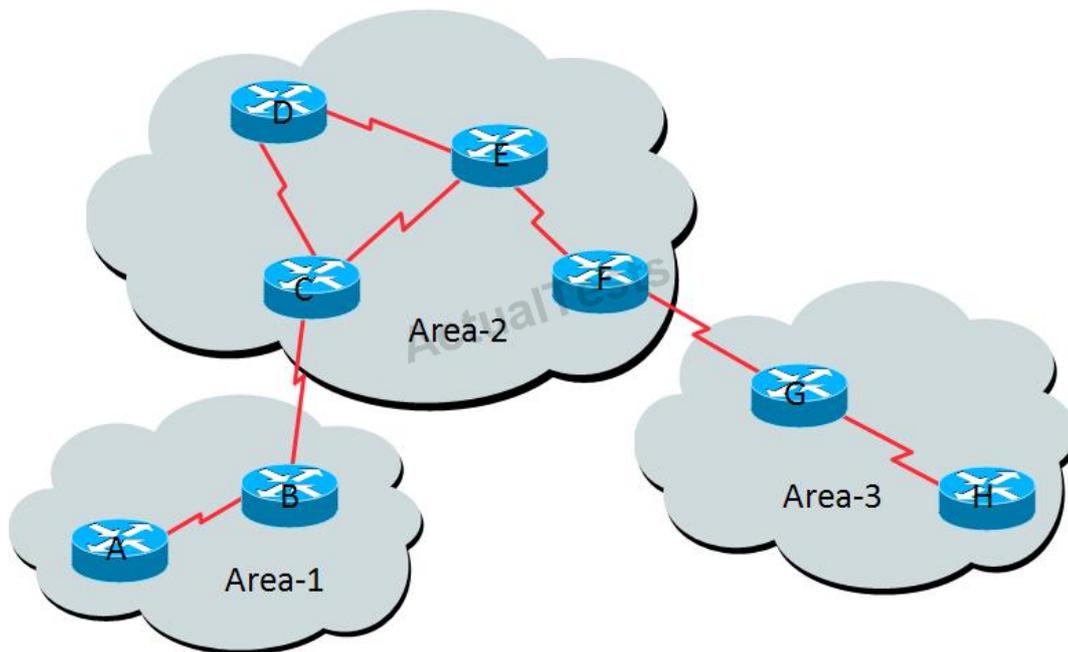
All routers are running IS-IS. Which three routers can be Level 1 Only routers? (Choose three.)

A. A
B. B
C. C
D. D
E. E
F. F
G. G
H. H

Answer: A,D,H
Explanation:

QUESTION NO: 370 DRAG DROP

Drag the IS-IS LSP packet on the left to the corresponding function on the right.	
CSNP	Establish and maintain adjacency
PSNP	Acknowledge acceptance of LSP update
IIH	Synchronize IS-IS database
LSP	Distribute and exchange routing information between IS-IS nodes

Answer:

Drag the IS-IS LSP packet on the left to the corresponding function on the right.	
CSNP	IIH
PSNP	PSNP
IIH	CSNP
LSP	LSP

Explanation:

IIH
PSNP
CSNP
LSP

QUESTION NO: 371 DRAG DROP

Drag the MPS label format on the left onto the correct target on right.

DLCI	Ethernet
NLPID	ATM
Label	Frame Relay
VPI	
VCI	
VPI and VCI	
VLAN ID	

Answer:

Drag the MPS label format on the left onto the correct target on right.

DLCI	Label
NLPID	VPI and VCI
Label	DLCI
VPI	
VCI	
VPI and VCI	
VLAN ID	

Explanation:

Label
VPI and VCI
DLCI

QUESTION NO: 372 DRAG DROP

Drag the OPSFv2 LSA type number on the left to the correct LSA name on the right.

1	NSSA External LSA
2	AS External LSA
3	Network LSA
4	Network Summary LSA
5	ASBR Summary LSA
6	Router LSA
7	Group Membership LSA

Answer:

Drag the OPSFv2 LSA type number on the left to the correct LSA name on the right.

1	7
2	5
3	2
4	3
5	4
6	1
7	6

Explanation:

7
5
2
3
4
1
6

QUESTION NO: 373 DRAG DROP

Drag the OSPFv3 LSA type number on the left to the correct LSA name on the right.	
0x2001	inter-area Prefix LSA
0x2002	AS External LSA
0x2003	Link LSA
0x2004	Router LSA
0x4005	intra-area Prefix LSA
0x2007	inter-area Router LSA
0x0008	Network LSA
0x2009	Type 7 LSA

Answer:

Drag the OSPFv3 LSA type number on the left to the correct LSA name on the right.	
0x2001	0x2003
0x2002	0x4005
0x2003	0x0008
0x2004	0x2001
0x4005	0x2009
0x2007	0x2004
0x0008	0x2002
0x2009	0x2007

Explanation:

0x2003

0x4005

0x0008

0x2001

0x2009

0x2004

0x2002

0x2007

QUESTION NO: 374 DRAG DROP

Drag the IS-IS TLV number on the left to the correct IS-IS TLV name on the right.	
1	IP internal reachability
2	IP external reachability
22	dynamic hostname
128	IS neighbors
129	protocols supported
130	extended IS reachability
132	area address
137	IP interface address

Answer:

Drag the IS-IS TLV number on the left to the correct IS-IS TLV name on the right.	
1	128
2	130
22	137
128	2
129	129
130	22
132	1
137	132

Explanation:

128
130
137
2
129
22
1
132

QUESTION NO: 375 DRAG DROP

Drag the actions on the left to the correct steps on the right to show how to perform an IOS-XR upgrade.

Install deactivate	Step 1
Install commit	Step 2
Install remove	Step 3
Install upgrade	Step 4
Install activate	Step 5
Install add	Step 6

Answer:

Drag the actions on the left to the correct steps on the right to show how to perform an IOS-XR upgrade.

Install deactivate	Install upgrade
Install commit	Install add
Install remove	Install activate
Install upgrade	Install commit
Install activate	Install deactivate
Install add	Install remove

Explanation:

Install upgrade
Install add
Install activate
Install commit
Install deactivate
Install remove

QUESTION NO: 376 DRAG DROP

Drag the protocol on left to the correct function on right to perform MPLS traffic engineering configuration with OSPF.

CSPF	path setup
OSPF	link information distribution
RSVP	forwarding traffic down tunnel
static route	path calculation

Answer:

Drag the protocol on left to the correct function on right to perform MPLS traffic engineering configuration with OSPF.

CSPF	RSVP
OSPF	OSPF
RSVP	static route
static route	CSPF

Explanation:

RSVP
OSPF
static route
CSPF

QUESTION NO: 377 DRAG DROP

Drag the command on the left to the correct step on the right to perform point-to-point Ethernet over MPLS configuration on a Cisco IOS-XR router.

interface name	Step 1
mpls static label	Step 2
xconnect group name	Step 3
l2vpn	Step 4
neighbor IP address pw-id value	Step 5
p2p name	Step 6

Answer:

Drag the command on the left to the correct step on the right to perform point-to-point Ethernet over MPLS configuration on a Cisco IOS-XR router.	
interface name	l2vpn
mpls static label	xconnect group name
xconnect group name	p2p name
l2vpn	interface name
neighbor IP address pw-id value	neighbor IP address pw-id value
p2p name	mpls static label

Explanation:

l2vpn
xconnect group name
p2p name
interface name
neighbor IP address pw-id value
mpls static label

QUESTION NO: 378 DRAG DROP

Drag the command on the left to the correct step on the right to perform VPLS configuration on a Cisco IOS-XR router.	
vfi name	Step 1
interface name	Step 2
bridge domain name	Step 3
bridge group name	Step 4
neighbor IP-address pw-id value	Step 5
l2vpn	Step 6

Answer:

Drag the command on the left to the correct step on the right to perform VPLS configuration on a Cisco IOS-XR router.	
vfi name	l2vpn
interface name	bridge group name
bridge domain name	bridge domain name
bridge group name	interface name
neighbor IP-address pw-id value	vfi name
l2vpn	neighbor IP-address pw-id value

Explanation:

l2vpn

bridge group name

bridge domain name

interface name

vfi name

neighbor IP-address pw-id value

QUESTION NO: 379 DRAG DROP

Drag the command on the left to the correct step on the right to perform Frame Relay interworking with Ethernet over MPLS on a Cisco IOS router.	
encapsulation mpls	Step 1
connect name serial-interface DLCI l2transport	Step 2
frame-relay switching	Step 3
xconnect IP address circuit-id pw-class name	Step 4
pseudowire-class name	Step 5
interworking	Step 6

Answer:

Drag the command on the left to the correct step on the right to perform Frame Relay interworking with Ethernet over MPLS on a Cisco IOS router.

encapsulation mpls	frame-relay switching
connect name serial-interface DLCI l2transport	pseudowire-class name
frame-relay switching	encapsulation mpls
xconnect IP address circuit-id pw-class name	interworking
pseudowire-class name	connect name serial-interface DLCI l2transport
interworking	xconnect IP address circuit-id pw-class name

Explanation:

frame-relay switching
pseudowire-class name
encapsulation mpls
interworking
connect name serial-interface DLCI l2transport
xconnect IP address circuit-id pw-class name

QUESTION NO: 380 DRAG DROP

Drag the command on the left to the correct step on the right to perform VPLS configuration on a Cisco IOS router.

neighbor ip-address send-community extended	Step 1
address-family l2vpn vpls	Step 2
neighbor ip-address activate	Step 3
l2 vfi vfi-name autodiscovery	Step 4
router bgp autonomous-system-number	Step 5
vpn id number	Step 6

Answer:

Drag the command on the left to the correct step on the right to perform VPLS configuration on a Cisco IOS router.	
neighbor ip-address send-community extended	l2 vfi vfi-name autodiscovery
address-family l2vpn vpls	vpn id number
neighbor ip-address activate	router bgp autonomous-system-number
l2 vfi vfi-name autodiscovery	address-family l2vpn vpls
router bgp autonomous-system-number	neighbor ip-address activate
vpn id number	neighbor ip-address send-community extended

Explanation:

l2 vfi vfi-name autodiscovery
vpn id number
router bgp autonomous-system-number
address-family l2vpn vpls
neighbor ip-address activate
neighbor ip-address send-community extended

QUESTION NO: 381 DRAG DROP

Drag the MPLS label element on the left to the correct length on the right.	
label value	1 bit
experimental use	3 bits
bottom of label stack	8 bits
TTL	20 bits

Answer:

Drag the MPLS label element on the left to the correct length on the right.

label value	bottom of label stack
experimental use	experimental use
bottom of label stack	TTL
TTL	label value

Explanation:

bottom of label stack
experimental use
TTL
label value
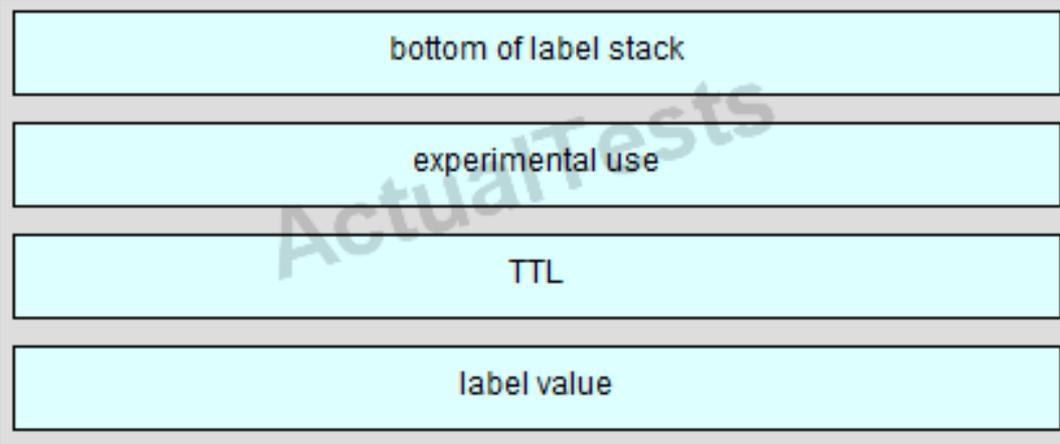
QUESTION NO: 382 DRAG DROP

Drag the Address Family Identifier number on the left to the correct protocol on the right.

1	DNS
2	L2VPN
16	IPv6
18	IPv4
25	AS number

Answer:

Drag the Address Family Identifier number on the left to the correct protocol on the right.

1	16
2	25
16	2
18	1
25	18

Explanation:

16

25

2

1

18

QUESTION NO: 383

One requirement of MP-BGP is that the NLRI and next hop both should belong to same address family. Similarly, if the route is a VPN route with an RD, the next hop should also be of the same address family.

For VPNv6 routes with an associated RD value, what is the RD for the next hop?

A. 16 because that is the global value for next hop RD.
B. 0 RD value.
C. Same as the RD for the VPN that is advertised.
D. Not enough information is available to determine the value.

Answer: B
Explanation:

QUESTION NO: 384

When the default MDT is configured, a multicast tunnel interface is created dynamically.

Which statement about MTI is true?

A. The MTI takes on the interface characteristics of same interface.
B. The MTI is the interface that connects the PE multicast environment to the service provider global environment.
C. The MTI is the interface that connects the customer multicast environment to the service provider global environment.
D. Unicast packets are forwarded over the MTI because this interface does not appear in the unicast routing table of the associated VRF.

Answer: C
Explanation:

QUESTION NO: 385

In MVPN GRE, what is the limitation for unicast GRE tunnels?

A. Support more than 500 GRE tunnels per system for multicast.
B. Transport header support is limited to IPv4.
C. Transport header support is limited to IPv6.
D. IPV4 multicast for GRE unicast tunnels is not supported.

Answer: B
Explanation:

QUESTION NO: 386

Refer to the exhibit.

```
*Mar  1 01:38:35.299:ISIS-Upd: TLV contents different, code 128
*Mar  1 01:38:35.300:ISIS-Upd: TLV code mismatch (2, 22)
*Mar  1 01:38:35.304:ISIS-Upd: TLV contents different, code 135

R4#show clns protocol
  System Id: 0000.0000.0004.00  IS-Type: level-1-2
  Generate narrow metrics: level-1-2
  Accept narrow metrics:   level-1-2
  Generate wide metrics:   none
  Accept wide metrics:     none

R4#show isis neighbors
System Id        Type Interface   IP Address      State Holdtime Circuit
R2               L1   Fa0/0       10.10.24.2      UP    23       R4.01
R2               L2   Fa0/0       10.10.24.2      UP    29       R4.01

R2#show clns protocol
  System Id: 0000.0000.0002.00  IS-Type: level-1-2
  Generate narrow metrics: none
  Accept narrow metrics:   none
  Generate wide metrics:   level-1-2
  Accept wide metrics:     level-1-2
```

Why is R4 unable to install any ISIS routes in the routing table?

A. ISIS LSP has an authentication issue.
B. No DR has been elected on this segment.
C. The metric style is mismatched.
D. Circuit levels are different.

