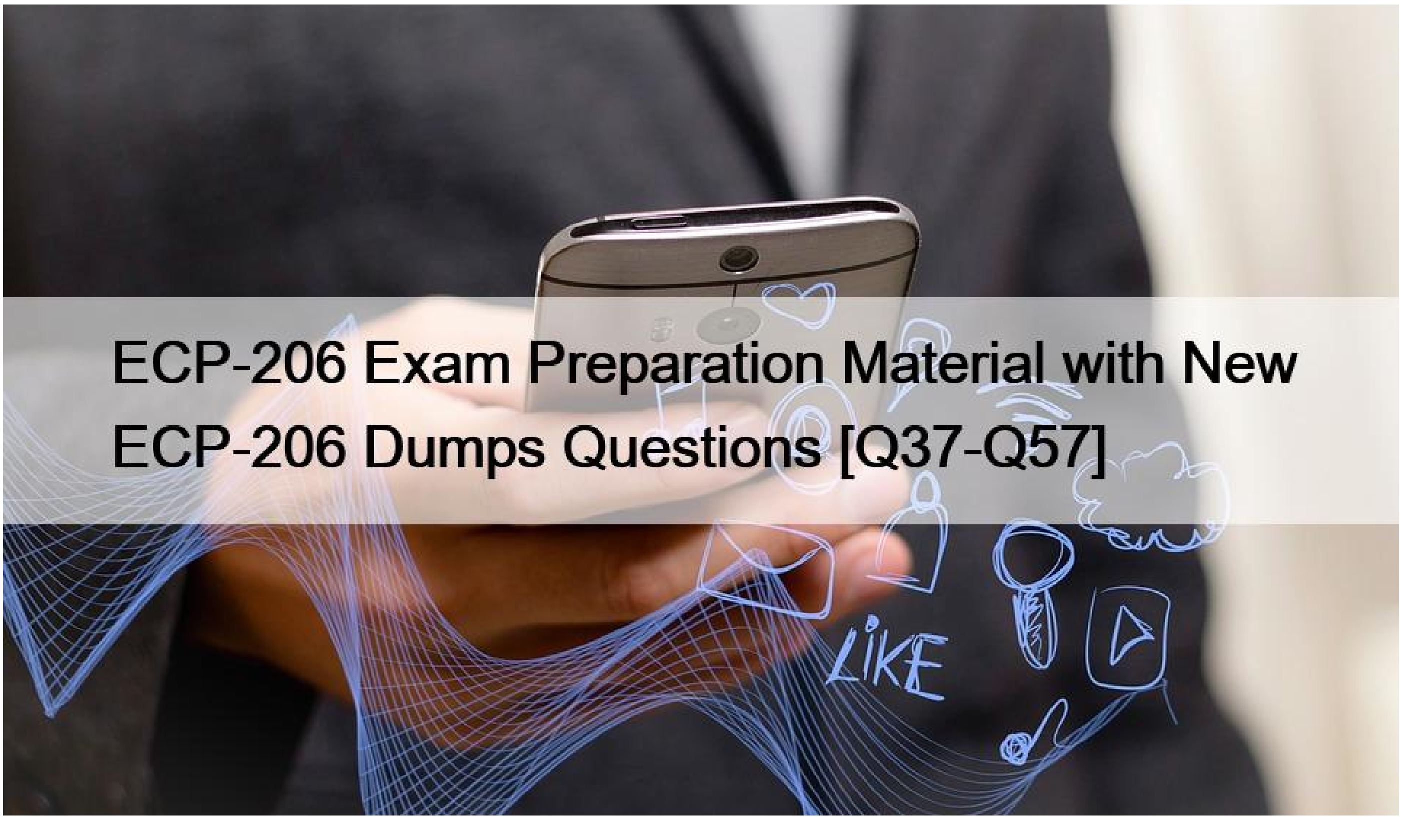
ECP-206 Exam Preparation Material with New ECP-206 Dumps Questions [Q37-Q57


ECP-206 Exam Preparation Material with New ECP-206 Dumps Questions [Q37-Q57]
LIKE

