

Part 4

QUESTION 301

When troubleshooting a T1 problem on your network, you discover that a number of RED alarms are being generated. What does this red alarm on a T1 indicate?

- A. The CSU cannot synchronize with the framing pattern on the T1 line.
- B. The far end equipment has a problem with the signal it is receiving from the upstream equipment.
- C. There is an alarm on the line upstream from the equipment connected to the port generating the alarm.
- D. There is an alarm from the equipment connected to the port generating the alarm.
- E. The CSU is in a loopback.

Answer: A

Explanation:

A RED alarm is known as a Transmit Sending Remote Alarm.

A Red alarm is declared when the channel service unit (CSU) cannot synchronize with the framing pattern on the T1 line.

Reference:

http://www.cisco.com/en/US/tech/CK713/CK628/technologies_tech_note09186a00801069ff.shtml#topic5

QUESTION 302

With regard to PPPoA, which of the following statements are true? (Choose all that apply.)

- A. PPPoA contains information about NCP LCP and supports all AAL.
- B. PPPoA uses adaptation layer 5 (AAL5) as the framed protocol and is used primarily in xDSL.
- C. PPPoA is not a standard based protocol.
- D. In PPPoA architecture, IP address allocation for the subscriber CPE uses IPCP negotiation.
- E. PPPoA supports all ppp features except password PAP CHAP.

Answer: B, D

Explanation:

Point-to-Point Protocol (PPP) (RFC 1331) provides a standard method of encapsulating higher layer protocols across point-to-point connections. It extends the High-Level Data Link Control (HDLC) packet structure with a 16-bit protocol identifier that contains information about the content of the packet.

The packet contains three types of information:

- Link Control Protocol (LCP) negotiates link parameters, packet size, or type of authentication

- Network Control Protocol (NCP) contains information about higher layer protocols including IP and IPX, and their control protocols (IPCP for IP)
- Data frames containing data

PPP over ATM adaptation layer 5 (AAL5) (RFC 2364) uses AAL5 as the framed protocol, which supports both PVC and SVC. PPPoA was primarily implemented as part of ADSL. It relies on RFC1483, operating in either Logical Link Control-Subnetwork Access Protocol (LLC-SNAP) or VC-Mux mode. A customer premise equipment (CPE) device encapsulates the PPP session based on this RFC for transport across the ADSL loop and the digital subscriber line access multiplexer (DSLAM).

Incorrect Answers:

- A. PPPoA does not support every AAL and uses only AAL5.
- C. PPPoA is standards based.
- E. CHAP (Challenge authentication protocol) is supported in PPPoA.

Reference:

http://www.cisco.com/warp/public/794/pppoa_arch.html

QUESTION 303

Under one of the serial interfaces of your router you see the following configured:

Interface serial 0/0

Encapsulation PPP

IP address 10.1.1.1 255.255.255.252

Invert txclock

What is a reason for the "invert txclock" command being configured?

- A. It synchronizes TXD and RXD clocks.
- B. It corrects systems that use long cables that experience high error rates when operating at the higher transmission speeds.
- C. It is used for adjusting the transmit clock properties of the PPP negotiation process.
- D. It inverts the phase of the local clock used for timing incoming data the serial line.
- E. It is used to allow the interface to provide clocking, rather than receiving clocking from the line.

Answer: B

Explanation:

Systems that use long cables or cables that are not transmitting the TxC signal (transmit echoed clock line, also known as TXCE or SCTE clock) can experience high error rates when operating at the higher transmission speeds. For example, if a PA-8T synchronous serial port adapter is reporting a high number of error packets, a phase shift might be the problem. Inverting the clock might correct this shift.

Incorrect Answers:

- B. The invert txclock command is not related to PPP.
- E. This describes the purpose of the clocking source configuration for a serial line. The correct configuration command for determining the clocking source is "clock source".

QUESTION 304

A router has a T1 private line connection, with the encapsulation type set to HDLC. Which of the following are transfer modes that could be supported over this HDLC circuit? (Choose all that apply)

- A. LAPB
- B. ARB
- C. ABM
- D. ARM
- E. NRM
- F. LAPD

Answer: A, C, D, and E

Explanation:

The following are all transfer types supported by HDLC:

ARM - Asynchronous Response Mode. It is an HDLC communication mode involving one primary and at least one secondary, where either the primary or one of the secondaries can initiate transmissions.

ABM - Asynchronous Balanced Mode. It is an HDLC and derivative protocol, communication mode supporting peer-oriented point-to-point communications between two stations, where either station can initiate transmission.

NRM - Normal Response Mode

LAPB - Link Access Procedure Balanced

Incorrect Answers:

B, F. ARB and LAPD are not acronyms that apply to HDLC.

QUESTION 305

A Certkiller branch office uses Telnet and FTP to access an application at the main office over a point to point T1 HDLC link. You wish to increase the performance over this link through the use of a compression algorithm. What compression type will provide the best performance improvement?

- A. Compressed Real-time Transport Protocol
- B. TCP header compression
- C. Stacker compression
- D. Predictor compression

Answer: C

Explanation:

You can configure point-to-point software compression for all LAPB, PPP, and HDLC encapsulations using either the predictor or stacker compression methods. Compression reduces the size of frames via lossless data compression. HDLC encapsulations support the Stacker compression algorithm. PPP and LAPB encapsulations support both predictor

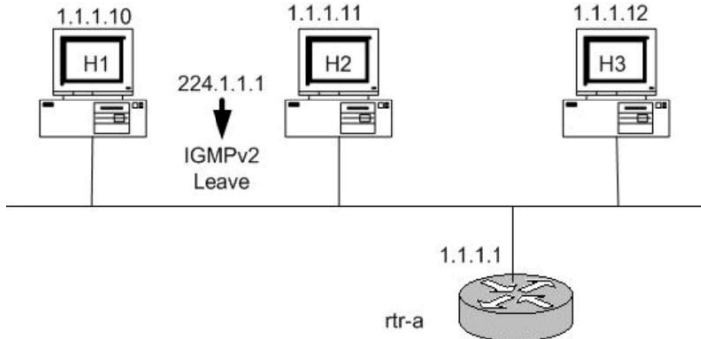
and Stacker compression algorithms.

When compression is performed in software installed in the router's main processor, it might significantly affect system performance.

Compression requires that both ends of the serial link be configured to use compression.

QUESTION 306

Part of the Certkiller IP multicast network is shown below:



H1, H2, H3, and rtr-a are all IGMP version 2 devices. Host 2 and Host 3 belong to the 224.1.1.1 group. After a while, H2 sends out an IGMPv2 Leave message to leave the 224.1.1.1 group. How will rtr-a react to this leave message?

- A. It will send an IGMPv2 Query to the all multicast hosts address 224.255.255.255.
- B. It will send an IGMPv2 Group Specific Query to 224.1.1.1
- C. It will send an IGMPv2 Leave Acknowledgement to Hosts H1 and H3.
- D. It will send an IGMPv2 General Query to 224.1.1.1
- E. It will send an IGMPv2 Group Specific Query to 224.0.0.1.

Answer: B

Explanation:

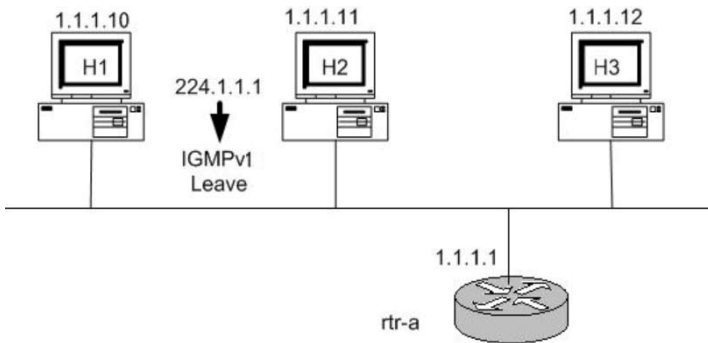
In IGMP version 2, a Leave message is responded by a group specific query from the router to check if there are any additional hosts participating in the multicast session. The group specific query is always destined for the multicast address that is being used.

Incorrect Answers:

- A. The address 224.255.255.255 would never be used in this situation. In fact, the notion of a multicast "broadcast" does not exist.
- C. Leave messages are not acknowledged.
- D. General Query messages are not used.
- E. The group specific query is always destined for the multicast address that is being used, which is 224.1.1.1 in this case.

QUESTION 307

The Certkiller network has a mix of IGMP version 1 and version 2 devices in its IP multicast network as shown below:



H1 and H2 are both IGMPv2 speakers and are also members of group 224.1.1.15. H3 is an IGMPv1 speaker and sends an IGMPv1 Membership Report to join group 224.1.1.15.

What will happen?

- A. The router rtr-a will do nothing, since there are already members of group 224.1.1.15 on the subnet.
- B. The router rtr-a will ignore all IGMPv2 Leave messages while the IGMPv1 host is a member of group 224.1.1.15.
- C. The router rtr-a will stop sending IGMPv2 Group-Specific queries in response to IGMPv1 Leaves received on this subnet for groups 224.1.1.15, while the IGMPv1 hosts is a member of group 224.1.1.15.
- D. The router rtr-a will ignore the IGMPv1 Membership Report because router rtr-a is an IGMPv2 speaker and IGMPv1 are not compatible.

Answer: B

Explanation:

With IGMP version 1 and version 2 on the same network, routers will revert to v1, so the router will ignore the leave requests from all v2 members as long as the v1 member is still active for that multicast session.

Incorrect Answers:

- A. Although there are already members on the same segment, the routers must be aware of the fact that there are a mix of v1 and v2 devices, so that the v2 leave messages can be ignored.
- C. When the v1 device leaves the multicast session, the router must still send the group query out to see if the v2 devices are also still actively participating in the multicast session.
- D. IGMP version 2 was designed to be backward compatible with version 1.

Reference:

"CCIE Professional Development Routing TCP/IP Volume II" by Jeff Doyle and Jennifer De Haven Carroll, Page 414.

QUESTION 308

IGMP is used to dynamically register individual hosts in a multicast group on a particular LAN. Hosts identify group memberships by sending IGMP messages to

their local multicast router. Under IGMP, routers listen to IGMP messages and periodically send out queries to discover which groups are active or inactive on a particular subnet.

Hosts need to actively communicate to the local multicast router that they intend to leave a group. If there are no replies, the router times out the group and stops forwarding the traffic. In order for this to work, what needs to be implemented?

- A. IGMPv1
- B. IGMPv2
- C. IGMPv3
- D. IGMPv4
- E. CGMP

Answer: B

Explanation:

The Internet Group Management Protocol (IGMP) is used by IP hosts to report their host group memberships to any immediately neighboring multicast routers. IGMP messages are encapsulated in IP datagrams, with an IP protocol number of 2. IGMP has versions IGMP v1, v2 and v3.

In IGMPv2, leave messages were added to the protocol. This allowed group membership termination to be quickly reported to the routing protocol, which is important for highbandwidth multicast groups and/or subnets with highly volatile group membership.

Incorrect Answers:

A. IGMPv1: Hosts can join multicast groups. There were no leave messages. Routers were using a time-out based mechanism to discover the groups that are of no interest to the members.

C. IGMPv3: Major revision of the protocol. It allows hosts to specify the list of hosts from which they want to receive traffic from. Traffic from other hosts is blocked inside the network. It also allows hosts to block inside the network packets that come from sources that sent unwanted traffic.

D. IGMPv4 is not yet in use.

E. CGMP is the Cisco Group Management Protocol (CGMP) which is a multicast protocol used by Cisco LAN switches, and not routers.

QUESTION 309

In the Certkiller network, hosts need to actively communicate to the local multicast router that they intend to leave a group. The router then sends out a group-specific query and determines if any remaining hosts are interested in receiving the traffic. If there are no replies, the router times out the group and stops forwarding the traffic. In order for this to work, what needs to be implemented?

- A. IGMPv1
- B. IGMPv2
- C. IGMP snooping

- D. DVMRO
- E. CGMP
- F. RGMP

Answer: B

Explanation:

IGMP version 2 is the Industry-standard protocol for managing multicast group membership, including support for IGMP-leave messages and group-specific queries. Leave Group message is a new type different from IGMP version 1. Membership Report is issued by host that want to join a specific multicast group (GDA). When IGMP router receive the Membership Report, it will add the GDA to the multicast routing table and start forwarding the IGMP traffic to this group. Membership Queries are issued by router at regular intervals to check whether there is still a host interested in the GDA in that segment. Host Membership Reports are sent either when the host wants to receive GDA traffic or response for a membership query from IGMP router.

If a host does not want to receive the IGMP traffic any more, it sends a Leave Group message. When the multicast router receives this Leave Group message, it removes the GDA from the multicast routing table. In addition, IGMP multicast routers periodically send Host Membership Query messages (hereinafter called Queries) to discover which host groups have members on their attached local networks. If no Reports are received for a particular group after some number of Queries, the routers assume that that group has no local members and that they need not forward remotely-originated multicasts for that group onto the local network. In addition, IGMP version 2 has leave mechanisms.

Incorrect Answers:

A. In IGMP version 1, hosts can join multicast groups. There were no leave messages. Routers were using a time-out based mechanism to discover the groups that are of no interest to the members.

D, F. These are incorrect terms for this IP multicasting functionality.

E. CGMP is used between Cisco switches and routers to provide for IP multicast information to be passed between the two.

QUESTION 310

Choose the correct protocols to handle IP multicast efficiently in the Certkiller layer 2 switched IP network. (Select the best choice).

A. Use Router-Port Group Mangement Protocol (RGMP) on subnets that include end users or receiver clients. Use Cisco Group Management Protocol (CGMP), IGMP Snooping on routed segments that contain only routers, such as in a collapsed backbone.

B. Use Router-Port Group Mangement Protocol (RGMP) on subnets that include end users or receiver clients and routes segments that contain only routers, such as in a collapsed backbone.

C. Use Cisco Group Management Protocol (CGMP), IGMP Snooping on subnets that include end users or receiver clients. Use Router-Port Group Management

Protocol (RGMP) on routed segments that contain only routers, such as in a collapsed backbone.

D. Use Cisco Group Management Protocol (CGMP) on subnets that include end users or receiver clients and routed segments that contain only routers, such as in a collapsed backbone.

E. Use IGMP Snooping on subnets that include end users or receiver clients and routed segments that contain only routers, such as in a collapsed backbone.

Answer: C

Explanation:

The purpose of Cisco Group Management Protocol (CGMP) and Internet Group Management Protocol (IGMP) snooping is to restrain multicast traffic in a switched network. By default, a LAN switch floods multicast traffic within the broadcast domain. This can consume a lot of bandwidth if many multicast servers are sending streams to the segment.

IGMP snooping is a feature that allows the switch to "listen in" on the IGMP conversations between hosts and routers. When a switch hears an IGMP report from a host for a given multicast group, the switch adds the host's port number to the GDA list for that group. And, when the switch hears an IGMP Leave, it removes the host's port from the CAM table entry.

RGMP constrains multicast traffic that exits the Cisco Router through ports to which only disinterested multicast routers are connected. RGMP reduces network congestion by forwarding multicast traffic to only those routers that are configured to receive it.

Note: To use RGMP, you must enable IGMP snooping on the Cisco router. IGMP snooping constrains multicast traffic that exits through LAN ports to which hosts are connected. IGMP snooping does not constrain traffic that exits through LAN ports to which one or more multicast routers are connected.

QUESTION 311

How are Layer 3 multicast IP addresses mapped to Token Ring MAC addresses? (Choose all that apply).

A. All IP Multicast addresses are mapped to broadcast MAC address FFFF.FFFF.FFFF.

B. All IP Multicast addresses are mapped to network MAC address 0000.0000.0000.

C. All IP Multicast addresses are mapped to Functional Address C000.0004.0000.

D. In the same method as is used in Ethernet networks.

E. Token ring MAC addresses are not mapped to IP multicast addresses.

Answer: A, C

Explanation:

By default, IP multicast datagrams on Token Ring LAN segments used the MAC-level broadcast address 0xFFFF.FFFF.FFFF. That places an unnecessary burden on all devices that do not participate in IP multicast. The IP multicast over Token Ring LANs feature

defines a way to map IP multicast addresses to a single Token Ring MAC address. This feature defines the Token Ring functional address (0xc000.0004.0000) that should be used over Token Ring. A functional address is a severely restricted form of multicast addressing implemented on Token Ring interfaces. Only 31 functional addresses are available. A bit in the destination MAC address designates it as a functional address. The implementation used by Cisco Systems complies with RFC 1469, IP Multicast over Token-Ring Local Area Networks.

Reference:

See RFC 1469, IP Multicast over Token-Ring Local Area Networks

Also see

http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/np1_c/1c_multi.htm#21101

QUESTION 312

The IANA owns a block of Ethernet MAC address that start with 01:00:5E in hexadecimal format. Half of this block is allocated for multicast addresses. The range from 0100.5e00.0000 through 0100.5e7f.ffff is the available range of Ethernet MAC address for IP multicast.

This allocation allow for 23 bits in the Ethernet address to correspond to the IP multicast group address. The mapping places the lower 23 bits of the IP multicast group address into these available 23 bits in the Ethernet address.

Because the upper five bits of the IP multicast address are dropped in this mapping, the resulting address is not unique. In fact, 32 different multicast group IDs map to the same Ethernet address.

225.1.1.1 and 237.1.1.1 have been assigned to map to the same multicast MAC address on a Layer 2 switch. What will occur?

- A. If one user is subscribed to Group A (as designated by 225.1.1.1) and the other user is subscribed to Group B (as designated by 237.1.1.1), they would both receive only the streams meant for them. Group A would go to 225.1.1.1 and group B would go to 237.1.1.1
- B. If one user is subscribed to Group A (as designated by 237.1.1.1) and the other user is subscribed to Group B (as designated by 225.1.1.1), they would both receive only the first stream that reached the network.
- C. If one user is subscribed to Group A (as designated by 225.1.1.1) and the other user is subscribed to Group B (as designated by 237.1.1.1), they would both receive both streams, A and B streams.
- D. If one user is subscribed to Group A (as designated by 225.1.1.1) and the other user is subscribed to Group B (as designated by 237.1.1.1), both of them would not receive A and B streams.
- E. None of the above

Answer: C

Explanation:

Although mathematically there are 32 possibilities for overlap of addresses it is very

unlikely to happen in real life. If it does, the impact is that another set of stations receives the multicast traffic. This is still far preferable to ALL stations receiving the traffic. This is always the case where two IP multicast addresses share the same MAC address.

QUESTION 313

Which IP address maps to the Ethernet multicast MAC address of 01-00-5e-10-20-02? (Choose all that apply)

- A. 224.128.10.2
- B. 225.128.10.2
- C. 224.10.20.2
- D. 225.10.20.2
- E. 239.144.32.2
- F. 224.16.32.2
- G. All of the above
- H. None of the above

Answer: E, F

Explanation:

Ethernet interfaces map the lower 23 bits of the IP multicast address to the lower 23 bits of the MAC 0100.5e00.0000. As an example, the IP multicast address 224.0.0.2 is mapped to the MAC layer as 0100.5e00.0002.

- HEX 01 = 00-5e (all Multicast Addresses);
- HEX 10 = 00010000 - could be both 16 and 144 (decimal) due to the fact that we ignore the first bit of the second octet when converting to binary;
- HEX 20 = 00100000 = 32;
- HEX 02 = 00000010 = 2.

QUESTION 314

What is the class D IP address range 239.0.0.0-239.255.255.255 used for?

- A. Administratively Scoped multicast traffic meant for internal use.
- B. Link-local multicast traffic made up of network control messages meant to stay in the local subnet.
- C. Global Internet multicast traffic meant to travel throughout the Internet.
- D. Any valid multicast data stream for use with multicast applications.
- E. Routing protocol use.

Answer: A

Explanation:

The 239 address range is reserved for IP multicast traffic that is to be used for internal use only. It is similar to RFC 1918 private IP address space, except instead of specifying unicast address ranges it specifies multicast.

Incorrect Answers:

B, E. Link level multicast messages, such as those used by routing protocols, use the 224.0.0.0 address range. For example, IGRP uses 224.0.0.10 and OSPF uses 224.0.0.5 and 224.0.0.6.

C, D. This address range should never be seen in the Internet. It is reserved for private use only.

Reference:

Jeff Doyle Volume II chapter on IP Multicast.

QUESTION 315

You wish to implement a multicast video application over your private, internal network. To do this, you need to use a private multicast range of IP addresses across your network. Which IP range should you use?

- A. 224.0.0.0 - 224.255.255.255
- B. 226.0.0.0 - 226.255.255.255
- C. 241.0.0.0 - 241.255.255.255
- D. 239.0.0.0 - 239.255.255.255
- E. 240.0.0.0 - 254.255.255.255.

Answer: D

Explanation:

The reserved, administratively scoped IPv4 multicast address space is defined to be the range 239.0.0.0 to 239.255.255.255. Administratively scoped multicast addresses are for use only on a private network and are not to be used on the Internet.

Reference:

RFC 2365 - <http://www.faqs.org/rfcs/rfc2365.html>

QUESTION 316

The Certkiller network is using IP multicast within to conserve bandwidth during the training video seminars. In this IP multicast network, which of the following correctly describes scoping?

- A. Scoping is the restriction of multicast data transport to certain limited regions of the network. There are two types: TTL scoping and administrative scoping.
- B. Scoping is used by SSM to locate the sources and receivers in certain limited regions of the network. There are two types: TTL scoping and administrative scoping.
- C. Scoping is a process used in MSDP to locate the sources and receivers in different AS.
- D. PIM dense mode uses scoping to locate the sources and receivers in order to built shared trees.

Answer: A

Explanation:

Traditionally, IP multicast uses a Time to Live (TTL) parameter in an IP multicast application and multicast routers to control the multicast distribution. When you define the TTL value in an IP multicast application, contents don't transmit beyond the TTL value. For example, if you set Site Server's Active Channel Multicaster TTL value to 10, you ensure that Site Server's Web contents don't multicast beyond 10 router hops. Each multicast packet carries a TTL value in its IP header. Just as in unicast, every time a multicast router forwards a multicast packet, the router decreases the packet's TTL by 1. As an alternative to TTL scoping, the Internet Engineering Task Force (IETF) proposed Administratively Scoped IP Multicast as an Internet standard in its Request for Comments (RFC) 2365 in July 1998. Administrative scoping lets you scope a multicast to a certain network boundary (e.g., within your organization) by using an administratively scoped address. IETF has designated IP multicast addresses between 239.0.0.0 and 239.255.255.255 as administratively scoped addresses for local use in intranets. You can configure routers that support administratively scoped addressing on the border of your network to confine your private multicast region. You can also define multiple isolated multicast regions in your network so that sensitive multicast data will travel only within a designated area.

QUESTION 317

The Certkiller network is implementing IP multicast and they want to ensure that the IP addresses they used are contained within the Certkiller autonomous system. What is the range of limited scope/administrative scope addresses that should be used?

- A. Addresses in the 232.0.0.0/8 range
- B. Addresses in the 239.0.0.0/8 range
- C. Addresses in the 224.0.0.0/8 range
- D. Addresses in the 229.0.0.0/8 range
- E. Addresses in the 234.0.0.0/8 range
- F. None of the above

Answer: B

Explanation

The range of addresses from 239.0.0.0 through 239.255.255.255 contains limited scope addresses or administratively scoped addresses. These are defined by RFC 2365 to be constrained to a local group or organization. Routers are typically configured with filters to prevent multicast traffic in this address range from flowing outside an autonomous system (AS) or any user-defined domain. Within an autonomous system or domain, the limited scope address range can be further subdivided so those local multicast boundaries can be defined. This also allows for address reuse among these smaller domains. These addresses are the IP multicast version of the private, RFC 1918, addresses used for unicast.

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

QUESTION 318

In an IP multicast network, the more sources an application has, the less frequently

traffic is sent from each end. Each time a source starts to send packets, protocol operations take place and a forwarding state is established. For applications with a large number of sources, this state can time-out before the source would only create a large number of sources, this state can time-out before sources would not only create a large amount of forwarding state (requiring memory), but they could also require high CPU usage of the routing processor due to the accounting of frequently changing state. In addition, the signaling within the router between the routing processor and forwarding hardware can become another potential bottleneck of continuously large amount of traffic signaling must go to the routing processor and equally large amounts of forwarding state changes must go to the forwarding engine(s).

The Certkiller network is implementing IP multicast, and they wish to avoid the problems described above. Based on this information, what IP multicast technology would you recommend?

