Implementing SD-WAN

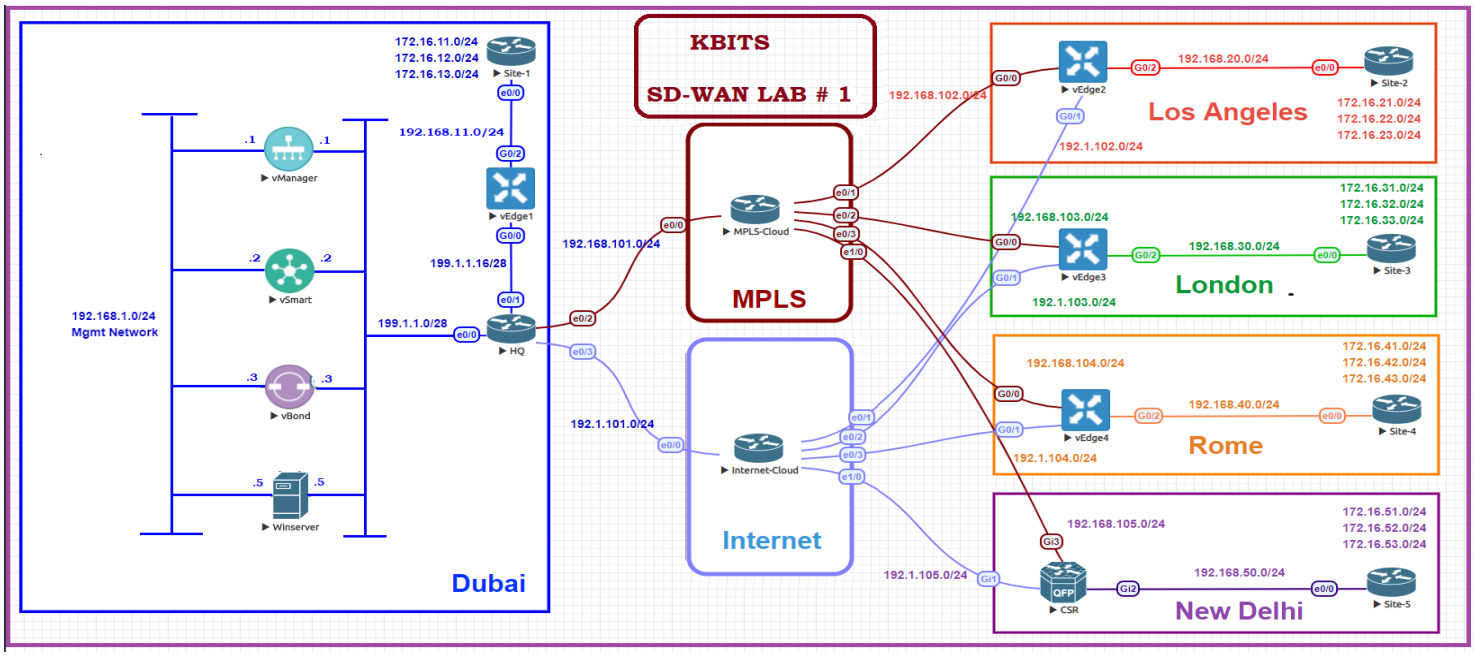
Authored By:

Khawar Butt
CCIE # 12353
Hepta CCIE#12353
CCDE # 20110020

Preparing the Network for SD-WAN

Website: http://www.kbits.in; Email: Khawarb@khawarb.com

Lab 1 – Configuring the WAN Components



Interface Configuration

HQ

Interface	IP Address	Subnet Mask
E 0/0	199.1.1.14	255.255.255.240
E 0/1	199.1.1.30	255.255.255.240
E 0/2	192.168.101.1	255.255.255.0
E 0/3	192.1.101.1	255.255.255.0

MPLS Cloud

Interface	IP Address	Subnet Mask
E 0/0	192.168.101.254	255.255.255.0
E 0/1	192.168.102.254	255.255.255.0
E 0/2	192.168.103.254	255.255.255.0
E 0/3	192.168.104.254	255.255.255.0
E 1/0	192.168.105.254	255.255.255.0

Internet Cloud

Interface	IP Address	Subnet Mask
E 0/0	192.1.101.254	255.255.255.0
E 0/1	192.1.102.254	255.255.255.0
E 0/2	192.1.103.254	255.255.255.0
E 0/3	192.1.104.254	255.255.255.0
E 1/0	192.1.105.254	255.255.255.0

Task 1 – HQ Router Configuration

- Configure the Interfaces based on the Logical Diagram
- Configure OSPF as the IGP to communicate with the MPLS Cloud. Enable all the interfaces.
- Make sure OSPF only sends and receives OSPF packets on the link towards the MPLS Cloud using the Passive-interface command.
- Configure a default route on the router towards the Internet. The IP Address of the Internet Router is 192.1.101.254

HQ Router

```
no ip domain-loo
line con 0
 logg sync
 no exec-timeout
!
Hostname HQ
!
Interface E 0/0
 ip address 199.1.1.14 255.255.255.240
 no shut
!
Interface E 0/1
 ip address 199.1.1.30 255.255.255.240
 no shut
!
Interface E 0/2
 ip address 192.168.101.1 255.255.255.0
 no shut
!
Interface E 0/3
 ip address 192.1.101.1 255.255.255.0
 no shut
!
router ospf 1
 network 192.168.101.0 0.0.0.255 area 0
 network 199.1.1.0 0.0.0.255 area 0
 passive-interface default
 no passive-interface E0/2
!
ip route 0.0.0.0 0.0.0.0 192.1.101.254
```

Task 2 – MPLS Cloud Router Configuration

- Configure the Interfaces based on the Logical Diagram.
- Configure OSPF as the IGP on all the interfaces.

MPLS Cloud Router

```
no ip domain-lookup
!
line con 0
 exec-timeout 0 0
 logging synchronous
!
hostname MPLS
!
interface Ethernet0/0
 ip address 192.168.101.254 255.255.255.0
 no shut
!
interface Ethernet0/1
 ip address 192.168.102.254 255.255.255.0
 no shut
!
interface Ethernet0/2
 ip address 192.168.103.254 255.255.255.0
 no shut
!
interface Ethernet0/3
 ip address 192.168.104.254 255.255.255.0
 no shut
!
interface Ethernet1/0
 ip address 192.168.105.254 255.255.255.0
 no shut
!
router ospf 1
 network 192.168.101.0 0.0.0.255 area 0
 network 192.168.102.0 0.0.0.255 area 0
 network 192.168.103.0 0.0.0.255 area 0
 network 192.168.104.0 0.0.0.255 area 0
 network 192.168.105.0 0.0.0.255 area 0
```

Task 3 – Internet Cloud Router Configuration

- Configure the Interfaces based on the Logical Diagram
- Configure a Static Route on the Router for the 199.1.1.0/24 network. The Next Hop should point towards the Internet IP of the HQ Router.

Internet Cloud Router

```
no ip domain lookup
!
line con 0
 exec-timeout 0 0
 logging synchronous
!
hostname Internet
!
interface Ethernet0/0
 ip address 192.1.101.254 255.255.255.0
 no shut
!
interface Ethernet0/1
 ip address 192.1.102.254 255.255.255.0
 no shut
!
interface Ethernet0/2
 ip address 192.1.103.254 255.255.255.0
 no shut
!
interface Ethernet0/3
 ip address 192.1.104.254 255.255.255.0
 no shut
!
interface Ethernet1/0
 ip address 192.1.105.254 255.255.255.0
 no shut
!
ip route 199.1.1.0 255.255.255.0 192.1.101.1
```

Lab 2 - Installing the Enterprise Certificate Server

Note: It builds on the topology created in the previous lab.

Task 1 – Configure the Interfaces

First Ethernet Interface:

IP Address: 192.168.1.5
Subnet Mask: 255.255.255.0

Third Ethernet Interface:

IP Address: 199.1.1.5
Subnet Mask: 255.255.255.240
Default Gateway: 199.1.1.14

Task 2 – Configure the Timezone and Time

Configure the appropiate Timezone and Time on the Windows Server.

Task 3 – Installing the Enterprise Root Certificate Server

- Open **Server Manager**
- Click **Roles**
- Click **Add Roles**
- Click **Next**
- Select the "**Active Directory Certificate Services**" and click **Next**
- Click Next
- Select "**Certification Authority Web Enrollment**" and click Next
- Leave it as Standalone and click **Next**
- Leave it as Root CA and click **Next**
- Leave "Create a new private key" and click **Next**
- Leave the default for the Cryptography for CA and click **Next**
- Set the Common name as **KBITS-CA** and click **Next**
- Leave the default for the Validity Period and click **Next**
- Click **Next**
- Click **Install**

Task 4 – Install WinSCP

- **Double-click** the WinSCP Installation file.
- Do a Default Installation.

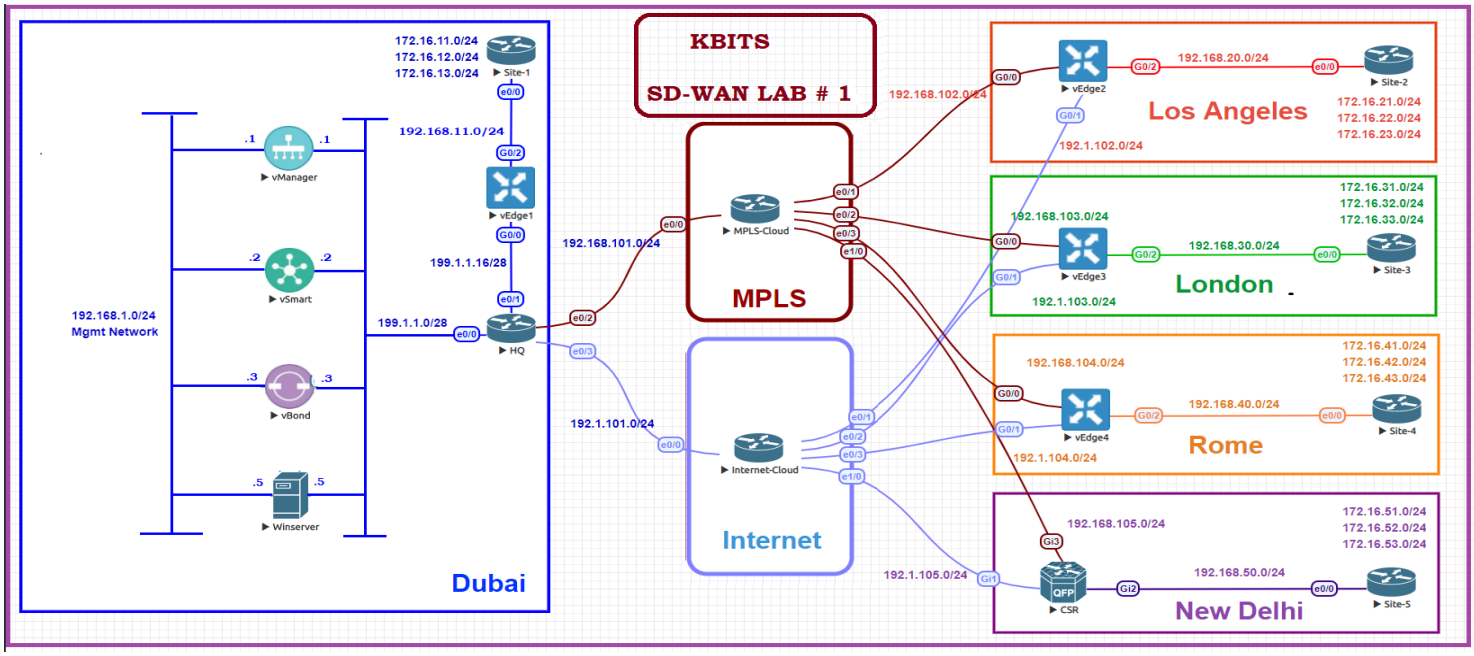
Implementing SD-WAN

Authored By:

Khawar Butt
CCIE # 12353
Hepta CCIE#12353
CCDE # 20110020

Initializing the Controllers

Lab 3 – Initializing vManage – CLI



Task 1 – Configuring the System Component

- Configure the System parameters based on the following:
  - Host-name : vManage1
  - Organization: KBITS
  - System-IP: 10.1.1.101
  - Site ID: 1
  - vbond Address: 199.1.1.3
  - Timezone: Based on the appropriate Timezone

Note: Default username: admin **Default password**: admin

vManage

```
config
!
system
 host-name vManage1
 system-ip 10.1.1.101
 site-id 1
 organization-name KBITS
```

```
clock timezone Asia/Muscat
vbond 199.1.1.3
!
commit
```

Task 2 – Configured the vpn parameters

- Configure the VPN parameters based on the following:
  - vpn 0
    - Interface eth1
    - IP Address: 199.1.1.1/28
    - Tunnel Interface
    - Tunnel Services (All, NetConf, SSHD)
    - Default Route: 199.1.1.14
  - vpn 512
    - Interface eth0
    - IP Address: 192.168.1.1/24

vManage

```
config
!
vpn 0
 no interface eth0
 interface eth1
  ip address 199.1.1.1/28
  tunnel-interface
   allow-service all
   allow-service netconf
   allow-service sshd
   no shut
 ip route 0.0.0.0/0 199.1.1.14
!
vpn 512
 interface eth0
  ip address 192.168.1.1/24
  no shut
!
commit
```

Lab 4 – Initializing vManage - GUI

Task 1 – Organization name & vBond Address

- Log into the vManage from the Server by browsing to https://192.168.1.1:8443 using a username of **admin** and a password of **admin.**
- Navigate to **Administration** -> **Settings**
- Click **Edit** on the Organization name and set it to **KBITS**. Confirm the Organization name. Click **OK.**
- Click **Edit** on the **vBond** address and change it to 199.1.1.3. Confirm and click **OK**.

Task 2 – Configure Controller Authorization as Enterprise Root and Download the Root Certificate.

- Browse to http://192.168.1.5/certsrv
- Click **"Download Root Certificate".**
- Select **"Base 64"**.
- Click "**Download CA Certificate".**
- Open Explorer and navigate to the downloads folder.
- Change the name of the Downloaded file "**Certnew**" to "**RootCert**".
- Open the "**RootCert.cer**" file using Notepad.
- Copy using **CTRL-A** and **CTRL-C**.
- In vManage, Navigate to **Administration -> Settings -> Controller Certiticate Authorization.**
- Change the "**Certificate Signing by:**" to "**Enterprise Root Certificate**".
- Paste the RootCert.cer that you had copied by using **CTRL-V.**

- Set the CSR Parameters with the Organization name, City, State, Country. Set the Time to 3 Years and save.

Task 3 – Generate a CSR for vManage

- Navigate to **Configuration -> Certificates -> Controllers -> vManage -> Generate CSR.**
- It will open a window with the CSR. Copy by using **CTRL-A** and **CTRL-C.**

Task 4 – Request a Certificate from the CA Server

- Browse to http://192.168.1.5/certsrv
- Click **"Request a Certificate".**
- Select **"Advanced"**.
- Paste the CSR in the box by using **CTRL-V** and click **Submit.**

Task 5 – Issue the Certificate from the CA Server

- Open Server Manager and navigate to **Active Directory Certificate Server -> KBITS-CA -> Pending Requests.**
- Right-Click the request and click "**Issue".**

Task 6 – Downloading the Issued Certificate

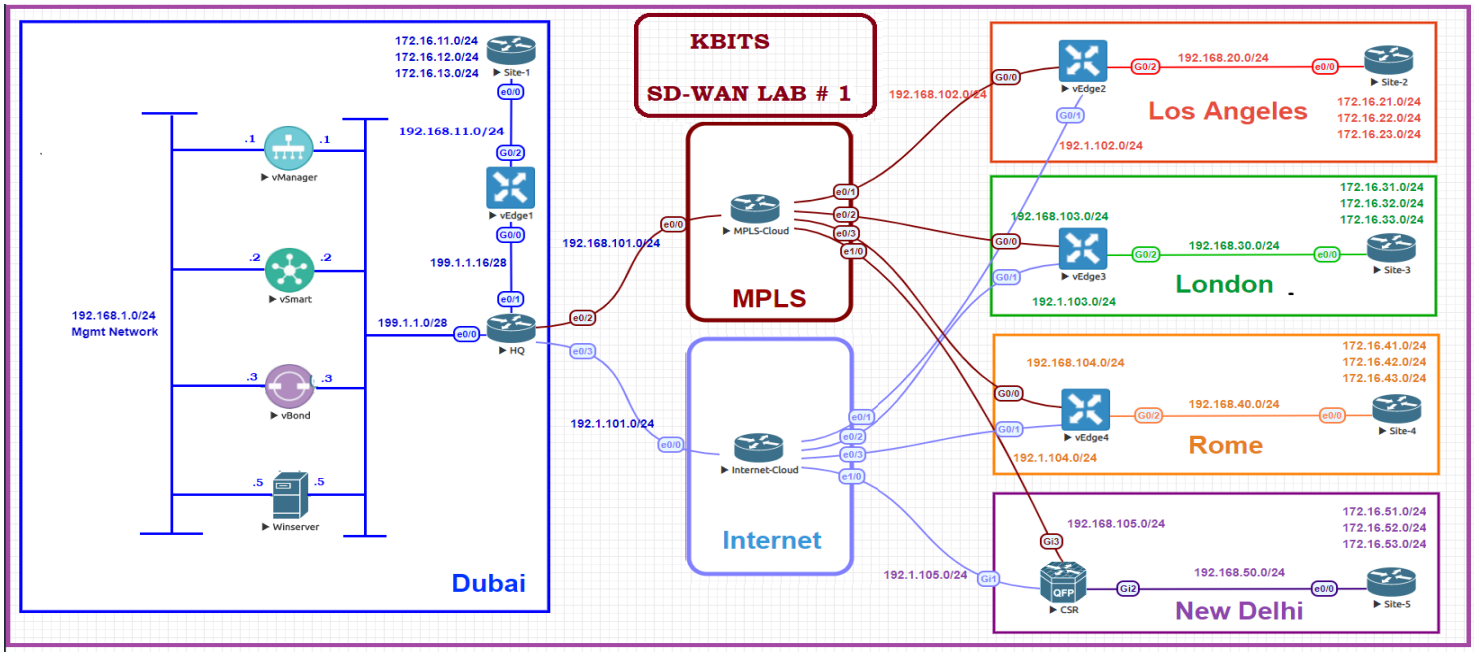
- Browse to http://192.168.1.5/certsrv
- Click **"Check on Pending request".**
- The issued certificate link will show up. Click on the link.
- Select "**Base 64"** and click "**Download"**
- Open Explorer and navigate to the downloads folder.
- Change the name of the Downloaded file "**Certnew**" to "**vManage**".
- Open the "**vManage.cer**" file using Notepad.

- Copy using **CTRL-A** and **CTRL-C**.

Task 6 – Installing the Identity Certificate for vManage

- In vManage, Navigate to **Configuration -> Certificates -> Controllers**
- Click on the **"Install"** button at the top right corner
- Paste the Certificate (CTRL-V).
- The Identity certificate should be installed on vManage.

Lab 5 – Initializing vBond – CLI



Task 1 – Configuring the System Component

- Configure the System parameters based on the following:
  - Host-name : vBond1
  - Organization: KBITS
  - System-IP: 10.1.1.103
  - Site ID: 1
  - vbond Address: 199.1.1.3
  - Timezone: Based on the appropriate Timezone

Note: Default username: admin **Default password**: admin

vBond

```
config
!
system
 host-name vBond1
 system-ip 10.1.1.103
 site-id 1
 organization-name KBITS
 clock timezone Asia/Muscat
 vbond 199.1.1.3 local
!
```

Commit

Task 2 – Configured the vpn parameters

- Configure the VPN parameters based on the following:
  - vpn 0
    - Interface Ge0/0
    - IP Address: 199.1.1.3/28
    - Tunnel Interface
    - Tunnel Services (All, NetConf, SSHD)
    - Encapsulation: IPSec
    - Default Route: 199.1.1.14
  - vpn 512
    - Interface eth0
    - IP Address: 192.168.1.3/24

vBond

```
config
!
vpn 0
 no interface eth0
 interface Ge0/0
  ip address 199.1.1.3/28
  tunnel-interface
   encapsulation ipsec
   allow-service all
   allow-service netconf
   allow-service sshd
   no shut
 ip route 0.0.0.0/0 199.1.1.14
!
vpn 512
 interface eth0
  ip address 192.168.1.3/24
  no shut
!
 commit
```

Lab 6 – Initializing vBond - GUI

Task 1 – Add vBond to vManage

- Navigate to **Configuration -> Devices -> Controllers -> Add Controllers -> vBond** and specify the following to add the vBond in vManage.
  - IP Address: **199.1.1.3**
  - Username: **Admin**
  - Password: **Admin**
  - Check Generate CSR
  - Click **OK**

Task 2 – View the generated CSR for vBond and Copy it

- Navigate to **Configuration -> Certificates -> Controllers -> vBond -> View CSR.**
- It will open a window with the CSR. Copy by using **CTRL-A** and **CTRL-C.**

Task 3 – Request a Certificate from the CA Server

- Browse to http://192.168.1.5/certsrv
- Click **"Request a Certificate".**
- Select **"Advanced"**.
- Paste the CSR in the box by using **CTRL-V** and click **Submit.**

Task 4 – Issue the Certificate from the CA Server

- Open Server Manager and navigate to **Active Directory Certificate Server -> KBITS-CA -> Pending Requests.**
- Right-Click the request and click "**Issue".**

Task 6 – Downloading the Issued Certificate

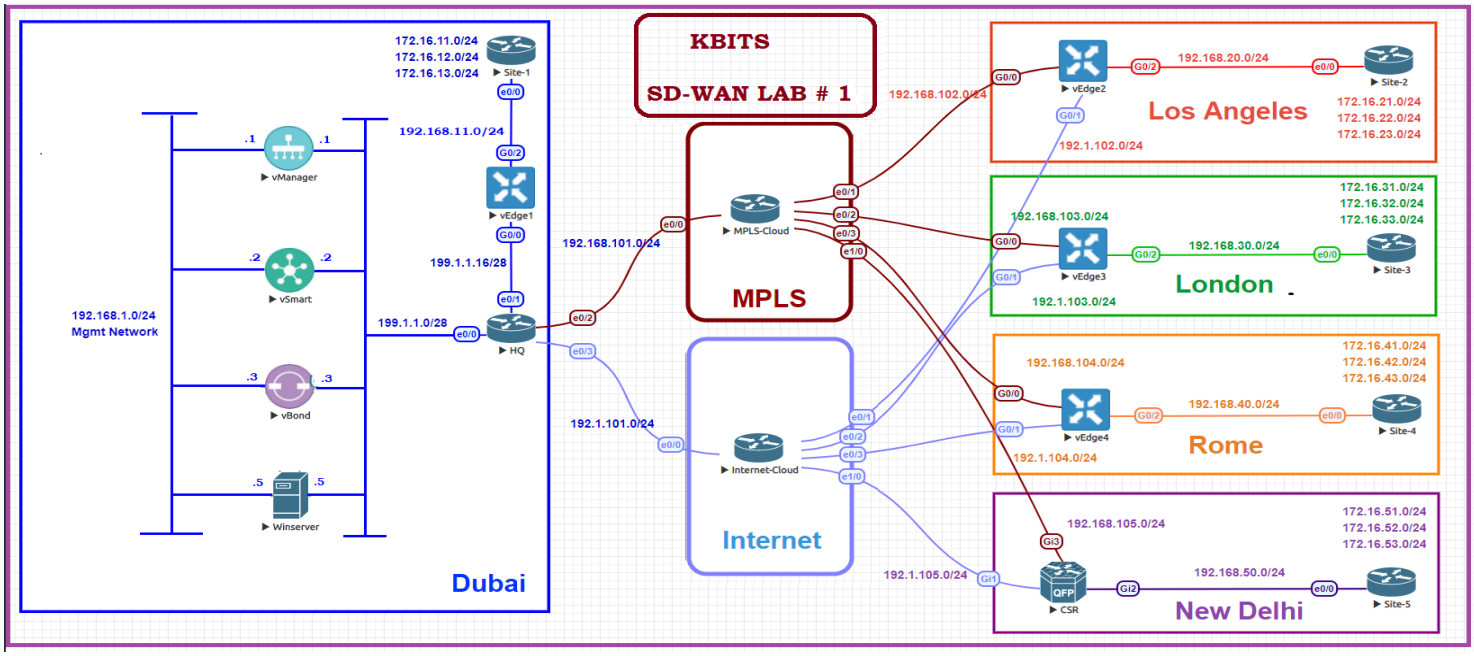
- Browse to http://192.168.1.5/certsrv

- Click **“Check on Pending request”.**
- The issued certificate link will show up. Click on the link.
- Select “**Base 64”** and click “**Download”**
- Open Explorer and navigate to the downloads folder.
- Change the name of the Downloaded file “**Certnew**” to “**vBond**”.
- Open the “**vBond.cer**” file using Notepad.
- Copy using **CTRL-A** and **CTRL-C**.

