**ÔN TẬP CCNA**

**LAB1:**

Connectivity between three routers has been established, and IP services must be configure in the order presented to completed the implementation. Tasks assigned include configuration of NAT, NTP DHCP, and SSH services.

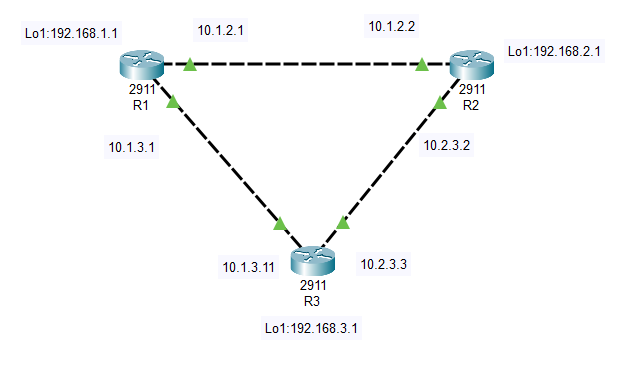
1. All traffic sent from R3 to R1 loopback address must be configured for NAT on R2. All source address must be translate from R3 to the IP address of Ethernet0/0 on R2, while using only a standard access list name PUBNET. To verify, a ping must be successful to the R1 loopback address source from R3. Do not use the NVI NAT configuration.

2. Configure R1 as an NTP server and R2 as a client, not as a peer, using the IP address of the R1 Ethernet0/2 interface. Set the lock on the NTP server for midnight on May 1, 2018.

3. configure R1 as a DHCP server for the network 10.1.3.0/24 in a pool named TEST. Using single command, exxclude address 1-10 from the range. Interface Ethernet0/2 on R3 must be issued the IP address of 10.1.3.11 via DHCP

4. Configure SSH connectivity from R1 to R3, while exxcluding access via other remote connection protocols. Access for user root and password cisco must be set on router R3 using RSA and 1024 bits.

Verify connecting using SSH session from router R1 using a destination address of 10.1.3.11. Do NOT modify console access or line numbers to accomplish this task.



**R1:**

Router>en

Router#clock set 00:00:00 1 may 2018

Router#config t

Router(config)#int g0/0

Router(config-if)#ip address 10.1.2.1 255.255.255.0

Router(config-if)#no shutdown

Router(config-if)#int g0/1

Router(config-if)#ip address 10.1.3.1 255.255.255.0

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#ntp master 1

Router(config)#ip dhcp excluded-address 10.1.3.1 10.1.3.10

Router(config)#ip dhcp pool TEST

Router(dhcp-config)#network 10.1.3.0 255.255.255.0

Router(dhcp-config)#default-router 10.1.3.1

Router(dhcp-config)#end

Router#wr

**R2:**

Router>en

Router#config t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname R2

R2(config)#int g0/0

R2(config-if)#ip address 10.1.2.2 255.255.255.0

R2(config-if)#no shutdown

R2(config-if)#int g0/1

R2(config-if)#ip address 10.2.3.2 255.255.255.0

R2(config-if)#no shutdown

R2(config-if)#exit

R2(config)#ip access-list standard PUBNET

R2(config-std-nacl)#permit 10.2.3.0 0.0.0.255

R2(config-std-nacl)#exit

R2(config)#ip nat inside source list PUBNET interface e0/0 overload

R2(config)#int g0/0

R2(config-if)#ip nat outside

R2(config-if)#int g0/1

R2(config-if)#ip nat inside

R2(config-if)#exit

R2(config)#ntp server 10.1.3.1

R2(config)#end

R2#wr

**R3:**

Router>en

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname R3

R3(config)#int g0/0

R3(config-if)#ip address 10.2.3.3 255.255.255.0

R3(config-if)#no shutdown

R3(config-if)#int g0/1

R3(config-if)#ip address 10.1.3.11 255.255.255.0

R3(config-if)#no shutdown

R3(config-if)#exit

R3(config)#int g0/2

R3(config-if)#ip address dhcp

R3(config-if)#exit

R3(config)#username root password cisco

R3(config)#crypto key generate rsa modulus 1024

R3(config)#line vty 0 4

R3(config-line)#login local

R3(config-line)#transport input ssh

R3(config-line)#end

R3#wr

**LAB2:**

R1 and R2 are pre-configured with all the necessary commands. All physical cabling is in place and verify.

Connectivity for PC1 and PC2 must be established to the switches; each port must only allow one VLAN and be operational.

1. confiure SW-1 with VLAN 15 and lablel it exactly as OPS

2. Configure SW-02 with VLAN 66 and label it exactly as ENGINEERING

3. Configure the switch port connecting to PC1.

4. Configure the switch port connecting to PC2.

5. Configure the Fa0/1 connection on SW-01 and SW-02 for neighbor discovery using the vendor-neutral standard protocol and ensure that F0/3 on both switches uses the Cisco proprietary protocol

A diagram of a computer network

AI-generated content may be incorrect.

