PASS ENTERPRISE LABS

CCIE Enterprise Infrastructure v1.0 Real Labs

Deploy Module

Lab Workbook Policy

1. We highly discourage sharing of the workbook hence the workbooks are mapped to Laptop/Desktop MAC address. If one tries to open the workbook on other desktop or laptop than the registered MAC address; account will get locked and we will not unlock it for any reasons.

2. The workbook does not have print access; kindly do not request to enable to print access. However you will have perpetual access to the workbook which you have purchased.

3. One will be provided with free updates up to 120 days from the date of purchase, post that one need to renew his/her account to access the latest update. However one will continue to have access to their existing workbooks. If you pass the lab within 120 days, you are not eligible for further updates.

4. If one wish to renew their subscription/account, you need to renew within 120 days or before the account gets expired. Post 120 days one can renew their account however the renewal will be considered has a new purchase. Hence we encourage one to renew within 120 days of the purchase.

5. The renewal cost is 999 USD if one pay within 120 days, if one fail to renew then the cost will be equivalent of a new purchase. (The renewal price can be changed at any time, without informing the client)

6. Every workbook is uniquely identified for each user with hidden words. If one shares his/her workbooks with others, and if the system detects the share, the account will be banned and we will not entertain any explanation of any sort.

7. For any queries regarding Questions/Solutions, you can contact us on email: support@chinesedumps.com or skype @ chinesexams@gmail.com. Response time to any of the queries is 24 hours.

8. We do require CISCO ID and Official email id for security purposes. We do not sell without these details. We do background verification of the details provided, so request to give us the correct CISCO ID and official email id.

9. The workbooks are in secured pdc format and delivered via email within 24 hours after payment is received.

10. License is provided for only one Device. And we don't give license again if the device crashes or company security policies. Please install license on the device cautiously as the license will not be provided again.

11. We do support devices running Windows OS, Mac OS, Android and Mac iOS only

12. We do not provide Refund in any circumstances once the product is sold.

13. This policy is in effect from 23 November 2016 and in immediate effect for new clients and new renewals. Old clients will continue with the old Policies until the accounts get expired.

14. If there is any update, one will receive the update automatically on their registered email id.

15. Design Module will be given only 3 days before the CCIE exam

16. For any future update you can check our 'updates' page.

17. Labs are always published in phases. For e.g. if there is a new lab we publish it as First, Second, Third ... till Final release.

18. Client who have purchased our worbooks and services and wishes to attempt the lab, need to consult our experts before their CCIE Lab.

CCIE Deploy, Operate and Optimize Guidelines

Before you begin, please read these guidelines:

Overall module guidelines:

1. The network that you will deploy, operate and optimize in this module will be similar, but not necessarily identical, to the network designed in the previous module. All relevant information that is needed to successfully complete this module can be found in this module itself and overrides any information that was provided in the previous module.

2. Before you start, confirm that all devices in your rack are accessible. During the exam, if any device becomes locked or inaccessible, you must recover it.

3. Your equipment is partially preconfigured. Do not change any of the preconfigured parameters unless you are specifically told to.

4. The partial configuration on the devices may deliberately contain mistakes and errors which may need to be corrected, or workarounds applied, in order to complete specific tasks. Therefore, consider troubleshooting as an integral part of this module.

5. Points are awarded only for fully working configurations. No partial scoring is provided. It is recommended that toward the end of the exam, you go back and test the functionality as per all question requirements.

6. If you need clarification on any of the questions, or if you suspect that there might be an issue with your equipment or exam environment, contact the lab proctor as soon as possible.

7. Item-level feedback can be provided at the question level. Feedback will be processed, but Cisco will not reach out to you to discuss any feedback provided. You will not be compensated for the time you spend while providing the feedback.

8. Access to select Cisco online documentation is available from your desktop. Access to select 3rd party product documentation (such as Python) is available from the Resources window under the “External Documentation category”.

9. When you finish the lab exam, make sure that all devices are accessible for the grading proctor by having them in EXEC mode and closing the console windows. A device that is not accessible for grading cannot be graded and this may cause you to lose substantial points.

10. You have 5 hours to complete this module. Upon finishing the exam, ensure that all devices are accessible. Any device that is not accessible for grading purposes may cause you to lose substantial points.

Track specific guidelines:

1. There are several end hosts present in the lab topology, named hostXY (for example, host11). They are all identical and they can all be used at your full discretion, including accessing the GUI of DNA Center, vManage and ISE through Firefox, performing IP connectivity tests, generating or capturing traffic, and performing coding in Python or C.

2. All hostXY devices are configured as DHCP clients. Should it be necessary to force the host to release and renew its DHCP lease, right-click on the icon of the network manager located between CPU utilization and check applets in the bottom task bar, then unselects “Enable Networking”, right-click on it again and select “Enable Networking”.

3. The web-based GUI of DNA center, vManage and ISE can only be accessed from the hostXY end hosts, using firefox installed on these end hosts. These servers cannot be accessed directly from the desktop you are just now working with. You must always connect to hostXY as a jump host and access the DNA center, vManage or ISE from there. Always ignore any SSL/TLS certificate warnings in Firefox that may be displayed.

4. Devices in the topology may have more interfaces, addresses and routes configured than what is shown in the diagrams and accompanying tables. Ignore such interfaces addresses and routes entirely, unless a task explicitly requires you to use or modify them.

5. Changing or removing parts of initial running configuration on devices, as opposed to adding new configuration, is allowed only if the task allows or requires it explicitly, or if there is no other way of accomplishing the task.

Diagram 01: Complete Topology

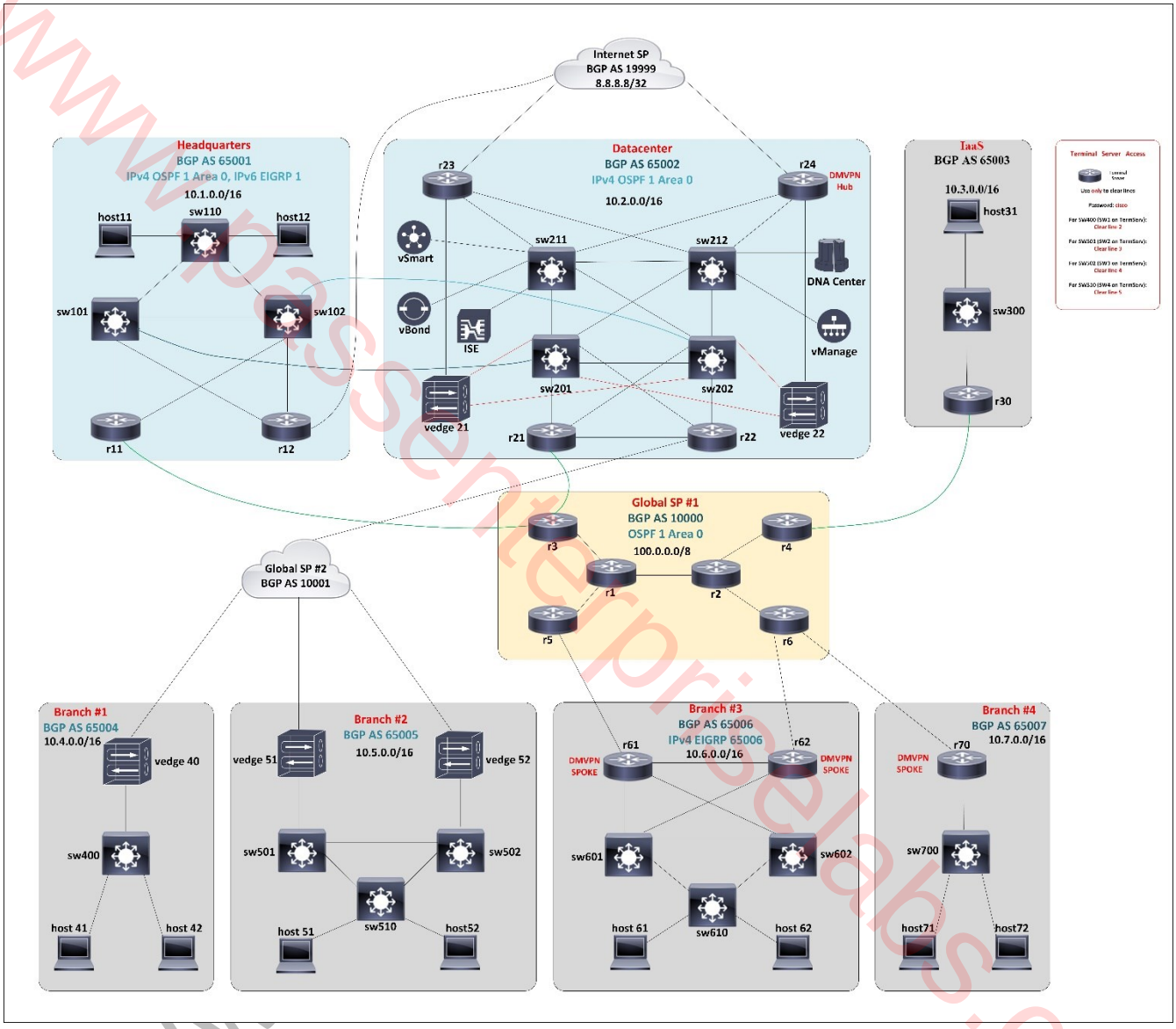
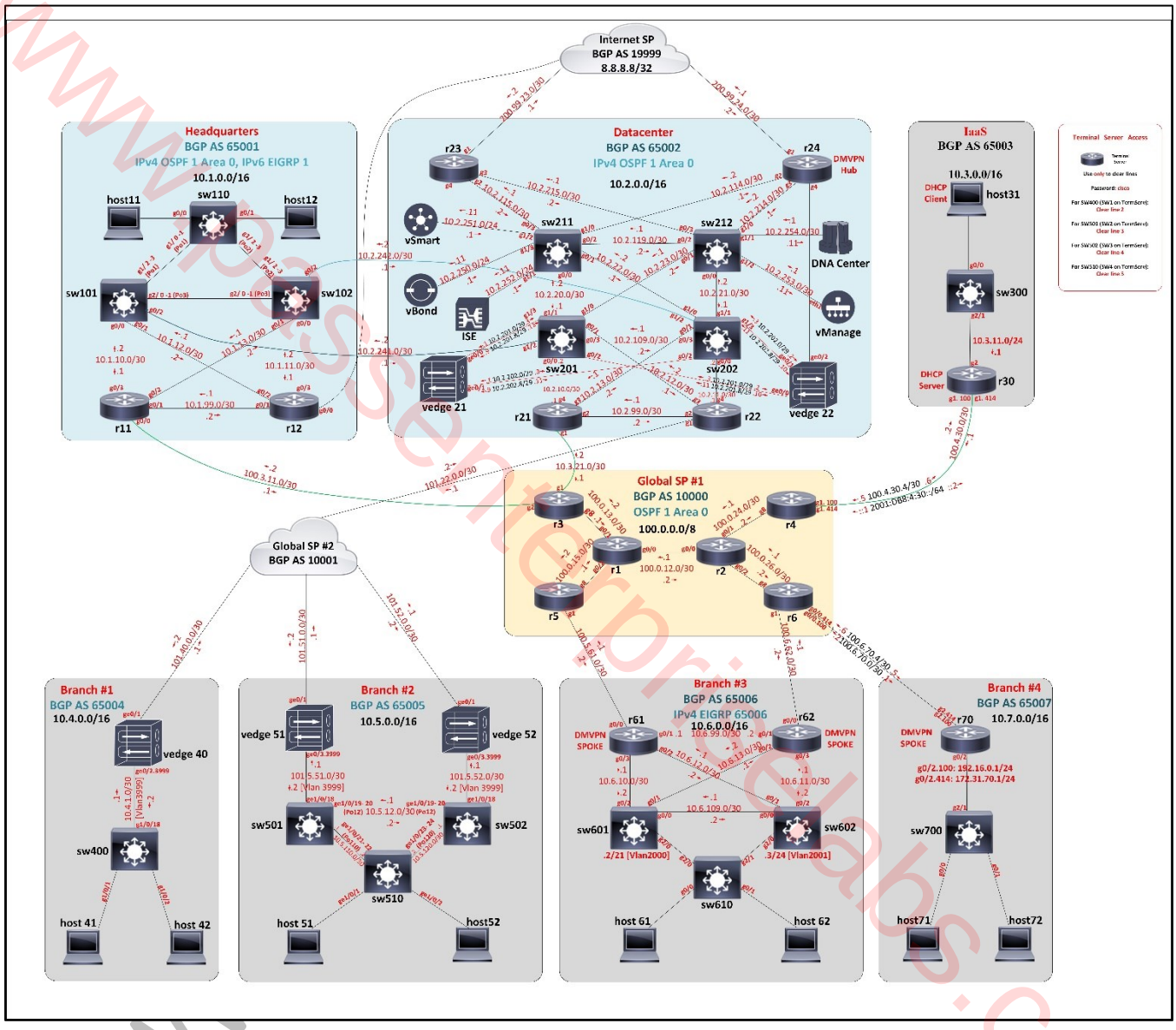


Diagram 02: Complete Topology with IP addressing



1.1: Introduction

Welcome back to the FABD2 company!

You will deploy, operate, and optimize our network. The topology you will be working with will be similar, but not necessarily identical to the network that was designed in the previous module and may include technologies and feature sets not touches upon previously.

The best of success!

1.2: Layer 2 Technologies in HQ

Complete and correct the EtherChannel configuration between switches sw101, sw102, sw110 according to these requirements:

- At the end of the task, all EtherChannels between switches sw101, sw102, sw110 must be up and operational including all their physical member links.
- Do not create new Port-channel interface; reuse those that already exist on the switches.
- When resolving existing issues, do not change the preconfigured negotiation protocol (if any)
- On EtherChannels that use a negotiation protocol, tune its mode of operation for the shortest link bundling time possible.

Configure spanning tree protocol on switches sw101, sw102, sw110 according to these requirements:

- The STP root for VLAN 2000 must be sw101.
- The STP root for VLAN 2001 must be sw102.
- STP roots must be elected based on bridge priorities.
- On the three switches, have STP perform cost calculations in 32-bit arithmetic.
- On the three switches, use the Rapid STP version and ensure that it can achieve rapid convergence on all interconnections between the switches.
- On Sw110, prevent all current and future access mode interfaces from being affected by the proposal/ Agreement process.

2 Points

Solution:

Chinese_dumps_sw110:

```
en
sw110#conf t
sw110(config)#spanning-tree mode rapid
sw110(config)#spanning-tree pathcost method long
sw110(config)#spanning-tree portfast edge default

sw110(config)#interface range gi1/2-3
sw110(config-if-range)#channel-group 2 mode active
```

Chinese_dumps_sw101:

```
en
sw101#config t
sw101(config)#spanning-tree mode rapid
sw101(config)#spanning-tree pathcost method long
sw101(config)#spanning-tree vlan 2000 priority 0
sw101(config)#spanning-tree vlan 1-4094 hello-time 1

sw101(config)#interface range gi1/2-3
sw101(config-if-range)#channel-group 1 mode on
```

Chinese_dumps_sw102:

```
en
sw102#conf t
sw102(config)#spanning-tree mode rapid
sw102(config)#spanning-tree pathcost method long
sw102(config)#spanning-tree vlan 2001 priority 0
sw102(config)#spanning-tree vlan 1-4094 hello-time 1

sw102(config)#interface range gi1/2-3
sw102(config-if-range)#channel-group 2 mode active
```

Verification:

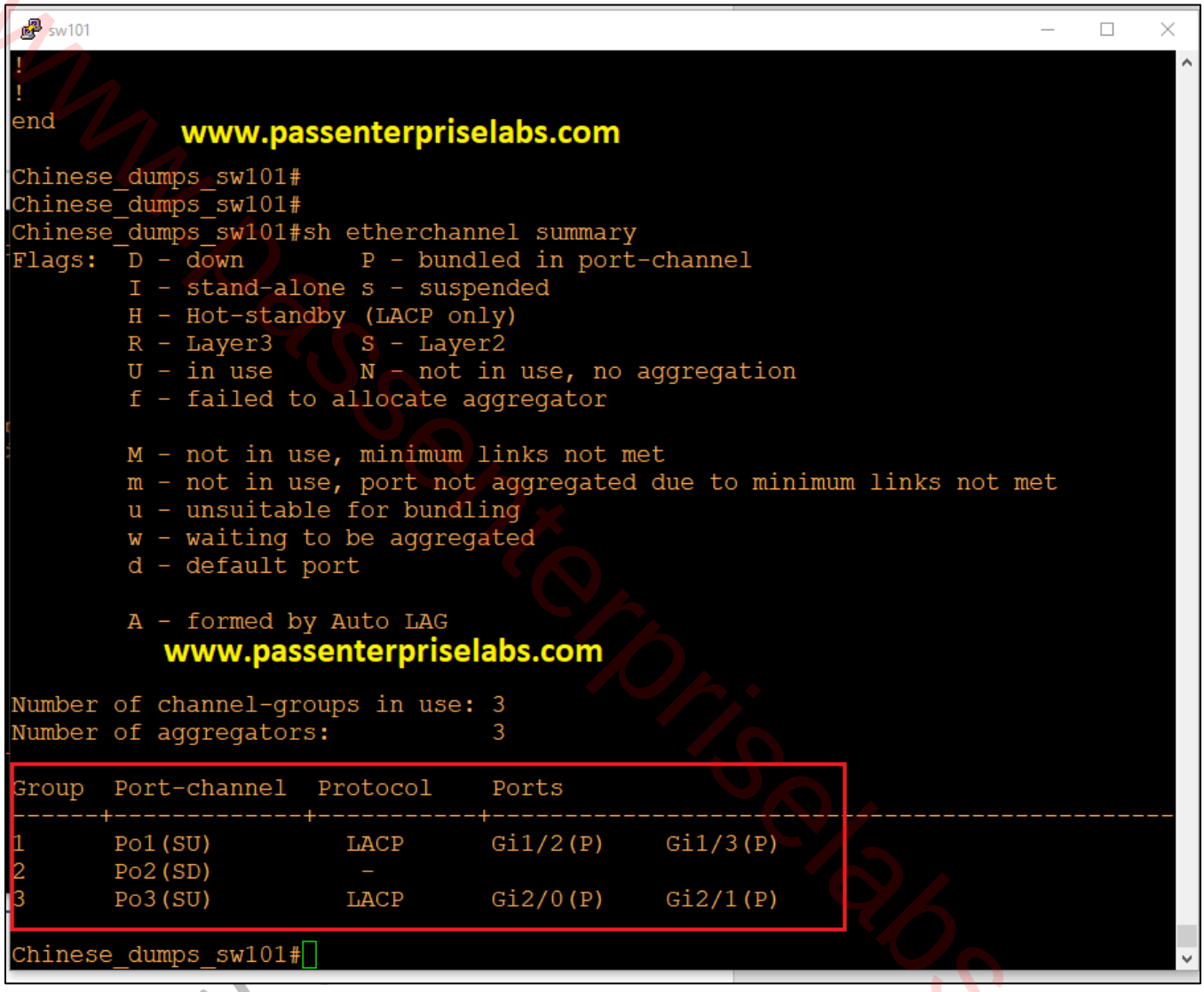
Chinese_dumps_sw110# sh etherchannel summary

```
sw110
Chinese_dumps_sw110#
Chinese_dumps_sw110#
Chinese_dumps_sw110#sh etherchanne
Chinese_dumps_sw110#sh etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator

        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG
                www.passenterpriselabs.com
Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Gi1/0(P)    Gi1/1(P)
2      Po2(SU)         LACP      Gi1/2(P)    Gi1/3(P)

Chinese_dumps_sw110#
Chinese_dumps_sw110#
```

Chinese_dumps_sw102# sh etherchannel summary

```
sw102
Chinese_dumps_sw102#sh etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator

        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG
        www.passenterpriselabs.com
Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
-----
2      Po2(SU)         LACP      Gi1/2(P)    Gi1/3(P)
3      Po3(SU)         LACP      Gi2/0(P)    Gi2/1(P)

Chinese_dumps_sw102#www.passenterpriselabs.com
```

Chinese_dumps_sw101# sh etherchannel summary



Chinese_dumps_sw110#sh spanning-tree

```
Chinese_dumps_sw110#sh spanning-tree

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID     Priority    32769
              Address     5000.0002.0000
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     5000.0002.0000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/2               Desg FWD 20000     128.3    Shr Edge
Gi0/3               Desg FWD 20000     128.4    Shr Edge
Po2                 Desg FWD 10000     128.65   Shr
Po1                 Desg FWD 10000     128.66   Shr


VLAN2000
  Spanning tree enabled protocol rstp
  Root ID     Priority    2000
              Address     5000.0003.0000
              Cost        10000
              Port        66 (Port-channel1)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    34768  (priority 32768 sys-id-ext 2000)
              Address     5000.0002.0000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/0               Desg FWD 20000     128.1    Shr Edge
Po2                 Desg FWD 10000     128.65   Shr
Po1                 Root FWD 10000     128.66   Shr


VLAN2001
  Spanning tree enabled protocol rstp
```

sw110

```
VLAN2001     www.passenterpriselabs.com
  Spanning tree enabled protocol rstp
  Root ID     Priority    2001
              Address     5000.0004.0000
              Cost        10000
              Port        65 (Port-channel2)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    34769  (priority 32768 sys-id-ext 2001)
              Address     5000.0002.0000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/1               Desg FWD 20000     128.2    Shr Edge
Po2                 Root FWD 10000     128.65   Shr
Po1                 Desg FWD 10000     128.66   Shr
                www.passenterpriselabs.com

Chinese_dumps_sw110#
```

Chinese_dumps_sw101#sh spanning-tree vlan 2000

```
sw101
Chinese_dumps_sw101#sh spanning-tree vlan 2000

VLAN2000        www.passenterpriselabs.com
  Spanning tree enabled protocol rstp
  Root ID     Priority    2000
              Address     5000.0003.0000
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    2000   (priority 0 sys-id-ext 2000)
              Address     5000.0003.0000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Po3                 Desg FWD 10000     128.66   Shr
Po1                 Desg FWD 10000     128.67   Shr
                www.passenterpriselabs.com
Chinese_dumps_sw101#
```

Chinese_dumps_sw102#sh spanning-tree vlan 2001

```
sw102
Chinese_dumps_sw102#sh spanning-tree vlan 2001
                www.passenterpriselabs.com
VLAN2001
  Spanning tree enabled protocol rstp
  Root ID     Priority    2001
              Address     5000.0004.0000
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    2001   (priority 0 sys-id-ext 2001)
              Address     5000.0004.0000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Po3                 Desg FWD 10000     128.65   Shr
Po2                 Desg FWD 10000     128.66   Shr
                www.passenterpriselabs.com
Chinese_dumps_sw102#
```

Chinese_dumps_sw110#sh spanning-tree interface g0/0 detail

```
sw110
SW110#
SW110#          www.passenterpriselabs.com
SW110#
SW110#show spanning
SW110#show spanning-tree inte
SW110#show spanning-tree interface g0/0 detail
SW110#show spanning-tree interface g0/0 detail
 Port 1 (GigabitEthernet0/0) of VLAN0001 is designated forwarding
   Port path cost 20000, Port priority 128, Port Identifier 128.1.
   Designated root has priority 32769, address 5000.0001.0000
   Designated bridge has priority 32769, address 5000.0001.0000
   Designated port id is 128.1, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   The port is in the portfast edge mode by default
   Link type is point-to-point by default
   BPDU: sent 50, received 0
SW110#
SW110#          www.passenterpriselabs.com
SW110#
SW110#
SW110#
SW110#
SW110#
```

Chinese_dumps_sw110#sh spanning-tree interface g0/1 detail

```
sw110
SW110#
SW110#
SW110#     www.passenterpriselabs.com
SW110#
SW110#
SW110#
SW110#show spanning-tree interface g0/1 detail
 Port 2 (GigabitEthernet0/1) of VLAN0001 is designated forwarding
   Port path cost 20000, Port priority 128, Port Identifier 128.2.
   Designated root has priority 32769, address 5000.0001.0000
   Designated bridge has priority 32769, address 5000.0001.0000
   Designated port id is 128.2, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   The port is in the portfast edge mode by default
   Link type is point-to-point by default
   BPDU: sent 120, received 0
SW110#
SW110#     www.passenterpriselabs.com
SW110#
SW110#
SW110#
SW110#
SW110#
```

1.3: First Hop Redundancy Protocol in HQ

For IPv4, implement an FHRP mechanism on sw101 and sw102 for VLANs 2000 and 2001 according to these requirements:

- Use Group number 100 for VLAN 2000 and group number 101 for VLAN 2001.
- Use the first available IPV4 address in the subnet for the address of the virtual router.
- For VLAN 2000, sw101 must be preferred gateway; for VLAN 2001, sw102 must be the preferred gateway. Do not rely on the IPv4 addresses of the switches as role tiebreakers. The role must determine by an explicit configuration solely on the intended preferred gateway.
- Each preferred gateway must monitor the reachability of both routers r11 and r12 using the loopback IPv4 addresses of the routers by an ICMP Echo. The reachability is to be verified every 5 seconds with a timeout of 400 msec. A router must be declared unreachable as soon as it does not respond to three probes in a row. If both r11 and r12 are declared unreachable from a preferred gateway, the other switch must be allowed to assume the gateway role.
- Use the FHRP protocol that allows the virtual IPv4 address to match the IPv4 address of a member router.

2 Points

Solution:

Chinese_dumps_sw101:

```
sw101#en
sw101#conf t
sw101(config)#int vlan 2000
sw101(config-if)#vrrp 100 ip 10.1.100.1
sw101(config-if)#vrrp 100 priority 105
sw101(config-if)#ip ospf 1 area 0
sw101(config-if)#vrrp 100 track 100
sw101(config-if)#exit


sw101(config)#int vlan 2001
sw101(config-if)#vrrp 101 ip 10.1.101.1
sw101(config-if)#ip ospf 1 area 0
sw101(config-if)#exit

sw101(config)#ip sla 1
sw101(config-ip-sla)#icmp-echo 10.1.255.11 source-interface vlan 2000
sw101(config-ip-sla-echo)#threshold 400
sw101(config-ip-sla-echo)#timeout 400
sw101(config-ip-sla-echo)#frequency 5
sw101(config-ip-sla-echo)#exit
sw101(config)#ip sla schedule 1 start-time now life forever

sw101(config)#ip sla 2
sw101(config-ip-sla)#icmp-echo 10.1.255.12 source-interface vlan 2000
sw101(config-ip-sla-echo)#threshold 400
sw101(config-ip-sla-echo)#timeout 400
sw101(config-ip-sla-echo)#frequency 5
sw101(config-ip-sla-echo)#exit
sw101(config)#ip sla schedule 2 start-time now life forever

sw101(config)#track 1 ip sla 1
sw101(config-track)#delay down 10
sw101(config)#exit
sw101(config)#track 2 ip sla 2
sw101(config-track)#delay down 10
```


```
sw101(config)#track 100 list boolean OR
sw101(config-track)#object 1
sw101(config-track)#object 2

sw101(config)#router ospf 1
sw101(config-router)#passive-interface vlan 2000
sw101(config-router)#passive-interface vlan 2001
```

Chinese_dumps_sw102:

```
sw102>en
sw102#conf t
sw102(config)#int vlan 2000
sw102(config-if)#vrrp 100 ip 10.1.100.1
sw102(config-if)#ip ospf 1 area 0
sw102(config-if)#exit

sw102(config)#int vlan 2001
sw102(config-if)#vrrp 101 ip 10.1.101.1
sw102(config-if)#vrrp 101 priority 105
sw102(config-if)#vrrp 101 track 101
sw102(config-if)#ip ospf 1 area 0
sw102(config-if)#exit

sw102(config)#ip sla 1
sw102(config-ip-sla)#icmp-echo 10.1.255.11 source-interface vlan 2001
sw102(config-ip-sla-echo)#threshold 400
sw102(config-ip-sla-echo)#timeout 400
sw102(config-ip-sla-echo)#frequency 5
sw102(config)#exit

sw102(config)#ip sla schedule 1 start-time now life forever
```

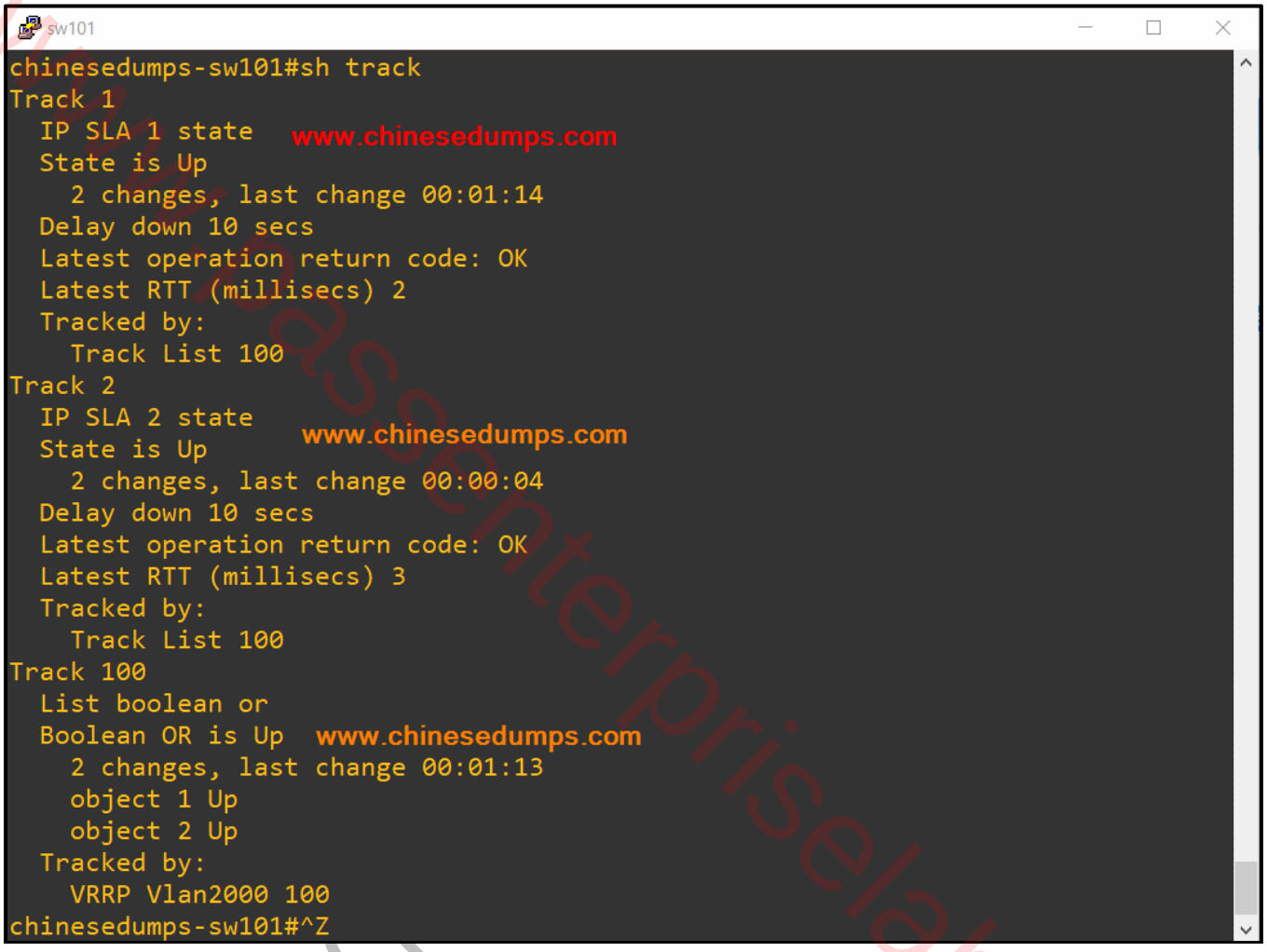

```
sw102(config)#ip sla 2
sw102(config-ip-sla-echo)#icmp-echo 10.1.255.12 source-interface vlan 2001
sw102(config-ip-sla-echo)#threshold 400
sw102(config-ip-sla-echo)#timeout 400
sw102(config-ip-sla-echo)#frequency 5
sw102(config-ip-sla-echo)#exit

sw102(config)#ip sla schedule 2 start-time now life forever

sw102(config)#track 1 ip sla 1
sw102(config-track)#delay down 10
sw102(config-track)#exit

sw102(config)#track 2 ip sla 2
sw102(config-track)#delay down 10
sw102(config-track)#exit

sw102(config)#track 101 list Boolean OR
sw102(config-track)#object 1
sw102(config-track)#object 2


sw102(config)#router ospf 1
sw102(config-router)#passive-interface vlan 2000
sw102(config-router)#passive-interface vlan 2001
```

Verification:

Chinese_dumps_sw101#sh vrrp

```
Chinese_dumps_sw101#sh vrrp
Vlan2000 - Group 100
  State is Master
  Virtual IP address is 10.1.100.1
  Virtual MAC address is 0000.5e00.0164
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 105
    Track object 100 state Up decrement 10
  Master Router is 10.1.100.2 (local), priority is 105
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.589 sec

Vlan2001 - Group 101
  State is Backup
  Virtual IP address is 10.1.101.1
  Virtual MAC address is 0000.5e00.0165
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 100
  Master Router is 10.1.101.3, priority is 105
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.609 sec (expires in 2.958 sec)

Chinese_dumps_sw101#
```

Chinese_dumps_sw101#sh track



Chinese_dumps_sw101#sh ip sla configuration

```
sw101
SW101#
SW101#
SW101#
SW101#sh ip sla configuration
IP SLAs Infrastructure Engine-III
Entry number: 1
Owner:     www.passenterpriselabs.com
Tag:
Operation timeout (milliseconds): 400
Type of operation to perform: icmp-echo
Target address/Source interface: 10.1.255.11/GigabitEthernet0/0
Type Of Service parameter: 0x0
Request size (ARR data portion): 28
Data pattern: 0xABCDABCD
Verify data: No
Vrf Name:      www.passenterpriselabs.com
Schedule:
   Operation frequency (seconds): 5  (not considered if randomly scheduled)
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled : FALSE
   Randomly Scheduled : FALSE
   Life (seconds): Forever
   Entry Ageout (seconds): never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
Threshold (milliseconds): 400
Distribution Statistics:
   Number of statistic hours kept: 2
   Number of statistic distribution buckets kept: 1
   Statistic distribution interval (milliseconds): 20
Enhanced History:
History Statistics:    www.passenterpriselabs.com
   Number of history Lives kept: 0
   Number of history Buckets kept: 15
   History Filter Type: None
```

sw101

```
   History Filter Type: None

Entry number: 2
Owner:
Tag:
Operation timeout (milliseconds): 400
Type of operation to perform: icmp-echo
Target address/Source interface: 10.1.255.12/GigabitEthernet0/1
Type Of Service parameter: 0x0
Request size (ARR data portion): 28
Data pattern: 0xABCDABCD
Verify data: No
Vrf Name:
Schedule:
   Operation frequency (seconds): 5  (not considered if randomly scheduled)
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled : FALSE
   Randomly Scheduled : FALSE
   Life (seconds): Forever
   Entry Ageout (seconds): never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
Threshold (milliseconds): 400
Distribution Statistics:
   Number of statistic hours kept: 2
   Number of statistic distribution buckets kept: 1
   Statistic distribution interval (milliseconds): 20
Enhanced History:
History Statistics:
   Number of history Lives kept: 0
   Number of history Buckets kept: 15
   History Filter Type: None

SW101#
SW101#
```

Chinese_dumps_sw102#sh vrrp

```
sw102
Chinese_dumps_sw102#sh vrrp
Vlan2000 - Group 100
  State is Backup
  Virtual IP address is 10.1.100.1
  Virtual MAC address is 0000.5e00.0164
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 100
  Master Router is 10.1.100.2, priority is 105
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.609 sec (expires in 3.164 sec)

Vlan2001 - Group 101
  State is Master
  Virtual IP address is 10.1.101.1
  Virtual MAC address is 0000.5e00.0165
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 105
    Track object 101 state Up decrement 10
  Master Router is 10.1.101.3 (local), priority is 105
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.589 sec

Chinese_dumps_sw102#
```

Chinese_dumps_sw102#sh track

```
sw102
chinesedumps-sw102#sh track
Track 1
  IP SLA 1 state
  State is Up
    2 changes, last change 00:00:10
  Delay down 10 secs
  Latest operation return code: OK
  Latest RTT (millisecs) 3
  Tracked by:
    Track List 101
Track 2
  IP SLA 2 state
  State is Up
    2 changes, last change 00:00:10
  Delay down 10 secs
  Latest operation return code: OK
  Latest RTT (millisecs) 4
  Tracked by:
    Track List 101
Track 101
  List boolean or
  Boolean OR is Up
    2 changes, last change 00:00:10
    object 1 Up
    object 2 Up
  Tracked by:
    VRRP Vlan2001 101
chinesedumps-sw102#
```

Chinese_dumps_sw102#sh ip sla configuration

```
sw101
SW101#
SW101#
SW101#
SW101#sh ip sla configuration
IP SLAs Infrastructure Engine-III
Entry number: 1
Owner:     www.passenterpriselabs.com
Tag:
Operation timeout (milliseconds): 400
Type of operation to perform: icmp-echo
Target address/Source interface: 10.1.255.11/GigabitEthernet0/0
Type Of Service parameter: 0x0
Request size (ARR data portion): 28
Data pattern: 0xABCDABCD
Verify data: No
Vrf Name:      www.passenterpriselabs.com
Schedule:
   Operation frequency (seconds): 5  (not considered if randomly scheduled)
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled : FALSE
   Randomly Scheduled : FALSE
   Life (seconds): Forever
   Entry Ageout (seconds): never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
Threshold (milliseconds): 400
Distribution Statistics:
   Number of statistic hours kept: 2
   Number of statistic distribution buckets kept: 1
   Statistic distribution interval (milliseconds): 20
Enhanced History:
History Statistics:    www.passenterpriselabs.com
   Number of history Lives kept: 0
   Number of history Buckets kept: 15
   History Filter Type: None
```

sw101

```
   History Filter Type: None

Entry number: 2
Owner:
Tag:
Operation timeout (milliseconds): 400
Type of operation to perform: icmp-echo
Target address/Source interface: 10.1.255.12/GigabitEthernet0/1
Type Of Service parameter: 0x0
Request size (ARR data portion): 28
Data pattern: 0xABCDABCD
Verify data: No
Vrf Name:
Schedule:
   Operation frequency (seconds): 5  (not considered if randomly scheduled)
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled : FALSE
   Randomly Scheduled : FALSE
   Life (seconds): Forever
   Entry Ageout (seconds): never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
Threshold (milliseconds): 400
Distribution Statistics:
   Number of statistic hours kept: 2
   Number of statistic distribution buckets kept: 1
   Statistic distribution interval (milliseconds): 20
Enhanced History:
History Statistics:
   Number of history Lives kept: 0
   Number of history Buckets kept: 15
   History Filter Type: None

SW101#
SW101#
```

To verify the gateway role:

sw101:

- Make the int g0/0 , g0/1 down (shutdown) and check "sh vrrp" , sw102 should be master for both the vlan (2000,2001)

sw102: sh vrrp

Note : If you make the interface of sw101 up , again it should retain its original role

sw102:

- Make the int g0/0 , g0/1 down (shutdown) and check "sh vrrp" , sw101 should be master for both the vlan (2000,2001)

sw101: sh vrrp

```
sw101
SW101#
SW101#sh vrrp
Vlan2000 - Group 100
  State is Master
  Virtual IP address is 10.1.100.1
  Virtual MAC address is 0000.5e00.0164
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 105
    Track object 100 state Up decrement 10
  Master Router is 10.1.100.2 (local), priority is 105
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.589 sec

Vlan2001 - Group 101
  State is Master
  Virtual IP address is 10.1.101.1
  Virtual MAC address is 0000.5e00.0165
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 100
  Master Router is 10.1.101.2 (local), priority is 100
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.609 sec

SW101#
```


Note : If you make the interfaces of sw102 up , again it should retain its original role

1.4: OSPFv2 between HQ and DC

Complete and correct the OSPF configuration on the switches sw101, sw102, sw201 and sw202 according to these requirements:

- Enable OSPFv2 on the redundant interconnections between the DC and HQ sites. Make sure that OSPF establishes adjacencies on these interconnections and exchanges routing information between the DC and HQ sites.
- Protect the authenticity and integrity of the OSPFv2 sessions on the redundant interconnections between DC and HQ with the SHA-384 mechanism. Use key ID 1 and a shared secret of “cci3” (without quotes).
- Improve the detection of unreachable OSPFv2 neighbors on the redundant interconnections between DC and HQ so that OSPF can detect the loss of a neighbor within 300 msec, with the probes being sent every 100 msec. it is not allowed to modify OSPF timers to accomplish this requirement.

3 Points

Solution:

Note: Try making the interface default if the interface showing not connect

Chinese_dumps_sw201:

```
sw201>en
sw201#conf t
sw201(config)#key chain DCHQ
sw201(config-keychainn)#key 1
sw201(config-keychain-key)#key-string cci3
sw201(config-keychain-key)#cryptographic-algorithm hmac-sha-384
sw201(config)#exit
sw201(config)#exit

sw201(config)#int g1/2
sw201(config-if)#ip ospf authentication key-chain DCHQ
sw201(config-if)#ip ospf bfd
sw201(config-if)#bfd interval 100 min_rx 100 multiplier 3
sw201(config-if)#exit

sw201#config t
sw201(config)#router ospf 1
sw201(config-router)#no passive-interface g1/2
```

Chinese_dumps_sw202:

```
sw202>en
sw202#conf t
sw202(config)#key chain DCHQ
sw202(config)#key 1
sw202(config-keychain)#key-string cci3
sw202(config-keychain)#cryptographic-algorithm hmac-sha-384
sw202(config-keychain)#exit
sw202(config)#exit

sw202(config)#int g1/2
sw202(config-if)#ip ospf authentication key-chain DCHQ
sw202(config-if)#ip ospf bfd
sw202(config-if)#bfd interval 100 min_rx 100 multiplier 3
sw202(config)#exit
```


```
sw202#config t
sw202(config)#router ospf 1
sw202(config)#no passive-interface g1/2
```

Chinese_dumps_sw101:

```
sw101>en
sw101#conf t
sw101(config)#key chain HQDC
sw101(config-keychain)#key 1
sw101(config-keychain-key)#key-string cci3
sw101(config-keychain-key)#cryptographic-algorithm hmac-sha-384
sw101(config-keychain-key)#exit
sw101(config)#exit

sw101(config)#int g0/2
sw101(config-if)#ip ospf authentication key-chain HQDC
sw101(config-if)#ip ospf bfd
sw101(config-if)#bfd interval 100 min_rx 100 multiplier 3
```

Chinese_dumps_sw102 :

```
sw102>en
sw102#conf t
sw102(config)#key chain HQDC
sw102(config-keychain)#key 1
sw102(config-keychain-key)#key-string cci3
sw102(config-keychain-key)#cryptographic-algorithm hmac-sha-384
sw102(config-keychain)#exit
sw102(config)#exit

sw102(config)#int g0/2
sw102(config-if)#ip ospf authentication key-chain HQDC
sw102(config-if)#ip ospf bfd
sw102(config-if)#bfd interval 100 min_rx 100 multiplier 3
```

Verification:

Chinese_dumps_sw101#sh key chain

```
SW101#show key chain
Key-chain HQDC:
    key 1 -- text "cci3"
        accept lifetime (always valid) - (always valid) [valid now]
        send lifetime (always valid) - (always valid) [valid now]
SW101#
SW101#
SW101#
SW101#
SW101#
```


Chinese_dumps_sw101#sh ip ospf interface g0/2

```
SW101#
SW101#sh ip ospf int g0/2
GigabitEthernet0/2 is up, line protocol is up (connected)
  Internet Address 10.2.241.2/30, Area 0, Attached via Interface Enable
  Process ID 1, Router ID 10.1.255.101, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1         no          no            Base
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State DR, Priority 1, BFD enabled
  Designated Router (ID) 10.1.255.101, Interface address 10.2.241.2
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:06
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/4/4, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
  Cryptographic authentication enabled
    Sending SA: Key 1, Algorithm HMAC-SHA-384 - key chain HQDC
SW101#
```

Chinese_dumps_sw101# sh bfd neighbor details

```
sw101
SW101#sh bfd neighbor details

IPv4 Sessions
NeighAddr      www.passenterpriselabs.comLD/RD         RH/RS     State     Int
10.2.241.1                                1/1          Up        Up        Gi0/2
Session state is UP and using echo function with 100 ms interval.
Session Host: Software
OurAddr: 10.2.241.2
Handle: 1      www.passenterpriselabs.com
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holddown (hits): 0(0), Hello (hits): 1000(8)
Rx Count: 10, Rx Interval (ms) min/max/avg: 2/938/737 last: 84 ms ago
Tx Count: 10, Tx Interval (ms) min/max/avg: 1/988/702 last: 405 ms ago
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: OSPF CEF
Uptime: 00:00:06     www.passenterpriselabs.com
Last packet: Version: 1                - Diagnostic: 0
             State bit: Up             - Demand bit: 0
             Poll bit: 0               - Final bit: 0
             C bit: 0
             Multiplier: 3             - Length: 24
             My Discr.: 1              - Your Discr.: 1
             Min tx interval: 1000000  - Min rx interval: 1000000
             Min Echo interval: 100000
SW101#
```

Chinese_dumps_sw101# sh key ip ospf neighbor

```
sw101
SW101#sh ip ospf neighbor
            www.passenterpriselabs.com
Neighbor ID     Pri   State           Dead Time   Address         Interface
10.1.255.102      1   FULL/DR         00:00:33    10.1.101.3      Vlan2001
10.1.255.102      1   FULL/DR         00:00:32    10.1.100.3      Vlan2000
10.2.255.201      1   FULL/BDR        00:00:36    10.2.241.1      GigabitEtherne
t0/2
10.1.255.12       1   FULL/DR         00:00:35    10.1.12.2       GigabitEtherne
t0/1
10.1.255.11       1   FULL/DR         00:00:32    10.1.10.1       GigabitEtherne
t0/0
            www.passenterpriselabs.com
SW101#
SW101#
SW101#
```

Chinese_dumps_sw102#sh key chain

```
sw102
sw102#
sw102#
sw102#sh key chain
Key-chain HQDC:    www.passenterpriselabs.com
    key 1 -- text "cci3"
        accept lifetime (always valid) - (always valid) [valid now]
        send lifetime (always valid) - (always valid) [valid now]
sw102#
```

Chinese_dumps_sw102#sh ip os interface g0/2

```
sw102
sw102#sh ip os int g0/2
GigabitEthernet0/2 is up, line protocol is up (connected)
  Internet Address 10.2.242.2/30, Area 0, Attached via Interface Enable
  Process ID 1, Router ID 10.1.255.102, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1          no          no            Base
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State DR, Priority 1, BFD enabled
  Designated Router (ID) 10.1.255.102, Interface address 10.2.242.2
  Backup Designated router (ID) 10.2.255.202, Interface address 10.2.24
2.1    www.passenterpriselabs.com
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:03
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/4/4, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)    www.passenterpriselabs.com
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 1 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.2.255.202  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
  Cryptographic authentication enabled
    Sending SA: Key 1, Algorithm HMAC-SHA-384 - key chain HQDC
sw102#
```

Chinese_dumps_sw102#sh bfd neighbor details

```
sw102
sw102#sh bfd neighbor details

IPv4 Sessions
NeighAddr                              LD/RD         RH/RS     State
  Int
10.2.242.1                              1/1          Up        Up
  Gi0/2
Session state is UP and using echo function with 100 ms interval.
Session Host: Software
OurAddr: 10.2.242.2
Handle: 1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holddown (hits): 0(0), Hello (hits): 1000(923)
Rx Count: 950, Rx Interval (ms) min/max/avg: 3/1022/855 last: 12 ms ago
Tx Count: 925, Tx Interval (ms) min/max/avg: 3/1004/878 last: 28 ms ago
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: OSPF CEF
Uptime: 00:13:31
Last packet: Version: 1                - Diagnostic: 0
             State bit: Up             - Demand bit: 0
             Poll bit: 0               - Final bit: 0
             C bit: 0
             Multiplier: 3             - Length: 24
             My Discr.: 1              - Your Discr.: 1
             Min tx interval: 1000000  - Min rx interval: 1000000
             Min Echo interval: 100000
sw102#
```


Chinese_dumps_sw102#sh ip ospf neighbor

```
sw102
sw102#
sw102#
sw102#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.1.255.101      1   FULL/BDR        00:00:34    10.1.101.2      Vlan2001
10.1.255.101      1   FULL/BDR        00:00:35    10.1.100.2      Vlan2000
10.2.255.202      1   FULL/BDR        00:00:37    10.2.242.1      GigabitEthernet0/
2
sw102#
```

Chinese_dumps_sw201#sh key chain

```
sw201
SW201#
SW201#sh key chai
SW201#sh key chain
Key-chain DCHQ:   www.passenterpriselabs.com
    key 1 -- text "cci3"
        accept lifetime (always valid) - (always valid) [valid now]
        send lifetime (always valid) - (always valid) [valid now]
SW201#
```

Chinese_dumps_sw201#sh ip ospf int g1/2

```
sw201
SW201#sh ip ospf int g1/2
GigabitEthernet1/2 is up, line protocol is up (connected)
  Internet Address 10.2.241.1/30, Area 0, Attached via Interface Enable
  Process ID 1, Router ID 10.2.255.201, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1         no          no            Base
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State BDR, Priority 1, BFD enabled
  Designated Router (ID) 10.1.255.101, Interface address 10.2.241.2
  Backup Designated router (ID) 10.2.255.201, Interface address 10.2.241.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:08   www.passenterpriselabs.com
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/7/7, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)  www.passenterpriselabs.com
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 1 msec, maximum is 1 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.1.255.101  (Designated Router)
  Suppress hello for 0 neighbor(s)
  Cryptographic authentication enabled
    Sending SA: Key 1, Algorithm HMAC-SHA-384 - key chain DCHQ
SW201#
```

Chinese_dumps_sw201#sh bfd neighbor details

```
sw201
SW201#sh bfd neighbor details

IPv4 Sessions
NeighAddr                              LD/RD         RH/RS     State     Int
10.2.241.2                             1/1           Up        Up        Gi1/2
Session state is UP and using echo function with 100 ms interval.
Session Host: Software
OurAddr: 10.2.241.1
Handle: 1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holddown (hits): 0(0), Hello (hits): 1000(1529)
Rx Count: 1490, Rx Interval (ms) min/max/avg: 1/1076/901 last: 690 ms ago
Tx Count: 1530, Tx Interval (ms) min/max/avg: 4/1005/878 last: 340 ms ago
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: OSPF CEF
Uptime: 00:22:23
Last packet: Version: 1                - Diagnostic: 0
             State bit: Up             - Demand bit: 0
             Poll bit: 0               - Final bit: 0
             C bit: 0
             Multiplier: 3             - Length: 24
             My Discr.: 1              - Your Discr.: 1
             Min tx interval: 1000000  - Min rx interval: 1000000
             Min Echo interval: 100000
SW201#
```


Chinese_dumps_sw201#sh ip ospf neighbor

```
sw201
SW201#
SW201#sh ip ospf nei
www.passenterpriselabs.com

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.1.255.101      1   FULL/DR         00:00:34    10.2.241.2      GigabitEthernet1/2
10.2.255.202      1   FULL/DR         00:00:39    10.2.109.2      GigabitEthernet0/3
SW201#
```

Chinese_dumps_sw202# sh key chain

```
sw202
SW202#
SW202#sh key chain
Key-chain DCHQ:    www.passenterpriselabs.com
    key 1 -- text "cci3"
        accept lifetime (always valid) - (always valid) [valid now]
        send lifetime (always valid) - (always valid) [valid now]
SW202#
```

Chinese_dumps_sw202# sh ip os int g1/2

```
sw202
SW202#sh ip ospf int g1/2
GigabitEthernet1/2 is up, line protocol is up (connected)
  Internet Address 10.2.242.1/30, Area 0, Attached via Interface Enable
  Process ID 1, Router ID 10.2.255.202, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1         no          no            Base
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State BDR, Priority 1, BFD enabled
  Designated Router (ID) 10.1.255.102, Interface address 10.2.242.2
  Backup Designated router (ID) 10.2.255.202, Interface address 10.2.242.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:00    www.passenterpriselabs.com
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/7/7, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0) www.passenterpriselabs.com
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 2 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.1.255.102  (Designated Router)
  Suppress hello for 0 neighbor(s)
  Cryptographic authentication enabled
    Sending SA: Key 1, Algorithm HMAC-SHA-384 - key chain DCHQ
SW202#
```

Chinese_dumps_sw202#sh bfd neighbor details

```
sw202
SW202#sh bfd nei details

IPv4 Sessions
NeighAddr                              LD/RD         RH/RS     State     Int
10.2.242.2                             1/1           Up        Up        Gi1/2
Session state is UP and using echo function with 100 ms interval.
Session Host: Software
OurAddr: 10.2.242.1
Handle: 1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holddown (hits): 0(0), Hello (hits): 1000(2165)
Rx Count: 2111, Rx Interval (ms) min/max/avg: 2/1073/898 last: 365 ms ago
Tx Count: 2166, Tx Interval (ms) min/max/avg: 1/1014/877 last: 35 ms ago
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: OSPF CEF
Uptime: 00:31:36
Last packet: Version: 1                - Diagnostic: 0
             State bit: Up             - Demand bit: 0
             Poll bit: 0               - Final bit: 0
             C bit: 0
             Multiplier: 3             - Length: 24
             My Discr.: 1              - Your Discr.: 1
             Min tx interval: 1000000  - Min rx interval: 1000000
             Min Echo interval: 100000
SW202#
```


Chinese_dumps_sw202: sh ip ospf neighbor

```
sw202
SW202#
SW202#sh ip ospf neighbor
                  www.pasenterpriselabs.com
Neighbor ID     Pri   State           Dead Time   Address         Interface
10.1.255.102      1   FULL/DR         00:00:30    10.2.242.2      GigabitEthernet1/2
10.2.255.201      1   FULL/BDR        00:00:36    10.2.109.1      GigabitEthernet0/3
SW202#
```

1.5: DHCP IPv4 service for HQ

Enable hosts in HQ VLAN 2000 and VLAN 2001 to obtain their IP configuration via DHCP according to these requirements:

- On sw211, create IPv4 DHCP pools named hq_v2000 and hq_v2001 for HQ VLANs 2000 and 2001, respectively. In each subnet, assign addresses from .101 upto .254 inclusively, and the appropriate gateway to clients.
- Enable DHCP snooping on sw110 in VLANs 2000 and 2001 to protect against DHCP-related attacks.
- Place host11 into VLAN 2000.
- Place host12 into VLAN 2001.
- Perform the necessary configuration on switches sw101, sw102, sw110 to enable hosts in VLANs2000 and 2001 to obtain IPv4 configuration through DHCP. The DHCP server running at sw211 in the DC must be referred to by its loopback IPv4 address 10.2.255.211. Do not disable the Option 82 insertion, and do not enable DHCP snooping on other switches.
- Verify that host11 and host12 have IP connectivity to the Cisco DNA Center, vManage and ISE running in the DC using their internal (In Band Connectivity) addresses.

