

# Cisco CCIE EI Lab Dumps Section 2.1-3



Hello, everyone. Last time we have finished talking about CCIE EI lab section 1. What do you think of the difficulty of CCIE EI lab exam? Do you think there are many configuration commands that are difficult to remember? Today, BestCiscoDumps brings you CCIE EI lab section 2. Compared with Section 1, Section 2 does not need to configure so many commands, but more operations on Webpage. Since section 2 contains a lot of content, today we will only talk about section 2.1-2.3.

In Section 2, there are many screenshots of webpage operation, so I have omitted the screenshots of operation for you. Only the text description is retained. If you want to get more complete CCIE EI lab dumps, please contact us online or leave us a message!

Click the link to view the complete [CCIE EI Lab topology](#)

Click the link to view the [CCIE EI Lab Dumps Section 1.1-1.9](#)

Click the link to view the [CCIE EI Lab Dumps Section 1.10-1.16](#)

The current page is CCIE EI Lab Dumps Section 2.1-2.3

Click the link to view the [CCIE EI Lab Dumps Section 2.4-2.6](#)

Click the link to view the [CCIE EI Lab Dumps Section 3.1-3.4](#)

## SECTION 2: Implementing Proof of Concept SDX Branches

### SECTION 2.1: Correcting the IP Address of Managed Switches in DNA Center

After Cisco DNA Center first achieves IP connectivity with the managed switches in Branch #1 & #2, it will place them into Maintenance mode due to their serial number being different from the DNA Center remembers. In addition, their management IP addresses in DNA Center will be automatically changed by appending them with the “dummy.com” string. As a result, after an initial contact, DNA Center will lose connectivity with the switches unless their management IP addresses are corrected in the DNA Center settings.

**Correct the IP addresses of managed switches in the DNA Center according to the following requirements:**

1. Use the host, such as host11 to access the DNA Center GUI website at <https://203.0.113.11> URL
2. Execute the Provision – Devices – Inventory – Global – Actions – Inventory – Resync Device action in DNA Center on all switches before proceeding further.
3. DNA Center API reference and sandbox is available at <https://203.0.113.11/dna/apitester> URL
4. The network-device/update-maintenance-device-ip-address API call description and sandbox are available in the inventory section of the API reference.
5. Use the network-device/update-maintenance-device-ip-address API call to correct the IP addresses of the switches in Branch #1 and #2 appended text

Note: These IP addresses cannot be changed from DNA Center GUI directly because they will become automatically invalidated again. This a built-in DNA Center behavior.

#### Solution

##### On DNAC (GUI access via host11)

## First Step: Changing Management ip address of sw400 via DNAC API Call

1. Navigate > Provision > Devices > Inventory > Global > Actions > Inventory > Resync Device
2. Use this link <https://203.0.113.11/dna/apitester>
3. Select Inventory
4. Select network-device : network-device API
5. Select network-device/update-maintenance-device-ip-address API call
6. In the box input the details as shown in screenshot
7. Click "Try it out!"
8. All Done

## SECTION 2.2: Completing VN Configuration in DNA Center

Using the DNA Center GUI, perform configuration tasks according to these requirements.

1. Add new Virtual Network name IoT for the internet-of-things network on the Branches #1 and #2.
2. Create new addresses pools for the IoT VN named Branch1-ForIoT and Branch2-ForIoT on the global level, and Branch1-IoT Branch1-IoT on the branch level.
3. For Branch #1 IoT VN, allocate the subnet 10.4.198.0/24 and gateway IP address 10.4.198.1
4. For Branch #2 IoT VN, allocate the subnet 10.5.198.0/24 and gateway IP address 10.5.198.1
4. Associate the Branch1-IoT and Branch2-IoT pools with IoT VN on the respective branches.
5. Complete the configuration of the address pools for the Guest VN in the DNA Center so that Branch #1 and Branch #2 can accommodate guest connections, if a new address pool needs to be created and an address range allocated to it, follow the established addressing plan.
6. For all address pools, use the DHCP server 10.2.255.211 to allocate addresses to clients.