Answer: C
Explanation:

QUESTION NO: 387

Refer to the exhibit.
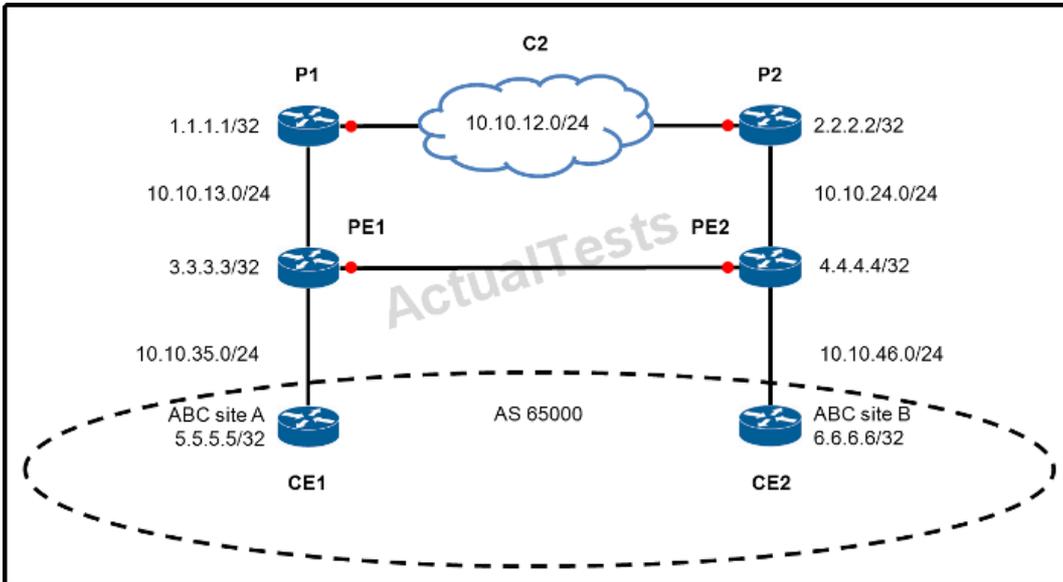
An engineer is viewing the CE1 routing table for CE2 Loopback 0. Each CE runs OSPF with its PE.

Which statement describes why the CE2 Loopback address is installed as an external OSPF route at the CE1 routing table?

A. PE1 and PE2 have mutual redistribution between OSPF and BGP.
B. CE2 is configured under OSPF with the command redistribute connected.
C. CE1 and CE2 are in different areas.
D. CE1 and CE2 have different OSPF processes.
E. PE1 and PE2 have different OSPF VRF processes.

Answer: E
Explanation:

QUESTION NO: 388

Refer to the exhibit.
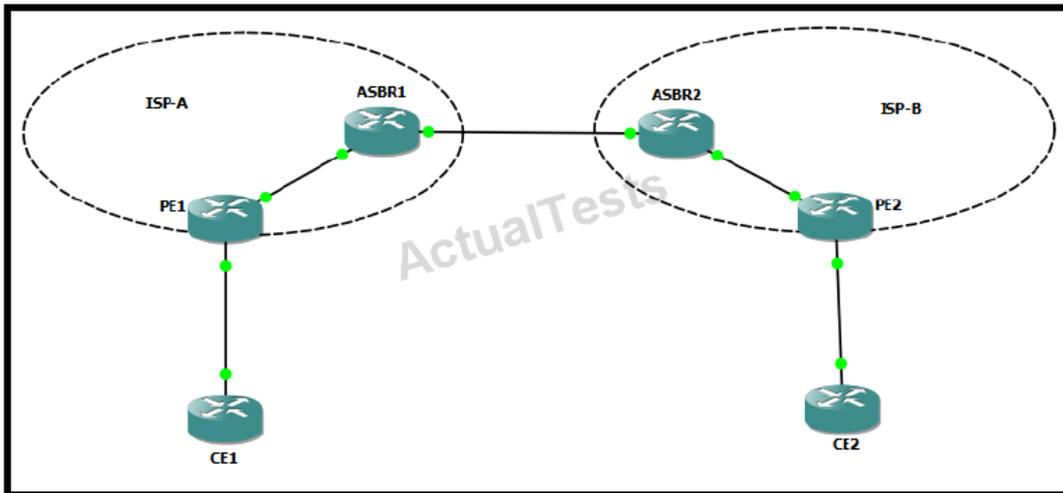
An inter-AS VPN between ISP-A and ISP-B is being deployed to support end-to-end connectivity for CE-1 and CE-2. For scalability reasons, the ASBR routers cannot exchange VPN routes for CE-1 and CE-2.

Which two configurations are needed to support this requirement? (Choose two.)

A. one VRF on the ASBRs for each CE
B. send-labels on the ASBRs
C. address-family VPNv4 on the ASBRs
D. ebgp-multihop between the PEs
E. ebgp-multihop between the ASBRs

Answer: B,D
Explanation:

QUESTION NO: 389

Refer to the exhibit.

```
XYZ-CE1#show ip route bgp | include 6.6.6.6
B          6.6.6.6 [20/0] via 10.10.35.3, 00:58:35

ABC-PE1#show ip bgp vpnv4 vrf XYZ 6.6.6.6/32
Paths: (1 available, best #1, table XYZ)
  65000
    4.4.4.4 from 4.4.4.4 (4.4.4.4)
    Origin incomplete, metric 0, localpref 100, valid, internal, best
      mpls labels in/out nolabel/18

ABC-PE1#show ip route 4.4.4.4 255.255.255.255
  Known via "bgp 100", distance 20, metric 0
  Tag 200, type external
  * 10.10.13.1, from 10.10.13.1, 00:01:30 ago
      MPLS label: none
```

AS 100 for ABC sites is used to carry XYZ customer traffic over ISP network. All routing between CEs to PEs are BGP-based. XYZ site 1 reports that it cannot reach XYZ site 2, although the destination network is installed in its routing table.

Which statement describes the cause of the problem?

A. LDP is not running between XYZ-CE1 and ABC_PE1.
B. LDP is not running between ABC_PE1 and PE1.
C. ABC_PE1 does not have an inbound label for subnet 6.6.6.6/32.
D. send-label command is missing from PE1 to ABC-PE1.

Answer: D
Explanation:

QUESTION NO: 390

A network engineer is trying to optimize convergence.

What action should be taken to overcome EBGP frequent session loss due to interface flapping between two different AS routers?

A. Tune the BGP session time-out.
B. Disable bgp fast-external-fallover.
C. Enable bgp fast-external fallover.
D. Use disable-connected-check.
E. Enable neighbor fall-over.

Answer: B
Explanation:

QUESTION NO: 391

A security agency wants to use the services of the service provider to interconnect the remote sites. However, they do not want to share the IP addresses of their sites and they want end-to-end security.

Which three services meet the design requirements? (Choose three.)

A. client mode VPN
B. tunnel mode VPN
C. L2VPN
D. L3VPN
E. PPTP
F. SSL VPN

Answer: A,B,C
Explanation:

QUESTION NO: 392

A network engineer is using IS-IS IGP protocol to design a network.

Which three design elements should be used to divide the network into a hierarchy of areas? (Choose three.)

A. Core routers will be only level-2.
B. Routers on the edge of the network will be only level-1.
C. Router between core and edge routers will be level-1-2.
D. Core routers will be only level-1.
E. Routers on the edge of the network will be only level-2.
F. Router between core and edge routers will be only level-2.
G. Router between core and edge routers will be only level-1.

Answer: A,B,C
Explanation:

QUESTION NO: 393

Refer to the exhibit.
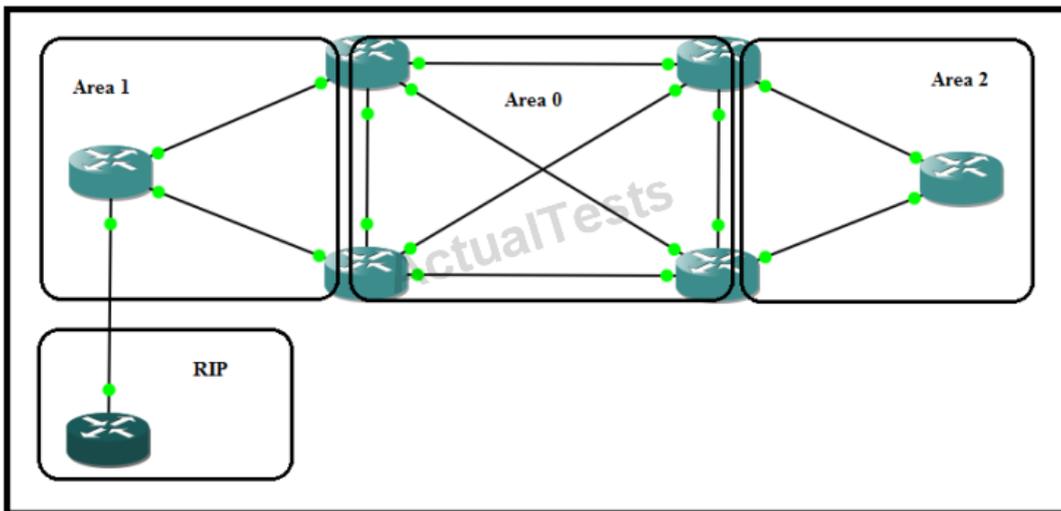
RIP network 192.168.1.0/24 is redistributed in OSPF Area 1; both Area 1 and Area 2 are configured as NSSAs.

Which three statements describe the OSPF behavior in this scenario? (Choose three.)

A. Area 2 does not see the network 192.168.1.0/24 in its link-state database.

B. Network 192.168.1.0/24 is advertised in a Type 7 LSA in Area 1.
C. Network 192.168.1.0/24 is advertised in a Type 5 LSA in Area 0.
D. Network 192.168.1.0/24 is advertised in a Type 7 LSA in Area 0.
E. ABR between Area 0 and Area 2 converts network 192.168.1.0/24 to a Type 7 LSA.
F. Network 192.168.1.0/24 is advertised in a Type 5 LSA in Area 2.

Answer: A,B,C
Explanation:

QUESTION NO: 394

A network engineer wants to deploy a VPLS service within the MPLS backbone. The backbone expert team advises that LDP for signaling is used.

Which two characteristics of LDP would influence their decision? (Choose two.)

A. BGP does not need to be run on the PE device.
B. Non-convergence with IP VPN operation.
C. There is no autodiscovery.
D. LDP signaling requires a loopback-based router ID.
E. CDP is not required on the PE routers.

Answer: A,C
Explanation:

QUESTION NO: 395

A network engineer wants to support Ethernet over MPLS and wants to share only a single VC across the MPLS backbone.

Which EoMPLS mode supports this feature?

A. port
B. VLAN
C. cell
D. frame
E. tunnel

Answer: A

Explanation:

QUESTION NO: 396

A customer requests that sites are connected over an MPLS backbone using the MPLS AToM service. However, the network engineer advises that the MPLS L3VPN service may be better for this situation. Which characteristic of MPLS L3VPN may make it a better option from the Service Provider perspective?

A. Reduction of operational complexity.
B. Support for multiple network layer protocols, such as IP, IPX, and SNA
C. Customer Layer 2 information will be maintained over the service provider core.
D. Transparent to the customer

Answer: A

Explanation:

QUESTION NO: 397

Refer to the exhibit.
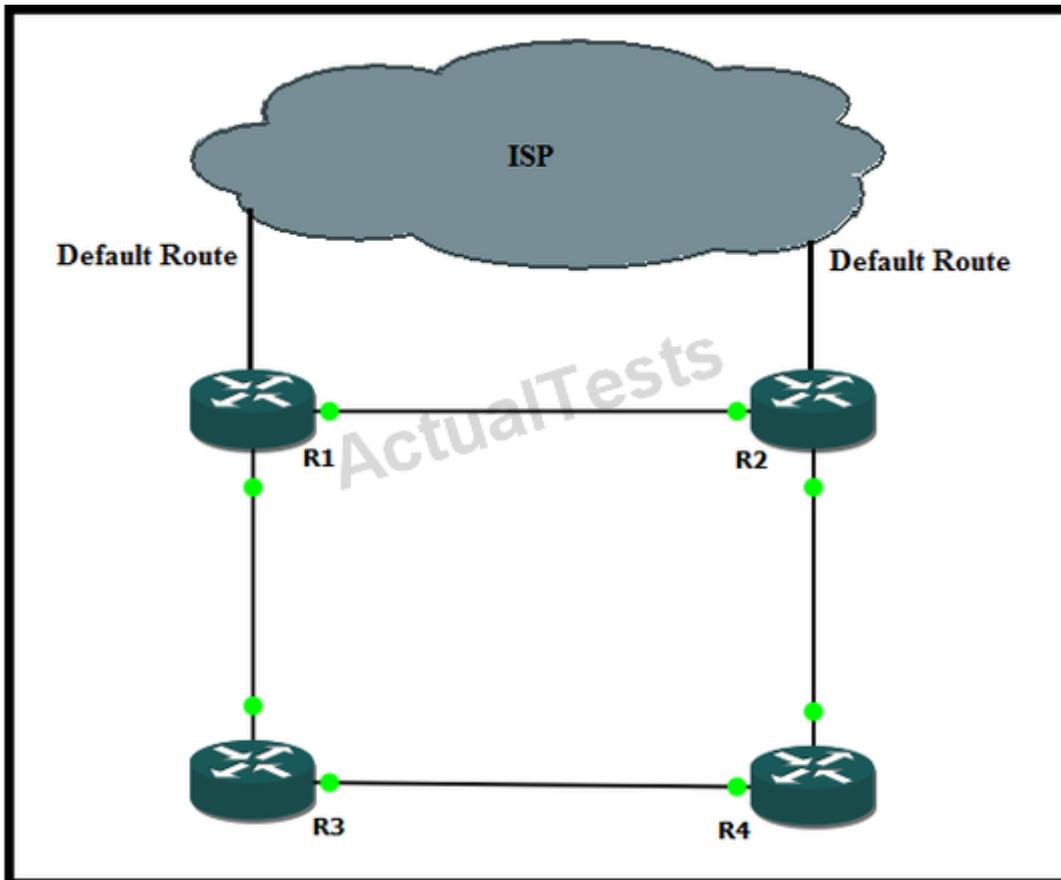
R1 and R2 have a static default route that is configured to point toward the ISP. Both R1 and R2 routers redistribute the default route into OSPF. R2 is the primary gateway toward the ISP and R1 is the backup gateway. All link metrics are the same. Which two steps ensure that traffic to the ISP flows through R2 when the network works properly? (Choose two.)

A. Modify the preference value of the default route on R1 so that it is less preferred than OSPF external routes.
B. Modify the preference value of the default route on R2 so that it is less preferred than OSPF external routes.
C. Redistribute the default route as a type 1 external route on R1 and a type 2 external route on R2.
D. Redistribute the default route as a type 2 external route on R1 and a type 1 external route on R2.
E. Redistribute the default route on R1 with a higher metric than the existing metric of the distributed default route on R2.

Answer: A,D
Explanation:

QUESTION NO: 398

Refer to the exhibit.

```
Lo0: 2001:db8::1/128          Lo0: 2001:db8::2/128              Lo0: 2001:db8::3/128

   R1              OSPF 1         R2         BGP AS 23         R3
        .1                  .2        2              .3
              2001:10:10:12::/64          2001:10:10:23::/64


R2#show running-config | section router bgp
router bgp 23
redistribute ospf 1
 neighbor 10.10.23.3 remote-as 23
 neighbor 2001:10:10:23::3 remote-as 23
!
 address-family ipv6
  redistribute ospf 1
  neighbor 2001:10:10:23::3 activate

R3#show bgp ipv6 unicast
   Network            Next Hop           Metric LocPrf Weight Path
*>i2001:DB8::1/128   2001:10:10:23::2        1    100      0    ?
```

A company is deploying IPv6 using a dual-stack approach. OSPFv2 is used for IPv4 routing and is redistributed into the BGP IPv4 address family. The network engineer also needs to enable OSPFv3 for IPv6 routing using the same design that is used for OSPFv2. All prefixes in the OSPFv3 database must be redistributed into the BGP IPv6 address family at router R2, but R3 does not receive the loopback 0 IPv6 address of R2 via BGP. Which action will fix this problem?

