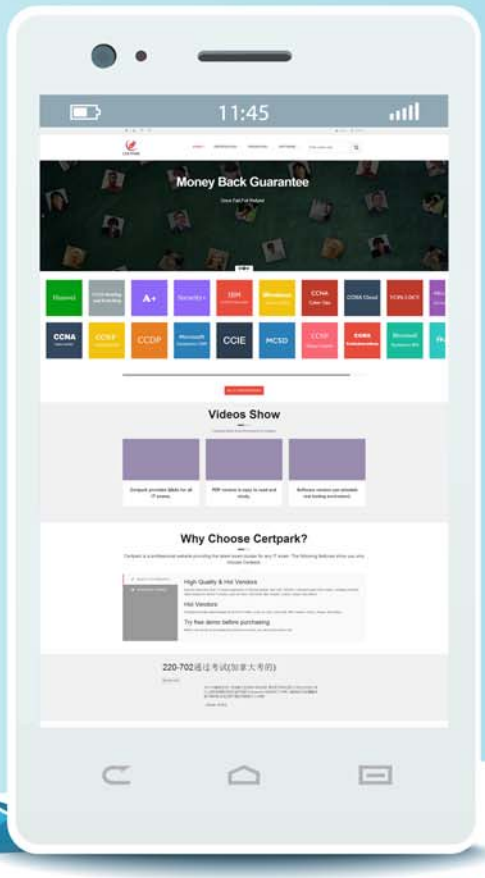
CERTPARK

QUESTION & ANSWER

CERTPARK.COM

Accurate Study Guides,
High Passing Rate!
provides update
free of charge
in one year!



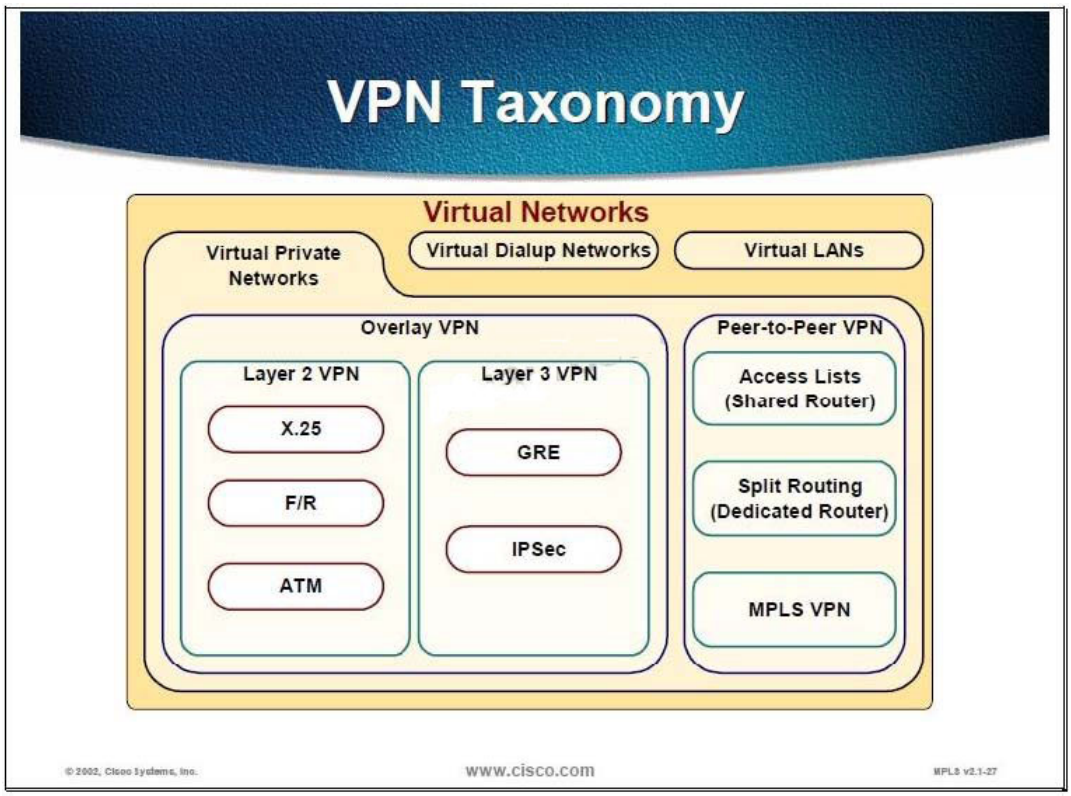
https://www.certpark.com

Exam : **642-889**

Title : Implementing Cisco Service Provider Next-Generation Egde Network Services

