CISCO SDWAN

INTERVIEW

QUESTIONS AND ANSWERS

www.networkershome.com

Ques 1. What are typical challenges in a WAN setup for any organization?
Below is list of common challenges faced with a WAN setup -

- Insufficient bandwidth
- Limited Application Awareness
- Fragmented Security
- No Cloud App Readiness
- Limited Scale
- High Cost
- Complex Operation

Ques 2. What are the benefits that SDWAN Viptela solution provides?
The key benefits that SDWAN Viptela solution renders are -

- Centralized routing intelligence and segmentation.
- Secure the network automatically.
- Managed via Central managed engine vManage.
- Influence reachability through centralized policy.
- Cloud readiness.

Ques 3. What is vManage NMS?
The vManage Network Management System is a centralized NMS that lets you configure and manage the whole overlay network from a simple GUI dashboard.

Ques 4. What is vSmart Controller?
The vSmart controller is the centralized engine of the Viptela solution, controlling and analysing the flow of data traffic throughout the network. The vSmart controller works with the vBond orchestrator to authenticate Viptela edge devices as they join the network and to orchestration connectivity among the vEdge routers.

Ques 5. What is vBond Orchestrator?
The vBond orchestrator automatically orchestrates connectivity in between the vEdge routers and the vSmart controllers. If the vEdge router or vSmart controller is behind a NAT, the vBond orchestrator also serves as an initial NAT-transversal orchestrator.

Ques 6. What are vEdge Routers?
The vEdge routers sit at the perimeter of a site (such as remote offices, branch, campuses, data centers) and provide connectivity among the sites. They can be either hardware devices or software called a vEdge cloud router that runs as a virtual machine. vEdge router handles the transmission of data traffic.

Ques 7. Provide comparison details of vEdge Routers wrt their technical specifications?
Below table depicts comparison of various variants of vEdge Routers –

vEdge 1000	vEdge 2000	vEdge 100	vEdge 100M
1 RU Rack Size	1 RU Rack Size	9" 1.75" *5.5"	9.19" 11.94" *5.375"
8 * GE SFP	4* Fixed GE SFP 2 Protocol Independent Module 8* 1 GE SFP 2* 10 GE SFP+	5 Ethernet Ports	5 Ethernet Ports One POE port Modem wireless MC7330
3G/4G via USB/Ethernet	3G/4G via USB/Ethernet	GPS	GPS/Built in LTE with Mini SIM
Encryption/QoS	Encryption/QoS	Security QoS	Security QoS
Dual Power Supplies	Dual Power Supplies	External AC Power	External AC Power
Low Power Consumption	Redundant Fans	Fan Less	Fan Less
TPM Chip	TPM Chip	TPM Chip	TPM Chip
1 GBPS capacity	10 GBPS capacity	100 MBPS AES-256	

Ques 8. Explain SDWAN architecture?

Cisco SD-WAN uses an abstracted architecture and is divided into the control plane and the forwarding plane. The SD-WAN architecture moves the control plane to a centralized location like an organization's headquarters to manage SD-WAN devices for central management. By doing so network can be managed remotely without the need for an on-premises support.

- **Data Plane:** Cisco SD-WAN solution refer to data plane as a WAN edge. WAN edge could be CISCO vEdge router or CISCO XE SD-WAN router. Data plane device are deployed at branch, data center, Large campus, colocation facilities. The vEdge routers are placed at the perimeter of a site (such as remote offices, branch, campuses, and data centers) and provide connectivity among the sites. vEdge can be either hardware devices or software that runs as a virtual machine. vEdge router handles the transmission of data traffic.
- **Management Plane:** vManage manages the management plane in SD-WAN. It can be utilized for onboarding, provisioning, policy creation, S/W management, troubleshooting and monitoring. vManage also supports communication via REST and NETCONF. Each WAN edge will form a single management plane connection to vManage.
- **Control Plane:** vSmart provides control plane functionality. vSmart is responsible for implementing control plane policies, centralized data policy and VPN topologies. vSmart learns all its routing information. It is the centralized control engine of the SD-WAN solution, controlling the flow of data traffic throughout the network. The vSmart controller works with the vBond orchestrator to authenticate SD-WAN devices as they join the network and to orchestration connectivity among the vEdge routers.
- **Orchestration Plane:** vBond manages orchestration plane in SD-WAN. The vBond orchestrator automatically orchestrates connectivity between vEdge routers and vSmart controllers with secure tunnel.

Ques 9. Explain entire Cisco SD-WAN system bring up process?

Below is the step by step process of SD-WAN solution process -

- Install hypervisor (KVM) on the server.
- Spin-up virtual machine on the server.
- Install images for vManage, vBond, vSmart and vEdges on the VMs.
- Create a minimal configuration for vManage (Deploy vManage) device.
- Create a minimal configuration for vBond (Deploy vBond) device.
- Create a minimal configuration for vSmart (Deploy vSmart) device.
- Enable connectivity between controllers.
- Generate CSR for each controller (overlay connection).
- Sign certificate to validate and authenticate the controller.

Ques 10. Explain in simple steps on how to bring up vEdge?

- Create a minimal configuration for vEdge and establish IP connectivity into the WAN circuits.
- Verify the vEdge router can reach the controller.
- Authenticate the vEdge router with vManage.
- Register each vEdge router with vManage.
- Verify that the vEdge are up in the vManage GUI dashboard.

