

Table of Contents

Lab1: Configure Service Provider #1 Topology with the following as below	3
Lab2: Configure iBGP for Service Provider 1	8
Lab 3: Configure Service Provider 2	11
Lab 4: Configure OSPF Authentication For Service Provider 2.....	13
Lab 5: Configure iBGP & Router Distribution for Service Provider 2.....	14
Lab 6: Configure MPLS Service Provider	16
Lab 7: Configure Headquarter Devices as per the diagram.....	22
Lab 8: Configure Data Center Devices as per the diagram and	26
Lab 9: Configure Base topology For	28
Lab 10: Configure eBGP relation between Service Provider 1 and Service Provider 2	34
Lab 11: Configure VLANs, DHCP & port-channels at Data Center.....	35
Lab 12: Configure BGP between Data Center and Service Provider #1	39
Lab 13: Configure BGP between Branch#8 and Service Provider #1	40
Lab 14: Configure BGP between Branch#6, Branch#9 and Service Provider #1.....	41
Lab 15: BGP path manipulation for Data Center	42
Lab 16: Configure DMVPN between DC (hub), Branch#6 (spoke) & Branch #8 (spoke) & Secure tunnel traffic using IPSEC	43
Lab 17: Configure named EIGRP on Branch #1 routers.....	45
Lab 18: Configure BGP between Branch#1 and Service Provider #1	46
Lab 19: Configure OSPF for Branch # 9.....	48
Lab 20: Create MPLS VPN between HQ1, BRANCH2 & BRANCH 3.....	51
Lab 21: SDWAN Troubleshooting.....	55
Lab 22: register your Vedges on Headquarter, Branch#4 and Branch #5 with Vmanage	58
Lab 23: SDWAN Templates for VPN0, VPN1 and OSPF	61
CCIE EI Design Questions	75

Lab1: Configure Service Provider #1 Topology with the following as below

- a) Base topology with IP addressing as per the diagram
- b) Configure IS-IS as IGP
 - o Configure IS-IS with the ISP using the following characteristics:
 - o **Area** – 49.0000
 - o **System-ID** –
 - **ISP-R1** – 0100.1111.1111
 - **ISP-R2** – 0100.2222.2222
 - **ISP-R3** – 0100.3333.3333
 - **ISP-R4** – 0100.4444.4444
 - **ISP-R5** – 0100.5555.5555
 - **ISP-R6-RR** – 0100.6666.6666
 - o **Level** – Level-2 Only
 - o **Metric-Style** – Wide

ISP1-R1

```
router isis
net 49.0000.0100.1111.1111.00
is-type level-2
metric-style wide

interface Loopback1
ip address 200.1.1.1 255.255.255.255
ip router isis

!
interface Ethernet0/0
ip address 192.168.10.1 255.255.255.0
ip router isis

duplex auto
!
interface Ethernet0/1
ip address 20.1.1.5 255.255.255.252
duplex auto
```

ISP1-R2

```
router isis
net 49.0000.0100.2222.2222.00
is-type level-2
metric-style wide

interface Loopback1
no shutdown
ip address 200.1.1.2 255.255.255.255
ip router isis

!
interface Ethernet0/0
no shutdown
ip address 192.168.10.2 255.255.255.0
```

```
ip router isis

duplex auto
!
interface Ethernet0/1
no shutdown
ip address 20.1.1.17 255.255.255.252
duplex auto
!
interface Ethernet0/2
no shutdown
ip address 20.1.1.21 255.255.255.252
duplex auto
```

ISP1-R3

```
router isis
net 49.0000.0100.3333.3333.00
is-type level-2
metric-style wide

interface Loopback1
no shutdown
ip address 200.1.1.3 255.255.255.255
ip router isis
!
interface Ethernet0/0
no shutdown
ip address 192.168.10.3 255.255.255.0
ip router isis
duplex auto
!
interface Ethernet0/1
no shutdown
ip address 20.1.1.25 255.255.255.252
duplex auto
```

ISP1-R4

```
router isis
net 49.0000.0100.4444.4444.00
is-type level-2
metric-style wide

interface Loopback1
no shutdown
ip address 200.1.1.4 255.255.255.255
ip router isis
!
interface Ethernet0/0
no shutdown
ip address 192.168.10.4 255.255.255.0
ip router isis
duplex auto
!
```

```
interface Ethernet0/1
  no shutdown
  ip address 20.1.1.29 255.255.255.252
  duplex auto
!
interface Ethernet0/2
  no shutdown
  ip address 20.1.1.33 255.255.255.252
  duplex auto
```

ISP1-R5

```
router isis
net 49.0000.0100.5555.5555.00
is-type level-2
metric-style wide

interface Loopback1
  no shutdown
  ip address 200.1.1.5 255.255.255.255
  ip router isis

!
interface Ethernet0/0
  no shutdown
  ip address 192.168.10.5 255.255.255.0
  ip router isis

  duplex auto
!
interface Ethernet0/1
  no shutdown
  ip address 20.1.1.37 255.255.255.252
  duplex auto
```

ISP1-RR

```
router isis
net 49.0000.0100.6666.6666.00
is-type level-2
metric-style wide

interface Loopback1
  no shutdown
  ip address 200.1.1.6 255.255.255.255
  ip router isis

!
interface Ethernet0/0
  no shutdown
  ip address 192.168.10.6 255.255.255.0
  ip router isis
  duplex auto
```

c) Secure your IGP using MD5

- Configure IS-IS to authenticate using MD5 authentication.
- Use a Key ID of 1 with a Key String of Cisco123

ISP1-R1

```
key chain Mohsin
key 1
key-string Cisco123
!
Interface E 0/0
isis authentication mode md5
isis authentication key-chain Mohsin
```

ISP1-R2

```
key chain Mohsin
key 1
key-string Cisco123
!
Interface E 0/0
isis authentication mode md5
isis authentication key-chain Mohsin
```

ISP1-R3

```
key chain Mohsin
key 1
key-string Cisco123
!
Interface E 0/0
isis authentication mode md5
isis authentication key-chain Mohsin
```

ISP1-R4

```
key chain Mohsin
key 1
key-string Cisco123
!
Interface E 0/0
isis authentication mode md5
isis authentication key-chain Mohsin
```

ISP1-R5

```
key chain Mohsin
key 1
key-string Cisco123
!
Interface E 0/0
isis authentication mode md5
```

```
isis authentication key-chain Mohsin
```

ISP1-RR

```
key chain Mohsin  
key 1  
key-string Cisco123  
!  
Interface E 0/0  
isis authentication mode md5  
isis authentication key-chain Mohsin
```

Lab2: Configure iBGP for Service Provider 1

Task1 - Create iBGP neighbors for ISP1 routers & RR

ISP1-R1

```
router bgp 200
 neighbor 200.1.1.6 remote-as 200
 neighbor 200.1.1.6 update-source Loopback1
 neighbor 200.1.1.6 next-hop-self
```

ISP1-R2

```
router bgp 200
 neighbor 200.1.1.6 remote-as 200
 neighbor 200.1.1.6 update-source Loopback1
 neighbor 200.1.1.6 next-hop-self
```

ISP1-R3

```
router bgp 200
 neighbor 200.1.1.6 remote-as 200
 neighbor 200.1.1.6 update-source Loopback1
 neighbor 200.1.1.6 next-hop-self
```

ISP1-R4

```
router bgp 200
 neighbor 200.1.1.6 remote-as 200
 neighbor 200.1.1.6 update-source Loopback1
 neighbor 200.1.1.6 next-hop-self
```

ISP1-R5

```
router bgp 200
 neighbor 200.1.1.6 remote-as 200
 neighbor 200.1.1.6 update-source Loopback1
 neighbor 200.1.1.6 next-hop-self
```

ISP1-RR

```
router bgp 200
 bgp log-neighbor-changes
 bgp listen range 200.1.1.0/24 peer-group PG
 neighbor PG peer-group
 neighbor PG remote-as 200
 neighbor PG update-source Loopback1
 neighbor PG route-reflector-client
```

Task2: Networks advertisement in BGP

- Ensure loopbacks are advertised to external neighbors not internal neighbors and it should be propagated with origin code as 'i', don't do this on router reflector
- Redistribute isis with origin of igp

ISP1-R1

```
ip prefix-list PL-L01 deny 200.1.1.0/24 le 32
ip prefix-list PL-L01 permit 0.0.0.0/0 le 32
!
route-map ML
match interface Loopback1
set origin igp
!
route-map RISIS
set origin igp
!
router bgp 200
redistribute connected route-map ML
redistribute isis route-map RISIS
neighbor 200.1.1.6 prefix-list PL-L01 out
```

ISP1-R2

```
ip prefix-list PL-L01 deny 200.1.1.0/24 le 32
ip prefix-list PL-L01 permit 0.0.0.0/0 le 32
!
route-map ML
match interface Loopback1
set origin igp
!
route-map RISIS
set origin igp
!
router bgp 200
redistribute connected route-map ML
redistribute isis route-map RISIS
neighbor 200.1.1.6 prefix-list PL-L01 out
```

ISP1-R3

```
ip prefix-list PL-L01 deny 200.1.1.0/24 le 32
ip prefix-list PL-L01 permit 0.0.0.0/0 le 32
!
route-map ML
match interface Loopback1
set origin igp
!
route-map RISIS
set origin igp
!
router bgp 200
redistribute connected route-map ML
redistribute isis route-map RISIS
neighbor 200.1.1.6 prefix-list PL-L01 out
```

ISP1-R4

```
ip prefix-list PL-L01 deny 200.1.1.0/24 le 32
ip prefix-list PL-L01 permit 0.0.0.0/0 le 32
!
route-map ML
match interface Loopback1
set origin igp
!
route-map RISIS
set origin igp
!
router bgp 200
redistribute connected route-map ML
redistribute isis route-map RISIS
neighbor 200.1.1.6 prefix-list PL-L01 out
```

ISP1-R5

```
ip prefix-list PL-L01 deny 200.1.1.0/24 le 32
ip prefix-list PL-L01 permit 0.0.0.0/0 le 32
!
route-map ML
match interface Loopback1
set origin igp
!
route-map RISIS
set origin igp
!
router bgp 200
redistribute connected route-map ML
redistribute isis route-map RISIS
neighbor 200.1.1.6 prefix-list PL-L01 out
```

Lab 3: Configure Service Provider 2

- Use OSPF as IGP protocol
- OSPF process 1 area 0
- Enable ospf on loopbacks **210.x.x.x/x**
- Secure OSPF using cryptographic algorithm sha-512
- Key chain Mohsin, key 1 & string ccie
- Enable bfd on OSPF and OSPF can detect the loss of a neighbor within 600 msec, with the probes being sent every 200 msec.
- Enable iBGP between routers and advertise networks, make sure loopbacks are not advertised in ibgp neighbors.
- Ensure loopbacks are advertised to external neighbors not internal neighbors and it should be propagated with origin code as 'i', don't do this on router reflector
- Redistribute ospf with origin of igp