Caution: This protocol should avoid maintaining source-specific forwarding state, thereby reducing the amount of memory needed by the number of sources per multicast group, requiring much less traffic signaling in the protocol, preventing the "bursty source" problem, saving on CPU requirements for protocol operations and avoiding potential internal performance limits.

- A. PIM Dense Mode (PIM DM)
- B. PIM Sparse Mode (PIM SM)
- C. Distance Vector Multicast Routing Protocol (DVMRP)
- D. Multicast Open Shortest Path First (MOSPF)
- E. Bi-directional PIM

Answer: E

Explanation:

Bidirectional-PIM is a variant of the Protocol Independent Multicast (PIM) suite of routing protocols for IP multicast. In PIM, packet traffic for a multicast group is routed according to the rules of the mode configured for that multicast group. The Cisco IOS implementation of PIM supports three modes for a multicast group:

- Bidirectional mode
- Dense mode
- Sparse mode

A router can simultaneously support all three modes or any combination of them for different multicast groups. In bidirectional mode, traffic is routed only along a bidirectional shared tree that is rooted at the rendezvous point (RP) for the group. In bidir-PIM, the IP address of the RP acts as the key to having all routers establish a loopfree spanning tree topology rooted in that IP address. This IP address need not be a router, but can be any unassigned IP address on a network that is reachable throughout the PIM domain. Using this technique is the preferred configuration for establishing a redundant RP configuration for bidir-PIM.

In PIM dense mode (PIM-DM), PIM-SM, and most other multicast routing protocols such as Distance Vector Multicast Routing Protocol (DVMRP) and Multicast Open

Shortest Path First (MOSPF), protocol operations and maintenance of packet forwarding state depend on signaling the presence or expiration of traffic (where "signaling" refers to both the packet forwarding engine to routing protocol process within the routers and the packet exchange part of the routing protocol). Triggering PIM assert messages, PIM register messages, and source tree forwarding state are all examples of traffic signaling. There are several advantages to traffic signaling, but they can lead to problems for applications with a large number of sources. For example, the more sources an application has, the less frequently traffic is sent from each sender. Each time a source starts to send packets, protocol operations take place and forwarding state is established. For applications with a large number of sources, this state can time out before the source sends again, resulting in "bursty sources." Therefore, applications with a large number of sources would not only create a large amount of forwarding state (requiring memory), but they also could require high CPU usage on the Route Processor due to the accounting of frequently changing state. In addition, the signaling within the router between the Route Processor and forwarding hardware can become a bottleneck if continuously large amounts of traffic signaling must go to the Route Processor and equally large amounts of forwarding state changes must go to the forwarding engines.

Bidir-PIM solves all these problems. Not only does bidir-PIM avoid maintaining sourcespecific forwarding state, therefore reducing the amount of memory needed by the number of sources per multicast group, but it also does not require any traffic signaling in the protocol. Thus, bidir-PIM prevents the "bursty source" problem, saving on CPU requirements for protocol operations and avoiding potential router internal performance limits.

Reference:http://www.cisco.com/en/US/products/sw/iosswrel/ps1612/products_feature_guide09186a0080080a41.html

QUESTION 319

You are a technician at Certkiller . Your newly appointed Certkiller trainee wants to know which IP protocol is used to send PIMv2 control messages.
What would your reply be?

- A. UDP
- B. TCP
- C. BGP
- D. Protocol number 107
- E. Protocol number 103

Answer: E

Explanation:

All PIM control messages have protocol number 103.

Reference:

<http://www.ietf.org/proceedings/99mar/I-D/draft-ietf-pim-v2-dm-01.txt>

QUESTION 320

IP multicast addresses in the range of 224.0.0.0 through 224.0.0.255 are reserved for

what purpose?

- A. It is reserved for Administratively Scoped multicast traffic intended to remain inside a private network.
- B. It is reserved for Administratively Scoped multicast traffic that is not supposed to be transmitted onto the Internet.
- C. It is reserved for link-local multicast traffic consisting of network control messages that is not supposed to leave the local subnet.
- D. Any valid multicast data stream used by multicast applications.
- E. Global Internet multicast traffic intended to travel throughout the Internet.

Answer: C

Explanation:

As found in RFC1112. These addresses are used by many routing protocols such as OSPF and RIPv2, in order to sent updates to all neighbors on the same segment.

Incorrect Answers:

- A, B. Administratively Scoped IP multicast addresses are contained in the 239.0.0.0-239.255.255.255 range.
- D, E. The 224.0.0.0/8 network range is not intended to be used outside of the local subnet link.

QUESTION 321

Which of the following PIMv2 Sparse mode control messages are also used in PIM Dense mode? (Choose all that apply.)

- A. Graft
- B. Join
- C. Prune
- D. Register
- E. Assert
- F. Hello
- G. Register

Answer: B, C, E, and F

PIM-DM uses the following PIMV2 messages.

- Hello
- Join/Prune
- Graft
- Graft-Ack
- Assert

PIM-SM uses the following PIMV2 messages

- Hello
- Bootstrap
- Candidate-RP-Advertisement
- Join/Prune

- Assert
- Register
- Register-Stop

Reference:

'CCIE Professional Development Routing TCP/IP Volume 2' in the section 'Understanding IP Multicast Routing' pages 475 and 488.

QUESTION 322

What best describes the Source Specific Multicast (SSM) functionality?

- A. SSM is an extension of the DVMRP protocol that allows for an efficient data delivery mechanism in one-to-many communications.
- B. SSM requires MSDP to discover the active sources in other PIM domains.
- C. In SSM routing of multicast traffic is entirely accomplished with source trees. The RP is used to direct receivers to the appropriate source tree.
- D. Using SSM, the receiver application can signal its intention to join a particular source by using the INCLUDE mode in IGMPv3.
- E. None of the above

Answer: D

Explanation:

The Internet Standard Multicast (ISM) service is described in RFC 1112, Host Extensions for IP Multicasting. This service consists of the delivery of IP datagrams from any source to a group of receivers called the multicast host group. The datagram traffic for the multicast host group consists of datagrams with an arbitrary IP unicast source address S and the multicast group address G as the IP destination address. Systems will receive this traffic by becoming members of the host group. Membership to a host group simply requires signalling the host group through IGMP Version 1, 2, or 3.

In SSM, delivery of datagrams is based on (S, G) channels. Traffic for one (S, G) channel consists of datagrams with an IP unicast source address S and the multicast group address G as the IP destination address. Systems will receive this traffic by becoming members of the (S, G) channel. In both SSM and ISM, no signalling is required to become a source. However, in SSM, receivers must subscribe or unsubscribe to (S, G) channels to receive or not receive traffic from specific sources. In other words, receivers can receive traffic only from (S, G) channels to which they are subscribed, whereas in ISM, receivers need not know the IP addresses of sources from which they receive their traffic. The proposed standard approach for channel subscription signalling utilizes IGMP INCLUDE mode membership reports, which are supported only in IGMPv3.

Incorrect Answers:

- A. SSM is associated with PIM in IPv6 multicast networks. It is not associated with DVMRP.
- B. SSM builds off of PIM-SM, but also requires an update to IGMP. IGMP version 3 includes a larger header, where the source address can be specified, in addition to the group address. This means that a router no longer needs to communicate with an RP in

order to locate the source, and also means that MSDP is no longer needed since its only purpose is to pass information among RPs.

C. PIM-SSM is made possible by IGMPv3. Because hosts can now indicate interest in specific sources using IGMPv3, PIM can create state directly along the path to those sources using SSM. SSM does not require a rendezvous point (RP) to operate.

QUESTION 323

The Certkiller network is setting up a VPN for the IP multicast traffic. What best describes the MDT role in MVPN operations?

A. PE routers that have CE routers who are intended recipients of the data only join data MDT. PE routers signal use of data-MDT via a UDP packet on port 3232, which is sent via the default MDT. This packet contains an all-PIM routers message, indicating the group is joined if required.

B. CE routers do not have a PIM adjacency across the provider network with remote CE routers, but rather have an adjacency with their local routes on the PE router. When the PE router receives an MDT packet, it performs an RPF check. During the transmission of the packet through the Provider network, the normal RPF rules apply. However, at the remote's PE, the router needs to ensure that the originating PE router was the correct one for that CE. It does this by checking the BGP next hop address of the customer's packet's source address. This next hop address should be the source address of the MDT packet. The PE also checks that there is a PIM neighbor relationship with the remote PE.

C. A unique Group address is required to be used as MDT for each particular customer. A unique source address for the Multicast packet in the provider network is also required. This source address is recommended to be the address of the loopback interface, which is used as the source for the IBGP, as this address is used for the RPF check at remote PE.

D. PE routers are the only routers that need to be MVPN aware and able to signal to remote PE's information regarding the MVPN. It is therefore fundamental that all PE routers have a BGP relationship with each other. Either directly or via a Route Reflector. The source address of the Default-MDT will be the same address used to source the IBGP sessions with the remote PE routers that belong to the same VPN and MVRP.

E. All of the above.

Answer: E

Explanation:

Cisco MVPN Details:

While there are significant deployment obstacles to each of the preceding MVPN solutions, Multicast Domains is the most attractive alternative because:

- The provider must configure a native IP multicast network within their core network; this includes both the P and PE routers.
- IP Multicast is a mature technology that has been deployed since Cisco IOS Software 10.0. This minimizes risk for the provider network, because a new

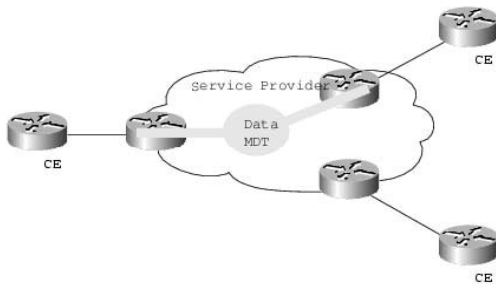
feature will not have to be introduced into its core to support MVPNs.

Multicast Domain Solution

This method originally had less than optimal performance, because it requires that all PE routers connected to a customer receive all of that customer's Multicast data regardless of the presence of an interested receiver in that location. When enhancements resolved this characteristic with a new methodology, it became a truly attractive solution.

Figure 3

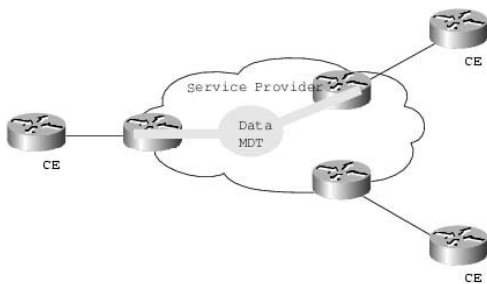
Default MDT Concept



The aforementioned enhancement is the addition of ephemeral trees that are created 'on the fly'. These trees distribute multicast group data that exceeds a certain configured threshold of Bandwidth (BW) to only those PE who have joined this new tree. These trees are called MDT-data trees. The word data is appended as these groups are designed to be used for groups that will require a higher amount of bandwidth to deliver their data.

Figure 4

Data MDT Concept



This diagram indicates that the Data MDT is only joined by those PE routers that have CE routers who are intended recipients of the data.

PE routers signal use of Data-MDT via a UDP packet on port number 3232, which is sent via the default MDT. This packet contains an all-PIM routers message, indicating the group to be joined if required.

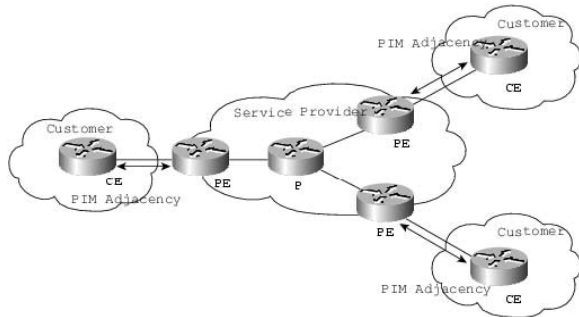
Interaction of Customer and Providers Multicast Network

It is important to remember that the customer's IP Multicast network has no relationship to the provider's multicast network. From the perspective of the provider, the customer's IP Multicast packets are merely data to the provider's distinctive IP Multicast network.

It is important to understand that PIM, and in particular PIM-SM, are the only supported multicast protocols for MVPN. Bi-Dir PIM may be supported in the future, when it is deemed stable enough for the core of a provider network.

Figure 5

Customer PIM Adjacencies



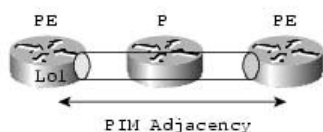
CE routers do not have a PIM adjacency across the provider network with remote CE routers, but rather have an adjacency with their local routers and the PE router. When the PE router receives an MDT packet, it performs an RPF check. During the transmission of the packet through the Provider network, the normal RPF rules apply. However, at the remote's PE, the router needs to ensure that the originating PE router was the correct one for that CE. It does this by checking the BGP next hop address of the customer's packet's source address. This next hop address should be the source address of the MDT packet. The PE also checks that there is a PIM neighbourhood with the remote PE.

Currently, only a single MVRP is supported per customer. This limitation precludes the customer also receiving Internet or any other outside domain's Multicast traffic. A unique Group address is required to be used as MDT for each particular customer. A unique source address for the Multicast packet in the provider network is also required. This source address is recommended to be the address of the loopback interface, which is used as the source for the iBGP, as this address is used for the RPF check at remote PE. If the provider uses MDT-data groups, then these will also need to be configured. These MDT-data groups must be unique for each customer.

The PE routers must have a PIM adjacency to each other. No other routing protocols may use these MTIs.

Figure 6

Provider's PIM Adjacencies



BGP Requirements

PE routers are the only routers that need to be MVPN aware and able to signal to remote PE's information regarding the MVPN. It is therefore fundamental that all PE routers have a BGP relationship with each other. Either directly or via a Route Reflector.

The source address of the Default-MDT will be the same address used to source the iBGP sessions with the remote PE routers that belong to the same VPN and MVRP. When PIM-SSM is used for transport inside the provider core, it is via this BGP relationship that the PEs indicate that they are MVPN capable and provide for source discovery. This capability is indicated via the updated BGP message.

Reference: http://www.cisco.com/en/US/tech/CK828/technologies_white_paper09186a00800a3db6.shtml

QUESTION 324

An enterprise customer runs their core network as an ISP network where they have different Autonomous Systems (AS). The BGP core runs OSPF for Intra-connection only. Data center A is in AS 1, data center B is in AS 2, and data center C is in AS 3. The remote locations will be running an IGP and redistribute their routes into BGP core. They would like to enable multicast throughout their network to support multicast applications.

Based upon the scenario, what would be the LEAST EFFECTIVE way to implement IP multicast?

A. This network runs essentially as an ISP's network with a BGP core and different AS. To implement multicast in this network they can enable MBGP over the BGP backbone.

B. This is customer's internal network and not a transit provider in the inter-domain SP routing. As long as there is no incongruence (between multicast and unicast topologies), there is no need to run MBGP. They simply run PIM-SM and MSDP for redundancy.

C. Running MBGP, besides BGP, should present negligible overhead and if done together with the introduction of IP multicast will help to avoid problems later on when the network has grown and some incongruence needs to be supported. At that point, the customer may need to upgrade to MBGP throughout the network to have the transitive nature of incongruence supported correctly, and this may then become an obstacle in deployment. Therefore, MBGP should be implemented.

D. It should be determined what IP multicast applications the customer is intending to run. Source Specific Multicast (SSM) should be recommended to the customer, since it would allow them to overcome MSDP and thus reduce the complexity of IP multicast in their deployment.

E. PIM uses the unicast routing information to perform the multicast forwarding function. They can simply implement Inter AS PIM (IAPIM) to exchange the multicast routing information. This would be the easiest way to implement multicast in the current network where they leverage all the current unicast routing protocol information to populate the multicast routing table, including Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest path First (OSPF), Border Gateway Protocol (BGP), and static routes. This approach would also cause less processing on the routers as PIM does not send and receive routing updates between routers.

Answer: B

Explanation:

The Multicast Source Discovery Protocol (MSDP) is a mechanism to connect multiple PIM sparse-mode (SM) domains. MSDP allows multicast sources for a group to be known to all rendezvous point(s) in different domains. Each PIM-SM domain uses its own rendezvous points and does not need to depend on them in other domains. A rendezvous point runs MSDP over TCP to discover multicast sources in other domains. MSDP is also used to announce sources sending to a group. These announcements must

originate at the domain's Rendezvous Point. MSDP depends heavily on MP-BGP for interdomain operation. Because of this, choice B is the least effective choice since it recommends running MSDP without MGBP.

QUESTION 325

Which of the following is used to calculate the upstream neighbor interface for a multicast route entry in a PIMv2 Sparse Mode network?

- A. The address of the Mapping Agent.
- B. The address of a directly connected member of the multicast group.
- C. The address of the currently active Rendezvous Point for the multicast group.
- D. The address of the PIM neighbor that sent the PIM Join message.
- E. The address of the PIM neighbor that sent the PIM Hello message.

Answer: C

Explanation:

The address of the upstream neighbor in any PIMv2 Sparse Mode network is always calculated via the neighbor closest to the Rendezvous Point (RP).

Incorrect Answers:

- A. The upstream neighbor for a multicast group is calculated from the RP, not the mapping agent.
- B. The directly connected multicast neighbor would only be used if it were the nearest upstream neighbor toward the RP, which will not always be the case.
- D, E. The neighbor that sends the PIM messages is not necessarily going to be the same neighbor that is upstream toward the RP, so these choices are also incorrect.

Reference:

CCIE Professional Development Routing TCP/IP Volume II by Jeff Doyle and Jennifer De Haven Carroll, Page 492.

QUESTION 326

What best describes PIM functionality?

- A. PIM uses the multicast routing information to perform the multicast forwarding function. PIM is a multicast routing protocol, and uses the multicast routing table to perform the RPF check. Like other routing protocols, PIM sends and receives routing updates between routers.
- B. PIM uses unicast routing protocol information that populates the unicast routing table, including EIGRP, OSPF, BGP, and static routes.
- C. PIM uses the multicast and unicast routing information to perform the multicast forwarding function. PIM uses the multicast routing table to perform the RPF check. Like other routing protocols, PIM does not send and receive routing updates between routers.
- D. PIM uses multicast routing protocols to populate the multicast routing table, including Distance Vector Multicast Routing Protocol (DVMRP); Multicast

OSPF (MOSPF), Multicast BGP

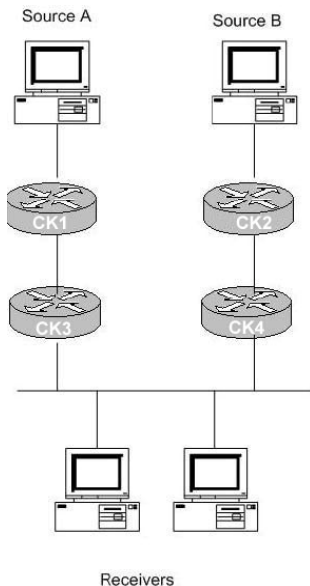
Answer: B

Explanation:

Protocol-independent multicast (PIM) gets its name from the fact that it is IP routing protocol-independent. PIM can leverage whichever unicast routing protocols are used to populate the unicast routing table, including EIGRP, OSPF, BGP, or static routes. PIM uses this unicast routing information to perform the multicast forwarding function, so it is IP protocol-independent. Although PIM is called a multicast routing protocol, it actually uses the unicast routing table to perform the reverse path forwarding (RPF) check function instead of building up a completely independent multicast routing table. PIM does not send and receive multicast routing updates between routers like other routing protocols do.

QUESTION 327

The Certkiller network is shown in the following exhibit:



Router CK1 is configured as follows:

```
ip multicast-routing
interface loopback0
ip address 192.168.1.1 255.255.255.0
ip pim send-RP-announce loopback0 scope 16 group-list 1
ip pim send-RP-discovery loopback0 scope 16
access-list 1 permit 239.0.0.0 0.255.255.255
```

Router CK2 is configured as follows:

```
ip multicast-routing
interface loopback 0
ip address 192.168.11.1 255.255.255.0
ip pim send-RP-announce loopback0 scope 16 group-list 1
ip pim send-RP-discovery loopback0 scope 16
access-list 1 permit 239.0.0.0 0.255.255.255
```

Which of the routers will take on the function of Mapping Agent and source Auto-RP Discovery messages to the 224.0.1.40 group?

- A. Router CK1
- B. Router CK2
- C. Both Router CK1 and Router CK2
- D. Neither, since the access lists configured do not match 224.0.1.40 multicast traffic.

Answer: C

Explanation:

If several RPs announce themselves for a multicast group range, the mapping agent chooses only one, which is the RP with the highest IP address. However, this is for selecting the RP. There is no election process for selecting the mapping agent that will source auto-RP discovery message. Both A and B will source this message.

Incorrect Answers:

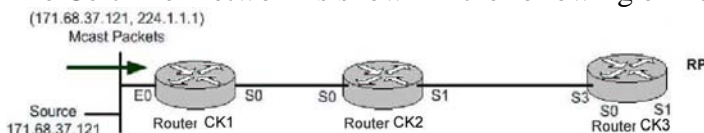
A, B. If only one router were elected as a mapping agent, this would adversely affect the other source, since it would not have a mapping agent.

B. This would be the correct choice if the question were related to the RP election, and not the mapping agent election. When multiple routers contend to be the Rendezvous Point, the router with the highest IP address wins the tie-breaker and will be elected as the RP. However, there can be multiple mapping agents in the network, as would be the case in this situation.

D. All PIM-enabled routers automatically join the Cisco RP discovery group (224.0.1.40) that allows them to receive all group-to-RP mapping information. This information is distributed by an entity called RP mapping agent. Therefore, the access list is irrelevant in this case.

QUESTION 328

The Certkiller network is shown in the following exhibit:



While troubleshooting a problem with the IP multicast network, you see the following on router CK1 :

(* , 224.1.1.1), 00:00:03/00:00:00, RP 171.68.28.140, flags:
SP

Incoming interface: Serial0, RPF nbr 171.68.28.191,

Outgoing interfaces list: Null

(171.68.37.121/32, 224.1.1.1), 00:00:03/00:02:56, flags FPT

Incoming interface: Ethernet0, RPF nbr 0.0.0.0, Registering

Outgoing interface list: Null

Which of the following could be the cause of the "Registering" condition on CK1 ?

(Choose all that apply)

- A. Router CK1 has incorrectly calculated the RPF interface for the source (171.68.37.121) as Serial1.
- B. Router CK3 (RP) failed to send a "Register-Stop" message to Router CK2 .
- C. Router CK2 is IGMP version 1 while Router CK1 is an IGMP version 2 speaker.
- D. PIM is not enabled on Router CK2 .
- E. Registering is the normal operational status of an operational multicast session.

Answer: B, D

Explanation:

The Rendezvous Point will need to send a "Register Stop" in order to clear the registration process, and all routers in between the RP and the multicast source must be multicast enabled.

Incorrect Answers:

- A. The output shows that this is not the problem, as router CK1 is correctly calculating the incoming interface as Ethernet 0.
- C. IGMP is used by hosts, and IGMP version 2 is backwards compatible with version 1.

Reference:

Developing IP Multicast Networks, (from page 259, PIM register process).

QUESTION 329

What interface command must be configured for auto-rp to function properly?

- A. ip pim dense-mode
- B. ip pim sparse-dense-mode
- C. ip pim sparse-mode
- D. ip multicast helper

Answer: B

Explanation:

RPs are used by senders to a multicast group to announce their existence and by receivers of multicast packets to learn about new senders.

Auto-RP is a feature that automates the distribution of group-to-RP mappings in a PIM network. Auto-RP has the following benefits:

- Configuring the use of multiple RPs within a network to serve different group ranges is easy.
- Auto-RP allows load splitting among different RPs and arrangement of RPs according to the location of group participants.
- Auto-RP avoids inconsistent, manual RP configurations that can cause connectivity problems.

Example configuration using Auto-RP:

```
ip multicast-routing
interface ethernet 0/0
ip pim sparse-dense-mode
```



```
ip pim send-rp-announce ethernet 0 scope 16 group-list 1
ip pim rp-address 10.8.0.20 1
```

Incorrect Answers:

- A. Rendezvous points are used in sparse mode multicasts, not dense mode.
- C. If router interfaces are configured in sparse mode only a static RP address must also be configured.
- D. This is an invalid command.

QUESTION 330

The Certkiller network is utilizing IP multicast technology. Along with this, router CK1 is configured as an anycast Rendezvous Point (RP). What best describes the functionality of Anycast RP?