Ques 11. What is the process of establishing Tunnel between vSmart/vManage/vBond?

- Certificates are exchange and mutual authentication take place.
- vBond validates vSmart controller and vManage certificate and serial number against authorized white-list added.
- vSmart controller and vManage validate vBond orchestrator certificate organization name against locally configured one.
- DTLS/TLS secure connection is established.

Ques 12. How does vEdge router establish identity on controllers?

- Private and Public keys are generated on the vEdge router.
- Certificate is generated.
- Certificate is signed by Avnet.
- Certificate is saved in the TPM-lite chip on the vEdge router.
- vEdge router has a root CA trust chain certificate.

Ques 13. What is TPM and what is its role?

TPM Chip is Trusted Platform Chip. TPM chip is used to load certificate on the vEdge router.

Ques 14. Illustrate the step by step secured connection establishment between SDWAN components?

- Certificates are exchange and mutual authentication takes place between vBond and vEdge – over IPSec encrypted tunnel.
- vBond validates vEdge router serial number and chassis ID against authorize vEdge white-list.
- vEdge router validates vBond certificate organization name against locally configured one.
- Provisional DTLS/TLS tunnel is established between vBond and vEdge.
- vBond returns to vEdge a list of vSmart controller and vManage.
- vBond notifies vSmart and vManage of vEdge router public IP address.
- Provisional DTLS/TLS tunnel terminated between vBond and vEdge.

Ques 15. How is connection secured between vEdge router and vSmart controller and vManage?

- Certificates are exchange and mutual authentication takes place between vSmart, vManage and vEdge.
- vSmart and vManage validates the vEdge router's serial number and chassis id against the authorize vEdge white-list.
- vEdge router validate vSmart and vManage certificate organization name against locally configured one.
- Permanent DTLS/TLS tunnel established between vEdge, vSmart and vManage.

Ques 16. Does SD-WAN deployment play important role in cloud-based and SaaS applications?

Yes, SD-WAN plays important role in Cloud-based and SaaS Applications.

Ques 17. Which of the main drivers for SD-WAN deployment?

- SD-WAN has ability to add edge branch sites more quickly
- SD-WAN meets the need for better connectivity to cloud applications using various links.
- Efficient network use resulting in cost savings

Ques 18. What's the difference between do-it-yourself (DIY) SD-WAN and managed SD-WAN deployment?

- DIY SD-WAN, enterprises purchase SD-WAN products directly from vendors and deploy the service themselves.
- Managed SD-WAN, enterprises purchase services through providers, rather than product vendors, and the providers manage the networks for the enterprises.

Ques 19. Which security features are most common to SD-WAN products?

- Traffic encryption
- Firewall capabilities
- Network segmentation

Ques 20. Is Scalability an important feature when it comes to SD-WAN deployment?

Yes

Ques 21. What are the basic SD-WAN features?

- Application-aware routing policy for best path selection and failover.
- Centralized management and real-time monitoring.
- SD-WAN is able to use multiple WAN connections, i.e. MPLS and broadband internet.

Ques 22. Does SD-WAN deployment limit hardware throughout at branch sites?

No

Ques 23. What are the prerequisites for SD-WAN deployment?

- A wide area network.
- A physical or virtual SD-WAN appliances at each site.
- Knowledge of existing WAN traffic patterns and existing WAN links

Ques 24. What is the principle underlying technology behind SD-WAN technology emerge?

SD-WAN stemmed from SDN technology that separates the control plane from the data plane and centralizes control and management.

Ques 25. What is the Cisco SD-WAN Solution?

Traditional Wide Area Networks (WAN) was designed using Multi-Protocol Label Switching (MPLS) for connectivity where majority of branch office traffic flows within an enterprise's intranet boundary. This infrastructure change creates a new requirement for security, application performance, cloud connectivity, WAN Management, and operations. Cisco SD-WAN offers a new way to manage and operate WAN Infrastructure and it is a cloud based solution that delivers a secure, flexible, and rich services architecture and scalability.

Ques 26. Which problems can a Cisco SD-WAN overcome which other SD-WAN Vendor can't?

Enlisted below are some of problems which Cisco SD-WAN Solutions can offer:

- Establish a transport independent WAN for high diversity and low cost and scalable.
- Due to low latency, SD-WAN meet Service Level Agreements (SLAs) for business critical and real time applications.
- SD-WAN provides End-to-End Segmentation for protecting critical enterprise compute resources.

Ques 27. Which sectors and industries have deployed the Cisco SD-WAN Solutions?

Cisco has one of the most widely deployed across enterprise SD-WAN solutions within the industry. Large deployments have been made in sectors like

- Retail
- Healthcare
- Financial services
- Energy

SD-WAN solution is deployed across Fortune 2000 enterprises with thousands of production sites in major industries including healthcare, manufacturing, retails, energy, oil and gas, insurance, finance, government, logistics, and distribution as some examples.

Ques 28. How is CISCO SD-WAN Solution managed and operated?

- Cisco SD-WAN is a centrally managed, orchestrated, and operated solution with a cloud-hosted Cisco vManage GUI management and provisioning platform, vSmart controller, and vBond orchestration layer at the core of the solution.
- vSmart Controllers are the centralized brain of the SD-WAN solution that implements policies and connectivity between SD-WAN vEdge branches.
- vBond Orchestrator initially bring-up by performing authentication and authorization of all components into the network.
- Cisco vManage manages the entire solution. Cisco's GUI based centralized management and provisioning platform.

