CCIE R&S Mock Lab Dumps Section 3-5

Hello, today, BestCiscoDumps will share all the remaining parts of CCIE R&S Lab1, that is, CCIE R&S mock lab dumps section 3-5. It includes some network security technologies and some advanced applications. Although these technologies are rarely used in peacetime, if you can carefully read and understand these knowledge points, your ability will be greatly improved! These technologies are skills that only CCIEer will know!

Click the link to view the CCIE R&S Lab Topology and CCIE R&S Mock Lab Dumps Section 1
Click the link to view the CCIE R&S Mock Lab Dumps Section 2
The current page is CCIE R&S Mock Lab Dumps Section 3-5

SECTION 3 – VPN Technology

SECTION 3.1: MPLS VPN Part 1

Refer to "Diagram 3: BGP Topology" and "Diagram 4: VPN Technology"

- The ACME Headquarters network (AS 12345) uses MPLS L3VPN in order to clearly separateremote site networks
- The ACME corporate security policies are centralized and enforced at the San Jose site (AS65112) for all remote sites. The policies require that all traffic that is originated from any remote sites (with the exception of AS 34567) to the Internet is routed via R20 in AS 65112 Configure MPLS L3VPN in the ACME network according to the following requirements
- Enable LDP only on required interfaces on all seven routers in AS 12345
- Use the interface Lo0 to establish LDP peering
- Ensure that no MPLS interface that belongs to any router in AS 12345 is visible on atraceroute that originates outside of the AS
- R2, R3, R6 and R7 must be configured as PE routers
- R1, R4 and R5 must be configured as P routers

Note: The simulator's R6, R7 includes: no mpls ip propagate-ttl

R2, R3, R6, and R7 on the examination room must manually type :no mpls ip propagate-ttl

Solution:

R1/R2/R3/R4/R5/R6/R7:

mpls ldp router-id lo0 force

router ospf 12345

mpls ldp autoconfig area 0

R2/R3/R6/R7:

no mpls ip propagate-ttl

Note: no ip igmp snooping //on the examination room, if the MPLS LDP neighbor does not established, type this command.

SECTION 3.2: MPLS VPN Part 2

Refer to "Diagram 3: BGP topology" and "Diagram 4: VPN Technology"

The global and regional service providers have agreed to transport the ACME network according to the following requirements

Complete the configuration of MPLS L3VPN in the ACME network according to the following requirements

- R1 must reflect VPNv4 prefixes from any PE to any other PE in AS 12345
- R2 and R3 must establish an EBGP peering with both global service providers (As 10001and AS 10002) for the following VRFs:
  - VRF “BLUE”
  - VRF “GREEN”
  - VRF “RED”
  - VRF “YELLOW”
  - VRF “INET”
- R6 must establish an EBGP peering with the regional service provider (AS 20001) for the following VRFs only:
  - VRF “GREEN”
  - VRF “BLUE”
  - VRF “INET”
- R7 must establish an EBGP peering with the regional service provider (AS 20002) for the following VRFs only:
  - VRF “BLUE”
  - VRF “RED”
  - VRF “INET”
- All IP addressed used for EBGP peering must pass the BGP's directly connected check
- No BGP speaker is AS 12345 may use the network or redistribute statement under anyaddress-family of the BGP router configuration
- At the end of the exam scenario, the interface e0/0 of the gateway router in any remotesite must be able connect to the interface e0/0 of any other remote gateway that belong to AS 65111 or AS 65112 and AS 65222
- Use the following tests as examples of connectivity checks

```
R12:ping 10.2.19.1 so e0/0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.19.1,timeout is 2 seconds:
Packet sent with a source address of 10.1.12.1
!!!!!
```

```
R12#trace 10.2.19.1 so e0/0
Type escape sequence to abort.
Tracing the route to 10.2.19.1
VRF info:(vrf in name/id,vrf out name/id)
1 201.1.12.1 [AS 65112] 1 msec 0 msec 0 msec
2 201.1.123.2 [AS 65112] 0 msec 1 msec 0 msec
3 10.120.12.1 [AS 65112] [MPLS Label 125 Exp 0] 1 msec 0 msec 1 msec
4 10.120.12.2 [AS 65112] 0 msec 1 msec 1 msec
5 10.120.15.1 [AS 65112] 1mesec 0 msec 5 msec
6 101.1.123.1 [AS 65112] 1 msec 1 msec 1 msec
7 100.1.3.2 [AS 65112] 1 msec 0 msec 1 msec
8 103.2.45.2 [AS 65112] 1mesc 1 msec 0 msec
9 123.20.1.10 [AS 65112] 1mec 1 msec 1 msec
10 10.18.19.19 [AS 65112] 9 msec * 11 msec
```