- A. Anycast RP is a useful application of MSDP, MBGP and SSM that configures a multicast sparse mode network to provide for fault tolerance and load sharing within a single multicast domain.
- B. Only a maximum of two RPs are configured with the same IP address (for example, 10.0.0.10) on loopback interfaces. The loopback address should not be configured as a host address (with a 32-bit mask). All the downstream routers are configured so that they know that 10.0.0.10 is the IP address of their local RP.
- C. IP routing automatically selects the topologically closest RP for each source and receiver. Because some sources use only one RP and some receivers a different RP, MBGP enables RPs to exchange information about active sources. All the RPs are configured to be MSDP peers of each other.
- D. Each RP will know about the active sources in its own area. If RP fails, IP routing converges and backup RP would become the active RP of this area using HSRP.
- E. Anycast RP is an implementation strategy that allows load sharing and redundancy in PIM sparse mode (PIM-SM) networks by configuring two or more RPs that have the same IP address and a CK using Multicast Source Discovery Protocol to share active source information.

Answer: E

Explanation:

IP multicast is deployed as an integral component in mission-critical networked applications throughout the world. These applications must be robust, hardened, and scalable to deliver the reliability that users demand.

Using Anycast RP is an implementation strategy that provides load sharing and redundancy in Protocol Independent Multicast sparse mode (PIM-SM) networks. Anycast RP allows two or more rendezvous points (RPs) to share the load for source registration and the ability to act as hot backup routers for each other. Multicast Source Discovery Protocol (MSDP) is the key protocol that makes Anycast RP possible.

The main purpose of an Anycast RP implementation is that the downstream multicast routers will "see" just one address for an RP.

Reference:

[http://www.cisco.com/en/US/tech/ CK8 28/technologies_white_paper09186a00800d6b60.shtml#57583](http://www.cisco.com/en/US/tech/CK8_28/technologies_white_paper09186a00800d6b60.shtml#57583)

QUESTION 331

The Certkiller network is using multicasting for corporate video training sessions. All routers in the Certkiller network are enabled for IP multicast. How are these video streaming multicast packets forwarded by these routers? (Choose all that apply)

- A. When a multicast packet arrives at a router, the router performs a Reverse Path forwarding (RPF) check on the packet. If the RPF check succeeds, the packet is forwarded, otherwise, it is dropped.
- B. When traffic is flowing down the source tree the router looks up the source address in the unicast routing table to determine if the packet has arrived on the interface that is on the reverse path back to the source, if the packet has arrived on the interface leading back to source, the PRF check succeeds and the packets is forward. Otherwise, it is dropped.
- C. When traffic is flowing down the source tree the router looks up the source address in the multicast routing table to determine if the packet has arrived on the interface that is on the reverse path back to the source. If the packet has arrived on the interface leading back to the source, the PRF check successfully the packets is forwarded. Otherwise, it is dropped.
- D. When traffic is flowing down the source tree the router looks up the source address in the multicast routing table to determine if the packet has arrived on the interface that is on the reverse path back to the source and forward path to the receiver. If the reverse path and forward path is found successfully the packet is forwarded. Otherwise, it is dropped.
- E. When a multicast packet arrives at a router, the router does not have to perform an RPF check on the packet. The router looks up the source address in the unicast routing table to determine if the destination path is present. If this succeeds the packet is forwarded. Otherwise, it is dropped.

Answer: A, B

Explanation:

Multicast Forwarding

In unicast routing, traffic is routed through the network along a single path from the source to the destination host. A unicast router does not consider the source address; it considers only the destination address and how to forward the traffic toward that destination. The router scans through its routing table for the destination address and then forwards a single copy of the unicast packet out the correct interface in the direction of the destination.

In multicast forwarding, the source is sending traffic to an arbitrary group of hosts that are represented by a multicast group address. The multicast router must determine which direction is the upstream direction (toward the source) and which one is the downstream direction (or directions). If there are multiple downstream paths, the router replicates the

packet and forwards it down the appropriate downstream paths (best unicast route metric)-which is not necessarily all paths. Forwarding multicast traffic away from the source, rather than to the receiver, is called Reverse Path Forwarding (RPF). RPF is described in the following section.

Reverse Path Forwarding (RPF)

PIM uses the unicast routing information to create a distribution tree along the reverse path from the receivers towards the source. The multicast routers then forward packets along the distribution tree from the source to the receivers. RPF is a key concept in multicast forwarding. It enables routers to correctly forward multicast traffic down the distribution tree. RPF makes use of the existing unicast routing table to determine the upstream and downstream neighbors. A router will forward a multicast packet only if it is received on the upstream interface. This RPF check helps to guarantee that the distribution tree will be loop-free.

RPF Check

When a multicast packet arrives at a router, the router performs an RPF check on the packet. If the RPF check succeeds, the packet is forwarded. Otherwise, it is dropped. For traffic flowing down a source tree, the RPF check procedure works as follows:

1. The router looks up the source address in the unicast routing table to determine if the packet has arrived on the interface that is on the reverse path back to the source.
2. If the packet has arrived on the interface leading back to the source, the RPF check succeeds and the packet is forwarded.
3. If the RPF check in Step 2 fails, the packet is dropped.

Incorrect Answers:

C, D. The RPF lookup is done on the unicast routing table, not the multicast routing table.

E. RPF checks must be done in order to maintain a loop free multicast topology.

QUESTION 332

While troubleshooting an IP multicast issue, you issue the "show ip mroute" command:

```
Router#show ip mroute 236.2.3.23
```

IP Multicast Routing table

Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned

R - RP-bit set, F - Register flag, T - SPT-bit set, J - JOIN SPT

X - Proxy Join Timer Running

Timers: uptime/Expires

Interface state: Interface, next-hop or VCD, State/Mode

(*, 236.2.3.23), 00:09:49/00:04:23 RP 10.1.24.1, flags: SC

Incoming interface: Serial1.708, RPF nbr 10.1.20.2

Outgoing interface list:

Ethernet0, Forward/Sparse, 00:09:50/00:04:12

You are trying to trace this multicast address back to the source of this multicast shared tree. Based on the information above, what is the IP address of the upstream neighbor?

- A. 10.1.24.1
- B. 10.1.24.2
- C. 10.1.20.2
- D. 10.1.20.3
- E. 236.2.3.23

Answer: C

Explanation:

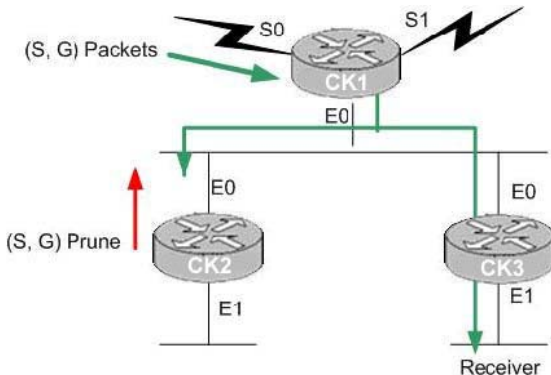
The upstream neighbor is the IP address associated with the Reverse Path Forwarding Neighbor (RPF nbr), which is 10.1.20.2 in this case.

Incorrect Answers:

- A. 10.1.24.1 is the IP address of the Rendezvous Point in this example, not the upstream neighbor.
- E. 236.2.3.23 is the IP address of the IP multicast session.

QUESTION 333

Part of the Certkiller IP multicast network is shown below:



Router CK2 sends a (S, G) Prune message to the LAN segment. Will this cause router CK1 to stop the multicast flow to router CK3 ?

- A. No. After seeing the Prune message from router CK2 , Router CK3 will send a Join message to router CK1 to override the Prune.
- B. No. After seeing the Prune message from router CK2 , Router CK3 will send a Join message to router CK2 to override the Prune.
- C. No. After seeing the Prune message from router CK2 , Router CK3 will send a Graft message to router CK2 to override the Prune from router CK2 .
- D. Yes. Router CK3 will need to send a new Join message to re-join the multicast session.
- E. It depends on whether the routers are IGMP version 1 or IGMP version 2.

Answer: A

Explanation:

After a prune, the router waits for joins, if none arrive, then the router drops the Group. In this case, router CK1 will hear the Join message from CK3 to prevent the flow of multicast traffic from being cut off to CK3 .

Incorrect Answers:

B. Router CK2 will send a Join message to the upstream neighbor, which is CK1 in this case, not CK2 .

C. No graft messages will be sent in this case.

E. IGMP versions are irrelevant.

QUESTION 334

What is the primary purpose for the RPF check in IP multicast networks?

- A. To establish reverse flow path of multicast traffic from the receiver to the source.
- B. To prevent multicast traffic looping through the network.
- C. To determine interfaces inclusion in the outgoing interface list.
- D. To prevent the movement of unauthorized multicast traffic.

Answer: B

Explanation:

Reverse Path Forwarding (RPF) provides loop avoidance. It is an algorithm used to forward multicast packets. The RPF rules are: If a router receives a datagram on an interface that it uses to send unicast packets to the source of that packet, then the packet has arrived on the RPF interface. If the packet arrives on the RPF interface, a router forwards the packet out the interfaces that are present in the outgoing interface list of a multicast routing table entry. If the packet does not arrive on the RPF interface, the packet is silently discarded.

QUESTION 335

Which Multicast Protocols use Reverse Path Forwarding (RPF) information when sending multicast traffic streams to the receivers within the Certkiller network? (Select two)

- A. DVMRP
- B. PIM Sparse Mode
- C. PIM Dense Mode
- D. Multicast OSPF
- E. PIM Sparse-Dense Mode

Answer: A, C

Explanation:

DVMRP uses a technique known as Reverse Path Forwarding. When a router receives a packet, it floods the packet out of all paths except the one that leads back to the packet's source. Doing so allows a data stream to reach all LANs (possibly multiple times). If a router is attached to a set of LANs that do not want to receive a particular multicast

group, the router can send a "prune" message back up the distribution tree to stop subsequent packets from traveling where there are no members.

Dense-mode PIM uses Reverse Path Forwarding and looks a lot like DVMRP. The most significant difference between DVMRP and dense-mode PIM is that PIM works with whatever unicast protocol is being used; PIM does not require any particular unicast protocol.

Incorrect Answers:

B. Sparse-mode PIM is optimized for environments where there are many multipoint data streams. Each data stream goes to a relatively small number of the LANs in the internetwork. For these types of groups, Reverse Path Forwarding techniques waste bandwidth. Sparse-mode PIM works by defining a Rendezvous Point. When a sender wants to send data, it first sends to the Rendezvous Point.

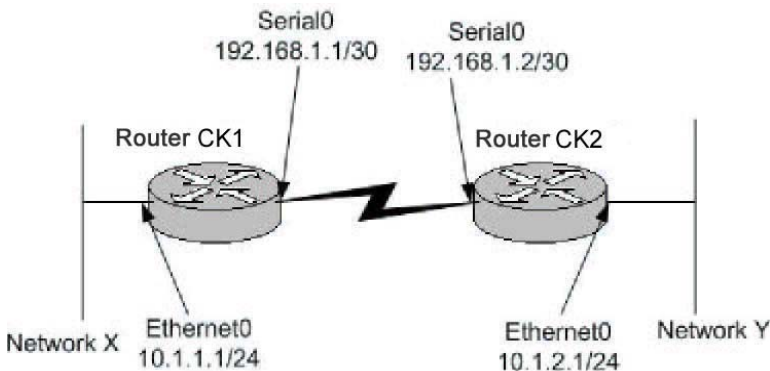
D. Multicast OSPF (MOSPF) was defined as an extension to the OSPF unicast routing protocol. OSPF works by having each router in a network understand all of the available links in the network. Each OSPF router calculates routes from itself to all possible destinations.

MOSPF works by including multicast information in OSPF link state advertisements. An MOSPF router learns which multicast groups are active on which LANs.

MOSPF builds a distribution tree for each source/group pair and computes a tree for active sources sending to the group. The tree state is cached, and trees must be recomputed when a link state change occurs or when the cache times out.

QUESTION 336

The Certkiller network consists of network X and Y that are connected via Router CK1 and Router CK2. The Certkiller network is shown in the following exhibit:



You wish to set up an IPSec VPN between routers CK1 and CK2. Now, which of the following crypto access-lists must be configured on Router CK1 in order to send LAN to LAN traffic across the encrypted VPN tunnel?

- A. access-list 101 permit ip host 192.168.1.1 host 192.168.1.2
- B. access-list 101 permit ip 10.1.1.0.0.0.0.255 host 192.168.1.2
- C. access-list 101 permit ip 10.1.1.0.0.0.0.255 10.1.2.0.0.0.0.255
- D. access-list 101 permit ip 10.1.1.0.0.0.0.255 10.1.2.0.0.0.0.255
- E. access-list 10 permit ip 10.1.1.0.0.0.0.255 10.1.2.0.0.0.0.255

Answer: C

Explanation:

The format of the command for configuring IPsec is shown below:

access-list 101 permit "Source Network Addresses on X" "Destination Network Subnets on Y"

Incorrect Answers:

- A. You define the traffic that is to be sent over the encrypted tunnel, which is all traffic from subnet X to subnet Y, not the serial interfaces.
- B. This would only be useful for traffic going from subnet X to the serial interface of CK2, not for LAN to LAN traffic.
- D. You only need to specify the traffic from X to Y on router CK1, as this is the traffic that will be encrypted. The second line of this access list would need to be applied to router CK2 only.
- E. Access list 100 or higher must be used, as this is an extended access list.

QUESTION 337

You try to perform a traceroute to an Internet destination from your PC, but the Traceroute hangs when it reaches the router. Currently, there is an inbound accesslist applied to the serial interface on the Internet router with a single line: "accesslist 101 permit tcp any any".

What access-list entry may you need to be added to the access-list in order to get traceroute to work?

- A. access-list 101 permit tcp any any
- B. access-list 101 permit icmp any any time-exceeded
access-list 101 permit icmp any any port-unreachable
- C. access-list 101 permit icmp any any time-exceeded
access-list 101 permit icmp any any echo-reply
- D. access-list 101 permit icmp any any echo
access-list 101 permit icmp any any net-unreachable
- E. access-list 101 permit udp any any
access-list 101 permit icmp any any protocol-unreachable

Answer: B

Explanation:

Port-unreachable and time-exceeded are the ICMP messages that Cisco traceroute uses, so these ports must be permitted to allow the traceroute to go through.

Incorrect Answers:

A, C, D, E. None of these options give us both the time-exceeded and port-unreachable ICMP ports that need to be opened in the access list to allow traceroute through.

QUESTION 338

You are writing an access list on a router to prevent users on the Ethernet LAN

connected to Ethernet interface 0 from accessing a TFTP server (10.1.1.5) located on the LAN connected to Ethernet interface 1. Which of the following would be the correct configuration change if applying the ACL inbound on the Ethernet 0 interface?

- A. access-list 1 deny tcp 0.0.0.0 255.255.255.255 10.1.1.5. 0.0.0.0 eq 69
- B. access-list 100 deny tcp 0.0.0.0 255.255.255.255 10.1.1.5. 0.0.0.0 eq 69
- C. access-list 100 deny tcp 0.0.0.0 255.255.255.255 10.1.1.5. 0.0.0.0 eq 68
- D. access-list 100 deny tcp 10.1.1.5 0.0.0.0 0.0.0.0 255.255.255.255 eq 69
- E. access-list 100 deny tcp 0.0.0.0 255.255.255.255 10.1.1.5. 0.0.0.0 eq port 68
- F. None of the above

Answer: F

Explanation:

TFTP uses UDP port 69, so choice F would be the correct access list entry. An extended access list is needed when filtering based on source and destination address, as well as layer 4 port information. However, all of the choices listed are filtering based on TCP ports, and since TFTP uses UDP none are correct.

Incorrect Answers:

- A. This is an invalid command, since using source and destination information along with port numbers requires an extended access list.
- B. This would be the correct choice if UDP was specified as the transport layer protocol instead of TCP.
- C, E. In addition to incorrectly specifying TCP instead of UDP, the port number of 68 is also incorrect.
- D. The order of the IP address arrangement is incorrect. This access list will block all TCP port 69 traffic sourced from the TFTP server, not destined to it. This choice is also incorrectly using TCP instead of UDP.

QUESTION 339

You wish to allow only telnet traffic to a server with an IP address 10.1.1.100. You add the following access list on the router:

```
access-list 101 permit tcp any host 10.1.1.100 eq telnet
access-list 101 deny ip any any
```

You then apply this access list to the inbound direction of the serial interface.

Which types of packets will be permitted through the router after this change?

(Choose all that apply)

- A. A non-fragment packet en route to the server on port 21.
- B. A non-initial fragment packet en route to the server on port 23.
- C. A non-initial fragment packet passing through to another host that's not 10.1.1.100.
- D. A non-initial fragment packet going to the server on port 21.
- E. An initial-fragment or non-fragment packet en route to the server on port 23.

Answer: B, D, E

Explanation:

B, E: Telnet (port 23) is permitted by ACL.

D: A non initial fragment destined to the server will indeed be permitted. The reason for this is that the first line of ACL has some L3 and some L4 information which needs to be matched for a packet to be permitted.

Since a non initial frame matches the L3 information it will pass the layer 3 check.

Moreover, since it is a non initial frame it will contain no L4 information in it. Hence the packet will be permitted.

Incorrect Answers:

A, C. For non-initial fragments, only telnet packets going to the 10.1.1.100 address will be allowed.

QUESTION 340

The following access list is configured on router CK1 :

```
access-list 100 deny udp 0.0.0.0 255.255.255.255 10.1.1.5 0.0.0.0 eq 69
```

What does the access-list accomplish?

Note: Assume that all other traffic is permitted with a permit all statement at the end of the access list.

A. It blocks all incoming traffic arriving on E0 from accessing any FTP server.

B. It blocks all incoming traffic, except traffic addresses to 10.1.1.5, from accessing any FTP servers.

C. It blocks all incoming traffic arriving on E0 from accessing the FTP server with an address of 10.1.1.5.

D. It blocks all incoming UDP traffic.

E. This access list is trying to block traffic from accessing a TFTP server. However, this is only half of what is needed to accomplish that. You would also need the following:

```
access-list deny tcp 0.0.0.0 255.255.255.255 10.1.1.5 0.0.0.0 eq 69
```

Answer: E

Explanation:

The access list shown above is designed to block UDP port 69 traffic from all sources to the destination device with the IP address of 10.1.1.5. Port 69 is used for TFTP. Both TCP and UDP ports are used with the TFTP application, so in order to block all TFTP traffic another access list block TCP port 69 should also be applied.

Incorrect Answers:

A, B: TFTP traffic is being blocked, not FTP. In addition, this traffic is being blocked only for traffic destined to a single server, not all traffic.

C. TFTP uses port 69, not FTP. FTP uses ports 20 and 21. Since TFTP uses both TCP and UDP, both ports will need to be filtered.

D. Only UDP port 69 traffic destined to a single server is being filtered, not all UDP

traffic.

Reference: <http://www.ibiblio.org/security/articles/ports.html>

QUESTION 341

Private VLANs are set up in a Cisco switch for 3 ports as shown below:

tamer (enable) show pvlan

tamer (enable) show pvlan

Primary	Secondary	Secondary-Type	Port
---------	-----------	----------------	------

500	501	community	5/37
500	502	isolated	5/38-39

tamer (enable) show pvlan mapping

Port	Primary	Secondary
------	---------	-----------

15/1	500	501-502
------	-----	---------

interface vlan 500

ip address 10.10.10.2 255.255.255.0

ip proxy-arp

A PC called TKHost is plugged in to port 5/38, using ip address 10.10.10.137/24.

Based on the information above, TKHost has which of the following?

- A. Layer 3 connectivity with Port 5/37 and port 5/39.
- B. Layer 2 connectivity with Port 5/39 but not with port 5/37.
- C. Layer 3 connectivity with Port 5/39 but not with port 5/37.
- D. Layer 2 connectivity with Port 5/37 and port 5/39.
- E. None of the above.

Answer: A

Private VLAN ports can be one of the following:

- Promiscuous- A promiscuous port can communicate with all interfaces, including the isolated and community ports within a PVLAN.
- Isolated- An isolated port has complete Layer 2 separation from the other ports within the same PVLAN, but not from the promiscuous ports. PVLANS block all traffic to isolated ports except traffic from promiscuous ports. Traffic from isolated port is forwarded only to promiscuous ports.
- Community- Community ports communicate among themselves and with their promiscuous ports. These interfaces are separated at Layer 2 from all other interfaces in other communities or isolated ports within their PVLAN.

In this case TKHost is in an isolated VLAN, so it will have complete layer 2 separation from all other ports. However, there is nothing preventing routing from taking place, and with inter-vlan routing TKHost will have layer 3 connectivity to the other ports.

QUESTION 342

The Certkiller network administrator wants to authenticate LAN users attached to ports on the existing Catalyst 6509 switch. In order to do this, the following is configured:

```
aaa new-model
username myname password abc123
aaa authentication ppp access-dotx local
aaa authentication login access1 local
aaa authentication dot1x default radius
dot1x system-auth-control
tacacs-server host 192.168.1.15 key qvert123
radius-server host 192.168.2.27 key poiuy098
!
interface fastethernet 5/1
dot1x port control auto
```

What is the effect of the configuration on users attempting to access FastEthernet 5/1?

- A. They will be authenticated via ppp using the local database.
- B. They will be authenticated via ppp using the server at IP address 192.168.1.15.
- C. They will be authenticated via ppp using the server at IP address 192.168.2.27
- D. They will be authenticated via 802.1x using the local database.
- E. They will be authenticated via 802.1x using the server at IP address 192.168.1.150.
- F. They will be authenticated via 802.1x using the server at IP address 192.168.2.27.

Answer: F

Explanation:

When you enable 802.1X port-based authentication, note the following syntax information:

- To create a default list that is used when a named list is not specified in the authentication command, use the default keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces.
- Enter at least one of these keywords:
 - group radius-Use the list of all RADIUS servers for authentication.
 - none-Use no authentication. The client is automatically authenticated by the switch without using the information supplied by the client.

This example shows how to enable AAA and 802.1X on Fast Ethernet port 5/1:

```
Router# configure terminal
CK1 (config)# aaa new-model
CK1 (config)# aaa authentication dot1x default group radius
CK1 (config)# dot1x system-auth-control
CK1 (config)# interface fastethernet 5/1
CK1 (config-if)# dot1x port-control auto
CK1 (config-if)# end
```

In this example, the default 802.1x authentication method is configured to be RADIUS, and the RADIUS server is located at IP address 192.168.2.27.

QUESTION 343

For security reasons, you wish to maintain a degree of logical separation between your servers and the rest of the LAN. The servers should be able to see broadcasts and multicasts only from each other and the default gateway. They should not see this type of traffic from other LAN devices. What kind of ports should be configured for these servers on the Catalyst switch?

- A. Span Ports.
- B. Private Ports.
- C. Community Ports.
- D. Isolated Ports.
- E. Promiscuous Ports.
- F. Access Ports.

Answer: C

Explanation:

Private VLANs provide Layer-2 isolation between ports within the same private VLAN on the Catalyst 6000 family switches. Ports belonging to a private VLAN are associated with a common set of supporting VLANs that are used to create the private VLAN structure.

There are three types of private VLAN ports: promiscuous, isolated, and community. Community ports communicate among themselves and with their promiscuous ports. These ports are isolated at Layer 2 from all other ports in other communities or isolated ports within their private VLAN. They communicate directly only with each other and their default gateway.

Incorrect Answers:

- A. SPAN ports are used for network analyzers to capture data packets. They do not provide any level of security between users.
- B. This question is an example of a type of private VLAN. However, there is no notion of a private port.
- D. A promiscuous port communicates with all other private VLAN ports and is the port used to communicate with devices such as routers, LocalDirector, backup servers, and administrative workstations.
- E. An isolated port has complete Layer 2 separation from all other ports within the same private VLAN with the exception of the promiscuous port.
- F. Access ports do not exist.

QUESTION 344

Based on the VLAN Access Control List (VACL) configuration below, how many total mask entries are required in the Ternary Content Addressable table?

```
set security acl ip Control_Access permit host 100.1.1.100
set security acl ip Control_Access deny 100.14.11.0 255.255.255.0
set security acl ip Control_Access permit host 172.16.84.99
set security acl ip Control_Access deny 177.163.4.0 255.255.255.128
```

```
set security acl ip Control_Access permit host 72.16.82.3
set security acl ip Control_Access deny host 175.17.1.4
set security acl ip Control_Access permit host 191.169.99.150
set security acl ip Control_Access deny host 191.169.230.1
```

- A. 2
- B. 3
- C. 4
- D. 6
- E. 8

Answer: B

Explanation:

There will be 3: One to cover the 6 separate host (255.255.255.255) masks, one for the 255.255.255.128 mask, and the third for the 255.255.255.0 mask.