2 Points

Solution:

Chinese_dumps_sw110:

```
sw110>en
sw110#conf t
sw110(config)#ip dhcp snooping
sw110(config)#ip dhcp snooping vlan 2000 2001
sw110(config)#int range po1,po2
sw110(config-if)#ip dhcp snooping trust
sw110(config-if)#exit

sw110(config)#int g0/0
sw110(config-if)#switchport mode access
sw110(config-if)#switchport access vlan 2000
sw110(config-if)#exit

sw110(config)#int g0/1
sw110(config-if)#switchport mode access
sw110(config-if)#switchport access vlan 2001
sw110(config-if)#exit
```

Chinese_dumps_sw101:

```
sw101>en
sw101#conf t
sw101(config)#int vlan 2000
sw101(config-if)#ip helper-address 10.2.255.211
sw101(config-if)#ip dhcp relay information trusted

sw101(config)#int vlan 2001
sw101(config-if)#ip helper-address 10.2.255.211
sw101(config-if)#ip dhcp relay information trusted
sw101(config-if)#exit
sw101(config)#exit
```

Chinese_dumps_sw102:

```
sw102>en
sw102#conf t
sw102(config)#int vlan 2000
sw102(config-if)#ip helper-address 10.2.255.211
sw102(config-if)#ip dhcp relay information trusted
sw102(config-if)#exit

sw102(config)#int vlan 2001
sw102(config-if)#ip helper-address 10.2.255.211
sw102(config-if)#ip dhcp relay information trusted
```

Chinesedumps.com-sw211:

```
sw211>en
sw211#conf t
sw211(config)#ip dhcp excluded-address 10.1.100.1 10.1.100.100
sw211(config)#ip dhcp pool hq_v2000
sw211(config-dhcp)#network 10.1.100.0 /24
sw211(config-dhcp)#default-router 10.1.100.1
sw211(config-dhcp)#exit

sw211(config)#ip dhcp excluded-address 10.1.101.1 10.1.101.100
sw211(config)#ip dhcp pool hq_v2001
sw211(config-dhcp)#network 10.1.101.0 /24
sw211(config-dhcp)#default-router 10.1.101.1
sw211(config)#exit
```

Verification:

Chinese_dumps_sw101#sh run int vlan 2000

```
sw101
SW101#sh run int vlan 2000
Building configuration...

Current configuration : 251 bytes
!   www.passenterpriselabs.com
interface Vlan2000
 ip dhcp relay information trusted
 ip address 10.1.100.2 255.255.255.0
 ip helper-address 10.2.255.211
 ip ospf 1 area 0
 ipv6 address FE80::101 link-local
 vrrp 100 ip 10.1.100.1
 vrrp 100 priority 105
 vrrp 100 track 100
end  www.passenterpriselabs.com

SW101#
SW101#
```

Chinese_dumps_sw101#sh run int vlan 2001

```
sw101
SW101#
SW101#sh run int vlan 2001
Building configuration...
  www.passenterpriselabs.com
Current configuration : 208 bytes
!
interface Vlan2001
 ip dhcp relay information trusted
 ip address 10.1.101.2 255.255.255.0
 ip helper-address 10.2.255.211
 ip ospf 1 area 0
 ipv6 address FE80::101 link-local
 vrrp 101 ip 10.1.101.1
end
  www.passenterpriselabs.com
SW101#
SW101#
SW101#
```

Chinese_dumps_sw102#sh run int vlan 2000

```
sw102
sw102#sh run int vlan 2000
Building configuration...
 www.passenterpriselabs.com
Current configuration : 208 bytes
!
interface Vlan2000
 ip dhcp relay information trusted
 ip address 10.1.100.3 255.255.255.0
 ip helper-address 10.2.255.211
 ip ospf 1 area 0
 ipv6 address FE80::102 link-local
 vrrp 100 ip 10.1.100.1
end
 www.passenterpriselabs.com
sw102#
sw102#
sw102#
```

Chinese_dumps_sw102#sh run int vlan 2001

```
sw102
sw102#sh run int vlan 2001
Building configuration...
 www.passenterpriselabs.com
Current configuration : 251 bytes
!
interface Vlan2001
 ip dhcp relay information trusted
 ip address 10.1.101.3 255.255.255.0
 ip helper-address 10.2.255.211
 ip ospf 1 area 0
 ipv6 address FE80::102 link-local
 vrrp 101 ip 10.1.101.1
 vrrp 101 priority 105
 vrrp 101 track 101
end
  www.passenterpriselabs.com
sw102#
```

Chinese_dumps_sw110#sh ip dhcp snooping

```
sw110
SW110#sh ip dhcp snooping
Switch DHCP snooping is enabled
Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
2000-2001
DHCP snooping is operational on following VLANs:
2000-2001
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
   remote-id: 5000.0001.0000 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                  Trusted    Allow option    Rate limit (pps)
-----------------------    -------    ------------    ----------------
GigabitEthernet1/0         yes        yes             unlimited
  Custom circuit-ids:
GigabitEthernet1/1         yes        yes             unlimited
  Custom circuit-ids:
GigabitEthernet1/2         yes        yes             unlimited
Interface                  Trusted    Allow option    Rate limit (pps)
-----------------------    -------    ------------    ----------------
  Custom circuit-ids:
GigabitEthernet1/3         yes        yes             unlimited
  Custom circuit-ids:
Port-channel1              yes        yes             unlimited
  Custom circuit-ids:
Port-channel2              yes        yes             unlimited
  Custom circuit-ids:
SW110#
```

Chinese_dumps_sw110#sh vlan brief

```
sw110
SW110#sho vlan bri

VLAN Name  www.passenterpriselabs.com  Status    Ports
---- ------------------------------- --------- -------------------------------
1    default                         active    Gi0/2, Gi0/3
1002 fddi-default                    act/unsup
1003 token-ring-default              act/unsup
1004 fddinet-default                 act/unsup
1005 trnet-default                   act/unsup
2000 VLAN2000                        active    Gi0/0
2001 VLAN2001                        active    Gi0/1
SW110#
SW110#      www.passenterpriselabs.com
SW110#
SW110#
SW110#
```

Chinese_dumps_sw110#sh run | s snooping

```
sw110
SW110#
SW110#
SW110#    www.passenterpriselabs.com
SW110#
SW110#sh run | s snooping
ip dhcp snooping vlan 2000-2001
ip dhcp snooping
 ip dhcp snooping trust
 ip dhcp snooping trust
 ip dhcp snooping trust
 ip dhcp snooping trust
 ip dhcp snooping trust
 ip dhcp snooping trust
SW110#    www.passenterpriselabs.com
SW110#
SW110#
```

Chinesedumps.com-sw211#sh ip dhcp pool

```
sw211
SW211#sh ip dhcp pool

Pool hq_v2000 :   www.passenterpriselabs.com
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Excluded addresses             : 100
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased/Excluded/Total
 10.1.100.102         10.1.100.1       - 10.1.100.254      1      / 100    / 254

Pool hq_v2001 :   www.passenterpriselabs.com
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Excluded addresses             : 100
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased/Excluded/Total
 10.1.101.102         10.1.101.1       - 10.1.101.254      1      / 100    / 254
SW211#
```

Chinesedumps.com-sw211#sh run | s dhcp

```
sw211
SW211#sh run | s dhcp
ip dhcp excluded-address 10.1.100.1 10.1.100.100
ip dhcp excluded-address 10.1.101.1 10.1.101.100
ip dhcp pool hq_v2000   www.passenterpriselabs.com
 network 10.1.100.0 255.255.255.0
 default-router 10.1.100.1
ip dhcp pool hq_v2001
 network 10.1.101.0 255.255.255.0
 default-router 10.1.101.1
SW211#
SW211#   www.passenterpriselabs.com
SW211#
SW211#
```

Host 11:

QEMU (host11)

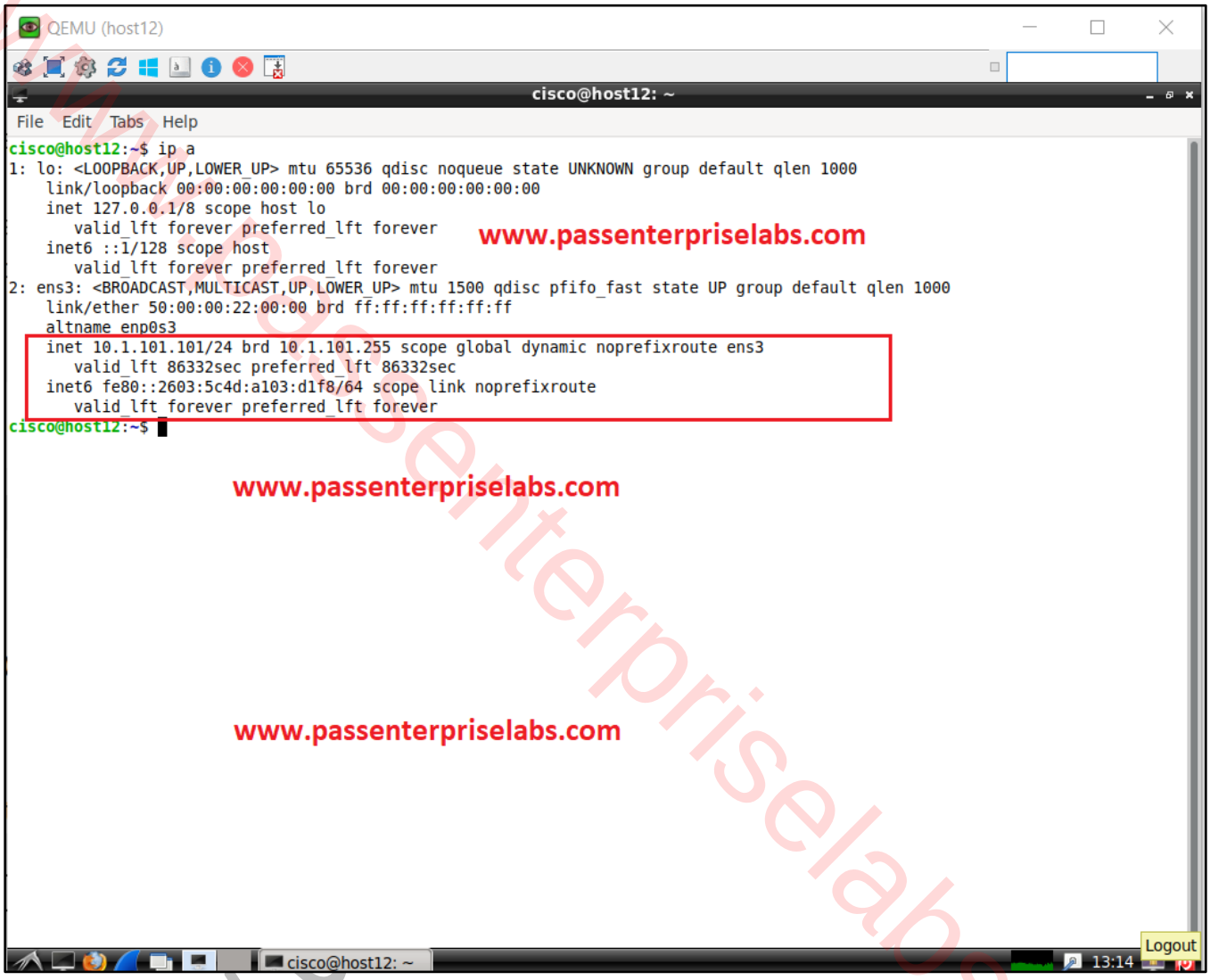
cisco@host11: ~

File Edit Tabs Help

```
cisco@host11:~$
cisco@host11:~$
cisco@host11:~$ ping 10.2.255.211
PING 10.2.255.211 (10.2.255.211) 56(84) bytes of data.
64 bytes from 10.2.255.211: icmp_seq=1 ttl=253 time=41.6 ms
64 bytes from 10.2.255.211: icmp_seq=2 ttl=253 time=46.0 ms
^C
--- 10.2.255.211 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 41.637/43.840/46.043/2.203 ms
cisco@host11:~$
cisco@host11:~$
cisco@host11:~$
cisco@host11:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:50:00:00:04:00 brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    inet 10.1.100.101/24 brd 10.1.100.255 scope global dynamic noprefixroute ens3
       valid_lft 86390sec preferred_lft 86390sec
    inet6 fe80::fe4f:8cc0:d7d0:5776/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
cisco@host11:~$
cisco@host11:~$
cisco@host11:~$
cisco@host11:~$
cisco@host11:~$
cisco@host11:~$
cisco@host11:~$
cisco@host11:~$
cisco@host11:~$
cisco@host11:~$
cisco@host11:~$
cisco@host11:~$
```


cisco@host11: ~ ScreenLock

Host 12:



1.6: IPv6 in HQ

Implement IPv6 on sw101 and sw102 for switch virtual interfaces (SVIs) Vlan 2000 and Vlan 2001 according to these requirements:

- Sw101
  Interface Vlan2000: 2001:db8:1:100::1/64
  Interface Vlan2001: 2001:db8:1:101::1/64
- Sw102
  Interface Vlan2000: 2001:db8:1:100::2/64
  Interface Vlan2001: 2001:db8:1:101::2/64
- The configuration must enable hosts in these VLANs to obtain their IPv6 configuration via SLAAC and keep a stable connectivity with other IPv6 networks.
- Use native IPv6 means to provide gateway redundancy, with sw101 being the preferred gateway in VLAN 2000 and sw102 being the preferred gateway in VLAN 2001. The role must be determined by an explicit configuration solely on the intended preferred gateway.
- Hosts must be able to detect the failure of the preferred gateway in as little as 3 seconds.

1 Point

Solution:

Chinese_dumps_sw101:

```
sw101>en
sw101#conf t
sw101(config)#int vlan 2000
sw101(config-if)#ipv6 enable
sw101(config-if)#ipv6 address 2001:db8:1:100::1/64
sw101(config-if)#ipv6 nd router-preference high
sw101(config-if)#ipv6 nd ra lifetime 3
sw101(config-if)#ipv6 nd ra interval msec 1000

sw101(config)#int vlan 2001
sw101(config-if)#ipv6 enable
sw101(config-if)#ipv6 address 2001:db8:1:101::1/64
sw101(config-if)#ipv6 nd ra lifetime 3
sw101(config-if)#ipv6 nd ra interval msec 1000
```

Chinese_dumps_sw102:

```
sw102>en
sw102(config)#conf t
sw102(config-if)#int vlan 2000
sw102(config-if)#ipv6 enable
sw102(config-if)#ipv6 address 2001:db8:1:100::2/64
sw102(config-if)#ipv6 nd ra lifetime 3
sw102(config-if)#ipv6 nd ra interval msec 1000

sw102(config)#int vlan 2001
sw102(config-if)#ipv6 enable
sw102(config-if)#ipv6 address 2001:db8:1:101::2/64
sw102(config-if)#ipv6 nd router-preference high
sw102(config-if)#ipv6 nd ra lifetime 3
sw102(config-if)#ipv6 nd ra interval msec 1000
```

Verification:

Chinese_dumps_sw101#sh run int vlan 2000

```
sw101
chinesedumps-sw101#
chinesedumps-sw101#
chinesedumps-sw101#sh run int vlan 2000
Building configuration...
       www.passenterpriselabs.com
Current configuration : 385 bytes
!
interface Vlan2000
 ip dhcp relay information trusted
 ip address 10.1.100.2 255.255.255.0
 ip helper-address 10.2.255.211
 ip ospf 1 area 0
 ipv6 address FE80::101 link-local
 ipv6 address 2001:DB8:1:100::1/64
 ipv6 enable
 ipv6 nd router-preference High
 ipv6 nd ra lifetime 3
 ipv6 nd ra interval msec 1000
 vrrp 100 ip 10.1.100.1
 vrrp 100 priority 105
 vrrp 100 track 100
end    www.passenterpriselabs.com

chinesedumps-sw101#
```

Chinese_dumps_sw101#sh run int vlan 2001

```
sw101

chinesedumps-sw101#sh run int vlan 2001
Building configuration...
     www.passenterpriselabs.com
Current configuration : 310 bytes
!
interface Vlan2001
 ip dhcp relay information trusted
 ip address 10.1.101.2 255.255.255.0
 ip helper-address 10.2.255.211
 ip ospf 1 area 0
 ipv6 address FE80::101 link-local
 ipv6 address 2001:DB8:1:101::1/64
 ipv6 enable
 ipv6 nd ra lifetime 3
 ipv6 nd ra interval msec 1000
 vrrp 101 ip 10.1.101.1
end    www.passenterpriselabs.com

chinesedumps-sw101#
chinesedumps-sw101#
chinesedumps-sw101#
chinesedumps-sw101#
chinesedumps-sw101#
```

Chinese_dumps_sw102#sh run int vlan 2000

```
sw102
chinesedumps-sw102#
chinesedumps-sw102#sh run int vlan 2000
Building configuration...
    www.passenterprielabs.com
Current configuration : 310 bytes
!
interface Vlan2000
 ip dhcp relay information trusted
 ip address 10.1.100.3 255.255.255.0
 ip helper-address 10.2.255.211
 ip ospf 1 area 0
 ipv6 address FE80::102 link-local
 ipv6 address 2001:DB8:1:100::2/64
 ipv6 enable
 ipv6 nd ra lifetime 3
 ipv6 nd ra interval msec 1000
 vrrp 100 ip 10.1.100.1
end
     www.passenterprielabs.com

chinesedumps-sw102#
chinesedumps-sw102#
chinesedumps-sw102#
chinesedumps-sw102#
chinesedumps-sw102#
```

Chinese_dumps_sw102#sh run int vlan 2001

```
sw102
chinesedumps-sw102#
chinesedumps-sw102#
chinesedumps-sw102#sh run int vlan 2001
Building configuration...
    www.passenterprielabs.com
Current configuration : 385 bytes
!
interface Vlan2001
 ip dhcp relay information trusted
 ip address 10.1.101.3 255.255.255.0
 ip helper-address 10.2.255.211
 ip ospf 1 area 0
 ipv6 address FE80::102 link-local
 ipv6 address 2001:DB8:1:101::2/64
 ipv6 enable
 ipv6 nd router-preference High
 ipv6 nd ra lifetime 3
 ipv6 nd ra interval msec 1000
 vrrp 101 ip 10.1.101.1
 vrrp 101 priority 105
 vrrp 101 track 101
end   www.passenterprielabs.com

chinesedumps-sw102#
```

Chinese_dumps_sw101#sh ipv6 int vlan 2000

```
sw101
chinesedumps-sw101#sh ipv6 int vlan 2000
Vlan2000 is up, line protocol is up   www.passenterpriselabs.com
  IPv6 is enabled, link-local address is FE80::101
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:1:100::1, subnet is 2001:DB8:1:100::/64
  Joined group address(es):
    FF02::1        www.passenterpriselabs.com
    FF02::2
    FF02::1:FF00:1
    FF02::1:FF00:101
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent   www.passenterpriselabs.com
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 1000 milliseconds
  ND router advertisements live for 3 seconds
  ND advertised default router preference is High
  Hosts use stateless autoconfig for addresses.
chinesedumps-sw101#
```

Chinese_dumps_sw101#sh ipv6 int vlan 2001

```
sw101
chinesedumps-sw101#sh ipv6 int vlan 2001
Vlan2001 is up, line protocol is up   www.passenterpriselabs.com
  IPv6 is enabled, link-local address is FE80::101
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:1:101::1, subnet is 2001:DB8:1:101::/64
  Joined group address(es):
    FF02::1        www.passenterpriselabs.com
    FF02::2
    FF02::1:FF00:1
    FF02::1:FF00:101
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent   www.passenterpriselabs.com
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 1000 milliseconds
  ND router advertisements live for 3 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
chinesedumps-sw101#
```

Chinese_dumps_sw102#sh ipv6 int vlan 2000

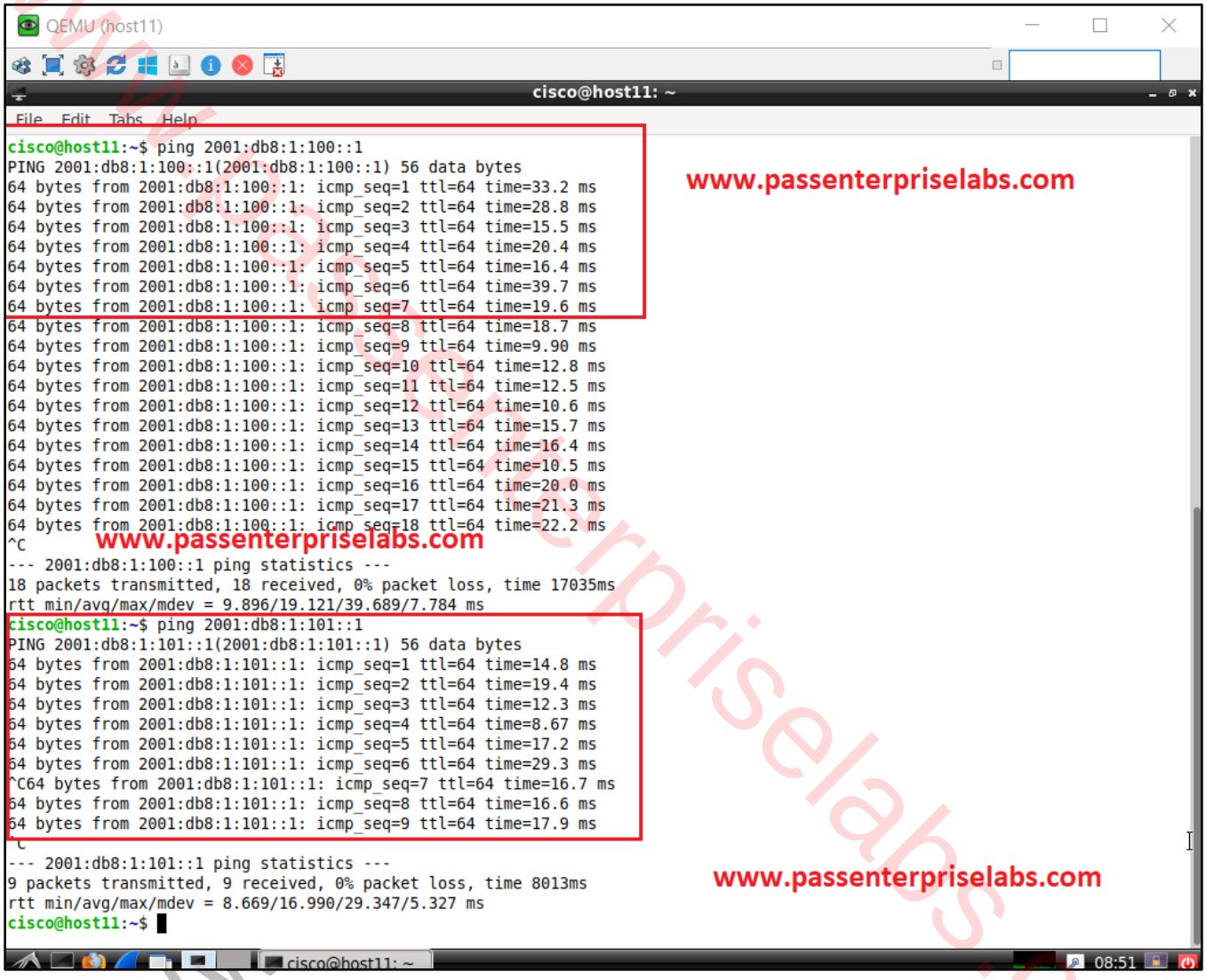
```
sw102
chinesedumps-sw102#sh ipv6 int vlan 2000
Vlan2000 is up, line protocol is up    www.passenterpriselabs.com
  IPv6 is enabled, link-local address is FE80::102
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:1:100::2, subnet is 2001:DB8:1:100::/64
  Joined group address(es):
    FF02::1    www.passenterpriselabs.com
    FF02::2
    FF02::1:FF00:2
    FF02::1:FF00:102
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent    www.passenterpriselabs.com
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 1000 milliseconds
  ND router advertisements live for 3 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
chinesedumps-sw102#
```

Chinese_dumps_sw102#sh ipv6 int vlan 2001

```
sw102
chinesedumps-sw102#sh ipv6 int vlan 2001
Vlan2001 is up, line protocol is up    www.passenterpriselabs.com
  IPv6 is enabled, link-local address is FE80::102
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:1:101::2, subnet is 2001:DB8:1:101::/64
  Joined group address(es):
    FF02::1    www.passenterpriselabs.com
    FF02::2
    FF02::1:FF00:2
    FF02::1:FF00:102
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent    www.passenterpriselabs.com
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 1000 milliseconds
  ND router advertisements live for 3 seconds
  ND advertised default router preference is High
  Hosts use stateless autoconfig for addresses.
chinesedumps-sw102#
```

To verify the task:

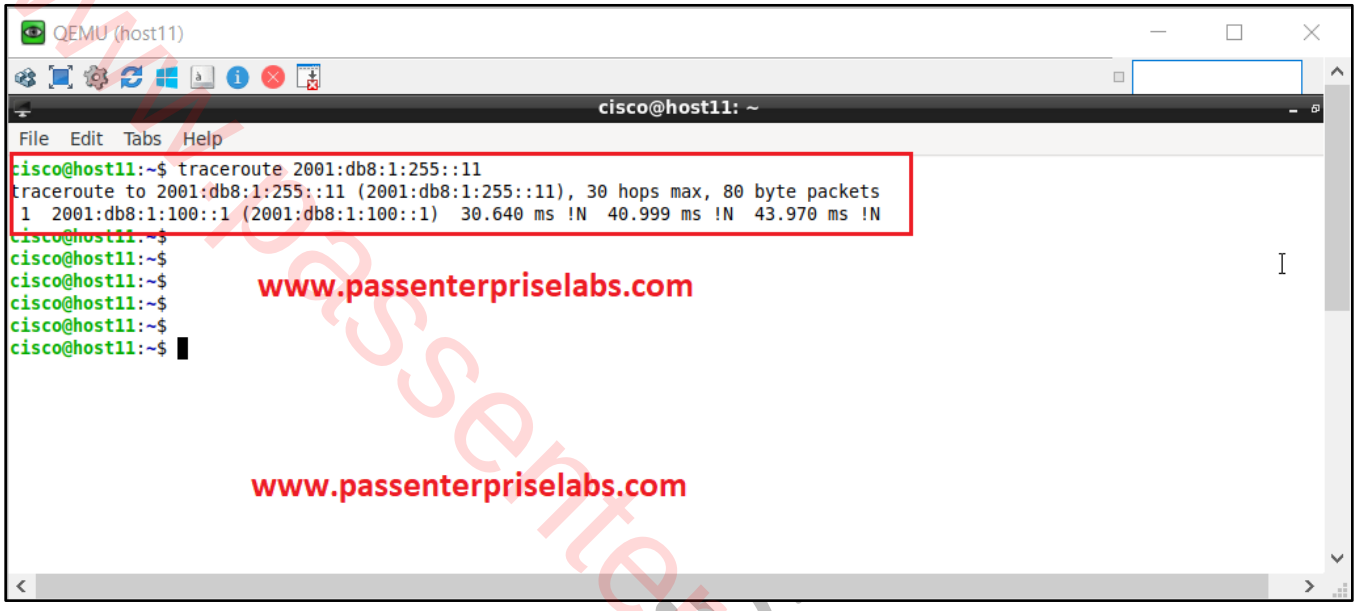
- Ping from host-11 to both the ipv6 vlan 2000 and 2001(2001:db8:1:100::1 , 2001:db8:1:101::1)



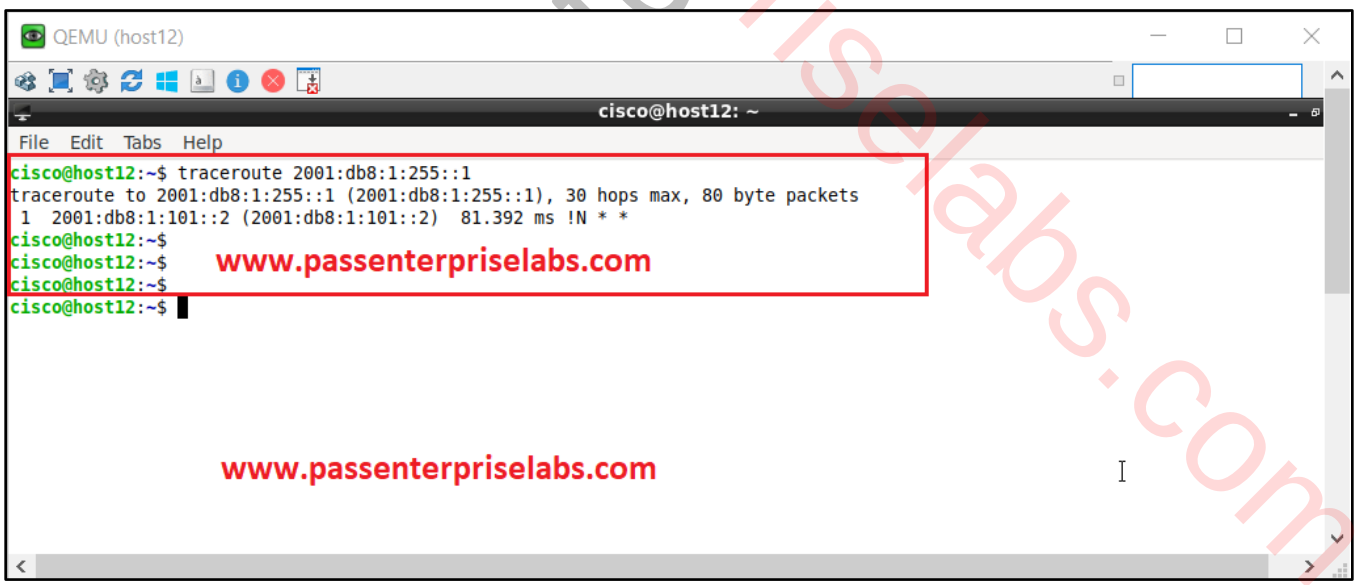
- Ping from host-12 to both the ipv6 vlan 2000 and 2001(2001:db8:1:100::1 , 2001:db8:1:101::1)

To verify the switching of gateway roles:

- Traceroute from both host-11 & host-12 to ipv6 loopback address of r11 (2001:db8:1:255::11)

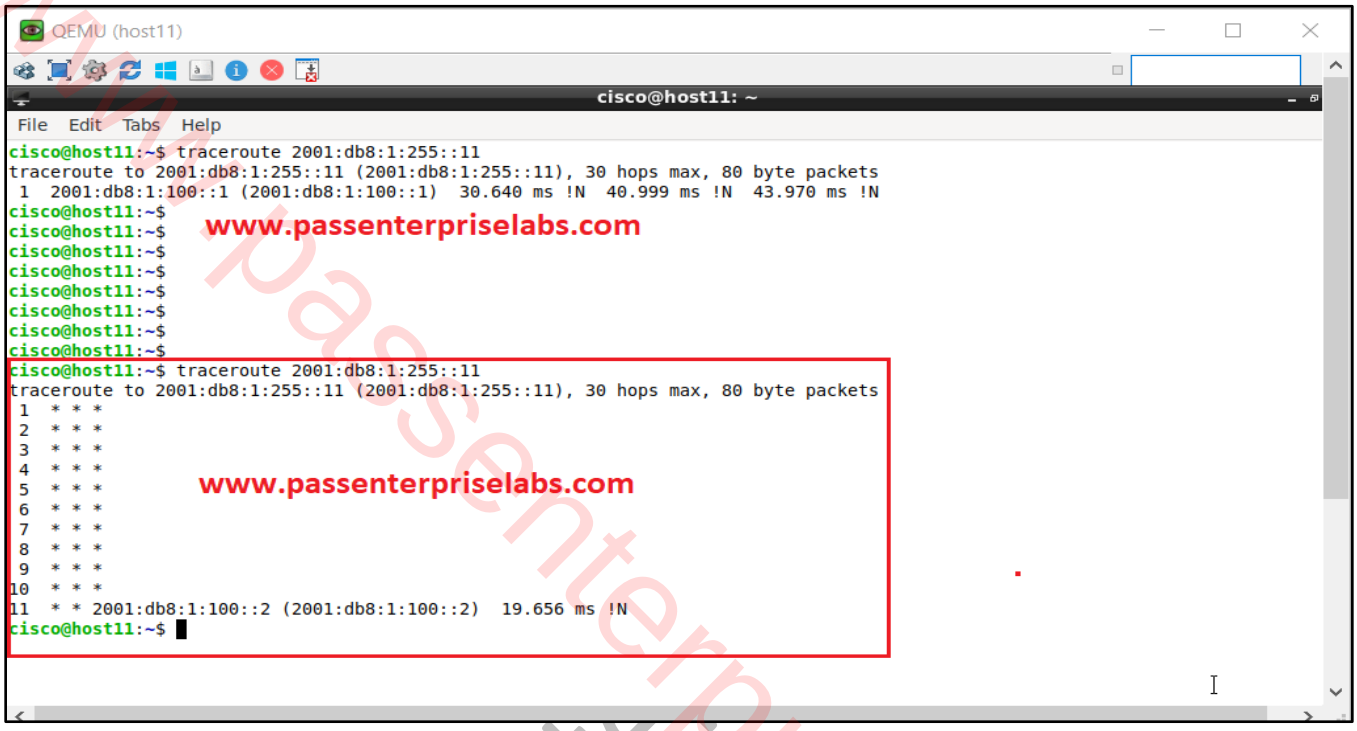


In the above output you can see host11 is using sw101 – vlan 2000 to reach r11



In the above output you can see host12 is using sw102 – vlan 2001 to reach r11

- After we shutdown the vlan 2000 on sw101 , the host11 will switch its gateway to sw102 – vlan 2000



- After we shutdown the vlan 2001 on sw102 , the host12 will switch its gateway to sw101 – vlan 2001

1.7: IPv6 EIGRP in HQ

In HQ, enable EIGRP for IPv6 on r11, r12, sw101 and sw102 according to these requirements:

- Use process name “ccie”(without the quotes) and AS number 65001.
- Do not configure any additional IPv6 addresses.
- IPv6 EIGRP may form adjacencies only over the physical Layer3 interfaces between r11, r12, sw101 and sw102.
- Prevent IPv6 EIGRP from automatically running on, or advertising attached prefixes from, new IPv6-enabled interfaces in the future unless allowed explicitly.
- Ensure that the attached IPv6 prefixes on SVIs Vlan2000 and Vlan2001 onsw101 and sw102 are advertised in IPv6 EIGRP and learned on r11 and r12.
- No route filtering is allowed to accomplish this entire task.

2 Points

Solution:

Chinese_dumps_sw101:

```
sw101>en
sw101#conf t
sw101(config)#router eigrp ccie
sw101(config-router)#address-family ipv6 unicast AS 65001
sw101(config-router-af)#af-interface default
sw101(config-router)#shutdown
sw101(config-router)#exit-af-interface
sw101(config-router)#af-interface vlan 2000
sw101(config-router-interface)#no shutdown
sw101(config-router-interface)#passive
sw101(config-router-interface)#af-interface vlan 2001
sw101(config-router-interface)#no shutdown
sw101(config-router-interface)#passive
sw101(config-router-interface)#af-interface g0/0
sw101(config-router-interface)#no shutdown
sw101(config-router-interface)#af-interface g0/1
sw101(config-router-interface)#no shutdown
```

Chinese_dumps_sw102:

```
sw102>en
sw102#conf t
sw102(conifg)#router eigrp ccie
sw102(config-router)#address-family ipv6 unicast AS 65001
sw102(config-router-af)#af-interface default
sw102(conifg-router-af)#shutdown
sw102(conifg-router-af)#af-interface vlan 2000
sw102(conifg-router-af)#no shutdown
sw102(conifg-router-af)#passive
sw102(conifg-router-af)#af-interface vlan 2001
sw102(conifg-router-af)#no shutdown
sw102(conifg-router-af)#passive
sw102(conifg-router-af)#af-interface g0/0
sw102(conifg-router-af)#no shutdown
sw102(conifg-router-af)#af-interface g0/1
sw102(conifg-router-af)#no shutdown
```

Chinese_dumps_r11:

```
r11>en
r11#conf t
r11(config)#router eigrp ccie
r11(config-router)#address-family ipv6 unicast AS 65001
r11(config-router-af)#af-interface default
r11(config-router-af)#shutdown
r11(config-router-af)#exit-af-interface

r11(config-router)#af-interface g0/2
r11(config-router-af)#no shutdown
r11(config-router-af)#af-interface g0/1
r11(config-router-af)#no shutdown
r11(config-router-af)#exit-af-interface

r11(config-router)#af-interface g0/3
r11(config-router-af)#no shutdown
```

Chinesedumps.com-r12:

```
r12>en
r12#conf t
r12(config)#router eigrp ccie
r12(config-router)#address-family ipv6 unicast AS 65001
r12(config-router-af)#af-interface default
r12(config-router-af)#shutdown
r12(config-router-af)#exit-af-interface

r12(config-router)#af-interface g0/2
r12(config-router-af)#no shutdown
r12(config-router)#af-interface g0/1
r12(config-router-af)#no shutdown
r12(config-router)#af-interface g0/3
r12(config-router-af)#no shutdown
```

Verification:

Chinese_dumps_sw101:show ipv6 eigrp neighbor

```
sw101
chinesedumps-sw101#
chinesedumps-sw101#
chinesedumps-sw101#sh ipv6 eigrp neighbors
EIGRP-IPv6 VR(ccie) Address-Family Neighbors for AS(65001)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q
Seq
                                                   (sec)         (ms)       Cnt
Num
1   Link-local address:     Gi0/1                    14 00:00:07 1798   5000  0
13
    FE80::12
0   Link-local address:     Gi0/0                    12 00:19:57 1194   5000  0
13
    FE80::11
chinesedumps-sw101#
chinesedumps-sw101#
```


Chinese_dumps_sw101:show ipv6 route eigrp

```
sw101
chinesedumps-sw101#
chinesedumps-sw101#
chinesedumps-sw101#sh ipv6 route eigrp
IPv6 Routing Table - default - 5 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       RL - RPL, la - LISP alt, lr - LISP site-registrations, ld - LISP dyn-eid
       lA - LISP away, a - Application
chinesedumps-sw101#
chinesedumps-sw101#
chinesedumps-sw101#
chinesedumps-sw101#
```

Chinese_dumps_sw101:show run | s router eigrp

```
sw101
chinesedumps-sw101#
chinesedumps-sw101#
chinesedumps-sw101#sh run | s router eigrp
router eigrp ccie
 !
 address-family ipv6 unicast autonomous-system 65001
  !
  af-interface default
   shutdown
  exit-af-interface
  !
  af-interface Vlan2000
   no shutdown
   passive-interface
  exit-af-interface
  !
  af-interface Vlan2001
   no shutdown
   passive-interface
  exit-af-interface
  !
  af-interface GigabitEthernet0/0
   no shutdown
  exit-af-interface
  !
  af-interface GigabitEthernet0/1
   no shutdown
  exit-af-interface
  !
  topology base
  exit-af-topology
 exit-address-family
chinesedumps-sw101#
```

Chinese_dumps_sw102:show ipv6 eigrp neighbor

```
sw102
chinesedumps-sw102#
chinesedumps-sw102#
chinesedumps-sw102#
chinesedumps-sw102#sh ipv6 eigrp neighbors
EIGRP-IPv6 VR(ccie) Address-Family Neighbors for AS(65001)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q
Seq
        www.passenterpriselabs.com                 (sec)         (ms)       Cnt
Num
1   Link-local address:     Gi0/0                    13 00:01:50 1661   5000  0
17
    FE80::12
0   Link-local address:     Gi0/1                    11 00:21:31   13   100  0
14
    FE80::11 www.passenterpriselabs.com
chinesedumps-sw102#
```

Chinese_dumps_sw101:show ipv6 route eigrp

```
sw102
chinesedumps-sw102#
chinesedumps-sw102#   www.passenterpriselabs.com
chinesedumps-sw102#
chinesedumps-sw102#sh ipv6 route eigrp
IPv6 Routing Table - default - 5 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       RL - RPL, la - LISP alt, lr - LISP site-registrations, ld - LISP dyn-eid
       lA - LISP away, a - Application
chinesedumps-sw102#
chinesedumps-sw102#    www.passenterpriselabs.com
chinesedumps-sw102#
chinesedumps-sw102#
```

Chinese_dumps_sw101:show run | s router eigrp

```
sw102
chinesedumps-sw102#sh run | s router eigrp
router eigrp ccie
 !                    www.passenterpriselabs.com
 address-family ipv6 unicast autonomous-system 65001
  !
  af-interface default
   shutdown
  exit-af-interface
  !
  af-interface Vlan2000
   no shutdown
   passive-interface    www.passenterpriselabs.com
  exit-af-interface
  !
  af-interface Vlan2001
   no shutdown
   passive-interface
  exit-af-interface
  !
  af-interface GigabitEthernet0/0
   no shutdown
  exit-af-interface     www.passenterpriselabs.com
  !
  af-interface GigabitEthernet0/1
   no shutdown
  exit-af-interface
  !
  topology base
  exit-af-topology
 exit-address-family
chinesedumps-sw102#
chinesedumps-sw102#   www.passenterpriselabs.com
chinesedumps-sw102#
chinesedumps-sw102#
```

Chinesedumps.com-r11:show ipv6 eigrp neighbor

```
R11
chinesedumps-r11#
chinesedumps-r11#sh ipv6 eigrp neighbors
EIGRP-IPv6 VR(ccie) Address-Family Neighbors for AS(65001)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
     www.passenterpriselabs.com                    (sec)         (ms)       Cnt Num
2   Link-local address:     Gi0/1                    11 00:09:44   15   150  0  15
    FE80::12
1   Link-local address:     Gi0/3                    11 00:31:36   32   192  0  6
    FE80::101
0   Link-local address:     Gi0/2                    12 00:31:37   16   100  0  6
    FE80::102       www.passenterpriselabs.com
chinesedumps-r11#
chinesedumps-r11#
```

Chinesedumps.com-r11:show ipv6 route eigrp

```
R11
chinesedumps-r11#sh ipv6 route eigrp      www.passenterpriselabs.com
IPv6 Routing Table - default - 4 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       RL - RPL, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       la - LISP alt, lr - LISP site-registrations, ld - LISP dyn-eid
       lA - LISP away, a - Application
D   2001:DB8:1:100::/64 [90/15360]
     via FE80::102, GigabitEthernet0/2
     via FE80::101, GigabitEthernet0/3
D   2001:DB8:1:101::/64 [90/15360]        www.passenterpriselabs.com
     via FE80::102, GigabitEthernet0/2
     via FE80::101, GigabitEthernet0/3
chinesedumps-r11#
```