On sw211 complete the DHCP server configuration according to these requirements.

1. Create four new DHCP pools for the IoT and Employees VNs on the respective branches.
  - Pool named br1\_iot for Branch #1 IoT VN
  - Pool named br1\_emp for Branch #1 Employees VN

- Pool named br2\_iot for Branch #2 IoT VN
  - Pool named br2\_emp for Branch #2 Employees VN
2. In each subnet, assign addresses from .101 to .254 inclusively, and the appropriate gateway to clients.

## Solution

### On DNAC (GUI access via host11)

#### First Step: Creating Virtual Network IoT

1. Navigate: DNA > Policy > Virtual Network
2. On Left Side Click "Add" Symbol
3. Input the Name as "IoT"
4. Try to find "IoT" in Available Scalable Groups -----> Currently in exam it is not there but if you find it in search than select it
5. Click "Save"

#### Next Step: Creating IP Address Pools for IoT on Global Level

1. Navigate: DNA > Design > Network Setting
2. From the drop-down list on Network Setting: select IP Address Pools
3. Select Global on left side.
4. To add a new ip pool address click "Add"
5. Input the details as
  - IP Pool Name: Branch1-ForIoT
  - Type : Keep it default
  - IP Address Space: Keep it default
  - IP Subnet: 10.4.198.0/24
  - Prefix length: /24 (255.255.255.0)
  - Click "Save"
6. Repeat the steps for adding the next ip address pool in global level
7. Select Global on left side.
8. To add a new ip pool address click "Add"
9. Input the details as
  - IP Pool Name: Branch2-ForIoT
  - Type : Keep it default
  - IP Address Space: Keep it default
  - IP Subnet: 10.5.198.0/24

- Prefix length: /24 (255.255.255.0)
- Click “Save”

10. Done

### Next Step: Creating IP Address Pools for IoT on Branch Level

1. Navigate: DNA > Design > Network Setting
2. From the drop-down list on Network Setting: select IP Address Pools
3. Select Branch1 on left side.
4. To add a new ip pool address click “Reserve”
5. Input the details as
  - IP Pool Name: Branch1-IoT
  - Type : Keep it default
  - IP Address Space: Keep it default
  - IPv4: Select the Global Pool --> 10.4.198.0/24 (Branch1-ForIoT)
  - Prefix length: /24 (255.255.255.0)
  - IP Subnet: 10.4.198.0/24
  - Gateway IP Address: 10.4.198.1
  - DHCP Server: 10.2.255.211
  - Click “Reserve”
6. Repeat the steps for adding the next ip address pool for Branch Level
7. Select Branch2 on left side.
8. To add a new ip pool address click “Reserve”
9. Input the details as
  - IP Pool Name: Branch2-IoT
  - Type : Keep it default
  - IP Address Space: Keep it default
  - IPv4: Select the Global Pool --> 10.5.198.0/24 (Branch2-ForIoT)
  - Prefix length: /24 (255.255.255.0)
  - IP Subnet: 10.5.198.0/24
  - Gateway IP Address: 10.5.198.1
  - DHCP Server: 10.2.255.211
  - Click “Reserve”

10. Done

### Next Step: Associating Branch1 with IoT Virtual Network & IP Pool Address

1. Navigate: DNA > Provision > Branches > Branch 1 > Host Onboarding
2. Click on Virtual Networks
3. Click “Add Virtual Network”
4. Select the box “IoT”
5. Click “Update”

6. Now Select the newly created Virtual Network IoT
7. To associate ip pool address with IoT VN click on “Add”
8. Input the details as
  - IP Address Pool: Select from the drop-down: Branch1-IoT (10.4.198.0/24)
  - Traffic: Select from the drop-down: Data
  - Select the boxes
    - Layer-2 Flooding
9. Click “Add”
10. Click “Save”
11. Done

**Next Step: Creating IP Address Pool for Guest on Branch Level (Only for Branch 2 because on Branch 1 it is already present)**

