PassQueen
a.k.a dumpsqueen.com

H19-402_V1.0HCSP-Presales-Data Center Network Planning and Design V1.0

Huawei h19-402_v1.0

Version Demo

Total Demo Questions: 7

Total Premium Questions: 73

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Data Center Network Overview	24
Topic 2, Huawei Data Center Network Solution	36
Topic 3, Data Center Network Planning and Design	13
Total	73

QUESTION NO: 1

Which of the following statements is false about IP routes?

A. The optimal route to a specific destination can be determined by only one routing protocol at a certain moment. To determine the optimal route, all routing protocols (including static routing) are configured with priorities.

B. Direct routes are the routes destined for the network segment to which directly connected interfaces belong.

C. Each routing protocol can import routes discovered by other routing protocols, direct routes, and static routes.

D. If routes to the same destination network are discovered by two routing protocols, the cost values of the routes are first compared, and then their priorities.

ANSWER: D

Explanation:

The false statement is: “If routes to the same destination network are discovered by two routing protocols, the cost values of the routes are first compared, and then their priorities.” On Huawei VRP devices, route selection between routes learned through different routing protocols starts with route preference, also called administrative preference or priority. The route with the lower preference value is preferred and is eligible to become the active route installed in the IP routing table. For example, a route learned by a protocol with a configured preference of 10 is selected ahead of an otherwise equivalent route whose protocol preference is 100.

A route cost or metric is not the first cross-protocol comparison criterion. Metrics are protocol-specific values calculated according to each protocol’s own rules, such as hop count, bandwidth, delay, or accumulated cost. Therefore, they are primarily used by a routing protocol to select among candidate routes learned by that same protocol after the protocol’s route-selection process. Huawei documents route preference as the mechanism for choosing among routes to the same destination from different sources, while protocol metrics support best-path selection within a routing domain. See Huawei’s VRP product documentation and the Huawei enterprise networking documentation portal.

QUESTION NO: 2

What are the layers in the health model of the CloudFabric Solution?

A. Service layer

B. Device layer

C. Overlay layer

D. Network layer

E. Protocol layer

ANSWER: A B C D E

Explanation:

The CloudFabric health model evaluates a data-center network end to end, rather than limiting health assessment to physical devices or a single forwarding domain. Its health-evaluation scope includes the **Service layer**, which represents the health and quality of delivered network services; the **Device layer**, which covers the operating condition and resource state of network nodes; and the **Network layer**, which assesses network connectivity, forwarding, and path conditions. It also includes the **Protocol layer**, allowing control-plane protocol status and related network behavior to be evaluated, as well as the **Overlay layer**, which is essential for assessing virtualized data-center network services built over the physical fabric.

Using these layers together enables CloudFabric intelligent operations and maintenance to correlate telemetry, alarms, logs, configuration information, and performance indicators. This layered approach helps operations personnel identify whether a detected service issue originates in infrastructure health, underlay connectivity, protocol operation, overlay-network behavior, or the delivered service itself. Therefore, all five listed layers are components of the CloudFabric health model. Huawei positions CloudFabric as an intelligent data-center networking solution with automated operations capabilities; see the Huawei CloudFabric solution overview and the Huawei CloudEngine data-center networking portfolio.

QUESTION NO: 3

Which of the following statements is false about the overlay network or underlay network?

A. The overlay network requires bare optical fibers for links.

B. The underlay network is transparent to devices (such as servers, VAS devices, and external routers) that are connected to NVEs.

C. The overlay network has an independent forwarding plane and an independent control protocol, which are VXLAN and BGP EVPN, respectively.

D. The overlay network is a logical network that is established over the underlay network through VXLAN.

ANSWER: A

Explanation:

The statement “The overlay network requires bare optical fibers for links.” is false. An overlay is a logical network constructed over an IP underlay, rather than a network defined by a particular physical transmission medium. The underlay’s role is to provide IP reachability between tunnel endpoints; it may use optical links, copper Ethernet, routed switches, or any other infrastructure capable of reliably forwarding IP packets. Optical fiber can certainly be part of a high-capacity data-center fabric, but it is not an inherent overlay requirement.

In a VXLAN-based implementation, a network virtualization edge encapsulates tenant Ethernet frames in UDP/IP packets for transport across the routed underlay. This separation allows logical tenant segments and virtual networks to be created without tying their design to individual physical links. The VXLAN specification describes this encapsulation model and the use of an IP network for the transport path: RFC 7348. When EVPN is used, its control-plane mechanisms distribute reachability information for the overlay while retaining the same underlay/overlay separation: RFC 7432. Therefore, requiring bare optical fibers incorrectly conflates physical underlay media with the logical overlay service.

QUESTION NO: 4

Which of the following technologies or protocols natively support encryption?

