Chapters 22 – 24: Network Design and Monitoring Exam (Answers)

itexamanswers.net/chapters-22-24-network-design-and-monitoring-exam-answers.html

December 19, 2020

CCNPv8 ENCOR (Version 8.0) – Network Design and Monitoring Exam

How to find: Press **“Ctrl + F”** in the browser and fill in whatever wording is in the question to find that question/answer. If the question is not here, find it in **Questions Bank**.

NOTE: If you have the new question on this test, please comment Question and Multiple-Choice list in form below this article. We will update answers for you in the shortest time. Thank you! We truly value your contribution to the website.

1. Which network design solution will best extend access layer connectivity to host devices?

- implementing redundancy
- implementing EtherChannel
- **implementing wireless connectivity**
- implementing routing protocols

Explanation: EtherChannel allows more data to be moved at the access layer, but does not provide network expansion. Redundancy is used to provide failover solutions but does not focus on network expansion. Routing protocols are not used to provide network expansion at the access layer. Wireless connectivity provides network access to a large number of users at the access layer.

2. A network designer must provide a rationale to a customer for a design which will move an enterprise from a flat network topology to a hierarchical network topology. Which two features of the hierarchical design make it the better choice? (Choose two.)

- **simpler deployment for additional switch equipment**
- **easier to provide redundant links to ensure higher availability**
- lower bandwidth requirements
- less required equipment to provide the same performance levels
- reduced cost for equipment and user training

Explanation: A hierarchical design for switches helps network administrators when planning and deploying a network expansion, performing fault isolation when a problem occurs, and providing resiliency when traffic levels are high. A good hierarchical design has redundancy when it can be afforded so that one switch does not cause all networks to be down.

3. What are three benefits of employing a hierarchical network design? (Choose three.)

- Use of a hierarchical design allows replacement of redundant devices with high-capacity network equipment.
- The hierarchical model allows the use of high-performance switches at all design layers, thus allowing for a fully-meshed topology.
- **Hierarchically designed networks can more easily be expanded to suit future needs.**
- **Hierarchical design models enhance existing bandwidth through the use of link aggregation.**
- A hierarchical design uses firewalls instead of complicated port-based and distribution layer security policies.
- **The hierarchical model allows for specialized functionality at each layer, simplifying device management.**

Explanation: Hierarchical design provides fault containment by constraining the network changes to a subset of the network, which affects fewer systems and makes it easy to manage as well as improve resiliency. In a modular layer design, network components can be placed or taken out of service with little or no impact to the rest of the network and this facilitates troubleshooting, problem isolation, and network management.

4. At the distribution layer of a hierarchical network, what are two advantages of using Layer 3 devices instead of Layer 2 switches? (Choose two.)

- creates fewer IP subnets to configure and manage
- **provides connectivity between different VLANs**
- **enables traffic filtering based on subnet addresses**
- provides reliable connectivity to end users
- reduces the number of redundant links required

Explanation: Communication between endpoints on different access layer switches occurs through the distribution layer. The distribution layer provides a boundary between the Layer 2 domain of the access layer and the Layer 3 domain of the core. This boundary provides two key functions for the LAN. On the Layer 2 side, the distribution layer creates a boundary for Spanning Tree Protocol (STP), limiting propagation of Layer 2 faults. On the Layer 3 side, the distribution layer provides a logical point to summarize IP routing information when it enters the core layer. The summarization reduces IP route tables for easier troubleshooting and reduces protocol overhead for faster recovery from failures.

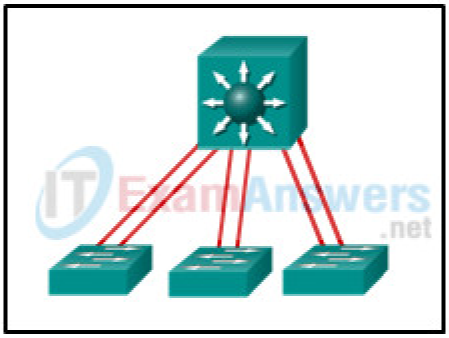
5. Which three characteristics are typically associated with the core layer in the Cisco hierarchical network design model? (Choose three.)

- packet manipulation
- monitoring of DMZ traffic
- **connectivity to the data center**
- **redundant paths**
- **rapid forwarding of traffic**

Explanation: The core layer is the backbone and aggregation point for multiple networks and provides scalability, high availability, and fast convergence to the network. It can provide high-speed connectivity for large enterprises with multiple campus networks distributed worldwide and it can also provide interconnectivity between the end-user/endpoint campus access layer and other network blocks such as the data center, the private cloud, the public cloud, the WAN, Internet edge, and network services. Packet filtering is a function of the distribution layer.