Ques 29. What are vSmart CONTROLLERS?

vSmart Controllers are the centralized engine of the SD-WAN solution that apply policy and connectivity between SD-WAN vEdge branches. SD-WAN vSmart Controllers provide centralized policy engine to manipulate routing information, access control, segmentation, extranets, and service chaining.

Ques 30. What is function of vBond orchestrator?

The vBond Orchestrator simplifies the initial bring-up by performing authentication and authorization of all elements into the network. Cisco vBond Orchestrator connects other components. vBond orchestrator plays an important role in facilitating Cisco SD-WAN devices that sit behind the Network Address Translation (NAT) to communicate with the network.

Ques 31. What is the cisco vManage?

Cisco vManage maintains the entire solution. Cisco's GUI based centralized management and provisioning platform for the whole Cisco SD-WAN infrastructure. It provides the ability to manage all aspects of the WAN from provisioning, monitoring, and upgrading routers to application visibility and troubleshooting the WAN.

Ques 32. Does Cisco SD-WAN Solution Support Network Segmentation and what are its benefits?

Yes, the Cisco SD-WAN solution supports network segmentation. Logical isolation on SD-WAN network, where each segment is defined as a separate VPN and controlled centrally by access-control policies. Some of the benefits of Network segmentation are:

- Increased security.
- Acquisitions can be integrated on the parent network and yet kept separate. Policies control what applications the acquired company can access.
- Guest Wi-Fi can be maintained on a separate, low-priority segment and offloaded onto the internet at the closest exit points.
- Business partners can each be defined in a separate segment or in a collective business-partner network segment. Polices control the access of business partners to data center applications.

Ques 33. What are the SD-WAN Security capabilities?

Cisco SD-WAN Security capabilities include

- An application-aware enterprise firewall
- Intrusion prevention
- DNS Layer Enforcement (Cisco Umbrella)
- URL filtering.
- It reduces complexity by having a single management interface (vManage) for both the network and security.

Ques 34. Can the Cisco SD-WAN Solution provide optimization for IaaS and SaaS platforms like AWS, Microsoft Azure and Office 365, Google, Salesforce.com, Cisco Webex, etc?

Yes, the Cisco SD-WAN fabric connects users at the branch to applications in the cloud in a seamless, secure, and reliable fashion. Cisco delivers this comprehensive capability for Infrastructure-asa-Service and Software-as-a-Service (IaaS/SaaS) applications with Cisco Cloud OnRamp, and is currently available with vEdge series platform SD-WAN solutions.

Ques 35. Does the Cisco SD-WAN Solution support Multi-Tenancy?

Yes, a Service Provider can manage multiple customers, called tenants, from vManage that is running in multitenant mode. All tenants share a single vBond orchestrator.

Ques 36. Is Cisco's SD-WAN solution programmable and does it support APIs?

Yes, the Cisco SD-WAN Solution is Open and Programmable and with open APIs, Cisco SD-WAN provides service providers and partners the opportunity to create new and unique services, including operational and business support systems. As part of the SD-WAN developer resources availability and learning content, there are two additional resources that are a great value added service for developers:

- DevNet Ecosystem Exchange
- DevNet Code Exchange

Ques 37. Is SD-WAN replacement of MPLS?

Multi-protocol label switching (MPLS) is a common choice for implementing reliable, high-performance wide area networking (WAN). However, it has its limitations, and causing many organizations to seek alternative options for their WAN connections. Software-defined WAN (SD-WAN) enables organizations to remove the constraints of legacy networking technologies and create a flexible, reliable, and high-performance network.

Ques 38. Why should one opt for SDN?

- Application Experience
- Best in Class Integrated Security
- Cloud Optimized
- Operational Simplification
- Rich Analytics

Ques 39. What is the latest software release version for the Cisco IOS XE SD-WAN image supported on the Cisco 1000 and 4000 Series ISRs, ASR 1000 Series, and 5000 Series ENCS platforms?

Cisco IOS XE SD-WAN Software Release 16.11.1 as on Mar2021.

Ques 40. Which all routing protocols are supported by Cisco SD-WAN Solution?

- OSPF
- external BGP (eBGP)
- internal BGP (iBGP)
- EIGRP
- Static
- Connected

Ques 41. What is Viptela SD-WAN?

Viptela was formed by the triumvirate of Alcatel Lucent, Cisco, and Juniper Networks network architects working on Software Defined Networking (SDN) at the WAN level.

Ques 42. What are the components of Viptela SD-WAN?

Components of Viptela SD-WAN are -

- **vSmart Controller –** vSmart controller is central management of routing, policy, security, segmentation, and authentication of devices.
- **vManage –** It is centralized dashboard for configuration and management.
- **vEdge Routers –** IP routers that perform standard functions such as BGP, OSPF, ACLs, QoS, and various routing policies in addition to the overlay communication.
- **vBond Orchestrator –** vBond orchestrator provides initial authentication and authorization of all elements into the network. It provides the information on how each of the components connects to other components.

Ques 43. What is Domain ID?

A domain is a logical grouping of vEdge routers and vSmart controllers that demarcates the span of control for the vSmart controllers. Each of the domain is identified by a unique integer called the domain ID. Currently, you can configure only one domain in a Viptela Overlay Network. Within a same domain, vEdge routers can connect only with the vSmart controllers in their own domain.

Ques 44. What are OMP Routes?

