PassQueen
a.k.a dumpsqueen.com

VMware SD-WAN Troubleshoot

VMware 5V0-41.20

Version Demo

Total Demo Questions: 5

Total Premium Questions: 57

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

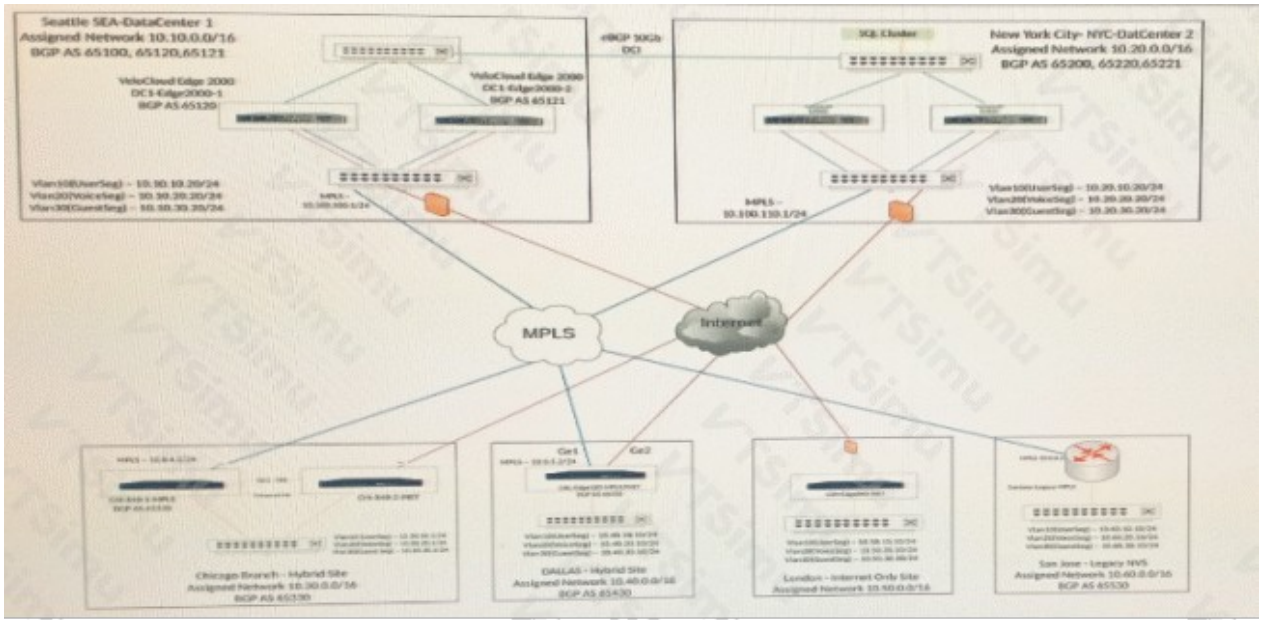
Topic	No. of Questions
Topic 1, Troubleshoot VMware SD-WAN	57
Total	57

QUESTION NO: 1

Scenario 3:

After resolving numerous connectivity issues throughout the various branch sites, connectivity between applications and users is finally present. The network administrator is informed that during certain tests, applications are not performing as they are expected to. Users report that call quality has not fully improved and that some of their calls either drop or have poor voice quality where the conversation is breaking up. Other users are noticing that file transfers are slower than expect. A group of users from a few sites have reported slowness in accessing internal and external applications.

Exhibit.



A network administrator is receiving complaints that a real-time voice application is not performing well, with choppy audio, and dead audio especially during peak traffic times.

What two actions can the administrator take to diagnose and fix the issue? (Choose two.)