Task 6 – Installing the Identity Certificate for vManage

- In vManage, Navigate to **Configuration -> Certificates -> Controllers**
- Click on the **“Install”** button at the top right corner
- Paste the Certificate (CTRL-V).
- The Identity certificate should be installed for vBond and pushed to it.

Lab 7 – Initializing vSmart – CLI



Task 1 – Configuring the System Component

- Configure the System parameters based on the following:
  - Host-name : vSmart1
  - Organization: KBITS
  - System-IP: 10.1.1.102
  - Site ID: 1
  - vbond Address: 199.1.1.3
  - Timezone: Based on the appropriate Timezone

Note: Default username: admin **Default password**: admin

vSmart

```
config
!
system
 host-name vSmart1
 system-ip 10.1.1.102
 site-id 1
 organization-name KBITS
 clock timezone Asia/Muscat
 vbond 199.1.1.3
!
```

Commit

Task 2 – Configured the vpn parameters

- Configure the VPN parameters based on the following:

  - vpn 0
    - Interface Eth1
    - IP Address: 199.1.1.2/28
    - Tunnel Interface
    - Tunnel Services (All, NetConf, SSHD)
    - Default Route: 199.1.1.14

  - vpn 512
    - Interface eth0
    - IP Address: 192.168.1.2/24

vSmart

```
config
!
vpn 0
 no interface eth0
 interface eth1
  ip address 199.1.1.2/28
  tunnel-interface
   allow-service all
   allow-service netconf
   allow-service sshd
   no shut
 ip route 0.0.0.0/0 199.1.1.14
!
vpn 512
 interface eth0
  ip address 192.168.1.2/24
  no shut
!
```

Commit

Lab 8 – Initializing vSmart - GUI

Task 1 – Add vSmart to vManage

- Navigate to **Configuration -> Devices -> Controllers -> Add Controllers -> vSmart** and specify the following to add the vBond in vManage.
  - IP Address: **199.1.1.2**
  - Username: **Admin**
  - Password: **Admin**
  - Check Generate CSR
  - Click **OK**

Task 2 – View the generated CSR for vBond and Copy it

- Navigate to **Configuration -> Certificates -> Controllers -> vSmart -> View CSR.**
- It will open a window with the CSR. Copy by using **CTRL-A** and **CTRL-C.**

Task 3 – Request a Certificate from the CA Server

- Browse to http://192.168.1.5/certsrv
- Click **"Request a Certificate".**
- Select **"Advanced"**.
- Paste the CSR in the box by using **CTRL-V** and click **Submit.**

Task 4 – Issue the Certificate from the CA Server

- Open Server Manager and navigate to **Active Directory Certificate Server -> KBITS-CA -> Pending Requests.**
- Right-Click the request and click "**Issue".**

Task 6 – Downloading the Issued Certificate

- Browse to http://192.168.1.5/certsrv

- Click **“Check on Pending request”.**
- The issued certificate link will show up. Click on the link.
- Select “**Base 64”** and click “**Download”**
- Open Explorer and navigate to the downloads folder.
- Change the name of the Downloaded file “**Certnew**” to “**vSmart**”.
- Open the “**vSmart.cer**” file using Notepad.
- Copy using **CTRL-A** and **CTRL-C**.

Task 6 – Installing the Identity Certificate for vManage

- In vManage, Navigate to **Configuration -> Certificates -> Controllers**
- Click on the **“Install”** button at the top right corner
- Paste the Certificate (CTRL-V).
- The Identity certificate should be installed for vSmart and pushed to it.

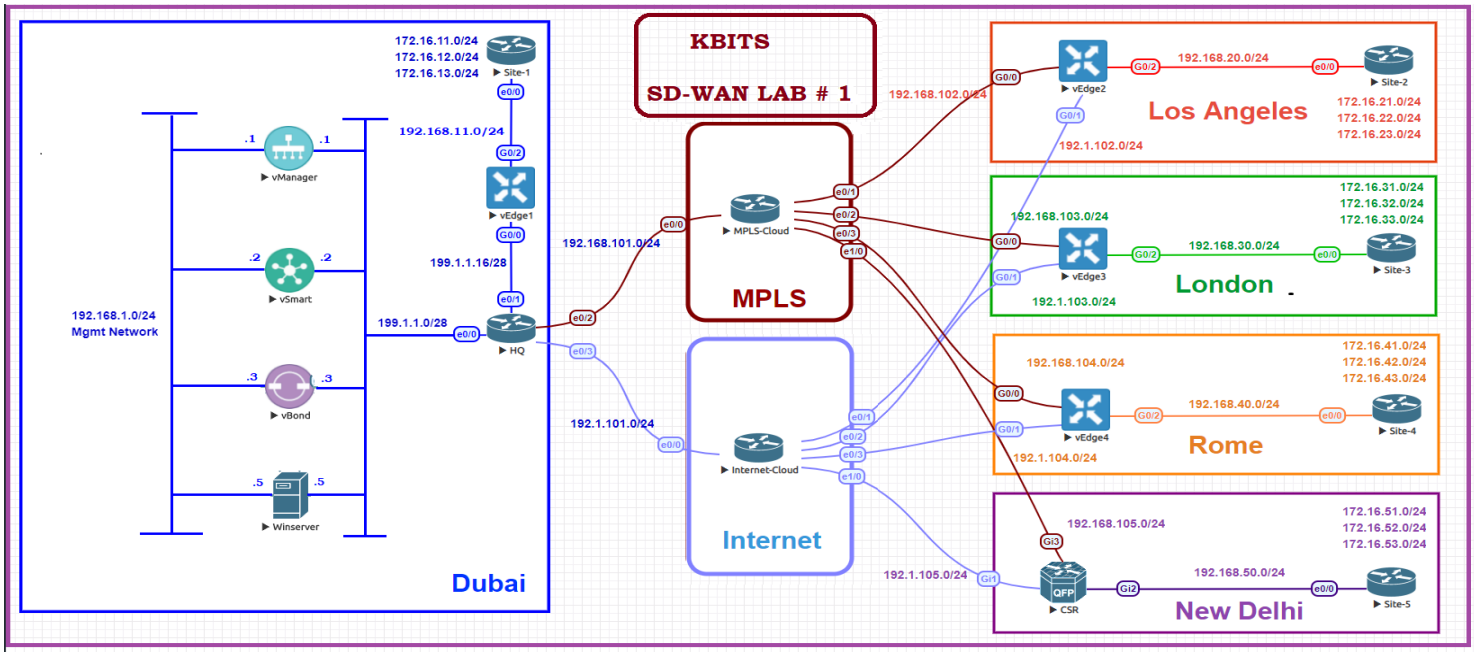
Implementing SD-WAN

Authored By:

Khawar Butt
CCIE # 12353
Hepta CCIE#12353
CCDE # 20110020

Initializing the WAN Edges

Lab 9 – Initializing vEdge – CLI



Task 1 – Upload the WAN Edge List

- On the vManage Main windows, Naviagte to **Configuration -> Devices**. Click on "**Upload WAN Edge List**".
- Select the file you downloaded from the PNP Portal. Upload it and check the **Validate** option.

vEDGE-1

Task 1 – Configuring the System Component

- Configure the System parameters based on the following:
  - Host-name : vEdge1
  - Organization: KBITS
  - System-IP: 10.2.2.201
  - Site ID: 1
  - vbond Address: 199.1.1.3
  - Timezone: Based on the appropriate Timezone

Note: Default username: admin **Default password**: admin

vEdge1

```
config
!
system
 host-name vEdge1
 system-ip 10.2.2.201
 site-id 1
 organization-name KBITS
 clock timezone Asia/Muscat
 vbond 199.1.1.3
!
 commit
```

Task 2 – Configure the vpn parameters

- Configure the VPN parameters based on the following:

  - vpn 0
    - Interface Ge0/0
    - IP Address: 199.1.1.17/28
    - Tunnel Interface
    - Encapsulation IPSec
    - Tunnel Services (All, NetConf, SSHD)
    - Default Route: 199.1.1.30

  - vpn 512
    - Interface eth0
    - IP Address: DHCP Client

vEdge1

```
config
!
vpn 0
 no interface eth0
 interface Ge0/0
  ip address 199.1.1.17/28
  tunnel-interface
   encapsulation ipsec
   allow-service all
   allow-service netconf
```

```
  allow-service sshd
  no shut
 ip route 0.0.0.0/0 199.1.1.30
!
vpn 512
 interface eth0
  ip dhcp-client
  no shutdown
 commit
```

vEDGE-2

Task 1 – Configuring the System Component

- Configure the System parameters based on the following:
  - Host-name : vEdge2
  - Organization: KBITS
  - System-IP: 10.2.2.202
  - Site ID: 2
  - vbond Address: 199.1.1.3
  - Timezone: Based on the appropriate Timezone

Note: Default username: admin **Default password**: admin

vEdge-2

```
config
!
system
 host-name vEdge2
 system-ip 10.2.2.202
 site-id 2
 organization-name KBITS
 clock timezone Asia/Muscat
 vbond 199.1.1.3
!
 commit
```

Task 2 – Configure the vpn parameters

- Configure the VPN parameters based on the following:
  - vpn 0

- Interface Ge0/0
- IP Address: 192.168.102.2/24
- Tunnel Interface
- Encapsulation IPSec
- Tunnel Services (All, NetConf, SSHD)
- Default Route: 192.168.102.254

- vpn 512
  - Interface eth0
  - IP Address: DHCP Client

vEdge2

```
config
!
vpn 0
 no interface eth0
 interface Ge0/0
  ip address 192.168.102.2/24
  tunnel-interface
   encapsulation ipsec
   allow-service all
   allow-service netconf
   allow-service sshd
   no shut
 ip route 0.0.0.0/0 192.168.102.254
!
vpn 512
 interface eth0
  ip dhcp-client
  no shutdown
 !
 commit
```

vEDGE-3

Task 1 – Configuring the System Component

- Configure the System parameters based on the following:

  - Host-name : vEdge3
  - Organization: KBITS
  - System-IP: 10.2.2.203
  - Site ID: 3

- vbond Address: 199.1.1.3
- Timezone: Based on the appropriate Timezone

Note: Default username: admin **Default password**: admin

vEdge-3

```
config
!
system
 host-name vEdge3
 system-ip 10.2.2.203
 site-id 3
 organization-name KBITS
 clock timezone Asia/Muscat
 vbond 199.1.1.3
!
 Commit
```

Task 2 – Configure the vpn parameters

- Configure the VPN parameters based on the following:

  - vpn 0
    - Interface Ge0/0
    - IP Address: 192.168.103.3/24
    - Tunnel Interface
    - Encapsulation IPSec
    - Tunnel Services (All, NetConf, SSHD)
    - Default Route: 192.168.103.254
  - vpn 512
    - Interface eth0
    - IP Address: DHCP Client

vEdge3

```
config
!
vpn 0
 no interface eth0
 interface Ge0/0
  ip address 192.168.103.3/24
  tunnel-interface
   encapsulation ipsec
   allow-service all
```

```
   allow-service netconf
   allow-service sshd
   no shut
 ip route 0.0.0.0/0 192.168.103.254
!
vpn 512
 interface eth0
  ip dhcp-client
  no shutdown
 !
 Commit
```

vEDGE-4

Task 1 – Configuring the System Component

- Configure the System parameters based on the following:
  - Host-name : vEdge4
  - Organization: KBITS
  - System-IP: 10.2.2.204
  - Site ID: 4
  - vbond Address: 199.1.1.3
  - Timezone: Based on the appropriate Timezone

Note: Default username: admin **Default password**: admin

vEdge-4

```
config
!
system
 host-name vEdge4
 system-ip 10.2.2.204
 site-id 4
 organization-name KBITS
 clock timezone Asia/Muscat
 vbond 199.1.1.3
!
 Commit
```

Task 2 – Configure the vpn parameters

- Configure the VPN parameters based on the following:

- vpn 0
  - Interface Ge0/0
  - IP Address: 192.168.104.4/24
  - Tunnel Interface
  - Encapsulation IPSec
  - Tunnel Services (All, NetConf, SSHD)
  - Default Route: 192.168.104.254

- vpn 512
  - Interface eth0
  - IP Address: DHCP Client

vEdge4

```
config
!
vpn 0
 no interface eth0
 interface Ge0/0
  ip address 192.168.104.4/24
  tunnel-interface
   encapsulation ipsec
   allow-service all
   allow-service netconf
   allow-service sshd
   no shut
 ip route 0.0.0.0/0 192.168.104.254
!
vpn 512
 interface eth0
  ip dhcp-client
  no shutdown
 !
 Commit
```

Lab 10 – Registering vEdges in vManage

vEDGE-1

Task 1 – Upload the Root Certificate to the vEdge

- On the Windows Server, open **WINSCP** application.
- **Connect** to vEdge1 using the following information:
  - IP Address : 199.1.1.17
  - Protocol - SFTP
  - Username : admin
  - Password : admin
- Copy the **RootCert.cer** file from the Downloads folder to the **/home/admin** folder on the vEdge1

Task 2 – Install the Root Certificate on vEdge1

- Connect to the console of vEdge1 and issue the following command:

  request root-cert-chain install /home/admin/RootCert.cer

Task 3 - Activate vEdge on vManage

- Navigate to **Configuration -> Devices**
- Note and use the **Chassis Number** and **Token number** for the 1st vEdge from vManage.
- Use the information from the previous step in the following command on the vEdge1 console.

  request vedge-cloud activate chassis-number **XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX** token **XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX**

- You should see the vEdge in the vManage console with a Certificate issued.

vEDGE-2

Task 1 – Upload the Root Certificate to the vEdge

- On the Windows Server, open **WINSCP** application.
- **Connect** to vEdge1 using the following information:
  - IP Address : 192.168.102.2
  - Protocol - SFTP
  - Username : admin
  - Password : admin
- Copy the **RootCert.cer** file from the Downloads folder to the **/home/admin** folder on the vEdge2

Task 2 – Install the Root Certificate on vEdge2

- Connect to the console of vEdge2 and issue the following command:

  request root-cert-chain install /home/admin/RootCert.cer

Task 3 - Activate vEdge on vManage

- Navigate to **Configuration -> Devices**
- Note and use the **Chassis Number** and **Token number** for the 2nd vEdge from vManage.
- Use the information from the previous step in the following command on the vEdge2 console.

  request vedge-cloud activate chassis-number **XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX** token **XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX**

- You should see the vEdge in the vManage console with a Certificate issued.

vEDGE-3

Task 1 – Upload the Root Certificate to the vEdge

- On the Windows Server, open **WINSCP** application.
- **Connect** to vEdge1 using the following information:
  - IP Address : 192.168.103.3
  - Protocol - SFTP
  - Username : admin
  - Password : admin
- Copy the **RootCert.cer** file from the Downloads folder to the **/home/admin** folder on the vEdge3

Task 2 – Install the Root Certificate on vEdge3

- Connect to the console of vEdge3 and issue the following command:

  request root-cert-chain install /home/admin/RootCert.cer

Task 3 - Activate vEdge on vManage

- Navigate to **Configuration -> Devices**
- Note and use the **Chassis Number** and **Token number** for the 3rd vEdge from vManage.
- Use the information from the previous step in the following command on the vEdge3 console.

  request vedge-cloud activate chassis-number **XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX** token **XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX**

- You should see the vEdge in the vManage console with a Certificate issued.

vEDGE-4

Task 1 – Upload the Root Certificate to the vEdge

- On the Windows Server, open **WINSCP** application.
- **Connect** to vEdge1 using the following information:
  - IP Address : 192.168.104.4
  - Protocol - SFTP
  - Username : admin
  - Password : admin
- Copy the **RootCert.cer** file from the Downloads folder to the **/home/admin** folder on the vEdge4

Task 2 – Install the Root Certificate on vEdge4

- Connect to the console of vEdge4 and issue the following command:

  request root-cert-chain install /home/admin/RootCert.cer

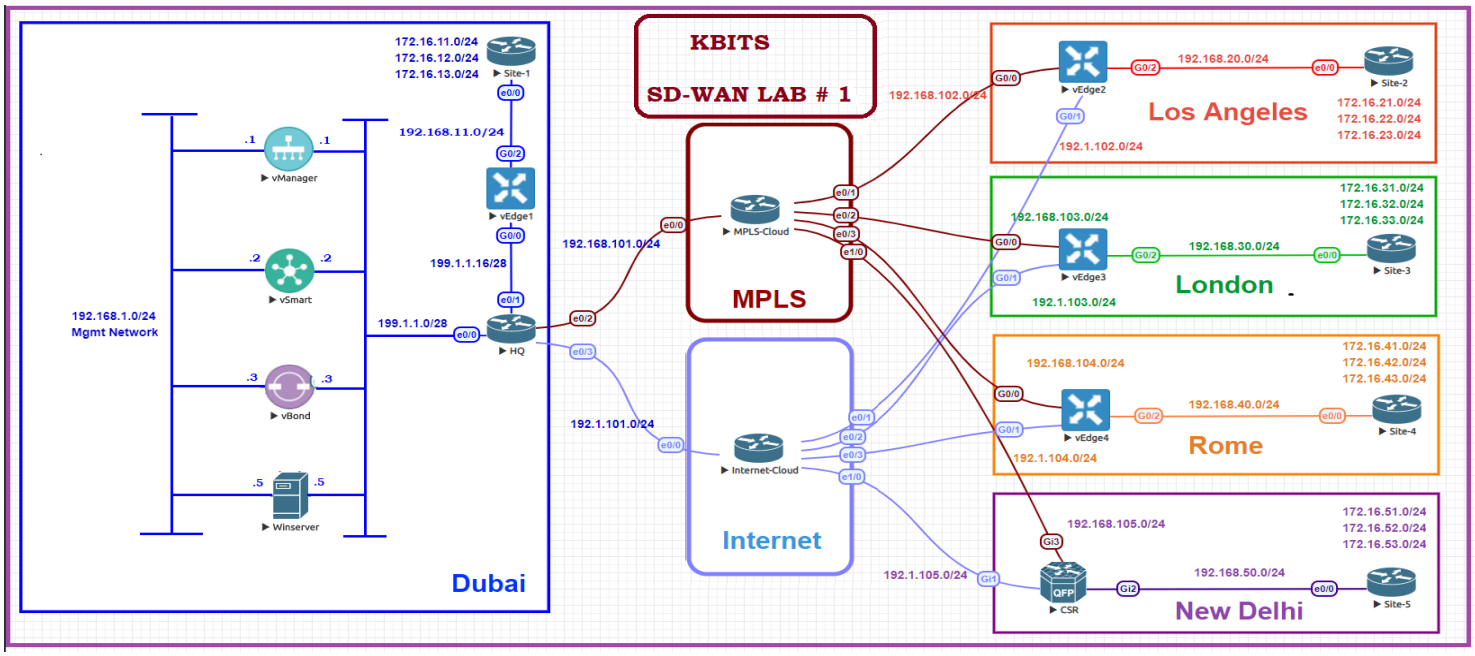
Task 3 - Activate vEdge on vManage

- Navigate to **Configuration -> Devices**
- Note and use the **Chassis Number** and **Token number** for the 4th vEdge from vManage.
- Use the information from the previous step in the following command on the vEdge4 console.

  request vedge-cloud activate chassis-number **XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX** token **XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX**

- You should see the vEdge in the vManage console with a Certificate issued.

Lab 11 – Initializing cEdge – CLI



cEDGE-1

Task 1 – Configuring the System Component

- Configure the System parameters based on the following:
  - Host-name : cEdge5
  - Organization: KBITS
  - System-IP: 10.2.2.205
  - Site ID: 5
  - vbond Address: 199.1.1.3
  - Timezone: Based on the appropriate Timezone

Note: Default username: admin **Default password**: admin

cEdge1

```
config-transaction
!
hostname cEdge1
!
system
 system-ip 10.2.2.205
 site-id 5
 organization-name KBITS
```

```
 vbond 199.1.1.3
 exit
!
clock timezone GST 4
commit
```

Task 2 – Configure the Interface and Tunnel Parameters

- Configure the Interface parameters based on the following:
  - GigabitEthernet1 Parameters
    - IP Address: 192.168.105.5/24
    - Default Route: 192.168.105.254
  - Tunnel Parameters Parameters
    - Tunnel Interface: Tunnel1
    - Tunnel Source: GigabitEthernet1
    - Tunnel Mode: SDWAN
  - SDWAN Interface Parameters
    - Interface: GigabitEthernet1
    - Encapsulation: IPSec
    - Color: default
    - Tunnel Services (All, NetConf, SSHD)

vEdge1

```
config-transaction
!
interface GigabitEthernet1
 no shutdown
 ip address 192.168.105.5 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 192.168.105.254
!
interface Tunnel1
 no shutdown
 ip unnumbered GigabitEthernet1
 tunnel source GigabitEthernet1
 tunnel mode sdwan
exit
!
sdwan
 interface GigabitEthernet1
  tunnel-interface
   encapsulation ipsec
   color default
```

```
    allow-service all
    allow-service sshd
    allow-service netconf
   exit
  exit
commit
```

Lab 12 – Registering cEdges in vManage

cEDGE-1

Task 1 – Upload the Root Certificate to the vEdge

- Open the **TFTP Application** on the Windows Server.
- Configure the Default Folder as the **Downloads** Folder and using the 199.1.1.5 as the TFTP Interface.
- Connect to the console of cEdge1 and copy the RootCert.cer file to flash: using the following command:

  copy tftp://199.1.1.5/RootCert.cer flash:

Task 2 – Install the Root Certificate on cEdge1

- Connect to the console of cEdge1 and issue the following command:

  request platform software sdwan root-cert-chain install bootflash:Root.cer

Task 3 - Activate cEdge on vManage

- Navigate to **Configuration -> Devices**
- Note and use the **Chassis Number** and **Token number** for the 1st CSR Device from vManage.
- Use the information from the previous step in the following command on the cEdge1 console.

  request platform software sdwan vedge_cloud activate chassis-number **CSR-XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX** token **XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX**

- You should see the vEdge in the vManage console with a Certificate issued.