ECP-206 Exam Preparation Material with New ECP-206 Dumps Questions
ECP-206 2024 Training With 62 QA's

QUESTION 37

Which device will fragment IPv6 packets?
* source host
* router
* firewall
* destination host
Explanation

The device that will fragment IPv6 packets is the source host. Fragmentation is a process of dividing a large packet into smaller pieces that can fit the maximum transmission unit (MTU) of the network link. In IPv4, fragmentation can be performed by either the source host or any intermediate router along the path. However, in IPv6, fragmentation is only allowed at the source host, and routers are not allowed to fragment packets. This reduces the processing overhead and complexity at routers and avoids potential fragmentation attacks. If a router receives an IPv6 packet that is too large for the next-hop link, it will drop the packet and send an ICMPv6 Packet Too Big message back to the source host56.

References: IPv6 address &#8211; Wikipedia, IPv6 Fragmentation &#8211; Cisco

QUESTION 38

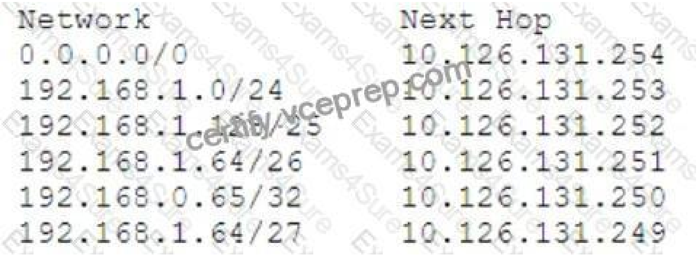
What is the function of LSR from an LDP perspective?
* The LSR distributes labels of LDP to its FEC peers.
* The LSR distributes packets of FEC to its LDP peers.
* The LSR distributes packets of LDP to its FEC peers.
* The LSR distributes labels of FEC to its LDP peers.
Explanation

The function of LSR from an LDP perspective is to distribute labels of FEC to its LDP peers. LSR stands for Label Switching Router, which is a router that forwards packets based on labels rather than IP addresses in an MPLS network. LDP stands for Label Distribution Protocol, which is a protocol that distributes labels for MPLS forwarding along the shortest path calculated by an IGP. FEC stands for Forwarding Equivalence Class, which is a group of packets that are forwarded in the same manner by an LSR. An LSR uses LDP to advertise the label mappings for each FEC to its LDP peers, which are other LSRs that have established an LDP session with it12.

References: Ldp | Microsoft Learn, Label Distribution Protocol &#8211; Wikipedia

QUESTION 39

Review the exhibit.



```
Network              Next Hop
0.0.0.0/0            10.126.131.254
192.168.1.0/24       10.126.131.253
192.168.1.128/25     10.126.131.252
192.168.1.64/26      10.126.131.251
192.168.0.65/32      10.126.131.250
192.168.1.64/27      10.126.131.249
```

Given the routing table shown in the exhibit, what is the next-hop to reach the host 192.168.1.129?
* 10.126.131.251
* 10.126.131.252
* 10.126.131.250
* 10.126.131.248
Explanation

The next-hop to reach the host 192.168.1.129 is 10.126.131.250. This can be determined by looking at the routing table in the exhibit. The host 192.168.1.129 falls within the range of the network 192.168.1.64/26, which has a next-hop of 10.126.131.250.
References: Ericsson IP Networking &#8211; IP Addressing, Software Installation and Upgrade Overview (Junos OS)

QUESTION 40

Which two protocols apply to both IPv4 and IPv6? (Choose two.)
* SNMP
* ARP
* DNS

* MD
Explanation

Two protocols that apply to both IPv4 and IPv6 are:

SNMP: This stands for Simple Network Management Protocol, which is a protocol that allows network administrators to monitor and manage network devices such as routers, switches, servers, printers, etc.

SNMP uses a client-server model, where an SNMP manager (client) can query or configure an SNMP agent (server) on a network device using SNMP messages. SNMP can operate over both IPv4 and IPv6 networks56.