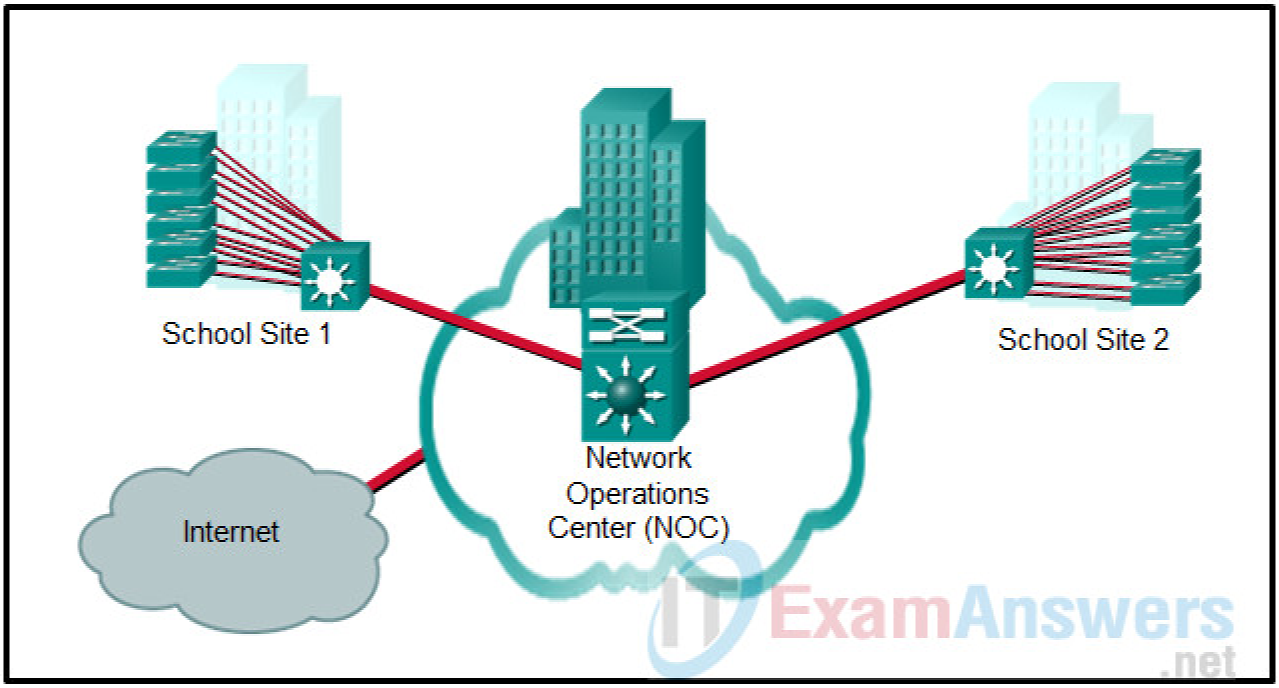
6. Refer to the exhibit. Which switching technology would allow each access layer switch link to be aggregated to provide more bandwidth between each Layer 2 switch and the Layer 3 switch?

- HSRP
- **EtherChannel**
- trunking
- PortFast



Explanation: PortFast is used to reduce the amount of time that a port spends going through the spanning-tree algorithm, so that devices can start sending data sooner. Trunking can be implemented in conjunction with EtherChannel, but trunking alone does not aggregate switch links. HSRP is used to load-balance traffic across two different connections to Layer 3 devices for default gateway redundancy. HSRP does not aggregate links at either Layer 2 or Layer 3 as EtherChannel does.

7. Refer to the exhibit. Which type of Cisco hierarchical LAN design model is used at school site 1?



- three-tier
- 7 layer
- 3 layer
- **two-tier collapsed core**

Explanation: In the two-tier collapsed core model, the distribution layer and the core layer are combined into one. The switch that connects the site to the NOC is serving as both a distribution layer switch and a core layer switch. The NOC is designed with other network devices that are not shown, such as the firewall, as part of an Internet edge design.

8. A network engineer is attempting to explain StackWise technology to a client who wants to deploy a simplified campus design. Which explanation accurately describes this technology?

- It allows the switch to deliver power to end devices by using existing Ethernet cabling.
- It allows up to eight ports to be bound together to increase available bandwidth.
- It allows the switch capabilities and ports to be expanded by the addition of line cards.
- **It allows multiple switches to function as a single logical switch.**

Explanation: The simplified campus design relies on switch clustering such as the Virtual Switching System (VSS) and stacking technologies such as Stackwise in which multiple physical switches act as a single logical switch.

9. On a campus network, personnel who are located in a five site college have access to servers found in one location. In which network block of the campus network architecture would these servers be found?

- WAN edge
- **data center**
- Internet edge
- network services

Explanation: In this hierarchical model, the distribution/core layer provides connectivity to the WAN edge block, the Internet edge block, the network services block, and data center. The WAN edge block is used to connect to remote data centers, remote branches or other campus networks. The Internet edge block is used for regular Internet access, ecommerce, to connect to remote branches, and remote VPN access. The data center/server room block is where business critical servers are placed to serve up websites, corporate e-mail, business applications, storage, big data processing, and backup services. The network services edge is where devices providing network services reside such as the Wireless LAN Controllers (WLCs), Identity Services Engine (ISE), Telepresence Manager, and Cisco Unified Communications Manager (CUCM).

10. In a new network design, an organization has decided to manage all of its wireless access points using a wireless network controller. In which network design block of the campus network architecture would the centralized wireless network controllers be found?

- **network services**
- internet edge
- data center
- WAN edge

Explanation: In this hierarchical model, the distribution/core layer provides connectivity to the WAN edge block, the Internet edge block, the network services block, and data center. The WAN edge block is used to connect to remote data centers, remote branches or other campus networks. The internet edge block is used for regular Internet access, ecommerce, to connect to remote branches, and remote VPN access. The data center/server room block is where business critical servers are placed to serve up websites, corporate e-mail, business applications, storage, big data processing, and backup services. The network services edge is where devices providing network services reside such as the Wireless LAN Controllers (WLCs), Identity Services Engine (ISE), Telepresence Manager, and Cisco Unified Communications Manager (CUCM).

11. A network engineer has to decide between a Layer 2 Access Layer (STP-based) and a Layer 3 Access Layer (Routed access) campus design option. Which statement must be considered for a decision to be made?

- The Routed access option is the best cost-effective solution.

- The STP based access option supports spanning VLANs across multiple access switches, whereas the Routed access option does not.
- **The Routed access option offers easier troubleshooting than the STP-based option.**
- The STP based option does not require FHRP, whereas the Routed access option does.

Explanation: The Routed access design has a number of advantages over the STP-based design:

No FHRP required – no need for FHRP protocols such as HSRP and VRRP.
No STP required – since there are no L2 links to block, this design removes the need for STP.
Easier troubleshooting – It offers common end-to-end troubleshooting tools (such as ping and traceroute).

