DEMO

EXAMS DUMPS.co

Instant Download After Purchase

100% Money Back Guarantee

PDF FILE FORMAT

90 Days Free Updates

CISCO

200-310

Q&As

2020 Latest EXAMSDUMPS 200-310 PDF Dumps Download. Following Questions and Answers are all new published by Cisco Official Exam Center

- **Latest 200-310 Dumps**
- **200-310 Practice Test**
- **200-310 Study Guide**

Pass CISCO 200-310 Exam with 100% Guarantee

Free Download Real Questions & Answers PDF and VCE file from:

Cisco 200-310

Designing for Cisco Internetwork Solutions

Version: 1.1

QUESTION NO: 1

Which of the following is a leased-line WAN technology that divides a link's bandwidth into equal-sized segments based on clock rate?

A.
TDM

B.
ATM

C.
WDM

D.
DWDM

E.
MPLS

F.
Metro Ethernet

Answer: A

Explanation:
Section: Enterprise Network Design Explanation

Time division multiplexing (TDM) is a leased-line WAN technology that divides a link's bandwidth into equal-sized segments based on clock rate. TDM enables several data streams to share a single physical connection. Each data stream is then allotted a fixed number of segments that can be used to transmit data. Because the number of segments dedicated to each data stream is static, unused bandwidth from one data stream cannot be dynamically reallocated to another data stream that has exceeded its available bandwidth. By contrast, statistical multiplexing dynamically allocates bandwidth to data streams based on their traffic flow. For example, if a particular data stream does not have any traffic to send, its bandwidth is reallocated to other data streams that need it.

Metro Ethernet does not divide a link's bandwidth into equal-sized segments based on clock rate. Metro Ethernet is a WAN technology that is commonly used to connect networks in the same metropolitan area.

For example, if a company has multiple branch offices within the same city, the company can use Metro Ethernet to connect the branch offices to the corporate headquarters. Metro Ethernet providers typically provide up to 1,000 Mbps of bandwidth.

Wavelength division multiplexing (WDM) does not divide a link's bandwidth into equal-sized

segments based on clock rate. WDM is a leased-line WAN technology used to increase the amount of data signals that a single fiber strand can carry. To accomplish this, WDM can transfer data of varying light wavelengths on up to 16 channels per single fiber strand. Whereas TDM divides the bandwidth in order to carry multiple data streams simultaneously, WDM aggregates the data signals being carried within the fiber strand.

Dense WDM (DWDM) does not divide a link's bandwidth into equal-sized segments based on clock rate. DWDM is a leased-line WAN technology that improves on WDM by carrying up to 160 channels on a single fiber strand. The spacing of DWDM channels is highly compressed, requiring a more complex transceiver design and therefore making the technology very expensive to implement.

Asynchronous Transfer Mode (ATM) uses statistical multiplexing and does not divide a link's bandwidth into equal-sized segments based on clock rate. ATM is a shared WAN technology that transports its payload in a series of 53byte cells. ATM has the unique ability to transport different types of traffic-including IP packets, traditional circuit-switched voice, and video-while still maintaining a high quality of service for delay-sensitive traffic, such as voice and video services. Although ATM could be categorized as a packet-switched WAN technology, it is often listed in its own category as a cell-switched WAN technology.

Multiprotocol Label Switching (MPLS) does not divide a link's bandwidth into equal-sized segments based on clock rate. MPLS is a shared WAN technology that makes routing decisions based on information contained in a fixed-length label. In an MPLS virtual private network (VPN), each customer site is provided with its own label by the service provider. This enables the customer site to use its existing IP addressing scheme internally while allowing the service provider to manage multiple sites that might have conflicting IP address ranges. The service provider then forwards traffic over shared lines between the sites in the VPN according to the routing information that is passed to each provider edge router.