A. Configure a QoS policy to rate limit all traffic during peak times.

B. Ensure that the realtime application is matching the correct application type using the diagnostics page.

C. Check the status of the links using the QoE and Transport tabs for any degraded underlay issues or congestion issues.

D. Configure a QoS policy to load balance the realtime traffic across all links.

ANSWER: B C

Explanation:

Ensure that the realtime application is matching the correct application type using the diagnostics page. VMware SD-WAN business policies depend on accurate application identification to apply the intended traffic class, service settings, and forwarding treatment. The Diagnostics area allows an administrator to verify the application recognition and classification observed by the Edge. Confirming that the voice flow is recognized as the expected real-time application type is essential before relying on policy-based handling; it also provides the basis for correcting an application map or policy classification if the traffic is not being identified as intended.

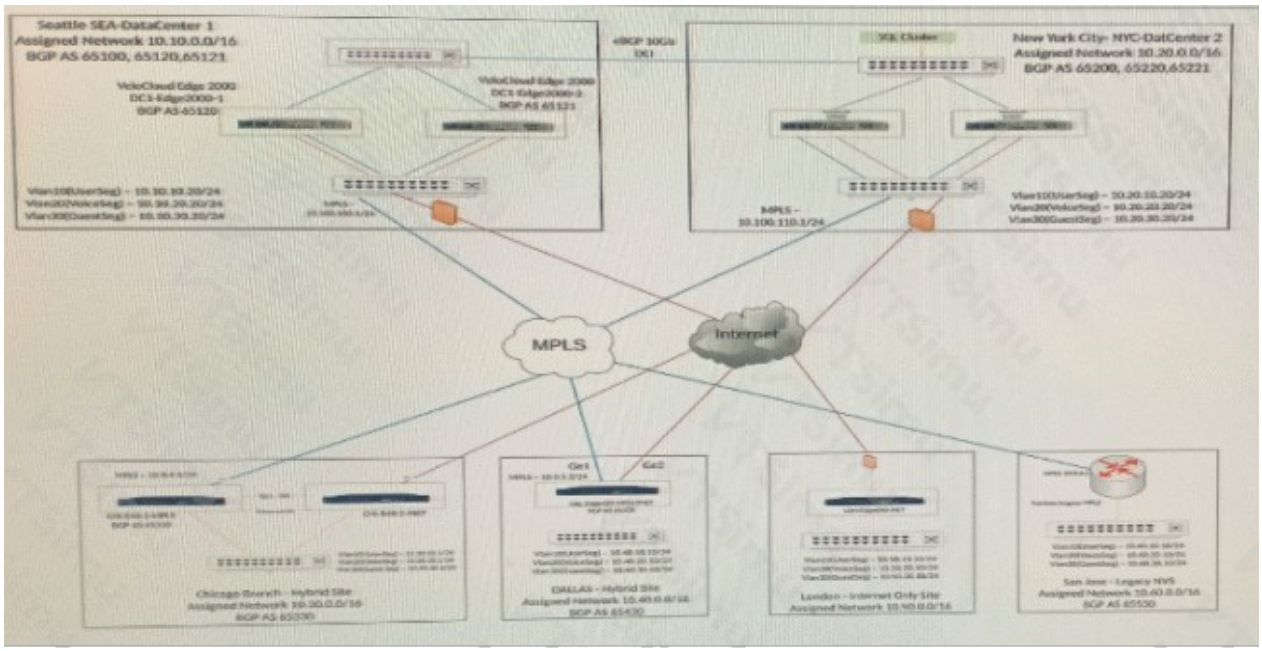
Check the status of the links using the QoE and Transport tabs for any degraded underlay issues or congestion issues. Choppy audio and periods of dead air are highly sensitive to underlay loss, jitter, latency, and bandwidth saturation, especially when traffic volume rises. VMware SD-WAN continuously measures these link-quality characteristics and presents them through monitoring views such as QoE and Transport. Reviewing the affected time window and WAN link measurements identifies whether a transport circuit is congested or degraded and supports remediation through link troubleshooting or appropriate path-selection policy. See the VMware SD-WAN documentation and the VMware SD-WAN product documentation resources.