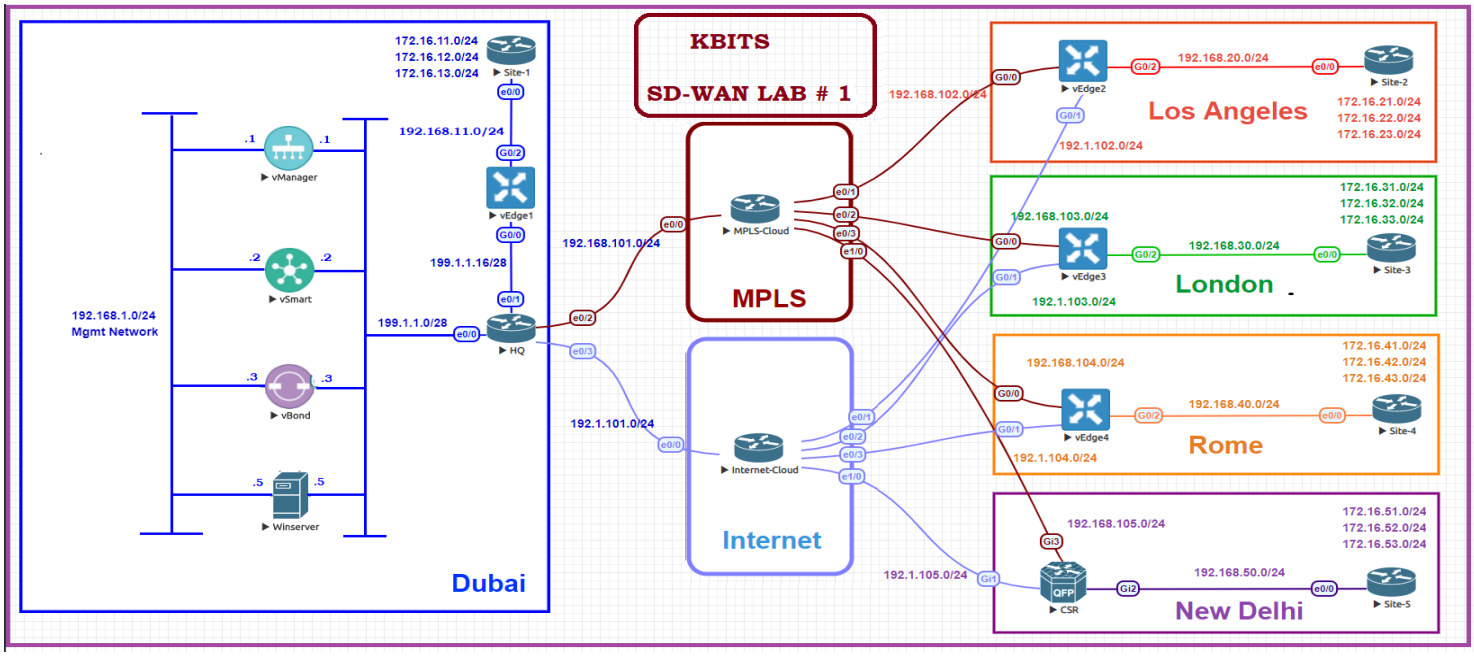
Implementing SD-WAN

Authored By:

Khawar Butt
CCIE # 12353
Hepta CCIE#12353
CCDE # 20110020

Configuring Templates

Lab 13 – Configuring Feature Template – System



Task 1 – Configure the System Template to be used by all vEdge-Cloud Devices

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vEdge Cloud -> Basic Information -> System**

- Configure the System parameters based on the following:

  - Template Name : **VE-System**
  - Description : **VE-System**
  - Site ID -> Device Specific
  - System IP ->Device Specific
  - Hostname -> Device Specific
  - Timezone -> Global : **Asia/Muscat**
  - Console Baud Rate -> **Default**

- Click **Save** to save the Template.

Task 2 – Configure the System Template to be used by all cEdge-Cloud Devices

- In vManage, Navigate to Configuration -> **Templates -> Feature -> CSR Cloud -> Basic Information -> System**

- Configure the System parameters based on the following:

  - Template Name : **CE-System**
  - Description : **CE-System**
  - Site ID -> Device Specific
  - System IP ->Device Specific
  - Hostname -> Device Specific
  - Timezone -> Global : **Asia/Muscat**
  - Console Baud Rate -> **Default**

- Click **Save** to save the Template.

Lab 14 – Configuring Feature Template – Banner

Task 1 – Configure the Banner Template to be used by all vEdge-Cloud Devices

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vEdge Cloud -> Basic Information -> Banner**

- Configure the Banner parameters based on the following:

  - Template Name : **VE-Banner**
  - Description : **VE-Banner**
  - Timezone -> Global : **Asia/Muscat**
  - Console Baud Rate -> **Default**

- Click **Save** to save the Template.

Task 2 – Configure the Banner Template to be used by all cEdge-Cloud Devices

- In vManage, Navigate to Configuration -> **Templates -> Feature -> CSR Cloud -> Basic Information -> Banner**

- Configure the Banner parameters based on the following:

  - Template Name : **VE-Banner**
  - Description : **CE-Banner**
  - Timezone -> Global : **Asia/Muscat**
  - Console Baud Rate -> **Default**

- Click **Save** to save the Template.

Lab 15 - Configuring Feature Templates - VPN & VPN Interfaces for VPN 0 & 512 — Branch Site(vEdges)

Task 1 – Configure a VPN Template to be used by all Branch vEdge-Cloud Devices for VPN 0

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vEdge Cloud -> VPN -> VPN**

- Configure the VPN parameters based on the following:

  - Template Name : **BR-VE-VPN-VPN0**
  - Description : **BR-VE-VPN-VPN0**

  Basic Configuration
  - VPN -> Global : **0**
  - Name -> Global : **Transport VPN**

  IPv4 Route
  - Prefix -> Global : 0.0.0.0/0
  - Next Hop -> Device Specific

- Click **Save** to save the Template.

Task 2 – Configure a VPN Template to be used by all Branch vEdge-Cloud Devices for VPN 512

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vEdge Cloud -> VPN -> VPN**

- Configure the VPN parameters based on the following:

  - Template Name : **BR-VE-VPN-VPN512**
  - Description : **BR-VE-VPN-VPN512**

  Basic Configuration
  - VPN -> Global : **512**
  - Name -> Global : **MGMT VPN**

- Click **Save** to save the Template.

Task 3 – Configure a VPN Interface Template to be used by all Branch vEdge-Cloud Devices for VPN 0 for Interface G0/0

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vEdge Cloud -> VPN -> VPN Interface Ethernet**

- Configure the VPN parameters based on the following:

  - Template Name : **BR-VE-VPNINT-VPN0-G0**
  - Description : **BR-VE-VPNINT-VPN0-G0**

  Basic Configuration
  - Shutdown -> Global : **No**
  - Interface Name -> Global : **Ge0/0**
  - IPv4 Address -> Static -> Device Specific

  Tunnel
  - Tunnel Inteface -> Global : **On**
  - Color -> Global : **MPLS**

  Allow Service
  - All -> Global : **On**
  - NETCONF -> Global : **On**
  - SSH -> Global : **On**

- Click **Save** to save the Template.

Task 4 – Configure a VPN Interface Template to be used by all Branch vEdge-Cloud Devices for VPN 0 for Interface G0/1

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vEdge Cloud -> VPN -> VPN Interface Ethernet**

- Configure the VPN parameters based on the following:

  - Template Name : **BR-VE-VPNINT-VPN0-G1**
  - Description : **BR-VE-VPNINT-VPN0-G1**

  Basic Configuration
  - Shutdown -> Global : **No**
  - Interface Name -> Global : **Ge0/1**
  - IPv4 Address -> Static -> Device Specific

  Tunnel
  - Tunnel Inteface -> Global : **On**
  - Color -> Global : **BIZ-Internet**

Allow Service

- All -> Global : **On**
- NETCONF -> Global : **On**
- SSH -> Global : **On**

Click **Save** to save the Template.

Task 5 – Configure a VPN Interface Template to be used by all Branch vEdge-Cloud Devices for VPN 512 for Interface Eth0

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vEdge Cloud -> VPN -> VPN Interface Ethernet**

- Configure the VPN parameters based on the following:

  - Template Name : **BR-VE-VPNINT-VPN512-E0**
  - Description : **BR-VE-VPNINT-VPN512-E0**

  Basic Configuration

  - Shutdown -> Global : **No**
  - Interface Name -> Global : **eth0**
  - IPv4 Address -> Dynamic

- Click **Save** to save the Template

Lab 16 - Configuring Feature Templates – External Routing - OSPF for VPN 0 – Branch Site(vEdges)

Task 1 – Configure a OSPF Template to be used by all Branch vEdge-Cloud Devices for VPN 0

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vEdge Cloud -> Other Templates -> OSPF**

- Configure the OSPF parameters based on the following:

  - Template Name : **BR-VE-OSPF-VPN0**
  - Description : **BR-VE-OSPF-VPN0**

  Area Configuration
  - Area Number -> Global : **0**
  - Area Type -> Default

  Interface Configuration
  - Interface Name: Ge0/0

  Advanced
  - OSPF Network Type: Point-to-Point

- Click **Add** to add the Interface and Click **Add** to add OSPF.

- Click **Save** to save the Template.

Lab 17 - Configuring and Deploying Device Templates for vEdge – Branch Site(vEdge2)

Task 1 – Configure a Device Template for Branch vEdge Devices.

- In vManage, Navigate to Configuration -> **Templates -> Device -> Create Template -> vEdge Cloud**

- Configure the Device Template based on the following:

  - Template Name : **BR-VE-TEMP**
  - Description : **BR-VE-TEMP**

  Basic Information
  - System -> **VE-System**

  Transport & Management
  - VPN 0 : **BR-VE-VPN-VPN0**
  - VPN Interface : **BR-VE-VPNINT-VPN0-G0**
  - VPN Interface : **BR-VE-VPNINT-VPN0-G1**
  - OSPF : **BR-VE-OSPF-VPN0**

  - VPN 512 : **BR-VE-VPN-VPN512**
  - VPN Interface : **BR-VE-VPNINT-VPN512-E0**

- Click **Save** to save the Template.

Task 2 – Attach vEdge2 to the Device Template

- In vManage, Navigate to Configuration -> **Templates -> Device -> BR-VE-TEMP.**

- Click on "**...**" towards the right-hand side.

- Click **Attach Devices.**

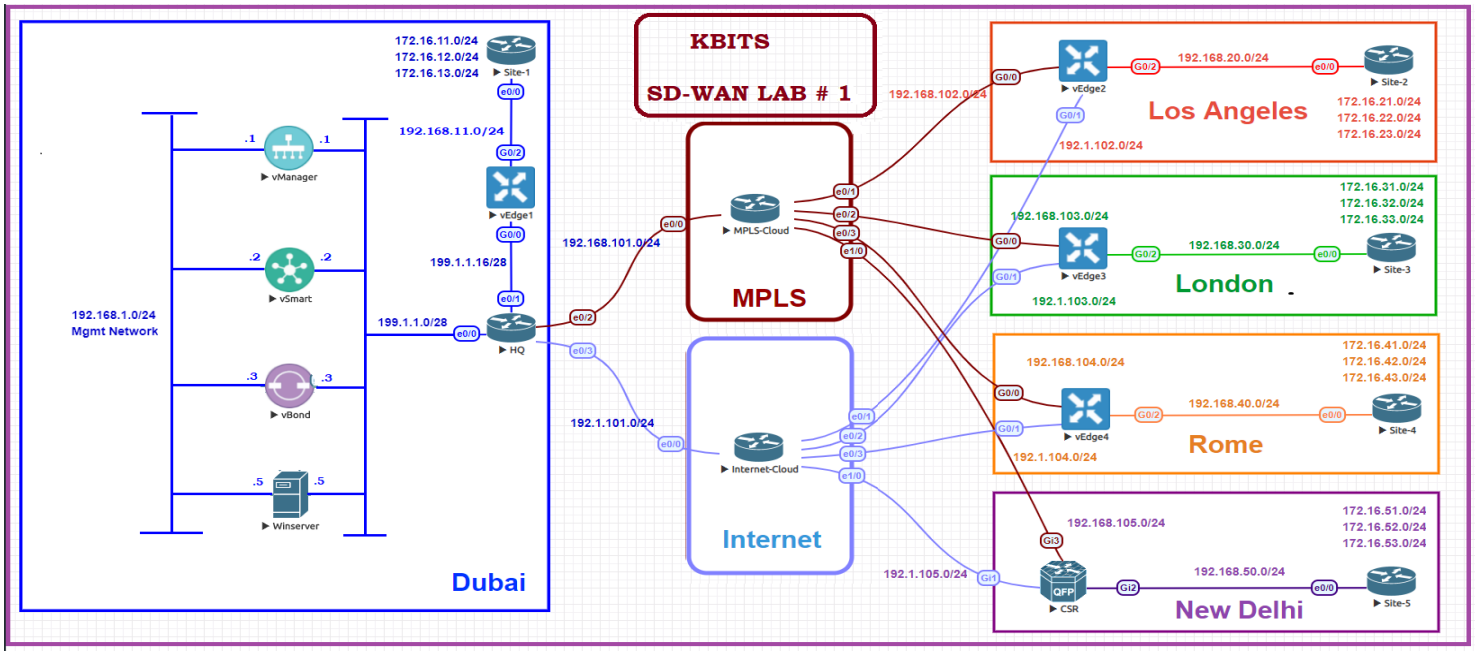
- Select **vEdge2** and click the " **->** " button.

- Click **Attach**.

Task 3 – Configure the Variable Parameters for the Feature Templates

- **vEdge2** will appear in the window.
- Click on "**...**" towards the right-hand side.
- Click **Edit Device Template.**
- Configure the variables based on the following:
  - Default Gateway for VPN0 : **192.1.102.254**
  - Interface IP for Ge0/1 :**192.1.102.2**
  - Interface IP for Ge0/0 :**192.168.102.2**
  - Hostname : **vEdge-2**
  - System IP : **10.2.2.202**
  - Site ID : **2**
- Click **Update.**
- Verify the Configuration & Click **Configure Devices.**
- Wait for it to update the device. It should come back with Status of **Success**.
- Verify the configuration on **vEdge2**. You can do that by verify OSPF Neighbor relationship with the MPLS Router by issuing the **Show ospf neighbor** command on **vEdge2.**
- Type **Show Ip route** on **vEdge2** to verify that you are receiving OSPF routes from the MPLS Router.

Lab 18 - Configuring Internal Routing Protocols on the Internal Routing Devices – HQ & All Branches



Interface Configuration

Site-1

Interface	IP Address	Subnet Mask
E 0/0	192.168.11.11	255.255.255.0
Loopback1	172.16.11.1	255.255.255.0
Loopback2	172.16.12.1	255.255.255.0
Loopback3	172.16.13.1	255.255.255.0

Site-2

Interface	IP Address	Subnet Mask
E 0/0	192.168.20.22	255.255.255.0
Loopback1	172.16.21.1	255.255.255.0
Loopback2	172.16.22.1	255.255.255.0
Loopback3	172.16.23.1	255.255.255.0
Loopback4	172.16.234.2	255.255.255.255

Site-3

Interface	IP Address	Subnet Mask
E 0/0	192.168.30.33	255.255.255.0
Loopback1	172.16.31.1	255.255.255.0
Loopback2	172.16.32.1	255.255.255.0
Loopback3	172.16.33.1	255.255.255.0
Loopback4	172.16.234.3	255.255.255.255

Site-4

Interface	IP Address	Subnet Mask
E 0/0	192.168.40.44	255.255.255.0
Loopback1	172.16.41.1	255.255.255.0
Loopback2	172.16.42.1	255.255.255.0
Loopback3	172.16.43.1	255.255.255.0
Loopback4	172.16.234.4	255.255.255.255

Site-5

Interface	IP Address	Subnet Mask
E 0/0	192.168.50.55	255.255.255.0
Loopback1	172.16.51.1	255.255.255.0
Loopback2	172.16.52.1	255.255.255.0
Loopback3	172.16.53.1	255.255.255.0

Task 1 – Internal Site Router Configurations

- Configure the Interfaces based on the Logical Diagram
- Configure OSPF as the IGP to communicate with the vEdge/cEdge devices. Enable all the interfaces under OSPF.
- Configure the Loopback Interfaces as OSPF Network Point-to-point Interfaces.

Site-1

```
no ip domain-loo
line con 0
 logg sync
 no exec-timeout
!
Hostname Site-1
!
Interface E 0/0
 ip address 192.168.11.11 255.255.255.0
 no shut
!
Interface Loopback1
 ip address 172.16.11.1 255.255.255.0
 ip ospf network point-to-point
!
Interface Loopback2
 ip address 172.16.12.1 255.255.255.0
 ip ospf network point-to-point
!
Interface Loopback3
 ip address 172.16.13.1 255.255.255.0
 ip ospf network point-to-point
!
router ospf 1
 network 192.168.11.0 0.0.0.255 area 0
 network 172.16.0.0 0.0.255.255 area 0
```

Site-2

```
no ip domain-loo
line con 0
 logg sync
 no exec-timeout
!
Hostname Site-2
!
Interface E 0/0
 ip address 192.168.20.22 255.255.255.0
 no shut
!
Interface Loopback1
 ip address 172.16.21.1 255.255.255.0
 ip ospf network point-to-point
!
Interface Loopback2
 ip address 172.16.22.1 255.255.255.0
 ip ospf network point-to-point
!
Interface Loopback3
 ip address 172.16.23.1 255.255.255.0
 ip ospf network point-to-point
!
Interface Loopback4
 ip address 172.16.234.2 255.255.255.255
 ip ospf network point-to-point
!
router ospf 1
 network 192.168.20.0 0.0.0.255 area 0
 network 172.16.0.0 0.0.255.255 area 0
```

Site-3

```
no ip domain-loo
line con 0
 logg sync
 no exec-timeout
!
Hostname Site-3
!
Interface E 0/0
 ip address 192.168.30.33 255.255.255.0
 no shut
!
Interface Loopback1
 ip address 172.16.31.1 255.255.255.0
 ip ospf network point-to-point
!
Interface Loopback2
 ip address 172.16.32.1 255.255.255.0
 ip ospf network point-to-point
!
Interface Loopback3
 ip address 172.16.33.1 255.255.255.0
 ip ospf network point-to-point
!
Interface Loopback4
 ip address 172.16.234.3 255.255.255.255
 ip ospf network point-to-point
!
router ospf 1
 network 192.168.30.0 0.0.0.255 area 0
 network 172.16.0.0 0.0.255.255 area 0
```

Site-4

```
no ip domain-loo
line con 0
 logg sync
 no exec-timeout
!
Hostname Site-4
!
Interface E 0/0
 ip address 192.168.40.44 255.255.255.0
 no shut
!
Interface Loopback1
 ip address 172.16.41.1 255.255.255.0
 ip ospf network point-to-point
!
Interface Loopback2
 ip address 172.16.42.1 255.255.255.0
 ip ospf network point-to-point
!
Interface Loopback3
 ip address 172.16.43.1 255.255.255.0
 ip ospf network point-to-point
!
Interface Loopback4
 ip address 172.16.234.4 255.255.255.255
 ip ospf network point-to-point
!
router ospf 1
 network 192.168.40.0 0.0.0.255 area 0
 network 172.16.0.0 0.0.255.255 area 0
```

Site-5

```
no ip domain-loo
line con 0
 logg sync
 no exec-timeout
!
Hostname Site-5
!
Interface E 0/0
 ip address 192.168.50.55 255.255.255.0
 no shut
!
Interface Loopback1
 ip address 172.16.51.1 255.255.255.0
 ip ospf network point-to-point
!
Interface Loopback2
 ip address 172.16.52.1 255.255.255.0
 ip ospf network point-to-point
!
Interface Loopback3
 ip address 172.16.53.1 255.255.255.0
 ip ospf network point-to-point
!
router ospf 1
 network 192.168.50.0 0.0.0.255 area 0
 network 172.16.0.0 0.0.255.255 area 0
```

Lab 19 - Configuring Feature Templates – Service VPN – VPN, VPN Interface and Internal Routing – Branch Site(vEdges)

Task 1 – Configure a VPN Template to be used by all Branch vEdge-Cloud Devices for VPN 1

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vEdge Cloud -> VPN -> VPN**

- Configure the VPN parameters based on the following:

  - Template Name : **BR-VE-VPN-VPN1**
  - Description : **BR-VE-VPN-VPN1**

  Basic Configuration
  - VPN -> Global : **1**
  - Name -> Global : **Data VPN**

- Click **Save** to save the Template.

Task 2 – Configure a VPN Interface Template to be used by all Branch vEdge-Cloud Devices for VPN 1 for Interface G0/2

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vEdge Cloud -> VPN -> VPN Interface Ethernet**

- Configure the VPN parameters based on the following:

  - Template Name : **BR-VE-VPNINT-VPN1-G2**
  - Description : **BR-VE-VPNINT-VPN1-G2**

  Basic Configuration
  - Shutdown -> Global : **No**
  - Interface Name -> Global : **Ge0/2**
  - IPv4 Address -> Static -> Device Specific

- Click **Save** to save the Template.

Task 3 – Configure a OSPF Template to be used by all Branch vEdge-Cloud Devices for VPN 1

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vEdge Cloud -> Other Templates -> OSPF**

- Configure the OSPF parameters based on the following:

  - Template Name : **BR-VE-OSPF-VPN1**
  - Description : **BR-VE-OSPF-VPN1**

  Redistribution
  - Protocol : **OMP**

  Area Configuration
  - Area Number -> Global : **0**
  - Area Type -> Default

  Interface Configuration
  - Interface Name: Ge0/2

- Click **Add** to add the Interface and Click **Add** to add OSPF.

- Click **Save** to save the Template.

Lab 20 - Implementing a Service VPN using Templates – Branch Site(vEdge2)

Task 1 – Edit the BR-VE-TEMP Device Template for Brance vEdge Devices.

- In vManage, Navigate to Configuration -> **Templates -> Device -> BR-VE-TEMP -> "…" -> Edit**

- Edit the BR-VE-TEMP Device Template based on the following:

  Service VPN
  - VPN 1 : **BR-VE-VPN-VPN1**
  - VPN Interface : **BR-VE-VPNINT-VPN1-G2**
  - OSPF : **BR-VE-OSPF-VPN1**

- Click **Save** to save the Template.