DNS: This stands for Domain Name System, which is a protocol that translates human-readable domain names (such as www.example.com) into numerical IPaddresses (such as 192.0.2.1 or 2001:db8::1) that identify network devices. DNS uses a hierarchical distributed database of name servers that store and resolve domain names and IP addresses. DNS can support both IPv4 and IPv6 addresses78.

References: Simple Network Management Protocol &#8211; Wikipedia, SNMP over IPv6 &#8211; Cisco, Domain Name System &#8211; Wikipedia, DNS for IPv6 &#8211; Cisco

QUESTION 41

Which two statements are true about link-state routing protocols? (Choose two.)
* The advertisement exchange is mainly triggered by a change in the network.
* Each router uses a reliable update mechanism to exchange topology information with its neighbors.

C Link-state routing protocols mainly use hop-counts to determine the link cost
* A distance vector algorithm is very processor intensive compared to Dijkstra&#8217;s algorithm.
Explanation

Link-state routing protocols are one of the two main classes of routing protocols used in packet switching networks for computer communications, the other being distance-vector routing protocols. Examples of link-state routing protocols include Open Shortest Path First (OSPF) and Intermediate System to Intermediate System (IS-IS). The basic concept of link-state routing is that every node constructs a map of the connectivity to the network, in the form of a graph, showing which nodes are connected to which other nodes. Each node then independently calculates the next best logical path from it to every possible destination in the network.

Each collection of best paths will then form each node&#8217;s routing table.

Two statements that are true about link-state routing protocols are:

The advertisement exchange is mainly triggered by a change in the network. Link-state routing protocols use a flooding mechanism to distribute information about the network topology to all routers in the same area or domain. This information is encapsulated in link-state packets (LSPs) or link-state advertisements (LSAs), which contain information about the router, its directly connected links, and the state of those links. LSPs or LSAs are sent only when there is a change in the topology, such as a link failure or recovery, or when a periodic refresh timer expires. This way, link-state routing protocols can quickly adapt to network changes and maintain an accurate and consistent view of the network.

Each router uses a reliable update mechanism to exchange topology information with its neighbors.

Link-state routing protocols use a reliable update mechanism to ensure that all routers receive and acknowledge the LSPs or LSAs sent by their neighbors. This mechanism involves sending hello messages to establish and maintain adjacencies with neighbors, sending acknowledgment messages to confirm the receipt of LSPs or LSAs, and requesting missing or outdated LSPs or LSAs from neighbors.

This mechanism ensures that all routers have a synchronized database of LSPs or LSAs, which is used to build a complete network connectivity map and to calculate the shortest path to destinations.

References: Link-state routing protocol &#8211; Wikipedia, Ericsson IP Networking &#8211; Routing Protocols

QUESTION 42

Which route type is restricted in an OSPF stub area?
* Type 1
* Type 2
* Type 3
* Type 5
Explanation

The route type that is restricted in an OSPF stub area is type 5. Type 5 LSAs are external LSAs that are generated by ASBRs to advertise routes from other routing domains or protocols into OSPF. Type 5 LSAs are flooded throughout the OSPF domain by default, except in stub areas. Stub areas are special OSPF areas that block type 5 LSAs from entering the area in order to reduce the size of the LSDB and the routing table. Stub areas only receive information about intra-area routes (type 1 and 2 LSAs), inter-area routes (type 3 LSAs), and a default route (type 3 LSA with destination 0.0.0.0/0) from the ABRs910.

References: Introduction to OSPF Stub Areas &#8211; NetworkLessons.com, What Are OSPF Areas and Virtual Links? &#8211; Cisco

QUESTION 43

In an Ethernet frame carrying a VLAN tag, where does the VLAN tag appear?
* after the type field
* before the length field
* before the type field
* after the length field
Explanation

In an Ethernet frame carrying a VLAN tag, the VLAN tag appears before the type field. A VLAN tag is a

