CCIE Enterprise Infrastructure v1.1:

Module 1# :Design V3

Design Lab V3

Initial Level Set

Introduction to XANDER Pharmaceuticals

Xander is a large multinational pharmaceutical company. headquartered in Manchester, United Kingdom, and with smaller branch level

The Xander board is planning to expand aggressively through acquisitions over the next 24 months to grow the business at the much faster now.

To support the aspirations of the board, the Chief Technical Officer (CTO) wants to take advantage of modern resource communication technology, such as software-define networking (SDN), However for us SDN proof of concept (PoC) has already been acquired and in being tested in data center.

The CTO has concerns around reliability with the current solution and must fine solutions that offer commercial flexibility, these two issues must be addressed simultaneously in any new solution proposed going forward. Also, the computer hardware in the data center is approaching End-of-life (EoL). and the CTO is keen to explore hybrid cloud solutions for the replacement of the old hardware.

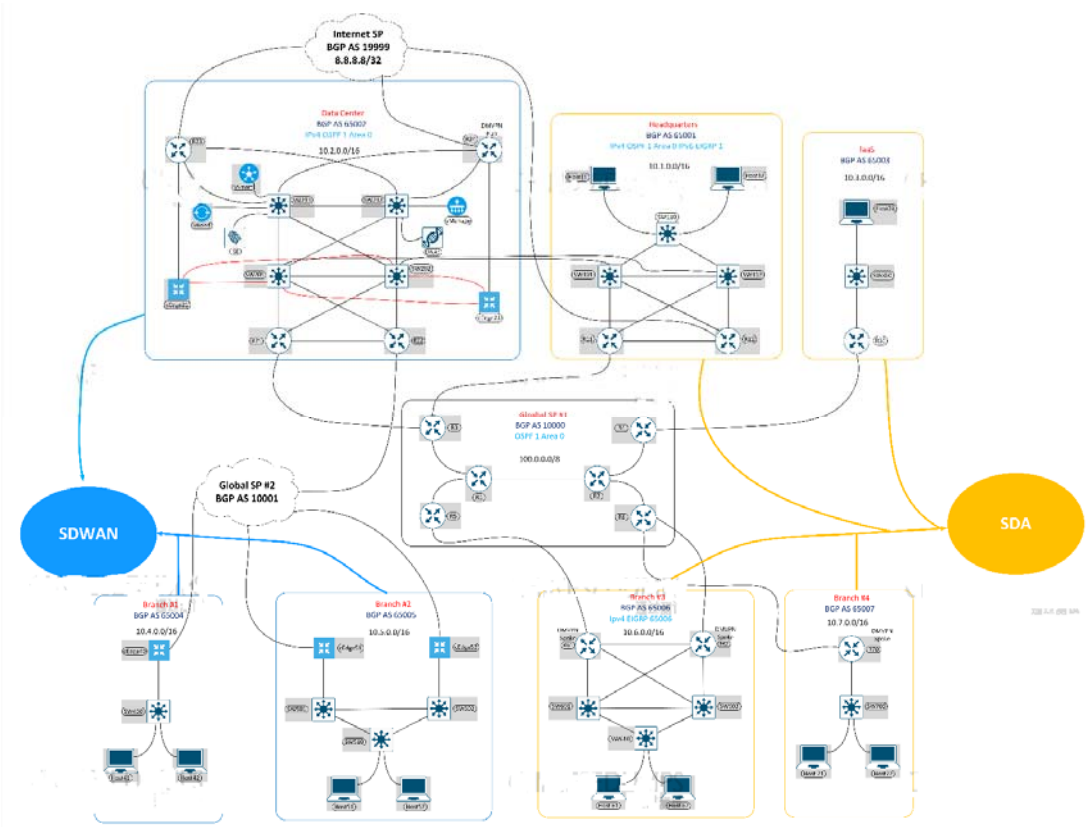
Xander has hired an external partner, CCIE20, to access and assist aspect of network design needs, including any necessary network upgrades and redesigns.