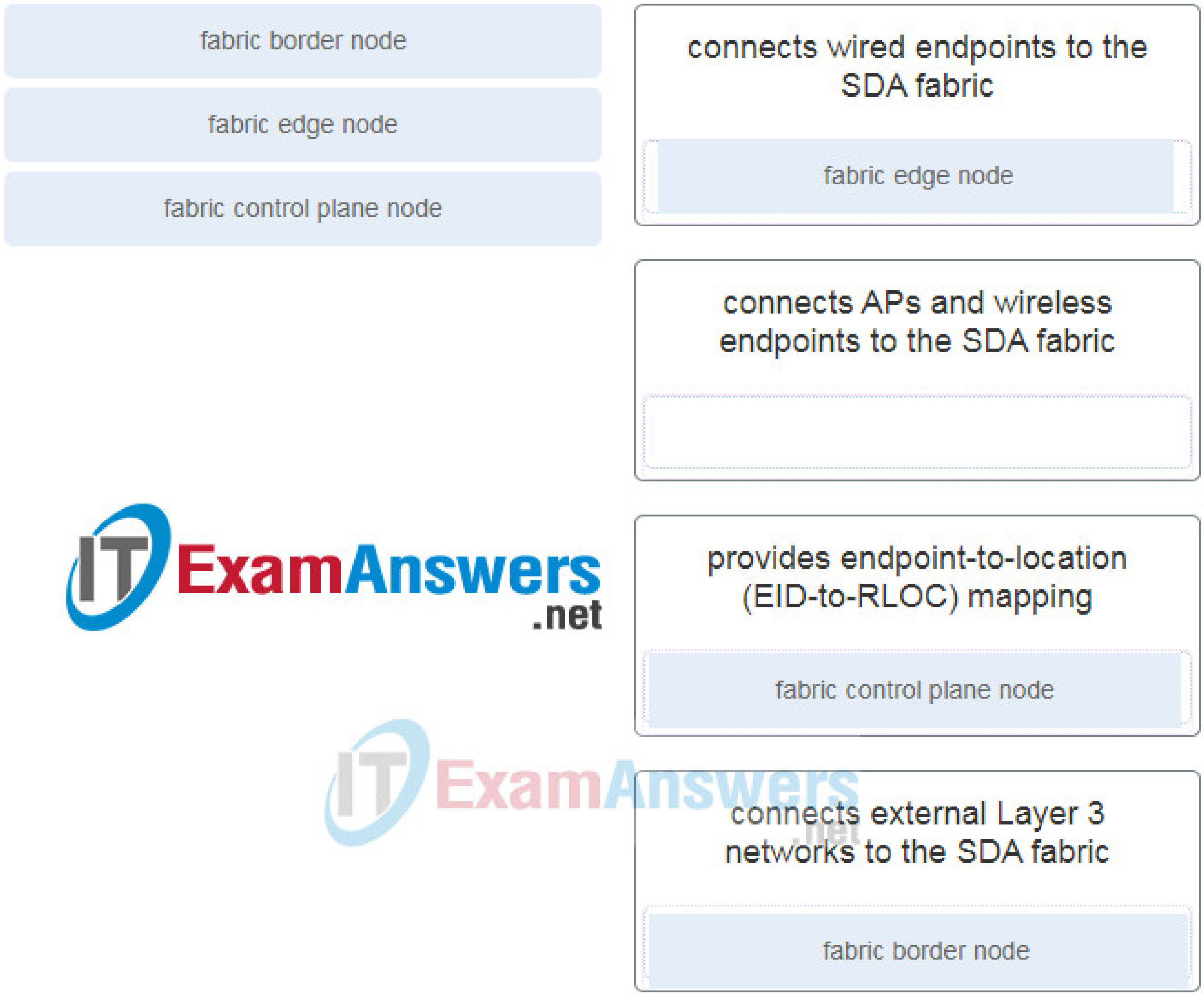
The Routed access is an excellent design for many environments, but it has the same limitation as the STP-based design, in which it does not support spanning VLANs across multiple access switches. Additionally, it might not be the most cost-effective solution because access layer switches with Layer 3 routing capability might cost more than Layer 2 switches do.

12. What is the description for a Syslog Level 3 event?

- **error condition**
- critical condition
- immediate action needed
- warning condition

Explanation: Syslog messages include a severity level with a value between 0 and 7, with a lower number being more severe. Each level also has an associated keyword and description.

13. Match the SD-Access fabric device role to the description. (Not all options are used.)



fabric border node

fabric edge node

fabric control plane node

connects wired endpoints to the SDA fabric

fabric edge node

connects APs and wireless endpoints to the SDA fabric

provides endpoint-to-location (EID-to-RLOC) mapping

fabric control plane node

connects external Layer 3 networks to the SDA fabric

fabric border node

- fabric edge node : connects wired endpoints to the SDA fabric
- connects APs and wireless endpoints to the SDA fabric
- fabric control plane node : provides endpoint-to-location (EID-to-RLOC) mapping
- fabric border node : connects external Layer 3 networks to the SDA fabric

14. Which protocol or service can be configured to send unsolicited messages to alert the network administrator about a network event such as an extremely high CPU utilization on a router?

- syslog
- **SNMP**
- NTP
- NetFlow

Explanation: SNMP can be used to collect and store information such as device CPU utilization. Syslog is used to access and store system messages. Cisco developed NetFlow for the purpose of gathering statistics on packets that are flowing through Cisco routers and multilayer switches. NTP is used to allow network devices to synchronize time settings.

15. An administrator issued the following commands on router R1:

```
R1(config)# logging 192.168.10.2
R1(config)# logging trap 5
```

What conclusion can be drawn from this configuration?

- The only messages that appear on the syslog server are those with severity level of 5.
- **Messages with severity level of 6 or higher appear only on the router console output.**
- Messages with severity level of 5 or higher appear on the router console output and are sent to the syslog server.
- The only messages that appear on the syslog server are those with severity level of 4 or lower.