Chinesedumps.com-r11:show run | s router eigrp

```
R11
chinesedumps-r11#sh run | s router eigrp
router eigrp ccie
 !                  www.passenterpriselabs.com
 address-family ipv6 unicast autonomous-system 65001
  !
  af-interface default
   shutdown
  exit-af-interface
  !                  www.passenterpriselabs.com
  af-interface GigabitEthernet0/2
   no shutdown
  exit-af-interface
  !
  af-interface GigabitEthernet0/1
   no shutdown
  exit-af-interface
  !                  www.passenterpriselabs.com
  af-interface GigabitEthernet0/3
   no shutdown
  exit-af-interface
  !
  topology base
  exit-af-topology www.passenterpriselabs.com
 exit-address-family
chinesedumps-r11#
```

Chinesedumps.com-r12:show ipv6 eigrp neighbor

```
R12
chinesedumps-r12#sh ipv6 eigrp neighbors
EIGRP-IPv6 VR(ccie) Address-Family Neighbors for AS(65001)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
    www.passenterpriselabs.com                     (sec)         (ms)       Cnt Num
2   Link-local address:     Gi0/3                    14 00:11:39   15   100  0  8
    FE80::102
1   Link-local address:     Gi0/1                    14 00:11:42    9   100  0  16
    FE80::11
0   Link-local address:     Gi0/2                    11 00:11:42   21   126  0  8
    FE80::101
chinesedumps-r12#
chinesedumps-r12#
chinesedumps-r12#   www.passenterpriselabs.com
chinesedumps-r12#
chinesedumps-r12#
```

Chinesedumps.com-r11:show ipv6 route eigrp

```
R12
chinesedumps-r12#
chinesedumps-r12#sh ipv6 route eigrp     www.passenterpriselabs.com
IPv6 Routing Table - default - 4 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       RL - RPL, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       la - LISP alt, lr - LISP site-registrations, ld - LISP dyn-eid
       lA - LISP away, a - Application
D   2001:DB8:1:100::/64 [90/15360]
     via FE80::101, GigabitEthernet0/2
     via FE80::102, GigabitEthernet0/3
D   2001:DB8:1:101::/64 [90/15360]       www.passenterpriselabs.com
     via FE80::101, GigabitEthernet0/2
     via FE80::102, GigabitEthernet0/3
chinesedumps-r12#
```

Chinesedumps.com-r11:show run | s router eigrp

```
R12
chinesedumps-r12#
chinesedumps-r12#sh run | s router eigrp
router eigrp ccie
 !                  www.passenterpriselabs.com
 address-family ipv6 unicast autonomous-system 65001
  !
  af-interface default
   shutdown
  exit-af-interface
  !                 www.passenterpriselabs.com
  af-interface GigabitEthernet0/2
   no shutdown
  exit-af-interface
  !
  af-interface GigabitEthernet0/1
   no shutdown
  exit-af-interface
  !                 www.passenterpriselabs.com
  af-interface GigabitEthernet0/3
   no shutdown
  exit-af-interface
  !
  topology base
  exit-af-topology  www.passenterpriselabs.com
 exit-address-family
chinesedumps-r12#
```

To verify the task:

- As you can see in the above screenshots for sw101 and sw 102 , there are routes advertised in eigrp because only the physical links are advertised in eigrp on r11 and r12
- To get the routes in eigrp on sw101 and sw102 , add the loopback interface on r11 to eigrp (just for testing purpose)

On r11 :

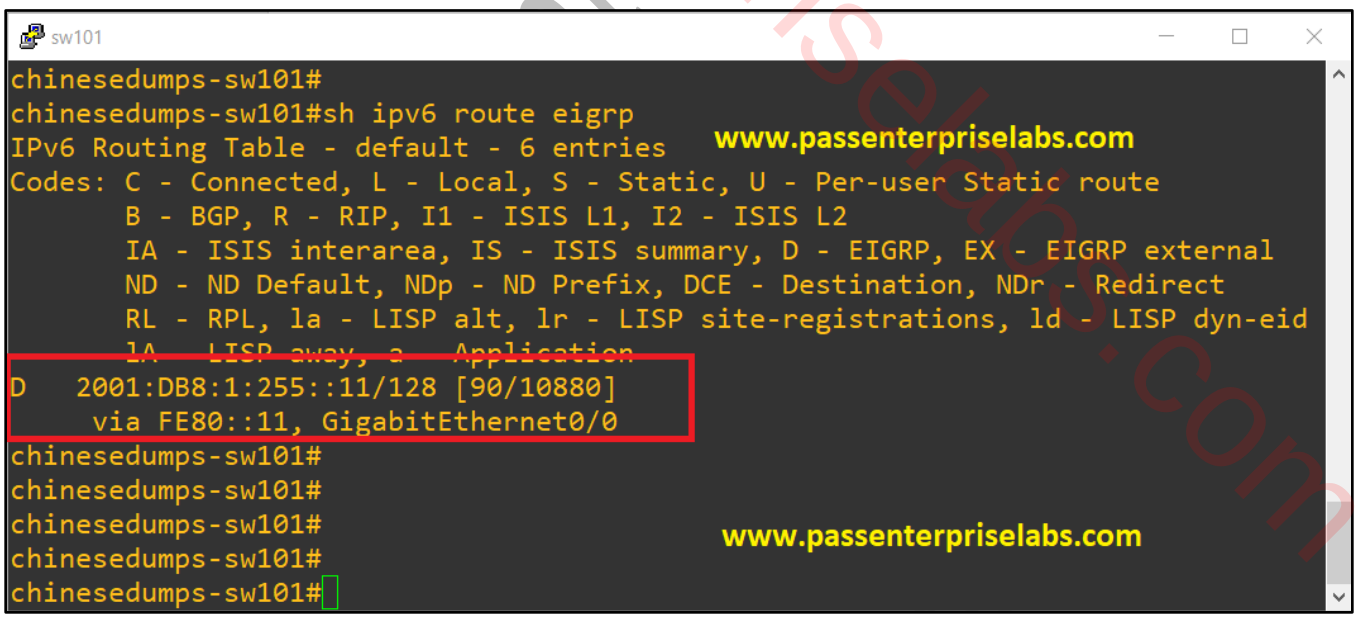
router eigrp ccie

address-family ipv6 unicast autonomous-system 65001

af-interface Loopback0
no shutdown
exit-af-interface

Output:

Sw101:



- In the above output you can see there is a route present in the eigrp routing table

Sw102:

- In the above output you can see there is a route present in the eigrp routing table

NOTE : After testing please remove the loopback 0 on r11 from eigrp

On r11 :

router eigrp ccie

address-family ipv6 unicast autonomous-system 65001

af-interface Loopback0
shutdown
exit-af-interface

1.8: OSPFv2 in DC

Configure devices in the DC according to these requirements:

- Switches sw201 and sw202 must establish a stable OSPF adjacency in the FULL state with vedge21 and vedge22 on interface Vlan3999. Any configuration changes and corrections necessary to meet this requirement may be performed only on the switches, and any mismatched parameters causing the issue must be changed to exactly match the configuration of the vEdges.
- All OSPF speakers in the DC running Cisco IOS and IOS-XE software must be configured to keep the number of advertised internal routes to an absolute minimum while not impacting the reachability of the services. This included the reachability of ISE, DNA center, vManage, vBond and vSmart on their internal (in Band Connectivity) addresses, as well as any existing and future devices in VLAN 4000 on sw201 and sw202. The configuration of this requirement must be completed exclusively within the “router ospf” and “interface vlan” contexts without causing any impact to existing OSPF adjacencies.
- Router r24 must advertise two prefixes, 10.6.0.0/15 and 10.200.0.0/24, as Type-5 LSAs in OSPFv2 to provide HQ and DC with the reachability to the DMVPN tunnel and branches #3 and #4. The configuration of this requirement must be completed exclusively within the “router ospf” context.
- Any route from the 10.2.0.0/16 range that keeps being advertised in OSPF must continue being advertised as an intra-area route.
- It is not allowed to modify existing areas to accomplish this entire task.

4 Points

Solution:

All DC DEVICES except Vedge21 , 22 , vsmart , vbond
---
router ospf 1
prefix-suppression

Chinese_Dumps_sw201, sw202

#conf t
(config)#int vlan 3999
(config-if)#ip mtu 1496

(config)#interface vlan 4000
(config-if)#ip ospf prefix-suppression disable

Chinese_Dumps_ r24

r24#conf t
r24(config)#router ospf 1
r24(config-router)#redistribute eigrp 65006 subnets
r24(config-router)#summary-address 10.6.0.0 255.254.0.0 tag 123

Chinese_Dumps_SW211:

sw211#conf t
sw211(config)#router ospf 1
sw211(config-router)#passive-interface gi1/1
sw211(config-router)#passive-interface gi1/2
sw211(config-router)#passive-interface gi1/3

Chinese_Dumps_SW212:

sw212#conf t
sw212(config)#router ospf 1
sw212(config-router)#passive-interface gi1/1
sw212(config-router)#passive-interface gi1/2

Verification:

Chinese_Dumps_sw201#show ip ospf neighbors

```
sw201
chinesedumps-sw201#
chinesedumps-sw201#sh ip ospf neighbor
                    www.passenterpriselabs.com          www.passenterpriselabs.com
Neighbor ID     Pri   State           Dead Time   Address         Interface
10.1.255.101      1   FULL/DR         00:00:39    10.2.241.2      GigabitEthernet1/2
1.1.2.1           1   FULL/BDR        00:00:39    10.2.201.1      Vlan4000
1.1.2.2           1   FULL/DROTHER    00:00:38    10.2.201.2      Vlan4000
1.99.2.1          1   FULL/BDR        00:00:38    10.2.201.9      Vlan3999
1.99.2.2          1   FULL/DROTHER    00:00:38    10.2.201.10     Vlan3999
10.2.255.211      1   FULL/BDR        00:00:38    10.2.20.2       GigabitEthernet1/1
10.2.255.212      1   FULL/BDR        00:00:38    10.2.23.2       GigabitEthernet1/0
10.2.255.202      1   FULL/DR         00:00:39    10.2.109.2      GigabitEthernet0/3
10.2.255.22       1   FULL/BDR        00:00:38    10.2.12.1       GigabitEthernet0/1
10.2.255.21       1   FULL/BDR        00:00:39    10.2.10.1       GigabitEthernet0/0
chinesedumps-sw201#
```

Chinese_Dumps_sw202#show ip ospf neighbors

```
sw202
chinesedumps-sw202#sh ip os nei
                    www.passenterpriselabs.com
Neighbor ID     Pri   State           Dead Time   Address         Interface
10.1.255.102      1   FULL/DR         00:00:39    10.2.242.2      GigabitEthernet1/2
1.1.2.1           1   FULL/BDR        00:00:37    10.2.202.1      Vlan4000
1.1.2.2           1   FULL/DROTHER    00:00:36    10.2.202.2      Vlan4000
1.99.2.1          1   FULL/BDR        00:00:37    10.2.202.9      Vlan3999
1.99.2.2          1   FULL/DROTHER    00:00:36    10.2.202.10     Vlan3999
10.2.255.212      1   FULL/BDR        00:00:35    10.2.21.2       GigabitEthernet1/1
10.2.255.211      1   FULL/BDR        00:00:38    10.2.22.2       GigabitEthernet1/0
10.2.255.201      1   FULL/BDR        00:00:38    10.2.109.1      GigabitEthernet0/3
10.2.255.21       1   FULL/BDR        00:00:34    10.2.13.1       GigabitEthernet0/1
10.2.255.22       1   FULL/BDR        00:00:39    10.2.11.1       GigabitEthernet0/0
chinesedumps-sw202#   www.passenterpriselabs.com
chinesedumps-sw202#
```

On all IOS and IOS-XE device in DC:

Chinesedumps.com-swXXX#show ip route ospf | in /30

The routes will be suppressed as we have implemented prefix-suppression

To verify the reachability go in HQ on any device and try to ping

Chinese_Dumps_r11#show ip ospf neighbors

```
R11
chinesedumps-r11#sh ip route 10.2.253.1
Routing entry for 10.2.253.0/24
  Known via "ospf 1", distance 110, metric 4, type intra area
  Last update from 10.1.13.2 on GigabitEthernet0/2, 00:26:56 ago
  Routing Descriptor Blocks:
    10.1.13.2, from 10.2.255.212, 00:26:56 ago, via GigabitEthernet0/2
      Route metric is 4, traffic share count is 1
  * 10.1.10.2, from 10.2.255.212, 00:26:56 ago, via GigabitEthernet0/3
      Route metric is 4, traffic share count is 1
chinesedumps-r11#
chinesedumps-r11#
chinesedumps-r11#
chinesedumps-r11#ping 10.2.253.1 so lo 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.253.1, timeout is 2 seconds:
Packet sent with a source address of 10.1.255.11
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 17/25/37 ms
chinesedumps-r11#
chinesedumps-r11#tracero
chinesedumps-r11#traceroute 10.2.253.1
Type escape sequence to abort.
Tracing the route to 10.2.253.1
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.10.2 27 msec
    10.1.13.2 23 msec
    10.1.10.2 21 msec
  2 10.2.242.1 22 msec
    10.2.241.1 18 msec
    10.2.242.1 35 msec
  3 10.2.23.2 24 msec
    10.2.21.2 32 msec *
chinesedumps-r11#
chinesedumps-r11#
```

NOTE : The above subnet that is reachable is of vmanage

1.9: BGP between HQ/DC and service providers

Configure the BGP peerings between HQ/DC and Global SP#1 and Global SP#2 according to these requirements:

- Bring up the BGP peering between HQ r11 and SP#1 r3
- Bring up the BGP peering between DC r21 and SP#1 r3
- Bring up the BGP peering between DC r22 and SP#2
- Ensure that the routes learned over eBGP sessions and further advertised in iBGP will be considered reachable even if the networks on inter-AS links are not advertised in OSPF. The configuration of this requirement must be completed exclusively within the "router bgp" context.
- On r11, r21 and r22 perform mutual redistribution between OSPFv2 and BGP. However, prevent routes that were injected into OSPF from BGP to be reinjected back into BGP. This requirement must be solved on r11, r21 and r22 using only a single route-map on each of the routers and without any reference to ACLs, prefix lists, or route types.
- Prevent HQ and DC from ever communicating through SP#1 r3. All communication between HQ and DC must occur only over the direct sw101/sw201 and sw102/sw202 interconnections. Any other communication must remain unaffected. This requirement must be solved on r21 and r22 by route filtering based on a well-known mandatory attribute without the use of route maps.
- No command may be removed from the configuration on r11 to accomplish this entire task.
- It is allowed to modify existing configuration commands on r21 and r22 to accomplish this entire task.

3 Points

Solution:

Chinesedumps-r11:

```
r11(config)#router bgp 65001
r11(config-router)#address-family ipv4
r11(config-router)#neighbor 100.3.11.1 remote-as 10000
r11(config-router)#neighbor 100.3.11.1 act
r11(config-router)#distance 200 100.3.11.1 0.0.0.0

r11(config)#router ospf 1
r11(config-router)#redistribute bgp 65001 subnets tag 123

r11(config-router)#route-map DENY deny 10
r11(config-router)#match tag 123
r11(config-router)#route-map DENY permit 20

r11(config)#router bgp 65001
r11(config-router)#address-family ipv4
r11(config-router)#redistribute ospf 1 match internal external 1 external 2 route-map DENY
```

Chinesedumps-r21:

```
r21#conf t
r21(config)#route-map DENY deny 10
r21(config-route-map)#match tag 123
r21(config)#route-map DENY permit 20

r21(config)#ip as-path access-list 100 deny _65001$
r21(config)#ip as-path access-list 100 permit .*

r21(config)#router bgp 65002
r21(config-router)#neighbor 100.3.21.1 remote-as 10000
r21(config-router)#neighbor 10.2.255.22 remote-as 65002
r21(config-router)#neighbor 10.2.255.22 next-hop-self
r21(config-router)#neighbor 10.2.255.22 update-source lo0
r21(config-router)#redistribute ospf 1 match internal external 1 external 2 route-map DENY
r21(config-router)#neighbor 100.3.21.1 filter-list 100 in

r21 (config)#router ospf 1
r21 (config-router)#redistribute bgp 65002 subnets tag 123
```

Chinesedumps-r22:

```
r22#conf t

r22(config)#route-map DENY deny 10
r22(config-route-map)#match tag 123
r22(config)#route-map DENY permit 20

r22(config)#router ospf 1
r22(config-router)#redistribute bgp 65002 subnets tag 123

r22(config)#router bgp 65002
r22(config-router)#neighbor 101.22.0.1 remote-as 10001
r22(config-router)#redistribute ospf 1 match internal external 1 external 2 route-map DENY
```

Verification:

Chinese_Dumps_r11#sh bgp ipv4 unicast summary

```
R11
chinesedumps-r11#
chinesedumps-r11#
chinesedumps-r11#  www.passenterpriselabs.com
chinesedumps-r11#
chinesedumps-r11#sh bgp ipv4 unicast  summary
BGP router identifier 10.1.255.11, local AS number 65001
BGP table version is 204, main routing table version 204
27 network entries using 3888 bytes of memory
27 path entries using 2268 bytes of memory
5/5 BGP path/bestpath attribute entries using 800 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 6956 total bytes of memory
BGP activity 78/51 prefixes, 150/123 paths, scan interval 60 secs
                  www.passenterpriselabs.com
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State
/PfxRcd
100.3.11.1      4        10000       0       0        1    0    0 00:11:19 Activ
e
chinesedumps-r11#
```

Chinese_Dumps_r21#sh ip bgp ipv4 unicast summary

```
r21
10.2.255.22     4        65002      36      30       55    0    0 00:16:30
 36
100.3.21.1      4        10000      19      12       55    0    0 00:01:54
  2
                  www.passenterpriselabs.com
chinesedumps-r21#
chinesedumps-r21#sh ip bgp  ipv4 unicast summary
BGP router identifier 10.2.255.21, local AS number 65002
BGP table version is 55, main routing table version 55
40 network entries using 9920 bytes of memory
74 path entries using 10064 bytes of memory
14/8 BGP path/bestpath attribute entries using 4032 bytes of memory
2 BGP AS-PATH entries using 64 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
2 BGP filter-list cache entries using 64 bytes of memory
BGP using 24144 total bytes of memory
BGP activity 40/0 prefixes, 79/5 paths, scan interval 60 secs
40 networks peaked at 07:35:31 May 4 2021 UTC (00:01:48.948 ago)
  www.passenterpriselabs.com                    www.passenterpriselabs.com
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.2.255.22     4        65002      37      30       55    0    0 00:16:39       36
100.3.21.1      4        10000      19      12       55    0    0 00:02:02        2

chinesedumps-r21#
```

Chinese_Dumps_r22# sh ip bgp ipv4 unicast summary

```
r22
chinesedumps-r22#
chinesedumps-r22#   www.passenterpriselabs.com
chinesedumps-r22#sh ip bgp ipv4 unicast summary
BGP router identifier 10.2.255.22, local AS number 65002
BGP table version is 61, main routing table version 61
45 network entries using 11160 bytes of memory
79 path entries using 10744 bytes of memory
15/10 BGP path/bestpath attribute entries using 4320 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 26272 total bytes of memory
BGP activity 47/2 prefixes, 84/5 paths, scan interval 60 secs
45 networks peaked at 07:37:32 May 4 2021 UTC (00:03:24.349 ago)

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.2.255.21     4        65002      34      42       61    0    0 00:20:14        38
101.22.0.1      4        10001       9      17       61    0    0 00:04:34         5

chinesedumps-r22#   www.passenterpriselabs.com
chinesedumps-r22#
```

To verify 4th point, we will create a loopback on r3 (int lo1 – 3.3.3.3/24)

- Create int lo1 with ip address 3.3.3.3/24
- Go on sw101 or sw102 or r12 and check the OSPF routes

```
sw101
chinesedumps-sw101#sh ip route ospf www.passenterpriselabs.com
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
  www.passenterpriselabs.com
Gateway of last resort is not set

      3.0.0.0/24 is subnetted, 1 subnets
O E1     3.3.3.0 [110/3] via 10.2.241.1, 00:00:31, GigabitEthernet0/2
      10.0.0.0/8 is variably subnetted, 35 subnets, 4 masks
O        10.1.11.0/30 [110/2] via 10.1.101.3, 01:19:40, Vlan2001
                      [110/2] via 10.1.100.3, 01:19:40, Vlan2000
                      [110/2] via 10.1.12.1, 01:23:34, GigabitEthernet0/1
O        10.1.13.0/30 [110/2] via 10.1.101.3, 01:19:40, Vlan2001
                      [110/2] via 10.1.100.3, 01:19:40, Vlan2000
                      [110/2] via 10.1.10.1, 01:24:08, GigabitEthernet0/0
O        10.1.99.0/30 [110/2] via 10.1.12.1, 01:23:34, GigabitEthernet0/1
 --More--
```

R12

```
chinesedumps-r12#sh ip route ospf www.passenterpriselabs.com
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
      www.passenterpriselabs.com
Gateway of last resort is not set

      3.0.0.0/24 is subnetted, 1 subnets
O E1     3.3.3.0 [110/4] via 10.1.12.2, 00:00:19, GigabitEthernet0/2
                 [110/4] via 10.1.11.2, 00:00:19, GigabitEthernet0/3
      10.0.0.0/8 is variably subnetted, 33 subnets, 4 masks
O        10.1.10.0/30 [110/2] via 10.1.99.1, 01:51:39, GigabitEthernet0/1
                      [110/2] via 10.1.12.2, 01:51:39, GigabitEthernet0/2
O        10.1.13.0/30 [110/2] via 10.1.99.1, 01:51:39, GigabitEthernet0/1
                      [110/2] via 10.1.11.2, 01:48:27, GigabitEthernet0/3
O        10.1.100.0/24 [110/2] via 10.1.12.2, 01:47:58, GigabitEthernet0/2
                       [110/2] via 10.1.11.2, 01:48:27, GigabitEthernet0/3
 --More--
```

To verify 5th point, we will use the previously created loopback on r3 (int lo1 – 3.3.3.3/24)

- int lo1 with ip address 3.3.3.3/24
- Remove next-hop-self command from r21 for neighbor 10.2.255.22
- For verification go on r22 and check bgp routes

```
r22
chinesedumps-r22#sh bgp ipv4 uni
BGP table version is 178, local router ID is 10.2.255.22
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path, L long-lived-stale
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 * i  3.3.3.3/24       100.3.21.1               0    100      0 10000 i
 * i  10.1.10.0/30     10.2.10.2                3    100      0 ?
 * i  10.1.11.0/30     10.2.13.2                3    100      0 ?
 * i  10.1.12.0/30     10.2.10.2                3    100      0 ?
 * i  10.1.13.0/30     10.2.13.2                3    100      0 ?
 * i  10.1.99.0/30     10.2.13.2                4    100      0 ?
 * i  10.1.100.0/24    10.2.13.2                3    100      0 ?
 * i  10.1.101.0/24    10.2.13.2                3    100      0 ?
 * i  10.1.255.11/32   10.2.13.2                4    100      0 ?
 * i  10.1.255.12/32   10.2.13.2                4    100      0 ?
 * i  10.1.255.101/32  10.2.10.2                3    100      0 ?
 * i  10.1.255.102/32  10.2.13.2                3    100      0 ?
 * i  10.2.10.0/30     10.2.255.21              0    100      0 ?
     Network          Next Hop            Metric LocPrf Weight Path
 * i  10.2.13.0/30     10.2.255.21              0    100      0 ?
```



```
r22
chinesedumps-r22#
chinesedumps-r22#sh ip route bgp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      100.0.0.0/30 is subnetted, 1 subnets
B        100.3.21.0 [200/0] via 100.3.21.1, 00:00:47
      101.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
B        101.40.0.0/30 [20/0] via 101.22.0.1, 00:02:30
B        101.51.0.0/30 [20/0] via 101.22.0.1, 00:02:30
B        101.52.0.0/30 [20/0] via 101.22.0.1, 00:02:30
      111.0.0.0/32 is subnetted, 1 subnets
B        111.111.111.111 [20/0] via 101.22.0.1, 00:02:30
chinesedumps-r22#
```


- From above output you can see the route is just showing as an ibgp route and also it is not present in the routing table of bgp

To get the output as per the requirement

- Add next-hop-self command on r21 for neighbor 10.2.255.22
- Verify with the same commands as above

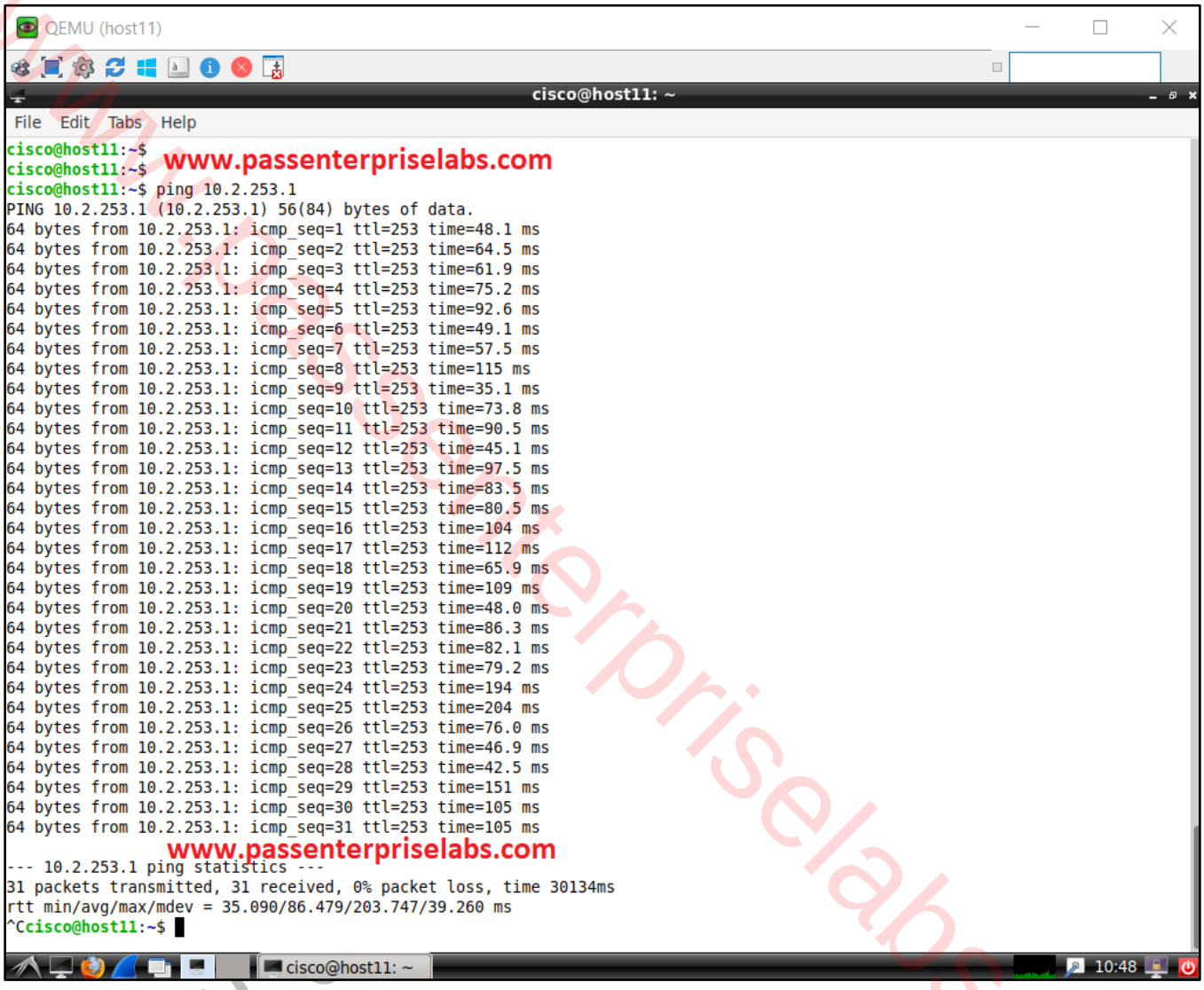
```
r22
chinesedumps-r22#sh ip route bgp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route   www.passenterpriselabs.com
       + - replicated route, % - next hop override, p - overrides from PfR
  www.passenterpriselabs.com
Gateway of last resort is not set

      3.0.0.0/24 is subnetted, 1 subnets
B        3.3.3.0 [200/0] via 100.3.21.1, 00:00:52
      10.0.0.0/8 is variably subnetted, 34 subnets, 4 masks
B        10.2.10.0/30 [200/0] via 10.2.255.21, 00:00:52
B        10.2.13.0/30 [200/0] via 10.2.255.21, 00:00:52  www.passenterpriselabs.com
      101.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
B        101.40.0.0/30 [20/0] via 101.22.0.1, 00:01:59
B        101.51.0.0/30 [20/0] via 101.22.0.1, 00:01:59
 --More--
```

```
r22
chinesedumps-r22#sh bgp ipv4 uni
BGP table version is 45, local router ID is 10.2.255.22
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path, L long-lived-stale,
Origin codes: i - IGP, e - EGP, ? - incomplete   www.passenterpriselabs.com
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>i  3.3.3.0/24       100.3.21.1               0    100      0 10000 i
 * i  10.1.10.0/30     10.2.10.2                3    100      0 ?
 *>                    10.2.99.1                4         32768 ?
 * i  10.1.11.0/30     10.2.13.2                3    100      0 ?
 *>                    10.2.99.1                4         32768 ?
 * i  10.1.12.0/30     10.2.10.2                3    100      0 ?
 *>                    10.2.99.1                4         32768 ?
 * i  10.1.13.0/30     10.2.13.2                3    100      0 ?
 *>                    10.2.99.1                4         32768 ?
 * i  10.1.99.0/30     10.2.13.2                4    100      0 ?
 *>                    10.2.99.1                5         32768 ?
 * i  10.1.100.0/24    10.2.13.2                3    100      0 ?
 *>                    10.2.99.1                4         32768 ?
     Network          Next Hop            Metric LocPrf Weight Path
```


From the above output you can see that the 3.3.3.0 loopback is showing as best route and also it is installed in the routing table.

Note: After performing the verification, please remove the loopback from r3

6th point :



From above output you can see the HQ devices are preferring links between sw101 – sw201 & sw102 – sw202 to reach any subnet in DC

To verify 6th point ,

- Shutdown the link between sw101 – sw201 & sw102 – sw202 and check if you are having reachability to DC subnets via SP-1

From above output you can see the HQ device host 11 cannot reach as the direct link between the switches sw101 – sw201 & sw102 – sw202

1.10: Bringing up VPNv4/VPNv6 in SP#1

Configure routers r3, r4, r5 and r6 in SP#1 according to these requirements:

- Configure r3 through r6 for mutual VPNv4 and VPNv6 route exchange without the use of a route reflector. Use Lo0 IPv4 addresses for peering's.
- Configure r3 through r6 to assign (allocate/bind) as few unique MPLS labels to all existing and future VPNv4 and VPNv6 routes as possible.
- On Routers r3 through r6, prevent any existing and future customer from discovering details about the inner topology of SP#1. It is not allowed to use ACLs to accomplish this requirement.

3 Point

Solution:

Chinesedumps.com-r3:

```
r3>en
r3#conf t
r3(config)#router bgp 10000
r3(config-router)#neighbor 100.255.254.4 remote-as 10000
r3(config-router)#neighbor 100.255.254.4 update-source lo0
r3(config-router)#neighbor 100.255.254.5 remote-as 10000
r3(config-router)#neighbor 100.255.254.5 update-source lo0
r3(config-router)#neighbor 100.255.254.6 remote-as 10000
r3(config-router)#neighbor 100.255.254.6 update-source lo0
r3(config-router)#address-family vpnv4
r3(config-router)#neighbor 100.255.254.4 activate
r3(config-router)#neighbor 100.255.254.5 activate
r3(config-router)#neighbor 100.255.254.6 activate
r3(config-router)#address-family vpnv6
r3(config-router)#neighbor 100.255.254.4 activate
r3(config-router)#neighbor 100.255.254.5 activate
r3(config-router)#neighbor 100.255.254.6 activate
```

Chinesedumps.com-r4:

```
r4>en
r4#conf t
r4(config)#router bgp 10000
r4(config-router)#neighbor 100.255.254.3 remote-as 10000
r4(config-router)#neighbor 100.255.254.3 update-source lo0
r4(config-router)#neighbor 100.255.254.5 remote-as 10000
r4(config-router)#neighbor 100.255.254.5 update-source lo0
r4(config-router)#neighbor 100.255.254.6 remote-as 10000
r4(config-router)#neighbor 100.255.254.6 update-source lo0
r4(config-router)#address-family vpnv4
r4(config-router)#neighbor 100.255.254.3 activate
r4(config-router)#neighbor 100.255.254.5 activate
r4(config-router)#neighbor 100.255.254.6 activate
r4(config-router)#address-family vpnv6
r4(config-router)#neighbor 100.255.254.3 activate
r4(config-router)#neighbor 100.255.254.5 activate
r4(config-router)#neighbor 100.255.254.6 activate
```

Chinesedumps.com-r5:

```
r5>en
r5#conf t
r5(config)#router bgp 10000
r5(config-router)#neighbor 100.255.254.3 remote-as 10000
r5(config-router)#neighbor 100.255.254.3 update-source lo0
r5(config-router)#neighbor 100.255.254.4 remote-as 10000
r5(config-router)#neighbor 100.255.254.4 update-source lo0
r5(config-router)#neighbor 100.255.254.6 remote-as 10000
r5(config-router)#neighbor 100.255.254.6 update-source lo0
r5(config-router)#address-family vpnv4
r5(config-router)#neighbor 100.255.254.3 activate
r5(config-router)#neighbor 100.255.254.4 activate
r5(config-router)#neighbor 100.255.254.6 activate
r5(config-router)#address-family vpnv6
r5(config-router)#neighbor 100.255.254.3 activate
r5(config-router)#neighbor 100.255.254.4 activate
r5(config-router)#neighbor 100.255.254.6 activate
```

Chinesedumps.com-r6:

```
r6>en
r6#conf t
r6(config)#router bgp 10000
r6(config-router)#neighbor 100.255.254.3 remote-as 10000
r6(config-router)#neighbor 100.255.254.3 update-source lo0
r6(config-router)#neighbor 100.255.254.4 remote-as 10000
r6(config-router)#neighbor 100.255.254.4 update-source lo0
r6(config-router)#neighbor 100.255.254.5 remote-as 10000
r6(config-router)#neighbor 100.255.254.5 update-source lo0
r6(config-router)#address-family vpnv4
r6(config-router)#neighbor 100.255.254.3 activate
r6(config-router)#neighbor 100.255.254.4 activate
r6(config-router)#neighbor 100.255.254.5 activate
r6(config-router)#address-family vpnv6
r6(config-router)#neighbor 100.255.254.3 activate
r6(config-router)#neighbor 100.255.254.4 activate
r6(config-router)#neighbor 100.255.254.5 activate
```

On all routers r3, r4, r5, r6

```
#conf t
#mpls label mode all-vrfs protocol bgp-vpnv4 per-vrf
#mpls label mode all-vrfs protocol bgp-vpnv6 per-vrf
#no mpls ip propagate-ttl forwarded
```

Verification:

Chinesedumps.com-r3#sh bgp vpnv4 unicast all summary

```
chinesedumps-r3#sh bgp vpnv4 unicast all  summary
BGP router identifier 100.255.254.3, local AS number 10000
BGP table version is 166, main routing table version 166
50 network entries using 12800 bytes of memory
65 path entries using 8840 bytes of memory
23/12 BGP path/bestpath attribute entries using 6992 bytes of memory
4 BGP AS-PATH entries using 112 bytes of memory
1 BGP extended community entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 28768 total bytes of memory
BGP activity 67/17 prefixes, 156/91 paths, scan interval 60 secs
50 networks peaked at 11:05:01 May 4 2021 UTC (00:15:08.660 ago)

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
100.3.11.2      4        65001     251     276      166    0    0 03:45:18       15
100.3.21.2      4        65002     325     282      166    0    0 03:44:52       36
100.255.254.4   4        10000      10      20      166    0    0 00:04:55        0
100.255.254.5   4        10000      24      32      166    0    0 00:16:01        3
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
100.255.254.6   4        10000      22      29      166    0    0 00:12:52        3

chinesedumps-r3#
```


Chinesedumps.com-r3#sh bgp vpnv6 unicast all summary


```
chinesedumps-r3#sh bgp vpnv6 unicast all  summary
BGP router identifier 100.255.254.3, local AS number 10000
BGP table version is 1, main routing table version 1
```



```
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
100.255.254.4   4        10000      11      21        1    0    0 00:06:19        0
100.255.254.5   4        10000      26      33        1    0    0 00:17:25        0
100.255.254.6   4        10000      23      31        1    0    0 00:14:12        0
```



```
chinesedumps-r3#
chinesedumps-r3#
chinesedumps-r3#
chinesedumps-r3#
```

Chinesedumps.com-r4#sh bgp vpnv4 unicast all summary

```
chinesedumps-r4# www.passenterpriselabs.com
chinesedumps-r4#sh bgp vpnv4 uni all summ
BGP router identifier 100.255.254.4, local AS number 10000
BGP table version is 3, main routing table version 3
1 network entries using 256 bytes of memory
1 path entries using 136 bytes of memory
1/1 BGP path/bestpath attribute entries using 304 bytes of memory
1 BGP extended community entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 720 total bytes of memory
BGP activity 1/0 prefixes, 1/0 paths, scan interval 60 secs
1 networks peaked at 11:15:08 May 4 2021 UTC (00:00:12.603 ago)
                www.passenterpriselabs.com
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
100.4.30.2      4        65003       0       0        1    0    0 never    Idle
100.255.254.3   4        10000      15       5        3    0    0 00:00:06        0
100.255.254.5   4        10000       7       5        3    0    0 00:00:03        0
100.255.254.6   4        10000       8       5        3    0    0 00:00:12        1

chinesedumps-r4#
chinesedumps-r4# www.passenterpriselabs.com
chinesedumps-r4#
chinesedumps-r4#
```

Chinesedumps.com-r4#sh bgp vpnv6 unicast all summary

```
chinesedumps-r4#
chinesedumps-r4# www.passenterpriselabs.com
chinesedumps-r4#sh bgp vpnv6 uni all summ
BGP router identifier 100.255.254.4, local AS number 10000
BGP table version is 1, main routing table version 1
                www.passenterpriselabs.com
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:DB8:4:30::2
                4        65003       0       0        1    0    0 never    Idle
100.255.254.3   4        10000      19       9        1    0    0 00:03:49        0
100.255.254.5   4        10000      11       8        1    0    0 00:03:46        0
100.255.254.6   4        10000      12       9        1    0    0 00:03:55        0

                www.passenterpriselabs.com
chinesedumps-r4#
chinesedumps-r4#
```

Chinesedumps.com-r5#sh bgp vpnv4 unicast all summary

```
r5
www.passenterpriselabs.com
chinesedumps-r5#sh bgp vpnv4 uni all summ
BGP router identifier 100.255.254.5, local AS number 10000
BGP table version is 101, main routing table version 101
85 network entries using 21760 bytes of memory
85 path entries using 11560 bytes of memory
14/13 BGP path/bestpath attribute entries using 4256 bytes of memory
4 BGP AS-PATH entries using 112 bytes of memory
1 BGP extended community entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 37712 total bytes of memory
BGP activity 85/0 prefixes, 88/3 paths, scan interval 60 secs
85 networks peaked at 11:04:59 May 4 2021 UTC (00:18:46.986 ago)
www.passenterpriselabs.com
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
100.5.61.2      4        65006     198      220      101    0    0 03:09:41        1
100.255.254.3   4        10000      35       28      101    0    0 00:19:37       38
100.255.254.4   4        10000      13       15      101    0    0 00:08:28        0
100.255.254.6   4        10000      30       28      101    0    0 00:18:46        3
www.passenterpriselabs.com
chinesedumps-r5#
chinesedumps-r5#
chinesedumps-r5#
```

Chinesedumps.com-r5#sh bgp vpnv6 unicast all summary

```
r5
chinesedumps-r5#
chinesedumps-r5#
chinesedumps-r5#  www.passenterpriselabs.com
chinesedumps-r5#
chinesedumps-r5#sh bgp vpnv6 unicast all summary
BGP router identifier 100.255.254.5, local AS number 10000
BGP table version is 1, main routing table version 1
                  www.passenterpriselabs.com
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
100.255.254.3   4        10000      16       9        1    0    0 00:02:58        0
100.255.254.4   4        10000       7       6        1    0    0 00:00:09        0
100.255.254.6   4        10000      11      10        1    0    0 00:02:24        0
                www.passenterpriselabs.com
chinesedumps-r5#
```

Chinesedumps.com-r6#sh bgp vpnv4 unicast all summary

```
chinesedumps-r6#
chinesedumps-r6#  www.passenterpriselabs.com
chinesedumps-r6#sh bgp vpnv4 unicast all summary
BGP router identifier 100.255.254.6, local AS number 10000
BGP table version is 86, main routing table version 86
76 network entries using 19456 bytes of memory
76 path entries using 10336 bytes of memory
11/11 BGP path/bestpath attribute entries using 3344 bytes of memory
3 BGP AS-PATH entries using 88 bytes of memory
2 BGP extended community entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 33272 total bytes of memory
BGP activity 76/0 prefixes, 80/4 paths, scan interval 60 secs
76 networks peaked at 09:11:52 May 5 2021 UTC (00:02:28.375 ago)
           www.passenterpriselabs.com
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
100.6.62.2      4        65006       0       0        1    0    0 never    Idle
100.6.70.2      4        65007       0       0        1    0    0 never    Active
100.255.254.3   4        10000      19      11       86    0    0 00:04:59        34
100.255.254.4   4        10000       9      10       86    0    0 00:02:28         1
100.255.254.5   4        10000      12      14       86    0    0 00:04:42         2
                    www.passenterpriselabs.com
chinesedumps-r6#
```

Chinesedumps.com-r6#sh bgp vpnv6 unicast all summary

```
   www.passenterpriselabs.com
chinesedumps-r6#sh bgp vpnv6 unicast all summary
BGP router identifier 100.255.254.6, local AS number 10000
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
100.255.254.3   4        10000       0       0        1    0    0 never    (NoNeg)
100.255.254.4   4        10000      11      12        1    0    0 00:03:48        0
100.255.254.5   4        10000      14      15        1    0    0 00:06:02        0
   www.passenterpriselabs.com
chinesedumps-r6#
```

1.11: Fixing Broken DMVPN between Dc and Branches #3 and #4

Correct the configuration issues resulting in broken DMVPN tunnel connectivity between DC, Branch3 and Branch4 according to these requirements:

- The DMVPN must operate in IPSec-protected phase 3 mode.
- Using the FVRF approach, safeguard the DMVPN operation against any potential recursive routing issues involving the tunnel.
- Do not create any new VRFs.
- Do not change the tunnel source commands on Tunnel interfaces.
- On Spokes, do not add new BGP neighbors; reuse those that are currently up while changing their VRF membership as needed.
- It is not allowed to modify configuration on DC r24 to complete this entire task.

