TechCast

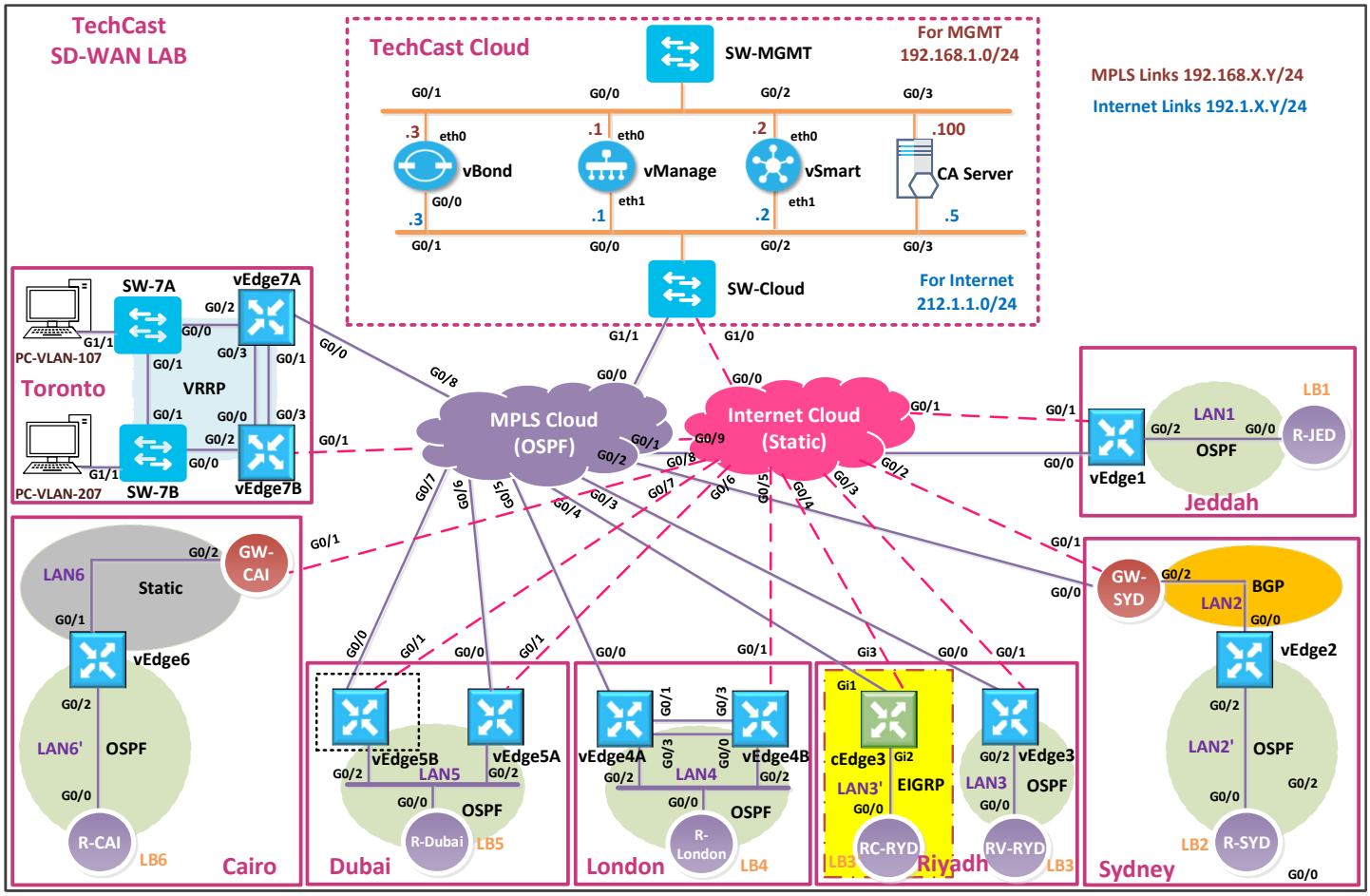
طريقك لاحتراف التقنية

CCIE Enterprise Infrastructure v1.0

SD-WAN

https://www.techcast.io

Topology



Device	WAN Edge's Interface	Link	Service Provider's Interface
vEdge1	**G 0/0** 192.168.101.1/24	MPLS	**G0/1** 192.168.101.254/24
	G 0/1 192.1.101.1/24	Internet	**G0/1** 192.1.101.254/24
	G 0/2 192.168.10.1/24	LAN1	R-JED G0/0
GW-SYD	**G 0/0** 192.168.102.2/24	MPLS	**G0/2** 192.168.102.254/24
	G 0/1 192.1.102.2/24	Internet	**G0/2** 192.1.102.254/24
	G 0/2 192.1.20.254/24	LAN2	**vEdge2**

vEdge2	**G 0/0** 192.1.20.2/24	**LAN2**	**GW-SYD G0/2** 192.1.20.254/24
	G 0/2 192.168.20.2/24	**LAN2'**	**R-SYD G0/0** 192.168.20.22/24
vEdge3	**G 0/0** 192.168.103.3/24	**MPLS**	**G0/3** 192.168.103.254/24
	G 0/1 192.1.103.3/24	**Internet**	**G0/3** 192.1.103.254/24
	G 0/2 192.168.30.3/24	**LAN3**	**RV-Riyadh G0/0** 192.168.30.33/24
cEdge3	**Gi1** 192.168.203.13/24	**MPLS**	**G0/4** 192.168.103.254/24
	Gi3 192.1.203.13/24	**Internet**	**G0/4** 192.1.203.254/24
	G 0/2 192.168.130.3/24	**LAN3'**	**RC-Riyadh G0/0** 192.168.130.33/24
VEdge4A	**G 0/0** 192.168.104.4/24	**MPLS**	**G0/5** 192.168.104.254/24
	G 0/1 192.1.214.4/24	**TLOC EXT. - Internet**	**vEdge4B G0/3** 192.1.214.14/24
	G 0/2 192.168.40.4/24	**LAN4**	**R-London G0/0** 192.168.40.44/24
	G 0/3 192.168.114.4/24	**TLOC EXT. - MPLS**	**vEdge4B G0/0** 192.168.114.14/24
VEdge4B	**G 0/0** 192.168.114.14/24	**TLOC EXT. - MPLS**	**VEdge4A G0/3** 192.168.114.4/24
	G 0/1 192.1.204.4/24	**Internet**	**G0/5** 192.1.204.254/24
	G 0/2 192.168.40.14/24	**LAN4**	**R-London G0/0** 192.168.40.44/24
	G 0/3 192.1.214.14/24	**TLOC EXT. - Internet**	**vEdge4A G0/1** 192.1.214.4/24
vEdge5A	**G 0/0** 192.168.105.5/24	**MPLS**	**G0/6** 192.168.105.254/24
	G 0/1 192.1.105.5/24	**Internet**	**G0/6** 192.1.105.254/24
	G 0/2 192.168.50.5/24	**LAN5**	**R-Dubai G0/0** 192.168.50.55/24
vEdge5B	**G 0/0** 192.168.205.5/24	**MPLS**	**G0/7** 192.168.205.254/24
	G 0/1 192.1.205.5/24	**Internet**	**G0/7** 192.1.205.254/24

	G 0/2 192.168.50.15/24	**LAN5**	**R-Dubai G0/0** 192.168.50.55/24
GW-Cairo	**G 0/1** 192.1.106.16/24	**Internet**	**G0/8** 192.1.106.254/24
	G 0/2 192.168.106.254/24	**LAN6**	**vEdge6 G0/1** 192.168.106.6/24
vEdge6	**G 0/1** 192.168.106.6/24	**LAN6**	**GW-Cairo G0/2** 192.168.106.254/24
	G 0/2 192.168.60.6/24	**LAN6'**	**R-Cairo G0/0** 192.168.60.66/24
VEdge7A	**G 0/0** 192.168.107.7/24	**MPLS**	**G0/8** 192.168.104.254/24
	G 0/1 192.1.217.7/24	**TLOC EXT. - Internet**	**vEdge7B G0/3** 192.1.217.17/24
	G 0/2.107 10.10.107.1/24	**VLAN 107**	**PC-VLAN-107** 10.10.107.107/24
	G 0/2.207 10.10.207.1/24	**VLAN 207**	**PC-VLAN-207** 10.10.207.207/24
	G 0/3 192.168.117.7/24	**TLOC EXT. - MPLS**	**VEdge7B G0/0** 192.168.117.17/24
VEdge7B	**G 0/0** 192.168.117.17/24	**TLOC EXT. - MPLS**	**VEdge7A G0/3** 192.168.117.7/24
	G 0/1 192.1.207.7/24	**Internet**	**G0/9** 192.1.207.254/24
	G 0/2.107 10.10.107.2/24	**VLAN 107**	**PC-VLAN-107** 10.10.107.107/24
	G 0/2.207 10.10.207.2/24	**VLAN 207**	**PC-VLAN-207** 10.10.207.207/24
	G 0/3 192.1.217.17/24	**TLOC EXT. - Internet**	**vEdge4A G0/1** 192.1.217.7/24

1 Non-SDWAN Network Preparation

1.1 Lab 01 – Service Providers' Infrastructure Pre-configuration

Interface Configuration

MPLS Cloud

Interface	IP Address	Subnet Mask
G 0/0	192.168.100.254	255.255.255.0
G 0/1	192.168.101.254	255.255.255.0
G 0/2	192.168.102.254	255.255.255.0
G 0/3	192.168.103.254	255.255.255.0
G 0/4	192.168.203.254	255.255.255.0
G 0/5	192.168.104.254	255.255.255.0
G 0/6	192.168.105.254	255.255.255.0
G 0/7	192.168.205.254	255.255.255.0
G 0/8	192.168.107.254	255.255.255.0

Internet Cloud

Interface	IP Address	Subnet Mask
G 0/0	192.1.100.254	255.255.255.0
G 0/1	192.1.101.254	255.255.255.0
G 0/2	192.1.102.254	255.255.255.0
G 0/3	192.1.103.254	255.255.255.0
G 0/4	192.1.203.254	255.255.255.0
G 0/5	192.1.204.254	255.255.255.0
G 0/6	192.1.105.254	255.255.255.0
G 0/7	192.1.205.254	255.255.255.0
G 0/8	192.1.106.254	255.255.255.0
G 0/9	192.1.207.254	255.255.255.0

1.1.1 Step 1 – MPLS-Cloud Router Configuration

- Configure the Interfaces based on the above topology

- Configure OSPF as the IGP on all the interfaces

```
 no ip domain-lookup
 !
 line con 0
 exec-timeout 0 0
 logging synchronous
 !
 hostname MPLS
 !
interface GigabitEthernet0/0
 ip address 192.168.100.254 255.255.255.0
 no shut
 !
 interface GigabitEthernet0/1
 ip address 192.168.101.254 255.255.255.0
 no shut
 !
 interface GigabitEthernet0/2
 ip address 192.168.102.254 255.255.255.0
 no shut
 !
 interface GigabitEthernet0/3
 ip address 192.168.103.254 255.255.255.0
 no shut
 !
 interface GigabitEthernet0/4
 ip address 192.168.203.254 255.255.255.0
 no shut
 !
 interface GigabitEthernet0/5
 ip address 192.168.104.254 255.255.255.0
 no shut
 !
 interface GigabitEthernet0/6
 ip address 192.168.105.254 255.255.255.0
 no shut
 !
 interface GigabitEthernet0/7
 ip address 192.168.205.254 255.255.255.0
 no shut
 !
 interface GigabitEthernet0/8
 ip address 192.168.107.7 255.255.255.0
 no shut
 !
```

```
!
router ospf 1
network 192.168.100.0 0.0.0.255 area 0
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
network 192.168.107.0 0.0.0.255 area 0
network 192.168.203.0 0.0.0.255 area 0
network 192.168.205.0 0.0.0.255 area 0
```

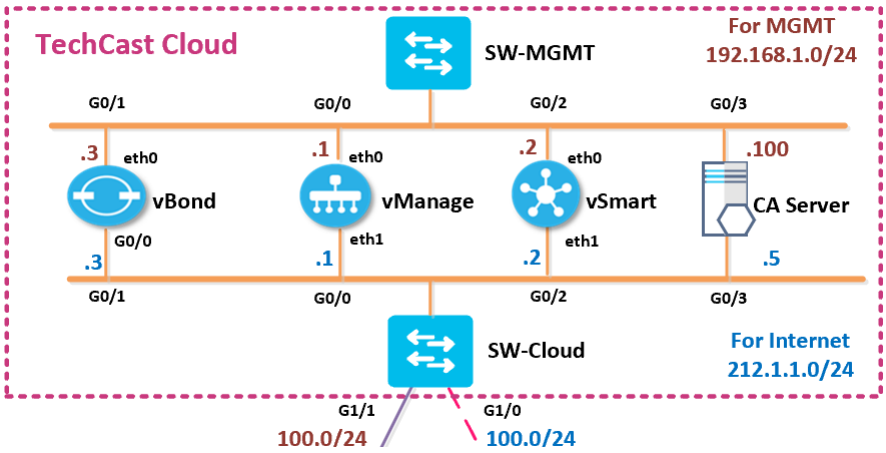
1.1.2 Step 2 – Internet-Cloud Router Configuration

- Configure the Interfaces based on the above topology
- Configure two Static Routes for the 212.1.1.0/24 network toward (TechCast-Cloud) infrastructure as a next-hop and 192.1.20.0/24 network toward (Sydney Site) as a next-hop

```
no ip domain lookup
!
line con 0
exec-timeout 0 0
logging synchronous
!
hostname Internet
!
interface GigabitEthernet0/0
ip address 192.1.100.254 255.255.255.0
no shut
!
interface GigabitEthernet0/1
ip address 192.1.101.254 255.255.255.0
no shut
!
interface GigabitEthernet0/2
ip address 192.1.102.254 255.255.255.0
no shut
!
interface GigabitEthernet0/3
```

```
ip address 192.1.103.254 255.255.255.0
no shut
!
interface GigabitEthernet0/4
ip address 192.1.203.254 255.255.255.0
no shut
!
interface GigabitEthernet0/5
ip address 192.1.204.254 255.255.255.0
no shut
!
interface GigabitEthernet0/6
ip address 192.1.105.254 255.255.255.0
no shut
!
interface GigabitEthernet0/7
ip address 192.1.205.254 255.255.255.0
no shut
!
interface GigabitEthernet0/8
ip address 192.1.106.254 255.255.255.0
no shut
!
interface GigabitEthernet0/9
ip address 192.1.207.254 255.255.255.0
no shut
!
ip route 212.1.1.0 255.255.255.0 192.1.100.1
ip route 192.1.20.0 255.255.255.0 192.1.102.2
ip route 192.1.214.0 255.255.255.0 192.1.204.4
ip route 192.1.217.0 255.255.255.0 192.1.207.7
```

1.2 Lab 02 – TechCast Cloud Infrastructure Pre-configuration



Interface Configuration

SW-MGMT

Interface	IP Address	Subnet Mask
VLAN 1	192.168.1.254	255.255.255.0

SW-Cloud

Interface	IP Address	Subnet Mask
G 1/0	192.1.100.1	255.255.255.0
VLAN 1	212.1.1.254	255.255.255.0

CA Server

Interface	IP Address	Subnet Mask/GW
Ethernet 1	192.168.1.100	255.255.255.0
Ethernet 3	212.1.1.5	255.255.255.0/ 212.1.1.254

1.2.1 Step 1 – Configure Management Switch "SW-MGMT"

```
no ip domain lookup
!
line con 0
exec-timeout 0 0
logging synchronous
!
Hostname SW-MGMT
!
Interface vlan 1
ip address 192.168.1.254 255.255.255.0
no shut
```

1.2.2 Step 2 – Configure Cloud Switch "SW-Cloud"

```
no ip domain lookup
!
line con 0
exec-timeout 0 0
logging synchronous
!
Hostname SW-Cloud
!
Interface GigabitEthernet1
no switchport
ip address 192.1.100.1 255.255.255.0
no shut
!
Interface GigabitEthernet2
no switchport
ip address 192.168.100.1 255.255.255.0
no shut
!
Interface vlan 1
ip address 212.1.1.254 255.255.255.0
no shut
```

```
!
router ospf 1
 passive-interface default
 no passive-interface GigabitEthernet1/1
 network 192.168.100.0 0.0.0.255 area 0
 network 212.1.1.0 0.0.0.255 area 0
!
ip route 0.0.0.0 0.0.0.0 192.1.100.254
```

1.2.3 Step 3 – Certificate Authorization – CA Server Installation

حنستخدم في اللاب هنا ويندوز سيرفر 2016 كسيرفر لاصدار التفويض لأجهزة شبكة **SD-WAN** واللي حنسميه **CA Server**
وبالتالي حنقوم بالخطوات التالي **:**

- Appropriate Time zone and Time on the Windows Server based on your area.
- Installing the Enterprise Root Certificate Server
  - Open **Server Manager**
  - Click **Manage**
  - Click **Add Roles and Features**
  - In **Before You Begin**, click **Next**
  - In **Select Installation Type**, ensure that **Role-Based or feature-based installation** is selected, and then click **Next**.
  - In **Select destination server**, ensure that **Select a server from the server pool** is selected.
  - In **Server Pool**, ensure that the local computer is selected and click **Next**.
  - In **Select Server Roles**, in **Roles**, select **Active Directory Certificate Services**. When you are prompted to add required features, click **Add Features**, and then click **Next**.
  - In **Select features**, click **Next.**
  - In **Active Directory Certificate Services**, read the provided information, and then click **Next**.
  - In **Confirm installation selections**, click **Install**. Do not close the wizard during the installation process. When installation is complete, click **Configure Active Directory Certificate Services on the destination server**. The AD CS Configuration wizard opens and then click **Next**.
  - In **Role Services**, click **Certification Authority**, and then click **Next**.
  - On the **Setup Type** page, verify that **Enterprise CA** is selected, and then click **Next**.
  - On the **Specify the type of the CA** page, verify that **Root CA** is selected, and then click **Next**.
  - On the **Specify the type of the private key** page, verify that **Create a new private key** is selected, and then click **Next**.
  - On the **Cryptography for CA** page, keep the default settings for CSP. Click **Next**.
  - On the **CA Name** page, change the name as **TECTCAST-CA** and click Next.
  - On the **Validity Period** page, in **Specify the validity period**, keep default setting of five years is recommended and click Next.
  - On the **CA Database** page, in **Specify the database locations**, keep

default setting and click Next.

- In **Confirmation**, click **Configure** to apply your selections, and then click **Close**.

1.2.4 Step 4 – File Transfer Tools installation (i.e. WinSCP, FileZilla, etc.)

- Follow a default installation as per our video.

1.3 Lab 03 – Sites' GWs/Internal Routers/Switches Pre-configuration

Interface Configuration

R-JEDDAH

Interface	IP Address	Subnet Mask
G 0/0	192.168.10.11	255.255.255.0
Loopback1	10.10.11.1	255.255.255.0
Loopback2	10.10.12.1	255.255.255.0
Loopback3	10.10.13.1	255.255.255.0
Loopback4	10.10.123.1	255.255.255.255

GW-SYDNEY

Interface	IP Address	Subnet Mask
G 0/0	192.168.102.1	255.255.255.0
G 0/1	192.1.102.1	255.255.255.0
G 0/2	192.1.20.254	255.255.255.0

R-SYDNEY

Interface	IP Address	Subnet Mask
G 0/0	192.168.20.22	255.255.255.0
Loopback1	10.10.21.1	255.255.255.0
Loopback2	10.10.22.1	255.255.255.0
Loopback3	10.10.23.1	255.255.255.0
Loopback4	10.10.123.2	255.255.255.255

RV-RIYADH

Interface	IP Address	Subnet Mask
G 0/0	192.168.30.33	255.255.255.0
Loopback1	10.10.31.1	255.255.255.0
Loopback2	10.10.32.1	255.255.255.0
Loopback3	10.10.33.1	255.255.255.0
Loopback4	10.10.123.3	255.255.255.255

RC-RIYADH

Interface	IP Address	Subnet Mask
G 0/0	192.168.130.33	255.255.255.0
Loopback1	10.10.31.1	255.255.255.0
Loopback2	10.10.32.1	255.255.255.0
Loopback3	10.10.33.1	255.255.255.0

R-LONDON

Interface	IP Address	Subnet Mask
G 0/0	192.168.40.44	255.255.255.0
Loopback1	10.10.41.1	255.255.255.0
Loopback2	10.10.42.1	255.255.255.0
Loopback3	10.10.43.1	255.255.255.0

R-DUBAI

Interface	IP Address	Subnet Mask
G 0/0	192.168.50.55	255.255.255.0
Loopback1	10.10.51.1	255.255.255.0
Loopback2	10.10.52.1	255.255.255.0
Loopback3	10.10.53.1	255.255.255.0
Loopback4	50.50.50.1	255.255.255.0

R-CAIRO

Interface	IP Address	Subnet Mask
G 0/0	192.168.60.66	255.255.255.0
Loopback1	10.10.61.1	255.255.255.0
Loopback2	10.10.62.1	255.255.255.0
Loopback3	10.10.63.1	255.255.255.0

SW-7A

Interface	IP Address	Subnet Mask
G 0/0	Trunk	Trunk
G 0/1	Trunk	Trunk
G 1/1	VLAN 107	VLAN 107

SW-7B

Interface	IP Address	Subnet Mask
G 0/0	Trunk	Trunk
G 0/1	Trunk	Trunk
G 1/1	VLAN 207	VLAN 207

1.3.1 Step 1 – Gateway Routers Configurations

- At this stage, we will configure ONLY GW-Sydney's Router's interfaces based on the above topology.
- In GW-Sydney's Router; configure OSPF as the IGP to communicate with the MPLS Cloud.
- In GW-Sydney's Router; configure a default route on the router towards the Internet. The IP Address of the Internet Router is 192.1.102.254

- In GW-Sydney's Router; configure BGP peering with vEdge2 (192.1.20.2) in 65001 and redistribute OPSF into BGP.

GW-Sydney

```
no ip domain-lookup
line con 0
logg sync
no exec-timeout
!
Hostname GW-Sydney
!
Interface G 0/0
ip address 192.168.102.2 255.255.255.0
no shut
!
Interface G 0/1
ip address 192.1.102.2 255.255.255.0
no shut
!
Interface G 0/2
ip address 192.1.20.254 255.255.255.0
no shut
!
router ospf 1
network 192.168.102.2 0.0.0.255 area 0
!
Router bgp 65001
Neighbor 192.1.20.2 remote-as 65001
Redistribute ospf 1
!
ip route 0.0.0.0 0.0.0.0 192.1.102.254
```

1.3.2 Step 2 – Internal Site Router Configurations

- Configure the interfaces based on the above topology.
- Only in **RC-Riyadh** router; configure EIGRP as the IGP to communicate with the cEdge devices.
- In the rest of internal routers, configure OSPF as the IGP to communicate with the vEdge devices. Enable all the interfaces under OSPF.