Ternary CAM (TCAM) is a hardware piece of memory designed for rapid table lookups by the ACL engine on the PFC and PFC2. The ACL engine performs ACL lookups based on packets passing through the switch's hardware. The result of the ACL engine lookup into the TCAM determines how the switch handles a packet. For example, the packet might be permitted or denied. The TCAM has a limited number of entries that are populated with mask values and pattern values.

Incorrect Answers:

A, C. In the example above there are 3 different subnet masks, not 2 or 4.

D. Although there are 6 different entries with host masks (255.255.255.255), we need to account for the other two mask entries.

E. Although there are a total of 8 VLAN access control entries in this example, there are only a total of 6 of them share a single mask entry and will be counted as only one in the TCAM.

References:

For a detailed discussion on TCAM refer the link below.

http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a00800c9470.shtml

QUESTION 345

With regard to the use of VLAN Access Control Lists (VACL) on a Catalyst 6500 series switch, which of the following are true statements? (Choose all that apply.)

- A. VACLs can be used to forward, drop, and redirect traffic based on Layer 2 and Layer 3 information.
- B. VACLs cannot be used when using QoS on the switch.
- C. VACLs can be used together with router interface access lists.
- D. VACLs can be used for traffic that is being Layer 3 switched.
- E. VACLs cause extra latency for traffic passing through the switch.

Answer: A, C, D

Explanation:

VACLs are similar to Router/IOS ACLs in terms of their definition, but they are used by Catalyst 6000 family switches to access control all packets it switches, including packets bridged within a VLAN. It can be used to act on layer 2 and 3 information, and can be used in conjunction with RACL's.

Incorrect Answers:

B. VACLs can be used when using QoS on the switch. VACLs cause extra latency for traffic passing through the switch. For a detailed discussion on VACLs please go through the link below.

E. VACLs can be configured on a Catalyst 6500 at L2 without the need for an additional router. They are enforced at wire speed so there is no performance penalty in configuring VACLs on a Catalyst 6500. Since the lookup of VACLs is performed in hardware, regardless of the size of the access list, the forwarding rate remains unchanged.

Reference:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_6_3/config_gd/acc_list.htm#1052397

QUESTION 346

A new Catalyst 6500 running Cat OS was recently installed in the Certkiller network. In order to increase the security of your LAN, you configure this Catalyst switch using port security. What statement is true about port security?

- A. Port security can be configured on a trunk port.
- B. Port security can be configured on a SPAN destination port.
- C. If a security violation occurs, the Link LED for that port turns orange, and a linkdown trap is sent to the Simple Network Management Protocol (SNMP) manager.
- D. Port security can be configured on a SPAN source port.
- E. Static CAM entries can be configured on a port configured with port security.
- F. Ports that were disabled due to security violations will be automatically reenabled when the host with the valid MAC address is re-connected.

Answer: C

Explanation:

Port Security Configuration Guidelines

When a secure port receives a packet, the source MAC address of the packet is compared to the list of secure source addresses that were manually configured or autoconfigured (learned) on the port. If a MAC address of a device attached to the port differs from the list of secure addresses, the port either shuts down permanently (default mode), shuts down for the time you have specified, or drops incoming packets from the insecure host. The port's behavior depends on how you configure it to respond to a security violation. If a security violation occurs, the Link LED for that port turns orange, and a link-down trap is sent to the Simple Network Management Protocol (SNMP) manager. An SNMP trap is not sent if you configure the port for restrictive violation mode. A trap is sent only if you configure the port to shut down during a security violation.

Reference:http://www.cisco.com/en/US/products/hw/switches/ps700/products_configuration_guide_chapter09186a008007fa13.html#xtocid256011

Incorrect Answers:

A, B, D, E. These incorrect answers can be summarized in the following statements:

- You cannot configure port security on the trunk port of a 6500 with Cat OS.
- You cannot enable port security on a SPAN destination port of the 6500 with Cat OS.
- You cannot configure dynamic, static, or permanent CAM entries on a secure port.
- When you enable port security on a port, any static or dynamic CAM entries associated with the port are cleared; any currently configured permanent CAM entries are treated as secure.

F. When a port becomes disabled due to a security violation, the switch port can only be enabled again after manual intervention.

Reference:http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a008007fb16.html

QUESTION 347

After properly configuring multiple VLANs, a The Certkiller network has decided to increase the security of its VLAN environment. Which of the following can be done on a switched network to enhance security measures? (Choose all that apply).

- A. If a port is connected to a "Foreign" device, make sure to disable CDP, DTP, PagP, UDLD, and any other unnecessary protocol, and to enable Uplinkfst/BPDU guard on it.
- B. Enable the rootguard feature to prevent a directly or indirectly connected STPcapable device to affect the location of the root bridge.
- C. Configure the VTP domains appropriately or turn off VTP altogether if you want to limit or prevent possible undesirable protocol interactions with regard to network-wide VLAN configuration.
- D. Disable all unused ports and place them in an unused VLAN to avoid unauthorized access.
- E. Set the native VLAN ID to match the port VLAN ID (PVID) of any 802.1Q trunks to prevent spoofing from one VLAN to another.

Answer: B, C, D

Explanation:

The root guard feature is designed to provide a way to enforce the root bridge placement in the network, and to prevent unauthorized devices from becoming the root.

Turning off VTP if it is not used is generally a good idea, as a new switch with a higher ID value that is inserted into the VTP domain can be used to modify and delete all of the VLANs in an existing network.

It is also a best practice to disable and isolate all unused ports, as this will prevent unauthorized users from entering the LAN, and plugging into the network via an unused port.

Incorrect Answers:

A. UDLD is a useful feature that provides no security risks. It is recommended to have this feature enabled. BPDU guard and root guard are similar, but their impact is different. BPDU guard disables the port upon BPDU reception if portfast is enabled on the port. This effectively denies devices behind such ports to participate in STP.

E. If a user's native VLAN ID is the same as the port VLAN ID (PVID) of the 802.1Q trunk, then the user can send frames from his VLAN and have them "hop" to other VLANs. This weakness is part of the 802.1Q specification and does not apply to Cisco ISL trunking ports.

The workaround for this threat is to ensure that every 802.1Q trunking port has a PVID, or native VLAN ID, that is unique throughout the campus network.

QUESTION 348

Passwords for Enterprise guests should normally be:

- A. Easy to remember
- B. Time limited to the guest visit
- C. Be the same as the username
- D. Be at least 10 characters
- E. Contain uppercase letters

Answer: B

Explanation:

When guest access is required for visitors to the enterprise, the most important security measures that should be taken is to ensure that the guest user access is restricted to only the network resources that are needed, and for the passwords to only be active for the duration of the visit. This will prevent future unauthorized access into the network using these passwords.

Incorrect Answers:

A. Generally, passwords should be somewhat easy to remember for the users, while remaining secure. It is more important to use passwords that are not easily guessed than to provide for an easy to remember one.

C. This should never be done, since it is so easily guessed.

D. Although having enough characters to provide for a secure password is essential, secure passwords can be created with the use of fewer than 10 characters. For regular users, enforcing a rule of long passwords may be preferred, it is generally not necessary for guest access.

E. Although passwords should indeed contain a mix of lower and upper case letters, as well as numerical and special characters, this is not necessarily a requirement for guest users.

QUESTION 349

When segmenting guest traffic across the enterprise wireless network you should

take which of the following approaches?

- A. Always give guest traffic higher priority
- B. Always give guest traffic lower priority
- C. Separate guest traffic as close to the edge as possible
- D. Use a firewall
- E. Use Access Lists
- F. None of the above

Answer: C

Explanation:

You should consider the following implementation criteria before deploying wireless VLANs:

- Use policy groups (a set of filters) to map wired policies to the wireless side.
- Use IEEE 802.1x to control user access to VLANs by using either RADIUS-based VLAN assignment or RADIUS-based SSID access control.
- Use separate VLANs to implement different classes of service.
- Adhere to any other criteria specific to your organization's network infrastructure.

Based on these criteria, you could choose to deploy wireless VLANs using the following strategies:

- Segmentation by user groups-you can segment your WLAN user community and enforce a different security policy for each user group. For example, you could create three wired and wireless VLANs in an enterprise environment for full- and part-time employees, as well as providing guest access.
- Segmentation by device types-You can segment your WLAN to enable different devices with different security levels to access the network. For example, you have handheld devices that support only 40- or 128-bit static WEP coexisting with other devices using IEEE 802.1x with dynamic WEP in the same ESS. Each of these devices would be isolated into separate VLANs.

For segmenting guest users from the rest of the network, the guest VLAN traffic should be segmented at the network edge, before the traffic reaches the core of the network. This is generally done at the VLAN level, before guest traffic reaches a router access list or firewall.

QUESTION 350

What are the differences between TACACS+ and RADIUS? (Choose all that apply)

- A. TACACS+ uses UDP while RADIUS uses TCP for transport.
- B. RADIUS and TACACS+ encrypts the entire body of the packet.
- C. RADIUS is an IETF standard, while TACACS+ is not.
- D. TACACS+ sends a separate request for authorization, while RADIUS uses the same request for authentication and authorization.
- E. RADIUS offers multi-protocol support while TACACS+ does not.

Answer: C, D

Explanation:

- RADIUS uses UDP while TACACS+ uses TCP.
- RADIUS encrypts only the password in the access-request packet, from the client to the server. The remainder of the packet is unencrypted while TACACS+ encrypts the entire body of the packet but leaves a standard TACACS+ header.
- RADIUS combines authentication and authorization while TACACS+ uses the AAA architecture, which separates authentication, authorization, and accounting.
- TACACS+ offers multiprotocol support while RADIUS does not support AppleTalk Remote Access (ARA) protocol, NetBIOS Frame Protocol Control protocol, Novell Asynchronous Services Interface (NASI) and X.25 PAD connection.
- RADIUS does not allow users to control which commands can be executed on a router and which cannot. Therefore, RADIUS is not as useful for router management or as flexible for terminal services. TACACS+ on the other hand does allow users to control the authorization of router commands on a per-user or per-group basis.

Reference:

TACACS+ and RADIUS Comparison, <http://www.cisco.com/warp/public/480/10.html>

QUESTION 351

You want to prevent all telnet access to your Cisco router. In doing so, you type in the following:

```
line vty 0 4
no login
password cisco
```

Will this prevent all telnet access to the router as desired?

- A. Yes. The "no login" command disables all telnet access, even though the password is cisco.
- B. Yes. The VTY password is needed but not set, so all access will be denied.
- C. No. The VTY password is cisco.
- D. No. No password is needed for VTY access.
- E. No. The password is login.

Answer: D

Explanation:

"No Login" will not prompt users for any initial login, allowing them to access the router without a password.

QUESTION 352

A new TACACS+ server is configured to provide authentication to a NAS for remote access users. A user tries to connect to the network and fails. The NAS reports a FAIL message. What could be the problem? (Choose all that apply).

- A. The TACACS+ service is not running on the server.
- B. The password for this user is incorrect.
- C. The username does not exist in the TACACS+ user database.
- D. The NAS server lost its route to the TACACS+ server.
- E. The TACACS+ server is down.

Answer: B, C

Explanation:

A FAIL condition is a result of incorrect username/password information. It means that an authentication request was successfully received, but that it had failed.

A FAIL response is significantly different from an ERROR. A FAIL means that the user has not met the criteria contained in the applicable authentication database to be successfully authenticated. Authentication ends with a FAIL response. An ERROR means that the security server has not responded to an authentication query. Because of this, no authentication has been attempted. Only when an ERROR is detected will AAA select the next authentication method defined in the authentication method list.

Reference:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgr/secur_c/scprt1/scdaaa.htm

Incorrect Answers:

A, D, E. These would have resulted in an ERROR condition instead of a FAIL condition. With an error, the NAS would query the next authentication method.

QUESTION 353

While setting up remote access for your network, you type in the "aaa new-model" configuration line in your Cisco router. Which authentication methods have you disabled as a result of this change? (Choose all that apply.)

- A. RADIUS
- B. RADIUS+
- C. Extended TACACS (XTACACS)
- D. TACACS
- E. TACACS+
- F. Kerberos

Answer: C, D

Explanation:

When you enable AAA, you can no longer access the commands to configure the older deprecated protocols, TACACS or Extended TACACS. If you decided to use TACACS or Extended TACACS in your security solution, do not enable AAA.

QUESTION 354

With regard to IPSec, which of the following are true?

- A. IPSec supports Multicast.
- B. IPSec does not support Multicast.
- C. IPSec supports Multicast in IOS 12.x or later.
- D. IPSec supports Multicast in IOS 10.x or earlier.
- E. IPSec supports Multicast only in combination with GRE tunnels.

Answer: B

Explanation:

IPSec does not support multicast, as secure IPSec tunnels are always between unicast hosts.

Incorrect Answers:

C, D, E. Cisco does not support IPSec protection for multicast traffic on any IOS release.

QUESTION 355

You are setting up a secure connection to another company's device. You are not certain that they are using Cisco so you want your router to manually exchange the RSA public keys between each other. How should you configure your router?

- A. Use IPSec with RSA signatures
- B. Use IPSec with RSA encrypted nonces
- C. Use IPSec with manual keying
- D. Use Cisco Encryption Technology
- E. Use IPSec using preshared keys
- F. Use IPSec using RSA authentication

Answer: C

Explanation:

Manual keying is usually only necessary when configuring a Cisco device to encrypt traffic to another vendor's device, which does not support IKE. If IKE is configurable on both devices, it is preferable to using manual keying.

Incorrect Answers:

A, B, F. In this question we want the keys to be exchanged manually, so this not the best choice.

E. Preshared keys are static keys that do not change, but they can not be keyed manually.

Reference:

Cisco - "Configuring IPSec Manual Keying between Routers"

QUESTION 356

Which of the following are security services provided by IPSec?

- A. Data integrity
- B. Data origin authentication
- C. Data confidentiality
- D. Protection for multicast/broadcast traffic

E. Anti-replay

Answer: A, B, C, and E

Explanation:

Data integrity, data origin authentication, data confidentiality, and protection from replay are all security features and functions of IPSec

Incorrect Answers:

D. IPSec provides no security against multicast and broadcast traffic. In fact, IPSec does not support multicast traffic.

QUESTION 357

You wish to change the IKE policies of your IPSec configuration in your site to site router VPN. Which of the following are valid ISAKMP policy parameters that can be changed in the configurations?

- A. Security Association's lifetime
- B. Encryption algorithm
- C. Hash algorithm
- D. Authentication method
- E. Diffie-Hellman group identifier
- F. All of the above
- G. None of the above

Answer: F

There are five parameters to define in each IKE policy:

Parameter	Accepted Values	Keyword	Default Value
encryption algorithm	56-bit DES-CBC	des	56-bit DES-CBC
hash algorithm	SHA-1 (HMAC variant) MD5 (HMAC variant)	sha md5	SHA-1
authentication method	RSA signatures RSA encrypted nonces pre-shared keys	rsa-sig rsa-encr pre-share	RSA signatures
Diffie-Hellman	768-bit Diffie-Hellman or 1024-bit Diffie-Hellman	1 2	768-bit Diffie-Hellman

group identifier			
security association's lifetime			

QUESTION 358

Unauthorized access to Cisco devices can be prevented through different privilege level settings. How many of these privilege levels exist?

- A. 5
- B. 16
- C. 4
- D. 0
- E. 15

Answer: B

Explanation:

There are 16 privilege-levels (0 to 15, inclusive).

Incorrect Answers:

- A. This is the default number of vty sessions that can be placed on a router for remote telnet access (vty levels 0-4, inclusive).
- E. The highest level is level 15, but we must also count the lowest level (level 0) for a total of 16.

QUESTION 359

Router CK1 has been configured for authentication as shown in the following display:

```
enable secret 483924
!
aaa new-model
username myname password abc123
aaa authentication login default enable
aaa authentication login access1 local
aaa authentication login access2 radius tacacs+
aaa authentication login access3 tacacs+ local
tacacs-server host 192.168.1.15 key qwert123
radius-server host 192.168.2.27 key poiuy098
!
Line console 0
login authentication access3
!
line vty 0 4
password dfgh456
```

login

What method is being used to secure the console port of this router?

- A. Authentication is being done using the local database.
- B. Authentication is being done using the login password dfgh456.
- C. Authentication is being done using the enable password as a default
- D. Authentication is being done using the server at IP address 192.168.1.15. If a connection to that server fails, the local database will be used.
- E. Authentication is being done using the server at IP address 192.168.2.27

Answer: D

Explanation:

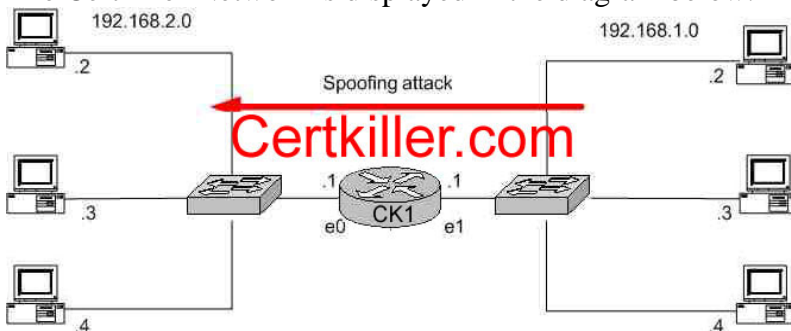
The router is using the keyword access3 for authentication for the console port. Access3 points to two different methods for authentication; the first is TACACS+ which is located at 192.168.1.15. If the authentication connection to the server fails, then the local database will be used as a backup.

Incorrect Answers:

- A. Based on the configuration file above, TACAS+ is the primary authentication method and the local database is to only be used as a backup method.
- B. This is the password that is to be used for Telnet access, not the console password.
- C. The enable password is not used, since the login authentication information is taken from the "access3" keyword.
- E. This is the IP address of the RADIUS server, not the TACACS+ server.

QUESTION 360

The Certkiller Network is displayed in the diagram below:



You want to block all IP spoofing attacks that originate on the 192.168.1.0 network using a spoofed address outside the 192.168.1.0 range from being sent into the 192.168.2.0 network. However, all other traffic must be permitted. No access lists currently exist on the router. Which of the following configurations would accomplish this task when applied to E1 on CK1 as an input filter?

- A. access-list 1 permit 192.168.1.0 0.0.0.255
- B. access-list 100 permit ip any 192.168.2.0 0.0.0.255
- C. access-list 1 deny 192.168.2.0 0.0.0.255

access-list 1 permit any
D. access-list 1 deny 192.168.2.0 0.0.0.255
access-list 1 deny 192.168.1.0 0.0.0.255
access-list 1 permit any
E. access-list 100 deny ip 192.168.2.0 0.0.0.255 any
access-list 100 permit ip any any

Answer: A

Explanation:

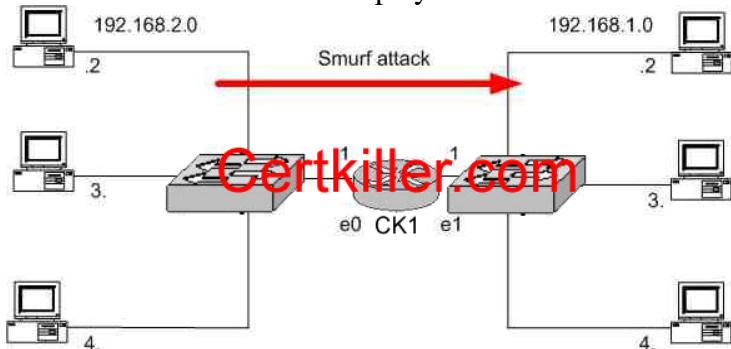
The access list in choice A will prevent all incoming traffic sourced from the 192.168.2.0/24 network from interface Ethernet 1 of router CK1 due to the implicit deny all. In the diagram above, hosts on the 192.168.2.0 network should only be used as a destination for traffic coming from this interface. Only traffic sourced from 192.168.1.0/24 should be seen in the input direction of this interface on CK1. If any traffic does not match the access list on choice A it could only be the result of a spoofed IP address and should be dropped.

Incorrect Answers:

B. This will allow all traffic (from any source) to reach the 192.168.2.0 network. This will not prevent spoofed IP addresses from the network on E1 to go through.
C. This would prevent spoofed packets that were spoofed only from the 192.168.2.0/24 network. This will not prevent all spoofed addresses outside of the 192.168.1.0 network, as required.
D. This will prevent the two networks from communicating at all.
E. This choice could also be used to prevent the spoofed traffic as required, but it will only prevent spoofed traffic that is IP based. Therefore, the access list in choice C is a better fit for this situation.

QUESTION 361

The Certkiller network is displayed in the exhibit below:



You want to block all Smurf attacks that originate on the 192.168.2.0 network from being sent into the 192.168.1.0 network. However, all other traffic must be permitted. No access lists currently exist on the router. Which of the following configuration excerpt would accomplish this task when applied to E0 on CK1 as an input filter?

A. access-list 1 permit 192.168.2.0 0.0.0.255

access-list 1 deny any
B. access-list 1 deny 192.168.1.0 0.0.0.255
access-list 1 permit any
C. access-list 100 permit ip any 192.168.1.0 0.0.0.255
access-list 100 deny ip any any
D. access-list 100 deny icmp any 192.168.1.255 0.0.0.0 echo
access-list 100 permit icmp any 192.168.1.0 0.0.0.255 echo
access-list 100 permit ip any any
E. access-list 100 deny icmp any 192.168.1.255 0.0.0.0 echo-reply
access-list 100 permit icmp any any echo-reply
access-list 100 permit ip any any

Answer: D

Explanation:

Anatomy of a SMURF Attack

A SMURF attack (named after the program used to perform the attack) is a method by which an attacker can send a moderate amount of traffic and cause a virtual explosion of traffic at the intended target. The method used is as follows:

- The attacker sends ICMP Echo Request packets where the source IP address has been forged to be that of the target of the attack.
- The attacker sends these ICMP datagrams to addresses of remote LANs broadcast addresses, using so-called directed broadcast addresses. These datagrams are thus broadcast out on the LANs by the connected router.
- All the hosts which are "alive" on the LAN each pick up a copy of the ICMP Echo Request datagram (as they should), and sends an ICMP Echo Reply datagram back to what they think is the source. If many hosts are "alive" on the LAN, the amplification factor can be considerably (100+ is not uncommon).
- The attacker can use largish packets (typically up to ethernet maximum) to increase the "effectiveness" of the attack, and the faster network connection the attacker has, the more damage he can inflict on the target and the target's network. Not only can the attacker cause problems for the target host, the influx of traffic can in fact be so great as to have a seriously negative effect on the upstream network(s) from the target. In fact, those institutions being abused as amplifier networks can also be similarly affected, in that their network connection can be swamped by the Echo Reply packets destined for the target.

In this example, answer choice D is correct as it prevents all ICMP messages destined to the broadcast IP address.

Note: The Cisco IOS command "no ip directed-broadcasts" is also an effective way to prevent smurf and fraggle attacks on the network.

Incorrect Answers:

A. This will permit all traffic sourced from the 192.168.2.0/24 network, including the smurf attack packets.

B. This choice will deny all traffic sourced from the 192.168.1.0 incoming on the e0 interface. Although this is probably a good choice, as it will effectively prevent all

spoofed IP traffic (as the 192.168.1.0/24 network should never be a source IP address in the incoming direction of this interface) we wish to only prevent the smurfed traffic, so E is a better choice.

C. This choice will only permit traffic that is destined to the 192.168.1.0 network. If additional networks exist behind the 192.168.1.0 network, such as traffic to the Internet, it will not be allowed through the CK1 router.

E. It would be preferable to stop the attack before the replies are sent, rather than simply filtering the replies.

QUESTION 362

The Certkiller network is connected to the Internet as shown in the diagram below:



Note: Private addressing is only used for reference

Certkiller 1 is currently configured and passing traffic. You want to block all IP spoofing attacks that originate in the Internet from being sent into the 192.168.1.0 network. However, normal traffic must be permitted. No access lists currently exist on the router. What configuration excerpt would accomplish this task when applied to Certkiller 1?