1. Navigate: DNA > Design > Network Setting
2. From the drop-down list on Network Setting: select IP Address Pools
3. Select Branch2 on left side.
4. To add a new ip pool address click “Reserve”
5. Input the details as
  - IP Pool Name: Branch2-Guest
  - Type : Keep it default
  - IP Address Space: Keep it default
  - IPv4: Select the Global Pool --> 10.5.199.0/24 (Branch2-ForGuest)
  - Prefix length: /24 (255.255.255.0)
  - IP Subnet: 10.5.199.0/24
  - Gateway IP Address: 10.5.199.1
  - DHCP Server: 10.2.255.211
  - Click “Reserve”
6. Done

**Next Step: Associating Branch2 with Guest Virtual Network & IP Pool Address**

1. Navigate: DNA > Provision > Branches > Branch 2 > Host Onboarding
2. Click on Virtual Networks
3. Click “Add Virtual Network”
4. Select the box “Guest”
5. Click “Update”
6. Now Select the newly created Virtual Network Guest
7. To associate ip pool address with Guest VN click on “Add”

8. Input the details as
  - IP Address Pool: Select from the drop-down: Branch2-Guest (10.5.199.0/24)
  - Traffic: Select from the drop-down: Data
  - Select the boxes
    - Layer-2 Flooding
    - Common Pool
9. Click "Add"
10. Click "Save"
11. Done

### **Next Step: Correcting IP Address Pools for Employees**

1. Steps for deleting associated IP Pool from Employees VN
  - a. Navigate: DNA > Provision > Fabric > Branches > Branch 2 > Host Onboarding
  - b. Click on Virtual Networks
  - c. Click on Employees
  - d. Select "Branch2-Employees"
  - e. Click on Action
  - f. Select "Delete"
  - g. This will release the ip pool from VN (if you don't do this step and try to delete directly from the ip address pool you will get error)
2. Steps for deleting IP Pool from Branch2-ForEmployees
  - a. Navigate: DNA > Design > Network Setting
  - b. Select Global
  - c. Find Branch2-ForEmployees
  - d. Click "Delete"
3. Steps for deleting IP Pool from Branch2-Employees
  - a. Navigate: DNA > Design > Network Setting
  - b. Select Branch2
  - c. Find Branch2-Employees
  - d. Click "Delete"

### **Next Step: Creating IP Address Pools for Branch2-ForEmployees on Global Level**

1. Navigate: DNA > Design > Network Setting
2. From the drop-down list on Network Setting: select IP Address Pools
3. Select Global on left side.
4. To add a new ip pool address click "Add"
5. Input the details as

- IP Pool Name: Branch2-ForEmployees
- Type : Keep it default
- IP Address Space: Keep it default
- IP Subnet: 10.5.200.0/24
- Prefix length: /24 (255.255.255.0)
- Click "Save"

6. Done

### **Next Step: Creating IP Address Pools for Branch2-Employees on Branch Level**

1. Navigate: DNA > Design > Network Setting
2. From the drop-down list on Network Setting: select IP Address Pools
3. Select Branch2 on left side.
4. To add a new ip pool address click "Reserve"
5. Input the details as
  - IP Pool Name: Branch2-Employees
  - Type : Keep it default
  - IP Address Space: Keep it default
  - IPv4: Select the Global Pool --> 10.4.198.0/24 (Branch1-ForIoT)
  - Prefix length: /24 (255.255.255.0)
  - IP Subnet: 10.5.200.0/24
  - Gateway IP Address: 10.5.200.1
  - DHCP Server: 10.2.255.211
  - Click "Reserve"

6. Done

### **Next Step: Associating Branch2 with IoT Virtual Network & IP Pool Address**

1. Navigate: DNA > Provision > Branches > Branch 2 > Host Onboarding
2. Click on Virtual Networks
3. Click "Add Virtual Network"
4. Select the box "Employees"
5. To associate ip pool address with Employees VN click on "Add"
6. Input the details as