Solution:

R1:

router bgp 12345 address-family vpnv4

neighbor 123.2.2.2 activate

neighbor 123.3.3.3 activate

neighbor 123.6.6.6 activate

neighbor 123.7.7.7 activate

neighbor IBGP route-reflector-client

R2/R3/R6/R7:

router bgp 12345 address-family vpnv4

neighbor 123.1.1.1 activate

R20:

router bgp 65112

neighbor 10.120.15.1 weight 1000 //Trace 10.2.19.1 source e0/0, let R12's next hop go through R3's e0/3

SECTION 3.3: DMVPN

Configure DMVPN phase 3 in the ACME APAC region (AS 45678 and 65222) as per the following requirements

- Use the preconfigured interface Tunnel0 on all the three routers in order to accomplish this task
- R17 must be configured as the hub router
- R18 and R19 must be the spoke routers and must participate in NHRP information exchange
- Disable send ICMP redirect messages on all three Tunnel0 interfaces

Configure the following parameters on all the three Tunnel0 interfaces

- Configure the bandwidth to 1000 kilobits per second
- Configure the delay to 10000 microseconds
- Adjust the IP MTU to 1400 bytes
- Adjust the TCP maximum segment size to 1360 bytes
- Authenticate NHRP using the string “45678key” (without quotes!)
- Use the NHRP network-id 45678
- Configure the NHRP hold time to 5 minutes
- Ensure that spoke-to-spoke traffic does not transit via the hub

Solution:

R17:

interface tunnel 0

ip address 10.18.19.1 255.255.255.0

tunnel source e0/3

tunnel mode gre multipoint

ip nhrp network-id 45678

ip nhrp map multicast dynamic

ip nhrp authentication 45678key

ip nhrp holdtime 300

no ip redirects

bandwidth 1000

delay 1000

ip mtu 1400

ip tcp adjust-mss 1360

router eigrp CCIE

address-family ipv4 unicast autonomous-system 45678

network 10.18.19.0 0.0.0.255

R18:

interface tunnel0

ip address 10.18.19.18 255.255.255.0

tunnel source Serial1/0

tunnel mode gre multipoint

ip nhrp network-id 45678

ip nhrp map multicast 203.3.17.2

ip nhrp nhs 10.18.19.1

ip nhrp map 10.18.19.1 203.3.17.2

ip nhrp authentication 45678key

ip nhrp holdtime 300

no ip redirects

bandwidth 1000

delay 1000 ip mtu 1400

ip tcp adjust-mss 1360

router eigrp 45678

network 10.18.19.0 0.0.0.255

R19:

interface tunnel0

ip address 10.18.19.19 255.255.255.0

tunnel source Serial1/0

tunnel mode gre multipoint

ip nhrp network-id 45678

ip nhrp map multicast 203.3.17.2

ip nhrp nhs 10.18.19.1

ip nhrp map 10.18.19.1 203.3.17.2

ip nhrp authentication 45678key

ip nhrp holdtime 300

no ip redirects

bandwidth 1000

delay 1000 ip mtu 1400

ip tcp adjust-mss 1360

router eigrp 45678

network 10.18.19.0 0.0.0.255

Meet the needs of the shortest path for data exchange between R18 and R19:

R17:

interface tunnel 0

ip nhrp redirect //Turn on nhrp redirect

router eigrp AS45678

address-family ipv4 unicast autonomous-system 45678

af-interface Tunnel0

no split-horizon

Note: You must turn off the split horizon under tun0. After typing, check that R18 R19 can learn each other's detailed routes.