- A. access-list 100 permit ip any 192.168.1.0 0.0.0.255
access-list 100 deny any any
interface Ethernet 0
access-group 100 in
- B. ip cef
interface Ethernet 0
ip verify unicast reverse-path
- C. ip cef
interface Ethernet 1
ip verify unicast reverse-path
- D. access-list 100 permit icmp 192.168.1.0 0.0.0.255 any echo
access list 100 deny ip any any
interface Ethernet 1
access-group 100 out
- E. access-list 100 permit icmp 192.168.1.0 0.0.0.255 any echo
access list 100 deny ip any any
interface Ethernet 0
access-group 100 in

Answer: B

Explanation:

Use the ip verify unicast reverse-path interface command to mitigate problems caused by malformed or forged (spoofed) IP source addresses that pass through a router. Malformed or forged source addresses can indicate denial-of-service (DoS) attacks based on source IP address spoofing.

When Unicast RPF is enabled on an interface, the router examines all packets received on that interface. The router checks to make sure that the source address appears in the routing table and matches the interface on which the packet was received. This "look backwards" ability is available only when Cisco Express Forwarding (CEF) is enabled on the router because the lookup relies on the presence of the Forwarding Information Base (FIB). CEF generates the FIB as part of its operation.

Unicast RPF is an input function and is applied only on the input interface of a router at the upstream end of a connection.

Reference:http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a00800ca7cf.html

QUESTION 363

While troubleshooting some intermittent 802.11b wireless LAN problems, you use a protocol analyzer. While looking at the wireless LAN packets, which of the following should you find as part of the Frame Control Field? (Choose all that apply)

- A. Duration
- B. Power Management
- C. Order
- D. Wired Equivalent Privacy
- E. Retry
- F. More Fragment

Answer: B, C, D, E, F

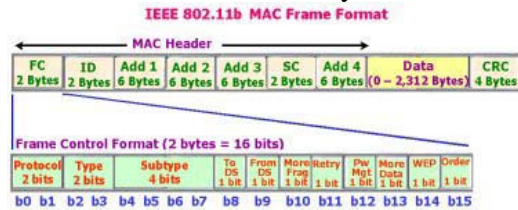
Explanation:

The IEEE 802.11b MAC Frame Format Contains the following:

- Frame Control (FC): protocol version and frame type (management, data and control).
- Duration/ID (ID)
 - o Station ID is used for Power-Save poll message frame type.
 - o The duration value is used for the Network Allocation Vector (NAV) calculation.
- Address fields (1-4) contain up to 4 addresses (source, destination, sender and receiver addresses) depending on the frame control field (the ToDS and FromDS bits).
- Sequence Control consists of fragment number and sequence number. It is used to

represent the order of different fragments belonging to the same frame and to recognize packet duplications.

- Data is information that is transmitted or received.
- CRC contains a 32-bit Cyclic Redundancy Check (CRC).



The Frame Control Format contains all of the following:

- Protocol Version indicates the version of IEEE 802.11 standard.
- Type & Subtype: Type - Management, Control and Data, Subtype - RTS, CTS, ACK etc
- To DS is set to 1 when the frame is sent to Distribution System (DS)
- From DS is set to 1 when the frame is received from the Distribution System (DS)
- More Fragment is set to 1 when there are more fragments belonging to the same frame following the current fragment
- Retry indicates that this fragment is a retransmission of a previously transmitted fragment. (For receiver to recognize duplicate transmissions of frames)
- Power Management indicates the power management mode that the station will be in after the transmission of the frame.
- More Data indicates that there are more frames buffered to this station.
- WEP indicates that the frame body is encrypted according to the WEP (wired equivalent privacy) algorithm.
- Order indicates that the frame is being sent using the Strictly-Ordered service class.

Incorrect Answers:

A. Duration is not a part of the FCF.

QUESTION 364

When comparing wireless Point to Point (p2p) and Point to Multipoint (p2mp) networks, which of the following statements are true?

- A. There are more bridges in a p2p network.
- B. There are more root bridges in a p2mp network.
- C. There is one root bridge and one or more non-root bridges in a p2mp network
- D. There is higher throughput in p2mp network.
- E. P2p networks are more secure

Answer: C

Wireless bridges can be deployed to establish a direct link between two sites. The network traffic between the two sites is bridged or forwarded to the other bridge as if it were within one network. This is called a point-to-point link.

A point-to-multipoint wireless link is an expansion of the point-to-point link in which one centralized bridge can establish multiple point-to-point links. Using point-to-multipoint

connections, multiple remote sites, such as buildings, can be linked together into a single logical network. In a point-to-multipoint architecture, these remote sites are linked to a single root bridge at a centralized site.

Incorrect Answers:

- A. In a point to point wireless connection there are only 2 bridges.
- B. There is only 1 root bridge in a multipoint network, while both bridges in a p2p network are considered to be root bridges.
- D. Because in a multipoint wireless network, such as a hot spot, the bandwidth is shared between the nodes there is less throughput.
- E. There are no security advantages to either method.

QUESTION 365

A wireless system based on the 802.1X standard is being implemented on the Certkiller network. What are the three main components of an 802.1X architecture?

- A. Authenticator, Certificate Server, Authentication Server
- B. Client, Authenticator, Certificate Server
- C. Authenticator, Authentication Server, Supplicant
- D. Client, Authentication Server, Supplicant
- E. Certificate Server, Supplicant, Authenticator

Answer: C

Explanation:

802.1X authentication for wireless LANs has three main components: The Supplicant (usually the client software); the Authenticator (usually the access point); and the Authentication Server (usually a Remote Authentication Dial-In User Service server, although RADIUS is not specifically required by 802.1X).

The client tries to connect to the access point. The access point detects the client and enables the client's port. It forces the port into an unauthorized state, so only 802.1X traffic is forwarded. Traffic such as Dynamic Host Configuration Protocol, HTTP, FTP, Simple Mail Transfer Protocol and Post Office Protocol 3 is blocked. The client then sends an EAP-start message.

The access point will then reply with an EAP-request identity message to obtain the client's identity. The client's EAP-response packet containing the client's identity is forwarded to the authentication server.

The authentication server is configured to authenticate clients with a specific authentication algorithm. The result is an accept or reject packet from the authentication server to the access point.

Upon receiving the accept packet, the access point will transition the client's port to an authorized state, and traffic will be forwarded.

QUESTION 366

CCX version 1 and version 2 require support for:

- A. WEP, Wi-Fi compliance, Cisco pre-standard TKIP
- B. WPA Compliance, and WPA 2 Compliance
- C. Cisco LEAP, support multiple SSIDs/VLANs, pre-standard eDCF
- D. AES Encryption
- E. All of the above

Answer: A

Explanation:

Makers of 802.11 wireless LAN clients now can make their products support special security features offered in Cisco wireless networks under Cisco Compatible Extensions (CCX), a licensing and testing program used to certify compatibility within Cisco wireless networks.

Cisco has already developed a CCX specification that includes the company's implementations of strong user authentication and encryption, Rossi said. CCX Version 1 includes compliance with the Cisco Wireless Security Suite, compatibility with Cisco's mechanism for assigning WLAN clients to virtual LANs, and full Wi-Fi and 802.11 standards compliance, according to the company.

CCX Version 2 will add support for the IEEE 802.1x authentication type PEAP (Protected Extensible Authentication Protocol) and compliance with WPA (Wi-Fi Protected Access) when using various 802.1x authentication types. It also will have some new Cisco WLAN capabilities that improve roaming and WLAN management. WPA is a specification developed by the Wi-Fi Alliance industry group.

Incorrect Answers:

B, C. These are all functions of CCX version 2 only and were not supported in version 1.
D. AES is the advanced encryption standard, used to increase the security of standard DES and 3DES encryption schemes. AES will be supported with CCX version 3.

QUESTION 367

The Certkiller network is replacing the 802.11 a/b devices with 802.11g devices. What statement is FALSE about the 802.11g standard?

- A. It operates in the same frequency spectrum as 802.11b.
- B. It has the same number of non overlapping channels as 802.11a.
- C. It requires antennas specific to the 2.4 GHz band.
- D. All statements above are true about the 802.11g standard.
- E. None of the above statements are correct.

Answer: B

Explanation:

802.11g is an extension to 802.11b, the basis of the majority of wireless LANs in existence today. 802.11g will broaden 802.11b's data rates to 54 Mbps within the 2.4 GHz band using OFDM (orthogonal frequency division multiplexing) technology. Because of backward compatibility, an 802.11b radio card will interface directly with an 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. You

should be able to upgrade the newer 802.11b access points to be 802.11g compliant via relatively easy firmware upgrades.

Similar to 802.11b, 802.11g operates in the 2.4GHz band, and the transmitted signal uses approximately 30MHz, which is one third of the band. This limits the number of nonoverlapping 802.11g channels to three, which is the same as 802.11b.

A big difference with 802.11a is that it operates in the 5GHz frequency band with twelve separate non-overlapping channels. As a result, you can have up to twelve access points set to different channels in the same area without them interfering with each other. This makes access point channel assignment much easier and significantly increases the throughput the wireless LAN can deliver within a given area. In addition, RF interference is much less likely because of the less-crowded 5 GHz band.

Reference: <http://www.wi-fiplanet.com/tutorials/article.php/1009431>

QUESTION 368

The IEEE standard controlling client network access in WPA authentication is:

- A. EAP-TLS
- B. EAP
- C. 802.1X
- D. 802.1Q
- E. All of the above

Answer: C

Explanation:

The IEEE 802.1x standard defines 802.1x port-based authentication as a client-server based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. The authentication server validates each client connected to a switch port before making available any services offered by the switch or the LAN.

Until the client is authenticated, 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port. In a Cisco wireless network, the 802.1X standard and the Extensible Authentication Protocol are synonymous, but the industry standard is the 802.1X method, making choice C the best answer.

QUESTION 369

What device can function as a Wireless Domain Server capable of RF aggregation?

- A. BR1300
- B. AP1200
- C. WLSM
- D. AP1100
- E. All of the above

Answer: E

Explanation:

Cisco SWAN Wireless Domain Services

Cisco SWAN Wireless Domain Services (WDS) is a collection of Cisco IOS Software features that expand WLAN client mobility, simplify WLAN deployment and management, and enhance WLAN security. These services-supported today on access points, Cisco and Cisco Compatible client devices, and the Cisco Catalyst 6500 Series WLSM, and other Cisco LAN switches and routers in 2005-include radio management aggregation, fast secure roaming, client tracking, and WAN link remote site survivability. Cisco SWAN WDS radio management aggregation supports RF managed services such as rogue access point detection for WLAN threat defense, interference detection, assisted site surveys, and self-healing WLANs.

Reference:http://www.cisco.com/en/US/products/ps6108/products_data_sheet0900aecd801b914f.html

QUESTION 370

You are in the planning stages for the new Certkiller wireless network, and are determining the types of antennas that should be utilized. Which are the four basic antenna types that can be used?

- A. Dipole, non-pole, ground effect, bipole
- B. Omnidirectional, patch, yagi, parabola
- C. High gain, omni, point to point, point to multi-point
- D. Wall mount, mast mount, pole mount, window mount
- E. Directional, omni-directional, dipole, distributed

Answer: B

Explanation:

The basic antenna types and their descriptions are provided below:

Omnidirectional Antennas:

An omnidirectional antenna provides a 360-degree radiation pattern. This type of antenna is used when coverage in all directions is required and when communicating with wireless client devices. Antennas in this category are available in different gain ratings (typically 2.2 to 12 dBi).

Directional Antennas:

A directional antenna provides a stronger radiation pattern in a specific direction by focusing the radiation energy to provide a greater coverage distance. Directional antennas include the Yagi antenna, the patch antenna, and the parabolic dish antenna.

QUESTION 371

You have been assigned the task of setting up access points within a building for wireless users. The best position for an Access Point in a corporate wireless network is: (Select the best answer).

- A. The center of the building
- B. In a position determined by a site survey
- C. At the edges of the building
- D. At the edge of the coverage area shown by the site survey in the ceiling or the floor
- E. Away from any metal or glass

Answer: B

Explanation:

Because of differences in component configuration, placement, and physical environment, every network application is a unique installation. Before installing the system, you should perform a site survey to determine the optimum utilization of networking components and to maximize range, coverage, and network performance. Consider the following operating and environmental conditions when performing a site survey:

- Data rates - Sensitivity and range are inversely proportional to data bit rates. The maximum radio range is achieved at the lowest workable data rate. A decrease in receiver threshold sensitivity occurs as the radio data increases.
- Antenna type and placement - Proper antenna configuration is a critical factor in maximizing radio range. As a general rule, range increases in proportion to antenna height.
- Physical environment - Clear or open areas provide better radio range than closed or filled areas. Also, the less cluttered the work environment, the greater the range.
- Obstructions - A physical obstruction such as metal shelving or a steel pillar can hinder performance of the client adapter. Avoid locating the workstation in a location where there is a metal barrier between the sending and receiving antennas.
- Building materials - Radio penetration is greatly influenced by the building material used in construction. For example, drywall construction allows greater range than concrete blocks. Metal or steel construction is a barrier to radio signals.

QUESTION 372

The Certkiller network is performing site surveys at all of their location in order to plan for the installation of wireless networking devices. In terms of wireless networking, what are leading indicators of links with excessive occlusion (blockage with physical elements)?

- A. Coverage area less than 10 square meters at signals greater than -65 dBm
- B. Drops in RF signal in excess of 20 dBm over distances of less than two meters
- C. Inability to physically see the infrastructure device
- D. Distance in excess of 20 meters from an infrastructure device in a carpeted environment
- E. All of the above.

Answer: C

Explanation:

Occlusion is defined as an obstruction or a closure of a passageway or vessel. If the wireless access point can not be physically seen, then there is an excessive amount of physical elements (boxes, walls, warehouse shelving, etc) that is blocking the view. This can lead to poor wireless signals.

QUESTION 373

What are the main advantages of the Cisco SWAN architecture?

- A. Security
- B. Layer 3 mobility
- C. Visibility and management of the wireless network
- D. Centralized Management
- E. None of the above

Answer: D

Explanation:

The Cisco Structured Wireless-Aware Network (SWAN) provides the framework to integrate and extend wired and wireless networks to deliver the lowest possible total cost of ownership for companies deploying wireless LANs (WLANs). Cisco SWAN extends "wireless awareness" into important elements of the network infrastructure, providing the same level of security, scalability, reliability, ease of deployment, and management for wireless LANs that organizations have come to expect from their wired LANs.

From small businesses to large-scale enterprise multinational companies; within WLAN campus deployments or branch offices; at universities; in retail, manufacturing, or healthcare industries; or at hot spot locations, Cisco SWAN reduces overall operational expenses by simplifying network deployment, operations and management. With Cisco SWAN, several, hundreds, or thousands of central or remotely located Cisco Aironet Series access points can be managed from a single management console. Cisco SWAN's flexibility allows network managers to design networks to meet their specific needs, whether implementing a highly integrated network design or a simple overlay network.

Reference:http://www.cisco.com/en/US/netsol/ns340/ns394/ns348/ns337/networking_solutions_package.html

QUESTION 374

As the administrator of the Certkiller network, you are considering the benefits and disadvantages of installing a wireless LAN at your Headquarters office. In weighing in these considerations, what is NOT a reason for deploying wireless in a corporate environment?

- A. There is a need to eliminate rogue Access Points in the organization and increase LAN security.

- B. The organization needs to provide greater mobility to users.
- C. Wireless is cheaper to deploy than a wired network.
- D. The employer wishes to obtain greater productivity from the employees.
- E. All of the above are wireless networking features

Answer: A

Explanation:

Although there are many benefits for deploying a wireless network from a cost and productivity perspective, it can introduce some security issues. Access points can be difficult to secure, and sometimes corporate employees will install their own access points within the office in order to increase the range. In addition, weak security measures are often used in wireless networks. The original IEEE 802.11 security standard had modest security goals in Wired Equivalent Privacy (WEP), including native authentication, where users are required to prove they are authorized for access and encryption to provide data protection. The protocols in WEP are now easily defeated.

Incorrect Answers:

- B. A major goal of the use of wireless networks is to provide for a more mobile workforce.
- C. Wireless networks can be cheaper to deploy in a new office environment, as the added costs associated with CAT5 cable drops are eliminated. In addition, fewer switches are needed, since each access point can handle many users, but only requires one switch port.
- D. This is true as users can now carry their laptops with them to other areas of a building, such as conference rooms, enabling them to continue working even during meetings and conferences.

QUESTION 375

The WLSE is being configured for managing the Certkiller WLAN. When the WLSE generates an alarm, what actions can the device take?

- A. Send an e-mail to an administrator
- B. Disable the switch port that the rouge Access Point is connected to
- C. Send a message to a syslog server
- D. Generate an SNMP trap
- E. All of the above

Answer: E

Explanation:

When a fault is detected, the WLSE can send automated notifications in the form of SNMP traps, syslog messages, and email alerts. You can specify multiple recipients for each notification type, and choose to deliver the message using either a plain text or XML format.

QUESTION 376

The Certkiller network plans to implement the use of Public Wireless hot spots and

security issues are a concern. Which of the following are primary requirements in PWLAN security? (Choose all that apply)

- A. Encryption of user data
- B. IPSec encryption
- C. Accounting of time, and throughput
- D. 802.1x
- E. Broadcast SSIDs

Answer: A, D

Explanation:

Two of the chief security concerns for public wireless (PWLAN) use is user authentication, which is addressed with the 802.1x/EAP suite of protocols, and the encryption of individual user data.

The Cisco PWLAN solution has implemented numerous features in the Cisco IOS Software for Cisco's access zone routers (AZR) that help mitigate the risk of session hijacking associated with malicious IP spoofing activity.

Operators can take advantage of key features available in Cisco access points to prevent local peer attacks as well as preventing man-in-the-middle spoofing of infrastructure addresses.

Cisco access points support all 802.1x/EAP methods available today, in addition to supporting WPA for air link encryption.

QUESTION 377

A wireless LAN needs to be implemented in a new Certkiller location. How is a baseline RF environment established?

- A. With a carefully detailed RF site survey and supporting documentation.
- B. With a carefully detailed RF site survey only.
- C. By using WLSE's Assisted Site Survey feature.
- D. Usually with a spectrum analyzer

Answer: A

Explanation:

To establish the feasibility of any wireless LAN (WLAN) or radio frequency (RF) project, a site survey, complete with supporting documentation, should be performed. A WLAN site survey takes into account the radius around one or more Access Points and the structural components of the facility to determine coverage. This survey involves verifying a clear line of site between points, consulting topographical maps, and global positioning systems to pinpoint locations and to evaluate needs relating to mounting equipment and towers. A number of documents are generated from this survey including a Bill of Materials, requirements for tower and antenna placement, drawings and siterelated documents including construction materials, and a plan to implement.

QUESTION 378

When implementing corporate guest access an important consideration of the RF coverage is:

- A. That the area RF coverage should offer high data rates only.
- B. That the RF coverage offers low latency roaming.
- C. That the area of RF coverage avoids leakage outside the building as much as possible.
- D. That the RF coverage is as secure as possible.
- E. That the area RF coverage is as large as possible.

Answer: C

Explanation:

When setting up a wireless network for corporate guest access, an important consideration is to ensure that the radio frequency coverage is maintained within the building. The leaking of the RF coverage to the outside leaves the potential for unauthorized access from unknown, outside users. When RF access leaks to the outside, hackers are able to pick up the signals and obtain unauthorized wireless Internet access.

QUESTION 379

Certkiller is using the WLSE to manage their Cisco wireless network. What network connectivity tools are available on the WLSE administration page?

- A. Ping and traceroute only
- B. SNMP reachable, Ping and Traceroute only
- C. Ping, Traceroute, and SNMP reachable only
- D. Ping, traceroute, nslookup, tcp port scan, SNMP reachable only
- E. Ping, Traceroute, L2 Traceroute, nslookup, and SNMP reachable only

Answer: D

Explanation:

The following chart display the various connectivity tools available on the WLSE administration interface:

Connectivity Tools		
Button	Description	Results
Ping	Tests device reachability.	If successful, statistics are displayed on the packets transmitted and received.
Traceroute	Detects routing errors between the WLSE and a device.	If successful, the routes to

		the device are displayed.
NSLookup	Looks up hostname or IP address information via the name server.	If successful, displays the name server name and IP address and the device name and IP address.
TCP Port Scan	Finds the active ports on a device.	Displays the active ports.
SNMP	Tries to reach a device by using SNMP. To reach a device by	If the device is
Reachable	using SNMP, the device's credentials must be in the WLSE database. To check credentials, select Administration > Devices > Discover > Device Credentials > SNMP Communities.	reachable, its sysObjID is displayed. If no sysObjID is returned: <ul style="list-style-type: none">• The query may be timing out because the device is busy or is remotely located.• The SNMP agent in the device may not be functioning.

Reference:http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_user_guide_chapter09186a00801d08a8.html

QUESTION 380

What is NOT an optimal method for detecting co-channel reference?

- A. A properly planned and documented site survey, with continued monitoring of the radiating environment.
- B. Well enforced policies on the deployment of rogue APs.
- C. Deploying WLSE
- D. Deploying SWAN

Answer: B

Explanation:

The use of rogue Access Points (APs) should be completely avoided within an enterprise wireless LAN. Simply establishing a policy against the deployment of rogue APs alone will not be effective. The Wireless site should be continuously maintained and monitored to ensure that the introduction of outside access points does not occur, via the Cisco SWAN model through the use of the WLSE.

QUESTION 381

The Certkiller WLAN is experiencing problems associated with poor link margins. What are the leading indicators of insufficient link margin?

- A. Difference of less than 10 dBm from signal to noise
- B. Links work fine initially but flap or go down shortly after being turned up
- C. Competing sources of 802.11 arrive in the radiating area
- D. Link initially deployed at full power settings on infrastructure and client devices but link still goes down shortly after being turned up.
- E. All of the above

Answer: E

Explanation:

Transmission range in a system is determined by link margin calculations. Figure 1 shows the overall link margin of a system that includes transmission power output, antenna gain, receiver sensitivity and path loss. Such path loss is due to cable and antenna attenuation, air content and obstacles preventing line-of-sight conditions. Achieving long range with wireless transceiver modules requires an effective combination of output power, antenna gain and receiver sensitivity. Each of these specifications can have dramatic effects on the link margin of a wireless link path.

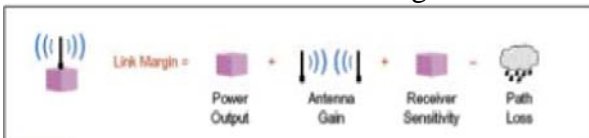


Figure 1 The overall link margin of a system includes transmission power output, antenna gain, receiver sensitivity and path loss. Path loss is caused by cable and antenna attenuation, air content and obstacles preventing line-of-sight conditions.

All of the answer choices are symptoms that can be caused by problems associated with poor link margin.

QUESTION 382

A Certkiller user has an 802.11g/a capable client card. They are able to associate to a Cisco BR1300 without any trouble; however, they are not able to associate to a Cisco BR1400, although all the wireless settings appear to be correctly configured. What is the most likely explanation?

- A. The BR1300 is hard-coded not to accept client associations, while the 1400 is capable of this feature.
- B. 802.11a bridging uses the UNII-3 frequency band which is in a different

frequency band than what 802.11a clients use.

- C. The BR1400 can only accept one associated connection, which is already taken up by the radio on the other end of the bridge link.
- D. The BR1400 uses a unique MAC layer protocol implementation that prevents any clients from associating.
- E. The user is trying associate to the root bridge of the 802.11a bridging link. Only non-root bridges can accept a client association.
- F. None of the above

Answer: D

Explanation:

The BR1400 only supports the Root BR and Non-Root BR roles, and does not support client associations. Only other BR1400s can associate to a root BR1400.

Reference: http://www.cisco.com/en/US/about/ac123/ac114/ac173/Q3-04/netpro_express.html

QUESTION 383

Certkiller is utilizing VOIP on a wireless LAN. How many simultaneous WLAN VOIP calls can be supported by an AP with Quality of Service enabled, assuming that the G.711 codec is used?

- A. 64
- B. 12
- C. 8
- D. 7
- E. None without proxy ARP enabled

Answer: D

Explanation:

The following network capacity guidelines apply to sizing the Wireless IP Telephony network:

- No more than 7 concurrent G.711 calls per AP.
- No more than 8 concurrent G.729 calls per AP.

Reference: http://www.cisco.com/en/US/products/hw/phones/ps379/products_implementation_design_guide_chapter09186a00802a0a05.html

QUESTION 384

What is eDCA?