- IP Address Pool: Select from the drop-down: Branch2-Employees (10.5.200.0/24)
  - Traffic: Select from the drop-down: Data
  - Select the boxes
    - Layer-2 Flooding
7. Click "Add"
  8. Click "Save"
  9. Done

On sw211

```
sw211(config)#ip dhcp pool br1_emp
```

```
sw211(dhcp-config)#network 10.4.200.0 255.255.255.0
```

```
sw211(dhcp-config)#default-router 10.4.200.1
```

```
sw211(dhcp-config)#exit
```

```
sw211(config)#
```

```
sw211(config)#ip dhcp pool br2_emp
```

```
sw211(dhcp-config)#network 10.5.200.0 255.255.255.0
```

```
sw211(dhcp-config)#default-router 10.5.200.1
```

```
sw211(dhcp-config)#exit
```

```
sw211(config)#
```

```
sw211(config)#ip dhcp pool br1_iot
```

```
sw211(dhcp-config)# network 10.4.198.0 255.255.255.0
```

```
sw211(dhcp-config)# default-router 10.4.198.1
```

```
sw211(dhcp-config)#exit
```

```
sw211(config)#
```

```
sw211(config)#ip dhcp pool br2_iot

sw211(dhcp-config)# network 10.5.198.0 255.255.255.0

sw211(dhcp-config)# default-router 10.5.198.1

sw211(dhcp-config)#exit

sw211(config)#

sw211(config)#ip dhcp excluded-address 10.4.198.1 10.4.198.100

sw211(config)#ip dhcp excluded-address 10.4.200.1 10.4.200.100

sw211(config)#ip dhcp excluded-address 10.5.198.1 10.5.198.100

sw211(config)#ip dhcp excluded-address 10.5.200.1 10.5.200.100
```

## SECTION 2.3: Mapping SDA VNs to SD-WAN VPNs

Using vManage GUI, perform configuration tasks according to these requirements.

1. Use any host, such as host11, to access the vManage GUI website at <https://203.0.113.21> URL
2. Create three new SD-WAN VPNs to carry the SDA VN traffic
  - VPN ID 198 for IoT VN
  - VPN ID 199 for Guest VN
  - VPN ID 200 for Employees VN
3. On Branch #1 and Branch #2 vEdges, for each of these VPNs:
  - Create a new subinterface on the interface towards the SDA border switch. Align the VLAN ID and IP address on the subinterface with the configuration generated by DNA Center on the border switches for the appropriate VN.
  - Peer the vEdges and the SDA border switch using iBGP. Ensure reachability between all locations of the same VPN.

### Solution

#### On vManage

#### First Step: Creating vSmart Feature Template – VPN0 Template

1. Navigate: Configuration > Template > Feature
2. Click "Add Template"
3. From the Drop-down list on left side: select vSmart
4. Right side under VPN: select "VPN"
5. Input the Template Name & Description: Name of your choice
6. Under Basic Configuration
  - VPN (Global): Select "VPN0"
7. Under IPv4 Route Configuration
  - Click New IPv4 Route
    - Prefix (Global): 0.0.0.0/0
    - Gateway (Default): "Next Hop"
8. Next Hop: Click on "Add Next Hop"
9. A dialog box will appear, again click on "Add Next Hop"
10. Input the Next Hop ip address: 10.2.251.1
11. Click on "Add"
12. Again Click on "Add"
13. Click "Save"

**Next Step: Creating vSmart Feature Template – VPN0 Interface Template via GUI.**

1. Navigate: Configuration > Template > Feature
2. Click "Add Template"
3. From the Drop-down list on left side: select vSmart
4. Right side under VPN: select "VPN Interface Ethernet"
5. Input the Template Name & Description: Name of your choice
6. Under Basic Configuration
  - Shutdown (Global): Select "No"
  - Interface Name (Global): eth1
  - IP address (Global): 10.2.251.11/24
7. Under Tunnel Configuration
  - Tunnel Interface (Global): Select "On"
8. Click "Save"