ISP-2-R1

```
interface Loopback1
 ip address 210.1.1.1 255.255.255.255
!
interface Ethernet0/0
 ip address 192.168.20.1 255.255.255.0
 duplex auto
!
interface Ethernet0/1
 ip address 20.1.1.30 255.255.255.252
 duplex auto

router ospf 1
 network 192.168.20.0 0.0.0.255 area 0
 network 210.1.1.1 0.0.0.0 area 0
```

ISP-2-R2

```
interface Loopback1
 ip address 210.1.1.2 255.255.255.255
!
interface Ethernet0/0
 ip address 192.168.20.2 255.255.255.0
 duplex auto
!
interface Ethernet0/1
 ip address 21.1.1.30 255.255.255.252
 duplex auto

router ospf 1
 network 192.168.20.0 0.0.0.255 area 0
 network 210.1.1.1 0.0.0.0 area 0
```

ISP-2-R3

```
interface Loopback1
 ip address 210.1.1.3 255.255.255.255
!
interface Ethernet0/0
 ip address 192.168.20.3 255.255.255.0
 duplex auto
!
interface Ethernet0/1
 no ip address
 shutdown
 duplex auto
!
interface Ethernet0/2
 ip address 21.1.1.5 255.255.255.252
 duplex auto
router ospf 1
 network 192.168.20.0 0.0.0.255 area 0
 network 210.1.1.1 0.0.0.0 area 0
```

ISP-2-RR

```
interface Loopback1
 ip address 210.1.1.4 255.255.255.255
!
interface Ethernet0/0
 ip address 192.168.20.4 255.255.255.0
 duplex auto
```

Lab 4: Configure OSPF Authentication For Service Provider 2

OSPF Authentication

ISP-2-R1

```
key chain Mohsin
key 1
key-string ccie
cryptographic-algorithm hmac-sha-512

int e0/0
ip ospf authentication key-chain Mohsin
bfd interval 200 min_rx 200 multiplier 3
ip ospf bfd
```

ISP-2-R2

```
key chain Mohsin
key 1
key-string ccie
cryptographic-algorithm hmac-sha-512

int e0/0
ip ospf authentication key-chain Mohsin
bfd interval 200 min_rx 200 multiplier 3
ip ospf bfd
```

ISP-2-R3

```
key chain Mohsin
key 1
key-string ccie
cryptographic-algorithm hmac-sha-512

int e0/0
ip ospf authentication key-chain Mohsin
bfd interval 200 min_rx 200 multiplier 3
ip ospf bfd
```

ISP-2-RR

```
key chain Mohsin
key 1
key-string ccie
cryptographic-algorithm hmac-sha-512

int e0/0
ip ospf authentication key-chain Mohsin
bfd interval 200 min_rx 200 multiplier 3
ip ospf bfd
```

Lab 5: Configure iBGP & Router Distribution for Service Provider 2

iBGP

ISP-2-R1

```
router bgp 100

neighbor 210.1.1.4 remote-as 100
neighbor 210.1.1.4 update-source Loopback1
neighbor 210.1.1.4 next-hop-self
```

ISP-2-R2

```
router bgp 100

neighbor 210.1.1.4 remote-as 100
neighbor 210.1.1.4 update-source Loopback1
neighbor 210.1.1.4 next-hop-self
```

ISP-2-R3

```
router bgp 100

neighbor 210.1.1.4 remote-as 100
neighbor 210.1.1.4 update-source Loopback1
neighbor 210.1.1.4 next-hop-self
```

ISP-2-RR

```
router bgp 100
  bgp log-neighbor-changes
  bgp listen range 210.1.1.0/24 peer-group IRR
  neighbor IRR peer-group
  neighbor IRR remote-as 100
  neighbor IRR update-source Loopback1
  neighbor IRR route-reflector-client
```

BGP route distribution**ISP-2-R1**

```
ip prefix-list PL-L01 deny 210.1.1.0/24 le 32
ip prefix-list PL-L01 permit 0.0.0.0/0 le 32
!
route-map ML
match interface Loopback1
set origin igp
!
route-map RISIS
set origin igp
!
router bgp 100
redistribute connected route-map ML
redistribute ospf 1 route-map RISIS
neighbor 210.1.1.4 prefix-list PL-L01 out
```

ISP-2-R2

```
ip prefix-list PL-L01 deny 210.1.1.0/24 le 32
ip prefix-list PL-L01 permit 0.0.0.0/0 le 32
!
route-map ML
match interface Loopback1
set origin igp
!
route-map RISIS
set origin igp
!
router bgp 100
redistribute connected route-map ML
redistribute ospf 1 route-map RISIS
neighbor 210.1.1.4 prefix-list PL-L01 out
```

Lab 6: Configure MPLS Service Provider

- Use OSPF as IGP protocol
- OSPF process 1 area 0
- Enable ospf on loopbacks 100.1.1.0/24
- Secure OSPF using cryptographic algorithm sha-512
- Key chain Mohsin, key 1 & string ccie
- Enable iBGP between routers and advertise networks
- Configure LDP with in MPLS Service Provider
- Enable MP-iBGP for MPLS Service Provider

MPLS-PE-1

```
interface Loopback1
  ip address 100.1.1.1 255.255.255.255
!
interface Ethernet0/0
  no shutdown
  ip address 192.168.100.1 255.255.255.0
  duplex auto

interface Ethernet0/1
  no shutdown
  ip address 192.168.40.1 255.255.255.0
  duplex auto

router ospf 1
  network 100.1.1.1 0.0.0.0 area 0
  network 192.168.100.0 0.0.0.255 area 0
```

MPLS-PE-2

```
interface Loopback1
  ip address 100.1.1.2 255.255.255.255
!
interface Ethernet0/0
  no shutdown
  ip address 192.168.100.2 255.255.255.0
  duplex auto

interface Ethernet0/1
  no shutdown
  ip address 192.168.41.1 255.255.255.0
  duplex auto

router ospf 1
  network 100.1.1.1 0.0.0.0 area 0
  network 192.168.100.0 0.0.0.255 area 0
```

MPLS-PE-3

```
interface Loopback1
  ip address 100.1.1.4 255.255.255.255
!
interface Ethernet0/0
  no shutdown
  ip address 192.168.100.4 255.255.255.0
  duplex auto

interface Ethernet0/1
  no shutdown
  ip address 192.168.42.1 255.255.255.0
  duplex auto

router ospf 1
  network 100.1.1.1 0.0.0.0 area 0
  network 192.168.100.0 0.0.0.255 area 0
```

MPLS-RR

```
interface Loopback1
  ip address 100.1.1.3 255.255.255.255
!
interface Ethernet0/0
  no shutdown
  ip address 192.168.100.3 255.255.255.0
  duplex auto

router ospf 1
  network 100.1.1.1 0.0.0.0 area 0
  network 192.168.100.0 0.0.0.255 area 0
```

Enable OSPF Authentication

MPLS-PE-1

```
key chain Mohsin
key 1
key-string ccie
cryptographic-algorithm hmac-sha-512

int e0/0
ip ospf authentication key-chain Mohsin
```

MPLS-PE-2

```
key chain Mohsin
key 1
key-string ccie
cryptographic-algorithm hmac-sha-512

int e0/0
ip ospf authentication key-chain Mohsin
```

MPLS-PE-3

```
key chain Mohsin
key 1
key-string ccie
cryptographic-algorithm hmac-sha-512

int e0/0
ip ospf authentication key-chain Mohsin
```

MPLS-RR

```
key chain Mohsin
key 1
key-string ccie
cryptographic-algorithm hmac-sha-512

int e0/0
ip ospf authentication key-chain Mohsin
```

Enable iBGP between routers and advertise networks**MPLS-PE-1**

```
router bgp 150
  bgp log-neighbor-changes
  neighbor 100.1.1.3 remote-as 150
  neighbor 100.1.1.3 update-source Loopback1
```

MPLS-PE-2

```
router bgp 150
  bgp log-neighbor-changes
  neighbor 100.1.1.3 remote-as 150
  neighbor 100.1.1.3 update-source Loopback1
```

MPLS-PE-3

```
router bgp 150
  bgp log-neighbor-changes
  neighbor 100.1.1.3 remote-as 150
  neighbor 100.1.1.3 update-source Loopback1
```

MPLS-RR

```
router bgp 150
  bgp log-neighbor-changes
  neighbor 100.1.1.1 remote-as 150
  neighbor 100.1.1.1 update-source Loopback1
  neighbor 100.1.1.2 remote-as 150
  neighbor 100.1.1.2 update-source Loopback1
  neighbor 100.1.1.4 remote-as 150
  neighbor 100.1.1.4 update-source Loopback1
```

Configure LDP with in MPLS Service Provider**MPLS-PE-1**

```
mpls label protocol ldp
mpls ldp router-id loopback1
!
Interface E 0/0
mpls ip
```

MPLS-PE-2

```
mpls label protocol ldp
mpls ldp router-id loopback1
!
Interface E 0/0
mpls ip
```

MPLS-PE-3

```
mpls label protocol ldp
mpls ldp router-id loopback1
!
Interface E 0/0
mpls ip
```

MPLS-RR

```
mpls label protocol ldp
mpls ldp router-id loopback1
!
Interface E 0/0
mpls ip
```

Enable MP-iBGP for MPLS Service Provider**MPLS-PE-1**

```
router bgp 150
address-family vpnv4
  neighbor 100.1.1.3 activate
  neighbor 100.1.1.3 send-community extended
exit-address-family
```

MPLS-PE-2

```
router bgp 150
address-family vpnv4
  neighbor 100.1.1.3 activate
  neighbor 100.1.1.3 send-community extended
exit-address-family
```

MPLS-PE-3

```
router bgp 150
address-family vpnv4
  neighbor 100.1.1.3 activate
  neighbor 100.1.1.3 send-community extended
exit-address-family
!
```

MPLS-RR

```
router bgp 150
address-family vpnv4
  neighbor 100.1.1.1 activate
  neighbor 100.1.1.1 send-community extended
  neighbor 100.1.1.1 route-reflector-client
  neighbor 100.1.1.2 activate
  neighbor 100.1.1.2 send-community extended
  neighbor 100.1.1.2 route-reflector-client
  neighbor 100.1.1.4 activate
  neighbor 100.1.1.4 send-community extended
  neighbor 100.1.1.4 route-reflector-client
exit-address-family
```

Lab 7: Configure Headquarter Devices as per the diagram

enable OSPF on the interfaces

VLAN 100 for SDWAN devices on HQ-SW2

HQ-SW2

```
Vlan 100
  name SDWAN

interface Ethernet0/0
  no switchport
  ip address 10.10.204.1 255.255.255.0
  ip ospf 1 area 0
!
interface Ethernet0/1
  no switchport
  ip address 10.10.206.1 255.255.255.0
  ip ospf 1 area 0
!
interface Ethernet0/2
  no switchport
  ip address 10.10.205.1 255.255.255.0
  ip ospf 1 area 0
!
interface Ethernet0/3
  switchport access vlan 100
  switchport mode access
!
interface Ethernet2/3
  no switchport
  ip address 10.10.207.1 255.255.255.0
  ip ospf 1 area 0
!
interface Ethernet3/1
  switchport access vlan 100
  switchport mode access
!
interface Ethernet3/2
  switchport access vlan 100
  switchport mode access
!
interface Ethernet3/3
  no switchport
  ip address 10.10.200.1 255.255.255.0
  ip ospf 1 area 0
!
interface Vlan100
  ip address 90.90.90.1 255.255.255.0
  ip ospf 1 area 0
!
router ospf 1
```