A. redistribution of BGP routes into OSPFv3
B. redistribution of OSPFv3 routes into BGP with include-connected
C. mutual redistribution of OSPFv3 and BGP routes
D. redistribution of connected OSPFv3 routes

Answer: B
Explanation:

QUESTION NO: 399

A network engineer is tasked with supporting traffic discrimination over MPLS traffic engineering tunnels. To allocate restricted bandwidth to a certain type of traffic with no QoS degradation, which technique must be used?

A. integrated services
B. MPLS TE Diff-Serv full allocation model
C. MPLS TE Diff-Serv Russian doll model
D. IP precedence

E. class of service

Answer: C
Explanation:

QUESTION NO: 400

In an OSPF domain, four routers are running the OSPF protocol over a LAN switch in a broadcast domain. What is the expected output of executing the show ip OSPF neighbor command on the router that is neither a DR nor a BDR?

A. one FULL state, two 2WAY states
B. two FULL states, one 2WAY state
C. three FULL states
D. three 2WAY states

Answer: B
Explanation:

QUESTION NO: 401

A security risk has been discovered on the Service Provider MPLS core network during a network audit. Traceroute between the customer sites displays IP addresses of the Service Provider MPLS core. What should be done to hide the IP addresses of the Service Provider MPLS core from the customer traceroute utility?

A. Configure an access list to block traceroute traffic.
B. Apply the no mpls ip propagate-ttl forward command.
C. Enable MPLS LDP session protection.
D. Configure an LDP label allocation filter.
E. Apply the no mpls ip propagate-ttl local command.

Answer: B
Explanation:

QUESTION NO: 402

An engineer is configuring a Cisco CRS-1 Multishelf System. Which option describes the minimum LCC and FCC requirements for proper functionality?

A. two LCCs and one FCC
B. one LCC and one FCC
C. two LCCs and two FCCs
D. one LCC and two FCCs

Answer: B
Explanation:

QUESTION NO: 403

Refer to the exhibit.


```
R4#show ip route ospf | begin 1.1
O        1.1.1.1 [110/3] via 10.10.34.3, 00:01:12, FastEthernet0/1
                 [110/3] via 10.10.24.2, 00:01:22, FastEthernet0/0
      2.0.0.0/32 is subnetted, 1 subnets
O        2.2.2.2 [110/2] via 10.10.24.2, 00:01:22, FastEthernet0/0
      3.0.0.0/32 is subnetted, 1 subnets
O        3.3.3.3 [110/2] via 10.10.34.3, 00:01:12, FastEthernet0/1
      10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
O        10.10.12.0/24 [110/2] via 10.10.24.2, 00:01:22, FastEthernet0/0
O        10.10.13.0/24 [110/2] via 10.10.34.3, 00:01:12, FastEthernet0/1
```

Which command group does a network administrator use to filter out R3 (3.3.3.3 subnet) from the R4 routing table?

A. R4(config)# router ospf 1
distribute-list prefix-list filter in
B. R2(config)# router ospf 1
distribute-list prefix-list filter out Fa0/1
C. R4(config)# router ospf1
distribute-list prefix-list filter in Fa 0/0
D. R3(config)# router ospf 1
distribute-list prefix-list filter out Fa 0/0

Answer: A
Explanation:

QUESTION NO: 404

In an OSPF domain, four routers have OSPF neighborship over a broadcast domain. What is the expected state after running the show ip OSPF neighbor command on the OSPF designated router?

A. one FULL state, two 2WAY states
B. two FULL states, one 2WAY state
C. three FULL states
D. three 2WAY states

Answer: C
Explanation:

QUESTION NO: 405

Refer to the exhibit.

Router1   Router2   Router3

Router1 —Area1—— Router2 ——Area0— Router3

Router-ID:
209.165.210.3

Router2#sh ip ospf database router 209.165.201.3

OSPF Router with ID (209.165.202.130) (Process ID 1)

Router Link States (Area 1)

LS age: 538
Options: (No TOS-capability, DC)
LS Type: Router Links
Link State ID: 209.165.201.3
Advertising Router: 209.165.201.3
LS Seq Number: 80000004
Checksum: 0x38CE
Length: 72
Number of Links: 4

 Link connected to: a Stub Network
  (Link ID) Network/subnet number: 209.165.201.2
  (Link Data) Network Mask: 255.255.255.255
   Number of TOS metrics: 0
    TOS 0 Metrics: 1

 Link connected to: a Stub Network
  (Link ID) Network/subnet number: 209.165.201.1
  (Link Data) Network Mask: 255.255.255.255
   Number of TOS metrics: 0
    TOS 0 Metrics: 1

 Link connected to: another Router (point-to-point)
  (Link ID) Neighboring Router ID: 209.165.202.130
  (Link Data) Router Interface address: 209.165.200.225
   Number of TOS metrics: 0
    TOS 0 Metrics: 1

 Link connected to: a Stub Network
  (Link ID) Network/subnet number: 209.165.200.224
  (Link Data) Network Mask: 255.255.255.224
   Number of TOS metrics: 0
    TOS 0 Metrics: 1

Router 2 connects OSPF area 1 and area 0. Router 2 receives LSA type 1 from Router 1 in area 1. How many type 3 LSAs will be generated by Router 2 into area 0 to advertise all prefixes that are announced by the Router 1 LSA type 1 packet?

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

Answer: C
Explanation:

QUESTION NO: 406

Two OSPF neighbor routers are stuck in the EXSTART state. After a while, the neighborship goes down. A network engineer is debugging the issue when both routers show the OSPF log message "too many retransmissions." What is the possible root cause?

A. OSPF area mismatch
B. OSPF hello-interval mismatch
C. interface MTU mismatch
D. interface network type mismatch

Answer: C
Explanation:

QUESTION NO: 407

Refer to the exhibit.

```
R2#show mpls ldp bindings
   tib entry: 1.1.1.1/32, rev 11
        remote binding: tsr: 1.1.1.1:0, tag: imp-null
   tib entry: 2.2.2.2/32, rev 12
        remote binding: tsr: 1.1.1.1:0, tag: 16
   tib entry: 3.3.3.3/32, rev 13
        remote binding: tsr: 1.1.1.1:0, tag: 17
   tib entry: 10.10.12.0/24, rev 14
        remote binding: tsr: 1.1.1.1:0, tag: imp-null
   tib entry: 10.10.13.0/24, rev 15
        remote binding: tsr: 1.1.1.1:0, tag: imp-null

R2#show mpls forwarding-table
Local   Outgoing    Prefix          Bytes tag  Outgoing    Next Hop
tag     tag or VC   or Tunnel Id    switched   interface
```

Routers R1 and R2 have exchanged label binding information. What is preventing the labels from populating the MPLS forwarding table?

A. MTU on the serial interface cannot accommodate labels.
B. Cisco Express Forwarding is not running.
C. The MPLS label distribution protocol is mismatched.
D. Inbound access list 100 is applied on the serial interface.

Answer: B
Explanation:

QUESTION NO: 408

A router is able to assign labels to the prefixes and MPLS is enabled on all of the router interfaces. However, this router is unable to establish an LDP session with its LDP neighbors. What could be the cause of this problem?

A. ip cef is not enabled.
B. mpls ip is missing in the global configuration mode.
C. The LDP router ID is unreachable.
D. LIB has no label.

Answer: C
Explanation:

QUESTION NO: 409

A network engineer is responsible for provisioning LDP and IGP over the IP core network to maintain the MPLS functionality as a day-to-day task. The IP engineer is looking for automation opportunities. Which feature allows the LDP protocol to be automatically enabled on interfaces that run IGP on the routers?

A. MPLS LDP autoconfiguration
B. MPLS LDP discovery
C. MPLS LDP-IGP synchronization
D. MPLS LDP session protection

Answer: A
Explanation:

QUESTION NO: 410

A network engineer wants to avoid route looping in an internal BGP. Which two BGP attributes are used by a route reflector to avoid this issue? (Choose two.)

A. originator ID
B. secure ID
C. cluster ID
D. network ID
E. reflector ID

Answer: A,C
Explanation:

QUESTION NO: 411

Refer to the exhibit.

```
R3#show ip bgp 1.1.1.1
BGP routing table entry for 1.1.1.1/32, version 11
Paths: (1 available, no best path)
  Not advertised to any peer
  1
    10.10.12.1 (inaccessible) from 10.10.23.2 (2.2.2.2)
      Origin incomplete, metric 0, localpref 100, valid, internal
```
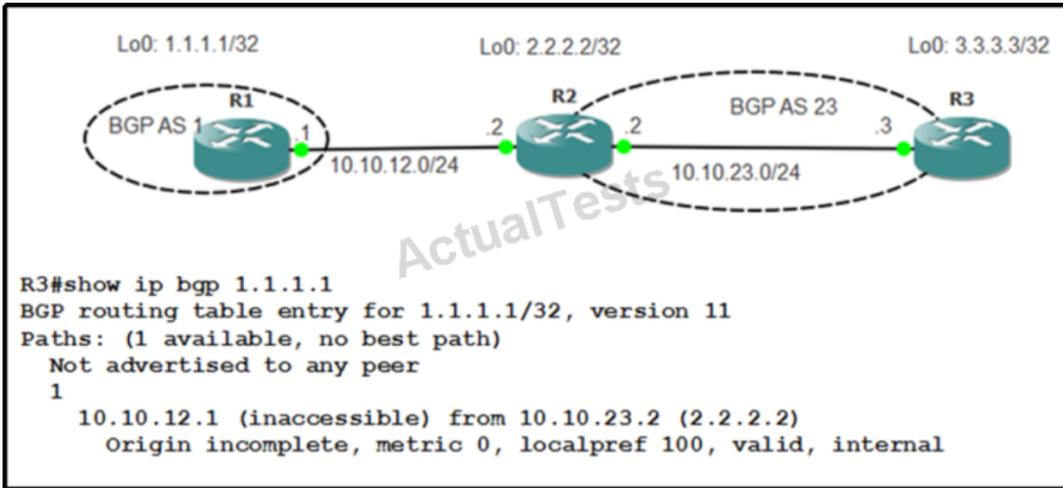
R3 is not able to install the R1 loopback address into its BGP routing table. What should be configured to install that route?

A. Configure R2 as a route reflector.
B. Enable EBGP multihop on R2.
C. Change the origin attribute to IGP on R3.
D. Configure the next-hop-self command on R2.
E. Configure the next-hop-unchanged command on R2.
F. Add a static route to reach 10.10.23.2 on R3.

Answer: D
Explanation:

QUESTION NO: 412

Refer to the exhibit.
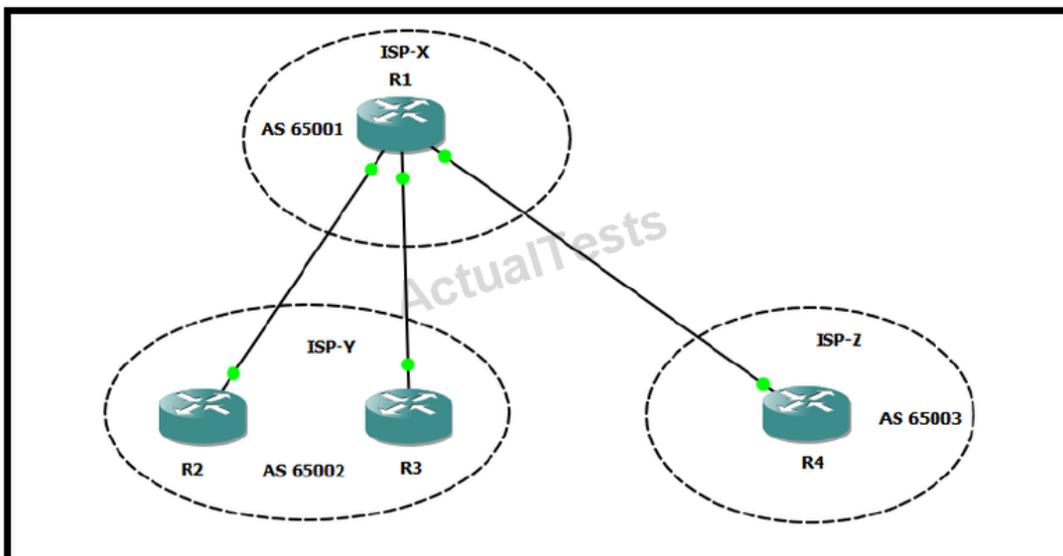
ISP-X customers must be able to reach both ISP-Y and ISP-Z, but ISP-X must not allow transit traffic between ISP-Y and ISP-Z at any time. Which two options satisfy this requirement? (Choose two.)

A. Use the MED to prefer the proper routes.
B. Use communities to identify and filter routes.
C. Use the atomic aggregate attribute.
D. Use a route map to filter routes on the AS number.
E. Use local preference to prefer the routes.

Answer: B,D
Explanation:

QUESTION NO: 413

A network engineer is having trouble overcoming a BGP rulE. "an EBGP neighbor address information is carried in the IBGP advertisement. This information does not change to the local ASBR address". Which BGP attribute can be modified to solve this network reachability issue in this type of scenario?

A. AS path
B. origin
C. weight
D. next-hop

Answer: D
Explanation:

QUESTION NO: 414

The SP core supports PIM-SM for multicast traffic, but one of these routers is not able to see one of its PIM neighbors. What is the most likely cause of this issue?

A. The router is an RP with high priority.
B. IGMP snooping is not enabled.
C. PIM sparse mode is not enabled on a participating multicast interface.
D. PIM protocols are not enabled in global configuration mode.
E. Auto-RP is not enabled on this network.

Answer: C

Explanation:

QUESTION NO: 415

Refer to the exhibit.
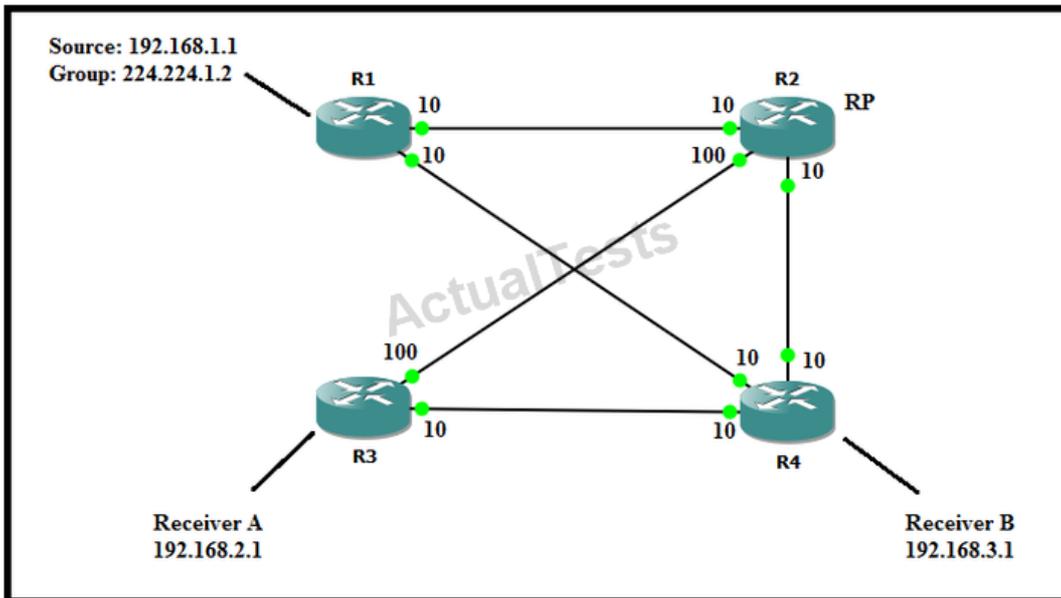
There are receivers that are registered at the RP. If the source begins sending multicast traffic toward R1, how will R1 handle that traffic?