Task 2 – Configure the Variable Parameters for the Feature Templates

- **vEdge2** will appear in the window.

- Click on "**…**" towards the right-hand side & click **Edit Device Template.**

- Configure the variables based on the following:

  - Interface IP for Ge0/2 :**192.168.20.2**

- Click **Update.**

- Verify the Configuration & Click **Configure Devices.**

- Wait for it to update the device. It should come back with Status of **Success**.

- Verify the configuration on **vEdge2**. You can do that by verify OSPF Neighbor relationship with the Site-2 Router by issuing the **Show ospf neighbor** command on **vEdge2.**

- Type **Show Ip route** on **vEdge2** to verify that you are receiving OSPF routes from the Internal Site Router.

Lab 21 - Pushing Template to configure other Branch Sites - – Branch Site(vEdge3 & vEdge4)

Task 1 – Attach the BR-VE-TEMP Device Template for Brance vEdge Devices.

- In vManage, Navigate to Configuration -> **Templates -> Device -> BR-VE-TEMP -> "…" -> Attach Devices.**
- Click **Attach Devices.**
- Select **vEdge3** & **vEdge4** and click the " **->** " button.
- Click **Attach**.
- **vEdge3** & **vEdge4** will appear in the window.
- Click on "**…**" towards the right-hand side for both devices, one at a time click **Edit Device Template.**
- Configure the variables based on the following:

  vEdge-3

  - Interface IP for Ge0/2 :**192.168.30.3**
  - Default Gateway for VPN0 : **192.1.103.254**
  - Interface IP for Ge0/1 :**192.1.103.3**
  - Interface IP for Ge0/0 :**192.168.103.3**
  - Hostname : **vEdge-3**
  - System IP : **10.2.2.203**
  - Site ID : **3**

- Click **Update.**

  vEdge-4

  - Interface IP for Ge0/2 :**192.168.40.4**
  - Default Gateway for VPN0 : **192.1.104.254**
  - Interface IP for Ge0/1 :**192.1.104.4**
  - Interface IP for Ge0/0 :**192.168.104.4**
  - Hostname : **vEdge-4**

- System IP : **10.2.2.204**
- Site ID : **4**

- Click **Update.**

- Verify the Configuration & Click **Configure Devices.**

- Wait for it to update the device. It should come back with Status of **Success**.

- Verify the configuration on **vEdge3** & **vEdge4**. You can do that by verify OSPF Neighbor relationship with the Internal Site Router by issuing the **Show ospf neighbor** command on the **vEdges.**

- Type **Show Ip route** on **Internal Site Routers** to verify that you are receiving OSPF routes from the other Sites.

- Verify reachability between the sites by Pinging the Internal Loopback to Loopback networks.

Lab 22 – Configuring Feature Templates for HQ-Site(vEdge1) – VPNs, VPN Interfaces, External & Internal Routing

VPN 0

Task 1 – Configure a VPN Template for HQ vEdge-Cloud Devices for VPN 0

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vEdge Cloud -> VPN -> VPN**

- Configure the VPN parameters based on the following:

  - Template Name : **HQ-VE-VPN-VPN0**
  - Description : **HQ-VE-VPN-VPN0**

  Basic Configuration
  - VPN -> Global : **0**
  - Name -> Global : **Transport VPN**

  IPv4 Route
  - Prefix -> Global : 0.0.0.0/0
  - Next Hop -> Device Specific

- Click **Save** to save the Template.

Task 2 – Configure a VPN Interface Template to be used by HQ vEdge-Cloud Devices for VPN 0 for Interface G0/0

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vEdge Cloud -> VPN -> VPN Interface Ethernet**

- Configure the VPN parameters based on the following:

  - Template Name : **HQ-VE-VPNINT-VPN0-G0**
  - Description : **HQ-VE-VPNINT-VPN0-G0**

  Basic Configuration
  - Shutdown -> Global : **No**
  - Interface Name -> Global : **Ge0/0**
  - IPv4 Address -> Static -> Device Specific

Tunnel

- Tunnel Inteface -> Global : **On**
- Color -> Default

Allow Service

- All -> Global : **On**
- NETCONF -> Global : **On**
- SSH -> Global : **On**

- Click **Save** to save the Template.

Task 3 – Configure a BGP Template to be used by HQ vEdge-Cloud Devices for VPN 0

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vEdge Cloud -> Other Templates -> BGP**

- Configure the BGP parameters based on the following:

  - Template Name : **HQ-VE-BGP-VPN0**
  - Description : **HQ-VE-BGP-VPN0**

  Basic Configuration

  - Shutdown -> Global : **No**
  - AS Number -> Global : **65001**

  Neighbor

  - Adddress -> Global : **199.1.1.17/28**
  - Remote AS -> Global : **65001**
  - Address Family -> Global : **On**
  - Address Family -> Global : **IPv4-Unicast**

- Click **Add** to add the Interface and Click **Add** to add BGP Neighbor.

- Click **Save** to save the Template.

VPN 512

Task 1 – Configure a VPN Template to be used by HQ vEdge-Cloud Devices for VPN 512

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vEdge Cloud -> VPN -> VPN**

- Configure the VPN parameters based on the following:

- Template Name : **HQ-VE-VPN-VPN512**
- Description : **HQ-VE-VPN-VPN512**

Basic Configuration

- VPN -> Global : **512**
- Name -> Global : **MGMT VPN**

- Click **Save** to save the Template.

Task 2 – Configure a VPN Interface Template to be used by HQ vEdge-Cloud Devices for VPN 512 for Interface Eth0

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vEdge Cloud -> VPN -> VPN Interface Ethernet**

- Configure the VPN parameters based on the following:

  - Template Name : **HQ-VE-VPNINT-VPN512-E0**
  - Description : **HQ-VE-VPNINT-VPN512-E0**

  Basic Configuration

  - Shutdown -> Global : **No**
  - Interface Name -> Global : **eth0**
  - IPv4 Address -> Dynamic

- Click **Save** to save the Template

VPN 1

Task 1 – Configure a VPN Template for HQ vEdge-Cloud Devices for VPN 1

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vEdge Cloud -> VPN -> VPN**

- Configure the VPN parameters based on the following:

  - Template Name : **HQ-VE-VPN-VPN1**
  - Description : **HQ-VE-VPN-VPN1**

  Basic Configuration
  - VPN -> Global : **1**
  - Name -> Global : **Data VPN**

- Click **Save** to save the Template.

Task 2 – Configure a VPN Interface Template to be used by HQ vEdge-Cloud Devices for VPN 1 for Interface G0/2

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vEdge Cloud -> VPN -> VPN Interface Ethernet**

- Configure the VPN parameters based on the following:

  - Template Name : **HQ-VE-VPNINT-VPN1-G2**
  - Description : **HQ-VE-VPNINT-VPN1-G2**

  Basic Configuration
  - Shutdown -> Global : **No**
  - Interface Name -> Global : **Ge0/2**
  - IPv4 Address -> Static -> Device Specific

- Click **Save** to save the Template.

Task 3 – Configure a OSPF Template to be used by HQ vEdge-Cloud Devices for VPN 1

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vEdge Cloud -> Other Templates -> OSPF**

- Configure the OSPF parameters based on the following:

- Template Name : **HQ-VE-OSPF-VPN1**
- Description : **HQ-VE-OSPF-VPN1**

Redistribution

- Protocol : **OMP**

Area Configuration

- Area Number -> Global : **0**
- Area Type -> Default

Interface Configuration

- Interface Name: Ge0/2

- Click **Add** to add the Interface and Click **Add** to add OSPF.

- Click **Save** to save the Template.

Lab 23 - Configuring Device Templates for HQ-Site(vEdge1) to deploy VPN 0, 1 and 512.

Task 1 – Configure a Device Template for HQ vEdge Devices.

- In vManage, Navigate to Configuration -> **Templates -> Device -> Create Template -> vEdge Cloud**

- Configure the Device Template based on the following:

  - Template Name : **HQ-VE-TEMP**
  - Description : **HQ-VE-TEMP**

  Basic Information
  - System -> **VE-System**

  Transport & Management
  - VPN 0 : **HQ-VE-VPN-VPN0**
  - VPN Interface : **HQ-VE-VPNINT-VPN0-G0**
  - BGP : **HQ-VE-BGP-VPN0**

  - VPN 512 : **HQ-VE-VPN-VPN512**
  - VPN Interface : **HQ-VE-VPNINT-VPN512-E0**

  Service VPN
  - VPN 1 : **HQ-VE-VPN-VPN1**
  - VPN Interface : **HQ-VE-VPNINT-VPN1-G2**
  - OSPF : **HQ-VE-OSPF-VPN1**

- Click **Save** to save the Template.

Task 2 – Attach vEdge1 to the Device Template

- In vManage, Navigate to Configuration -> **Templates -> Device -> HQ-VE-TEMP.**

- Click on "**...**" towards the right-hand side.

- Click **Attach Devices.**

- Select **vEdge1** and click the " **->** " button.

- Click **Attach**.

Task 3 – Configure the Variable Parameters for the Feature Templates

- **vEdge1** will appear in the window.
- Click on "**...**" towards the right-hand side.
- Click **Edit Device Template.**
- Configure the variables based on the following:
  - Interface IP for Ge0/2 :**192.168.11.1**
  - Default Gateway for VPN0 : **199.1.1.30**
  - Interface IP for Ge0/0 :**199.1.1.17/28**
  - Hostname : **vEdge-1**
  - System IP : **10.2.2.201**
  - Site ID : **1**
- Click **Update.**
- Verify the Configuration & Click **Configure Devices.**
- Wait for it to update the device. It should come back with Status of **Success**.
- Verify the configuration on **vEdge1**. You can do that by verify OSPF Neighbor relationship with the Internal Router by issuing the **Show ospf neighbor** command on **vEdge1.**
- Type **Show Ip route** on **vEdge2** to verify that you are receiving OSPF routes from the MPLS Router.
- Type **Show Ip route** on **Internal Site Routers** to verify that you are receiving OSPF routes from the other Sites.
- Verify reachability between the sites by Pinging the Internal Loopback to Loopback networks.

Lab 24 – Configuring Feature Templates for CSR – VPNs, VPN Interfaces, External & Internal Routing

VPN 0

Task 1 – Configure a VPN Template by CSR for VPN 0

- In vManage, Navigate to Configuration -> **Templates -> Feature -> CSR1000v -> VPN -> VPN**

- Configure the VPN parameters based on the following:

  - Template Name : **BR-CSR-VPN-VPN0**
  - Description : **BR-CSR -VPN-VPN0**

  Basic Configuration
  - VPN -> Global : **0**
  - Name -> Global : **Transport VPN**

  IPv4 Route
  - Prefix -> Global : 0.0.0.0/0
  - Next Hop -> Device Specific

- Click **Save** to save the Template.

Task 2 – Configure a VPN Interface Template to be used by CSR for VPN 0 for Interface GigabitEthernet1

- In vManage, Navigate to Configuration -> **Templates -> Feature -> CSR1000v -> VPN -> VPN Interface Ethernet**

- Configure the VPN parameters based on the following:

  - Template Name : **BR-CSR-VPNINT-VPN0-G1**
  - Description : **BR-CSR-VPNINT-VPN0-G1**

  Basic Configuration
  - Shutdown -> Global : **No**
  - Interface Name -> Global : **GigabitEthernet1**
  - IPv4 Address -> Static -> Device Specific

Tunnel

- Tunnel Inteface -> Global : **On**
- Color -> Default

Allow Service

- All -> Global : **On**
- NETCONF -> Global : **On**
- SSH -> Global : **On**

- Click **Save** to save the Template.

Task 3 – Configure a VPN Interface Template to be used by CSR for VPN 0 for Interface GigabitEthernet2

- In vManage, Navigate to Configuration -> **Templates -> Feature -> CSR1000v -> VPN -> VPN Interface Ethernet**

- Configure the VPN parameters based on the following:

  - Template Name : **BR-CSR-VPNINT-VPN0-G2**
  - Description : **BR-CSR-VPNINT-VPN0-G2**

  Basic Configuration

  - Shutdown -> Global : **No**
  - Interface Name -> Global : **GigabitEthernet2**
  - IPv4 Address -> Static -> Device Specific

  Tunnel

  - Tunnel Inteface -> Global : **On**
  - Color -> Default

  Allow Service

  - All -> Global : **On**
  - NETCONF -> Global : **On**
  - SSH -> Global : **On**

- Click **Save** to save the Template.

Task 4 – Configure a OSPF Template to be used by CSR for VPN 0

- In vManage, Navigate to Configuration -> **Templates -> Feature -> CSR1000v -> Other Templates -> OSPF**

- Configure the OSPF parameters based on the following:

  - Template Name : **BR-CSR-OSPF-VPN0**
  - Description : **BR-CSR-OSPF-VPN0**

Area Configuration

- Area Number -> Global : **0**
- Area Type -> Default

Interface Configuration

- Interface Name: **GigabitEthernet1**
- OSPF Network Type: **Point-to-Point**

- Click **Add** to add the Interface and Click **Add** to add OSPF.

- Click **Save** to save the Template.

VPN 512

Task 1 – Configure a VPN Template to be used by CSR for VPN 512

- In vManage, Navigate to Configuration -> **Templates -> Feature -> CSR1000v -> VPN -> VPN**

- Configure the VPN parameters based on the following:

  - Template Name : **BR-CSR-VPN-VPN512**
  - Description : **BR-CSR-VPN-VPN512**

  Basic Configuration

  - VPN -> Global : **512**
  - Name -> Global : **MGMT VPN**

- Click **Save** to save the Template.

Task 2 – Configure a VPN Interface Template to be used by CSR for VPN 512 for Interface GigabitEthernet4

- In vManage, Navigate to Configuration -> **Templates -> Feature -> CSR1000v -> VPN -> VPN Interface Ethernet**

- Configure the VPN parameters based on the following:

  - Template Name : **BR-CSR-VPNINT-VPN512-G4**
  - Description : **BR-CSR-VPNINT-VPN512-G4**

  Basic Configuration

  - Shutdown -> Global : **No**

- Interface Name -> Global : **GigabitEthernet4**
- IPv4 Address -> Dynamic

- Click **Save** to save the Template

VPN 1

Task 1 – Configure a VPN Template for CSR for VPN 1

- In vManage, Navigate to Configuration -> **Templates -> Feature -> CSR1000v -> VPN -> VPN**

- Configure the VPN parameters based on the following:

  - Template Name : **BR-CSR-VPN-VPN1**
  - Description : **BR-CSR-VPN-VPN1**

  Basic Configuration
  - VPN -> Global : **1**
  - Name -> Global : **Data VPN**

- Click **Save** to save the Template.

Task 2 – Configure a VPN Interface Template to be used by CSR for VPN 1 for Interface G3

- In vManage, Navigate to Configuration -> **Templates -> Feature -> CSR -> VPN -> VPN Interface Ethernet**

- Configure the VPN parameters based on the following:

  - Template Name : **BR-CSR-VPNINT-VPN1-G3**
  - Description : **BR-CSR-VPNINT-VPN1-G3**

  Basic Configuration
  - Shutdown -> Global : **No**
  - Interface Name -> Global : **GigabitEthernet3**
  - IPv4 Address -> Static -> Device Specific

- Click **Save** to save the Template.

Task 3 – Configure a OSPF Template to be used by CSR for VPN 1

- In vManage, Navigate to Configuration -> **Templates -> Feature -> CSR -> Other Templates -> OSPF**

- Configure the OSPF parameters based on the following:

  - Template Name : **BR-CSR-OSPF-VPN1**
  - Description : **BR-CSR-OSPF-VPN1**

  Redistribution
  - Protocol : **OMP**

  Area Configuration
  - Area Number -> Global : **0**
  - Area Type -> Default

  Interface Configuration
  - Interface Name: **GigabitEthernet3**

- Click **Add** to add the Interface and Click **Add** to add OSPF.

- Click **Save** to save the Template.

Lab 25 - Configuring Device Templates for CSR to deploy VPN 0, 1 and 512

Task 1 – Configure a Device Template for CSR Branch Devices.

- In vManage, Navigate to Configuration -> **Templates -> Device -> Create Template -> CSR1000v**

- Configure the Device Template based on the following:

  - Template Name : **BR-CSR-TEMP**
  - Description : **BR-CSR-TEMP**

  Basic Information
  - System -> **CE-System**

  Transport & Management
  - VPN 0 : **BR-CSR-VPN-VPN0**
  - VPN Interface : **BR-CSR-VPNINT-VPN0-G1**
  - VPN Interface : **BR-CSR-VPNINT-VPN0-G2**
  - OSPF : **BR-CSR-OSPF-VPN0**

  - VPN 512 : **BR-CSR-VPN-VPN512**
  - VPN Interface : **BR-CSR-VPNINT-VPN512-E0**

  Service VPN
  - VPN 1 : **BR-CSR-VPN-VPN1**
  - VPN Interface : **BR-CSR-VPNINT-VPN1-G3**
  - OSPF : **BR-CSR-OSPF-VPN1**

- Click **Save** to save the Template.

Task 2 – Attach vEdge1 to the Device Template

- In vManage, Navigate to Configuration -> **Templates -> Device -> HQ-VE-TEMP.**

- Click on "**...**" towards the right-hand side.

- Click **Attach Devices.**

- Select **cEdge1** and click the " **->** " button.

- Click **Attach**.

Task 3 – Configure the Variable Parameters for the Feature Templates

- **cEdge1** will appear in the window.
- Click on "**...**" towards the right-hand side.
- Click **Edit Device Template.**
- Configure the variables based on the following:
  - Interface IP for GigabitEthernet3 :**192.168.50.5**
  - Default Gateway for VPN0 : **192.1.105.254**
  - Interface IP for GigabitEthernet2 :**192.1.105.5/24**
  - Interface IP for GigabitEthernet1 :**192.168.105.5/24**
  - Hostname : **cEdge-1**
  - System IP : **10.2.2.205**
  - Site ID : **5**
- Click **Update.**
- Verify the Configuration & Click **Configure Devices.**
- Wait for it to update the device. It should come back with Status of **Success**.
- Verify the configuration on **cEdge1**. You can do that by verify OSPF Neighbor relationship with the Internal Router by issuing the **Show ip ospf neighbor** command on **cEdge1.**
- Type **Show Ip route** on **cEdge1** to verify that you are receiving OSPF routes from the MPLS Router.
- Type **Show Ip route** on **Internal Site Routers** to verify that you are receiving OSPF routes from the other Sites.
- Verify reachability between the sites by Pinging the Internal Loopback to Loopback networks.

Lab 26 - Configuring and Deploying Feature and Device Templates for vSmart Controllers

Task 1 – Configure a VPN Template to be used by vSmart Controllers for VPN 0

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vSmart -> VPN -> VPN**

- Configure the VPN parameters based on the following:

  - Template Name : **vSmart-VPN-VPN0**
  - Description : **vSmart-VPN-VPN0**

  Basic Configuration
  - VPN -> Global : **0**
  - Name -> Global : **Transport VPN**

  IPv4 Route
  - Prefix -> Global : **0.0.0.0/0**
  - Next Hop -> Global : **199.1.1.14**

- Click **Save** to save the Template.

Task 2 – Configure a VPN Template to be used by vSmart Controllers for VPN 512

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vSmart -> VPN -> VPN**

- Configure the VPN parameters based on the following:

  - Template Name : **vSmart -VPN-VPN512**
  - Description : **vSmart -VPN-VPN512**

  Basic Configuration
  - VPN -> Global : **512**
  - Name -> Global : **MGMT VPN**

- Click **Save** to save the Template.

Task 3 – Configure a VPN Interface Template to be used by vSmart Controllers for VPN 0 for Interface Eth1

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vSmart -> VPN -> VPN Interface Ethernet**

- Configure the VPN parameters based on the following:

  - Template Name : **vSmart-VPNINT-VPN0-E1**
  - Description : **vSmart-VPNINT-VPN0-E1**

  Basic Configuration
  - Shutdown -> Global : **No**
  - Interface Name -> Global : **eth1**
  - IPv4 Address -> Static -> Device Specific

  Tunnel
  - Tunnel Inteface -> Global : **On**
  - Color -> default

  Allow Service
  - All -> Global : **On**
  - NETCONF -> Global : **On**
  - SSH -> Global : **On**

- Click **Save** to save the Template.

Task 4 – Configure a VPN Interface Template to be used vSmart Controllers for VPN 512 for Interface Eth0

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vSmart -> VPN -> VPN Interface Ethernet**

- Configure the VPN parameters based on the following:

  - Template Name : **vSmart-VPNINT-VPN512-E0**
  - Description : **vSmart-VPNINT-VPN512-E0**

  Basic Configuration
  - Shutdown -> Global : **No**
  - Interface Name -> Global : **eth0**
  - IPv4 Address -> Static -> Device-Specific

- Click **Save** to save the Template

Task 5 – Configure a Device Template for vSmart Controllers.

- In vManage, Navigate to Configuration -> **Templates -> Device -> Create Template -> vSmart**

- Configure the Device Template based on the following:

  - Template Name : **vSmart-TEMP**
  - Description : **vSmart-TEMP**

  Basic Information
  - System -> **VE-System**

  Transport & Management
  - VPN 0 : **vSmart-VPN-VPN0**
  - VPN Interface : **vSmart-VPNINT-VPN0-E1**

  - VPN 512 : **vSmart-VPN-VPN512**
  - VPN Interface : **vSmart-VPNINT-VPN512-E0**

- Click **Save** to save the Template.

Task 6 – Attach vSmart to the Device Template

- In vManage, Navigate to Configuration -> **Templates -> Device -> vSmart-TEMP**

- Click on "**...**" towards the right-hand side.