OMP is the control protocol that is used to exchange routing, policy, and management information between the vSmart controllers and vEdge routers in the overlay network. It is enabled by default, so after you start up the vSmart controllers and vEdge routers, it is not necessary to explicitly configure or enable OMP.

Ques 45. What are types of routes wrt SD-WAN?

- Transport Locations (TLOCs)
- Service Routes
- OMP Routes (vRoutes)

Ques 46. What is Site ID?

Site is a particular physical location within the Viptela Overlay Network, such as a branch office, a data center, or a campus. Each site is identified by a unique integer, called a Site-ID, and a site is identified by the same site ID. All the vSmart controllers and any vEdge routers are configured with the same site ID within a site.

Ques 47. What is System IP Address?

Each vEdge router and vSmart Controller is assigned a system IP address, which identifies the physical system independently of any interface addresses. System IP address is similar to the Router ID on a regular router. It provides permanent network overlay addresses for vEdge routers and vSmart controllers, and allows the physical interfaces to be renumbered as needed without affecting the reachability of the Viptela device.

Ques 48. What is TLOC?

TLOC, or Transport Location, identifies the physical interface where a vEdge router connects to the WAN Transport Network or to a NAT gateway. In contrast with BGP, the TLOC acts as the next hop for OMP routes. Transport Location is the only entity of the OMP routing domain that is visible to the underlying network, and it must be reachable through routing in the underlying network. TLOC can be accessible by an entry in the routing table of the physical network.

Ques 49. Give a brief about Cisco SD-WAN Solution Architecture.

The Cisco SD-WAN solution incorporates separate orchestration, management, control, and data planes.

- Orchestration plane is responsible for the automatic on boarding of the SD-WAN routers.
- Management plane is responsible for central configuration and monitoring.
- Control plane creates and maintains the network topology and makes decisions on where traffic flows.
- Data plane is responsible for forwarding packets based on decisions from the control plane.

Ques 50. What is a Color wrt vEdge Routers?
On vEdge routers, the color attribute helps to identify an individual WAN transport tunnel. Color should be unique on single vEdge router.

Ques 51. Draw TLOC Routes and OMP?

Ques 52. What is a Zero-Touch Provisioning (ZTP) Process?
ZTP (Zero Touch Provisioning) is an automatic provisioning procedure which starts when the vEdge router is powered up for the first time. vEdge will try to connect to a ZTP server with the hostname ztp.viptela.com, where it will get its vBond orchestrator information. When vBond orchestrator information is obtained and connections to the vManage and vSmart controllers to get its full configuration and join the overlay network.

Ques 53. What are the requirements for ZTP Provisioning?
Certain ports on vEdge appliances are configured by default as client interface and can be used for ZTP. vEdge router in the network should have access to reach ztp.viptela.com. Device configuration template for vEdge router is pushed by vManage for configuration. ZTP needs system IP and site ID to complete configuration.

Ques 54. What are Controller Connections?
When a vEdge router has multiple tunnel interfaces and hence multiple TLOCs, the router establishes only a single control connection to the vManage NMS. The router chooses a TLOC at random for this control connection, selecting one that is operational (that is, one whose administrative status is up). If the chosen TLOC becomes non-operational, the router chooses another one. The secure sessions between the vEdge routers and the controllers (and between controllers), by default are DTLS, which is User Datagram Protocol (UDP)-based. The default base source port is 12346. IPSec tunnels and BFD formed between a vEdge routers use UDP with similar ports as defined by DTLS.

Ques 55. What are Configuration templates?
Configurations and policies are applied to vEdge routers and vSmart controllers which enable traffic to flow between the data center and between the branches. Administrators can push configurations
and policies via the Command-Line Interface (CLI) using console or Secure Shell (SSH) on the vEdge device, or remotely through the vManage GUI.

Ques 56. What is a Device Template?
Device templates are specific to only one vEdge, but you may need to create multiple device templates of the same model type due to their location and function in the network. Device template features all configuration of device. Device template can't be shared between vEdge models, but a feature template can span across several model types and be used by different device templates.

Ques 57. Mention Device Template Components.
Below are components of Device Template -

- Basic Information – In includes configuration of logging, AAA, OMP, BFD, security, archive and NTP feature templates.
- Transport and Management VPN - This tab includes the templates used to configure VPN 0 and VPN 512, which includes BGP, OSPF, VPN interface, VPN interface cellular, VPN interface GRE, and VPN interface PPP feature templates.
- Service VPN – Service VPN template used to configure BGP, IGMP, Multicast, OSPF, PIM, VPN interface, VPN interface bridge, VPN interface GRE, VPN interface IPSec, VPN interface Nat pool, and DHCP server feature templates.
- Additional Templates – Additional template contains banner, Simple Network Management Protocol (SNMP), bridge, localized policy, and cellular feature templates.

Ques 58. What are Configuring Parameters?

An Administrator uses vManage to configure device and feature templates, specifying variables where needed since template can apply to multiple vEdge device that have unique settings. When configuring value of parameter inside of feature templates, three different types of values are there:

- Global – When you specify a global value, you specify the desired value, either by entering the value in box. Whatever you select will applied to all device feature template.
- Device specific – Device template used to create variable name and applied when device template used.
- Default - A specific default value applied to all devices. Specific value applied in text box and applied to all feature template in device.

Ques 59. How is Device Templates deployed?