**R1:**

Router>en

Router#conf t

Router(config)#int gigabitEthernet 0/0.15

Router(config-subif)#encapsulation dot1Q 15

Router(config-subif)#ip address 172.16.15.1 255.255.0.0

Router(config-subif)#no shutdown

Router(config-subif)#exit

Router(config)#interface gigabitEthernet 0/0

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#end

Router#wr

R2:

Router>en

Router#configure terminal

Router(config)#interface gigabitEthernet 0/0.66

Router(config-subif)#encapsulation dot1Q 66

Router(config-subif)#ip address 192.168.66.1 255.255.0.0

Router(config-subif)#no shutdown

Router(config-subif)#exit

Router(config)#interface gigabitEthernet 0/0

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#end

Router#write memory

**SW1:**

Switch>enable

Switch#configure terminal

Switch(config)#lldp run

Switch(config)#vlan 15

Switch(config-vlan)#name OPS

Switch(config-vlan)#exit

Switch(config)#int fa0/2

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 15

Switch(config-if)#exit

Switch(config)#interface fa0/1

Switch(config-if)#lldp transmit

Switch(config-if)#lldp receive

Switch(config-if)#exit

Switch(config)#interface fa0/2

Switch(config-if)#cdp enable

Switch(config-if)#exit

Switch(config)#end

Switch#wr

**SW2:**

Switch>en

Switch#configure terminal

Switch(config)#lldp run

Switch(config)#vlan 66

Switch(config-vlan)#name ENGINEERING

Switch(config-vlan)#exit

Switch(config)#interface fa0/2

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 66

Switch(config-if)#exit

Switch(config)#interface fa0/1

Switch(config-if)#lldp transmit

Switch(config-if)#lldp receive

Switch(config-if)#exit

Switch(config)#int fa0/2

Switch(config-if)#cdp enable

Switch(config-if)#exit

Switch(config)#end

Switch#wr

**LAB3:**

Tasks 1

Configure a local account on Sw101 with telnet access only on virtual ports 0-4. Use the following information:

1. username: support

2. Password: max2learn

3. Privilege level: Exec mode

Tasks 2

Configure and apply a single NACL on Sw101 using the following:

1. Name: ENT\_ACL

2. Restrict only PC2 on VLAN 200 from pinging PC1

3. Allow only PC2 on VLAN 200 to telnet to Sw101

4. Prevent all other devices from telnetting from VLAN 200

5. Allow all other network traffic from VLAN 200

Tasks 3

Configure security on interface Fa0/2 of Sw102:

1. Set the maximum number of the secure MAC address to four:

2. Drop packet with unknown source addresses until the number of secure MAC addresses drops below maximum value. No notification action iss required.

3. Allow secure MAC address to be learn dynamically.

A diagram of a network

AI-generated content may be incorrect.

**R0:**

Router>en

Router#configure terminal

Router(config)#hostname R0

R0(config)#interface GigabitEthernet0/0

R0(config-if)#ip address 192.168.1.1 255.255.255.0

R0(config-if)#no shutdown

R0(config-if)#exit

R0(config)#interface GigabitEthernet0/1

R0(config-if)#ip address 209.165.201.1 255.255.255.252

R0(config-if)#no shutdown

R0(config-if)#exit

R0(config)#line vty 0 4

R0(config-line)#password cisco

R0(config-line)#login

R0(config-line)#transport input telnet

R0(config-line)#exit

R0(config)#end

R0#wr

**SW1:**

Switch> enable

Switch# configure terminal

Switch(config)# hostname Sw1

Switch(config)# vlan 100

Switch(config-vlan)# name VLAN100

Switch(config-vlan)# exit

Switch(config)# interface FastEthernet0/3

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 100

Switch(config-if)# no shutdown

Switch(config-if)# exit

Switch(config)# interface FastEthernet0/1

Switch(config-if)# switchport trunk encapsulation dot1q

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport trunk allowed vlan add 100,200

Switch(config-if)# no shutdown

Switch(config-if)# exit

Switch(config)# username support privilege 15 password max2learn

Switch(config)# line vty 0 4

Switch(config-line)# login local

Switch(config-line)# transport input telnet

Switch(config-line)# exit

Switch(config)# ip access-list extended ENT ACL

Switch(config-ext-nacl)# deny icmp host 192.168.200.10 host 192.168.100.10

Switch(config-ext-nacl)# permit tcp host 192.168.200.10 any eq telnet

Switch(config-ext-nacl)# deny tcp 192.168.200.0 0.0.0.255 any eq telnet

Switch(config-ext-nacl)# permit ip any any

Switch(config-ext-nacl)# exit

Switch(config)# interface vlan 200

Switch(config-if)# ip access-group ENT ACL in

Switch(config-if)# exit

Switch(config)# end

**SW2**:

Switch> en

Switch# configure terminal

Switch(config)# hostname Sw2

Switch(config)# vlan 200

Switch(config-vlan)# name VLAN200

Switch(config-vlan)# exit

Switch(config)# interface FastEthernet0/2

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 200

Switch(config-if)# no shutdown

Switch(config-if)# exit

Switch(config)# interface FastEthernet0/1

Switch(config-if)# switchport trunk encapsulation dot1q

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport trunk allowed vlan add 100,200