QUESTION NO: 2

Scenario 2:

After completing the branch activation activities for all required branches, the network administrator attempts to test connectivity between the various branches and between the hubs and branches. The administrator notices a lack of connectivity despite being certain that configurations have been complete. The administrator also observed that several users are reporting intermittent connectivity to some of the applications they are accessing. Other users are reporting no access to these applications. Other users at some of the branches claim they cannot get to certain public resources. The administrator wants to ensure that all sites can talk to each other and all resources are accessible.

Exhibit.



A network administrator is investigating connectivity issues between Chicago and San Jose. The administrator browses to the Overlay Flow Control (OFC) window and notices that the screen is blank with no routes shown in the OFC.

What is a possible reason for this?

A. Cloud VPN for the Edges / Profiles is not enabled.

B. There is an invalid MTU configuration at Chicago.

C. OSPF or BGP is not enabled.

D. The routing table on the Edges has not been initialized.

ANSWER: A

Explanation:

Cloud VPN for the Edges / Profiles is not enabled. Cloud VPN is the VMware SD-WAN feature that establishes the secure overlay connectivity between participating Edges and distributes reachable routes across that overlay. An Edge must have Cloud VPN enabled through its assigned profile or through an Edge-level configuration override, and it must be included in the applicable Cloud VPN topology/segment. When Cloud VPN participation is not enabled, the Edge does not exchange the overlay route information needed for branch-to-branch or hub-and-branch forwarding. Consequently, the Overlay Flow Control view can contain no overlay routes for the affected Edge relationship, producing a blank display such as the one described for Chicago and San Jose. Enabling Cloud VPN for the relevant profile or Edges, verifying that both sites participate in the same intended segment and topology, and then allowing configuration activation and route exchange to complete restores the route information visible in OFC. This aligns with VMware SD-WAN's documented Cloud VPN model, in which overlay VPN connectivity and route sharing are controlled centrally through the Orchestrator configuration. See the VMware SD-WAN documentation portal and the Broadcom VMware SD-WAN technical documentation for Cloud VPN configuration and operational details.

QUESTION NO: 3

A Business Policy is configured to steer a specific SaaS application over a preferred WAN link. Flow Details shows that the traffic is identified as SSL rather than as the expected SaaS application.

Why does the Business Policy rule not match the flow?

A. The detected application does not match the application configured in the rule

B. The Edge has learned too many routes from the Gateway

C. The WAN link has a lower configured bandwidth than the Internet circuit

D. The remote site is assigned to a different Gateway pool

ANSWER: A

Explanation:

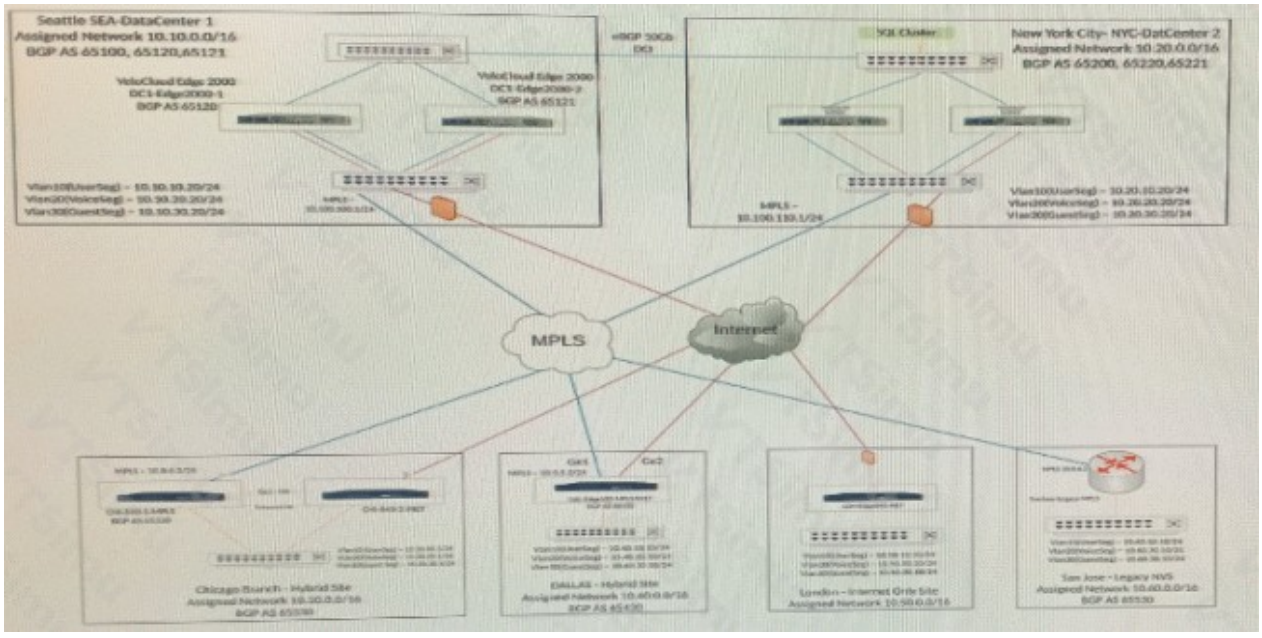
Application-based Business Policy matching depends on the application identified for the flow. A flow classified as SSL does not satisfy a rule that matches a different SaaS application, even when the destination is associated with that service.