Explanation: When these commands are issued, the only messages that appear on the syslog server are those with severity level of 5 or lower. The messages with severity level of 6 or higher appear on the router console output, but do not appear on the syslog server output because the logging trap command limits by severity level the syslog messages that are sent to the syslog server.

16. What is the description for a Syslog Level 1 event?

- system unusable
- **immediate action needed**
- error condition
- critical condition

Explanation: Syslog messages include a severity level with a value between 0 and 7, with a lower number being more severe. Each level also has an associated keyword and description.

17. What is the purpose of ERSPAN?

- **to mirror traffic from a remote location**
- to log information from monitored network devices
- to provide standardization for traffic sent from network devices to a logging server
- to analyze the type and frequency of specific data types for QoS purposes

Explanation: Encapsulated Remote Switched Port Analyzer (ERSPAN) is used to route monitored traffic from one network to another through Layer 3 routing instead of Layer 2 port mirroring as other SPAN technologies do.

18. What is a primary function of the Cisco IOS IP Service Level Agreements feature?

- **to measure network performance and discover a network failure as early as possible**
- to detect potential network attacks
- to adjust network device configurations to avoid congestion
- to provide network connectivity for customers

Explanation: The Cisco IOS IP Service Level Agreements (SLAs) feature is a useful tool to discover a network failure as early as possible. It uses generated traffic to measure network performance in real time. The results can help network administrators detect signs of network issues at an early stage.

19. What is a tool in the Cisco DNA Center that can apply machine learning in order to diagnose network issues and offer guided remediation steps to fix issues?

- **DNA Assurance**
- syslog
- RSPAN
- SNMP
- ERSPAN

Explanation: DNA Assurance is part of the Cisco DNA Center. The Cisco DNA Center has the ability to apply machine learning to diagnose network issues and offer guided remediation steps used to fix an issue. The ASSURANCE page shows the overall health of the network including wired and wireless client data as well as access to dashboards, issues, and a way to drill down on single users and their problems.

20. What is the description for a Syslog Level 5 event?

- **normal, but significant condition**
- debugging message
- warning condition
- informational message

21. What is the description for a Syslog Level 6 event?

- normal, but significant condition
- **informational message**
- debugging message
- warning condition

22. Which layer of the Cisco SD-Access Architecture contains the underlay and the overlay networks?

- controller
- **network**
- management
- physical

Explanation: The network layer of the Cisco SD-Access Architecture contains the underlay and the overlay network which together deliver data packets to and from the network devices participating in SD-Access.

23. Which two statements describe the SD-Access overlay network? (Choose two.)

- It provides underlay and fabric automation and orchestration.
- **It is a virtualized network interconnecting all network devices.**
- **It has three planes of operation: control, data, and policy.**
- It is the underlying physical layer transporting data between network devices.
- It includes all devices that actively participate in the SD-Access fabric.

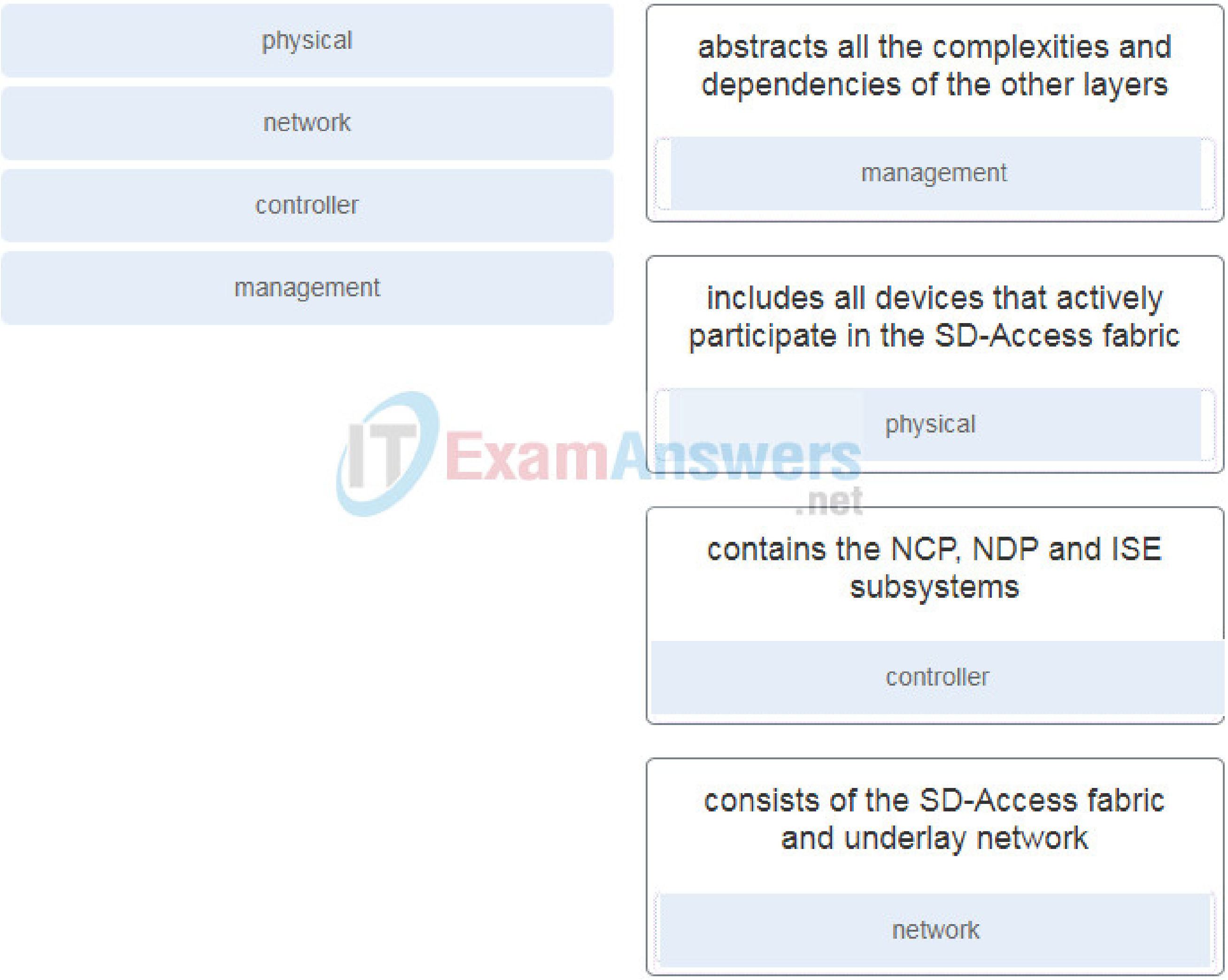
Explanation: The SD-Access overlay network, also known as the SD-Access fabric, is a virtual network that interconnects all of the network devices to form a fabric of interconnected nodes. The overlay network includes three planes of operation: the control plane, the data plane, and the policy plane.