Reference:

CCDA 200-310 Official Cert Guide, Chapter 6, TimeDivision Multiplexing, p. 225

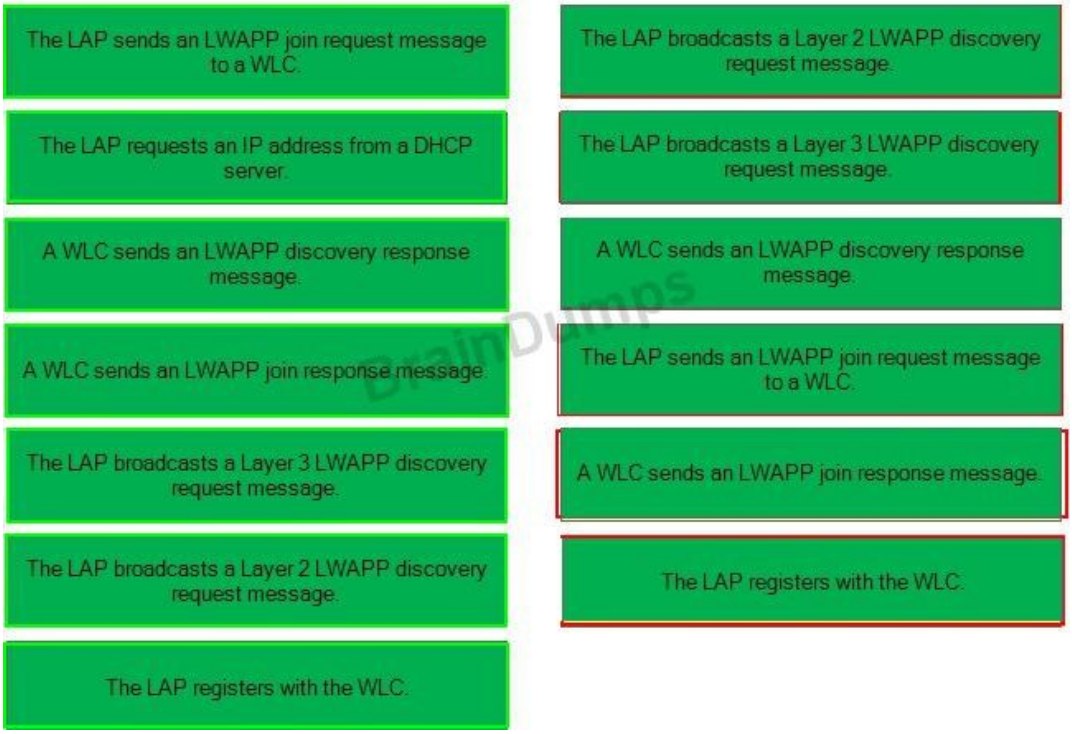
Cisco: ISDN Voice, Video and Data Call Switching with Router TDM Switching Features