A. R1 forwards the multicast packets on the (S, G) tree toward the RP.
B. R1 encapsulates the multicast packets into a PIM register multicast packet.
C. R1 encapsulates the multicast packets into a PIM join unicast packet.
D. R1 tunnels the multicast packets in PIM register messages toward the RP.

Answer: D
Explanation:

QUESTION NO: 416

A network architect is tasked to design and deploy multicast in a service provider core. There is a requirement to have two PIM RP routers for PIM-SM distribute mode. What can the network architect do to satisfy this requirement?

A. Set two RPs with same priority.
B. Set two RPs, one with high priority and the other with low priority.
C. Set one RP as the main RP and another as a backup RP.
D. Set the RP-BSR method with one high-priority RP and one low-priority RP.

Answer: D

Explanation:

QUESTION NO: 417

Which three of these options can be a forwarding equivalence class? (Choose three.)

A. groups of IP addresses
B. bridge or switch instance
C. traffic engineering tunnel
D. IPsec tunnel
E. routing equivalence paths
F. a bgp prefix

Answer: A,B,C

Explanation:

QUESTION NO: 418

Which two statements best describe the functionality of the BGP graceful restart capability? (Choose two.)

A. The peer router sends an end-of RIB message to the restarting router.
B. The peer router immediately removes the BGP routes that it learned from the restarting router from its BGP routing table.
C. The restarting router does not remove any stale prefixes after the timer for stale entries expires.
D. The router establishes BGP sessions with other routers and relearns the BGP routes from other routers that are also capable of graceful restart. The restarting router waits to receive updates from the neighboring routers. When the neighboring routers send end-of-RIB messages to indicate that they are done sending updates, the restarting router starts sending its own updates.
E. The restarting router removes any stale prefixes after the timer for stale entries expires.

Answer: D,E

Explanation:

QUESTION NO: 419

Refer to the exhibit.

```
                              AS 123
     R3           R1                   AS 2 R2


          AS 13


router bgp 13
 bgp confederation identifier 123
 bgp confederation peers 2
 bgp suppress-inactive
 network 11.11.11.11 mask 255.255.255.255
 neighbor 10.10.12.2 remote-as 2
 neighbor 10.10.12.2 advertise-map SUBNET_A non-exist-map SUBNET_B
 neighbor 10.10.13.3 remote-as 13

ip prefix-list SUBNET_A seq 5 permit 33.33.33.33/32
ip prefix-list SUBNET_B seq 5 permit 11.11.11.11/32

route-map SUBNET_A permit 10
 match ip address prefix-list SUBNET_A
route-map SUBNET_B permit 10
 match ip address prefix-list SUBNET_B

R1#show ip bgp 33.33.33.33
BGP routing table entry for 33.33.33.33/32, version 6
Paths: (1 available, best #1, table Default-IP-Routing-Table, RIB-
failure(17))
  Not advertised to any peer
  Local
     10.10.13.3 from 10.10.13.3 (33.33.33.33)
       Origin IGP, metric 0, localpref 100, valid, confed-internal, best

R1#show ip route 33.33.33.33
Routing entry for 33.33.33.33/32
  Known via "ospf 1", distance 110, metric 11, type intra area
  * 10.10.13.3, from 10.10.13.3, 00:02:42 ago, via FastEthernet0/1

R1#show ip route 11.11.11.11
Routing entry for 11.11.11.11/32
  Known via "connected", distance 0, metric 0 (connected, via interface)

R2#show ip bgp 33.33.33.33
% Network not in table
```

Based on the topology, the BGP configuration in R1, and the outputs from R1 and R2; identify why was subnet 33.33.33.33/32 not received on the R2 BGP table?

A. R2 is not a route reflector client for R1.
B. R1 is configured to suppress all inactive (RIB failure) routes.
C. The 33.33.33.33/32 subnet must be learned through BGP.
D. The 11.11.11.11/32 subnet exists in the routing table.

Answer: D
Explanation:

QUESTION NO: 420

Refer to the exhibit.

```
R1                  10.10.12.0/24        R2
                   f0/0   AS 12   f0/0
1.1.1.1/32                    2.2.2.2/32

R2#show ip ospf neighbor
Neighbor ID      Pri   State          Dead Time    Address        Interface
1.1.1.1            1   FULL/BDR       00:00:37     10.10.12.1     FastEthernet0/0

R2#show mpls forwarding-table
Local      Outgoing   Prefix           Bytes Label  Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched     interface

R2#show ip route 1.1.1.1
Routing entry for 1.1.1.1/32
  Known via "bgp 12", distance 200, metric 0, type internal
  * 10.10.12.1, from 10.10.12.1, 00:01:31 ago

R2#show ip interface fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
  Internet address is 10.10.12.2/24
  MTU is 1400 bytes
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP CEF Fast switching turbo vector
```

The R1 and R2 routers are running OSPF, LDP, and BGP. Why is the label for 1.1.1.1 prefix absent in the R2's MPLS forwarding table?

A. IP MTU cannot accommodate labels.
B. The MPLS tunnel is not enabled for the Fast Ethernet 0/0 interface.
C. The subnet is not learned via OSPF.
D. The bgp send-label command is not enabled between R1 and R2.

Answer: C
Explanation:

QUESTION NO: 421

A network engineer is redistributing BGP prefixes into RIP. These prefixes are unreachable in the RIP network. Which the two actions could resolve the issue based on this scenario? (Choose two.)

A. Enable BGP synchronization.
B. Enable BGP AS-override.
C. Rewrite RIP hop count for the redistributed prefixes.
D. Enable internal BGP redistribution.
E. Rewrite BGP next hop.
F. Apply BGP next-hop-self.

Answer: C,D

Explanation:

QUESTION NO: 422

Which are the three mandatory BGP attributes? (Choose three.)

A. AS path
B. origin
C. local preference
D. next hop
E. MED value
F. communities

Answer: A,B,D

Explanation:

QUESTION NO: 423

An engineer is designing a security method for a service provider company that needs to secure BGP peering with external peers. Based on the options provided, which three security precautions should be taken? (Choose three.)

A. Enable BGP neighbor authentication with MD5.
B. Enable the BGP Time to Live Security Check feature.
C. Limit the AS path length.
D. Disable ebgp-multihop.
E. Enable bgp bestpath as-path ignore.
F. Enable bgp-policy.

Answer: A,B,C

Explanation:

QUESTION NO: 424

Refer to the exhibit.
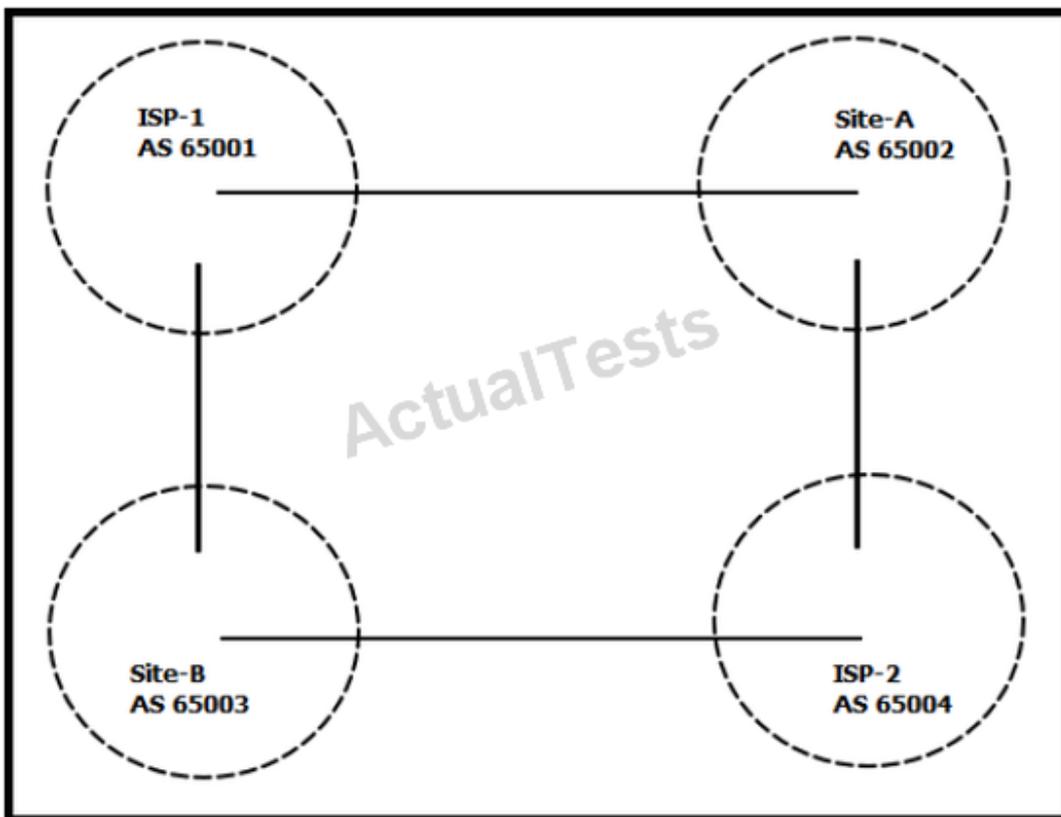
Each AS domain contains more than one BGP router. Site-B sends traffic to ISP-1 over a directly connected link, but Site-B is not used as an AS transit for the ISP-1 backbone. How should the routes be advertised by ISP-1 towards Site-B to accomplish this task?

A. Prefixes from site-A should be advertised with the no-export community
B. Prefixes from site-B should be advertised with the no-export community
C. Prefixes from site-B should be advertised with the no-advertise community
D. Prefixes from site-A should be advertised with the as-path prepend attribute
E. Prefixes from site-A should be advertised with the no-advertise community

Answer: B
Explanation:

QUESTION NO: 425

A customer is connected to a service provider by a low-speed link and wants to increase the bandwidth of this connectivity without creating additional IP addresses. Multiple physical links with

the same bandwidth value are already available between the customer and the service provider. Which technology can be used to achieve these requirements?

A. HDLC
B. PPTP
C. Multilink PPP
D. Frame Relay

Answer: C
Explanation:

QUESTION NO: 426

A company has a backup T1 link to its corporate head office. To minimize costs, the company will use the T1 link only for email downloads from the corporate email server. The PPP dialer initiates only when the internal server initiates an email connection to the corporate email server. However, the PPP connection does not disconnect after emails are downloaded. What is the cause of this issue?

A. The dialer-map command is not configured.
B. The interface is not added in the dialer-group command.
C. The dialer-list command is incorrectly configured.
D. The dialer time-out command is not configured.

Answer: C
Explanation:

QUESTION NO: 427

A router is unable to route packets over a PPPoE link. What could be the cause of this issue?

A. incorrect IPCP connection for the agreed-upon IP address
B. incorrect dialer map profile
C. incorrect username of the PPP connection
D. incorrect access list

Answer: B
Explanation:

QUESTION NO: 428

Two routers that use a POS interface are connected back-to-back. The interfaces are operational with no alarms appearing. When the routers are connected using an SDH network, alarms appear on the router and the interface status goes down. Which action will fix this issue?

A. Reset the POS interface.
B. Check the ADM switch for correct framing.
C. Change the framing type on the router POS interface.
D. Swap the POS interface.

Answer: C
Explanation:

QUESTION NO: 429

Refer to the exhibit.

The link payload rate is subdivided into multiple fixed-rate channels. In addition, the data rate of a single cell or packet flow is limited by the bandwidth of an individual channel. If the link is an OC-48, into how many channels can the link be subdivided?

A. four OC-12 channels
B. two OC-24 channels
C. one OC-48 channel
D. three OC-16 channels

Answer: A
Explanation:

QUESTION NO: 430

A company is using a Layer 2 Frame Relay network. Which circuit emulation will a network engineer use to extend the customer Frame Relay network over the Service Provider backbone?

A. GRE
B. L3VPN
C. AToM
D. VPLS

Answer: C
Explanation:

QUESTION NO: 431

Refer to the exhibit.


```
PE1#show running-config | section router bgp
router bgp 12
 address-family ipv4 vrf ABC
  neighbor 10.10.13.3 remote-as 65000
  neighbor 10.10.13.3 activate
  neighbor 10.10.13.3 as-override

PE2#show running-config | section router bgp
router bgp 12
 address-family ipv4 vrf ABC
  neighbor 10.10.24.4 remote-as 65000
  neighbor 10.10.24.4 activate
```
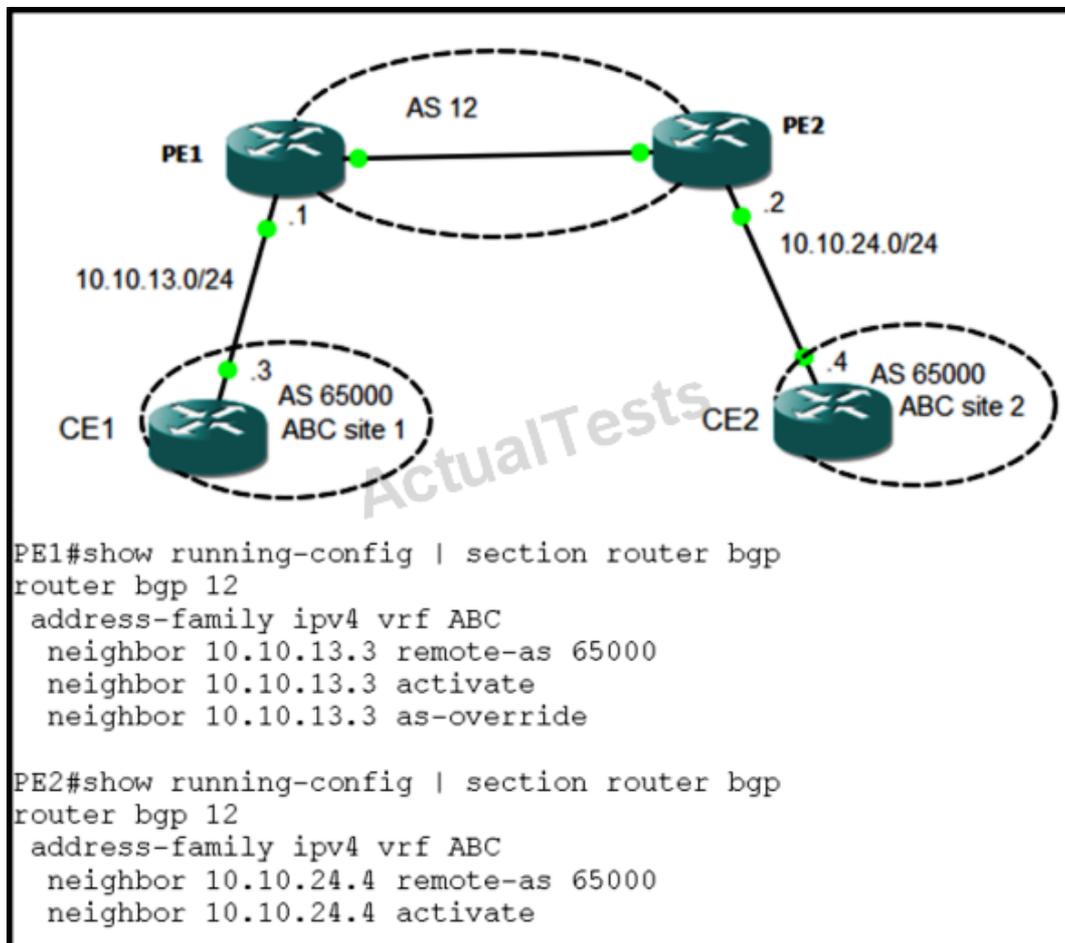
An MPLS VPN service has been provisioned for an ABC customer. Based on the output from the VRF BGP configuration of PE1 and PE2, which statement describes the route exchange between ABC site 1 and site 2?