3 Point

Solution:

Chinesedumps.com-r61:

```
r61>en
r61#conf t
r61(config)#int lo 0
r61(config-if)#vrf forwarding WAN
r61(config-if)#ip address 10.6.255.61 255.255.255.255

r61(config)#int g0/0
r61(config-if)#vrf forwarding WAN
r61(config-if)#ip address 100.5.61.2 255.255.255.252

r61(config)#router bgp 65006
r61(config-router)#address-family ipv4 vrf WAN
r61(config-router)#network 10.6.255.61 mask 255.255.255.255
r61(config-router)#neighbor 100.5.61.1 remote-as 10000
r61(config-router)#neighbor 100.5.61.1 act

r61(config)#interface tunnel 0
r61(config-if)#no  ip nhrp map 10.2.255.24 10.200.0.1
r61(config-if)#ip nhrp map 10.200.0.1 10.2.255.24
r61(config-if)#no ip nhrp redirect
r61(config-if)#ip nhrp shortcut
r61(config-if)#tunnel vrf WAN
r61(config-if)#ip mtu 1440

r61(config)#crypto isakmp policy 10
r61(config)#no hash md5
r61(config)#no crypto isakmp key cisco address 0.0.0.0
r61(config)#crypto keyring KR vrf WAN
r61(config)#pre-shared-key address 0.0.0.0 0.0.0.0 key cisco
r61(config)#crypto ipsec profile prof
```


```
r61(config)#router eigrp ccie
r61(config-router)#address-family ipv4 unicast autonomous-system 65006
r61(config-af-interface)#af-interface default
r61(config-af-interface)#passive-interface
r61(config-router)#exit-af-interface
r61(config-af-interface)#af-interface Tunnel0
r61(config-af-interface)#no passive-interface
r61(config-af-interface)#exit-af-interface
```

Chinesedumps.com-r62:

```
r62>en
r62#conf t
r62(config)#int lo 0
r62(config-if)#vrf forwarding WAN
r62(config-if)#ip address 10.6.255.62 255.255.255.255

r62(config)#int g0/0
r62(config-if)#vrf forwarding WAN
r62(config-if)#ip address 100.6.62.2 255.255.255.252
r62(config-if)#router bgp 65006
r62(config-if)#address-family ipv4 vrf WAN
r62(config-if)#network 10.6.255.62 mask 255.255.255.255
r62(config-if)#neighbor 100.6.62.1 remote-as 10000

r62(config)#int tunnel 0
r62(config-if)#no  ip nhrp map 10.2.255.24 10.200.0.1
r62(config-if)#ip nhrp map 10.200.0.1 10.2.255.24
r62(config-if)#no ip nhrp redirect
r62(config-if)#ip nhrp network-id 1010
r62(config-if)#tunnel vrf WAN
r62(config-if)#ip mtu 1440
r62(config-if)#ip nhrp shortcut


r62(config)#crypto isakmp policy 10
r62(config)#no hash md5
r62(config)#no crypto isakmp key cisco address 0.0.0.0
r62(config)#crypto keyring KR vrf WAN
r62(config)#pre-shared-key address 0.0.0.0 0.0.0.0 key cisco
r62(config)#crypto ipsec profile prof
```


```
r61(config)#router eigrp ccie
r61(config-router)#address-family ipv4 unicast autonomous-system 65006
r61(config-af-interface)#af-interface default
r61(config-af-interface)#passive-interface
r61(config-router)#exit-af-interface
r61(config-af-interface)#af-interface Tunnel0
r61(config-af-interface)#no passive-interface
r61(config-af-interface)#exit-af-interface
```

Chinesedumps.com-r70:

```
r70>en
r70#conf t
r70(config)#int tunnel 0
r70(config-if)#tunnel vrf WAN
r70(config-if)#ip mtu 1440
r70(config-if)#no ip nhrp redirect
r70(config-if)#ip nhrp shortcut

r70(config)#crypto isakmp policy 10
r70(config)#no hash md5
r70(config)#crypto ipsec profile prof



r70(config)#router eigrp ccie
r70(config-router)#address-family ipv4 unicast autonomous-system 65006
r70(config-router)#af-interface Tunnel0
r70(config-af-interface)#no passive-interface
r70(config-router)#exit-af-interface
```

Solution Steps:

Match the crypto configs on r24 and then configure the spokes (r70 , r61 ,r62)

Faults On Spoke :

1. Hashing needs to be removed on spokes as there is no hash configured on r24 in pre-configuration

crypto isakmp policy 10
no hash md5

2.

a. On r24 legacy key is configured
b. on spokes we will need to complete the key ring configuration for isakmp

crypto keyring KR vrf WAN
pre-shared-key address 0.0.0.0 0.0.0.0 key cisco

3. The DMVPN must operate in IPSec-protected phase 3 mode.

a. On hub (r24)" **ip nhrp redirect** " : - This command says that we are running phase 3 mode
b. On Spokes (r61,r62,r70) " **ip nhrp shortcut** "

Verification:

Chinesedumps.com-r61#sh crypto session

```
chinesedumps-r61#
chinesedumps-r61#
chinesedumps-r61#sh cry sess
chinesedumps-r61#sh cry session
Crypto session current status

Interface: Tunnel0
Profile: IPSEC-PROF
Session status: UP-ACTIVE
Peer: 10.2.255.24 port 500
  Session ID: 0
  IKEv1 SA: local 10.6.255.61/500 remote 10.2.255.24/500 Active
  IPSEC FLOW: permit 47 host 10.6.255.61 host 10.2.255.24
        Active SAs: 2, origin: crypto map

chinesedumps-r61#
chinesedumps-r61#
chinesedumps-r61#
```


Chinesedumps.com-r61#sh dmvpn

```
chinesedumps-r61#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable, I2 - Temporary
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel0, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 10.2.255.24           10.200.0.1    UP 00:14:15     S

chinesedumps-r61#
```

Chinesedumps.com-r61#sh ip eigrp neighbor

```
EIGRP-IPv4 VR(ccie) Address-Family Neighbors for AS(65006)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q
Seq
                                                   (sec)         (ms)       Cnt
Num
0   10.200.0.1              Tu0                      14 01:55:28  309  1854  0
9
chinesedumps-r61#sh ip eigrp neighbors
EIGRP-IPv4 VR(ccie) Address-Family Neighbors for AS(65006)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
0   10.200.0.1              Tu0                      13 01:55:33  309  1854  0  9
chinesedumps-r61#
```


Chinesedumps.com-r61#sh ip nhrp detail

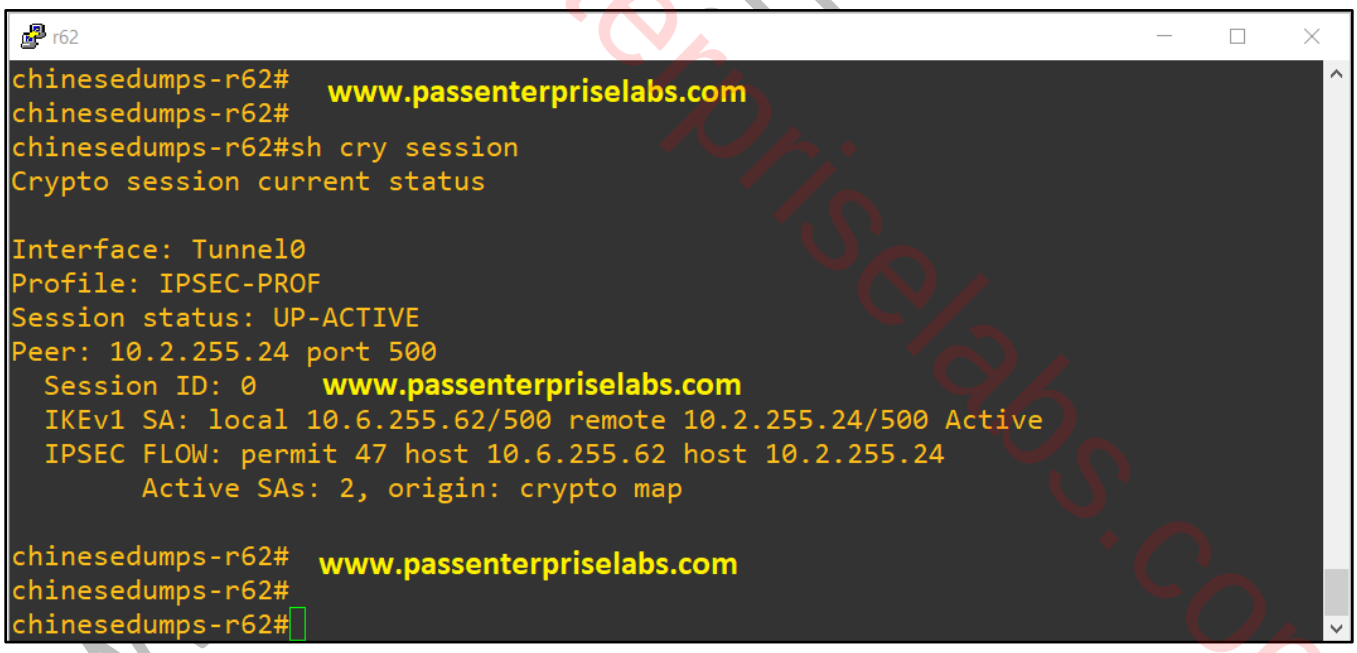
```
chinesedumps-r61#
chinesedumps-r61#
chinesedumps-r61#
chinesedumps-r61#
chinesedumps-r61#sh ip nhrp detail
10.200.0.1/32 via 10.200.0.1
   Tunnel0 created 00:30:01, never expire
   Type: static, Flags: used
   NBMA address: 10.2.255.24
   Preference: 255
chinesedumps-r61#
```


Chinesedumps.com-r61#ping 10.200.0.70

```
chinesedumps-r61#ping 10.200.0.70
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.200.0.70, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 119/209/373 ms
chinesedumps-r61#
chinesedumps-r61#
chinesedumps-r61#traceroute  10.200.0.70
Type escape sequence to abort.
Tracing the route to 10.200.0.70
VRF info: (vrf in name/id, vrf out name/id)
  1 10.200.0.70 99 msec *  36 msec
chinesedumps-r61#
chinesedumps-r61#
chinesedumps-r61#
```

Chinesedumps.com-r61#traceroute 10.200.0.70

Chinesedumps.com-r62#sh crypto session



Chinesedumps.com-r62#sh dmvpn

```
r62
chinesedumps-r62#sh dmvpn www.passenterpriselabs.com
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable, I2 - Temporary
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================
                          www.passenterpriselabs.com
Interface: Tunnel0, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 10.2.255.24           10.200.0.1    UP 00:02:13     S
                          www.passenterpriselabs.com
chinesedumps-r62#
```

Chinesedumps.com-r62#sh ip nhrp detail

```
r62
chinesedumps-r62#  www.passenterpriselabs.com
chinesedumps-r62#
chinesedumps-r62#sh ip nhrp detail
10.200.0.1/32 via 10.200.0.1
   Tunnel0 created 00:32:39, never expire
   Type: static, Flags: used
   NBMA address: 10.2.255.24
   Preference: 255
                          www.passenterpriselabs.com
chinesedumps-r62#
chinesedumps-r62#
chinesedumps-r62#
```

Chinesedumps.com-r70#sh crypto session

```
r70
chinesedumps-r70# www.passenterpriselabs.com
chinesedumps-r70#sh cry session
Crypto session current status

Interface: Tunnel0
Profile: IPSEC-PROF
Session status: UP-ACTIVE
Peer: 10.2.255.24 port 500
  Session ID: 0   www.passenterpriselabs.com
  IKEv1 SA: local 10.7.255.70/500 remote 10.2.255.24/500 Active
  IPSEC FLOW: permit 47 host 10.7.255.70 host 10.2.255.24
        Active SAs: 6, origin: crypto map

chinesedumps-r70#
chinesedumps-r70# www.passenterpriselabs.com
chinesedumps-r70#
chinesedumps-r70#
```

Chinesedumps.com-r70#sh dmvpn

```
r70
chinesedumps-r70#sh dmvpn    www.passenterpriselabs.com
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable, I2 - Temporary
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================
                              www.passenterpriselabs.com
Interface: Tunnel0, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 10.2.255.24          10.200.0.1    UP 00:02:11     S
                              www.passenterpriselabs.com
chinesedumps-r70#
```

Chinesedumps.com-r70#sh ip nhrp detail

```
chinesedumps-r70#
chinesedumps-r70#
chinesedumps-r70#
chinesedumps-r70#sh ip nhrp detail
10.200.0.1/32 via 10.200.0.1
   Tunnel0 created 00:31:23, never expire
   Type: static, Flags: used
   NBMA address: 10.2.255.24
   Preference: 255
chinesedumps-r70#
chinesedumps-r70#
```


Chinesedumps.com-r24#sh ip eigrp neighbor

```
chinesedumps-r24#
chinesedumps-r24#
chinesedumps-r24#sh ip eigrp nei
EIGRP-IPv4 VR(ccie) Address-Family Neighbors for AS(65006)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
2   10.200.0.70             Tu0                      13 01:41:44  166  1476  0  3
1   10.200.0.62             Tu0                      13 02:10:17  413  2478  0  11
0   10.200.0.61             Tu0                      13 02:10:56  187  1476  0  11
chinesedumps-r24#
chinesedumps-r24#
```


Chinesedumps.com-r24#sh ip route eigrp

```
chinesedumps-r24#sh ip route eigrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 44 subnets, 5 masks
D        10.6.10.0/30 [90/76805120] via 10.200.0.61, 02:13:34, Tunnel0
D        10.6.11.0/30 [90/76805120] via 10.200.0.62, 02:12:57, Tunnel0
D        10.6.12.0/30 [90/76805120] via 10.200.0.61, 02:13:34, Tunnel0
D        10.6.13.0/30 [90/76805120] via 10.200.0.62, 02:12:57, Tunnel0
D        10.6.14.14/32 [90/76800640] via 10.200.0.70, 01:44:18, Tunnel0
D        10.6.99.0/30 [90/76805120] via 10.200.0.62, 02:12:57, Tunnel0
                      [90/76805120] via 10.200.0.61, 02:12:57, Tunnel0
chinesedumps-r24#
```

Chinesedumps.com-r24#sh ip nhrp detail

1.12: Tuning EIGRP on DMVPN and DMVPN-enabled Sites

Optimize the DMVPN operation according to these requirements:

- Ensure that Branches #3 and #4 receive only a default route over EIGRP in DMVPN.
- The default route origination must be done on DC r24 without the use of any static routes, redistribution, or route filtering.
- It is not allowed to modify the configuration of r61 and r62 in Branch #3 to accomplish this task;
- It is allowed to add commands to the configuration of r70 in branch #4 to accomplish this task; none of the existing configuration on r70 may be removed to accomplish this task.

Configure sw601 and sw602 at Branch#3 according to these requirements:

- Routers r61 and r62 must not send EIGRP queries to sw601 and sw602.
- Switches sw601 and sw602 must allow advertising any current or future directly connected network to r61 and r62 after the network is added to EIGRP.
- Switches Sw601 and sw602 must continue to propagate the default route received from r61 and r62 to each other. To select the default route, use a prefix list with a “permit”- type entry only.
- Switches sw601 and sw602 must not propagate the default route back to r61 and r62.
- If the prefix list that allows the propagation of selected EIGRP-learned networks between sw601 and sw602 is modified in the future, the same set of networks must be disallowed from being advertised back to r61 and r62 automatically, without any additional commands

3 Points

Solution:

Chinesedumps-r24:

```
r24>en
r24#conf t
r24(config)#router eigrp ccie
r24(config-router)#address-family ipv4 as 65006
r24(config-router)#network 10.200.0.0 0.0.0.255
r24(config-router)#af-interface tunnel 0
r24(config-router)#summary-address 0.0.0.0/0
r24(config-router)#topology base
```

Chinesedumps-r70:

```
r70#conf t
r70(config)#router eigrp ccie
r70(config-router)#address-family ipv4 as 65006
r70(config-router)#af-interface tunnel 0
r70(config-router)#no passive
```

Chinesedumps-sw601# & sw602:

```
sw>en
sw#conf t
sw(config)#ip prefix-list ALLOW-DEF seq 5 permit 0.0.0.0/0
sw(config)#route-map ALLOW-DEF permit 10
sw (config)#match ip address prefix-list ALLOW-DEF

sw (config)##route-map BLOCK-DEF deny 10
sw (config)##match ip address prefix-list ALLOW-DEF
sw (config)##route-map BLOCK-DEF permit 20
```


```
sw (config)#router eigrp ccie
sw (config)#address-family ipv4 unicast autonomous-system 65006
sw (config-router)##eigrp stub connected leak-map ALLOW-DEF
sw (config-router)#af-interface vlan 2000
sw (config-router)#passive
sw (config)#af-interface vlan 2001
sw (config-if)#passive
sw (config-if)#topology base
sw (config-if)#distribute-list route-map BLOCK-DEF out GigabitEthernet0/1
sw (config-if)#distribute-list route-map BLOCK-DEF out GigabitEthernet0/2
```

Verification:

Chinesedumps-r61:

```
r61
chinesedumps-r61#
chinesedumps-r61#   www.passenterpriselabs.com
chinesedumps-r61#
chinesedumps-r61#sh ip route eig
chinesedumps-r61#sh ip route eigrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
                   www.passenterpriselabs.com
Gateway of last resort is 10.200.0.1 to network 0.0.0.0

D*    0.0.0.0/0 [90/76800640] via 10.200.0.1, 00:06:17, Tunnel0
chinesedumps-r61#
chinesedumps-r61#
```

Chinesedumps-r62:

```
r62
chinesedumps-r62#
chinesedumps-r62#   www.passenterpriselabs.com
chinesedumps-r62#sh ip ro ei
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
                   www.passenterpriselabs.com
Gateway of last resort is 10.200.0.1 to network 0.0.0.0

D*    0.0.0.0/0 [90/76800640] via 10.200.0.1, 00:08:08, Tunnel0
chinesedumps-r62#
chinesedumps-r62#
```

Chinesedumps-r70:

```
r70
chinesedumps-r70#
chinesedumps-r70#
chinesedumps-r70#sh ip ro ei
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is 10.200.0.1 to network 0.0.0.0

D*    0.0.0.0/0 [90/76800640] via 10.200.0.1, 00:09:32, Tunnel0
chinesedumps-r70#
chinesedumps-r70#
```


While checking the default route information is present on sw601 & sw602

Chinesedumps-sw601:sh ip route

```
sw601
chinesedumps-sw601#sh ip route
*May  6 05:24:01.914: %SYS-5-CONFIG_I: Configured from console by pel on console
chinesedumps-sw601#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 14 subnets, 3 masks
C        10.6.10.0/30 is directly connected, GigabitEthernet0/2
L        10.6.10.2/32 is directly connected, GigabitEthernet0/2
D        10.6.11.0/30 [90/15360] via 10.6.109.2, 00:00:05, GigabitEthernet0/0
D        10.6.12.0/30 [90/15360] via 10.6.109.2, 00:00:05, GigabitEthernet0/0
C        10.6.13.0/30 is directly connected, GigabitEthernet0/1
L        10.6.13.2/32 is directly connected, GigabitEthernet0/1
C        10.6.100.0/24 is directly connected, Vlan2000
L        10.6.100.2/32 is directly connected, Vlan2000
C        10.6.101.0/24 is directly connected, Vlan2001
L        10.6.101.2/32 is directly connected, Vlan2001
C        10.6.109.0/30 is directly connected, GigabitEthernet0/0
L        10.6.109.1/32 is directly connected, GigabitEthernet0/0
```

Found that r61 was not sending default route on sw601 (same for sw602)

Issue :

- While working performed a check on r61 (sh ip eigrp neighbor)
- Found that there was no neighborship between r61 and sw601 , sw602

- From the above output you can see that sw 601 is only neighbor with sw 602
- To confirm the neighborship issue on r61 : sh run | s router eigrp

- From above output you can see that in eigrp af-interface default is made passive and only tunnel interface is removed from passive state

NOTE : Whenever we make an interface passive in eigrp the router stops sending eigrp messages including Hello messages and the devices need Hello messages for neighborship

- **To resolve the neighborship issue :**

On r61 and r62:

```
router eigrp ccie
 address-family ipv4 unicast autonomous-system 65006
    af-interface GigabitEthernet0/2
       no passive-interface
    exit-af-interface

    af-interface GigabitEthernet0/3
       no passive-interface
    exit-af-interface
```

- After removing the connected interface on r61 and r62 to the downstream switches from passive-interface we are getting the default route information on sw601 and sw602

```
sw601
chinesedumps-sw601#sh ip route www.passenterpriselabs.com
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route  www.passenterpriselabs.com
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 10.6.13.1 to network 0.0.0.0
                          www.passenterpriselabs.com
D*    0.0.0.0/0 [90/76805760] via 10.6.13.1, 00:00:22, GigabitEthernet0/1
                [90/76805760] via 10.6.10.1, 00:00:22, GigabitEthernet0/2
      10.0.0.0/8 is variably subnetted, 16 subnets, 3 masks
C        10.6.10.0/30 is directly connected, GigabitEthernet0/2
L        10.6.10.2/32 is directly connected, GigabitEthernet0/2
D        10.6.11.0/30 [90/15360] via 10.6.109.2, 00:46:17, GigabitEthernet0/0
                      [90/15360] via 10.6.13.1, 00:46:17, GigabitEthernet0/1
D        10.6.12.0/30 [90/15360] via 10.6.109.2, 00:46:17, GigabitEthernet0/0
                      [90/15360] via 10.6.10.1, 00:46:17, GigabitEthernet0/2
C        10.6.13.0/30 is directly connected, GigabitEthernet0/1
 --More--
```

sw602

```
chinesedumps-sw602#sh ip route www.passenterpriselabs.com
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route    www.passenterpriselabs.com
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 10.6.12.1 to network 0.0.0.0

D*    0.0.0.0/0 [90/76805760] via 10.6.12.1, 00:02:34, GigabitEthernet0/1
                [90/76805760] via 10.6.11.1, 00:02:34, GigabitEthernet0/2
      10.0.0.0/8 is variably subnetted, 16 subnets, 3 masks
D        10.6.10.0/30 [90/15360] via 10.6.109.1, 00:48:43, GigabitEthernet0/0
                      [90/15360] via 10.6.12.1, 00:48:43, GigabitEthernet0/1
C        10.6.11.0/30 is directly connected, GigabitEthernet0/2
L        10.6.11.2/32 is directly connected, GigabitEthernet0/2
C        10.6.12.0/30 is directly connected, GigabitEthernet0/1
L        10.6.12.2/32 is directly connected, GigabitEthernet0/1
D        10.6.13.0/30 [90/15360] via 10.6.109.1, 00:48:48, GigabitEthernet0/0
 --More--                        www.passenterpriselabs.com
```

- **To verify "Switches sw601 and sw602 must not propagate the default route back to r61 and r62."**

- Shutdown the interface on r62 that is connected to r6 in SP 1

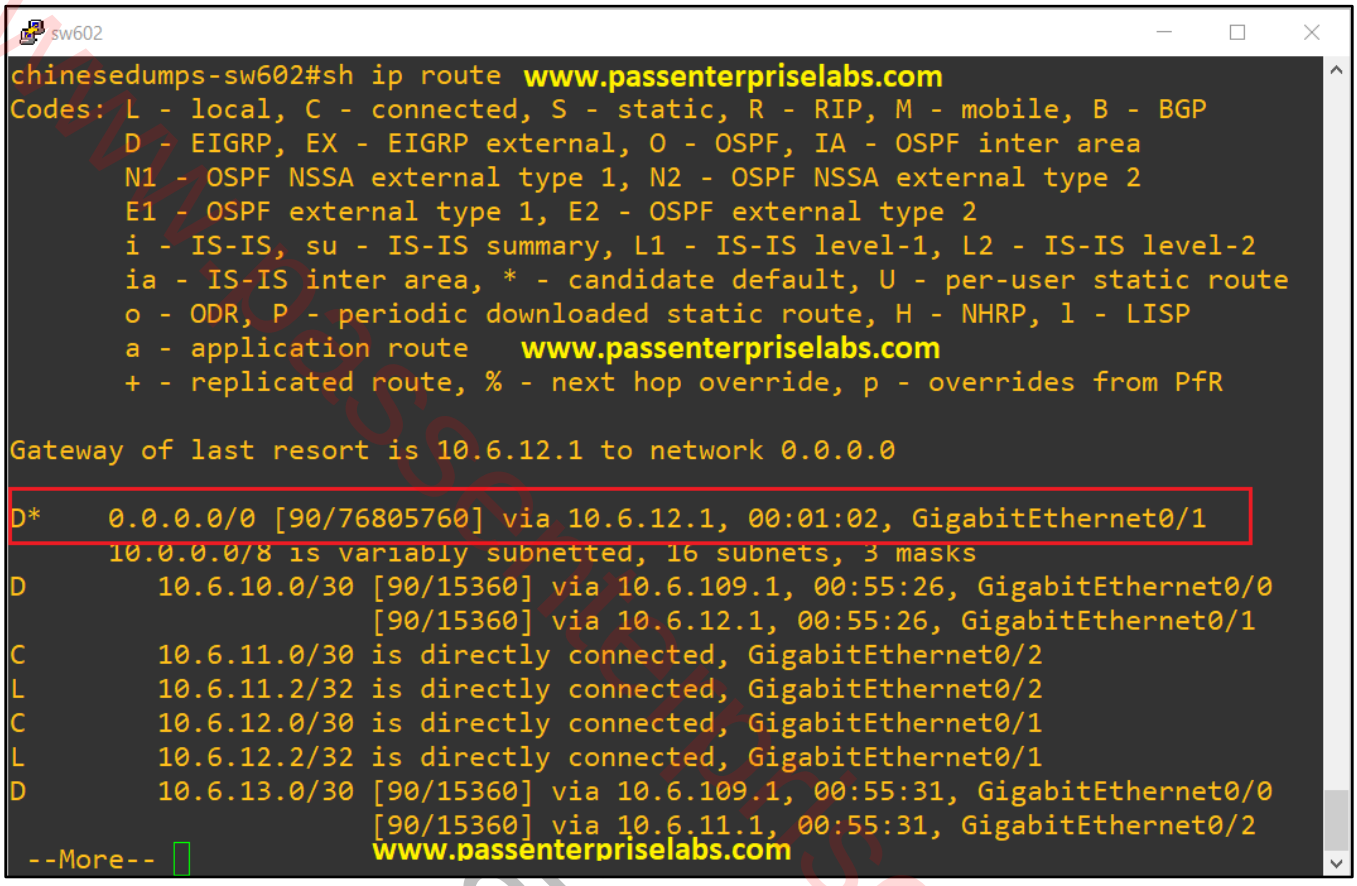
On r62:

Int g0/0
Shutdown

```
r62
chinesedumps-r62#sh ip route www.passenterpriselabs.com
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route www.passenterpriselabs.com
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set
                              www.passenterpriselabs.com
      10.0.0.0/8 is variably subnetted, 15 subnets, 3 masks
D        10.6.10.0/30 [90/15360] via 10.6.13.2, 00:56:57, GigabitEthernet0/2
C        10.6.11.0/30 is directly connected, GigabitEthernet0/3
L        10.6.11.1/32 is directly connected, GigabitEthernet0/3
D        10.6.12.0/30 [90/15360] via 10.6.11.2, 01:00:24, GigabitEthernet0/3
C        10.6.13.0/30 is directly connected, GigabitEthernet0/2
L        10.6.13.1/32 is directly connected, GigabitEthernet0/2
C        10.6.99.0/30 is directly connected, GigabitEthernet0/1
L        10.6.99.2/32 is directly connected, GigabitEthernet0/1
D        10.6.100.0/24 [90/15360] via 10.6.13.2, 00:56:57, GigabitEthernet0/2
 --More--
```

- After shutting down the interface on r62 we can see from the above output that there is no default route in the routing table

- If we check on sw601 or sw602 they should have the default route present in the routing table



1.13: IPv4 Networks on Legacy Branches

On sw211 in DC, complete the DHCP server configuration according to these requirements:

- Create IPv4 DHCP pools named br3_v2000 and br3_v2001 for Branch #3 VLANs 2000 (10.6.100.0/24) and 2001 (10.6.101.0/24) respectively.
- Create IPv4 DHCP pool named br4_v1 for the subnet 10.7.1.0/24 on branch #4.
- In each subnet, assign addresses from .101 up to .254 inclusively, and the appropriate gateway to clients.

On Branch #3, Complete and correct the configuration on switches sw601, sw602 and sw610 to allow HSRP and DHCP relay operation in VLANs 2000 and 2001 according to these requirements:

- HSRP must implicitly use the vMAC address range of 0000.0c9f.f000 through 0000.0c9f.ffff
- The group member must be 100 for VLAN 2000 and 101 for VLAN 2001
- Sw601 must be the Active gateway for VLAN 2000 with a priority of 110; the Active role ownership must be deterministic
- Sw602 must be the Active gateway for VLAN 2001 with a priority of 110; the Active role ownership must be deterministic
- Each active switch must track its uplink interfaces gi0/1 and gi0/2 if either of these interfaces goes down; the active switch must allow the other switch to become Active. However, it is not allowed for the tracking to modify the HSRP priority to accomplish this requirement.
- Both sw601 and sw602 must be configured as DHCP relay agents in both VLANs 2000 and 2001, pointing toward the DHCP server 10.2.255.211 at sw211. However, at any time, only the Active router in the particular VLAN should relay the DHCP messages.
- Place host61 and host62 into VLANs 2000 and 2001, respectively, and make sure they are assigned their correct IPv4 configuration.

It is not permitted to use any kind of scripting to complete this task.

On Branch #4, complete the configuration of the router r70 according to these requirements;

- Assign IP address 10.7.1.1/24 to gi0/2
- Enable DHCP relay on this interface and point it to the DHCP server 10.2.255.211 at sw211
- It is allowed to add one additional missing command to the r70 configuration to allow DHCP clients connected to gi0/2 obtain their IPv4 configuration.
- Make sure that host71 and host72 are assigned their correct IPv4 configuration.

2 Points

Solution:

Chinesedumps.com-sw211:

```
sw211>en
sw211#conf t
sw211(config-dhcp)#ip dhcp excluded-address 10.6.100.1 10.6.100.100
sw211(config)#ip dhcp pool br3_v2000
sw211(config-dhcp)#network 10.6.100.0 /24
sw211(config-dhcp)#default-router 10.6.100.1

sw211(config-dhcp)#ip dhcp excluded-address 10.6.101.1 10.6.101.100
sw211(config)#ip dhcp pool br3_v2001
sw211(config-dhcp)#network 10.6.101.0 /24
sw211(config-dhcp)#default-router 10.6.101.1

sw211(config-dhcp)#ip dhcp excluded-address 10.7.1.1 10.7.1.100
sw211(config)#ip dhcp pool br4_v1
sw211(config-dhcp)#network 10.7.1.0 /24
sw211(config-dhcp)#default-router 10.7.1.1
```

Chinesedumps.com-sw601:

```
sw601>en
sw601#conf t
sw601(config)#int vlan 2000
sw601(config-if)#standby version 2
sw601(config-if)#standby 100 ip 10.6.100.1
sw601(config-if)#standby 100 preempt
sw601(config-if)#standby 100 priority 110
sw601(config-if)#standby 100 track 1 shut
sw601(config-if)#standby 100 track 2 shut
sw601(config-if)#standby 100 name VLAN2K
sw601(config-if)#ip helper-address 10.2.255.211 redundancy VLAN2K

sw601(config)#int vlan 2001
sw601(config-if)#standby 101 ip 10.6.101.1
sw601(config-if)#standby version 2
sw601(config-if)#standby 101 name VLAN2K1
sw601(config-if)#ip helper-address 10.2.255.211 redundancy VLAN2K1
```


```
sw601(config-if)#track 1 interface g0/1 line-protocol
sw601(config-if)#track 2 interface g0/0 line-protocol
```

Chinesedumps.com-sw602:

```
sw602>en
sw602#conf t
sw602 (config)#int vlan 2001
sw602 (config-if)#standby version 2
sw602 (config-if)#no standby 0 ip 10.6.101.1
sw602 (config-if)#standby 101 ip 10.6.101.1
sw602 (config-if)#standby 101 priority 110
sw602 (config-if)#standby 101 preempt
sw602 (config-if)#standby 101 track 1 shut
sw602 (config-if)#standby 101 track 2 shut
sw602 (config-if)#standby 101 name VLAN2K1
sw602 (config-if)#ip helper-address 10.2.255.211 redundancy VLAN2K1

sw602 (config)#int vlan 2000
sw602 (config-if)#standby version 2
sw602 (config-if)#standby 100 ip 10.6.100.1
sw602 (config-if)#standby 100 name VLAN2K
sw602 (config-if)#ip helper-address 10.2.255.211 redundancy VLAN2K

sw602 (config-if)#track 1 interface g0/1 line-protocol
sw602 (config-if)#track 2 interface g0/0 line-protocol
```

Chinesedumps.com-sw610:

```
sw610>en
sw610#conf t
sw610(config-if)#int range g2/0-1
sw610(config-if)#switch trunk allowed vlan add 2001

sw610(config)#int g0/0
sw610(config-if)#switchport mode access
sw610(config-if)#switchport access vlan 2000

sw610(config)#int g0/1
sw610(config-if)#switchport mode access
sw610(config-if)#switchport access vlan 2001
```

Chinesedumps.com-r70:

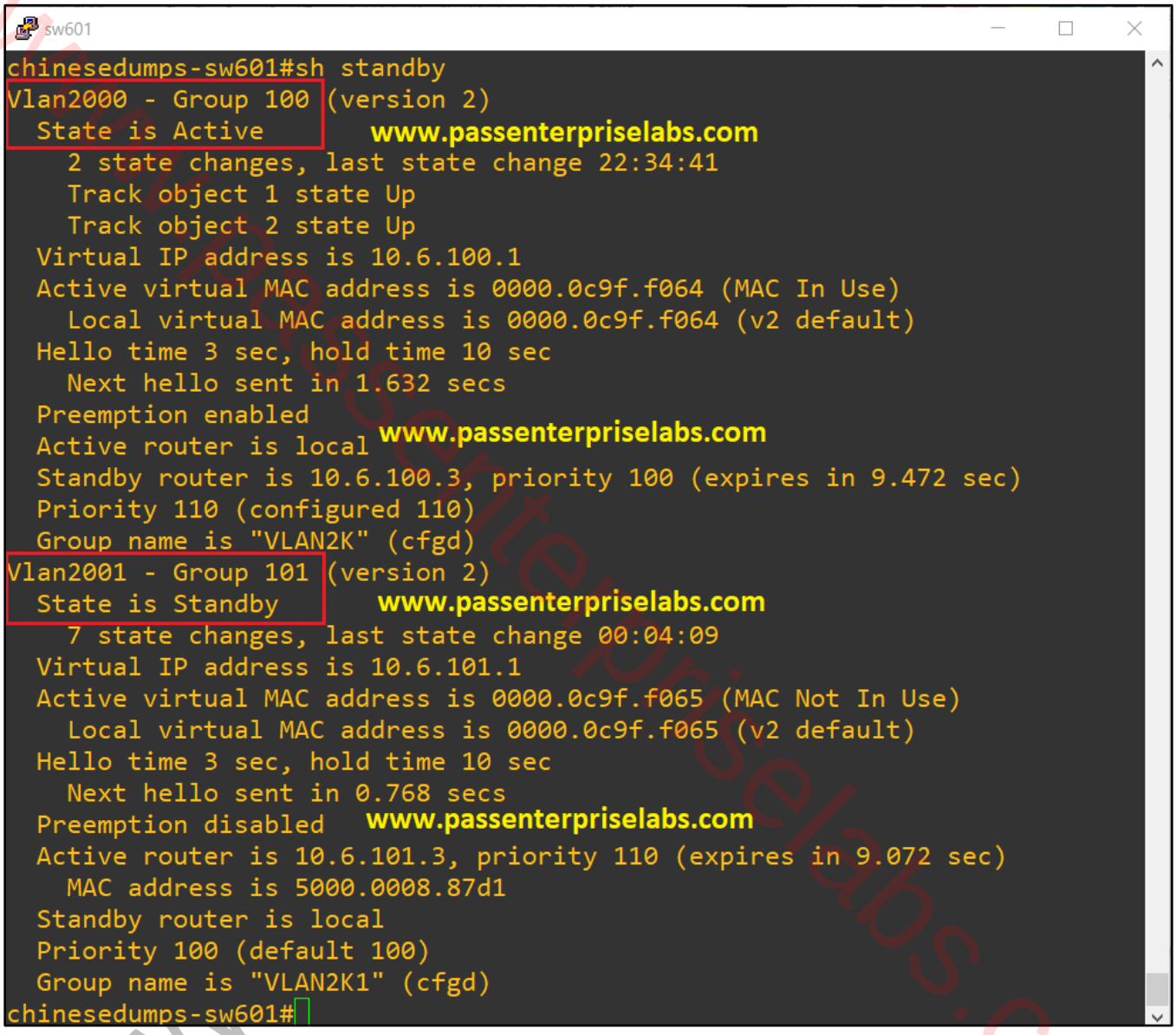
```
r70>en
r70#conf t
r70(config)#interface GigabitEthernet0/2
r70(config-if)#ip address 10.7.1.1 255.255.255.0
r70(config-if)#ip helper-address 10.2.255.211

r70(config)#router eigrp ccie
r70(config-router)#address-family ipv4 unicast autonomous-system 65006
r70(config-router)#network 10.7.1.0 0.0.0.255
```

Verification:

Chinesedumps.com-r211:

```
sw211
chinesedumps-sw211#sh run | s dhcp  www.passenterpriselabs.com
ip dhcp excluded-address 10.1.100.1 10.1.100.100
ip dhcp excluded-address 10.1.101.1 10.1.101.100
ip dhcp excluded-address 10.6.100.1 10.6.100.100
ip dhcp excluded-address 10.6.101.1 10.6.101.100
ip dhcp excluded-address 10.7.1.1 10.7.1.100
ip dhcp pool hq_v2000
 network 10.1.100.0 255.255.255.0
 default-router 10.1.100.1
ip dhcp pool hq_v2001
 network 10.1.101.0 255.255.255.0
 default-router 10.1.101.1          www.passenterpriselabs.com
ip dhcp pool br3_v2000
 network 10.6.100.0 255.255.255.0
 default-router 10.6.100.1
ip dhcp pool br3_v2001
 network 10.6.101.0 255.255.255.0
 default-router 10.6.101.1
ip dhcp pool br4_v1
 network 10.7.1.0 255.255.255.0
 default-router 10.7.1.1
chinesedumps-sw211#                www.passenterpriselabs.com
chinesedumps-sw211#
chinesedumps-sw211#
```

Chinesedumps.com-sw601:

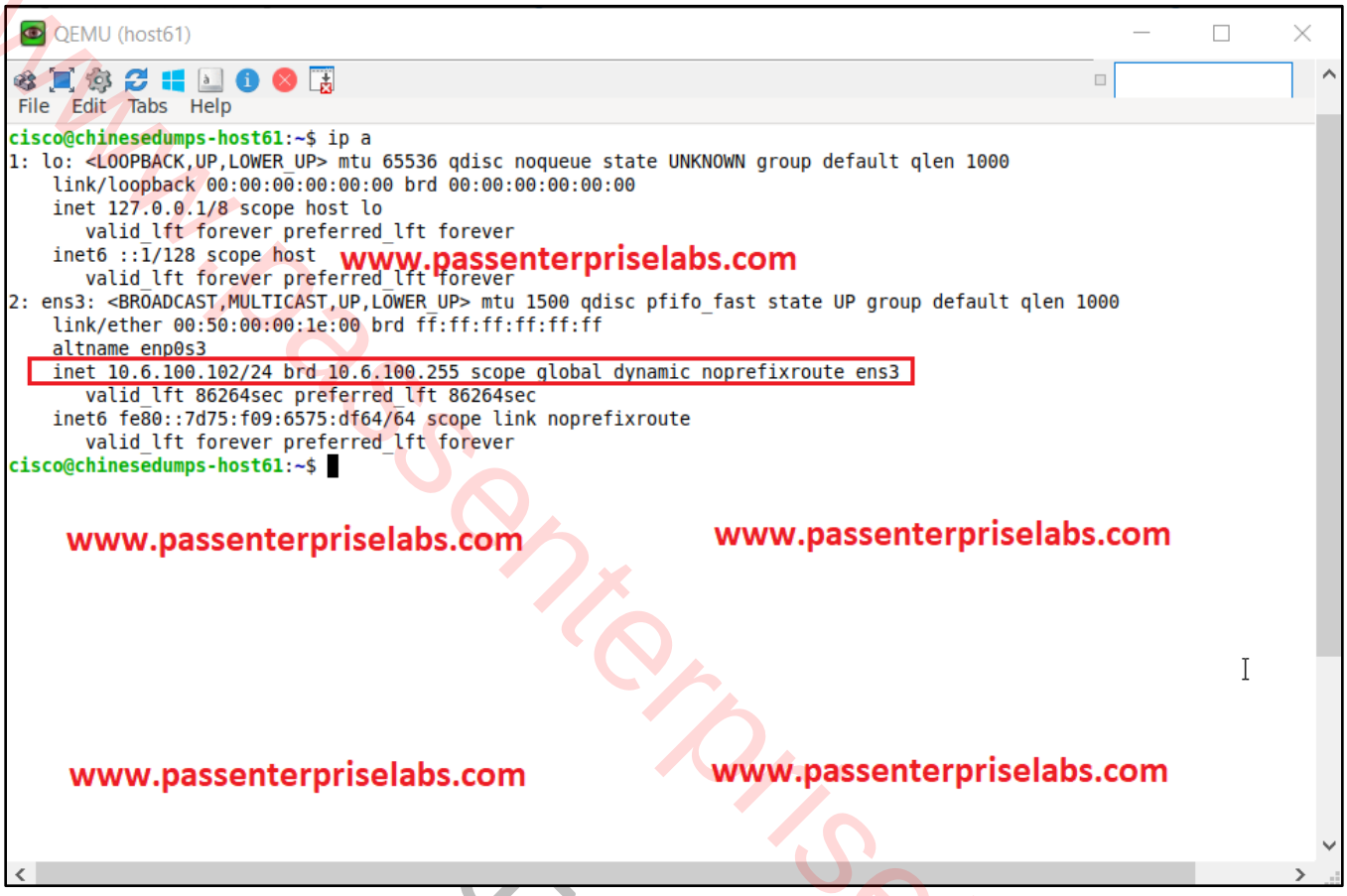


Chinesedumps.com-sw602:

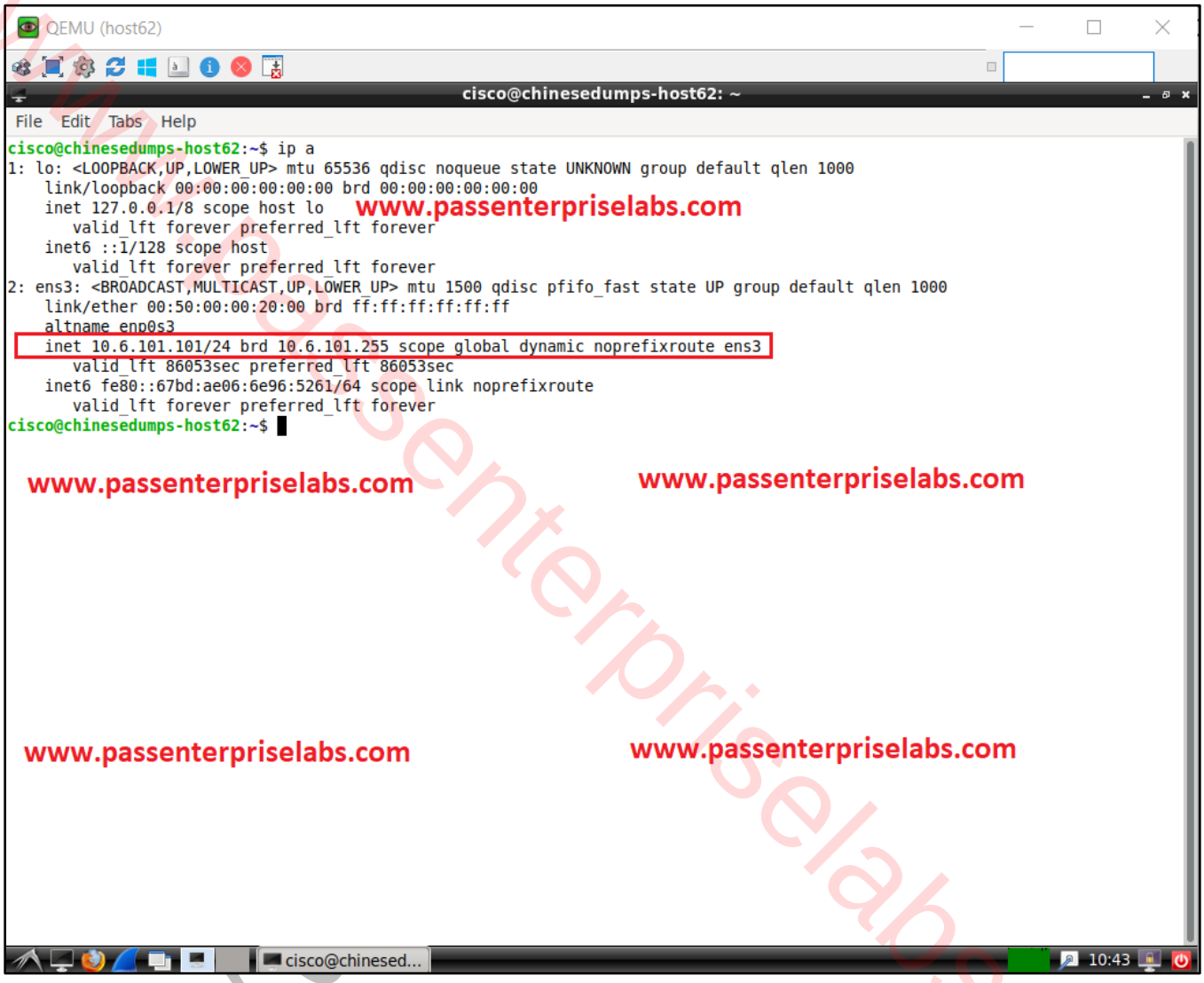
sw602

```
chinesedumps-sw602#sh standby
Vlan2000 - Group 100 (version 2)
  State is Standby          www.passenterpriselabs.com
    7 state changes, last state change 00:00:03
  Virtual IP address is 10.6.100.1
  Active virtual MAC address is 0000.0c9f.f064 (MAC Not In Use)
    Local virtual MAC address is 0000.0c9f.f064 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.016 secs
  Preemption disabled
  Active router is 10.6.100.2, priority 110 (expires in 9.936 sec)
    MAC address is 5000.0007.87d0
  Standby router is local
  Priority 100 (default 100)
  Group name is "VLAN2K" (cfgd)
Vlan2001 - Group 101 (version 2)
  State is Active           www.passenterpriselabs.com
    2 state changes, last state change 00:17:33
    Track object 1 state Up
    Track object 2 state Up
  Virtual IP address is 10.6.101.1
  Active virtual MAC address is 0000.0c9f.f065 (MAC In Use)
    Local virtual MAC address is 0000.0c9f.f065 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.632 secs
  Preemption enabled
  Active router is local
  Standby router is 10.6.101.2, priority 100 (expires in 9.584 sec)
  Priority 110 (configured 110)
  Group name is "VLAN2K1" (cfgd)  www.passenterpriselabs.com
chinesedumps-sw602#
```

Chinesedumps-host61:



Chinesedumps-host62:

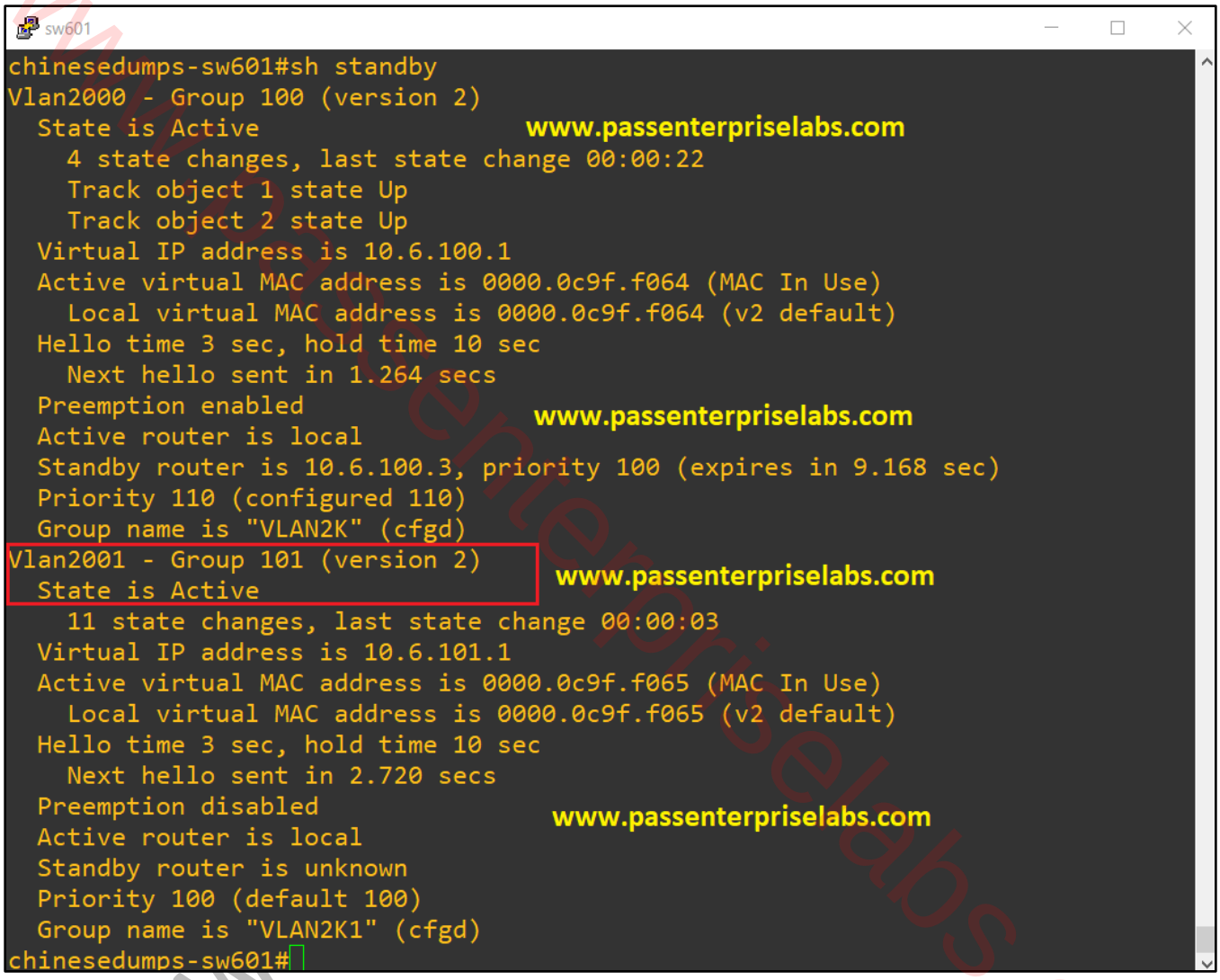


- To verify “Each active switch must track its uplink interfaces gi0/1 and gi0/2/ if either of these interfaces goes down; the active switch must allow the other switch to become Active. However,, it is not allowed for the tracking to modify the HSRP priority to accomplish this requirement. “

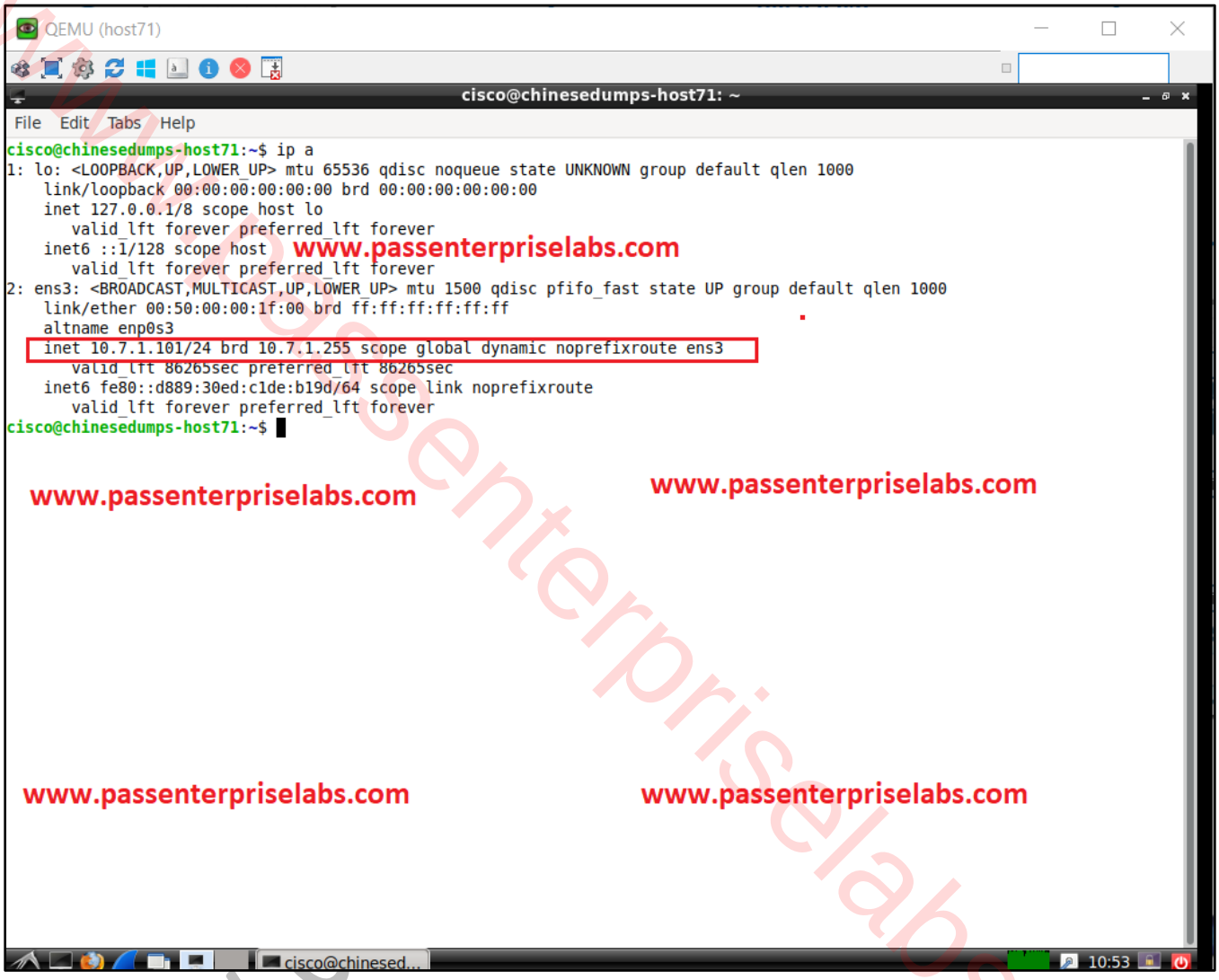
- Go on sw601 and shutdown the interface g0/2 or g0/1 , and then check on sw602 that it should become the gateway now for vlan 2000

```
sw602
chinesedumps-sw602#sh standby
Vlan2000 - Group 100 (version 2)
  State is Active
    11 state changes, last state change 00:02:53
  Virtual IP address is 10.6.100.1
  Active virtual MAC address is 0000.0c9f.f064 (MAC In Use)
    Local virtual MAC address is 0000.0c9f.f064 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.224 secs
  Preemption disabled
  Active router is local
  Standby router is unknown
  Priority 100 (default 100)
  Group name is "VLAN2K" (cfgd)
Vlan2001 - Group 101 (version 2)
  State is Active
    2 state changes, last state change 01:23:54
    Track object 1 state Up
    Track object 2 state Up
  Virtual IP address is 10.6.101.1
  Active virtual MAC address is 0000.0c9f.f065 (MAC In Use)
    Local virtual MAC address is 0000.0c9f.f065 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.584 secs
  Preemption enabled
  Active router is local
  Standby router is 10.6.101.2, priority 100 (expires in 8.832 sec)
  Priority 110 (configured 110)
  Group name is "VLAN2K1" (cfgd)
chinesedumps-sw602#
```