QUESTION NO: 2 DRAG DROP

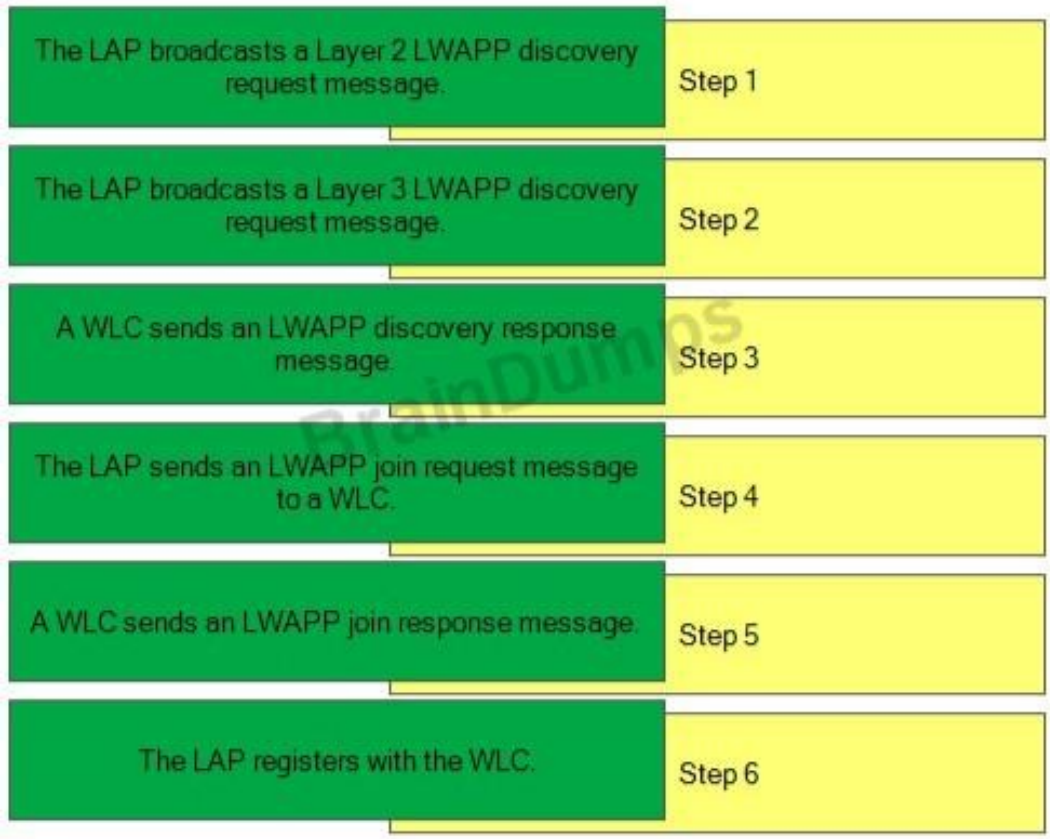
You are adding an additional LAP to your current wireless network, which uses LWAPP. The LAP is configured with a static IP address. You want to identify the sequence in which the LAP will connect to and register with a WLC on the network.

Select the lap connection steps on the left, and drag them to the appropriate location on the right. Not all steps will be used.

Answer:



Explanation:



Section:

Considerations for Expanding an Existing Network Explanation

When you add a lightweight access point (LAP) to a Wireless network that uses Lightweight Access Point Protocol (LWAPP), the LAP goes through a sequence of steps to register with a Wireless LAN controller (WLC) on the network. First, if Open Systems Interconnection (OSI) Layer 2 LWAPP mode is supported, the LAP attempts to locate a WLC by broadcasting a Layer 2 LWAPP discovery request message. If a WLC does not respond to the Layer 2 broadcast, the LAP will broadcast a

Layer 3 LWAPP discovery request message.

Once a WLC receives the LWAPP discovery message, the WLC will send an LWAPP discovery response message to the LAP; the discovery response will contain the IP address of the WLC. The LAP compiles a list of all discovery responses it receives. The list is cross-referenced against the LAP's internal configuration. The LAP will then send an LWAPP join request message to one of the WLCs on its list of responses.

If the LAP has been configured with a primary, secondary, and tertiary WLC, the LAP will first send an LWAPP join request message to the primary WLC. If no response is received from the primary WLC, the LAP will try the secondary and tertiary WLCs in sequence. If no response is received from either the secondary or tertiary WLCs, the LAP will examine the responses on its list for a master controller ag. If one of the WLCs is configured as a master, the LAP will send an LWAPP join request message to the master WLC. If there is no master configured, or if the master does not respond, the LAP will examine its list of responses and send an LWAPP join request message

to the WLC with the greatest capacity.

When a WLC responds with an LWAPP join response message, the authentication process begins. After the LAP and the WLC authenticate with each other, the LAP will register with the WLC.

Reference:

Cisco: Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC): Register the LAP with the WLC

QUESTION NO: 3

Which of the following statements best describes the purpose of CDP?

A.
CDP is a proprietary protocol used by Cisco devices to detect neighboring Cisco devices.

B.
CDP is a standard protocol used to power IP devices over Ethernet.

C.
CDP is a proprietary protocol used to power IP devices over Ethernet.

D.
CDP is a standard protocol used by Cisco devices to detect neighboring devices of any type.

Answer: A

Explanation:
Section: Design Methodologies Explanation

Cisco Discovery Protocol (CDP) is a Cisco-proprietary protocol used by Cisco devices to detect neighboring Cisco devices. For example, Cisco switches use CDP to determine whether an attached Voice over IP (VoIP) phone is manufactured by Cisco or by a third party. CDP is enabled by default on Cisco devices. You can globally disable CDP by issuing the no cdp run command in global configuration mode. You can disable CDP on a perinterface basis by issuing the no cdp enable command in interface configuration mode.

