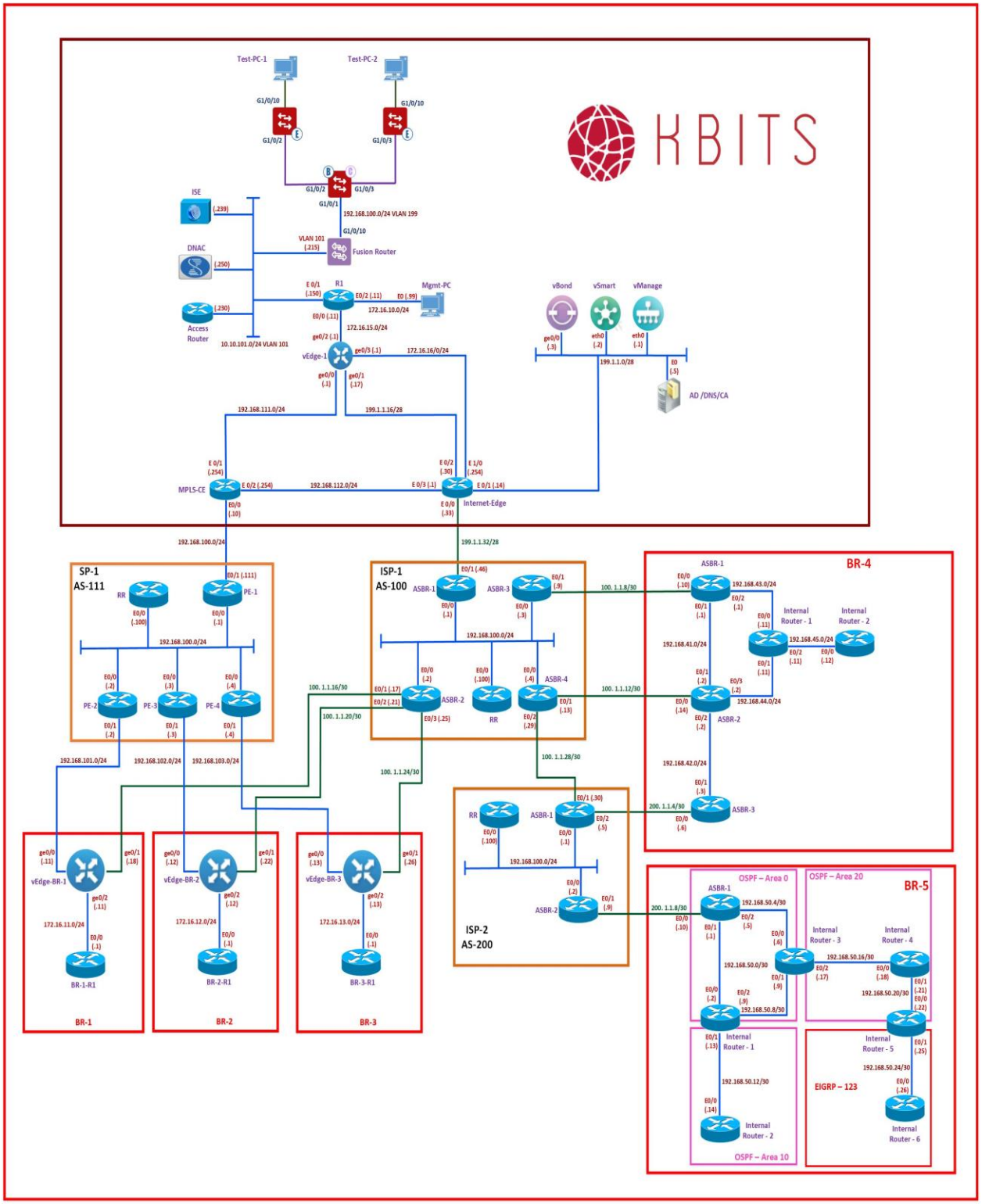
CCIE Enterprise Infrastructure – Super Lab

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

Section 1

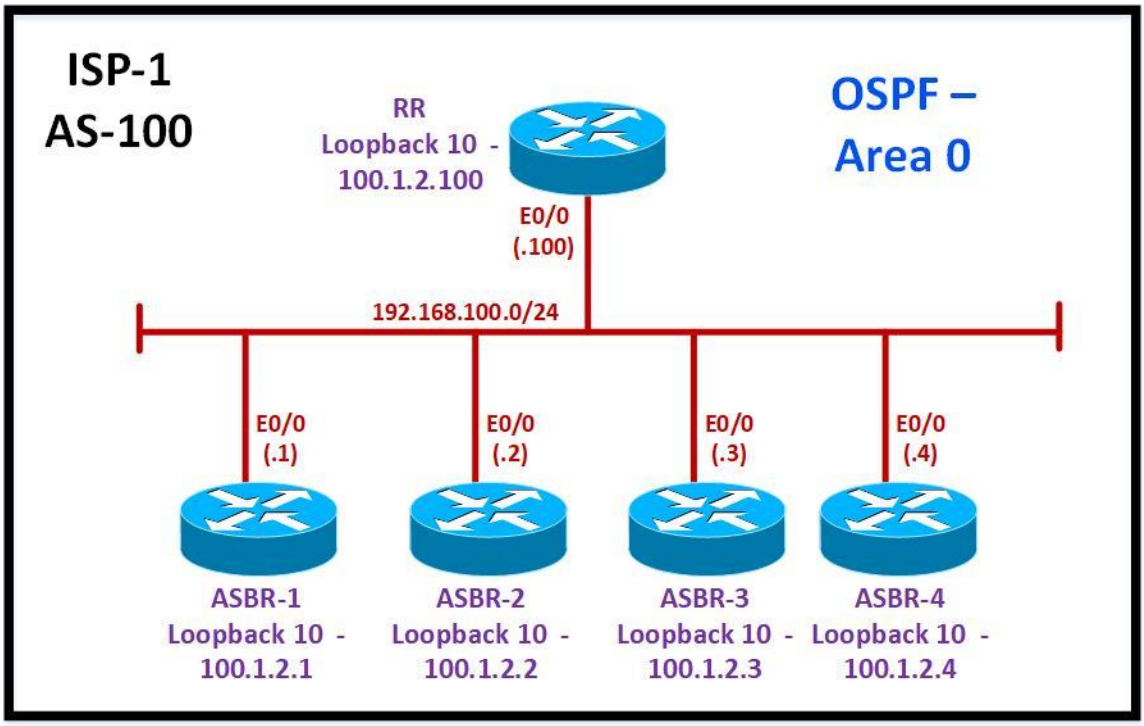
IGP/LDP/BGP Setup – SP/ISP's

Full Logical Topology



Lab 1 – Configuring OSPF & LDP – ISP-1 (AS-100)

Physical Layout



Interface Configuration (Pre-Configured)

ISP-1-ASBR-1

Interface	IP Address	Subnet Mask
E 0/0	192.168.100.1	255.255.255.0
E 0/1	199.1.1.46	255.255.255.240
Loopback10	100.1.2.1	255.255.255.255

ISP-1-ASBR-2

Interface	IP Address	Subnet Mask
E 0/0	192.168.100.2	255.255.255.0
E 0/1	100.1.1.17	255.255.255.252
E 0/2	100.1.1.21	255.255.255.252
E 0/3	100.1.1.25	255.255.255.252
Loopback10	100.1.2.2	255.255.255.255

ISP-1-ASBR-3

Interface	IP Address	Subnet Mask
E 0/0	192.168.100.3	255.255.255.0
E 0/1	100.1.1.9	255.255.255.252
Loopback10	100.1.2.3	255.255.255.255

ISP-1-ASBR-4

Interface	IP Address	Subnet Mask
E 0/0	192.168.100.4	255.255.255.0
E 0/1	100.1.1.13	255.255.255.252
E 0/2	100.1.1.29	255.255.255.252
Loopback10	100.1.2.4	255.255.255.255

ISP-1-RR

Interface	IP Address	Subnet Mask
E 0/0	192.168.100.100	255.255.255.0
Loopback10	100.1.2.100	255.255.255.255

Task 1 – Configure OSPF as the underlay IGP for ISP-1

- Configure OSPF as the underlay IGP for ISP-1 using the following characteristics:
  - Area – 0
  - Router-ID
    - ASBR-1 – 0.0.100.1
    - ASBR-2 – 0.0.100.2
    - ASBR-3 – 0.0.100.3
    - ASBR-4 – 0.0.100.4
    - RR – 0.0.100.100
- Enable OSPF on the Loopback 10 Interface and the Internal segment (192.168.100.0/24).

Task 2 – Secure the OSPF Neighbor relationships with MD5

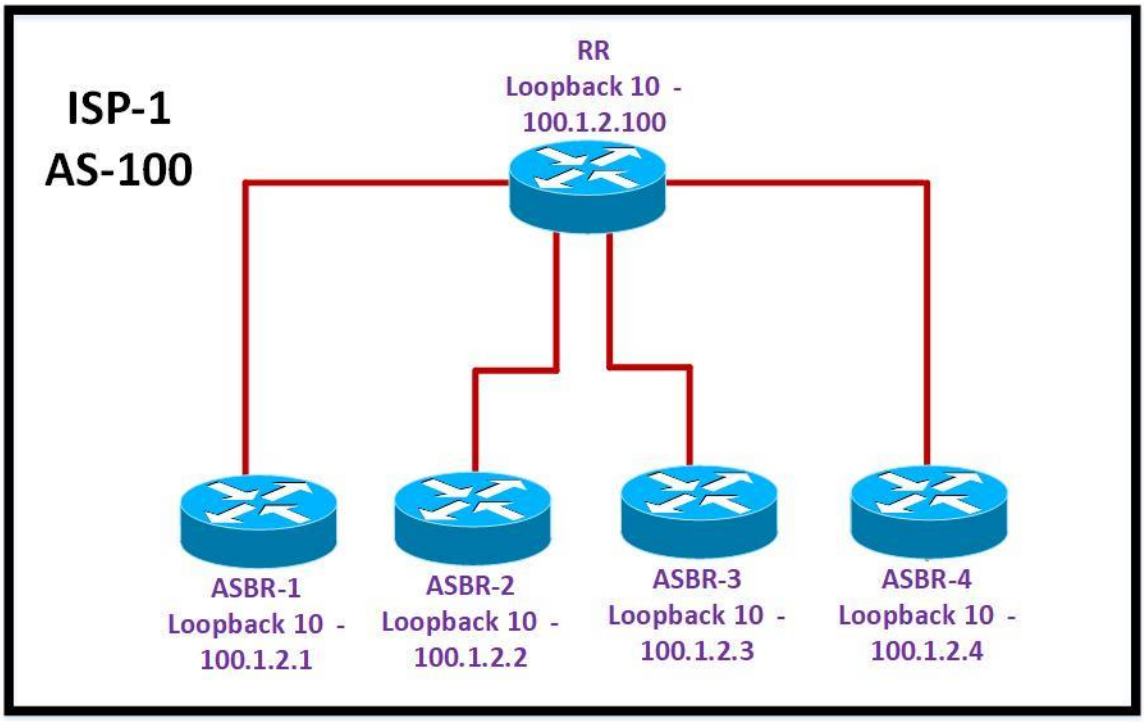
- Configure OSPF to authenticate using MD5 authentication.
- Use a Key ID of **100** with a Key String of **Kbits@123**.

Task 3 – Configure LDP within the ISP Network

- Configure LDP as the Label Protocol within ISP-1 on all the internal links.
- Configure Loopback10 as the MPLS Router-ID.

Lab 2 – Configure iBGP withing ISP – 1

BGP Logical Layout

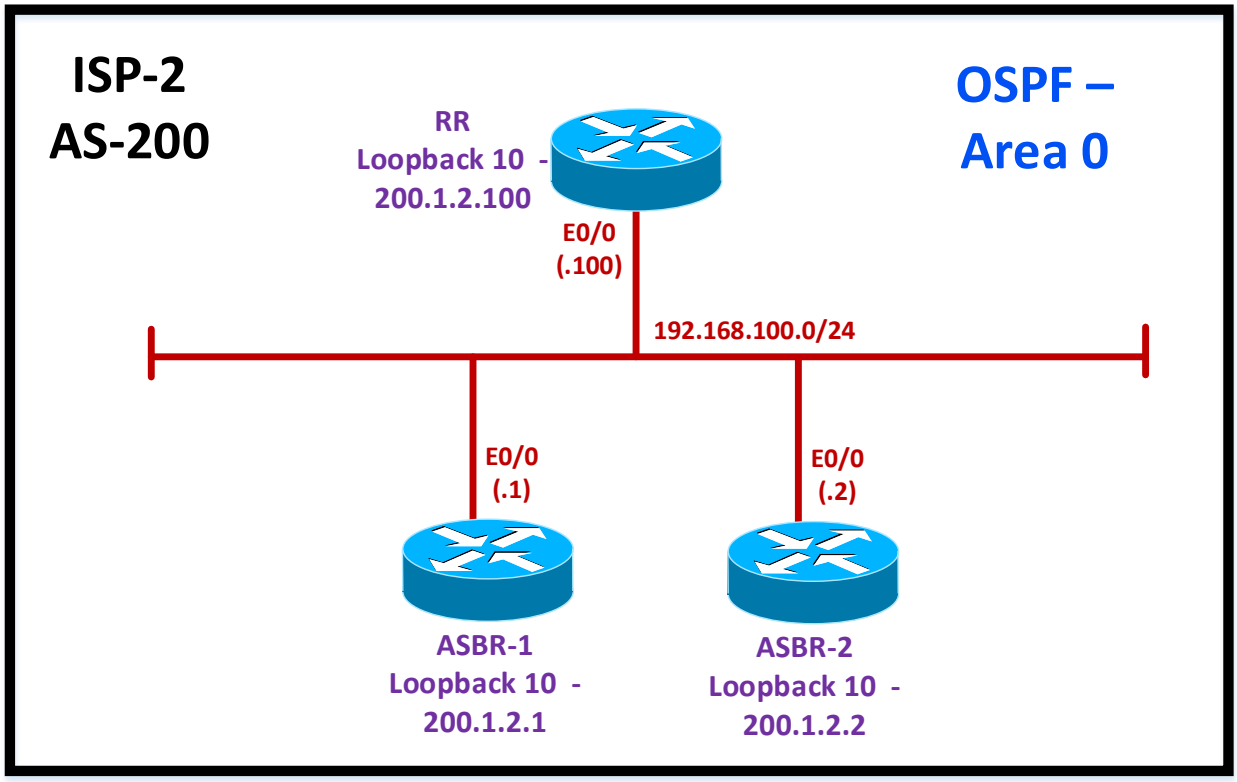


Task 1 – Configure iBGP relationships between the ASBRs & RR

- Configure the ASBRs to communicate with the RR using Loopback addresses.
- Make sure that ASBRs propagate routes within the AS using itself as the Next-hop.
- Allow the RR to accept dynamic neighbors from the 100.1.2.0/24 range. Use Peer-groups on RR to minimize the configuration.

Lab 3 – Configuring OSPF as the IGP – ISP-2 (AS-200)

Physical Layout



Interface Configuration (Pre-Configured)

ISP-2-ASBR-1

Interface	IP Address	Subnet Mask
E 0/0	192.168.100.1	255.255.255.0
E 0/1	100.1.1.30	255.255.255.252
E 0/2	200.1.1.5	255.255.255.252
Loopback10	200.1.2.1	255.255.255.255

ISP-2-ASBR-2

Interface	IP Address	Subnet Mask
E 0/0	192.168.100.2	255.255.255.0

E 0/1	200.1.1.9	255.255.255.252
Loopback10	200.1.2.2	255.255.255.255

ISP-2-RR

Interface	IP Address	Subnet Mask
E 0/0	192.168.100.100	255.255.255.0
Loopback10	200.1.2.100	255.255.255.255

Task 1 – Configure OSPF as the underlay IGP for ISP-2

- Configure OSPF as the underlay IGP for ISP-2 using the following characteristics:
  - Area – 0
  - Router-ID
    - ASBR-1 – 0.0.200.1
    - ASBR-2 – 0.0.200.2
    - RR – 0.0.200.100

- Enable OSPF on the Loopback 10 Interface and the Internal segment (192.168.100.0/24).

Task 2 – Secure the OSPF Neighbor relationships with MD5

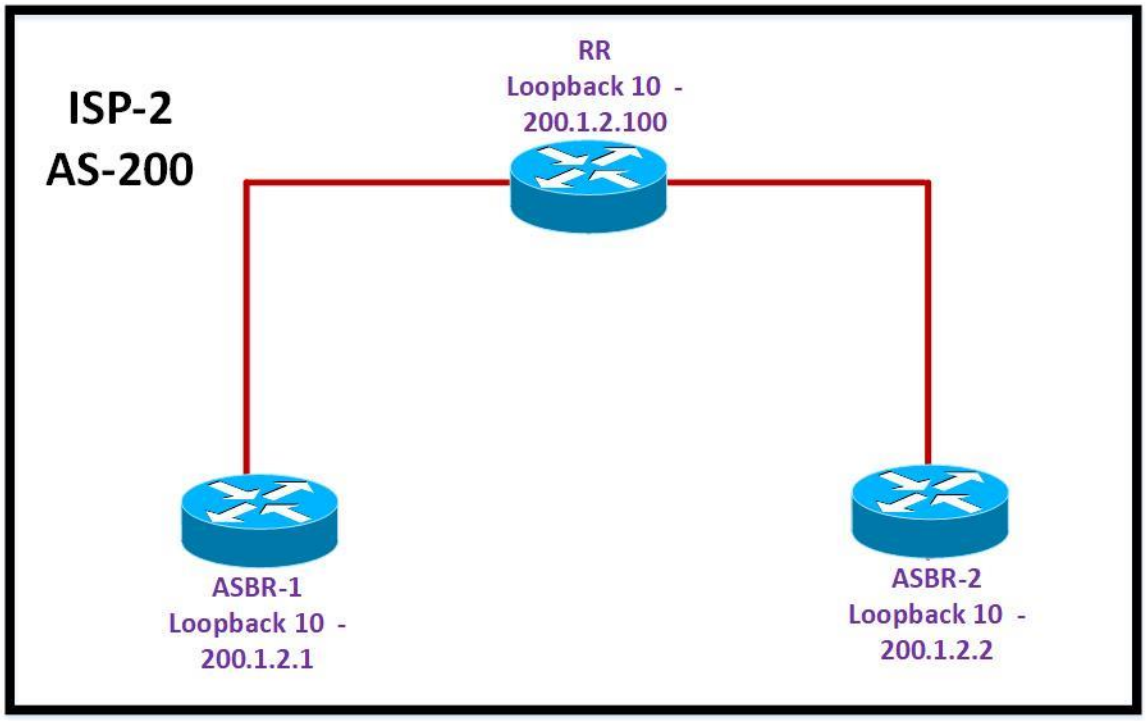
- Configure OSPF to authenticate using MD5 authentication.
- Use a Key ID of **100** with a Key String of **Kbits@123**.

Task 3 – Configure LDP within the ISP Network

- Configure LDP as the Label Protocol within ISP-2 on all the internal links.
- Configure Loopback10 as the MPLS Router-ID.

Lab 4 – Configure iBGP withing ISP – 2

BGP Logical Layout

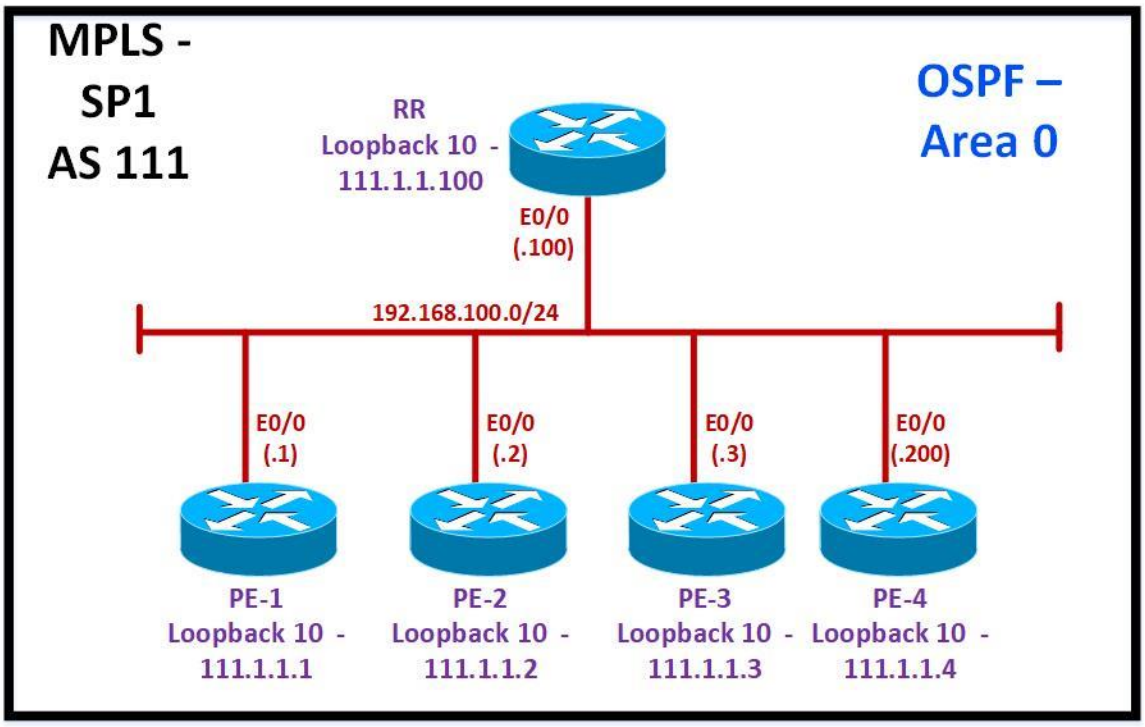


Task 1 – Configure iBGP relationships between the ASBRs & RR

- Configure the ASBRs to communicate with the RR using Loopback addresses.
- Make sure that ASBRs propagate routes within the AS using itself as the Next-hop.
- Allow the RR to accept dynamic neighbors from the 200.1.2.0/24 range. Use Peer-groups on RR to minimize the configuration.

Lab 5 – Configuring OSPF as the IGP – SP-1 (AS-111)

Physical Layout



Interface Configuration (Pre-Configured)

SP-1-PE-1

Interface	IP Address	Subnet Mask
E 0/0	192.168.100.1	255.255.255.0
E 0/1	192.168.100.111	255.255.255.0
Loopback10	111.1.1.1	255.255.255.255

SP-1-PE-2

Interface	IP Address	Subnet Mask
E 0/0	192.168.100.2	255.255.255.0
E 0/1	192.168.101.2	255.255.255.0
Loopback10	111.1.1.2	255.255.255.255

SP-1-PE-3

Interface	IP Address	Subnet Mask
E 0/0	192.168.100.3	255.255.255.0
E 0/1	192.168.102.3	255.255.255.0
Loopback10	111.1.1.3	255.255.255.255

SP-1-PE-4

Interface	IP Address	Subnet Mask
E 0/0	192.168.100.4	255.255.255.0
E 0/1	192.168.103.4	255.255.255.0
Loopback10	111.1.1.4	255.255.255.255

SP-1-RR

Interface	IP Address	Subnet Mask
E 0/0	192.168.100.4	255.255.255.0
Loopback10	111.1.1.100	255.255.255.255

Task 1 – Configure OSPF as the underlay IGP for SP-1

- Configure OSPF as the underlay IGP for SP-1 using the following characteristics:
  - Area – 0
  - Router-ID
    - PE-1 – 0.0.111.1
    - PE-2 – 0.0.111.2
    - PE-3 – 0.0.111.3
    - PE-4 – 0.0.111.4
    - RR – 0.0.111.100

- Enable OSPF on the Loopback 10 Interface and the Internal segment (192.168.100.0/24).

Task 2 – Secure the OSPF Neighbor relationships with MD5

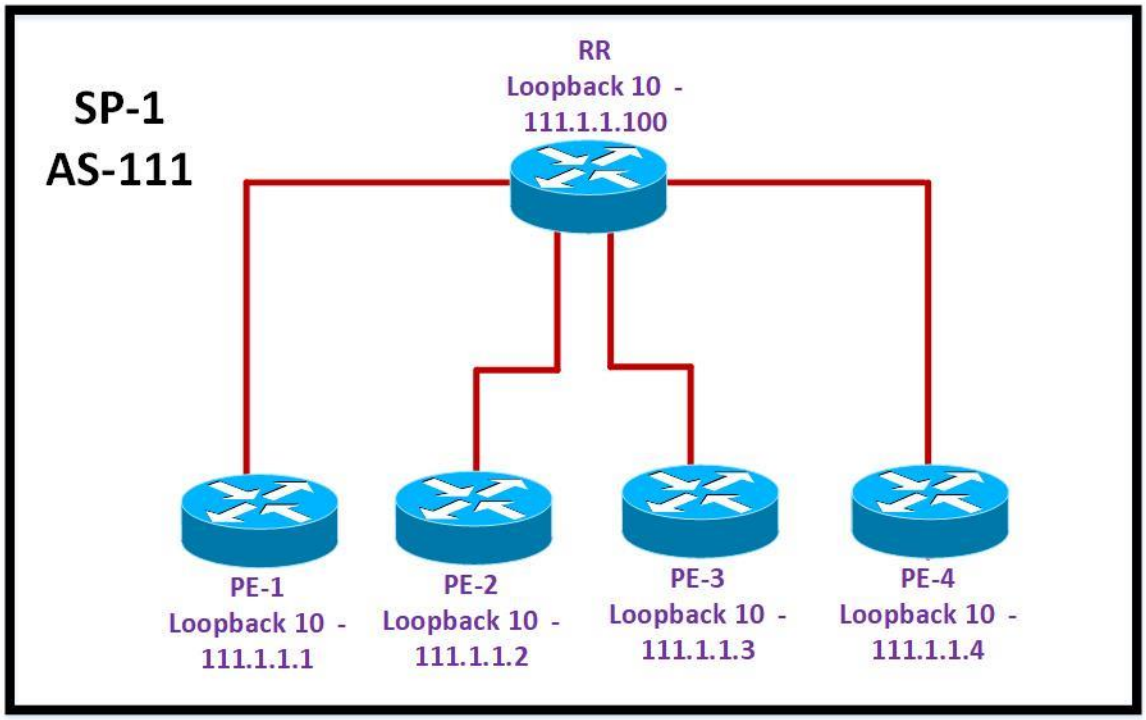
- Configure OSPF to authenticate using MD5 authentication.
- Use a Key ID of **100** with a Key String of **Kbits@123**.