R-Jeddah

```
no ip domain-lookup
line con 0
logg sync
no exec-timeout
!
Hostname R-Jeddah
!
Interface G 0/0
ip address 192.168.10.11 255.255.255.0
no shut
!
Interface Loopback1
ip address 10.10.11.1 255.255.255.0
!
Interface Loopback2
ip address 10.10.12.1 255.255.255.0
!
Interface Loopback3
ip address 10.10.13.1 255.255.255.0
!
Interface Loopback4
ip address 10.10.123.1 255.255.255.255
!
router ospf 1
network 192.168.10.0 0.0.0.255 area 0
network 10.10.0.0 0.0.255.255 area 0
```

R-SYD

```
no ip domain-loo
line con 0
logg sync
no exec-timeout
!
Hostname R-SYD
!
Interface G 0/0
ip address 192.168.20.22 255.255.255.0
no shut
!
Interface Loopback1
ip address 10.10.21.1 255.255.255.0
!
!
Interface Loopback2
ip address 10.10.22.1 255.255.255.0
!
!
Interface Loopback3
ip address 10.10.23.1 255.255.255.0
!
!
Interface Loopback4
ip address 10.10.123.2 255.255.255.255
!
router ospf 1
network 192.168.20.0 0.0.0.255 area 0
network 10.10.0.0 0.0.255.255 area 0
```

RV-Riyadh

```
no ip domain-lookup
line con 0
logg sync
no exec-timeout
!
Hostname RV-Riyadh
!
Interface G 0/0
ip address 192.168.30.33 255.255.255.0
no shut
!
Interface Loopback1
ip address 10.10.31.1 255.255.255.0
!
!
Interface Loopback2
ip address 10.10.32.1 255.255.255.0
!
!
Interface Loopback3
ip address 10.10.33.1 255.255.255.0
!
!
Interface Loopback4
ip address 10.10.123.3 255.255.255.255
!
!
router ospf 1
network 192.168.30.0 0.0.0.255 area 0
network 10.10.0.0 0.0.255.255 area 0
```

RC-Riyadh

```
no ip domain-lookup
line con 0
logg sync
no exec-timeout
!
Hostname RC-Riyadh
!
Interface G 0/0
ip address 192.168.130.33 255.255.255.0
no shut
!
Interface Loopback1
ip address 10.10.131.1 255.255.255.0
!
!
Interface Loopback2
ip address 10.10.132.1 255.255.255.0
!
!
Interface Loopback3
ip address 10.10.133.1 255.255.255.0
!
!
Interface Loopback4
ip address 10.10.123.3 255.255.255.255
!
!
router eigrp 1
 network 10.0.0.0
 network 192.168.130.0
```

R-London

```
no ip domain-lookup
line con 0
logg sync
no exec-timeout
!
Hostname R-London
!
Interface G 0/0
ip address 192.168.40.44 255.255.255.0
no shut
!
Interface Loopback1
ip address 10.10.41.1 255.255.255.0
!
!
Interface Loopback2
ip address 10.10.42.1 255.255.255.0
!
!
Interface Loopback3
ip address 10.10.43.1 255.255.255.0
!
router ospf 1
network 192.168.40.0 0.0.0.255 area 0
network 10.10.0.0 0.0.255.255 area 0
```

R-Dubai

```
no ip domain-lookup
line con 0
logg sync
no exec-timeout
!
Hostname R-Dubai
!
Interface G 0/0
ip address 192.168.50.55 255.255.255.0
no shut
!
Interface Loopback1
ip address 10.10.51.1 255.255.255.0
!
Interface Loopback2
ip address 10.10.52.1 255.255.255.0
!
Interface Loopback3
ip address 10.10.53.1 255.255.255.0
!
Interface Loopback4
Ip address 50.50.50.1 255.255.255.0

router ospf 1
network 192.168.50.0 0.0.0.255 area 0
network 10.10.0.0 0.0.255.255 area 0
network 50.50.50.0 0.0.255.255 area 0
```

R-Cairo

```
no ip domain-loo
line con 0
logg sync
no exec-timeout
!
Hostname R-Cairo
!
Interface G 0/0
ip address 192.168.60.66 255.255.255.0
no shut
!
Interface Loopback1
ip address 10.10.61.1 255.255.255.0
!
!
Interface Loopback2
ip address 10.10.62.1 255.255.255.0
!
!
Interface Loopback3
ip address 10.10.63.1 255.255.255.0
!
!
router ospf 1
network 192.168.60.0 0.0.0.255 area 0
network 10.10.0.0 0.0.255.255 area 0
```

1.3.3 Step 3 – SW-7A and SW-7B Configurations

- Configure the interfaces based on the above topology
- Configure Trunks between SW-7A and vEdge7A
- Configure Trunks between SW-7B and vEdge7B
- Configure Trunks between SW-7A and SW-7B
- Configure Host Interfaces. **VLAN 107** for **Staff** and **VLAN 207** for **Guests**

SW-7A

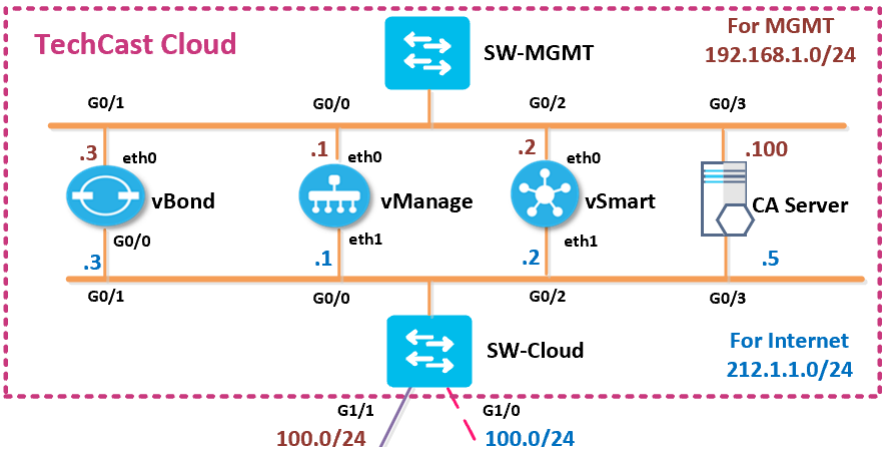
```
conf t
no ip domain-lookup
line con 0
logg sync
no exec-timeout
!
Hostname SW-7A
!
interface g0/0
description <<To vEdge7A>>
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 107,207
no shut
!
interface g0/1
description <<To SW7B>>
switchport trunk encapsulation dot1q
switchport mode trunk
no shut
!
interface g1/1
description <<To PC-VLAN-107>>
switchport mode access
switchport access vlan 107
negotiation auto
no shut
!
vlan 107
name Staff
!
vlan 207
name Guests
```

SW-7B

```
conf t
no ip domain-lookup
line con 0
logg sync
no exec-timeout
!
Hostname SW-7B
!
interface g0/0
description <<To vEdge7B>>
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 107,207
no shut
!
interface g0/1
description <<To SW7A>>
switchport trunk encapsulation dot1q
switchport mode trunk
no shut
!
interface g1/1
description <<To PC-VLAN-207>>
switchport mode access
switchport access vlan 207
negotiation auto
no shut
!
vlan 107
name Staff
!
vlan 207
name Guests
```

2 Controllers Bring Up & Initialization

2.1 Lab 04 – vManage Bring Up CLI Configuration



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

2.1.1 Step 1 – Configuring the System Component

- Configure the System parameters based on the following:
  - HOST-NAME: VMANAGE1
  - ORGANIZATION: TECTCAST
  - SYSTEM-IP: 100.100.100.101
  - SITE ID: 100
  - VBOND ADDRESS: 212.1.1.3
  - TIMEZONE: SELECT TIMEZONE BASED ON YOUR DEVICE LOCATION

vManage

```
config
!
system
 host-name vManage1
 system-ip 100.100.100.101
 site-id 100
 organization-name TECHCAST
 clock timezone America/Toronto
 vbond 212.1.1.3
!
commit
```

2.1.2 Step 2 – Configured the VPN parameters

- Configure the VPN parameters based on the following:

VPN 0

- Interface eth1
- IP Address: 212.1.1.1/24
- Tunnel Interface
  - Tunnel Services (All, NetConf, SSHD)
- Default Route: 212.1.1.254

VPN 512

- Interface eth0
- IP Address: 192.168.1.1/24

vManage

```
config
!
vpn 0
 no interface eth0
 interface eth1
  ip address 212.1.1.1/24
  tunnel-interface
   allow-service all
   allow-service netconf
   allow-service sshd no
   shut
 ip route 0.0.0.0/0 212.1.1.254
!
vpn 512
interface eth0
  ip address 192.168.1.1/24
  no shut
!
 commit
```

2.2 Lab 05 – vManage GUI Initialization

2.2.1 Step 1 – Organization name & vBond Address

- Open the browser
- 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 **TECTCAST**. Confirm the Organization name. Click **OK.**
- Click **Edit** on the **vBond** address and change it to 212.1.1.3. Confirm and click **OK**.

2.2.2 Step 2 – Configure Controller Authorization as Enterprise Root and Download the Root Certificate

في هذه الخطوة سوف نجعل Controller Authorization يعمل ك Enterprise Root ثم نعمل تنزيل لكل Root Certificates من خلاله.

- Browse to http://192.168.1.100/certsrv
- Click **"Download a CA 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 as per our videos.

2.2.3 Step 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.**

2.2.4 Step 4 – Request a Certificate from the CA Server

- Browse t http://192.168.1.100/certsrv
- Click **"Request a Certificate".**
- Select **"Advanced"**.
- Paste the CSR in the box by using **CTRL-V** and click **Submit.**

2.2.5 Step 5 – Issue the Certificate from the CA Server

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

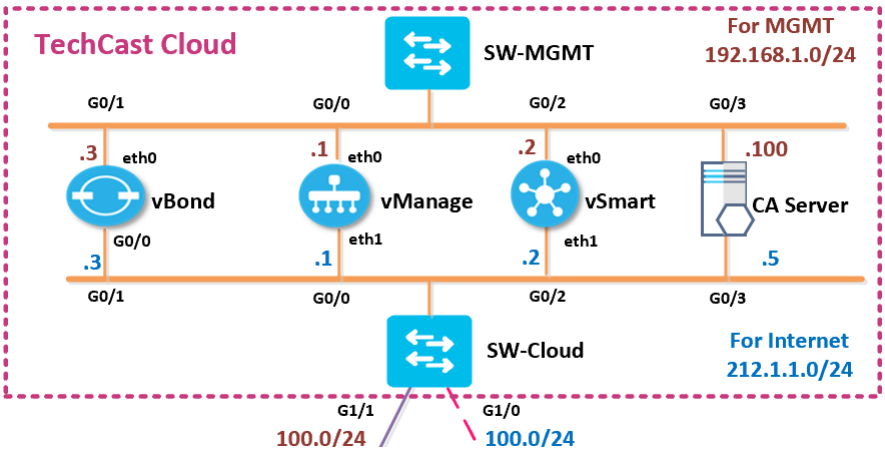
2.2.6 Step 6 – Downloading the Issued Certificate

- Browse to http://192.168.1.100/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**.

2.2.7 Step 7 – 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.

2.3 Lab 06 – vBond Bring Up CLI Configuration



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

2.3.1 Step 1 – Configuring the System Component

- Configure the System parameters based on the following:
  - HOST-NAME : VBOND1
  - ORGANIZATION: TECTCAST
  - SYSTEM-IP: 100.100.100.103
  - SITE ID: 100
  - VBOND ADDRESS: 212.1.1.3
  - TIMEZONE: SELECT TIMEZONE BASED ON YOUR DEVICE LOCATION

vBond

```
config
!
system
 host-name vBond1
 system-ip 100.100.100.103
 site-id 100
 organization-name TECHCAST
 clock timezone America/Toronto
 vbond 212.1.1.3 local
!
 Commit
```

2.3.2 Step 2 – Configured the VPN parameters

- Configure the VPN parameters based on the following:

VPN 0

- Interface ge0/0
- IP Address: 212.1.1.3/24
- Tunnel Interface
  - Tunnel Services (All, NetConf, SSHD)
  - Encapsulation: IPSec
- Default Route: 212.1.1.254

VPN 512

- Interface eth0
- IP Address: 192.168.1.3/24

vBond

```
config
!
vpn 0
 no interface eth0
 interface ge0/0
  ip address 212.1.1.3/24
   tunnel-interface
   encapsulation ipsec
    allow-service all
    allow-service netconf
    allow-service sshd
    no shut
 ip route 0.0.0.0/0 212.1.1.254
!
vpn 512
interface eth0
  ip address 192.168.1.3/24
  no shut
!
 commit
```

2.4 Lab 07 – vBond GUI Initialization

2.4.1 Step 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: 212.1.1.3
  - USERNAME: ADMIN
  - PASSWORD: ADMIN
  - CHECK GENERATE CSR
  - CLICK ADD

2.4.2 Step 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.**

2.4.3 Step 3 – Request a Certificate from the CA Server

- Browse to http://192.168.1.100/certsrv
- Click **"Request a Certificate".**
- Select **"Advanced certificate request"**.
- Paste the CSR in the box by using **CTRL-V** and click **Submit.**

2.4.4 Step 4 – Issue the Certificate from the CA Server

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

2.4.5 Step 5 – Downloading the Issued Certificate

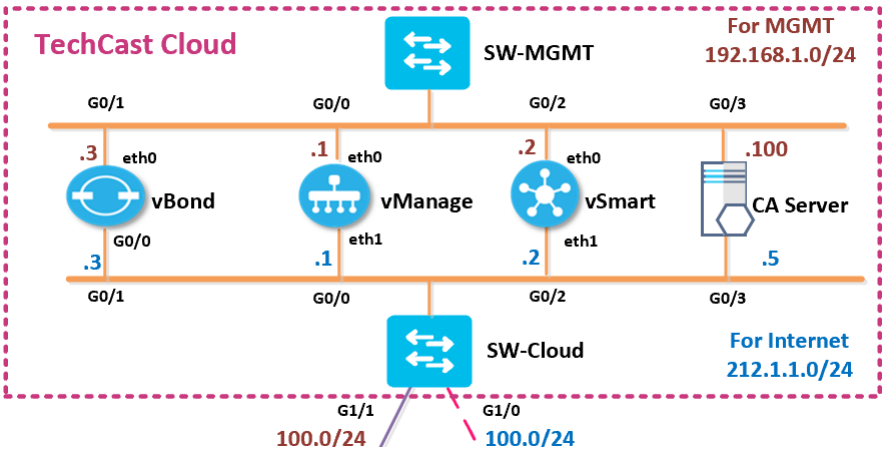
- Browse to http://192.168.1.100/certsrv
- Click **"View the status of a pending certificate request".**
- The issued certificate link will show up. Click on the link.

- 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**.

2.4.6 Step 6 – Installing the Identity Certificate for vBond

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

2.5 Lab 08 – vSmart Bring Up CLI Configuration



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

2.5.1 Step 1 – Configuring the System Component

- Configure the System parameters based on the following:
  - HOST-NAME: VSMART1
  - ORGANIZATION: TECTCAST
  - SYSTEM-IP: 100.100.100.102
  - SITE ID: 100
  - VBOND ADDRESS: 212.1.1.3
  - TIMEZONE: SELECT TIMEZONE BASED ON YOUR DEVICE LOCATION

vSmart

```
config
!
system
 host-name vSmart1
 system-ip 100.100.100.102
 site-id 100
 organization-name TECHCAST
 clock timezone America/Toronto
 vbond 212.1.1.3
!
 Commit
```

2.5.2 Step 2 – Configured the VPN parameters

- Configure the VPN parameters based on the following:

VPN 0

- Interface Eth1
- IP Address: 212.1.1.2/24
- Tunnel Interface
  - Tunnel Services (All, NetConf, SSHD)
- Default Route: 212.1.1.254

VPN 512

- Interface eth0
- IP Address: 192.168.1.2/24

vSmart

```
config
!
vpn 0
 no interface eth0
 interface eth1
  ip address 212.1.1.2/24
  tunnel-interface
   allow-service all
   allow-service netconf
   allow-service sshd
   no shut
 ip route 0.0.0.0/0 212.1.1.254
!
vpn 512
interface eth0
  ip address 192.168.1.2/24
  no shut
!
 Commit
```

2.6 Lab 09 – vSmart GUI Initialization

2.6.1 Step 1 – Add vSmart to vManage

- Navigate to **Configuration -> Devices -> Controllers -> Add Controllers -> vSmart** and specify the following to add the vSmart in vManage.
  - IP Address: 212.1.1.2
  - Username: Admin
  - Password: Admin
  - Check Generate CSR
  - Click OK

2.6.2 Step 2 – View the generated CSR for vSmart 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.**

2.6.3 Step 3 – Request a Certificate from the CA Server

- Browse to http://192.168.1.100/certsrv
- Click **"Request a Certificate".**
- Select **"Advanced"**.
- Paste the CSR in the box by using **CTRL-V** and click **Submit.**

2.6.4 Step 4 – Issue the Certificate from the CA Server

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

2.6.5 Step 5 – Downloading the Issued Certificate

- Browse to http://192.168.1.100/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**.

2.6.6 Step 6 – Installing the Identity Certificate for vSmart

- 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

3 WAN Edges Bring Up Configuration & Registeration

3.1 Lab 10 – vEdges Bring Up CLI Configuration

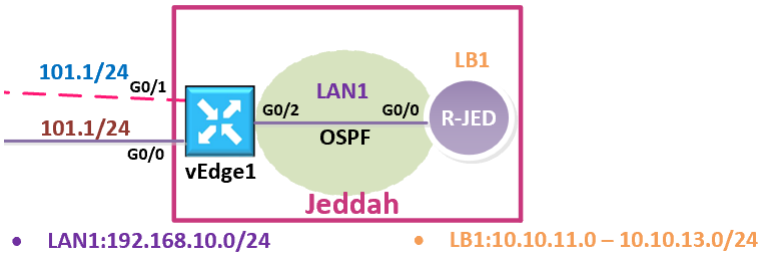
3.1.1 Step 0 – Upload the WAN Edge List

- 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.

Note: for all vEdges >> Default username: admin **Default password**: admin

---

vEdge-1



3.1.2 Step 1 – Configuring the System Component

- Configure the System parameters based on the following:
  - Host-name: vEdge1
  - Organization: TECTCAST
  - System-IP: 200.200.200.201
  - Site ID: 1
  - vbond Address: 212.1.1.3
  - Timezone: Select timezone based on your device location

```
vEdge1

config t
!
system
 host-name vEdge1
 system-ip 200.200.200.201
 site-id 1
 organization-name "viptela sdwan"
 clock timezone Asia/Riyadh
 vbond 212.1.1.3
!
 commit
```

3.1.3 Step 2 – Configure the VPN parameters

- Configure the VPN parameters based on the following:

VPN 0

- Interface ge0/0
- IP Address: 192.168.101.1/24
- Tunnel Interface
  - Encapsulation IPSec
  - Tunnel Services (All, NetConf, SSHD)
- Default Route: 192.168.101.254

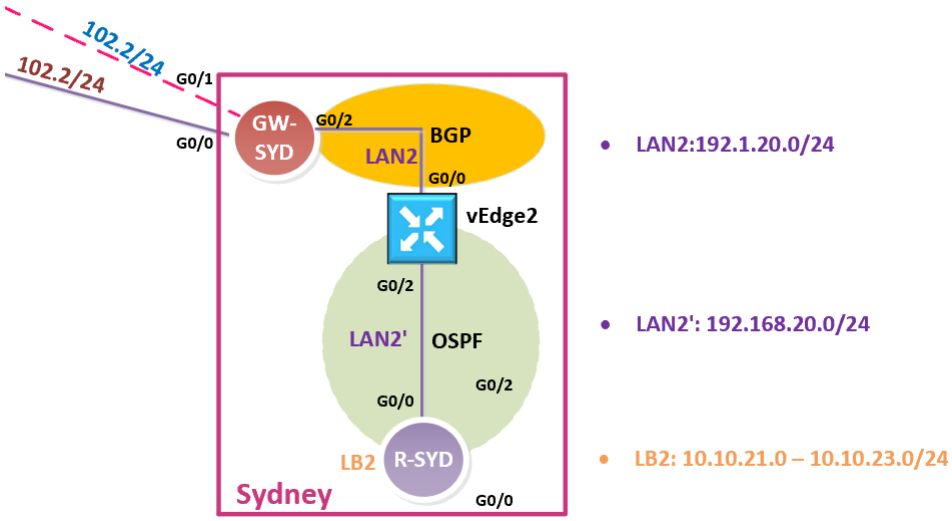
VPN 512

- Interface eth0
- IP Address: DHCP Client

vEdge1

```
config t
!
vpn 0
 no interface eth0
 interface ge0/0
  ip address 192.168.101.1/24
  tunnel-interface
  encapsulation ipsec
  allow-service all
  allow-service netconf
  allow-service sshd
  no shut
 ip route 0.0.0.0/0 192.168.101.254
!
vpn 512
interface eth0
 ip dhcp-client
 no shutdown
!
commit
```

vEdge2



3.1.4 Step 1 – Configuring the System Component

- Configure the System parameters based on the following:

- Host-name : vEdge2
- Organization: TECTCAST
- System-IP: 200.200.200.202
- Site ID: 2
- vbond Address: 212.1.1.3
- Timezone: Select timezone based on your device location

vEdge-2

```
config
 !
 system
  host-name vEdge2
  system-ip 200.200.200.202
  site-id 2
  organization-name "viptela sdwan"
  clock timezone Australia/Sydney
  vbond 212.1.1.3
 !
 commit
```

3.1.5 Step 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

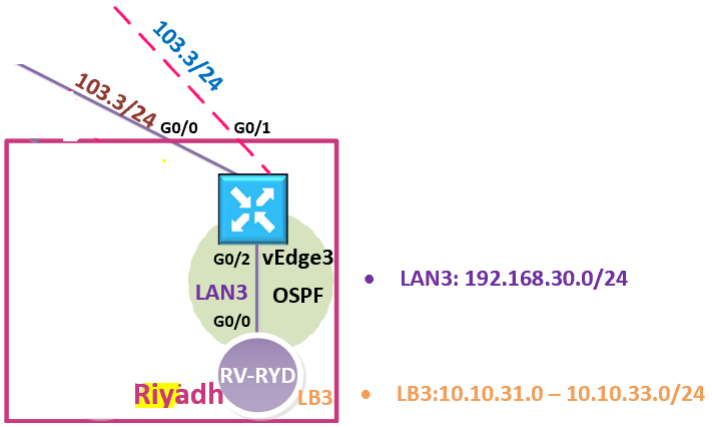
VPN 512

- Interface eth0
- IP Address: DHCP Client

vEdge2

```
config
!
 vpn 0
  no interface eth0
  interface ge0/0
   ip address 192.1.20.2/24
   tunnel-interface
   encapsulation ipsec
   allow-service all
   allow-service netconf
   allow-service sshd
   no shut
  ip route 0.0.0.0/0 192.1.20.254
 !
 vpn 512
  interface eth0
   ip dhcp-client
   no shutdown!
 commit
```

vEdge-3



3.1.6 Step 1 – Configuring the System Component

- Configure the System parameters based on the following:
  - HOST-NAME : VEDGE3
  - ORGANIZATION: TECTCAST

- System-IP: 200.200.200.203
- Site ID: 3
- vBond Address: 212.1.1.3
- Timezone: Select timezone based on your device location

vEdge-3

```
config
!
system
 host-name vEdge3
 system-ip 200.200.200.203
 site-id 3
 organization-name TECHCAST
 clock timezone Asia/Riyadh
 vbond 212.1.1.3
!
 Commit
```

3.1.7 Step 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

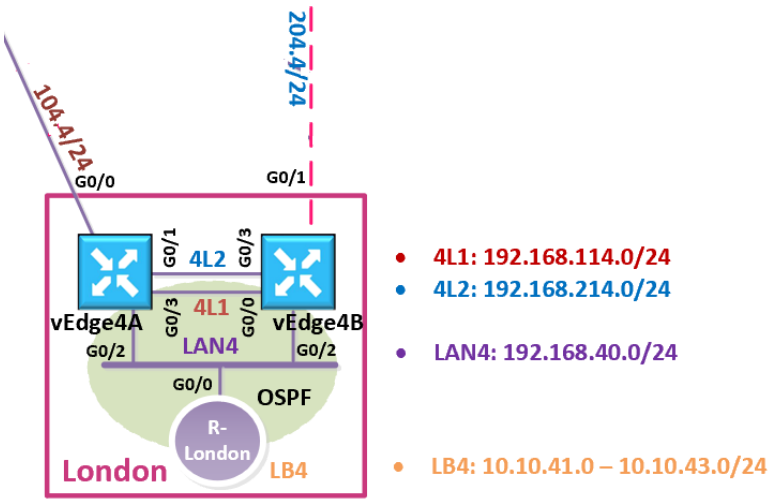
VPN 512

- 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-4A



3.1.8 Step 1 – Configuring the System Component

- Configure the System parameters based on the following:
  - Host-name : vEdge4A
  - Organization: TECTCAST
  - System-IP: 200.200.200.204
  - Site ID: 4
  - vbond Address: 212.1.1.3
  - Timezone: Select timezone based on your device location

vEdge-4A

```
config
!
system
 host-name vEdge4A
 system-ip 200.200.200.204
 site-id 4
 organization-name TECHCAST
 clock timezone Europe/London
 vbond 212.1.1.3
!
 Commit
```

3.1.9 Step 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

```
vEdge4A

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
```

vEdge-4B

3.1.10 Step 1 – Configuring the System Component

- Configure the System parameters based on the following:
  - Host-name : vEdge4B
  - Organization: TECTCAST
  - System-IP: 200.200.200.214
  - Site ID: 4
  - vbond Address: 212.1.1.3
  - Timezone: Select timezone based on your device location

```
vEdge-4B

config
!
system
 host-name vEdge4B
 system-ip 200.200.200.214
 site-id 4
 organization-name TECHCAST
 clock timezone Europe/London
 vbond 212.1.1.3
!
 Commit
```

3.1.11 Step 2 – Configure the vpn parameters

- Configure the VPN parameters based on the following:

VPN 0

- Interface ge0/1
- IP Address: 192.1.204.4/24
- Tunnel Interface
  - Encapsulation IPSec
  - Tunnel Services (All, NetConf, SSHD)
- Default Route: 192.1.204.254

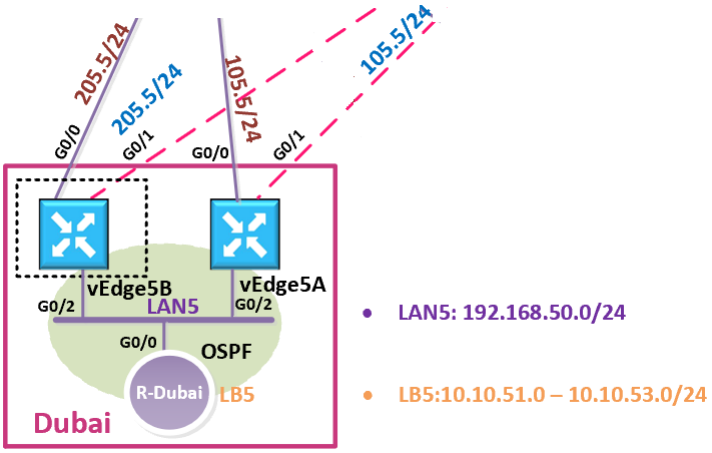
VPN 512

- Interface eth0
- IP Address: DHCP Client

vEdge4B

```
config
!
 vpn 0
  no interface ge0/0
  interface ge0/1
   ip address 192.1.204.4/24
   tunnel-interface
   encapsulation ipsec
   allow-service all
   allow-service netconf
   allow-service sshd
   no shut
  ip route 0.0.0.0/0 192.1.204.254
 !
 vpn 512
  interface eth0
   ip dhcp-client
   no shutdown
 !
 Commit
```

vEdge-5A



3.1.12 **Step 1 – Configuring the System Component**

- Configure the System parameters based on the following:
  - HOST-NAME : VEDGE5A

- Organization: TECTCAST
- System-IP: 200.200.200.205
- Site ID: 5
- vbond Address: 212.1.1.3
- Timezone: Select timezone based on your device location

vEdge-5A

```
config
!
system
 host-name vEdge5A
 system-ip 200.200.200.205
 site-id 5
 organization-name TECHCAST
 clock timezone Asia/Dubai
 vbond 212.1.1.3
!
 Commit
```

3.1.13 Step 2 – Configure the vpn parameters

- Configure the VPN parameters based on the following:

VPN 0

- Interface ge0/0
- IP Address: 192.168.105.5/24
- Tunnel Interface
  - Encapsulation IPSec
  - Tunnel Services (All, NetConf, SSHD)
- Default Route: 192.168.105.254

VPN 512

- Interface eth0
- IP Address: DHCP Client

vEdge5A

```
config t
!
vpn 0
 no interface eth0
 interface ge0/0
  ip address 192.168.105.5/24
   tunnel-interface
   encapsulation ipsec
  allow-service all
  allow-service
  netconf allow-
  service sshd
  no shut
 !
 ip route 0.0.0.0/0 192.168.105.254
!
vpn 512
interface eth0
 ip dhcp-client
 no shutdown
 !
 Commit
```

vEdge-5B

3.1.14 Step 1 – Configuring the System Component

- Configure the System parameters based on the following:
  - Host-name : vEdge5B
  - Organization: TECTCAST
  - System-IP: 200.200.200.215
  - Site ID: 5
  - vbond Address: 212.1.1.3
  - Timezone: Select timezone based on your device location

```
vEdge-5B

config
!
system
 host-name vEdge5B
 system-ip 200.200.200.215
 site-id 5
 organization-name TECHCAST
 clock timezone Asia/Dubai
 vbond 212.1.1.3
!
 Commit
```

3.1.15 Step 2 – Configure the vpn parameters

- Configure the VPN parameters based on the following:

VPN 0

- Interface ge0/0
- IP Address: 192.168.205.5/24
- Tunnel Interface
  - Encapsulation IPSec
  - Tunnel Services (All, NetConf, SSHD)
- Default Route: 192.168.205.254

VPN 512

- Interface eth0
- IP Address: DHCP Client

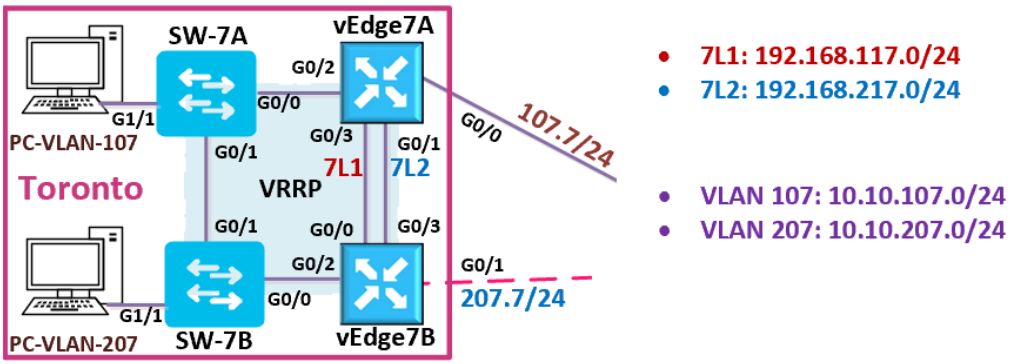
vEdge5B

```
config
!
vpn 0
 no interface eth0
 interface ge0/0
  ip address 192.168.205.5/24
   tunnel-interface
   encapsulation ipsec
  allow-service all
  allow-service
  netconf allow-
  service sshd
  no shut
!
 ip route 0.0.0.0/0 192.168.205.254
!
vpn 512
 interface eth0
 ip dhcp-client
 no shutdown
 !
 Commit
```

vEdge-6

بالنسبة لتجهيز vEdge6 سنقوم بتأجيل هذه الخطوة وحيكون لها للاب منفصل لأنه محتاجين نقوم ببعض الكونفقريشن على الرواتر الخارجي GW-Cairo واللي من خلاله سيسمح لجهاز vEdge6 بامكانية التسجيل مع vManage بكل سهولة ويسر.

vEdge-7A



3.1.16 Step 1 – Configuring the System Component

- Configure the System parameters based on the following:
  - Host-name : vEdge7A
  - Organization: TECTCAST
  - System-IP: 200.200.200.207
  - Site ID: 7
  - vbond Address: 212.1.1.3
  - Timezone: Select timezone based on your device location

vEdge-7A

```
config
!
system
 host-name vEdge7A
 system-ip 200.200.200.207
 site-id 7
 organization-name TECHCAST
 clock timezone America/Toronto
 vbond 212.1.1.3
!
 Commit
```

3.1.17 Step 2 – Configure the vpn parameters

- Configure the VPN parameters based on the following:

VPN 0

- Interface ge0/0
- IP Address: 192.168.107.7/24
- Tunnel Interface
  - Encapsulation IPSec
  - Tunnel Services (All, NetConf, SSHD)
- Default Route: 192.168.107.254

VPN 512

- Interface eth0
- IP Address: DHCP Client

vEdge7A

```
config t
!
vpn 0
 no interface eth0
  interface ge0/0
   ip address 192.168.107.7/24
   tunnel-interface
   encapsulation ipsec
  allow-service all
  allow-service
  netconf allow-
  service sshd
  no shut
 !
 ip route 0.0.0.0/0 192.168.107.254
!
vpn 512
 interface eth0
 ip dhcp-client
 no shutdown
 !
 Commit
```

vEdge-7B

3.1.18 Step 1 – Configuring the System Component

- Configure the System parameters based on the following:
  - Host-name : vEdge7B
  - Organization: TECTCAST
  - System-IP: 200.200.200.217
  - Site ID: 7
  - vbond Address: 212.1.1.3
  - Timezone: Select timezone based on your device location

```
vEdge-7B

config
!
system
 host-name vEdge7B
 system-ip 200.200.200.217
 site-id 7
 organization-name TECHCAST
 clock timezone America/Toronto
 vbond 212.1.1.3
!
 Commit
```

3.1.19 Step 2 – Configure the VPN parameters

- Configure the VPN parameters based on the following:

VPN 0

- Interface ge0/1
- IP Address: 192.1.207.7/24
- Tunnel Interface
  - Encapsulation IPSec
  - Tunnel Services (All, NetConf, SSHD)
- Default Route: 192.1.207.254

VPN 512

- Interface eth0
- IP Address: DHCP Client

vEdge7B

```
config
!
vpn 0
 no interface eth0
  interface ge0/1
  ip address 192.1.207.7/24
  tunnel-interface
  encapsulation ipsec
   allow-service all
   allow-service netconf
   allow-service sshd
   no shut
 !
 ip route 0.0.0.0/0 192.1.207.254
!
vpn 512
 interface eth0
 ip dhcp-client
 no shutdown
 !
 Commit
```

3.2 Lab 11 – vEdges Registeration

3.2.1 Step 0 – Upload the WAN Edges licenses

- مثل ماذكرنا من خلال الفيديو الخاص بهذا اللاب. هناك طريقتن لتسجيل WAN Edges أما بطريقة يدوية أو عن طريق ZTP/PnP.
- في كتابنا العملي, حنتبع الطريقة اليدوية في عملية التسجيل وذلك باتباع الخطوات التالية:
  - من حسابك Cisco Smart account قم بتنزيل الملف الخاص بالتراخيص التي تم شراؤها من شركة سيسكو كملف Viptela.Serial
  - من خلال جهاز vManage, قم برفع هذا الملف بنفس الطريقة المتبعة في الفيديو الخاص بهذا اللاب
  - اتبع الخطوات التالية في اكمال عملية التسجيل لجميع أجهزة WAN Edges

vEdge-1

3.2.2 Step 1 – Upload the Root Certificate to the vEdge

- On the Windows Server, open **WINSCP** application.
- **Connect** to vEdge1 using the following information:
  - IP ADDRESS : 192.168.101.1
  - PROTOCOL - SFTP
  - USERNAME : ADMIN
  - PASSWORD : ADMIN
- Copy the **RootCert.cer** file from the Downloads folder to the **/home/admin** folder on the vEdge1

3.2.3 Step 1' – This is another way to upload RootCert.cer to the vEdge

- On the Windows Server, open **RootCer.cer** file we saved in CA folder
- Righ-click on it and open it using notepad
- Copy using **CTRL-A** and **CTRL-C**.
- Go to vEdge-1

- In exec-mode; to enter vshell mode >> Type "**vshell**" and enter
- Type "**vim RootCert.cer**" and click enter
- Click letter " **i** " and click enter
- Paste the **RootCert** using **CTRL-V**
- Click "**Esc**" key and the type " **:wq** " and click enter
- Type "**exit** " and enter to exit vshell mode.

3.2.4 Step 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

3.2.5 Step 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 XYZ token XYZ

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

---

vEdge-2

3.2.6 Step 1 – Upload the Root Certificate to the vEdge

- On the Windows Server, open **WINSCP** application.
- **Connect** to vEdge2 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

3.2.7 Step 1' – This is another way to upload RootCert.cer to the vEdge

- On the Windows Server, open **RootCert.cer** file we saved in CA folder
- Righ-click on it and open it using notepad
- Copy using **CTRL-A** and **CTRL-C**.
- Go to vEdge- 2
    - In exec-mode; to enter vshell mode >> Type "**vshell**" and enter
    - Type "**vim RootCert.cer**" and click enter
    - Click letter " **i** " and click enter
    - Paste the **RootCert** using **CTRL-V**
    - Click "**Esc**" key and the type " **:wq** " and click enter
    - Type " **exit** " and enter to exit vshell mode.

3.2.8 Step 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

3.2.9 Step 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 XYZ token XYZ

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

---

vEdge-3

3.2.10 Step 1 – Upload the Root Certificate to the vEdge

- On the Windows Server, open **WINSCP** application.
- **Connect** to vEdge3 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.

3.2.11 Step 1' – This is another way to upload RootCert.cer to the vEdge

- On the Windows Server, open **RootCert.cer** file we saved in CA folder
- Righ-click on it and open it using notepad
- Copy using **CTRL-A** and **CTRL-C**.
- Go to vEdge-3
  - In exec-mode; to enter vshell mode >> Type "**vshell**" and enter
  - Type "**vim RootCert.cer**" and click enter
  - Click letter " **i** " and click enter
  - Paste the **RootCert** using **CTRL-V**
  - Click "**Esc**" key and the type " **:wq** " and click enter
  - Type " **exit** " and enter to exit vshell mode.

3.2.12 Step 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

3.2.13 Step 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 XYZ token XYZ

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

---

vEdge-4A

3.2.14 Step 1 – Upload the Root Certificate to the vEdge

- On the Windows Server, open **WINSCP** application.

- **Connect** to vEdge-4A 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 vEdge-4A

3.2.15 Step 1' – This is another way to upload RootCert.cer to the vEdge

- On the Windows Server, open **RootCert.cer** file we saved in CA folder
- Righ-click on it and open it using notepad
- Copy using **CTRL-A** and **CTRL-C**.
- Go to vEdge-4A
  - In exec-mode; to enter vshell mode >> Type "**vshell**" and enter
  - Type "**vim RootCert.cer**" and click enter
  - Click letter " **i** " and click enter
  - Paste the **RootCert** using **CTRL-V**
  - Click "**Esc**" key and the type " **:wq** " and click enter
  - Type " **exit** " and enter to exit vshell mode.

3.2.16 Step 2 – Install the Root Certificate on vEdge-4A

- Connect to the console of vEdge4A and issue the following command:

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

3.2.17 Step 3 - Activate vEdge on vManage

- Navigate to **Configuration -> Devices**
- Note and use the **Chassis Number** and **Token number** for vEdge-4A from vManage.
- Use the information from the previous step in the following command on the vEdge4A console.

request vedge-cloud activate chassis-number XYZ token XYZ

- You should see the vEdge4A in the vManage console with a Certificate issued.

vEdge-4B

3.2.18 Step 1 – Upload the Root Certificate to the vEdge

- On the Windows Server, open **WINSCP** application.
- **Connect** to vEdge-4B using the following information:
  - IP ADDRESS : 192.1.204.4
  - PROTOCOL - SFTP
  - USERNAME : ADMIN
  - PASSWORD : ADMIN
- Copy the **RootCert.cer** file from the Downloads folder to the **/home/admin** folder on the vEdge-4B

3.2.19 Step 1' – This is another way to upload RootCert.cer to the vEdge

- On the Windows Server, open **RootCert.cer** file we saved in CA folder
- Righ-click on it and open it using notepad
- Copy using **CTRL-A** and **CTRL-C**.
- Go to vEdge-4B
  - In exec-mode; to enter vshell mode >> Type "vshell" and enter
  - Type "**vim RootCert.cer**" and click enter
  - Click letter " **i** " and click enter
  - Paste the **RootCert** using **CTRL-V**
  - Click "**Esc**" key and the type " **:wq** " and click enter
  - Type " **exit** " and enter to exit vshell mode.

3.2.20 Step 2 – Install the Root Certificate on vEdge-4B

- Connect to the console of vEdge4B and issue the following command:

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

3.2.21 Step 3 - Activate vEdge on vManage

- Navigate to **Configuration -> Devices**
- Note and use the **Chassis Number** and **Token number** for vEdge-4B from vManage.
- Use the information from the previous step in the following command on the vEdge4B console.

request vedge-cloud activate chassis-number XYZ token XYZ

- You should see the vEdge4B in the vManage console with a Certificate issued.

---

vEdge-5A

3.2.22 Step 1 – Upload the Root Certificate to the vEdge

- On the Windows Server, open **WINSCP** application.
- **Connect** to vEdge-5A using the following information:
  - IP ADDRESS : 192.168.105.5
  - PROTOCOL - SFTP
  - USERNAME : ADMIN
  - PASSWORD : ADMIN
- Copy the **RootCert.cer** file from the Downloads folder to the **/home/admin** folder on the vEdge-5A

3.2.23 Step 1' – This is another way to upload RootCert.cer to the vEdge

- On the Windows Server, open **RootCert.cer** file we saved in CA folder
- Righ-click on it and open it using notepad
- Copy using **CTRL-A** and **CTRL-C**.
- Go to vEdge-5A
  - In exec-mode; to enter vshell mode >> Type "**vshell**" and enter
  - Type "**vim RootCert.cer**" and click enter
  - Click letter " **i** " and click enter
  - Paste the **RootCert** using **CTRL-V**
  - Click "**Esc**" key and the type " **:wq** " and click enter
  - Type " **exit** " and enter to exit vshell mode.

3.2.24 Step 2 – Install the Root Certificate on vEdge-5A

- Connect to the console of vEdge5A and issue the following command:

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

3.2.25 Step 3 - Activate vEdge on vManage

- Navigate to **Configuration -> Devices**
- Note and use the **Chassis Number** and **Token number** for vEdge-5A from vManage.
- Use the information from the previous step in the following command on the vEdge5A console.

request vedge-cloud activate chassis-number XYZ token XYZ

- You should see the vEdge-5A in the vManage console with a Certificate issued.

---

vEdge-5B

3.2.26 Step 1 – Upload the Root Certificate to the vEdge

- On the Windows Server, open **WINSCP** application.
- **Connect** to vEdge-5B using the following information:
  - IP ADDRESS : 192.168.205.5
  - PROTOCOL - SFTP
  - USERNAME : ADMIN
  - PASSWORD : ADMIN
- Copy the **RootCert.cer** file from the Downloads folder to the **/home/admin** folder on the vEdge-5B

3.2.27 Step 1' – This is another way to upload RootCert.cer to the vEdge

- On the Windows Server, open RootCert.cer file we saved in CA folder
- Righ-click on it and open it using notepad
- Copy using CTRL-A and CTRL-C.
- Go to vEdge-5B

- In exec-mode; to enter vshell mode >> Type "**vshell**" and enter
- Type "**vim RootCert.cer**" and click enter
- Click letter " **i** " and click enter
- Paste the **RootCert** using **CTRL-V**
- Click "**Esc**" key and the type " **:wq** " and click enter
- Type " **exit** " and enter to exit vshell mode.

3.2.28 Step 2 – Install the Root Certificate on vEdge-5B

- Connect to the console of vEdge-5B and issue the following command:

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

3.2.29 Step 3 - Activate vEdge on vManage

- Navigate to **Configuration -> Devices**
- Note and use the **Chassis Number** and **Token number** for vEdge-5B from vManage.
- Use the information from the previous step in the following command on the vEdge5B console.

request vedge-cloud activate chassis-number XYZ token XYZ

- You should see the vEdge-5B in the vManage console with a Certificate issued.

---

vEdge-7A

3.2.30 Step 1 – Upload the Root Certificate to the vEdge

- On the Windows Server, open **WINSCP** application.
- **Connect** to vEdge-7A using the following information:
  - IP Address : 192.168.107.7
  - Protocol - SFTP
  - Username : admin
  - Password : admin
- Copy the **RootCert.cer** file from the Downloads folder to the **/home/admin** folder on the vEdge-7A

3.2.31 Step 1' – This is another way to upload RootCert.cer to the vEdge

- On the Windows Server, open **RootCert.cer** file we saved in CA folder
- Righ-click on it and open it using notepad
- Copy using **CTRL-A** and **CTRL-C**.
- Go to vEdge-7A
  - In exec-mode; to enter vshell mode >> Type "vshell" and enter
  - Type "**vim RootCert.cer**" and click enter
  - Click letter " **i** " and click enter
  - Paste the **RootCert** using **CTRL-V**
  - Click "**Esc**" key and the type " **:wq** " and click enter
  - Type " **exit** " and enter to exit vshell mode.

3.2.32 Step 2 – Install the Root Certificate on vEdge-7A

- Connect to the console of vEdge7A and issue the following command:

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

3.2.33 Step 3 - Activate vEdge on vManage

- Navigate to **Configuration -> Devices**
- Note and use the **Chassis Number** and **Token number** for vEdge-7A from vManage.
- Use the information from the previous step in the following command on the vEdge7A console.

request vedge-cloud activate chassis-number XYZ token XYZ

- You should see the vEdge7A in the vManage console with a Certificate issued.

---

vEdge-7B

3.2.34 Step 1 – Upload the Root Certificate to the vEdge

- On the Windows Server, open **WINSCP** application.
- **Connect** to vEdge-7B using the following information:

- IP ADDRESS : 192.1.207.7
- PROTOCOL - SFTP
- USERNAME : ADMIN
- PASSWORD : ADMIN

- Copy the **RootCert.cer** file from the Downloads folder to the **/home/admin** folder on the vEdge-7B

3.2.35 Step 1' – This is another way to upload RootCert.cer to the vEdge

- On the Windows Server, open **RootCert.cer** file we saved in CA folder
- Righ-click on it and open it using notepad
- Copy using **CTRL-A** and **CTRL-C**.
- Go to vEdge-7B
  - In exec-mode; to enter vshell mode >> Type "**vshell**" and enter
  - Type "**vim RootCert.cer**" and click enter
  - Click letter " **i** " and click enter
  - Paste the **RootCert** using **CTRL-V**
  - Click "**Esc**" key and the type " **:wq** " and click enter
  - Type " **exit** " and enter to exit vshell mode.

3.2.36 Step 2 – Install the Root Certificate on vEdge-7B

- Connect to the console of vEdge7B and issue the following command:

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

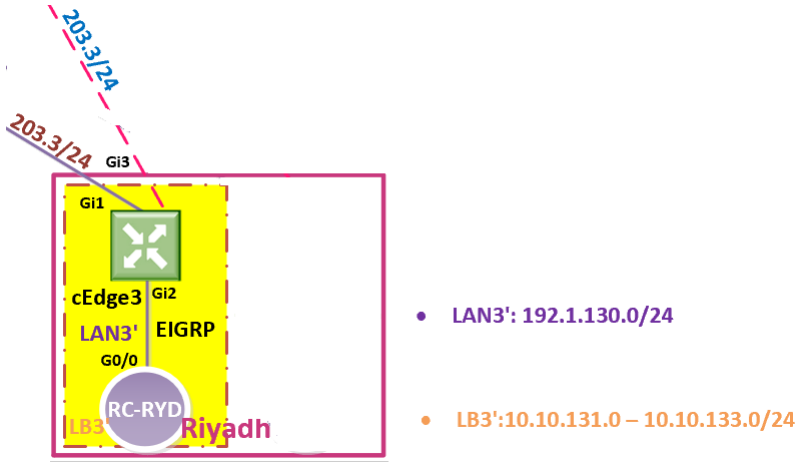
3.2.37 Step 3 - Activate vEdge on vManage

- Navigate to **Configuration -> Devices**
- Note and use the **Chassis Number** and **Token number** for vEdge-7B from vManage.
- Use the information from the previous step in the following command on the vEdge7B console.

request vedge-cloud activate chassis-number XYZ token XYZ

- You should see the vEdge7B in the vManage console with a Certificate issued.

3.3 Lab 12 – cEdges Bring Up CLI Configuration



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

cEdge-3

3.3.1 Step 1 – Configuring the System Component

- Configure the System parameters based on the following:
  - HOST-NAME : CEDGE3
  - ORGANIZATION: TECTCAST
  - SYSTEM-IP: 200.200.200.213
  - SITE ID: 13
  - VBOND ADDRESS: 212.1.1.3
  - TIMEZONE: SELECT TIMEZONE BASED ON YOUR DEVICE LOCATION

cEdge3

```
config-transaction
!
hostname cEdge3
!
system
 system-ip 200.200.200.213
 site-id 13
 organization-name TECHCAST
 vbond 212.1.1.3
 exit
!
clock timezone GST 1
commit
```

3.3.2 Step 2 – Configure the Interface and Tunnel Parameters

- Configure the Interface parameters based on the following:
  - **GigabitEthernet1 Interface**
    - IP Address: 192.168.203.13/24
    - Default Route: 192.168.203.254
  - **Tunnel Interface**
    - Tunnel Interface: Tunnel1
    - Tunnel Source: GigabitEthernet1
    - Tunnel Mode: SDWAN
  - **SDWAN Interface**
    - Interface: GigabitEthernet1
    - Encapsulation: IPSec
    - Color: default
    - Tunnel Services (All, NetConf, SSHD)

cEdge3

```
config-transaction
!
interface GigabitEthernet1
 no shutdown
 ip address 192.168.203.13 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 192.168.203.254
!
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
```

3.4 Lab 13 – cEdges Registeration

3.4.1 Step 1 – Upload the Root Certificate to the cEdge

- Open the **FTP Application** on the Windows Server.
- Configure the Default Folder as the **Downloads** Folder and using the 212.1.1.5 **(Windows Server)** as the FTP Interface.
- Connect to the console of cEdge3 and copy the RootCert.cer file to flash: using the following command:

copy ftp://212.1.1.5/RootCert.cer flash:

3.4.2 Step 2 – Install the Root Certificate on cEdge3

- Connect to the console of cEdge3 and issue the following command:

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

3.4.3 Step 3 - Activate cEdge on vManage

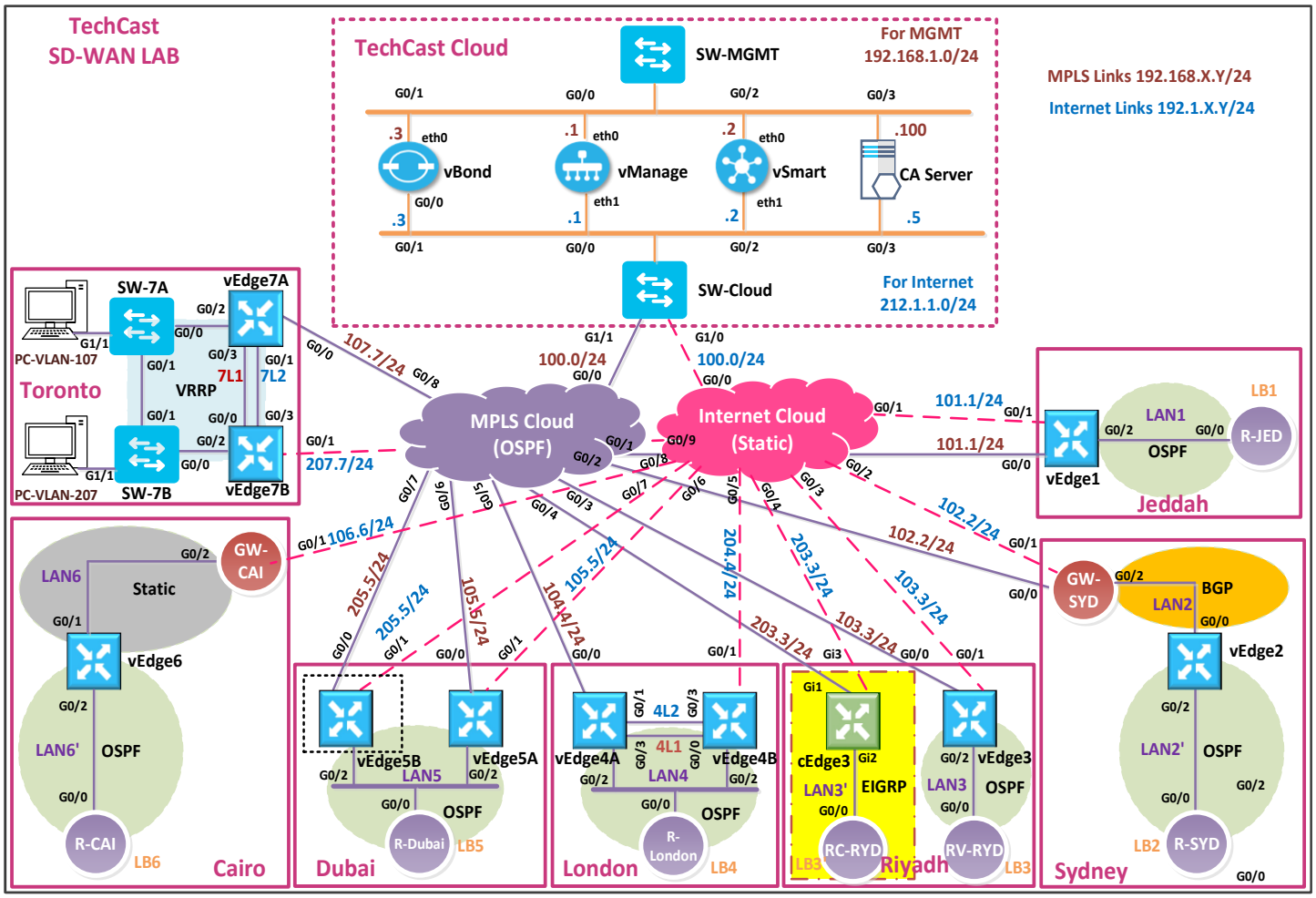
- Navigate to **Configuration -> Devices**
- Note and use the **Chassis Number** and **Token number** for the 1st CSR Device (cEdge3) from vManage.
- Use the information from the previous step in the following command on the cEdge3 console.

request platform software sdwan vedge_cloud activate chassis- number CSR-XYZ token XYZ

- You should see the cEdge3 in the vManage console with a Certificate issued.

4 Feature & Device Templates Configuration

4.1 Lab 14 – System - Feature Template



4.1.1 Step 1 – Configure the System Template to be used by all cEdge-Cloud Device

- 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 (bps) -> Default

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

4.1.2 Step 2 – Configure the System Template to be used by cEdge- Cloud Device

- In vManage, Navigate to Configuration.

- Configure the System parameters based on the following:

  - Template Name: **CE-System**
  - Description: **CE-System**
  - Site ID -> 3
  - System IP -> Device Specific
  - Hostname -> Device Specific
  - Timezone -> Asia/Riyadh

- Click **Save** to save the Template

4.2 Lab 15 – Banner - Feature Template

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

- In vManage, Navigate to Configuration.

- Configure the Banner parameters based on the following:
  - TEMPLATE NAME : **VE-BANNER**
  - DESCRIPTION : **VE-BANNER**
  - BANNER: **TECTCAST AUTHORIZED USERS ONLY!**
  - MOTD: **WELCOME OF SD-WAN LAB!**
- Click **Save** to save the Template.

4.2.2 Step 2 – Configure the Banner Template to be used by cEdge- Cloud Device

- In vManage, Navigate to Configuration.