A. Only CE1 will be able to install CE2 BGP updates in its BGP table.
B. Only CE2 will be able to install CE1 BGP updates in its BGP table.

C. CE1 can install the CE2 subnets in its BGP table and CE2 can install the CE1 subnets its BGP table.

D. CE1 cannot install the CE2 subnets in its BGP table and CE2 cannot install the CE1 subnets its BGP table.

E. "as-override" feature cannot be used in this scenario.

Answer: A

Explanation:

QUESTION NO: 432

A network engineer observes increasing output drops on the serial interface. Which two solutions can be implemented to minimize these drops? (Choose two.)

A. Increase the MTU size on the link.
B. Replace the serial cable between the connecting devices.
C. Turn on fast switching.
D. Increase the output hold queue size.
E. Implement priority queuing on slower serial links by configuring priority lists.

Answer: D,E

Explanation:

QUESTION NO: 433

A network engineer is connecting a router that is not manufactured by Cisco to a Cisco 7613 Router with a 10 Gigabit Ethernet Route Switch Processor uplink interface. The uplink interface is not in shutdown mode, but the interface does not come up. What is the most likely cause of the issue in this scenario?

A. The remote device does not support 10 Gigabit Ethernet.
B. Autonegotiation is enabled.
C. There is a faulty interface.
D. There is a faulty cable.

Answer: B

Explanation:

QUESTION NO: 434

An ISP provides DSL services to home customers. Each customer is given a username and a password. The ISP RADIUS server is configured to send a challenge to its clients along with the server hostname. Which two protocols should be used to deliver this service? (Choose two.)

A. PPP
B. PPPoE
C. PAP
D. CHAP
E. HDLC

Answer: B,D
Explanation:

QUESTION NO: 435

Refer to the exhibit.
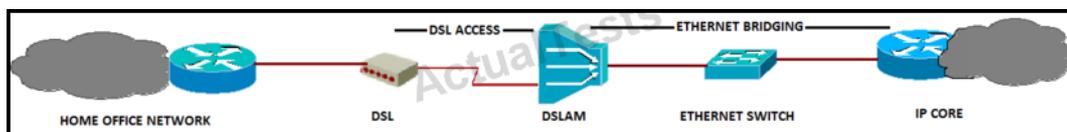
A home office user sends IP datagrams from the local router, which sends Ethernet datagrams to the DSL modem. The DSL modem encapsulates the Ethernet frames in which frame format before sending them over the physical DSL link to DSLAM?

A. RFC 1483
B. PPPoE
C. PPPoA
D. IP over ATM

Answer: A
Explanation:

QUESTION NO: 436

Refer to the exhibit.
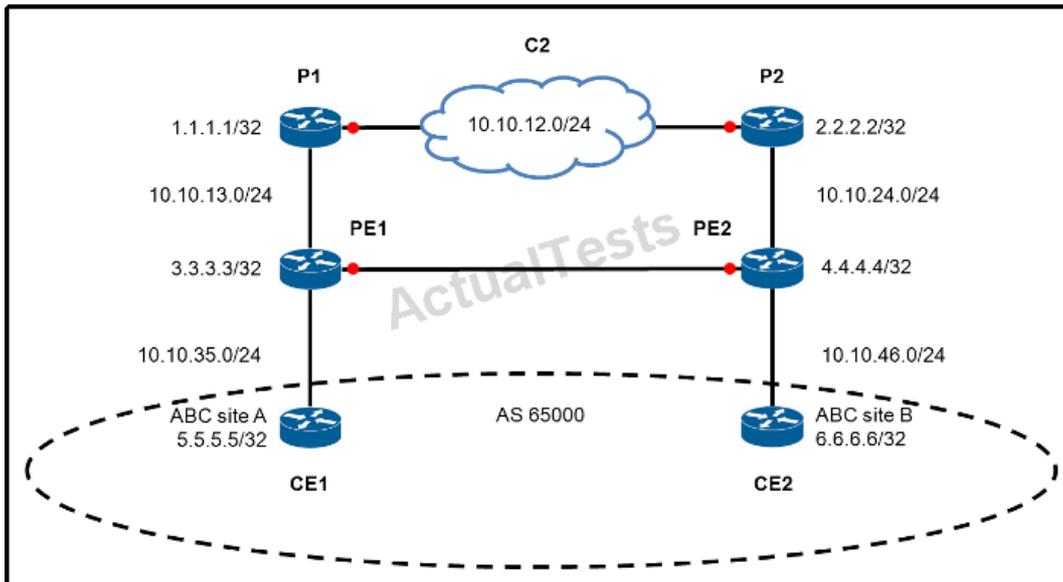
An engineer is looking the CE1 routing table for CE2 Loopback 0. Each CE runs OSPF with its PE.

Which statement describes why the CE2 Loopback address is installed as an external OSPF route at the CE1 routing table?

A. PE1 and PE2 have mutual redistribution between OSPF and BGP.
B. CE1 is configured under OSPF with the command redistribute connected.
C. CE1 and CE2 are in different areas.
D. CE1 and CE2 have different OSPF processes.
E. PE1 and PE2 have different OSPF VRF processes.

Answer: E
Explanation:

QUESTION NO: 437

Two customers have routers that run OSPF and belong to the same OSPF area. These two routers are connected by an MPLS backbone and by a low-bandwidth point-to-point link (used as a backup link). Which two minimum configurations are required to connect these two routers? (Choose two.)

A. site-of-origin
B. sham-link
C. domain tag
D. down bit

E. link cost
F. virtual-link

Answer: B,E
Explanation:

QUESTION NO: 438

An engineer is looking into a solution for two customers that are using the network prefix 10.10.1.0/24. The network engineer wants the network prefix to remain the same for both customers, while maintaining unique network information for each. Which approach can be used to achieve this requirement?

A. Assign a unique RD per customer.
B. Assign a unique RT per customer.
C. Assign a unique SOO per customer.
D. Assign a unique TE per customer.

Answer: A
Explanation:

QUESTION NO: 439

An MPLS VPN service is deployed over an MPLS provider. A customer wants all sites to run BGP with his provider, given that all CEs have the same AS value. Which feature on the service provider PEs can allow communication among different sites?

A. BGP allow-AS
B. BGP weight
C. BGP multihop
D. BGP AS-override

Answer: D
Explanation:

QUESTION NO: 440

Refer to the exhibit.
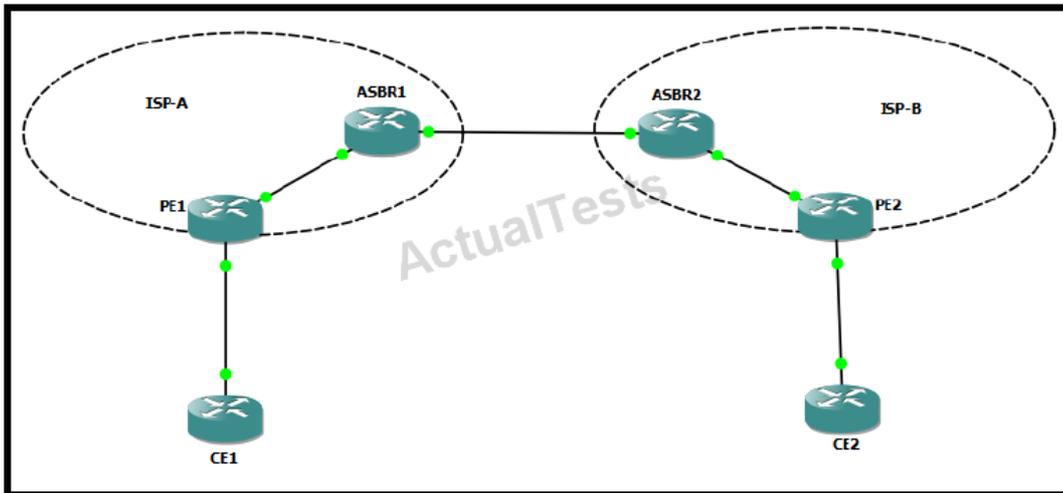
Customer ABC uses RFC 1918 addresses within its network. Customer ABC wants the Internet access for all the branch offices to transit through the head office for security and NAT purposes. The PE routers in the service provider network contain Internet routes in the global routing table. Which option describes the router or routers that should be configured to accomplish the administrative goal of the customer?

A. all the PE routers and the P router
B. both PE2 and PE3 routers
C. only the PE1 router
D. only the P router

Answer: C
Explanation:

QUESTION NO: 441

A customer requests a MPLS VPN service with dual-home connection to the service provider. Which BGP attribute can prevent routes originated from the customer from being readvertised back to them?

A. site-of-origin
B. local-AS
C. AS-path
D. next-hop

Answer: A
Explanation:

QUESTION NO: 442

A network engineer is looking for a specific VRF routing table in the PE router of an Service Provider. Which two information points will be listed in the routing table? (Choose two.)

A. routes received from the directly connected CE
B. routes received from the other MP-BGP PE peer
C. routes received from the other IGP PE peer
D. routes received from the same AS
E. routes of the global routing table

Answer: A,B
Explanation:

QUESTION NO: 443

A network engineer wants to use Telnet to access a CE device in a VRF from a PE device that runs Cisco IOS Software. How can a CE device with IP address 1.1.1.2 be accessed by the PE device?

A. telnet 1.1.1.2 /vrf vrf-name
B. telnet 1.1.1.2 vrf vrf name
C. telnet 1.1.1.2 vrf
D. telnet vrf vrf name 1.1.1.2

Answer: A
Explanation:

QUESTION NO: 444

An ISP provides MPLS L3VPN services and is required to set up a multicast VPN. Which routers will be enabled with MDT to support a multicast VPN?

A. All service provider routers participating in the multicast VPN.
B. All service provider route reflectors.
C. All service provider PE routers.
D. All service provider P routers.
E. All service providers P, PE and route reflector routers.

Answer: A

Explanation:

QUESTION NO: 445

In the Carrier Supporting Carrier (CsC) feature, which two options represent protocols that run between CSC-PE and CSC-CE? (Choose two.)

A. IGP and EBGPv4
B. IGP and RSVP
C. IGP and LDP
D. EBGPv4 with a sending community
E. EBGPv4 with a sending label

Answer: C,E
Explanation:

QUESTION NO: 446

In relation to MPLS Multicast VPN, which three statements about multicast distribution tree (MDT) groups are true? (Choose three.)

A. MDTs are built in customer networks.
B. MDTs are built in provider networks.
C. The number of MDTs depends on PIM modes of MDT groups.
D. Default MDT groups are used for PIM control traffic, low-bandwidth sources, and flooding of sparse mode traffic.
E. Data MDT groups are used for high-bandwidth sources to reduce replication to uninterested PEs.
F. Data MDT groups forward multicast packets using MPLS labels and Default MDT groups forward multicast packets using GRE tunnels.

Answer: B,C,E
Explanation:

QUESTION NO: 447

A network engineer is requested to have load sharing over two links to the same destination prefix. The traffic share for the first link must be two times the traffic share of the second link. Which two

protocols can fulfill this requirement? (Choose two.)

A. EIGRP
B. BGP
C. ISIS
D. OSPF
E. RIP
F. IGRP

Answer: A,B
Explanation:

QUESTION NO: 448

A network engineer is asked to monitor the VPLS services using IP LSP traceroute and ping.
Which feature should be used to achieve this goal?

A. MPLS OAM
B. IP SLA
C. PW
D. AToM

Answer: A
Explanation:

QUESTION NO: 449

Refer to the exhibit.
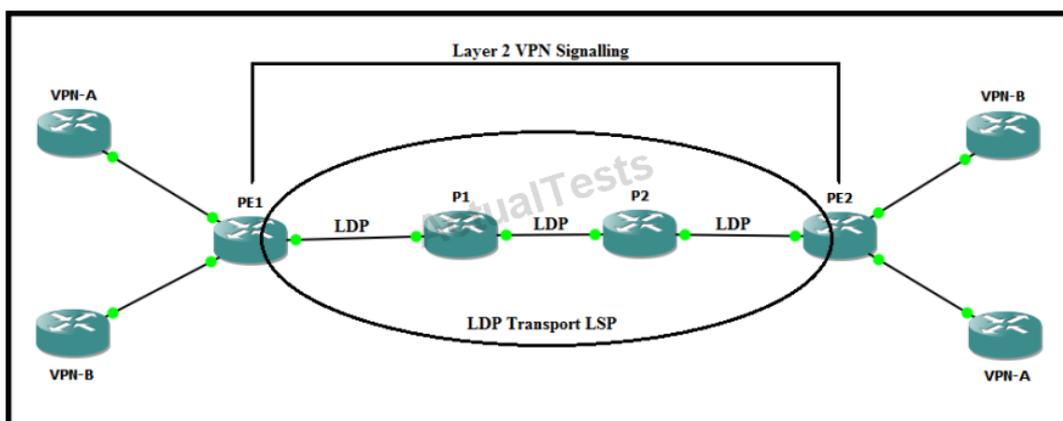
An MPLS L2VPN service is provisioned for VPN-A and VPN-B. Which two statements describe the label exchange and the LDP session requirement for MPLS L2VPN signaling? (Choose two.)

A. PE1 uses the label value that is received from PE2 for VPN-B as the inner label for VPN-B.
B. PE2 uses the label value that is received from PE1 for VPN-B as the transport label for VPN-B.
C. LDP must be enabled on the address that is used as the LDP ID between PE1 and PE2.
D. T-LDP sessions are established between PE1, P1, P2, and PE2.
E. BGP is required for LDP, based on the Layer 2 VPN.
F. PE1 uses the label value that is received from PE2 for VPN-B as the transport label for VPN-B.

Answer: A,C
Explanation:

QUESTION NO: 450

Which MPLS technology will achieve LAN extensions over the service provider backbone?

A. AToM
B. VPLS
C. L2VPN
D. L2TPv3

Answer: B
Explanation:

QUESTION NO: 451

A network engineer is asked to connect two customer sites using Layer 2 connectivity over an MPLS backbone. One customer site uses PPP connectivity with the service provider and the other customer site uses Frame Relay connectivity with the service provider. Which option can the network engineer use to enable network connectivity between these two customer sites?

A. GRE tunnels
B. IP interworking
C. Ethernet interworking
D. L2TPv3 tunnels

Answer: B
Explanation:

QUESTION NO: 452

A network engineer receives a request to tunnel Frame Relay traffic for DCLI 100 over the MPLS cloud while maintaining circuit information. Which solution meets this requirement?

A. L2VPN
B. L3VPN
C. VPLS
D. GRE

Answer: A
Explanation:

QUESTION NO: 453

Which transparent LAN service allows a service provider to offer Layer 2 Ethernet service to connect an enterprise in a metro region?

A. AToM
B. VPLS
C. PPP over MPLS
D. HDLC over MPLS

Answer: B
Explanation:

QUESTION NO: 454

A network engineer wants customers to retain routing information and Layer 2 connectivity for non-Ethernet VPNs within their networks. Which two technologies can be used to accomplish this goal? (Choose two.)