A. VXLAN

B. GRE

C. SSL VPN

D. IPsec VPN

ANSWER: C D

Explanation:

SSL VPN and IPsec VPN natively provide encryption because their designs include cryptographic protection as a fundamental function rather than merely carrying encapsulated traffic. SSL VPN establishes protected remote-access sessions using SSL/TLS. TLS negotiates cryptographic parameters and protects data exchanged between the client and VPN gateway, providing confidentiality for authorized application or network-access traffic. This makes SSL VPN appropriate where users need secure access across an untrusted network such as the Internet.

IPsec VPN provides security at the IP layer. Its security architecture supports authenticated key management and security associations, while Encapsulating Security Payload can provide confidentiality through encryption as well as integrity and origin authentication protections. Consequently, IPsec is a standard choice for encrypted site-to-site VPN connectivity, including enterprise branch and data-center interconnection scenarios. Huawei VPN solutions use both SSL VPN and IPsec VPN as security technologies for protected communications. The Internet Engineering Task Force defines the IPsec architecture in RFC 4301 and the TLS protocol used by SSL-based secure communications in RFC 8446. Therefore, the technologies with native encryption support are SSL VPN and IPsec VPN.

QUESTION NO: 5

(During data center network design, if the number of TOR switches is less than 100, which of the following protocols is recommended for underlay routing?)

A. IS-IS

B. RIP

C. OSPF

D. BGP

ANSWER: C

Explanation:

OSPF is the recommended underlay routing protocol when a data center has fewer than 100 ToR switches. At this scale, OSPF provides a practical balance of fast convergence, link-state visibility, equal-cost multipath forwarding support, and straightforward operations. A spine-leaf underlay requires all leaf-to-spine links to be advertised reliably and to converge quickly after a link or device failure; OSPF supplies these capabilities using its link-state database and shortest-path-first calculation.

For a relatively small fabric, the operational model remains manageable: the OSPF topology database, route scale, and neighbor relationships do not impose the complexity that can become significant in very large fabrics. Network designers can use point-to-point OSPF interfaces and ECMP routes across the spine layer to create the required resilient IP fabric for overlay traffic. This lets the underlay deliver stable IP reachability while VXLAN/EVPN or other overlay technologies provide virtual-network services. Huawei's data-center networking materials describe the spine-leaf fabric approach and its use of dynamic routing, while Huawei routing documentation details OSPF's link-state and ECMP capabilities. See Huawei Data Center Networking and Huawei OSPF Configuration Documentation.

QUESTION NO: 6

(In the intelligent O & M scenario of the CloudFabric Solution, which of the following southbound collection protocol is not supported?)

A. NetStream

B. Qx

C. ERSPAN

D. SNMP

E. Telemetry

ANSWER: B

Explanation:

Qx is the correct answer because it is not a recognized southbound data-collection protocol in Huawei CloudFabric intelligent operations and maintenance architecture. CloudFabric's intelligent O&M capabilities obtain device, performance, traffic, and packet-level information through established network-management and observability mechanisms. These mechanisms support automated visibility, fault analysis, and service assurance across the data-center fabric. Huawei's CloudFabric solution emphasizes intelligent management and O&M based on collection of real-time network data and traffic information from network devices. Qx does not identify a Huawei-defined telemetry, network-management, flow-export, or traffic-mirroring interface used for this purpose. Therefore, it cannot serve as a supported southbound collection protocol in the stated scenario. This conclusion is consistent with Huawei's CloudFabric solution overview, which describes intelligent network operations based on device and network data collection, and Huawei's documentation describing telemetry as a data-subscription and streaming mechanism for network monitoring. See Huawei's CloudFabric product page and Telemetry overview.

QUESTION NO: 7

A customer plans to deploy VXLAN services between leaf switches in a new spine-leaf fabric. Select three design requirements that ensure tenant traffic can be encapsulated and transported reliably across the underlay network.

A. Ensure that the underlay provides IP reachability between VTEP addresses.

B. Plan an IP MTU that accommodates VXLAN encapsulation overhead.

C. Map the intended Layer 2 service to a consistent VNI on participating VTEPs.

D. Require BGP EVPN as the only supported VXLAN control plane.

E. Configure the same local VLAN ID for the tenant on every leaf switch.

ANSWER: A B C

Explanation:

VXLAN requires IP reachability between VTEP addresses so that the outer IP packets can traverse the underlay. A loopback interface is normally used as the stable VTEP source address, and the underlay routing protocol must advertise reachability to that address. The IP MTU must also accommodate VXLAN encapsulation overhead; otherwise, large tenant packets can be fragmented or dropped. In addition, the Layer 2 service must be mapped consistently to the intended VXLAN network identifier on the relevant VTEPs.

BGP EVPN is a commonly used overlay control plane, but it is not the only possible control-plane option and is therefore not an absolute prerequisite for VXLAN encapsulation. A tenant VLAN does not need to use the same local VLAN ID on every leaf, because the VNI identifies the overlay segment.