You will be playing the role of James Wilmore, Principal Architect at CCIE20 and main point of contact for Xander at CCIE20 for the duration of the project. As part of your role, you will be interacting ___people at Xander's end, including

- **CTO Maria Lopes – mlopes@xander.co.uk**
- **CSO Bruce Wayre – Bwayre@xander.co.uk**
- **Head of operations Rick fury – rfury@xander.co.uk**
- **Head of networks Natalie Roman nroman@xander.co.uk**

Diagrams

Main Topology



Questions1:

Welcome to the Design Module for XANDER PHARMACEUTICALS.

Please read all the available resources before starting the scenario by clicking 'Next item'

Questions2:

Refer to the new resource(s) available.

This item consists of multiple questions you may need to scroll down to be able to see all

Questions.2.1

Which scalable, switch-level feature must be used to prevent access from an employee-owned wireless access point connected to the corporate network?

A. bridge protocol data unit guard

B. port security

C. security group tags

D. MAC access control lists

Questions.2.2

Hi James, and apologies :(

Our CSO has stepped in on this one and decided that regardless of your advice on the previous question and the "switch-level" feature requirement. He wants us to try to use port security to solve this issue.

We have now enabled port security on the access ports of all the switches at HQ as per his decisions, with no other extra configurations added.

However, our CSO is now suggestion some additional requirements for this solution

- **He wants only the first device that connects to a switch port to be allowed on the network. Even between reboots of the switch**
- **Also, if another device attempts to connect to the network via that port. Intervention from our IT team should be required to recover the port**

Which two additional solutions must be used to meet these extra requirements? (Choose two)

A. Set the maximum number of MAC address to 1.

B. Specify the MAC address of the allowed device in the switch interface configuration.

C. Ensure that errdisable recovery is disabled for port security events.

D. Ensure that the first dynamically learned MAC address is sticky in the switch interface configuration.

E. Set the port security violation action to Project.

Questions3:

Refer to the new resource(s) available.

This item consists of multiple questions. You may need to scroll down to be able to see all

Questions 3.1

Which Layer 2 feature must be used to help mitigate the dropped traffic on EtherChannel between the switches?

A. Loop guard

B. Bridge Assurance

C. Bidirectional Forwarding Detection

D. UnDirectional Link Detection

Questions 3.2

Which solution mitigates the switch CPU utilization issues and avoids considerable changes to the data center network?

A. Reduce the number of STP instances that use MST

B. Convert each switch to the router configuration with the Layer 3 underlay and a BGP EVPN VXLAN based overlay.

C. Put each bridge protocol data unit into the switch software for management by the control plane.

D. Enable IGMP snooping on each switch

Questions4:

Refer to the new resource(s) available.

Which load-balancing algorithms should the operations team use as a reusable standard?

A. src-dst-mac

B. vlan-src-ip

C. src-dst-ip

D. src-mixed-ip-port

Questions5:

Note: Pay special attention to this question, as there may be several different variations.

Refer to the new resource(s) available.

To ensure traffic does not bypass the DMVPN, identify which design changes should be implemented on which routers.

Version 1： Original version, but any rows and columns in the matrix may be removed.

Routers				
Designs changes	R21	R70	R61	R62
Advertise default route into DMVPN	☐	☐	☐	☐
Stop sending 10.7.0.0/16 routers into BGP	☐	☐	☐	☐
Redistribute default route into BGP	☐	☐	☐	☐
Stop sending 10.6.0.0/16 routes into BGP	☐	☐	☐	☐
Ensure default routes forwards into the DMVPN	☐	☐	☐	☐
Only send DMVPN tunnel endpoint address into BGP	☐		☐	☐

Answer:

Version 1： Original version, but any rows and columns in the matrix may be removed.

Routers				
Designs changes	R21	R70	R61	R62
Advertise default route into DMVPN	☐	☐	☐	☐
Stop sending 10.7.0.0/16 routers into BGP		✓	☐	☐
Redistribute default route into BGP	☐	☐	☐	☐
Stop sending 10.6.0.0/16 routes into BGP	☐	☐	✓	✓
Ensure default routes forwards into the DMVPN	☐	☐	☐	☐
Only send DMVPN tunnel endpoint address into BGP	✓	✓	✓	✓

Note: "Only send DMVPN tunnel endpoint address into BGPn and "Only send nhrp NBMA address into BGPn have the same meaning here.