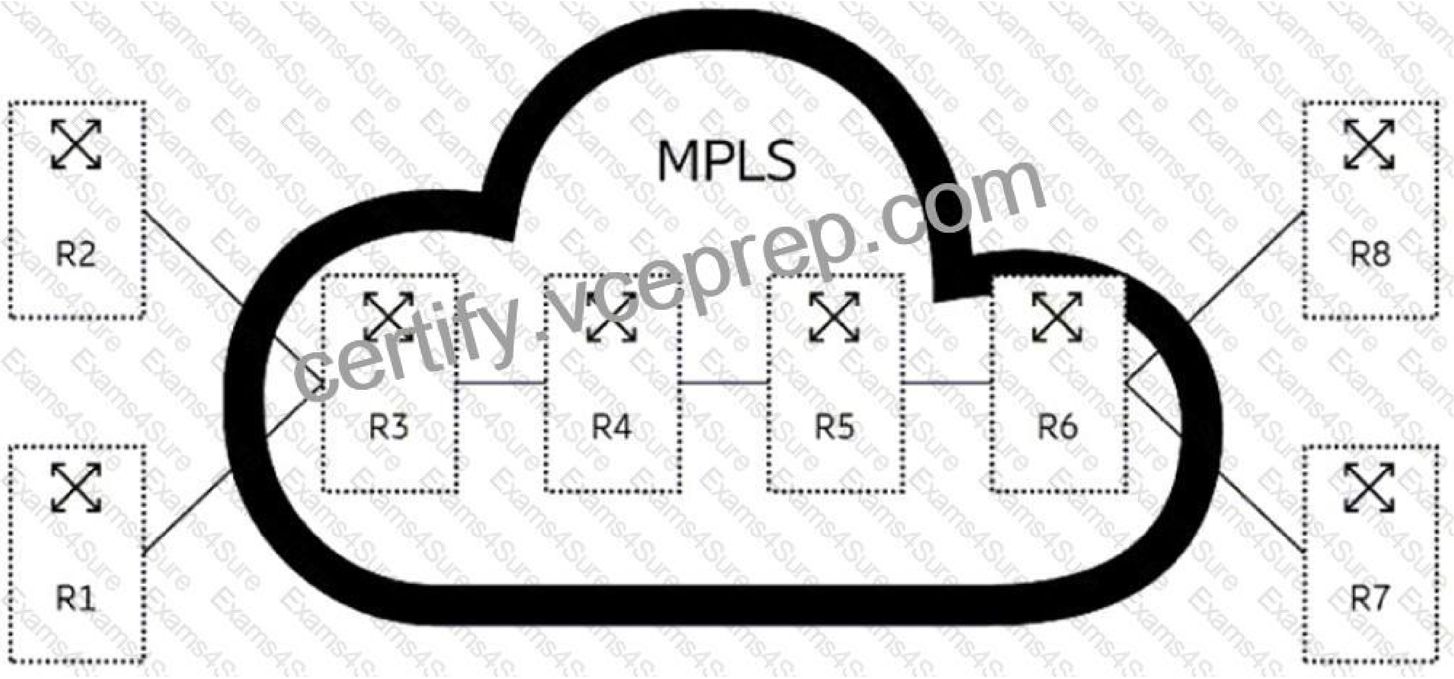
4-byte field that is inserted into an Ethernet frame to indicate the VLAN membership and priority of the frame.

The VLAN tag consists of two subfields: the tag protocol identifier (TPID) and the tag control information (TCI). The TPID subfield is a 16-bit field that identifies the frame as an IEEE 802.1Q-tagged frame, with a value of 0x8100. The TCI subfield is a 16-bit field that contains the priority code point (PCP), the drop eligible indicator (DEI), and the VLAN identifier (VID). The VLAN tag appears between the source MAC address and the type fields of the original frame, shifting the type field by four bytes. The type field indicates the type of the payload, such as IP or ARP .

References: [IEEE 802.1Q &#8211; Wikipedia], [VLAN Tagging Explained with DTP Protocol &#8211; GeeksforGeeks]

QUESTION 44

Review the exhibit.



In the exhibit, which action is performed by router R4?

* pop
* push
* PHP
* swap

Explanation

In the exhibit, router R4 is performing a swap action. This means that router R4 is replacing the incoming label with a new label and forwarding the packet to the next hop along the LSP. In this case, router R4 receives a packet with label 20 from router R3 and swaps it with label 30 before sending it to router R5.