HQ-SW1

```
interface Ethernet0/0
  no switchport
  ip address 10.10.208.1 255.255.255.0
  ip ospf 1 area 0
!
interface Ethernet0/1
  no switchport
  ip address 10.10.209.1 255.255.255.0
  ip ospf 1 area 0
!
interface Ethernet0/2
!
interface Ethernet0/3
  no switchport
  ip address 10.10.210.1 255.255.255.0
  ip ospf 1 area 0
!
interface Ethernet1/2
  no switchport
  ip address 10.10.220.1 255.255.255.0
  ip ospf 1 area 0
!
interface Ethernet2/3
  no switchport
  ip address 10.10.207.2 255.255.255.0
  ip ospf 1 area 0
```

HQ-SW3

```
interface Ethernet0/0
  no switchport
  ip address 10.10.213.1 255.255.255.0
  ip ospf 1 area 0
!
interface Ethernet0/1
  no switchport
  ip address 10.10.204.2 255.255.255.0
  ip ospf 1 area 0
!
interface Ethernet0/2
  no switchport
  ip address 10.10.211.1 255.255.255.0
  ip ospf 1 area 0
!
interface Ethernet0/3
  no switchport
  ip address 10.10.212.1 255.255.255.0
  ip ospf 1 area 0
!
interface Ethernet1/0
  no switchport
  ip address 10.10.250.1 255.255.255.0
```

HQ-SW4

```
interface Ethernet0/1
  no switchport
  ip address 10.10.210.2 255.255.255.0
  ip ospf 1 area 0
!
interface Ethernet0/2
  no switchport
  ip address 10.10.211.2 255.255.255.0
  ip ospf 1 area 0
!
interface Ethernet0/3
  no switchport
  ip address 10.10.214.1 255.255.255.0
  ip ospf 1 area 0
!
interface Ethernet1/0
  no switchport
  ip address 10.10.215.1 255.255.255.0
  ip ospf 1 area 0
```

R36

```
interface Ethernet0/0
  no switchport
  ip address 10.10.215.2 255.255.255.0
  ip ospf 1 area 0
!
interface Ethernet0/1
  no switchport
  ip address 10.10.212.2 255.255.255.0
  ip ospf 1 area 0
!
interface Ethernet0/2
  no switchport
  ip address 10.10.216.1 255.255.255.0
  ip ospf 1 area 0
```

HQ-1

```
interface Ethernet0/0
  ip address 192.168.42.2 255.255.255.0
  duplex auto
!
interface Ethernet0/1
  ip address 10.10.216.2 255.255.255.0
  ip ospf 1 area 0
  duplex auto
```

Vedge-HQ

```
interface GigabitEthernet2
 ip address 10.10.250.2 255.255.255.0
```

R23

```
interface Loopback1
 ip address 160.1.1.1 255.255.255.0
 ip ospf 1 area 0
!
interface Ethernet0/0
 ip address 25.25.25.1 255.255.255.0
 ip ospf 1 area 0
 duplex auto
!
```

Lab 8: Configure Data Center Devices as per the diagram and

- Vlan 10 – 10.20.10.0/24 should be part of OSPF process 1
- Vlan 20 – 10.20.20.0/24 should be part of OSPF process 1
- Base configuration and add interfaces in OSPF process 1 as per diagram

R59

```
interface Ethernet1/0
  switchport access vlan 10
!
interface Ethernet1/1
  switchport access vlan 20
!

interface Vlan10
  ip address 10.20.10.1 255.255.255.0
  ip ospf 1 area 0
!
interface Vlan20
  ip address 10.20.20.1 255.255.255.0
  ip ospf 1 area 0
```

R3

```
interface Ethernet1/0
  no switchport
  ip address 10.10.217.1 255.255.255.0
  ip ospf 1 area 0
!
interface Ethernet1/1
  no switchport
  ip address 10.10.209.2 255.255.255.0
  ip ospf 1 area 0
!
interface Vlan10
  ip address 10.20.10.100 255.255.255.0
  ip ospf 1 area 0
```

R58

```
interface Ethernet1/0
  no switchport
  ip address 10.10.218.1 255.255.255.0
  ip ospf 1 area 0
!
interface Ethernet1/1
  no switchport
  ip address 10.10.206.2 255.255.255.0
  ip ospf 1 area 0
!
interface Vlan20
  ip address 10.20.20.100 255.255.255.0
  ip ospf 1 area 0
```

DC-R1

```
interface Ethernet0/0
 ip address 20.1.1.6 255.255.255.252
 duplex auto
!
interface Ethernet0/1
 ip address 10.10.217.2 255.255.255.0
 ip ospf 1 area 0
 duplex auto
```

DC-R2

```
interface Loopback1
 ip address 172.16.9.1 255.255.255.0
!
!
interface Ethernet0/1
 ip address 20.1.1.10 255.255.255.252
 duplex auto
!
ip route 0.0.0.0 0.0.0.0 20.1.1.9
```

DC-R3

```
interface Ethernet0/1
 ip address 10.10.218.2 255.255.255.0
 ip ospf 1 area 0

interface Ethernet0/0
 ip address 20.1.1.162 255.255.255.252
 duplex auto
```

Lab 9: Configure Base topology For

- Branch # 1
- Branch # 2
- Branch # 3
- Branch # 4
- Branch # 5
- Branch # 6
- Branch # 8
- Branch # 9

Branch1-R1

```
interface Ethernet0/0
 ip address 20.1.1.26 255.255.255.0
 duplex auto
!
interface Ethernet0/1
 ip address 192.168.80.1 255.255.255.0
 duplex auto
!
interface Ethernet0/2
 ip address 192.168.81.1 255.255.255.0
 duplex auto
```

Branch1-R2

```
interface Ethernet0/0
 ip address 20.1.1.34 255.255.255.252
 duplex auto
!
interface Ethernet0/1
 ip address 192.168.80.2 255.255.255.0
 duplex auto
!
interface Ethernet0/2
 ip address 192.168.82.2 255.255.255.0
 duplex auto
```

Branch1-R3

```
interface Ethernet0/0
 ip address 192.168.81.2 255.255.255.0
 duplex auto
!
interface Ethernet0/1
 ip address 192.168.82.1 255.255.255.0
 duplex auto
```

Branch2-Router

```
interface Ethernet0/0
 ip address 192.168.40.2 255.255.255.0
 duplex auto

interface Ethernet0/1
 ip address 10.10.10.1 255.255.255.0
 duplex auto
```

Branch2-Server

```
interface Ethernet0/0
 ip address 10.10.10.2 255.255.255.0
 duplex auto

ip route 0.0.0.0 0.0.0.0 10.10.10.1
```

Branch3-Router

```
interface Ethernet0/0
 ip address 192.168.41.2 255.255.255.0
 duplex auto

interface Ethernet0/1
 ip address 10.20.60.1 255.255.255.0
 duplex auto
```

Branch3-Server

```
interface Ethernet0/0
 ip address 10.20.60.2 255.255.255.0
 duplex auto

ip route 0.0.0.0 0.0.0.0 10.20.60.1
```

Branch-4-Vedge

```
config-transaction
!  
interface GigabitEthernet2  
no shutdown  
ip address 20.1.1.18 255.255.255.252  
!  
ip route 0.0.0.0 0.0.0.0 20.1.1.17  
!  
interface Tunnell  
no shutdown  
ip unnumbered GigabitEthernet2  
tunnel source GigabitEthernet2  
tunnel mode sdwan  
exit  
!  
sdwan  
interface GigabitEthernet2  
tunnel-interface  
encapsulation ipsec  
color default  
allow-service all  
allow-service sshd  
allow-service netconf  
exit  
exit  
commit
```

Branch-5-Vedge

```
config-transaction  
!  
interface GigabitEthernet2  
no shutdown  
ip address 20.1.1.22 255.255.255.252  
!  
ip route 0.0.0.0 0.0.0.0 20.1.1.21  
!  
interface Tunnell  
no shutdown  
ip unnumbered GigabitEthernet2  
tunnel source GigabitEthernet2  
tunnel mode sdwan  
exit  
!  
sdwan  
interface GigabitEthernet2  
tunnel-interface  
encapsulation ipsec  
color default  
allow-service all  
allow-service sshd  
allow-service netconf  
exit  
exit
```

```
commit
```

Branch #6

BR6-Spoke

```
interface Ethernet0/1
 ip address 21.1.1.29 255.255.255.252
 duplex auto

interface Ethernet0/0
 ip address 172.16.11.1 255.255.255.0
 duplex auto

ip route 0.0.0.0 0.0.0.0 21.1.1.30
```

Branch6-PC

```
interface Ethernet0/1
 ip address 172.16.11.2 255.255.255.0
 duplex auto

ip route 0.0.0.0 0.0.0.0 172.16.11.1
```

Branch #8

BR8-Spoke

```
interface Ethernet0/0
 ip address 20.1.1.38 255.255.255.252
 duplex auto

interface Ethernet0/1
 ip address 172.16.10.1 255.255.255.250
 duplex auto

ip route 0.0.0.0 0.0.0.0 20.1.1.37
```

Branch #9

BR9-R1

```
interface Ethernet0/0
 ip address 21.1.1.6 255.255.255.252
 duplex auto
!
interface Ethernet0/1
 ip address 192.168.50.1 255.255.255.252
 duplex auto
!
interface Ethernet0/2
 ip address 192.168.50.5 255.255.255.252
 duplex auto
```

BR9-R2

```
interface Loopback1
 ip address 150.1.60.1 255.255.255.255
!
interface Ethernet0/0
 ip address 192.168.50.2 255.255.255.252
 duplex auto
!
interface Ethernet0/1
 ip address 192.168.50.13 255.255.255.252
 duplex auto
!
interface Ethernet0/2
 ip address 192.168.50.9 255.255.255.252
 duplex auto
```

BR9-R3

```
interface Loopback1
 ip address 150.1.60.2 255.255.255.255
!
interface Ethernet0/0
 ip address 192.168.50.14 255.255.255.252
 duplex auto
!
```

BR9-R4

```
interface Loopback1
 ip address 150.1.60.3 255.255.255.255
!
interface Ethernet0/0
 ip address 192.168.50.6 255.255.255.252
 duplex auto
!
interface Ethernet0/1
 ip address 192.168.50.10 255.255.255.252
 duplex auto
!
interface Ethernet0/2
 ip address 192.168.50.17 255.255.255.252
 duplex auto
```

BR9-R5

```
interface Loopback1
 ip address 150.1.60.4 255.255.255.255
!
interface Ethernet0/0
 ip address 192.168.50.18 255.255.255.252
 duplex auto
!
```

Lab 10: Configure eBGP relation between Service Provider 1 and Service Provider 2