24. What is the role of the fabric edge node in the SD-Access fabric overlay?

- **connecting wired endpoints to the SDA fabric**
- providing endpoint-to-location (EID-to-RLOC) mapping to the SDA fabric
- connecting APs and wireless endpoints
- connecting external Layer 3 networks to the SDA fabric

Explanation: There are five basic device roles in the SDA fabric overlay. The role of the fabric edge node is to connect wired endpoints to the SDA fabric.

25. Match the layer of the Cisco SD-Access Architecture with the description.



physical

network

controller

management

abstracts all the complexities and dependencies of the other layers

management

includes all devices that actively participate in the SD-Access fabric

physical

contains the NCP, NDP and ISE subsystems

controller

consists of the SD-Access fabric and underlay network

network

- abstracts all the complexities and dependencies of the other layers
- includes all devices that actively participate in the SD-Access fabric
- contains the NCP, NDP and ISE subsystems
- consists of the SD-Access fabric and underlay network

26. Which IGP is used in the automated underlay model of the Cisco SD-Access architecture?

- OSPF
- BGP
- **IS-IS**
- EIGRP

Explanation: In an automated underlay model, the Cisco DNA Center LAN automation feature creates a Layer 3 routed access campus design through the use of IS-IS.

27. Which tunneling technology is used by the SD-Access fabric data plane to create the overlay network for the SD-Access fabric?

- **VXLAN**
- MPLS
- LISP
- GRE

Explanation: The overlay network is built by the SD-Access fabric data plane over an underlay network by using VXLAN tunneling technology. Using VXLAN allows the SD-Access fabric to support Layer 2 and Layer 3 virtual topologies (overlays) and the ability to operate over any IP-based network.

28. What is the responsibility of the ISE subsystem within the Cisco SD-Access Architecture controller layer?

- It provides all the underlay and fabric automation and orchestration services for the physical and network layers.
- **It provides all the identity and policy services for the physical layer and network layer.**
- It analyzes and correlates network events and identifies historical trends.
- It provides network operational status and other information to the management layer.

Explanation: There are three control layer subsystems in the Cisco SD-Access Architecture.
Cisco Network Control Platform (NCP) – provides underlay and fabric automation and orchestration
Cisco Network Data Platform (NDP) – analyzes and correlates network events
Cisco Identity Services Engine (ISE) – provides identity and policy services

1.23.3 SD-Access Architecture
29. What function is provided by the vManage Network Management System in the Cisco SD-WAN solution?

- **Providing the single pane of glass (GUI) for the SD-WAN solution.**
- Managing software images, maintenance updates, version compliance, and the deployment of device images.
- Providing the best application quality of experience (QoE) for SaaS applications.
- Authenticating the vSmart controllers and the SD-WAN routers and orchestrates connectivity between them.

Explanation: The vManage NMS enables centralized provisioning and simplifies network changes.

30. What are three functions of the Cisco SD-WAN vBond orchestrator? (Choose three.)

- delivering quality of experience (QoE) for SaaS applications
- providing a single pane of glass network management system
- **providing a control plane connection over DTLS tunnels to communicate with SD-WAN routers**
- forecasting and what-if analysis
- **providing NAT traversal between SD-WAN routers**
- **providing load balancing of SD-WAN routers**

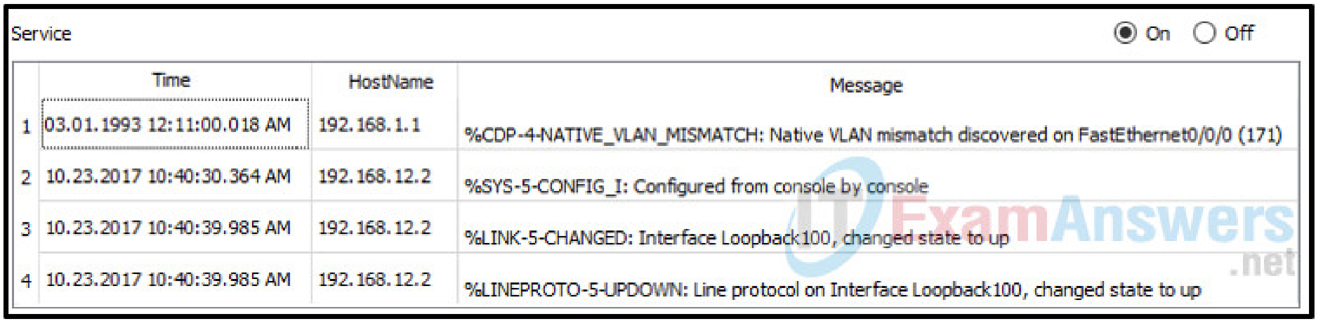
Explanation: There are three components of the vBond orchestrator:
The control plane connection over DTLS tunnels for communication with SD-WAN routers
NAT traversal to connect SD-WAN routers and vSmart controllers
Load balancing of SD-WAN routers across the vSmart controllers

31. In a domain with multiple vSmart controllers, which Cisco SD-WAN solution performs automatic load balancing of SD-WAN routers across multiple controllers?