Task 3 – Configure LDP within the ISP Network

- Configure LDP as the Label Protocol within SP-1 on all the internal links.
- Configure Loopback10 as the MPLS Router-ID.

Lab 6 – Configure MP-iBGP within SP – 1

BGP Logical Layout



Task 1 – Configure iBGP relationships between the PE's & RR

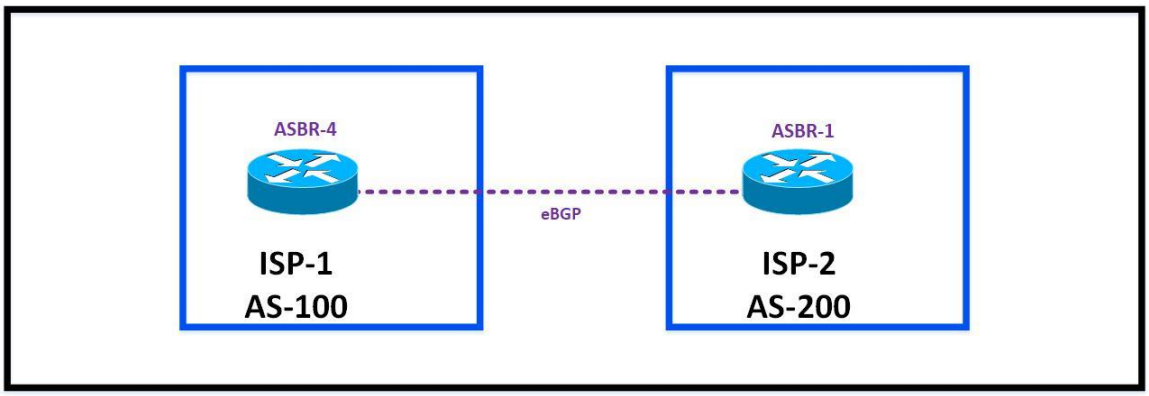
- Configure the PE to communicate with the RR using Loopback addresses.
- Use Peer-groups on RR to minimize the configuration.
- Enable the neighbors to exchange MPLS VPN routes for the IPv4 Address family.

Task 2 – iBGP Neighbor Authentication

- Configure the neighbor relationships with the highest level of authentication.
- Use **Kbits@123** as the password.

Lab 7 – Configuring eBGP between ISP-1 & ISP-2

Physical & BGP Layout



Interface Configuration (Pre-Configured)

ISP-1-ASBR-4

Interface	IP Address	Subnet Mask
E 0/2	100.1.1.29	255.255.255.252

ISP-2-ASBR-1

Interface	IP Address	Subnet Mask
E 0/0	100.1.1.30	255.255.255.252

Task 1 – Configure an eBGP neighbor relationship between AS-100 & AS-200

- Configure eBGP neighbor relationship between AS-100 & AS-200. Use ASBR-4 in AS-100 & ASBR-1 in AS-200 to set this neighbor relationship up.

Task 2 – Secure the BGP Neighbor relationships with MD5

- Configure BGP to authenticate the neighbor relationship using MD5 authentication.
- Use a password of **Kbits@123**.

Task 3 – Advertise all the Loopback Networks to each other.

- Advertise the Loopback 10 interfaces of all the routers in BGP.
- Summarize the networks using a /24 mask towards each other.

CCIE Enterprise Infrastructure – Super Lab

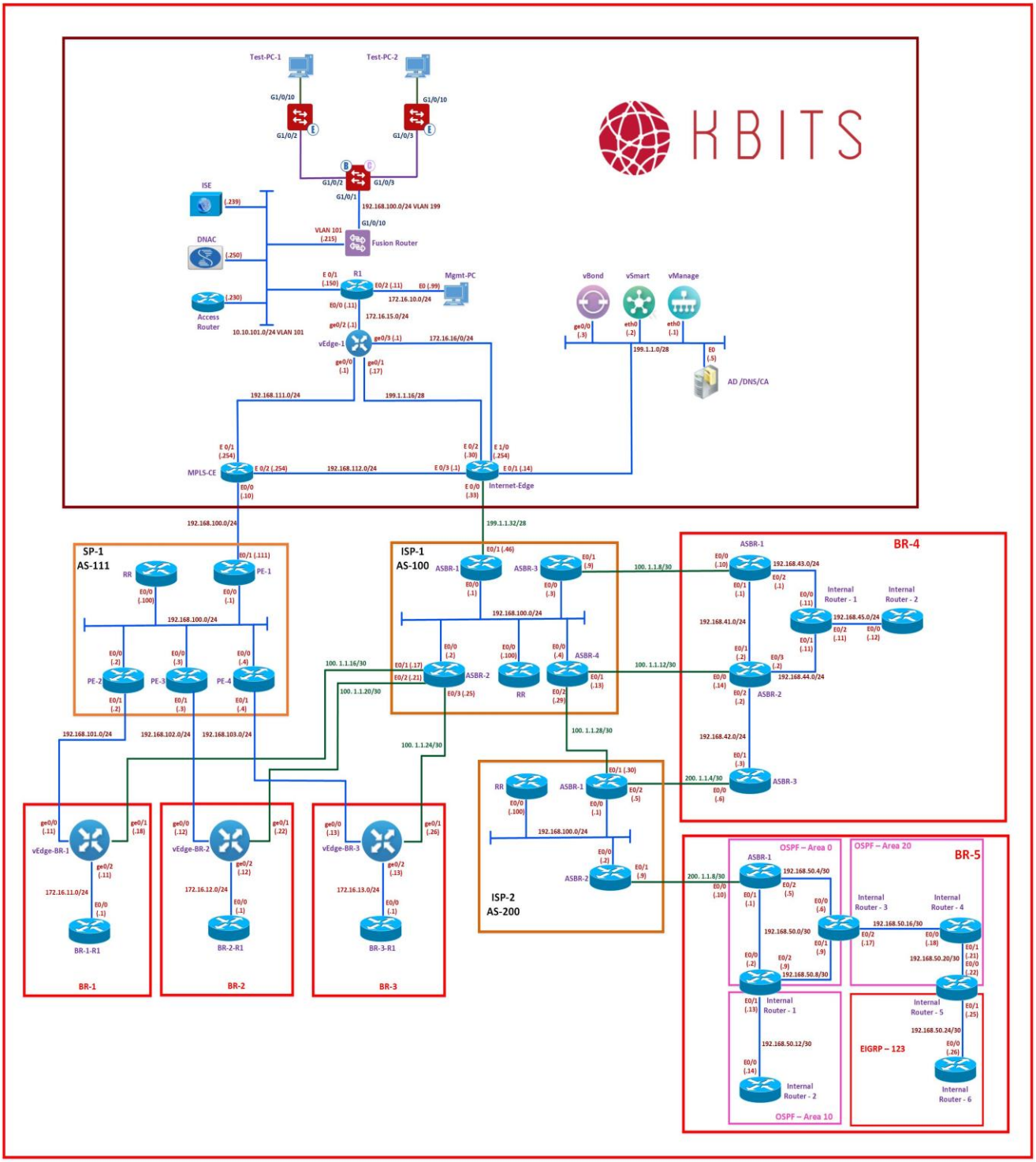
Khawar Butt
CCIE # 12353
Hepta CCIE#12353
CCDE # 20110020

Section 2

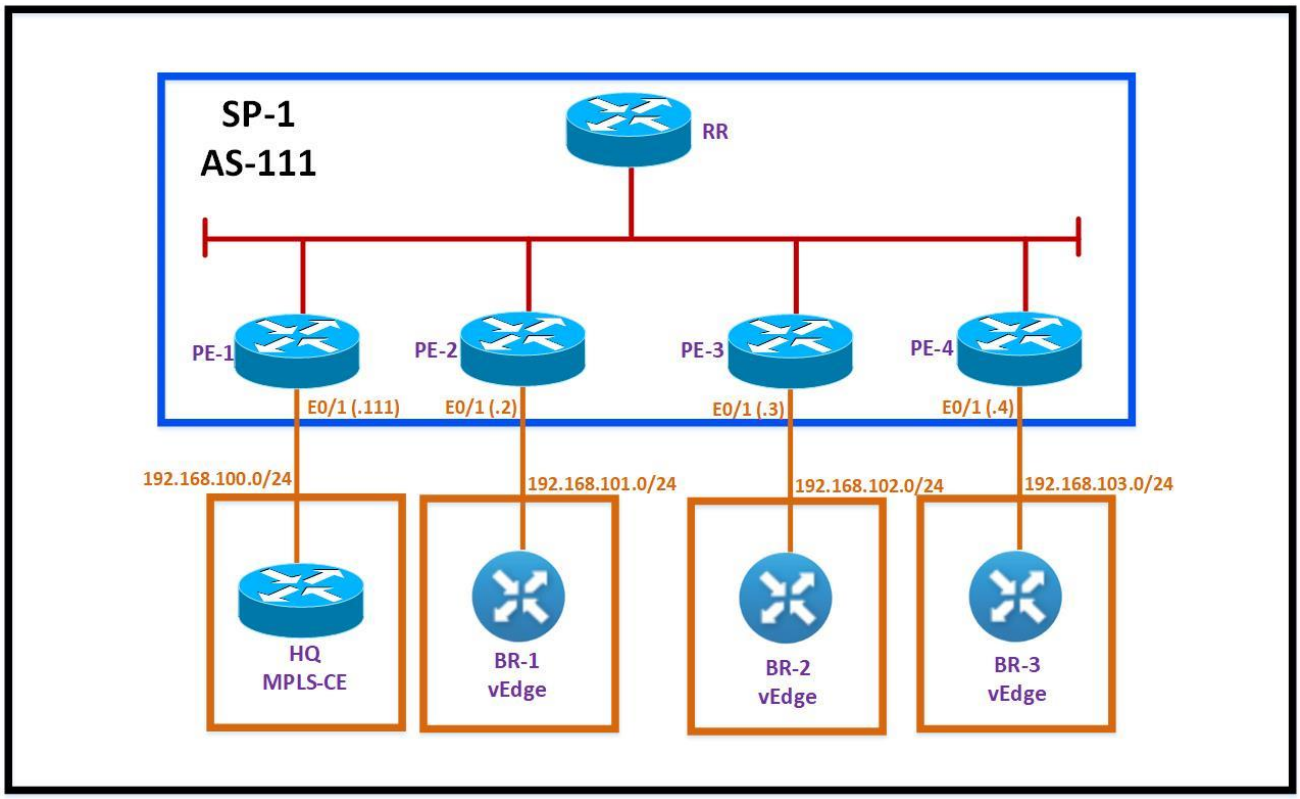
Intra-AS MPLS VPN

Lab 1 – Configuring MPLS CE Router at HQ

Full Topology



MPLS VPN Topology

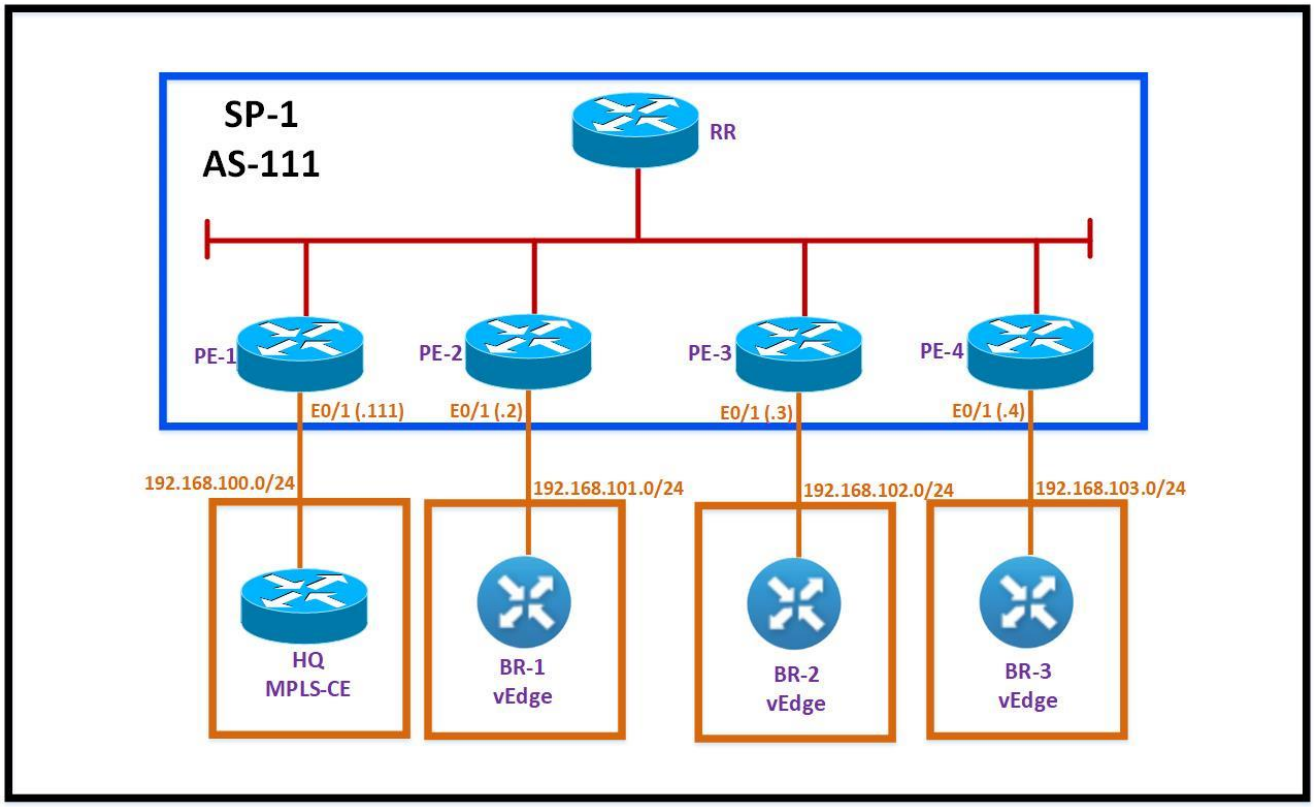


Task 1 – Configure MPLS-CE at the HQ-Site

- Configure BGP as the PE-CE Protocol. Configure MPLS-CE in AS 65010.
- Configure a BGP neighbor relationship towards PE-1. PE-1 will be using an IP Address of 192.168.100.111.
- Configure a BGP neighbor relationship towards vEdge-1. vEdge-1 will be using an IP Address of 192.168.111.1. vEdge-1 will also be configured in AS 65010. Change the next-hop to the Self for this neighbor relationship.

Lab 2 – Configure VRFs on PE Routers

MPLS VPN Topology



Task 1 – Configure VRFs on PE-1 for Intra-AS MPLS VPN towards HQ Site

- Configure a VRF on PE-1 Router to accommodate the HQ site for a client Kbits.live using the following parameters:
  - VRF Name: KBITS
  - RD & RT Values: 111:1
  - Interface Configuration:
    - Interface: E 0/1
    - IP Address: 192.168.100.111/24

Task 2 – Configure VRFs on PE-2 for Intra-AS MPLS VPN towards BR-1 Site

- Configure a VRF on PE-2 Router to accommodate the BR-1 site for a client Kbits.live using the following parameters:
  - VRF Name: KBITS
  - RD & RT Values: 111:1
  - Interface Configuration:
    - Interface: E 0/1
    - IP Address: 192.168.101.2/24

Task 3 – Configure VRFs on PE-3 for Intra-AS MPLS VPN towards BR-2 Site

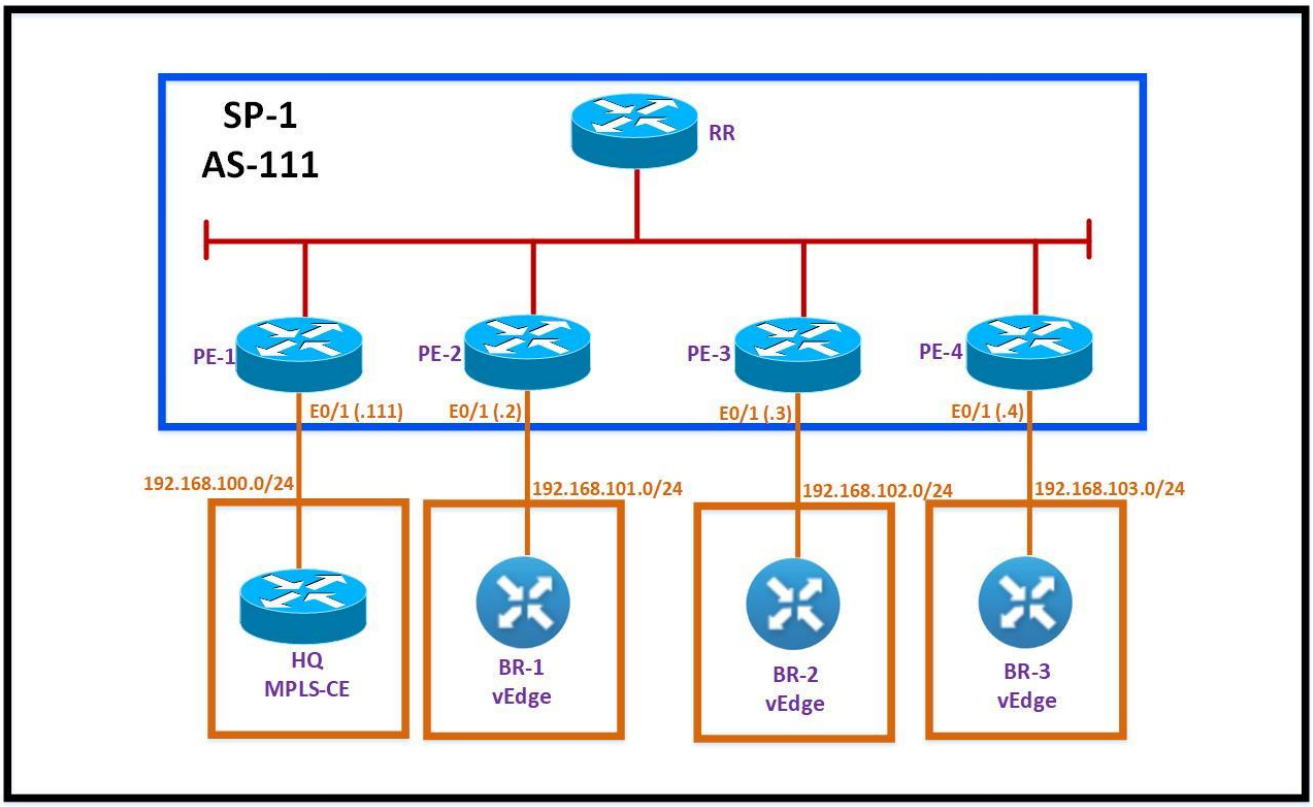
- Configure a VRF on PE-3 Router to accommodate the BR-2 Site for a client Kbits.live using the following parameters:
  - VRF Name: KBITS
  - RD & RT Values: 111:1
  - Interface Configuration:
    - Interface: E 0/1
    - IP Address: 192.168.102.3/24

Task 4 – Configure VRFs on PE-4 for Intra-AS MPLS VPN towards BR-3 Site

- Configure a VRF on PE-4 Router to accommodate the BR-3 Site for a client Kbits.live using the following parameters:
  - VRF Name: KBITS
  - RD & RT Values: 111:1
  - Interface Configuration:
    - Interface: E 0/1
    - IP Address: 192.168.103.4/24

Lab 3 – Configure PE-CE Routing on PE Routers

MPLS VPN Topology



Task 1 – Configure BGP as the PE-CE Routing Protocol on PE-1

- Configure BGP as the PE-CE Protocol.
- Configure a BGP neighbor relationship towards the MPLS CE Router (192.168.100.10) within the KBITS VRF.
- Redistribute the connected route into BGP.
- The MPLS CE Router should have been configured in AS 65010.

Task 2 – Configure BGP as the PE-CE Routing Protocol on PE-2

- Configure BGP as the PE-CE Protocol.
- Configure a BGP neighbor relationship towards BR-1 vEdge Router (192.168.101.11) within the KBITS VRF.
- Redistribute the connected route into BGP.
- The BR-1 vEdge device will be configured in AS 65011.

Task 3 – Configure BGP as the PE-CE Routing Protocol on PE-3

- Configure BGP as the PE-CE Protocol.
- Configure a BGP neighbor relationship towards BR-2 vEdge Router (192.168.102.12) within the KBITS VRF.
- Redistribute the connected route into BGP.
- The BR-2 vEdge device will be configured in AS 65012.

Task 4 – Configure BGP as the PE-CE Routing Protocol on PE-4

- Configure BGP as the PE-CE Protocol.
- Configure a BGP neighbor relationship towards BR-3 vEdge Router (192.168.103.13) within the KBITS VRF.
- Redistribute the connected route into BGP.
- The BR-1 vEdge device will be configured in AS 65013.

CCIE Enterprise Infrastructure – Super Lab

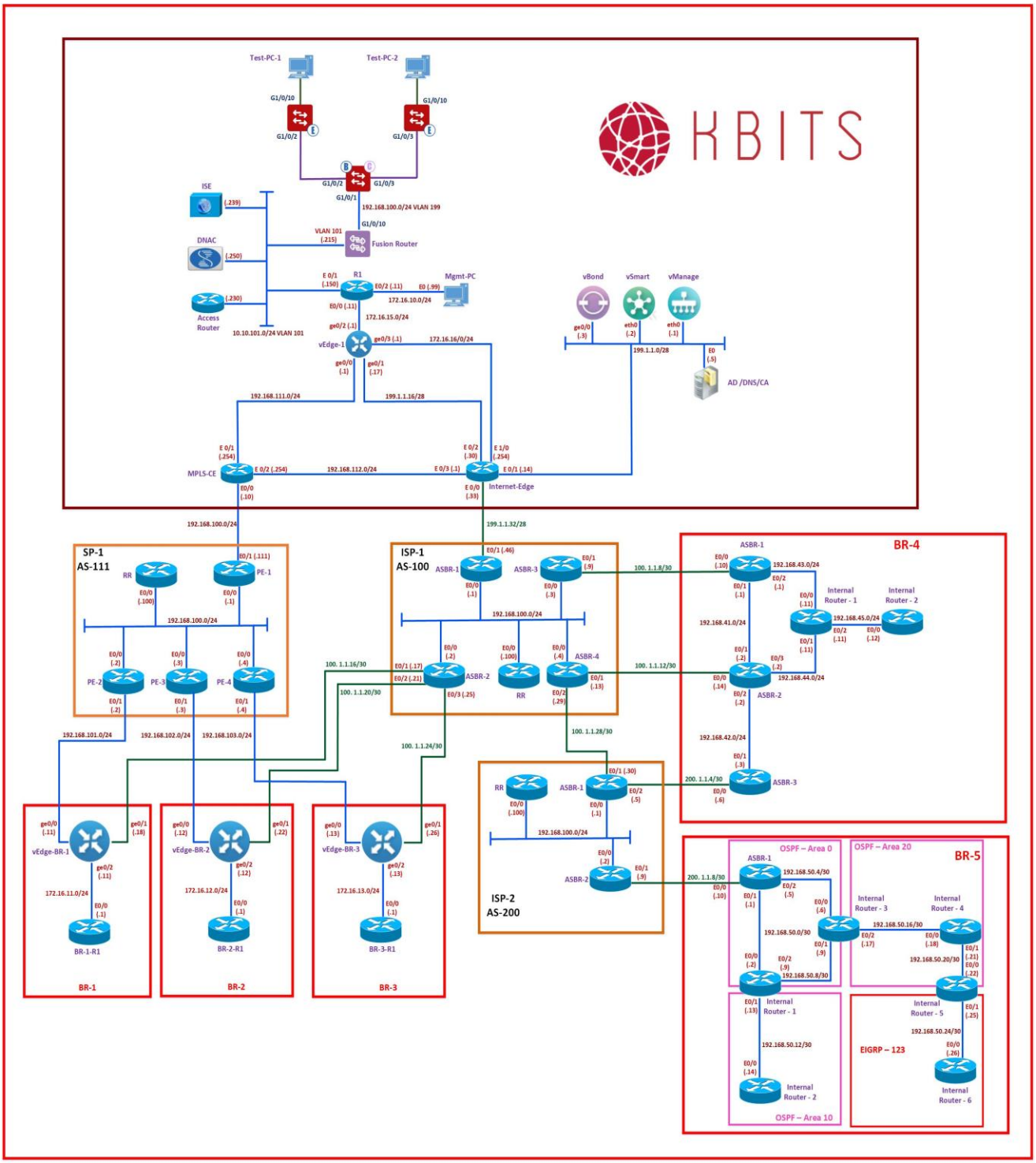
Khawar Butt
CCIE # 12353
Hepta CCIE#12353
CCDE # 20110020