- Click **Attach Devices.**

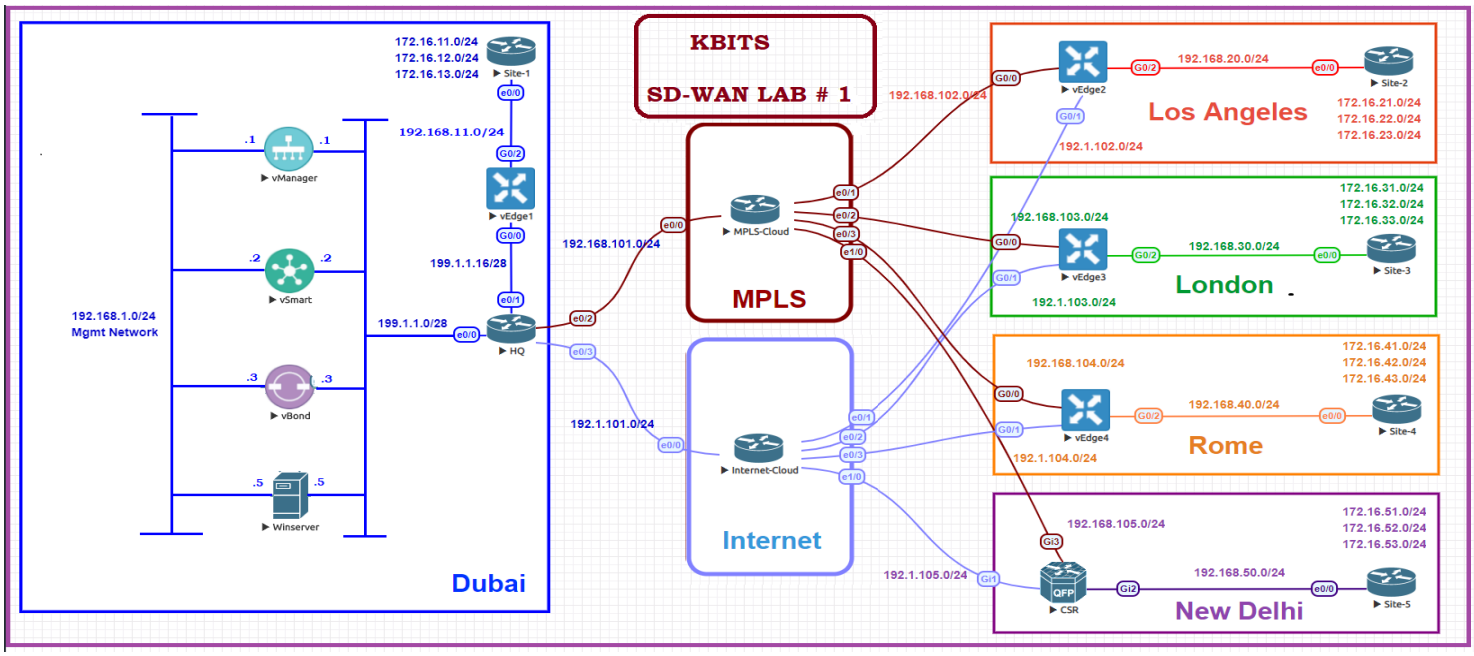
- Select **vSmart** and click the " **->** " button.

- Click **Attach**.

Task 7 – Configure the Variable Parameters for the Feature Templates

- **vSmart** will appear in the window.
- Click on "**...**" towards the right-hand side.
- Click **Edit Device Template.**
- Configure the variables based on the following:
  - Interface IP for Eth1 :**199.1.1.2/28**
  - Interface IP for Eth1 :**192.168.1.2/24**
  - Hostname : **vSmart-1**
  - System IP : **10.1.1.102**
  - Site ID : **1**
- Click **Update.**
- Verify the Configuration & Click **Configure Devices.**
- Wait for it to update the device. It should come back with Status of **Success**.

Lab 27 - Configuring Application Aware Policies using Telnet and Web



Requirements:

- Los Angeles & London Sites should use the MPLS Transport for Telnet Traffic and the Biz-Internet Transport for Web Traffic.
- Telnet Should have a SLA based on the following:
  - Loss – 5%
  - Latency – 200
  - Jitter – 100ms
- Web Should have a SLA based on the following:
  - Loss – 10%
  - Latency – 500
  - Jitter – 100ms
- Create the Sites for Los Angeles and London.
- Create the VPN for VPN ID 1.

Task 1 – Configure Groups of Interests/List that will be used for Telnet & Web Application Aware Routing (AAR) Policy

- In vManage, Navigate to **Configuration -> Policies -> Custom Options -> Centralized Policy -> Lists.**

- Click **SLA Class** and select **New SLA Class list.** Create 2 policies based on the following:

  - Name : **SLA-Telnet**
  - Loss : **5%**
  - Latency : **200**
  - Jitter : **100ms**

  - Name : **SLA-Web**
  - Loss : **10%**
  - Latency : **500**
  - Jitter : **100ms**

- Click **VPN** and select **New VPN list.** Create 1 policy based on the following:

  - Name : **VPN1**
  - ID : **1**

- Click **Site** and select **New Site list.** Create 2 policies based on the following:

  - Name : **Los Angeles**
  - Site ID : **2**

  - Name : **London**
  - Site ID : **3**

Task 2 – Configure an AAR policy based on the Requirements

- In vManage, Navigate to **Configuration -> Policies -> Custom Options -> Centralized Policy -> Traffic Policy.**

- Configure 2 App Routes based on the following:

  - Policy Name : **TELNET-WEB-Policy**
  - Description : **TELNET-WEB-Policy**

  Telnet Sequence
  Match Conditions:
  - Protocol : **6**
  - Port : **23**

  Action
  - SLA Class List: **SLA-Telnet**
  - Color : **mpls**
  - Backup Preferred Color: **biz-internet**

  - Click **Save Match and Actions** to save the Sequence.

  Web Sequence
  Match Conditions:
  - Protocol : **6**
  - Port : **80**

  Action
  - SLA Class List: **SLA-Web**
  - Color : **biz-internet**
  - Backup Preferred Color: **mpls**

  - Click **Save Match and Actions** to save the Sequence.

  - **Save the Policy.**

Task 3 – Create a Centralized Policy and call the Traffic Policy

- In vManage, Navigate to **Configuration -> Policies -> Custom Options -> Centralized Policy -> Add Centralized Policy**

- Click **Next** on the **"Group of Interests"** page as we have already created the required lists.

- Click **Next** on the **"Topology and VPN Membership"** page as we are not using any Control Policies.

- Click **Add Policy** on the **"Configure Traffic Rules"** page.
- Click "**Import Existing"** and select the **TELNET-WEB-POLICY** from the drop-down list and click **Import**.

- Click **Next** to move to the "**Apply Policy to Sites and VPNs**" Page.

- Click the "**Appliacation-Aware Policy"** tab.

- The **TELNET-WEB-Policy** will be there. Click "**New Site List and VPN List"** button.

- Select **Los Angeles** and **London** in the Site List.

- Select **VPN1** in the Site List.

- Click **Add.**

- Assign the Policy a name and Desription based on the following:

  - Policy Name : **Main-Central-Policy**
  - Description : **Main-Central-Policy**

- Click the **Save Policy** button towards the button.

- Activate the policy.

- Wait for it to push the policy to the reachable vSmart Controller(s).

- Verify the policy by using the **Monitor -> Network -> vEdge2 -> Troubleshooting -> Simulate Flows** Tool.

- Telnet from Los Angeles or London should only use the **mpls** transport.

- Web from Los Angeles or London should only use the **biz-internet** transport.

- Normal Ping from Los Angeles or London should use both the Transports.

Lab 28 - Configuring Application Aware Policies using Chat Applications

Requirements:

- Rome should use the Internet Transport for AOL-Messenger, MSN Messenger & Whatsapp Messenger application. It should not use the MPLS Transport at all.
- The Chat applications should have a SLA based on the following:
  - Loss – 10%
  - Latency – 600
  - Jitter – 100ms
- Create a Site for Rome

Task 1 – Configure Groups of Interests/List that will be used for Chat-based Application Aware Routing (AAR) Policy

- In vManage, Navigate to **Configuration -> Policies -> Custom Options -> Centralized Policy -> Lists.**

- Click **Applications** and select **New Application list.** Create a policy based on the following:

  - Name : **Chat-Apps**
  - Appls: Aol-Messenger, MSN-Messenger & WhatsApp Messenger

- Click **SLA Class** and select **New SLA Class list.** Create a policy based on the following:

  - Name : **SLA-CHATS**
  - Loss : **25%**
  - Latency : **600**
  - Jitter : **100ms**

- Click **Site** and select **New Site list.** Create a policy based on the following:

  - Name : **Rome**
  - Site ID : **4**

Task 2 – Configure an AAR policy based on the Requirements

- In vManage, Navigate to **Configuration -> Policies -> Custom Options -> Centralized Policy -> Traffic Policy.**

- Configure 1 App Routes based on the following:

  - Policy Name : **CHAT-Policy**
  - Description : **CHAT-Policy**

  Telnet Sequence
  Match Conditions:
  - Application List: **Chat-Apps**

  Action
  - SLA Class List: **SLA-CHATS**
  - Color : **mpls**
  - Backup Preferred Color: **biz-internet**

  - Click **Save Match and Actions** to save the Sequence.

  Web Sequence
  Match Conditions:
  - Protocol : **6**
  - Port : **80**

  Action
  - SLA Class List: **SLA-Web**
  - Color : **biz-internet**
  - Strict: **Checked**

  - Click **Save Match and Actions** to save the Sequence.

  - **Save the Policy.**

Task 3 – Modify the existing Centralized Policy "Main-Central-Policy" and call the Traffic Policy

- In vManage, Navigate to **Configuration -> Policies -> Custom Options -> Centralized Policy -> Main-Central-Policy -> Click "..." -> Edit.**

- Click **Traffic Rules** on the **Top** of the page.

- Click **Add Policy**.

- Click "**Import Existing"** and select the **CHAT-POLICY** from the drop-down list and click **Import**.
- Click **Policy Application** on the **Top** of the page.
- Click the "**Appliacation-Aware Policy"** tab.
- The **CHAT-Policy** will be there. Click "**New Site List and VPN List"** button.
- Select **Rome** in the Site List.
- Select **VPN1** in the Site List.
- Click **Add.**
- Click the **Save Policy** button towards the button.
- **Activate** the policy.
- Wait for it to push the policy to the reachable vSmart Controller(s).
- Verify the policy by using the **Monitor -> Network -> vEdge3 -> Troubleshooting -> Simulate Flows** Tool.
- Normal Ping from Rome should use both the Transports.
- Use **Aol-messenger** as the appliacation and simulate from Rome. It should only use the **biz-internet** transport.
- Use **Aol-messenger** as the appliacation and simulate from Los Angeles or London. It should use both the Transports.

Lab 29 - Manipulating Traffic flow using TLOCs

Requirements:

- Rome should only the MPLS TLOC as the preferred color while communicating to Los Angeles. The Internet TLOC should be backup TLOC.

Task 1 – Configure Groups of Interests/List that will be used for Traffic Engineering Policy for Rome

- In vManage, Navigate to **Configuration -> Policies -> Custom Options -> Centralized Policy -> Lists.**

- Click **TLOCs** and select **New TLOC list.** Create a policy based on the following:

  - Name : **LA-TLOC-MPLS-INT**
  - TLOC#1:
    - IP Address: 10.2.2.202
    - Color: MPLS
    - Encapsulation: IPSec
    - Preference: 300
  - TLOC#2:
    - IP Address: 10.2.2.202
    - Color: Biz-internet
    - Encapsulation: IPSec
    - Preference: 200

Task 2 – Configure Control/Topology policy based on the Requirements

- In vManage, Navigate to **Configuration -> Policies -> Custom Options -> Centralized Policy -> Topology.**

- Configure 1 Route Policy based on the following:

  - Policy Name : **LA-MPLS-INT**
  - Description : **LA-MPLS-INT**

  Route Sequence

Match Conditions:

- Site List: **LosAngeles**
- VPN List: **VPN1**

Action

- TLOC/TLOC List: **LA-MPLS-INT**
- Click **Save Match and Actions** to save the Sequence.

Default Sequence

Action

- Accept
- Click **Save Match and Actions** to save the Sequence.
- Save the Policy

Task 3 – Modify the existing Centralized Policy "Main-Central-Policy" and call the Topology Policy

- In vManage, Navigate to **Configuration -> Policies -> Custom Options -> Centralized Policy -> Main-Central-Policy -> Click "..." -> Edit.**
- Click **Topology** on the **Top** of the page.
- Click **Add Topology**.
- Click "**Import Existing"** and select the **LA-MPLS-INT** from the drop-down list and click **Import**.
- Click **Policy Application** on the **Top** of the page.
- Click the "**Topology"** tab.
- The **LA-MPLS-INT-Policy** will be there. Click "**New Site"** button.
- Select **Rome** in the Outbound Site List.
- Click **Add.**
- Click the **Save Policy** button towards the button.
- **Activate** the policy.
- Wait for it to push the policy to the reachable vSmart Controller(s).

- Verify by using the **Show IP route vpn 1** command on the Rome vEdge (vEdge4).

- It should only have 1 TLOC for Los Angeles routes (10.2.2.202 – MPLS), whereas it will have 2 TLOCs for London (10.2.2.203-MPLS, 10.2.2.203-Biz-Internet).

Lab 30 - Configuring Route Filtering

Requirements:

- The 172.16.234.2/32, 172.16.234.3/24 & 172.16.234.4/24 should not be propagated to the Dubai Site.

Task 1 – Configure Groups of Interests/List that will be used for Route Filtering Policy for Dubai

- In vManage, Navigate to **Configuration -> Policies -> Custom Options -> Centralized Policy -> Lists.**

- Click **Prefix** and select **New Prefix list.** Create a policy based on the following:

  - Name : **PL-234**
  - Prefix List Entry: **172.16.234.0/24 le 32**

- Click **Site** and select **New Site list.** Create a policy based on the following:

  - Name : **Dubai**
  - Site ID : **1**

Task 2 – Configure Control/Topology policy based on the Requirements

- In vManage, Navigate to **Configuration -> Policies -> Custom Options -> Centralized Policy -> Topology.**

- Configure 1 Route Policy based on the following:

  - Policy Name : **PREF-234-NOT-2-DXB**
  - Description : **PREF-234-NOT-2-DXB**

  Route Sequence
  Match Conditions:
  - Prefix List: **PL-234**

  Action: Reject

  - Click **Save Match and Actions** to save the Sequence.

  Default Sequence

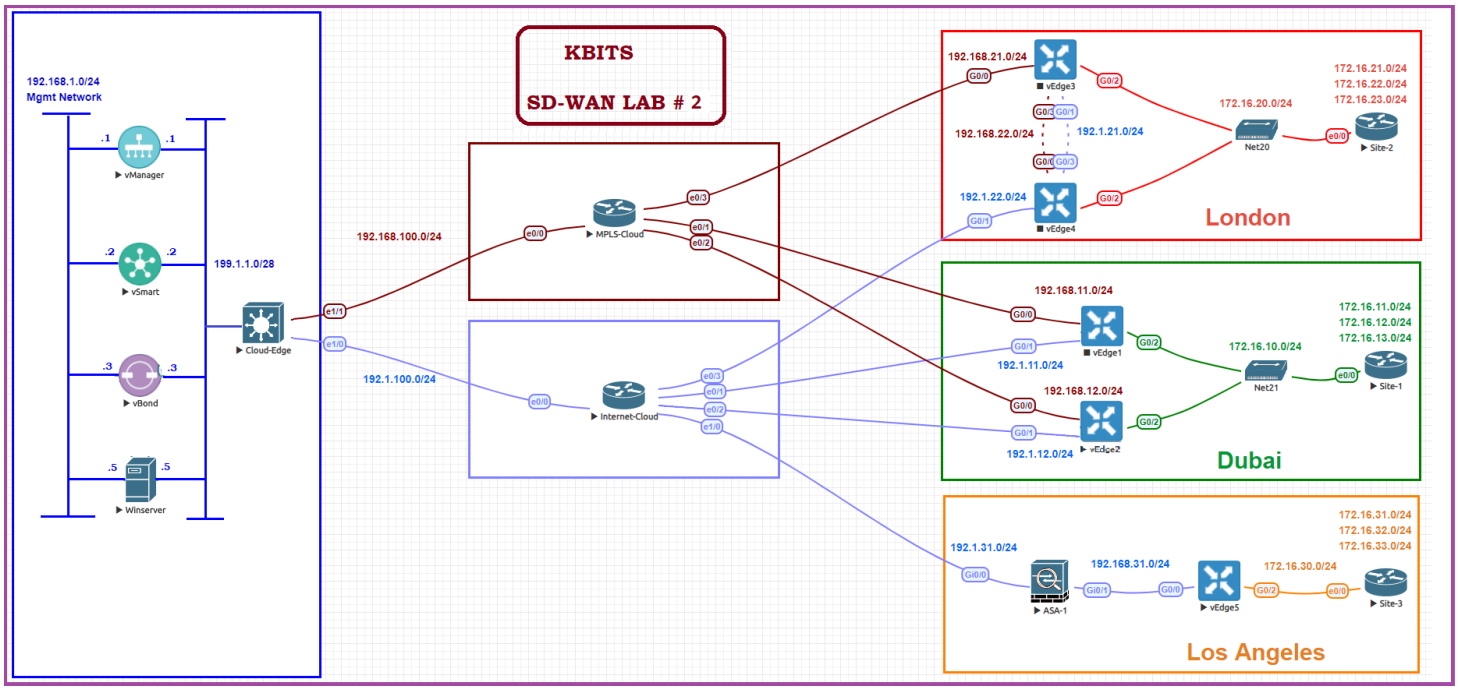
Action

- Accept
- Click **Save Match and Actions** to save the Sequence.
- Save the Policy

Task 3 – Modify the existing Centralized Policy "Main-Central-Policy" and call the Topology Policy

- In vManage, Navigate to **Configuration -> Policies -> Custom Options -> Centralized Policy -> Main-Central-Policy -> Click "..." -> Edit.**
- Click **Topology** on the **Top** of the page.
- Click **Add Topology**.
- Click "**Import Existing"** and select the **PREF-234-NOT-2-DXB** from the drop-down list and click **Import**.
- Click **Policy Application** on the **Top** of the page.
- Click the "**Topology"** tab.
- The **PREF-234-NOT-2-DXB** will be there. Click "**New Site"** button.
- Select **Dubai** in the Outbound Site List.
- Click **Add.**
- Click the **Save Policy** button towards the button.
- **Activate** the policy.
- Wait for it to push the policy to the reachable vSmart Controller(s).
- Verify by using the **Show IP route vpn 1** command on the Dubai vEdge (vEdge1).
- It should all the routes from the Branches except the 172.16.234.X/32 routes.
- These routes should be present in the vEdge2, vEdge3 and vEdge4 routers. You can use the **Show IP route vpn 1** command to verify.

Lab 31 – Configuring the WAN Components



Interface Configuration

Cloud Edge

Interface	IP Address	Subnet Mask
E 0/0	199.1.1.14	255.255.255.240
E 0/1	192.168.100.1	255.255.255.0
E 0/2	192.1.100.1	255.255.255.0

MPLS Cloud

Interface	IP Address	Subnet Mask
E 0/0	192.168.100.254	255.255.255.0
E 0/1	192.168.11.254	255.255.255.0
E 0/2	192.168.12.254	255.255.255.0
E 0/3	192.168.21.254	255.255.255.0

Internet Cloud

Interface	IP Address	Subnet Mask
E 0/0	192.1.100.254	255.255.255.0
E 0/1	192.1.11.254	255.255.255.0
E 0/2	192.1.12.254	255.255.255.0
E 0/3	192.1.22.254	255.255.255.0
E 1/0	192.1.31.254	255.255.255.0

WAN Setup

Task 1 – Cloud Edge Router Configuration

- Configure the Interfaces based on the Logical Diagram
- Configure OSPF as the IGP to communicate with the MPLS Cloud. Enable all the interfaces.
- Make sure OSPF only sends and receives OSPF packets on the link towards the MPLS Cloud using the Passive-interface command.
- Configure a default route on the router towards the Internet. The IP Address of the Internet Router is 192.1.100.254

Cloud Edge Router

```
no ip domain-loo
line con 0
 logg sync
 no exec-timeout
!
Hostname Cloud Edge
!
Interface E 0/0
 ip address 199.1.1.14 255.255.255.240
 no shut
!
Interface E 0/1
 ip address 192.168.100.1 255.255.255.240
 no shut
!
Interface E 0/2
 ip address 192.1.100.1 255.255.255.0
 no shut
!
router ospf 1
 network 192.168.100.0 0.0.0.255 area 0
 network 199.1.1.0 0.0.0.255 area 0
 passive-interface default
 no passive-interface E0/1
!
ip route 0.0.0.0 0.0.0.0 192.1.100.254
```

Task 2 – MPLS Cloud Router Configuration

- Configure the Interfaces based on the Logical Diagram.
- Configure OSPF as the IGP on all the interfaces.

MPLS Cloud Router

```
no ip domain-lookup
!
line con 0
 exec-timeout 0 0
 logging synchronous
!
hostname MPLS
!
interface Ethernet0/0
 ip address 192.168.100.254 255.255.255.0
 no shut
!
interface Ethernet0/1
 ip address 192.168.11.254 255.255.255.0
 no shut
!
interface Ethernet0/2
 ip address 192.168.12.254 255.255.255.0
 no shut
!
interface Ethernet0/3
 ip address 192.168.21.254 255.255.255.0
 no shut
!
router ospf 1
 network 192.168.100.0 0.0.0.255 area 0
 network 192.168.11.0 0.0.0.255 area 0
 network 192.168.12.0 0.0.0.255 area 0
 network 192.168.21.0 0.0.0.255 area 0
```

Task 3 – Internet Cloud Router Configuration

- Configure the Interfaces based on the Logical Diagram
- Configure a Static Route on the Router for the 199.1.1.0/24 network. The Next Hop should point towards the Internet IP of the HQ Router.

Internet Cloud Router

```
no ip domain lookup
!
line con 0
 exec-timeout 0 0
 logging synchronous
!
hostname Internet
!
interface Ethernet0/0
 ip address 192.1.100.254 255.255.255.0
 no shut
!
interface Ethernet0/1
 ip address 192.1.11.254 255.255.255.0
 no shut
!
interface Ethernet0/2
 ip address 192.1.12.254 255.255.255.0
 no shut
!
interface Ethernet0/3
 ip address 192.1.22.254 255.255.255.0
 no shut
!
interface Ethernet1/0
 ip address 192.1.31.254 255.255.255.0
 no shut
!
ip route 199.1.1.0 255.255.255.0 192.1.100.1
```

Server Setup

Task 1 – Configure the Interfaces

First Ethernet Interface:

IP Address: 192.168.1.5
Subnet Mask: 255.255.255.0

Third Ethernet Interface:

IP Address: 199.1.1.5
Subnet Mask: 255.255.255.240
Default Gateway: 199.1.1.14

Task 2 – Configure the Timezone and Time

Configure the appropiate Timezone and Time on the Windows Server.

Task 3 – Installing the Enterprise Root Certificate Server

- Open **Server Manager**
- Click **Roles**
- Click **Add Roles**
- Click **Next**
- Select the "**Active Directory Certificate Services**" and click **Next**
- Click Next
- Select "**Certification Authority Web Enrollment**" and click Next
- Leave it as Standalone and click **Next**
- Leave it as Root CA and click **Next**
- Leave "Create a new private key" and click **Next**
- Leave the default for the Cryptography for CA and click **Next**
- Set the Common name as **KBITS-CA** and click **Next**
- Leave the default for the Validity Period and click **Next**
- Click **Next**
- Click **Install**

Task 4 – Install WinSCP

- **Double-click** the WinSCP Installation file.
- Do a Default Installation.