- Secure your eBGP relationship with a key Cisco123
- For loopbacks on each ISPs, only send summary addresses with a mask of /24

ISP-1-R4

```
router bgp 200

neighbor 20.1.1.30 remote-as 100
neighbor 20.1.1.30 password Cisco123
```

ISP-2-R3

```
router bgp 100

neighbor 20.1.1.29 remote-as 100
neighbor 20.1.1.29 password Cisco123
```

ISP-1-R4

```
router bgp 200

aggregate-address 200.1.1.0 255.255.255.0 summary-only
```

ISP-2-R3

```
router bgp 100

aggregate-address 210.1.1.0 255.255.255.0 summary-only
```

Lab 11: Configure VLANs, DHCP & port-channels at Data Center & Branch 8

- Create DHCP pools for VLAN 10 & VLAN 20 respectively
- VLAN 10 named as Sales, VLAN 20 named as HR
- Use LACP to establish the Port-Channel
- Configure the Port-Channel as a Trunk using Dot1q Trunking (3 switches on Data centre)
- Ensure access ports for VLAN 10 & VLAN 20 bypass learning & listening states
- Configure VLAN 30, VLAN 40 at branch 8, use eigrp as routing protocol
- Configure L3 port-channels as per the topology

R59

```
VLAN 10
  Name sales
VLAN 20
  Name HR
ip dhcp pool VLAN10
  network 10.20.10.0 255.255.255.0
  default-router 10.20.10.1
!
ip dhcp pool VLAN20
  network 10.20.20.0 255.255.255.0
  default-router 10.20.20.1

interface Port-channel10
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
interface Port-channel20
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
interface Ethernet0/0
  switchport trunk encapsulation dot1q
  switchport mode trunk
  channel-group 10 mode active
!
interface Ethernet0/1
  switchport trunk encapsulation dot1q
  switchport mode trunk
  channel-group 10 mode active
!
interface Ethernet0/2
  switchport trunk encapsulation dot1q
  switchport mode trunk
  channel-group 20 mode active
!
interface Ethernet0/3
  switchport trunk encapsulation dot1q
  switchport mode trunk
  channel-group 20 mode active
!
interface Ethernet1/0
  switchport access vlan 10
!
interface Ethernet1/1
  switchport access vlan 20
```

R3	R58
<pre>Vlan 10 interface Port-channel10 switchport trunk encapsulation dot1q switchport mode trunk ! interface Port-channel30 switchport trunk encapsulation dot1q switchport mode trunk ! interface Ethernet0/0 switchport trunk encapsulation dot1q switchport mode trunk channel-group 30 mode active ! interface Ethernet0/1 switchport trunk encapsulation dot1q switchport mode trunk channel-group 30 mode active ! interface Ethernet0/2 switchport trunk encapsulation dot1q switchport mode trunk channel-group 10 mode active ! interface Ethernet0/3 switchport trunk encapsulation dot1q switchport mode trunk channel-group 10 mode active</pre>	<pre>Vlan 20 interface Port-channel20 switchport trunk encapsulation dot1q switchport mode trunk ! interface Port-channel30 switchport trunk encapsulation dot1q switchport mode trunk ! interface Ethernet0/0 switchport trunk encapsulation dot1q switchport mode trunk channel-group 30 mode active ! interface Ethernet0/1 switchport trunk encapsulation dot1q switchport mode trunk channel-group 30 mode active ! interface Ethernet0/2 switchport trunk encapsulation dot1q switchport mode trunk channel-group 20 mode active ! interface Ethernet0/3 switchport trunk encapsulation dot1q switchport mode trunk channel-group 20 mode active</pre>

R59
<pre>interface Ethernet1/0 spanning-tree portfast ! interface Ethernet1/1 spanning-tree portfast</pre>

R28

```
interface Port-channel1
  no switchport
  ip address 10.10.15.5 255.255.255.252
!
interface Port-channel2
  no switchport
  ip address 10.10.15.9 255.255.255.252
!
interface Ethernet0/0
  no switchport
  no ip address
  channel-group 2 mode active
!
interface Ethernet0/1
  no switchport
  no ip address
  channel-group 2 mode active
!
interface Ethernet0/2
  no switchport
  no ip address
  channel-group 1 mode active
!
interface Ethernet0/3
  no switchport
  no ip address
  channel-group 1 mode active
!
interface Ethernet1/0
  switchport access vlan 30
!
interface Ethernet1/1
  switchport access vlan 40
!
!
interface Vlan30
  ip address 10.10.30.1 255.255.255.0
!
interface Vlan40
  ip address 10.10.40.1 255.255.255.0
!
!
router eigrp 1
  network 10.10.0.0 0.0.255.255
```

R17

```
interface Port-channel2
  no switchport
  ip address 10.10.15.10 255.255.255.252
!
interface Port-channel3
  no switchport
  ip address 10.10.15.2 255.255.255.252
!
interface Ethernet0/0
  no switchport
  no ip address
  channel-group 3 mode active
!
interface Ethernet0/1
  no switchport
  no ip address
  channel-group 3 mode active
!
interface Ethernet0/2
  no switchport
  no ip address
  channel-group 2 mode active
!
interface Ethernet0/3
  no switchport
  no ip address
  channel-group 2 mode active
!
interface Ethernet1/0
  no switchport
  ip address 172.16.10.3 255.255.255.0
!
interface Ethernet1/1
!
interface Ethernet1/2
!
interface Ethernet1/3
!
!
router eigrp 1
  network 10.10.0.0 0.0.255.255
  network 172.16.10.0 0.0.0.255
```

R16

```
interface Port-channel1
  no switchport
  ip address 10.10.15.6 255.255.255.252
!
interface Port-channel3
  no switchport
  ip address 10.10.15.1 255.255.255.252
!
interface Ethernet0/0
  no switchport
  no ip address
  channel-group 3 mode active
!
interface Ethernet0/1
  no switchport
  no ip address
  channel-group 3 mode active
!
interface Ethernet0/2
  no switchport
  no ip address
  channel-group 1 mode active
!
interface Ethernet0/3
  no switchport
  no ip address
  channel-group 1 mode active
!
interface Ethernet1/0
  no switchport
  ip address 172.16.10.2 255.255.255.0
!
interface Ethernet1/1
!
interface Ethernet1/2
!
interface Ethernet1/3
!
!
router eigrp 1
  network 10.10.0.0 0.0.255.255
  network 172.16.10.0 0.0.0.255
!
```

Lab 12: Configure BGP between Data Center and Service Provider #1

- Redistribute ospf into BGP from Data Center to Service Provider # 1
- Ensure routers in Data center receive only Service provider networks i.e. 20.1.1.0/24 & 21.1.1.0/24
- Advertise your connected interfaces (not loopbacks) of ISP-R1 to all other routers

DC-R1

```
router bgp 65001
  bgp log-neighbor-changes
  redistribute ospf 1
  neighbor 20.1.1.5 remote-as 200
```

DC-R3

```
router bgp 65001
  bgp log-neighbor-changes
  redistribute ospf 1
  neighbor 20.1.1.161 remote-as 200
```

DC-R2-hub

```
router bgp 65530
  bgp log-neighbor-changes
  neighbor 20.1.1.9 remote-as 200
```

ISP-R1

```
ip prefix-list ISP-R1-OUT seq 10 permit 20.1.1.0/24 le 32
ip prefix-list ISP-R1-OUT seq 20 permit 21.1.1.0/24 le 32

route-map CON-INT
  match interface e0/1 e0/2 e0/3

router bgp 200
  neighbor 20.1.1.6 remote-as 65001
  neighbor 20.1.1.162 remote-as 65001
  neighbor 20.1.1.10 remote-as 65530
  neighbor 20.1.1.6 prefix-list ISP-R1-OUT out
  neighbor 20.1.1.162 prefix-list ISP-R1-OUT out
  neighbor 20.1.1.10 prefix-list ISP-R1-OUT out
  redistribute connected route-map CON-INT
```

Lab 13: Configure BGP between Branch#8 and Service Provider #1

- Ensure routers in Branch#1 receive only Service provider networks i.e. 20.1.1.0/24 & 21.1.1.0/24 & 90.90.90.0/24 (For SDWAN)
- Advertise your connected interfaces (not loopbacks) of ISP-5 to all other routers

Branch8-Spoke

```
router bgp 65532
  bgp log-neighbor-changes
  neighbor 20.1.1.37 remote-as 200
```

ISP-1-R5

```
ip prefix-list ISP-R1-OUT seq 10 permit 20.1.1.0/24 le 32
ip prefix-list ISP-R1-OUT seq 20 permit 21.1.1.0/24 le 32
ip prefix-list ISP-R1-OUT seq 30 permit 90.90.90.0/24 le 32

route-map CON-INT
  match interface e0/1

router bgp 200
  neighbor 20.1.1.38 remote-as 65532
  neighbor 20.1.1.38 prefix-list ISP-R1-OUT out
  redistribute connected route-map CON-INT
```

Lab 14: Configure BGP between Branch#6, Branch#9 and Service Provider #1

- Ensure routers in Branch#1 receive only Service provider networks i.e. 20.1.1.0/24 & 21.1.1.0/24 & 90.90.90.0/24 (for SDWAN only towards Branch#6)
- Advertise your connected interfaces (not loopbacks) of ISP-5 to all other routers

Branch6-Spoke

```
router bgp 65002
  bgp log-neighbor-changes
  neighbor 21.1.1.30 remote-as 100
```

Branch9-R1

```
router bgp 65004
  bgp log-neighbor-changes
  neighbor 21.1.1.5 remote-as 100
```

ISP-2-R2

```
ip prefix-list ISP-R1-OUT seq 10 permit 20.1.1.0/24 le 32
ip prefix-list ISP-R1-OUT seq 20 permit 21.1.1.0/24 le 32
ip prefix-list ISP-R1-OUT seq 30 permit 90.90.90.0/24 le 32
```

```
route-map CON-INT
  match interface e0/1
```

```
router bgp 100
  neighbor 21.1.1.29 remote-as 65002
  neighbor 21.1.1.29 prefix-list ISP-R1-OUT out
  redistribute connected route-map CON-INT
```

ISP-2-R3

```
ip prefix-list ISP-R1-OUT seq 10 permit 20.1.1.0/24 le 32
ip prefix-list ISP-R1-OUT seq 20 permit 21.1.1.0/24 le 32
```

```
route-map CON-INT
  match interface e0/2
```

```
router bgp 100
  neighbor 21.1.1.6 remote-as 65004
  neighbor 21.1.1.6 prefix-list ISP-R1-OUT out
  redistribute connected route-map CON-INT
```

Lab 15: BGP path manipulation for Data Center

- Create iBGP for DC-R1 & DC-R3 although they're not directly connected, for multi-hop use maximum hop limit as 3
- For outbound traffic use DC-R1 as preferred path
- For inbound traffic use DC-R2 as preferred path

DC-R1

```
router bgp 65001
  bgp log-neighbor-changes
  neighbor 10.10.218.2 remote-as 65001
  neighbor 10.10.218.2 ebgp-multihop 3
```