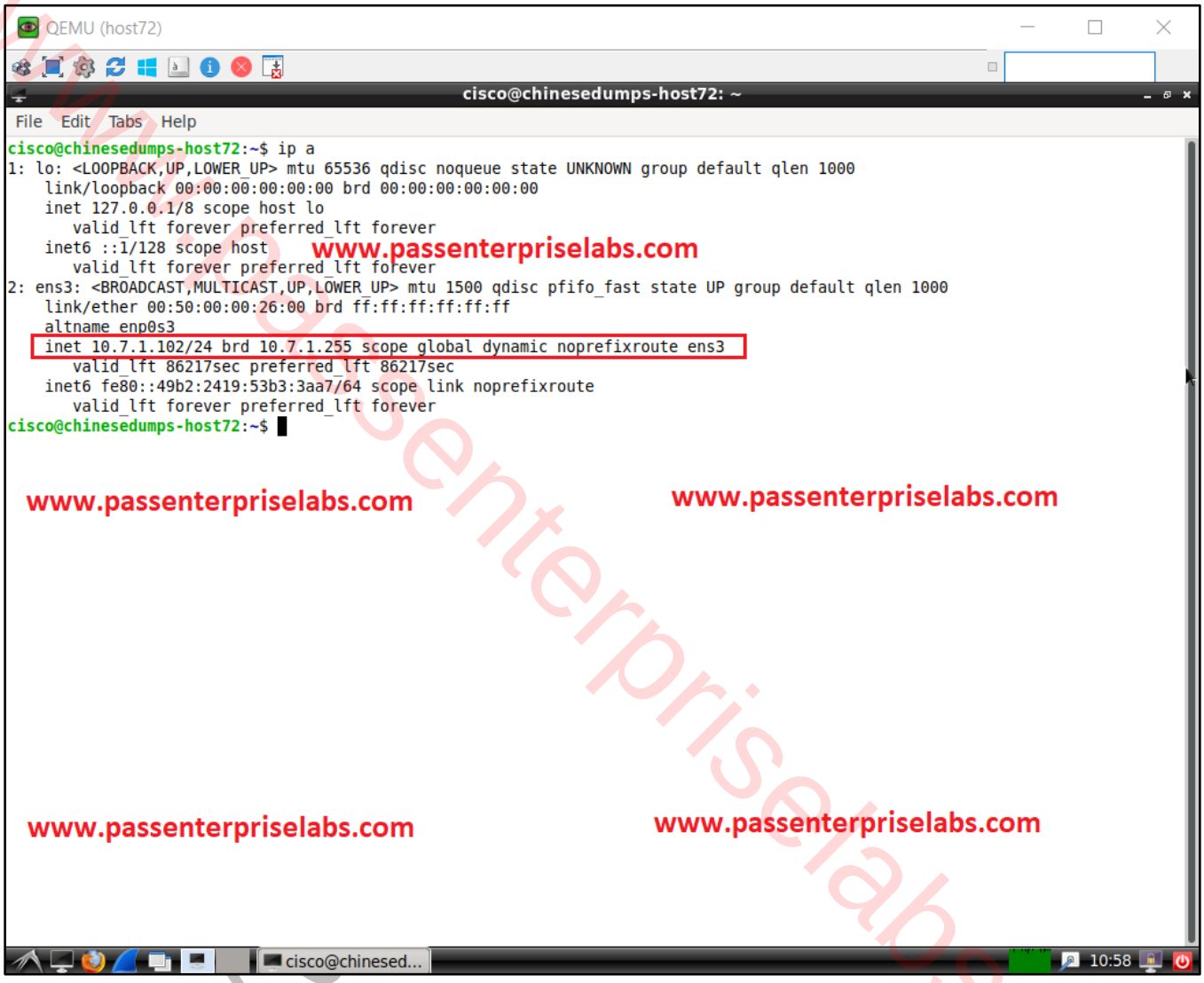
- Go on sw602 and shutdown the interface g0/2 or g0/1, and then check on sw601 that it should become the gateway now for vlan 2001



Chinesedumps-host71:



Chinesedumps-host72:



1.14: Multicast in FABD2

FABD2 is preparing to enable PIM Sparse mode multicast routing in its network. As a part of validating the runbooks, FABD2 requires a sanity check to prevent inappropriate use of multicast-related configuration commands on different router types:

- First Hop Routers – routers where multicast sources are connected
- Last Hop Routers- routers where multicast receivers (subscribers) are connected
- Intermediary Hop Routers- routers on the path between First Hop and Last Hop routers

In the Table below, for each configuration command, select all router type where the use of the command is appropriate. (Select all that apply)

Command	Router Type		
	First Hop Router	Intermediary Hop Router	Last Hop Router
ip pim register-source	☐	☐	☐
ip igmp version	☐	☐	☐
ip pim spt-threshold	☐	☐	☐
ip pim rp-address	☐	☐	☐
ip pim sparse-mode	☐	☐	☐

2 points

Answer:

Command	Router Type		
	First Hop Router	Intermediary Hop Router	Last Hop Router
ip pim register-source	☐	☐	☐
ip igmp version	☐	☐	☐
ip pim spt-threshold	☐	☐	☐
ip pim rp-address	☐	☐	☐
ip pim sparse-mode	☐	☐	☐

1.15: Extending Connectivity to IaaS Site

Extend the IPv6 connectivity from HQ through the SP into the giosk VRF on the IaaS site according to these requirements:

Set up global IPv6 addressing on the link between r11 and r3

- On r11, assign 2001:2710:311::2/64 to g0/0
- On r3, assign 2001:2710:311::1/64 to g1
- Enable the existing IPv4 BGP session between r11 and r3 to also advertise IPv6 prefixes. Do not configure a standalone IPv6 BGP session between these two routers.
- Perform bidirectional route redistribution between the IPv6 EIGRP and BGP processes on r11
- Ensure that all current and future IPv6 prefixes advertised between r11 and r3 will be installed into the RIB of these routers with the next hop address set to the proper global unicast address on their interconnection. Any policy that accomplishes this requirement must be applied in the inbound direction.
- The giosk VRF on r4 that extends the IPv6 connectivity from r4 to r30 on the IaaS site is a separate VRF independent of fabd2 VRF. Any route leaking from fabd2 VRF into giosk VRF must be done on per-site basis and only for those FABD2 sites that need connectivity in the IaaS site.
- By configuring r3 and r4 only, ensure that the HQ FABD2 site will have mutual visibility with the IaaS site while preventing
    - Any other FABD2 site from possibly learning about the routes on the IaaS site
    - The IaaS site from possibly learning about the routes on any other FABD2 site
- Use the minimum amount of commands necessary to accomplish this requirement. Do not remove any existing configuration. If necessary, you are allowed to use an additional route target with the value of 10000:3681.
- Verify that host11 and host12 can ping 2001:db8:14::1 located at the IaaS site. It is permitted to modify one existing configuration command on one of the SP routers to meet this requirement

3 Points

Solution:

Chinese_Dumps_r11:

```
r11(config-if)#int gi0/0
r11(config-if)#ipv6 address 2001:2710:311::2/64

r11(config-if)#route-map NH-IPV6 per 10
r11(config-if)#set ipv6 next-hop 2001:2710:311::1

r11(config)#router bgp 65001
r11(config-router)#address-family ipv6
r11(config-router)#address-family ipv6 unicast
r11(config-router)#neighbor 100.3.11.1 remote-as 10000
r11(config-router)#neighbor 100.3.11.1 route-map NH-IPV6 in
r11(config-router)#redistribute eigrp 65001

r11(config)#router eigrp ccie
r11(config-router)#address-family ipv6 unicast autonomous-system 65001
 r11(config-router)#topology base
 r11(config-router)#redistribute bgp 65001 metric 100 50 255 1 1500
```

Chinese_Dumps_r4:

```
r4(config)#vrf definition giosk
r4(config)#route-target import 10000:3681

r4(config)#int lo0
r4(config-if)#ip address 100.255.254.4 255.255.255.255
```

Chinese_Dumps_r3:

```
r3(config)#vrf definition fabd2
r3(config)#route-target export 10000:3681
r3(config)#route-target import 10000:414
r3(config-vrf)#address-family ipv6
r3(config-af)#exit-address-family
```


```
r3(config)#int g1
r3(config-if)#ipv6 address 2001:2710:311::1/64
r3(config-if)#route-map NH-IPV6 per 10
r3(config-if)#set ipv6 next-hop 2001:2710:311::2

r3(config-if)#router bgp 10000
r3(config-router)#address-family ipv6 vrf fabd2
r3(config-router)#neighbor 100.3.11.2 remote-as 65001
r3(config-router)#neighbor 100.3.11.2 route-map NH-IPV6 in
```

To test R30 connectivity as per question, I created a loopback interface on R30

```
interface Loopback414
 no ip address
 ipv6 address 2001:DB8:14::1/128
 ipv6 enable
```

NOTE : On r4 there is loopback in pre-configs with /31 mask , we need to correct the loopback mask to /32

Verification:

Chinesedumps-r3: sh bgp vpnv6 unicast all

```
chinesedumps-r3#sh bgp vpnv6 unicast all
BGP table version is 3, local router ID is 100.255.254.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path, L long-lived-stale,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
       www.passenterpriselabs.com                    www.passenterpriselabs.com
     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 10000:1 (default for vrf fabd2)
 *>   2001:DB8:1:100::/64
                      2001:2710:311::2
                                               15360             0 65001 ?
 *>   2001:DB8:1:101::/64
                      2001:2710:311::2
                                               15360             0 65001 ?
chinesedumps-r3#
```

Chinesedumps-r11: sh bgp ipv6 unicast neighbors 100.3.11.1 advertised-routes

```
225A1D3z 225BBE8z 225BD8Ez 14F306Dz 14ED2B2z 147C524z
chinesedumps-r11#
chinesedumps-r11#
chinesedumps-r11#    www.passenterpriselabs.com
chinesedumps-r11#sh bgp ipv6 unicast neighbors 100.3.11.1 advertised-routes
BGP table version is 3, local router ID is 10.1.255.11
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>   2001:DB8:1:100::/64
                       FE80::102                15360         32768 ?
 *>   2001:DB8:1:101::/64
                       FE80::102                15360         32768 ?

                                 www.passenterpriselabs.com
Total number of prefixes 2
chinesedumps-r11#
```

Chinesedumps-r3: sh ip route vrf fabd2 100.4.30.5

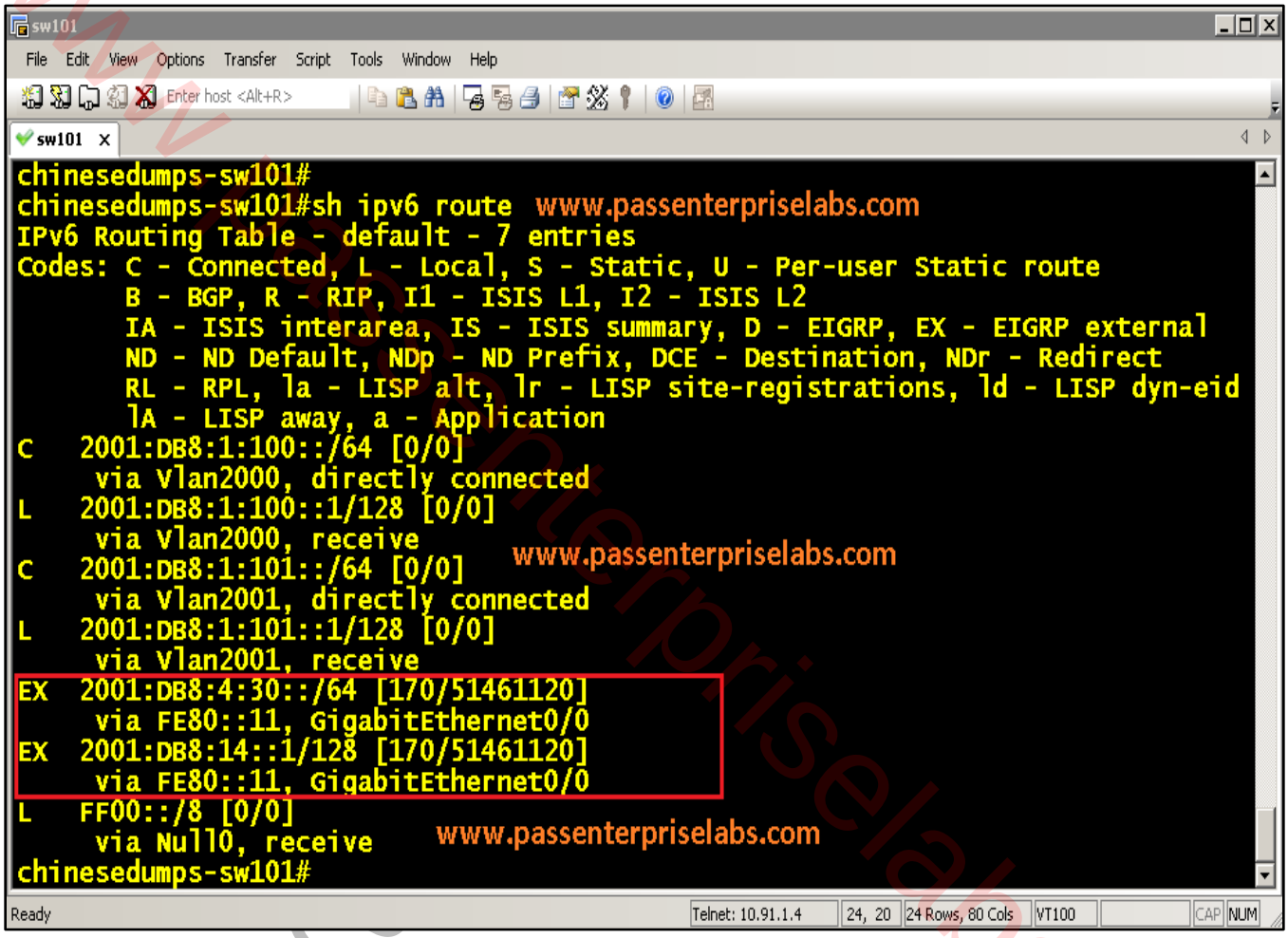
```
chinesedumps-r3#
chinesedumps-r3#   www.passenterpriselabs.com
chinesedumps-r3#sh ip route vrf fabd2 100.4.30.5

Routing Table: fabd2
Routing entry for 100.4.30.4/30
  Known via "bgp 10000", distance 200, metric 0, type internal
  Last update from 100.255.254.4 00:36:47 ago
  Routing Descriptor Blocks:
  * 100.255.254.4 (default), from 100.255.254.4, 00:36:47 ago
      Route metric is 0, traffic share count is 1
      AS Hops 0
      MPLS label: 16
      MPLS Flags: MPLS Required
chinesedumps-r3#   www.passenterpriselabs.com
chinesedumps-r3#
```

- From above output we can see that the giosk network (100.4.30.5) is present on r3 in fabd2
- And in the below output on r5 we can see that the giosk network (100.4.30.5) is not present in fabd2

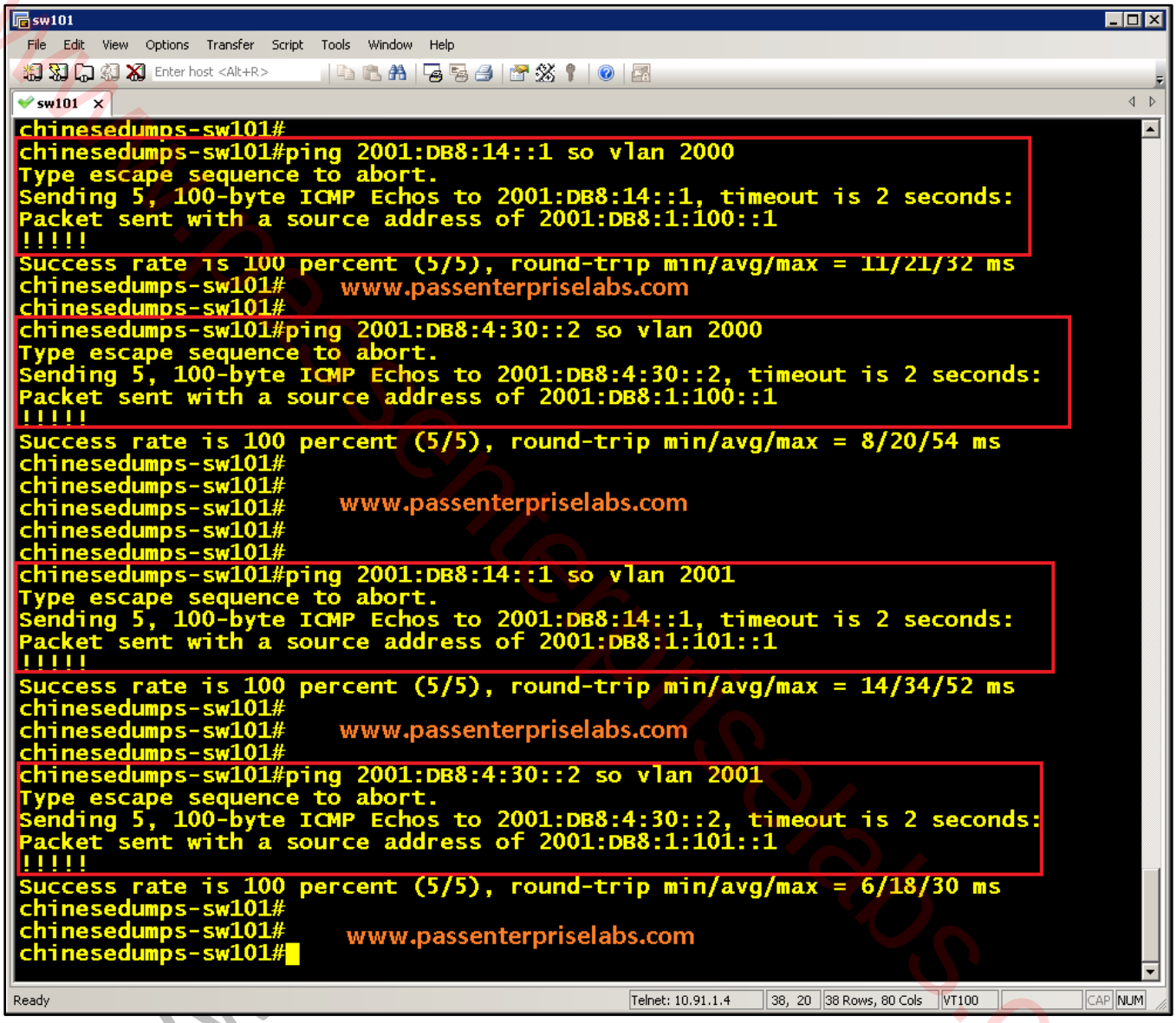
```
chinesedumps-r5#
chinesedumps-r5#   www.passenterpriselabs.com
chinesedumps-r5#
chinesedumps-r5#
chinesedumps-r5# sh ip route vrf fabd 100.4.30.5
% IP routing table vrf fabd does not exist
chinesedumps-r5#
chinesedumps-r5#   www.passenterpriselabs.com
chinesedumps-r5#
chinesedumps-r5#
```

- Verify that host11 and host12 can ping 2001:db8:14::1 located at the laaS site.

Chinesedumps-sw101: sh ipv6 route



Chinesedumps-sw101:

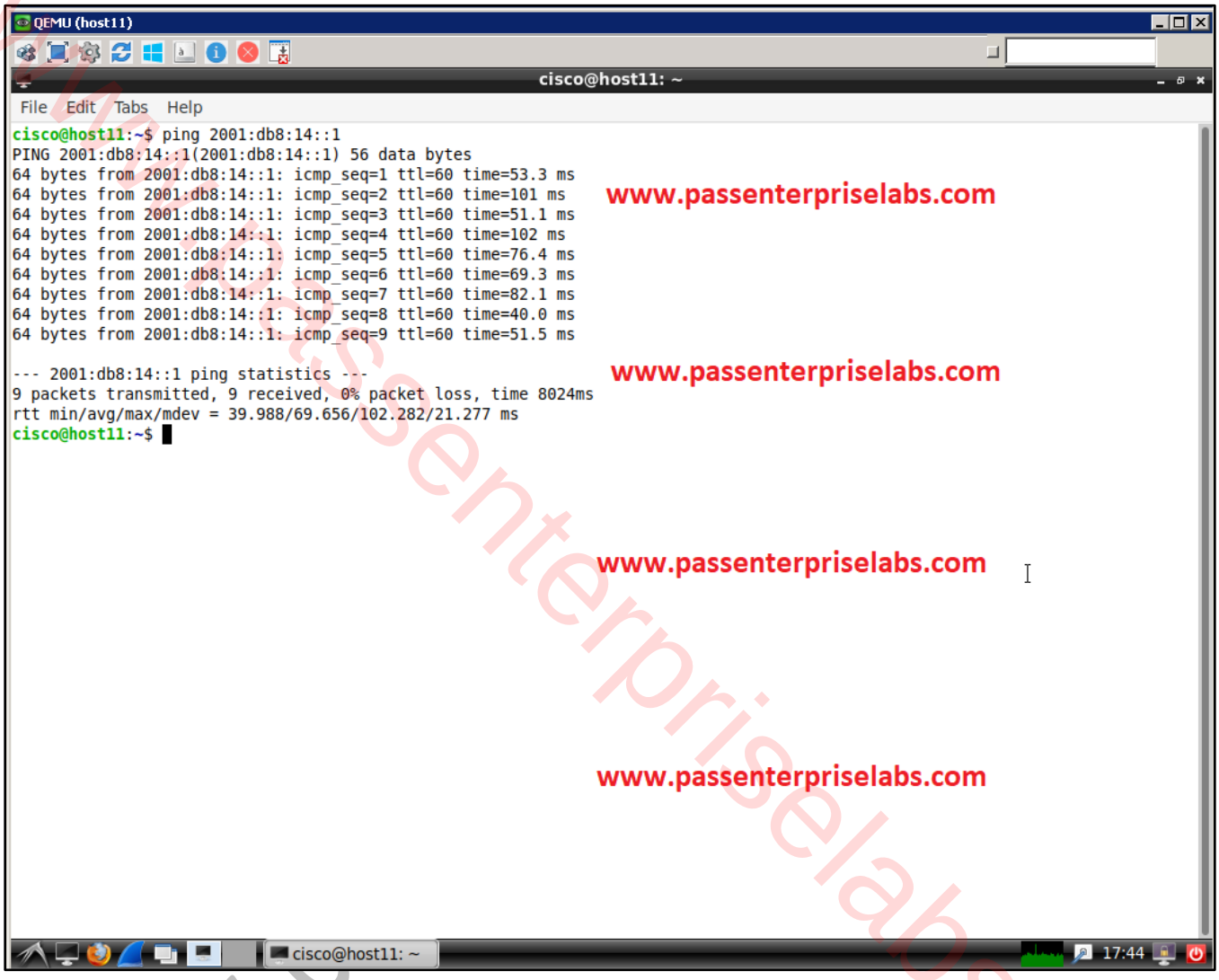


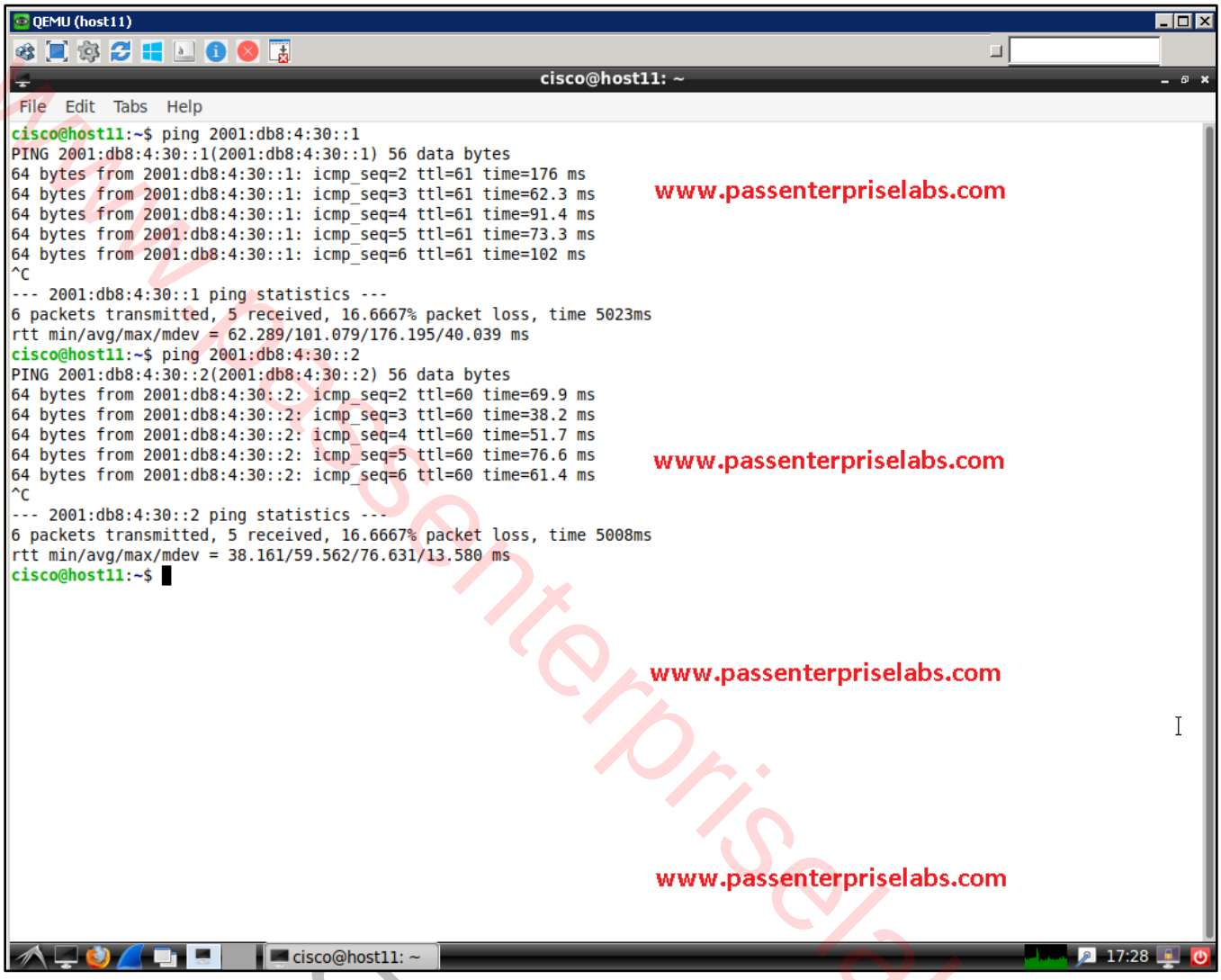
Chinesedumps-r11: sh bgp ipv6 unicast

```
R11
chinesedumps-r11#
chinesedumps-r11#      www.passenterpriselabs.com
chinesedumps-r11#
chinesedumps-r11#sh bgp ipv6 unicast
BGP table version is 4, local router ID is 10.1.255.11
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
                    www.passenterpriselabs.com
     Network          Next Hop            Metric LocPrf Weight Path
 *>   2001:DB8:1:100::/64
                      FE80::102                15360         32768 ?
 *>   2001:DB8:1:101::/64
                      FE80::102                15360         32768 ?
 r>   2001:2710:311::/64
                      2001:2710:311::1                       www.passenterpriselabs.com
                                                        0             0 10000 ?
chinesedumps-r11#
```

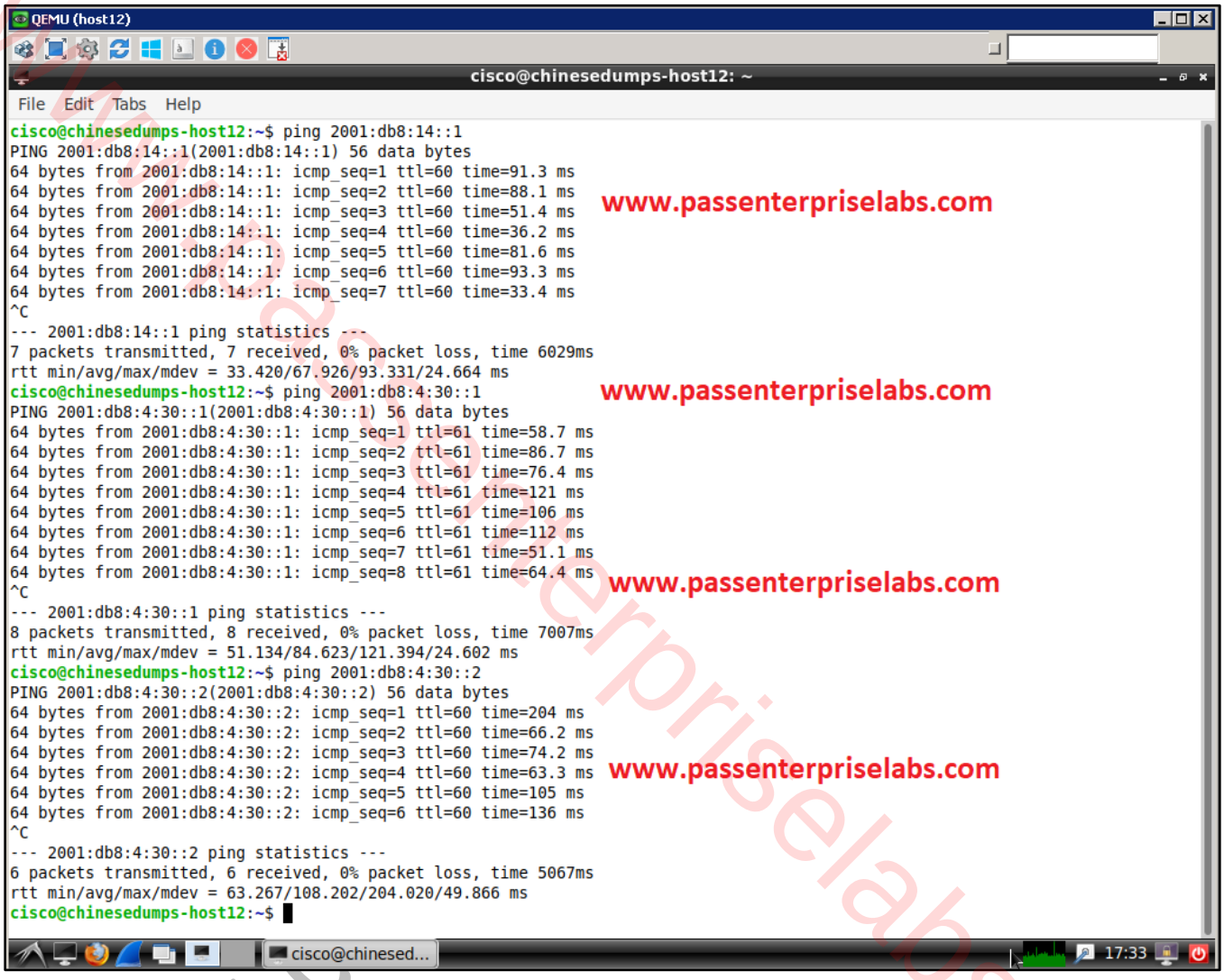
```
R11
File  Edit  View  Options  Transfer  Script  Tools  Window  Help
Enter host <Alt+R>
R11
chinesedumps-r11#sh bgp ipv6 uni
BGP table version is 10, local router ID is 10.1.255.11
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
                                                  www.passenterpriselabs.com
     Network          Next Hop            Metric LocPrf Weight Path
 *>   2001:DB8:1:100::/64
                      FE80::102                15360         32768 ?
 *>   2001:DB8:1:101::/64
                      FE80::102                15360         32768 ?
 *>   2001:DB8:4:30::/64
                      2001:2710:311::1                       0 10000 65003 ?
 *>   2001:DB8:14::1/128
                      2001:2710:311::1                       0 10000 65003 ?
 r>   2001:2710:311::/64
                      2001:2710:311::1
                                                        0             0 10000 ?
chinesedumps-r11#
Ready  Telnet: 10.91.1.4  24, 18  24 Rows, 80 Cols  VT100  CAP  NUM
```

Chinesedumps-host11:





Chinesedumps-host12:



1.16: Enabling Internet Access for FABD2

Enable highly available internet access for the FABD2 company network according to these requirements:

- On routers r12, r23 and r24, bring up IPv4 BGP peerings with the ISP, make sure that a default route is received over these peerings
- On router r12 and r23, inject default route into OSPF if it present in the routing table from a different routing source than the OSPFv2 process 1. On each router, this requirement must be completed using the minimum possible number of commands
- On route r24, inject default route into OSPF if any only if it is learned from ISP over BGP. To accomplish this requirement, it is allowed to use a route-map that referenced both a prefix-list and tag. This requirement must be completed using the minimum possible number of commands
- Router r12 may be used as an internet exit for the FABD2 company network only if neither r23 nor r24 are advertising the default route in OSPF. This requirement must be accomplished exclusively in “router ospf” mode on router r12 without changing the default parameters on routers r23 and r24
- On routers r12, r23 and r24, configure PAT and translate the entire FABD2 internal network 10.0.0.0/8 to the router address on the link toward the ISP. Create a standard ACL named NAT for this purpose. Do not use NAT pools
- Ensure that the internet connectivity of the FABD2 company network makes use of the highly availability provided by r12, r23 and r24.

1 Point

Solution:

Chinesedumps.com-r12:

```
r12(config)#router bgp 65001
r12(config-router)#address-family ipv4 unicast
r12(config-router)#neighbor 200.99.12.1 remote-as 19999
r12(config-router)#neighbor 200.99.12.1 activate


r12(config)#router ospf 1
r12(config-router)#default-information originate

r12(config)#int g0/0
r12(config-if)#ip nat outside
r12(config)#int range g0/1-3
r12(config-if)#ip nat inside
r12(config)#int lo0
r12(config-if)#ip nat inside
r12(config-if)#ip access-list standard NAT
r12(config-std-acl)#permit 10.0.0.0 0.255.255.255
r12(config)#ip nat inside source list NAT interface g0/0 overload
```

Chinesedumps.com-r23:

```
r23(config)#router bgp 65002
r23(config-router)#neighbor 200.99.23.1 remote-as 19999
r23(config)#router ospf 1
r23(config-router)#default-information originate metric-type 1

r23(config)#int g1
r23(config-if)#ip nat outside
r23(config)#int range g2-4
r23(config-if)#ip nat inside
r23(config)#int lo0
r23(config-if)#ip nat inside
r23(config-if)#ip access-list standard NAT
r23(config-if)#permit 10.0.0.0 0.255.255.255
r23(config-if)#ip nat inside source list NAT interface g1 overload
```

Chinesedumps.com-r24:

r24(config)#router bgp 65002
r24(config-router)#neighbor 200.99.24.1 remote-as 19999

r24(config)#ip prefix-list DEFAULT permit 0.0.0.0/0

r24(config)#route-map ISP permit 10
r24(config-route-map)#match ip address prefix-list DEFAULT
r24(config-route-map)#match tag 19999

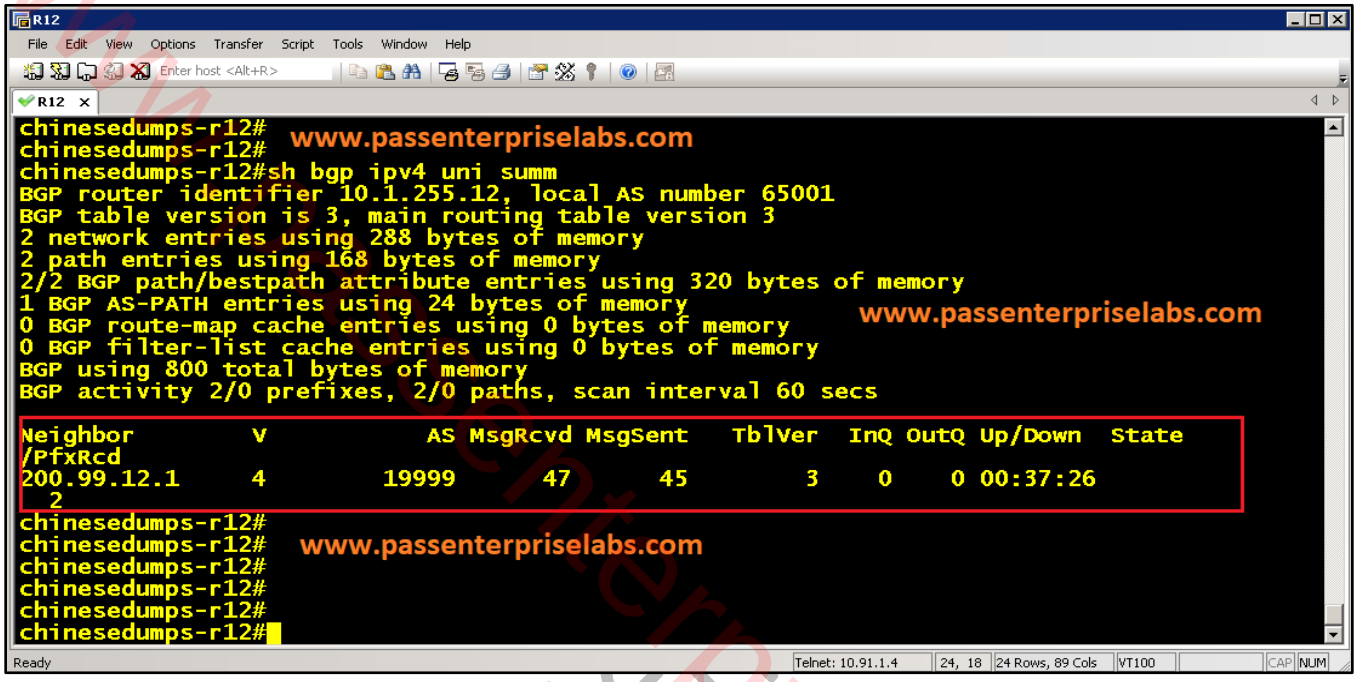
r24(config)#router ospf 1
r24(config-router)#default-information originate route-map ISP metric-type 1

r24(config)#interface g1
r24(config-if)#ip nat outside
r24(config-if)#int range g2-4,tunnel 0
r24(config-if)#ip nat inside
r24(config-if)#int lo0
r24(config-if)#ip nat inside
r24(config-if)#ip access-list standard NAT
r24(config-if)#permit 10.0.0.0 0.255.255.255
r24(config-if)#ip nat inside source list NAT interface g1 overload

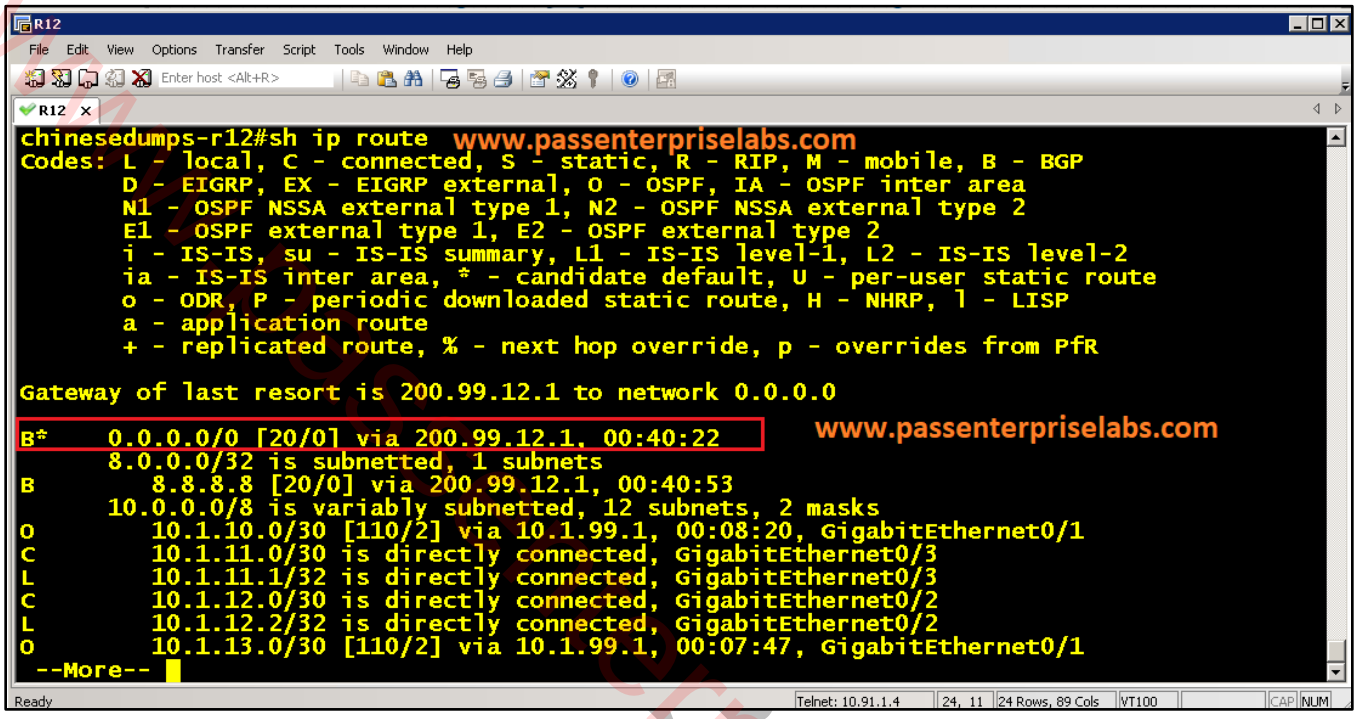
r24(config)#router eigrp ccie
r24(config-router)#address-family ipv4 unicast autonomous-system 65006
r24(config-router-af)#topology base
r24(config-router-af)#summary-metric 0.0.0.0/0 distance 254

Verification:

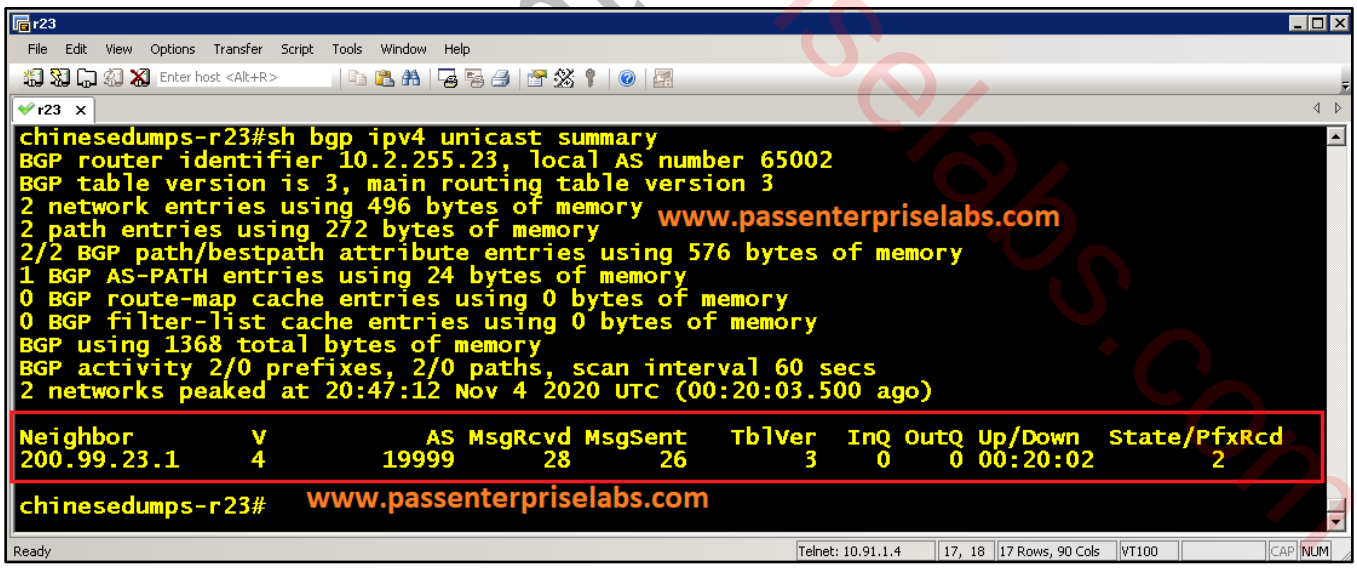
Chinesedumps-r12: sh bgp ipv4 unicast summary