Version : DEMO

1.Which type of VPN requires a full mesh of virtual circuits to provide optimal site-to-site connectivity?
A. MPLS Layer 3 VPNs
B. Layer 2 overlay VPNs
C. GET VPNs
D. peer-to-peer VPNs
Answer: B
Explanation:



http://etutorials.org/Networking/MPLS+VPN+Architectures/Part+2+MPLSbased+Virtual+Private+Networks/Chapter+7.+Virtual+Private+Network+VPN+Implementation+Options/Overlay+and+Peerto-peer+VPN+Model/
Two VPN implementation models have gained widespread use: The overlay model, where the service provider provides emulated leased lines to the customer. The service provider provides the customer with a set of emulated leased lines. These leased lines are called VCs, which can be either constantly available (PVCs) or established on demand (SVCs). The QoS guarantees in the overlay VPN model usually are expressed in terms of bandwidth guaranteed on a certain VC (Committed Information Rate or CIR) and maximum bandwidth available on a certain VC (Peak Information Rate or PIR). The committed bandwidth guarantee usually is provided through the statistical nature of the Layer 2 service but depends on the overbooking strategy of the service provider The peer-to-peer model, where the service provider and the customer exchange Layer 3 routing information and the provider relays the data between the customer sites on the optimum path between the sites and without the customer's involvement. The peer-to-peer VPN model was introduced a few years ago to alleviate the drawbacks of the overlay VPN model. In the peer-to-peer model, the Provider Edge (PE) device is a router (PE-router) that directly exchanges routing information with the CPE router. The Managed Network service offered by many service providers, where the service provider also manages the CPE devices, is not relevant to this

discussion because it's only a repackaging of another service. The Managed Network provider concurrently assumes the role of the VPN service provider (providing the VPN infrastructure) and part of the VPN customer role (managing the CPE device).
The peer-to-peer model provides a number of advantages over the traditional overlay model: Routing (from the customer's perspective) becomes exceedingly simple, as the customer router exchanges routing information with only one (or a few) PE-router, whereas in the overlay VPN network, the number of neighbor routers can grow to a large number. Routing between the customer sites is always optimal, as the provider routers know the customer's network topology and can thus establish optimum inter-site routing. Bandwidth provisioning is simpler because the customer has to specify only the inbound and outbound bandwidths for each site (Committed Access Rate [CAR] and Committed Delivery Rate [CDR]) and not the exact site-to-site traffic profile. The addition of a new site is simpler because the service provider provisions only an additional site and changes the configuration on the attached PE-router. Under the overlay VPN model, the service provider must provision a whole set of VCs leading from that site to other sites of the customer VPN.
Prior to an MPLS-based VPN implementation, two implementation options existed for the peer-topeer VPN model: The shared-router approach, where several VPN customers share the same PE-router. The dedicated-router approach, where each VPN customer has dedicated PE-routers. Overlay VPN paradigm has a number of drawbacks, most significant of them being the need for the customer to establish point-to-point links or virtual circuits between sites. The formula to calculate how many point-to-point links or virtual circuits you need in the worst case is ((n)(n-1))/2, where n is the number of sites you need to connect. For example, if you need to have full–mesh connectivity between 4 sites, you will need a total of 6 point-to-point links or virtual circuits. To overcome this drawback and provide the customer with optimum data transport across the Service Provider backbone, the peer-to-peer VPN concept was introduced where the Service Provider actively participates in the customer routing, accepting customer routes, transporting them across the Service Provider backbone and finally propagating them to other customer sites.

2.Which three Layer 3 VPN technologies are based on the overlay model? (Choose three.)
A. ATM virtual circuits
B. Frame Relay virtual circuits
C. GRE/IPsec
D. L2TPv3
E. MPLS Layer 3 VPNs
F. DMVPNs
Answer: C,D,F
Explanation:
The overlay model, where the service provider provides emulated leased lines to the customer. The service provider provides the customer with a set of emulated leased lines. These leased lines are called VCs, which can be either constantly available (PVCs) or established on demand (SVCs). The QoS guarantees in the overlay VPN model usually are expressed in terms of bandwidth guaranteed on a certain VC (Committed Information Rate or CIR) and maximum bandwidth available on a certain VC (Peak Information Rate or PIR). The committed bandwidth guarantee usually is provided through the statistical nature of the Layer 2 service but depends on the overbooking strategy of the service provider
The peer-to-peer model, where the service provider and the customer exchange Layer 3 routing

information and the provider relays the data between the customer sites on the optimum path between the sites and without the customer's involvement.
The peer-to-peer VPN model was introduced a few years ago to alleviate the drawbacks of the overlay VPN model. In the peer-to-peer model, the Provider Edge (PE) device is a router (PErouter) that directly exchanges routing information with the CPE router. The Managed Network service offered by many service providers, where the service provider also manages the CPE devices, is not relevant to this discussion because it's only a repackaging of another service. The Managed Network provider concurrently assumes the role of the VPN service provider providing the VPN infrastructure) and part of the VPN customer role (managing the CPE device).
The peer-to-peer model provides a number of advantages over the traditional overlay model: Routing (from the customer's perspective) becomes exceedingly simple, as the customer router exchanges routing information with only one (or a few) PE-router, whereas in the overlay VPN network, the number of neighbor routers can grow to a large number.
Routing between the customer sites is always optimal, as the provider routers know the
customer's network topology and can thus establish optimum inter-site routing. Bandwidth provisioning is simpler because the customer has to specify only the inbound and outbound bandwidths for each site (Committed Access Rate [CAR] and Committed Delivery Rate [CDR]) and not the exact site-to-site traffic profile.
The addition of a new site is simpler because the service provider provisions only an additional site and changes the configuration on the attached PE-router. Under the overlay VPN model, the service provider must provision a whole set of VCs leading from that site to other sites of the customer VPN.
Prior to an MPLS-based VPN implementation, two implementation options existed for the peer-topeer VPN model: The shared-router approach, where several VPN customers share the same PE-router. The dedicated-router approach, where each VPN customer has dedicated PE-routers.