CDP packets are broadcast from a CDPenabled device on a multicast address. Each directly connected CDPenabled device receives the broadcast and uses that information to build a CDP

table. Detailed information about neighboring CDP devices can be viewed in IOS by issuing the show cdp neighbor detail command in global configuration mode. The following abbreviated sample output shows information obtained from CDP about the IP phone named SEP00123456789A:

```
Device ID: SEP00123456789A
Entry address(es):
  IP address: 10.11.12.13
Platform: Cisco IP Phone 7961,  Capabilities: Host Phone
Interface: FastEthernet 0/8, Port ID (outgoing port): Port 1
Holdtime : 166 sec

Version : SCCP41.8-0-4SR3AS
advertisement version: 2
Duplex: full
Power drawn: 6.300 Watts
Power request id: 27263, Power management id: 3
Power request levels are:6300 0 0 0 0
```


Link Layer Detection Protocol (LLDP), not CDP, is a standard protocol that detects neighboring devices of any type. Cisco devices also support LLDP. LLDP can be used in a heterogeneous network to enable Cisco devices to detect non-Cisco devices and vice versa. LLDP, which is enabled by default, can be disabled globally by issuing the no lldp run command. You can reenable LLDP by issuing the lldp run command.

CDP is not a protocol used to power IP devices over Ethernet, although an IP phone can provide Power over Ethernet (PoE) requirements to a switch by using CDP. A Catalyst switch can provide power to both Cisco and non-Cisco IP phones that support either the 802.3af standard method or the Cisco prestandard method of PoE. For a Catalyst switch to successfully power an IP phone, both the switch and the IP phone must support the same PoE method. After a common PoE method is determined, CDP messages sent between Catalyst switches and Cisco IP phones can further refine the amount of power allocated to each device.

Reference:

CCDA 200-310 Official Cert Guide, Chapter 15, CDP, p. 629

Cisco: Catalyst 3750 Switch Software Configuration Guide, 12.2(40)SE: Configuring CDP

QUESTION NO: 4

Which of the following statements are true regarding standard IP ACLs? (Choose two.)

A.
Standard ACLs should be placed as close to the source as possible.

B.
Standard ACLs can filter traffic based on source and destination address.

C.
Standard ACLs can be numbered in the range from 1 through 99 or from 1300 through 1999.

D.
Standard ACLs can filter traffic based on port number.

E.
Standard ACLs can filter traffic from a specific host or a specific network.

Answer: C,E

Explanation:
Section: Considerations for Expanding an Existing Network Explanation

Standard IP access control lists (ACLs) can be numbered in the range from 1 through 99 or from 1300 through 1999 and can filter traffic from a specific host or a specific network. ACLs are used to control packet flow across a network. For example, you could use an ACL on a router to restrict a specific type of traffic, such as Telnet sessions, from passing through a corporate network. There are two types of IP ACLs: standard and extended. Standard IP ACLs can be used to filter based only on source IP addresses; standard IP ACLs cannot be used to filter based on source and destination address. Standard ACLs should be placed as close to the destination as possible so that other traffic originating from the source address is not affected by the ACL.

Extended IP ACLs enable you to permit or deny packets based on not only source IP address but destination network, protocol, or destination port. In contrast to standard IP ACLs, extended IP ACLs should be placed as close to the source as possible. This ensures that traffic being denied by the ACL does not unnecessarily traverse the network. Extended ACLs have access list numbers from 100 through 199 and from 2000 through 2699.

Reference:

CCDA 200-310 Official Cert Guide, Chapter 13, Identity and Access Control Deployments, pp. 532-533 Cisco: Configuring IP Access Lists

QUESTION NO: 5

In which of the following situations would static routing be the most appropriate routing mechanism?