QUESTION NO: 4

Scenario 3:

After resolving numerous connectivity Issues throughout the various branch sites, connectivity between applications and users is finally present. The network administrator is informed that during certain tests, applications are not performing as they are expected to. Users report that call quality has not fully improved and that some of their calls either drop or have poor voice quality where the conversation is breaking up. Other users are noticing that file transfers are slower than expect. A group of users from a few sites have reported slowness in accessing internal and external applications.

Exhibit.



Users at a remote office are complaining about poor performance with certain applications. The network administrator has already verified the configuration is correct.

Which two parameters should the administrator review to troubleshoot this issue? (Choose two.)

A. Check the underlay network (bandwidth, latency, jitter, packet loss)

B. Change the bandwidth measurement under WAN Overlay Advanced Settings

C. Check the flows to verify which Business Policy the traffic of interest is matching

D. Look under Monitor, check Business priority tab

ANSWER: A D

Explanation:

Check the underlay network (bandwidth, latency, jitter, packet loss) because real-time voice quality and application throughput depend directly on the available WAN capacity and on transport quality. Excess latency, jitter, or loss can produce broken audio and dropped calls, while a constrained or lossy underlay can reduce file-transfer and general application performance. SD-WAN continuously measures these transport characteristics so that the administrator can identify whether an affected circuit is unable to meet the traffic requirements.