Once feature templates are configured, the device template configuration is completed by referencing the desired feature template in each configuration category. Device template is attached to a specific vEdge device. When attached, you will be required to fill in the values for any variables in the template for each vEdge the template will apply to before the configuration can be deployed. Values can be entered through the vManage GUI directly, or by filling out a .csv file that can be uploaded.

Ques 60. Explain Centralized and Localized Policies?

Policy Overview

Policy influences the flow of data traffic and routing information among Cisco vEdge devices in the overlay network.

Routing policy - which affects the flow of routing information in the network's control plane.

Data policy - which affects the flow of data traffic in the network's data plane.

Control and Data Policy

Control policy is the equivalent of routing protocol policy, and data policy is equivalent to what are commonly called access control lists (ACLs) and firewall filters.

Centralized and Localized Policy

The Cisco SD-WAN policy design provides a clear separation between centralized and localized policy. In short, centralized policy is provisioned on the centralized Cisco vSmart Controllers in the overlay network, and the localized policy is provisioned on Cisco vEdge devices, which sit at the network edge between a branch or enterprise site and a transport network, such as the Internet, MPLS, or metro Ethernet.

Ques 61. How is Localized Policy configured?

Step 1: In the vManage GUI, create the localized policy under Configuration > Policies and select the Localized Policy tab.

Step 2: Enter the name of the localized policy.

Step 3: Select any policy components, like route policies and prefix lists, inside the feature templates.

Ques 62. What is difference between SDN and SD-WAN?

Difference between SDN and SD-WAN is shared in below table –

Parameter	SDN	SD-WAN
Abbreviation for	Software-Defined Networking	Software-Defined Wide Area Network
Target Area	Focused on Customer LAN or Data Center environment	Focused on providing software defined routing over WAN
Programming	Configuration and management is performed by customer itself	Configuration and management is performed by Service provider and not customer
Chronology	Was developed 1st and is building stone for SD-WAN	SD-WAN came later and is based on SDN technology
Key vendors	● Open Daylight ● VMware ● Juniper ● ConteXtream ● Big Switch Networks ● Cyan ● Alcatel-Lucent/Nokia ● Cisco	● Aryaka ● Cisco ● Citrix ● CloudGenix ● FatPipe ● Riverbed ● Silverpeak ● Talari

Ques 63. How would you Copy/Edit/View/Delete Centralized Policy?

Centralized policy refers to policy provisioned on Cisco vSmart Controllers, which are the centralized controllers in the Cisco SD-WAN overlay network. Centralized policy comprises two components:

- Control policy, which affects the overlay network–wide routing of traffic.
- Data policy, which affects the data traffic flow throughout the VPN segments in the network.

To View Centralized or Localized Policies

- From the Centralized Policy or Localized Policy tab, select a policy
- click More Actions and click View
- Click More Actions and click Preview

To copy a policy:

- From the Centralized Policy or Localized Policy tab, select a policy.
- Click More Actions and click Copy.
- In the Policy Copy popup window
- Click Copy

To edit policies created using the Cisco vManage policy configuration wizard:

- Click More Actions and click Edit
- Edit the policy as needed
- Click Save Policy Changes

To delete policies:

- From the Centralized Policy or Localized Policy tab, select a policy
- Click More Actions and click Delete
- Click OK to confirm deletion of the policy

Ques 64. What are the Types of Policy Definition?

Different types of policy definition are -

- App-route Policy – It creates an application-aware routing policy which tracks path characteristics such as loss, latency, and jitter.
- Cflowd Template - Allows you to enable cflowd, which sends sampled network data flows to collector.
- Control Policy – Operates on the control plane traffic and effects the routing paths in the network.
- Data Policy – Data policy flow on data plane to Influence the flow of data traffic based on the fields in the IP packet header.
- VPN Membership Policy – It restricts participation in VPNs on vEdge routers and the population of their route tables.

Ques 65. What is the Order of Operations in SD-WAN?

Order of Operation on WAN edge devices is -

- Local policy/configuration – such as QoS classification, policer, and marking
- Centralized application-aware routing policy
- Centralized data policy such as QoS classification, policer, marking.
- Routing/forwarding
- Scheduling and queueing
- Local policy shaping i.e. shaping, re-marking, policer and ACL.

Ques 66. What parameters does system configuration contain?

System configuration contains following parameters -

- System IP address (Unique)
- Site-id
- System Organization name (This needs to be same for all)
- vBond IP address
- Host-name (Unique)

Ques 67. Which types of VPNs does overlay network have?

- Transport VPN (VPN 0) – It carries control traffic via the configured WAN transport interfaces.
- Management Interface (VPN 512) – It carries out-of-band network management traffic in the overlay network. The interface used for management traffic resides in VPN 512
- Service Interface (VPN 1-65535 except VPN0 and 512) – It includes VPNs 1 through VPN 65535 except for VPN 0 and VPN 512. All service-side interfaces activated in these VPNs connect to a local or branch network and is generally located at the same site as the Cisco SD-WAN router.

Ques 68. What is the minimal basic Configuration of vSmart via CLI?

```
vSmart#config t
vSmart(config)#system
vSmart(config-system)#system ip X.X.X.X
vSmart(config-system)#site-id XXX
vSmart(config-system)#commit
```

Ques 69. What are the vEdge configuration elements?