The exhibit shows an example of an MPLS network with four routers: R1, R2, R3, and R4. Router R1 is the ingress PE router and router R4 is the egress PE router. Router R2 and R3 are P routers. Router R1 assigns label 10 to the packet and sends it to router R2. Router R2 swaps label 10 with label 20 and sends it to router R3. Router R3 swaps label 20 with label 30 and sends it to router R4. Router R4 removes label 30 from the packet and forwards it based on its IP header or another label in the stack.

Therefore, the answer is D.

References: MPLS Label Switching | MPLS Operation | Push, Swap,Push IPCisco, A Complete Guide to Multiprotocol Label Switching (MPLS) &#8211; G2, Multiprotocol Label Switching &#8211; Wikipedia

QUESTION 45

In your network, video traffic is being marked with DSCP code AF31.

Based on industry standard practice, which code would you use to assign higher priority to VoIP traffic?

* EF
* DF

* AF11
* AF21
Explanation

The code that is commonly used to assign higher priority to VoIP traffic is EF, which stands for Expedited Forwarding. EF is a per-hop behavior (PHB) defined by the Differentiated Services (DiffServ) model for QoS.

EF provides low delay, low jitter, and low loss for real-time applications such as VoIP. EF is marked by setting the DSCP value to 101110, which corresponds to decimal 4678. AF31, which stands for Assured Forwarding class 3 low drop probability, is another PHB defined by DiffServ, but it provides lower priority than EF. AF31 is marked by setting the DSCP value to 011010, which corresponds to decimal 2678. DF, which stands for Default Forwarding, is a PHB defined by DiffServ that provides best-effort service for unmarked traffic. DF is marked by setting the DSCP value to 000000, which corresponds to decimal 078.

AF11, which stands for Assured Forwarding class 1 low drop probability, is another PHB defined by DiffServ, but it provides lower priority than EF and AF31. AF11 is marked by setting the DSCP value to 001010, which corresponds to decimal 1078.

References: Differentiated services &#8211; Wikipedia, Solved: Cisco VoIP Phone traffic marking &#8211; Cisco Community

QUESTION 46

Based on industry standard practice, what is the correct order of DiffServ priority (highest to lowest) for the DiffServ classes: Default Forwarding (DF), Network Control (NC), Assured Forwarding (AF), and Expedited Forwarding (EF)?
* EF, NC, AF, DF
* EF, AF, NC, DF
* NC, EF, DF, AF
* NC, EF, AF, DF
Explanation

The correct order of DiffServ priority (highest to lowest) for the DiffServ classes: Default Forwarding (DF), Network Control (NC), Assured Forwarding (AF), and Expedited Forwarding (EF) is EF, NC, AF, DF.

DiffServ is a QoS model that classifies and prioritizes traffic into different service classes based on the DSCP field in the IP header. The DSCP field is a 6-bit field that can encode up to 64 different per-hop behaviors (PHBs). The DiffServ classes are predefined groups of PHBs that have similar characteristics and requirements. The four main DiffServ classes are:

EF: This class provides the highest priority and lowest delay for real-time applications such as voice and video. The DSCP value for EF is 101110 or 46 in decimal12.

NC: This class provides the second highest priority and low delay for network control traffic such as routing protocols and network management. The DSCP value for NC is 110000 or 48 in decimal12.

AF: This class provides four levels of assured forwarding with different drop probabilities for each level. AF is suitable for applications that require guaranteed bandwidth and delivery assurance, such as web browsing and email. The DSCP values for AF range from 001010 to 011110 or 10 to 46 in decimal12.

DF: This class provides the lowest priority and best-effort service for applications that can tolerate packet loss and delay, such as file transfer and backup. The DSCP value for DF is 000000 or 0 in decimal12.