- **vBond orchestrator**
- vManage Network Management System
- vSmart controller
- Cloud OnRamp

Explanation: The three major components of the vBond orchestrator are as follows:
The control plane connection over DTLS tunnels for communication with SD-WAN routers
NAT traversal to connect SD-WAN routers and vSmart controllers
Load balancing of SD-WAN routers across the vSmart controllers

32. Refer to the exhibit. A junior network engineer is handed a print-out of the network information shown. Which protocol or service originated the information shown in the graphic?



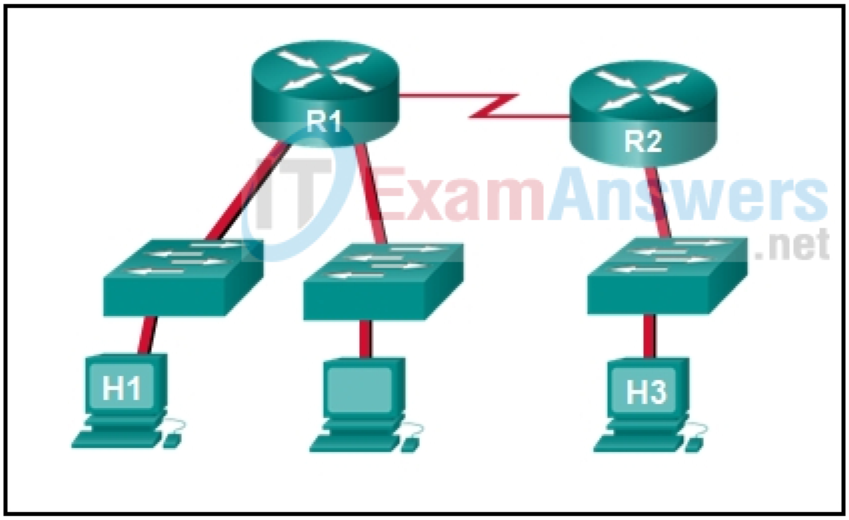
Service ● On ○ Off

	Time	HostName	Message
1	03.01.1993 12:11:00.018 AM	192.168.1.1	%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/0/0 (171)
2	10.23.2017 10:40:30.364 AM	192.168.12.2	%SYS-5-CONFIG_I: Configured from console by console
3	10.23.2017 10:40:39.985 AM	192.168.12.2	%LINK-5-CHANGED: Interface Loopback100, changed state to up
4	10.23.2017 10:40:39.985 AM	192.168.12.2	%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback100, changed state to up

- **Syslog**
- RADIUS
- NetFlow
- TACACS+

Explanation: Syslog clients send log entries to a syslog server. The syslog server concentrates and stores log entries. Log entries are categorized by seven severity levels: emergencies (0), alerts (1), critical (2), errors (3), warnings (4), notifications (5), informational (6), and debugging (7).

33. Refer to the exhibit. Host H3 is having trouble communicating with host H1. The network administrator suspects a problem exists with the H3 workstation and wants to prove that there is no problem with the R2 configuration. What tool could the network administrator use on router R2 to prove that communication exists to host H1 from the interface on R2, which is the interface that H3 uses when communicating with remote networks?



- Telnet
- show cdp neighbors
- **an extended ping**
- traceroute

Explanation: An extended ping allows an administrator to select specific ping features. For example in this situation, the network administrator could do an extended ping and specify a source address of the gigabit Ethernet port on the router. The destination address would be the IP address of host H1. If the ping succeeds connectivity exists from the Ethernet router interface on R2 to device H1.

34. In the data gathering process, which type of device will listen for traffic, but only gather traffic statistics?

- **NetFlow collector**
- SNMP agent
- NMS
- syslog server

Explanation: A NetFlow collector is the device that receives traffic statistics from networking devices. NetFlow only gathers traffic statistics, unlike syslog and SNMP which can collect various network events.

35. Which type of information can an administrator obtain with the show ip cache flow command?

- the NetFlow version that is enabled
- **the protocol that uses the largest volume of traffic**
- whether NetFlow is configured on the correct interface and in the correct direction
- the configuration of the export parameters

Explanation: The show ip cache flow command provides information about the flow of data through the network, not specific information about configuration.

36. Which network monitoring tool can provide a complete audit trail of basic information of all IP flows on a Cisco router and forward the data to a device?

- **NetFlow**
- SIEM
- SPAN
- Wireshark

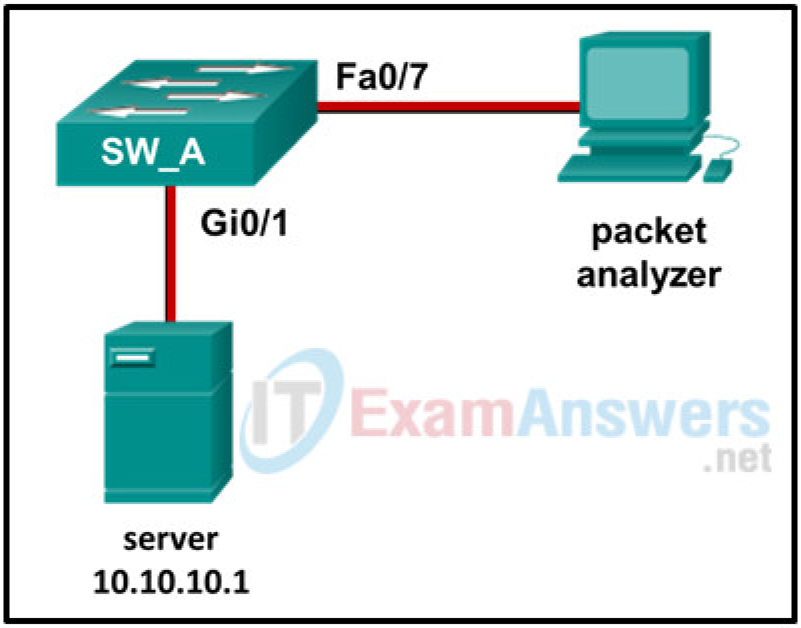
Explanation: NetFlow is a Cisco technology that provides statistics on packets flowing through a Cisco router or multilayer switch.