- Configure the Banner parameters based on the following:
  - TEMPLATE NAME : **CE-BANNER**
  - DESCRIPTION : **CE-BANNER**
  - BANNER: **TECTCAST AUTHORIZED USERS ONLY!**
  - MOTD: **WELCOME OF SD-WAN LAB!**
- Click **Save** to save the Template.

4.3 Lab 16 – VPN0 & VPN512 - Feature Template (VEs)

4.3.1 Step 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: **VE-VPN-VPN0**
  - Description: **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.

4.3.2 Step 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 : **VE-VPN-VPN512**
  - Description : **VE-VPN-VPN512**

Basic Configuration

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

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

4.3.3 Step 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 : **VE-VPN0-IF-G0/0**
  - Description : **VE-VPN0-IF-G0/0**

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.

4.3.4 Step 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 : **VE-VPN0-IF-G0/1**
  - Description : **VE-VPN0-IF-G0/1**

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.

4.3.5 Step 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.

- Configure the VPN parameters based on the following:

  - Template Name : **VE-VPN512-IF-E0**
  - Description : **VE-VPN512-IF-E0**

Basic Configuration

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

- Click **Save** to save the Template

4.4 Lab 17 – VPN0 External Routing - Feature Template (VEs)

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

- In vManage, Navigate to Configuration.

- Configure the OSPF parameters based on the following:
  - TEMPLATE NAME : **VE-VPN0-OSPF**
  - DESCRIPTION : **VE-VPN0-OSPF**

Area Configuration

  - AREA NUMBER -> GLOBAL : **0**
  - AREA TYPE -> DEFAULT

INTERFACE CONFIGURATION

  - INTERFACE NAME: **GE0/0**

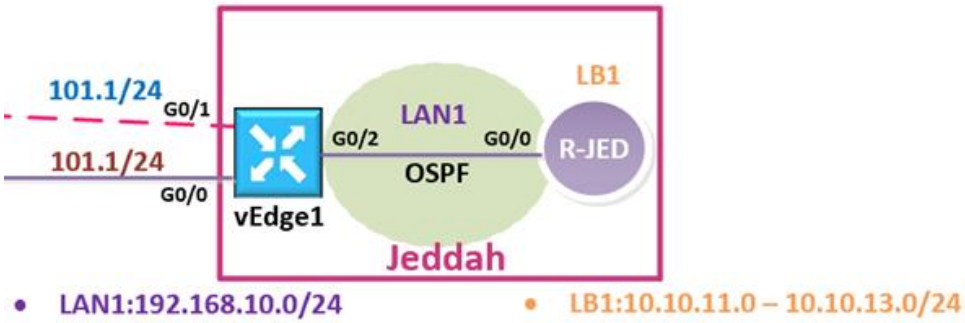
- Click **Add** to add the Interface and Click **Add** to add OSPF.

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

ملاحظة: كل اللي سويناه حتى الأن في هذا اللاب هو الكونفقريشن الأساسي لاضافة وتشغيل برتوكول OSPF ولكن تقدر تعمل كونفقريشن للخصائص الأخرى لبرتوكول OSPF مثل OSPF network Type, Area Type وغيرها حسب التصميم الخاص بشبكتك. أقتراحنا دائما أنه تبدأ بالكونفقريشن الأساسية والغير معقده وبعد ماتتأكد أنه كل شي شغال أبدء في التدرج في أستخدام الأعدادت الأخرى الأكثر صعوبة .

ملاحظة: تذكر دائما عندما تقوم بهذه الأعدادت advanced, على سبيل المثال عندما تختار OSPF Type تكون"point-to-point" . تأكد بأن تجعل كل interfaces المتصلة ببعضها نفس OSPF Type .

4.5 Lab 18 – Configuring & Deploying - Device Template (Jeddah vEdge1)



4.5.1 Step 1 – Configure a Device Template for Branch vEdge Devices.

- In vManage, Navigate to Configuration.

Templates → Device → Create Template → From Feature Template → vEdge Cloud

- Configure the Device Template based on the following:
  - TEMPLATE NAME : **VE-DEV-TEMP**
  - DESCRIPTION : **VE-DEV-TEMP**

Basic Information

  - SYSTEM -> **VE-SYSTEM**

Transport & Management

  - VPN 0: **VE-VPN-VPN0**
  - VPN INTERFACE: **VE-VPN0-IF-G0/0**
  - VPN INTERFACE: **VE-VPN0-IF-G0/1**
  - OSPF: **VE-VPN0-OSPF**

  - VPN 512: **VE-VPN-VPN512**
  - VPN INTERFACE: **VE-VPN512-IF-E0**

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

4.5.2 Step 2 – Attach vEdge1 to the Device Template

- In vManage, Navigate to Configuration.

Templates > **Device** > **VE-DEV-TEMP**

- Click on "**…**" towards the right-hand side.
- Click **Attach Devices.**
- Select **vEdge1** and click the " **->** " button.
- Click **Attach**.

4.5.3 Step 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:
  - DEFAULT GATEWAY FOR VPN0 : **192.1.101.254**
  - INTERFACE IP FOR GE0/1 :**192.1.101.1/24**
  - INTERFACE IP FOR GE0/0 :**192.168.101.1/24**
  - HOSTNAME : **VEDGE-1**
  - SYSTEM IP : **200.200.200.201**
  - 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 MPLS Router by issuing the **Show ospf neighbor** command on **vEdge1.**
- Type **Show Ip route** on **vEdge1** to verify that you are receiving OSPF routes from the MPLS Router.

4.6 Lab 19 – Service VPN & Internal Routing - Feature Template (VEs)

4.6.1 Step 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 : **VE-VPN-VPN1**
  - Description : **VE-VPN-VPN1**

Basic Configuration

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

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

4.6.2 Step 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 : **VE-VPN1-IF-G0/2**
  - Description : **VE-VPN1-IF-G0/2**

Basic Configuration

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

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

4.6.3 Step 3 –Configure a VPN 1 Interface Template for Interface LoopBack1 which would be used for Testing purposed.

ملاحظة: هذه الخطوة أختيارية ولكن الهدف من استخدامها هنا لأنه نبغى نستخدمها في اللاب الخاص ب **AAR policy (Application Aware Routing)**

- In vManage, Navigate to Configuration.

Templates > **Feature** > **vEdge Cloud** > **VPN** > **VPN Interface Ethernet**

- Configure the VPN parameters based on the following:
  - TEMPLATE NAME : **VE-VPN1-IF-LB1**
  - DESCRIPTION : **VE-VPN1-IF-LB1**

Basic Configuration

  - SHUTDOWN -> GLOBAL : **NO**
  - INTERFACE NAME -> GLOBAL : **LOOPBACK1**
  - IPV4 ADDRESS -> STATIC -> DEVICE SPECIFIC

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

4.6.4 Step 4 – Configure a Internal Routing-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 : **VE-VPN1-OSPF**
  - DESCRIPTION : **VE-VPN1-OSPF**

Redistribution

  - PROTOCOL : **OMP**

Area Configuration

  - AREA NUMBER -> GLOBAL : **0**
  - AREA TYPE -> DEFAULT

INTERFACE CONFIGURATION

- INTERFACE NAME: **GE0/2**
- INTERFACE NAME: **LOOPBACK1**

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

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

ملاحظة: كل اللي سويناه حتى الأن في هذا اللاب هو الكونفقريشن الأساسي لاضافة وتشغيل برتوكول OSPF ولكن تقدر تعمل كونفقريشن للخصائص الأخرى لبرتوكول OSPF مثل OSPF network Type, Area Type وغيرها حسب التصميم الخاص بشبكتك. أقتراحنا دائما أنه تبدأ بالكونفقريشن الأساسية والغير معقده وبعد ماتتأكد أنه كل شي شغال أبدء في التدرج في أستخدام الأعدادت الأخرى الأكثر صعوبة .

ملاحظة: تذكر دائما عندما تقوم بهذه الأعدادت advanced, على سبيل المثال عندما تختار OSPF Type تكون"point-to-point" . تأكد بأن تجعل كل interfaces المتصلة ببعضها نفس OSPF Type .

4.7 Lab 20 – Deploying Service VPN - Device Template (Jeddah vEdge1)

4.7.1 Step 1 – Edit the VE-DEV-TEMP Device Template for Branch vEdge Devices

- In vManage, Navigate to Configuration.

Templates > **Device** > **VE-DEV-TEMP** > **"..."** > **Edit**

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

Service VPN

- VPN 1 : **VE-VPN-VPN1**
- VPN INTERFACE : **VE-VPN1-IF-G0/2**
- VPN INTERFACE : **VE-VPN1-IF-LB1**
- OSPF : **VE-VPN1-OSPF**

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

4.7.2 Step 2 – 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.**

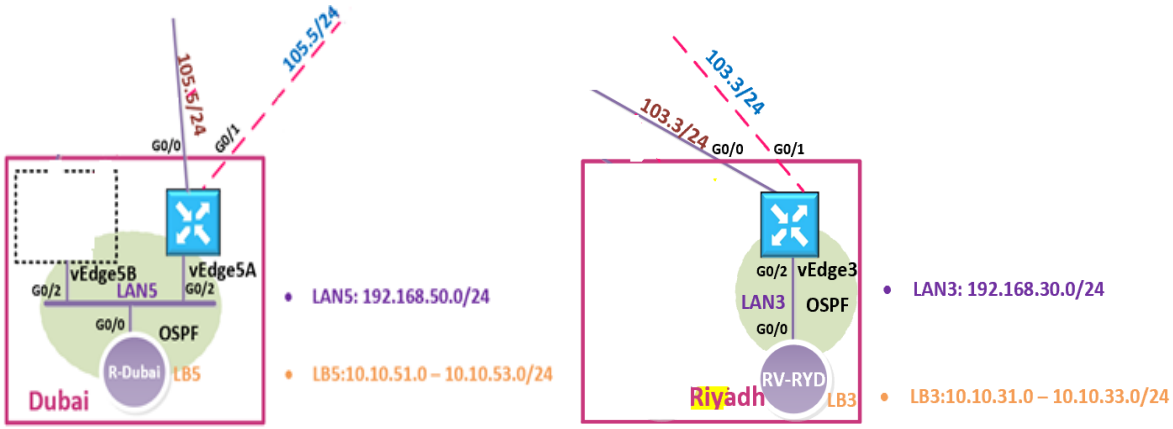
- Configure the variables based on the following:

  - INTERFACE IP FOR GE0/2 :**192.168.10.1/24**
  - INTERFACE IP FOR LOOPBACK1 :**1.1.1.1/32**

- 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 R-Jeddah Router by issuing the **Show ospf neighbor** command on **vEdge1.**
- Type **Show Ip route** on **vEdge1** to verify that you are receiving OSPF routes from the Internal Site Router.

4.8 Lab 21 – Attach Device Template to other Sites VEs (vEdge3/vEdge5A)



4.8.1 Step 1 – Attach the VE-DEV-TEMP Device Template for Branch vEdge Devices

- In vManage, Navigate to Configuration.

Templates → Device → VE-DEV-TEMP → "..." → Attach Devices

- Click **Attach Devices.**
- Select **vEdge3 & vEdge5A** and click the " **->** " button.
- Click **Attach**.
- **vEdge3 & vEdge5A** 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 :**192.168.30.3/24**
- DEFAULT GATEWAY FOR VPN0 : **192.1.103.254**
- INTERFACE IP FOR LOOPBACK1 :**3.3.3.3/32**
- INTERFACE IP FOR GE0/1 :**192.1.103.3/24**
- INTERFACE IP FOR GE0/0 :**192.168.103.3/24**
- HOSTNAME : **VEDGE-3**
- SYSTEM IP : **200.200.200.203**
- SITE ID : **3**

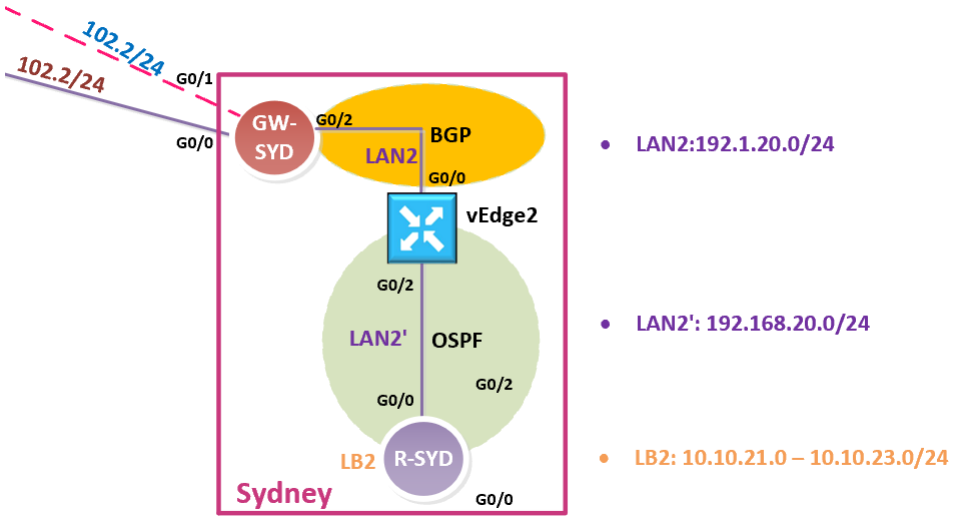
- Click **Update.**

Vedge-5A

- Interface IP for ge0/2 :**192.168.50.5/24**
- Default Gateway for VPN0 : **192.1.105.254**
- Interface IP for Loopback1 :**5.5.5.5/32**
- Interface IP for ge0/1 :**192.1.105.5/24**
- Interface IP for ge0/0 :**192.168.105.5/24**
- Hostname : **vEdge-5A**
- System IP : **200.200.200.205**
- 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 **vEdge3 & vEdge5A**. You can do that by verify OSPF Neighbor relationship with the Internal Site Router and MPLS-Cloud 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 as "OE2".
- Verify reachability between the sites by Pinging the Internal Loopback to Loopback network in the other sites.

4.9 Lab 22 – VPN0, VPN512 & its Routing - Feature Template (Sydney vEdge2)



في هذا اللاب نحتاج فقط لانشاء two more template for VPN0 وهي External Routing Protocol-BGP و Interface G0/0 Templates. ثم نقوم باعادة استخدام الـ Templates الأخرى التي تم انشائها مسبقا مثل VPN0, VPN512 and VPN1 templates كما هي ولكن كمراجعة لنا, حنقوم بانشاء Templates خاصة بموقعنا في Sydney .

VPN 0

4.9.1 Step 1 – Configure a VPN Template for SYDNEY 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 : **SYD-VE-VPN-VPN0**
  - DESCRIPTION : **SYD-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.

4.9.2 Step 2 – Configure a VPN Interface Template to be used by TechCast SYDNEY vEdge-Cloud Devices for VPN 0 for Interface G0/0

- In vManage, Navigate to Configuration.

- Configure the VPN parameters based on the following:

  - Template Name : **SYD-VE-VPN0-IF-G0/0**
  - Description : **SYD-VE-VPN0-IF-G0/0**

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.

4.9.3 Step 3 – Configure a BGP Template to be used by TechCast SYDNEY 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 : **SYD-VE-VPN0-BGP**
  - Description : **SYD-VE-VPN0-BGP**

Basic Configuration

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

Neighbor

  - Adddress -> Global : **192.1.20.254**
  - Remote AS -> Global : **65001**
  - Address Family -> Global : **On**
  - Address Family -> Global : **IPv4-Unicast**

- Click **Add** to add BGP Neighbor.
- Click **Save** to save the Template.

VPN 512

4.9.4 Step 1 – Configure a VPN Template to be used by TechCast SYDNEY 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 : **SYD-VE-VPN-VPN512**
  - Description : **SYD-VE-VPN-VPN512**

Basic Configuration

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

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

4.9.5 Step 2 – Configure a VPN Interface Template to be used by TechCast SYDNEY 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 : **SYD-VE-VPN512-IF-E0**
  - Description : **SYD-VE-VPN512-IF-E0**

Basic Configuration

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

- Click **Save** to save the Template

VPN 1

4.9.6 Step 1 – Configure a VPN Template for TechCast SYDNEY 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 : **SYD-VE-VPN-VPN1**
  - Description : **SYD-VE-VPN-VPN1**

Basic Configuration

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

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

4.9.7 Step 2 – Configure a VPN Interface Template to be used by TechCast SYDNEY vEdge-Cloud Devices for VPN 1 for Interface G0/2

- In vManage, Navigate to Configuration.

- Configure the VPN parameters based on the following:
  - TEMPLATE NAME : **SYD-VE-VPN1-IF-G0/2**
  - DESCRIPTION : **SYD-VE-VPN1-IF-G0/2**

Basic Configuration

  - SHUTDOWN -> GLOBAL : **NO**
  - INTERFACE NAME -> GLOBAL : **GE0/2**
  - IPV4 ADDRESS -> STATIC -> DEVICE SPECIFIC

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

4.9.8 Step 3 –Configure a VPN Interface Template which would be used for administration purposed to be used by TechCast SYDNEY vEdge-Cloud Devices for VPN 1 for Interface LoopBack1.

ملاحظة: هذه الخطوة أختيارية ولكن الهدف من استخدامها هنا لأنه نبغى نستخدمها في اللاب الخاص ب AAR policy (Application Aware Routing)

- In vManage, Navigate to Configuration.

- Configure the VPN parameters based on the following:
  - TEMPLATE NAME : **VE-VPN1-IF-LB1**
  - DESCRIPTION : **VE-VPN1-IF-LB1**

Basic Configuration

  - SHUTDOWN -> GLOBAL : **NO**
  - INTERFACE NAME -> GLOBAL : **LOOPBACK1**

- IPv4 Address -> Static -> Device Specific

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

4.9.9 Step 4 – Configure a OSPF Template to be used by TechCast SYDNEY vEdge-Cloud Devices for VPN 1

- In vManage, Navigate to Configuration.

- Configure the OSPF parameters based on the following:

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

Redistribution

  - Protocol : **OMP** (هنا محتاجين نعمل **redistribution** من **OMP** الى **OSPF**)
  -

Area Configuration

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

Interface Configuration

  - Interface Name: **ge0/2**
  - Interface Name: **loopback1**

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

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

4.10 Lab 23 – Configuring & Deploying - Device Template (Sydney vEdge2)

4.10.1 Step 1 – Configure a Device Template for SYDNEY vEdge Devices.

- In vManage, Navigate to Configuration.

Templates > Device > Create Template > From Feature Template > vEdge Cloud

- Configure the Device Template based on the following:
  - TEMPLATE NAME : **SYD-VE-DEV-TEMP**
  - DESCRIPTION : **SYD-VE-DEV-TEMP**

Basic Information

  - SYSTEM -> **VE-SYSTEM**

Transport & Management

  - VPN 0 : **SYD-VE-VPN-VPN0**
  - VPN INTERFACE : **SYD-VE-VPN0-IF-G0/0**
  - BGP : **SYD-VE-VPN0-BGP**

  - VPN 512 : **SYD-VE-VPN-VPN512**
  - VPN INTERFACE : **SYD-VE-VPN512-IF-E0**

Service VPN

  - VPN 1 : **SYD-VE-VPN-VPN1**
  - VPN INTERFACE : **SYD-VE-VPN1-IF-G0/2**
  - VPN INTERFACE : **VE-VPN1-IF-LB1**
  - OSPF : **SYD-VE-VPN1-OSPF**

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

4.10.2 Step 2 – Attach vEdge2 to the Device Template

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

Templates > Device > SYD-VE-DEV-TEMP

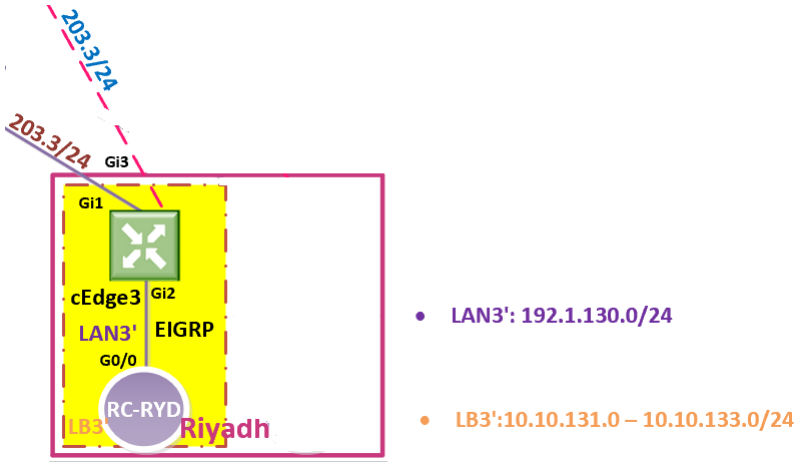
- Click on "**…**" towards the right-hand side.

- Click **Attach Devices.**
- Select **vEdge2** and click the " **->** " button.
- Click **Attach**.

4.10.3 Step 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:
  - INTERFACE IP FOR GE0/2 :**192.168.20.2/24**
  - DEFAULT GATEWAY FOR VPN0 : **192.1.20.254**
  - INTERFACE IP FOR LOOPBACK1 : **2.2.2.2/32**
  - INTERFACE IP FOR GE0/0 :**192.1.20.2/24**
  - HOSTNAME : **vEDGE-2**
  - SYSTEM IP : **200.200.200.202**
  - 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 Internal Router by issuing the **Show ospf neighbor** command on **vEdge2.**
- Type **Show Ip route** on **vEdge2** to verify that you are receiving BGP routes from GW-Sydney Router about Transport network subnets. Also, you can verify that you are receiving OMP routes about LAN subnets of other sites.
- Type **Show Ip route** on **R-SYD Router** to verify that you are receiving OSPF routes from the other Sites as OE2.
- Verify reachability between the sites by Pinging the Internal Loopback to Loopback networks of other sites.

4.11 Lab 24 – VPN0, VPN512 & its Routing-Feature Template (RC-RYD cEdge3)



VPN 0

4.11.1 Step 1 – Configure a VPN Template by cEdge for VPN 0

- In vManage, Navigate to Configuration.

Templates > Feature > CSR1000v > VPN > VPN

- Configure the VPN parameters based on the following:
  - Template Name : **CE-VPN-VPN0**
  - Description : **CE-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.

4.11.2 Step 2 – Configure a VPN Interface Template to be used by cEdge 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 : CE-VPN0-IF-G1
  - Description : CE-VPN0-IF-G1

Basic Configuration

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

Tunnel

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

Allow Service

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

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

4.11.3 Step 3 – Configure a VPN Interface Template to be used by cEdge for VPN 0 for Interface GigabitEthernet3

- In vManage, Navigate to Configuration.

Templates > Feature > CSR1000v > VPN > VPN Interface Ethernet

- Configure the VPN parameters based on the following:
  - Template Name : CE-VPN0-IF-G3
  - Description : CE-VPN0-IF-G3

Basic Configuration

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

Tunnel

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

Allow Service

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

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

4.11.4 Step 4 – Configure a OSPF Template to be used by cEdge for VPN 0

- In vManage, Navigate to Configuration.

Templates → Feature → CSR1000v → Other Templates → OSPF

- Configure the OSPF parameters based on the following:

  - Template Name : **CE-VPN0-OSPF**
  - Description : **CE-VPN0-OSPF**

Area Configuration

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

Interface Configuration

- Interface Name: **GigabitEthernet1**

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

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

VPN 512

4.11.5 Step 1 – Configure a VPN Template to be used by cEdge for VPN 512

- In vManage, Navigate to Configuration.

- Configure the VPN parameters based on the following:
  - Template Name : **CE-VPN-VPN512**
  - Description : **CE-VPN-VPN512**

Basic Configuration

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

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

4.11.6 Step 2 – Configure a VPN Interface Template to be used by cEdge for VPN 512 for Interface GigabitEthernet4

- In vManage, Navigate to Configuration.

- Configure the VPN parameters based on the following:
  - Template Name : **CE-VPN512-IF-G4**
  - Description : **CE-VPN512-IF-G4**

Basic Configuration

  - Shutdown -> Global : **No**
  - Interface Name -> Global : **GigabitEthernet4**
  - IPv4 Address -> Dynamic

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

VPN 1

4.11.7 Step 1 – Configure a VPN Template for cEdge for VPN 1

- In vManage, Navigate to Configuration.

Templates > **Feature** > **CSR1000v** > **VPN** > **VPN**

- Configure the VPN parameters based on the following:
  - Template Name : **CE-VPN-VPN1**
  - Description : **CE-VPN-VPN1**

Basic Configuration

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

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

4.11.8 Step 2 – Configure a VPN Interface Template to be used by cEdge for VPN 1 for Interface G2

- In vManage, Navigate to Configuration.

Templates > **Feature** > **CSR1000v** > **VPN** > **VPN Interface Ethernet**

- Configure the VPN parameters based on the following:
  - Template Name : **CE-VPN1-IF-G2**
  - Description : **CE-VPN1-IF-G2**

Basic Configuration

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

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

4.11.9 Step 3 – Configure EIGRP Template to be used by cEdge for VPN1

- In vManage, Navigate to Configuration.

Templates > Feature > CSR1000v > Other Template > EIGRP

- Configure the OSPF parameters based on the following:
  - Template Name: **CE-VPN1-EIGRP**
  - Description: **CE-VPN1-EIGRP**

Basic Configuration

  - Autonomous System ID -> Global : **1**

Redistribution

  - Protocol : **OMP**

Network

  - Network Prefix : **192.168.130.0/24**
  - Click **Add**

Interface

  - Interface Name: **GigabitEthernet2**
  - Shutdown -> Global : **No**

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

4.11.10 Step 4 – Configure OMP Template to advertise EIGRP routes received by cEdge3 from RC-Riyadh router to other sites

- In vManage, Navigate to Configuration.

Templates > Feature > CSR1000v > Basic Config > OMP

- Configure the OMP parameters based on the following:
  - Template Name : **CE-OMP**
  - Description : **CE-OMP**

Advertise

- EIGRP -> GLOBAL : **ON**

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

4.12 Lab 25 – Configuring & Deploying - Device Template (RC-RYD cEdge3)

4.12.1 Step 1 – Configure a Device Template for CSR Branch Devices.

- In vManage, Navigate to Configuration.