Switch(config-if)# no shutdown

Switch(config-if)# exit

Switch(config)# interface FastEthernet0/2

Switch(config-if)# switchport port-security

Switch(config-if)# switchport port-security maximum 4

Switch(config-if)# switchport port-security violation protect

Switch(config-if)# switchport port-security mac-address sticky

Switch(config-if)# exit

Switch(config)# end

**LAB4:**

All physical cabling is in place and verify. Connectivity between all four switches must be established and operational. All ports are pre-configured as 802.1q trunks.

1. Configure both SW-1 and SW-2 ports e0/1 and e0/2 to permit only the allowed VLANs.

2. Configure both SW-3 and SW-4 ports e0/2 to permit only the allowed VLANs.

3. Configure both SW-1 and SW-2 e0/1 ports to send and receive untagged traffic over VLAN 99.

4. Configure both SW-3 and SW-4 ports e0/0 and e0/1 for link aggregation using the industry standard protocol. All port must immediately negotiate the link aggregation

5. Permit only the allowed VLANs on the new link.

A diagram of a computer network

AI-generated content may be incorrect.

**SW1:**

Switch>en

Switch#configure terminal

Switch(config)#hostname SW1

SW1(config)#interface range fastEthernet 0/1 - 2

SW1(config-if-range)#switchport trunk allowed vlan 56,77,99

SW1(config-if-range)#exit

SW1(config)#interface FastEthernet 0/1

SW1(config-if)#switchport trunk native vlan 99

SW1(config-if)#exit

SW1(config)#end

SW1#wr

**SW2:**

Switch>en

Switch#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#hostname SW2

SW2(config)#interface range fastEthernet 0/1 - 2

SW2(config-if-range)#switchport trunk allowed vlan 56,77,99

SW2(config-if-range)#exit

SW2(config)#interface FastEthernet 0/1

SW2(config-if)#switchport trunk native vlan 99

SW2(config-if)#exit

SW2(config)#end

SW2#wr

**SW3:**

Switch>en

Switch#configure terminal

Switch(config)#hostname SW3

SW3(config)#interface range fastEthernet 0/0-1

SW3(config)#channel-group 34 mode active

SW3(config)#exit

SW3#interface FastEthernet 0/2

SW3#switchport trunk allowed vlan 56,77,99

SW3#exit

**SW4:**

Switch>en

Switch#conf t

Switch(config)#hostname SW4

SW4(config)#int range fastEthernet 0/2 - 3

SW4(config-if-range)#channel-group 34 mode active

SW4(config-if-range)#exit

SW4(config)#interface FastEthernet 0/1

SW4(config-if)#switchport trunk allowed vlan 56,77,99

SW4(config-if)#exit

SW4(config)#interface Port-channel 34

SW4(config)#switchport trunk allowed vlan 56,77,99

SW4(config)#exit

SW4#end

**LAB5:**

All physical cabling in this place. Routers R3 and R4 are fully configure and inaccessible. Configure static routes for various connectivity to the ISP and the LAN that resides on R4

1. Configure a route on R1 to ensure that R1 prefers R2 when traffic is destined to the server only.

2. Configure a default route on R2 to the ISP

3. Configure a route on R1 to ensure that R1 will use R2 for the R4 LAN if the link fails between R3 and R4

4. Configure a route on R1 to ensure that R1 prefers R3 when traffic is destined to the R4 LAN at 10.0.41.0/24

A diagram of a network

AI-generated content may be incorrect.