References: Differentiated Services &#8211; Wikipedia, DSCP &#8211; Differentiated Services Code Point &#8211; Mpirical

QUESTION 47

Which operating system is used in Ericsson Router 6000 products?
- SE-OS
- ERS
- ERS
- IPOS
- Junos

Explanation

The operating system used in Ericsson Router 6000 products is ERS (Ericsson Router Software). ERS is based on IPOS (IP Operating System), which is a common operating system for Ericsson&#8217;s IP portfolio. ERS provides advanced features and functionality for IP transport, such as MPLS, Segment Routing, QoS, IPSec, synchronization, SDN, and more. ERS also supports seamless integration with Ericsson Radio System and Ericsson Network Manager.

References: Router 6000 Series &#8211; Ericsson, Router 6675 Datasheet &#8211; Winncom

QUESTION 48

Regarding the BGP decision algorithm, which two statements are correct? (Choose two.)
- A higher local-preference attribute will be favored over a lower local-preference attribute.
- The most important criteria is the administrative distance.
- A path cannot be considered if the next-hop is inaccessible.
- A lower local-preference attribute will be favored over a higher local-preference attribute.

Explanation

Regarding the BGP decision algorithm, two statements that are correct are:

A higher local-preference attribute will be favored over a lower local-preference attribute. The local-preference attribute is used by BGP routers within an AS to indicate their preference for an exit point from the AS. A higher value means a more preferred path. The local-preference attribute is exchanged only between iBGP peers and does not leave the AS boundary89.

A path cannot be considered if the next-hop is inaccessible. The next-hop attribute is used by BGP routers to determine where to forward packets for a given destination prefix. The next-hop attribute is usually set to the IP address of the eBGP neighbor that advertises the prefix. If there is no IGP route to reach the next-hop address, the path is marked as invalid and ignored by BGP1011.

The other two statements are incorrect because:

The most important criteria is not the administrative distance, but rather the weight attribute. The administrative distance is used by routers to choose between routes from different routing protocols, not within BGP. The weight attribute is a Cisco-specific attribute that is used by BGP routers to prefer one path over another within the same router. The weight attribute is local to the router and not advertised to any peers1213.

A lower local-preference attribute will not be favored over a higher local-preference attribute, as explained above.

References: BGP Best Path Selection Algorithm &#8211; Cisco, Understanding BGP Local Preference Attribute &#8211; NetworkLessons.com, BGP Next Hop Attribute Explained &#8211; NetworkLessons.com, BGP Next Hop Processing

&#8211; Cisco Press, BGP Weight Attribute Explained &#8211; NetworkLessons.com, Understanding BGP Weight Attribute

&#8211; Cisco Community

QUESTION 49

IPv6 link-local addresses are designed to be used in which three situations? (Choose three.)
* for neighbor discovery
* for local IP communication on the IPv6 capable routers
* addressing on a single link for purposes such as auto-address configuration
* by routers to forward packets with link-local source addresses to other links
* when routers are not present
Explanation

IPv6 link-local addresses are designed to be used in three situations: for neighbor discovery, for local IP communication on the IPv6 capable routers, and for addressing on a single link for purposes such as auto-address configuration. Neighbor discovery is a protocol that allows IPv6 nodes to discover each other and learn their link-layer addresses on a local network. Neighbor discovery uses link-local addresses to send and receive messages such as router advertisements, router solicitations, neighbor advertisements, and neighbor solicitations34. Local IP communication on the IPv6 capable routers refers to the ability of routers to exchange routing information or management traffic using their link-local addresses as source and destination addresses. This reduces the need for global unicast addresses on router interfaces that are not reachable from outside the local network35. Addressing on a single link for purposes such as auto-address configuration refers to the use of link-local addresses to enable IPv6 nodes to obtain an address without manual configuration or a DHCP server. Link-local addresses can be automatically derived from the interface identifier in the modified EUI-64 format or randomly generated. Link-local addresses can also be used to test the connectivity of a link before obtaining a global unicast address36.