Templates > Device > Create Template > From Feature Template > CSR1000v

- Configure the Device Template based on the following:
  - Template Name : **CE-DEV-TEMP**
  - Description : **CE-DEV-TEMP**

Basic Information

  - System -> **CE-System**
  - OMP -> **CE-OMP**

Transport & Management

  - VPN 0 : **CE-VPN-VPN0**
  - VPN Interface : **CE-VPN0-IF-G1**
  - VPN Interface : **CE-VPN0-IF-G3**
  - OSPF : **CE-VPN0-OSPF**

  - VPN 512 : **CE-VPN-VPN512**
  - VPN Interface : **CE-VPN512-IF-G4**

Service VPN

  - VPN 1 : **CE-VPN-VPN1**
  - VPN Interface : **CE-VPN1-IF-G2**
  - EIGRP : **CE-VPN1-EIGRP**

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

4.12.2 Step 2 – Attach cEdge3 to the Device Template

- In vManage, Navigate to Configuration.

Templates > Device > CE-DEV-TEMP

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

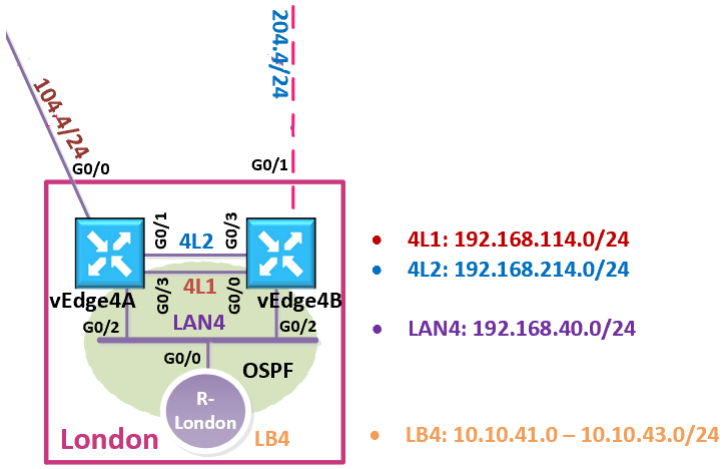
- Click **Attach Devices.**
- Select **cEdge3** and click the " **->** " button.
- Click **Attach**.

4.12.3 Step 3 – Configure the Variable Parameters for the Feature Templates

- **cEdge3** 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 GIGABITETHERNET2 :**192.168.130.3/24**
  - DEFAULT GATEWAY FOR VPN0 : **192.1.203.254**
  - INTERFACE IP FOR GIGABITETHERNET1 :**192.168.203.13/24**
  - INTERFACE IP FOR GIGABITETHERNET3 :**192.1.203.13/24**
  - HOSTNAME : **CEDGE-3**
  - SYSTEM IP : **200.200.200.213**
  - 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**.
- Verify the configuration on **cEdge3**. You can do that by verify OSPF Neighbor relationship MPLS-Cloud Router by issuing the **Show ip ospf neighbor** command on **cEdge3.**
- Type **Show Ip route** on **cEdge3** to verify that you are receiving OSPF routes from the MPLS Router.
- Type **Show Ip route vrf 1 eigrp** on **cEdge3** to verify that you are receiving EIGRP routes from the **RC-Riyadh** Router.
- Type **Show sdwan omp routes** on **cEdge3** to verify that you are receiving OMP routes about other sites' LAN subnets.
- Type **Show Ip route** on **RC-Riyadh** Router to verify that you are receiving EIGRP routes from the other Sites as "D EX".
- Verify reachability between the sites by Pinging the Internal Loopback to Loopback networks of other sites.

5 SDWAN Advance Templates Configuration

5.1 Lab 26 – TLOC Extensions – London (vEdge4A | vEdge4B)



vEdge4A and vEdge4B Templates Creation

VPN 0

5.1.1 Step 1 – Configure a VPN Template to be used by Site-4 vEdges for VPN0

- In vManage, Navigate to Configuration.

Templates > **Feature** > **vEdge Cloud** > **VPN** > **VPN**

- Configure the VPN parameters based on the following:
  - TEMPLATE NAME : **TLOC-VE-VPN-VPN0**
  - DESCRIPTION : **TLOC-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.

5.1.2 Step 2 – Configure a VPN Interface Template to be used by all SITE4 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 : **TLOC-VE-VPN0-IF-G0/0**
  - Description : **TLOC-VE-VPN0-IF-G0/0**

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.

5.1.3 Step 3 – Configure a VPN Interface Template to be used by all SITE4 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 : **TLOC-VE-VPN0-IF-G0/1**
  - Description : **TLOC-VE-VPN0-IF-G0/1**

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

5.1.4 Step 4 – Configure a Template that will be used for TLOC-Extension on Site-4 vEdges

- In vManage, Navigate to Configuration.

- Configure the VPN parameters based on the following:
  - Template Name : **TLOC-VE-VPN0-IF-G0/3**
  - Description : **TLOC-VE-VPN0-IF-G0/3**

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.

5.1.5 Step 5 – Configure an External Routing-OSPF Template to be used by vEdge4A for VPN 0

- In vManage, Navigate to Configuration.

- Configure the OSPF parameters based on the following:

  - Template Name : **TLOC-VE-A-VPN0-OSPF**
  - Description : **TLOC-VE-A-VPN0-OSPF**

Area Configuration

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

Interface Configuration

  - Interface Name: **ge0/0**
  - Interface Name: **ge0/3**

- Click **Add** to add interfaces and then click **Add** to add OSPF area.

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

5.1.6 Step 6 – Configure an External Routing-OSPF Template to be used by vEdge4B for VPN 0

- In vManage, Navigate to Configuration.

- Configure the OSPF parameters based on the following:

  - Template Name : **TLOC-VE-B-VPN0-OSPF**
  - Description : **TLOC-VE-B-VPN0-OSPF**

Area Configuration

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

- Area Type -> Default

Interface Configuration

- Interface Name: **ge0/0**

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

---

vEdge4A Templates Deployment

5.1.7 Step 1 – Configure a Device Template for Site-4 vEdge4A

- In vManage, Navigate to Configuration.

- Configure the Device Template based on the following:

  - Template Name : **vEdge4A-DEV-TEMP**
  - Description : **vEdge4A-DEV-TEMP**

Basic Information

- System -> **VE-System**

Transport & Management

- VPN 0 : **TLOC-VE-VPN-VPN0**
- VPN Interface : **TLOC-VE-VPN0-IF-G0/0**
- VPN Interface : **TLOC-VE-VPN0-IF-G0/1**
- VPN Interface : **TLOC-VE-VPN0-IF-G0/3**
- OSPF: **TLOC-VE-A-VPN0-OSPF**

- VPN 512 : **VE-VPN-VPN512**
- VPN Interface : **VE-VPN512-IF-E0**

Service VPN

- VPN 1 : **VE-VPN-VPN1**
- VPN Interface : **VE-VPN1-IF-G0/2**

- VPN INTERFACE : **VE-VPN1-IF-LB1**
- OSPF: **VE-VPN1-OSPF**

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

5.1.8 Step 2 – Attach vEdge4A to the Device Template

- In vManage, Navigate to Configuration.

Templates > **Device** > **vEdge4A-DEV-TEMP**

- Click on "**…**" towards the right-hand side.
- Click **Attach Devices.**
- Select **vEdge4A** and click the " **->** " button.
- Click **Attach**.

5.1.9 Step 3 – Configure the Variable Parameters for the Feature Templates

- **vEdge4A** 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 : **192.1.214.14**
  - INTERFACE IP FOR GE0/0 :**192.168.104.4/24**
  - INTERFACE IP FOR GE0/1 :**192.1.214.4/24**
  - INTERFACE IP FOR GE0/2 :**192.168.40.4/24**
  - INTERFACE IP FOR GE0/3 :**192.168.114.4/24**
  - INTERFACE IP FOR LOOPBACK1 :**4.4.4.4/24**
  - TLOC EXTENSION: **GE0/0**
  - TIMEZONE: **EUROPE/LONDON**
  - HOSTNAME : **VEDGE-4A**
  - SYSTEM IP : **200.200.200.204**
  - 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**.

vEdge4B Templates Deployment

5.1.10 Step 1 – Configure a Device Template for Site-4 vEdge4B

- In vManage, Navigate to Configuration.

- Configure the Device Template based on the following:
  - TEMPLATE NAME : **VEDGE4B-DEV-TEMP**
  - DESCRIPTION : **VEDGE4B-DEV-TEMP**

Basic Information

- SYSTEM -> **VE-SYSTEM**

Transport & Management

- VPN 0 : **TLOC-VE-VPN-VPN0**
- VPN INTERFACE : **TLOC-VE-VPN0-IF-G0/0**
- VPN INTERFACE : **TLOC-VE-VPN0-IF-G0/1**
- VPN INTERFACE : **TLOC-VE-VPN0-IF-G0/3**
- OSPF: **TLOC-VE-B-VPN0-OSPF**

- VPN 512 : **VE-VPN-VPN512**
- VPN INTERFACE : **VE-VPN512-IF-E0**

Service VPN

- VPN 1 : **VE-VPN-VPN1**
- VPN INTERFACE : **VE-VPN1-IF-G0/2**
- VPN INTERFACE : **VE-VPN1-IF-LB1**
- OSPF: **VE-VPN1-OSPF**

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

5.1.11 Step 2 – Attach vEdge4B to the Device Template

- In vManage, Navigate to Configuration.

Templates > **Device** > **vEdge4B-DEV-TEMP**

- Click on "**…**" towards the right-hand side.
- Click **Attach Devices.**
- Select **vEdge4B** and click the " **->** " button.
- Click **Attach**.

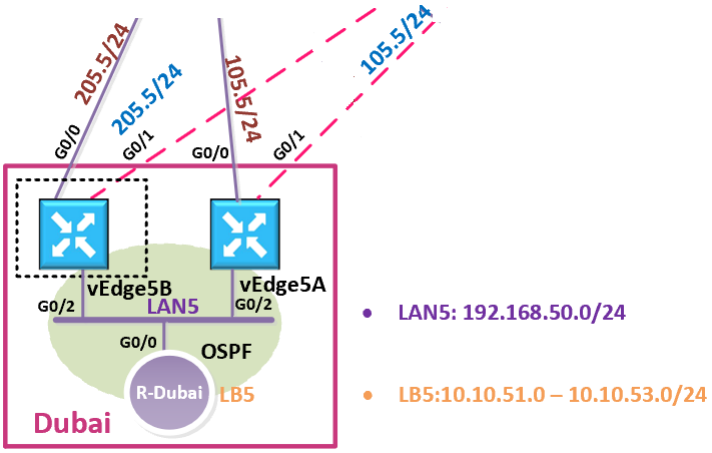
5.1.12 Step 3 – Configure the Variable Parameters for the Feature Templates

- **vEdge4B** 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 : **192.1.204.254**
  - Interface IP for ge0/0 :**192.168.114.14/24**
  - Interface IP for ge0/1 :**192.1.204.4/24**
  - Interface IP for ge0/2 :**192.168.40.14/24**
  - Interface IP for ge0/3 :**192.1.214.14/24**
  - Interface IP for loopback1 :**140.140.140.4/24**
  - TLOC Extension: **ge0/1**
  - Timezone: **Europe/London**
  - Hostname : **vEdge-4B**
  - System IP : **200.200.200.214**
  - 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**.

Verification

- Verify the configuration on **vSmart**. You can do that by making sure that you are receiving 2 TLOCS for vEdge4A and 2 TLOCS for vEdge4B. The command to verify is **show omp tlocs.**
- Verify the policy by using the **Monitor -> Network -> vEdge4A/vEdge4B -> Troubleshooting -> Simulate Flows** Tool and you should receive 2 TLOCS for vEdge4A/vEdge4B through both transports connections.
- Type **Show Ip route** on **R-London** Router to verify that you are receiving OSPF routes from the other Sites as “OE2”.
- Verify reachability between the sites by Pinging the Internal Loopback to Loopback networks of other sites.

5.2 Lab 27 – Load Balancing – Dubai (vEdge5B)



كما تعلمون أنه احنا أنشائنا ونفذنا vEdge5A template وربطنا فرع تك كاست في دبي ولكن بعد نقل فريق تك كاست التقني لدبي, أصبحت الحاجة ملحة أنه بأن نحقق high availability وبالتالي كان لابد من اضافة لينك تاني لتفادي أي انقطاع في الخدمات. لذلك في هذا اللاب نقوم بانشاء vEdge5B template .

وكما ترون بأن vEdge5B مشابه في اعدادته لمواقع تك كاست الأخرى مثل vEdge2, vEdge3, and vEdge5A. لذلك حنستخدم نفس templates عن طريق attaching vEdge5B الى **"VE-DEV-TEMP"** Device Template وبكدا نقدر نتطبق في هذا اللاب عملية Load Balancing.

5.2.1 Step 1 – Attach vEdge5B to the VE-DEV-TEMP Device Template

- In vManage, Navigate to Configuration.

- Click **Attach Devices.**
- Select **vEdge5B** and click the " **->** " button.
- Click **Attach**.
- **vEdge5B** will appear in the window.
- Click on "**…**" towards the right-hand side for vEdge5B and click **Edit Device Template.**

vEdge5B Templates Deployment

- Configure the variables based on the following:

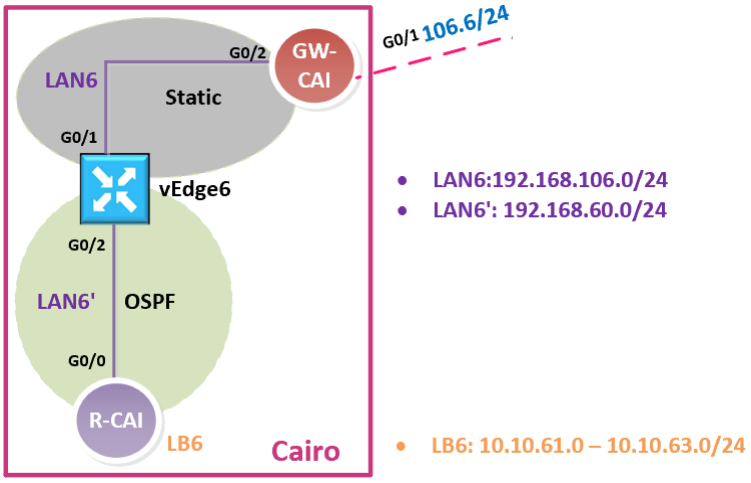
- Interface IP for ge0/2 :**192.168.50.15/24**
- Default Gateway for VPN0 : **192.1.205.254**
- Interface IP for ge0/1 :**192.1.205.5/24**
- Interface IP for ge0/0 :**192.168.205.5/24**
- Interface IP for loopback1 :**150.150.150.5/24**
- Hostname : **vEdge-5B**
- System IP : **200.200.200.215**
- Site 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**.

Verification

- Verify the configuration on **vEdge5B**. You can do that by verify OSPF Neighbor relationship with the Internal Site Router by issuing the **Show ospf neighbor** command on the **vEdge5B.**
- Type **Show ip route omp** on **vEdge5A/vEdge5B** to verify that you are receiving 4 TLOC routes per subnet from the other Sites.
- Verify the policy by using the **Monitor -> Network -> vEdge5A/vEdge5B -> Troubleshooting -> Simulate Flows** Tool and you should receive 4 TLOCS for vEdge5A/vEdge5B through both transports connections.
- Verify reachability between the sites by Pinging the Internal Loopback to Loopback networks from **Site-5 Internal Router**.

5.3 Lab 28 – Allow NATed SDWAN Traffic – Cairo (GW-Cairo)



Interface Configuration

GW-Cairo

Interface	IP Address	Subnet Mask
G 0/1	192.1.106.16	255.255.255.0
G 0/2	192.168.106.254	255.255.255.0

GW-Cairo Configuration

5.3.1 Step 1 – Interface Configuration and Default Routing on GW-Cairo

- Configure the Interfaces based on the Logical Diagram along IP addresses.
- Configure a default route on the GW-Cairo pointing towards the Internet Cloud.

```
no ip domain-lookup
line con 0
logg sync
no exec-timeout
!
Hostname GW-Cairo
!
Interface G 0/1
ip address 192.1.106.16 255.255.255.0
no shut
!
Interface G 0/2
ip address 192.168.106.254 255.255.255.0
no shut
!
ip route 0.0.0.0 0.0.0.0 192.1.106.254
```

5.3.2 Step 2 – Configure static NATing to translate vEdge6 to outside network.

- Statically Translate vEdge6 as 192.1.106.6 on the outside Interface.
- The Private address that will be assigned to vEdge6 is 192.168.106.6.

```
interface GigabitEthernet1
ip nat outside
!
interface GigabitEthernet2
ip nat inside
!
ip nat inside source static 192.168.106.6 192.1.106.6
```

5.4 Lab 29 – Configuring & Deploying SDWAN Templates – Cairo (vEdge6)

vEDGE-6 Initialization – (CLI)

5.4.1 Step 1 – Configuring the System Component on vEdge6

- Configure the System parameters based on the following:
  - HOST-NAME : **VEDGE6**
  - ORGANIZATION: **TECTCAST**
  - SYSTEM-IP: **200.200.200.206**
  - SITE ID: **6**
  - VBOND ADDRESS: **212.1.1.3**
  - TIMEZONE: SELECT TIMEZONE BASED ON YOUR DEVICE LOCATION

```
config
!
system
 host-name vEdge6
 system-ip 200.200.200.206
 site-id 6
 organization-name TECHCAST
 clock timezone Africa/Cairo
 vbond 212.1.1.3
!
 Commit
```

5.4.2 Step 2 – Configure the vpn parameters

- Configure the VPN parameters based on the following:

VPN 0

- INTERFACE **GE0/0**
- IP ADDRESS: **192.168.106.6/24**

  TUNNEL INTERFACE
  - ENCAPSULATION IPSEC
  - TUNNEL SERVICES (ALL, NETCONF, SSHD)
- DEFAULT ROUTE: 192.168.106.254

VPN 512

- INTERFACE **ETH0**
- IP ADDRESS: DHCP CLIENT

```
config
!
vpn 0
 no interface eth0
 interface ge0/1
  ip address 192.168.106.6/24
  tunnel-interface
  encapsulation ipsec
   allow-service all
   allow-service netconf
   allow-service sshd
   no shut
 ip route 0.0.0.0/0 192.168.106.254
!
vpn 512
 interface eth0
 ip dhcp-client
 no shutdown
 !
 Commit
```

vEDGE-6 Initialization – vManage (GUI)

5.4.3 Step 1 – Upload the Root Certificate to the vEdge

- On the Windows Server, open **WINSCP** application.
- **Connect** to vEdge6 using the following information:
  - IP ADDRESS : **192.1.106.6**
  - PROTOCOL - **SFTP**
  - USERNAME : **ADMIN**
  - PASSWORD : **ADMIN**
- Copy the **RootCert.cer** file from the Downloads folder to the **/home/admin** folder on the vEdge6.

5.4.4 Step 1' – This is another way to upload RootCert.cer to the vEdge

- On the Windows Server, open **RootCert.cer** file we saved in CA folder
- Righ-click on it and open it using notepad
- Copy using **CTRL-A** and **CTRL-C**.
- Go to vEdge-6
  - In exec-mode; to enter vshell mode >> Type "**vshell**" and enter
  - Type "**vim RootCert.cer**" and click enter
  - Click letter " **i** " and click enter
  - Paste the **RootCert** using **CTRL-V**
  - Click "**Esc**" key and the type " **:wq** " and click enter
  - Type " **exit** " and enter to exit vshell mode.

5.4.5 Step 3 – Install the Root Certificate on vEdge6

- Connect to the console of vEdge6 and issue the following command:

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

5.4.6 Step 4 - Activate vEdge on vManage

- Navigate to **Configuration -> Devices**
- Note and use the **Chassis Number** and **Token number** for the 6th vEdge from vManage.
- Use the information from the previous step in the following command on the vEdge6 console.

request vedge-cloud activate chassis-number XYZ token XYZ

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

---

vEdge6 Templates Creation

VPN 0

5.4.7 Step 1 – Configure a VPN Template to be used by vEdge6 for VPN0

- In vManage, Navigate to Configuration.

- Configure the VPN parameters based on the following:
  - Template Name : **CAI-VE-VPN-VPN0**
  - Description : **CAI-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.

5.4.8 Step 2 – Configure a VPN Interface Template to be used by vEdge6 for VPN 0 for Interface G0/1

- In vManage, Navigate to Configuration.

- Configure the VPN parameters based on the following:
  - Template Name : **CAI-VE-VPN0-IF-G0/1**
  - Description : **CAI-VE-VPN0-IF-G0/1**

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.

ملاحظة: في هذا اللاب مانحتاج نقوم بانشاء feature templates لكل من VPN 512 و VPN 1 لجهاز vEdge6
ولذلك حنقوم باستخدام نفس feature templates اللي تم انشائها سابقا وهي كلأتي:

- VPN 512: **VE-VPN-VPN512**
- VPN 512 E0: **VE-VPN512-IF-E0**
- VPN 1: VE-VPN-VPN1
- VPN 1 G0/2: **VE-VPN1-IF-G0/2**
- VPN 1 loopback1 : **VE-VPN1-IF-LB1**
- VPN 1 Internal-Routing OSPF: **VE-VPN1-OSPF**

---

vEdge6 Templates Deployment

5.4.9 Step 1 – Configure a Device Template for Site-6 vEdge Devices

- In vManage, Navigate to Configuration.

- Configure the Device Template based on the following:

  - Template Name : **CAI-VE-DEV-TEMP**
  - Description : **CAI-VE-DEV-TEMP**

Basic Information

- System -> **VE-System**

Transport & Management

- VPN 0 : **CAI-VE-VPN-VPN0**

- VPN 0 INTERFACE : **CAI-VE-VPN0-IF-G0/1**

- VPN 512: **VE-VPN-VPN512**
- VPN 512 E0: **VE-VPN512-IF-E0**

Service VPN

- VPN 1: VE-VPN-VPN1
- VPN 1 G0/2: **VE-VPN1-IF-G0/2**
- VPN 1 LOOPBACK1 : **VE-VPN1-IF-LB1**
- VPN 1 INTERNAL-ROUTING OSPF: **VE-VPN1-OSPF**

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

5.4.10 Step 2 – Attach vEdge6 to the Device Template

- In vManage, Navigate to Configuration.

Templates > **Device** > **CAI-VE-DEV-TEMP**

- Click on "**…**" towards the right-hand side.
- Click **Attach Devices.**
- Select **vEdge6** and click the " **->** " button.
- Click **Attach**.

5.4.11 Step 3 – Configure the Variable Parameters for the Feature Templates

- **vEdge6** 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 : **192.168.106.254**
  - INTERFACE IP FOR GE0/1 : **192.168.106.6/24**
  - INTERFACE IP FOR GE0/2 :**192.168.60.6/24**
  - INTERFACE IP FOR LB1: **6.6.6.6/32**
  - TIMEZONE: AFRICA/CAIRO

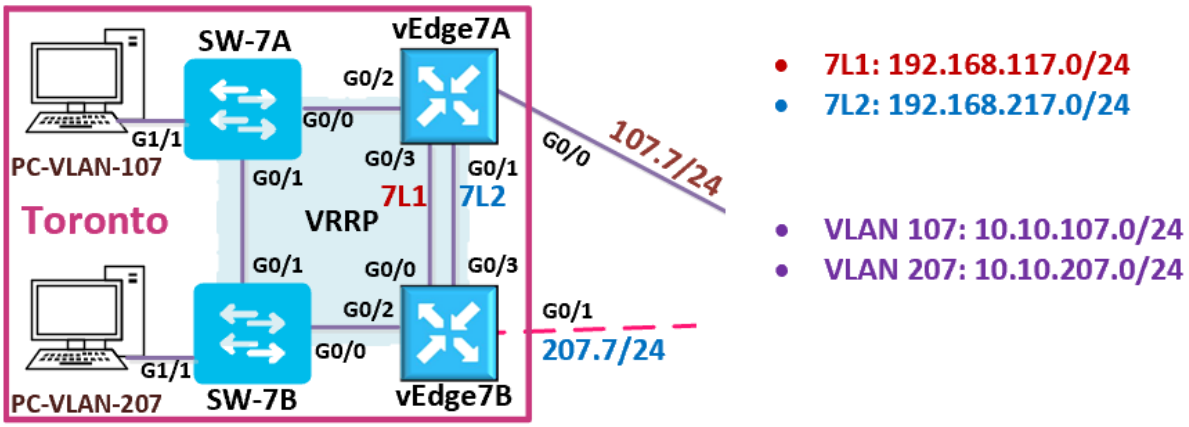
- HOSTNAME : **VEDGE-6**
- SYSTEM IP : **200.200.200.206**
- SITE ID : **6**

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

Verification

- Verify the configuration on **vEdge6**. You can do that by verify OSPF Neighbor relationship with the **R-Cairo Router** by issuing the **Show ospf neighbor** command on **vEdge6.**
- Verify received OMP routes on **vEdge6** for other sites subnets 10.10.xx.1/24, using **Show ip route omp** command on **vEdge6.**
- Verify received routes in **R-Cairo Router** as OE2 routes.
- Check reachability to these received OE2 routes on **R-Cairo Router** using **Ping** command.

5.5 Lab 30 – Configuring VRRP – Toronto (vEdge7A | vEdge7B)



تستطيع في هذا اللاب التركز على عمل الكونفقريشن لل **VRRP templates** ولذلك سوف نعيد استخدام **TLOC Extension templates** اللي تم انشائها سابقا بدلا من انشائها مرة أخرى لموقع تك كاست في تورنتو.

ولهذا سنقوم بنسخ **Device Template** الخاصة بجهاز **vEdge4A** وتغيير الأسم الى **"vEdge7A-DEV-TEMP"** لنخصصها لجهاز **vEdge7A** ونعدل عليها بناءا على المعطيات الجديدة . نفس الشي حينطبق على **vEdge7B** بحيث ننسخ **Device Template** الخاصة بجهاز **vEdge4B** وتغيير الأسم الى **"vEdge7B-DEV-TEMP"** .

ولكن حابين نعمل الخطوات كاملة كنوع من الاعادة والتذكير بهذه الخطوات حتى تساعد الطالب على التطبيق المتكرر ولكن هذا لايفضل عمله في الحياة العملية حتى تلتمس الفائدة من استخدام ميزة **templates** في حلول **SD-WAN**.

---

vEdge7A and vEdge7B Templates Creation

VPN 0

5.5.1 Step 1 – Configure a VPN Template to be used by Site-7 vEdges for VPN0

- In vManage, Navigate to Configuration.

Templates > **Feature** > **vEdge Cloud** > **VPN** > **VPN**

- Configure the VPN parameters based on the following:
  - TEMPLATE NAME : **TLOC-VE-VPN-VPN0**
  - DESCRIPTION : **TLOC-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.