Controller Setup – vManage

Task 1 – Configuring the System Component

- Configure the System parameters based on the following:

  - Host-name : vManage1
  - Organization: KBITS
  - System-IP: 10.1.1.101
  - Site ID: 1
  - vbond Address: 199.1.1.3
  - Timezone: Based on the appropriate Timezone

Note: Default username: admin **Default password**: admin

vManage

```
config
!
system
 host-name vManage1
 system-ip 10.1.1.101
 site-id 1
 organization-name KBITS
 clock timezone Asia/Muscat
 vbond 199.1.1.3
!
 Commit
```

Task 2 – Configured the vpn parameters

- Configure the VPN parameters based on the following:

  - vpn 0
    - Interface eth1
    - IP Address: 199.1.1.1/28
    - Tunnel Interface
    - Tunnel Services (All, NetConf, SSHD)
    - Default Route: 199.1.1.14

- vpn 512
  - Interface eth0
  - IP Address: 192.168.1.1/24

vManage

```
config
!
vpn 0
 no interface eth0
 interface eth1
  ip address 199.1.1.1/28
  tunnel-interface
   allow-service all
   allow-service netconf
   allow-service sshd
   no shut
 ip route 0.0.0.0/0 199.1.1.14
!
vpn 512
 interface eth0
  ip address 192.168.1.1/24
  no shut
!
 commit
```

Task 3 – Organization name & vBond Address

- Log into the vManage from the Server by browsing to https://192.168.1.1:8443 using a username of **admin** and a password of **admin.**
- Navigate to **Administration** -> **Settings**
- Click **Edit** on the Organization name and set it to **KBITS**. Confirm the Organization name. Click **OK.**
- Click **Edit** on the **vBond** address and change it to 199.1.1.3. Confirm and click **OK**.

Task 4 – Configure Controller Authorization as Enterprise Root and Download the Root Certificate.

- Browse to http://192.168.1.5/certsrv
- Click **"Download Root Certificate".**
- Select **"Base 64"**.
- Click "**Download CA Certificate".**
- Open Explorer and navigate to the downloads folder.
- Change the name of the Downloaded file "**Certnew**" to "**RootCert**".
- Open the "**RootCert.cer**" file using Notepad.
- Copy using **CTRL-A** and **CTRL-C**.
- In vManage, Navigate to **Administration -> Settings -> Controller Certiticate Authorization.**
- Change the "**Certificate Signing by:**" to "**Enterprise Root Certificate**".
- Paste the RootCert.cer that you had copied by using **CTRL-V.**
- Set the CSR Parameters with the Organization name, City, State, Country. Set the Time to 3 Years and save.

Task 5 – Generate a CSR for vManage

- Navigate to **Configuration -> Certificates -> Controllers -> vManage -> Generate CSR.**
- It will open a window with the CSR. Copy by using **CTRL-A** and **CTRL-C.**

Task 6 – Request a Certificate from the CA Server

- Browse to http://192.168.1.5/certsrv
- Click **"Request a Certificate".**

- Select **“Advanced”**.
- Paste the CSR in the box by using **CTRL-V** and click **Submit.**

Task 7 – Issue the Certificate from the CA Server

- Open Server Manager and navigate to **Active Directory Certificate Server -> KBITS-CA -> Pending Requests.**
- Right-Click the request and click “**Issue”.**

Task 8 – Downloading the Issued Certificate

- Browse to http://192.168.1.5/certsrv
- Click **“Check on Pending request”.**
- The issued certificate link will show up. Click on the link.
- Select “**Base 64”** and click “**Download”**
- Open Explorer and navigate to the downloads folder.
- Change the name of the Downloaded file “**Certnew**” to “**vManage**”.
- Open the “**vManage.cer**” file using Notepad.
- Copy using **CTRL-A** and **CTRL-C**.

Task 9 – Installing the Identity Certificate for vManage

- In vManage, Navigate to **Configuration -> Certificates -> Controllers**
- Click on the **“Install”** button at the top right corner
- Paste the Certificate (CTRL-V).
- The Identity certificate should be installed on vManage.

Controller Setup – vBond

Task 1 – Configuring the System Component

- Configure the System parameters based on the following:

  - Host-name : vBond1
  - Organization: KBITS
  - System-IP: 10.1.1.103
  - Site ID: 1
  - vbond Address: 199.1.1.3
  - Timezone: Based on the appropriate Timezone

Note: **Default username**: admin **Default password**: admin

vBond

```
config
!
system
 host-name vBond1
 system-ip 10.1.1.103
 site-id 1
 organization-name KBITS
 clock timezone Asia/Muscat
 vbond 199.1.1.3 local
!
 Commit
```

Task 2 – Configured the vpn parameters

- Configure the VPN parameters based on the following:

  - vpn 0
    - Interface Ge0/0
    - IP Address: 199.1.1.3/28
    - Tunnel Interface
    - Tunnel Services (All, NetConf, SSHD)
    - Encapsulation: IPSec
    - Default Route: 199.1.1.14

  - vpn 512
    - Interface eth0
    - IP Address: 192.168.1.3/24

vBond

```
config
!
vpn 0
 no interface eth0
 interface Ge0/0
  ip address 199.1.1.3/28
  tunnel-interface
   encapsulation ipsec
   allow-service all
   allow-service netconf
   allow-service sshd
   no shut
 ip route 0.0.0.0/0 199.1.1.14
!
vpn 512
 interface eth0
  ip address 192.168.1.3/24
  no shut
!
 Commit
```

Task 3 – Add vBond to vManage

- Navigate to **Configuration -> Devices -> Controllers -> Add Controllers -> vBond** and specify the following to add the vBond in vManage.

  - IP Address: **199.1.1.3**
  - Username: **Admin**
  - Password: **Admin**
  - Check Generate CSR
  - Click **OK**

Task 4 – View the generated CSR for vBond and Copy it

- Navigate to **Configuration -> Certificates -> Controllers -> vBond -> View CSR.**

- It will open a window with the CSR. Copy by using **CTRL-A** and **CTRL-C.**

Task 5 – Request a Certificate from the CA Server

- Browse to http://192.168.1.5/certsrv
- Click **"Request a Certificate".**
- Select **"Advanced"**.
- Paste the CSR in the box by using **CTRL-V** and click **Submit.**

Task 6 – Issue the Certificate from the CA Server

- Open Server Manager and navigate to **Active Directory Certificate Server -> KBITS-CA -> Pending Requests.**
- Right-Click the request and click "**Issue".**

Task 7 – Downloading the Issued Certificate

- Browse to http://192.168.1.5/certsrv
- Click **"Check on Pending request".**
- The issued certificate link will show up. Click on the link.
- Select "**Base 64"** and click "**Download"**
- Open Explorer and navigate to the downloads folder.
- Change the name of the Downloaded file "**Certnew**" to "**vBond**".
- Open the "**vBond.cer**" file using Notepad.
- Copy using **CTRL-A** and **CTRL-C**.

Task 8 – Installing the Identity Certificate for vManage

- In vManage, Navigate to **Configuration -> Certificates -> Controllers**
- Click on the **"Install"** button at the top right corner
- Paste the Certificate (CTRL-V).

- The Identity certificate should be installed for vBond and pushed to it.

Controller Setup – vSmart

Task 1 – Configuring the System Component

- Configure the System parameters based on the following:

  - Host-name : vSmart1
  - Organization: KBITS
  - System-IP: 10.1.1.102
  - Site ID: 1
  - vbond Address: 199.1.1.3
  - Timezone: Based on the appropriate Timezone

Note: Default username: admin **Default password**: admin

vSmart

```
config
!
system
 host-name vSmart1
 system-ip 10.1.1.102
 site-id 1
 organization-name KBITS
 clock timezone Asia/Muscat
 vbond 199.1.1.3
!
 Commit
```

Task 2 – Configured the vpn parameters

- Configure the VPN parameters based on the following:

  - vpn 0
    - Interface Eth1
    - IP Address: 199.1.1.2/28
    - Tunnel Interface
    - Tunnel Services (All, NetConf, SSHD)
    - Default Route: 199.1.1.14

  - vpn 512
    - Interface eth0

- IP Address: 192.168.1.2/24

vSmart

```
config
!
vpn 0
 no interface eth0
 interface eth1
  ip address 199.1.1.2/28
  tunnel-interface
   allow-service all
   allow-service netconf
   allow-service sshd
   no shut
 ip route 0.0.0.0/0 199.1.1.14
!
vpn 512
 interface eth0
  ip address 192.168.1.2/24
  no shut
!
 Commit
```

Task 3 – Add vSmart to vManage

- Navigate to **Configuration -> Devices -> Controllers -> Add Controllers -> vSmart** and specify the following to add the vBond in vManage.

  - IP Address: **199.1.1.2**
  - Username: **Admin**
  - Password: **Admin**
  - Check Generate CSR
  - Click **OK**

Task 4 – View the generated CSR for vBond and Copy it

- Navigate to **Configuration -> Certificates -> Controllers -> vSmart -> View CSR.**

- It will open a window with the CSR. Copy by using **CTRL-A** and **CTRL-C.**

Task 5 – Request a Certificate from the CA Server

- Browse to http://192.168.1.5/certsrv
- Click **"Request a Certificate".**
- Select **"Advanced"**.
- Paste the CSR in the box by using **CTRL-V** and click **Submit.**

Task 6 – Issue the Certificate from the CA Server

- Open Server Manager and navigate to **Active Directory Certificate Server -> KBITS-CA -> Pending Requests.**
- Right-Click the request and click "**Issue".**

Task 7 – Downloading the Issued Certificate

- Browse to http://192.168.1.5/certsrv
- Click **"Check on Pending request".**
- The issued certificate link will show up. Click on the link.
- Select "**Base 64"** and click "**Download"**
- Open Explorer and navigate to the downloads folder.
- Change the name of the Downloaded file "**Certnew**" to "**vSmart**".
- Open the "**vSmart.cer**" file using Notepad.
- Copy using **CTRL-A** and **CTRL-C**.

Task 8 – Installing the Identity Certificate for vManage

- In vManage, Navigate to **Configuration -> Certificates -> Controllers**
- Click on the **"Install"** button at the top right corner
- Paste the Certificate (CTRL-V).

- The Identity certificate should be installed for vSmart and pushed to it.

WAN Edge Setup – (CLI)

Task 1 – Upload the WAN Edge List

- On the vManage Main windows, Naviagte to **Configuration -> Devices**. Click on "**Upload WAN Edge List**".

- Select the file you downloaded from the PNP Portal. Upload it and check the **Validate** option.

vEDGE-1

Task 1 – Configuring the System Component

- Configure the System parameters based on the following:

  - Host-name : vEdge1
  - Organization: KBITS
  - System-IP: 10.2.2.201
  - Site ID: 1
  - vbond Address: 199.1.1.3
  - Timezone: Based on the appropriate Timezone

Note: **Default username**: admin **Default password**: admin

vEdge1

```
config
!
system
 host-name vEdge1
 system-ip 10.2.2.201
 site-id 1
 organization-name KBITS
 clock timezone Asia/Muscat
 vbond 199.1.1.3
!
 commit
```

Task 2 – Configure the vpn parameters

- Configure the VPN parameters based on the following:

  - vpn 0
    - Interface Ge0/0
    - IP Address: 192.168.11.1/24
    - Tunnel Interface
    - Encapsulation IPSec
    - Tunnel Services (All, NetConf, SSHD)
    - Default Route: 192.168.11.254

  - vpn 512
    - Interface eth0
    - IP Address: DHCP Client

vEdge1

```
config
!
vpn 0
 no interface eth0
 interface Ge0/0
  ip address 192.168.11.1/24
  tunnel-interface
   encapsulation ipsec
   allow-service all
   allow-service netconf
   allow-service sshd
   no shut
 ip route 0.0.0.0/0 192.168.11.254
!
vpn 512
 interface eth0
  ip dhcp-client
  no shutdown
 commit
```

vEDGE-2

Task 1 – Configuring the System Component

- Configure the System parameters based on the following:

  - Host-name : vEdge2
  - Organization: KBITS
  - System-IP: 10.2.2.202
  - Site ID: 1
  - vbond Address: 199.1.1.3
  - Timezone: Based on the appropriate Timezone

Note: Default username: admin **Default password**: admin

vEdge-2

```
config
!
system
 host-name vEdge2
 system-ip 10.2.2.202
 site-id 1
 organization-name KBITS
 clock timezone Asia/Muscat
 vbond 199.1.1.3
!
 commit
```

Task 2 – Configure the vpn parameters

- Configure the VPN parameters based on the following:

  - vpn 0
    - Interface Ge0/0
    - IP Address: 192.168.12.2/24
    - Tunnel Interface
    - Encapsulation IPSec
    - Tunnel Services (All, NetConf, SSHD)
    - Default Route: 192.168.12.254

  - vpn 512
    - Interface eth0
    - IP Address: DHCP Client

vEdge2

```
config
!
vpn 0
 no interface eth0
 interface Ge0/0
  ip address 192.168.12.2/24
  tunnel-interface
   encapsulation ipsec
   allow-service all
   allow-service netconf
   allow-service sshd
   no shut
 ip route 0.0.0.0/0 192.168.102.254
!
vpn 512
 interface eth0
  ip dhcp-client
  no shutdown
 !
 commit
```

vEDGE-3

Task 1 – Configuring the System Component

- Configure the System parameters based on the following:
  - Host-name : vEdge3
  - Organization: KBITS
  - System-IP: 10.2.2.203
  - Site ID: 2
  - vbond Address: 199.1.1.3
  - Timezone: Based on the appropriate Timezone

Note: Default username: admin **Default password**: admin

vEdge-3

```
config
!
system
```

```
 host-name vEdge3
 system-ip 10.2.2.203
 site-id 2
 organization-name KBITS
 clock timezone Asia/Muscat
 vbond 199.1.1.3
!
 Commit
```

Task 2 – Configure the vpn parameters

- Configure the VPN parameters based on the following:
  - vpn 0
    - Interface Ge0/0
    - IP Address: 192.168.21.3/24
    - Tunnel Interface
    - Encapsulation IPSec
    - Tunnel Services (All, NetConf, SSHD)
    - Default Route: 192.168.21.254
  - vpn 512
    - Interface eth0
    - IP Address: DHCP Client

vEdge3

```
config
!
vpn 0
 no interface eth0
 interface Ge0/0
  ip address 192.168.21.3/24
  tunnel-interface
   encapsulation ipsec
   allow-service all
   allow-service netconf
   allow-service sshd
   no shut
 ip route 0.0.0.0/0 192.168.21.254
!
vpn 512
 interface eth0
  ip dhcp-client
  no shutdown
 !
```

Commit

vEDGE-4

Task 1 – Configuring the System Component

- Configure the System parameters based on the following:

  - Host-name : vEdge4
  - Organization: KBITS
  - System-IP: 10.2.2.204
  - Site ID: 2
  - vbond Address: 199.1.1.3
  - Timezone: Based on the appropriate Timezone

Note: Default username: admin **Default password**: admin

vEdge-4

```
config
!
system
 host-name vEdge4
 system-ip 10.2.2.204
 site-id 2
 organization-name KBITS
 clock timezone Asia/Muscat
 vbond 199.1.1.3
!
```
Commit

Task 2 – Configure the vpn parameters

- Configure the VPN parameters based on the following:

  - vpn 0
    - Interface Ge0/1
    - IP Address: 192.1.22.4/24
    - Tunnel Interface
    - Encapsulation IPSec
    - Tunnel Services (All, NetConf, SSHD)
    - Default Route: 192.168.22.254

  - vpn 512

- Interface eth0
- IP Address: DHCP Client

vEdge4

```
config
!
vpn 0
 no interface eth0
 interface Ge0/1
  ip address 192.1.22.4/24
  tunnel-interface
   encapsulation ipsec
   allow-service all
   allow-service netconf
   allow-service sshd
   no shut
 ip route 0.0.0.0/0 192.168.22.254
!
vpn 512
 interface eth0
  ip dhcp-client
  no shutdown
 !
 Commit
```

WAN Edge Setup – vManage (GUI)

vEDGE-1

Task 1 – Upload the Root Certificate to the vEdge

- On the Windows Server, open **WINSCP** application.
- **Connect** to vEdge1 using the following information:
  - IP Address : 192.168.11.1
  - Protocol - SFTP
  - Username : admin
  - Password : admin
- Copy the **RootCert.cer** file from the Downloads folder to the **/home/admin** folder on the vEdge1

Task 2 – Install the Root Certificate on vEdge1

- Connect to the console of vEdge1 and issue the following command:

  request root-cert-chain install /home/admin/RootCert.cer

Task 3 - Activate vEdge on vManage

- Navigate to **Configuration -> Devices**
- Note and use the **Chassis Number** and **Token number** for the 1st vEdge from vManage.
- Use the information from the previous step in the following command on the vEdge1 console.

  request vedge-cloud activate chassis-number **XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX** token **XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX**
- You should see the vEdge in the vManage console with a Certificate issued.

vEDGE-2

Task 1 – Upload the Root Certificate to the vEdge

- On the Windows Server, open **WINSCP** application.
- **Connect** to vEdge1 using the following information:
  - IP Address : 192.168.12.2
  - Protocol - SFTP
  - Username : admin
  - Password : admin
- Copy the **RootCert.cer** file from the Downloads folder to the **/home/admin** folder on the vEdge2

Task 2 – Install the Root Certificate on vEdge2

- Connect to the console of vEdge2 and issue the following command:

  request root-cert-chain install /home/admin/RootCert.cer

Task 3 - Activate vEdge on vManage

- Navigate to **Configuration -> Devices**
- Note and use the **Chassis Number** and **Token number** for the 2nd vEdge from vManage.
- Use the information from the previous step in the following command on the vEdge2 console.

  request vedge-cloud activate chassis-number **XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX** token **XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX**

- You should see the vEdge in the vManage console with a Certificate issued.

vEDGE-3

Task 1 – Upload the Root Certificate to the vEdge

- On the Windows Server, open **WINSCP** application.
- **Connect** to vEdge1 using the following information:
  - IP Address : 192.168.21.3
  - Protocol - SFTP
  - Username : admin
  - Password : admin
- Copy the **RootCert.cer** file from the Downloads folder to the **/home/admin** folder on the vEdge3

Task 2 – Install the Root Certificate on vEdge3

- Connect to the console of vEdge3 and issue the following command:

  request root-cert-chain install /home/admin/RootCert.cer

Task 3 - Activate vEdge on vManage

- Navigate to **Configuration -> Devices**
- Note and use the **Chassis Number** and **Token number** for the 3rd vEdge from vManage.
- Use the information from the previous step in the following command on the vEdge3 console.

  request vedge-cloud activate chassis-number **XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX** token **XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX**

- You should see the vEdge in the vManage console with a Certificate issued.

vEDGE-4

Task 1 – Upload the Root Certificate to the vEdge

- On the Windows Server, open **WINSCP** application.
- **Connect** to vEdge1 using the following information:
  - IP Address : 192.1.22.4
  - Protocol - SFTP
  - Username : admin
  - Password : admin
- Copy the **RootCert.cer** file from the Downloads folder to the **/home/admin** folder on the vEdge4

Task 2 – Install the Root Certificate on vEdge4

- Connect to the console of vEdge4 and issue the following command:

  request root-cert-chain install /home/admin/RootCert.cer

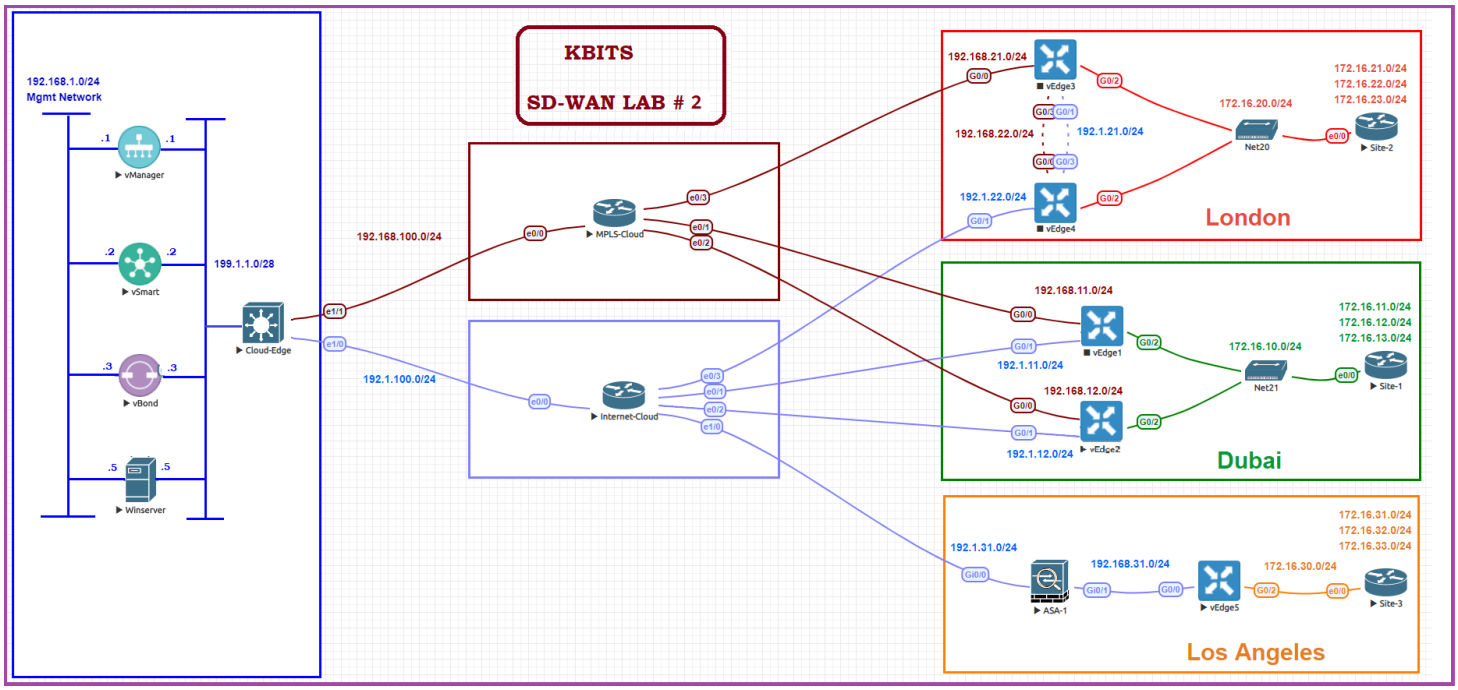
Task 3 - Activate vEdge on vManage

- Navigate to **Configuration -> Devices**
- Note and use the **Chassis Number** and **Token number** for the 4th vEdge from vManage.
- Use the information from the previous step in the following command on the vEdge4 console.

  request vedge-cloud activate chassis-number **XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX** token **XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX**

- You should see the vEdge in the vManage console with a Certificate issued.

Lab 32 – Configuring Firewalls to supports SD-WAN



Interface Configuration

ASAv1

Interface	IP Address	Subnet Mask
Gig 0/0	192.1.31.10	255.255.255.0
Gig 0/0	192.168.31.10	255.255.255.0

Firewall Configuration

Task 1 – Interface Configuration and Default Routing on ASA in Los Angeles

- Configure the Interfaces based on the Logical Diagram.
- Configure Gig 0/0 with a Name of **"Outside"** using the default Security Level.
- Configure Gig 0/1 with a Name of **"Inside"** using the default Security Level.
- Configure a default route on the ASA pointing towards the Internet Cloud thru the Outside Interface.