**Next Step: Creating vSmart Device Template from Feature Templates via GUI.**

1. Navigate: Configuration > Template > Device
2. Click "Create Template"
3. Select "From Feature Template"
4. Details:
  - Device Model: vSmart
  - Template Name: Name of your choice
  - Description: Name of your choice

5. Click Transport & Management VPN
  - VPN0: Select “vSmart-VPN0”
  - Add the vpn interface by clicking “VPN Interface” on right side
  - VPN Interface: Select “vSmart-Interface”
6. Click “Create”
7. A Device Template is now created
8. Click on the three dots on right side and click “Attach Device”
9. A Windows will appear: Select the “vSmart” and click on the “Right Arrow”
10. Click “Attach”
11. Click on the three dots on right side and click “Edit Device Template”
12. Input the proper values and click “Update”
13. Click “Next”
14. Click “Configure Devices”
15. All Done

### **Next Step: Creating Feature Template - VPN’s Template for IoT & Guest & Employees**

#### **For VPN198**

1. Navigate: Configuration > Template > Feature
2. Click “Add Template”
3. From the Drop-down list on left side: select vEdge Cloud
4. Right side under VPN: select “VPN”
5. Input the Template Name & Description: You can use any name of your choice
6. Under Basic Configuration
  - VPN (Global): Input “198”
7. Click “Save”

#### **For VPN199**

1. Navigate: Configuration > Template > Feature
2. Click “Add Template”
3. From the Drop-down list on left side: select vEdge Cloud
4. Right side under VPN: select “VPN”
5. Input the Template Name & Description: You can use any name of your choice
6. Under Basic Configuration
  - VPN (Global): Input “199”
7. Click “Save”

#### **For VPN200**

1. Navigate: Configuration > Template > Feature
2. Click "Add Template"
3. From the Drop-down list on left side: select vEdge Cloud
4. Right side under VPN: select "VPN"
5. Input the Template Name & Description: You can use any name of your choice
6. Under Basic Configuration
  - VPN (Global): Input "200"
7. Click "Save"

### **Next Step: Creating Feature Template – VPN Interface for Branch 1 vEdge40: IoT & Guest & Employees**

#### **For VPN198 Interface**

1. Navigate: Configuration > Template > Feature
2. Click "Add Template"
3. From the Drop-down list on left side: select vEdge Cloud
4. Right side under VPN: select "VPN Interface"
5. Input the Template Name & Description: You can use any name of your choice
6. Under Basic Configuration
  - Shutdown (Global): Select "No"
  - Interface Name (Global): Input "ge0/2.3001"
  - Ipv4 Address: 10.4.254.2
7. Click "Save"

#### **For VPN199 Interface**

1. Navigate: Configuration > Template > Feature
2. Click "Add Template"
3. From the Drop-down list on left side: select vEdge Cloud
4. Right side under VPN: select "VPN Interface"
5. Input the Template Name & Description: You can use any name of your choice
6. Under Basic Configuration
  - Shutdown (Global): Select "No"
  - Interface Name (Global): Input "ge0/2.3004"
  - Ipv4 Address: 10.4.254.6
7. Click "Save"

#### **For VPN200 Interface**

1. Navigate: Configuration > Template > Feature

2. Click "Add Template"
3. From the Drop-down list on left side: select vEdge Cloud
4. Right side under VPN: select "VPN Interface"
5. Input the Template Name & Description: You can use any name of your choice
6. Under Basic Configuration
  - Shutdown (Global): Select "No"
  - Interface Name (Global): Input "ge0/2.3007"
  - Ipv4 Address: 10.4.254.10
7. Click "Save"

### Next Step: Creating Feature Template – VPN Interface for Branch 2 vEdge51: IoT & Guest & Employees

#### For VPN198 Interface

1. Navigate: Configuration > Template > Feature
2. Click "Add Template"
3. From the Drop-down list on left side: select vEdge Cloud
4. Right side under VPN: select "VPN Interface"
5. Input the Template Name & Description: You can use any name of your choice
6. Under Basic Configuration
  - Shutdown (Global): Select "No"
  - Interface Name (Global): Input "ge0/3.3003"
  - Ipv4 Address: 10.5.254.6
7. Click "Save"