Section 3

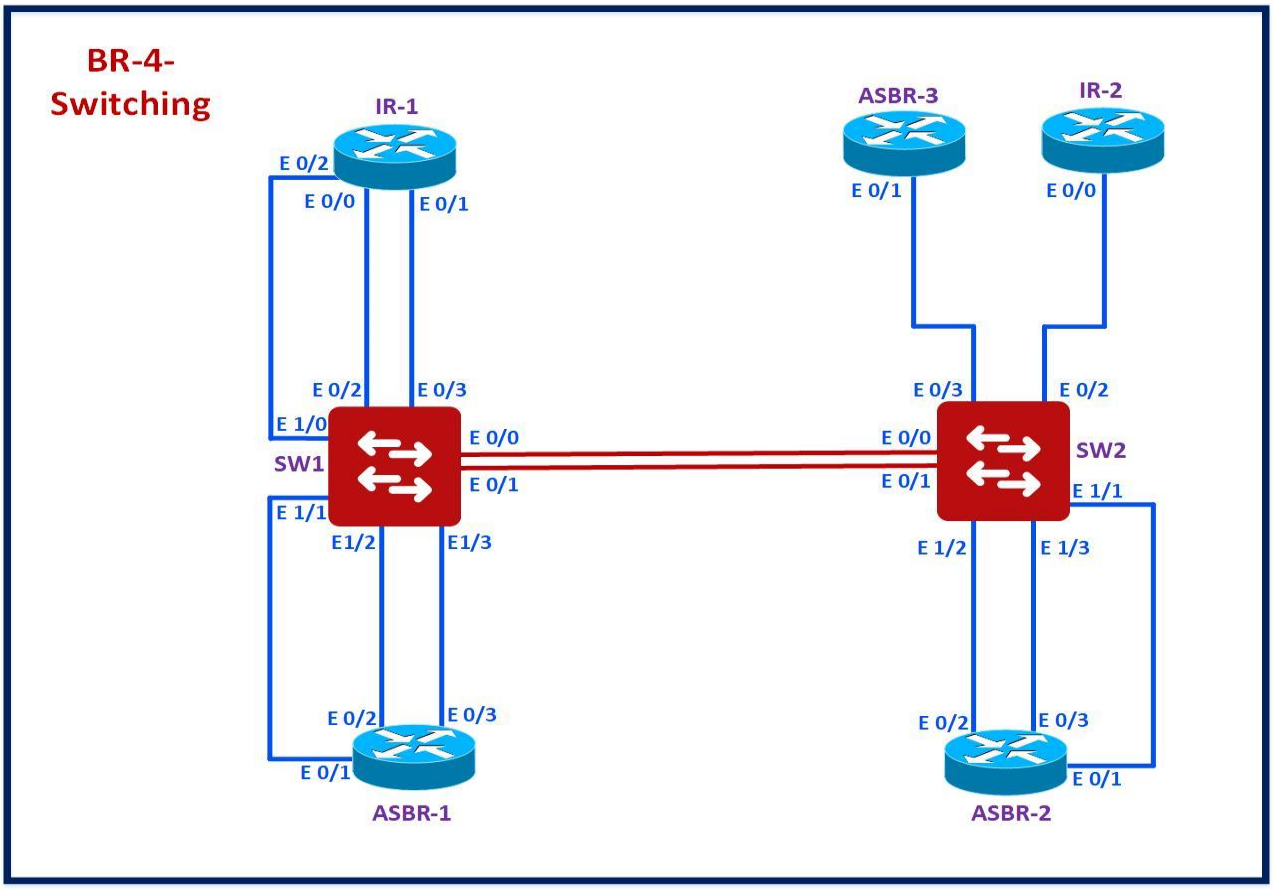
Switching

Lab 1 – Configuring Port-Channels, Trunks & VLANS – BR – 4

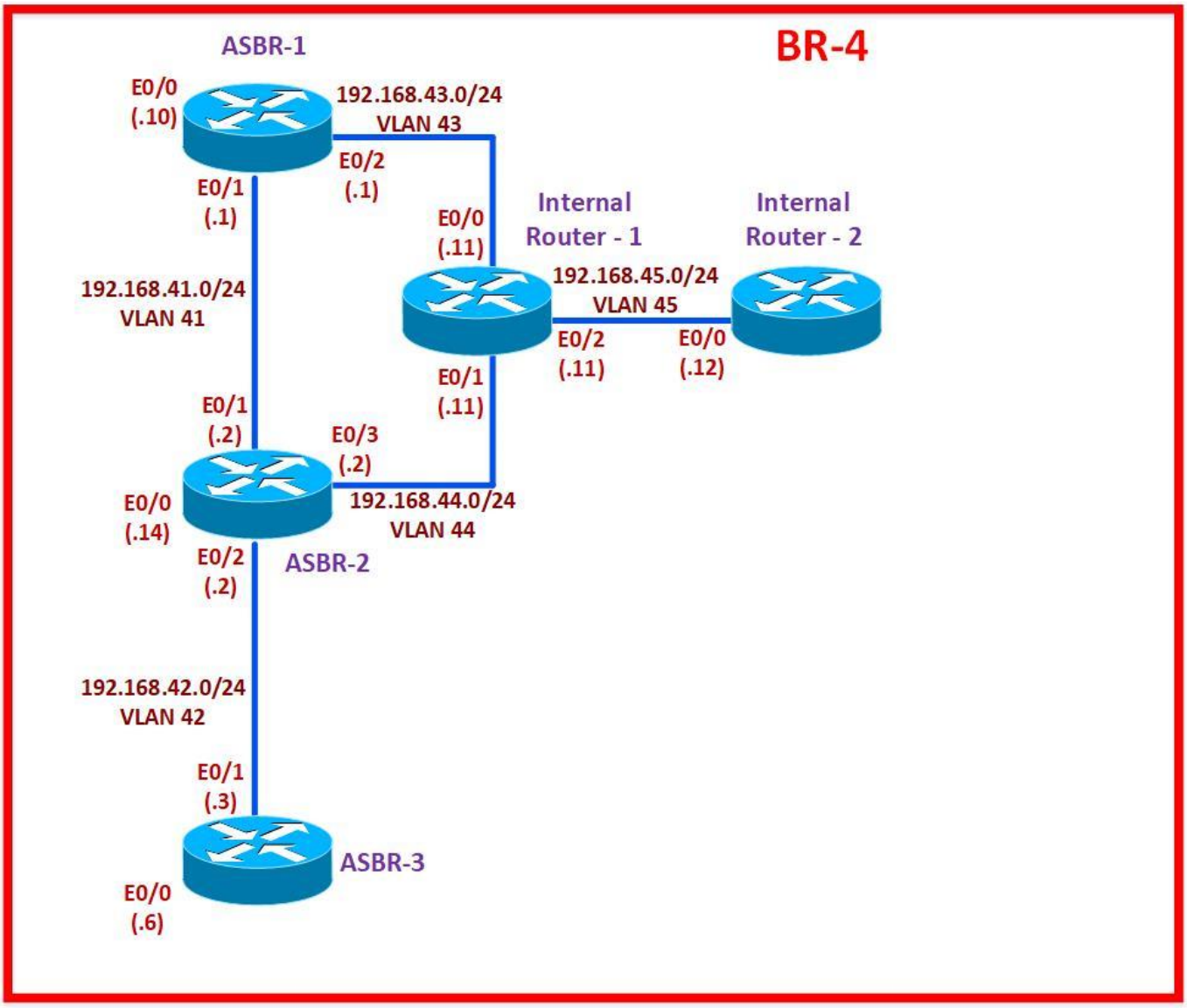
Full Topology



BR-4 Physical Topology



BR – 4 Logical Topology (L3)



Task 1 – Configure a Port-Channel between SW1 & SW2

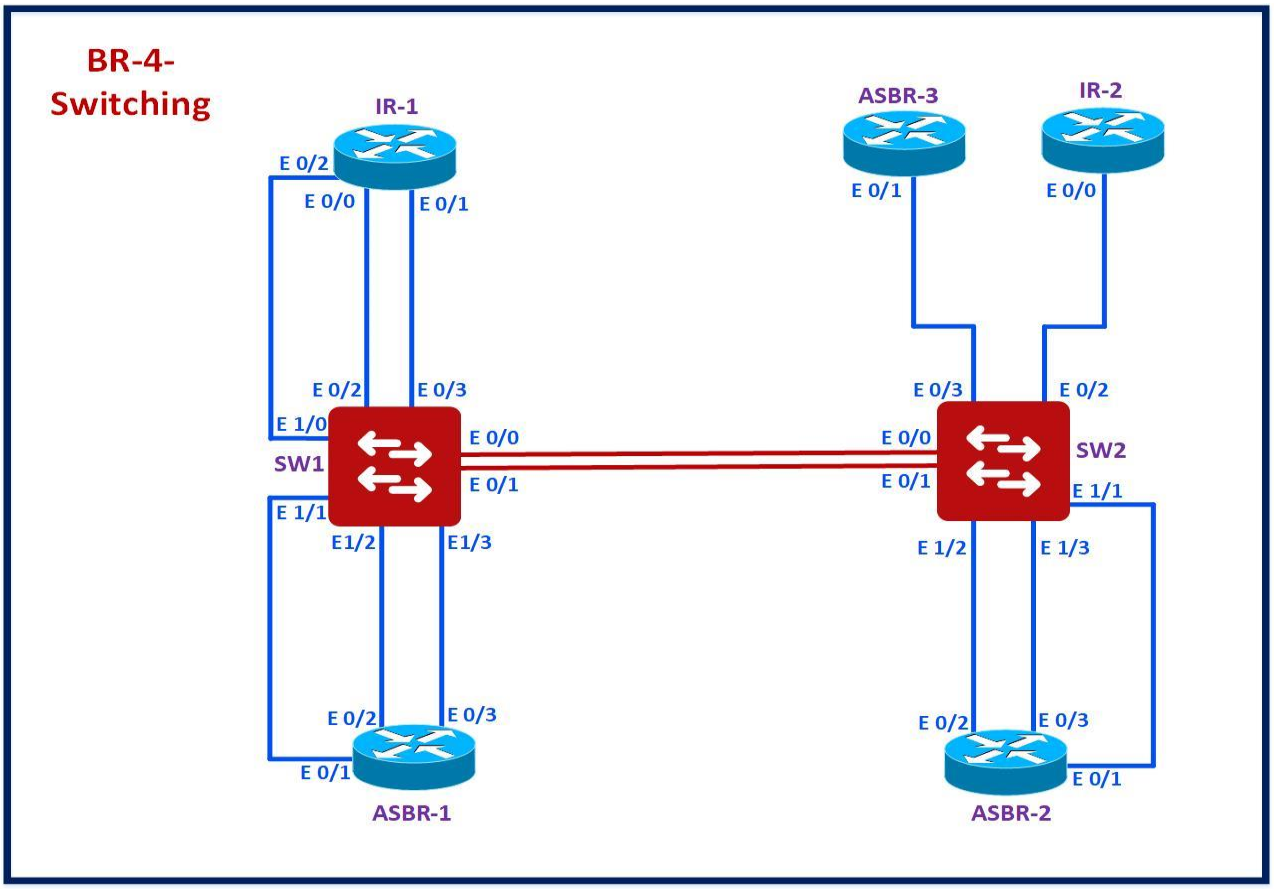
- Configure a Port-Channel between SW1 & SW2.
- Use Port-Channel ID of 10.
- Use LACP to establish the Port-Channel
- Configure the Port-Channel as a Trunk using Dot1q Trunking.

Task 2 – Create all the required VLANs on SW1 & SW2

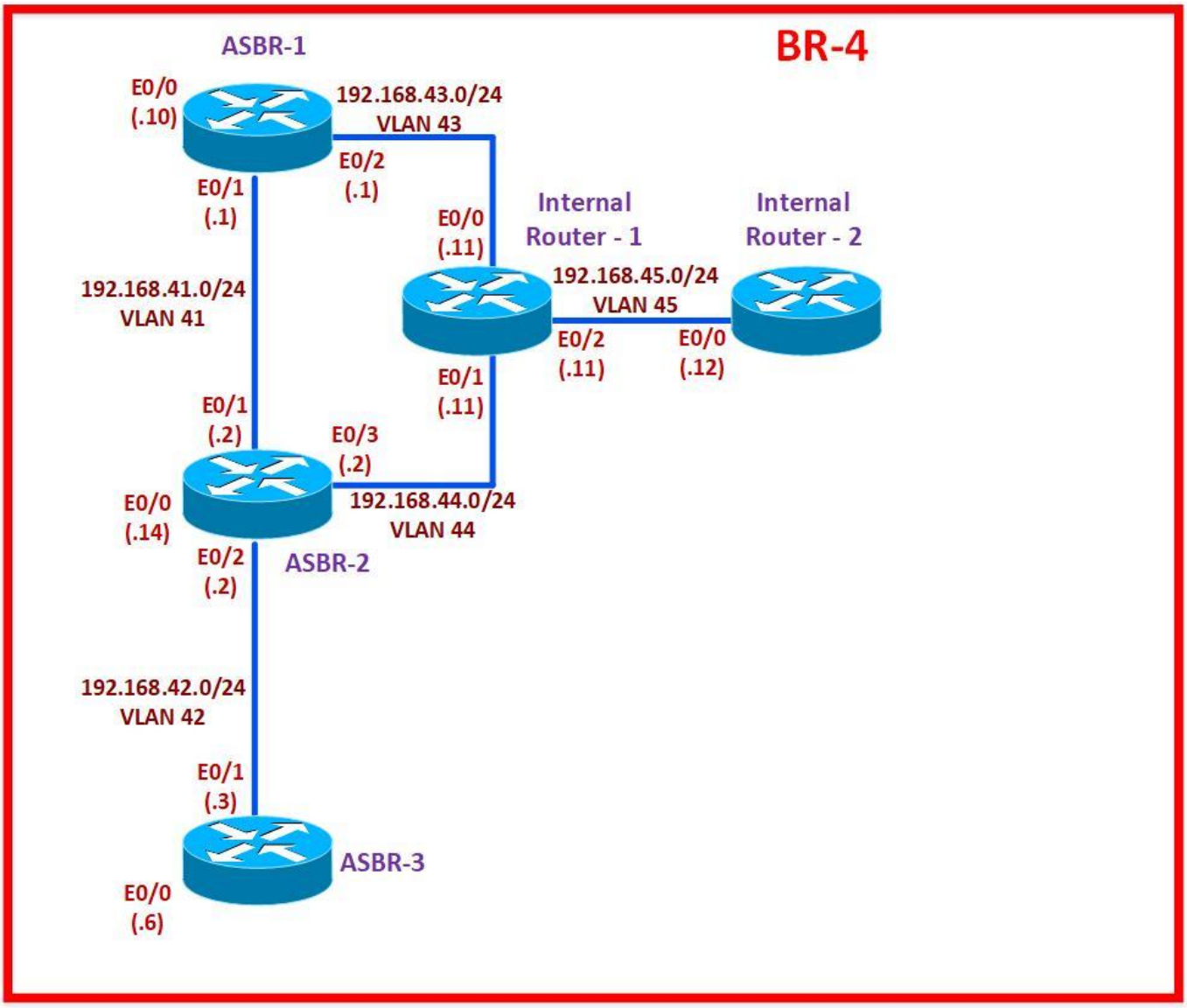
- Configure the following VLANs on both the HQ Switches.
  - ID: VLAN 41 – Name: OUTSIDE-1
  - ID: VLAN 42 – Name: OUTSIDE-2
  - ID: VLAN 43 – Name: INSIDE-1
  - ID: VLAN 44 – Name: INSIDE-2
  - ID: VLAN 45 – Name: INSIDE-3

Lab 2 – Mapping Physical Topology to Logical Topology for BR-4

BR-4 Physical Topology



BR – 4 Logical Topology (L3)



BR-4-ASBR1

Interface	IP Address	Subnet Mask
E 0/0	100.1.1.10	255.255.255.252
E 0/1	192.168.41.1	255.255.255.0
E 0/2	192.168.43.1	255.255.255.0

BR-4-ASBR2

Interface	IP Address	Subnet Mask
E 0/0	100.1.1.14	255.255.255.252
E 0/1	192.168.41.2	255.255.255.0
E 0/2	192.168.44.2	255.255.255.0
E 0/3	192.168.42.2	255.255.255.0

BR-4-ASBR3

Interface	IP Address	Subnet Mask
E 0/0	200.1.1.6	255.255.255.252
E 0/1	192.168.42.3	255.255.255.0

BR-4-Internal-1

Interface	IP Address	Subnet Mask
E 0/0	192.168.43.4	255.255.255.0
E 0/1	192.168.44.4	255.255.255.0
E 0/2	192.168.45.4	255.255.255.0
Loopback1	192.168.46.1	255.255.255.0
Loopback2	192.168.47.1	255.255.255.0

BR-4-Internal-2

Interface	IP Address	Subnet Mask
E 0/0	192.168.45.5	255.255.255.0
Loopback1	192.168.48.1	255.255.255.0
Loopback2	192.168.49.1	255.255.255.0

Task 1 – Assign appropriate ports to VLAN 41 – OUTSIDE-1

- Assign the appropriate ports on SW-1 & SW-2 to VLAN 41. They should bypass the STP learning & listening states.
- ASBR-1 & ASBR-2 should be able to communicate to each other at the completion of this task.

Task 2 – Assign appropriate ports to VLAN 42 – OUTSIDE-2

- Assign the appropriate ports on SW-1 & SW-2 to VLAN 42. They should bypass the STP learning & listening states.
- ASBR-2 & ASBR-3 should be able to communicate to each other at the completion of this task.

Task 3 – Assign appropriate ports to VLAN 43 – INSIDE-1

- Assign the appropriate ports on SW-1 & SW-2 to VLAN 43. They should bypass the STP learning & listening states.
- ASBR-1 & Internal Router-1 should be able to communicate to each other at the completion of this task.

Task 4 – Assign appropriate ports to VLAN 44 – INSIDE-2

- Assign the appropriate ports on SW-1 & SW-2 to VLAN 44. They should bypass the STP learning & listening states.
- ASBR-2 & Internal Router-1 should be able to communicate to each other at the completion of this task.

Task 5 – Assign appropriate ports to VLAN 45 – INSIDE-3

- Assign the appropriate ports on SW-1 & SW-2 to VLAN 45. They should bypass the STP learning & listening states.
- Internal Router-1 & Internal Router-2 should be able to communicate to each other at the completion of this task.

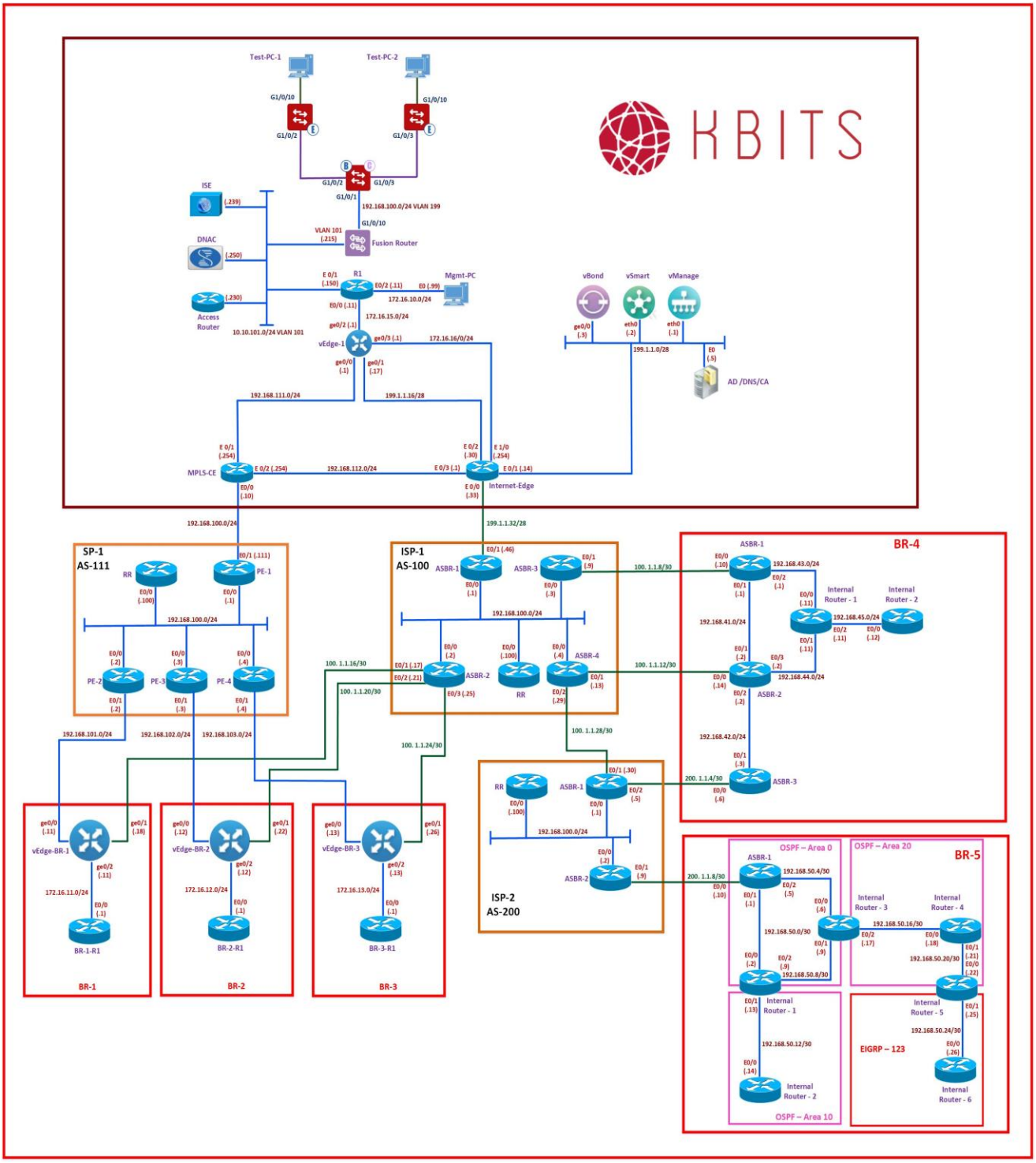
CCIE Enterprise Infrastructure – Super Lab

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

Section 4

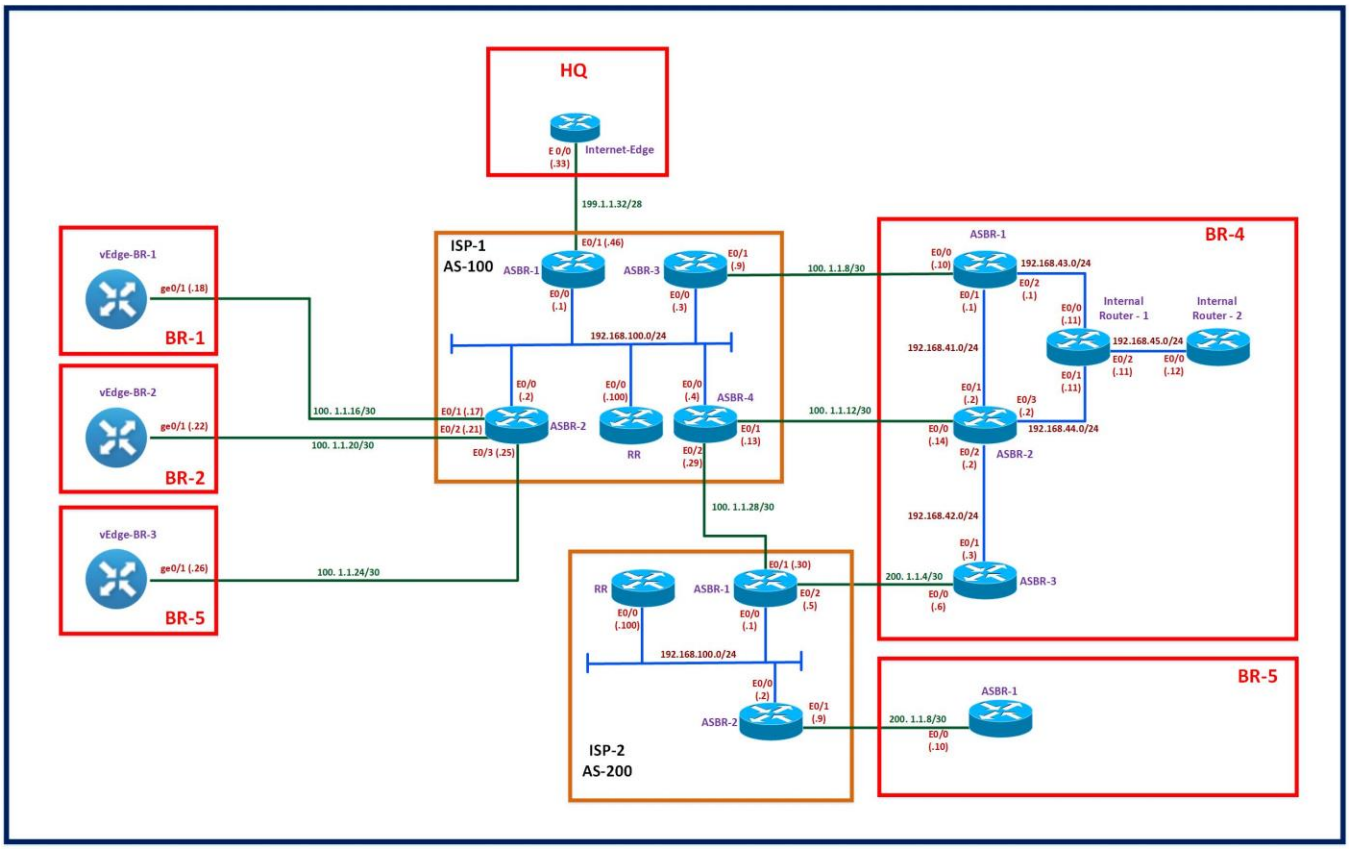
Configuring BGP

Full Topology



Lab 1 – Configuring BGP – HQ & ISP-1

BGP Topology



External Interface Configuration (Pre-Configured)

ISP-1-ASBR-1

Interface	IP Address	Subnet Mask
E 0/1	199.1.1.46	255.255.255.240

ISP-1-ASBR-2

Interface	IP Address	Subnet Mask
E 0/1	100.1.1.17	255.255.255.252
E 0/2	100.1.1.21	255.255.255.252
E 0/3	100.1.1.25	255.255.255.252

ISP-1-ASBR-3

Interface	IP Address	Subnet Mask
E 0/1	100.1.1.9	255.255.255.252

ISP-1-ASBR-4

Interface	IP Address	Subnet Mask
E 0/1	100.1.1.13	255.255.255.252
E 0/2	100.1.1.29	255.255.255.252

ISP-2-ASBR-1

Interface	IP Address	Subnet Mask
E 0/1	100.1.1.30	255.255.255.252
E 0/2	200.1.1.5	255.255.255.252

ISP-2-ASBR-2

Interface	IP Address	Subnet Mask
E 0/1	200.1.1.9	255.255.255.252

HQ-Internet-Edge

Interface	IP Address	Subnet Mask
E 0/0	199.1.1.33	255.255.255.240

BR-1-vEdge

Interface	IP Address	Subnet Mask
Ge0/0	100.1.1.18	255.255.255.252

BR-2-vEdge

Interface	IP Address	Subnet Mask
Ge0/0	100.1.1.22	255.255.255.252

BR-3-vEdge

Interface	IP Address	Subnet Mask
Ge0/0	100.1.1.26	255.255.255.252

BR-4-ASBR-1

Interface	IP Address	Subnet Mask
E 0/0	100.1.1.10	255.255.255.252

BR-4-ASBR-2

Interface	IP Address	Subnet Mask
E 0/0	100.1.1.14	255.255.255.252

BR-4-ASBR-3

Interface	IP Address	Subnet Mask
E 0/0	200.1.1.6	255.255.255.252

BR-5-ASBR-1

Interface	IP Address	Subnet Mask
E 0/0	200.1.1.10	255.255.255.252
E 0/1	192.168.50.1	255.255.255.252
E 0/2	192.168.50.5	255.255.255.252
Loopback1	192.168.51.1	255.255.255.0

Task 1 – Configure BGP between HQ Internet Edge Router & ISP-1-ASBR-1

- Configure BGP in AS 65111 on Internet Edge Router in HQ. It should form a neighbor relationship with ISP-1-ASBR based on the diagram.
- Redistribute the Connected ISP1-Internet Edge link on ISP-1-ASBR.