DC-R3

```
router bgp 65001
  bgp log-neighbor-changes
  neighbor 10.10.217.2 remote-as 65001
  neighbor 10.10.217.2 ebgp-multihop 3
```

- (default Local Pref value is 100, so we will increase it for outbound traffic)
- (For incoming traffic, MED is 0 by default so we will change MED size on DC-R1 making it worse)

DC-R1

```
route-map DC-R1-LP
  set local-preference 120
route-map DC-R1-MED
  set metric 120
router bgp 65001
  neighbor 20.1.1.5 route-map DC-R1-LP in
  neighbor 20.1.1.5 route-map DC-R1-MED out
```

Lab 16: Configure DMVPN between DC (hub), Branch#6 (spoke) & Branch #8 (spoke) & Secure tunnel using IPSEC

- Ensure Branch#8 sends VLAN30, VLAN 40 subnets only to Hub and spoke

DC-R2-Hub

```
interface Loopback1
 ip address 172.16.9.1 255.255.255.0
!
interface Tunnell
 ip address 192.168.1.1 255.255.255.0
 tunnel source E0/0
 tunnel mode gre multipoint
 ip nhrp network-id 1
 ip nhrp map multicast dynamic
 no ip split-horizon eigrp 1

router eigrp 1
 network 172.16.9.0 0.0.0.255
 network 192.168.1.0
```

Branch6-Spoke

```
interface Loopback1
 ip address 172.16.11.1 255.255.255.0
!
interface Tunnell
 ip address 192.168.1.3 255.255.255.0
 ip nhrp map 192.168.1.1 20.1.1.10
 ip nhrp map multicast 20.1.1.10
 ip nhrp nhs 192.168.1.1
 tunnel source Ethernet0/1
 tunnel mode gre multipoint
 ip nhrp network-id 1

router eigrp 1
 network 172.16.11.0 0.0.0.255
 network 192.168.1.0
```

Branch8-Spoke

```
interface Loopback1
 ip address 172.16.10.1 255.255.255.0
!
interface Tunnell
 ip address 192.168.1.2 255.255.255.0
 ip nhrp map 192.168.1.1 20.1.1.10
 ip nhrp map multicast 20.1.1.10
 ip nhrp network-id 1
 ip nhrp nhs 192.168.1.1
 tunnel source Ethernet0/0
 tunnel mode gre multipoint

router eigrp 1
 network 172.16.11.0 0.0.0.255
 network 192.168.1.0
```

For phase II

DC-R2-Hub

```
Interface Tunnel1
no ip next-hop-self eigrp 1
```

For phase III

DC-R2-Hub

```
Interface Tunnel 1
ip nhrp redirect
```

Branch8-Spoke

```
Interface Tunnel 1
ip nhrp shortcut
```

Branch6-Spoke

```
Interface Tunnel 1
ip nhrp shortcut
```

Configuring IPSEC On DC-R2-Hub, Branch8-Spoke & Branch6-Spoke

```
crypto isakmp policy 10
  encr 3des
  hash md5
  authentication pre-share
  group 2
crypto isakmp key mohsin123 address 0.0.0.0
!
!
crypto ipsec transform-set TS esp-3des esp-sha-hmac
mode tunnel
!
crypto ipsec profile DMVPNPROF
set transform-set TS

Interface Tunnel1
tunnel protection ipsec profile IPROF
```

Ensure Branch-spoke only sends 172.16.10.0/24, VLAN 30 & VLAN 40 networks to Hub and other spokes

Branch-Spoke

```
ip prefix-list VLANS seq 5 permit 10.10.30.0/24 le 32
ip prefix-list VLANS seq 10 permit 10.10.40.0/24 le 32
ip prefix-list VLANS seq 15 permit 172.16.10.0/24 le 32
ip prefix-list VLANS seq 20 permit 172.16.11.0/24 le 32
ip prefix-list VLANS seq 25 permit 172.16.9.0/24 le 32
router eigrp 1
  distribute-list prefix VLANS out eigrp 1
```

Lab 17: Configure named EIGRP on Branch #1 routers

- Eigrp name should be CCIE and AS 65003
- Configure EIGRP to authenticate the neighbor relationships using SHA authentication with a password of Cisco123

Branch1-R3

```
interface Loopback1
 ip address 101.1.1.1 255.255.255.0

router eigrp CCIE
 address-family ipv4 unicast autonomous-system 65003
  network 101.1.1.0 255.255.255.0
  network 192.168.81.0
  network 192.168.82.0
af-interface Ethernet0/0
 authentication mode hmac-sha-256 Cisco123
af-interface Ethernet0/1
 authentication mode hmac-sha-256 Cisco123
```

Branch1-R1

```
router eigrp CCIE
 address-family ipv4 unicast autonomous-system 65003
  network 192.168.81.0
  network 192.168.80.0
af-interface Ethernet0/2
 authentication mode hmac-sha-256 Cisco123
af-interface Ethernet0/1
 authentication mode hmac-sha-256 Cisco123
```

Branch1-R2

```
router eigrp CCIE
 address-family ipv4 unicast autonomous-system 65003
  network 192.168.82.0
  network 192.168.80.0
af-interface Ethernet0/2
 authentication mode hmac-sha-256 Cisco123
af-interface Ethernet0/1
 authentication mode hmac-sha-256 Cisco123
```

Lab 18: Configure BGP between Branch#1 and Service Provider #1

- Configure iBGP between all routers in Branch #1
- Ensure routers in Branch#1 receive only Service provider networks i.e. 20.1.1.0/24 & 21.1.1.0/24
- Advertise your connected interfaces (not loopbacks) of ISP-R3 & ISP-R4 to all other routers
- Ensure Branch#1 R2, use both ISPs to go out
- redistribute eigrp (Branch#1) in to bgp only 101.1.1.0/24 network

Branch1-R1

```
router bgp 65003
  bgp log-neighbor-changes
  neighbor 20.1.1.25 remote-as 200
  neighbor 192.168.80.2 remote-as 65003
  neighbor 192.168.81.2 remote-as 65003
```

Branch1-R2

```
router bgp 65003
  bgp log-neighbor-changes
  neighbor 20.1.1.33 remote-as 200
  neighbor 192.168.80.1 remote-as 65003
  neighbor 192.168.82.1 remote-as 65003
```

Branch1-R3

```
router bgp 65003
  bgp log-neighbor-changes
  neighbor 192.168.81.1 remote-as 65003
  neighbor 192.168.82.2 remote-as 65003
```

ISP-1-R3

```
ip prefix-list ISP-R1-OUT seq 10 permit 20.1.1.0/24 le 32
ip prefix-list ISP-R1-OUT seq 20 permit 21.1.1.0/24 le 32

route-map CON-INT
  match interface e0/1

router bgp 200
  neighbor 20.1.1.26 remote-as 65003
  neighbor 20.1.1.26 prefix-list ISP-R1-OUT out
  redistribute connected route-map CON-INT
```

ISP-1-R4

```
ip prefix-list ISP-R1-OUT seq 10 permit 20.1.1.0/24 le 32
ip prefix-list ISP-R1-OUT seq 20 permit 21.1.1.0/24 le 32

route-map CON-INT
  match interface e0/2 e0/1

router bgp 200
  neighbor 20.1.1.34 remote-as 65003
  neighbor 20.1.1.34 prefix-list ISP-R1-OUT out
  redistribute connected route-map CON-INT
```

Branch1-R2

```
router bgp 65003
  maximum-paths eibgp 2
```

On both routers Branch1-R1 & Branch1-R2

```
ip prefix-list EIGRP-RED seq 5 permit 101.1.1.0/24 le 32
!
route-map REB permit 10
  match ip address EIGRP-RED

router bgp 65003
  bgp log-neighbor-changes
  redistribute eigrp 65003 route-map REB
```

Lab 19: Configure OSPF for Branch # 9

- Configure OSPF in Branch 9 for Area 0, Area 10 and Area 20
- Configure the Router-IDs based on the following:
 - Branch9-R1 – 0.0.0.1
 - Branch9-R2 – 0.0.0.2
 - Branch9-R3 – 0.0.0.3
 - Branch9-R4 – 0.0.0.4
 - Branch9-R5 – 0.0.0.5
- Configure loopbacks on each router as 150.1.60.x and advertise them in respective area
- Redistribute BGP routers into OSPF using metric type 1 and with a metric 200
- Redistribute your OSPF routes only 150.1.60.x into BGP and ensure they're propagated with an origin code of "i"
- Configure Area 10 such that no external routes are propagated into it.
- Area 10 should maintain full reachability towards them.
- Configure Area 20 such that no backbone external routes are propagated into it.
- Area 20 should maintain full reachability towards the Backbone external routes.
- Default-Route should be injected in as a Type 7 LSA.

Branch9-R1

```
interface Loopback1
 ip address 150.1.60.1 255.255.255.255

router ospf 1
 router-id 0.0.0.1
 network 192.168.50.0 0.0.0.3 area 0
 network 192.168.50.4 0.0.0.3 area 0
 network 150.1.60.1 255.255.255.255 area 0
```

Branch9-R2

```
interface Loopback1
 ip address 150.1.60.2 255.255.255.255

router ospf 1
 router-id 0.0.0.2

network 192.168.50.0 0.0.0.3 area 0
network 192.168.50.8 0.0.0.3 area 0
network 192.168.50.12 0.0.0.3 area 10
network 150.1.60.2 255.255.255.255 area 10
```

Branch9-R3

```
interface Loopback1
 ip address 150.1.60.3 255.255.255.255

router ospf 1
 router-id 0.0.0.3
 network 150.1.60.3 0.0.0.0 area 10
 network 192.168.50.12 0.0.0.3 area 10
```

Branch9-R4

```
interface Loopback1
 ip address 150.1.60.4 255.255.255.255

router ospf 1
 router-id 0.0.0.4
 network 150.1.60.4 0.0.0.0 area 20
 network 192.168.50.4 0.0.0.3 area 0
 network 192.168.50.8 0.0.0.3 area 0
 network 192.168.50.16 0.0.0.3 area 20
```

Branch9-R5

```
interface Loopback1
 ip address 150.1.60.5 255.255.255.255

router ospf 1
 router-id 0.0.0.5
 network 150.1.60.5 0.0.0.0 area 20
 network 192.168.50.16 0.0.0.3 area 20
```

Branch9-R1

```
router ospf 1
 redistribute bgp 65004 metric-type 1 metric 200

ip prefix-list PL-1 permit 150.1.60.0/24 le 32
!
route-map O2B
 match ip address prefix PL-1
 set origin igp

router bgp 65115
 redistribute ospf 1 route-map O2B match internal external
```

Another Scenario: Redistribute BGP routes as type 2 in to OSPF

```
router ospf 1
 redistribute bgp 65004 metric-type 2 metric 200
```

Area 10 as Stub	Area 20 as NSSA
Branch9-R2 router ospf 1 area 10 stub	Branch9-R4 router ospf 1 area 20 nssa default-information-originate
Branch9-R3 router ospf 1 area 10 stub	Branch9-R5 router ospf 1 area 20 nssa