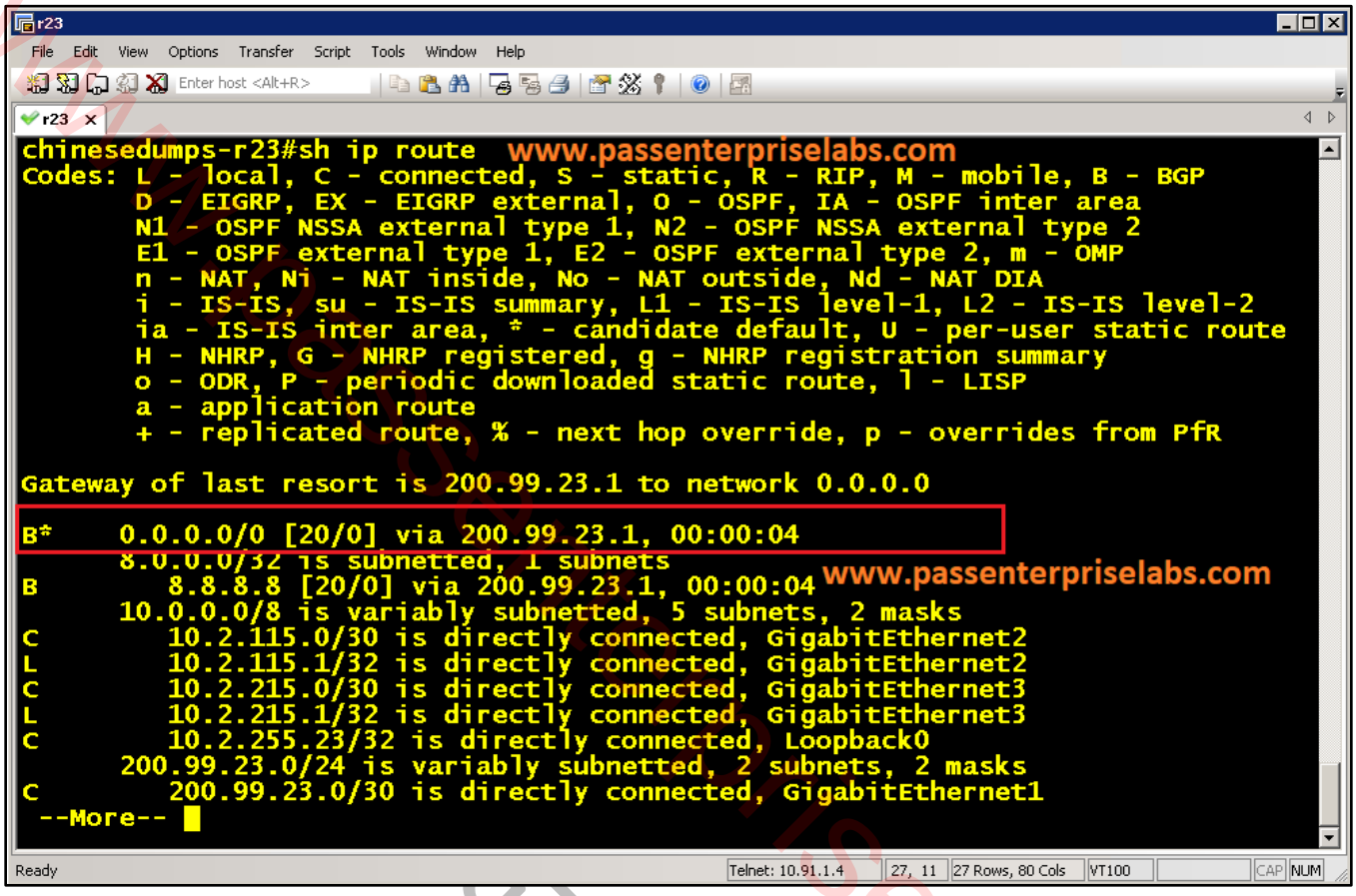
Chinesedumps.com-r24:sh ip route



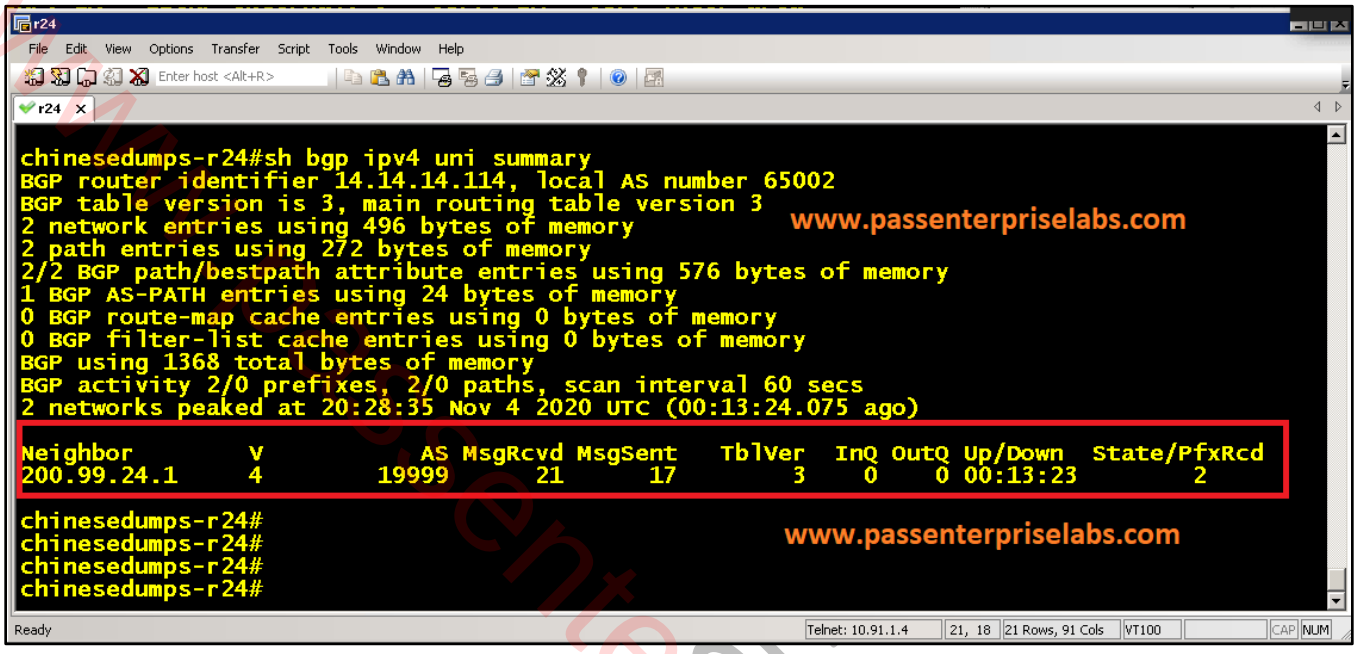
Chinesedumps.com-r23:sh bgp ipv4 unicast summary



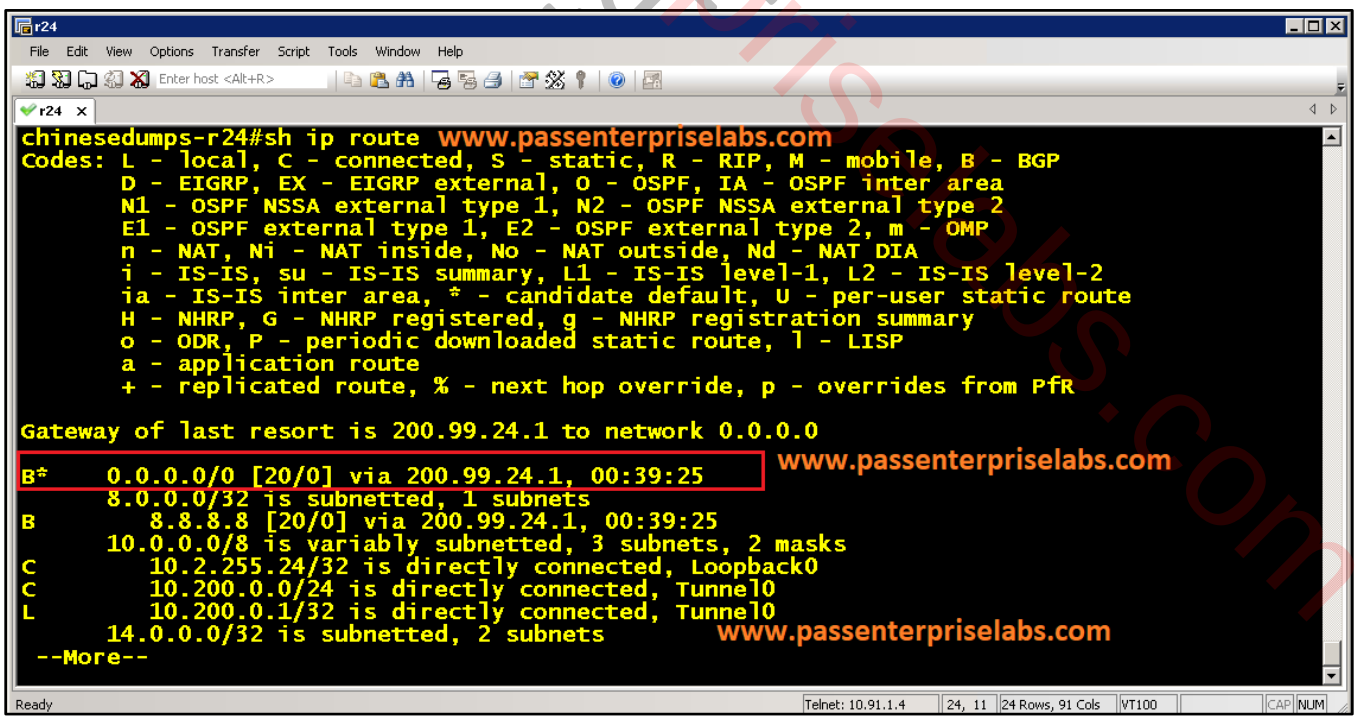
Chinesedumps.com-r23:sh ip route



Chinesedumps.com-r24: sh bgp ipv4 unicast summary



Chinesedumps.com-r24: sh ip route



2.1: Correcting the IP addresses of Managed switches in DNA center

After Cisco DNA center first achieves IP connectivity with the managed switches in Branches #1 and #2, it will place them into maintenance mode due to their serial number being different from the one DNA center remember. 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:

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

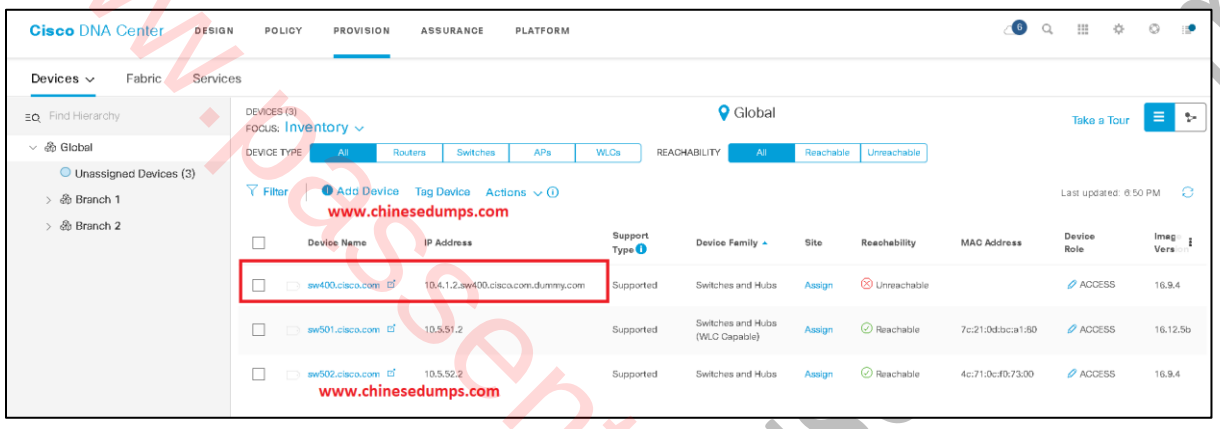
Note: These IP addresses cannot be changed from DNA Center GUI directly because they will become automatically invalidated again. This is a built-in DNA Center behavior.

3 points

Solution:

Step 1:

Access DNA Center and then go to PROVISION

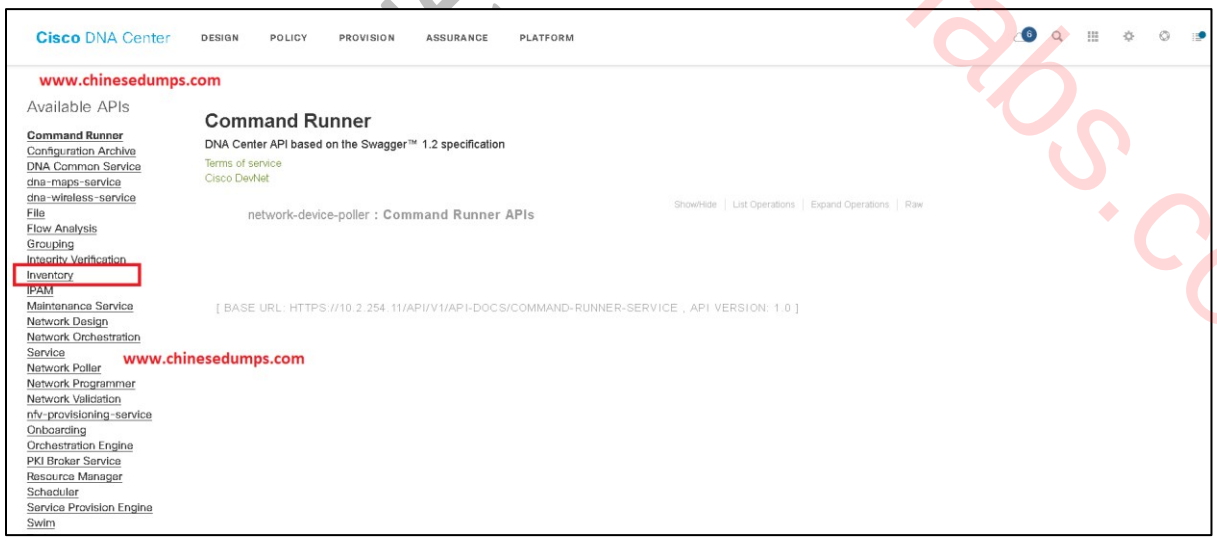


Above Output will be displayed for all the 3 switches (sw400 , sw501 , sw502)

Step 2:

To complete the task you have to go to below URL

https://10.2.254.11/dna/apitester



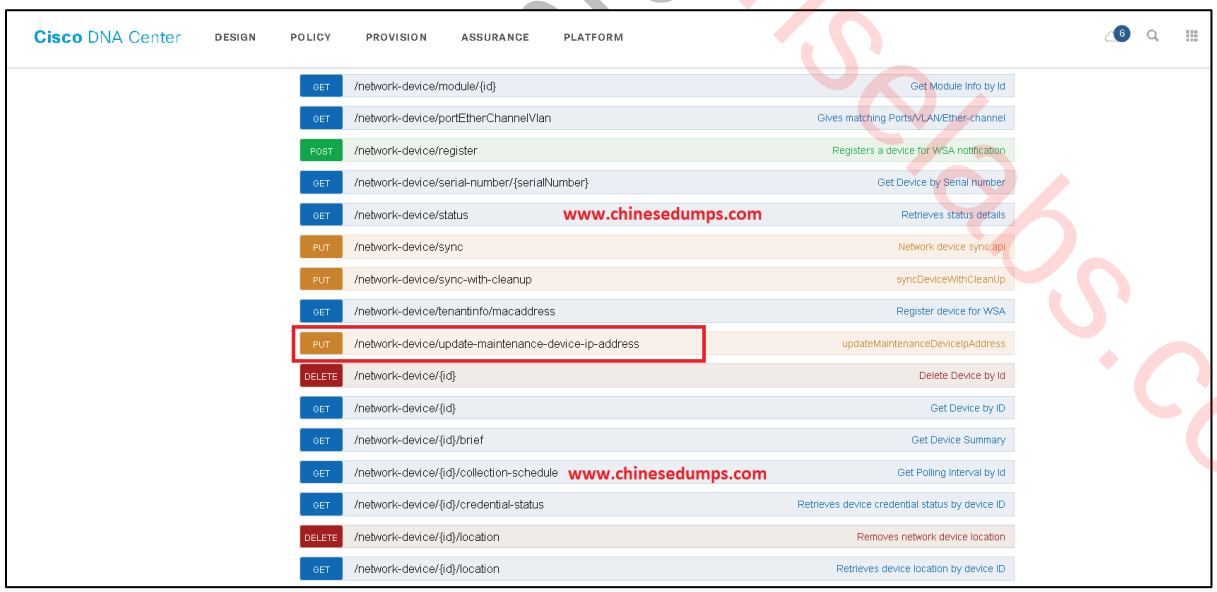
Click on **Inventory** option

Step 3:

Scroll down and Click on **network-device**

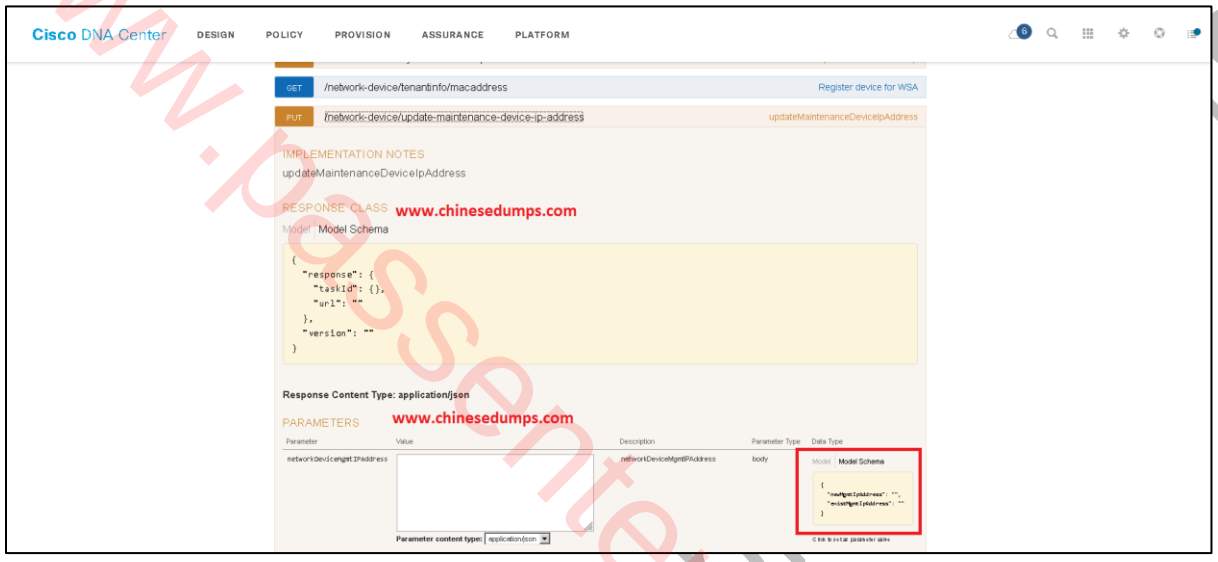
Step 4:

- Scroll down and click on **/network/device-update-maintainance-device-ip-address**



Step 5:

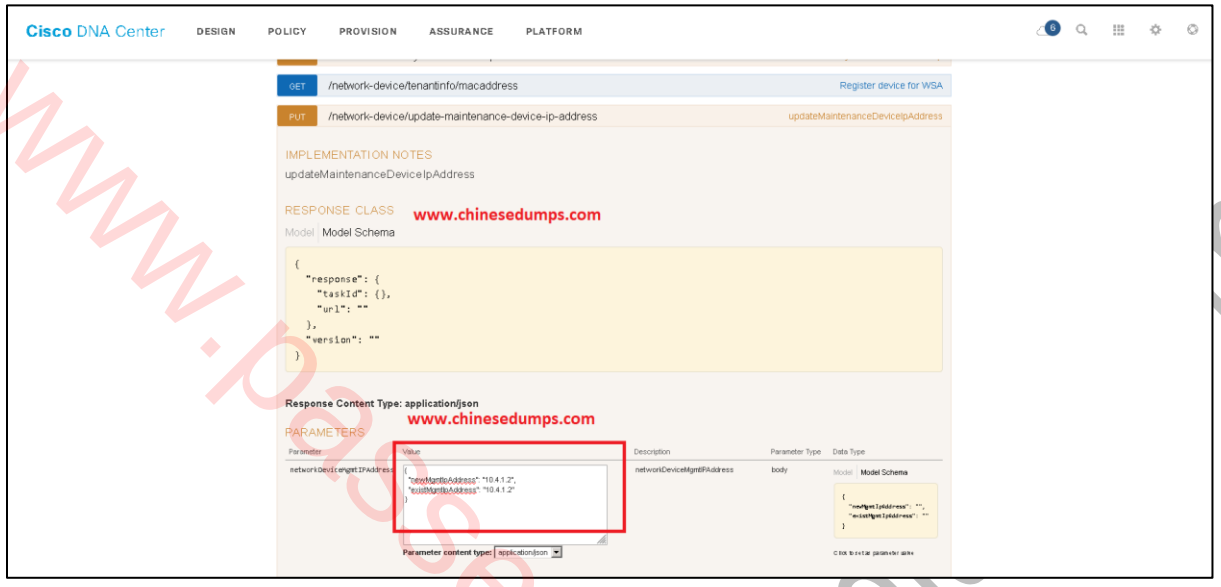
- Scroll down and at the right hand side you will see **Model Schema**
- Just click inside the box where the code is written



Step 6:

- The code will be copied in the right side blank box
- Then change the **NewMgmtIpAddress – "10.4.255.11",**
  existMgmtIpAddress – "10.4.255.11.dummy.com"

```
{
 "newMgmtIpAddress": "10.4.1.2",
 "existMgmtIpAddress": "10.4.255.11dummy.com"
}
```



Step 7:

- Scroll down and click **Try it out** button

2.2: Completing VN Configuration in DNA center

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

- Add new virtual Network named IoT for the internet-of-things network on the Branches #1 & #2
- Create new address pools for the IoT VN named Branch1-For IoT and Branch2-For IoT on the global level, and branch1-IoT and Branch2-IoT on the Branch level.
- For Branch #1 IoT VN, allocate the subnet 10.4.198.0/24 and the gateway IP address 10.4.198.1.
- For Branch #2 IoT VN, allocate the subnet 10.5.198.0/24, and the gateway IP address 10.5.198.1.
- Associate the Branch1-IoT and Branch2-IoT pools with the IoT VN on the respective branches.
- 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.
- Correct the addressing information currently defined for the Branch2-For Employees and Branch2-Employees address pool.
- For all address pools, use the DHCP server 10.2.255.211 to allocate addresses to clients.

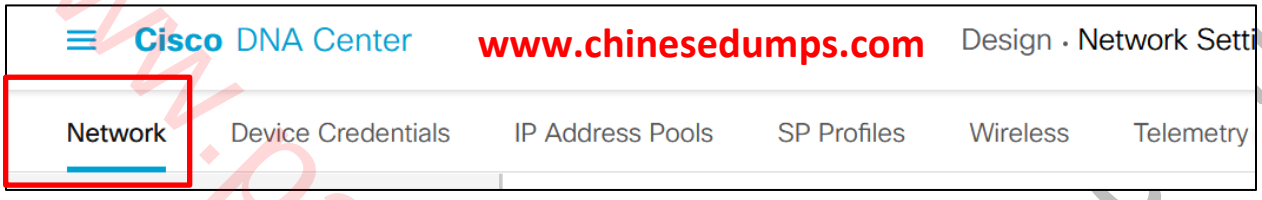
On sw211, complete the DHCP server configuration according to these requirements:

- Create four new DHCP pools for the IoT and Employees VNs on 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
- In each subset, assign addresses from .101 up to .254 inclusively, and the appropriate gateway to clients.

3 Points

Solution:

Step 1:

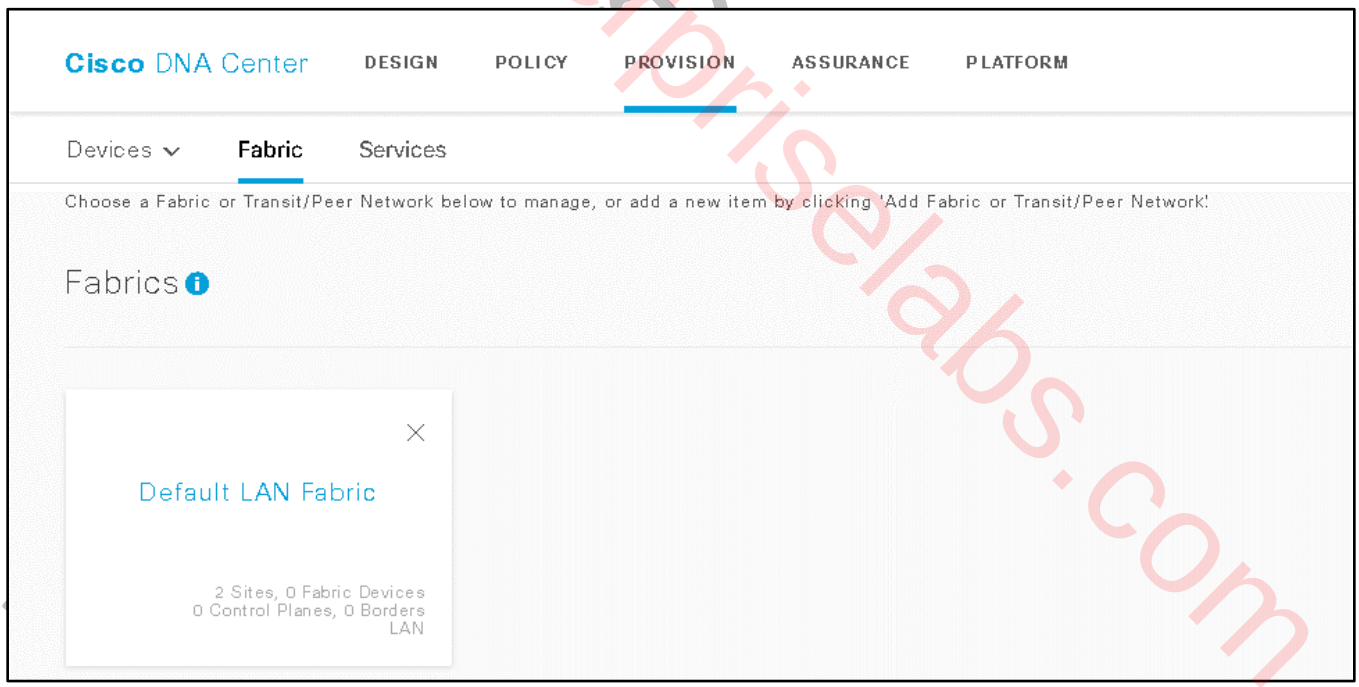


Configure DHCP server under network setting 10.2.255.211. Click Save.

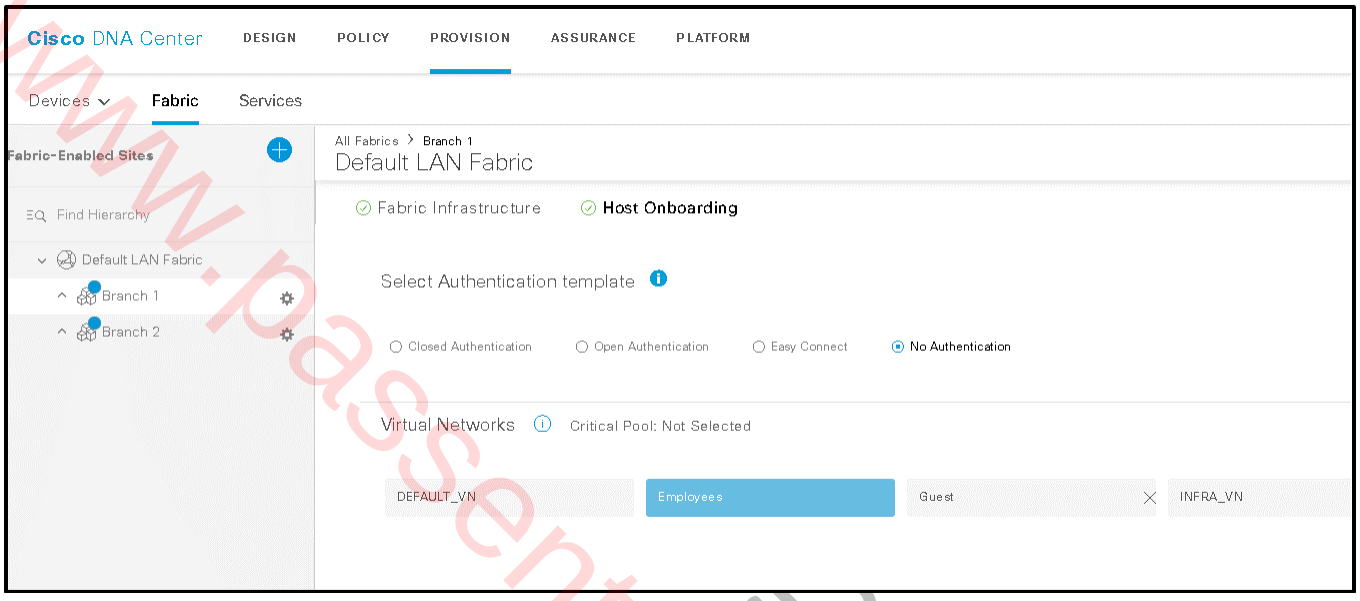
Note: The pools that will be pre-configured will not have DHCP server attached with them , so we need to add DHCP server before moving forward to create other pools

How to add DHCP to preconfigured IP Pools :

a. Go under Provision > Fabric > Default LAN_FABRIC



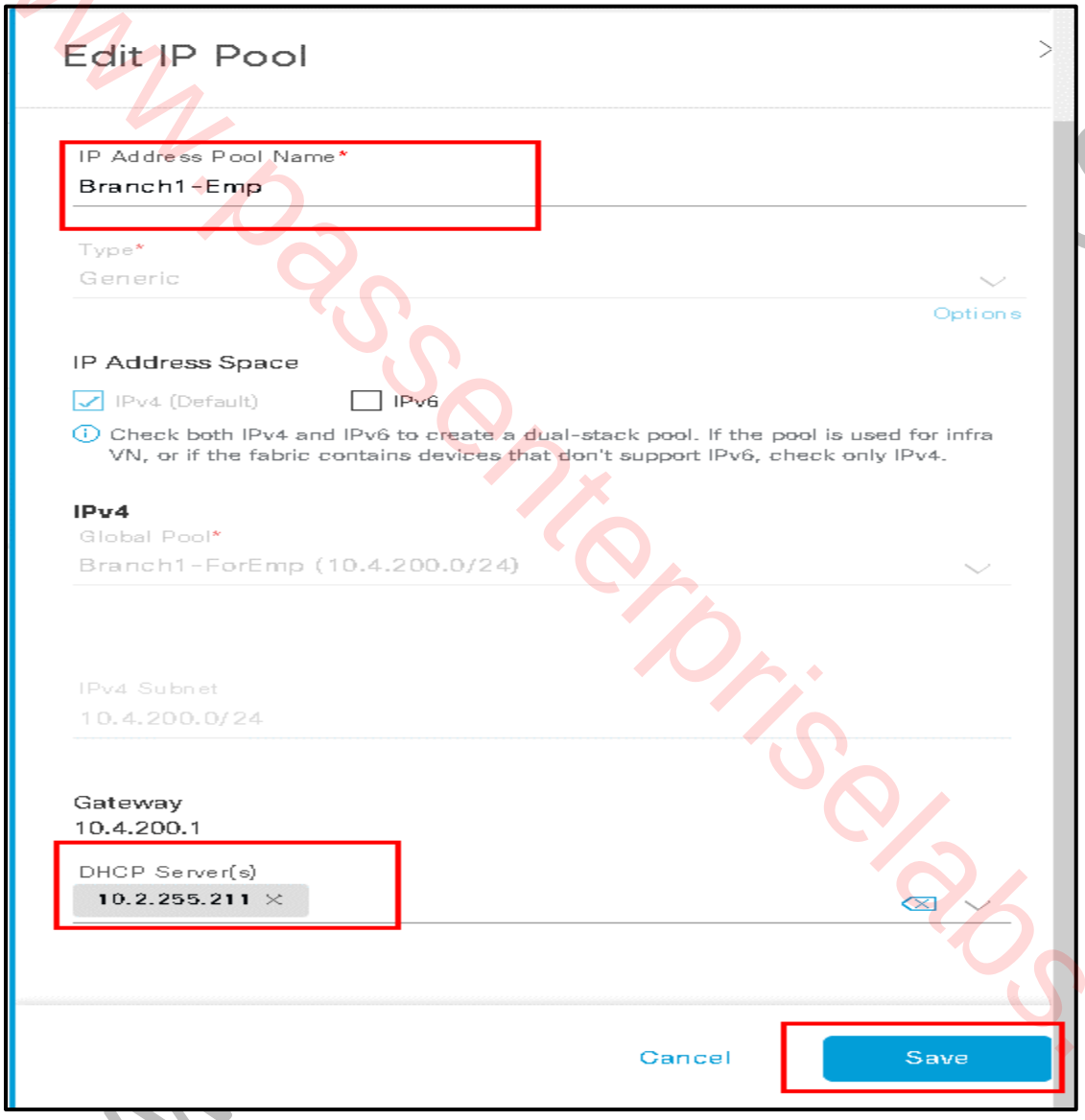
b. Select Branch1 and go under Host Onboarding and Select Employees VN



c. Then got Actions and delete the associated to Employee VN

d. After deleting go under Design > Network Settings > IP pools

e. Select Branch1_Emp pool and add DHCP server and reserve it to Fabric again



f. Edit the Branch1_Emp pool and add DHCP as shown and then save it

g. Just again add the pool to fabric

Step 2:

Under IP Address pool on global level

Click Add

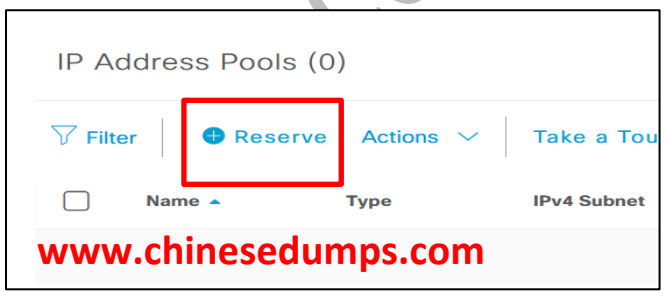
Fill in info Branch1-ForIoT

IP 10.4.198.0/24

Select the DHCP pool created in step 1. Repeat for Branch 2.

Step 3:

Go under each branch under Global and click Reserve



Name the IP pool Branch1-IoT

Select the Global pool created in step 2 for Branch1.

Select prefix length /24

Select the DHCP server 10.2.255.211

Click reserve.

Repeat for Branch 2

(Verify that the employee IP pool have the DHCP server selected and have the correct gateway and is reserved under Branch 1 and 2)

(If a new Guest IP pool is needed to be created. Configure them in the same way as IoT but different IP range)

Step 4:

Under Policy>Virtual Network. Click Create Virtual Network.

Enter the name IoT

Step 5:

Under Provisioning>Fabric select Branch 1.

Select Host Onboarding > Virual Networks and click Add Virtual Network

Select the VN IoT and click update. The click on the Grey VN Iot

Select the IP Address pool for Branch1-IoT

Repeat for Branch 2

(If needed add the created IP pool to the Guest VN)

Step 6:

DCHP server on sw211

ip dchp exclude10.4.198.1 10.1.100.100
ip dchp exclude 10.5.198.1 10.1.101.100

ip dhcp pool br1_iot
network 10.4.198.0 /24
default-router 10.4.198.1
exit

ip dhcp pool br2_iot
network 10.5.198.0 /24
default-router 10.5.198.1

2.3: Mapping SDA VNs to SD-WAN VPNs

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

- Use any host, such as host11, to access the vManage GUI website at https://203.0.113.21 URL.
- 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
- On Branch #1 and Branch #2 vEdges, for each of these VPNs:
  - Create a new sub-interface on the interface toward the SDA border switch. Align the VLAN ID and IP address on the sub interface with the configuration generated by DNA Center on the border switches for the appropriate VN.
  - Peer the vEdge and the SDA border switch using iBGP. Ensure full reachability between all locations of the same VPN.

4 Points

Solution:

Step 1:

Select the device template where the Branch Vedges are attached. Click the Three dots <…> and Edit Device Template.

Go under Service VPN and click Add VPN

On the bottom of the page click Create VPN Template

Give the template a name and add the VPN number 198

Under Advertise OMP Click on for BGP

Click Save and repeat for VPN 199 and 200

Step 2:

Select all three VPNs and click Next

Pick BGP and VPN Interface Ethernet

Press the BGP drop down bar and press create template.

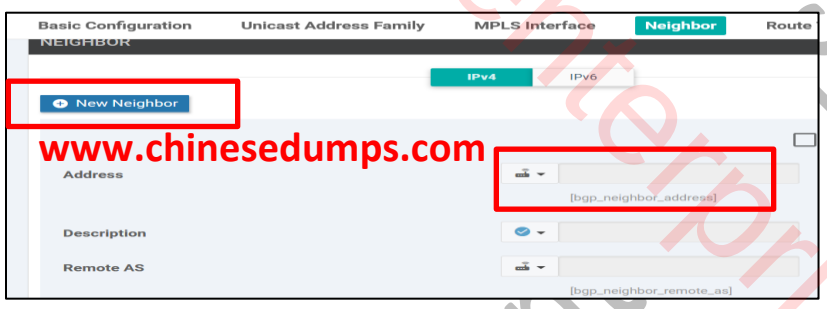
Give the template a name.

Leave BGP AS number to Device specific

Under Unicast Address Family click New Redistribute and under Protocol choose OMP and click Add.

Under Neighbor Click New Neighbor.

Change Address to device specific and click Add. Then Click Save



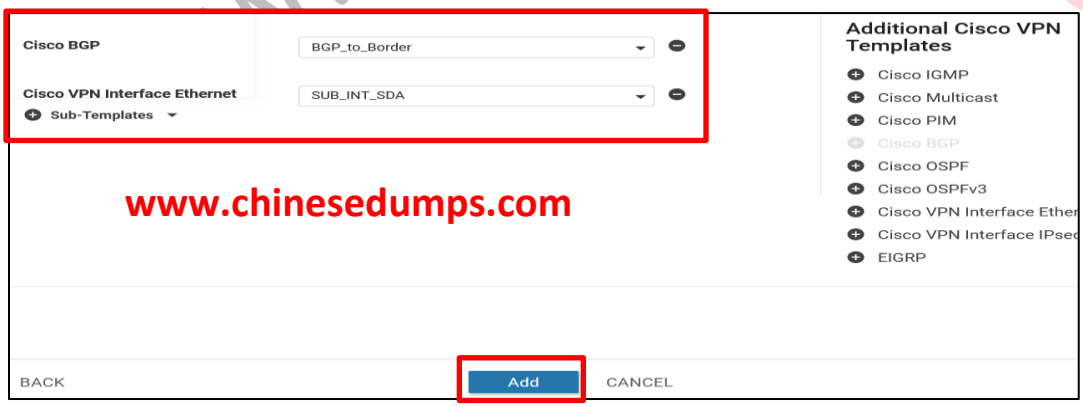
Step 3:

a. Create the VPN interface Template
b. Click Create new VPN Interface Ethernet Template
c. Give the template a name and description.
d. Change Shutdown to be Global No
e. Change Interface Name to be Device specific

Change IPv4 Address to be device specific.

Under Advanced change the MTU to be Global 1496 and click Save.

Add both template that was created and click Add and the press Update\



Click the three dots on the right to add the deivces values <…> For branch1 Router vEdge 40 Set BGP AS number to 65004 and Vedge 51 and 52 AS 65005

Place cursor on the three dots <…> to verify the interfaces.

Repeat for Vedge 51 and 52.

Then click Update and Next and push the config to the devices.

Step 4:

*Configure the SDA Border switches Sw 400, Sw 501 and Sw 502.

*DNA center should have generated VRFs for Employee VN, Guest VN and IoT VN.

Under Sw 400

Interface Vlan 198
Vrf forwarding IoT
Ip add 10.4.198.2 255.255.255.0
Interface Vlan 199
Vrf forwarding Guest
Ip add 10.4.199.2 255.255.255.0

Interface Vlan 200
Vrf forwarding Employees
Ip add 10.4.200.2 255.255.255.0

Router bgp 65004
Address-family ipv4 vrf IoT
Neighbor 10.4.198.1 remote-as 65004
Neighbor 10.4.198.1 activate
Network 10.4.1.0 mask 255.255.255.0

Address-family ipv4 vrf Guest
Neighbor 10.4.199.1 remote-as 65004
Neighbor 10.4.199.1 activate
Network 10.4.2.0 mask 255.255.255.0

Address-family ipv4 vrf Employees
Neighbor 10.4.200.1 remote-as 65004
Neighbor 10.4.200.1 activate
Network 10.4.3.0 mask 255.255.255.0

Add Network statement of the IP pools that was created in DNAC in question 2.1
Repeat this configuration for switch 501 and 502

2.4: Configuring SD-WAN VPN Route Leaking

To allow the traditional parts of the FABD2 network to communication with the employees and IoT VPNs/VNs, configure route leaking in SD-WAN according to these requirements:

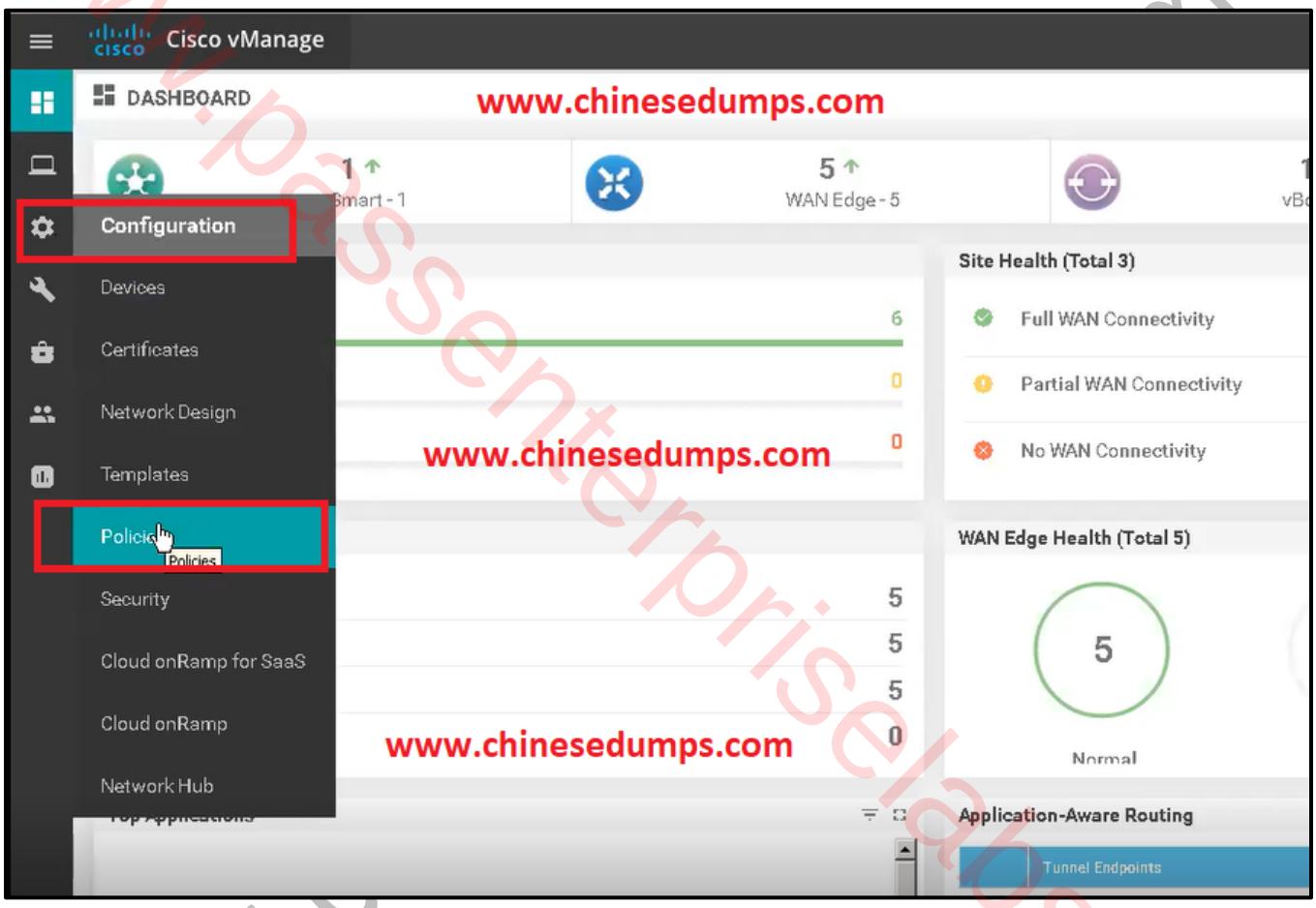
- Prefixes in the IoT VPN 198 must be imported into the existing SDA Underlay VPN 999 and tagged with the tag value of 198
- Prefixes in the Employees VPN 200 must be imported into the existing SDA underlay VPN 999 and tagged with the tag value of 200
- Prefixes in the SDA underlay VPN 999 advertised form the DC that are within the 10.4.0.0/15 range must be rejected. Other prefixes in the SDA underlay VPN 999 advertise from DC must be accepted and also imported into IoT VPN 198 and Employees VPN 200
- Redistribution from OMP into OSPF on Branches #1 and #2 in VPN 999 must exclude vRoutes tagged with values 198 or 200.
- Place host41 into Employees VN. Place host51 into IoT VN. Make sure both hosts receive their IP settings from DHCP.
- Ensure that the IoT and Employees VPNs on Branches #1 and #2 have reachability to Branches #3 and #4. It is allowed to modify the VPN 999 OMP settings to accomplish this requirement.