Task 2 – Authenticate the Neighbor relationships between AS 65111 & AS 100 using MD5

- Configure BGP to authenticate the neighbor relationships using MD5 authentication.
- Use password of **Kbits@123**.

Task 3 – Advertise the External Links on ISP-1 ASBR-2

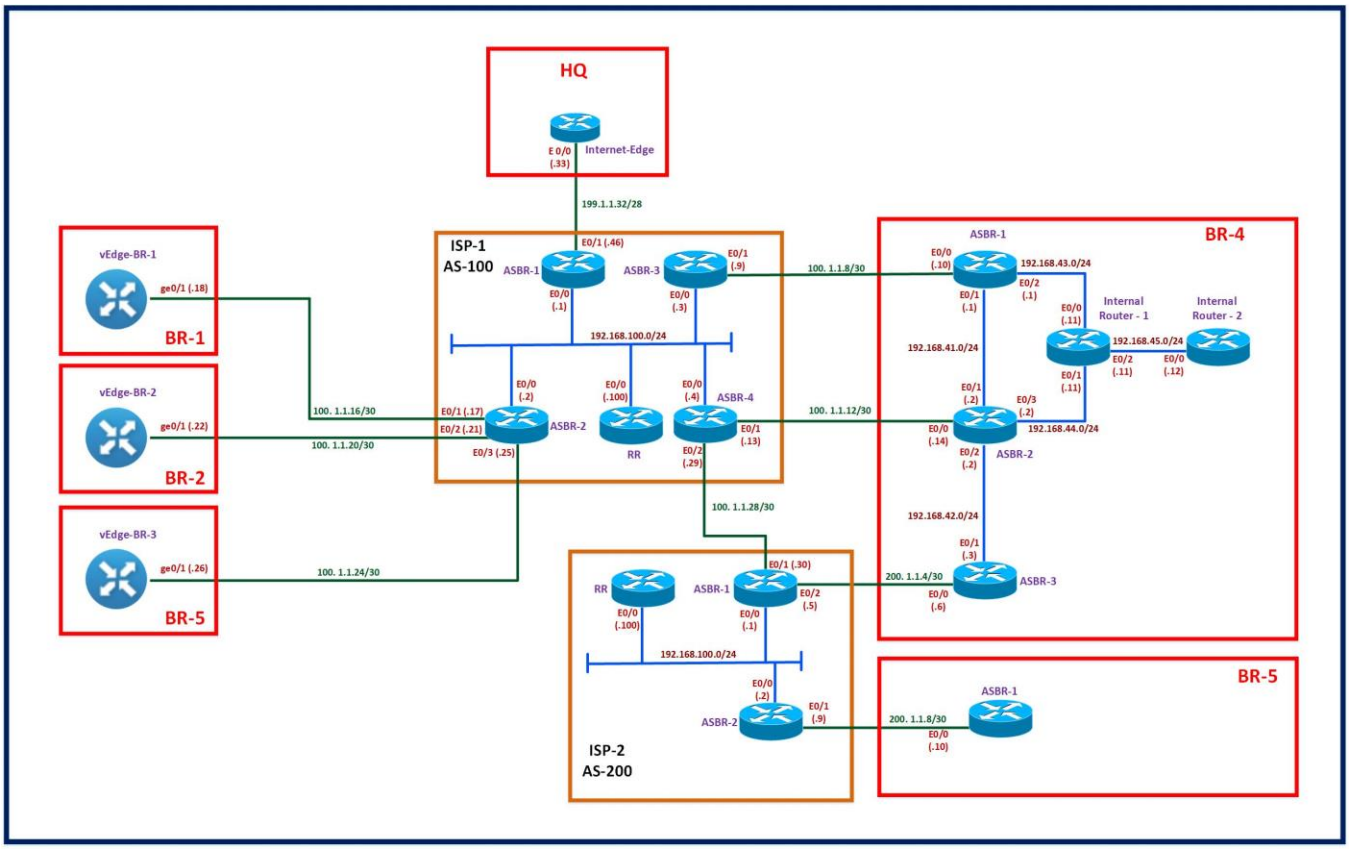
- Advertise the External Links on ISP-1 ASBR-2 connecting towards BR-1, BR-2 & BR-3 in BGP.

Task 4 – Advertise the Local Public networks in BGP on the Internet Edge Router

- Advertise 199.1.1.0/28 & 199.1.1.16/28 networks in BGP on the Internet Edge Router.

Lab 2 – Configuring eBGP – Branch-4

BGP Topology



Task 1 – Configure BGP between Branch-4 Routers (BR-4-ASBR-1 & BR-4-ASBR-2) & ISP-1

- Configure BGP in AS 65114 on BR-4-ASBR-1 & BR-4-ASBR-2. They should form a neighbor relationship with ISP-1-ASBRs based on the diagram.
- Redistribute the Connected Links between ISP1 & Branch4 on the ISP-1 ASBRs.

Task 2 – Authenticate the Neighbor relationships between AS 65114 & AS 100 using MD5

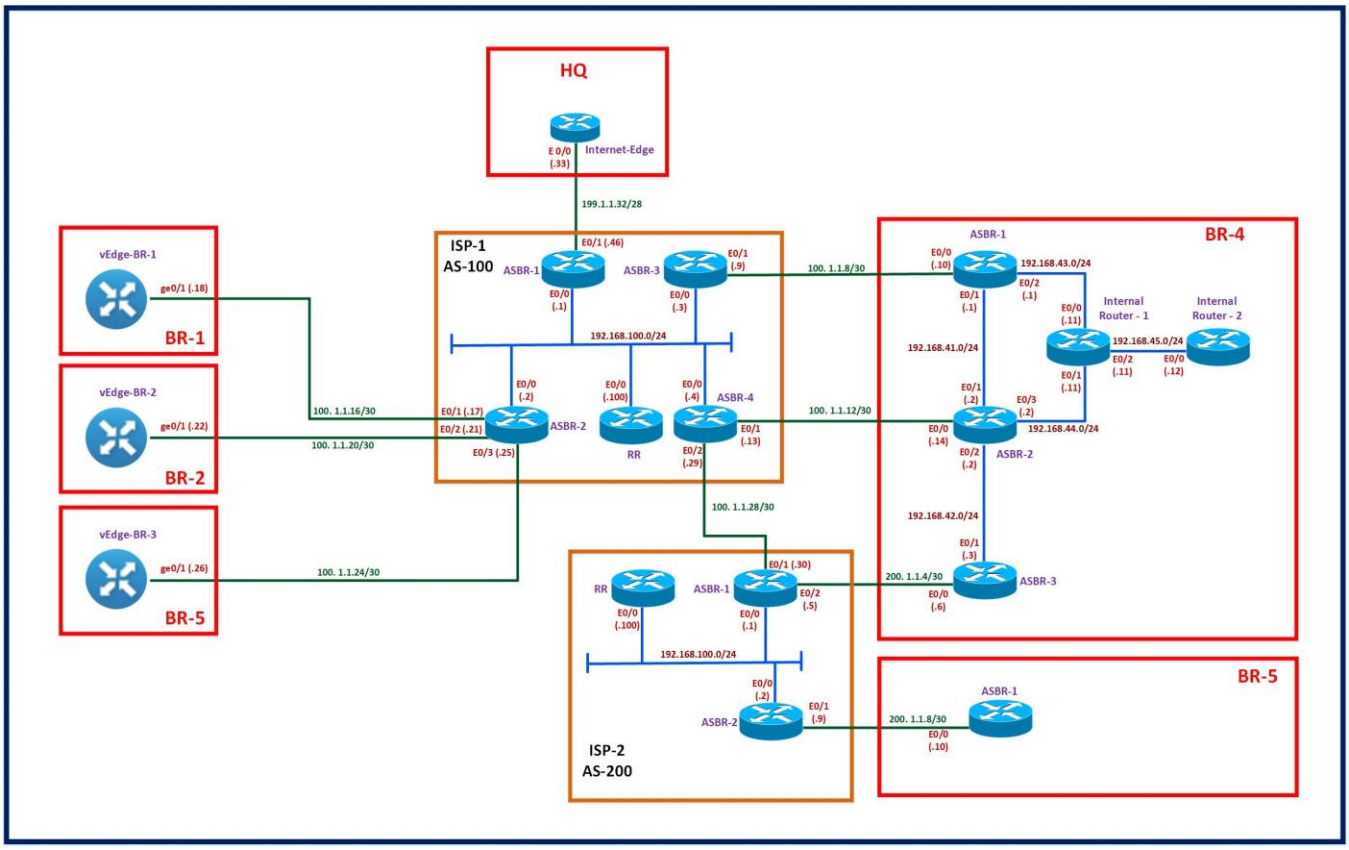
- Configure BGP to authenticate the neighbor relationships using MD5 authentication.
- Use password of **Kbits@123**.

Task 3 – Configure BGP between BR-4-ASBR-3 & ISP-2

- Configure BGP in AS 65114 on BR-4-ASBR-3. It should form a neighbor relationship with ISP-2-ASBR-1.
- Redistribute the Connected Links between ISP2 & Branch4 on the ISP-2 ASBR.

Lab 3 – Configuring BGP – Branch-5

BGP Topology



Task 1 – Configure BGP between BR-5-ASBR-1 & ISP-2

- Configure BGP in AS 65115 on BR-5-ASBR-1. It should form a neighbor relationship with ISP-2-ASBR-2 based on the diagram.
- Redistribute the Connected Links between ISP2 & Branch5 on the ISP-2-ASBR-2.

Task 2 – Authenticate the Neighbor relationships between AS 65115 & AS 200 using MD5

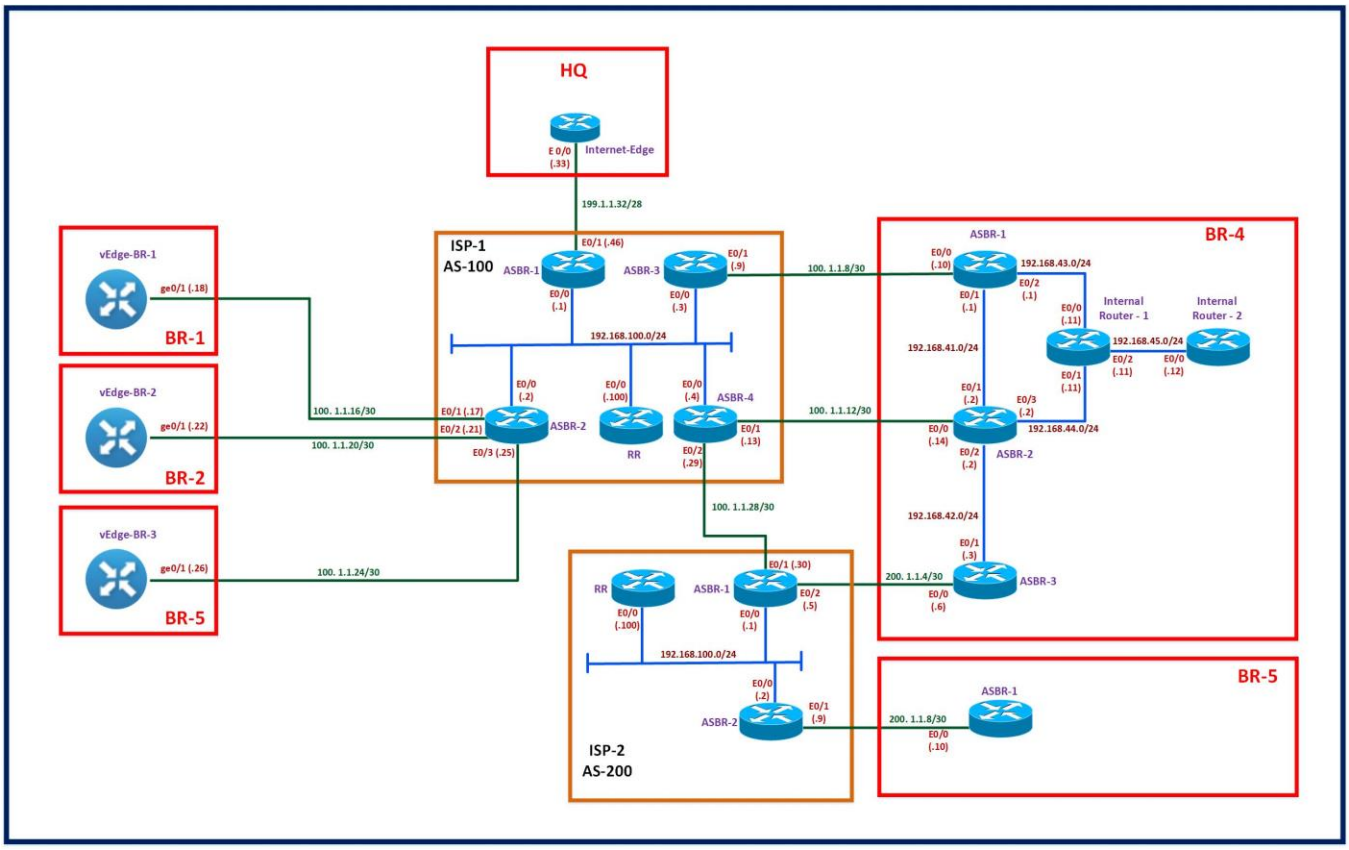
- Configure BGP to authenticate the neighbor relationships using MD5 authentication.
- Use password of **Kbits@123**.

Task 3 – Injecting a Default Route

- Configure ISP-2-ASBR-2 to inject a default route into 65115.

Lab 4 – Configuring IGP – EIGRP

BGP Topology



Task 1 – Configure new networks on the Internal Networks and run EIGRP as the IGP

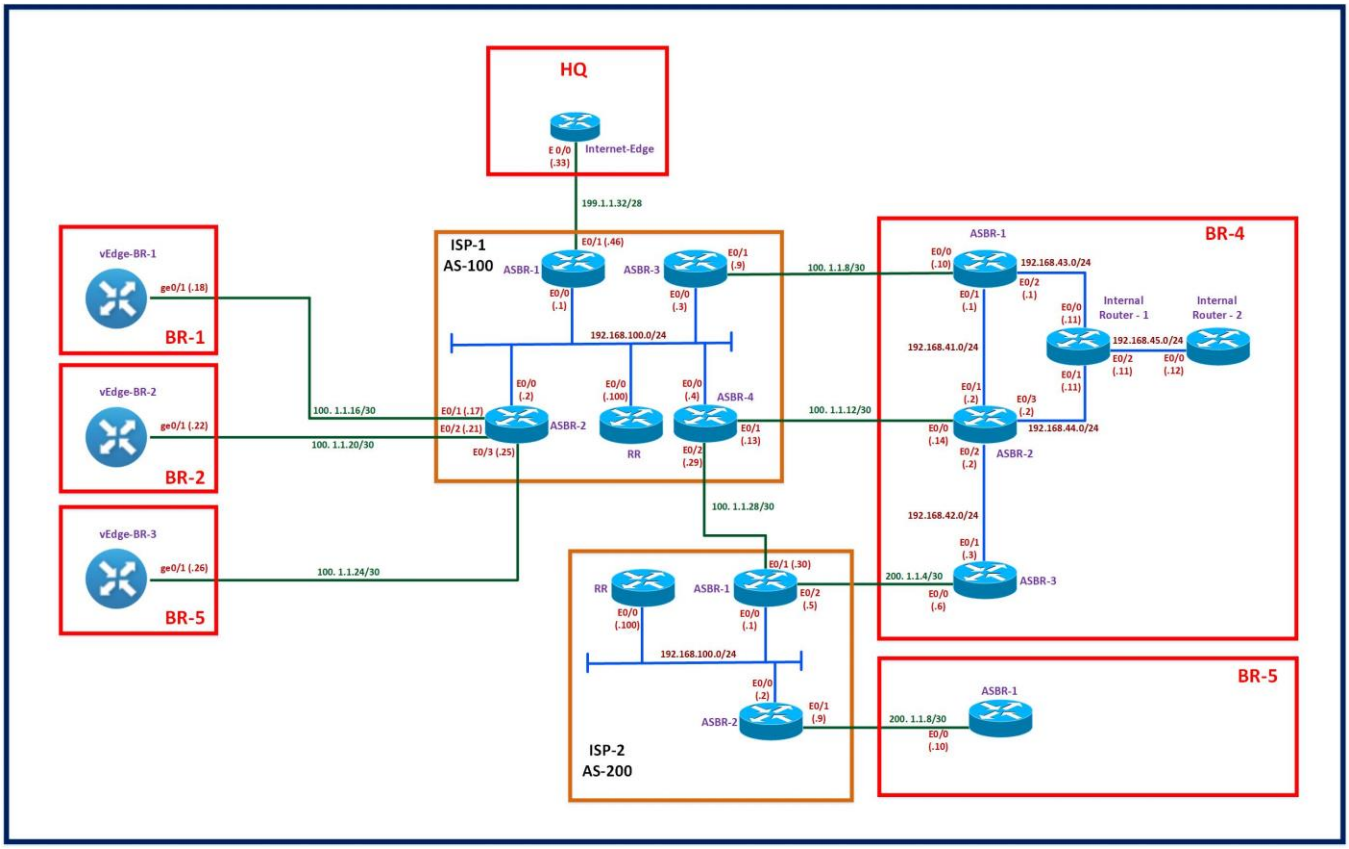
- Configure the following loopbacks on BR-4-Internal-Router-2:
  - Loopback101 – 200.1.5.1/28
  - Loopback102 – 200.1.5.17/28
  - Loopback103 – 200.1.5.33/28
  - Loopback104 – 200.1.5.49/28
- Configure EIGRP in AS 65114 between BR-4-Internal-Router-1 & BR-4-Internal-Router-2.
- Enable all interfaces on BR-4-Internal-Router-2 in EIGRP.
- Enable the 2 Loopbacks and E 0/2 Interfaces only in EIGRP on BR-4-Internal-Router-1.

Task 2 – Authentication

- Configure EIGRP to authenticate the neighbor relationships using SHA authentication.
- Use a password of **Kbits@123**.

Lab 5 – Configuring Advanced BGP Features

BGP Topology



Task 1 – Configure iBGP between the BR-4-ASBR-1 & BR-4-ASBR-2

- Configure iBGP neighor relationship between BR-4-ASBR-1 & BR-4-ASBR-2 in AS 65114 using the Physical Interface IP's.
- Make sure to configure the "Next-hop-Self" option towards each other.

Task 2 – Configure iBGP between the BR-4-ASBR-2 & BR-4-ASBR-3

- Configure iBGP neighor relationship between BR-4-ASBR-2 & BR-4-ASBR-3 in AS 65114.
- Make sure to configure the "Next-hop-Self" option towards each other.

Task 3 – Enable Multi-Path

- Configure Multi-Pathing on BR-4-ASBR-2.
- It should be able to use multiple paths to get to AS 100 routes.

Task 4 – Route-Reflection

- Configure BR-4-ASBR-2 as a Route-reflector to propagate routes between BR-4-ASBR-1 & BR-4-ASBR-3.
- Make sure that the routes are getting injected into the BGP Table.

Task 5 – Redistribution

- Configure iBGP between BR-4-ASBR-1 & BR-4-Internal-Router-1.
- Configure iBGP between BR-4-ASBR-2 & BR-4-Internal-Router-1.
- Configure Route Redistribution between EIGRP and BGP on BR-4-Internal-Router-1.
- Only inject 200.1.5.X/24 routes from EIGRP into BGP.
- Make sure that all BGP routes show up on BR-4-Internal-Router-2.

CCIE Enterprise Infrastructure – Super Lab

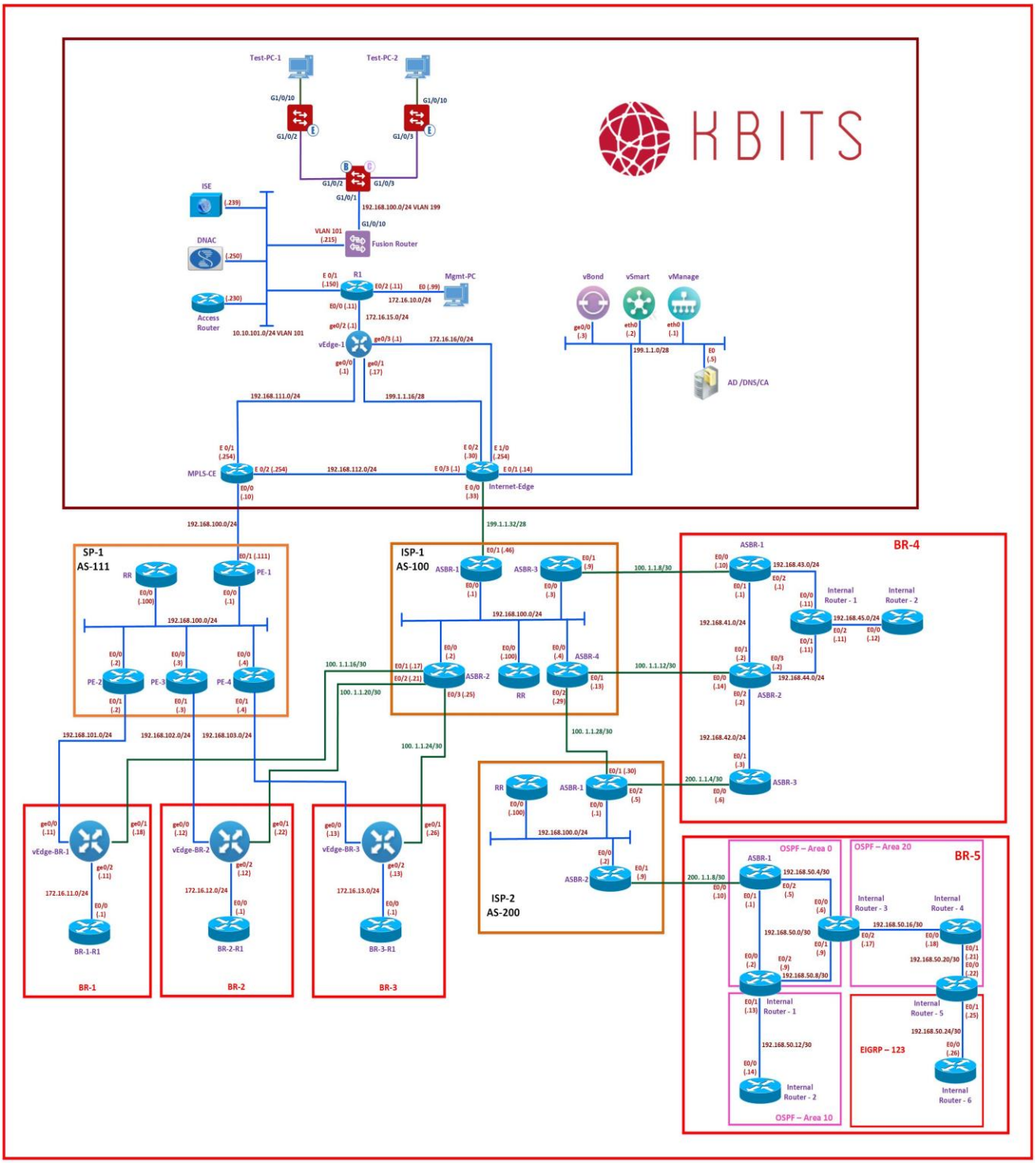
Khawar Butt
CCIE # 12353
Hepta CCIE#12353
CCDE # 20110020

Section 5

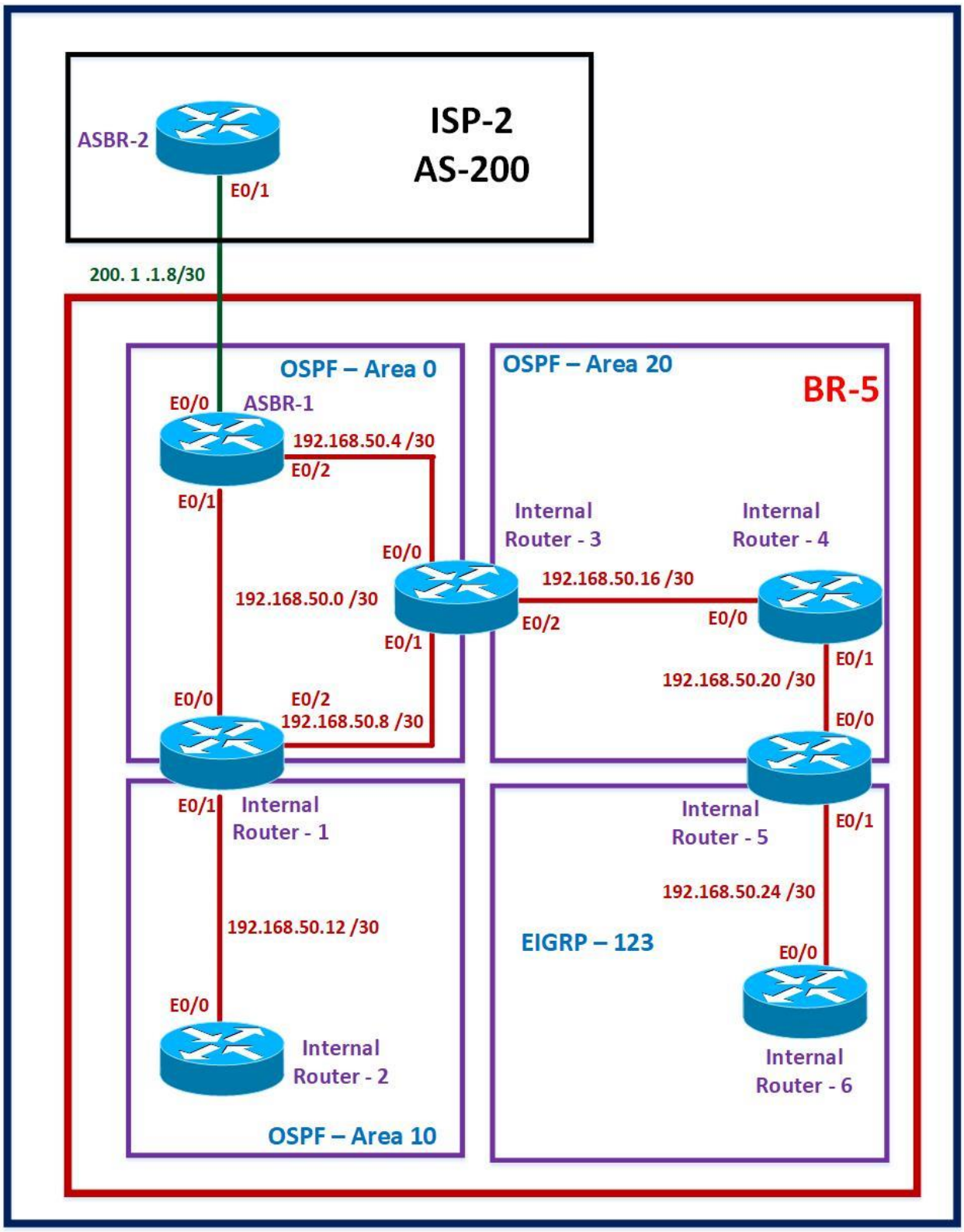
Configuring IGPs

Lab 1 – Configuring OSPF – Basic

Full Topology



Branch 5 – IGP



Interface Configuration (Pre-Configured)