3.Which VPN technology uses the Group Domain of Interpretation as the keying protocol and IPsec for encryption that is often deployed over a private MPLS core network?
A. DMVPN
B. GET VPN
C. SSL VPN
D. L2TPv3
Answer: B
Explanation:
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6635/ps7180/deployment_guide_c07_554713.html

4.What is the primary difference between 6PE and 6VPE?
A. 6VPE does not require an MPLS core.
B. 6VPE requires an IPv6-aware core.
C. 6VPE provides IPv6 VPN services.
D. 6VPE tunnels IPv6 packets inside IPv4 packets.
Answer: C
Explanation:
6PE is for transporting ipv6 natively and 6VPE is for ipv6 mpls vpns

5.Refer to the Cisco IOS XR router output exhibit,

```
RP/0/RP1/CPU0:R1#show route vrf red ipv6

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - ISIS, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, su - IS-IS summary null, * - candidate default
       U - per-user static route, o - ODR, L - local
Gateway of last resort is not set
B    2001:db80:beef:1::/64
     [200/0] via ::ffff:192.168.253.6 (nexthop in vrf default),07:04:14
```

which method is being used to transport IPv6 traffic over the service provider network?

A. 6PE

B. 6VPE

C. native IPv6

D. native IPv4

E. dual stack

Answer: B

Explanation:

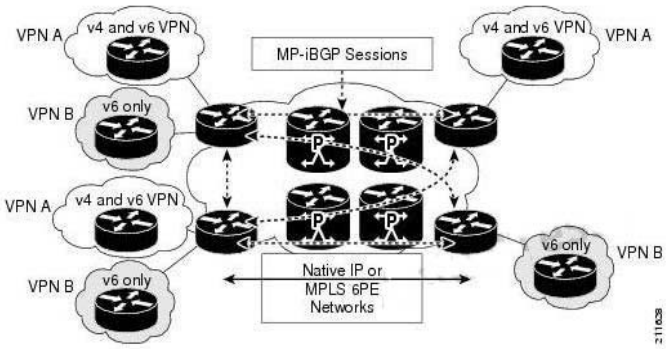
NOT SURE THIS MATCHES ANSWER

IPv6 VPN Provider Edge Router (6VPE)

Cisco Systems's 6VPE solution smoothly introduces IPv6 VPN service in a scalable way, without any IPv6 addressing restrictions. It does not jeopardize a well-controlled service provider IPv4 backbone or any customer networks. VPN service backbone stability is a key issue for those service providers who have recently stabilized their IPv4 infrastructure. For IPv4 VPN customers, IPv6 VPN service is exactly the same as MPLS VPN for IPv4.

The IPv6 MPLS VPN service model is similar to that of IPv4 MPLS VPNs. Service providers who have already deployed MPLS IPv4 VPN services over an IPv4 backbone can deploy IPv6 MPLS VPN services over the same IPv4 backbone by upgrading the PE router IOS version and dual-stack configuration, without any change on the core routers. IPv4 services can be provided in parallel with IPv6 services. A PE-CE link can be an IPv4 link, an IPv6 link, or a combination of an IPv4 and IPv6 link, as shown in Figure 4-1.

Figure 4-1 6VPE Deployment



IPv6 VPN service is exactly the same as MPLS VPN for IPv4. 6VPE offers the same architectural features as MPLS VPN for IPv4. It offers IPv6 VPN and uses the same components, such as:

- Multiprotocol BGP (MP-BGP) VPN address family
- Route distinguishers
- VPN Routing and Forwarding (VRF) instances
- Site of Origin (SoO)
- Extended community
- MP-BGP

The 6VPE router exchanges either IPv4 or IPv6 routing information through any of the supported routing protocols, and switches IPv4 and IPv6 traffic using the respective fast switching CEF or distributed CEF path over the native IPv4 and IPv6 VRF interfaces. The 6VPE router exchanges reachability information with the other 6VPE routers in the MPLS domain using Multiprotocol BGP, and shares a common IPv4 routing protocol (such as OSPF or IS-IS) with the other P and PE devices in the domain. Separate routing tables are maintained for the IPv4 and IPv6 stacks. A hierarchy of MPLS labels is imposed on an incoming customer IPv6 packet at the edge LSR:

- Outer label (IGP Label) for iBGP next-hop, distributed by LDP.
- Inner label (VPN Label) for the IPv6 prefix, distributed by MP-BGP.

Incoming customer IPv6 packets at the 6VPE VRF interface are transparently forwarded inside the service provider's IPv4 core, based on MPLS labels. This eliminates the need to tunnel IPv6 packets. P routers inside the MPLS core are unaware that they are switching IPv6 labelled packets.