5.5.2 Step 2 – Configure a VPN Interface Template to be used by all SITE7 vEdge-Cloud Devices for VPN 0 for Interface G0/0

- In vManage, Navigate to Configuration.

- Configure the VPN parameters based on the following:
  - Template Name : **TLOC-VE-VPN0-IF-G0/0**
  - Description : **TLOC-VE-VPN0-IF-G0/0**

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.

5.5.3 Step 3 – Configure a VPN Interface Template to be used by all SITE7 vEdge-Cloud Devices for VPN 0 for Interface G0/1

- In vManage, Navigate to Configuration.

- Configure the VPN parameters based on the following:
  - Template Name : **TLOC-VE-VPN0-IF-G0/1**
  - Description : **TLOC-VE-VPN0-IF-G0/1**

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.

5.5.4 Step 4 – Configure a Template that will be used for TLOC-Extension on Site-7 vEdges

- In vManage, Navigate to Configuration.

- Configure the VPN parameters based on the following:
  - Template Name : **TLOC-VE-VPN0-IF-G0/3**
  - Description : **TLOC-VE-VPN0-IF-G0/3**

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.

5.5.5 Step 5 – Configure an External Routing-OSPF Template to be used by vEdge7A 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 : **TLOC-VE-A-VPN0-OSPF**
  - Description : **TLOC-VE-A-VPN0-OSPF**

Area Configuration

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

Interface Configuration

- Interface Name: **ge0/0**
- Interface Name: **ge0/3**

- Click **Add** to add interfaces and then click **Add** to add OSPF area.

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

5.5.6 Step 6 – Configure an External Routing-OSPF Template to be used by vEdge7B 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 : **TLOC-VE-B-VPN0-OSPF**
- Description : **TLOC-VE-B-VPN0-OSPF**

Area Configuration

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

Interface Configuration

- Interface Name: **ge0/0**

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

---

vEdge7A Templates Deployment

5.5.7 Step 1 – Configure a Device Template for Site-7 vEdge7A

- In vManage, Navigate to Configuration.

- Configure the Device Template based on the following:

- Template Name : **vEdge7A-DEV-TEMP**
- Description : **vEdge7A-DEV-TEMP**

Basic Information

- System -> **VE-System**

Transport & Management

- VPN 0 : **TLOC-VE-VPN-VPN0**
- VPN Interface : **TLOC-VE-VPN0-IF-G0/0**
- VPN Interface : **TLOC-VE-VPN0-IF-G0/1**
- VPN Interface : **TLOC-VE-VPN0-IF-G0/3**
- OSPF: **TLOC-VE-A-VPN0-OSPF**

- VPN 512 : **VE-VPN-VPN512**
- VPN Interface : **VE-VPN512-IF-E0**

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

5.5.8 Step 2 – Attach vEdge7A to the Device Template

- In vManage, Navigate to Configuration -> **Templates -> Device -> vEdge7A-DEV-TEMP**

Templates > **Device** > **vEdge7A-DEV-TEMP**

- Click on "**…**" towards the right-hand side.
- Click **Attach Devices.**
- Select **vEdge7A** and click the " **->** " button.
- Click **Attach**.

5.5.9 Step 3 – Configure the Variable Parameters for the Feature Templates

- **vEdge7A** 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 : **192.1.217.17**
  - Interface IP for ge0/0 :**192.168.107.7/24**
  - Interface IP for ge0/1 :**192.1.217.7/24**
  - Interface IP for ge0/3 :**192.168.117.7/24**
  - TLOC Extension: **ge0/0**
  - Timezone: *America/Toronto*
  - Hostname : **vEdge-7A**
  - System IP : **200.200.200.207**
  - Site ID : **7**
- Click **Update.**
- Verify the Configuration & Click **Configure Devices.**
- Wait for it to update the device. It should come back with Status of **Success**.

---

vEdge7B Templates Deployment

5.5.10 Step 1 – Configure a Device Template for Site-7 vEdge7B.

- In vManage, Navigate to Configuration.

- Configure the Device Template based on the following:
  - TEMPLATE NAME : **VEDGE7B-DEV-TEMP**
  - DESCRIPTION : **VEDGE7B-DEV-TEMP**

Basic Information

  - SYSTEM -> **VE-SYSTEM**

Transport & Management

  - VPN 0 : **TLOC-VE-VPN-VPN0**
  - VPN INTERFACE : **TLOC-VE-VPN0-IF-G0/0**
  - VPN INTERFACE : **TLOC-VE-VPN0-IF-G0/1**
  - VPN INTERFACE : **TLOC-VE-VPN0-IF-G0/3**
  - OSPF: **TLOC-VE-B-VPN0-OSPF**

  - VPN 512 : **VE-VPN-VPN512**
  - VPN INTERFACE : **VE-VPN512-IF-E0**

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

5.5.11 Step 2 – Attach vEdge7B to the Device Template

- In vManage, Navigate to Configuration.

- Click on "**…**" towards the right-hand side.
- Click **Attach Devices.**
- Select **vEdge7B** and click the " **->** " button.
- Click **Attach**.

5.5.12 Step 3 – Configure the Variable Parameters for the Feature Templates

- **vEdge7B** 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 : **192.1.207.254**
  - Interface IP for ge0/0 :**192.168.117.17/24**
  - Interface IP for ge0/1 :**192.1.207.7/24**
  - Interface IP for ge0/3 :**192.1.217.17/24**
  - TLOC Extension: **ge0/1**
  - Timezone: **America/Toronto**
  - Hostname : **vEdge-7B**
  - System IP : **200.200.200.217**
  - Site ID : **7**
- Click **Update.**
- Verify the Configuration & Click **Configure Devices.**
- Wait for it to update the device. It should come back with Status of **Success**.

5.5.13 Step 4 – Configure the Feature Templates for VRRP LAN 1 Interface

- In vManage, Navigate to Configuration.

Templates → **Feature** → **vEdge Cloud** → **VPN** → **VPN Interface Ethernet**

- Configure the VPN Interface parameters based on the following:
  - Template Name : **VRRP-VE-VPN1-IF-LAN1**
  - Description : **VRRP-VE-VPN1-IF-LAN1**

Basic Configuration

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

VRRP

- Group ID -> Device Specific
- Priority -> Device Specific
- IP Address -> Device Specific

- Click **Add** and then click **Save** to save the Template.

5.5.14 Step 5 – Configure the Feature Templates for VRRP LAN 2 Interface

- In vManage, Navigate to Configuration.

Templates > Feature > vEdge Cloud > VPN > VPN Interface Ethernet

- Configure the VPN Interface parameters based on the following:

  - Template Name : **VRRP-VE-VPN1-IF-LAN2**
  - Description : **VRRP-VE-VPN1-IF-LAN2**

Basic Configuration

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

VRRP

- Group ID -> Device Specific
- Priority -> Device Specific
- IP Address -> Device Specific

- Click **Add** and then click **Save** to save the Template.

5.5.15 Step 6 – Configure the Feature Templates for VRRP LAN Parent Interface

- In vManage, Navigate to Configuration.

Templates > Feature > vEdge Cloud > VPN > VPN Interface Ethernet

- Configure the VPN interface parameters based on the following:

  - Template Name : **VRRP-VE-VPN0-PARENT-IF**
  - Description : **VRRP-VE-VPN0-PARENT-IF**

Basic Configuration

- Shutdown -> Global : **No**
- Interface Name -> Global : **ge0/2**

Advance

- IP MTU -> Global : **1504**

- Click **Add** and then click **Save** to save the Template.

5.5.16 Step 7 – Modify the Device Templates for VRRP vEdge7A

- In vManage, Navigate to Configuration.

- Configure the Device Template based on the following:

Transport & Management VPN (VPN 0)

- VPN Interface : **VRRP-VE-VPN0-PARENT-IF**

Service VPN

- VPN Interface : **VRRP-VE-VPN1-IF-LAN1**
- VPN Interface : **VRRP-VE-VPN1-IF-LAN2**

ملاحظة: في هذا اللاب محتاجين نخلي الأفضلية لل **MPLS link** للترافيك االصادر من فريق تك كاست **" staff traffic"** اللي جاي من **PC-VLAN-107**. بالنسبة للترافيك الصادر من الضيوف **" guest traffic"** عن طريق الأجهزة ضمن **VLAN 207** زي مثلا **PC-VLAN-207** أنها تطلع عبر اللينك المفضل **Internet link** .

5.5.17 Step 8 – Configure the Variable Parameters for the Feature Templates

- **vEdge7A** will appear in the window.

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

- Click **Edit Device Template.**

- Configure the variables based on the following:

- IPv4 Address(LB1): **7.7.7.7/32**

LAN1

- Interface Name(IF-LAN1): **ge0/2.100**
- IPv4 Address (VLAN 107-Staff IP): **10.10.107.1/24**
- Group ID: **107**
- Priority: **200**
- IP Address (VIP-LAN1 address): **10.10.107.254**

LAN2

- Interface Name(IF-LAN2): **ge0/2.200**
- IPv4 Address (VLAN 207-Staff IP): **10.10.207.1/24**
- Group ID: **207**
- Priority: **100**
- IP Address (VIP-LAN2 address): **10.10.207.254**

5.5.18 Step 9 – Modify the Device Templates for VRRP vEdge7B

- In vManage, Navigate to Configuration.

- Configure the Device Template based on the following:

Transport & Management VPN (VPN 0)

- VPN Interface : **VRRP-VE-VPN0-PARENT-IF**

Service VPN

- VPN Interface : **VRRP-VE-VPN1-IF-LAN1**
- VPN Interface : **VRRP-VE-VPN1-IF-LAN2**

5.5.19 Step 10 – Configure the Variable Parameters for the Feature Templates

- **vEdge7B** will appear in the window.
- Click on "**…**" towards the right-hand side.
- Click **Edit Device Template.**
- Configure the variables based on the following:

- IPv4 Address(LB1): **17.17.17.17/32**

LAN1

- Interface Name(IF-LAN1): **ge0/2.100**
- IPv4 Address (VLAN 107-Staff IP): **10.10.107.2/24**
- Group ID: **107**
- Priority: **100**
- IP Address (VIP-LAN1 address): **10.10.107.254**

LAN2

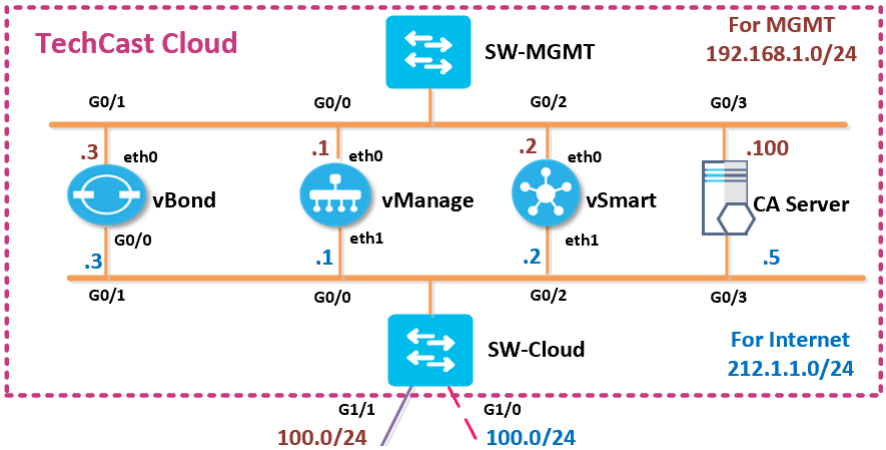
- Interface Name(IF-LAN2): **ge0/2.200**
- IPv4 Address (VLAN 207-Staff IP): **10.10.207.2/24**
- Group ID: **207**
- Priority: **200**
- IP Address (VIP-LAN2 address): **10.10.207.254**

Verification

- Verify the configuration on **vSmart**. You can do that by making sure that you are receiving 2 TLOCS for vEdge4A and 2 TLOCS for vEdge4B. The command to verify is **show omp tlocs.**
- Verify the policy by using the **Monitor -> Network -> vEdge4A/vEdge4B -> Troubleshooting -> Simulate Flows** Tool and you should receive 2 TLOCS for vEdge4A/vEdge4B through both transports connection
- Verify connectivity from PC-VLAN-107 or PC-VLAN-207 by using Ping to other remote sites' LANs.
- Verify that the **staff traffic (PC-VLAN-107)** prefers MPLS link through vEdge7A to reach other remote sites' LANs.
- Verify that the **guest traffic (PC-VLAN-207)** prefers Internet link through vEdge7B to reach other remote sites' LANs.

6 Policy Templates Configuration

6.1 Lab 31 – vSmart Feature & Device Templates Configuration



6.1.1 Step 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 : **212.1.1.254**

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

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

- In vManage, Navigate to Configuration.

- 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.

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

- In vManage, Navigate to Configuration.

- Configure the VPN parameters based on the following:
  - TEMPLATE NAME : **VSMART-VPN0-IF-E1**
  - DESCRIPTION : **VSMART-VPN0-IF-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.

6.1.4 Step 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-VPN512-IF-E0**
  - DESCRIPTION : **VSMART-VPN512-IF-E0**

Basic Configuration

  - SHUTDOWN -> GLOBAL : **NO**
  - INTERFACE NAME -> GLOBAL : **ETH0**
  - IPV4 ADDRESS -> STATIC -> DEVICE-SPECIFIC

- Click **Save** to save the Template

6.1.5 Step 5 – Configure a Device Template for vSmart Controllers

- In vManage, Navigate to Configuration.

Templates > Device > Creat Template > From Feature Template > vSmart

- Configure the Device Template based on the following:
  - TEMPLATE NAME : **VSMART-DEV-TEMP**
  - DESCRIPTION : **VSMART-DEV-TEMP**

Basic Information

  - SYSTEM ->**VSMART-SYSTEM**

في هذه المرة حنعمل الكونفقريشن لهذه الخطوة داخل **Device Template**
عشان نشوف الفروقات ان وجدت.

Transport & Management

  - VPN 0 : **VSMART-VPN-VPN0**
  - VPN INTERFACE : **VSMART-VPN0-IF-E1**

  - VPN 512 : **VSMART-VPN-VPN512**
  - VPN INTERFACE : **VSMART-VPN512-IF-E0**

- Click **Save** to save the Template

6.1.6 Step 6 – Attach vSmart to the Device Template

- In vManage, Navigate to Configuration.

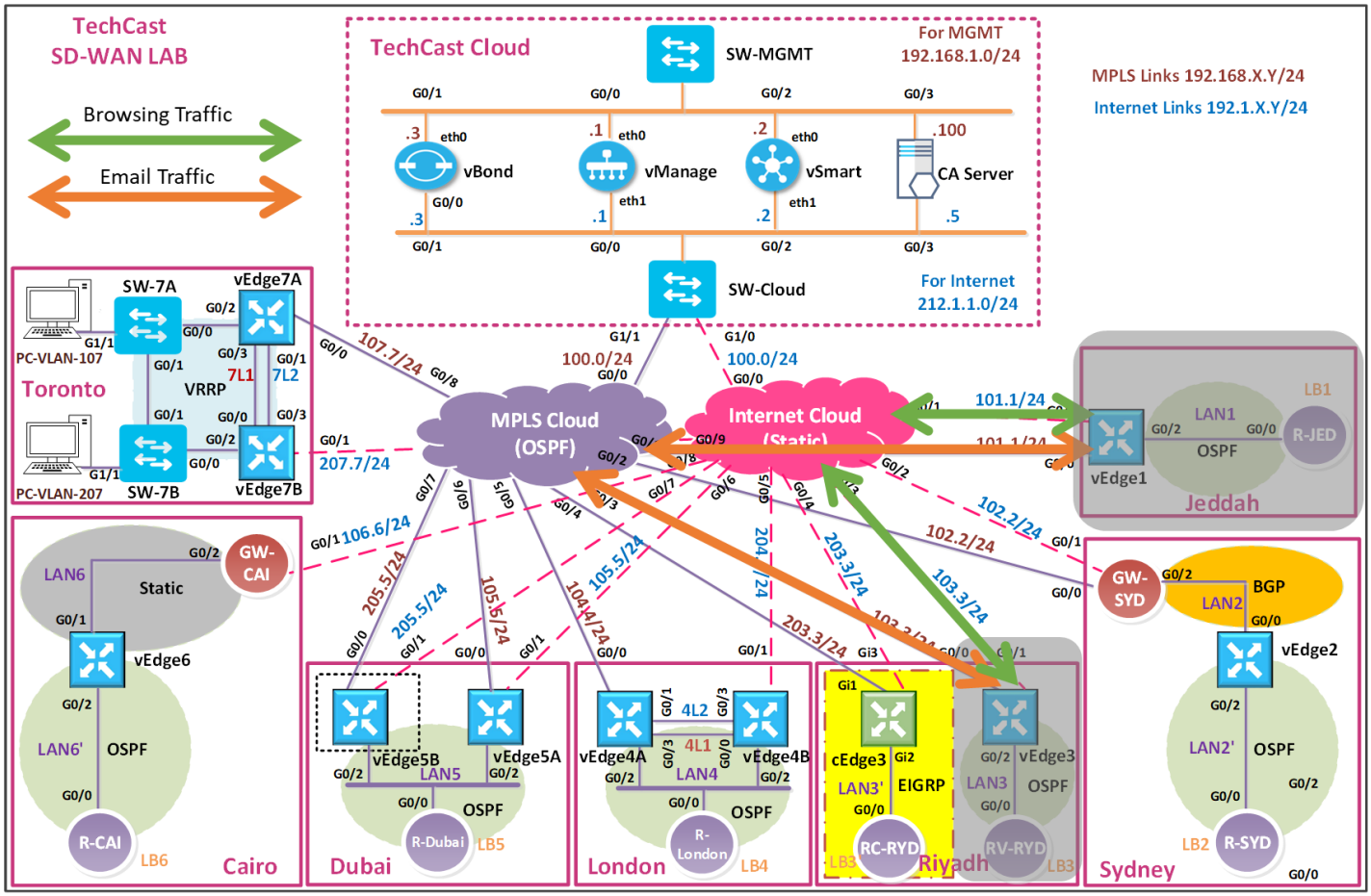
Templates > **Device** > **vSmart-DEV-TEMP**

- Click on "**…**" towards the right-hand side.
- Click **Attach Devices.**
- Select **vSmart** and click the " **->** " button.
- Click **Attach**.

6.1.7 Step 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 :**212.1.1.2/24**
  - INTERFACE IP FOR ETH0 :**192.168.1.2/24**
  - HOSTNAME : **VSMART-1**
  - SYSTEM IP : **100.100.100.102**
  - SITE ID : **100**
- Click **Update.**
- Verify the Configuration & Click **Configure Devices.**
- Wait for it to update the device. It should come back with Status of **Success**.

6.2 Lab 32 – Application Aware Policies (TCP Traffic)



في هذا اللاب سوف نقوم بانشاء وتنفيذ AAR Policies لترافيك TCP بين موقعين (Jeddah & RV-Riyadh) وحنستخدم Email و Browsing ترافيك كمثال على TCP ترافيك بناءا على المعايير التالية لكل ترافيك.

- Jeddah & RV-Riyadh Sites should use the MPLS Transport for Email Traffic and the Biz-Internet Transport for Browsing Traffic.
- Email Should have an SLA based on the following:
  - Loss – 5%
  - Latency – 100
  - Jitter – 100ms
- Browsing Should have an SLA based on the following:
  - Loss – 15%
  - Latency – 600
  - Jitter – 150ms
- Create the Sites for Jeddah and Riyadh.
- Create the VPN for VPN ID 1.

6.2.1 Step 1 – Configure Groups of Interests/List that will be used for Email & Browsing Application Aware Routing (AAR) Policy

- In vManage, Navigate to Configuration.

- Click **SLA Class** and select **New SLA Class list.** Create 2 policies based on the following:
  - NAME : **EMAIL-SLA**
  - LOSS : **5%**
  - LATENCY : **100**
  - JITTER : 1**00MS**

  - NAME : **BROWSING-SLA**
  - LOSS : **15%**
  - LATENCY : **600**
  - JITTER : **150MS**
- 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 : **JEDDAH**
  - SITE ID : **1**

  - NAME : **RV-RIYADH**
  - SITE ID : **3**

6.2.2 Step 2 – Configure an AAR policy based on the Requirements

- In vManage, Navigate to Configuration

- Configure 2 App Routes based on the following:
  - POLICY NAME : **TCP-TRAFFIC-POLICY**

- Description : **TCP-Traffic-Policy**

Email Sequence

Match Conditions

- Protocol : **6**
- Port : **25 110 143** **(Email protocols: SMTP=25, POP3=110 and IMAP=143)**

Action

- SLA Class List: **Email-SLA**
- Color : **mpls**
- Restrict: **Yes.** Just click checkbox
- Backup Preferred Color: **biz-internet**

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

Browsing Sequence

Match Conditions

- Protocol : 6
- Port : 80 443 **(Browsing protocols: HTTP=80 and HTTPS=443)**

Action

- SLA Class List: **Browsing-SLA**
- Color : **biz-internet**
- Restrict: **Yes.** Just click checkbox
- Backup Preferred Color: **mpls**

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

- Click **Save App Aware Routing Policy** to save the policy.

6.2.3 Step 3 – Create a Centralized Policy and call the Traffic Policy

- In vManage, Navigate to Configuration.

Configuration > **Policies** > **Centralized Policy** > **Add Centralized Policy**

- Click **Next** on the **"Group of Interests"** page because in Step#1 we have already created the required lists.

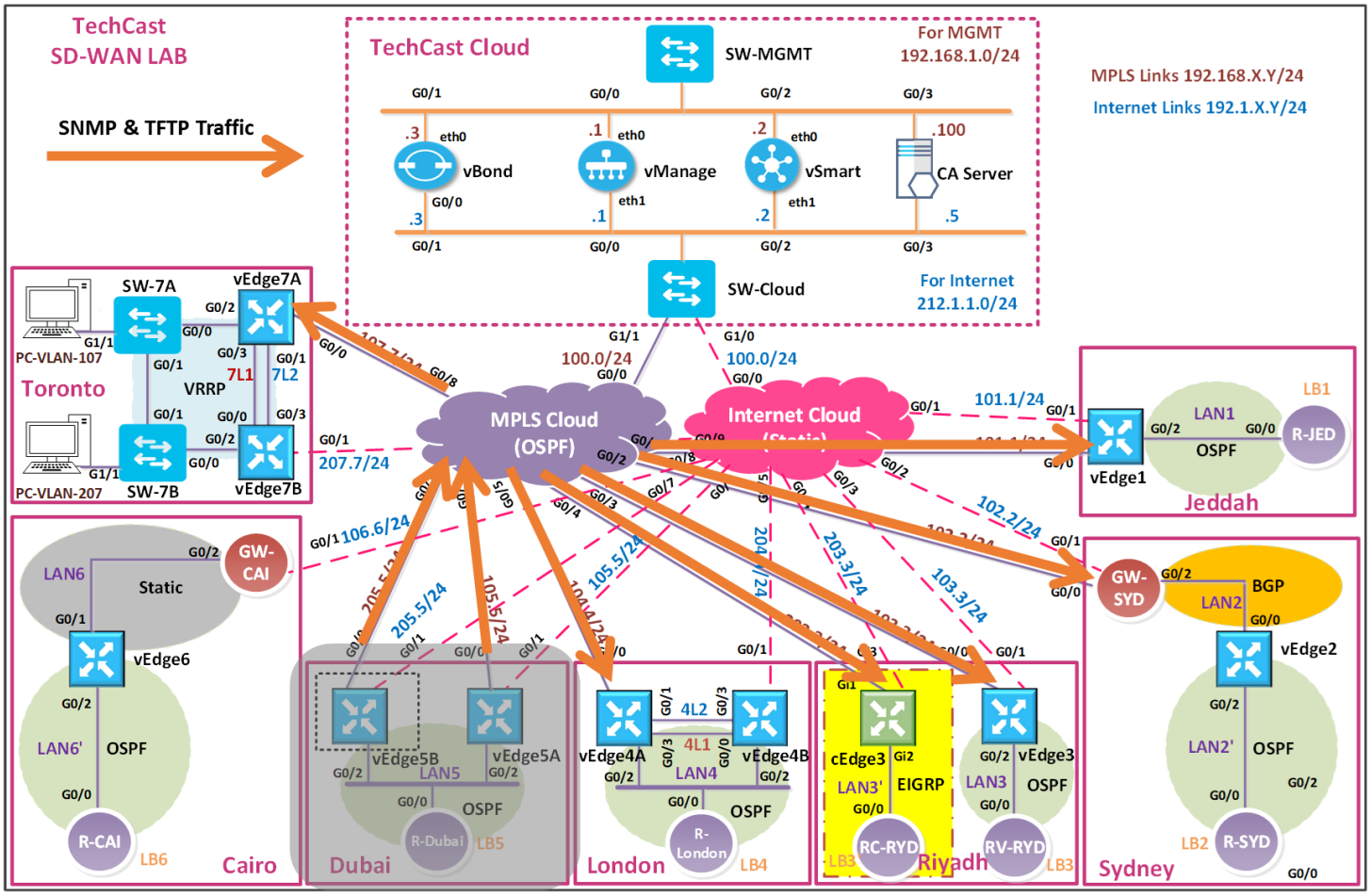
- Click **Next** on the **"Topology and VPN Membership"** page as we are not using any Control Policies.

- Click **Add Policy** on the **"Configure Traffic Rules"** page.
- Click "**Import Existing"** and select the **TCP-Traffic-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 **TCP-Traffic-Policy** will be there. Click "**New Site List and VPN List"** button.
- Assign the Policy a name and Description based on the following:
    - POLICY NAME: **TECHCAST-POLICY**
    - DESCRIPTION: **TECHCAST-POLICY**
- Select **Jeddah** and **Riyadh** 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).

Verification

- Verify the policy by using the **Monitor -> Network -> vEdge1 -> Troubleshooting -> Simulate Flows** Tool.
- Email traffic simulation from Jeddah or Riyadh should only use the **mpls** transport.
- Browsing traffic simulation from Jeddah or Riyadh should only use the **biz-internet** transport.
- Other normal traffic like Ping from Jeddah or Riyadh should use both Transports links.

6.3 Lab 33 – Application Aware Policies (UDP Traffic)



في هذا اللاب, نريد التحكم في **UDP (SNMP and TFTP)** ترافيك اللي طالعة تحديدا عن طريق **TechCast network administrators** الموجودين في موقع تك كاست في دبي واللي بيستخدمو شبكة 50.50.50.0/24 بأن يطلع الترافيك تبعهم عن طريق **MPLS transport** لمواقع تك كاست الأخرى.