ISP-2-ASBR-1

Interface	IP Address	Subnet Mask
E 0/1	200.1.1.9	255.255.255.252

BR-5-ASBR-1

Interface	IP Address	Subnet Mask
E 0/0	200.1.1.10	255.255.255.252
E 0/1	192.168.50.1	255.255.255.252
E 0/2	192.168.50.5	255.255.255.252

BR-5-Internal-Router-1

Interface	IP Address	Subnet Mask
E 0/0	192.168.50.2	255.255.255.252
E 0/1	192.168.50.13	255.255.255.252
E 0/2	192.168.50.9	255.255.255.252
Loopback 1	150.1.50.193	255.255.255.240

BR-5-Internal-Router-2

Interface	IP Address	Subnet Mask
E 0/0	192.168.50.14	255.255.255.252
Loopback 1	150.1.50.1	255.255.255.240
Loopback 2	150.1.50.17	255.255.255.240
Loopback 3	150.1.50.33	255.255.255.240
Loopback 4	150.1.50.49	255.255.255.240

BR-5-Internal-Router-3

Interface	IP Address	Subnet Mask
E 0/0	192.168.50.6	255.255.255.252
E 0/1	192.168.50.10	255.255.255.252
E 0/2	192.168.50.17	255.255.255.252
Loopback 1	150.1.50.209	255.255.255.240

BR-5-Internal-Router-4

Interface	IP Address	Subnet Mask
E 0/0	192.168.50.18	255.255.255.252
E 0/1	192.168.50.21	255.255.255.252
Loopback 1	150.1.50.65	255.255.255.240
Loopback 2	150.1.50.81	255.255.255.240
Loopback 3	150.1.50.97	255.255.255.240
Loopback 4	150.1.50.113	255.255.255.240

BR-5-Internal-Router-5

Interface	IP Address	Subnet Mask
E 0/0	192.168.50.22	255.255.255.252
E 0/1	192.168.50.25	255.255.255.252
Loopback 1	150.1.50.225	255.255.255.240

BR-5-Internal-Router-6

Interface	IP Address	Subnet Mask
E 0/0	192.168.50.26	255.255.255.252
Loopback 1	150.1.50.129	255.255.255.224
Loopback 2	150.1.50.145	255.255.255.224
Loopback 3	150.1.50.161	255.255.255.224
Loopback 4	150.1.50.177	255.255.255.224

Task 1 – Configure OSPF in Area 0

- Configure OSPF in Area 0 based on the diagram.
- Configure the Router-ID's based on the following:
  - ASBR-1 – 0.0.5.0
  - Internal-Router-1 – 0.0.5.1
  - Internal-Router-3 – 0.0.5.3
- Loopback Interfaces should be advertised based on the Interface Mask.

Task 2 – Configure OSPF in Area 10

- Configure OSPF in Area 10 based on the diagram.
- Configure the Router-ID's based on the following:
  - Internal-Router-2 – 0.0.5.2
- Loopback Interfaces on Internal-Router-2 should be advertised based on the Interface Mask.

Task 3 – Configure OSPF in Area 20

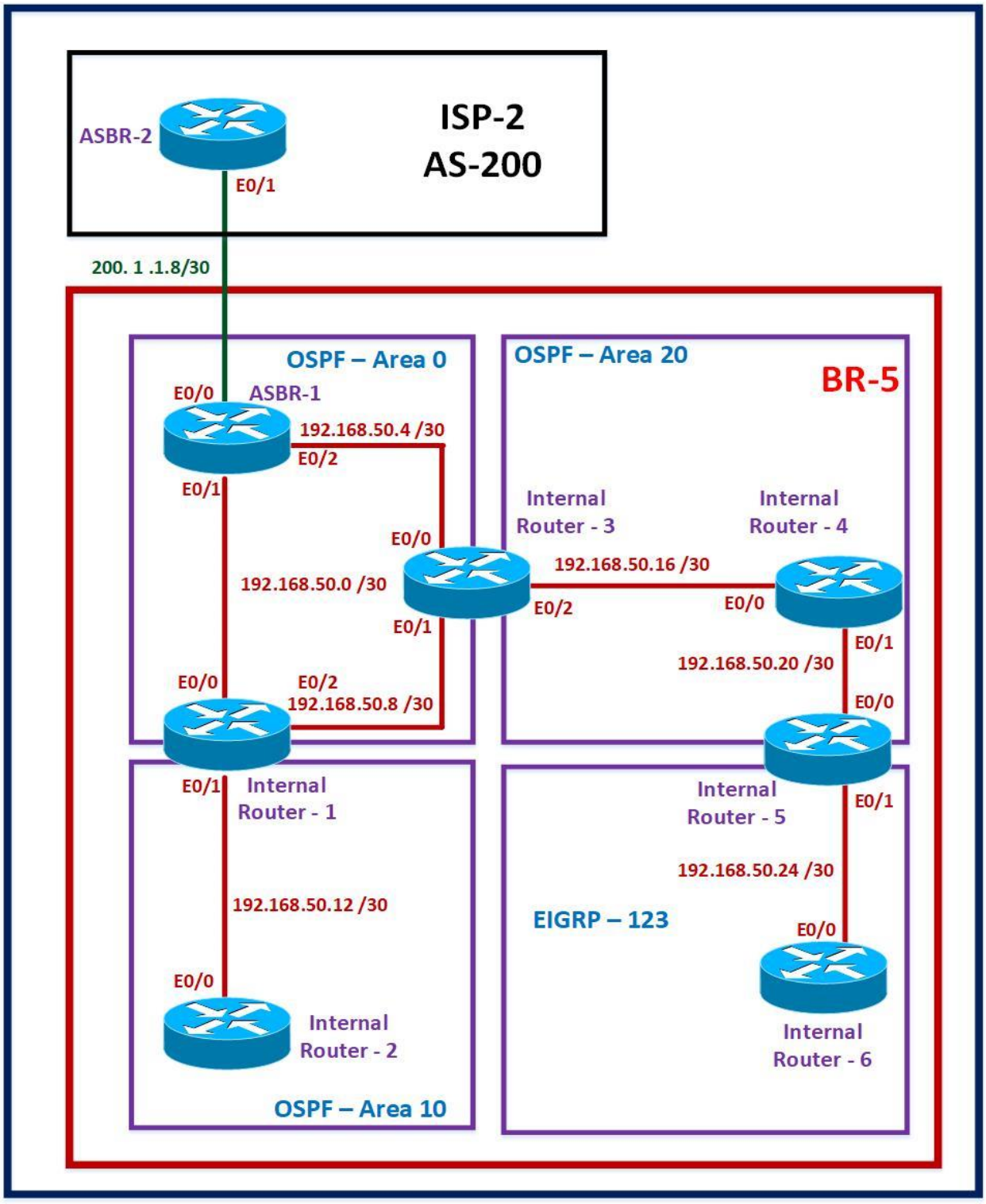
- Configure OSPF in Area 20 based on the diagram.
- Configure the Router-ID's based on the following:
  - Internal-Router-4 – 0.0.5.4
  - Internal-Router-5 – 0.0.5.5
- Loopback Interfaces on Internal-Router-4 should be advertised based on the Interface Mask.
- Do not advertise the Loopback of Internal-Router-5 in OSPF.

Task 4 – Authenticate the Neighbor relationships in Area 0

- Configure OSPF to authenticate the neighbor relationships between all routers in Area 0 using MD5 authentication.
- Use Key of 123 and a password of **Kbits@123**.

Lab 2 – Configuring EIGRP – Basic

Branch 5 – IGP



Task 1 – Configure EIGRP in AS 123

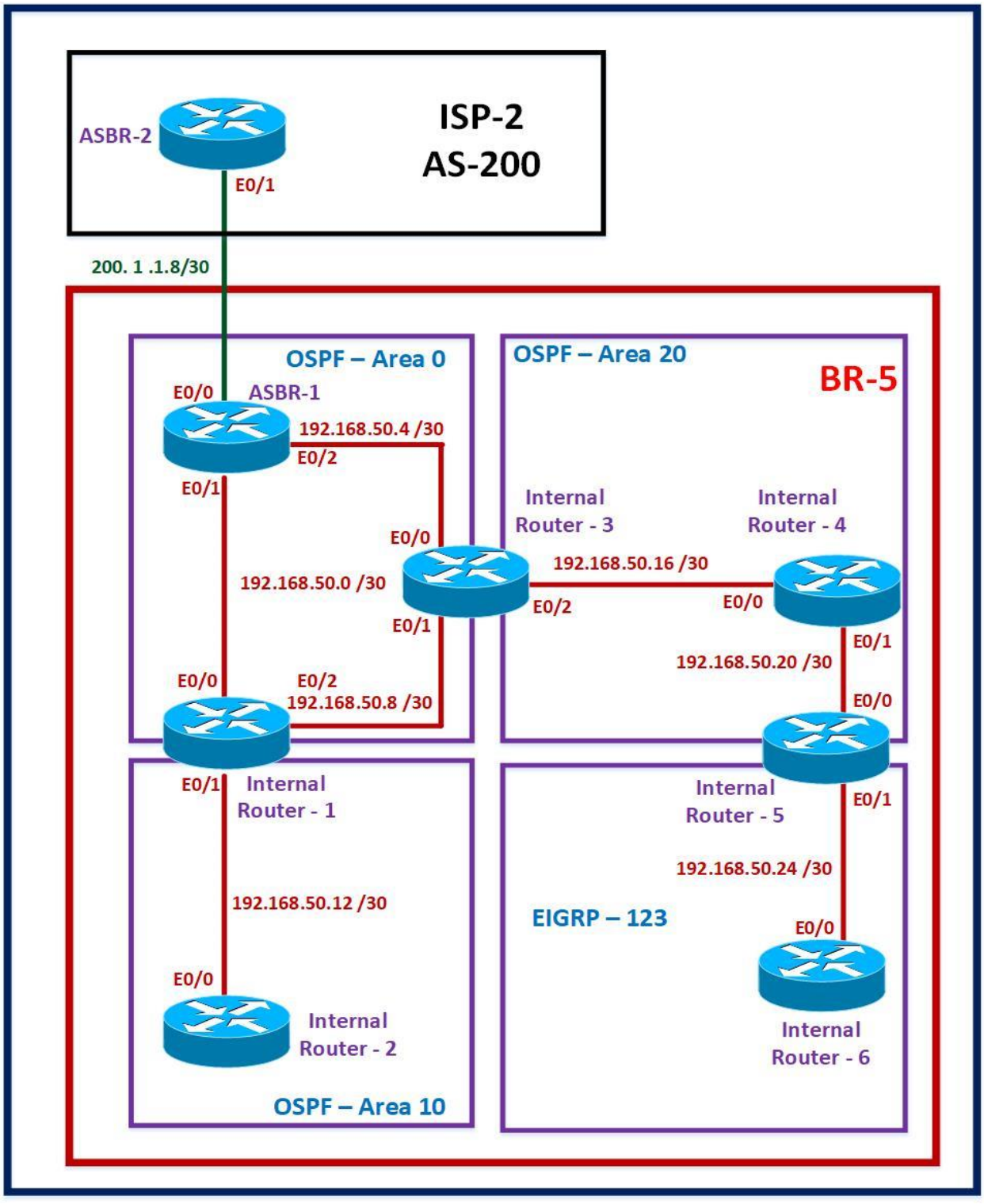
- Configure EIGRP in 123 based on the diagram.
- Use a name of **KBITS** for the EIGRP Configuration.
- Advertise the Loopback Interfaces on the 2 routers in EIGRP.

Task 2 – Authenticate the Neighbor relationships in EIGRP 123

- Configure EIGRP to authenticate the neighbor relationships using SHA authentication.
- Use password of **Kbits@123**.

Lab 3 – Configuring Route Redistribution

Branch 5 – IGP



Task 1 – Configure Redistribution between OSPF & BGP

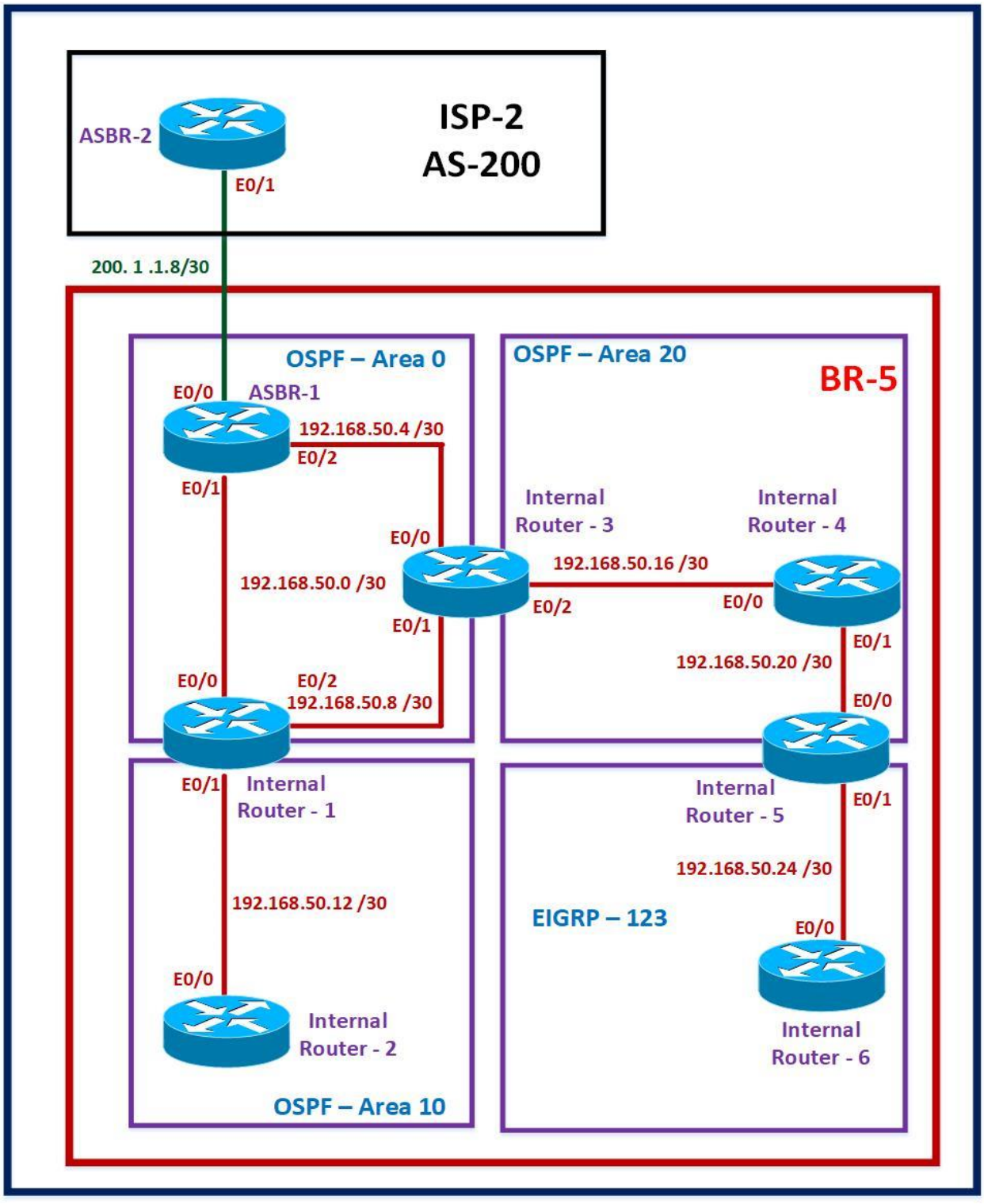
- Redistribute BGP Routes into OSPF on BR-5-ASBR-1.
- These routes should have a seed metric of 100.
- The Interface cost should be added to the metric as the BGP routes are propagated into the OSPF domain.
- Redistribute only the 150.1.50.0/24 networks into BGP. These routes should be seen with an origin code of "i" in BGP.
- Make sure all the 150.1.50.X routes in Branch-5 are seen in BGP.

Task 2 – Configure Redistribution between OSPF & EIGRP

- Configure Redistribution between OSPF & EIGRP on the appropriate router.
- OSPF should add the cost of the link to the metric as the EIGRP routes are propagated into the OSPF domain.

Lab 4 – Configuring Route Summarization

Branch 5 – IGP



Task 1 – Configure OSPF Inter-Area Route Summarization

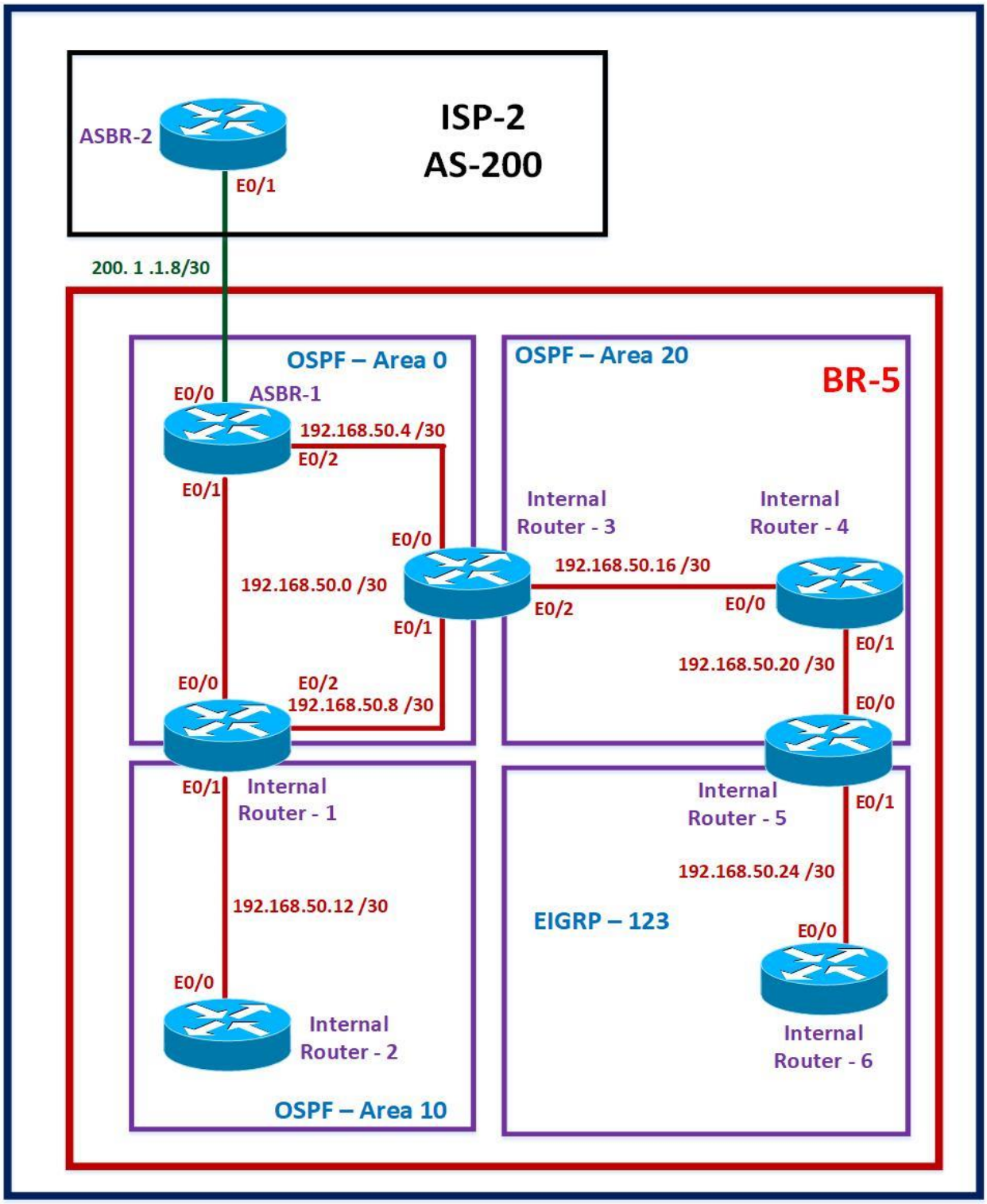
- Configure Route summarization for the Loopback networks behind Internal-Router-2 and Internal-Router-4 on the appropriate routers.
- Use the longest summarization possible.

Task 2 – Configure External Route Summarization

- Summarize all BGP routes in the 100.0.0.0/8 major network toward OSPF.

Lab 5 – Configuring OSPF Area Types

Branch 5 – IGP



Task 1 – Controlling Routes into Area 10

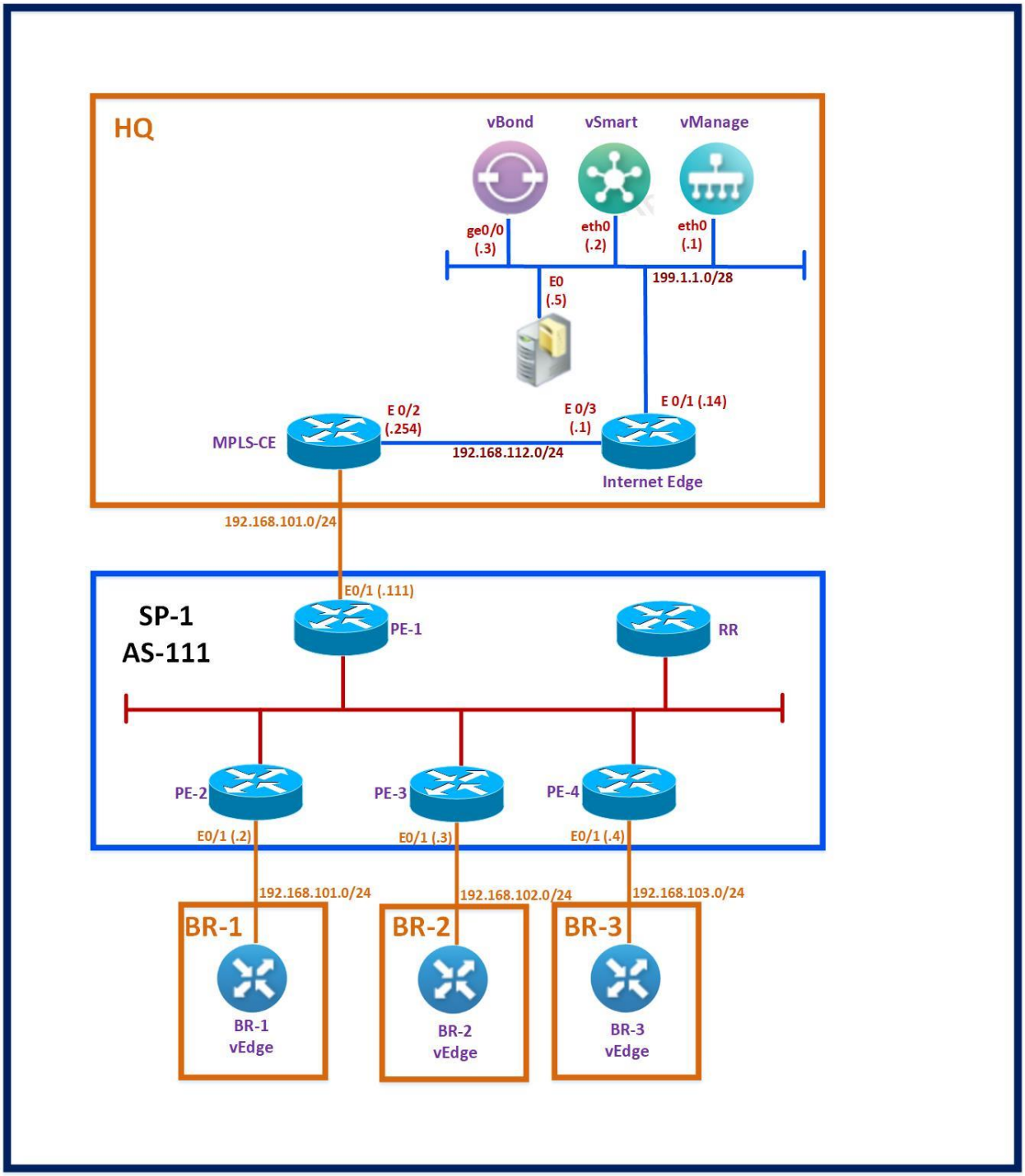
- Configure Area 10 such that no external routes are propagated into it.
- Area 10 should maintain full reachability towards them.

Task 2 – Controlling Routes into Area 20

- Configure Area 20 such that no backbone external routes are propagated into it.
- EIGRP routes from AS 123 should continue to propagate into Area 20.
- Area 20 should maintain full reachability towards the Backbone external routes.
- Default-Route should be injected in as a Type 7 LSA.