#### For VPN199 Interface

1. Navigate: Configuration > Template > Feature
2. Click "Add Template"
3. From the Drop-down list on left side: select vEdge Cloud
4. Right side under VPN: select "VPN Interface"
5. Input the Template Name & Description: You can use any name of your choice
6. Under Basic Configuration
  - Shutdown (Global): Select "No"
  - Interface Name (Global): Input "ge0/3.3006"
  - Ipv4 Address: 10.4.254.14
7. Click "Save"

#### For VPN200 Interface

1. Navigate: Configuration > Template > Feature
2. Click "Add Template"
3. From the Drop-down list on left side: select vEdge Cloud
4. Right side under VPN: select "VPN Interface"
5. Input the Template Name & Description: You can use any name of your choice
6. Under Basic Configuration
  - Shutdown (Global): Select "No"
  - Interface Name (Global): Input "ge0/3.3009"
  - Ipv4 Address: 10.4.254.22
7. Click "Save"

### **Next Step: Creating Feature Template – VPN Interface for Branch 2 vEdge52: IoT & Guest & Employees**

#### **For VPN198 Interface**

1. Navigate: Configuration > Template > Feature
2. Click "Add Template"
3. From the Drop-down list on left side: select vEdge Cloud
4. Right side under VPN: select "VPN Interface"
5. Input the Template Name & Description: You can use any name of your choice
6. Under Basic Configuration
  - Shutdown (Global): Select "No"
  - Interface Name (Global): Input "ge0/3.3002"
  - Ipv4 Address: 10.5.254.2
7. Click "Save"

#### **For VPN199 Interface**

1. Navigate: Configuration > Template > Feature
2. Click "Add Template"
3. From the Drop-down list on left side: select vEdge Cloud
4. Right side under VPN: select "VPN Interface"
5. Input the Template Name & Description: You can use any name of your choice
6. Under Basic Configuration
  - Shutdown (Global): Select "No"
  - Interface Name (Global): Input "ge0/3.3005"
  - Ipv4 Address: 10.4.254.10
7. Click "Save"

#### **For VPN200 Interface**

1. Navigate: Configuration > Template > Feature
2. Click "Add Template"
3. From the Drop-down list on left side: select vEdge Cloud
4. Right side under VPN: select "VPN Interface"
5. Input the Template Name & Description: You can use any name of your choice
6. Under Basic Configuration
  - Shutdown (Global): Select "No"
  - Interface Name (Global): Input "ge0/3.3008"
  - Ipv4 Address: 10.4.254.18
7. Click "Save"

### **Next Step: Creating Feature Template – BGP for: IoT & Guest & Employees**

#### **For VPN198 BGP-IoT**

1. Navigate: Configuration > Template > Feature
2. Click "Add Template"
3. From the Drop-down list on left side: select vEdge Cloud
4. Right side under Other Templates: select "BGP"
5. Input the Template Name & Description: You can use any name of your choice
6. Under Basic Configuration
  - AS Number (Device Specific): You can use any name of your choice
7. Under Unicast Address Family
  - Select: New-Redistribute
  - Select: (Global) "omp"
  - Add/Save Changes
8. Under Neighbor
  - Click "New Neighbor"
  - Address (Device Specific): You can use any name of your choice
  - Click Advanced Option
  - Source Interface Address (Device Specific): You can use any name of your choice
9. Click "Add"
10. Click "Save"

#### **For VPN199 BGP-Guest**

1. Navigate: Configuration > Template > Feature
2. Click "Add Template"
3. From the Drop-down list on left side: select vEdge Cloud
4. Right side under Other Templates: select "BGP"



5. Input the Template Name & Description: You can use any name of your choice
6. Under Basic Configuration
  - AS Number (Device Specific): You can use any name of your choice
7. Under Unicast Address Family
  - Select: New-Redistribute
  - Select: (Global) "omp"
  - Add/Save Changes
8. Under Neighbor
  - Click "New Neighbor"
  - Address (Device Specific): You can use any name of your choice
  - Click Advanced Option
  - Source Interface Address (Device Specific): You can use any name of your choice
9. Click "Add"
10. Click "Save"