- A. The difference in the delay used by 802.11 management frames, and data frames
- B. The time taken between the when a channel becomes free and a radio tries to send a frame
- C. The standard 802.11 contention mechanism
- D. A mechanism for adjusting the random backoff of WLAN traffic based in traffic

classification

E. An authentication type for handheld devices

Answer: D

Explanation:

EDCA (Enhanced Distributed Channel Access) was specified in the 802.11e draft. EDCA, also known as prioritized DCF, improves on DCF by giving higher-priority traffic an advantage during contention. Instead of waiting the normal period before transmitting after the back-off period expires, higher-priority traffic can attempt to transmit only after a PIFS (point coordination function interframe space) period and associated back-off time. Using the EDCA scheme, nodes that offer high-priority traffic, an example being VoIP phones, have a higher probability of gaining channel access than the nodes offering lower-priority traffic, such as PC downloads.

QUESTION 385

The Certkiller network is utilizing Voice over Wireless LANs to provide for a mobile workforce. How would you design frequency overlap for voice over WLAN versus 802.11 for data only?

- A. You would ensure that all areas where an 802.11 voice call could be initiated is covered by at least two RF infrastructure devices.
- B. You would configure all the RF infrastructure devices to select optimal channels as required.
- C. You would ensure each cell is at least 20% overlapped by second RF infrastructure device.
- D. You would ensure all infrastructure RF devices were set to maximum power.
- E. None of the above.

Answer: C

Explanation:

The critical components in the wireless network are the access points (APs) that provide the "hot spots" or wireless links to the network. Cisco requires that Cisco IOS is running on the APs that support voice calls since Cisco IOS provides features for managing voice traffic.

The AP has a transmission range or coverage area that depends on its type of antenna and transmission power. The access point coverage range generally varies from 500 to 1000 feet. To provide effective coverage, access points need a range overlap of approximately 20 percent to allow uninterrupted connections as phone users roam from one access point to another.

Reference:

http://www.cisco.com/en/US/products/hw/phones/ps379/products_administration_guide_chapter09186a008024662c.html

QUESTION 386

The Certkiller network has recently installed a Cisco Works Wireless LAN Solutions Engine (WLSE) to aid in the maintenance and management of the wireless LAN devices. When upgrading the firmware on access points, the WLSE can perform which of the following functions? (Choose the best option)

- A. Upgrade firmware, validate the target AP type and convert configurations from VxWorks to IOS all at a scheduled time/date
- B. Upgrade firmware of the access point only
- C. Upgrade firmware, and convert configurations from VxWorks to IOS at a scheduled time/date
- D. Update firmware, and convert configuration from VxWorks to IOS immediately

Answer: A

Explanation:

The WLSE is a hardware and software solution for managing Cisco wireless devices. The configuration feature allows you to apply a set of configuration changes to access points and connected switch ports. Using the firmware feature, you can upgrade the firmware on access points and bridges. You can also use the WLSE to schedule tasks to be performed at a later date, and to convert non-IOS (VxWorks) configuration file versions to IOS versions. Upon completion of any scheduled tasks, the WLSE attempts to verify that the task had indeed completed successfully.

QUESTION 387

The Certkiller network is utilizing the Cisco Wireless LAN Solution Engine (WLSE) to manage the structured WLAN. The WLSE Location Manager performs which of the following functions:

- A. Discovers the location of APs, and the links them with imported site survey data
- B. Is a separate module in the Catalyst 6500 providing location based services for Mobile Applications
- C. Builds a database of APs location, that is used in device grouping, and radio management
- D. Contains the location of AP management devices, allowing them to correlate GPS data
- E. None of the above.

Answer: C

Explanation:

The CiscoWorks WLSE is a centralized, systems-level solution for managing the entire Cisco Aironet wireless LAN (WLAN) infrastructure. The advanced radio frequency (RF) and device management features of the CiscoWorks WLSE simplify the everyday operation of WLANs, ensure smooth deployment, enhance security, and maximize network availability, while reducing deployment and operating expense. The CiscoWorks

WLSE enables administrators to detect, locate, and mitigate rogue access points and RF interference. The assisted site survey feature automates the previously manual, expensive, and time consuming process of determining optimal access point settings including transmit power and channel selection. The CiscoWorks WLSE automatically configures access points and bridges, assures the consistent application of security policies, and proactively monitors faults and performance. The CiscoWorks WLSE is a core component of the Cisco Structured Wireless-Aware Network.

The Location Manager is a GUI that displays wireless access points and bridges on a building floor plan. The location of rogue access points and RF interference is represented visually on the floor plan, as is the coverage area of each access point.

QUESTION 388

What is the primary purpose of a template in the WLSE?

- A. A template is used to model the RF distribution pattern from Access Points in Location Manager.
- B. Templates are used to set up a model for setting alarm levels in the WLSE.
- C. A template is used as create a configuration model for Access Points in the network.
- D. Templates push out configuration files to the Access Points.
- E. Templates are used to generate firmware upgrades to the WLAN components.

Answer: C

Explanation:

The WLSE is a GUI based Cisco works based tool used to maintain and manage Cisco Wireless networks. It centrally identifies and configures Access Points (AP) in customerdefined groups and reports on throughput and client associations, enabling optimized wireless network performance and overall operational efficiency. WLSE's centralized management capabilities are further enhanced with an integrated template-based configuration tool for added configuration ease and improved productivity. You can think of a configuration template as a configuration update file for an access point. This file might contain the update for only one parameter or a complete access point configuration.

QUESTION 389

The Cisco Compatible Extensions Program (CCX) provides which of the following with regards to wireless networking?

- A. A way for Cisco to avoid joining the standards bodies for wireless LAN
- B. Cheaper wireless network.
- C. A more secure wireless network.
- D. Faster wireless network with faster L3 roaming times.
- E. A way for Cisco to accelerate the deployment of wireless features.

Answer: E

Explanation:

The Cisco Compatible Extensions Program for WLAN devices provides tested compatibility with licensed Cisco infrastructure innovations. Compatibility is assured through extensive, independent testing of third-party. The Cisco Compatible Extensions Program enables the widespread availability of wireless client devices that take advantage of the Cisco wireless network, accelerating the availability of innovative features while maintaining interoperability.

QUESTION 390

As part of the new Certkiller wireless network implementation, the use of the WLSE Radio Manager is planned. What are the main functions of the Radio Manager in the WLSE?

- A. Rogue access point detection, interference detection and client walk about
- B. Client walkabout, AP scanning, RM assisted configuration, self healing and auto re-site survey
- C. Client walkabout, interference detection, rogue access point detection, location based services.
- D. RM assisted configuration, rouge access point detection, interference detection, location based services.
- E. None of the above.

Answer: C

Explanation:

Radio Management

The Radio Manager tab displays information to help you manage your WLAN radio environment. All the device information shown under this tab is polled from the managed devices in your network.

The Radio Manager tab includes these options:

- Radio Monitoring
- AP Radio Scan
- Client Walkabout
- Location Manager
- RM Assisted Configuration
- Manage RM Measurements

The Radio Manager features simplify the deployment, expansion, and day-to-day management of the WLAN by:

- Automatically configuring network-wide radio parameters during initial deployment and network expansion.
- Continuously monitoring the radio environment, detecting interference and rogue APs, and alerting the WLAN administrator to radio network changes.
- Providing information to help visualize the network radio topology, including the path loss between APs and RF coverage

The Radio Manager provides these features:

- Rogue AP detection
- Interference detection
- Automatic radio parameter generation

The Radio Manager can generate optimal values for the radio parameters of a given group of APs. Each set of radio parameters can modify the following:

- AP frequency
- AP transmit power
- AP beacon interval

You can also choose to run these features manually. The following table summarizes which procedures produce the data required by the different Radio Manager features:

Feature	Run these procedures	Results are used in:
Rogue AP detection	Radio Monitoring	Location Manager
	AP Radio Scan	Faults
Interference detection	Radio Monitoring	Faults
Automatic radio parameter generation	AP Radio Scan	RM Assisted Configuration
	Client Walkabout (recommended)	Location Manager
		Radio Manager Reports

Feature Run these procedures Results are used in:

Rogue AP detection

Radio Monitoring

AP Radio Scan

Location Manager

Faults

Interference detection Radio Monitoring Faults

Automatic radio parameter generation

AP Radio Scan

Client Walkabout (recommended)

RM Assisted

Configuration

Location Manager

Radio Manager Reports

The results produced by these features constitute the radio knowledge base. This knowledge base is saved in the WLSE database and accessed by other Radio Manager features.

QUESTION 391

The new Cisco WDS features are being implemented in the Certkiller wireless network. What is true of the Wireless Domain Service (WDS)?

A. It runs only on an AP, connects to WLSE, responsible for all authentications from other APs on the subnet.

- B. It runs only on an AP, implements CCKM, implements QoS for the wireless traffic.
- C. It often runs on the AP, implements CCKM, securely connects to other APs on the subnet, connects to the WLSE and delegates Radio Management jobs from the WLSE to all other APs.
- D. It connects the WLSE to the other APs on the subnet and delegates RM jobs from the WLSE.
- E. Often runs on the AP, securely connects to other APs on the subnet, connects to the WLSE and delegates Radio Management jobs from the WLSE to all other APs.

Answer: A

Explanation:

WDS is a new feature for access points in Cisco IOS Software. WDS is a core functionality that enables other features such as Fast Secure Roaming, Wireless LAN Solution Engine (WLSE) interaction, and Radio Management. Relationships between the access points that participate in WDS must be established before any of these other WDS-based features can work. One of the primary purposes for WDS is to eliminate the need to have the authentication server validate user credentials every time and thereby reduce the time required for client authentications.

Client authentication is defined by one or more client server groups on the WDS access points.

When a client attempts to associate to an infrastructure access point, the infrastructure access point passes the user's credentials to the WDS access point for evaluation. If it is the first time that the WDS access point has seen a given user's credentials, it uses the authentication server to validate the credentials. The WDS access point then caches the user's credentials, so it does not have to return to the authentication server when that user attempts authentication again (for example, reauthentication for rekeying, for roaming, or for when the user starts up the client device).

QUESTION 392

A new Cisco Works Wireless LAN Solutions Engine (WLSE) is being implemented into the Certkiller network. This WLSE does NOT perform what network management function?

- A. Aggregating SNMP and syslogs from its managed APs.
- B. SNMP queries of the APs
- C. The aggregation of Radio Management data
- D. CDP Discovery
- E. The WLSE performs none of the above functions.

Answer:

Explanation:

CiscoWorks WLSE may be transparently integrated with other network management

systems, operations support systems, and CiscoWorks applications through syslog messages, Simple Network Management Protocol (SNMP) traps, and an Extensible Markup Language (XML) interface. Although the WLSE can be used with Syslog and SNMP servers, it can not be used as a Syslog or SNMP server. Syslog and SNMP messages can not be effectively sent to the WLSE from the access points.

Incorrect Answers:

B. One of the tools available via the WLSE is the SNMP Query Tool. This tool allows you to find the value of a specified SNMP variable. Normally, this tool is used under the direction of Cisco TAC when they are assisting you with troubleshooting a problem.

C. Following are some of the WLSE radio management features that are supported: Radio Monitoring, AP Radio Scan, Client Walkabout, RM Assisted Configuration, Self Healing, Auto Re-Site Survey, Location Manager.

D. By default, the WLSE runs a CDP discovery every 24 hours.

Reference:

http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_data_sheet0900aecd801d706e.html

QUESTION 393

An SSG is being utilized within the Certkiller Public Wireless LAN. What best describes the function of an SSG in a Public Wireless LAN (PWLAN)?

A. The SSG provides connectivity, client address management, security services, and routing across a WAN from each wireless access point to the service provider data center.

B. The SSG provides subscriber authentication and maintains the state of all users in the hotspot.

C. The SSG is an http proxy that provides captive portal capabilities to the service provider hot spot network.

D. The SSG is a central device that allows wireless clients to cross layer three subnets with sub-second roam times.

E. The SSG provides central management for the PWLAN hotspot network

Answer: B

Explanation:

Access control of the PWLAN is based on the extremely flexible Cisco IOS Service Selection Gateway (SSG) technology that is now available across a broad range of platforms, including the Cisco 2651XM Router, Cisco 2691 Router, Cisco 3725 Router, Cisco 3745 Router, Cisco 7200 Series, and Cisco 7301 Router. Together with the Cisco CNS Subscriber Edge Services Manager (SESM), the Cisco SSG provides subscriber authentication, service selection, service connection, and accounting capabilities to subscribers of Internet and intranet services.

The Cisco CNS SESM works with the Cisco SSG to provide complete control over the subscriber experience, supporting customization and personalization based on device, client, location, service, and other criteria to offer higher value to end users and maximize service and advertising revenue.

The Cisco SSG access control platform can proxy EAP authentication messages from hot-spot access points and automatically create user sessions upon successful EAP authentication, thereby eliminating the need for "double authentication," first at Layer 2 with 802.1x/EAP and then at Layer 3 through the Web portal. This feature allows an operator to take advantage of the Cisco SSG for centralized accounting record generation for both 802.1x/EAP and Web-authenticated users.

Reference:

<http://www.cisco.com/en/US/netsol/ns341/ns396/ns177/ns436/netbr09186a00801f9f3d.html>

QUESTION 394

You wish to manually fail over of your SONET APS ring from the active path to the back-up path. Which command will accomplish this?

- A. aps clear sonet
- B. aps auto circuit-number
- C. aps force circuit-number
- D. aps force secondary
- E. aps back-up circuit.-number

Answer: C

A is the correct command syntax.

Incorrect Answers:

A. The aps clear sonnet is used to remove all externally initiated SONET automatic protection switching (APS) commands configured on a Cisco AS5850, use the aps clear sonet command in privileged EXEC mode.

Reference:

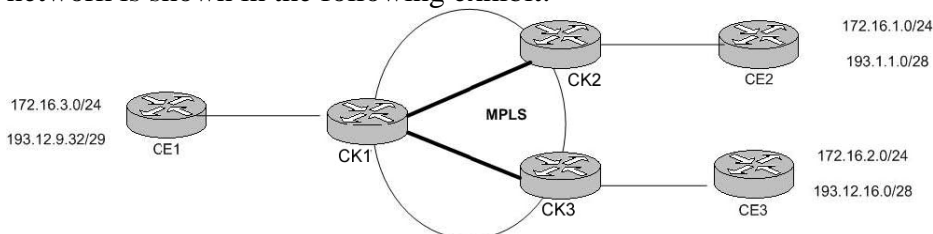
For details and functionality of any command make use of the link below. CCO login required.

[http://www.cisco.com/cgi-bin/Support/Cmdlookup/ios-commandlookup.pl?type=reference&query=no+login+&paging=25&counter=0&release=123&su=](http://www.cisco.com/cgi-bin/Support/Cmdlookup/ios-commandlookup.pl?type=reference&query=no+login+&paging=25&counter=0&release=123&su=Submit)

[Submit](http://www.cisco.com/cgi-bin/Support/Cmdlookup/ios-commandlookup.pl?type=reference&query=no+login+&paging=25&counter=0&release=123&su=Submit)

QUESTION 395

Certkiller is an ISP providing MPLS VPNs to their customers. Part of the Certkiller network is shown in the following exhibit:



You are trying to verify that the correct paths are configured within the CK routers. Which networks should show up in the same Forwarding Equivalence Class (FEC) on Router CK1 ?

- A. 172.16.3.0/24 and 192.1.1.0/28
- B. 172.16.1.0/24, 172.16.2.0/24, and 172.16.3.0/24
- C. 172.16.1.0/24 and 193.1.1.0/28
- D. 172.16.1.0/24 and 172.16.2.0/24
- E. 172.16.0.0/16 and 193.0.0.0/8

Answer: C

Explanation:

Both networks in answer C are along the same path, so they would both be in the same FEC.

Reference:

For a better understanding of MPLS TE and FEC go through the (white paper link) below.

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

QUESTION 396

In an MPLS network, which protocol is used to distribute traffic engineering information? (Choose all that apply)

- A. EIGRP or IGRP
- B. BGP MEDs
- C. OSPF Opaque LSAs or IS-IS TLVs
- D. RTP or RTCP packets
- E. None of the above

Answer: C

Explanation:

OSPF Opaque LSA provides a generalized mechanism for OSPF to carry additional information. The new information can be used directly by OSPF or indirectly by other applications, which use OSPF to distribute information. This document defines how to use opaque LSA to carry additional information for traffic engineering.

Reference:

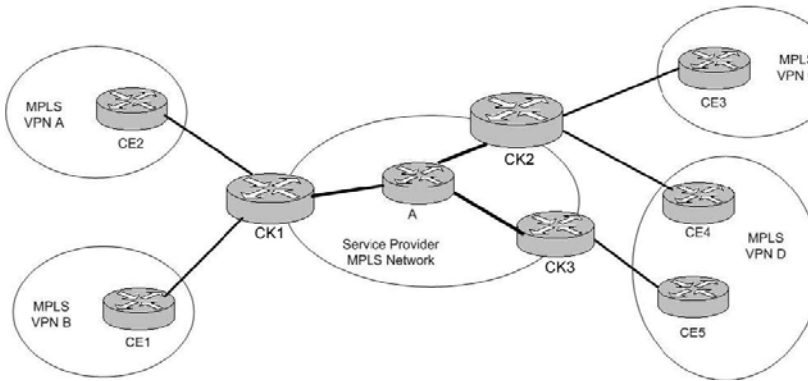
<http://www.watersprings.org/links/mlr/id/draft-yeung-ospf-traffic-00.txt>

Incorrect Answers:

- A. Interior routing protocols are used to distribute the interior network routes, but are not used to carry TE information.
 - B. BGP MEDs are used to influence the incoming traffic from a BGP neighbor.
 - D. RTP is the Real Time Protocol, used for setting up voice and video traffic.
-

QUESTION 397

Router CK1 , CK2 , and CK3 are MPLS provider edge routers as shown below:



How many routing tables should there be on Router CK2 ?

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

Answer: A

Explanation:

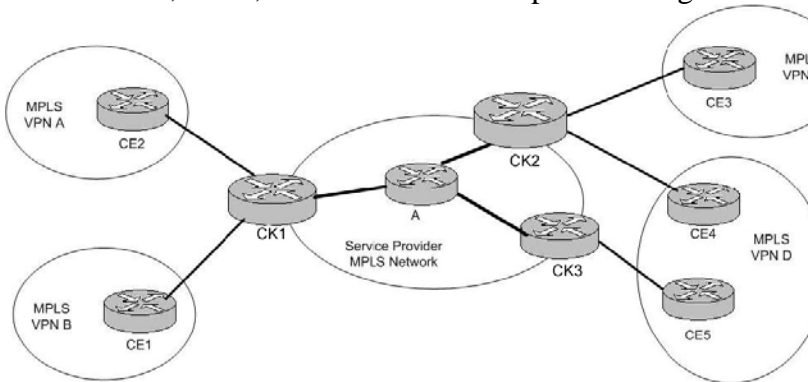
There should always be only one routing table within an MPLS network.

Incorrect Answers:

B. In this case there would be 2 VRF (Virtual Routing and Forwarding) tables, but still only 1 routing table.

QUESTION 398

Router CK1 , CK2 , and CK3 are MPLS provider edge routers as shown below:



How many VRF tables will be on router CK2 ?

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

Answer: B

Explanation:

Router CK2 must keep track of two separate VPN customers, VPN C and VPN D. Each VPN will have its own VRF table.

Incorrect Answers:

A. This would be the correct choice if the question were asking how many routing tables existed on CK2 , as there would only be one routing table.

QUESTION 399

What is the signaling protocol used for the MPLS fast reroute (FRR) feature?

- A. B-ISUP
- B. LDP
- C. RSVP
- D. SS7
- E. TDP

Answer: C

Cisco FRR utilizes MPLS label stacking with RSVP signaling to create a backup tunnel around the link or node that needs to be protected. On detection of loss of signal from the link, the MPLS FRR application in Cisco IOS Software starts forwarding the traffic onto the backup tunnel, transparent to end users or applications such as VoIP or video, in 50 ms or less (actual failover time may be greater or less than 50ms, depending on the hardware platform, the number of TE Tunnels and/or Network prefixes).

Incorrect Answers:

A. The ITU-T's broadband ISDN user part (B-ISUP) is based on signaling system no. 7 (SS7) and is used for signaling between the nodes of a public ATM network, that is, across an NNI.

B, E. LDP is the Label Distribution Protocol used to distribute label information across the MPLS network. TDP is the Tag Distribution Protocol, which is the Cisco proprietary method of distributing tags across the network in tag switching. MPLS is founded on Cisco's tag switching.

D. SS7 is a signaling protocol normally found in Voice circuits. It is not related to MPLS fast reroute.

Reference:

White Paper, Deploying Guaranteed-Bandwidth Services with MPLS

http://www.cisco.com/en/US/tech/CK436/CK428/technologies_white_paper09186a00800a3e69.shtml

QUESTION 400

What is an LSP known as in an MPLS network?

- A. Label Switched Pair

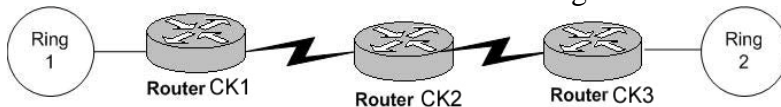
- B. Label Switched Path
- C. Link Switch Path
- D. Liability Switched Pair
- E. Label Switched Protocol
- F. Link State Path

Answer: B

Explanation: The MPLS traffic engineering Internet Protocol (IP) explicit address exclusion feature provides a means to exclude a link or node from the path for an MPLS traffic engineering label-switched path (LSP). MPLS networks consist of Label Switched Paths that are used as the means to transfer data.

QUESTION 401

The Certkiller network includes three routers: Router CK1 , Router CK2 and Router CK3 . The network is shown in the following exhibit:



There are DLSW+ peers between Router CK1 and Router CK2 , as well as between Router CK2 and Router CK3 . Router CK1 uses virtual ring number 50, while Router CK2 and Router CK3 use virtual ring number 70. Certkiller users on Ring 1 complain that they cannot reach hosts on Ring 2. All DLSW peers show a state of CONNECT.

What could be the cause of this problem?

- A. The dlsw bridge-group command on Router CK3 does not match the virtual ring number.
- B. Router CK2 and Router CK3 cannot have the same virtual ring number.
- C. Router CK1 must have a virtual ring number of 70.
- D. The ring numbers must be the same.

Answer: C

Explanation:

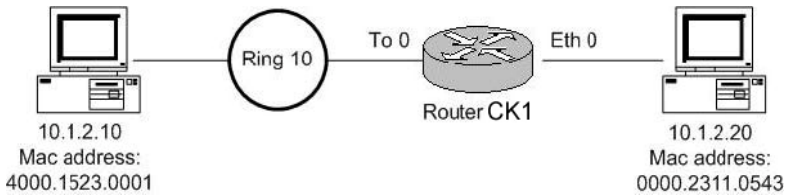
DLSW requires a single virtual-ring. Routers CK2 and CK3 are both configured for ring 70, so changing CK1 to 70 will fix the problem.

Incorrect Answers:

- A. The number associated with the bridge group does not necessarily have to match the virtual ring numbers.
- B. All routers within the virtual ring must share the same virtual ring number.
- D. The end ring numbers (ring 1 and ring 2) should be different.

QUESTION 402

You are the network administrator at Certkiller . The Certkiller network is shown in the following exhibit:



You perform the following configuration on Router CK1 :

Router CK1 :

no ip routing

!

source-bridge ring-group 111

source-bridge transparent 100 200 1 1

!

interface Ethernet 0

no ip address

bridge-group 1

!

InterfaceToken ring 0

no ip address

source-bridge 10 1 111

source-bridge spanning

!

bridge 1 protocol ieee

bridge 1 bitswap-layer3-addresses

What will happen to the frame if a non source route ARP Request that is sourced by 10.1.2.10 and destined to 10.1.2.20?

- A. Router CK1 would bitswap the MAC addresses before forwarding the frame out of the Ethernet.
- B. Router CK1 would forward the ARP request as is to the Ethernet interface within the frame.
- C. Router CK1 will not be able to forward the frame because it is not source routable.
- D. Router CK1 would cache the Routing Information Field (RIF), bitswap the MAC addresses then forward the frame out of the Ethernet.

Answer: C

Explanation:

In SR/TLB for a request from the TR side to be able to reach the Ethernet side it is essential that the source route information be included in the request packets. If a nonsource routable request is encountered then it will be dropped, as the SR/TLB will not be able to act upon it due to the lack of source route information.

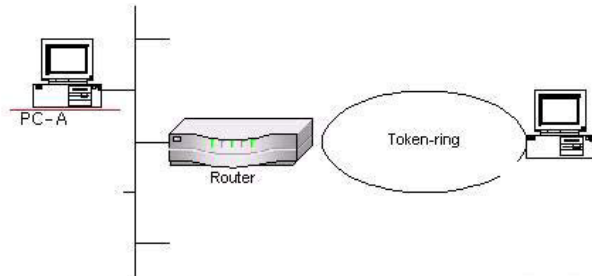
Incorrect Answers:

A, B, D. The following example describes the 3 ways in which communication between these hosts can be achieved. Solution 3 is close to the configuration in this question, but as you can see the Token Ring will need to be included in the bridge-group, which it is

not.