Lab 6 – Configuring EIGRP in HQ

HQ



Task 1 – Configuring EIGRP as the IGP between the MPLS CE & Internet Edge Routers

- Configure EIGRP in AS 12353 between MPLS CE & the Internet Edge router.
- Enable the 192.168.111.0/24 (vEdge network) in EIGRP on the MPLS CE Router.
- Enable the 199.1.1.0/28 (Controller Network) in EIGRP on the Internet Edge Router.
- No EIGRP updates should be sent towards the Controllers or vEdge-1.

Task 2 – Redistribution between BGP & EIGRP on the MPLS CE Router

- Configure Mutual redistribution between BGP and EIGRP on the MPLS CE router.

CCIE Enterprise Infrastructure – Super Lab

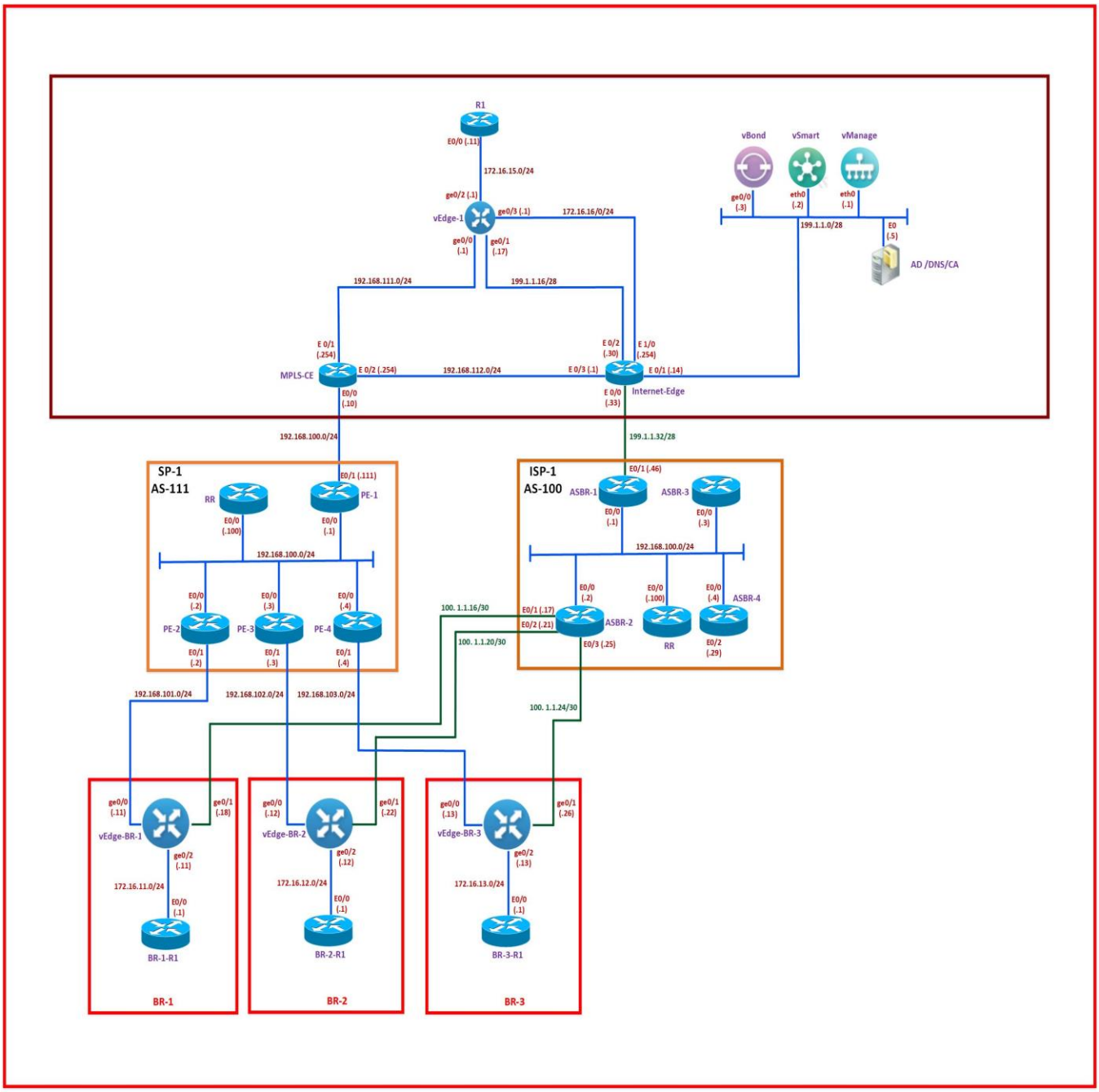
Khawar Butt
CCIE # 12353
Hepta CCIE#12353
CCDE # 20110020

Section 6

Configuring SD-WAN

Lab 1 – Registering the vEdges on vManage

SD-WAN Logical Topology



Pre-Configuration:

Controller Setup – vManage

Task 1 – Configuring the System Component

- Configure the System parameters based on the following:

  - Host-name: vManage1
  - Organization: KBITS
  - System-IP: 10.1.1.101
  - Site ID: 100
  - vbond Address: 199.1.1.3
  - Timezone: Dubai

Task 2 – Configured the vpn parameters

- Configure the VPN parameters based on the following:

  - vpn 0
    - Interface eth0
    - IP Address: 199.1.1.1/28
    - Tunnel Interface
    - Tunnel Services (NetConf, SSHD)
    - Default Route: 199.1.1.14

Task 3 – Organization name & vBond Address

- Configure the Administrator Settings based on parameters given below by logging into GUI of vManage thru the Management VPN.

  - Organization Name: **KBITS**
  - vBond Address: **199.1.1.3**

Task 4 – Configure Controller Authorization as Enterprise Root

- Configure the Controller Authorization via an Enterprise Root Server.
- The Enterprise CA Server is located at http://199.1.1.5/certsrv. Download and install the CA Root Certificate.
- Configure the CSR Properties based on the following:
  - Domain Name: kbits.live
  - Organization Units: KBITS
  - Organization: Viptela LLC
  - City: Dubai
  - State: Dubai
  - Country: AE

Task 5 – Generate a CSR for vManage. Register and download the vManage Identity Certificate from the CA Server

- Generate a CSR for vManage.
- Request and Download the Identity Certificate from the Enterprise CA Server.
- Install the vManage Identity Certificate on vManage.

Controller Setup – vBond

Task 1 – Configuring the System Component

- Configure the System parameters based on the following:

  - Host-name: vBond1
  - Organization: KBITS
  - System-IP: 10.1.1.103
  - Site ID: 100
  - vbond Address: 199.1.1.3 (Local)
  - Timezone: Dubai

Task 2 – Configured the vpn parameters

- Configure the VPN parameters based on the following:

  - vpn 0
    - Interface ge0/0
    - IP Address: 199.1.1.3/28
    - Tunnel Interface
    - Tunnel Services (NetConf, SSHD)
    - Default Route: 199.1.1.14

Task 3 – Add vBond to vManage

- Add the vBond controller to vManage. Use the default username/password combinaton (admin/admin).
- Generate a CSR for vBond at the time of adding vBond to vManage.

Task 4 – Register and Download the vBond Identity Certificate from the CA Server

- Request and Download the Identity Certificate from the Enterprise CA Server.
- Install the vBond Identity Certificate on vManage.

Controller Setup – vSmart

Task 1 – Configuring the System Component

- Configure the System parameters based on the following:

  - Host-name: vSmart1
  - Organization: KBITS
  - System-IP: 10.1.1.102
  - Site ID: 100
  - vbond Address: 199.1.1.2
  - Timezone: Dubai

Task 2 – Configured the vpn parameters

- Configure the VPN parameters based on the following:

  - vpn 0
    - Interface eth0
    - IP Address: 199.1.1.2/28
    - Tunnel Interface
    - Tunnel Services (NetConf, SSHD)
    - Default Route: 199.1.1.14

Task 3 – Add vSmart to vManage

- Add the vSmart controller to vManage. Use the default username/password combinaton (admin/admin).
- Generate a CSR for vSmart at the time of adding vBond to vManage.

Task 4 – Register and Download the vSmart Identity Certificate from the CA Server

- Request and Download the Identity Certificate from the Enterprise CA Server.
- Install the vSmart Identity Certificate on vManage.

Configuration:

vEDGE-HQ-1

Task 1 – Configuring the System Component

- Configure the System parameters based on the following:

  - Host-name: vEdge-HQ-1
  - Organization: KBITS
  - System-IP: 10.2.2.201
  - Site ID: 1
  - vbond Address: 199.1.1.3
  - Timezone: Dubai

Task 2 – Configured the VPN parameters

- Configure the VPN parameters based on the following:

  - vpn 0
    - Interface ge0/0
    - IP Address: 192.168.111.1/24
    - Tunnel Interface
    - Tunnel Services (NetConf, SSHD)
    - Default Route: 192.168.111.254

Task 3 – Upload the Root Certificate to the vEdge-HQ-1

- Use the WINSCP application to transfer the Root Certicate for the Enterprise Server to vEdge-HQ-1 using the following:

  - IP Address: 192.168.111.1
  - Protocol - SFTP
  - Username: admin
  - Password: admin

Task 4 – Install the Root Certificate on vEdge-HQ-1

- Connect to the console of vEdge-HQ-1 and install th Downloaded Root certificate.

Task 5 - Activate vEdge

- Use the 1st vEdge Chassis Number for the WAN-Edge along with the corresponding token to register vEdge-HQ-1 into vManage.

vEDGE-BR-1

Task 1 – Configuring the System Component

- Configure the System parameters based on the following:

  - Host-name: vEdge-BR-1
  - Organization: KBITS
  - System-IP: 10.2.2.211
  - Site ID: 11
  - vbond Address: 199.1.1.3
  - Timezone: Dubai

Task 2 – Configure the VPN parameters

- Configure the VPN parameters based on the following:

  - vpn 0
    - Interface ge0/0
    - IP Address: 192.168.101.11/24
    - Tunnel Interface
    - Tunnel Services (NetConf, SSHD)
    - Default Route: 192.168.101.2

Task 3 – Transfer the Root Certificate to the vEdge-BR-1

- Use the following information to transfer the Enterprise Root Certificate to vEdge-BR-1:

  - IP Address: 192.168.101.11
  - Protocol - SFTP
  - Username: admin
  - Password: admin

Task 4 – Install the Root Certificate on vEdge-BR-1

- Connect to the console of vEdge-BR-1 and install the Downloaded Root certificate.

Task 5 - Activate vEdge

- Use the 2nd vEdge Chassis Number for the WAN-Edge along with the corresponding token to register vEdge-BR-1 into vManage.

vEDGE-BR-2

Task 1 – Configuring the System Component

- Configure the System parameters based on the following:

  - Host-name: vEdge-BR-2
  - Organization: KBITS
  - System-IP: 10.2.2.212
  - Site ID: 12
  - vbond Address: 199.1.1.3
  - Timezone: Dubai

Task 2 – Configure the VPN parameters

- Configure the VPN parameters based on the following:

  - vpn 0
    - Interface ge0/0
    - IP Address: 192.168.102.12/24
    - Tunnel Interface
    - Tunnel Services (NetConf, SSHD)
    - Default Route: 192.168.102.3

Task 3 – Transfer the Root Certificate to the vEdge-BR-2

- Use the following information to transfer the Enterprise Root Certificate to vEdge-BR-2:

  - IP Address: 192.168.102.12
  - Protocol - SFTP
  - Username: admin
  - Password: admin

Task 4 – Install the Root Certificate on vEdge-BR-2

- Connect to the console of vEdge-BR-2 and install the Downloaded Root certificate.

Task 5 - Activate vEdge

- Use the 3rd vEdge Chassis Number for the WAN-Edge along with the corresponding token to register vEdge-BR-2 into vManage.

vEDGE-BR-3

Task 1 – Configuring the System Component

- Configure the System parameters based on the following:

  - Host-name: vEdge-BR-3
  - Organization: KBITS
  - System-IP: 10.2.2.213
  - Site ID: 13
  - vbond Address: 199.1.1.3
  - Timezone: Dubai

Task 2 – Configure the VPN parameters

- Configure the VPN parameters based on the following:

  - vpn 0
    - Interface ge0/0
    - IP Address: 192.168.103.13/24
    - Tunnel Interface
    - Tunnel Services (NetConf, SSHD)
    - Default Route: 192.168.103.4

Task 3 – Transfer the Root Certificate to the vEdge-BR-3

- Use the following information to transfer the Enterprise Root Certificate to vEdge-BR-3:

  - IP Address: 192.168.103.13
  - Protocol - SFTP
  - Username: admin
  - Password: admin

Task 4 – Install the Root Certificate on vEdge-BR-3

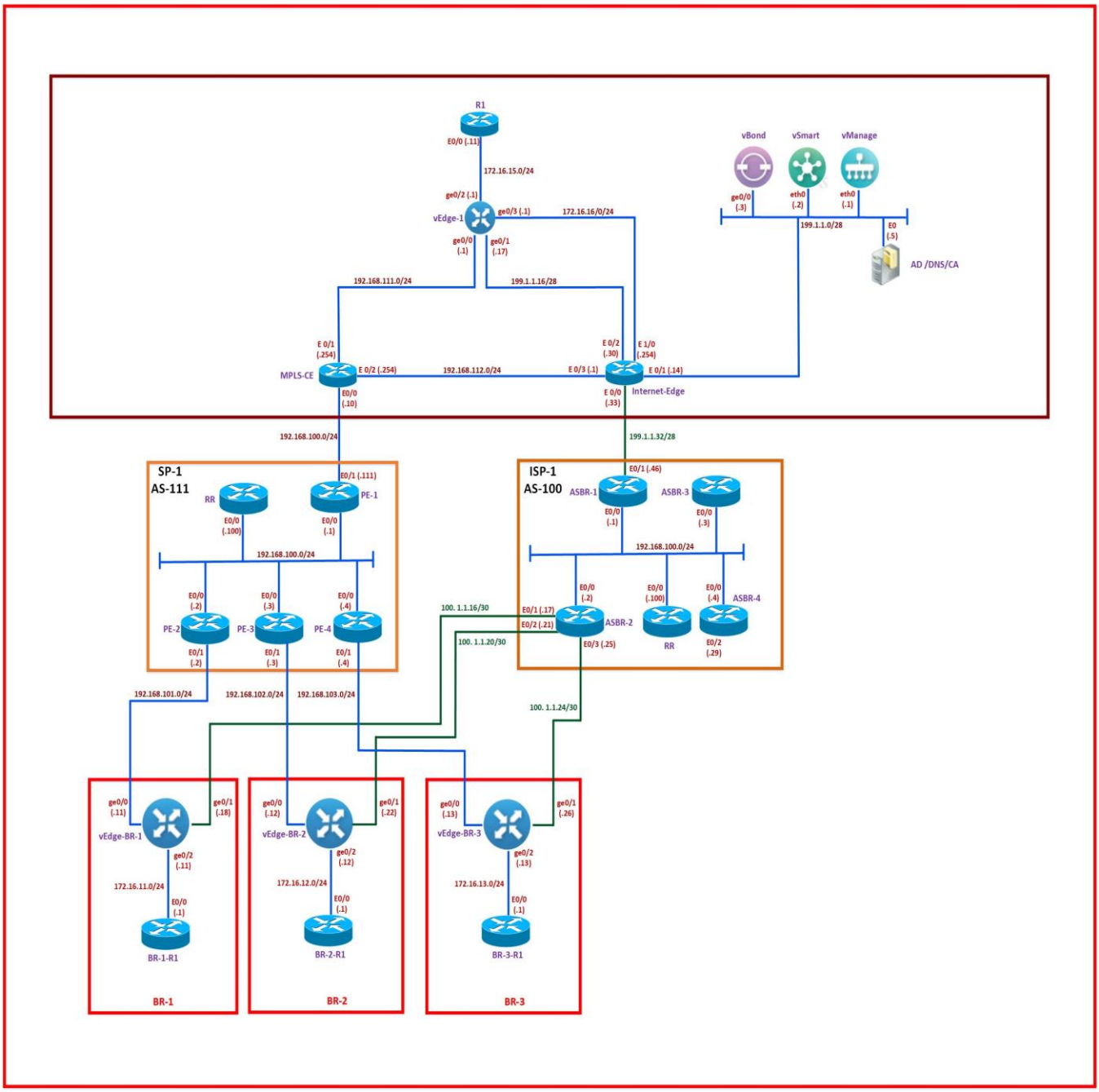
- Connect to the console of vEdge-BR-3 and install the Downloaded Root certificate.

Task 5 - Activate vEdge

- Use the 4th vEdge Chassis Number for the WAN-Edge along with the corresponding token to register vEdge-BR-2 into vManage.

Lab 2 – Configuring the vEdges using Templates

SD-WAN Logical Topology



Template Creation

System

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

- Configure the System parameters based on the following:

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

VPN 0

Task 1 – Configure a VPN Template to be used by all vEdge-Cloud Devices for VPN0

- 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** [**DEF-GW**]

Task 2 – Configure a VPN Interface Template to be used by all vEdge-Cloud Devices for Interface Ge0/0

- Configure the VPN parameters based on the following:

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

  #### Basic Configuration

- Shutdown -> Global: **No**
- Interface Name -> Global: **ge0/0**
- IPv4 Address -> Static -> **Device Specific** [**G0**]

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

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

Task 3 – Configure a VPN Interface Template to be used by all vEdge-Cloud Devices for Interface Ge0/1

- Configure the VPN parameters based on the following:

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

  Basic Configuration
  - Shutdown -> Global: **No**
  - Interface Name -> Global: **ge0/1**
  - IPv4 Address -> Static -> **Device Specific** [**G1**]

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

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

Task 4 – Configure a BGP Template to be used by all vEdge-Cloud Devices for Interface Ge0/0

- Configure the VPN parameters based on the following:

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

  Basic Configuration
  - Shutdown -> Global: **No**
  - AS Number -> **Device Specific**: [**ASN]**

  Neighbor
  - Address -> **Device Specific**: [BGP-PEER]
  - Remote AS -> **Device Specific**: [REMOTE-AS]

VPN512

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

- 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**

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

- Configure the VPN parameters based on the following:

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

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

VPN 10

Task 1 – Configure a VPN Template to be used all vEdge-Cloud Devices for VPN 10

- Configure the VPN parameters based on the following:

  - Template Name: **VE-VPN-VPN10**
  - Description: **VE-VPN-VPN10**

  Basic Configuration
  - VPN -> Global: **10**

Task 2 – Configure a VPN Interface Template to be used all vEdge-Cloud Devices for VPN 10 for Interface Ge0/2

- Configure the VPN parameters based on the following:

  - Template Name: **VE-VPNINT-VPN10-G2**
  - Description: **VE-VPNINT-VPN10-G2**

  Basic Configuration
  - Shutdown -> Global: **No**
  - Interface Name -> Global: **ge0/2**
  - IPv4 Address -> Static -> **Device Specific** [**G2**]

Task 3 – Configure a OSPF Template to be used all vEdge-Cloud Devices for VPN 10

- Configure the OSPF parameters based on the following:

  - Template Name: **VE-OSPF-VPN10**
  - Description: **VE-OSPF-VPN10**

  Redistribution
  - Protocol: **OMP**

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

  Interface Configuration
  - Interface Name: ge0/2

Template Deployment

Task 1 – Configure a Device Template for vEdge Devices.

- 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-VPNINT-VPN0-G0**
  - VPN Interface: **VE-VPNINT-VPN0-G1**
  - BGP: **VE-BGP-VPN0**

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

  Service VPN
  - VPN 10: **VE-VPN-VPN10**
  - VPN Interface: **VE-VPNINT-VPN10-G2**
  - OSPF: **VE-OSPF-VPN10**

Task 2 – Attach vEdge-HQ-1, vEdge-BR-1, vEdge-BR-2 & vEdge-BR3 to the Device Template

- Attach all the vEdges to the Device Template created in the previous task.

Task 3 – Configure the Variable Parameters for the Feature Templates

- All vEdges will appear in the window.
- Configure the Variable parameters based on the following table:

	vEdge-HQ-1	**vEdge-BR-1**	**vEdge-BR-2**	**vEdge-BR-3**
Hostname	vEdge-HQ-1	vEdge-BR-1	vEdge-BR-2	vEdge-BR-3
Sys-ip	10.2.2.201	10.2.2.211	10.2.2.212	10.2.2.213
Site-ID	1	11	12	13
Timezone	Dubai	Los Angeles	London	Rome
Gateway	199.1.1.30	100.1.1.17	100.1.1.21	100.1.1.25
Ge0/0	192.168.111.1/24	192.168.101.11/24	192.168.102.12/24	192.168.103.13/24
Ge0/1	199.1.1.17/28	100.1.1.18/30	100.1.1.22/30	100.1.1.26/30
Ge0/2	172.16.15.1/24	172.16.11.11/24	172.16.12.12/24	172.16.13.13/24
Local AS	65010	65011	65012	65013
Remote AS	65010	111	111	111
Neighbor	192.168.111.254	192.168.101.2	192.168.102.3	192.168.103.4

- Verify that the Devices are successfully configured.

Router Configuration on Internal Routers

Task 1 – Configure the Internal Routers – BR-1

- Configure OSPF on BR-1 Internal Router in Area 0 on all interfaces including the link towards vEdge-BR-1.

Task 2 – Configure the Internal Routers – BR-2

- Configure OSPF on BR-2 Internal Router in Area 0 on all interfaces including the link towards vEdge-BR-2.

Task 3 – Configure the Internal Routers – BR-3

- Configure OSPF on BR-3 Internal Router in Area 0 on all interfaces including the link towards vEdge-BR-3.

CCIE Enterprise Infrastructure – Super Lab

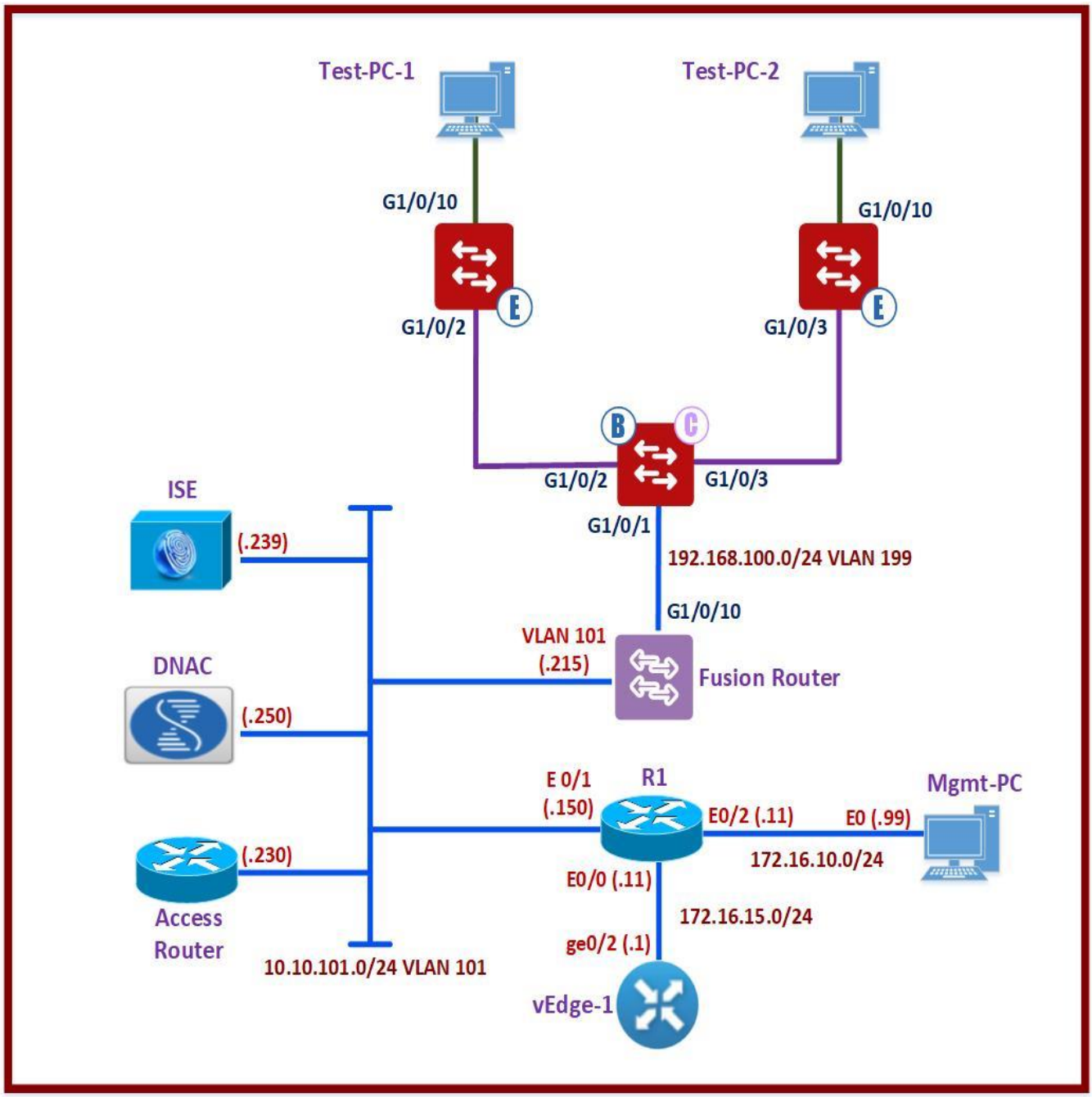
Khawar Butt
CCIE # 12353
Hepta CCIE#12353
CCDE # 20110020

Section 7

Configuring SDA

Lab 1 – Configurig the Border and Fusion Devices

SDA Logical Topology



Pre-Configuration:

DNAC – ISE Integration

- pxGrid Service has been enabled on ISE
  - Administration -> System -> Deployment
- ERS Read/Write settings enabled on ISE
  - Administration -> System -> Settings -> ERS Settings
- DNAC setup with a relationship with ISE
  - System -> System Settings -> Authentication & Policy Servers
    - Server IP Address: 10.10.101.239
    - Shared Secret: Cisco@123
    - Cisco ISE Server: Slide to Enable
    - Username: admin
    - Password: Cisco@123
    - FQDN: dnac-ise.kbits.local
    - Subsriber Name: DNAC-KBITS
- SGTs Migrated over to DNAC on DNAC
  - Policy -> Start Migration

ISE Configuration

- Users & Groups created based on the following:

  - Name: **IT1**
  - Password: **Cisco@123**
  - Group: **IT-DATA-1**

  - Name: **IT2**
  - Password: **Cisco@123**
  - Group: **IT-DATA-2**

  - Name: **SALES1**
  - Password: **Cisco@123**
  - Group: **SALES-DATA-1**

  - Name: **SALES2**
  - Password: **Cisco@123**
  - Group: **SALES-DATA-2**

- Authorization Profile created based on the following:

  - Name: **IT-DATA-1-PROF**
  - VLAN: **IT-DATA-1**

  - Name: **IT-DATA-2-PROF**
  - VLAN: **IT-DATA-2**

  - Name: **SALES-DATA-1-PROF**
  - VLAN: **SALES-DATA-1**

  - Name: **SALES-DATA-2-PROF**
  - VLAN: **SALES-DATA-2**

- Authorization Policy created based on the following:

  - Name: **IT-DATA-1-POLICY**
  - Identity Group: **IT-DATA-1**
  - Authentication Method: **Wired_802.1x**
  - Permission: **IT-DATA-1-PROF**

  - Name: **IT-DATA-2-POLICY**
  - Identity Group: **IT-DATA-2**
  - Authentication Method: **Wired_802.1x**
  - Permission: **IT-DATA-2-PROF**

  - Name: **SALES-DATA-1-POLICY**
  - Identity Group: **SALES-DATA-1**
  - Authentication Method: **Wired_802.1x**
  - Permission: **SALES-DATA-1-PROF**

  - Name: **SALES-DATA-2-POLICY**
  - Identity Group: **SALES-DATA-2**
  - Authentication Method: **Wired_802.1x**
  - Permission: **SALES-DATA-2-PROF**

Configuration:

Fusion Router

Task 1 – Configuring the Fusion Router to communicate to the Border device

- Configure Gig 1/0/10 interface on the Fusion router as a trunk towards the Border Switch.
- Create a VLAN 199 to connect the Fusion Router to the Border Switch.
- Assign it an IP Address of 192.168.100.1/24.