Lab 20: Create MPLS VPN between HQ1, BRANCH2 & BRANCH 3

- On HQ-1 router, ensure you only send 10.10.216.0/24 route into BGP
- Redistribute routes from BGP 65000 into OSPF process
- Create a common VRF named as GREEN on all routers

HQ-1

```
ip prefix-list OSPF seq 5 permit 10.10.216.0/24 le 32

route-map OUT
 match ip address prefix-list OSPF

router ospf 1
 redistribute bgp 65000 subnets
 !
router bgp 65000
 bgp log-neighbor-changes
 redistribute ospf 1 route-map OUT
 neighbor 192.168.42.1 remote-as 150
```

MPLS-PE-3

```
vrf definition GREEN
 rd 100:1
 !
 address-family ipv4
  route-target export 100:1
  route-target import 100:1
 exit-address-family

interface Ethernet0/1
 vrf forwarding GREEN

router bgp 150
 address-family ipv4 vrf GREEN
  neighbor 192.168.42.2 remote-as 65000
  neighbor 192.168.42.2 activate
 exit-address-family
```

MPLS VPN using BGP

MPLS-PE-1

```
vrf definition GREEN
rd 100:1
!
address-family ipv4
 route-target export 100:1
 route-target import 100:1
exit-address-family

interface Ethernet0/1
 vrf forwarding GREEN

router bgp 150

address-family ipv4 vrf GREEN
 neighbor 192.168.40.2 remote-as 65044
 neighbor 192.168.40.2 activate
exit-address-family
```

BR2-Router

```
router bgp 65044
 bgp log-neighbor-changes
 network 10.10.10.0 mask 255.255.255.0
 neighbor 192.168.40.1 remote-as 150
```

MPLS-PE-2

```
vrf definition GREEN
rd 100:1
!
address-family ipv4
 route-target export 100:1
 route-target import 100:1
exit-address-family

interface Ethernet0/1
 vrf forwarding GREEN

router bgp 150

address-family ipv4 vrf GREEN
 neighbor 192.168.41.2 remote-as 65045
 neighbor 192.168.41.2 activate
exit-address-family
```

BR3-Router

```
router bgp 65045
 bgp log-neighbor-changes
 network 10.20.60.0 mask 255.255.255.0
 neighbor 192.168.41.1 remote-as 150
!
```

MPLS VPN using EIGRP/OSPF & Redistribution in BGP

MPLS-PE-1	Branch #2
<pre> router bgp 150 no address-family ipv4 vrf GREEN router eigrp 1 address-family ipv4 vrf GREEN autonomous-system 1 network 192.168.40.0 redistribute bgp 150 metric 10 10 10 10 10 ! router bgp 150 address-family ipv4 vrf GREEN redistribute eigrp 1 </pre>	<pre> no router bgp 65044 router eigrp 1 network 10.10.10.0 mask 255.255.255.0 network 192.168.40.0 </pre>
MPLS-PE-2	Branch #2
<pre> router bgp 150 no address-family ipv4 vrf GREEN router ospf 6 vrf GREEN network 192.168.41.0 0.0.0.255 area 0 redistribute bgp 150 subnets ! router bgp 150 address-family ipv4 vrf GREEN redistribute ospf 6 </pre>	<pre> no router bgp 65044 router ospf 6 network 10.20.60.0 0.0.0.255 area 0 network 192.168.41.0 0.0.0.255 area 0 </pre>

Communication between different VRF's

MPLS-PE	MPLS-PE-1
<pre>vrf definition YELLOW rd 100:20 ! address-family ipv4 route-target export 100:20 route-target import 100:1 interface Ethernet0/1 vrf forwarding YELLOW ip address 192.168.42.1 255.255.255.0 duplex auto router bgp 150 address-family ipv4 vrf YELLOW neighbor 192.168.42.2 remote-as 65000 neighbor 192.168.42.2 activate exit-address-family</pre>	<pre>vrf definition GREEN rd 100:1 ! address-family ipv4 route-target export 100:1 route-target import 100:1 route-target import 100:20 exit-address-family</pre>
	<div style="background-color: #c8e6c9; padding: 2px;">MPLS-PE-2</div> <pre>vrf definition GREEN rd 100:1 ! address-family ipv4 route-target export 100:1 route-target import 100:1 route-target import 100:20 exit-address-family</pre>

Lab 21: SDWAN Troubleshooting

Issue#1, Vmanage is unable to communicate to Vbond, resolve the issue

Vmanage

```
system
host-name          vmanage
system-ip          1.1.1.1
site-id            1
organization-name  ABC-SDWAN
vbond 10.2.250.11
```

Solution

```
vmanage# config terminal
Entering configuration mode terminal
vmanage(config)# system
vmanage(config-system)# vbond 90.90.90.3
vmanage(config-system)# commit
```

Issue#2, Vbond is unable to ping VLAN100 GW for Headquarters, RESOLVE IT !!**Vbond**

```
system
host-name          vbond
system-ip          1.1.1.2
site-id            2
organization-name  ABC-SDWAN
vbond 10.2.250.11 local

vpn 0
interface ge0/0
ip address 10.2.250.11/24
ipv6 dhcp-client
tunnel-interface
encapsulation ipsec
no allow-service bgp
allow-service dhcp
allow-service dns
allow-service icmp
no allow-service sshd
no allow-service netconf
no allow-service ntp
no allow-service ospf
no allow-service stun
allow-service https
!
no shutdown
!
ip route 0.0.0.0/0 10.2.250.1
```

Solution

```
vbond# config terminal
Entering configuration mode terminal
vbond(config)# system
vbond(config-system)# vbond 90.90.90.3 local

vbond(config)# vpn 0
vbond(config-vpn-0)# interface ge0/0
vbond(config-interface-ge0/0)# ip address 90.90.90.3/24
vbond(config-interface-ge0/0)# exit
vbond(config-vpn-0)# ip route 0.0.0.0/0 90.90.90.1
vbond(config-vpn-0)# commit
```

Issue#3, Vsmart is showing down in Vmanage Gui, Find and fix the issue

VSmart

```
system
host-name          vsmart
system-ip          1.1.1.3
site-id            3
admin-tech-on-failure
no vrrp-advt-with-phymac
organization-name  ABC-SDWAN
vbond 10.60.60.4

vpn 0
interface eth0
ip address 22.22.22.1/24
tunnel-interface
allow-service dhcp
allow-service dns
allow-service icmp
no allow-service sshd
no allow-service netconf
no allow-service ntp
no allow-service stun
!
no shutdown
!
ip route 0.0.0.0/0 23.23.23.1
```

Solution

```
system
host-name          vsmart
system-ip          1.1.1.3
site-id            3
admin-tech-on-failure
no vrrp-advt-with-phymac
organization-name  ABC-SDWAN
vbond 90.90.90.3

vpn 0
interface eth0
ip address 90.90.90.4/24
tunnel-interface
allow-service dhcp
allow-service dns
allow-service icmp
no allow-service sshd
no allow-service netconf
no allow-service ntp
no allow-service stun
!
no shutdown
!
ip route 0.0.0.0/0 90.90.90.1
```

Lab 22: register your Vedges on Headquarter, Branch#4 and Branch #5 with Vmanage**ISP-1-R2**

```
route-map CON-INT
  match interface e0/1 e0/2

router bgp 200
  redistribute connected route-map CON-INT
```

Branch-4-Vedge

```
config-transaction
!
hostname BR-4-Vedge
!
system
system-ip 1.1.5.2
site-id 5
organization-name ABC-SDWAN
vbond 90.90.90.3

interface GigabitEthernet2
no shutdown
ip address 20.1.1.18 255.255.255.252
!
ip route 0.0.0.0 0.0.0.0 20.1.1.17
!
interface Tunnell
no shutdown
ip unnumbered GigabitEthernet2
tunnel source GigabitEthernet2
tunnel mode sdwan
exit
!
sdwan
interface GigabitEthernet2
tunnel-interface
encapsulation ipsec
color default
allow-service all
allow-service sshd
allow-service netconf
exit
exit
commit
```

Branch-5-Vedge

```
config-transaction
!
hostname BR-5-Vedge
!
system
system-ip 1.1.6.2
site-id 6
organization-name ABC-SDWAN
vbond 90.90.90.3

interface GigabitEthernet2
no shutdown
ip address 20.1.1.22 255.255.255.252
!
ip route 0.0.0.0 0.0.0.0 20.1.1.21
!
interface Tunnell
no shutdown
ip unnumbered GigabitEthernet2
tunnel source GigabitEthernet2
tunnel mode sdwan
exit
!
sdwan
interface GigabitEthernet2
tunnel-interface
encapsulation ipsec
color default
allow-service all
allow-service sshd
allow-service netconf
exit
exit
commit
```

HQ-Vedge

```
config-transaction
!  
hostname HQ-Vedge  
  
!  
system  
system-ip 1.1.7.2  
site-id 7  
organization-name ABC-SDWAN  
vbond 90.90.90.3  
  
interface GigabitEthernet2  
no shutdown  
ip address 10.10.250.2 255.255.255.254  
!  
ip route 0.0.0.0 0.0.0.0 10.10.250.1  
!  
interface Tunnell  
no shutdown  
ip unnumbered GigabitEthernet2  
tunnel source GigabitEthernet2  
tunnel mode sdwan  
exit  
!  
sdwan  
interface GigabitEthernet2  
tunnel-interface  
encapsulation ipsec  
color default  
allow-service all  
allow-service sshd  
allow-service netconf  
exit  
exit  
commit
```

Lab 23: SDWAN Templates for VPN0, VPN1 and OSPF

- Configure a VPN Template to be used by all branches for VPN0
- Configure a VPN Template to be used by all branches for VPN1
- Configure a OSPF Template to be used by all branches for VPN 1

Create template for VPN0 (Internet), VPN1 (Service VPN and enable OSPF)

Parameters	Vedge-HQ	Vedge-BR4	Vedge-BR5
Gi2	10.10.250.2/24	20.1.1.18/30	20.1.1.22/30
ISP GW	10.10.250.1	20.1.1.17	20.1.1.21
Gi3	25.25.25.2/24	26.26.26.1/24	27.27.27.1/24

Template for VPN-0

Manage, Navigate to Configuration -> Templates -> Feature Templates-> CSR8000v -> CiscoVPN

Cisco SD-WAN
Select Resource Group ▾
Configuration · Templates

i Enhance ECMP Keying can only be turned on in VPN0

Feature Template > Add Template > Cisco VPN

Device Type: C8000v

Template Name*

Description*

∨
BASIC CONFIGURATION

VPN

IPv4 ROUTE

New IPv4 Route

Mark as Optional Row

Prefix: 0.0.0.0/0

Gateway: Next Hop Null 0 VPN DHCP

Next Hop: Add Next Hop

Next Hop With Tracker: Add Next Hop With Tracker

Add Cancel

Add nexthop, in the address select Device Specific

Next Hop

Address	Distance
[Gateway for ISP]	1

Template for VPN-0-Interface IP

Configuration Groups Feature Profiles Device Templates Feature Templates

Feature Template > Add Template > Cisco VPN Interface Ethernet

Device Type: C8000v

Template Name*: CSR-VPN0-InterfacelP

Description*: CSR-VPN0-InterfacelP

Basic Configuration Tunnel NAT VRRP ACL/QoS ARP TrustSec Advanced

BASIC CONFIGURATION

Shutdown: Yes No

Interface Name: GigabitEthernet2

Description: [Empty]