Below are the vedge configuration elements –

System	Transport VPN	Service VPN	Management VPN	Policy
Host-name	VPN 0	Non-Zero VPN	VPN 512	Local Policy
GPS Location	Interfaces	Non-Management VPN		
Clock Time Zone	Routing (OSPF/	Interfaces		
AAA	BGP/Static)	Routing (OSPF/		
Logging		BGP/Static)		
TACAS/RADIUS				
OMP				
SNMP				
Security				
System-IP				
Site-ID				
Org-name				
VBond				

Ques 70. Write the commands to configure GPS location on vEdge via CLI?

Below is the configuration for CLI -

```
vEdge#config t
vEdge(config)#system
vEdge(config-system)#gps-location longitude XX
vEdge(config-system)#gps-location latitude -YY
vEdge(config-system)#commit
```

Ques 71. What are the commands to verify connections with controller?

Below are the 2 commands to verify connections with controllers -

- show control connections
- show control connection-history

Ques 72. Share some sample vEdge configuration Via CLI?

Below is a sample configuration of vEdge -

```
vEdge#conf t
vEdge_TEST(config)#system
vEdge_TEST(config-system)#host-name IPWITHEASE_vEdge
IPWITHEASE_vEdge(config-system)# gps-location longitude XX
IPWITHEASE_vEdge(config-system)# gps-location latitude -YY
IPWITHEASE_vEdge(config-system)#system-ip X.X.X.X
IPWITHEASE_vEdge(config-system)#site-id XXX
IPWITHEASE_vEdge(config-system)# organization-name ‘’ipwithease”
IPWITHEASE_vEdge(config-system)#vbond Y.Y.Y.Y
IPWITHEASE_vEdge(config-system)#omp
IPWITHEASE_vEdge(config-system)#no shutdown
IPWITHEASE_vEdge(config-system)#ecmp-limit X
IPWITHEASE_vEdge(config-system)# advertise ospf external
IPWITHEASE_vEdge(config-system)# advertise connected
IPWITHEASE_vEdge(config-system)# interface g0/2
IPWITHEASE_vEdge(config-system)# ip address X.X.X.X/XX
IPWITHEASE_vEdge(config-system)# nat
IPWITHEASE_vEdge(config-system)# tunnel-interface
IPWITHEASE_vEdge(config-system)# encapsulation ipsec
IPWITHEASE_vEdge(config-system)# color biz-internal restrict
IPWITHEASE_vEdge(config-system)# max-control-connections 1
```

```
IPWITHEASE_vEdge(config-system)# no-allow service bgp
IPWITHEASE_vEdge(config-system)# allow-service dhcp
IPWITHEASE_vEdge(config-system)# allow-service dns
IPWITHEASE_vEdge(config-system)# allow-service icmp
IPWITHEASE_vEdge(config-system)# allow-service ntp
IPWITHEASE_vEdge(config-system)# no shutdown
IPWITHEASE_vEdge(config-system)# ip route 0.0.0.0/0 X.X.X.
IPWITHEASE_vEdge(config-system)# router
IPWITHEASE_vEdge(config-system)# ospf
IPWITHEASE_vEdge(config-system)# router-id X.X.X.X
IPWITHEASE_vEdge(config-system)# timer spf 200 1000 10000
IPWITHEASE_vEdge(config-system)# redistribute omp
IPWITHEASE_vEdge(config-system)# area 0
IPWITHEASE_vEdge(config-system)# interface Gx/x
IPWITHEASE_vEdge(config-system)# exit
IPWITHEASE_vEdge(config)#vpn 512
IPWITHEASE_vEdge(config)# interface gx/x
IPWITHEASE_vEdge(config)#ip address x.x.x.x/xx
IPWITHEASE_vEdge(config)#no shutdown
IPWITHEASE_vEdge(config)#commit
```

Ques 73. What is Device Template?

Device template defines a device's complete operational configuration. A device template consists of a number of feature templates. Each feature template defines the configuration for a particular protocol. For software feature template that have a factory-default template, you can use either the
factory-default template (named factory_default_fetaure-name_template) or can create a custom feature template.

Ques 74. How can one create Device Template?

Go to Configuration > Device Template > Create template. Fill all the options. Device template can also be created from CLI.

Ques 75. Why we need QoS in Viptela?

With SD-WAN, quality of service (QoS) rules, path selection and traffic shaping can be applied to ensure that high-priority applications always perform well. End-to-end QoS provides last-mile awareness preventing oversubscription and wasted utilization.

Ques 76. How is a QoS policy configured?

To configure a QoS Policy:

- QoS map each forwarding class to an output queue.
- Configure the QoS policy for each forwarding class.
- Group the QoS scheduler into a QoS map.
- Define an access list to specify match condition for packet transmission.
- Apply the ACL to a specific interface.
- Apply the queue map and the rewrite rule to the egress interface.

Ques 77. What are three building blocks of vSmart Policy?

3 building blocks of vSmart Policy are -
a) Lists: Defines the targets of policy application or matching. These include -

- Data Prefix-list of prefixes for use with a data-policy.
- Prefix-list – Prefix list used with any other policy.
- Site-list –Site list of site-ids for use in policy and apply policy.
- TLOC-list – TLOC list of tlocs for use in policy.
- VPN-List – List of VPNs for used in policy.

b) Policy Definition: controls aspects of control and forwarding. Different types of policies are -

- App-route-policy is used together with sla-class for application-aware-routing.
- Cflowd template is used to configure the cflowd agents on the vEdge nodes.
- Control-policy controls OMP routing control.
- Data-policy provides vpn-wide policy-based routing.
- VPN-membership-policy controls vpn membership across nodes.

c) Policy Application

- Apply-policy is used in combination with a site-list to determine where policies are applied.
- Policy definition configured on vSmart and applied either on vSmart or on vEdge.