Border Switch

Task 1 – Configuring the Border Switch to communicate to the Fusion Router

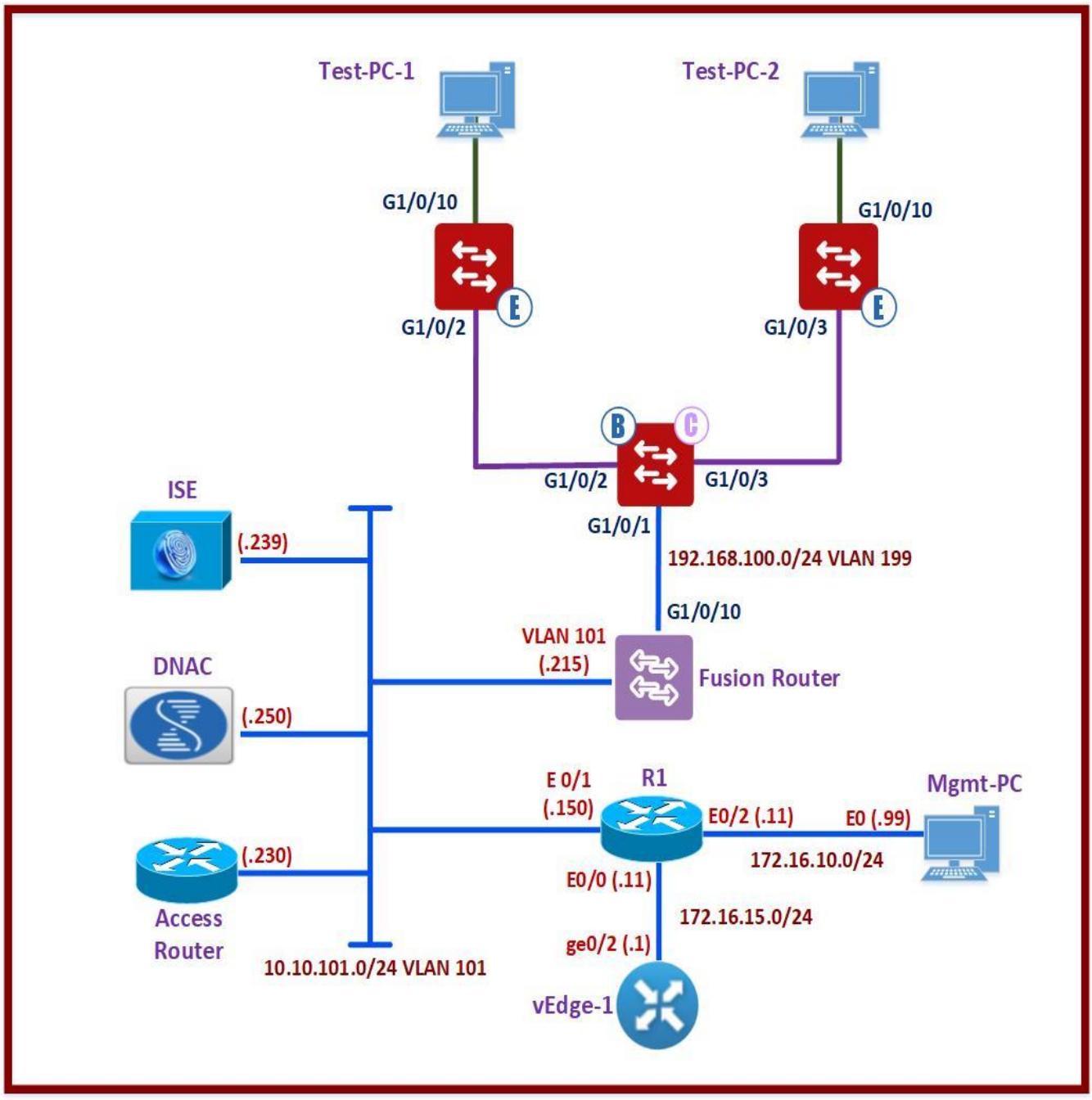
- Configure Gig 1/0/1 interface on the Border Switch as a trunk towards the Fusion Router.
- Create a VLAN 199 to connect the Fusion Router to the Border Switch.
- Assign it an IP Address of 192.168.100.2/24.
- The Border Switch should use the Fusion Router to reach all external networks.

Task 2 – Configure CLI Credentials and SNMP Community Parameters

- Configure the Border Switch with a username of **kbits** with a password of **Cisco@123**. The user should be assigned a privilege level of 15.
- Configure SNMP Read-Only and Read-Write communities to be used for SNMPv2C using the following:
  - Read-Only: public
  - Read-Write: private

Lab 2 – DNAC Design Configuration

SDA Logical Topology



Task 1 – Create an Area and Building based on the following

- Area Name: **Los Angeles**
- Parent: **Global**

- Building Name: **HQ**
- Parent: **Los Angeles**
- Address: **2640 Main Street, Irvine, California 92614, US**

Task 2 – Creating Entries for Network Servers

- Configure the following Network Server Settings under Global:
  - ISE
    - Type: Client/Endpoint
    - Protocol: RADIUS
    - The ISE Server that has been integrated

  - DHCP
    - IP Address: 10.10.101.230

  - DNS
    - IP Address: 10.10.101.230
    - Domain Name: kbits.live

  - NTP Server
    - IP Address: 10.10.101.230

Task 3 – Creating Device Credentials

- Configure the following Device Credentials under Global:
  - CLI Credentials
    - Name: FabricAdmin
    - Username: kbits
    - Password: Cisco@123

  - SNMPv2C – Read-Only
    - Type: SNMP v2C
    - Community Type: Read-only
    - Name: RO
    - Community: public

  - SNMPv2C – Read-Write
    - Type: SNMP v2C
    - Community Type: Read-Write
    - Name: RW
    - Community: private

Task 4 – Creating IP Address Pools

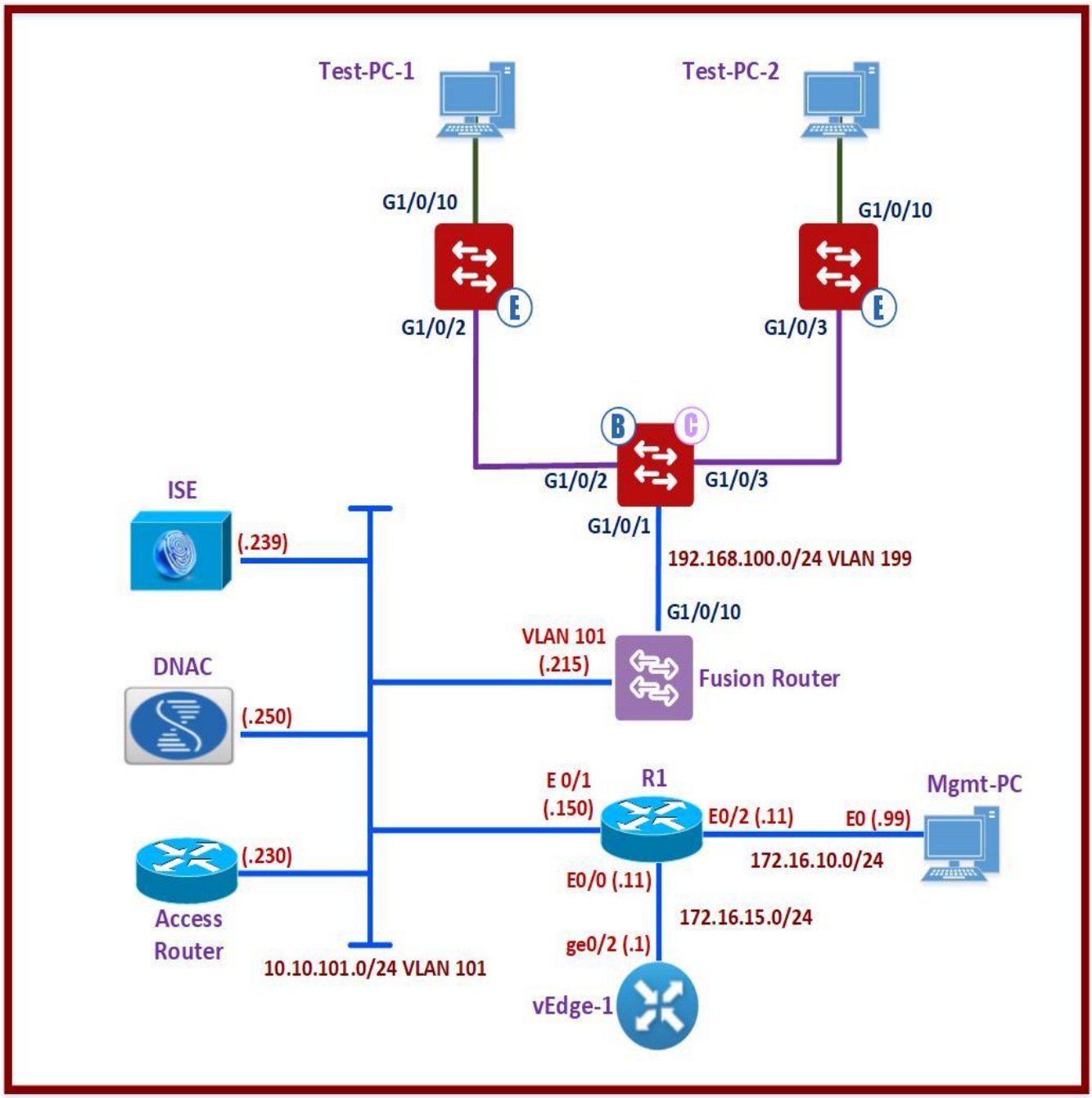
- Configure the following IP Address Pools under Global:

  - Name: LA-OVERLAY-POOL
    - Type: Generic
    - IP Address Space: (IPv4)
    - Subnet: 172.16.0.0
    - Prefix-Length: 16

  - Name: LA-UNDERLAY-POOL
    - Type: Generic
    - IP Address Space: (IPv4)
    - Subnet: 172.20.0.0
    - Prefix-Length: 16

Lab 3 – LAN Automation & Provisioning Devices

SDA Logical Topology



Task 1 – Discover the Border Device

- Discover the Border Device using its IP Address.
- Use the CLI Credentials & SNMP v2C communities created in the previous Labs.
- Assign the Border Device to the HQ Building.

Task 2 – Configure the pre-requisites for LAN Automation

- The HQ LAN Automation should be able to use the CLI Credentials & SNMP Community parameters created in the previous labs.

- The HQ LAN Automation should use the following Pool:

  - Name: LA-LAN-AUTOMATION-POOL
    - Subnet: 172.20.0.0
    - Prefix-Length: 24

- Use Static Routing to provide the Fusion Router with reachability to the LAN Automation Pool

Task 3 – Configure LAN Automation to discover the 9300E1 & 9300E2 nodes

- Configure LAN Automation using the following parameters to on board the 9300 Edge Switches:

  - Primary Site: **Global/Los Angeles/HQ**
  - Primary Device: **9300CB**
  - Selected Ports of Primary Device: **Gig1/0/2 & Gig1/0/3**

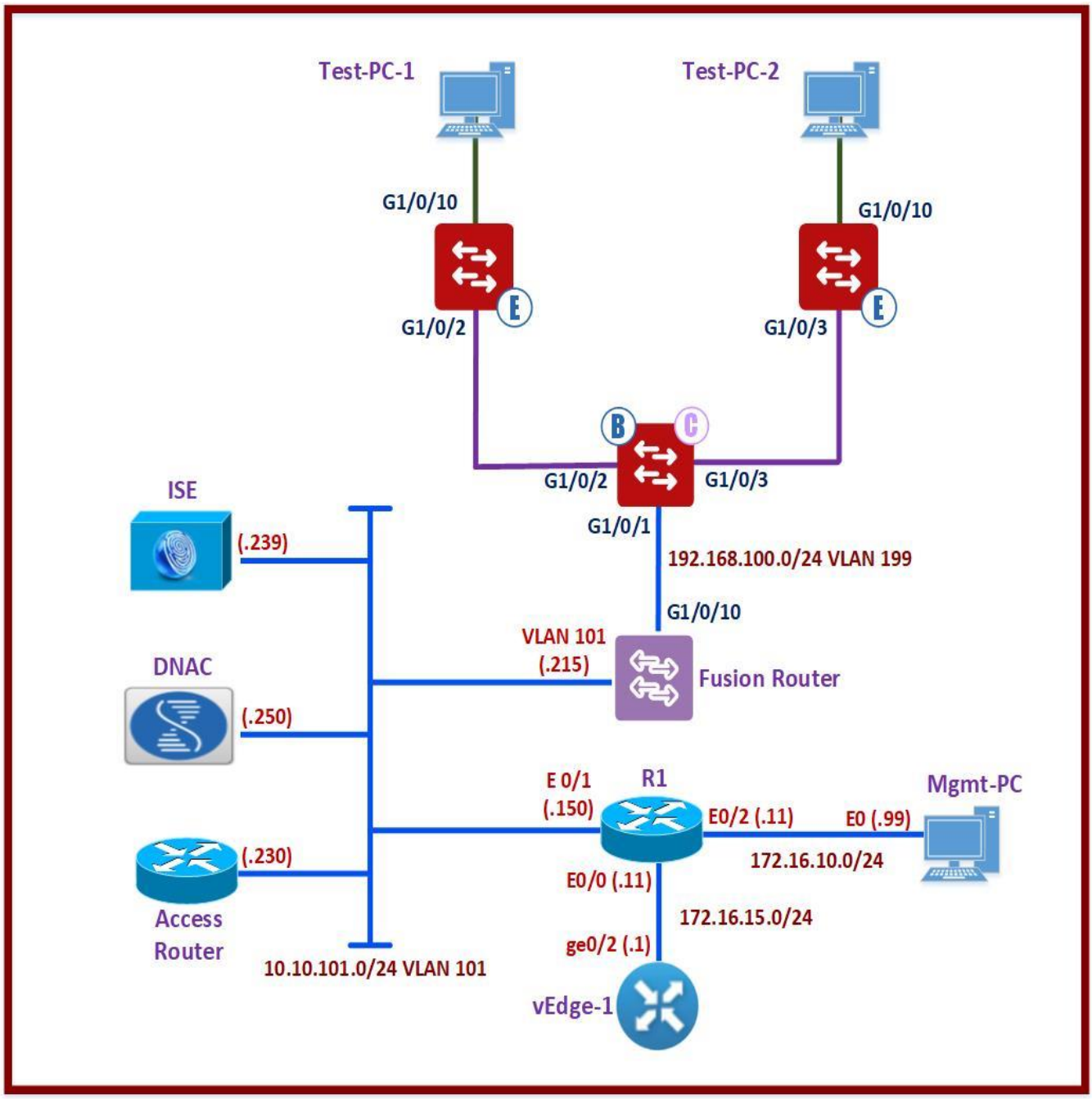
  - Discoverd Device Site: **HQ**
  - IP Pool: **LA-LAN-AUTOMATION-POOL**
  - IS-IS Domain Password: **Cisco@123**
  - Multicast Routing: **Enabled**

Task 4 – Provision all the Switches

- Provision all the switches in the HQ Building.

Lab 4 – Fabric Configuration

SDA Logical Topology



Task 1 – Configure the Pools

- Configure Pools to be used by the End Users based on the following:

  - Name: IT-DATA-1
    - Subnet: 172.16.1.0
    - Prefix-Length: 24
    - Default Gateway: 172.16.1.254
    - DHCP Server: 10.10.101.230

  - Name: IT-DATA-2
    - Subnet: 172.16.2.0
    - Prefix-Length: 24
    - Default Gateway: 172.16.2.254
    - DHCP Server: 10.10.101.230

  - Name: SALES-DATA-1
    - Subnet: 172.16.3.0
    - Prefix-Length: 24
    - Default Gateway: 172.16.3.254
    - DHCP Server: 10.10.101.230

  - Name: SALES-DATA-2
    - Subnet: 172.16.4.0
    - Prefix-Length: 24
    - Default Gateway: 172.16.4.254
    - DHCP Server: 10.10.101.230

- Configure Pools to be used for L3 Handoff based on the following:

  - Name: L3-HANDOFF
    - Subnet: 172.20.1.0
    - Prefix-Length: 24

Task 2 – Creating the VNs

- Create the following 2 VNs:

  - Name: SALES_VN

  - Name: IT_VN

Task 3 – Configure the L3 Handoff Network

- Configure the L3 Handoff Peer Network based on the following:

  - Name: L3HANDOFF
    - Transit Type: IP-Based
    - Protocol: BGP
    - Type: AS-Plain
    - AS #: 65001

Task 4 – Create the HQ Fabric

- Create the HQ Fabric based on the following:

  - Name: HQ_FABRIC
    - VNs: INFRA, SALES_VN & IT_VN

Task 5 – Configure Host Onboarding

- Configure Host Onboarding based on the following:

Authentication Template

- Closed Authentication (Set it as the Default)

Virtual Network – IT_VN

- IP Address Pool: IT-DATA-1
- Authentication Policy: IT-DATA-1
- Type: Data

- IP Address Pool: IT-DATA-2
- Authentication Policy: IT-DATA-2
- Type: Data

Virtual Network – SALES_VN

- IP Address Pool: SALES-DATA-1
- Authentication Policy: SALES-DATA-1
- Type: Data

- IP Address Pool: SALES-DATA-2
- Authentication Policy: SALES-DATA-2
- Type: Data

Task 6 – Configure the Border/Control Node

- Configure the 9300CB device as the Border & Control node based on the following:

Device Role

- Control
- Border

Border L3 Handoff Configuration Parameters:

- BGP AS Type: AS Plain
- Local AS: 65002

- Configure the device to inject all external routes as well as act as the default to all VNs

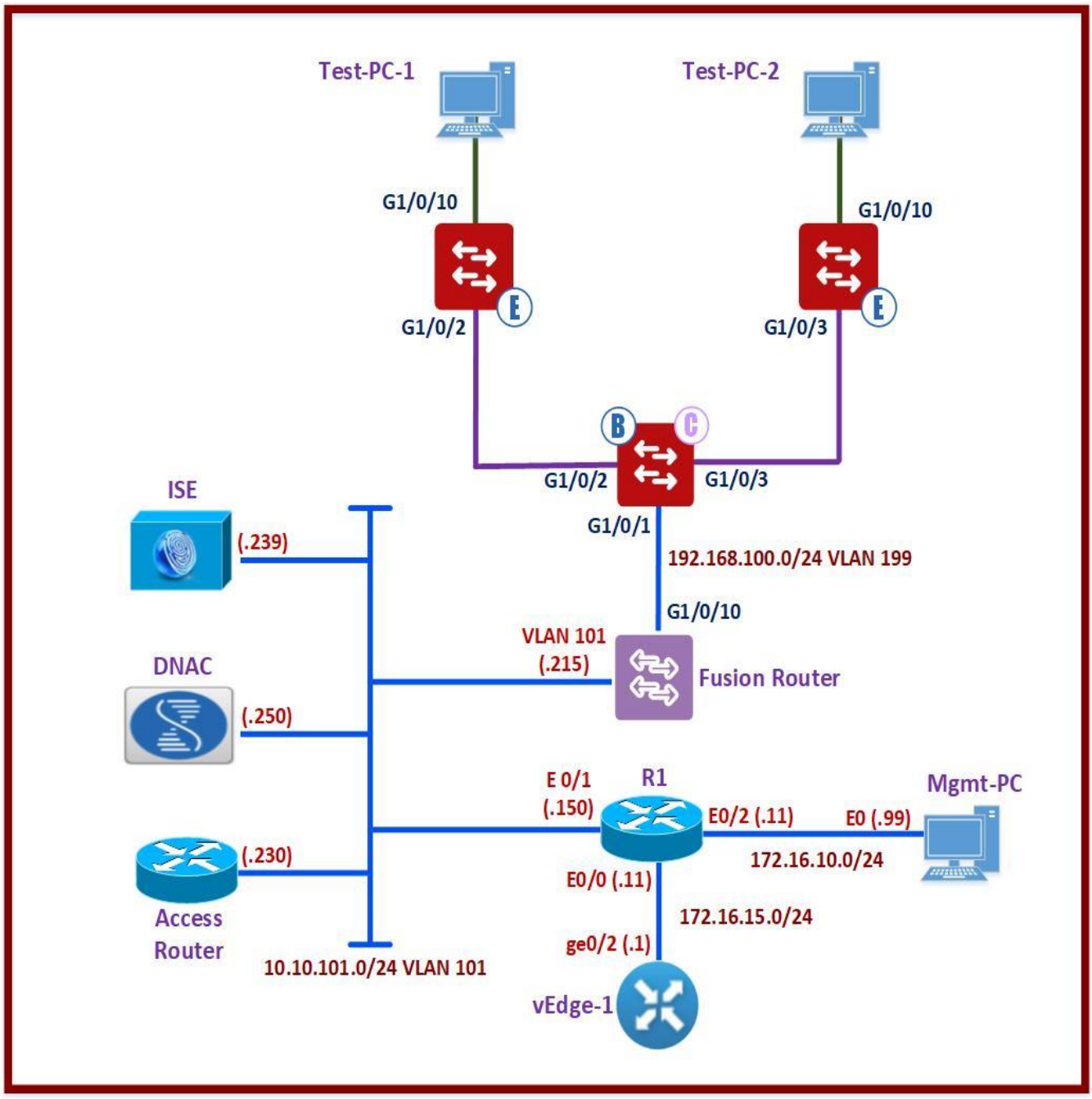
- L3 Handoff Pool: L3-HANDOFF
- External Interface: Gig 1/0/1
- VNs: INFRA, SALES_VN & IT_VN

Task 7 – Configure Edges Nodes

- Configure the 9300E1 & 9300E2 devices as Edge nodes.

Lab 5 – Fusion Router Configuration

SDA Logical Topology



Task 1 – Configure OSPF between R1 and the Fusion Router

- R1 has been configured with OSPF in Area 0.
- Configure the Fusion Router to establish an OSPF relationship with R1.
- These routes will be injected into the Border Switch in a later task.

Task 2 – Configure the VRFs & VLANs on the Fusion Router

- Create the VRFs on the Fusion Router to match the DNAC-Configured Border Switch.
- Create the VLANs on the Fusion Router to match the DNAC-Configured Border Switch.

Task 3 – Configure the SVIs on the Fusion Router

- Create the SVIs on the Fusion Router to match the DNAC-Configured Border Switch.
- Make sure the Border – Fusion is communicating based on the Global routing table and the VRFs.

Task 4 – Configure BGP on the Fusion Router

- Configure BGP on the Fusion Router to match the DNAC-Configured Border Switch.
- The Fusion Router should inject a default route towards the Border Switch in the Global Routing table and the 2 VRFs.

Task 5 – Import Routes from the Global Routing Table to the VRFs

- Import the following routes into the 2 VRFs:
  - Any Route in the 172.16.0.0/24 Major Network.
  - 192.168.100.0/24
  - 192.168.101.0/24
  - 192.168.102.0/24
  - 192.168.103.0/24
  - 192.168.111.0/24
  - 192.168.112.0/24
  - 10.10.101.0/24
- These routes should be injected towards the Border Switch using BGP.

Task 6 – Configuring Static Routes for the VN Data Networks

- Configure Static Routes for the 2 Data networks for each of the 2 VRFs using the appropriate Exit SVI.
- This should provide reachability from the Fusion router to the SDA Fabric Data networks (172.16.1.0/24, 172.16.2.0/24, 172.16.3.0/24 & 172.16.4.0/24).
- R1 should also be able to access these networks. No configuration can be done on R1 for this task.

Task 7 – Configuring the Access Server as a DHCP Server

- Configure the Access Server (10.10.101.230) as a DHCP Server for the SDA Fabric End Host Subnets based on the following:

  - Subnet: 172.16.1.0/24
    - Range: 172.16.1.101 – 172.16.1.253
    - Default Gateway: 172.16.1.254

  - Subnet: 172.16.2.0/24
    - Range: 172.16.2.101 – 172.16.2.253
    - Default Gateway: 172.16.2.254

  - Subnet: 172.16.3.0/24
    - Range: 172.16.3.101 – 172.16.3.253
    - Default Gateway: 172.16.3.254

  - Subnet: 172.16.4.0/24
    - Range: 172.16.4.101 – 172.16.4.253
    - Default Gateway: 172.16.4.254

Task 8 – Verification

- Log into the End Points using the Credentials specified in the Pre-Configurations.
- The SALES_VN & IT_VN users should be able to access the data networks in BR1, BR2 & BR3.