A. VPLS
B. L2TPv3
C. L3VPN
D. AToM
E. IPsec

Answer: B,D

Explanation:

QUESTION NO: 455

Two customer sites are connected to a service provider backbone through L2VPN. GRE is carrying L2VPN circuits across the backbone. Which part of the packet carries the information to route the L2VPN circuits?

A. GRE header
B. LDP header
C. IP header
D. Layer 2 packet header

Answer: A

Explanation:

QUESTION NO: 456

Refer to the exhibit.

PPP	IP	UDP	RTP	Voice Data 100110100110101
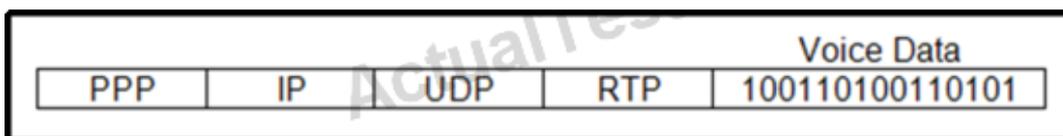
RTP header compression is used on the link for the voice packet. If the header overhead starts reducing at 70%, and is reduced to the maximum amount, what will the overhead percentage be?

A. 0.22
B. 0.33
C. 0.44
D. 0.55

Answer: A

Explanation:

QUESTION NO: 457

Which protocol is used to establish LSP tunnels, enabling resource allocation such as bandwidth along the path?

A. LDP
B. RSVP
C. TDP
D. IPsec

Answer: B
Explanation:

QUESTION NO: 458

A customer wants the minimum delay for the transit traffic that traverses the service provider core. An engineer realizes that the customer sites are remotely dispersed and wants to give them a specific path through the MPLS core with guaranteed bandwidth and without relying on the shortest path of OSPF as the customer IGP. Which technology will achieve the required result?

A. L2VPN
B. IPsec tunnel
C. MPLS TE tunnel
D. L3VPN
E. mGRE with extensions

Answer: C
Explanation:

QUESTION NO: 459

A network engineer is implementing an MPLS network among devices from different vendors. The devices must be configured with MPLS VPN service and MPLS TE. Based on options provided, which three protocols fulfill all of these requirements? (Choose three.)

A. RSVP
B. LDP
C. TDP
D. EIGRP
E. IGRP
F. BGP

G. RIP

Answer: A,B,F
Explanation:

QUESTION NO: 460

Refer to the exhibit.
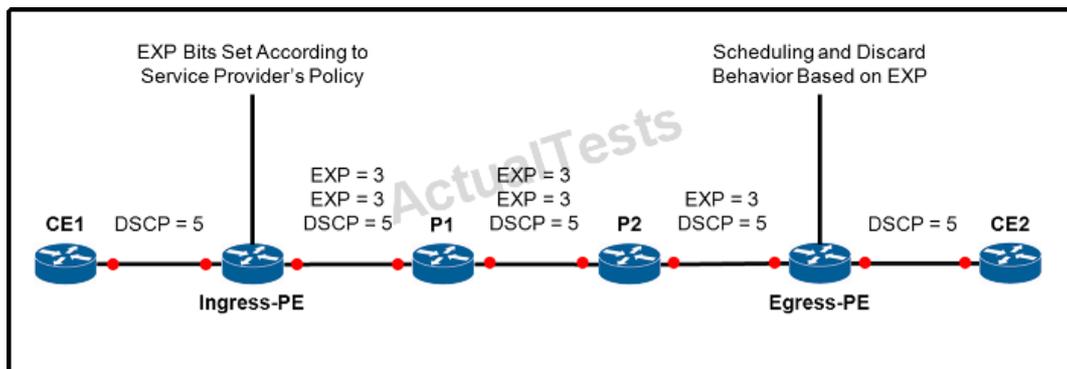
An MPLS-based service provider wants to deploy QoS over its backbone. Original customer QoS information must be preserved when the packet leaves the MPLS network. In addition, the egress LSR must forward packets according to the LSP Diff-Service information, as depicted in the topology. Which QoS model satisfies these requirements?

A. uniform model
B. pipe model
C. short-pipe model
D. IntServ model

Answer: B
Explanation:

QUESTION NO: 461

A network engineer wants to leak only IPv6 loopback addresses from level 2 to level 1. All of the other level 2 prefixes should not be advertised into level 1. Which technique will achieve this goal, based on IOS SRE release?

A. route-policy

B. access-list
C. distribute-list
D. policy-map

Answer: C
Explanation:

QUESTION NO: 462 DRAG DROP

Drag the Layer 2 QoS marking types on the left to the correct Layer 2 QoS names on the right.	
1-bit drop eligibility flag	experimental bit
3-bit 802.1p field in 802.1Q header	discard eligibility
1-bit drop eligibility flag	class of service
3-bit on MPLS header	cell loss priority

Answer:

Drag the Layer 2 QoS marking types on the left to the correct Layer 2 QoS names on the right.	
1-bit drop eligibility flag	3-bit on MPLS header
3-bit 802.1p field in 802.1Q header	1-bit drop eligibility flag
1-bit drop eligibility flag	3-bit 802.1p field in 802.1Q header
3-bit on MPLS header	1-bit drop eligibility flag

Explanation:

3-bit on MPLS header
1-bit drop eligibility flag
3-bit 802.1p field in 802.1Q header
1-bit drop eligibility flag

QUESTION NO: 463 DRAG DROP

A network engineer is configuring L2VPN static point-to-point cross connect on the CRS router. Drag the configuration steps on the left in the correct order on the right.

Configure point-to-point cross-connect.	Step 1
Select the interface.	Step 2
Commit changes.	Step 3
Enable L2VPN mode.	Step 4
Enable internetworking for IPv4.	Step 5
Configure a cross-connect group.	Step 6
Enable configure mode.	Step 7
Configure the **neighbor pw-id** command.	Step 8

Answer:

A network engineer is configuring L2VPN static point-to-point cross connect on the CRS router. Drag the configuration steps on the left in the correct order on the right.

Configure point-to-point cross-connect.	Enable configure mode.
Select the interface.	Enable L2VPN mode.
Commit changes.	Configure a cross-connect group.
Enable L2VPN mode.	Configure point-to-point cross-connect.
Enable internetworking for IPv4.	Enable internetworking for IPv4.
Configure a cross-connect group.	Select the interface.
Enable configure mode.	Configure the **neighbor pw-id** command.
Configure the **neighbor pw-id** command.	Commit changes.

Explanation:

Enable configure mode.
Enable L2VPN mode.
Configure a cross-connect group.
Configure point-to-point cross-connect.
Enable internetworking for IPv4.
Select the interface.
Configure the **neighbor pw-id** command.
Commit changes.

QUESTION NO: 464 DRAG DROP

Drag and arrange the Ethernet Q-in-Q frame format fields on the left in the correct sequence on the right.	
Etype	1
Outer VLAN tag	2
FCS	3
Destination Address	4
Data	5
Inner VLAN tag	6
Source Address	7

Answer:

Drag and arrange the Ethernet Q-in-Q frame format fields on the left in the correct sequence on the right.	
Etype	Destination Address
Outer VLAN tag	Source Address
FCS	Outer VLAN tag
Destination Address	Inner VLAN tag
Data	Etype
Inner VLAN tag	Data
Source Address	FCS

Explanation:

Destination Address
Source Address
Outer VLAN tag
Inner VLAN tag
Etype
Data
FCS

New Questions

QUESTION NO: 465

Refer to the exhibit.


```
*Mar   1 00:02:24.279: PIM(0): Received v2 Bootstrap on FastEthernet0/0 from 10.10.24.2
*Mar   1 00:02:24.287: PIN-BSR(0): bootstrap on non-RPF path FastEthernet0/0
R4#show ip route 2.2.2.2
Routing entry for 2.2.2.2/32
     Known via "ospf 1", distance 110, metric 22, type intra area
     Last update from 10.10.34.3 on FastEthernet0/1, 00:01:58 ago
     Routing Descriptor Blocks:
     * 10.10.34.3, from 2.2.2.2, 00:01:58 ago via FastEthernet0/1
             Route metric is 22, traffic share count is 1


R4#show ip pim interface

Address       Interface      Ver/   Nbr    Query   DR      DR
                             Mode   Count  Intvl   Prior
10.10.24.4    FastEthernet0/0  v2/S   1      30      1       10.10.24.4
10.10.34.4    FastEthernet0/1  v2/S   0      30      1       10.10.34.4
10.10.46.4    FastEthernet1/0  v2/S   1      30      1       10.10.46.4

R6#show ip mroute | begin 234
(*, 234.1.1.1), 00:17:54/00:02:56, RP 0.0.0.0, flags: SJCL
   Incoming interface: Null, RPF nbr 0.0.0.0
   Outgoing interface list:
         FastEthernet0/0, Forward/Sparse, 00:17:54/00:02:56

(*, 224.0.1.40), 00:17:54/00:02:59, RP 0.0.0.0, flags: DCL
   Incoming interface: Null, RPF nbr 0.0.0.0
   Outgoing interface list:
         FastEthernet0/0, Forward/Sparse, 00:17:54/00:02:59
```

A client is unable to receive traffic from multicast streamer (R5) on 234.1.1.1, even though multicast routing is established in the network.

Which statement describes how to resolve this issue?

A. IGMP must be enabled for the client.
B. R4 must be the DR on the R4-R6 segment.
C. RP announcements have no multicast routing table entry.

D. The RP must be reachable via Fa0/0.

E. A static mroute must be configured to point to RP via Fa0/1 on R4.

Answer: D

Explanation:

QUESTION NO: 466

A service provider with MPLS traffic-eng tunnels is supporting multicast traffic that uses RPF to ensure the source of the sender. The unicast routing table points the source through TE, which does not support multicast and RPF fails.

Which action fixes the issue?

A. Use auto-route announce under MPLS TE.

B. Use multicast-intact under IGP.

C. Use IGMP snooping.

D. Use CGMP.

Answer: B

Explanation:

QUESTION NO: 467

A service provider is using QoS to manage customer traffic over the MPLS backbone. Which three statements about the behavior of each MPLS QoS mode based on QoS policy in the service provider core are true? (Choose three.)

A. Uniform mode does not change the original CE IP packet markings.

B. Uniform mode changes the original CE IP packet markings.

C. Pipe mode does not change the original CE IP packet markings.

D. Pipe mode changes the original CE IP packet markings.

E. Short-pipe mode does not change the original CE IP packet markings.

F. Short-pipe mode changes the original CE IP packet markings.

Answer: B,C,E

Explanation:

QUESTION NO: 468

Which feature provides rapid failure detection times between the forwarding engines, while maintaining low overhead?

A. Resource Reservation protocol
B. Precision Time protocol
C. bidirectional forwarding detection
D. MPLS traffic engineering
E. fast hello
F. nonstop forwarding

Answer: C

Explanation:

QUESTION NO: 469

Refer to the exhibit.

```
SLOT  6 (RP/LC 6): 1 Port ISE Packet Over SONET OC-48c/STM-16
Single Mode/SR SC-SC connector
  MAIN: type 77,  800-18817-08 rev A0 dev 0
        HW config: 0x02    SW key: 00-00-00
  PCA:  73-7398-12 rev B0 ver 7
        HW version 1.0  S/N SAD10020ACF
  MBUS: Embedded Agent
        Test hist: 0x00    RMA#: 00-00-00    RMA hist: 0x00
  DIAG: Test count: 0x00000001    Test results: 0x80000000
  FRU:  Linecard/Module: OC48X/POS-SR-SC
        Route Memory: MEM-LC-512=
        Packet Memory: MEM-LC1-PKT-512=
L3 Engine: 3 - ISE OC48 (2.5 Gbps)
MBUS Agent Software version 4.6 (RAM) (ROM version is 4.6)
Using CAN Bus A
ROM Monitor version 17.1
Fabric Downloader version used 8.0 (ROM version is 8.0)
Primary clock is CSC0
Persistent LOS to slot 16
Persistent LOS to slot 18
Persistent LOS to slot 19
Persistent LOS to slot 20
Board State is BRINGDOWN
Last Reset Reason: Initial load
Insertion time: Sun Jun 29 00:00:34 2014 (00:08:45 ago)
DRAM size: 1073741824 bytes
FrFab SDRAM size: 268435456 bytes
ToFab SDRAM size: 268435456 bytes
0 resets since restart/fault forgive
```

A network engineer installs a Cisco XR 12416 with several modules. One of the modules fails to

load Cisco IOS-XR version 3.9.1 and is stuck in the BRINGDOWN state. Which issue is the source of the problem?

A. insufficient route memory to boot the blade
B. insufficient packet memory to boot the blade
C. insufficient DRAM to boot the blade
D. blade in the incorrect slot

Answer: A
Explanation:

QUESTION NO: 470

A network administrator has configured an IPsec security policy index at the OSPFv3 Area level.

Which interfaces are applied with OSPFv3 IPsec authentication?

A. interfaces exclusively configured with OSPFv3
B. all interfaces in the OSPFv3 area
C. all interfaces in SPI
D. all interfaces in an OSPFv2 and OSPFv3

Answer: B
Explanation:

QUESTION NO: 471

Which series of commands allow a port to transition to an up state in Cisco IOS XR when a non-OEM Cisco TenGigabit Ethernet receiver is installed?

A. RP/0/RSP0/CPU0:ios#conf t
RP/0/RSP0/CPU0:ios(config)#int gigabitEthernet 0/5/0/0
RP/0/RSP0/CPU0:ios(config--if)#transceiver permit pid all
RP/0/RSP0/CPU0:ios(config--if)#commit
B. RP/0/RSP0/CPU0:ios#conf t
RP/0/RSP0/CPU0:ios(config)#int tenGigE 0/5/0/0
RP/0/RSP0/CPU0:ios(config--if)#transceiver permit pid all
RP/0/RSP0/CPU0:ios(config--if)#commit
C. RP/0/RSP0/CPU0:ios#conf t
RP/0/RSP0/CPU0:ios(config)#int tenGigE 0/5/0/0

RP/0/RSP0/CPU0:ios(config--if)#shut
RP/0/RSP0/CPU0:ios(config--if)#commit
RP/0/RSP0/CPU0:ios(config--if)#no shut
RP/0/RSP0/CPU0:ios(config--if)#commit
D. RP/0/RSP0/CPU0:ios#conf t
RP/0/RSP0/CPU0:ios(config)#int gigabitEthernet 0/5/0/0
RP/0/RSP0/CPU0:ios(config--if)#speed 10000
RP/0/RSP0/CPU0:ios(config--if)#commit

Answer: B

Explanation:

QUESTION NO: 472

Refer to the exhibit.

```
Rack1SW1#show etherchannel summary
Flags:  D - down          P - bundled in port-channel
        I - stand-alone s - suspended
        R - Layer3        S - Layer2
        U - in use        f - failed to allocate aggregator


Group  Port-channel  Protocol    Ports
------+-------------+-----------+----------------------------
12     Po12(SU)         -          Fa0/13(s)   Fa0/14(P)

interface FastEthernet0/13
 description -- TO_R1 --
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 200,300,400,500
 switchport mode trunk
 load-interval 30
 channel-group 12 mode on

interface FastEthernet0/14
 description -- R1 --
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100,200,300,400,500
 switchport mode trunk
 duplex auto
 channel-group 12 mode on
```

Which action can fix the problem with the port channel?

A. Unify interface descriptions on both interfaces.
B. Unify load-interval on both interfaces.
C. Add duplex full on interface F0/13.
D. Add VLAN 100 to VLAN allowed list on Fa0/13.

Answer: D

Explanation:

QUESTION NO: 473

MPLS LDP was configured on two Cisco IOS XR routers, but LDP was not established. Which two issues may cause this problem? (Choose two.)