### **For VPN200 BGP-Employees**

1. Navigate: Configuration > Template > Feature
2. Click "Add Template"
3. From the Drop-down list on left side: select vEdge Cloud
4. Right side under Other Templates: select "BGP"
5. Input the Template Name & Description: You can use any name of your choice
6. Under Basic Configuration
  - AS Number (Device Specific): You can use any name of your choice
7. Under Unicast Address Family
  - Select: New-Redistribute
  - Select: (Global) "omp"
  - Add/Save Changes
8. Under Neighbor
  - Click "New Neighbor"
  - Address (Device Specific): You can use any name of your choice
  - Click Advanced Option
  - Source Interface Address (Device Specific): You can use any name of your choice
9. Click "Add"
10. Click "Save"

### **Next Step: Creating Feature Template – OMP Template**

1. Navigate: Configuration > Template > Feature
2. Click "Add Template"

3. From the Drop-down list on left side: select vEdge Cloud
4. Right side under Other Templates: select "OMP"
5. Input the Template Name & Description: You can use any name of your choice
6. Under advertise: ipv4
  - Select: (Global) BGP : "On"
  - Keep all rest as default
7. Under advertise: ipv6
  - Select all: (Global): "Off"
  - (switch off all services for ipv6 or else you will get error)
8. Click "Save"

### **Next Step: Creating Device Template From Feature Template – Branch1 vedge40**

1. Navigate: Configuration > Template > Device
2. Select Branch1\_vedges
3. Click on the three dots on the right side corner to edit the template
4. Under Basic Information
  - Select: OMP Feature Template
5. Under Service VPN: Click on "Add Symbol"
6. To Add BGP and VPN Interface: Click on the right side on BGP and VPN Interface
  - VPN: Employees-VN --->Select the template name which you have given
  - BGP: Employees-IBP-VPN-200 --->Select the template name which you have given
  - VPN Interface: Branch1\_ge0/2.3001 ---> Select the template name which you have given
7. Under Service VPN: Click on "Add Symbol"
8. To Add BGP and VPN Interface: Click on the right side on BGP and VPN Interface
  - VPN: Guest-VN --->Select the template name which you have given
  - BGP: Guest-IBP-VPN-199 --->Select the template name which you have given
  - VPN Interface: Branch1\_ge0/2.3004 ---> Select the template name which you have given
9. Under Service VPN: Click on "Add Symbol"
10. To Add BGP and VPN Interface: Click on the right side on BGP and VPN Interface
  - VPN: IoT-VN --->Select the template name which you have given
  - BGP: IoT-IBP-VPN-198 --->Select the template name which you have given

- VPN Interface: Branch1\_ge0/2.3007 ---> Select the template name which you have given
11. Click "Update"
  12. A Device Template is now updated (but not yet attached)
  13. Select the updated device template and click on the three dots on right side and click "Edit Device Template"
  14. Input the proper values as given in the screenshots and click "Update"
  15. Click "Next"
  16. Click "Configure Devices"
  17. A dialog box will appear: Select "Confirm" and click "OK" ---> May be Optional
  18. All Done

### **Next Step: Creating Device Template From Feature Template – Breaking Branch2\_vedges Single Template into Two templates**

1. Navigate: Configuration > Template > Device
2. Select Branch2\_vedges
3. Click on the three dots on the right side corner to copy the template
4. Name the copied device template as : Branch2\_vedges\_51
5. And Now again Select Branch2\_vedges
6. Click on the three dots on the right side corner to Delete the template
7. Select Branch2\_vedges\_51
8. Click on the three dots on the right side corner to copy the template
9. Name the copied device template as : Branch2\_vedges\_52
10. Now you have separate device templates for Branch2\_vedge51 & Branch\_vedge52