Example:

Problem



Ethernet and Token Ring topologies read MAC addresses differently. For example, a MAC address of 4040.4040.4040 on Ethernet is read as 0202.0202.0202 on Token Ring. When a device on one media pings to a device on the other media and the Cisco device is acting as a transparent bridge, the Address Resolution Protocol (ARP) response has data in the higher layer of the response that is not bitflipped. For example, PC-A's MAC address is 4040.4040.4040 on Ethernet, and pings to PC-B with a MAC address of 1234.5678.9abc. On Token Ring, the ARP request is read leaving PC-A on Ethernet sourced from 4040.4040.4040 and destination to FFFF.FFFF.FFFF. The Cisco device will bitflip the MAC addresses and send the ARP request to the Token Ring, and the frame will be read as sourced from 0202.0202.0202 to destination FFFF.FFFF.FFFF.

PC-B will now reply with the ARP reply sourcing the frame from 1234.5678.9abc to destination 0202.0202.0202 and will add into the data portion of the frame the IP address of PC-B, as associated with MAC address 1234.5678.9abc. The ARP reply will be bridged through the Cisco device and delivered onto the Ethernet with a source MAC address of 482c.6a1e.593d, and to a destination of 4040.4040.4040. The problem resides in the fact the data returned in the ARP reply indicates to PC-A that the MAC address of PC-B is 1234.5678.9abc. PC-A believes it knows the MAC address of PC-B and sends the Internet Control Message Protocol (ICMP) to the 1234.5678.9abc MAC address and not to the bitflipped version of PC-B's address, which would be 482c.6a1e.3d.

Solution(s)

The bridge x bitswap-layer3-addresses command resolves this inconsistency by changing the ARP reply data to match the bitflipping at the source and destination MAC addressing. When this command is issued, the router will change the ARP reply's data indicating PC-B's MAC address is 1234.5678.9abc to the Ethernet version of 482c.6a1e.593d. PC-B will reply normally, but the Cisco device will alter the packet as it is delivered onto the Ethernet so that the source MAC address matches the data portion of the ARP reply.

The bitswap-layer3-addresses command only resolves IP ARP.

Since Dynamic Host Configuration Protocol (DHCP) / Bootstrap Protocol (BOOTP) requests usually include MAC addressing in the data portion of the requests, this implementation does not accommodate DHCP or BOOTP requests through the Cisco router. The IPX protocol suffers from the same issue as described above with MAC addressing, however bitswap-layer3-addresses do not include IPX. Therefore, IPX should be routed on the Cisco device and is an independent configuration. For Layer 2 (L2) protocols, such as Netbios not encapsulated into IP, Systems Network Architecture (SNA), and DLC, a Source-Route Bridging (SRB) configuration should be used. The IPX is an independent protocol configuration.

Solution 1

In the most simple case, the configuration below on the router allows IP communication for devices through the router.

no ip routing

interface ethernet0

```
bridge-group 1
interface tokenring0
bridge-group 1
bridge 1 protocol ieee
bridge 1 bitswap-layer3-addresses
```

Solution 2

IPX routing is added to the configuration. Novell server(s) on the respective media will have different external network numbers and these numbers will be configured on the Cisco device to match these external network numbers. Networks 1 and 2 are used as examples. Of course, the internal network numbers must be unique in the network.

```
no ip routing
ipx routing
interface ethernet0
bridge-group 1
ipx network 1
interface tokenring0
bridge-group 1
ipx network 2
bridge 1 protocol ieee
bridge 1 bitswap-layer3-addresses
```

Solution 3

For solutions requiring IP connectivity for IP and SNA/DLC/NetBIOS connectivity, the bitswap-layer3-addresses command is issued to pass the IP traffic, and a SRTLB configuration is used to bridge the L2 protocols. Again, the numbers used are arbitrary and are used for the sample configurations. In most cases, the most important number in this sample configuration is the ring-number used on the Token Ring interface. It is vital that all devices are configured to indicate the same physical ring number. In this configuration, the ring number is configured to be 10 or hexadecimal 0xA.

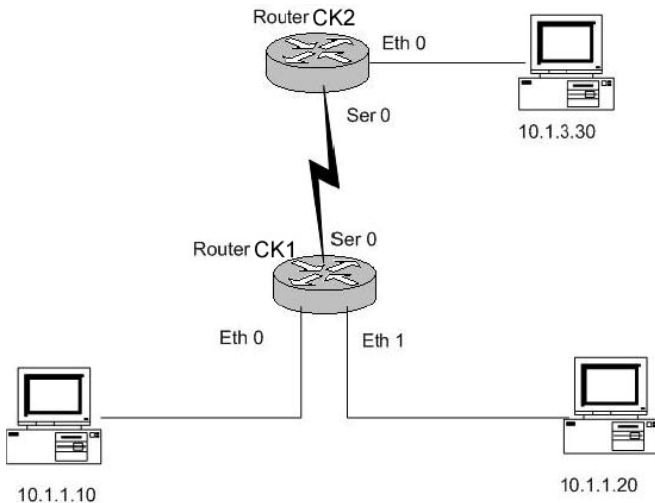
```
no ip routing
source-bridge ring-group 999
source-bridge transparent 999 998 2 1
interface Ethernet0
bridge-group 1
interface tokenring0
bridge-group 1
source-bridge 10 1 999
source-bridge spanning
bridge 1 protocol ieee
bridge 1 bitswap-layer3-addresses
```

Reference:

http://www.cisco.com/en/US/tech/CK331/CK660/technologies_tech_note09186a008012811e.shtml

QUESTION 403

The Certkiller network consists of 2 routers and 3 end stations as shown in the following exhibit:



You perform the following configuration:

Router CK1 :

```
bridge irb
```

```
!
```

```
interface Ethernet 0
```

```
no ip address
```

```
bridge-group 1
```

```
!
```

```
interface Ethernet 1
```

```
no ip address
```

```
brige-group 1
```

```
!
```

```
interface serial 0
```

```
ip address 10.1.2.1 255.255.255.0
```

```
!
```

```
interface BVI 1
```

```
ip address 10.1.1.1 255.255.255.0
```

```
no ip directed-broadcast
```

```
!
```

```
router eigrp 1
```

```
network 10.1.0.0
```

```
!
```

```
bridge 1 protocol ieee
```

```
bridge 1 route ip
```

Router CK2 :

```
interface Ethernet 0
```

```
ip address 10.1.3.1 255.255.255.0
```

```
!
```

```
interface serial 0
```

```
ip address 10.1.2.2. 255.255.255.0
```

```
!
```

```
router eigrp 1
```

```
network 10.1.0.0
```


If a user on the station with IP address 10.1.1.10 tries to FTP data to the station located at 10.1.3.30. Based on the above information, router CK1 will forward these TCP data packets out which interface?

- A. Both Serial 0 and Ethernet 1.
- B. Only Serial 0.
- C. Only Ethernet 1.
- D. Router CK1 will not forward the packets out of any interface.

Answer: B

Explanation:

Integrated routing and bridging makes it possible to route a specific protocol between routed interfaces and bridge groups, or route a specific protocol between bridge groups. Local or unroutable traffic can be bridged among the bridged interfaces in the same bridge group, while routable traffic can be routed to other routed interfaces or bridge groups.

When you enable routing for a given protocol on the bridge-group virtual interface, packets coming from routed interface, but destined for a host in a bridged domain, are routed to the bridge-group virtual interface and are forwarded to the corresponding bridged interface. All traffic routed to the bridge-group virtual interface is forwarded to the corresponding bridge group as bridged traffic. All routable traffic received on a bridged interface is routed to other routed interfaces as if it is coming directly from the bridge-group virtual interface.

Since the FTP packets are routable packets, it will be routed to other routed interface as described above.

Reference:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ibm_c/bcprt1/bcdtb.htm

QUESTION 404

Both bridging and DLSW are configured on router CK1 . CK1 receives packets via DLSW that are destined for a host on the local Ethernet attached to CK1 , but the packets are unable to reach the host. What could be the reason this?

- A. The DLSW+ peer cost doesn't match the Ethernet bridge group peer cost.
- B. SRTLB should be configured between the source route Virtual Ring and the Ethernet.
- C. The DLSW+ bridge-group command was not configured.
- D. The bridge-group value on the Ethernet is too low.
- E. All of the above are potential reasons.

Answer: C

Explanation:

Use the dlsw bridge-group global configuration command to link DLSw+ to the bridge

group of the Ethernet LANs.

The bridge-group needs to be configured on both the DLSW process and the Ethernet in order for hosts on that Ethernet segment to receive and send SNA data across the DLSW network.

Incorrect Answers:

A. The DLSW peer cost is needed for the Spanning Tree Protocol, but the cost does not need to match.

B. DLSW does perform frame translation, so SRTLb is not needed.

D. The bridge group number has local significance only and should match between bridged interfaces. In this case there is just one Ethernet segment on CK1 that is part of the bridge group.

QUESTION 405

Which of the following statements are true regarding Integrated Routing and Bridging (IRB)? (Choose all that apply)

A. IRB will allow the same protocol to be bridged and routed through a single physical interface.

B. IRB makes use of a virtual interface for connectivity between bridges and routed interfaces.

C. IRB can support multiple protocols on the same router.

D. IRB allows the same protocol to be bridged and routed on the same router.

Answer: B, C, D

Explanation:

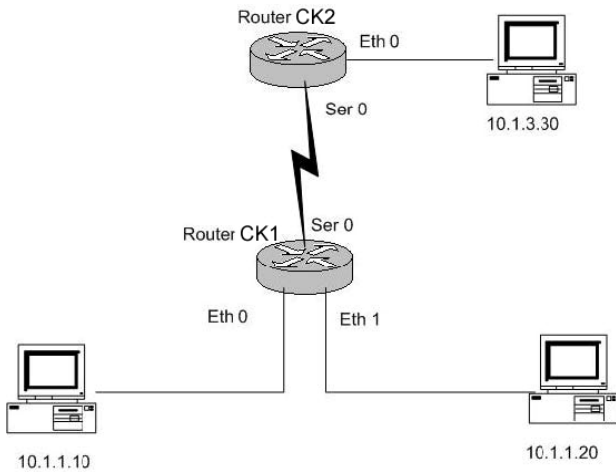
Integrated Routing and Bridging (IRB), allows you to route a given protocol between routed interfaces and bridge groups within a single switch router. IRB provides multiprotocol support for bridging and routing on the same router through the use of a virtual BVI interface.

Incorrect Answers:

A. IRB allows the same protocol to be bridged and routed through the virtual interface, not through the same physical interface.

QUESTION 406

The Certkiller network consists of 2 routers and 3 stations as shown in the following exhibit:



Router CK1 is configured as follows:

```
bridge irb
!  
interface Ethernet 0  
no ip address  
bridge-group 1  
!  
interface Ethernet 1  
no ip address  
brige-group 1  
!  
interface serial 0  
ip address 10.1.2.1 255.255.255.0  
!  
interface BVI 1  
ip address 10.1.1.1 255.255.255.0  
no ip directed-broadcast  
!  
router eigrp 1  
network 10.1.0.0  
!  
bridge 1 protocol ieee  
bridge 1 route ip
```

Router CK2 is configured as follows:

```
interface Ethernet 0  
ip address 10.1.3.1 255.255.255.0  
!  
interface serial 0  
ip address 10.1.2.2. 255.255.255.0  
!  
router eigrp 1  
network 10.1.0.0
```

The network has just been brought up. You supervisor asks you how Router CK1 would forward a broadcast if device 10.1.1.10 sends a UDP broadcast to

FFFF.FFFF.FFFF at the MAC layer. Which interface will router CK1 use to forward this broadcast message?

- A. Both Serial 0 and Ethernet 1.
- B. Ethernet 1 only.
- C. Serial 0 only.
- D. Router CK1 will not forward the UDP broadcast out any interface.

Answer: B

Explanation:

By default, routers do not forward any broadcast traffic out any interface. In this case, IRB is configured so both Ethernet segments appear as one single bridge group. Integrated routing and bridging makes it possible to route a specific protocol between routed interfaces and bridge groups, or route a specific protocol between bridge groups. Local or unroutable traffic can be bridged among the bridged interfaces in the same bridge group, while routable traffic can be routed to other routed interfaces or bridge groups.

When you enable routing for a given protocol on the bridge-group virtual interface, packets coming from routed interface, but destined for a host in a bridged domain, are routed to the bridge-group virtual interface and are forwarded to the corresponding bridged interface. All traffic routed to the bridge-group virtual interface is forwarded to the corresponding bridge group as bridged traffic. All routable traffic received on a bridged interface is routed to other routed interfaces as if it is coming directly from the bridge-group virtual interface. S0 is a routing port and will not forward broadcasts.

QUESTION 407

Your DLSW routers show a state of CONNECT. What must these routers have accomplished in order to achieve this state?

- A. Both routers must have sent test frame broadcasts to each other.
- B. Both peers must have finished their Capabilities Exchange.
- C. Both routers must have had their CUR/ICR information exchanged.
- D. Nothing - there is no such stage as a "CONNECT" state.

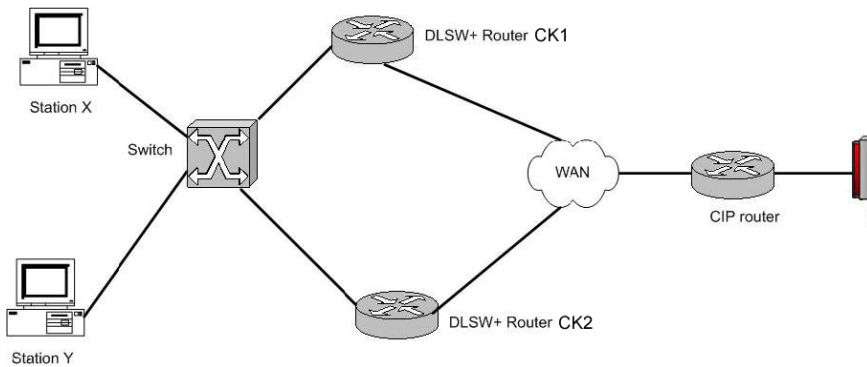
Answer: B

Explanation:

DLSW peers enter the connect state after the capabilities exchange.

QUESTION 408

The Certkiller network consists of two end stations in VLAN A that are connected via Data Link Switching Plus (DLSW+) routers. The DLSW+ routers have peers to the Channel Interface Processor (CIP) router. The Certkiller network is shown in the following exhibit:



SNA sessions from the stations to the host drop periodically even though IP connectivity is not affected. Both DLSW+ routers show they can reach the Host. Which DLSW+ feature can you use to fix the problem?

- A. Load Balancing.
- B. Ethernet Redundancy.
- C. Equal Cost Multi-path routing.
- D. Static Paths.
- E. All of the above.

Answer: B

Ethernet Redundancy with switch devices requires further changes because of the way in which switches handle and direct traffic. Switches direct traffic by observing a frame's SMAC and by observing from which port the frame arrives. They forward all traffic to a particular address from a specific port rather than flooding all of its ports. In a normal Ethernet environment, this method is sufficient because there can only be one unique path to any MAC address. However, this method does not work in an environment where there are multiple DLSW+ routers on the same transparent bridged domain that can reach the same MAC address.

Because Routers CK1 and CK2 are hooked to different ports on the Ethernet switch, the switch sees traffic from one SMAC coming into multiple ports. The Ethernet switch thinks the MAC address of the Host appears on two different places on a LAN. This design breaks the Ethernet rule of having only one path to any MAC address. It gives the appearance of a bridging loop that the Spanning-Tree Protocol did not resolve. Because SNA is connection oriented, the session is eventually torn down.

The DLSw+ Ethernet Redundancy feature solves this problem with MAC address mapping. MAC address mapping ensures that a particular SMAC is seen by the switch on only one port at a time. Furthermore, the routers monitor each other's MAC address mapping so that they adequately serve as each other's back up in the case of a router failure.

Incorrect Answers:

A. In Cisco IOS Release 12.0(3)T, the `dls w load-balance` command replaced the `dls w duplicate-path-bias load-balance` command. Although the `dls w duplicate-path-bias load-balance` command continues to be accepted, it is converted to the new command if the configuration is displayed or saved. As with the `dls w duplicate-path-bias load-balance` command, how the cache entries are used depends on which keyword (round-robin or

circuit count) is specified.

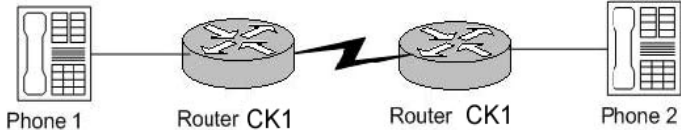
C. This would affect the IP routing, which as stated was not an issue.

Reference:

http://www.cisco.com/warp/public/cc/pd/ibsw/ibdlsw/prodlit/dls12_rg.htm

QUESTION 409

The Certkiller network is shown in the following exhibit:



You wish to give Phone 1 the ability to place a VOIP call to Phone2.

What must you configure on Router CK1 in order to do this?

- A. dial-peer voice 3 voip
destination-pattern 5550303
session target 10.10.10.1
- B. dial-peer voice 5550303 voip
destination-number 3
session target ip 10.10.10.1
- C. dial-peer voice 3 voip
destination-pattern ipv4: 10.10.10.1
session target voice
- D. dial-peer voice 3 voip
destination-pattern 5550303
session target ipv4: 10.10.10.1

Answer: D

D is the correct syntax.

QUESTION 410

What is the maximum round trip delay that is recommended by the ITU for VOIP applications?

- A. 300 milliseconds
- B. 3 seconds
- C. 150 milliseconds
- D. 140 milliseconds
- E. 15 milliseconds

Answer: A

Explanation:

300 ms is the recommended maximum delay for round trip traffic.

Incorrect Answers:

- C. 150 ms is the recommended one-way round trip delay.
-

QUESTION 411

Which of the following are associated with Signaling System No. 7? Choose all that apply.

- A. TCAP
- B. MTP
- C. ISUP
- D. SIP
- E. SCCP

Answer: A, B, C, and E

Explanation:

TCAP, MTP, ISUP, and SCCP are all functions of SS7, which is the signaling protocol used primarily for legacy voice applications.

Incorrect Answers:

D. SIP is the Session Initiation Protocol, which is a protocol used for voice and video applications over IP. It is not associated with SS7.

QUESTION 412

Which mechanism will be the best choice to prioritize any audio and video clips that are served by a web server over the static content such as text and graphics as integral parts of http flow?

- A. LLC
- B. CBWFQ
- C. WRED
- D. NBAR
- E. LFI
- F. FIFO

Answer: D

Explanation:

Network-Based Application Recognition (NBAR) solves this problem by adding intelligent network classification to network infrastructures. NBAR is a new classification engine that recognizes a wide variety of applications; including web-based and other difficult-to-classify protocols that utilize dynamic TCP/UDP port assignments. When an application is recognized and classified by NBAR, a network can invoke services for that specific application. NBAR ensures that network bandwidth is used efficiently by working with QoS features.

Incorrect Answers:

- A. LLC is a sub layer of the OSI data link layer. It has nothing to do with classifying content as described in this question.
- B, C, F. These are all different methods of quality of service and queuing, but they will

not provide the type of service needed, which is to dynamically allocate bandwidth for the needed applications.

E. LFI is Link Fragmentation and Interleaving, which is an important component for making sure that the serialization delay is not too long as to affect the relatively small voice and video packets. However, this technology alone is not able to provide for prioritization of the audio and video clips on the website.

Reference:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e2/nbar2e.htm>

QUESTION 413

A 6509 with inline power is used to power IP phones for a VOIP network. You issue the "show environment power" command as shown below:

6509A (enable) show environment power

PS1 Capacity 1153.32 Watts (27.46 Amps @42V)

PS2 Capacity 1153.32 Watts (27.46 Amps @42V)

PS Configuration: PS1 and PS2 in Redundant Configuration.

Total Power Available: 1153.32 Watts (27.46 Amps @42V)

Total Power Available for line Card Usage: 1153.32 Watts (27.46 Amps @42V)

Total Power Drivers From the System: 952.98 Watts (22.69 Amps @42V)

Remaining Power in the System: 200.34 Watts (4.77 Amps @42V)

Default Inline Power allocation per point: 7.00 Watts (0.16 Amps @42V)

You want the power supplies to continue to operate in redundant mode after the task is complete. There are currently no IP phones plugged into this switch.

However, there are various devices that are connected to the switch now and must remain plugged in. Based on this information, how many IP phones can receive power from this switch?

- A. None
- B. 7
- C. 28
- D. 48
- E. 164

Answer: C

Explanation:

Remaining Power in system = 200.34

Default Line Power per point = 7 W

Number of IP phones=200.34/7 = 28

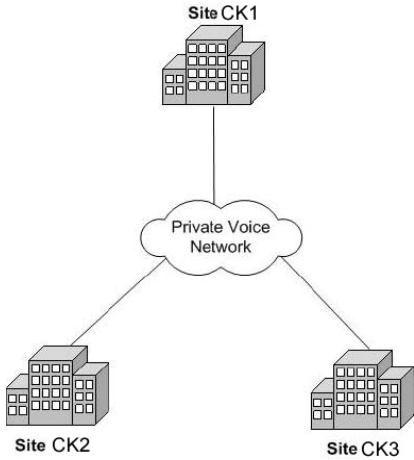
Incorrect Answers:

B. Each device requires 7 watts, not 7 IP phones for available capacity.

E. Here we need to look at the remaining power in the switch, which is 200.34 Watts. 164 would be the answer if we were to use the total power available of 1153.32 watts.

QUESTION 414

The Certkiller 3 site VOIP network is outlined below:



Some Certkiller users on Site CK1 complain that voice calls from Site CK2 and Site CK3 are loud and distorted. Meanwhile, Certkiller users on Site CK3 complain that voice calls from Site CK1 are too soft and hard to hear.

Which of the following will fix these problems? (Choose all that apply)

- A. Apply padding outbound to site CK2 .
- B. Apply padding inbound to Site CK1 .
- C. Apply gain inbound to Site CK3 .
- D. Apply gain outbound from Site CK1 .
- E. Apply gain inbound to site CK2 .

Answer: C, D, and E

Explanation:

Increase the volume. You can increase the gain of a signal coming into the router. If the voice level is too low, you can increase the input gain by using the input gain command. In this case we need to apply gain inbound on CK3 and CK2 , as well as outbound gain on site CK1 .

Incorrect Answers:

A, B. In this case we only need to apply gain. Padding will not help fix the problems associated with this example.

QUESTION 415

Which ISUP message is sent first by an SS7 switch while establishing a call?

- A. A RLC
- B. An IAM
- C. A REL
- D. An ACM

Answer: B

Explanation:

IAM (Initial Address Message) is the first message sent by an SS7 switch during call establishment.

Incorrect Answers:

A. An RLC is a Release Complete message, and is sent in response to acknowledge a REL.

C. An REL is a Release message, and is sent when either party hangs up the call.

D. An ACM is an address Complete Message, and is sent in the backward direction to indicate that the remote end of a trunk has been reserved

Reference:

http://www.cisco.com/en/US/partner/products/hw/switches/ps2246/products_preinstallation_guide_chapter09186a00800ea6d4.html

QUESTION 416

In your Voice over IP network, you wish to deploy the codec that will enable you to conserve the most bandwidth. Which of the following codec should you use?

A. G.729

B. G.723

C. GSM

D. G.711

E. G.728

Answer: B

G.723 is the most bandwidth efficient codec available today.

Incorrect Answers:

A, C, D, E. The other codecs consume more bandwidth than G.723. The most bandwidth intensive codec is G.711, as it consumes over 80Kbps per call.

Reference:

http://www.cisco.com/en/US/partner/tech/CK652/CK698/technologies_tech_note09186a0080094ae2.shtml

QUESTION 417

H.225 is responsible for Call Signaling as a subset of the H.323 specification. Which OSI model layer is H.225 associated with?

A. Application

B. Presentation

C. Session

D. Transport

E. Network

F. Data-Link

G. Physical

Answer: C

Explanation:

H.323 and the subset H.225 is above TCP or UDP in OSI-layer 5, which is the session layer.