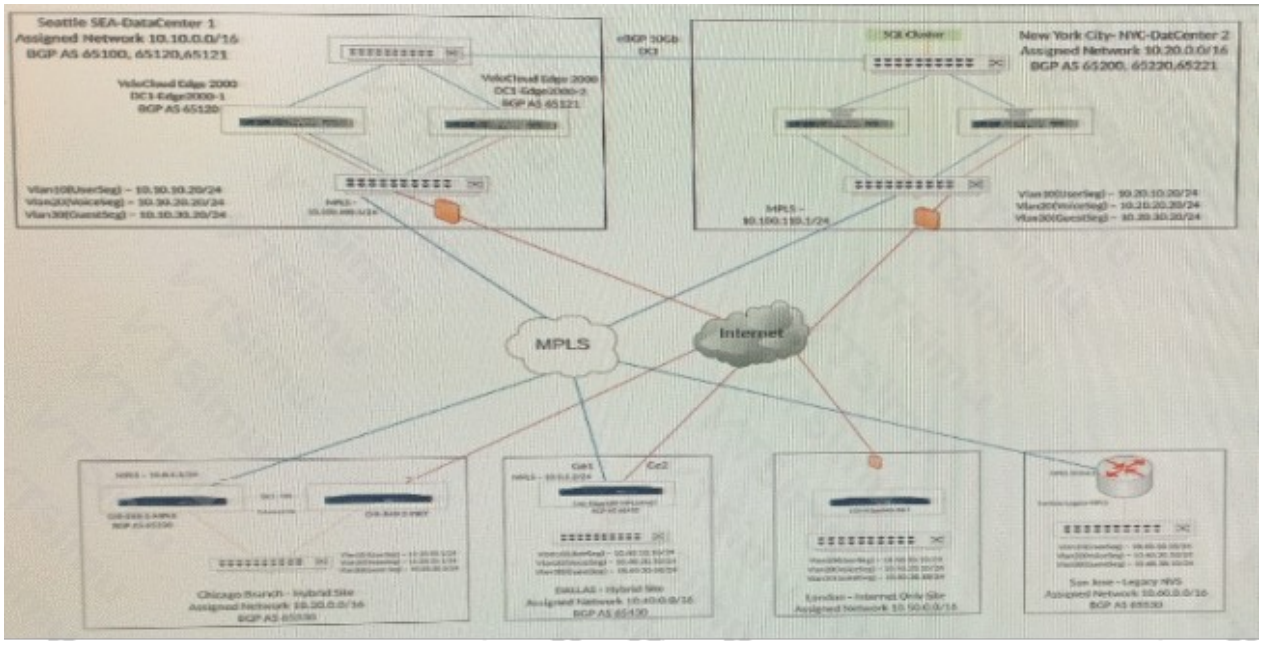
Look under Monitor, check Business priority tab because this view helps correlate the reported application experience with the edge's traffic prioritization and available bandwidth. Business Priority monitoring shows the effect of configured priority treatment and bandwidth consumption, enabling the administrator to determine whether voice, business-critical applications, or bulk traffic are receiving the expected service under current load. Reviewing this operational data is appropriate after configuration has been validated, since it distinguishes an application-priority or capacity condition from a purely configuration-related problem. VMware SD-WAN monitoring and diagnostics are designed to expose WAN-link quality and application/business-policy traffic behavior for this type of investigation. See the VMware SD-WAN Administration Guide and the VMware SD-WAN documentation portal.

QUESTION NO: 5

Scenario 2:

After completing the branch activation for all required branches, the network administrator attempts to test connectivity between the various branches and between hubs and branches. The administrator notices a lack of connectivity despite being certain that configurations have been complete. The administrator also observed that several users are reporting intermittent connectivity to some of the some applications they are accessing. Other users are reporting no access to these applications. Other users at some of the branches claim they cannot get to certain public resources. The administrator wants to ensure that all sites can talk to each other and all resources are accessible.

Exhibit.



A technician has added Edges to an East Coast Profile. These Edges are not able to communicate via dynamic tunnels to Edges in the West_Coast profile. The technician has noticed that some Edges are able to establish dynamic tunnels.

What could be preventing Edges from being able to establish dynamic tunnels?

A. The profiles are not configured to allow dynamic branch to branch VPNs.

B. The profiles are configured to only allow dynamic branch to branch for Edges within the same profile.

C. None of the existing profiles have Cloud VPN enabled thus preventing dynamic tunnels.

D. Neither profile has been configured to utilize cloud gateways.

ANSWER: B

Explanation:

The profiles are configured to only allow dynamic branch to branch for Edges within the same profile. VMware SD-WAN profile-level Cloud VPN policy can limit dynamic branch-to-branch tunnel formation to Edge instances assigned to that specific profile. Consequently, dynamic tunnels can be successfully established among sites that share a profile, while direct dynamic tunnels between the East Coast and West_Coast profiles are not formed. This behavior directly matches the observation that some Edge instances establish dynamic tunnels but the sites split across the two profiles cannot communicate through such tunnels. The administrator should review the Cloud VPN and dynamic branch-to-branch settings applied to both profiles and use a configuration that permits the required inter-profile connectivity. This ensures that the intended topology and reachability policy include all participating branches, rather than only the Edge instances grouped under one profile. VMware documents Cloud VPN configuration and branch connectivity behavior in its SD-WAN administration documentation. See the VMware SD-WAN documentation portal and the Broadcom VMware SD-WAN technical documentation.