Dynamic Static

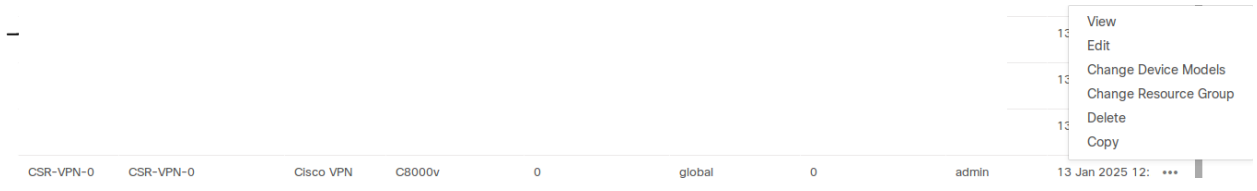
IPv4 Address/ prefix-length [GIG2-address]

Secondary IP Address (Maximum: 4) [+ Add](#)

Allow Service

All	<input checked="" type="radio"/> On	<input type="radio"/> Off
BGP	<input type="radio"/> On	<input checked="" type="radio"/> Off
DHCP	<input checked="" type="radio"/> On	<input type="radio"/> Off
DNS	<input checked="" type="radio"/> On	<input type="radio"/> Off
ICMP	<input checked="" type="radio"/> On	<input type="radio"/> Off
NETCONF	<input checked="" type="radio"/> On	<input type="radio"/> Off
NTP	<input type="radio"/> On	<input checked="" type="radio"/> Off
OSPF	<input type="radio"/> On	<input checked="" type="radio"/> Off
SSH	<input checked="" type="radio"/> On	<input type="radio"/> Off
STUN	<input type="radio"/> On	<input checked="" type="radio"/> Off

For Service VPN i.e. VPN1, please copy templates from Vmanage and just change settings



Template for VPN1

Template Copy

Template Name

Description

Copy

Cancel

Feature Template > Cisco VPN > CSR-VPN-1

Template Name*
Description*

Basic Configuration | DNS | Advertise OMP | IPv4 Route | IPv6 Route | Service | Service Route | GRE Route | IPSEC Route | NAT
Route Leak

▼ BASIC CONFIGURATION

VPN

Name

Enhance ECMP Keying On Off

OMP Admin Distance IPv4

OMP Admin Distance IPv6

Template for VPN-1-Interface IP

Template Copy

Template Name

Description

Copy

Cancel

Feature Template > Cisco VPN Interface Ethernet > CSR-VPN1-InterfacelP

Device Type: C8000v

Template Name*:

Description*:

Basic Configuration | Tunnel | NAT | VRRP | ACL/QoS | ARP | TrustSec | Advanced

▼ BASIC CONFIGURATION

Shutdown: Yes No

Interface Name:

Description:

IPv4

IPv6

Dynamic Static

IPv4 Address/ prefix-length: [GIG1-address]

Secondary IP Address (Maximum: 4) [+ Add](#)

▼ TUNNEL

Tunnel Interface: On Off

Per-tunnel Qos: On Off

Color:

Allow Service		
All	<input checked="" type="radio"/> On	<input type="radio"/> Off
BGP	<input type="radio"/> On	<input checked="" type="radio"/> Off
DHCP	<input checked="" type="radio"/> On	<input type="radio"/> Off
DNS	<input checked="" type="radio"/> On	<input type="radio"/> Off
ICMP	<input checked="" type="radio"/> On	<input type="radio"/> Off
NETCONF	<input checked="" type="radio"/> On	<input type="radio"/> Off
NTP	<input type="radio"/> On	<input checked="" type="radio"/> Off
OSPF	<input type="radio"/> On	<input checked="" type="radio"/> Off
SSH	<input checked="" type="radio"/> On	<input type="radio"/> Off

Template for OSPF to deploy on CSR's

Cisco SD-WAN | Select Resource Group | Configuration - Templates

Configuration Groups | Feature Profiles | Device Templates | **Feature Templates**

Feature Template > Add Template > Cisco OSPF

REDISTRIBUTE

Mark as Optional Row

Protocol:

Route Policy:

AREA

New Area

Area Number

Set the area type

Interface [+ Add Interface](#)

Range [+ Add Range](#)

Mark as Optional Row

Add Cancel

Interface

Add Interface

GigabitEthernet3

Interface Name

Hello Interval (seconds)

Dead Interval (seconds)

LSA Retransmission Interval (seconds)

Interface Cost

Advanced Options >

Add Cancel

Attach Feature Templates to Device Templates.

Cisco SD-WAN | Select Resource Group | Configuration - Templates

Configuration Groups | Feature Profiles | **Device Templates** | Feature Templates

Transport & Management VPN

Cisco VPN 0 * (1)

Cisco VPN Interface Ethernet (2)

Additional Cisco VPN 0 Templates

- Cisco BGP
- Cisco OSPF
- Cisco OSPFv3
- Cisco Secure Internet Gateway
- Cisco VPN Interface Ethernet
- Cisco VPN Interface GRE
- Cisco VPN Interface IPsec
- VPN Interface Cellular
- VPN Interface Multilink Controller

Add VPN | 192.168.0.79:3277

Select VPNs | Select Sub-Templates

Select one or more Service VPNs to add: | 1 Items Selected

ID	Template Name
5e40d159-ab8c-45be-8db0-f64b...	Default_SDBranch_MGMT_VPN511...
bf5417f5-8d94-4a93-8592-ca68...	Default_SDBranch_MGMT_VPN511...
9ebe851b-d4fe-4b7c-aa9f-fc2af3...	Default_SDBranch_Service_VPN1...
3c530e5b-d9de-4099-b4d1-40fc...	Default_VPN_1_Cisco_V01
373b63e5-4893-46d1-a9ae-c50...	Factory_Default_Retail_Acquisition...
e91980da-20aa-405e-8290-37a3...	Factory_Default_Retail_Employee...
846baeba-75e1-49c4-8582-933...	Factory_Default_Retail_Guest_Wif...

Service VPN (circled in sidebar)

Selected VPN Templates: 7e1b7892-1d8a-4cb9-9d89-ac43... CSR-VPN-1

Add VPN

Select VPNs Select Sub-Templates

Include sub-templates to attach to ALL selected service VPNs:

Additional Cisco VPN Templates

- Cisco IGMP
- Cisco Multicast
- Cisco PIM
- Cisco BGP
- Cisco OSPF 1
- Cisco OSPFv3
- Cisco VPN Interface Ethernet 2
- Cisco VPN Interface IPsec
- EIGRP
- VPN Interface MultiLink Controller
- VPN Interface SVI

Add VPN

Select VPNs Select Sub-Templates

Include sub-templates to attach to ALL selected service VPNs:

Cisco OSPF

CSR-OSPF



Cisco VPN Interface Ethernet

CSR-VPN 1-InterfaceIP



Sub-Templates

Device template is ready, now attach devices

Search

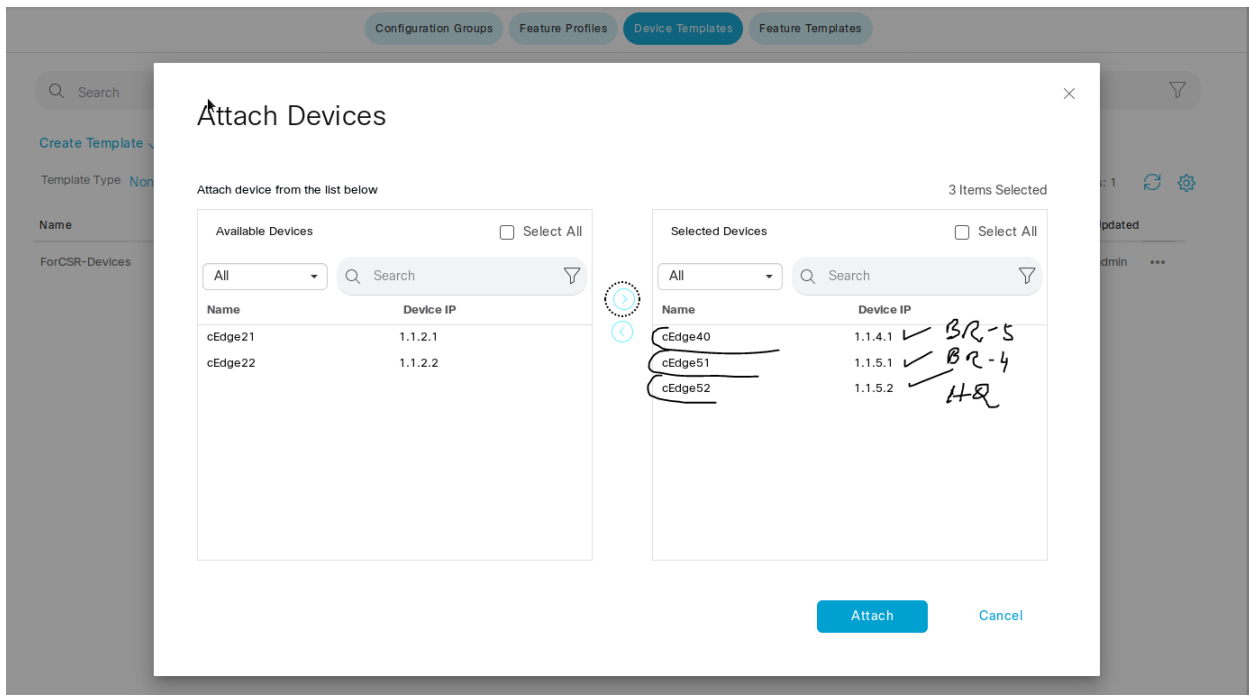
Create Template

Template Type: Non-Default

Total Rows: 1

Name	Description	Type	Device Model	Device Role	Resource Group	Feature Templates	Draft Mode	Devices Attached	Updater
ForCSR-Devices	ForCSR-Devices	Feature	C8000v	SDWAN Edge	global	14	Disabled	0	admin

- Edit
- View
- Delete
- Copy
- Enable Draft Mode
- Attach Devices
- Change Resource Group
- Export CSV



s Number	System IP	Hostname	IPv4 Address/ prefix-length(GIG3-address)	Address(ISP-GW)	IPv4 Address/ prefix-
A413929-447C-5E6D-3999-B20F...	1.1.4.1	cEdge40	20.1.1.22/24	20.1.1.22/24	20. ...
A469151-F96B-096B-5271-D369...	1.1.5.1	cEdge51			...
91A6D79-0E2A-E224-8B84-4069...	1.1.5.2	cEdge52			...