OSI Layer	OSI Layer Name	VoIP Protocol and Function :
7	Application:	NetMeeting/Applications
6	Presentation:	CODECSs
5	Session:	H.323/MGCP/SIP
4	Transport:	RTP/TCP/UDP
3	Network:	IP
2	Data Link:	Frame Relay, ATM, Ethernet, PPP, etc.

H.323-the International Telecommunication Union-Telecommunications Standardization Sector (ITU-T) specification for sending voice, video, and data across a network. The H.323 specification includes several related standards, such as H.225 (call control), H.235 (security), H.245 (media path and parameter negotiation), and H.450 (supplementary services).

MGCP-Media Gateway Control Protocol, an Internet Engineering Task Force (IETF) draft standard for controlling voice gateways through IP networks.

SIP-Session Initiation Protocol, defined in IETF RFC 2543.

QUESTION 418

Which of the following special characters is used as a wildcard in a destination pattern string?

- A. pound sign (#)
- B. dash (-)
- C. asterix (*)
- D. period (.)
- E. plus (+)
- F. comma (,)

Answer: D

Explanation:

The string is a series of digits that specify the E.164 or private dialing plan telephone number. Valid entries are the digits 0 through 9 and the letters A through D. The period (.) can be used as a trailing character, and is used as a wildcard character.

Incorrect Answers:

A, C. The star character (*) and the pound sign (#) that appear on standard touch-tone dial pads can be used in any dial string. However, these characters cannot be used as leading characters in a string (for example, *650).

B. The dash is not used

E. The plus symbol (+) can be used to indicate an E.164 standard number.

F. The comma (,) can be used only in prefixes, and is used to insert a one-second pause or a delay

QUESTION 419

In VOIP, which of the following operate at layer 4 of the OSI model?

- A. MGCP
- B. SIP
- C. H323
- D. RTP
- E. None of the above

Answer: D

Explanation:

Layer 4 is the transport layer. The various layers associated with multimedia are shown below:

Presentation: ---

G.729(A)/G.723.1/G.711

Session: H.323/SIP/SDP

Transport: RTP/UDP/RSVP

Network: IP/WFQ/IP-prec

DataLink: CRTP/MP

Physical --- ---

Incorrect Answers:

B, C. SIP and H.323 operate at layer 5 (Session layer) of the OSI model.

QUESTION 420

Of the following, which IETF protocol is used by SIP for the purpose of call routing?

- A. BGP
- B. SAP
- C. EIGRP
- D. TRIP
- E. OSPF
- F. RIP

Answer: D

Explanation:

This explanation presents the Telephony Routing over IP (TRIP). TRIP is a policy driven inter-administrative domain protocol for advertising the reachability of telephony destinations between location servers, and for advertising attributes of the routes to those destinations. TRIP's operation is independent of any signaling protocol, hence TRIP can serve as the telephony routing protocol for any signaling protocol. The Border Gateway Protocol (BGP-4) is used to distribute routing information between administrative domains. TRIP is used to distribute telephony routing information between telephony administrative domains. The similarity between the two protocols is obvious, and hence

TRIP is modeled after BGP-4.

The Border Gateway Protocol (BGP-4) is used to distribute routing information between administrative domains. TRIP is used to distribute telephony routing information between telephony administrative domains. The similarity between the two protocols is obvious, and hence TRIP is modeled after BGP-4.

Routing protocols for VoIP allow intermediaries, such as SIP proxies and H.323 gatekeepers, to make call routing decisions based on reachability information learned from peer elements. The iptel group has already defined a protocol, Telephony Routing over IP (TRIP), RFC 3219, which solves one aspect of this problem. Specifically, it handles the case where calls need to be routed between domains. It allows for the exchange of routing information between these providers, so that policies can be applied to the resulting data to create a forwarding information base.

Incorrect Answers:

A, C, E, F. These are all routing protocols, not IETF protocols. They are not used by SIP for call routing.

B. SAP is Session announcement protocol, which is used to assist in the advertisement of multicast sessions. It is not used specifically for call routing.

Reference: <http://www.iptel.org/info/players/ietf/numbering/>

QUESTION 421

Which ITU standard was developed to define a global phone numbering plan system and to specify country codes?

- A. G.124
- B. E.164
- C. E.124
- D. G.164
- E. None of the above

Answer: B

Explanation:

The objective of E.164 is to specify a methodology that will provide a standardized method for presenting the domestic numbering plans of all countries (i.e., each country's application of E.164). This recommendation also includes a method by which this information is made available to all interested parties as well as timely information on numbering plan changes that influence the routing, charging, and accounting of international telecommunications traffic.

- ITU-T Recommendation E.164: "The international public telecommunication numbering plan"
- Tied to treaty obligations (specific roles and obligations defined for ITU Member States and ITU-T TSB Director)
- defines number structure and functionality for four principal categories of numbers

Incorrect Answers:

- A. G.124 is not a defined ITU standard.
- C. E.124 deals with the discouragement of frivolous international calling to unassigned or vacant numbers answered by recorded announcements without charge. It does not relate to the worldwide numbering plan.
- D. G.164 deals with echo suppression.

QUESTION 422

You wish to specify the IP address of the terminating router for your VOIP configuration. Which command does this?

- A. destination address
- B. terminate gateway target
- C. session target
- D. dial-peer address
- E. session address
- F. destination port
- G. destination pattern

Answer: C

Explanation:

The following is a sample VOIP configuration. As you can see, the correct syntax for specifying the terminating gateway is "session target".

```
dial-peer voice 30 voip
destination-pattern 1111
session target ipv4:24.247.46.33
```

Incorrect Answers:

- A, B, E, F. These are all invalid commands.
- D. The dial peer command is used to specify the VOIP parameters, using following commands.
- G. The destination pattern command is used to specify the dialed digits, not the terminating gateway.

QUESTION 423

You have a Catalyst 6500 with a Supervisor IA with a MSFC. After a power outage, the MSFC has lost its boot image and now will only boot into ROMMON mode. You want to load a new image onto the Catalyst MSFC boot flash. What method can you use?

- A. Console connection using Xmodem
- B. FTP
- C. TFTP
- D. SNMP
- E. SSH

Answer: A

Explanation:

The Catalyst 6000 Supervisor I and II modules have an onboard Flash file system that can handle several image files. In addition to this Flash, they also have a PCMCIA Flash slot. These Supervisors run their software from RAM and do not need their Flash system once correctly booted up. If an image is then corrupted or deleted, the standard upgrade procedure is always possible as long as the Supervisor is running a valid image. If the Supervisor is not booting up because there is no valid image to boot from the ROMMON, you will have to use the recovery procedure.

1. Booting from a PCMCIA Flash Card

2. Console Download using Xmodem

In this situation option 2 is the only choice, since the MSFC has lost its boot image. Refer to the link below for a detailed discussion of recovery procedures for Catalyst Switches.

Reference:

http://www.cisco.com/en/US/products/hw/switches/ps663/products_tech_note09186a00800949c3.shtml#cat6k:

QUESTION 424

From the "show version" command you see that the system file image is c2500-js-l_121-7.bin. What IOS feature set is loaded on this router?

- A. Enterprise
- B. IP
- C. IP/IPX/AT/DEC
- D. Enterprise Plus
- E. IP Plus IPsec 3DES

Answer: D

Explanation:

The system image file name in the exhibit is c2500-js-l_121-12.bin

The table below shows the possible options

IOS feature	file name
IP Plus	c2500-is-l.121-7.bin
IP	c2500-i-l.121-7.bin
Enterprise Plus IPSEC 56	c2500- jk8s -l.121-7.bin
Enterprise Plus	c2500-js-l.121-7.bin
Enterprise	c2500-j-l.121-7.bin

QUESTION 425

You have forgotten the password to your Catalyst 5000 switch. Immediately after power cycling the switch, you are faced with the password prompt. What default password should you type in?

- A. cisco

- B. abc123
- C. sanfran
- D. CTRL+ESC
- E. No password, just hit the Enter key

Answer: E

Explanation:

Password recovery in Cat 5000 switch is performed in the following way. Power cycle the switch. Hit the Enter key during the first 30 sec. The switch will allow you to get into the enable mode. You will have 60 seconds to change the password and save the configuration change made during this period.

QUESTION 426

You have forgotten the password to a Catalyst switch and need to perform a password recovery. What is the first step that should be taken to do this?

- A. Reboot the switch using the reload command.
- B. Reboot the switch using the restart command.
- C. Set the configuration register to ignore the startup configuration.
- D. Set the boot register to 0x42.
- E. Power cycle the switch.
- F. Type in "config-register".

Answer: E

Explanation:

The switch must be manually turned off (or unplugged), and then turned back on (plugged back in). Power cycling the switch is the only way to get into password recovery.

Reference:

http://www.cisco.com/warp/public/474/pswdrec_6000.html

QUESTION 427

You need to upgrade the IOS on your Cisco router. What is the correct command needed to download the IOS image from a TFTP server with an IP address of 10.10.1.5/24?

- A. Copy tftp server from flash 10.10.1.5 "source file name" "destination file name" enter
- B. Copy flash tftp 10.10.1.5 255.255.255 "source-file-name" "destination-file-name" enter
- C. Copy tftp flash 10.10.1.5 "source-file-name" "destination-file-name" enter
- D. Copy flash tftp "source-file-name" "destination-file-name" 10.10.1.5 255.255.255.0 enter
- E. Copy tftp server 10.10.1.5 "destination-file-name" "source-file-name" enter

Answer: C

Explanation:

The correct syntax is copy tftp flash source-name destination-name as shown below:

Router# copy tftp: flash:

System flash partition information:

Partition Size Used Free Bank-Size State Copy-Mode

1 4096K 2048K 2048K 2048K Read Only RXBOOT-FLH

2 4096K 2048K 2048K 2048K Read/Write Direct

[Type ?<no> for partition directory; ? for full directory; q to abort]

Which partition? [default = 2]

**** NOTICE ****

Flash load helper v1.0

This process will accept the copy options and then terminate the current system image to use the ROM based image for the copy.

Routing functionality will not be available during that time.

If you are logged in via telnet, this connection will terminate.

Users with console access can see the results of the copy operation.

---- ***** ----

Proceed? [confirm]

System flash directory, partition 1:

File Length Name/status

1 3459720 master/igs-bfpx.100-4.3

[3459784 bytes used, 734520 available, 4194304 total]

Address or name of remote host [255.255.255.255]? 172.16.1.1

Source file name? master/igs-bfpx-100.4.3

Destination file name [default = source name]?

Loading master/igs-bfpx.100-4.3 from 172.16.1.111: !

Erase flash device before writing? [confirm]

Flash contains files. Are you sure? [confirm]

Copy 'master/igs-bfpx.100-4.3' from TFTP server

as 'master/igs-bfpx.100-4.3' into Flash WITH erase? [yes/no] yes

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_command_reference_chapter09186a008017d031.html#1030138

QUESTION 428

You are the network administrator at Certkiller . You want to gain access on Router CertK on the Certkiller network. The current configuration is shown in the following exhibit:

!

version 12.2

service timestamps log update

no service password-encryption

!

hostname CertK

!

enable secret 5 \$1\$XV53\$hqb0R7gwpky0\$

enable password sanfran

What must you type to gain access to Router CertK ?

A. cisco

B. CertK

C. sanfran

D. \$1\$XV53\$hqb0R7gwpky0\$

E. Enter key

F. Unable to be determined

Answer: F

Explanation:

The enable secret password takes precedence over the enable password. In this example, the enable secret is encrypted. You would need to type the unencrypted password to gain access. In the configuration file, you can tell that the enable secret command is encrypted due to the fact that the number 5 (for MD5) precedes the password.

Incorrect Answers:

B. CertK is simply the host name associated with the router. It has nothing to do with the password.

C. The enable secret password always overrides the enable password. Note that in this case the enable password is also normally encrypted (using a less secure type 7 encryption algorithm). However, since the "no service password-encryption" command was used, the normal enable password is shown in the clear. However, this does not apply to the enable secret password.

QUESTION 429

While troubleshooting an issue with one of the slots on your Cisco device, you issue the "show diag" command as shown below:

Router#show diag 10

Slot 10:

Physical slot 10, ~physical slot 0x5, logical slot 10, CBus 0

Microcode Status 0x4

Master Enable, LED, WCS Loaded

Board is analyzed

Pending I/O Status: None

EEPROM format version 1

VIP2 RSK controller, HW rev 2.02, board revision D0

Serial number: 17090200 Part number: 73-2167-05

Test history: 0x00 RMA number: 00-00-00

Flags: cisco 7000 board; 7500 compatible

EEPROM contents (hex):

0x20: 01 1E 02 02 01 04 C6 98 49 08 77 05 00 00 00 00

0x30: 68 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Slot database information:

Flags: 0x4 Insertion time: 0x18C0 (00:29:13 ago)

Controller Memory Size: 32 Mbytes DRAM, 4096 Kbytes SRAM

Based on the information above, what is the model of the Versatile Interface Processor (VIP)?

- A. VIP2.50
- B. VIP2.40
- C. VIP2-30
- D. VIP2-20
- E. VIP2-10

Answer: A

Explanation:

How to Identify the VIP2 Model

There are five different versions of the VIP2: the VIP2-10, the VIP2-15, the VIP2-20, the VIP2-40, and the VIP2-50. The VIP2-10, VIP2-15, VIP2-20, and VIP2-40 all use the same motherboard, but differ in the amount of DRAM and SRAM. You can upgrade to a higher performing VIP2 simply by upgrading the DRAM and SRAM.

The VIP2-50 uses a different motherboard and SDRAM and SRAM memory devices than the other VIP2 models; therefore, you cannot install VIP2-50 SDRAM or SRAM memory devices on the earlier VIP2 models, and you cannot install DRAM or SRAM memory devices from earlier VIP2 models on the VIP2-50. Also, you cannot use DRAM designated for the Route Switch Processor (RSP) on the VIP2 models.

Reference:

http://www.ciscosystems.lt/en/US/products/hw/routers/ps359/prod_module_installation_guide09186a00800fd116.html#108093

QUESTION 430

The modules of a Catalyst 6509 are shown below:

```
6509b> show module
Mod Slot Ports Module-Type      Model          Sub Status
-----
1 1 2  *000BaseX Supervisor  WS-X6K-SUP2-2GE  yes ok
15 1 1  Multilayer Switch Feature WS-F6K-MSFC2    no ok
2 2 2  *000BaseX Supervisor  WS-X6K-SUP2-2GE  yes standby
16 2 1  Multilayer Switch Feature WS-F6K-MSFC2    no ok
3 3 16  1000BaseX Ethernet    WS-X6516-GBIC   no ok
4 4 16  1000BaseX Ethernet    WS-X6516-GBIC   no ok
5 5 0   Switch Fabric Module  WS-C6500-SFM    no ok
7 7 16  1000BaseX Ethernet    WS-X6516-GBIC   no ok
8 8 16  1000BaseX Ethernet    WS-X6516-GBIC   no ok
```

The switch is currently running Hybrid code. You wish to convert this switch to native Cisco IOS. What is the correct IOS version needed to do this?

- A. c6sup12-jsv-mz.121-7a.E1.bin
- B. c6sup22-jsv-mz.121-8a.E3.bin
- C. c6msfc2-jsv-mz.121-7a.E1.bin
- D. cat6000-sup2.6-3-3.bin
- E. cat6000-sup6-3-3.bin

Answer: B

Explanation:

There are currently four different types of images for the Catalyst Native IOS, based on the MSFC and Supervisor installed. The naming convention is as follows:

C6supxy-Indicates the Supervisor/MSFC combination, where x=supervisor and y=MSFC.

The four types are:

1. c6sup-original name for the native IOS. Runs on the original supervisor 1, MSFC1.
2. c6sup11 - supervisor 1, MSFC 1
3. c6sup12 - supervisor 1, MSFC 2
4. c6sup22 - supervisor 2, MSFC 2

As you can see from the output on this question, the CAT has a SUP2/MSFC2, so option B is our only choice.

Supervisor Engine 2 with MSFC2 Software Images and Ordering Information

Product Number	Description	Image
S6S22AV-12113E	Cisco Catalyst 6000 and Cisco 7600 Supervisor Engine 2/MSFC2 Cisco IOS Enterprise with Versatile Interface Processor (VIP) Software Release 12.1(13)E1	c6sup22-jsv-mz.121-13.E1
S6S22ALV-12113E	Cisco Catalyst 6000 and Cisco 7600 Supervisor Engine 2/MSFC2 Cisco IOS Enterprise LAN Only Software Release 12.1(13)E1	c6sup22-js-mz.121-13.E1
S6S22AK2-12113E	Cisco Catalyst 6000 and Cisco 7600 Supervisor Engine 2/MSFC2 Cisco IOS Enterprise with VIP and 3DES Software Release 12.1(13)E1	c6sup22-jk2sv-mz.121-13.E1

Incorrect Answers:

- A. This would be the correct native IOS for a Catalyst with a supervisor 1.
- C. This is not using the correct naming convention used by Cisco.
- D, E. IOS that starts with cat6000 means that is Hybrid IOS.

QUESTION 431

You have lost the password to your Cisco 3550 switch. Which of the following choices display the correct order for resetting the password?

- A. Unplug power, Hold mode button down, Connect PC with terminal emulation software to console port, plug power in, issue flash_init, issue load_helper, issue rename flash:config.text flash:config.old, issue boot, issue no, issue enable, issue rename flash:config.old flash:config.text, reload
- B. Connect PC with terminal emulation software to console port, Unplug power, Hold mode button down, ,plug power in, issue flash_init, issue load_helper, issue rename flash:config.etxt flash:config.old, issue boot, issue no, issue enable, issue rename flash:config.old flash:config.text, issue config t, issue no enable secret, issue write mem
- C. Unplug power, Hold mode button down, plug power in, issue rename flash:config.text flash:config.old, issue boot, issue no, issue enable, issue rename flash:config.old flash:config.text, issue copy flash:config.text system runningconfig,

issue config t, issue no enable secret, reload

D. Connect PC with terminal emulation software to console port, Unplug power, plug power in, issue flash_init, issue load_helper, issue rename flash:config.text flash:config.old, issue boot issue no, issue enable, issue rename flash:config.old flash:config.text, issue copy flash:config.text system running-config, issue config t, issue no enable secret, issue write mem

E. Connect PC with terminal emulation software to console port, Unplug power, Hold mode button down, ,plug power in, issue flash_init, issue load_helper, issue rename flash:config.text flash:config.old, issue boot, issue no, issue enable, issue rename flash:config.old flash:config.text, issue copy flash:config.text system running-config, issue config t, issue no enable secret, issue write mem

Answer: E

Explanation:

The following is the complete step by step password recovery procedure for a Cisco 3550:

1. Attach a terminal or PC with terminal emulation (for example, Hyper Terminal) to the console port of the switch. Use the following terminal settings:

- Bits per second (baud): 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow Control: Xon/Xoff

Note: For additional information on cabling and connecting a terminal to the console port, refer to Connecting a Terminal to the Console Port on Catalyst Switches.

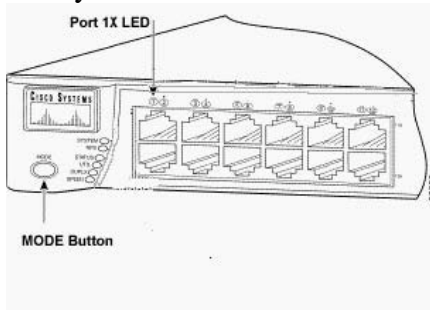
2. Unplug the power cable.

3. Hold down the mode button located on the left side of the front panel, while reconnecting the power cable to the switch.

For 2900/3500XL and 3550 Series switches: release the mode button after the LED above Port 1x goes out.

Note: LED position may vary slightly depending on the model.

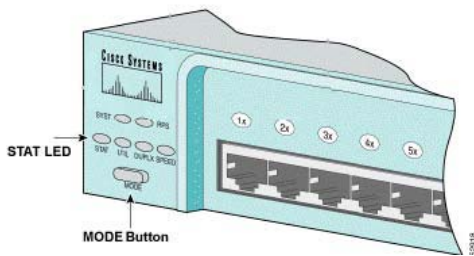
Catalyst 3524XL



For 2950 Series switches: release the mode button after the STAT LED goes out.

Note: LED position may vary slightly depending on the model.

Catalyst 2950-24



The following instructions appear:

The system has been interrupted prior to initializing the flash filesystem. The following commands will initialize the flash filesystem, and finish loading the operating system software:

```
flash_init
```

```
load_helper
```

```
boot
```

```
switch:
```

!--- This output is from a 3500XL switch. Output from a 2900XL, 2950 or 3550 will vary slightly.

4. Issue the flash_init command.

```
switch: flash_init
```

```
Initializing Flash...
```

```
flashfs[0]: 143 files, 4 directories
```

```
flashfs[0]: 0 orphaned files, 0 orphaned directories
```

```
flashfs[0]: Total bytes: 3612672
```

```
flashfs[0]: Bytes used: 2729472
```

```
flashfs[0]: Bytes available: 883200
```

```
flashfs[0]: flashfs fsck took 86 seconds
```

```
....done Initializing Flash.
```

```
Boot Sector Filesystem (bs:) installed, fsid: 3
```

```
Parameter Block Filesystem (pb:) installed, fsid: 4
```

```
switch:
```

!--- This output is from a 2900XL switch. Output from a 3500XL, 3550 or 2950 will vary slightly.

5. Issue the load_helper command.

```
switch: load_helper
```

```
switch:
```

6. Issue the dir flash: command.

The switch file system is displayed:

```
switch: dir flash:
```

```
Directory of flash:/
```

```
2 -rwx 1803357 <date> c3500xl-c3h2s-mz.120-5.WC7.bin
```

!--- This is the current version of software.

```
4 -rwx 1131 <date> config.text
```

!--- This is the configuration file.

```
5 -rwx 109 <date> info
```

```
6 -rwx 389 <date> env_vars
```

```
7 drwx 640 <date> html
18 -rwx 109 <date> info.ver
403968 bytes available (3208704 bytes used)
switch:
!--- This output is from a 3500XL switch. Output from a 2900XL,
2950 or 3550 will vary slightly.
7. Type rename flash:config.text flash:config.old to rename the configuration file.
switch: rename flash:config.text flash:config.old
switch:
!--- The config.text file contains the password definition.
8. Issue the boot command to boot the system.
switch: boot
Loading "flash:c3500xl-c3h2s-mz.120-
5.WC7.bin" ...#####
#####
#####
#####
#####
File "flash:c3500xl-c3h2s-mz.120-5.WC7.bin" uncompressed and
installed, entry po
int: 0x3000
executing...
!--- Output truncated.
!--- This output is from a 3500XL switch. Output from a 2900XL,
2950 or 3550 will vary slightly.
9. Enter "n" at the prompt to start the Setup program.
--- System Configuration Dialog ---
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Continue with configuration dialog? [yes/no]: n
!--- Type "n" for no.
Press RETURN to get started.
!--- press Return or Enter.
Switch>
!--- The Switch> prompt is displayed.
10. At the switch prompt type en to enter enable mode.
Switch>en
Switch#
11. Type rename flash:config.old flash:config.text to rename the configuration file
with its original name.
Switch#rename flash:config.old flash:config.text
Destination filename [config.text]
!--- Press Return or Enter.
Switch#
12. Copy the configuration file into memory:
```

```
Switch#copy flash:config.text system:running-config
Destination filename [running-config]?
!--- Press Return or Enter.
1131 bytes copied in 0.760 secs
Switch#
The configuration file is now reloaded.
13. Change the password:
Switch#configure terminal
Switch(config)#no enable secret
!--- This step is necessary if the switch had an enable secret
password.
Switch(config)#enable password Cisco
Switch#(config)#^Z
!--- Control/Z.
14. Write the running configuration to the configuration file with the write memory
command:
Switch#write memory
Building configuration...
[OK]
Switch#
```

QUESTION 432

The flash on your Cisco 2500 shows that it is running c2500-js-l_121-12.bin as the IOS. What IOS feature set is this?

- A. IP/IPX/AT/IBM
- B. IP
- C. Enterprise Plus IPSEC 3DES
- D. Enterprise Plus
- E. Enterprise

Answer: D

Explanation:

The system image file name in the exhibit is c2500-js-l_121-12.bin, so it's Enterprise Plus. The following table shows the possible IOS feature sets:

IOS feature	file name
IP Plus	c2500-is-l.121-12.bin
IP	c2500-i-l.121-12.bin
Enterprise Plus IPSEC 56	c2500- jk8s -l.121-12.bin
Enterprise Plus	c2500-js-l.121-12.bin
Enterprise	c2500-j-l.121-12.bin

Reference:

CCO login required

http://www.cisco.com/warp/customer/432/features.html#select_s