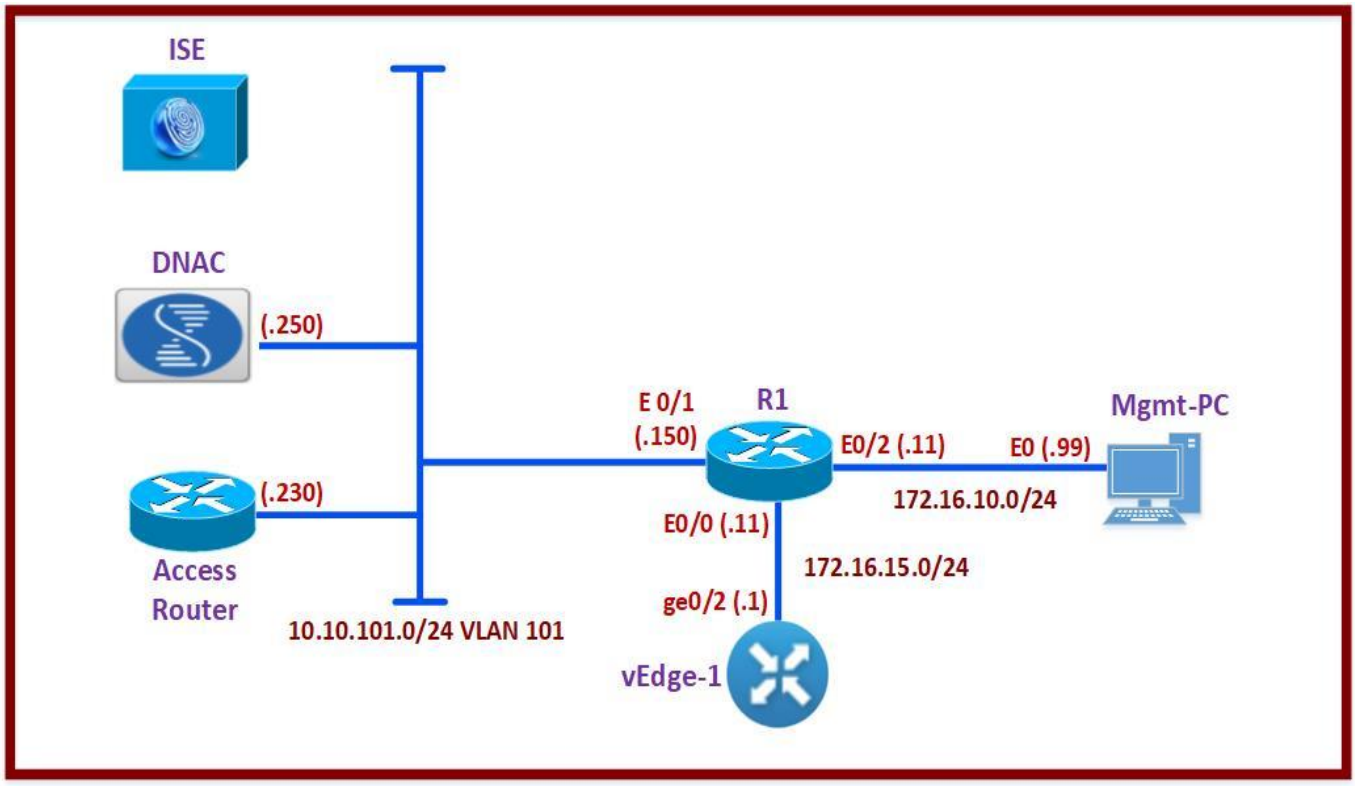
CCIE Enterprise Infrastructure – Super Lab

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

Section 8

Automation

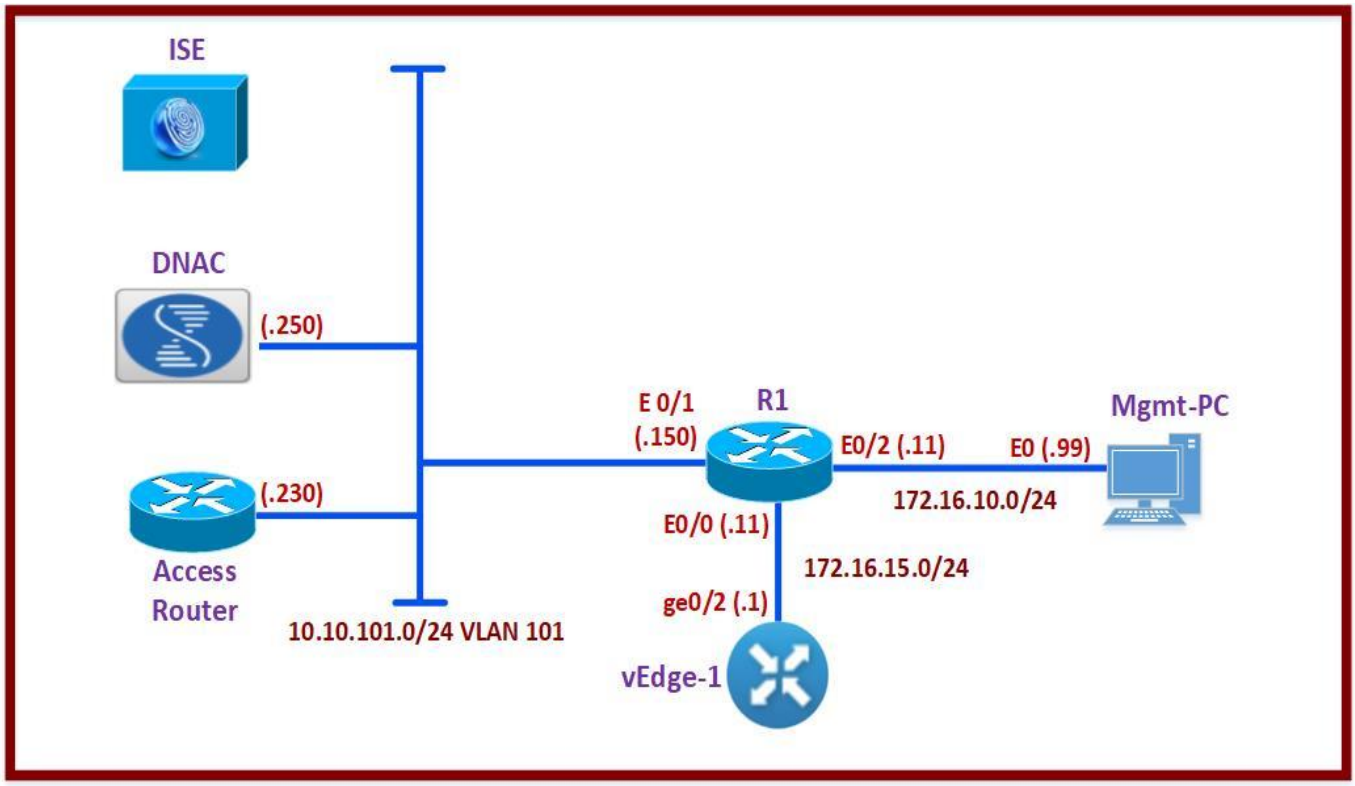
Lab 1 – Displaying the Interface Status of Devices



Task 1 – Configure a Python Script to retrieve the status of interfaces on a specified device

- Use the MGMT-PC to write a Python script to accomplish the following:
  - Prompt the Operator for the IP Address of the device
  - Prompt the Operator for the Username & Password for the device
  - Execute the “Show ip int brief” command.
  - Display the output on the screen.

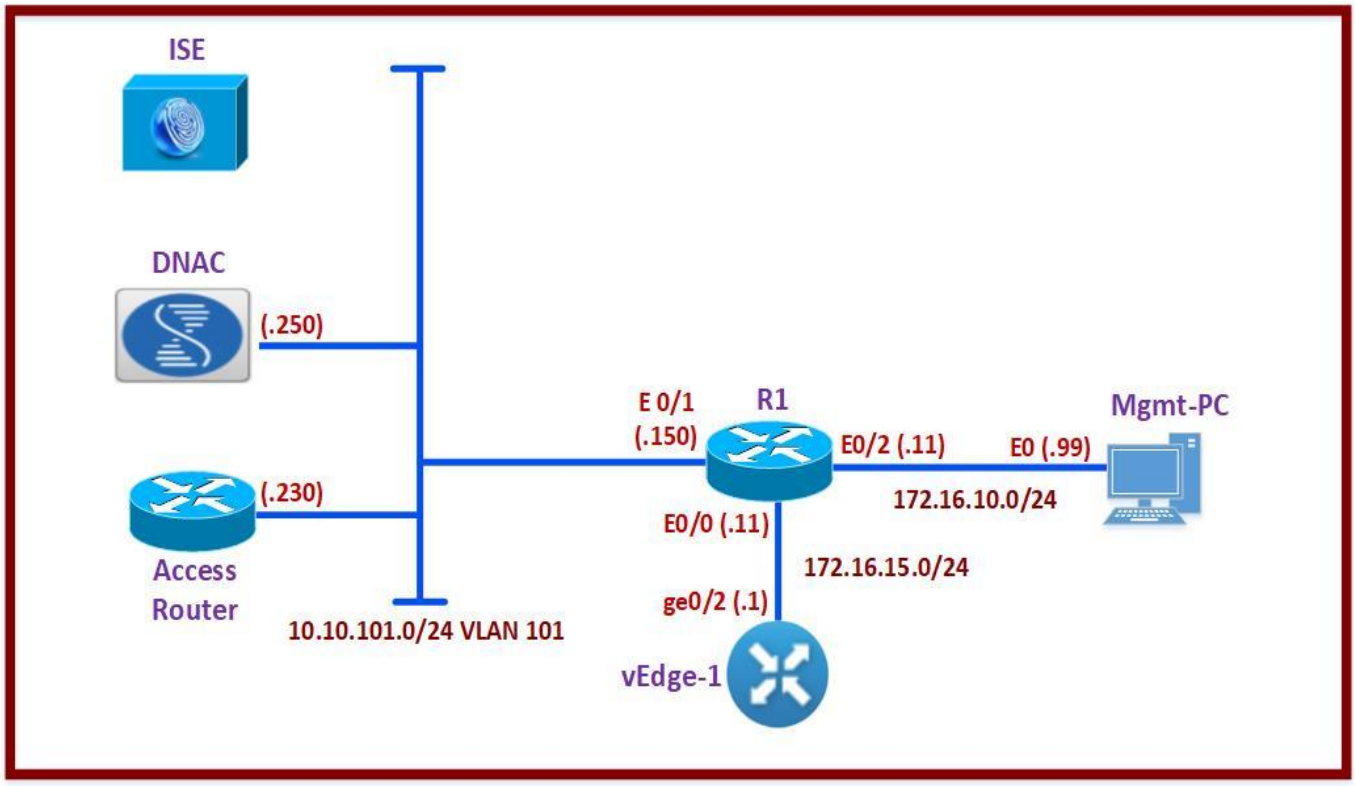
Lab 2 – Backing up the Router Configuration to a File



Task 1 – Configure a Python Script to backup the Running Configuration to a specified File

- Use the MGMT-PC to write a Python script to accomplish the following:
  - Prompt the Operator for the IP Address of the device
  - Prompt the Operator for the Username & Password for the device
  - Backup the Running Configuration to a file based on the following format
    - *<IP Address of the device>*-backup.txt'

Lab 3 – Creating Usernames on Routers



Task 1 – Configure a Python Script to Create Usernames on a specified Device

- Use the MGMT-PC to write a Python script to accomplish the following:
  - Prompt the Operator for the IP Address of the device
  - Prompt the Operator for the Username & Password for the device
  - Prompt the Operation for the # of Users that need to be created.
  - For each user prompt for the username & password.
  - Use a while loop to create the required users. Assign a privilege level of 15 to all users.
  - Print the output of the "show run | include username" command.

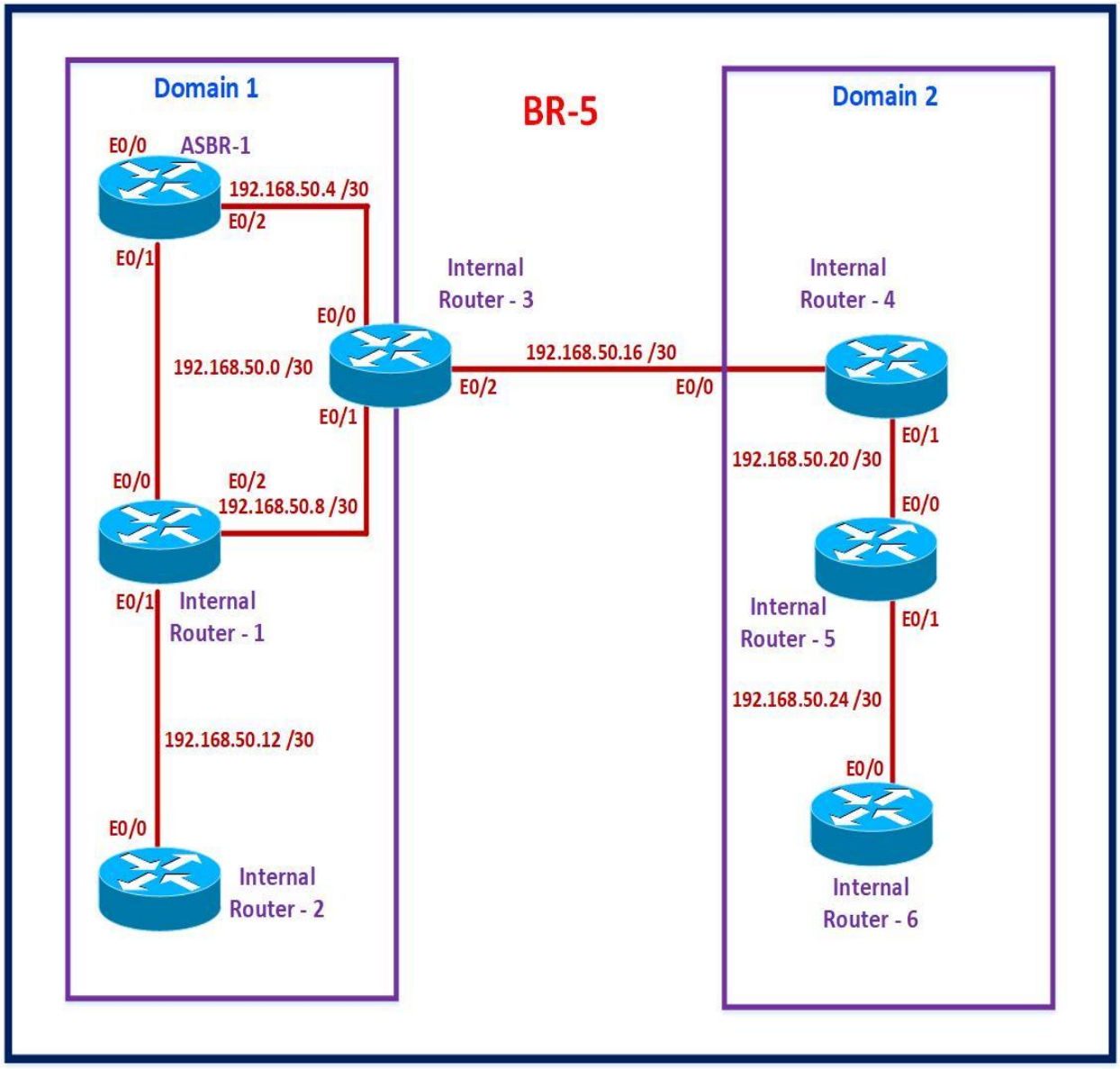
CCIE Enterprise Infrastructure – Super Lab

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

Section 9

Multicast Routing & QoS

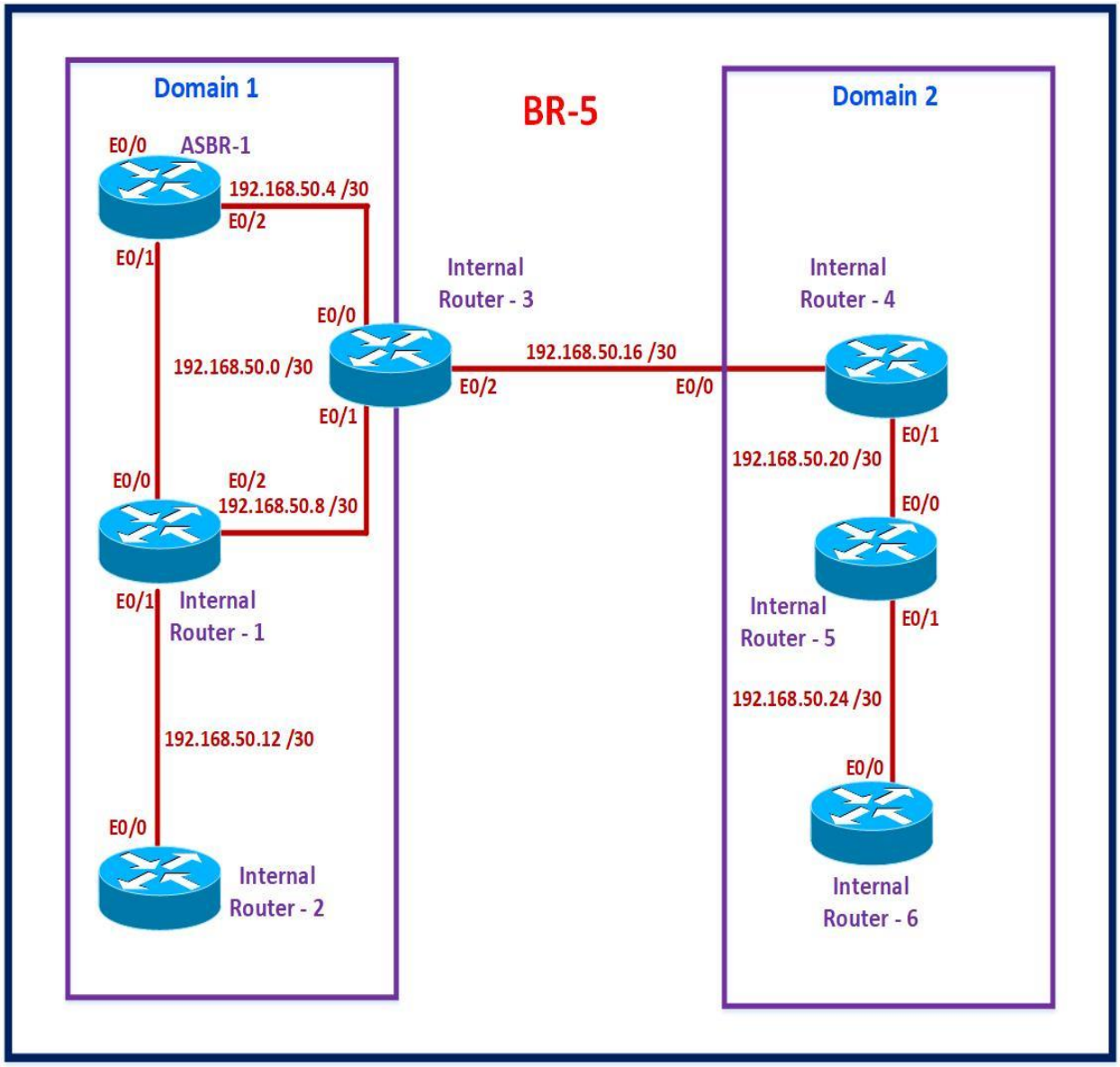
Lab 1 – Multicast-Routing using PIM Sparse-Dense-Mode – Auto RP



Task 1 – Configure Auto-RP for Domain 1

- Configure Internal Router-3 as the RP for Domain 1.
- Internal Router-3 should announce itself as an RP Candidate using a Cisco Proprietary method.
- It should be the RP-Candidate for the following groups only:
  - 225.1.2.3
  - 225.11.22.33
- Configure Internal Router-1 as the Mapping Agent.
- Configure a static join on Loopback 1 interfaces for the following groups:
  - Internal Router-1 – 225.1.2.3, 225.11.22.33 & 225.10.10.10
  - Internal Router-2 – 225.1.2.3, 225.11.22.33 & 225.10.10.10
  - Internal Router-3 – 225.1.2.3 & 225.10.10.10
- Make sure that all multicast groups are working.
- Make sure all routers in Domain 1 are multicast capable.

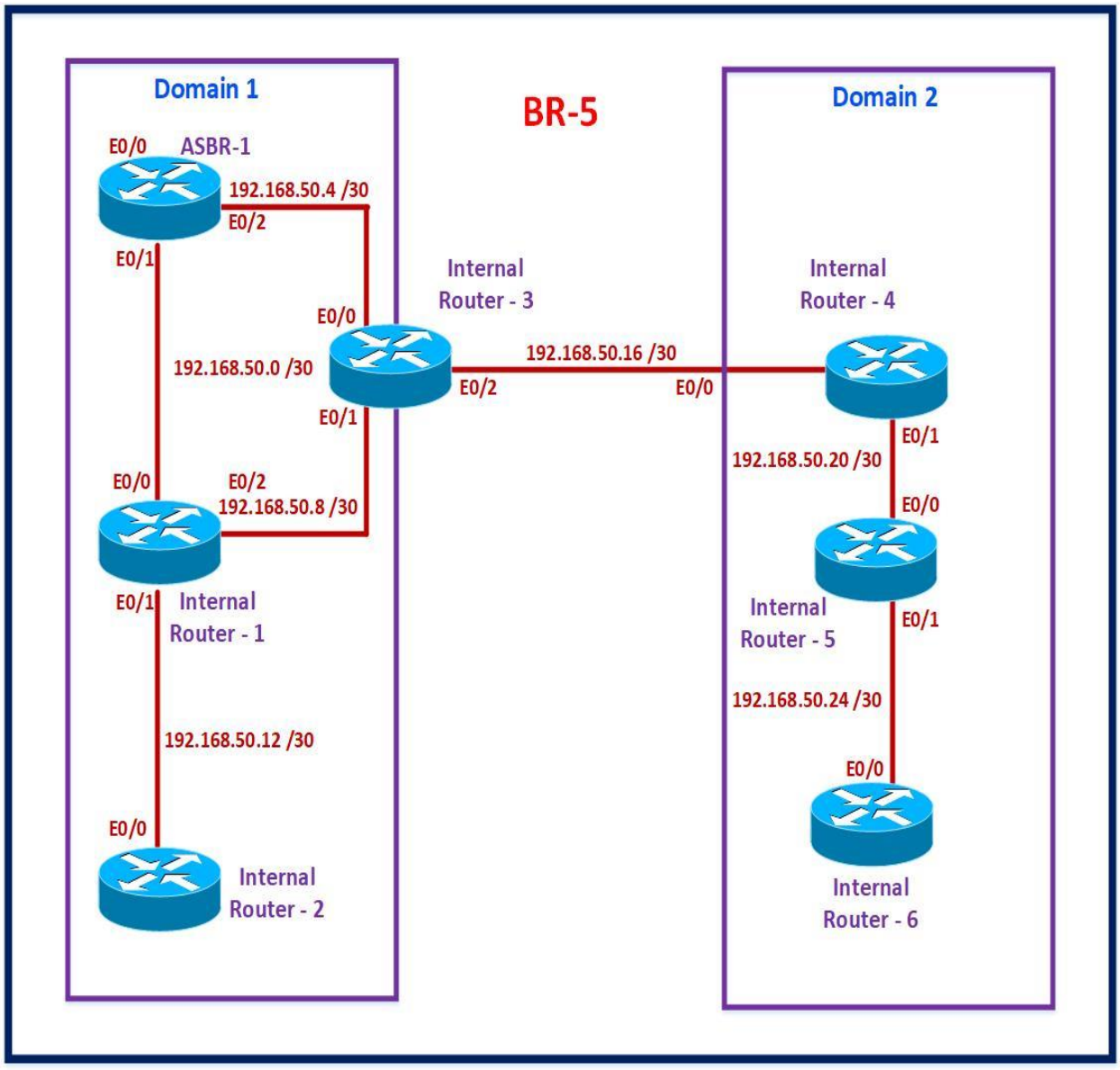
Lab 2 – Multicast-Routing using PIM Sparse-Mode – BSR



Task 1 – Configure BSR for Domain 2

- Configure Internal Router-4 as the RP for Domain 2.
- Internal Router-4 should announce itself as an RP Candidate using an Open Standard method.
- It should be the RP-Candidate for the following groups only:
  - 225.4.5.6
  - 225.44.55.66
  - 225.10.10.10
- Configure Internal Router-5 as the BSR Candidate Router.
- Configure a static join on Loopback 1 interfaces for the following groups:
  - Internal Router-4 – 225.4.5.6, 225.44.55.66 & 225.10.10.10
  - Internal Router-5 – 225.4.5.6, 225.44.55.66 & 225.10.10.10
  - Internal Router-6 – 225.4.5.6 & 225.10.10.10
- Make sure that all multicast groups are working.
- Make sure all routers in Domain 2 are multicast capable.

Lab 3 – Quality of Service (QoS)



Task 1 – Configuring Bandwidth Reservation

- Configure the Link on Internal Router-3 towards Internal Router-4 for Bandwidth Reservation using the following:
  - HTTP and HTTPS traffic = Reserve 30% of the Bandwidth
  - Telnet Traffic = Reserve 10% of the Bandwidth

Task 2 – Configuring Low Latency Queuing (LLQ)

- Configure the Link on Internal Router-3 towards Internal Router-4 for Strict priority using the following:
  - SSH Traffic = Reserve 10% of the Bandwidth with Strict Priority

Task 3 – Configuring Policing

- Configure the Link on Internal Router-4 towards Internal Router-3 for policing using the following:
  - Police HTTP downloading at 100 kbps for *.gif or *.jpg files.
  - This policy should apply to the following networks only:
- 150.1.50.224/28
- 150.1.50.128/28
- 150.1.50.144/28
- 150.1.50.160/28
- 150.1.50.176/28