37. Which monitoring technology mirrors traffic flowing through a switch to an analysis device connected to another switch port?

- SIEM
- **SPAN**
- NetFlow
- SNMP

Explanation: When enabled on a switch, SPAN or port mirroring, copies frames sent and received by the switch and forwards them to another port, known as a Switch Port Analyzer port, which has a analysis device attached.

38. Refer to the exhibit. Which command or set of commands will configure SW_A to copy all traffic for the server to the packet analyzer?



Sw_A(config)# monitor session 5 source interface gi0/1
Sw_A(config)# monitor session 6 destination interface fa0/7

Sw_A(config)# monitor session 1 destination interface fa0/7

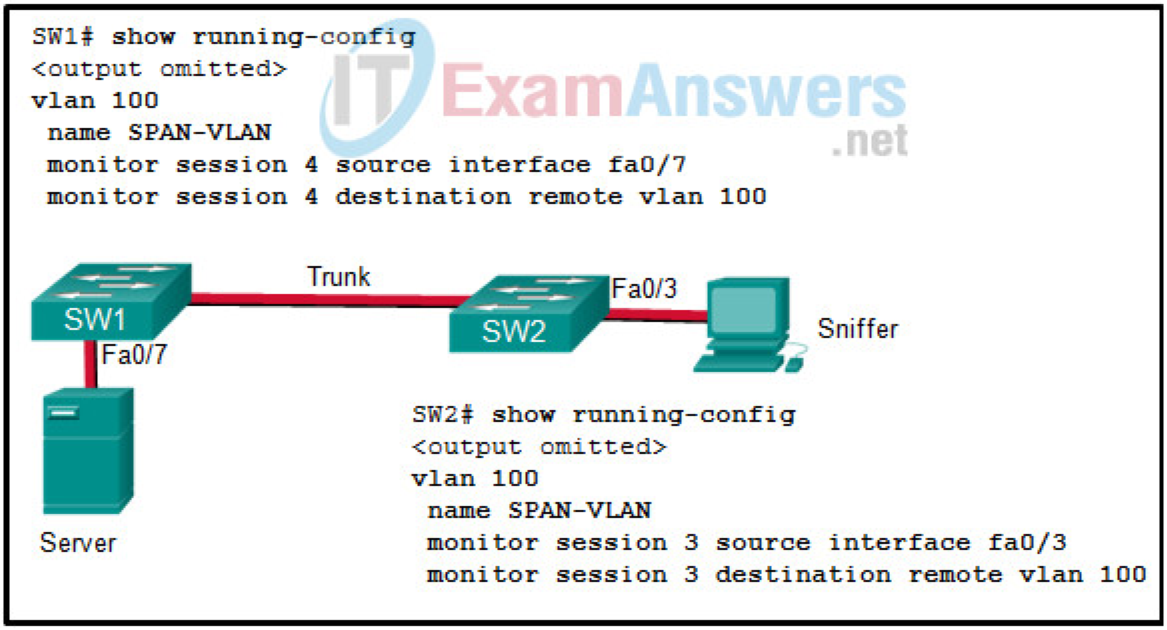
Sw_A(config)# monitor session 5 source interface gi0/1
Sw_A(config)# monitor session 5 destination interface fa0/7

Sw_A(config)# monitor session 1 destination interface gi0/1
Sw_A(config)# monitor session 1 source interface fa0/1

Sw_A(config)# monitor session 1 source interface fa0/7

Explanation: The local SPAN configuration requires two statements to identify the source and destination ports for the mirrored traffic. The statements must use the same session number. In this example, the source port is the port connected to the server (Gi0/1) and the destination port is the port attached to the packet analyzer (Fa0/7).

39. Refer to the exhibit. The RSPAN configuration for each switch is shown. The network administrator has configured RSPAN to allow the monitoring of traffic to a corporate server. Unfortunately, the administrator is unable to sniff any traffic from the link. Why is the administrator unable to sniff traffic?



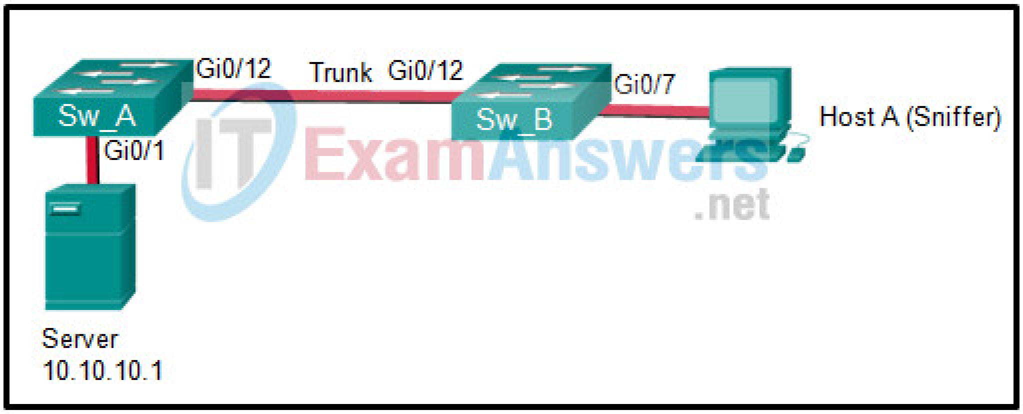
```
SW1# show running-config
<output omitted>
vlan 100
 name SPAN-VLAN
 monitor session 4 source interface fa0/7
 monitor session 4 destination remote vlan 100
```

```
SW2# show running-config
<output omitted>
vlan 100
 name SPAN-VLAN
 monitor session 3 source interface fa0/3
 monitor session 3 destination remote vlan 100
```

- **VLAN 100 has not been properly configured as an RSPAN VLAN.**
- Only VLAN 1 can be used as the RSPAN VLAN.
- The source and destination interfaces are reversed on SW2.
- The session numbers on the two switches do not match.
- The remote interface on SW1 should be identified as fa0/3.