References: Understand the IPv6 Link-Local Address &#8211; Cisco, Link Local Address &#8211; GeeksforGeeks, IPv6 Address Types | Link-Local, Global Unicast, etc. IPCisco, MPLS Label Distribution Protocol Commands &#8211; Cisco

QUESTION 50

What is an important difference between OSPF and IS-IS?
* OSPF runs directly on IP, while IS-IS runs directly on Ethernet.
* OSPF is a link state protocol, while IS-IS is a distance vector protocol.
* OSPF runs directly on Ethernet, while IS-IS runs directly on IP.
* OSPF is a distance vector protocol, while IS-IS is a link state protocol.
Explanation

OSPF runs directly on IP, while IS-IS runs directly on Ethernet. This means that OSPF uses IP addresses to identify routers and links, while IS-IS uses MAC addresses or other link-layer identifiers. OSPF also requires an IP header for each packet, while IS-IS does not. Both OSPF and IS-IS are link state protocols, which means that they flood information about the network topology to all routers in the same area or domain. References: Ericsson IP Networking &#8211; Routing Protocols, Ericsson Router 6000 Series &#8211; Ericsson

QUESTION 51

In OSPFv2, which route characteristic is used to determine the best path?
* jitter
* packet loss
* cost
* delay
Explanation

In OSPFv2, the route characteristic that is used to determine the best path is the cost. The cost is a metric that represents the link bandwidth, delay, reliability, or other factors. The cost is inversely proportional to the bandwidth, meaning that a higher bandwidth link has a lower cost. The cost of a route is calculated by adding the costs of all links along the path. OSPFv2 uses the following formula to calculate the cost of an interface:

Cost = Reference bandwidth / Interface bandwidth in bps

The reference bandwidth is a constant value that can be configured by the network administrator. By default, it is 100 Mbps. The interface bandwidth is the actual bandwidth of the interface in bits per second. For example, if an interface has a bandwidth of 10 Mbps, its cost would be 100 Mbps / 10 Mbps = 101415.

OSPFv2 does not use jitter, packet loss, or delay as route characteristics to determine the best path. Jitter is the variation in latency or delay between packets. Packet loss is the percentage of packets that are dropped or corrupted during transmission. Delay is the time it takes for a packet to travel from source to destination. These characteristics are not part of the OSPFv2 protocol and are not advertised in OSPFv2 LSAs1617.

References: OSPF Metric cost Calculation Formula Explained &#8211; ComputerNetworkingNotes, OSPF Cost &#8211; OSPF Routing Protocol Metric Explained &#8211; Study-CCNA, Open Shortest Path First &#8211; Wikipedia, OSPF Metric

= Cost &#8211; Cisco

QUESTION 52

Which action will influence BGP route selection within your AS?
* reducing number of hops in the network
* changing the default value of the local preference
* changing the default link metric
* changing the administrative distance for eBGP
Explanation

The action that will influence BGP route selection within your AS is changing the default value of the local preference attribute. The local preference attribute is used to indicate the preference of a path among multiple paths learned from different external BGP neighbors or autonomous systems (ASes). The higher the local preference value, the more preferred the path is within your AS, and vice versa. The default value of local preference is 100, but you can change it using route maps or other configuration methods on your BGP routers. References: Ericsson IP Networking &#8211; Routing Protocols, BGP Attributes and Path Selection, BGP Local Preference Attribute: Controlling Traffic Like a Pro

QUESTION 53

In an Ericsson Router 6000, which command is used to begin making changes to the router settings?
* capabilities
* commit
* configure
* set metric
Explanation

The command that is used to begin making changes to the router settings in an Ericsson Router 6000 is configure. This command enters the configuration mode, where various commands can be used to modify the router parameters, such as interfaces, protocols, services, security, etc. To exit the configuration mode, the command end can be used. To save the changes made in the configuration mode, the command commit can be used56.

References: Router 6000 Series &#8211; Ericsson, Ericsson Router 6000 series (6471/6672/6675) Commands for

2G/3G/4G/5G technologies&#8230; &#8211; YouTube

QUESTION 54

What is the correct abbreviation for the IP address: BFEA:DACA:0000:0000:9390:0000:0000:D91?
* BFEA:DACA::9390::D91
* BFEA:DACA::9390:0:D91
* BFEA:DACA::D91/6
* BFEA:DACA::9390:0:0:D91
Explanation

The correct abbreviation for the IP address BFEA:DACA:0000:0000:9390:0000:0000:D91 is BFEA:DACA::9390:0:D91. IPv6 addresses are represented in hexadecimal notation, with eight 16-bit segments separated by colons. To simplify the address representation, IPv6 supports two types of abbreviations. The first abbreviation allows us to skip leading zeros within a segment, while the second abbreviation allows us to drop one or more consecutive segments that contain only zeros, using a double colon (::) instead. However, the double colon can be used only once in an address, to avoid ambiguity34.