ASAv Firewall

```
Hostname ASAv1
!
Interface Gig 0/0
 Nameif Outside
 ip address 192.1.31.10 255.255.255.0
 no shut
!
Interface Gig 0/1
 Nameif Inside
 ip address 192.168.31.10 255.255.255.240
 no shut
!
Route Outside 0.0.0.0 0.0.0.0 192.1.31.254
```

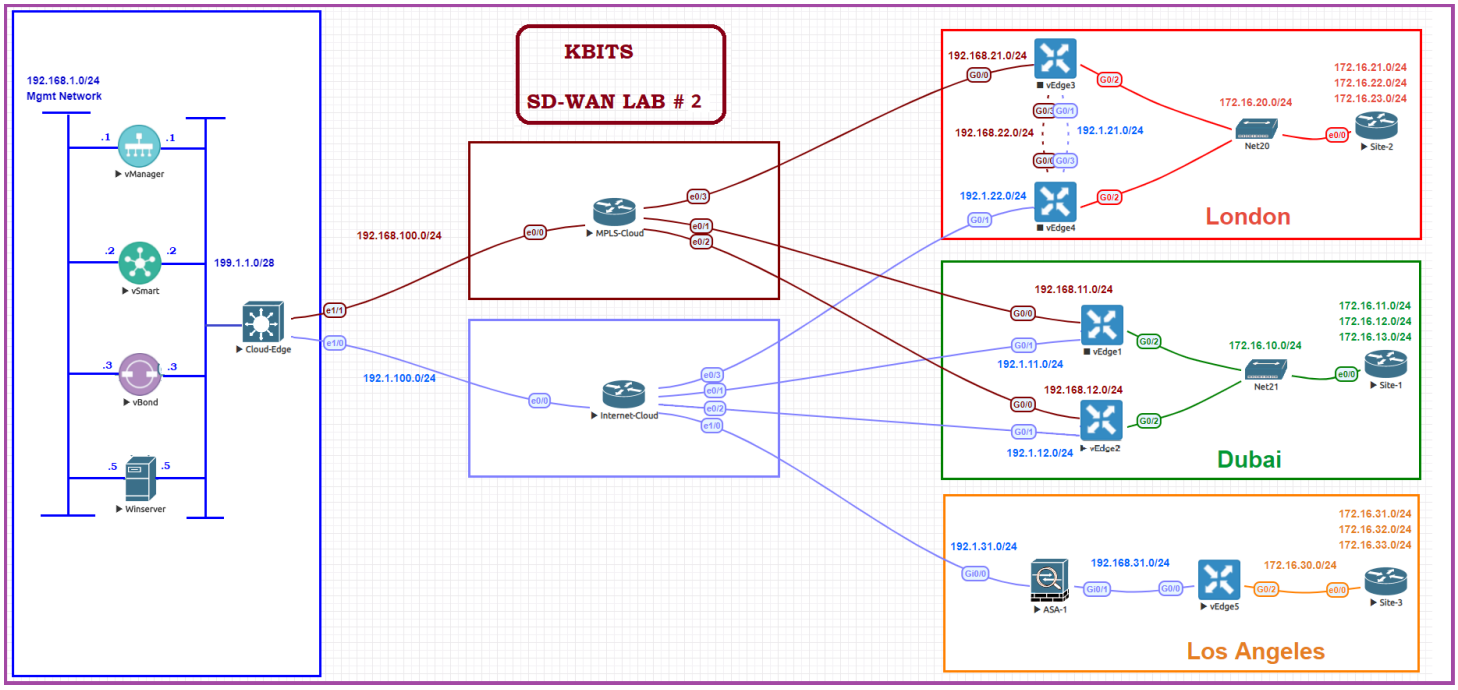
Task 2 – Translate vEdge5 on the Outside.

- Statically Translate vEdge5 as 192.1.31.5 on the Outside.
- The Private address that will be assigned to vEdge5 is 192.168.31.5.

ASAv Firewall

```
Object network vEdge5
 Host 192.168.31.5
 Nat (Inside,Outside) static 192.1.31.5
```

Lab 33 – Configuring vEdges with NAT thru Firewalls



vEDGE-5 Initialization – (CLI)

Task 1 – Configuring the System Component on vEdge5

- Configure the System parameters based on the following:
  - Host-name : vEdge5
  - Organization: KBITS
  - System-IP: 10.2.2.205
  - Site ID: 3
  - vbond Address: 199.1.1.3
  - Timezone: Based on the appropriate Timezone

Note: **Default username**: admin **Default password**: admin

vEdge-5

```
config
!
system
 host-name vEdge5
```

```
 system-ip 10.2.2.205
 site-id 3
 organization-name KBITS
 clock timezone Asia/Muscat
 vbond 199.1.1.3
!
 Commit
```

Task 2 – Configure the vpn parameters on vEdge5

- Configure the VPN parameters based on the following:
  - vpn 0
    - Interface Ge0/0
    - IP Address: 192.168.31.5/24
    - Tunnel Interface
    - Encapsulation IPSec
    - Tunnel Services (All, NetConf, SSHD)
    - Default Route: 192.168.31.10
  - vpn 512
    - Interface eth0
    - IP Address: DHCP Client

vEdge3

```
config
!
vpn 0
 no interface eth0
 interface Ge0/0
  ip address 192.168.31.5/24
  tunnel-interface
   encapsulation ipsec
   allow-service all
   allow-service netconf
   allow-service sshd
   no shut
 ip route 0.0.0.0/0 192.168.31.10
!
vpn 512
 interface eth0
  ip dhcp-client
  no shutdown
 !
 Commit
```

vEDGE-5 Initialization – vManage(GUI)

Task 1 – Configure an ACL on ASAv to allow the Certificate server to SFTP to vEdge5 to upload the Root Certificate

ASAv

```
Access-list OUTSIDE permit tcp host 199.1.1.5 host 192.168.31.5 eq 22
!
Access-group OUTSIDE in interface Outside
```

Task 2 – Upload the Root Certificate to the vEdge

- On the Windows Server, open **WINSCP** application.
- **Connect** to vEdge5 using the following information:
  - IP Address : 192.1.31.5
  - Protocol - SFTP
  - Username : admin
  - Password : admin
- Copy the **RootCert.cer** file from the Downloads folder to the **/home/admin** folder on the vEdge3

Task 3 – Install the Root Certificate on vEdge3

- Connect to the console of vEdge5 and issue the following command:

request root-cert-chain install /home/admin/RootCert.cer

Task 4 - Activate vEdge on vManage

- Navigate to **Configuration -> Devices**
- Note and use the **Chassis Number** and **Token number** for the 5th vEdge from vManage.
- Use the information from the previous step in the following command on the vEdge5 console.

request vedge-cloud activate chassis-number **XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX** token **XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX**

- You should see the vEdge in the vManage console with a Certificate issued.

vEdge5 Templates Creation

System

Task 1 – Configure the System Template to be used by all vEdge-Cloud Devices

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vEdge Cloud -> Basic Information -> System**

- Configure the System parameters based on the following:

  - Template Name : **VE-System**
  - Description : **VE-System**
  - Site ID -> Device Specific
  - System IP ->Device Specific
  - Hostname -> Device Specific
  - Timezone -> Device Specific
  - Console Baud Rate -> **Default**

- Click **Save** to save the Template.

VPN 0

Task 1 – Configure a VPN Template to be used by all BR3 vEdges (vEdge5) for VPN0

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vEdge Cloud -> VPN -> VPN**

- Configure the VPN parameters based on the following:

  - Template Name : **BR3-VE-VPN-VPN0**
  - Description : **BR3-VE-VPN-VPN0**

  Basic Configuration
  - VPN -> Global : **0**

- Name -> Global : **Transport VPN**

IPv4 Route
- Prefix -> Global : 0.0.0.0/0
- Next Hop -> Device Specific

- Click **Save** to save the Template.

Task 2 – Configure a VPN Interface Template to be used by all BR3 vEdge-Cloud Devices for VPN 0 for Interface G0/0

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vEdge Cloud -> VPN -> VPN Interface Ethernet**

- Configure the VPN parameters based on the following:

  - Template Name : **BR3-VE-VPNINT-VPN0-G0**
  - Description : **BR3-VE-VPNINT-VPN0-G0**

  Basic Configuration
  - Shutdown -> Global : **No**
  - Interface Name -> Global : **Ge0/0**
  - IPv4 Address -> Static -> Device Specific

  Tunnel
  - Tunnel Inteface -> Global : **On**
  - Color -> Global : **Biz-internet**

  Allow Service
  - All -> Global : **On**
  - NETCONF -> Global : **On**
  - SSH -> Global : **On**

- Click **Save** to save the Template.

VPN512

Task 1 – Configure a VPN Template to be used by all Branch vEdge-Cloud Devices for VPN 512

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vEdge Cloud -> VPN -> VPN**

- Configure the VPN parameters based on the following:

  - Template Name : **BR-VE-VPN-VPN512**

- Description : **BR-VE-VPN-VPN512**

Basic Configuration

- VPN -> Global : **512**
- Name -> Global : **MGMT VPN**

- Click **Save** to save the Template.

Task 2 – Configure a VPN Interface Template to be used by all Branch vEdge-Cloud Devices for VPN 512 for Interface Eth0

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vEdge Cloud -> VPN -> VPN Interface Ethernet**

- Configure the VPN parameters based on the following:

  - Template Name : **BR-VE-VPNINT-VPN512-E0**
  - Description : **BR-VE-VPNINT-VPN512-E0**

  Basic Configuration

  - Shutdown -> Global : **No**
  - Interface Name -> Global : **eth0**
  - IPv4 Address -> Dynamic

- Click **Save** to save the Template

VPN 1

Task 1 – Configure a VPN Template to be used by all Brance vEdge-Cloud Devices for VPN 1

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vEdge Cloud -> VPN -> VPN**

- Configure the VPN parameters based on the following:

  - Template Name : **BR-VE-VPN-VPN1**
  - Description : **BR-VE-VPN-VPN1**

  Basic Configuration

  - VPN -> Global : **1**
  - Name -> Global : **Data VPN**

- Click **Save** to save the Template.

Task 2 – Configure a VPN Interface Template to be used by all Branch vEdge-Cloud Devices for VPN 1 for Interface G0/2

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vEdge Cloud -> VPN -> VPN Interface Ethernet**

- Configure the VPN parameters based on the following:

  - Template Name : **BR-VE-VPNINT-VPN1-G2**
  - Description : **BR-VE-VPNINT-VPN1-G2**

  Basic Configuration
  - Shutdown -> Global : **No**
  - Interface Name -> Global : **Ge0/2**
  - IPv4 Address -> Static -> Device Specific

- Click **Save** to save the Template.

Task 3 – Configure a OSPF Template to be used by all Branch vEdge-Cloud Devices for VPN 1

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vEdge Cloud -> Other Templates -> OSPF**

- Configure the OSPF parameters based on the following:

  - Template Name : **BR-VE-OSPF-VPN1**
  - Description : **BR-VE-OSPF-VPN1**

  Redistribution
  - Protocol : **OMP**

  Area Configuration
  - Area Number -> Global : **0**
  - Area Type -> Default

  Interface Configuration
  - Interface Name: Ge0/2

- Click **Add** to add the Interface and Click **Add** to add OSPF.

- Click **Save** to save the Template.

vEdge5 Templates Deployment

Task 1 – Configure a Device Template for BR3 vEdge Devices.

- In vManage, Navigate to Configuration -> **Templates -> Device -> Create Template -> vEdge Cloud**

- Configure the Device Template based on the following:

  - Template Name : **BR3-VE-TEMP**
  - Description : **BR3-VE-TEMP**

  Basic Information
  - System -> **VE-System**

  Transport & Management
  - VPN 0 : **BR3-VE-VPN-VPN0**
  - VPN Interface : **BR3-VE-VPNINT-VPN0-G0**

  - VPN 512 : **BR-VE-VPN-VPN512**
  - VPN Interface : **BR-VE-VPNINT-VPN512-E0**

  Service VPN
  - VPN 1 : **BR-VE-VPN-VPN1**
  - VPN Interface : **BR-VE-VPNINT-VPN1-G2**
  - OSPF: **BR-VE-OSPF-VPN1**

- Click **Save** to save the Template.

Task 2 – Attach vEdge5 to the Device Template

- In vManage, Navigate to Configuration -> **Templates -> Device -> BR3-VE-TEMP.**

- Click on "**...**" towards the right-hand side.

- Click **Attach Devices.**

- Select **vEdge5** and click the " **->** " button.

- Click **Attach**.

Task 3 – Configure the Variable Parameters for the Feature Templates

- **vEdge5** will appear in the window.
- Click on "**...**" towards the right-hand side.
- Click **Edit Device Template.**
- Configure the variables based on the following:
  - Default Gateway for VPN0 : **192.168.31.10**
  - Interface IP for Ge0/0 :**192.168.31.5/24**
  - Interface IP for Ge0/2 :**172.16.30.5/24**
  - Timezone: **America/Los_Angeles**
  - Hostname : **vEdge-5**
  - System IP : **10.2.2.205**
  - Site ID : **3**
- Click **Update.**
- Verify the Configuration & Click **Configure Devices.**
- Wait for it to update the device. It should come back with Status of **Success**.

Site-3 Internal Router Configuration

Site-3 Internal Router

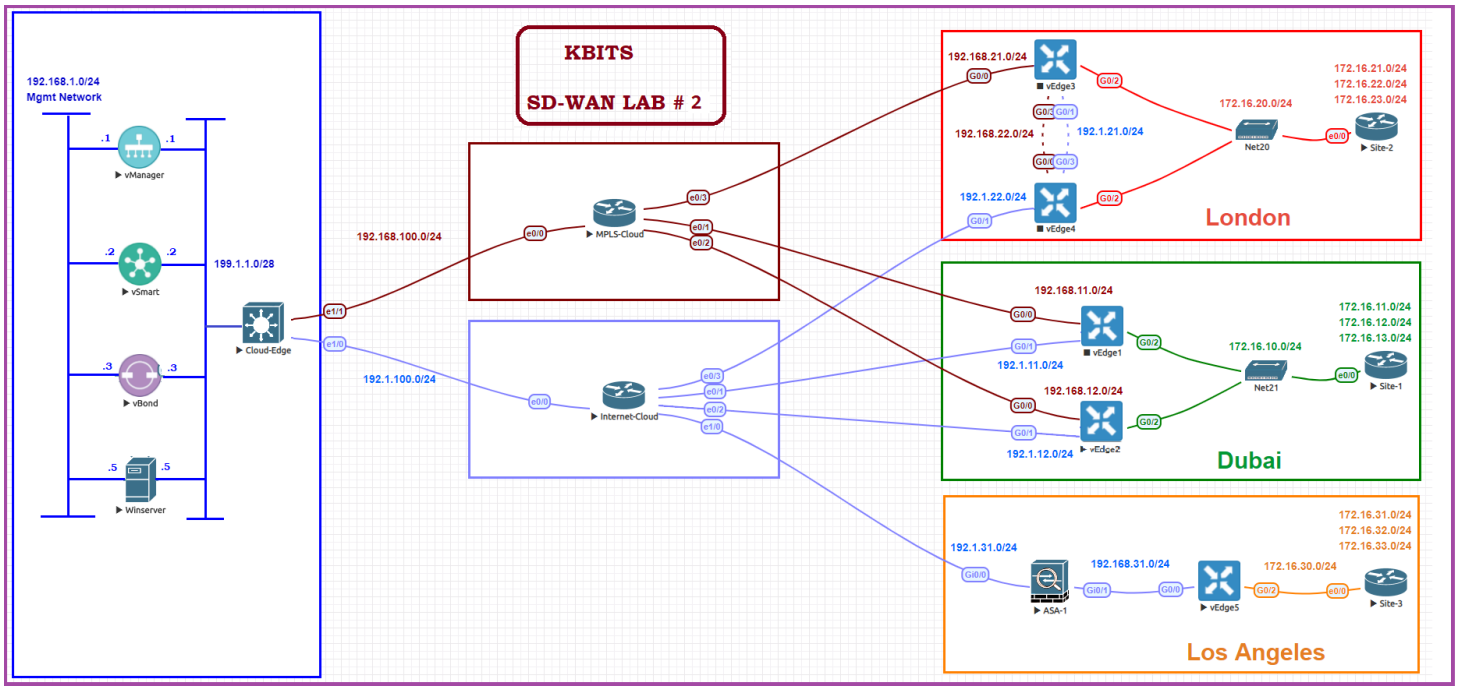
```
No ip domain-lookup
!
Hostname R3
!
Interface E 0/0
 Ip address 172.16.30.33 255.255.255.0
 No shut
!
Interface loopback1
 Ip address 172.16.31.1 255.255.255.0
 Ip ospf network point-to-point
!
Interface loopback2
 Ip address 172.16.32.1 255.255.255.0
 Ip ospf network point-to-point
```

```
!
Interface loopback3
 Ip address 172.16.33.1 255.255.255.0
 Ip ospf network point-to-point
!
Router ospf 1
 Network 172.16.0.0 0.0.255.255 area 0
```

Verification

- Verify the configuration on **vEdge5**. You can do that by verify OSPF Neighbor relationship with the MPLS Router by issuing the **Show ospf neighbor** command on **vEdge5.**

Lab 34 – Configuring TLOC Extensions



vEdge3 Templates Creation

VPN 0

Task 1 – Configure a VPN Template to be used by BR2 vEdges for VPN0

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vEdge Cloud -> VPN -> VPN**

- Configure the VPN parameters based on the following:

  - Template Name : **BR2-VE-VPN-VPN0**
  - Description : **BR2-VE-VPN-VPN0**

  Basic Configuration
  - VPN -> Global : **0**
  - Name -> Global : **Transport VPN**

  IPv4 Route
  - Prefix -> Global : 0.0.0.0/0
  - Next Hop -> Device Specific

- Click **Save** to save the Template.

Task 2 – Configure a VPN Interface Template to be used by all BR2 vEdge-Cloud Devices for VPN 0 for Interface G0/0

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vEdge Cloud -> VPN -> VPN Interface Ethernet**

- Configure the VPN parameters based on the following:

  - Template Name : **BR2-VE-VPNINT-VPN0-G0**
  - Description : **BR2-VE-VPNINT-VPN0-G0**

  Basic Configuration
  - Shutdown -> Global : **No**
  - Interface Name -> Global : **Ge0/0**
  - IPv4 Address -> Static -> Device Specific

  Tunnel
  - Tunnel Inteface -> Global : **On**
  - Color -> Global : **Mpls**

  Allow Service
  - All -> Global : **On**
  - NETCONF -> Global : **On**
  - SSH -> Global : **On**

- Click **Save** to save the Template.

Task 3 – Configure a VPN Interface Template to be used by all BR2 vEdge-Cloud Devices for VPN 0 for Interface G0/1

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vEdge Cloud -> VPN -> VPN Interface Ethernet**

- Configure the VPN parameters based on the following:

  - Template Name : **BR2-VE-VPNINT-VPN0-G1**
  - Description : **BR2-VE-VPNINT-VPN0-G1**

  Basic Configuration
  - Shutdown -> Global : **No**
  - Interface Name -> Global : **Ge0/1**
  - IPv4 Address -> Static -> Device Specific

Tunnel

- Tunnel Inteface -> Global : **On**
- Color -> Global : **Biz-Internet**

Allow Service

- All -> Global : **On**
- NETCONF -> Global : **On**
- SSH -> Global : **On**

- Click **Save** to save the Template.

Task 4 – Configure a Template that will be used for TLOC-Extension on BR2 vEdges

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vEdge Cloud -> VPN -> VPN Interface Ethernet**

- Configure the VPN parameters based on the following:

  - Template Name : **BR2-VE-VPNINT-VPN0-TLOC-G3**
  - Description : **BR2-VE-VPNINT-VPN0-TLOC-G3**

  Basic Configuration

  - Shutdown -> Global : **No**
  - Interface Name -> Global : **Ge0/3**
  - IPv4 Address -> Static -> Device Specific

  Advanced

  - TLOC Extension: Device Specific

- Click **Save** to save the Template.

Task 5 – Configure a OSPF Template to be used by vEdge3 for VPN 0

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vEdge Cloud -> Other Templates -> OSPF**

- Configure the OSPF parameters based on the following:

  - Template Name : **BR2-VE-vEdge3-OSPF-VPN0**
  - Description : **BR-VE-vEdge3-OSPF-VPN0**

  Area Configuration

  - Area Number -> Global : **0**
  - Area Type -> Default

  Interface Configuration

- Interface Name: **Ge0/0**
- Interface Name: **Ge0/3**

➢ Click **Save** to save the Template.

vEdge3 Templates Deployment

Task 1 – Configure a Device Template for BR2 vEdge3.

➢ In vManage, Navigate to Configuration -> **Templates -> Device -> Create Template -> vEdge Cloud**

➢ Configure the Device Template based on the following:

- Template Name : **BR2-VE-vEdge3-TEMP**
- Description : **BR2-VE-vEdge3-TEMP**

Basic Information

- System -> **VE-System**

Transport & Management

- VPN 0 : **BR2-VE-VPN-VPN0**
- VPN Interface : **BR2-VE-VPNINT-VPN0-G0**
- VPN Interface : **BR2-VE-VPNINT-VPN0-G1**
- VPN Interface : **BR2-VE-VPNINT-VPN0-TLOC-G3**
- OSPF: **BR2-VE-vEdge3-OSPF-VPN0**

- VPN 512 : **BR-VE-VPN-VPN512**
- VPN Interface : **BR-VE-VPNINT-VPN512-E0**

Service VPN

- VPN 1 : **BR-VE-VPN-VPN1**
- VPN Interface : **BR-VE-VPNINT-VPN1-G2**
- OSPF: **BR-VE-OSPF-VPN1**

➢ Click **Save** to save the Template.

Task 2 – Attach vEdge3 to the Device Template

➢ In vManage, Navigate to Configuration -> **Templates -> Device -> BR2-VE-vEdge3-TEMP**

➢ Click on "**...**" towards the right-hand side.

➢ Click **Attach Devices.**

- Select **vEdge3** and click the " **->** " button.
- Click **Attach**.

Task 3 – Configure the Variable Parameters for the Feature Templates

- **vEdge3** will appear in the window.
- Click on "**...**" towards the right-hand side.
- Click **Edit Device Template.**
- Configure the variables based on the following:
  - Default Gateway for VPN0 : **192.1.21.4**
  - Interface IP for Ge0/0 :**192.168.21.3/24**
  - Interface IP for Ge0/1 :**192.1.21.3/24**
  - Interface IP for Ge0/2 :**172.16.20.3/24**
  - Interface IP for Ge0/3 :**192.168.22.3/24**
  - TLOC Extension: **ge0/0**
  - Timezone: **Europe/London**
  - Hostname : **vEdge-3**
  - System IP : **10.2.2.203**
  - Site ID : **2**
- Click **Update.**
- Verify the Configuration & Click **Configure Devices.**
- Wait for it to update the device. It should come back with Status of **Success**.

vEdge4 Templates Creation

VPN 0

Task 1 – Configure a OSPF Template to be used by vEdge4 for VPN 0

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vEdge Cloud -> Other Templates -> OSPF**

- Configure the OSPF parameters based on the following:

  - Template Name : **BR2-VE-vEdge4-OSPF-VPN0**
  - Description : **BR-VE-vEdge4-OSPF-VPN0**

  Area Configuration
  - Area Number -> Global : **0**
  - Area Type -> Default

  Interface Configuration
  - Interface Name: **Ge0/0**

- Click **Save** to save the Template.

vEdge4 Templates Deployment

Task 1 – Configure a Device Template for BR2 vEdge4.