R18/R19:

interface tunnel 0

ip nhrp shortcut

SECTION 3.4: Encryption

Refer to "Diagram 4: VPN Technology"

Secure the DMVPN tunnel with IPsec according to the following requirements Configure IKE Phase 1 according to the following requirements

- Use AES encryption with the pre-shared key “CCIE” (without quotes)
- The key must appear in plain text in the configuration
- All IPsec tunnels must be authenticated using the same IKE Phase 1 pre-shared key
- Use 1024 bits for the key exchange using the Diff-Hellman algorithm
- Configure a single policy using priority 10

Configure IKE Phase 2 according to the following requirements

- Use CCIEXFORM as the transform-set name
- Use DMVPNPROFILE as the IPsec profile name
- Use IPsec in transport mode
- Use the IPsec security protocol ESP and algorithm AES with 128 bits
- Ensure that the DMVPN cloud is secured using the above parameters
- Use tunnel protection in your configuration

Solution:

R17/R18/R19:

crypto isakmp policy 10

encryption aes

authentication pre-share

group 2

crypto isakmp key 0 CCIE address 0.0.0.0

crypto ipsec transform-set CCIEXFORM esp-aes 128

mode transport

crypto ipsec profile DMVPNPROFILE

set transform-set CCIEXFORM

interface tunnel 0

tunnel protection ipsec profile DMVPNPROFILE

SECTION 4 – Infrastructure Security

- Check what is already preconfigured before jumping to configuration!
- Think about smart configuration options that can greatly speed up the time spent at typing on the key board(use copy/paste when possible)!

SECTION 4.1: Device Security

Configure R20 in the ACME San Jose office as per the following requirements

- All users who connect to R20 via the console port via any vty line using SSH must be prompted with the below message before any other prompt is displayed
  - WARNING!ACCESS RESTRICTED!
- Do not include any extra spaces or any other characters as the ones shown above

Solution:

R20:

banner login #WARNING!ACCESS RESTRICTED!#

banner motd #WARNING!ACCESS RESTRICTED!#

On the examination room, if the desired phenomenon does not appear, knock in the privileged mode: terminal moniter

Or:

line con 0

pass XXX

logging local

no pass

SECTION 4.2 Network Security

Configure the ACME New York office as per the following requirements

- Ensure that interface E0/0-3 of SW3 forward traffic that was sent from expected and legitimate hosts and servers
- SW3 must dynamically learn only one MAC address per port and must save the MAC address in its startup configuration
- SW3 must shut down the port if a security violation occurs any of these four ports

Solution:

SW3:

int range e0/0 - 3

switchport mode access //Pre-configured

switchport port-security

switchport port-security mac-address sticky

switchport port-security violation shutdown //Default

switchport port-security maximum 1 //Default

SECTION 5 – Infrastructure Services

- Check what is already preconfigured before jumping to configuration!
- Think about smart configuration options that can greatly speed up the time spent at typing on the key board(use copy/paste when possible)!

SECTION 5.1: System Management

Configure R20 in the ACME San Jose office as per the following requirements

- Enable SSH access in R20 using the domain name “acme.org”
- R20 must accept up to five remote authorized users to connect at the same time using SSH
- Create the user "test" with the password "test" in the local database of R20
- R20 must produce a syslog message for all SSH connection attempts, regardless of whether it is permitted or denied
- When authenticated, the user “test” must be granted with the privilege level 1
- Do not enable the aaa new-model Command on R20
- Ensure that SSH is the only remote access method that is permitted on VTY lines of R20
- Ensure that the console is not affected by your solution and that no “username” prompt is presented on the console port
- Test your solution from any device that is located in AS 34567 and ensure that the following sequence of commands produces the same output

Solution:

R20:

username test privilege 1 password test

ip domain-name acme.org

crypto key generate rsa modulus 1024

ip ssh maxstartups 5

privilege exec level 1 show privilege

login on-failuer log

login on-success log

ip ssh logging events

line vty 0 4

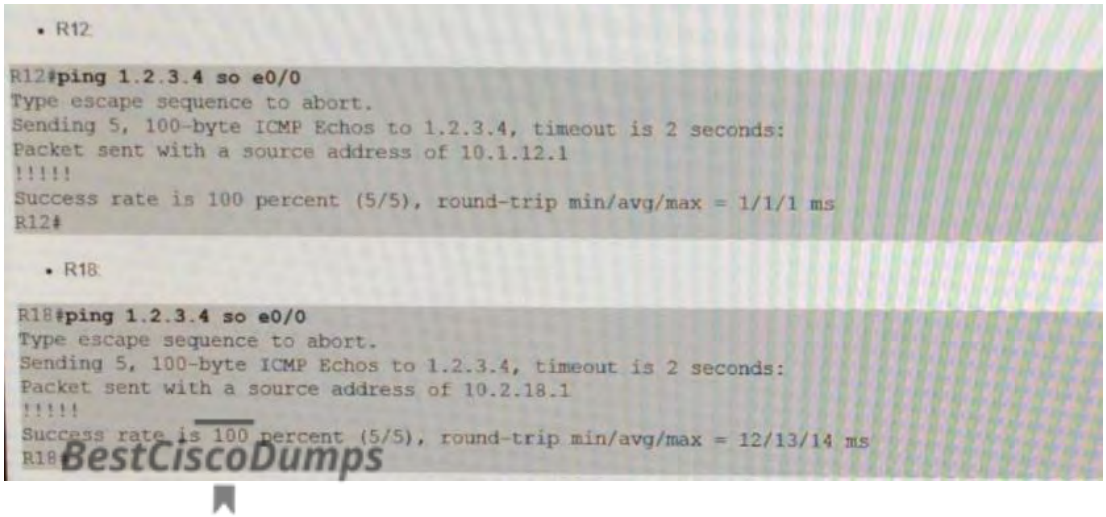
login local

transport input ssh

SECTION 5.2: Network Services

Configure the ACME network as per the following requirements

- R20 must enable all private corporate traffic that is originated from any host with source ip address in 10.1.0.0/16 or in 10.2.0.0/16 to connect to any public destination that is located in AS 34567 or in any services
- All remote sites in AS 65111 and AS 65222 must be able to connect to these public destinations
- R20 must swap the source ip address in these packets with the ip address of its interfaceLo0
- R20 must allow multiple concurrent connections
- Use a standard access-list to accomplish the above requirements
- The following tests must succeed after the above requirements (in addition to previous requirements) are acheived



Solution:

NAT for originating data flows in AS65111

R20:

access-list 20 per 10.1.0.0 0.0.255.255

int e0/0.12

ip nat inside //R12

int e0/0.13

ip nat inside //R13

int e0/0.14

ip nat inside //R14

int e0/1.99

ip nat outside

int e0/0.99

ip nat outside //Since the weight was added to the R20 route, it must be 10.120.99.6, but it can also be used as a backup route for 10.120.99.2

ip nat inside source list 20 interface lo0 overload

Test:

R12: ping 1.2.3.4 source 10.1.12.1 //same as R13/R14

If you do not do NAT on R20, it is impossible to ping successfully because ISP7 does not have a return route.

R20:

debug ip nat

sh ip nat translations

NAT for originating data flows in AS65222

R16:

router bgp 45678

nei 203.3.16.1 prefix-list NAT in

ip prefix-list NAT permit 0.0.0.0/0

ip prefix-list NAT permit 203.3.16.0/22 le 30

R17:

router bgp 45678

nei 203.3.17.1 prefix-list NAT in

ip prefix-list NAT permit 0.0.0.0/0

ip prefix-list NAT permit 203.3.16.0/22 le 30

R18:

router bgp 65222

nei 203.3.18.1 prefix-list NAT in

ip prefix-list NAT permit 0.0.0.0/0

ip prefix-list NAT permit 203.3.16.0/22 le 30

R19:

router bgp 65222

nei 203.3.19.1 prefix-list NAT in

ip prefix-list NAT permit 0.0.0.0/0

ip prefix-list NAT permit 203.3.16.0/22 le 30

R20:

access-list 20 per 10.2.0.0 0.0.255.255

int e0/0.15 ip nat inside

int e0/1.15

ip nat inside //Back up, because ISP3 goes to 1.2.3.4 to match the default route in VRF YELLOW