References: IPv6 Address Types, Notation, and Structure Explained, IPv6 address &#8211; Wikipedia

QUESTION 55

Which two statements are true about router node hardening? (Choose two.)
* LDAP, using the TLS protocol, should be implemented for remote logging.
* Any unnecessary services should be disabled within each context.
* IPsec should be implemented to secure IGP routing protocols.
* Enabling syslog ensures system events are logged to a remote server.
Explanation

Two statements that are true about router node hardening are:

Any unnecessary services should be disabled within each context. Router node hardening is a process of securing a router from unauthorized access and attacks by applying various configurations and policies.

One of these configurations is to disable any services that are not needed for the router&#8217;s functionality or purpose, such as telnet, ftp, http, etc. This reduces the attack surface of the router and prevents potential exploits of these services91.

Enabling syslog ensures system events are logged to a remote server. Syslog is a protocol that allows a router to send system messages and events to a remote server for logging and analysis. By enabling syslog on a router, network administrators can monitor the router&#8217;s activity and performance, troubleshoot problems, detect anomalies, and audit security events101.

References: Cisco Router Hardening Step-by-Step | SANS Institute, Security Hardening Checklist Guide for Cisco Routers/Switches in 10 Steps, CCNA SEC: Router Hardening &#8211; Cisco Press

QUESTION 56

What are two roles of the DHCP protocol in a network? (Choose two.)

* It is used by hosts to obtain the IP address and other parameters from the DHCP server.
* It is used to inform hosts about the default gateway.
* It provides information about the number of hops between the source and the destination.
* It provides the authorization function to the network.
Explanation

Two roles of the DHCP protocol in a network are:

It is used by hosts to obtain the IP address and other parameters from the DHCP server. DHCP stands for Dynamic Host Configuration Protocol, which is a protocol that provides automatic and centralized management of IP addresses and other network configuration parameters for devices connected to a network. A host that needs an IP address can send a request to a DHCP server, which will assign an available IP address from a pool and lease it to the host for a certain period of time34.

It is used to inform hosts about the default gateway. The default gateway is the IP address of the router that connects the host to other networks. The default gateway is one of the parameters that can be delivered by the DHCP server to the host, along with other parameters such as subnet mask, DNS server, domain name, etc. The host can use the default gateway to send packets to destinations outside of its local network34.

References: What Is DHCP? (Dynamic Host Configuration Protocol) &#8211; Lifewire, Dynamic Host Configuration Protocol &#8211; Wikipedia

QUESTION 57

Which two statements are true about priority queuing (PQ)? (Choose two.)
* Traffic in the highest priority queue will experience the least amount of jitter and delay compared to traffic in the other queues.
* Traffic in the highest priority queue is only reserved for voice traffic.
* Traffic in lower priority queues can be starved of bandwidth.
* Traffic in all queues are always guaranteed a minimum bandwidth.
Explanation

Priority queuing (PQ) is a queuing method that establishes four interface output queues that serve different priority levels: high, medium, normal, and low. Traffic in the highest priority queue will experience the least amount of jitter and delay compared to traffic in the other queues, because PQ always services the higher-priority queues first. However, this can also cause traffic in lower priority queues to be starved of bandwidth, especially if the highest priority queue is oversubscribed. Traffic in the highest priority queue is not only reserved for voice traffic, but can also include network control and routing traffic. Traffic in all queues are not always guaranteed a minimum bandwidth, because PQ does not provide any bandwidth reservation mechanism. References: Quality of Service (QoS) Queues and Queuing Explained, Chapter:

Configuring Priority Queueing &#8211; Cisco