A. The access list is configured to block TCP port 646.
B. The interface has not been placed under the MPLS LDP configuration.
C. The access list is configured to block TCP port 711.
D. MPLS LDP is always enabled by default in Cisco IOS XR.
E. MPLS LDP has not been placed under the interface configuration.

Answer: A,B

Explanation:

QUESTION NO: 474

A company is given a 20 Mbps bandwidth guarantee provided over a FastEthernet connection by an ISP. Which QoS technology should be used to ensure that traffic conforms to the 20 Mbps contract?

A. shaping
B. LFI
C. CIR
D. burst protection

Answer: A

Explanation:

QUESTION NO: 475

An engineer is designing a SONET network using Cisco 7600 and the ONS 15454 platform. Which Cisco 7600 module allows for three 45 Mbps serial interfaces?

A. OC-12c/STM-4c ATM
B. OC-12/STM4 to DS3/E3

C. OC-3c/STM-1 POS/SDH
D. OC-12c/STM-4 POS/SDH

Answer: B

Explanation:

QUESTION NO: 476

Which two characteristics must be considered when implementing IP dampening on Cisco IOS? (Choose two.)

A. The maximum suppress threshold time should be less than the reuse threshold.
B. The half-life period increases the penalty by half each time the interface comes up.
C. The reuse threshold defaults to 1000 penalties if it is not configured.
D. IP dampening can track the individual subinterfaces on an interface.
E. The maximum suppress threshold time should be more than the reuse threshold.

Answer: C,E

Explanation:

QUESTION NO: 477

Which ITU publication defines the requirements for communicating data over an optical network?

A. G.706
B. G.707
C. G.708
D. G.709

Answer: D

Explanation:

QUESTION NO: 478

Which three counters from a show interface output indicate that data packets were dropped on that interface? (Choose three.)

A. pause input

B. collisions
C. lost carrier
D. frame
E. runts
F. input error

Answer: B,D,E
Explanation:

QUESTION NO: 479

From the show interface output, which two options describe the two fields that are indicated as "unknown protocol drops"? (Choose two.)

A. packet drops for protocols that are not configured on the interface
B. packet drops for protocols that are not recognized by the interface
C. packet drops for protocols that are not destined for the interface
D. packet drops for protocols that are not sourced by the interface
E. packet drops for protocols that are denied in the ACL attached on the interface

Answer: A,B
Explanation:

QUESTION NO: 480

You have a Cisco 7600 Series Router with two route processors installed and with SSO enabled. Which three conditions must apply? (Choose three.)

A. The route processors must be running the same version of the Cisco IOS Software.
B. The route processors must have the same amount of DRAM.
C. The route processors must be preloaded with configurations.
D. The route processors must load share responsibilities between them.
E. The route processors must have the same configuration register values.
F. A switchover between the two route processors does not result in the reset of any line cards.

Answer: A,E,F
Explanation:

QUESTION NO: 481

Which three options are reasons to deploy BFD? (Choose three.)

A. BFD is a fast hello protocol that exhibits lower overhead than aggressive hellos.
B. BFD is a fast hello protocol that provides reaction time under a second.
C. BFD is a fast hello protocol that provides reaction time over a second.
D. BFD provides fast converges to Layer 2 bundling protocol LAGs.
E. HSRP protocol supports BFD.
F. BFD uses a reliable transport for Hello packets, which increases the fast converge if an ACK is not received.

Answer: A,B,E
Explanation:

QUESTION NO: 482

What is the recommended codepoint as per the RFC 2598 "An Expedited Forwarding PHB" for a packet to receive expedited forwarding PHB?

A. 101111
B. 101110
C. 111111
D. 110111
E. 101101
F. 110110

Answer: B
Explanation:

QUESTION NO: 483

Which two actions of Cisco IOS Software prevent a DDOS attack? (Choose two.)

A. Filter all source addresses from which traffic is not expected in the network, including RFC 1918 addresses.
B. Filter all traffic for TCP ports in the range 1014-49151.
C. Enable BFD to have links taken down when there is an attack.
D. Enable the ip verify reverse-path command on the interface.
E. Allow only static routes; dynamic routing protocols should not be allowed.

Answer: A,D

Explanation:

QUESTION NO: 484

In which three scenarios does multihoming in IS-IS work? (Choose three.)

A. merging Level 1 areas
B. splitting the Level 1 area
C. renumbering NSAP addresses
D. modifying the system ID
E. merging Level 2 areas
F. splitting the Level 2 area
G. creating an alternative path to the exit point

Answer: A,B,C

Explanation:

QUESTION NO: 485

Which three BGP features improve convergence? (Choose three.)

A. route reflector
B. BGP cost community
C. BGP autodiscovery
D. BGP soft reconfiguration
E. Fast Peering Session Deactivation
F. eBGP multihop
G. BGP PIC
H. next-hop address tracking

Answer: E,G,H

Explanation:

QUESTION NO: 486

Which option is the main task of the BGP I/O?

A. handles queuing and processing of BGP packets

B. performs BGP peer establishment

C. imports and exports routes into a particular VPN routing and forwarding instance

D. calculates the best BGP path

E. interacts with the routing information base

Answer: A

Explanation:

QUESTION NO: 487

What are the three operating modes of HDLC? (Choose three.)

A. Normal Peer Mode

B. Asynchronous Balanced Mode

C. Asynchronous Client Mode

D. Normal Response Mode

E. Asynchronous Response Mode

F. Normal Balanced Mode

Answer: B,D,E

Explanation:

QUESTION NO: 488

In inter-AS multicast, which two optional nontransitive path attributes were introduced in BGP to carry unicast and multicast routing information for RPF check at the AS borders? (Choose two.)

A. MP_UNREACH_NLRI

B. MP_REACH_NLRI

C. FWDR_PREF Details

D. MP_PERF_NLRI

E. ORIGINATOR_ID

Answer: A,B

Explanation:

QUESTION NO: 489

Which three options are tasks of the BGP scanner process? (Choose three.)

A. processing of BGP packets
B. processing any route "churn"
C. updating IP RIB
D. providing BGP Dampening information updates
E. performing Conditional Advertisement checks
F. performing BGP synchronization
G. checking next-hop reachability

Answer: D,E,G
Explanation:

QUESTION NO: 490

Refer to the exhibit.

```
RR# show ip bgp 192.168.1.0
BGP routing table entry for 192.168.1.0/24, version 13
Paths: (2 available, best #2)
Flag: 0x900
  Advertised to update-groups:
     1          2
  Local, (Received from a RR-client)
    10.10.10.21 (inaccessible) from 10.10.10.21 (10.10.10.21)
      Origin IGP, metric 0, localpref 100, valid, internal
  Local, (Received from a RR-client)
    10.10.10.22 (metric 41) from 10.10.10.22 (10.10.10.22)
      Origin IGP, metric 0, localpref 100, valid, internal, best
```

Which BGP feature causes the BGP RIB entry "inaccessible"?

A. BGP synchronization
B. eBGP multihop
C. BGP scanner
D. BGP NHT

Answer: D
Explanation:

QUESTION NO: 491

Which option is the minimum MTU of a link to form a full IS-IS adjacency successfully?

A. 4096 bytes
B. 1500 bytes
C. 1492 bytes
D. 1460 bytes

Answer: C
Explanation:

QUESTION NO: 492

Refer to the exhibit.
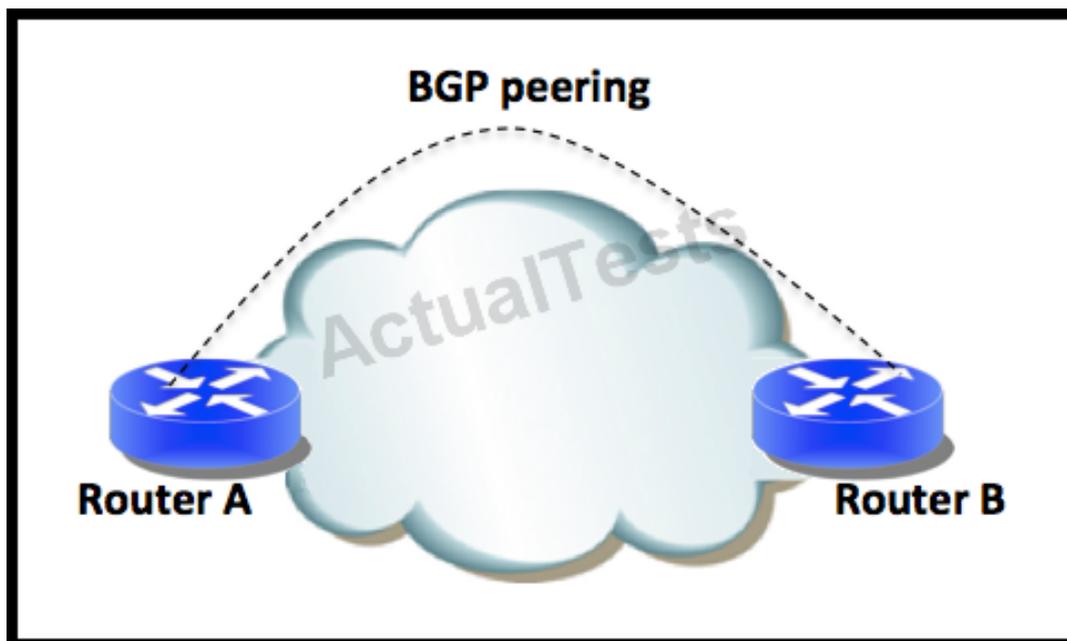
Router A is configured with a BGP keepalive timer of 20 seconds and a BGP holddown timer interval of 60 seconds. The BGP peer router B is configured with 5 seconds of keepalive interval and 15 seconds of holddown timer interval.

Which option is the value of the keepalive interval and holddown timers, respectively, after the successful BGP TCP negotiation between router A and router B?

A. BGP TCP negotiation will not be successful.
B. 20 and 60 seconds

C. 5 and 15 seconds
D. Router A will use 20 and 60 seconds and router B will use 5 and 15 seconds.
E. Router B will use 20 and 60 seconds and router A will use 5 and 15 seconds.

Answer: C
Explanation:

QUESTION NO: 493

Which statement about the Link Control Protocol is true?

A. LCP is used for basic PPP link setup and operation.
B. LCP is used for PPP CHAP authentication.
C. LCP is used for PPP over ATM setup.
D. LCP is used for PPP over Ethernet setup.
E. LCP is used for PPP over Frame Relay setup.

Answer: A
Explanation:

QUESTION NO: 494

Which SONET protocol layer is in charge of clock synchronization and timing issues?

A. Photonic
B. Section
C. Path
D. Line

Answer: B
Explanation:

QUESTION NO: 495

Which IEEE task group provides a method to implement QoS on an Ethernet level?

A. 802.1ab
B. 802.1p

C. 802.1q
D. 802.1s
E. 802.1w

Answer: B
Explanation:

QUESTION NO: 496

Which E3 alarm indicates that there could be an issue with the transmit signal with the local equipment?

A. rxLoS
B. rxLoF
C. rxRAI
D. txRAI
E. txLoF
F. txLoS

Answer: C
Explanation:

QUESTION NO: 497

What is the payload capacity of an SDH/STM1 circuit?

A. 155.52 Mbps
B. 150.336 Mbps
C. 153.472 Mbps
D. 151.424 Mbps

Answer: B
Explanation:

QUESTION NO: 498

Which option is the SONET frame format of the STM-4 SDH circuit?

A. STS-1
B. STS-192
C. STS-12
D. STS-3

Answer: C

Explanation:

QUESTION NO: 499

Refer to the exhibit.

```
Router A
interface TenGigabitEthernet1/1
  description connection to Tengig1/1 Router B
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 1-209,212-468,723-724,726-4094
  switchport mode trunk
  mls qos trust dscp                    ActualTests

Router B
interface TenGigabitEthernet1/1
  description connection to Tengig1/1 Router A
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 1-209,213-466,723-724,726-4094
  switchport mode trunk
  mls qos trust dscp
```

Which two Layer 2 headers of the frames that are initiated from router A will successfully reach router B? (Choose two.)

A. 04 fe 7f b0 08 c1 c4 7d 4f 8f 8a 68 81 00 00 d2 08 00
B. 04 fe 7f b0 08 c1 c4 7d 4f 8f 8a 68 81 00 00 d5 08 00
C. 04 fe 7f b0 08 c1 c4 7d 4f 8f 8a 68 81 00 01 d2 08 00
D. 04 fe 7f b0 08 c1 c4 7d 4f 8f 8a 68 81 00 01 d5 08 00
E. 04 fe 7f b0 08 c1 c4 7d 4f 8f 8a 68 81 00 02 d2 08 00
F. 04 fe 7f b0 08 c1 c4 7d 4f 8f 8a 68 81 00 02 d5 08 00

Answer: B,C

Explanation:

QUESTION NO: 500

What are three advantages of PPPoA implementation? (Choose three.)

A. NAP and NSP provide secure access to corporate gateways without managing end-to-end PVCs. NAP and NSP use Layer 3 routing, Layer 2 Forwarding, or Layer 2 Tunneling Protocol tunnels. Hence, they can scale their business models for selling wholesale service.
B. Only a single session per CPE on one virtual channel (VC). The username and password are configured on the CPE, so all users behind the CPE for that particular VC can access only one set of services. Users cannot select different sets of services, although using multiple VCs and establishing different PPP sessions on different VCs is possible.
C. The NSP can oversubscribe by deploying idle and session timeouts using an industry standard RADIUS server for each subscriber.
D. If a single IP address is provided to the CPE, and NAT or PAT is implemented, certain applications such as IPTV, which embed IP information in the payload, will not work. Additionally, if an IP subnet feature is used, an IP address also has to be reserved for the CPE.
E. PPPoA can use the features on the SSG.
F. Cisco Service Selection Gateway is not compatible with PPPoA.

Answer: A,C,E
Explanation:

QUESTION NO: 501

Router 1 is a PE router within the MPLS core network. The router is designed to provide multicast VPN services for VRF A. A requirement of the core network prevents RP configuration and focuses on SSM for all multicast traffic. Consider this configuration:

Router 1

!

vrf definition A

rd 1001:1001

!

address-family ipv4

route-target export 1001:1001

route-target import 1001:1001

mdt default 235.1.1.1

Which configuration is needed to support MDT?

A. access-list 110 permit 235.1.1.1 0.0.0.0
ip pim ssm range 110
B. access-list 110 permit 235.1.1.1 0.0.0.0
ip pim ssm default access-list 110
C. access-list 10 permit 235.1.1.0 0.0.0.255
ip pim ssm range 10
D. access-list 10 permit 235.1.1.0 0.0.0.255
ip pim ssm default access-list 10

Answer: C
Explanation:

QUESTION NO: 502

Refer to the exhibit.
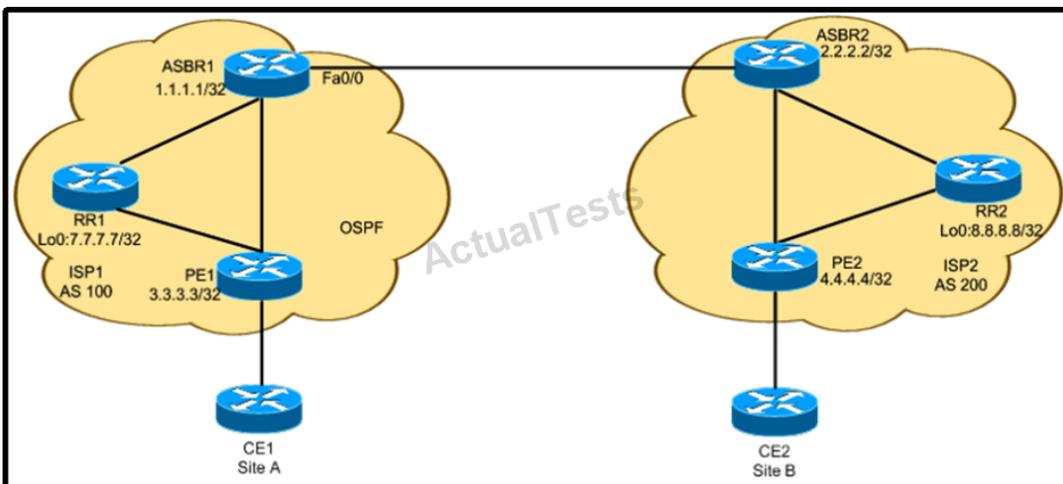
MPLS VPN service has been provisioned for customer ABC using an inter-AS MPLS option C. A network admin on ISP1 decided not to redistribute ISP2 received loopback addresses into IGP.