.

- TechCast Dubai site & all remote sites should use the MPLS Transport for SNMP and TFTP traffic for security purposes.

- SNMP Should have an SLA based on the following:
  - Loss – 5%
  - Latency – 150
  - Jitter – 100ms

- TFTP Should have an SLA based on the following:
  - Loss – 10%
  - Latency – 300
  - Jitter – 150ms

- Create the Site for Dubai.
- Create the VPN for VPN ID 1

6.3.1 Step 1 – Configure Groups of Interests/List that will be used for SNMP and TFTP Application Aware Routing (AAR) Policy

- In vManage, Navigate to Configuration.

- Click **SLA Class** and select **New SLA Class list.** Create 2 policies based on the following:
  - NAME : **SNMP-SLA**
  - LOSS : **5%**
  - LATENCY : **100**
  - JITTER : **100MS**

  - NAME : **TFTP-SLA**
  - LOSS : **10%**
  - LATENCY : **300**
  - JITTER : **150MS**

- Click **VPN** and just make sure that Service VPN (VPN1) was created based on the previous based on the following:
  - NAME : **VPN1**
  - ID : **1**

- Click **Site** and select **New Site list.** Create the site based on the following:
  - NAME : **DUBAI**
  - SITE ID : **5**

6.3.2 Step 2 – Configure a Traffic policy based on the Requirements

- In vManage, Navigate to Configuration.

- Configure 2 App Routes based on the following:

- Policy Name : **UDP-Traffic-Policy**
- Description : **UDP-Traffic-Policy**

SNMP Sequence

Match Conditions

- Protocol : **17**
- Port : **161**
- Source IP: **50.50.50.0/24**

Action

- SLA Class List: **SNMP-SLA**
- Color : **mpls**
- Restrict: **Yes.** Just click checkbox
- Backup Preferred Color: **biz-internet**

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

TFTP Sequence

Match Conditions

- Protocol : **17**
- Port : **69**
- Source IP: **50.50.50.0/24**

Action

- SLA Class List: **TFTP-SLA**
- Color : **mpls**
- Restrict: **Yes.** Just click checkbox
- Backup Preferred Color: **biz-internet**

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

- **Save the Policy.**

6.3.3 Step 3 – Modify the existing Centralized Policy "TechCast-Policy" and call the Traffic Policy

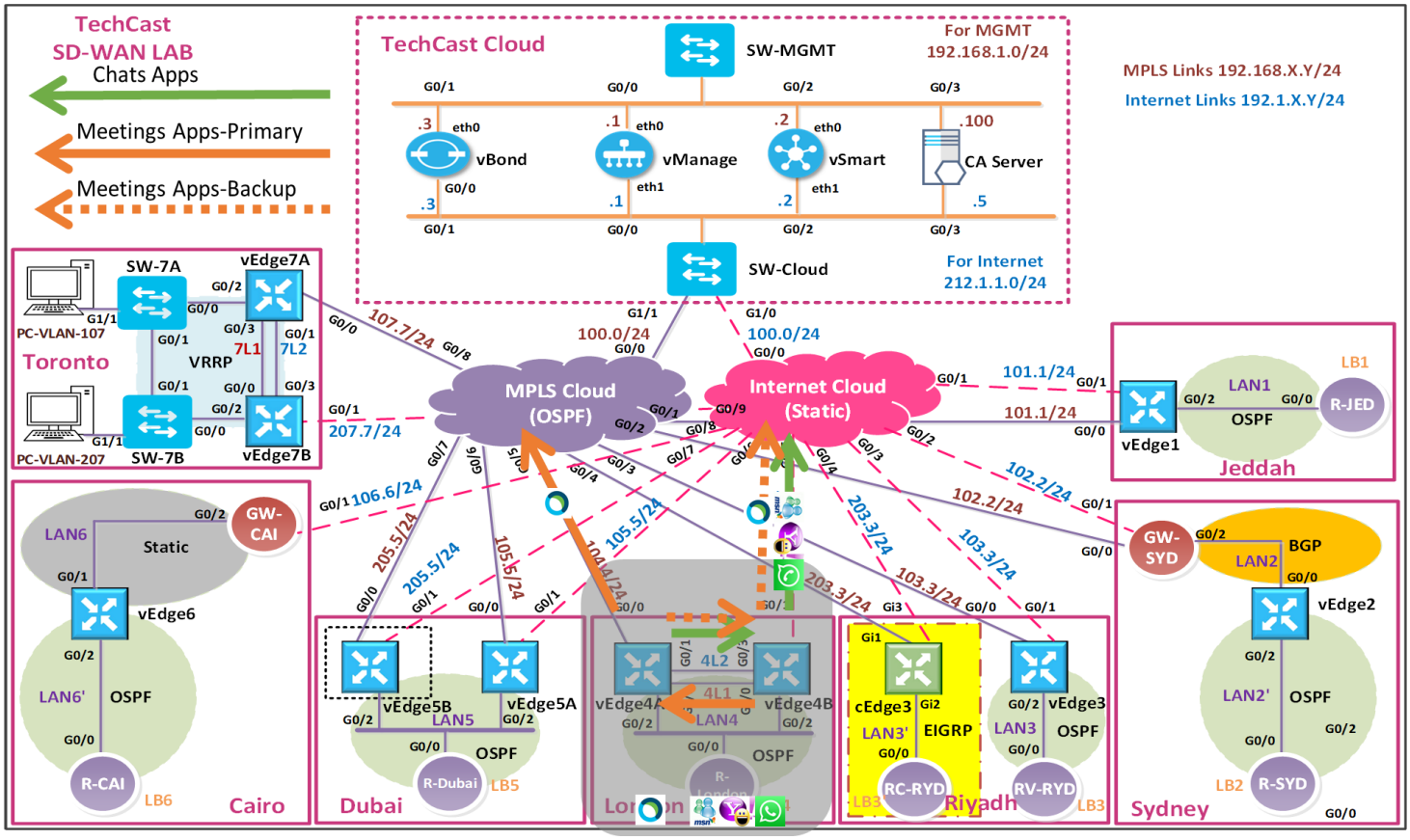
- In vManage, Navigate to Configuration.

- Click **Traffic Rules** on the **Top** of the page.
- Click **Add Policy**.
- Click "**Import Existing"** and select the **UDP-Traffic-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 **UDP-Traffic-Policy** will be there. Click "**New Site List and VPN List"** button.
- Select **Dubai** in the Site List.
- Select **VPN1** in the Site List.
- Click **Add.**
- Click the **Save Policy Changes.**
- **Activate** the policy.
- Wait for it to push the policy to the reachable vSmart Controller(s).

Verification

- Verify the policy by using the **Monitor -> Network -> vEdge5A or vEdge5B-> Troubleshooting -> Simulate Flows** Tool.
- SNMP traffic simulation from Dubai site using source IP **50.50.50.1** to any remote site should only use the **mpls** transport.
- TFTP traffic simulation from Dubai site using source IP **50.50.50.1** to any remote site should only use the **mpls** transport.

6.4 Lab 34 – Application Aware Policies (DPI Traffic)



في هذا اللاب, حنستخدم Deep Packet Inspection-DPI بحيث نطبق هذه policy على تطبيقات Chat و Meetings.

- موقع تك كاست في لندن يجب أن يستخدم Internet Transport لتطبيقات Chats مثل MSN Messenger و Yahoo Messenger و Whatsapp Messenger applications.
  ملاحظة: كل تطبيقات Chats لن تستخدم MPLS Transport على الاطلاق.

- موقع تك كاست في لندن يجب أن يستخدم MPLS Transport وبأن يكون الينك المفضل لتطبيقات Meetings مثل Webex. أضف اللى ذلك هذي التطبيقات تستخدم Internet Transpor كخط بديل Backup .

- The Chat applications should have a SLA based on the following:
  - Loss – 25%
  - Latency – 600
  - Jitter – 120ms
- The Meeting applications should have a SLA based on the following:
  - Loss – 5%
  - Latency – 100
  - Jitter – 100ms

6.4.1 Step 1 – Configure Groups of Interests/List that will be used for Chat-based and Meetings Applications Aware Routing (AAR) Policy

- In vManage, Navigate to Configuration.

- Click **Applications** and select **New Application list.** Create a policy based on the following:
  - NAME : **CHAT-APPS**
  - APPLS: **MSN MESSENGER, YAHOO MESSENGER & WHATSAPP MESSENGER**

  - NAME : **MEETINGS-APPS**
  - APPLS: **WEBEX & MICROSOFT TEAMS**

- Click **SLA Class** and select **New SLA Class list.** Create a policy based on the following:
  - NAME : **CHATS-SLA**
  - LOSS : **25%**
  - LATENCY : **600**
  - JITTER : **150MS**

  - NAME : **MEETINGS-SLA**
  - LOSS : **5%**
  - LATENCY : **100**
  - JITTER : **100MS**

- Just double check if you already created a VPN 1 or 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 London based on the following:
  - NAME : **LONDON**
  - SITE ID : **4**

6.4.2 Step 2 – Configure an AAR policy based on the Requirements

- In vManage, Navigate to Configuration.

- Configure 1 App Routes based on the following:
  - Policy Name : **DPI-Traffic-POLICY**
  - Description : **DPI-Traffic-POLICY**

Chats Sequence

Match Conditions

- Application List: **Chat-Apps**

Action

- SLA Class List: **CHATS-SLA**
- Preferred Color: **Biz-Internet**

- Click **Save Match and Actions** to save the Sequence.
- Click **Save App Aware Routing Policy.**

Meetings Sequence

Match Conditions

- Application List: **Meetings-Apps**

Action

- SLA Class List: **Meetings-SLA**
- Preferred Color: **MPLS**
- Backup Color: **Biz-Internet**

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

6.4.3 Step 3 – Modify the existing Centralized Policy "TechCast-Policy" and call the Traffic Policy

- In vManage, Navigate to Configuration.

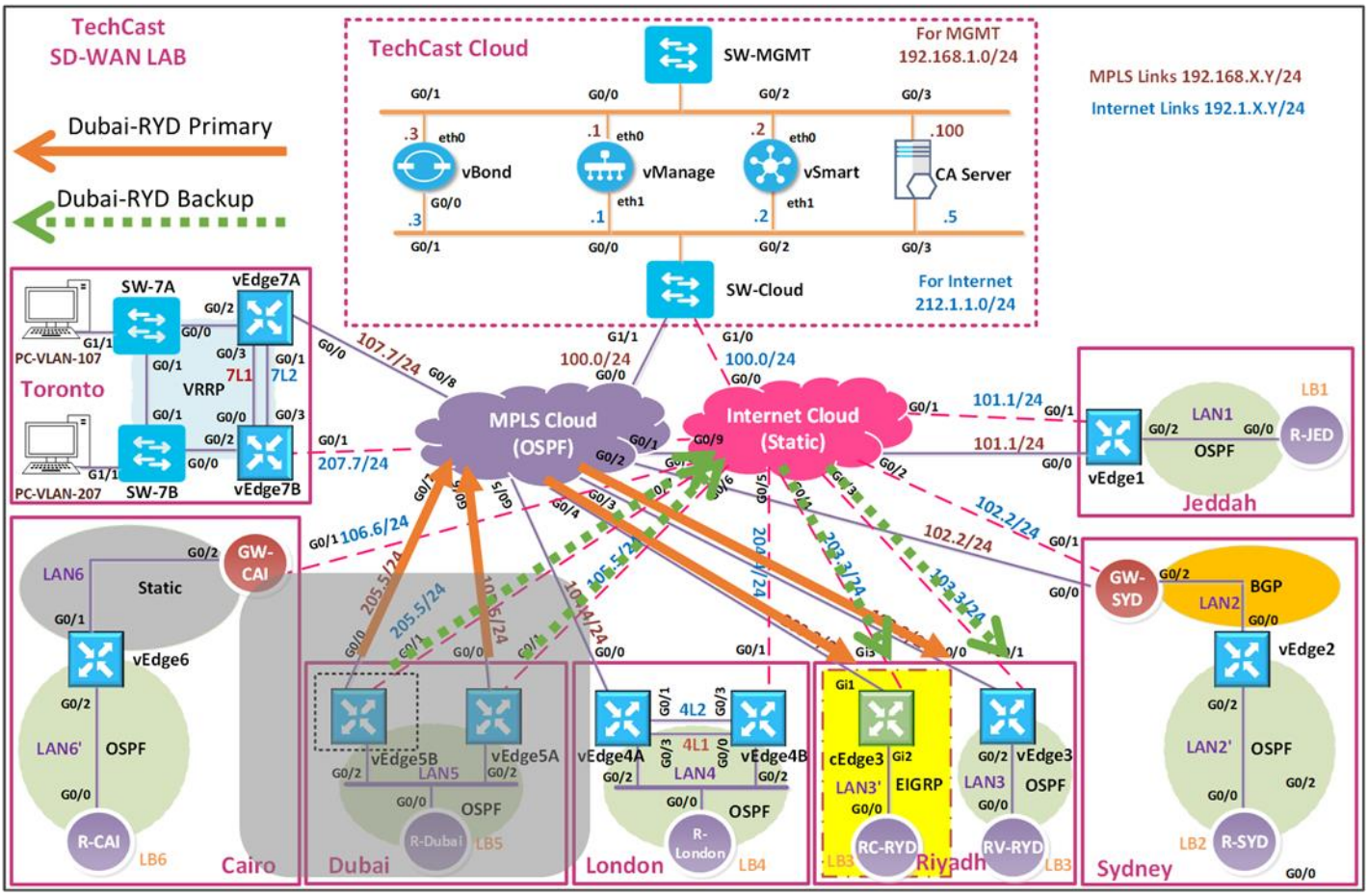
- Click **Traffic Rules** on the **Top** of the page.

- Click **Add Policy**.
- Click "**Import Existing"** and select the **DPI-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 **DPI-Traffic-POLICY** will be there. Click "**New Site List and VPN List"** button.
- Select **London** in the Site List.
- Select **VPN1** in the Site List.
- Click **Add.**
- Click the **Save Policy Changes**.
- **Activate** the policy.
- Wait for it to push the policy to the reachable vSmart Controller(s).

Verification

- Verify the policy by using the **Monitor -> Network ->vEdge4A/vEdge4B -> Troubleshooting -> Simulate Flows** Tool.
- Normal Ping from any London should use both the Transports.
- Use **MSN Messenger/ Yahoo Messenger/WhatsApp** as the application and simulate from London site. It should only use the **biz-internet** transport.
- Use **Webex** as the application and simulate London site. It should use **MPLS** transports.

6.5 Lab 35 – Traffic Flow Manipulation



في هذا اللاب, نبغى موقع تك كاست في دبي عندما يتواصل مع مواقعنا في الرياض بأن يكون الينك المفضل هو MPLS TLOC وبأن يكون Internet TLOC هو backup TLOC في حالة حدوث أي مشكلة على اللينك الرئيسي.

6.5.1 Step 1 – Configure Groups of Interests/List that will be used for Traffic Engineering Policy for Riyadh

- In vManage, Navigate to Configuration.

- Click **TLOCs** and select **New TLOC list.** Create a policy based on the following:
  - NAME : **RYD-TLOC-MPLS-INTERNET**
  - **TLOC#1:**
    - IP ADDRESS: **200.200.200.203**
    - COLOR: **MPLS**
    - ENCAPSULATION: **IPSEC**

- Preference: **300**

- **TLOC#2:**
  - IP Address: **200.200.200.203**
  - Color: **Biz-internet**
  - Encapsulation: **IPSec**
  - Preference: **200**

- **TLOC#3:**
  - IP Address: **200.200.200.213**
  - Color: **MPLS**
  - Encapsulation: **IPSec**
  - Preference: **300**

- **TLOC#4:**
  - IP Address: **200.200.200.213**
  - Color: **Biz-internet**
  - Encapsulation: **IPSec**
  - Preference: **200**

- Just double check if you already created a VPN 1 or Click **VPN** and select **New VPN list.** Create VPN based on the following:

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

- Click **Site** and select **New Site list.** Create Riyadh Sites based on the following:

  - Name : **Riyadh-Sites**
  - Site ID : **3, 13**

6.5.2 Step 2 – Configure Control/Topology policy based on the Requirements

- In vManage, Navigate to Configuration.

- Configure 1 Route Policy based on the following:

  - Policy Name: **RYD-Policy**
  - Description: **RYD-Policy**

Route Sequence

Match Conditions

- SITE LIST: RIYADH-SITES
- VPN LIST:
  VPN1

Action

- TLOC/TLOC LIST: **RYD-TLOC-MPLS-INTERNET**

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

Default Sequence

Action

- ACCEPT

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

- Click **Save** the Policy

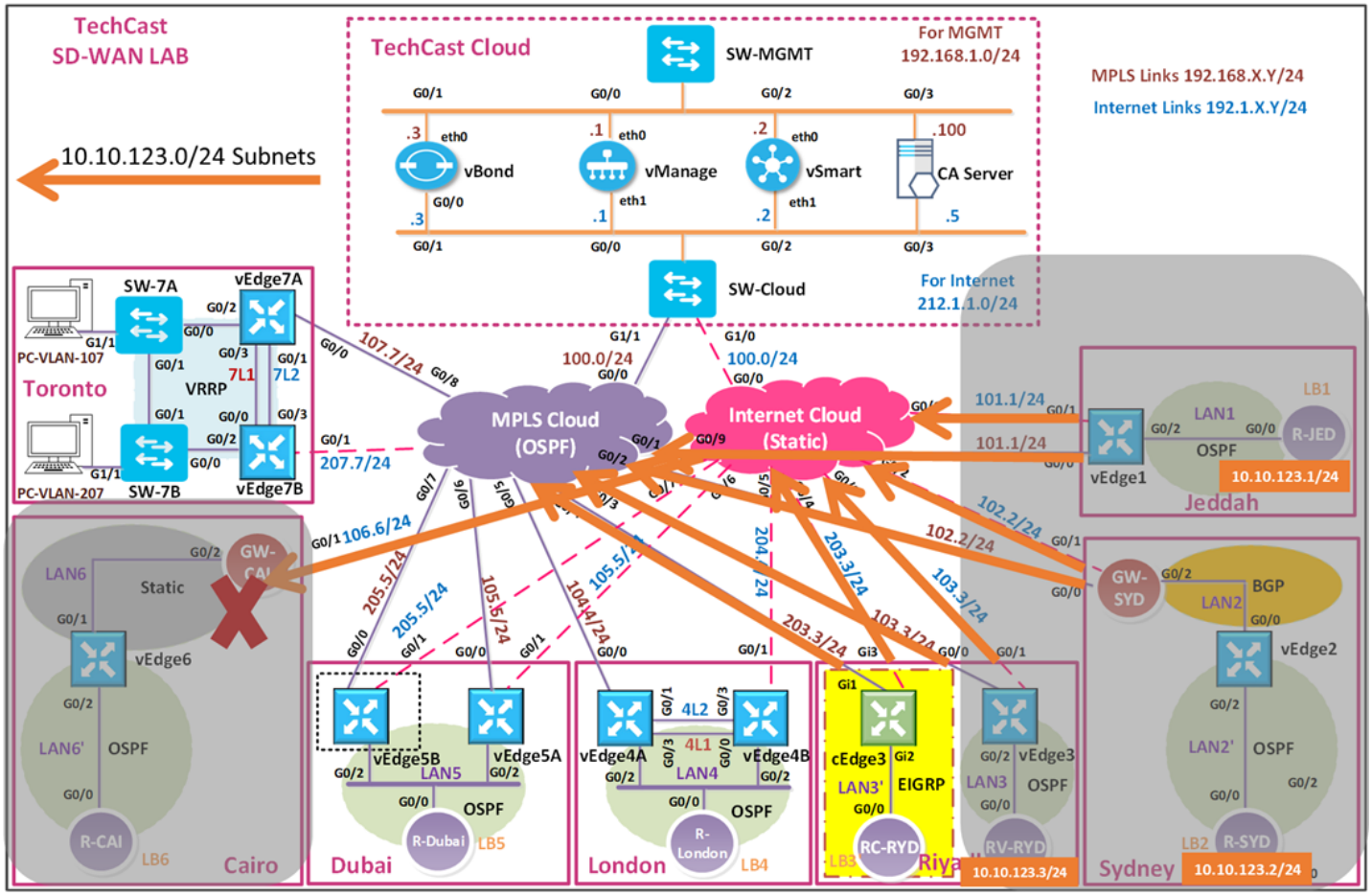
6.5.3 Step 3 – Modify the existing Centralized Policy "TechCast-Policy" and call the Topology Policy

- In vManage, Navigate to Configuration.

- Click **Topology** on the **Top** of the page.
- Click **Add Topology**.
- Click "**Import Existing"** and select the **RYD-Policy** from the drop- down list and click **Import**.
- Click **Policy Application** on the **Top** of the page.
- Click the "**Topology"** tab.
- The **RYD-Policy** Policy will be there. Click "**New Site"** button.
- Select **Dubai** in the Outbound Site List.
- Click **Add.**

- Click the **Save Policy Changes.**
- **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 (vEdge5A and vEdge5B).
- It should only have;
    - 2 TLOCs for Riyadh routes (200.200.200.203 – MPLS) and (200.200.200.213 – MPLS), whereas it will have;
    - 4 TLOCs for Toronto site (200.200.200.207-MPLS, 200.200.200.207-Biz-Internet, 200.200.200.217-MPLS, 200.200.200.217-Biz-Internet) as an example.
- Verify the policy by using the **Monitor -> Network ->vEdge5A/vEdge5B -> Troubleshooting -> Simulate Flows** Tool.

6.6 Lab 36 – Route Filtering



في هذا اللاب حنقوم بعملية فلتره للشبكات اللي المفروض ما ترسل لموقع تك كاست في القاهرة وهي 10.10.123.1/32, 10.10.123.2/24 & 10.10.123.3/24

6.6.1 Step 1 – Configure Groups of Interests/List that will be used for Route Filtering Policy for Cairo

- In vManage, Navigate to Configuration.

- Click **Prefix** and select **New Prefix list.** Create a policy based on the following:
  - NAME : **PLIST-123**
  - PREFIX LIST ENTRY: **10.10.123.0/24 LE 32**

- Add Cairo site by click **Site** and select **New Site list.** Create a policy based on the following:
  - NAME : **CAIRO**
  - SITE ID : **6**

6.6.2 Step 2 – Configure Control/Topology policy based on the Requirements

- In vManage, Navigate to **Configuration.**

Configuration > **Policies** > **Custom Options** > **Centralized Policy** > **Topology**

- Configure 1 Route Policy based on the following:
  - POLICY NAME : **DENY-123-IN-CAI**
  - DESCRIPTION : **DENY-123-IN- CAI**

Route Sequence

Match Conditions

- PREFIX LIST: **PLIST-123**

Action

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

Default Sequence

Action

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

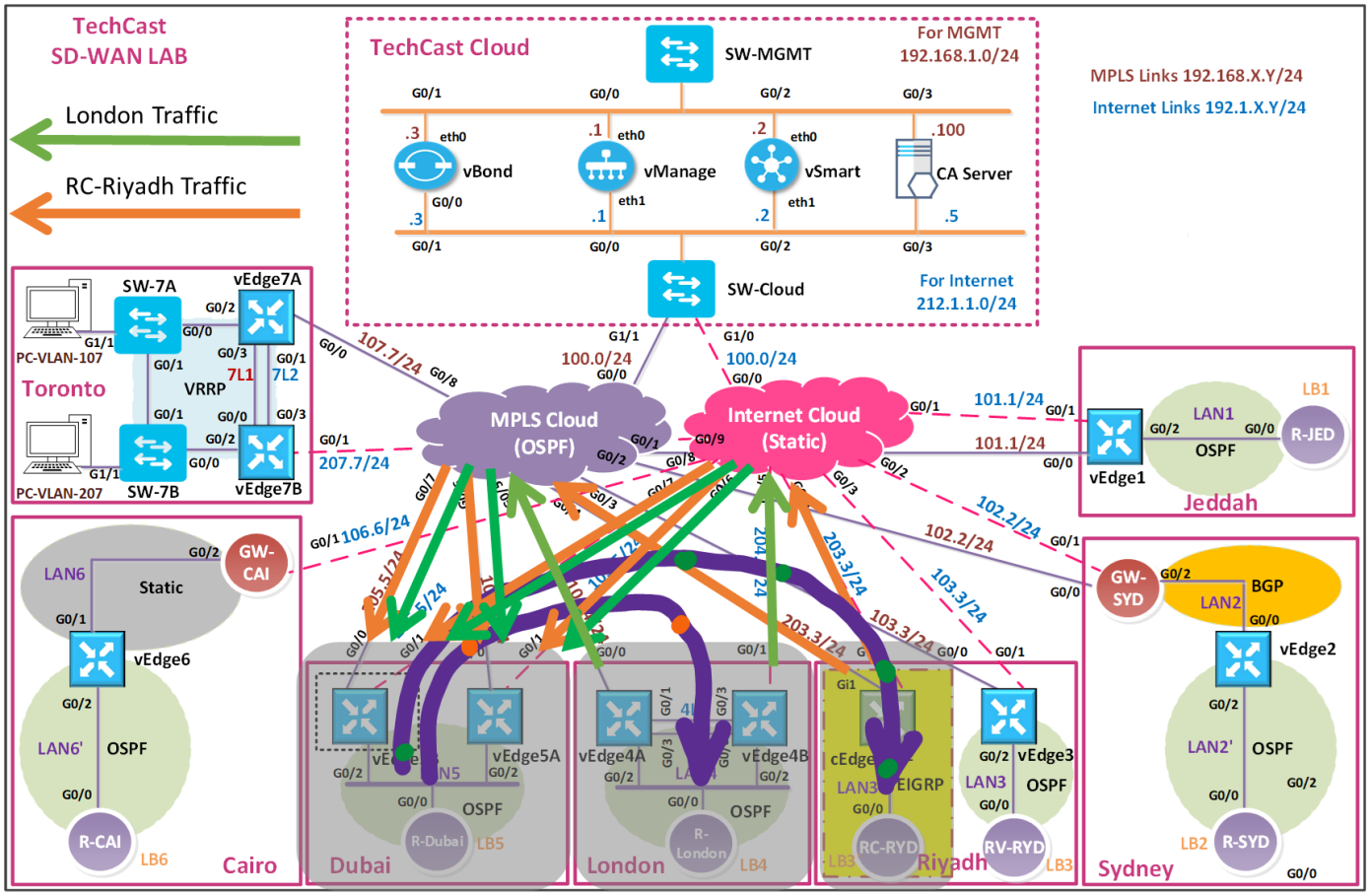
6.6.3 Step 3 – Modify the existing Centralized Policy "TechCast-Policy" and call the Topology Policy

- In vManage, Navigate to Configuration.