Test:

R18: ping 1.2.3.4 source 10.2.18.1 //same as R19

If you do not do NAT on R20, there is no return route in ISP2's VRF INET. It is not possible to ping successfully.

NAT for originating data flows in AS65112

R20:

int lo1

ip nat inside

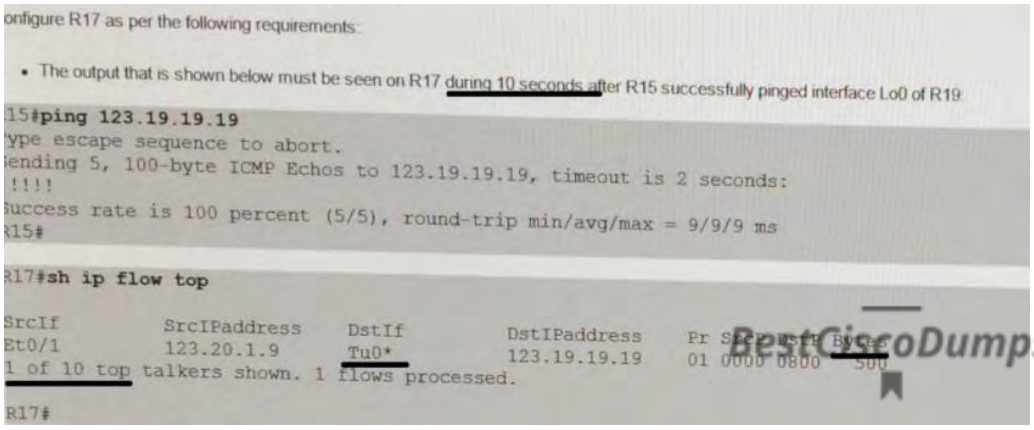
int lo2

ip nat inside

SECTION 5.3: Network Optimization

Configure R17 as per the following requirements

- The output that is shown below must be seen on R17 during 10 seconds after R15successfully pinged interface Lo0 of R19



Solution:

R17:

ip flow-export version 9

ip flow-top-talkers

top 10

sort-by bytes

cache-timeout 10000

match output-interface tunnel0

match source address 123.20.1.9 255.255.255.255

match destination address 123.19.19.19 255.255.255.255

interface tunnel0

ip flow egress

shell processing full

SECTION 5.4: Network Services

Configure ACME network as per the following requirements

- SW3 must provide an authoritative time source to the ACME network
- R10 and R12 must synchronise their clock to SW3 using NTPv4 for ipv6
- R10 and R12 must operate in client mode
- SW3 must not capture or use any time information that is sent by R10 and R12
- All NTP traffic must rely on IPv6 connectivity only
- All NTP traffic must be sourced and destined to the interface Lo0 of the corresponding devices

Solution:

R10/R12/R14/SW3:

ntp source lo0

interface lo0

ntp disable ip

clock timezone BEIJING +8

SW3:

clock set XXXXXXXX

ntp master

R10/R12/R14:

ntp server 2001:CC1E:BEEF:33:123:33:33:33 version 4 //Ipv6 address of SW3 lo0 port

Note: The Lo0 port address on SW3 serves as the source address for NTP synchronization. You need to look at show ipv6 int brief on SW3, and show run interface lo0 cannot see it.

The above is the whole content of CCIE R&S mock lab dumps section 3-5. CCIE RS Lab1 is completed. I wonder if you have gained anything? Do you want to learn more about CCIE Lab dumps? If you think the content we share is good, you can click the share button below to share these useful CCIE Lab Dumps to more people in need. Your support will be the driving force for BestCiscoDumps to move forward!