Parameters	Vedge-HQ	Vedge-BR4	Vedge-BR5
Gi2	10.10.250.2/24	20.1.1.18/30	20.1.1.22/30
ISP GW	10.10.250.1	20.1.1.17	20.1.1.21
Gi3	25.25.25.2/24	26.26.26.1/24	27.27.27.1/24

Variable List (Hover over each field for more information)

Status	in_complete
Chassis Number	C8K-3A413929-447C-5E6D-3999-B20F3A963494
System IP	1.1.4.1
Hostname	cEdge40
IPv4 Address/ prefix-length(GiG3-address)	<input type="text" value="20.1.1.22/24"/>
Address(ISP-GW)	<input type="text" value="20.1.1.21/24"/>
IPv4 Address/ prefix-length(GiG2-address)	<input type="text" value="27.27.27.1/24"/>
Hostname	<input type="text" value="BR-5-Vedge"/>
System IP	<input type="text"/>
Site ID	<input type="text"/>

Repeat the same for other devices, BR-4 and HQ- vedge

Total Rows: 3 ↑ ↓

S...	Chassis Number	System IP	Hostname	IPv4 Address/ prefix-length(GIG3-address)	Address(ISP-GW)	IPv4 Address/ prefix-l	
✓	C8K-3A413929-447C-5E6D-3999-B20F...	1.1.4.1	cEdge40	20.1.1.22/30	20.1.1.21/30	27.27.27.1/24	...
✓	C8K-8A469151-F96B-096B-5271-D369...	1.1.5.1	cEdge51	20.1.1.18/30	20.1.1.17/30	26.26.26.1/24	...
✓	C8K-991A6D79-0E2A-E224-8B84-4069...	1.1.5.2	cEdge52	10.10.250.2/24	10.10.250.1/24	25.25.25.2/24	...

Device Template
Total

ForCSR-Devices
1

Device list (Total: 3 devices)

C8K-3A413929-447C-5E6D-3999-B20F3A963494

cEdge40|1.1.4.1

C8K-8A469151-F96B-096B-5271-D369C85E1E11

cEdge51|1.1.5.1

C8K-991A6D79-0E2A-E224-8B84-406908FASDD7

cEdge52|1.1.5.2

Please select a device from the device list

Configure Device Rollback Timer

Back
Configure Devices
Cancel

HQ-R23

```
interface Loopback1
 ip address 160.1.1.1 255.255.255.0
 ip ospf 1 area 0
!
interface Ethernet0/0
 ip address 25.25.25.1 255.255.255.0
 ip ospf 1 area 0
 duplex auto
```

Branch#4 router

```
interface Loopback1
 ip address 161.1.1.1 255.255.255.0
 ip ospf 1 area 0
!
interface Ethernet0/0
 ip address 26.26.26.2 255.255.255.0
 ip ospf 1 area 0
 duplex auto
!
```

Branch#5 router

```
interface Loopback1
 ip address 162.1.1.1 255.255.255.0
 ip ospf 1 area 0
!
interface Ethernet0/0
 ip address 27.27.27.2 255.255.255.0
 ip ospf 1 area 0
 duplex auto
```

Verification

HQ-R23#

Gateway of last resort is not set

```
      25.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C      25.25.25.0/24 is directly connected, Ethernet0/0
L      25.25.25.1/32 is directly connected, Ethernet0/0
      26.0.0.0/24 is subnetted, 1 subnets
O E2   26.26.26.0 [110/16777214] via 25.25.25.2, 00:10:57, Ethernet0/0
      27.0.0.0/24 is subnetted, 1 subnets
O E2   27.27.27.0 [110/16777214] via 25.25.25.2, 00:13:56, Ethernet0/0
      160.1.0.0/16 is variably subnetted, 2 subnets, 2 masks
C      160.1.1.0/24 is directly connected, Loopback1
L      160.1.1.1/32 is directly connected, Loopback1
      161.1.0.0/32 is subnetted, 1 subnets
O E2   161.1.1.1 [110/16777214] via 25.25.25.2, 00:08:11, Ethernet0/0
      162.1.0.0/32 is subnetted, 1 subnets
O E2   162.1.1.1 [110/16777214] via 25.25.25.2, 00:10:17, Ethernet0/0
```

BR-4-router#

```
      25.0.0.0/24 is subnetted, 1 subnets
O E2   25.25.25.0 [110/16777214] via 26.26.26.1, 00:08:53, Ethernet0/0
      26.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C      26.26.26.0/24 is directly connected, Ethernet0/0
L      26.26.26.2/32 is directly connected, Ethernet0/0
      27.0.0.0/24 is subnetted, 1 subnets
O E2   27.27.27.0 [110/16777214] via 26.26.26.1, 00:08:53, Ethernet0/0
      160.1.0.0/32 is subnetted, 1 subnets
O E2   160.1.1.1 [110/16777214] via 26.26.26.1, 00:07:50, Ethernet0/0
      161.1.0.0/16 is variably subnetted, 2 subnets, 2 masks
C      161.1.1.0/24 is directly connected, Loopback1
L      161.1.1.1/32 is directly connected, Loopback1
      162.1.0.0/32 is subnetted, 1 subnets
O E2   162.1.1.1 [110/16777214] via 26.26.26.1, 00:08:53, Ethernet0/0
```

BR5-router#

```
      25.0.0.0/24 is subnetted, 1 subnets
O E2   25.25.25.0 [110/16777214] via 27.27.27.1, 00:11:48, Ethernet0/0
      26.0.0.0/24 is subnetted, 1 subnets
O E2   26.26.26.0 [110/16777214] via 27.27.27.1, 00:11:48, Ethernet0/0
      27.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C      27.27.27.0/24 is directly connected, Ethernet0/0
L      27.27.27.2/32 is directly connected, Ethernet0/0
      160.1.0.0/32 is subnetted, 1 subnets
O E2   160.1.1.1 [110/16777214] via 27.27.27.1, 00:08:22, Ethernet0/0
      161.1.0.0/32 is subnetted, 1 subnets
O E2   161.1.1.1 [110/16777214] via 27.27.27.1, 00:09:24, Ethernet0/0
      162.1.0.0/16 is variably subnetted, 2 subnets, 2 masks
C      162.1.1.0/24 is directly connected, Loopback1
L      162.1.1.1/32 is directly connected, Loopback1
```

CCIE EI Design Questions

Question 1: High Availability Design

You are designing a network for a company that requires high availability between two data centers. The data centers should relate to redundancy, and if one data center fails, the other should take over without impacting service. Which of the following solutions will best meet the requirement?

- A) Use a single routed link between the two data centers and configure HSRP.
- B) Implement dual Active-Active data centers with VRRP on core routers.**
- C) Use a single data center with a backup generator for power redundancy.
- D) Configure BGP between the two data centers and rely on the ISP's failover.

Correct Answer: B) Implement dual Active-Active data centers with VRRP on core routers.

Question 2: VLAN Design

Your company is expanding and requires a VLAN design that can scale as more users and departments are added. You need to separate traffic for different departments (HR, IT, and Finance) while ensuring flexibility. Which of the following is the best practice to implement a scalable VLAN architecture?

- A) Use a single VLAN for all departments and segment traffic using ACLs.
- B) Configure a separate VLAN for each department and implement VLAN trunking between switches.**
- C) Use private VLANs (PVLANS) for each department to isolate them without using additional switches.
- D) Configure a large subnet and assign all users to the same IP range to avoid VLAN overhead.

Correct Answer: B) Configure a separate VLAN for each department and implement VLAN trunking between switches.

Question 3: Network Security Design

Your company has sensitive financial data and needs to secure its network. The network should protect against unauthorized access while ensuring legitimate users can access necessary resources. Which of the following is the most secure and scalable solution for user authentication on the network?

- A) Use static IP addresses for each user and configure ACLs to restrict access.
- B) Implement 802.1X network access control with RADIUS for centralized authentication.**
- C) Configure port security on all switches to limit the number of MAC addresses per port.
- D) Use password-based authentication on routers and switches to control access to the network.

Correct Answer: B) Implement 802.1X network access control with RADIUS for centralized authentication.

Question 4: SD-WAN Design

A company wants to implement SD-WAN to reduce costs and improve branch office connectivity. The SD-WAN solution should allow the branches to use both MPLS and broadband internet connections, and prioritize traffic for critical applications such as VoIP and video conferencing. What is the most important consideration when designing the SD-WAN architecture?

- A) Ensure MPLS is the only path for all traffic to guarantee maximum security.
- B) Use SD-WAN to dynamically select the best path based on application type and performance.**
- C) Configure SD-WAN to block all internet access to ensure security at branch locations.
- D) Enable SD-WAN for routing traffic between data centers but not for branch offices.

Correct Answer: B) Use SD-WAN to dynamically select the best path based on application type and performance.

Question 5: IP Addressing and Subnetting

You are tasked with assigning IP addresses for a new office network that includes 6 departments, each requiring 30 hosts. You need to subnet a network to accommodate these requirements while using the fewest possible subnets. What is the minimum subnet mask you should use for each department?

- A) /26
- B) /27
- C) /28
- D) /29

Correct Answer: A) /26

Question 6: Network Redundancy

You are tasked with designing a highly available network for a large enterprise with multiple remote offices. The solution should allow seamless failover between two internet connections. Which technology would you implement to provide redundancy and automatic failover for internet connectivity?

- A) BGP (Border Gateway Protocol)
- B) OSPF (Open Shortest Path First)
- C) EIGRP (Enhanced Interior Gateway Routing Protocol)
- D) HSRP (Hot Standby Router Protocol)

Correct Answer: A) BGP (Border Gateway Protocol)

Question 7: Inter-VLAN Routing Design

You have designed a network where different departments are assigned to different VLANs. The departments need to communicate with each other, but traffic between the VLANs should be controlled for security purposes. Which device should be used to enable communication between VLANs?

- A) Layer 2 switch
- B) Layer 3 switch with SVIs (Switched Virtual Interfaces)
- C) Access point
- D) Load balancer

Correct Answer: B) Layer 3 switch with SVIs (Switched Virtual Interfaces)

Question 8: Network Monitoring and Troubleshooting

You are troubleshooting a network and need to collect data to understand traffic flow and identify issues. Which of the following tools would provide visibility into both the performance and security of the network?

- A) Ping and Traceroute
- B) SNMP and NetFlow
- C) ARP and DHCP logs
- D) Port scanning tools

Correct Answer: B) SNMP and NetFlow

Question 9: Quality of Service (QoS) Design

Your company is deploying VoIP and video conferencing solutions across the enterprise network. To ensure high-quality audio and video calls, you need to prioritize this traffic over less time-sensitive traffic such as email. Which of the following QoS mechanisms is best suited to prioritize VoIP and video conferencing traffic?

- A) Use **DSCP (Differentiated Services Code Point)** to mark VoIP and video packets with a higher priority.
- B) Use **TCP congestion control** to prioritize VoIP traffic over other types.
- C) Configure **Static routing** to guarantee that VoIP traffic takes the shortest path.
- D) Apply **NAT (Network Address Translation)** to VoIP traffic to prevent congestion.

Correct Answer: A) Use DSCP (Differentiated Services Code Point) to mark VoIP and video packets with a higher priority.