- In vManage, Navigate to Configuration -> **Templates -> Device -> Create Template -> vEdge Cloud**

- Configure the Device Template based on the following:

  - Template Name : **BR2-VE-vEdge4-TEMP**
  - Description : **BR2-VE-vEdge4-TEMP**

  Basic Information
  - System -> **VE-System**

  Transport & Management
  - VPN 0 : **BR2-VE-VPN-VPN0**
  - VPN Interface : **BR2-VE-VPNINT-VPN0-G0**
  - VPN Interface : **BR2-VE-VPNINT-VPN0-G1**
  - VPN Interface : **BR2-VE-VPNINT-VPN0-TLOC-G3**
  - OSPF: **BR2-VE-vEdge4-OSPF-VPN0**

- VPN 512 : **BR-VE-VPN-VPN512**
- VPN Interface : **BR-VE-VPNINT-VPN512-E0**

Service VPN

- VPN 1 : **BR-VE-VPN-VPN1**
- VPN Interface : **BR-VE-VPNINT-VPN1-G2**
- OSPF: **BR-VE-OSPF-VPN1**

- Click **Save** to save the Template.

Task 2 – Attach vEdge4 to the Device Template

- In vManage, Navigate to Configuration -> **Templates -> Device -> BR2-VE-vEdge4-TEMP**
- Click on "**...**" towards the right-hand side.
- Click **Attach Devices.**
- Select **vEdge4** and click the " **->** " button.
- Click **Attach**.

Task 3 – Configure the Variable Parameters for the Feature Templates

- **vEdge4** will appear in the window.
- Click on "**...**" towards the right-hand side.
- Click **Edit Device Template.**
- Configure the variables based on the following:

  - Default Gateway for VPN0 : **192.1.22.254**
  - Interface IP for Ge0/0 :**192.168.22.4/24**
  - Interface IP for Ge0/1 :**192.1.22.4/24**
  - Interface IP for Ge0/2 :**172.16.20.4/24**
  - Interface IP for Ge0/3 :**192.1.21.4/24**
  - TLOC Extension: **ge0/1**
  - Timezone: **Europe/London**
  - Hostname : **vEdge-4**
  - System IP : **10.2.2.204**
  - Site ID : **2**

- Click **Update.**
- Verify the Configuration & Click **Configure Devices.**
- Wait for it to update the device. It should come back with Status of **Success**.

Site-2 Internal Router Configuration

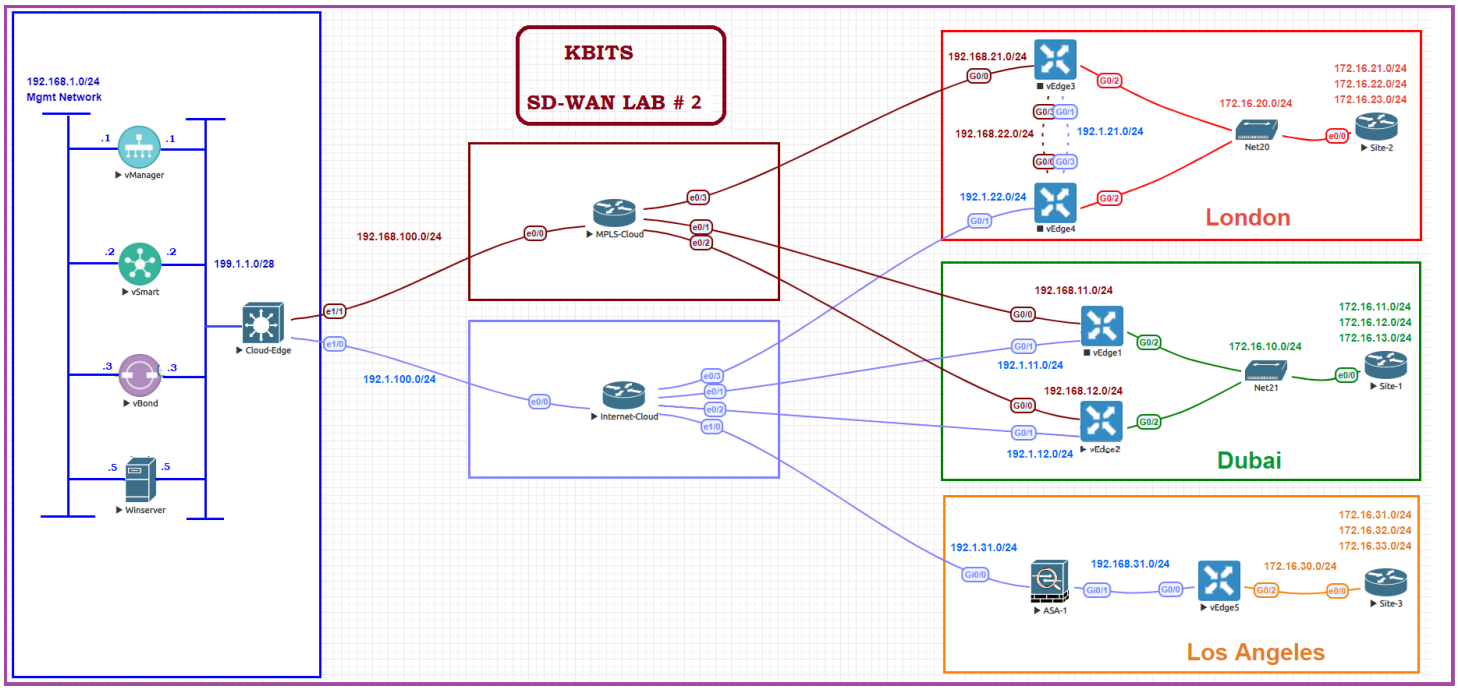
Site-2 Internal Router

```
No ip domain-lookup
!
Hostname R2
!
Interface E 0/0
 Ip address 172.16.20.22 255.255.255.0
 No shut
!
Interface loopback1
 Ip address 172.16.21.1 255.255.255.0
 Ip ospf network point-to-point
!
Interface loopback2
 Ip address 172.16.22.1 255.255.255.0
 Ip ospf network point-to-point
!
Interface loopback3
 Ip address 172.16.23.1 255.255.255.0
 Ip ospf network point-to-point
!
Router ospf 1
 Network 172.16.0.0 0.0.255.255 area 0
```

Verification

- Verify the configuration on **vSmart**. You can do that by making sure that you are receiving 2 TLOCS for vEdge3 and 2 TLOCS for vEdge4. The command to verify is **show omp tlocs.**

Lab 35 – Load Balancing using Multiple vEdges



vEdge1 Templates Creation

VPN 0

Task 1 – Configure a VPN Template to be used by BR2 vEdges for VPN0

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vEdge Cloud -> VPN -> VPN**

- Configure the VPN parameters based on the following:

  - Template Name : **BR1-VE-VPN-VPN0**
  - Description : **BR1-VE-VPN-VPN0**

  Basic Configuration
  - VPN -> Global : **0**
  - Name -> Global : **Transport VPN**

  IPv4 Route
  - Prefix -> Global : 0.0.0.0/0
  - Next Hop -> Device Specific

- Click **Save** to save the Template.

Task 2 – Configure a VPN Interface Template to be used by all BR2 vEdge-Cloud Devices for VPN 0 for Interface G0/0

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vEdge Cloud -> VPN -> VPN Interface Ethernet**

- Configure the VPN parameters based on the following:

  - Template Name : **BR1-VE-VPNINT-VPN0-G0**
  - Description : **BR1-VE-VPNINT-VPN0-G0**

  Basic Configuration
  - Shutdown -> Global : **No**
  - Interface Name -> Global : **Ge0/0**
  - IPv4 Address -> Static -> Device Specific

  Tunnel
  - Tunnel Inteface -> Global : **On**
  - Color -> Global : **Mpls**

  Allow Service
  - All -> Global : **On**
  - NETCONF -> Global : **On**
  - SSH -> Global : **On**

- Click **Save** to save the Template.

Task 3 – Configure a VPN Interface Template to be used by all BR2 vEdge-Cloud Devices for VPN 0 for Interface G0/1

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vEdge Cloud -> VPN -> VPN Interface Ethernet**

- Configure the VPN parameters based on the following:

  - Template Name : **BR1-VE-VPNINT-VPN0-G1**
  - Description : **BR1-VE-VPNINT-VPN0-G1**

  Basic Configuration
  - Shutdown -> Global : **No**
  - Interface Name -> Global : **Ge0/1**
  - IPv4 Address -> Static -> Device Specific

Tunnel

- Tunnel Inteface -> Global : **On**
- Color -> Global : **Biz-Internet**

Allow Service

- All -> Global : **On**
- NETCONF -> Global : **On**
- SSH -> Global : **On**

- Click **Save** to save the Template.

Task 4 – Configure a OSPF Template to be used by all BR2 vEdge-Cloud Devices for VPN 0

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vEdge Cloud -> Other Templates -> OSPF**

- Configure the OSPF parameters based on the following:

  - Template Name : **BR1-VE-OSPF-VPN0**
  - Description : **BR1-VE-OSPF-VPN0**

  Area Configuration

  - Area Number -> Global : **0**
  - Area Type -> Default

  Interface Configuration

  - Interface Name: **Ge0/0**

- Click **Save** to save the Template.

vEdge1&2 Templates Deployment

Task 1 – Configure a Device Template for BR2 vEdges.

- In vManage, Navigate to Configuration -> **Templates -> Device -> Create Template -> vEdge Cloud**

- Configure the Device Template based on the following:

  - Template Name : **BR1-VE-TEMP**
  - Description : **BR1-VE-TEMP**

  Basic Information

  - System -> **VE-System**

  Transport & Management

- VPN 0 : **BR1-VE-VPN-VPN0**
- VPN Interface : **BR1-VE-VPNINT-VPN0-G0**
- VPN Interface : **BR1-VE-VPNINT-VPN0-G1**
- OSPF: **BR1-VE-OSPF-VPN0**

- VPN 512 : **BR-VE-VPN-VPN512**
- VPN Interface : **BR-VE-VPNINT-VPN512-E0**

Service VPN

- VPN 1 : **BR-VE-VPN-VPN1**
- VPN Interface : **BR-VE-VPNINT-VPN1-G2**
- OSPF: **BR-VE-OSPF-VPN1**

- Click **Save** to save the Template.

Task 2 – Attach vEdge1 & 2 to the Device Template

- In vManage, Navigate to Configuration -> **Templates -> Device -> BR2-VE-TEMP**

- Click on "**...**" towards the right-hand side.

- Click **Attach Devices.**

- Select **vEdge1 & vEdge2** and click the " **->** " button.

- Click **Attach**.

Task 3 – Configure the Variable Parameters for the Feature Templates

- **vEdge1 & vEdge2** will appear in the window.

- Click on "**...**" towards the right-hand side.

- Click **Edit Device Template.**

- Configure the variables based on the following:

vEdge1

- Default Gateway for VPN0 : **192.1.11.254**
- Interface IP for Ge0/0 :**192.168.11.1/24**
- Interface IP for Ge0/1 :**192.1.11.1/24**
- Interface IP for Ge0/2 :**172.16.10.1/24**

- Timezone: **Asia/Dubai**
- Hostname : **vEdge-1**
- System IP : **10.2.2.201**
- Site ID : **1**

vEdge2

- Default Gateway for VPN0 : **192.1.12.254**
- Interface IP for Ge0/0 :**192.168.12.2/24**
- Interface IP for Ge0/1 :**192.1.12.2/24**
- Interface IP for Ge0/2 :**172.16.10.2/24**
- Timezone: **Asia/Dubai**
- Hostname : **vEdge-2**
- System IP : **10.2.2.202**
- Site ID : **1**

- Click **Update.**
- Verify the Configuration & Click **Configure Devices.**
- Wait for it to update the device. It should come back with Status of **Success**.

Site-1 Internal Router Configuration

Site-1 Internal Router

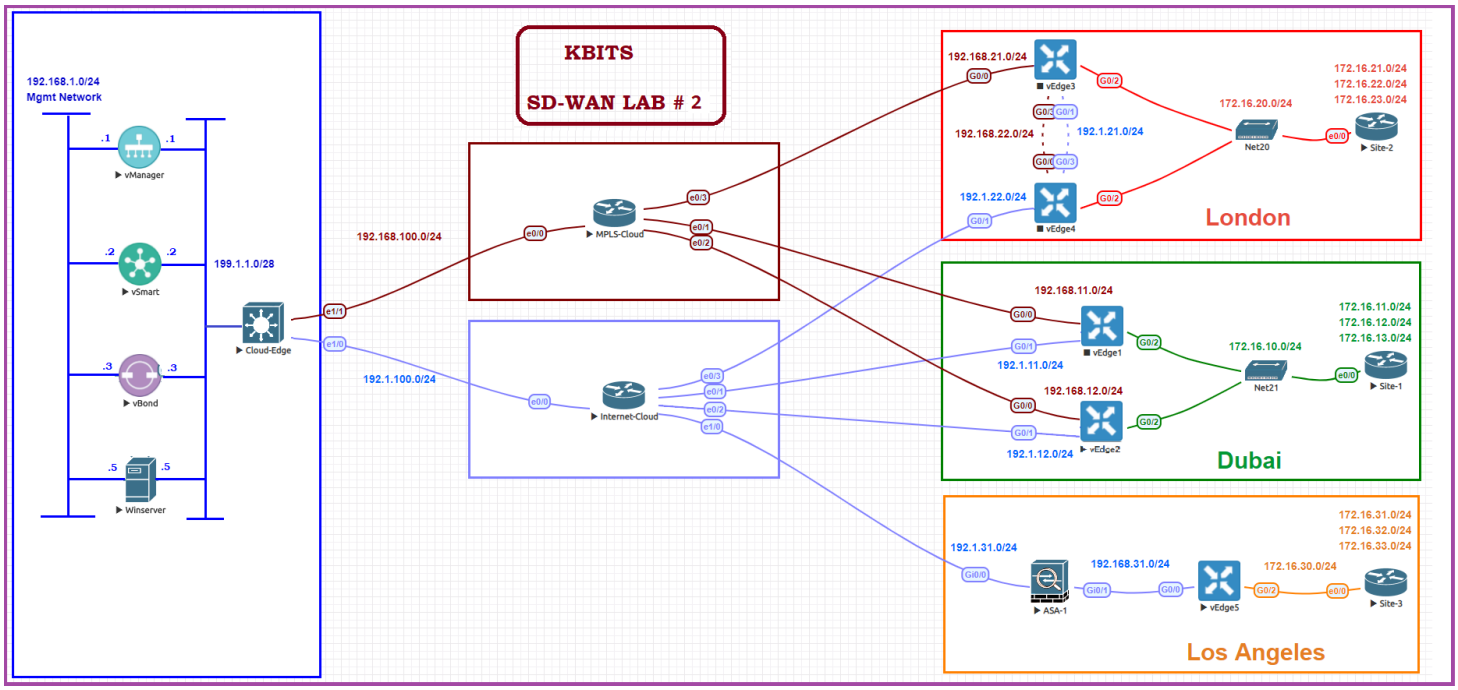
```
No ip domain-lookup
!
Hostname R1
!
Interface E 0/0
 Ip address 172.16.10.11 255.255.255.0
 No shut
!
Interface loopback1
 Ip address 172.16.11.1 255.255.255.0
 Ip ospf network point-to-point
!
Interface loopback2
 Ip address 172.16.12.1 255.255.255.0
 Ip ospf network point-to-point
!
Interface loopback3
```

```
 Ip address 172.16.13.1 255.255.255.0
 Ip ospf network point-to-point
!
Router ospf 1
 Network 172.16.0.0 0.0.255.255 area 0
```

Verification

- Verify the configuration on **vEdge1 & vEdge2**. You can do that by verify OSPF Neighbor relationship with the MPLS Router by issuing the **Show ospf neighbor** command on **vEdge1 & vEdge2.**

Lab 36 – Configuring A Hub-n-Spoke Topology using a TLOC



Task 1 – Configure a VPN Template to be used by vSmart Controllers for VPN 0

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vSmart -> VPN -> VPN**

- Configure the VPN parameters based on the following:

  - Template Name : **vSmart-VPN-VPN0**
  - Description : **vSmart-VPN-VPN0**

  Basic Configuration
  - VPN -> Global : **0**
  - Name -> Global : **Transport VPN**

  IPv4 Route
  - Prefix -> Global : **0.0.0.0/0**
  - Next Hop -> Global : **199.1.1.14**

- Click **Save** to save the Template.

Task 2 – Configure a VPN Template to be used by vSmart Controllers for VPN 512

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vSmart -> VPN -> VPN**

- Configure the VPN parameters based on the following:

  - Template Name : **vSmart-VPN-VPN512**
  - Description : **vSmart-VPN-VPN512**

  Basic Configuration
  - VPN -> Global : **512**
  - Name -> Global : **MGMT VPN**

- Click **Save** to save the Template.

Task 3 – Configure a VPN Interface Template to be used by vSmart Controllers for VPN 0 for Interface Eth1

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vSmart -> VPN -> VPN Interface Ethernet**

- Configure the VPN parameters based on the following:

  - Template Name : **vSmart-VPNINT-VPN0-E1**
  - Description : **vSmart-VPNINT-VPN0-E1**

  Basic Configuration
  - Shutdown -> Global : **No**
  - Interface Name -> Global : **eth1**
  - IPv4 Address -> Static -> Device Specific

  Tunnel
  - Tunnel Inteface -> Global : **On**
  - Color -> default

  Allow Service
  - All -> Global : **On**
  - NETCONF -> Global : **On**
  - SSH -> Global : **On**

- Click **Save** to save the Template.

Task 4 – Configure a VPN Interface Template to be used vSmart Controllers for VPN 512 for Interface Eth0

- In vManage, Navigate to Configuration -> **Templates -> Feature -> vSmart -> VPN -> VPN Interface Ethernet**

- Configure the VPN parameters based on the following:

  - Template Name : **vSmart-VPNINT-VPN512-E0**
  - Description : **vSmart-VPNINT-VPN512-E0**

  Basic Configuration
  - Shutdown -> Global : **No**
  - Interface Name -> Global : **eth0**
  - IPv4 Address -> Static -> Device-Specific

- Click **Save** to save the Template

Task 5 – Configure a Device Template for vSmart Controllers.

- In vManage, Navigate to Configuration -> **Templates -> Device -> Create Template -> vSmart**

- Configure the Device Template based on the following:

  - Template Name : **vSmart-TEMP**
  - Description : **vSmart-TEMP**

  Basic Information
  - System -> **VE-System**

  Transport & Management
  - VPN 0 : **vSmart-VPN-VPN0**
  - VPN Interface : **vSmart-VPNINT-VPN0-E1**

  - VPN 512 : **vSmart-VPN-VPN512**
  - VPN Interface : **vSmart-VPNINT-VPN512-E0**

- Click **Save** to save the Template.

Task 6 – Attach vSmart to the Device Template

- In vManage, Navigate to Configuration -> **Templates -> Device -> vSmart-TEMP**

- Click on "**...**" towards the right-hand side.
- Click **Attach Devices.**
- Select **vSmart** and click the " **->** " button.
- Click **Attach**.

Task 7 – Configure the Variable Parameters for the Feature Templates

- **vSmart** will appear in the window.
- Click on "**...**" towards the right-hand side.
- Click **Edit Device Template.**
- Configure the variables based on the following:
  - Interface IP for Eth1 :**199.1.1.2/28**
  - Interface IP for Eth1 :**192.168.1.2/24**
  - Hostname : **vSmart-1**
  - System IP : **10.1.1.102**
  - Site ID : **1**
- Click **Update.**
- Verify the Configuration & Click **Configure Devices.**
- Wait for it to update the device. It should come back with Status of **Success**.

Policy Requirements:

- Los Angeles & London Sites are communicating to each other directly. You can verify this by checking the routes. The routes should be pointing directly at the TLOCs of the Branch Sites directly.

- All traffic between the sites should be forwarded via the HQ Site Dubai. Use a TLOC list to accomplish this task.

Task 1 – Configure Groups of Interests/List that will be used for Hub-n-Spoke

- In vManage, Navigate to **Configuration -> Policies -> Custom Options -> Centralized Policy -> Lists.**

- Click **VPN** and select **New VPN list.** Create 1 policy based on the following:

  - Name : **VPN1**
  - ID : **1**

- Click **Site** and select **New Site list.** Create 2 policies based on the following:

  - Name : **Dubai**
  - Site ID : **1**

  - Name : **London**
  - Site ID : **2**

  - Name : **Los Angeles**
  - Site ID : **3**

- Click **TLOC** and select **New TLOC list.** Create 1 policies based on the following:

  - Name : **TLOC-Dubai**
  - **TLOCs**
    - 10.2.2.201 – mpls – IPSec – 500
    - 10.2.2.202 – mpls – IPSec – 500
    - 10.2.2.201 – biz-internet – IPSec – 400
    - 10.2.2.202 – biz-internet – IPSec – 400

Task 2 – Configure a Topology based on the Requirements

- In vManage, Navigate to **Configuration -> Policies -> Custom Options -> Centralized Policy -> Topology -> Add Topology -> Custom ->**

- Configure the topology based on the following:

  - Policy Name : **Hub-n-Spoke**
  - Description : **Hub-n-Spoke**

  Route Sequence- London
  Match Conditions:
  - Site: London

  Action
  - TLOC: **TLOC-List = Dubai-TLOC**

  - Click **Save Match and Actions** to save the Sequence.

  Route Sequence- Los Angeles
  Match Conditions:
  - Site: Los Angeles

  Action
  - TLOC: **TLOC-List = Dubai-TLOC**

  - Click **Save Match and Actions** to save the Sequence.

  Default
  Action
  - Accept

  Click **Save Match and Actions**
  - Click **Save Match and Actions** to save the Sequence.

  - **Save Control Policy.**

Task 3 – Create a Centralized Policy and call the Traffic Policy

- In vManage, Navigate to **Configuration -> Policies -> Custom Options -> Centralized Policy -> Add Centralized Policy**

- Click **Next** on the **"Group of Interests"** page as we have already created the required lists.

- Click **Add Policy** on the **"Topology and VPN Membership"** page.
- Click "**Import Existing",** Select **Custom** and select the **Hub-n-Spoke** from the drop-down list and click **Import**. Click **Next.**
- Click **Next** on the **"Configure Traffic Rules"** page as we are not using any Control Policies. You will move to the "**Apply Policy to Sites and VPNs**" Page.
- The **Hub-n-Spoke** policy will be there. Click "**New Site"** button.
- Select **Los Angeles** and **London** in the Outbound Site List.
- Click **Add.**
- Assign the Policy a name and Desription based on the following:
    - Policy Name : **Main-Central-Policy**
    - Description : **Main-Central-Policy**
- Click the **Save Policy** button towards the button.
- Activate the policy.
- Wait for it to push the policy to the reachable vSmart Controller(s).
- You can verify this by doing checking the routes. The routes should be pointing directly at the TLOCs of Dubai and all traffic will be forwarded thru Dubai.