3 Points

Solution:

Step 1:

In vManage GUI go to **Configuration** tab and select **Policies**



Step 2:

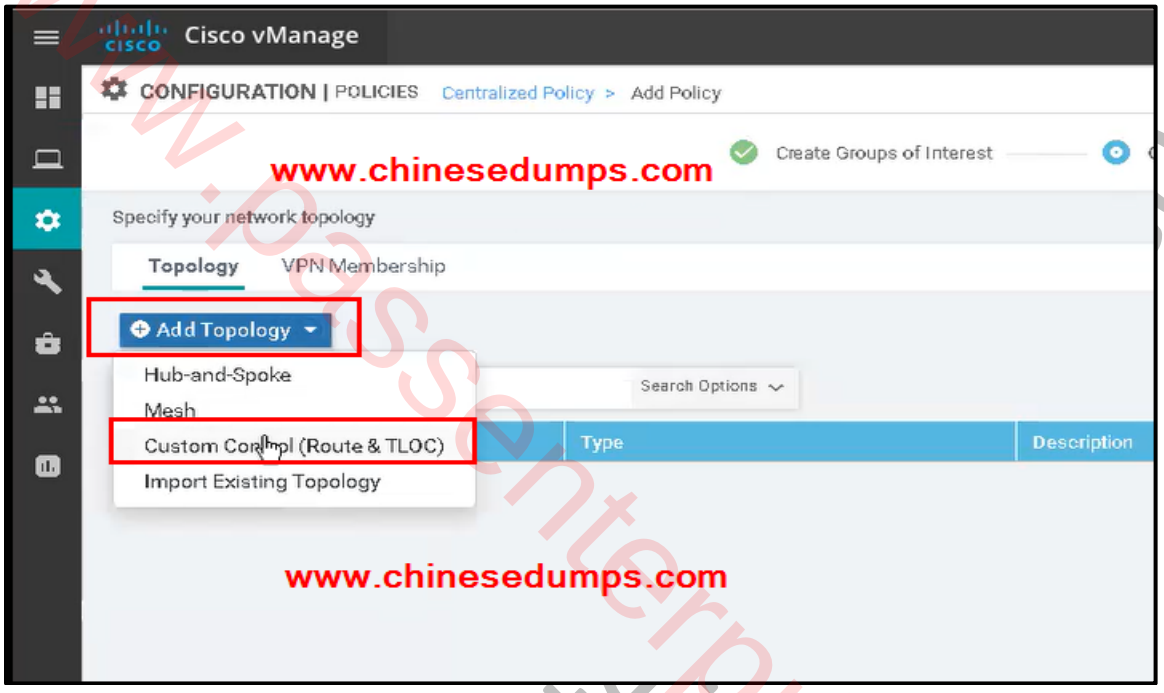
Under **Policies** Select **Centralized policy** and click on **add**

Step 3:

Now under centralized Policy check in the site tab which sites are pre-configured then hit **NEXT** at the bottom of the page

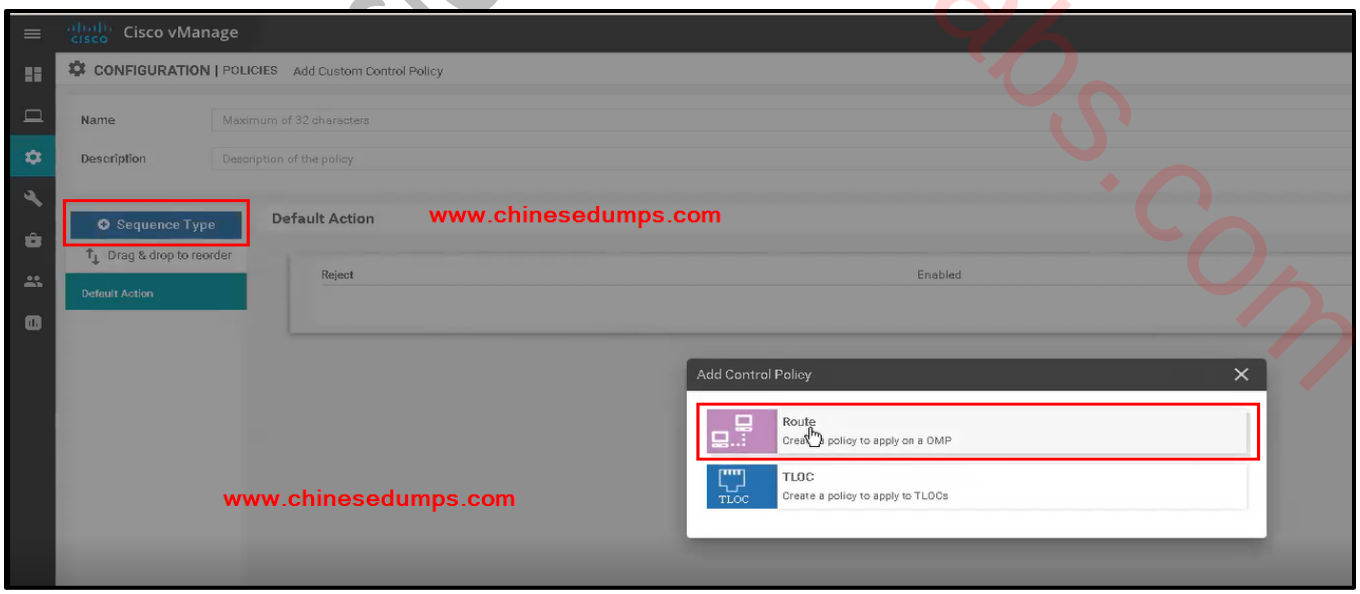
Step 5:

Click on Add **Topology** and select **Custom Control**



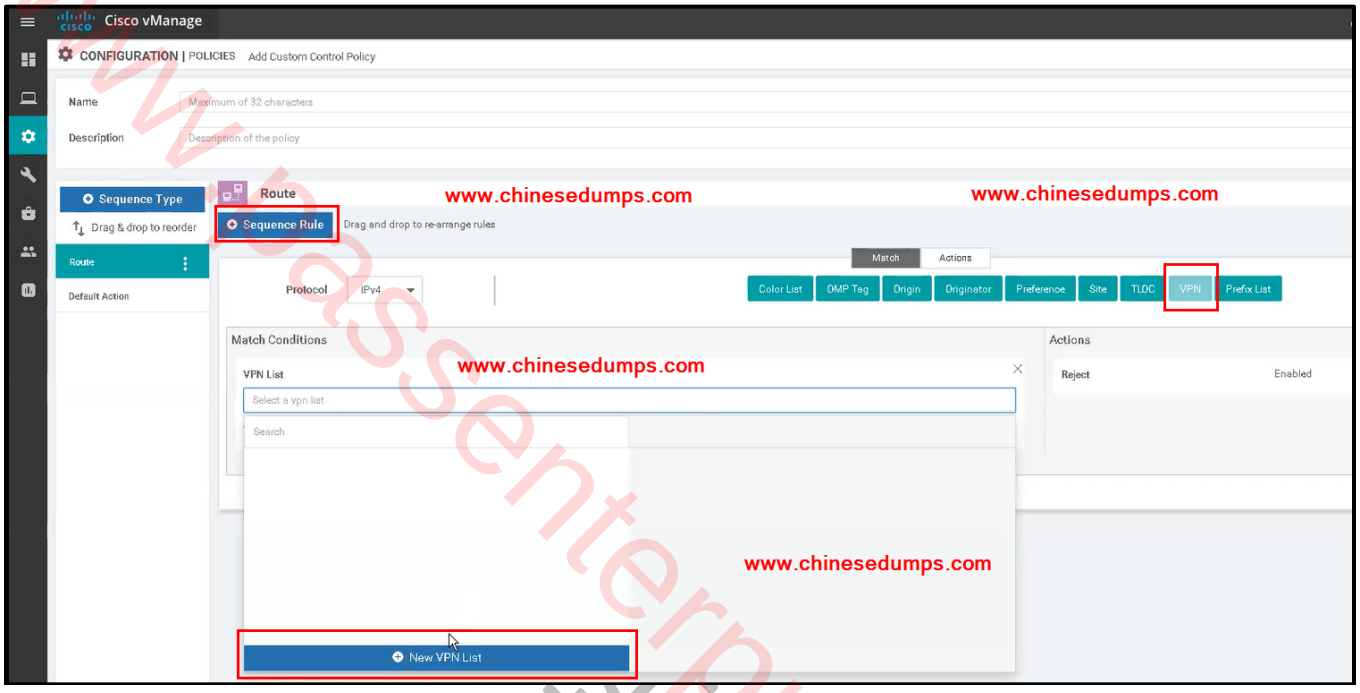
Step 6:

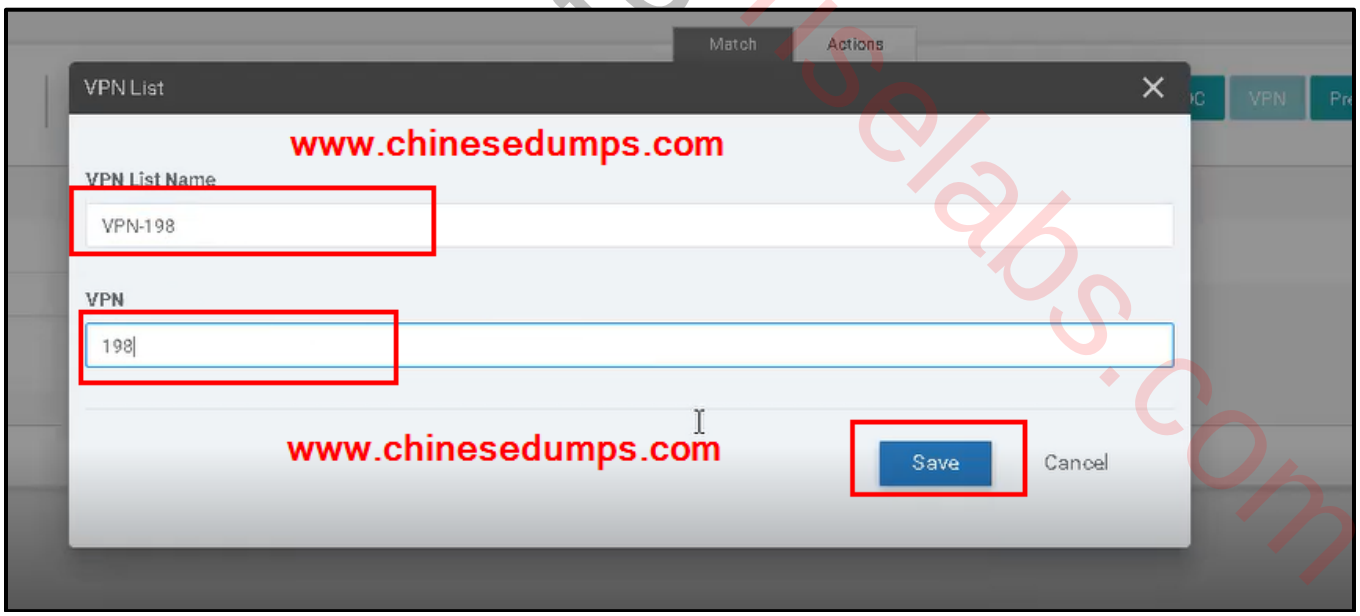
Add a **Sequence Type** and add a **Route Control Policy**



Step 7:

Select VPN list under **Match Conditions** and add a new VPN list





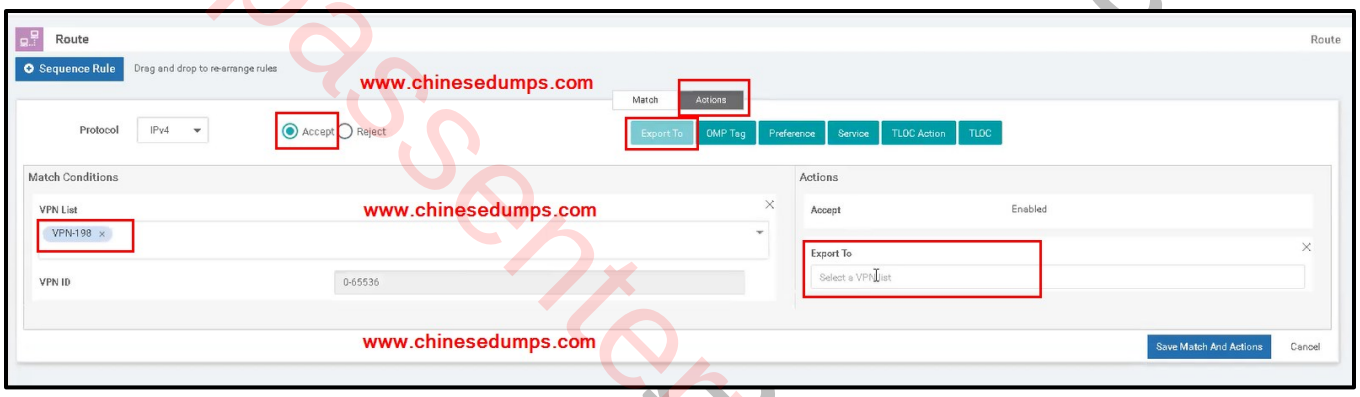
Step 8:

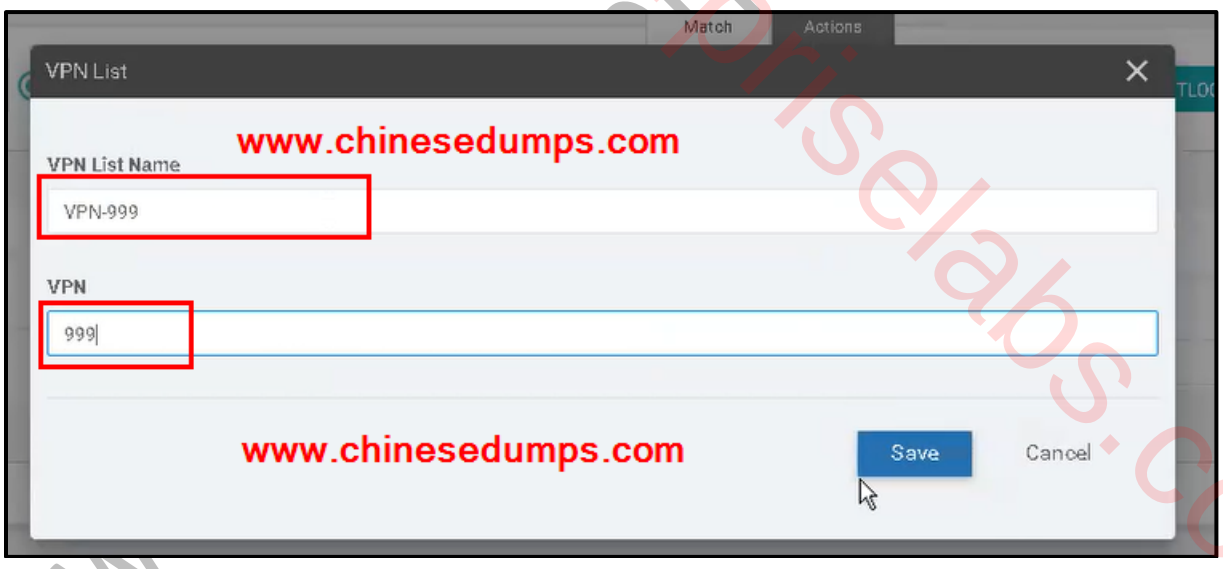
Select the **New VPN list** created

Go to **Actions** Tab

Select **Accept**

Select **Export** to and create a New VPN list VPN 999 (If not present already)





Step 9:

Select the VPN 999 in Export to

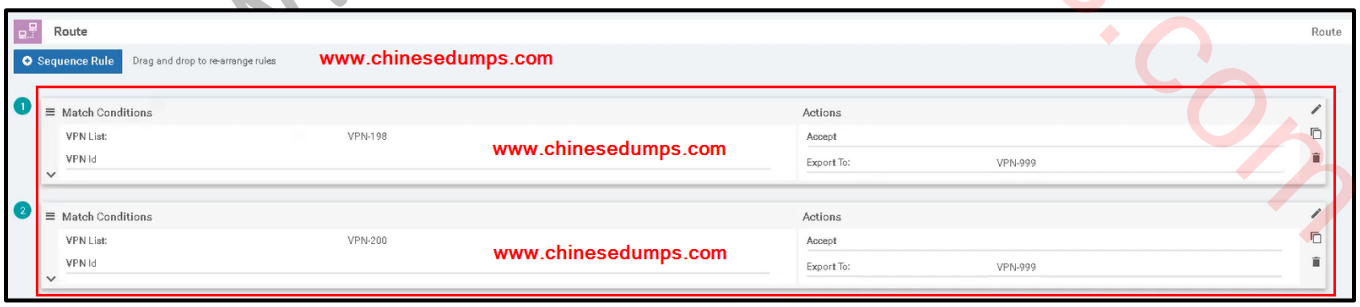
Click on **OMP Tag**

Add **OMP Tag as 198** and **Save Match and Actions**

Step 10:

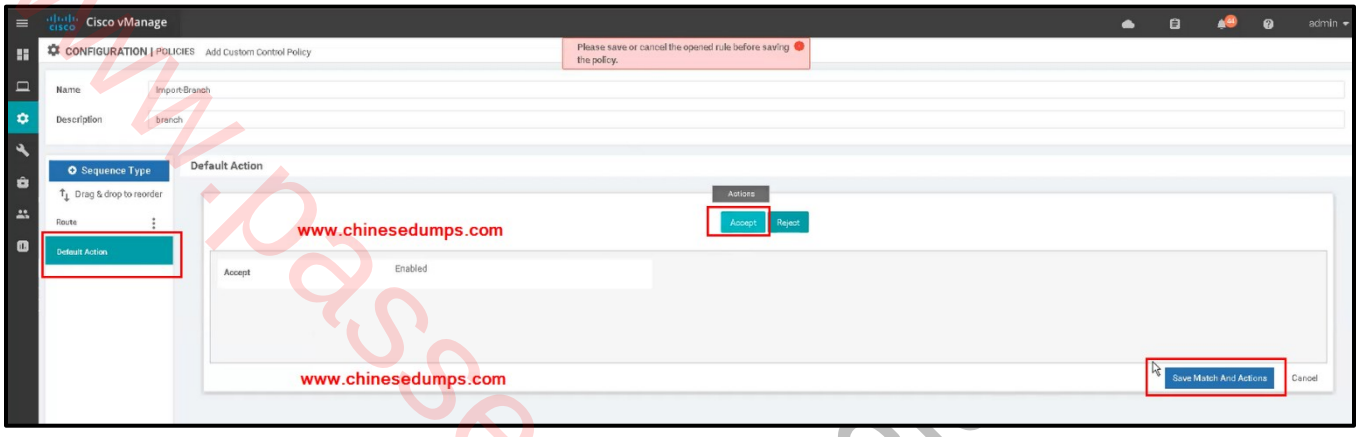
Repeat step 7, Step 8, Step 9 for VPN 200

Just in OMP Tag select 200



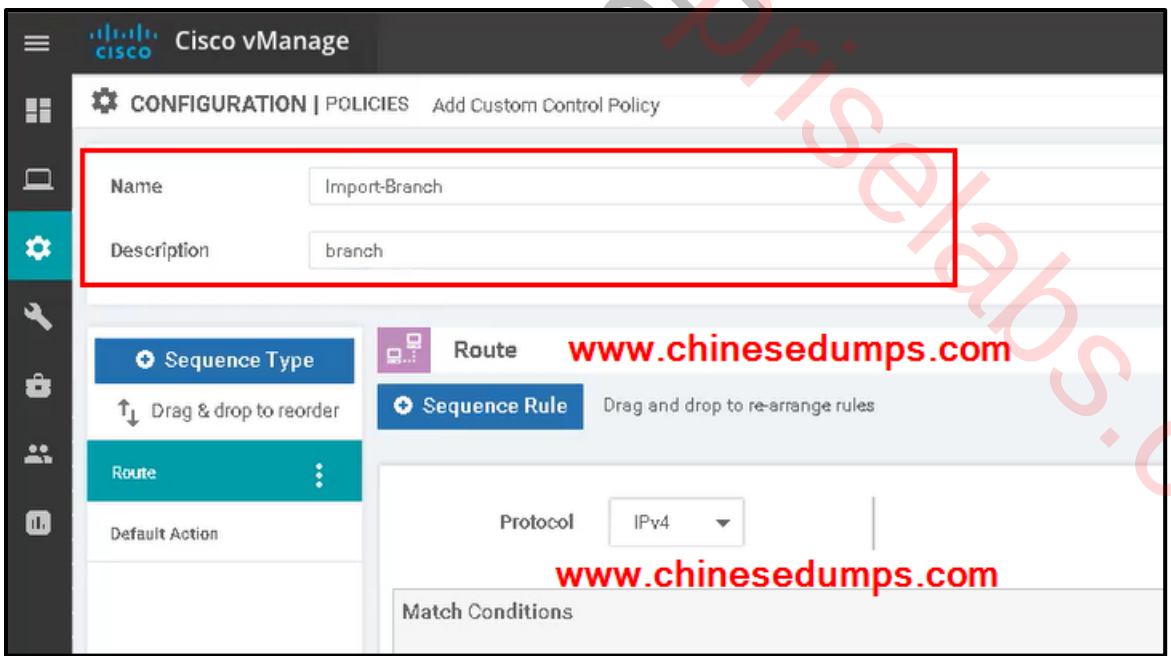
Step 11:

In Default Actions select Accept



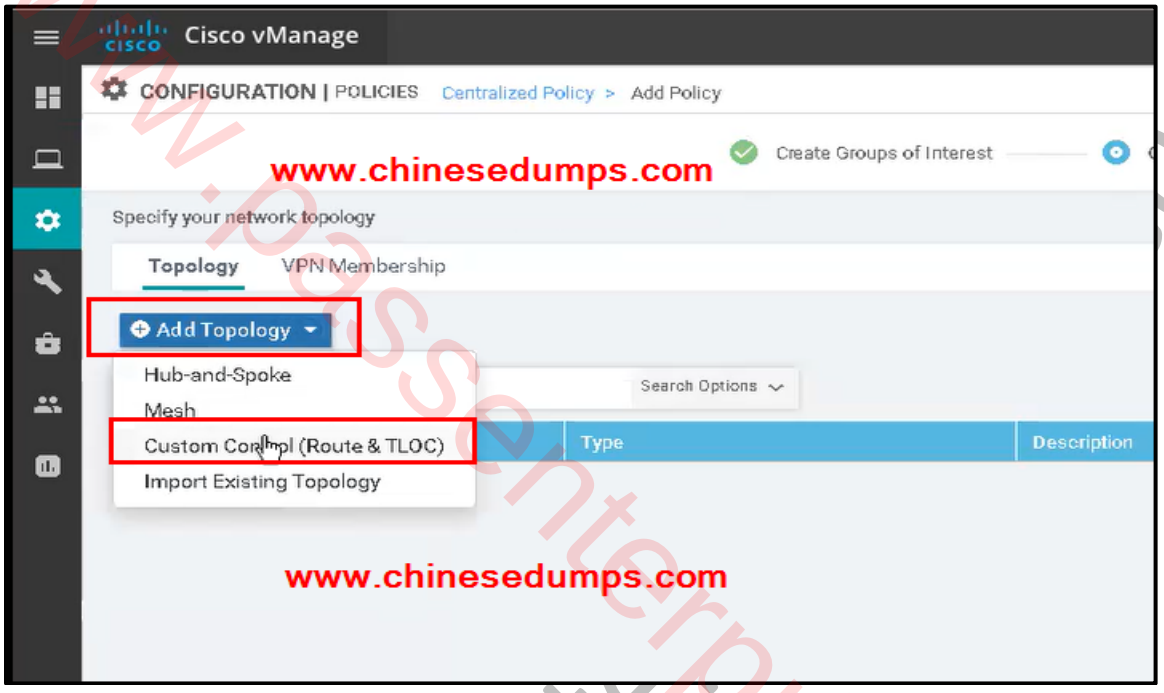
Step 12:

Enter **Name** and **Description** and **Save Control Policy**



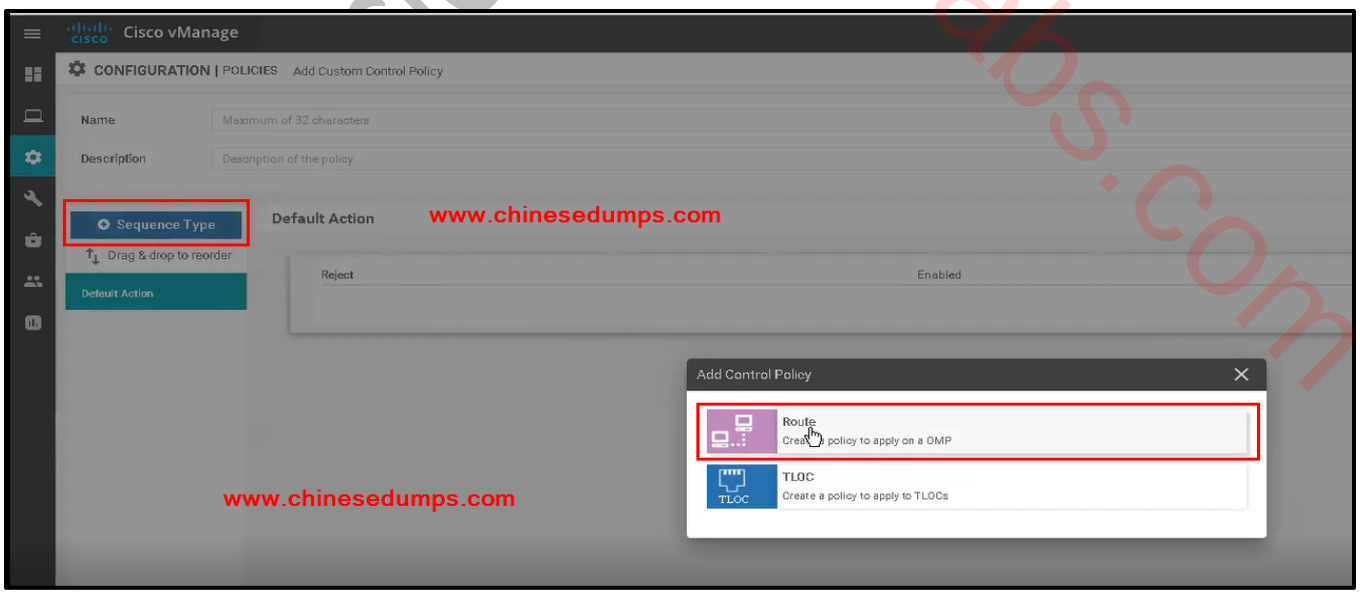
Step 13:

Click on Add **Topology** and select **Custom Control** to add another Policy



Step 14:

Add a **Sequence Type** and add a **Route Control Policy**

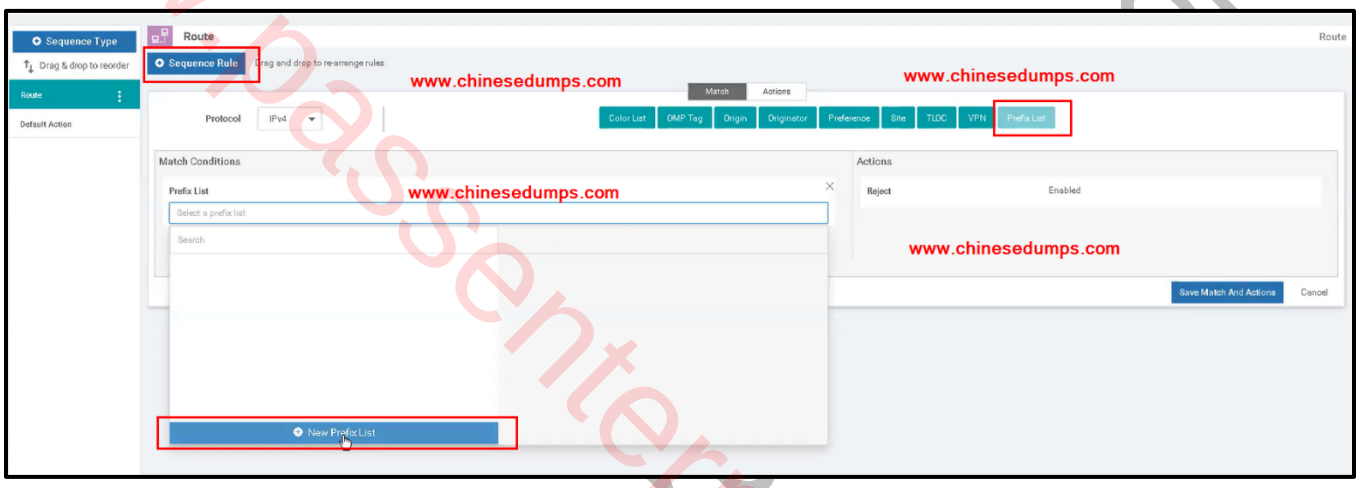


Step 15:

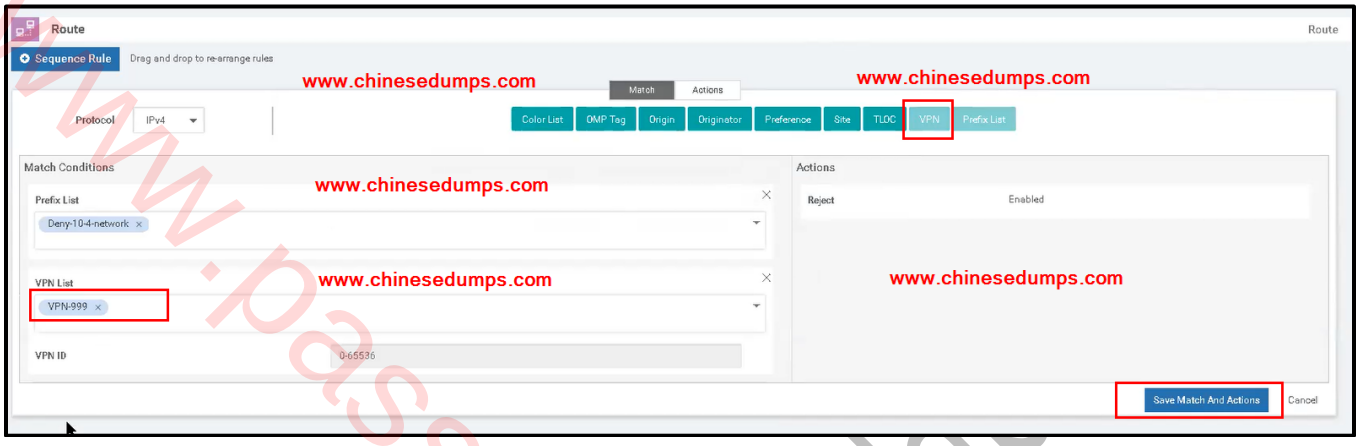
Add **New Sequence**

Select **Prefix-list**

Add **New-Prefix-list**



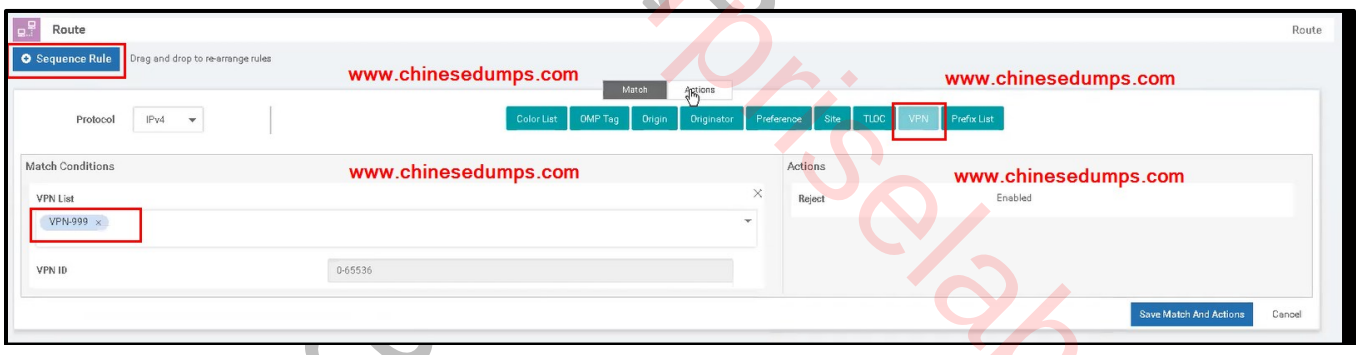
Click on VPN and select VPN 999



Step 16:

Add another Sequence Rule for VPN 999

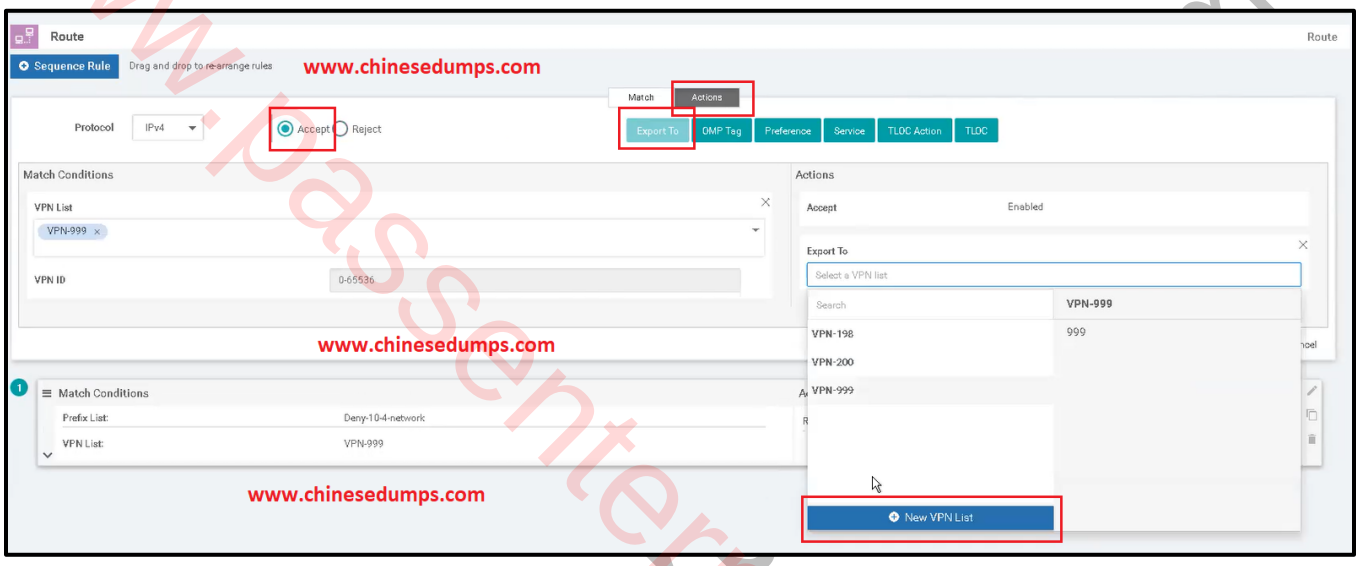
Select VPN 999 from VPN list

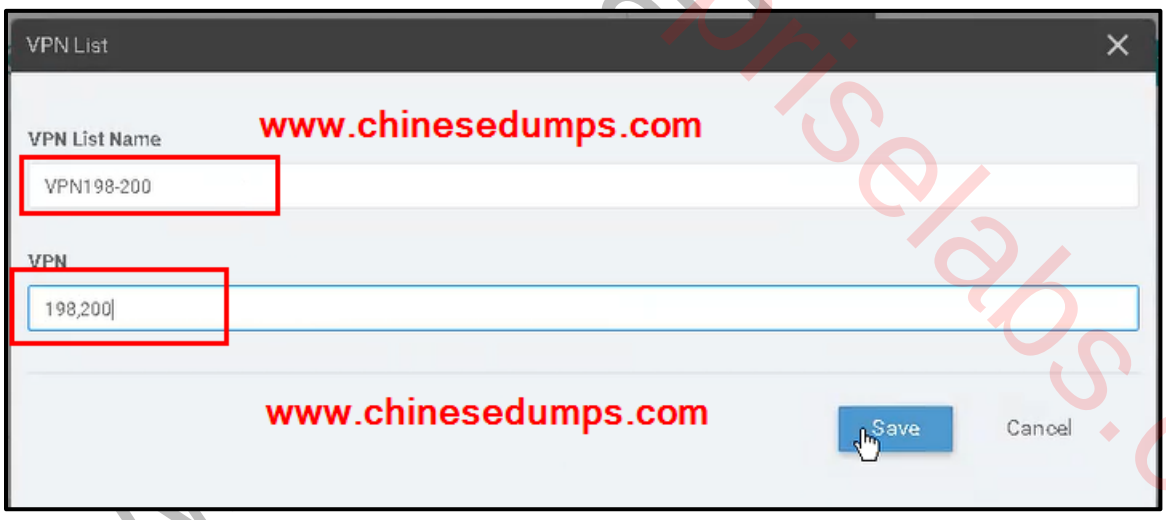


Go to Actions

Select Accept

Select Export To and add a NEW VPN LIST





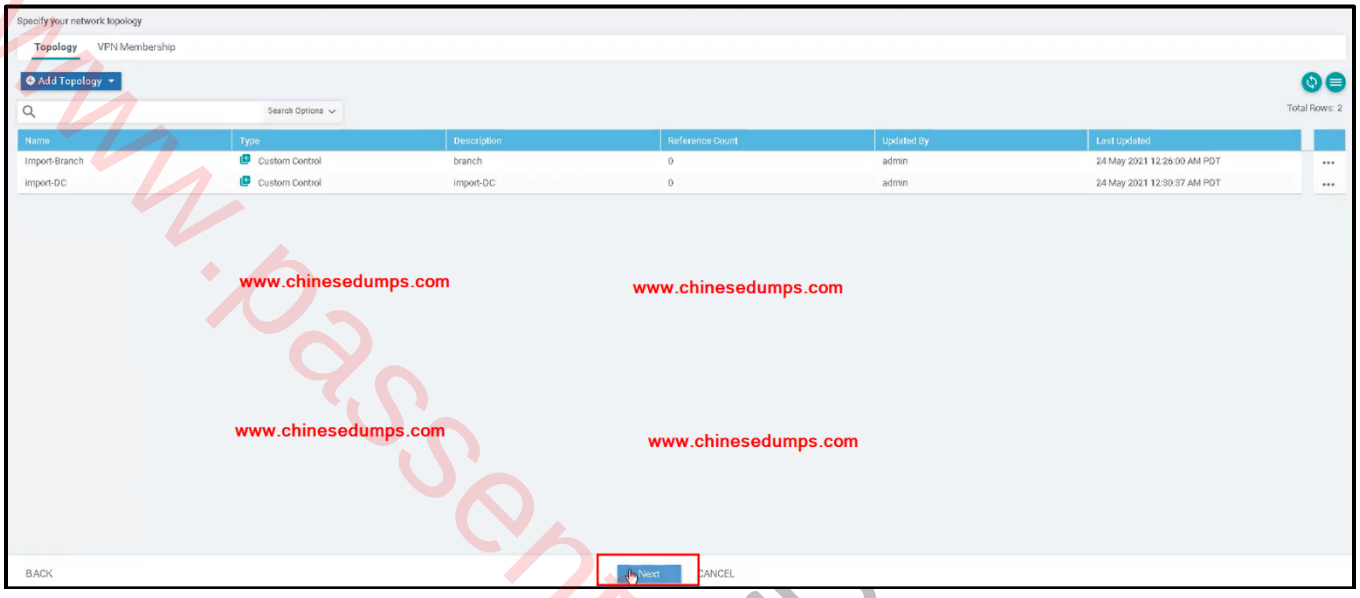
Select VPN list 198-200 under Export To and Save Match and Actions

Step 17:

In Default Actions select Accept

Also Give Name and Description

After adding Hit next 2 times



Step 18:

Under Add Policy

Policy Name

Description

Under **Import-DC**

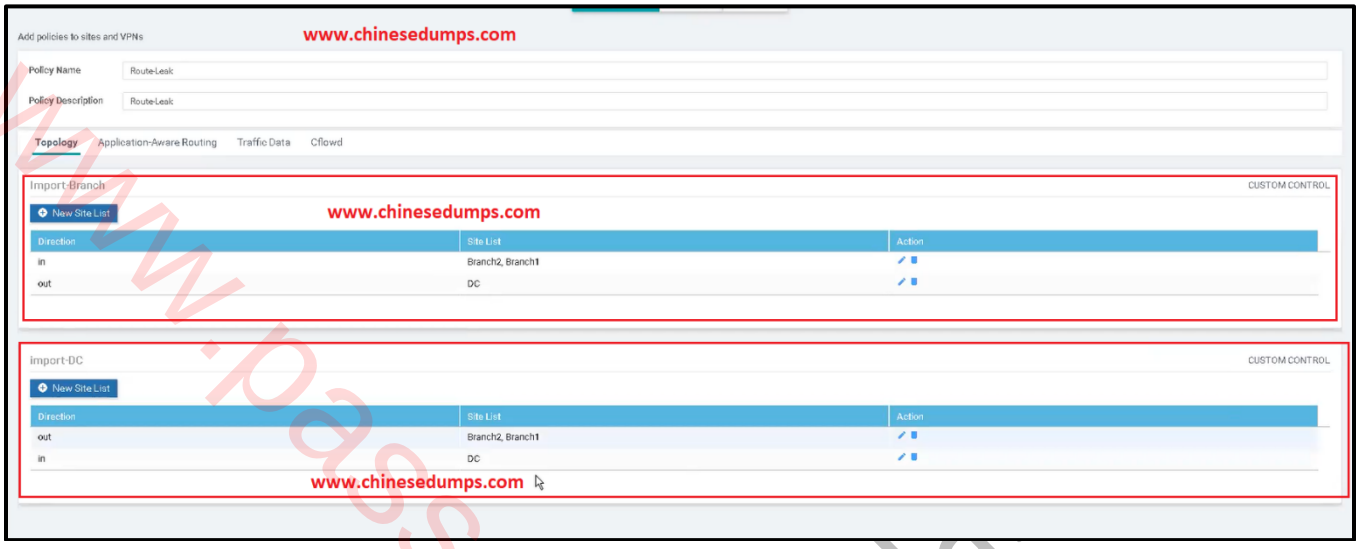
In **New Site List** in **Outbound List** Select **Branch 1** and **Branch 2**

In **New Site List** in **Inbound List** Select **DC**

Under **Import-Branch**

In **New Site List** in **Inbound List** Select **Branch 1** and **Branch 2**

In **New Site List** in **Outbound List** Select **DC**

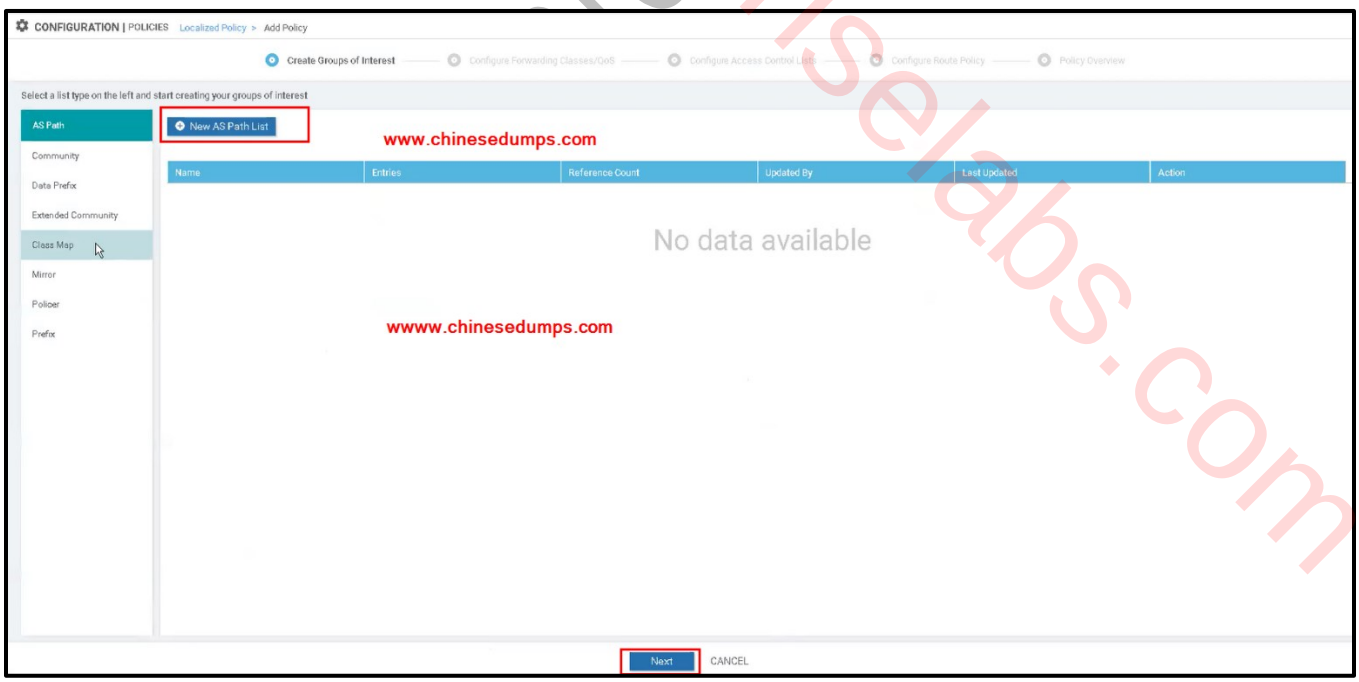


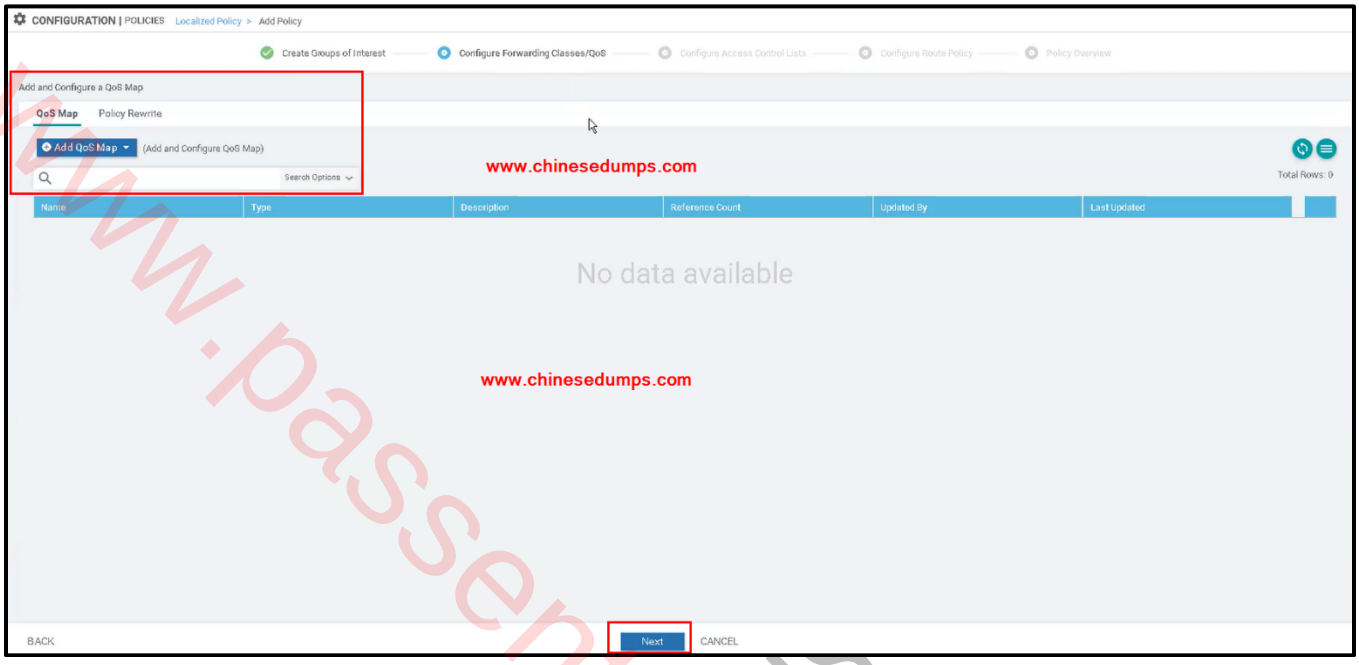
Also Add **New Site-list** as **DC**

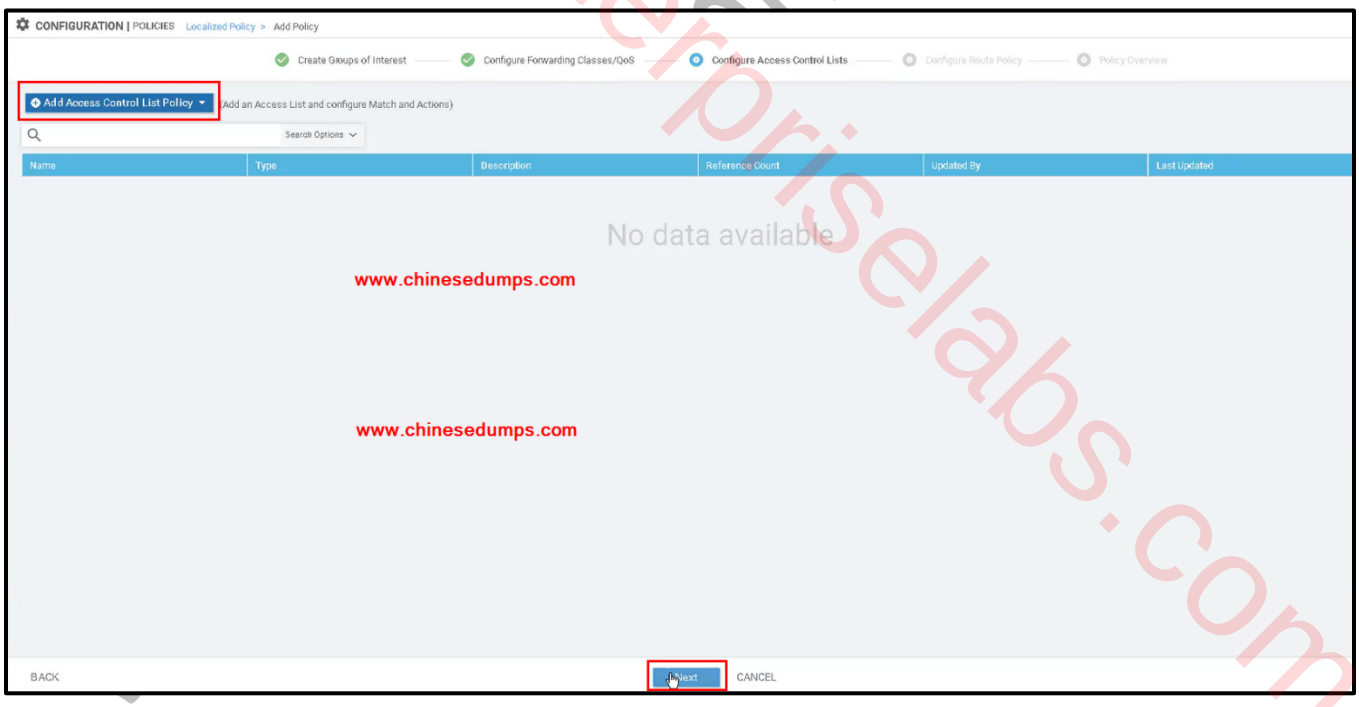
Then Save Policy

Step 19:

Create a Localized Policy







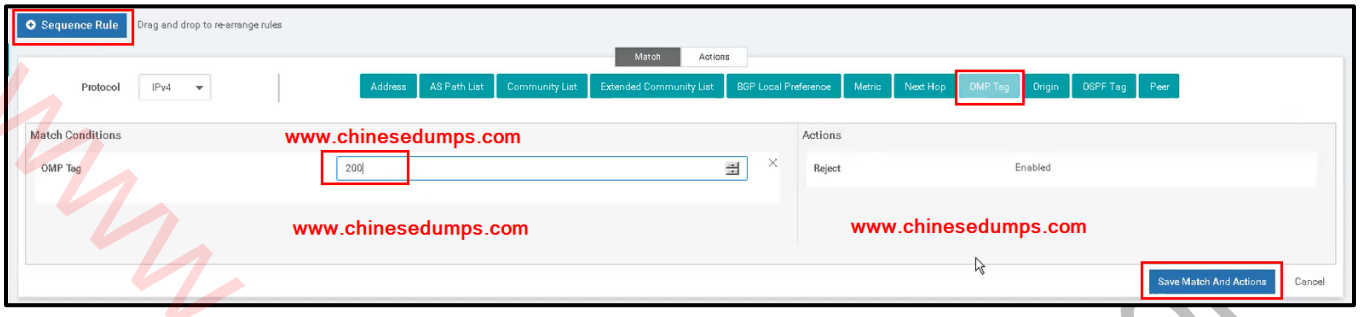
Click on Add Route Policy

Add Name of the Policy

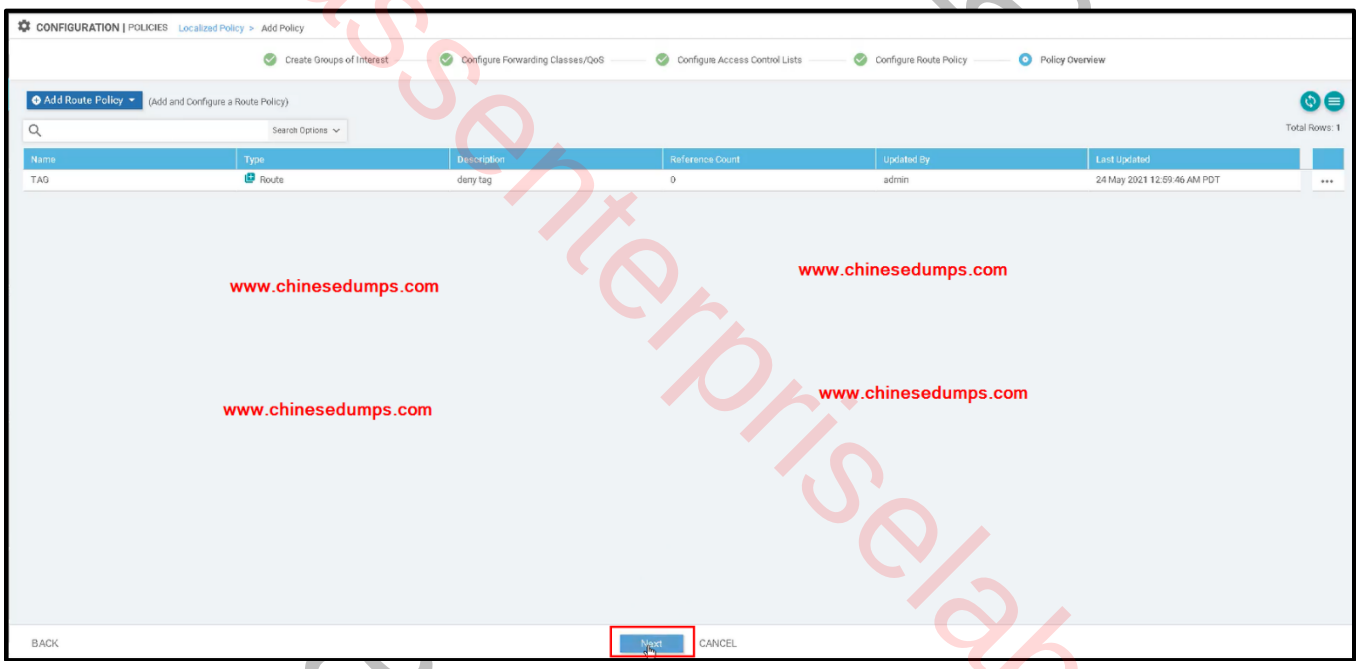
Add Description

Create Sequence Rule for 198 and 200 as below

In Default Action select Accept



Hit NEXT



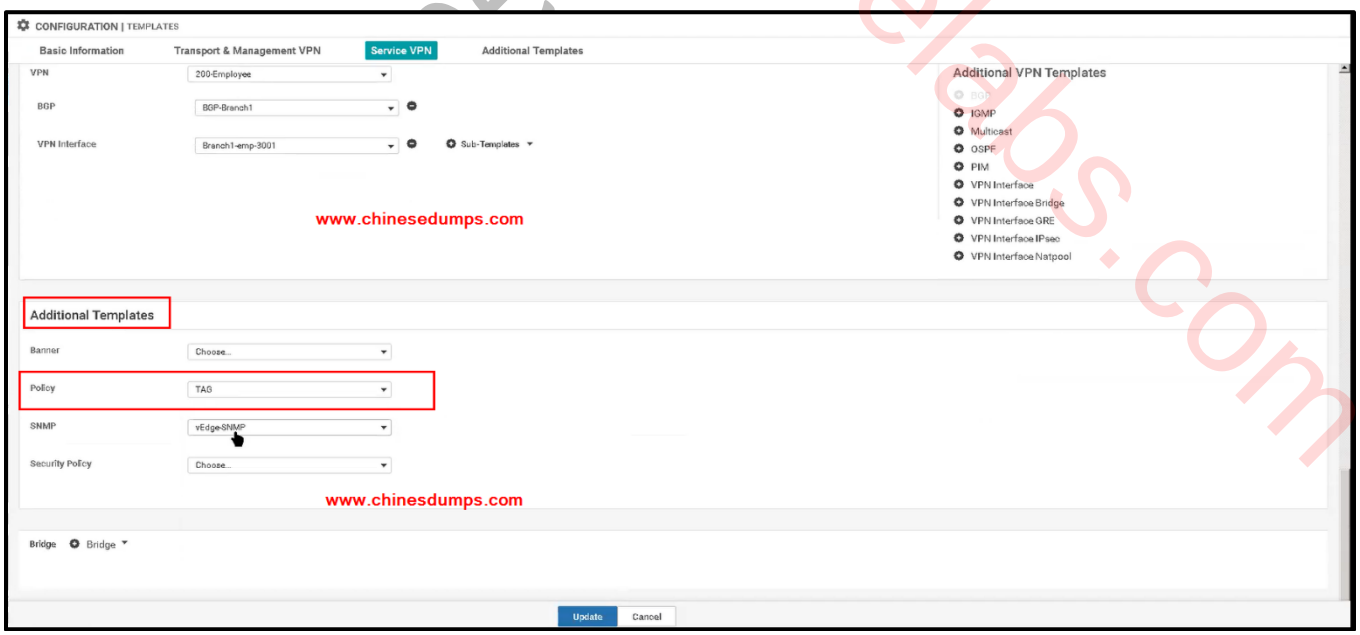
Step 20:

Go Under Device Template

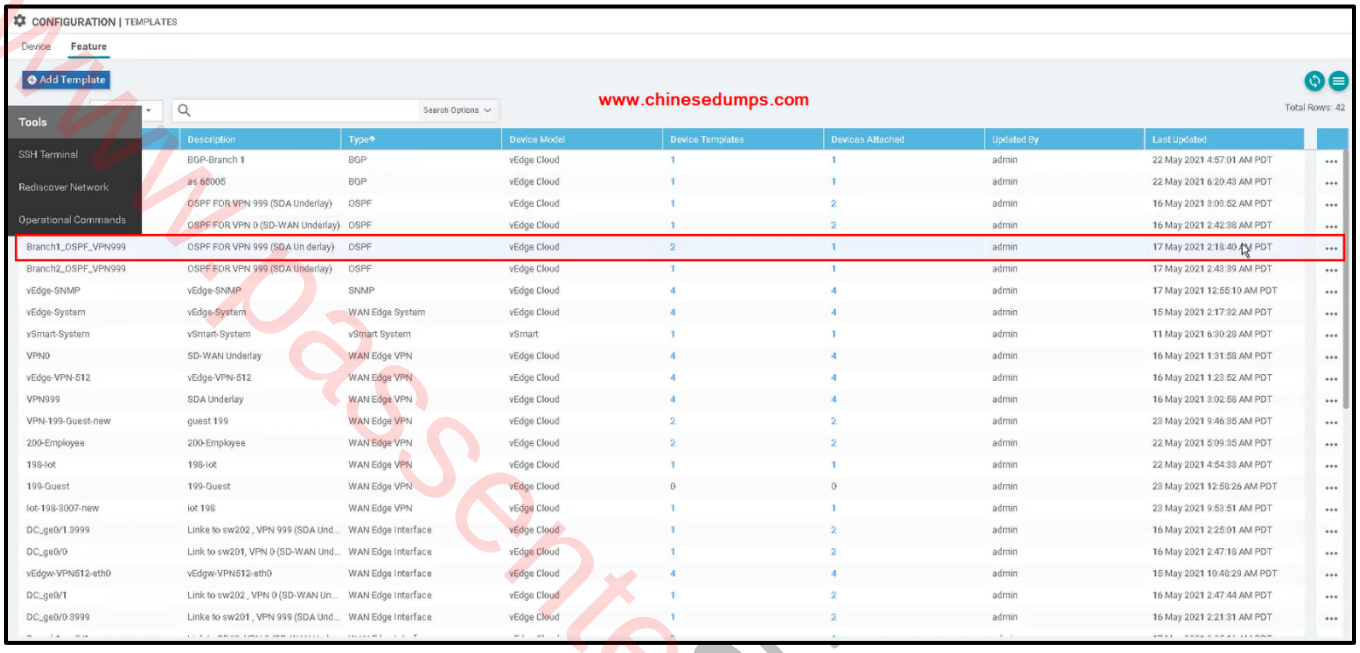
Select Branch 1 Device Template

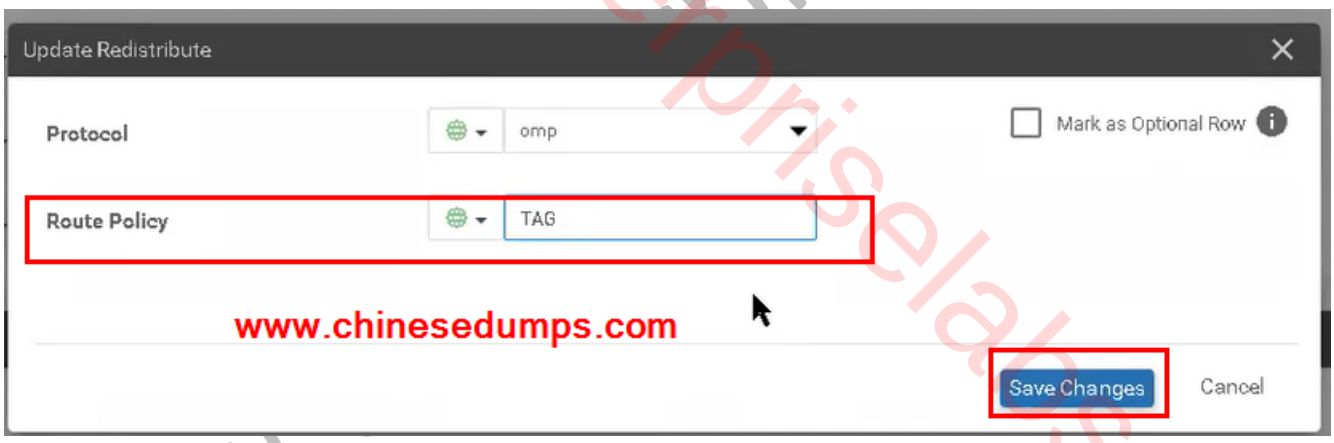
Under Branch 1 Device Template Go to Additional Templates

Add Policy



Go to Branch 1 OSPF VPN 999 Feature Template and add the tag under New redistribution





Click on Update

Repeat the Step 20 for Branch 2

2.5: Handling Guest Traffic

The guest VN/VPN on Branches #1 and #2 must remain isolated from the rest of the company network. It is only allowed to reach internet through r23 and r24 in the DC. Enable internet connectivity for the Guest VPN according to these requirements:

- On vedge21 and vedge22, place the ge0/2 interfaces into the Guest VPN 199.
- On r23 and r24, create a new VRF named Guest using the RD of 65002:199, and place the gi4 interfaces into this VRF.
- Assign addresses to these interfaces:
  - R23 gi4: 10.2.123.1/24
  - R24 gi4: 10.2.224.1/24
  - Vedge21 ge0/2: 10.2.123.2/24
  - Vedge22 ge0/2: 10.2.224.2/24
- Peer r23 and vedge21 in the Guest VRF/VPN using iBGP.
- Peer r24 and vedge22 in the Guest VRF/VPN using iBGP.
- Ensure that r23 and r24 learn the routes in the Guest VRF/VPN over iBGP.
- On r23 and r24, configure a static default route in the Guest VRF and point it to the ISP's IP address 200.99.23.1 or 200.99.24.1 as appropriate. Advertise this default route in iBGP to vedge21 and vedge22.
- On r23 and r24, configure PAT to allow the Guest VPN to access internet by translating it to the router address on the link toward the ISP. Reuse the NAT ACL already created on the router. Do not use NAT pools.

Configure r23 as the DHCP server for Guest VPN according to these requirements:

- Create Loopback1 interface on r23 associated with the Guest VRF and having the IP address 10.2.255.211/32
- Advertise this prefix in BGP toward vedge21.
- Create DHCP pool named br1_guest for branch #1 Guest subnet.
- Create DHCP Pool names br2_guest for branch #2 Guest subnet.
- Explicitly associate both DHCP pools with the VRF guest.
- In each subnet, assign addresses from .101 up to .254 inclusively, and the appropriate gateway to clients.
- Associate host42 and host52 with the guest VN in DNAC, and make sure that both hosts receive the appropriate address.
- Make sure that host42 and host52 can ping 8.8.8.8 in the ISP cloud

4 Points

Solution:

r23

```
router bgp 65002
neighbor 200.99.23.1 remote 19999

vrf def Guest
rd 65002:199
address-fam ipv4
exit

int gi 4
vrf for Guest
ip add 10.2.123.1 255.255.255.0
ip nat inside

int gi 1
ip nat out
exit

ip access-list stand NAT
permit 10.0.0.0 0.255.255.255
exit

router bgp 65002
address-fam ipv4 vrf Guest
neighbor 10.2.123.2 remote 65002
network 10.2.255.211 mask 255.255.255.255
net 0.0.0.0 mask 0.0.0.0

ip nat inside list NAT int gig 1 vrf Guest overload

ip route vrf Guest 0.0.0.0 0.0.0.0 200.99.23.1 global

int loo1
vrf for Guest
ip add 10.2.255.211
exit
```


```
ip dhcp class branch1
exit

ip dhcp pool br1_guest
network 10.4.199.0 /24
default-router 10.4.199.1
class branch1
address range 10.4.199.101 10.4.199.254

ip dhcp class branch2
exit

ip dhcp pool br2_guest
network 10.5.199.0 /24
default-router 10.5.199.1
class branch2
address range 10.5.199.101 10.5.199.254
ip dhcp use connected vrf
```

r24

```
vrf def Guest
rd 65002:199
address-fam ipv4
exit

int gi 4
vrf for Guest
ip add 10.2.224.1 255.255.255.0
ip nat inside

int gi 1
ip nat out

ip access-list stand NAT
permit 10.0.0.0 0.255.255.255
exit
```

router bgp 65002
address-fam ipv4 vrf Guest
neighbor 10.2.224.2 remote 65002
network 0.0.0.0 mask 0.0.0.0

ip nat inside list NAT int gig 1 vrf Guest overload
ip route vrf Guest 0.0.0.0 0.0.0.0 200.99.23.1 global

ip dhcp use connected vrf

Step 1:

In DC Device Templates

Under Service VPN add VPN 199 (Guest)

Under VPN 199 add Interface Template and BGP Template

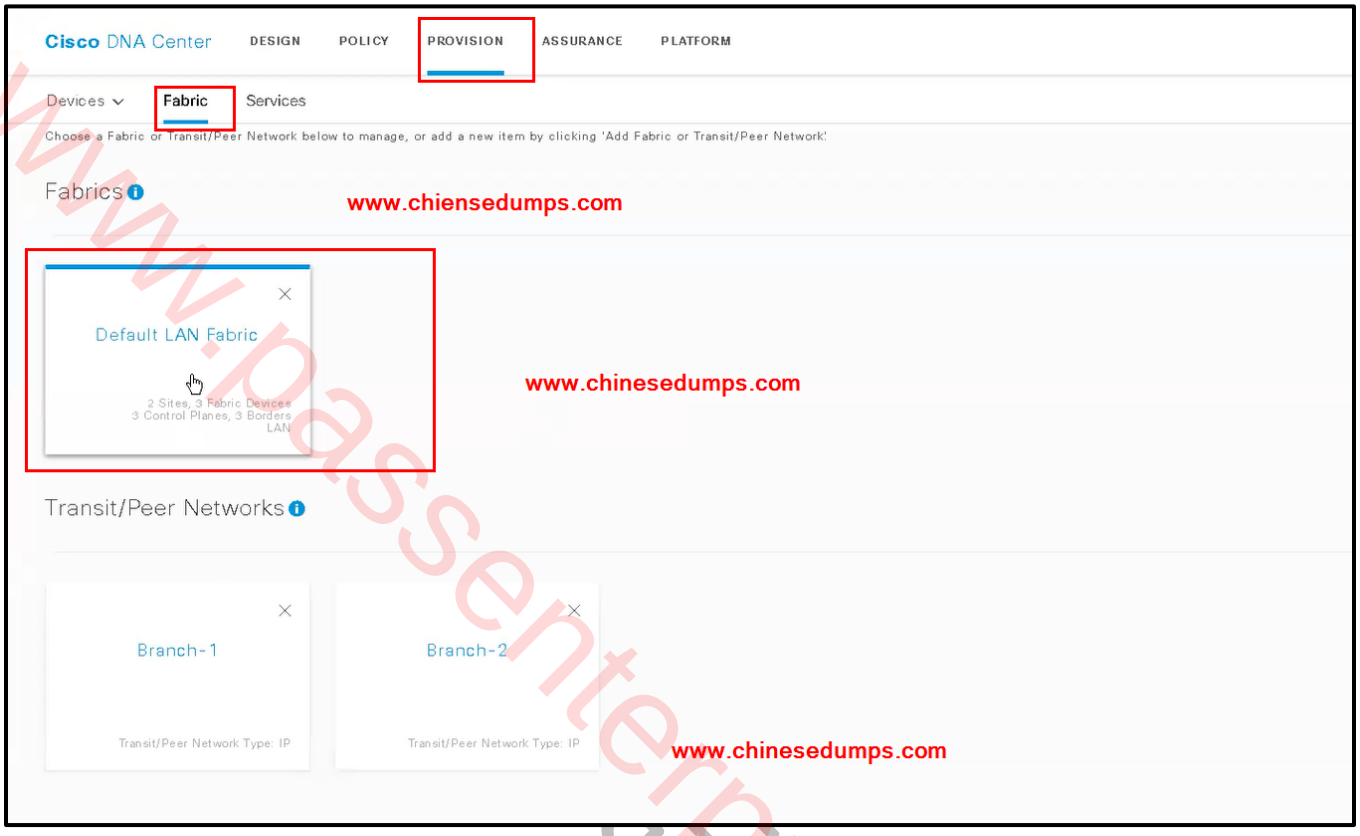
Click **SAVE**

Click Update in DC Device Template

Step 2:

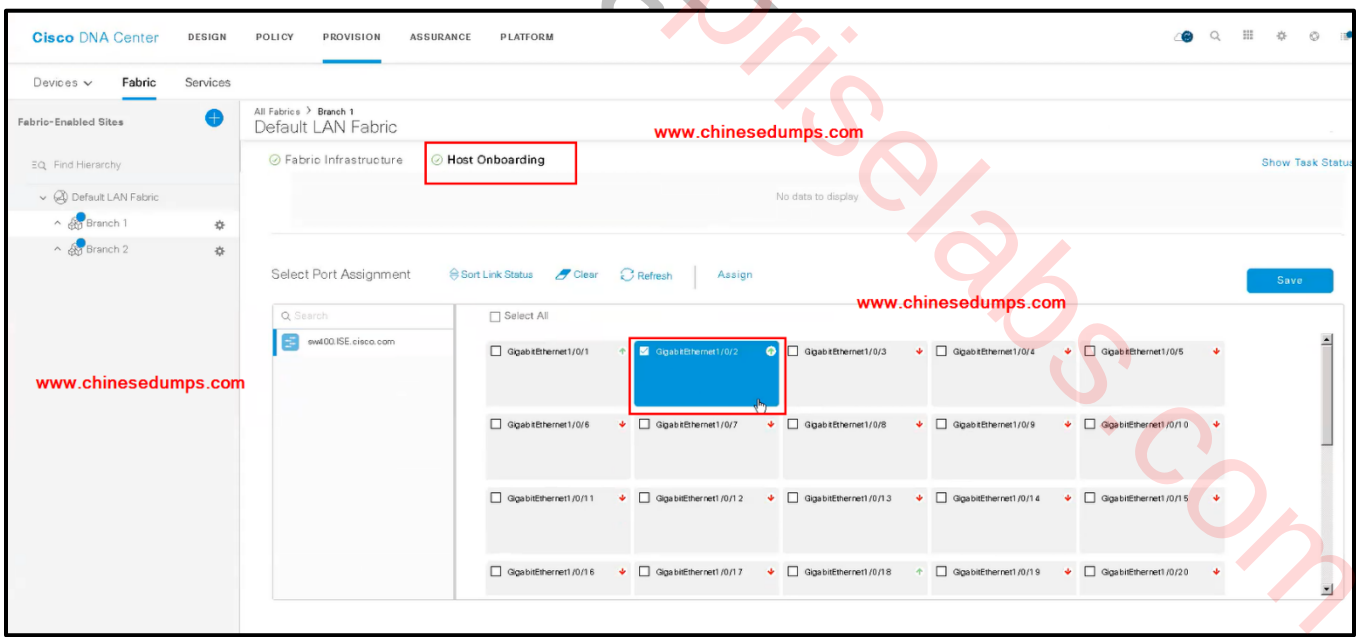
Go Under DNAC

Go to Provision > Fabric Default LAN Fabric

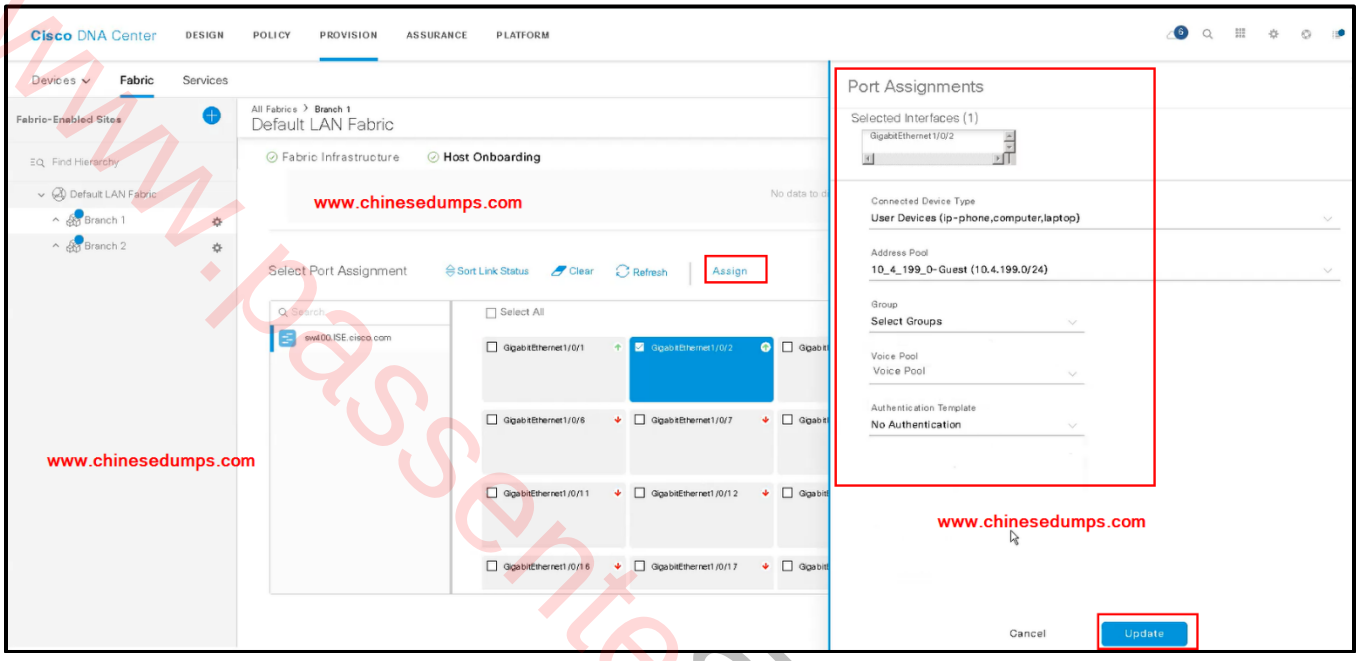


Select Branch 1

Go to Host Onboarding



Select the details as per below screenshot



Then SAVE and Apply

2.6: Support for silent Hosts in Branch #2

This item consists of multiple questions. You may need to scroll down to be able to see all questions.
In future, Branch #2 will be equipped with IP-based IoT endpoints operating in speak-when-spoken-to mode, also called silent hosts. Which of the following SDA features enables a working connectivity with these IoT endpoints?

- Native Multicast
- Endpoint Mobility
- Layer 2 Flooding
- Layer 2 Extension

In the statement below, select one of the options from the drop-down list to complete the sentence and form a correct statement.

For SDA to support silent hosts, _____Select Option_____ in the underlay as a prerequisite.

Options:

- IP multicast routing with PIM-SM must be enabled
- No additional capability aside from unicast IP connectivity is required
- IS-IS must be used as a routing protocol
- DHCP Snooping must be enabled

3 Points

Answer: Layer 2 Flooding
Answer: IP Multicast routing with PIM-SM must be enabled

3.1: Enabling CLI access to r30

There is no direct console access provided to the router r30. Moreover, r30 does not accept any remote connections because its VTY lines are configured with transport input none. Using RESTCONF, enable remote access to r30 for all remote access protocols, according to these requirements:

- You can use host31 to access router r30 using IP address 10.3.11.1
- You can use any method of accessing the RESTCONF API on r30 from host31, including curl, Python, or Postman
- You must change the input transport protocol on all configurable VTY lines
- The input transport protocol value setting must be changed from none to all

Important parameters:

- Username/password for HTTP authentication
  - admin/admin
- URL
  - https://10.3.11.1:443/restconf/data/Cisco-IOS-XE-native/line/vty
- HTTP method to retrieve the configuration
  - GET
- HTTP method to modify the configuration
  - PATCH
- HTTP headers
  - Content-Type: application/yang-data+json
  - Accept: application/yang-data+json
- Recommended curl switches
  - –i,-k,-X,-H,-u,-d

2 Points

Solution:

On Chinesedumps.com-r30:

Chinesedumps.com-r30#conf t
Chinesedumps.com-r30(config)# ip http server
Chinesedumps.com-r30(config)# ip http authentication local
Chinesedumps.com-r30(config)# ip http secure-server

Chinesedumps.com-r30(config)# username admin privi 15 secret admin

Chinesedumps.com-r30(config)# restconf

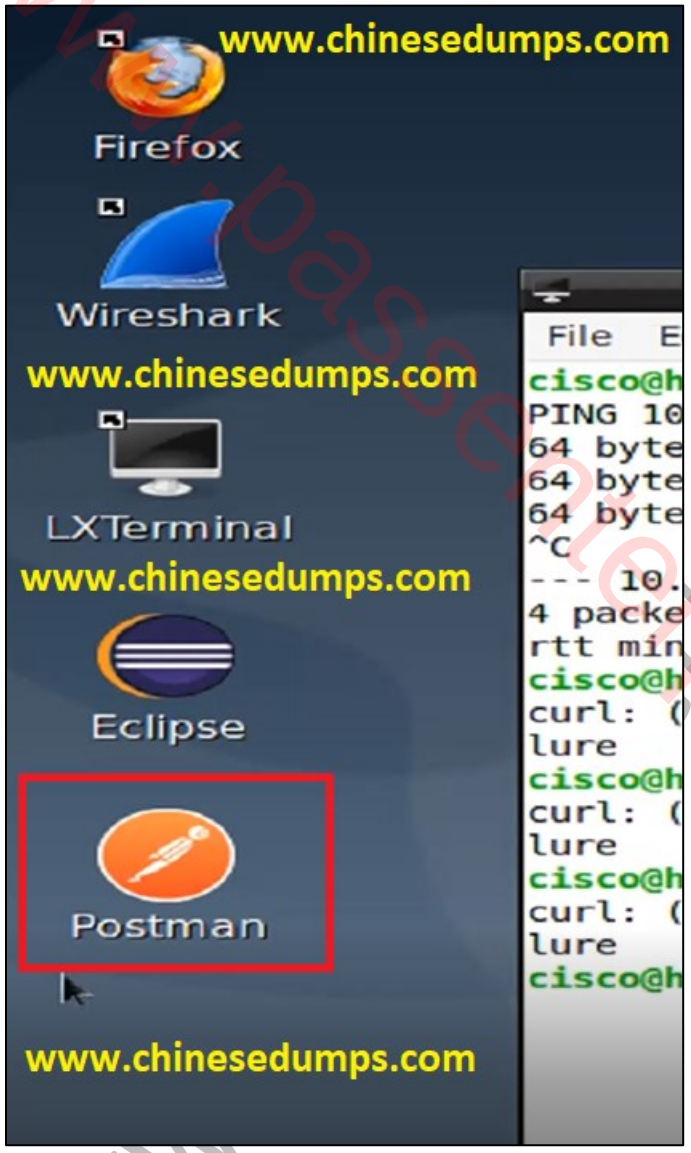
Chinesedumps.com-r30(config)#interface GigabitEthernet2
Chinesedumps.com-r30(config-if)#no shutdown
Chinesedumps.com-r30(config-if)#ip address 10.3.11.1 255.255.255.0
Chinesedumps.com-r30(config-if)#negotiation auto

Step 1:

Open Linux machine host31 and check reachability for r30 , also check restconf reachability

Step 2:

From linux Machine open Postman

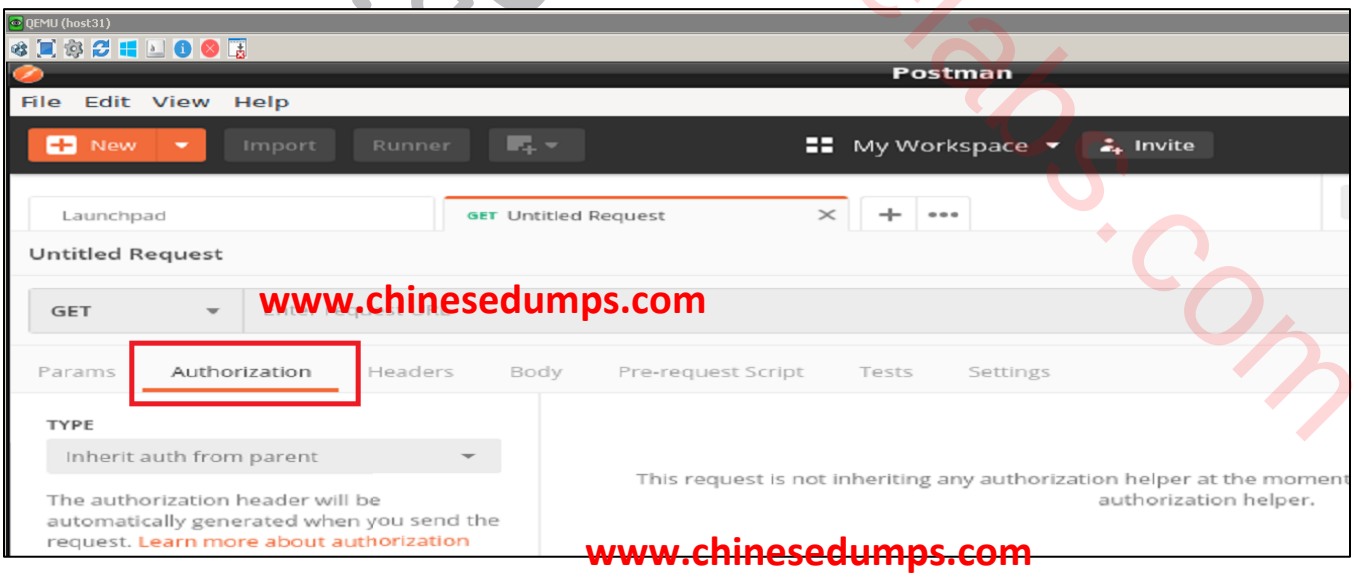


Step 3:

In postman select **Create a request**

Step 4:

Go under **Authorization** tab

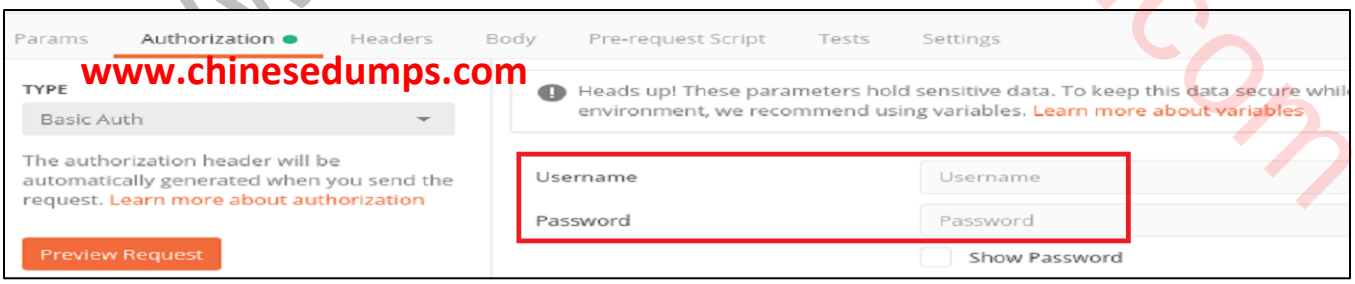


Step 5:

Under **Type** select **Basic Auth**

Step 6:

Insert Username/Pasword : **admin/admin**

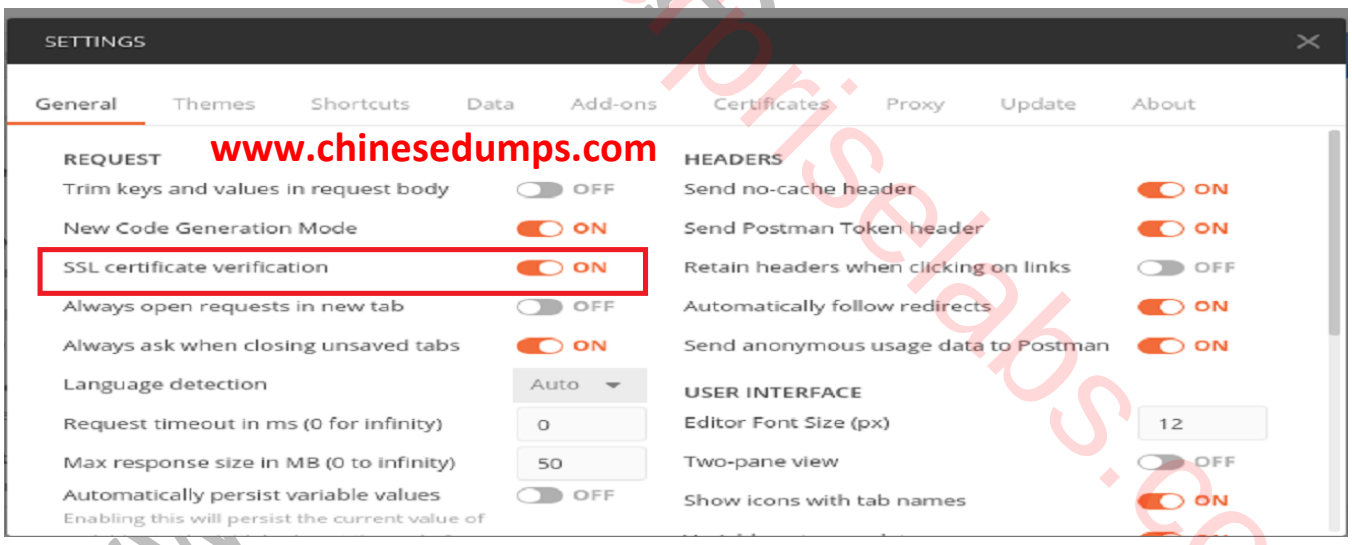


Step 7:

Select **Setting** and then **Default setting**

Step 8:

Turn off the **SSL Certificate verification**

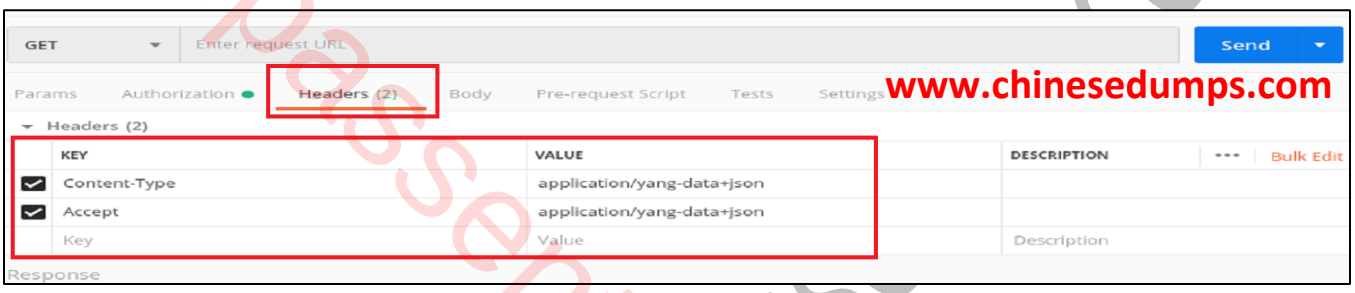


NOTE: This step 8 is sometimes not mandatory to perform in LAB

Step 9:

Select **Headers** tab and create to header

- HTTP headers
  - Content-Type: application/yang-data+json
  - Accept: application/yang-data+json



Step 10:

Enter the **URL** under **GET** and hit **SEND**

- URL
  - https://10.3.11.1:443/restconf/data/Cisco-IOS-XE-native:native/line/vty

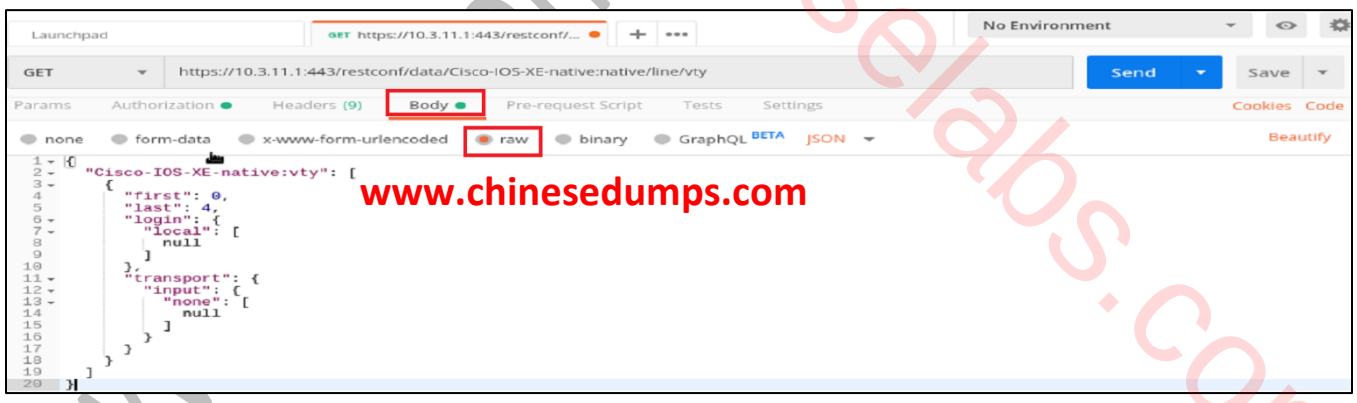
Step 11:

The above step 10 will generate an output in **Body** tab

Copy the generated output

Step 12:

Paste the generated output in **Body** > **RAW**



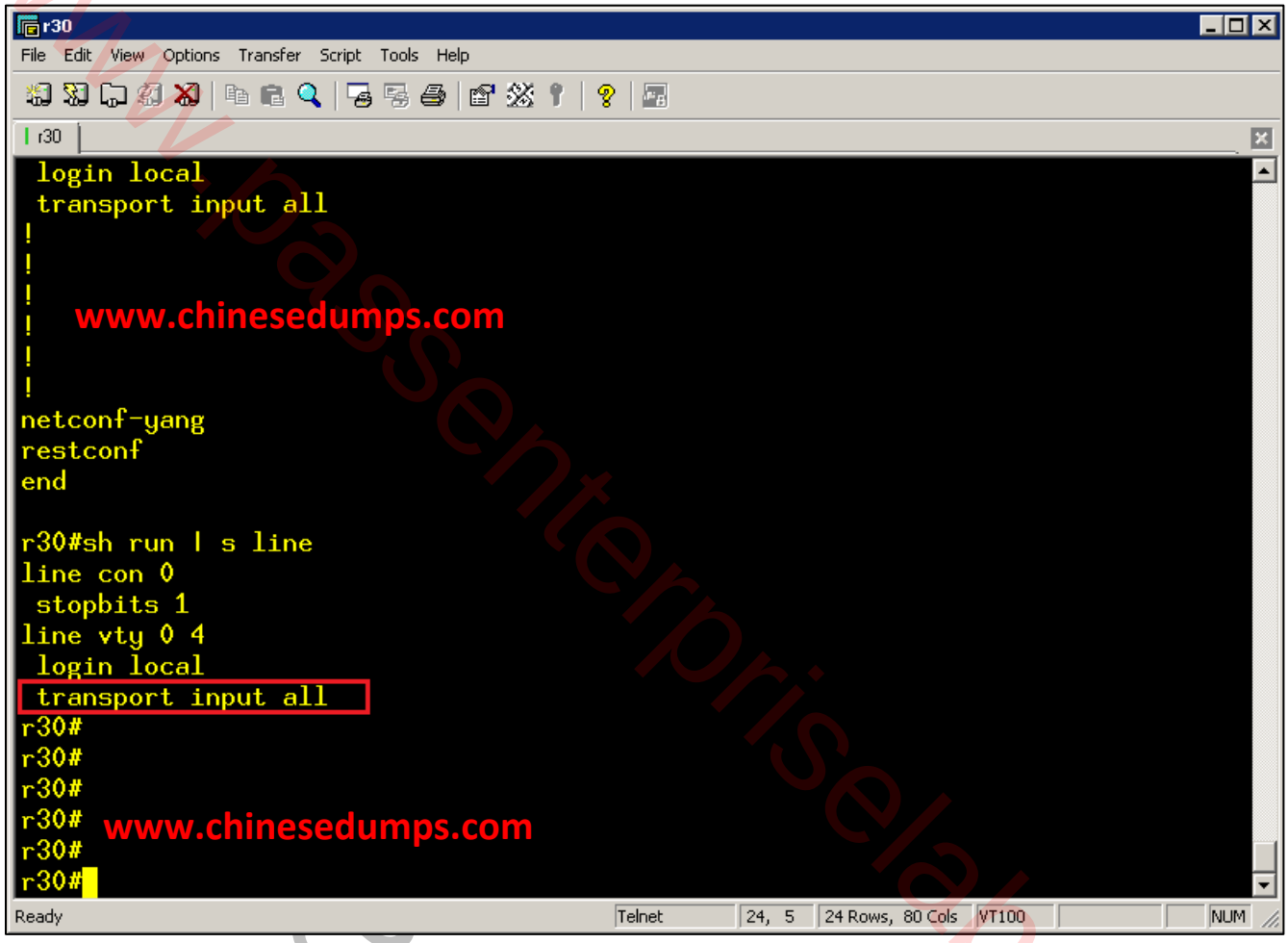
Step 13:

Change the **transport input** option from **"none"** to **"all"**

Then **Patch** the output by selecting **Patch** from the list

Verification:

Go to **CLI of r30** and run command **show run | s line**



3.2: Using Guest shell and python on r30

On r30, enable guestshell and create a python script named ribdump.py in the guestshell according to these requirements:

- If an additional IP network is necessary to start guestshell, you are allowed to use addresses from the range 192.168.255.0/24. This range must not be advertised in any routing protocol.
- The python script must be saved under the name ribdump.py in the home directory of the guestshell user.
- The purpose of the script is to display the complete contents of all routing tables in non-default VRFs created on the router.
- The script must execute the show ip route vrf… or show ipv6 route vrf… command for every non default VRF created on the router, depending on what address families are enabled in that VRF.
- The script must determine the list of created VRFs and enabled address families dynamically every time it is run using, for example, show vrf brief | include ipv
- The script must not attempt to display the VRF routing table for an address family that is not enabled in the VRF.
- It must be possible to run the script using the guestshell run python ribdump.py command from privileged EXEC mode.

3 Points

Solution:

- Need to enable Guestshell which needs IOX service to run
- Intent of script
- Execute command "show vrf brief | include ipv" and store output in a variable named vrf
- Run for loop for each vrf in variable vrf
- Check if ipv4 and ipv6 address family is in the vrf
- And execute the "show ipvx route vrf x" command per vrf, keep the output in variable and print the variable

Chinesedumps.com-r30

r30#conf t
r30(config)#iox

r30(config)#interface VirtualPortGroup0
r30(config-if)#ip address 192.168.255.1 255.255.255.0
r30(config)#exit

r30(config)#app-hosting appid guestshell
r30(config)#app-vnic gateway1 virtualportgroup 0 guest-interface 0
r30(config)#guest-ipaddress 192.168.255.2 netmask 255.255.255.0
r30(config)#app-default-gateway 192.168.255.1 guest-interface 0
r30(config)#name-server0 8.8.8.8
r30(config)#end

***Block this prefix to get advertised out in case connected redistribute or network statement is advertising this subnet**
***create a prefix list to deny 192.168.255./24 and allow everything else**
***apply on bgp neighbor**

r30#guestshell enable

***wait untili guestshell is enabled**

r30#guestshell run bash

***you will get its Linux BASH shell (most of linux bash shell commands will run)**
***create a file named rib dump using vi editor (better learn the shortcut/commands to use vi editor)**

vi ribdump.py

The above command will edit the ribdump.py file

To insert into the editor hit " i "

Paste the below Script in the file and save

Script : Be mindful of indentation used else script will fail

```
import sys
import cli

vrf = cli.execute('show vrf brief | include ipv')
for line in vrf.splitlines():
 ipv4 = False
 ipv6 = False
 vrfString = line.split()
 if(vrfString[2] == "ipv4"):
  ipv4 = True
 elif(vrfString[2] == "ipv6"):
  ipv6 = True
 elif(vrfString[2] == "ipv4,ipv6"):
  ipv4 = True
  ipv6 = True
 if(ipv4 == True):
  vrfv4 = cli.execute('show ip route vrf ' + vrfString[0])
  print(vrfv4)
 if(ipv6 == True):
  vrfv6 = cli.execute('show ipv6 route vrf ' + vrfString[0])
  print(vrfv6)
```

To exit the editor :

Press ESC then :wq

Then run the file with the below command

guestshell run python ribdump.py

guestshell ls

Alternate Solution:

Chinesedumps.com-r30

conf t
iox

interface VirtualPortGroup0
ip address 192.168.255.1 255.255.255.0
ip nat inside
exit
ip nat inside source list GS_NAT_ACL interface GigabitEthernet1 overload

ip access-list standard GS_NAT_ACL
permit 192.168.0.0 0.0.255.255

app-hosting appid guestshell
app-vnic gateway1 virtualportgroup 0 guest-interface 0
guest-ipaddress 192.168.255.2 netmask 255.255.255.0
app-default-gateway 192.168.255.1 guest-interface 0
name-server0 8.8.8.8
end

int gi1.100
ip nat outside

guestshell enable
guestshell run bash

vi ripdump.py

The above command will edit the ribdump.py file

To insert into the editor hit " i "

Paste the below Script in the file and save

Script : Be mindful of indentation used else script will fail

```
import sys
import cli

vrf = cli.execute('show vrf brief | include ipv')
for line in vrf.splitlines():
 ipv4 = False
 ipv6 = False
 vrfString = line.split()
 if(vrfString[2] == "ipv4"):
  ipv4 = True
 elif(vrfString[2] == "ipv6"):
  ipv6 = True
 elif(vrfString[2] == "ipv4,ipv6"):
  ipv4 = True
  ipv6 = True
 if(ipv4 == True):
  vrfv4 = cli.execute('show ip route vrf ' + vrfString[0])
  print(vrfv4)
 if(ipv6 == True):
  vrfv6 = cli.execute('show ipv6 route vrf ' + vrfString[0])
  print(vrfv6)
```

To exit the editor :

Press ESC then :wq

Then run the file with the below command

guestshell run python ribdump.py

3.3: Automated Configuration Backup Script

This item consists of multiple questions. You may need to scroll down to be able to see all questions. You are tasked with writing a python script to back up the configuration of a number of IOS-XE devices through RESTCONF, and store the configurations in text files. The starting section of this script has already been written and contains the following lines:

```
#!/usr/bin/python3

import requests

Credentials = [ (“192.168.1.1”, “admin”, “s3cr3t”),
                (“192.168.1.2”, “netadmin”, “0th3rs3cr3t”) ]

Headers = { “Content-Type” : “application/yang-data+Jason”,
            “Accept” : “application/yang-data+Jason” }
```

This script needs to be completed by dragging the individual’s command lines below into their correct order to allow the script to correctly accomplish its purpose. Indicate the ends of the **for** block and of the **while** block by properly placing the **“- -End of for**” and **“- - End of while**” symbols.

Drag the lines into their correct order to complete the script as required. Make sure to also properly place the **“- - End of for**” and **“- - End of with**” symbols to indicate the end of the respective blocks in code.

-- End of with	Command
Response= requests.get (URL,auth=(Login,Password),headers=Headers,verify=False)	Command
For IP,Login,Password in Credentials:	Command
URL=f”https://{IP}:443/restconf/data/Cisco-IOS-XE-native:native”	Command
File.write(Response.text)	Command
With open(f”{IP}.conf”,”w”) as File:	Command
-- End of for	Command

There are plans to extend the script to display a list of known IOS-XE devices by their IP addresses and allow the administrator to select which devices to backup. Aside from other necessary changes in the script, which of the following storage options for the credentials would allow for the most straight forward implementation?

- Credentials = [("192.168.1.1", “admin”, “s3cr3t”),
  (“192.168.1.2”, “netadmin”, “oth3rs3cr3t”)]
- Credentials = { “192.168.1.1” : (“admin”, “s3cr3t”),
  “192.168.1.2”: (“netadmin”, “ oth3rs3cr3t”) }
- Credentials = “192.168.1.1,admin,s3cr3t,” \
  “192.168.1.2,netadmin,oth3rs3cr3t”
- Credentials = [“192.168.1.1, admin, s3cr3t”,
  “192.168.1.2, netadmin, oth3rs3cr3t”]

2 Points

Solution:

```
for IP,Login,Password in credentials:
URL=f"https://{ip}:443/restconf/data/cisco-IOS-XE-native:native"
   Response=request.get(URL,auth=(login,Password),headers=Headers,verify=false)

with open(f"{ip}.conf,"w") as file:
   file.write(reponse.text)let
end of with
end of for
```

Answer: B

Thank You for choosing www.passenterpriselabs.com Workbooks.