Explanation: Both switches need the VLAN configuration mode command of remote-span to be added.

40. Refer to the exhibit. Host A is monitoring data and RSPAN is configured on Sw_A with the following commands:



```
Sw_A# show running-config

...output omitted...

monitor session 5 source interface gi0/1
monitor session 5 destination remote vlan 75

...output omitted...

vlan 75
name RSPAN
remote span
```

Which set of commands would complete the RSPAN configuration?

Sw_B(config)# monitor session 5 source remote vlan 75
Sw_B(config)# monitor session 5 destination interface gi0/12
Sw_B(config)# vlan 75
Sw_B(config-vlan)# name RSPAN
Sw_B(config-vlan)# remote-span

Sw_B(config)# monitor session 5 source interface gi0/12
Sw_B(config)# monitor session 5 destination remote vlan 75
Sw_B(config)# vlan 75
Sw_B(config-vlan)# name RSPAN
Sw_B(config-vlan)# remote-span

Sw_B(config)# monitor session 5 source interface Gi0/1
Sw_B(config)# monitor session 5 destination remote vlan 75
Sw_B(config)# vlan 75
Sw_B(config-vlan)# name RSPAN
Sw_B(config-vlan)# remote-span

Sw_B(config)# monitor session 5 source remote vlan 75
Sw_B(config)# monitor session 5 destination interface gi0/7
Sw_B(config)# vlan 75
Sw_B(config-vlan)# name RSPAN
Sw_B(config-vlan)# remote-span

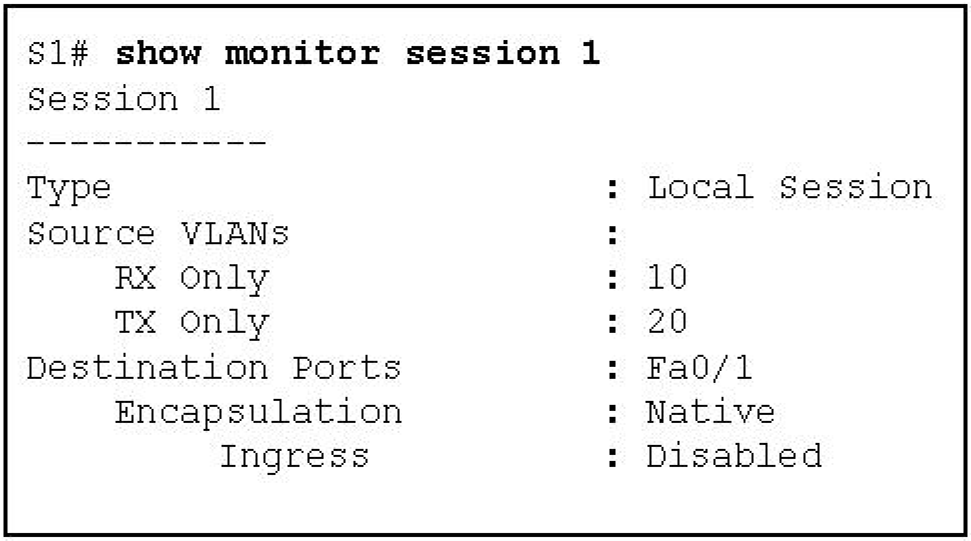
Explanation: The Sw_B configuration is almost identical to the Sw_A configuration except the destination interface for the monitor session is Gi0/12 (the port to which host A connects).

41. A network administrator is using the Cisco DNA Center to monitor network health and to troubleshoot network issues. Which area should the administrator use to perform these tasks?

- **ASSURANCE**
- PROVISION
- PLATFORM
- POLICY

Explanation: The Cisco DNA Center has five main areas:
Design – Model the entire network, from sites and buildings to devices and links, both physical and virtual, across campus, branch, WAN and cloud.
Policy – Use policies to automate and simplify network management, reducing cost and risk while speeding rollout of new and enhanced services.
Provision – Provide new services to users with ease, speed, and security across your enterprise network, regardless of network size and complexity.
Assurance – Use proactive monitoring and insights from the network, devices, and applications to predict problems faster and ensure that policy and configuration changes achieve the business intent and the user experience you want.
Platform – Use APIs to integrate with the preferred IT systems to create end-to-end solutions and add support for multi-vendor devices.

42. Refer to the exhibit. Based on the output generated by the show monitor session 1 command, how will SPAN operate on the switch?



```
S1# show monitor session 1
Session 1
-----------
Type                        : Local Session
Source VLANs                :
    RX Only                 : 10
    TX Only                 : 20
Destination Ports           : Fa0/1
    Encapsulation           : Native
         Ingress            : Disabled
```

1.JPG

- **All traffic received on VLAN 10 or transmitted from VLAN 20 is forwarded to FastEthernet 0/1.**
- All traffic transmitted from VLAN 10 or received on VLAN 20 is forwarded to FastEthernet 0/1.
- Native VLAN traffic received on VLAN 10 or transmitted from VLAN 20 is forwarded to FastEthernet 0/1.
- Native VLAN traffic transmitted from VLAN 10 or received on VLAN 20 is forwarded to FastEthernet 0/1.

Explanation: The show monitor session command is used to verify how SPAN is configured (what ports are involved in the traffic mirroring).

43. What is the description for a Syslog Level 0 event?

- error condition
- critical condition
- **system unusable**
- immediate action needed