Which five commands can be configured to guarantee an end-to-end connectivity between ABC sites? (Choose five.)

A. configure on ASBR1 BGP VPNv4 address-family neighbor 7.7.7.7 send-label

B. configure on ASBR1 BGP VPNv4 address-family neighbor 7.7.7.7 next-hop-self
C. configure on RR1 BGP VPNv4 address-family neighbor 1.1.1.1 send-label
D. configure on RR1 BGP IPv4 address-family neighbor 1.1.1.1 send-label
E. configure on RR1 BGP IPv4 address-family neighbor 3.3.3.3 send-label
F. configure on RR1 BGP VPNv4 address-family neighbor 3.3.3.3 send-label
G. configure on ASBR1 BGP IPv4 address-family neighbor 7.7.7.7 send-label
H. configure on ASBR1 BGP IPv4 address-family neighbor 7.7.7.7 next-hop-self
I. configure on PE1 BGP VPNv4 address-family neighbor 7.7.7.7 next-hop-self
J. configure on PE1 BGP IPv4 address-family neighbor 7.7.7.7 next-hop-self

Answer: D,E,G,H,J
Explanation:

QUESTION NO: 503

Which two VPN Inter-AS options require the no bgp default route-target filter command? (Choose two.)

A. MPLS VPN Inter-AS with ASBRs exchanging VPN-IPv4 addresses
B. MPLS VPN Inter-AS with ASBRs exchanging IPv4 routes and MPLS labels
C. MPLS VPN Inter-AS Option AB
D. MPLS VPN Carrier Supporting Carrier using LDP and IGP
E. MPLS VPN Carrier Supporting Carrier with BGP
F. MPLS VPN eBGP multipath support for CSC

Answer: A,C
Explanation:

QUESTION NO: 504

Which Cisco IOS command must be applied to create a multiprotocol VRF?

A. ip vrf
B. ip vrf forwarding
C. vrf definition
D. vrf downgrade-cli
E. vrf forwarding

Answer: C
Explanation:

QUESTION NO: 505

Refer to the exhibit.


```
PE1#
router bgp 100
 no bgp default ipv4-unicast
 neighbor 44.44.44.44 remote-as 100
 neighbor 44.44.44.44 update-source Loopback 3
 address-family vpnv4
  neighbor 44.44.44.44 activate
  neighbor 44.44.44.44 send-community extended

PE1# show ip pim vrf XYZ interface
Address     Interface       Ver/  Nbr   Query DR    DR
                            Mode  Count Intvl Prior
10.10.35.3  FastEthernet1/1 V2/S  1     30    1      10.10.35.5
3.3.3.3     Tunnel1         V2/S  0     39    1      3.3.3.3

PE1#show ip pim vrf XYZ rp mapping
PIM Group-to-RP Mapping
```

XYZ is using the BSR method and PE1 has the configuration shown.

A. Which statement describes why PE1 is unable to receive RP information from XYZ site 2?
B. IPv4 MDT address family is not activated between PE1 and PE2.
C. Loopback 3 is not enabled with PIM.
D. A mismatch exists for update source interface between PE1 and PE2.
E. A mismatch exists in MDT data subnet for XYZ VRF between PE1 and PE2.

Answer: B
Explanation:

QUESTION NO: 506

Refer to the exhibit.

```
vrf definition CUST-1          vrf definition INTERNET        vrf definition CUST-2
rd 100:1                       rd 100:3                       rd 100:2
route-target export 100:1      route-target export 100:3      route-target export 100:2
route-target import 100:1      route-target import 100:3      route-target import 100:2
```

An ISP network runs L3VPN MPLS over the IP core to deliver internet service for the customer as a central service through a dedicated VRF.

Which route target plan delivers the internet service to customers while preserving customer VRF privacy?

A. vrf definition CUST-1
route-target export 100:2
route-target import 100:2
!
vrf definition CUST-2
route-target export 100:1
route-target import 100:1
!
vrf definition INTERNET
route-target export 100:1
route-target import 100:2
B. vrf definition CUST-1
route-target export 100:3
route-target import 100:3
!
vrf definition CUST-2
route-target export 100:3
route-target import 100:3
!
vrf definition INTERNET
route-target export 100:1
route-target import 100:2
C. vrf definition CUST-1
route-target export 100:3
!
vrf definition CUST-2
route-target export 100:3
!
vrf definition INTERNET
route-target import 100:1
route-target import 100:2

D. vrf definition CUST-1
route-target import 100:3
!
vrf definition CUST-2
route-target import 100:3
!
vrf definition INTERNET
route-target import 100:1
route-target import 100:2

Answer: D
Explanation:

QUESTION NO: 507

Which Inter-AS option allows a service provider to provision AToM along with L3VPN provisioning?

A. MPLS VPN Inter-AS with ASBRs exchanging VPN-IPv4 addresses
B. MPLS VPN Inter-AS with ASBRs exchanging IPv4 routes and MPLS labels
C. MPLS VPN Inter-AS Option AB
D. back-to-back VRFs

Answer: B
Explanation:

QUESTION NO: 508

Which option is the ATM Cell Relay feature that enhances throughtput and uses bandwidth more efficiently?

A. EXP marking match QoS LLD PHB
B. preferred-interface
C. cell packing
D. MPLS experimental bit
E. RSVP bandwidth reservation

Answer: C
Explanation:

QUESTION NO: 509

What are the three building blocks of the Cisco VPLS architecture? (Choose three.)

A. L2VPN
B. Ethernet Virtual Switch Interface
C. VLAN Trunk Protocol
D. State Synchronization Protocol
E. Label Distribution Protocol
F. Resource Reservation Protocol

Answer: A,B,E
Explanation:

QUESTION NO: 510

Refer to the exhibit.

```
Router# show mpls l2transport vc
Local intf    Local circuit          Dest address    VC ID    Status
-----------   --------------------   ------------     ---------  --------
Gi4/0.1       Eth VLAN 2             11.1.1.1            2       UP
Gi8/0/1       Ethernet               11.2.1.1            8       UP
AT1/0         ATM CELL ATM2/0        11.3.1.1          110       UP
Se5/0         FR DLCI 55             11.4.1.1           55       UP
```

Which attached circuit interface shown uses VC Type 4?

A. Gi8/0/1
B. AT1/0
C. Se5/0
D. ATM2/0
E. Gi4/0.1

Answer: E
Explanation:

QUESTION NO: 511

A company plans to secure its connectivity over its provider. Which method can reduce overhead

and provide encryption for Layer 2 over the provider cloud?

A. MACsec
B. IPsec
C. L2VPN with 802.1X extensions
D. L2TPv3

Answer: A
Explanation:

QUESTION NO: 512

A service provider engineer has been requested to preserve QoS values when customer packets cross the MPLS backbone. Which Cisco IOS command should the engineer apply and what should the label value be when the LSR at the penultimate hop forwards the MPLS label packets toward the egress PE?

A. mpls ldp explicit-null with label value of zero
B. mpls ldp implicit-null with label value of zero
C. mpls ldp explicit-null with label value of three
D. mpls ldp implicit-null with label value of three

Answer: A
Explanation:

QUESTION NO: 513

Which two statements about a backup tunnel to avoid the SRLGs of its protected interface are true? (Choose two.)

A. Tunnel is not created unless it avoids SRLGs on the protected interface.
B. If it is not possible to avoid SRLG of the protected interface, backup tunnel will be created anyways.
C. If it is not possible to avoid SRLG of the protected interface, backup tunnel will not be created.
D. Backup tunnel can be created between IGP areas as long as SRLG is configured along the path.
E. Manually created backup tunnel do automatically avoid SRLG of protected interfaces.

Answer: A,B
Explanation:

QUESTION NO: 514

Which option propagates SRLG membership information to the network?

A. BGP attribute
B. IGP extension
C. RSVP extension
D. LDP extension
E. PIM extension

Answer: B
Explanation:

QUESTION NO: 515

Refer to the exhibit.
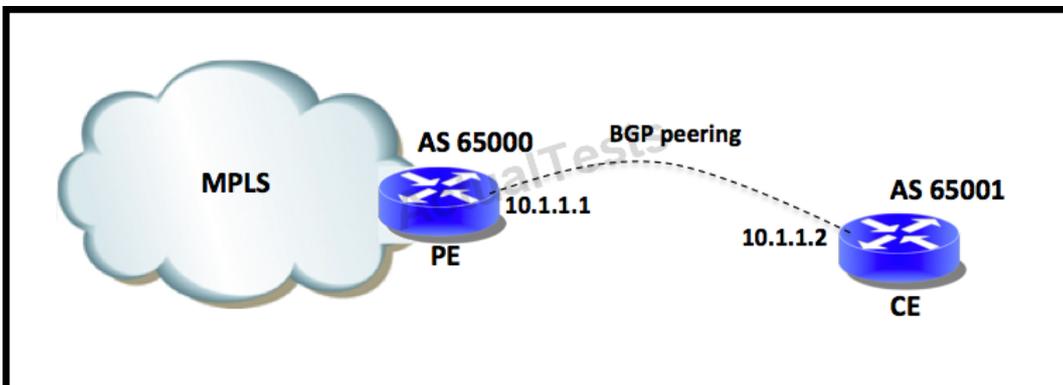
An ISP engineer has been asked to identity a method to protect the PE and to control the number of BGP prefixes learned from his customers. The BGP session should be dropped if the PE router receives more than 1000 BGP prefixes. A syslog message should be generated when the number of BGP prefixes learned from CE exceeds 850.

Which Cisco IOS command should the engineer apply on PE routers?

A. neighbor 10.1.1.2 maximum-prefix 1000 85
B. neighbor 10.1.1.2 maximum-prefix 1000 850
C. neighbor 10.1.1.2 maximum-prefix 1000 85 warning-only

"Pass Any Exam. Any Time." - www.actualtests.com

273

D. neighbor 10.1.1.2 maximum-prefix 1000 850 warning-only

Answer: A
Explanation:

QUESTION NO: 516 DRAG DROP

Drag and drop the appropriate AFI/SAFI description on the left to the corresponding identifier on the right.	
VPNv6	1/1
VPNv4	2/1
IPv4 Unicast	1/128
VPLS	2/128
IPv6 Unicast	25/65

Answer:

Drag and drop the appropriate AFI/SAFI description on the left to the corresponding identifier on the right.	
VPNv6	IPv4 Unicast
VPNv4	IPv6 Unicast
IPv4 Unicast	VPNv4
VPLS	VPNv6
IPv6 Unicast	VPLS

Explanation:

IPv4 Unicast
IPv6 Unicast
VPNv4
VPNv6
VPLS

QUESTION NO: 517 DRAG DROP

Drag and drop the Cisco IOS XR commands used to create a policy that will limit all traffic to 20% of interface POS 0/0/0/0 on the left to the correct order for implementation on the right.

exceed-action drop	1
exit	2
class TRAFFIC_CLASS	3
service-policy output POLICE_POLICY	4
policy-map POLICE_POLICY	5
configure	6
commit	7
interface pos 0/0/0/0	8
conform-action transmit	9
police rate percent 20	10

Answer:

Drag and drop the Cisco IOS XR commands used to create a policy that will limit all traffic to 20% of interface POS 0/0/0/0 on the left to the correct order for implementation on the right.

exceed-action drop	configure
exit	policy-map POLICE_POLICY
class TRAFFIC_CLASS	class TRAFFIC_CLASS
service-policy output POLICE_POLICY	police rate percent 20
policy-map POLICE_POLICY	conform-action transmit
configure	exceed-action drop
commit	exit
interface pos 0/0/0/0	interface pos 0/0/0/0
conform-action transmit	service-policy output POLICE_POLICY
police rate percent 20	commit

Explanation:

configure
policy-map POLICE_POLICY
class TRAFFIC_CLASS
police rate percent 20
conform-action transmit
exceed-action drop
exit
interface pos 0/0/0/0
service-policy output POLICE_POLICY
commit

QUESTION NO: 518 DRAG DROP

Drag the T1 parameters on the left to the corresponding category on the right. Not all options are used.	
B6ZS	**T1 Framing**
SF	
B3ZS	
B8ZS	**T1 Line Coding**
AMI	
CBIT	
ESF	

Answer:

Drag the T1 parameters on the left to the corresponding category on the right. Not all options are used.

B6ZS	
SF	
B3ZS	
B8ZS	
AMI	
CBIT	
ESF	

T1 Framing

SF
ESF

T1 Line Coding

B8ZS
AMI

Explanation:

T1 Framing

SF
ESF

T1 Line Coding

B8ZS
AMI

QUESTION NO: 519 DRAG DROP

Drag and drop the SONET parity error bit on the left to the corresponding SONET layer on the right.
Not all options will be used.

B1	section
E1	line
B2	path
E2	
B3	
E3	

Answer:

Drag and drop the SONET parity error bit on the left to the corresponding SONET layer on the right.
Not all options will be used.

B1		B1
E1		B2
B2		B3
E2		
B3		
E3		

Explanation:

| B1 |
| B2 |
| B3 |

QUESTION NO: 520 DRAG DROP

Drag and drop the appropriate default next-hop behavior on the left to the corresponding BGP routing prefix updates on the right.

iBGP to iBGP update	BGP next-hop changes by default
iBGP to eBGP update	
eBGP to iBGP update	
eBGP to eBGP update	
MP-iBGP to MP-iBGP update	
MP-iBGP to MP-eBGP update	BGP next-hop does not change by default
MP-eBGP to MP-iBGP update	
MP-eBGP to MP-eBGP update	

Answer:

Drag and drop the appropriate default next-hop behavior on the left to the corresponding BGP routing prefix updates on the right.

Left boxes
iBGP to iBGP update
iBGP to eBGP update
eBGP to iBGP update
eBGP to eBGP update
MP-iBGP to MP-iBGP update
MP-iBGP to MP-eBGP update
MP-eBGP to MP-iBGP update
MP-eBGP to MP-eBGP update

BGP next-hop changes by default

- iBGP to eBGP update
- eBGP to eBGP update
- MP-iBGP to MP-eBGP update
- MP-eBGP to MP-eBGP update

BGP next-hop does not change by default

- iBGP to iBGP update
- eBGP to iBGP update
- MP-iBGP to MP-iBGP update
- MP-eBGP to MP-iBGP update

Explanation:

BGP next-hop changes by default

- iBGP to eBGP update
- eBGP to eBGP update
- MP-iBGP to MP-eBGP update
- MP-eBGP to MP-eBGP update

BGP next-hop does not change by default

- iBGP to iBGP update
- eBGP to iBGP update
- MP-iBGP to MP-iBGP update
- MP-eBGP to MP-iBGP update