Configuration > **Policies** > **Centralized Policy** > **TechCast-Policy** > **"..."** > **Edit**

- Click **Topology** on the **Top** of the page.
- Click **Add Topology**.
- Click "**Import Existing"** and select the **DENY-123-IN-CAI** from the drop-down list and click **Import**.
- Click **Policy Application** on the **Top** of the page.
- Click the "**Topology"** tab.
- The **DENY-123-IN-CAI** will be there. Click "**New Site"** button.
- Select **Cairo** in the Outbound Site List.
- Click **Add.**
- Click the **Save Policy Changes.**
- **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 Cairo vEdge (vEdge6). You should not find 10.10.123.X/32 routes.
- Verify by using the **Show IP route ospf** command on the R-Cairo router. You should not find 10.10.123.X/32 routes.
- These 10.10.123.X/32 routes should be present in the other sites WAN Edges. You can use the **Show IP route vpn 1** command to verify it.

6.7 Lab 37 – Hub & Spoke Topology



- RC-Riyadh و London بيتواصلو مع بعض بشكل مباشر. تأكد من ذلك من خلال routes اللي بيستقبلوها وهذه routes يجب أن تكون موجهه بشكل مباشر على TLOCs للموقع الأخر.
- في هذا اللاب, نبغى نخلي كل الترافيك لهذين الموقعين يجب أن يتم توجيهه أو أرساله الى موقع تك كاست في Dubai. لتنفيذ هذا الحل حنستخدم TLOC list.

6.7.1 Step 1 – Configure Groups of Interests/List that will be used for Hub-n-Spoke

- In vManage, Navigate to Configuration.

- Just double check that you created VPN1 under VPN list or you can create it by click **VPN** and select **New VPN list.** Create 1 policy based on the following:

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

- Just double check that you created these sites under Site list or you can create them by Click **Site** and select **New Site list.** Create these sites based on the following:

  - Name : **Dubai**
  - Site ID : **5**

  - Name : **London**
  - Site ID : **4**

  - Name : **RC-Riyadh**
  - Site ID : **13**

- Click **TLOC** and select **New TLOC list.** Create 1 policies based on the following:

  - Name : **Dubai-TLOC**
  - **TLOCs**
    - **200.200.200.205 – MPLS – IPSec – 555**
    - **200.200.200.215 – MPLS – IPSec – 555**
    - **200.200.200.205 – BIZ-INTERNET – IPSec – 500**
    - **200.200.200.215 – BIZ-INTERNET – IPSec – 500**

Note, here we prefer MPLS link, but it can be equal.

6.7.2 Step 2 – Configure a Topology based on the Requirements

- In vManage, Navigate to Configuration.

- 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- RC-Riyadh

Match Conditions

- SITE: **RC-RIYADH**

Action

- TLOC: TLOC-LIST = **DUBAI-TLOC**

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

Default

Action

- ACCEPT

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

- Click **Save Control Policy**

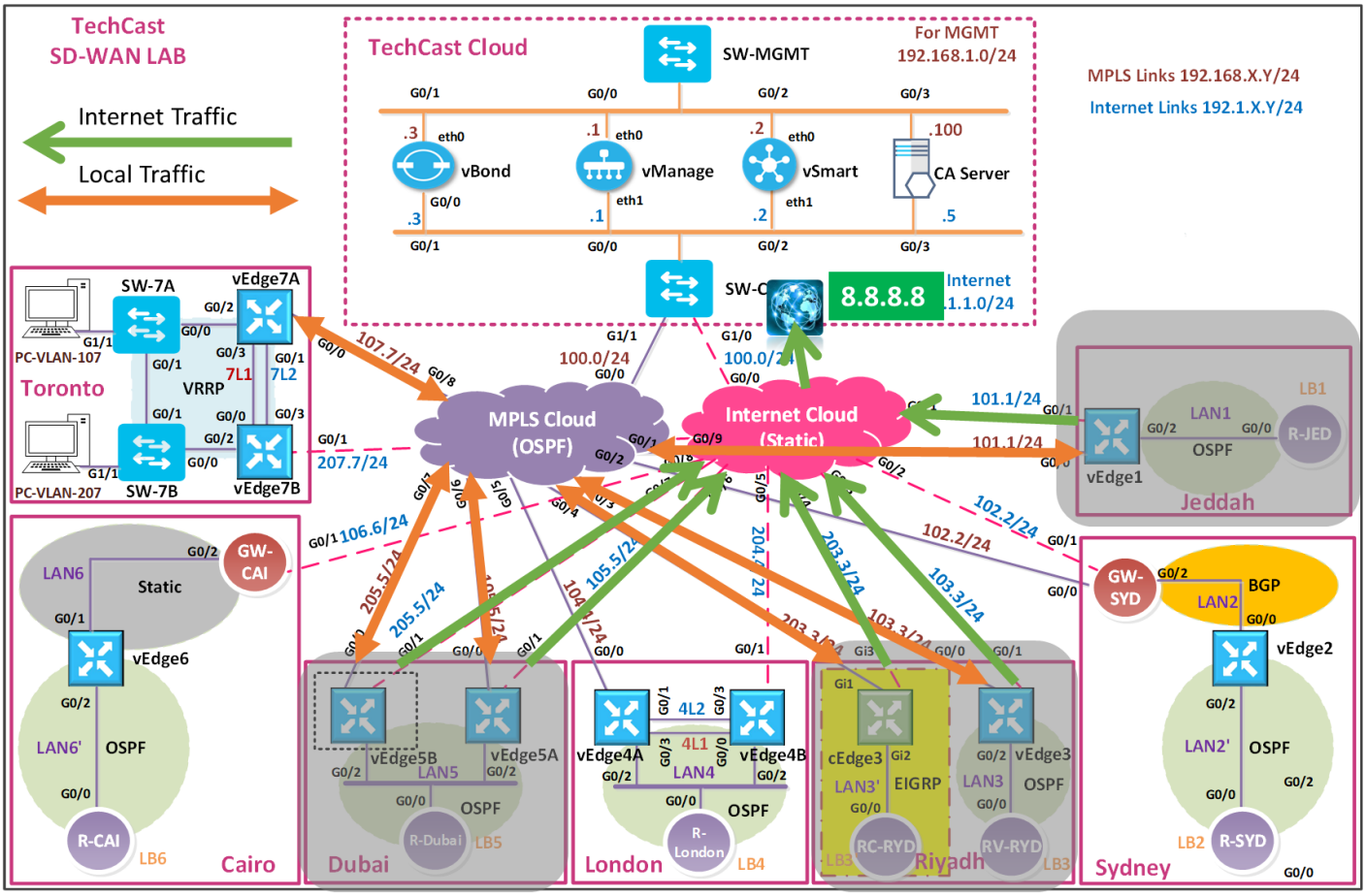
6.7.3 Step 3 – Modify the existing Centralized Policy "TechCast-Policy" and call the Traffic Policy

- In vManage, Navigate to Configuration.

- Click **Topology** on the **Top** of the page.
- Click **Add Topology**.
- Click "**Import Existing"** and select the **Hub-n-Spoke** from the drop-down list and click **Import**.
- Click **Policy Application** on the **Top** of the page.
- Click the "**Topology"** tab.
- The **Hub-n-Spoke** will be there. Click "**New Site"** button.
- Select **London and RC-Riyadh** in the Outbound Site List.

- Click **Add.**
- Click the **Save Policy Changes.**
- 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 in cEdge3 using **Show ip route vrf 1.** The routes should be pointing directly at the TLOCs of Dubai and all traffic will be forwarded thru Dubai.
- You can verify this by doing checking the routes in vEdge4A or vEdge4B using **Show ip routes omp.** The routes should be pointing directly at the TLOCs of Dubai and all traffic will be forwarded thru Dubai.
- Verify this in RC-Riyadh router by using traceroute and you should note that traffic goes to Hub site (Dubai) then to London site.

6.8 Lab 38 – Local Internet Breakout



في هذا اللاب نهدف الى تمكين المتسخدمين في مواقع تك كاست في جدة و الرياض ودبي من الوصول لشبكة الانترنت بشكل مباشر بدلا من انه الانترنت ترافيك يروح لل **DC** للوصول لبشكة الانترنت.

وهناك طريقيتين لعمل الكونفقريشن لل default route, اما manually في كل الروترات الداخلية مثل R-Jeddah على سبيل المثال نعمل كونفقريشن لل default route داخلها. والطريقة الثانية هو باستخدام VPN1 OSPF Template وتطبيقها على كل vEdges المرتبطة بهذه Template.

- اعمل كونفقريشن static default route في الراوترات الداخلية المتصلة ب vEdge/cEdge G0/2 interface.

OR

- اعمل كونفقريشن static default route باستخدام vEdge/cEdge templates.

6.8.1 Step 1 – Configure Default Route for vEdges

- Configure default route using vEdge templates by enabling “default-gateway originate” under VPN1 OSPF which will affect (vEdge1, vEdge3, vEdge5A and vEdge5B)
- In vManage, Navigate to Configuration.

- Click on **Advance** tab.
- Originate -> change it to "**Global**"
- Enable **Originate** by change it to -> "**On**"
- Always -> change it to "**Global**"
- Enable **Always** by change it to -> "**On**"
- Click on "**Update**"
- You will see the list of vEdges might impact by this change; Click "**Next**"
- Check configuration under VPN1 OSPF and you suppose to see command "**default-information originate always**" added.
- Click on "**Configure Devices**"
- Check the box of confirm configuration changes in these vEdges
- Wait till you get the "Success" status

6.8.2 Step 2 – Configure vEdges' outside interface to enable NATing;

- In vManage, Navigate to Configuration.

- Click on **NAT** tab.
  - NAT -> change it to "**Global**"
  - Enable **NAT** by change it to -> "**On**"
  - Click on "**Update**"
  - You will see the list of vEdges might impact by this change; Click "**Next**"
  - Check configuration under G0/1 and you suppose to see "NAT".
  - Click on "**Configure Devices**"
  - Check the box of confirm configuration changes in these vEdges
  - Wait till you get the "Success" status

6.8.3 Step 3 – Configure Default Route for cEdges

- Configure default route using CEdge templates by configuring static route toward Null0 and then redistribute static route into EIGRP AS 1;
  - In vManage, Navigate to Configuration.

  - Click on **IPv4 Route** tab.
  - Click on **New IPv4 Route** button and add the following;
    - PREFIX: **0.0.0.0/0**

- GATEWAY: **NULL0**
  - Enable Null0 -> change it to "**Global**"
  - Enable **Enable Null0** by change it to -> "**On**"
  - Click on "**Add**"
  - Click on "**Update**"
  - You will see the list of cEdges "i.e. cEdge3" might impact by this change; Click "**Next**"
  - Check configuration under VPN1 and you suppose to see command "**ip route vrf 1 0.0.0.0 0.0.0.0 Null0 1**" added.
  - Click on "**Configure Devices**"
  - Wait till you get the "Success" status

6.8.4 Step 4 – Configure Static Route redistribution into EIGRP AS1;

- In vManage, Navigate to Configuration.

Templates > **Feature** > **CE-VPN1-EIGRP** > **"..."** > **Edit**

- Click on **IPv4 Unicast Address Family** tab.
  - Click on "**RE-DISTRIBUTE"** tab.
  - Click on "**New Redistribute"** tab and select the following;
  - Protocol: **Static**
  - Click on "**Add**"
  - Click on "**Update**"
  - You will see the list of cEdges might impact by this change; Click "**Next**"
  - Check configuration under EIGRP and you suppose to see "redistribute static".
  - Click on "**Configure Devices**"
  - Wait till you get the "Success" status.

6.8.5 Step 5 – Configure cEdges' outside interface to enable NATing;

- In vManage, Navigate to Configuration.

Templates > **Feature** > **CE-VPN0-IF-Gi3** > **"..."** > **Edit**

- Click on **NAT** tab.
  - NAT -> change it to "**Global**"
  - Enable **NAT** by change it to -> "**On**"
  - Click on "**Update**"
  - You will see the list of cEdges might impact by this change; Click "**Next**"
  - Check configuration under Gi3 and you suppose to see "ip nat outside".
  - Click on "**Configure Devices**"
  - Check the box of confirm configuration changes in these vEdges

- Wait till you get the “Success” status.

6.8.6 Step 6 – Configure centralized policy to control which traffic to be NATTed;

- In vManage, Navigate to Configuration.

- Just double check that you created VPN1 under VPN list or you can create it by click **VPN** and select **New VPN list.** Create 1 policy based on the following:
  - NAME : **VPN1**
  - ID : **1**

- Just double check that you created these targeted sites under Site list or you can create them by Click **Site** and select **New Site list.** Create these sites based on the following:
  - NAME : **JEDDAH**
  - SITE ID : **1**

  - NAME : **RV-RIYADH**
  - SITE ID : **3**

  - NAME : **RC-RIYADH**
  - SITE ID : **13**

  - NAME : **DUBAI**
  - SITE ID : **5**

- Click **Data Prefix** and select **New Data Prefix list.** Create 1 policies based on the following:
  - NAME : **TECHCAST-NETWORKS**
  - ADD DATA PREFIX : **10.10.0.0/16**
  - Click on “Add”

- Click **Custom Options -> Centralized Policy -> Traffic Policy.**
  - Click on “**Traffic Data**” tab
  - Click on “**Add policy**” and click on “**Create New**”
    - NAME: **DIA-POLICY**
    - DESCRIPTION: **DIA-POLICY**
    - Click on “**Sequence Type**” and select “**Custom**”
    - Click on “**Sequence Rule**”

Match Conditions

- Select "**Source Data Prefix**" and "**Destination Data Prefix**"
- SOURCE DATA PREFIX LIST: **TECHCAST-NETWORKS**
- DESTINATION DATA PREFIX LIST: **TECHCAST-NETWORKS**

Action

- ENABLE IT BY SELECT "ACCEPT"

- Click on "**Save Match and Actions**"

- Copy the 1st Match Condition and edit it as per the following;

Match Conditions

- Select "**Source Data Prefix**" and "**Destination Data Prefix**"
- SOURCE DATA PREFIX LIST: **TECHCAST-NETWORKS**

Action

- Select "**NAT VPN**"

- Click on "**Save Match and Actions**"
- Click on "**Default Actions**" and select "**Accept**"

- Click on "**Save Data Policy**"

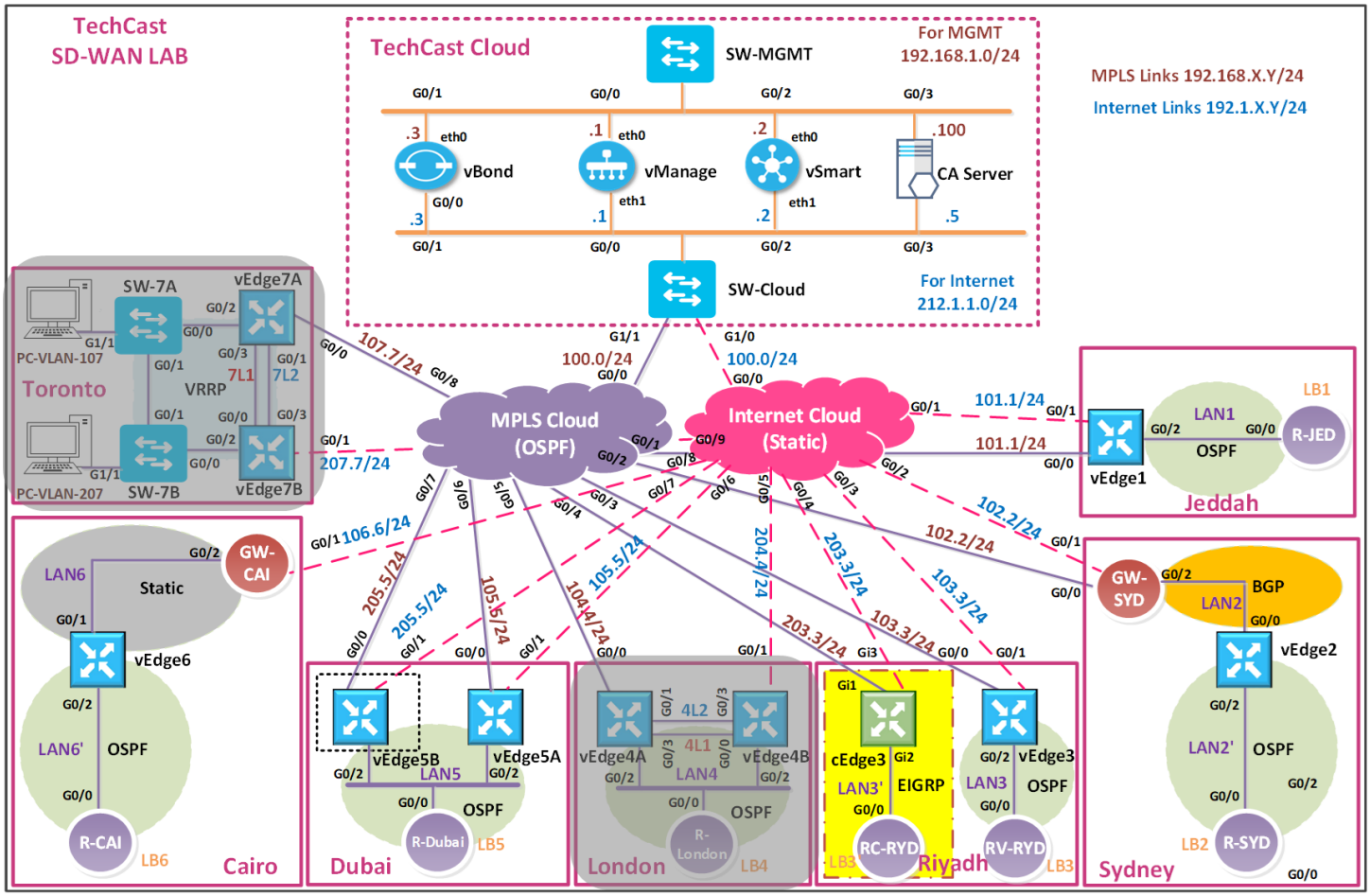
6.8.7 Step 7 – Apply DIA policy by modify the existing Centralized Policy "TechCast-Policy" and call the Traffic Policy

- In vManage, Navigate to Configuration.

- Click on **"Traffic Rules"** tab
- Click on **"Traffic Data"** tab
- Click on **"Add Policy"** and then select **"Import Existing"**
- Policy: "**DIA Policy**" and click "**Import**"
- Click on **"Policy Application"** tab
- Click on **"Traffic Data"** tab. We will see "DIA Policy" listed there.
- Click on **"New Site List and VPN List"** tab
- Select "**From Service**". It's by default selected.
- Select "**Site List**": Jeddah, RV-Riyadh, RC-Riyadh and Dubai
- Select "**VPN List**": Service_VPN_VPN 1
- Click on **"Add"**
- Click on **"Save Policy Changes"**
- Click on **"Activate"**
- Wait till you get the "**Success**" status.

- Wait for it to push the policy to the reachable vSmart Controller(s).
- You can verify this by doing the following in R-Jeddah, RV-Riyadh, RC-Riyadh and R-Dubai routers;
    - Check if do you receive default route pointing to vEdge as OE2 route or pointing to cEdge3 as D*EX route.
    - You should be able Ping or Telnet 8.8.8.8 with source interfaces (Loopback1, Loopback2, or Loopback3)
    - Also, you should be able Ping other TechCast-Networks for other sites as before with source interfaces (Loopback1, Loopback2, or Loopback3).

6.9 Lab 39 – QoS



في هذا اللاب, خلينا نفترض أنه عندنا لينك من مقدم الخدمة بسرعة 100Mbps وحابيين نعمل كونفقريشن QoS لل Voice, Web و Best Effort-BE ترافيك بناءا على المعطيات التالية:

Voice

- **Bandwidth = 35%**
- **Queue = 0**

Web

- **Bandwidth = 25%**
- **Queue = 1**

BE

- **Bandwidth = 40%**
- **Queue = 2**

6.9.1 Step 1 – Create Class-MAPs and Queue Mapping

- In vManage, Navigate to Configuration.

  - Create Voice Class-Map and tied it to Queue by clicking on "**New Class List**"
    - CLASS: **VOICE**
    - QUEUE: **0**
  - Create Web Class-Map and tied it to Queue by clicking on "**New Class List**"
    - CLASS: **WEB**
    - QUEUE: **1**
  - Create BE Class-Map and tied it to Queue by clicking on "**New Class List**"
    - CLASS: **BE**
    - QUEUE: **2**

6.9.2 Step 2 – Classify the traffic by creating ACL

- In vManage, Navigate to Configuration

- Click **Add Access Control Lists Policy**
- Click **Add IPv4 ACL Policy**
- Configure ACL Policy based on the following:
  - POLICY NAME : **TECHCAST-QOS-ACL**
  - DESCRIPTION : **TECHCAST-QOS-ACL**
  - CLICK ON **"ADD ACL SEQUENCE"**
  - CLICK ON **"SEQUENCE RULE"**

Voice

Match Conditions

- DSCP: **46**

Action

- CLASS: **VOICE**

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

Web

Match Conditions

- DESTINATION PORT: **80 443**

Action

- CLASS: **WEB**

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

BE

Action

- CLASS: **BE**

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

Default Sequence

Action

- ACCEPT

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

6.9.3 Step 3 – Assign the Bandwidth to Queue by creating QoS MAP (which called Scheduler)

- In vManage, Navigate to Configuration.

- Click **Add QoS Map** and Click **Create New**
- Configure ACL Policy based on the following:

- Policy Name : **TechCast-QOS-MAP**
- Description : **TechCast-QOS-MAP**

- Define bandwidth for **Web Traffic** by clicking on "**Add Queue**"
  - Queue: **1**
  - Bandwidth %: **25**
  - Buffer %: **25**
  - Drops: **Random Early** (because it's TCP traffic)
  - Click on **Save Queue**

- Define bandwidth for **BE Traffic** by clicking on "**Add Queue**"
  - Queue: **2**
  - Bandwidth %: **40**
  - Buffer %: **40**
  - Drops: **Tail**
  - Click on **Save Queue**
- Click **Save Policy.**

ملاحظة: "0" Queue ل voice ترافيك حيكون مضاف by default بشكل تلقائي.

6.9.4 Step 4 – Create Localized Policy and using created QoS MAP and ACL

- In vManage, Navigate to Configuration.

Configuration > **Policies** > **Localized Policy** > **Add Policy**

- Under "**Create Group of Interest**"
  - Click on "**Class Map**" and you should see the created class maps
  - Click "**Next**"

- Under "**Configure Forwarding Classes/QoS**"
  - Click on "**Add QoS Map**"
  - Click on "**Import Existing"**
  - Policy**: "TechCast-QOS-MAP"**
  - Click "**Import**"
  - Click "**Next**"
- Under "**Configure Access Control Lists**"
  - Click on "**Add Access Control Lists Policy**"
  - Click on "**Import Existing"**
  - Policy**: "TechCast-QOS-ACL"**
  - Click "**Import**"
  - Click "**Next**"

-
- Under "**Route Policy**"
  - Click "**Next**"
- Under "**Policy Overview**"
  - POLICY NAME: **TECHCAST-LOCALIZED-POLICY**
  - POLICY DESCRIPTION: **TECHCAST-LOCALIZED-POLICY**
  - Click "**Save Policy**"

6.9.5 Step 5 – Apply Localized Policy on vEdges through Device Templates

- In vManage, Navigate to **Configuration -> Templates -> Device;**
- Select London vEdge4A "**vEdge4A-DEV-TEMP**" device template.
- Click on "**Edit**" and go to "**Additional Templates**" section
- Click on "**Policy**" and select "**TechCast-Localized-Policy"**
- Click on "**Update**"
- Click on "**Next**"
- Check configuration on each vEdge device (optional).
- Click on "**Configure Devices**"
- Check the box of confirm configuration changes in these vEdges
- Wait till you get the "**Success**" status
- Repeat the same with other sites' vEdges "**vEdge4B-DEV-TEMP**", "**vEdge5A-DEV-TEMP**" and "**vEdge5B-DEV-TEMP**" device templates

6.9.6 Step 6 – Configure Shaping and QoS Mapping on VPN 0 Interfaces (Outgoing)

كل مواقع لندن وتورنتو عندهم **two VPN 0 interfaces** اللي هما **G0/0 0** متصل ب **MPLS Cloud** و **G0/1** المتصل ب **Internet Cloud**. وبالتالي نقدر ننفذه هذه الخطوة على كلاهما أو أي واحد منهما بناءا على احتياجات البزنس الخاص بشركتك.

خلينا نفترض هنا أنه سرعة لينك **Internet** لهذه المواقع مش **dedicated** وهذا معناته انه نحتاج **QoS** حتى نتمكن من **allocate the bandwidth and prioritize** للترافيك في حالة **congestion**. لذلك خلينا نركز في هذا اللاب على **VPN 0 G0/1 interface**.

- In vManage, Navigate to **Configuration -> Templates -> Feature;**
- Select "**TLOC-VE-VPN0-IF-G0/1**" device template.
- Click on "**Edit**"
- Click on "**ACL/QOS**" tab
  - Shaping Rate (Kbps) -> change it to "**Global**": **100,000**
  - QoS Map -> change it to "**Global**": **TechCast-QOS-MAP** **(Case sensitive)**
- Click on "**Update**"
- Click on "**Next**"
- Check configuration on each vEdge device (optional).
- Click on "**Configure Devices**"
- Check the box of confirm configuration changes in these vEdges

- Wait till you get the “Success” status

6.9.7 Step 7 – Apply Ingress ACL on G0/2 Incoming Traffic (Inbound Direction)

- In vManage, Navigate to **Configuration -> Templates -> Feature;**
- Select “**BR-VE-VPNINT-VPN1-G0/2**” device template.
- Click on “**Edit**”
- Click on “**ACL/QOS**” tab
  - Ingress ACL - IPv4 -> “**Global**” -> “**On**”
  - IPv4 Ingress Access List: **TechCast-QOS-ACL** **(Case sensitive)**
- Click on “**Update**”
- Click on “**Next**”
- Check configuration on each vEdge device (optional).
- Click on “**Configure Devices**”
- Check the box of confirm configuration changes in these vEdge
- Wait till you get the “**Success**” status.

TechCast

CCIE Enterprise Infrastructure Workbook