Ques 78. Explain centralized control policy: inbound vs outbound?

- In-bound Policy: In-bound policy selects the routes to be installed in the local routing database of the vSmart controller.
- Out-bound Policy: Is applied after a route is retrieved from routing database, however BEFORE the vSmart controller advertises it.

Ques 79. What is vSmart Policies?

All vSmart policies are configured on the vSmart controller using a combination of policy definition, apply policy and lists.

VSmart Policy is of 2 types –

- Control Policy – Impacts flow of information in Network's Control Plane
- Data Policy – Impacts flow of information in Network's Data Plane

Control Policy can be further subdivided into Centralized (Network Wide) and Localized (site Local) Policies. In the same way, Data policy is also of 2 types i.e. Centralized (Network Wide) and Localized (includes ACLs and limited to single Interface of Router) Policies.

Ques 80. What is OMP Path Selection Checklist

Following are the checklist which OMP uses to select the best path among two or more similar paths.

- Check whether OMP route is valid or not, if not it will be ignored.
- Select the route with the lower AD value.
- If AD values are same select the route with higher preference value for vRoute.
- If OMP preference values are equal select the route with the higher TLOC preference value.
- If the TLOC preference values are equal select the route on the basis of origin in the following order:
  - Connected
  - Static
  - EBGP
  - OSPF Intra-area
  - OSPF inter-area
  - OSPF external
  - iBGP
  - Unknown
- If the Origin is also same select the route based with lower IGP metric.

vIf the origin type and IGP metric is also the same select the route coming from a system having higher router ID.

- If the router IDs are equal, a vEdge router selects the OMP route with the higher private IP address. If a vSmart controller receives the same prefix from two different sites and if all attributes are equal, the vSmart controller chooses both of them.

If a vSmart controller receives a route from a vEdge router and same route from another vSmart controller, assuming all the values above are equal the route from the vEdge will be a preferred one.
If vSmart controller receives the same route from two vEdge routers and assuming all the values above are equal, both the routes will be installed in the routing table. By default, we can have up to 4 equal-cost routes selected and advertised.
vEdge router installs a route in the routing table only if the remote TLOC is active. To check if the remote TLOC is active a BFD session established between the local and remote TLOC. One BFD session exists per TLOC on a Viptela device. If a BFD session goes down the vSmart controller will remove all the routes that point to that TLOC as the next hop.

Ques 81. What are vSmart Policy Components?

VSmart Policy components are -

- Data-prefix-list is used in data-policy to advertise prefix and upper layer ports, either individual or jointly, for traffic matching.
- Prefix-list is used in control policy to advertise prefixes for matching RIB entries.
- Site-list is used in control policy to compare source sites, and apply policy to define sites for policy application.
- TLOC-list is used in control policy to define TLOC for matching RIB entries and to implement TLOC to vRoutes.
- VPN-list is used in control policy to advertise prefixes for matching RIB entries, and in data policy and app route-policy to define VPNs for policy application.

Ques 82. Provide an example or syntax of Policy Configuration?

Commands	Commands
Apply-policy Site-list site 1 Control-policy prefer local_out	Apply the defined policy towards the sites in site-list
Policy Lists Site-list siteX Site-id XXX TLOC-list prefer siteX TLOC x.x.x.x color mpls encap ipsec preference XXX	Define the list required for apply-policy and for use within the policy
Control-policy prefer_local Sequence XX Match route Site-list siteX Action accept Set TLOC-list prefer_siteX	Define the actual policy to be applied List previously defined used within policy

Ques 83. What are Cisco SD-WAN SEN Software Services?

2 key SEN services are –

- CloudExpress service - This service optimizes the performance of SaaS cloud applications and renders clear visibility of the performance of individual applications and automatically chooses the best path for each one. CloudExpress service computes metrics about loss and latency based on customized criteria for each application.
- vAnalytics platform - vAnalytics platform is a SaaS service hosted by Cisco SD-WAN as part of the SEN solution. It provides graphical representations of the performance of your entire overlay network over time and lets you drill down upto a single carrier, tunnel, or application at a particular time.

Ques 84. What are the Advanced Features of Viptela Policy?

Advanced features of Viptela Policy are -

- Service Chaining, which redirects data traffic toward firewall, IDS and IPS, load balancer and other devices before the traffic is delivered to its destination. Service chaining keep off the need to have a separate device at each branch site.
- Cflowd, for monitoring traffic flow.
- Converting a vEdge router into a NAT device, to allow traffic destined for the internal or other public network can exit directly from the vEdge router.

Ques 85. How does VRRP respond to host?

- vEdge routers are Layer 2 adjacent to the hosts and default gateway for the hosts.
- VRRP works between the two redundant vEdge routers, Active/Active in the group.
- VRRP Active vEdge responds to all ARP requests from internal network for the virtual IP with its physical interface MAC address.
- In such scenario of failover, new VRRP Active vEdge router sends out gratuitous ARP to update ARP table on the hosts and mac address table on the intermediate L2 switches.

Ques 86. Provide the CLI Commands for configuring VRRP on vEdge?