A.
when the router has a single link to a router within the same AS

B.
when the router has redundant links to a router within the same AS

C.
when the router has a single link to a router within a different AS

D.
when the router has redundant links to a router within a different AS

Answer: C

Explanation:
Section: Addressing and Routing Protocols in an Existing Network Explanation

Static routing would be the most appropriate routing mechanism for a router that has a single link to a router within a different autonomous system (AS). An AS is defined as the collection of all areas that are managed by a single organization. Because an interdomain routing protocol, such as Border Gateway Protocol (BGP), can be complicated to configure and uses a large portion of a router's resources, static routing is recommended if dynamic routing information is not exchanged between routers that reside in different ASes. For example, if you connect a router to the Internet through a single Internet service provider (ISP), it is not necessary for the router to run BGP, because the router will use this single connection to the Internet for all traffic that is not destined to the internal network.

External BGP (eBGP), not static routing, would be the most appropriate routing protocol for a router that has redundant links to a router within a different AS. BGP is typically used to exchange routing information between ASes, between a company and an ISP, or between ISPs. BGP routers within the same AS communicate by using internal BGP (iBGP), and BGP routers in different ASes communicate by using eBGP.

An intradomain routing protocol, such as Enhanced Interior Gateway Routing Protocol (EIGRP) or Open Shortest Path First (OSPF), would be the most appropriate routing protocol for a router that has a single link or redundant links to a router within the same AS.

Reference:

CCDA 200-310 Official Cert Guide, Chapter 10, Static Versus Dynamic Route Assignment, pp. 380-381

QUESTION NO: 6

You are installing a 4U device in a data center.

Which of the following are you installing?

A.
cabling at the demarc

B.
an environmental control

C.
a network device in a 7inch space

D.
a lock for rack security

Answer: C

Explanation:
Section: Considerations for Expanding an Existing Network Explanation

You are installing a network device in a 7inch (18centimeter) space if you are installing a 4unit (U) device in a data center. Although most racks adhere to a standard width of 19 inches (about 48 centimeters), a certain number of U, or height, of space must be available within a rack to allow the installation of your equipment and to allow space between your equipment and other equipment that is contained within the rack. A U is equivalent to 1.75 inches (about 4.5 centimeters) of height. Therefore, if the device you want to install is a 2U device, the rack should have at least 3.5 inches (about 9 centimeters) of available space to accommodate the device and more to allow for space above and below the device. A 4U device will fit into a 7inch (18centimeter) rack space.

You are not installing a lock for rack security. However, rack security is likely to be a concern when installing a server in a third-party data center. Commercial data centers house devices for multiple customers within the same physical area. Although many data centers are physically secured against intruders who might steal or modify equipment, the data center's other customers have the same access to the physical area that you do. Therefore, you should install physical security mechanisms, such as a lock, at the rack level to ensure that your company’s devices cannot be accessed by others.

You are not installing an environmental control. However, an environmental control such as airflow, which helps prevent devices from overheating, is likely to be a concern when installing a server in a third-party data center. You should choose a data center that provides environmental controls. For example, a hot and cold aisle layout is a data center design that attempts to control the airflow within the room in order to mitigate problems that can result from overheated servers? it

essentially prevents hot air from mixing with cold air. A raised floor layout is a data center design that puts the heating, ventilation, and air conditioning (HVAC) ductwork below the floor tiles. The tiles, which are typically located in the aisles between the server racks in this type of environment, are perforated so that airflow can be directed and concentrated in the exact locations desired.

You are not installing cabling at the demarc, or demarcation point. The demarc is the termination point between a physical location and its service provider. In other words, it is the point where the responsibility of the physical location ends and the responsibility of the service provider begins. At a third-party data center, the demarc is the responsibility of the data center provider and its service provider, not the data center's customers.

Reference:

CCDA 200-310 Official Cert Guide, Chapter 4, Data Center Facility Aspects, pp. 136-138

Cisco: Cabinet and Rack Installation