### **Next Step: Creating Device Template From Feature Template – Branch2 vedge51**

1. Navigate: Configuration > Template > Device
2. Select Branch2\_vedges\_51
3. Click on the three dots on the right side corner to edit the template
4. Under Basic Information
  - Select: OMP Feature Template
5. Under Service VPN: Click on "Add Symbol"
6. To Add BGP and VPN Interface: Click on the right side on BGP and VPN Interface
  - VPN: Employees-VN ---> Select the template name which you have given
  - BGP: Employees-IBP-VPN-200 ---> Select the template name which you have given

- VPN Interface: Branch1\_ge0/3.3003 ---> Select the template name which you have given
7. Under Service VPN: Click on “Add Symbol”
  8. To Add BGP and VPN Interface: Click on the right side on BGP and VPN Interface
    - VPN: Guest-VN --->Select the template name which you have given
    - BGP: Guest-IBP-VPN-199 --->Select the template name which you have given
    - VPN Interface: Branch1\_ge0/3.3006 ---> Select the template name which you have given
  9. Under Service VPN: Click on “Add Symbol”
  10. To Add BGP and VPN Interface: Click on the right side on BGP and VPN Interface
    - VPN: IoT-VN --->Select the template name which you have given
    - BGP: IoT-IBP-VPN-198 --->Select the template name which you have given
    - VPN Interface: Branch1\_ge0/3.3009 ---> Select the template name which you have given
  11. Click “Update”
  12. A Device Template is now updated (but not yet attached)
  13. Select the updated device template and click on the three dots on right side and click “Attach Device”
  14. Input the proper values as given in the screenshots and click “Update”
  15. Click “Next”
  16. Click “Configure Devices”
  17. A dialog box will appear: Select “Confirm” and click “OK” ---> May be Optional
  18. All Done

### **Next Step: Creating Device Template From Feature Template – Branch2 vedge52**

1. Navigate: Configuration > Template > Device
2. Select Branch2\_vedges\_52
3. Click on the three dots on the right side corner to edit the template
4. Under Basic Information
  - Select: OMP Feature Template
5. Under Service VPN: Click on “Add Symbol”
6. To Add BGP and VPN Interface: Click on the right side on BGP and VPN Interface
  - VPN: Employees-VN --->Select the template name which you have given
  - BGP: Employees-IBP-VPN-200 --->Select the template name which you have given

- VPN Interface: Branch1\_ge0/3.3002 ---> Select the template name which you have given
7. Under Service VPN: Click on “Add Symbol”
  8. To Add BGP and VPN Interface: Click on the right side on BGP and VPN Interface
    - VPN: Guest-VN --->Select the template name which you have given
    - BGP: Guest-IBP-VPN-199 --->Select the template name which you have given
    - VPN Interface: Branch1\_ge0/3.3005 ---> Select the template name which you have given
  9. Under Service VPN: Click on “Add Symbol”
  10. To Add BGP and VPN Interface: Click on the right side on BGP and VPN Interface
    - VPN: IoT-VN --->Select the template name which you have given
    - BGP: IoT-IBP-VPN-198 --->Select the template name which you have given
    - VPN Interface: Branch1\_ge0/3.3008 ---> Select the template name which you have given
  11. Click “Update”
  12. A Device Template is now updated (but not yet attached)
  13. Select the updated device template and click on the three dots on right side and click “Attach Device”
  14. Input the proper values as given in the screenshots and click “Update”
  15. Click “Next”
  16. Click “Configure Devices”
  17. A dialog box will appear: Select “Confirm” and click “OK” ---> May be Optional
  18. All Done

The above is about section 2.1-2.3 in CCIE EI lab dumps. If you want to get the follow-up part in CCIE EI lab dumps, please always pay attention to our website, because [BestCiscoDumps](https://www.bestciscodumps.com/) will share the follow-up part and more benefits that are helpful to Cisco candidates from time to time!

If you want to get more verification about the questions and a more complete [CCIE EI lab dumps](https://www.bestciscodumps.com/), please contact us!