Below is the syntax -

vpn vpn-id
interface geslot/port[.subinterface]
vrrp group-number
ipv4 ip-address
priority number
timer seconds
(track-omp | track-prefix-list list-name)

Ques 87. How is master vEdge router elected based on priority number?

The router with the highest priority is elected as master. If two vEdge routers have the same priority, the one with the higher IP address of physical active interface is elected as master. Range is from 1 through 254. Default value is 100.

Ques 88. Kindly elaborate on following VRRP terms –

- **Track Interface State**
- **Virtual Router ID:**
- **Virtual IP Address:**
  - Track Interface State: By default, VRRP uses the LAN interface on which it is running to determine which vEdge router is the master virtual router.
  - Virtual Router ID: Virtual router ID, which is a numeric identifier of the virtual router. For each interface or sub interface, you can configure only a single VRRP group. Range: 1 through 255.
  - Virtual IP Address: It is IP address of the virtual router. The virtual IP address is different from the configured interface IP addresses of both the local vEdge router and the peer running VRRP. Single virtual IP for each interface or sub interface.

Ques 89. What are the key verification commands for VRRP troubleshooting?

Below are some of key VRRP troubleshooting commands -

- show running-config vpn 10
- Show vrrp interfaces
- Show vrrp vpn 10
- Show vrrp vpn 10 interface ge0/0 group 11
- Show vrrp vpn 10 interfaces groups
- Show vrrp vpn 10 interfaces group 10

Ques 90. What problems does SD WAN solve?
SD-WAN intelligently monitors and manages all underlay transport services. SD-WAN resolves challenges of packet loss, latency and jitter to deliver the best application performance and QoEX to users, even when WAN transport services are impaired.

Ques 91. Briefly share what is Cisco SD WAN solution?
SD-WAN solution offers a complete SD-WAN fabric with centralized management and security built in, creating a secure overlay WAN architecture across campus, branch, and data center and multi cloud applications. Cisco SD-WAN uses the OMP route to control the entire network.

Ques 92. What is Service route?
Identifiers that tie an OMP route to a service in the network, specifying the location of the service in the network. Services include firewalls, IDS and IPS and load balancers.

Ques 93. How to activate Centralized Policy on Cisco vSmart Controllers?
- In the title bar, click the Custom Options drop-down.
- In the Centralized Policy tab, and then select a policy.
- Click More Actions and click Activate.
- In the Activate Policy popup, click Activate to push the policy to all reachable Cisco vSmart Controllers in the network.
- Click OK to confirm activation of the policy on all Cisco vSmart Controllers.
- To deactivate the centralized policy, select the = tab, and then select a policy.
- Click More Actions and click Deactivate.
- In the Deactivate Policy popup, click Deactivate to confirm that you want to remove the policy from all reachable Cisco vSmart Controllers.

Ques 94. What are components of Centralized Policy?
- CLI policy - Create the policy using the command-line interface rather than the policy configuration wizard.
- Lists - Create groups of interest to import in the Group of Interest screen in the policy configuration wizard.
- Topology - Create a hub-and-spoke, mesh, or custom topology or a VPN membership to import in the Topology screen in the policy configuration wizard.
- Traffic Policy - Create an application-aware routing, traffic data, or cflowd policy to import in the Traffic Rules screen in the policy configuration wizard.

Ques 95. What are the SD-WAN Licensing options under DNA software subscriptions?
The subscription licensing available for Cisco SD-WAN are as follows:
- Cisco DNA Essentials: Standard SD-WAN upto 50 devices.
- Cisco DNA Advantage: Cloud-Scale SD-WAN
- Cisco DNA Premier: Advanced Cloud security SD-WAN

Ques 96. How many vSmart controllers does vEdge connect to for redundancy?
vEdge routers connect to up to three vSmart controllers for redundancy.

Ques 97. What will happen if all the vSamrt controllers go down?
If all vSmart controllers fail or are unable to communicate, vEdge routers will still continue to operate as per last known good state for a configurable amount of time (min of re-key timer and GR timer)
- No updates to reachability
- No IPSec rekey
- No policy changes propagation

Ques 99. In case of Dual homed Branch setup, what will be the traffic flow?

- Active/Active
- Active/backup?

Default traffic flow in case of more than one link is Auto-Load balancing i.e. Active/Active

Ques 100. Which CLI command is used to verify that the candidate configuration contains no errors.

Validate

Ques 101. Enumerate the differences between MPLS and SD-WAN?

Below tables enlists the difference between MPLS and SD-WAN –

Parameter	MPLS	SD-WAN
Abbreviation for	Multiprotocol Label Switching	Software Defined - Wide Area Network
Provisioning time	High	Very low
Configuration	Manual Configuration	"Zero Touch provisioning" allows no need to perform manual configuration
Management	Decentralized control over variety of networking equipment	Centralized control of devices
Cost impact	High	Low since Internet links are used which are much cheaper than MPLS
Security	Good	Very High
Application Level Visibility	Low visibility of application performance	Deep application visibility
Bandwidth Scaling	Time consuming	Immediate
Geographical Reach	Limited to reach of Provider MPLS Cloud	Much Wider spread and highly scalable than MPLS

Head Office:

L-149, 1st, 2nd and 3rd Floor, Eshwari Mansion, 5th Main Road, Sector-6 HSR Layout,
Bengaluru, Karnataka 560102, India
Mobile No: **+91-9611027980** | **+91-9354284954**, Email: **info@networkershome.com**