**R1:**

en

configure terminal

interface GigabitEthernet0/0

ip address 10.0.12.1 255.255.255.252

no shutdown exit

interface GigabitEthernet0/1

ip address 10.0.13.1 255.255.255.224

no shutdown

exit

ip route 10.0.41.0 255.255.255.0 10.0.13.2

ip route 10.0.41.0 255.255.255.0 10.0.12.2 5

exit

wr

**R2:**

en

configure terminal

interface GigabitEthernet0/0

ip address 10.0.12.2 255.255.255.252

no shutdown

exit

interface GigabitEthernet0/1

ip address 10.0.24.1 255.255.255.248

no shutdown

exit

interface GigabitEthernet0/2

ip address 209.165.200.226 255.255.255.224

no shutdown exit

ip route 0.0.0.0 0.0.0.0 209.165.200.225

exit

wr

**R3:**

enable

configure terminal

interface GigabitEthernet0/0

ip address 10.0.13.2 255.255.255.224

no shutdown

exit

interface GigabitEthernet0/1

ip address 10.0.34.1 255.255.255.240

no shutdown exit

ip route 10.0.41.0 255.255.255.0 10.0.34.2

ip route 209.165.200.224 255.255.255.224 10.0.13.1

ip route 10.0.24.0 255.255.255.248 10.0.34.2

ip route 10.0.12.0 255.255.255.252 10.0.13.1

exit

wr

**R4:**

en

configure terminal

interface GigabitEthernet0/0

ip address 10.0.24.2 255.255.255.248

no shutdown exit

interface GigabitEthernet0/1

ip address 10.0.34.2 255.255.255.240

no shutdown exit

interface GigabitEthernet0/2

ip address 10.0.41.1 255.255.255.0

no shutdown exit

ip route 209.165.200.224 255.255.255.224 10.0.24.1

ip route 10.0.12.0 255.255.255.252 10.0.24.1

ip route 10.0.13.0 255.255.255.224 10.0.34.1

exit

wr

**LAB6:**

R1 has been pre-configured with all the necessary command. All physical cabling is in place and verify. Connectivity from PC1, PC3 and the Server must be established to the switches

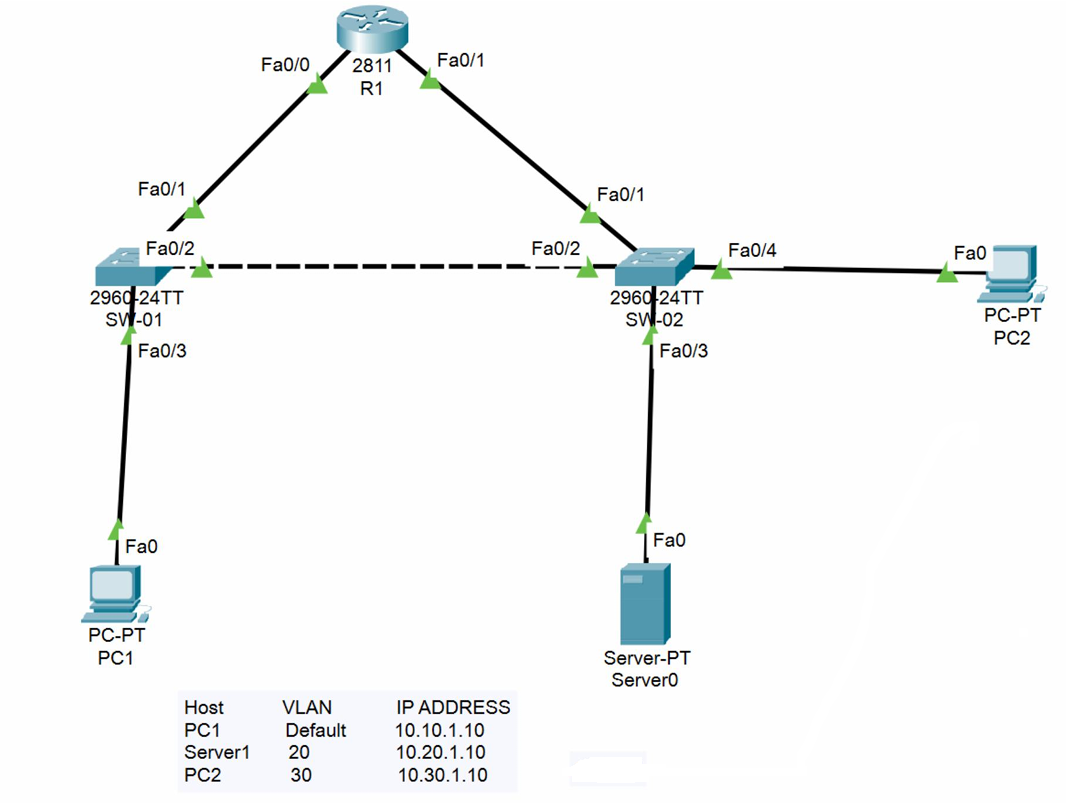
and each port must only allow one VLAN.

1. Configure the VLAN connectto the switch port for PC3 with the name "SALES"

2. Configure the switch port connecting to Server1.

3. Configure the switch port connecting to PC3.

4. Ensure R1 discovers SW-1 via the Cisco proprietary neighbor discovery protocoland all other devices on the network are unable to discover Sw-1



**SW1:**

enable

configure terminal

interface fa0/2 no cdp enable

exit

interface fa0/3 no cdp enable

exit

interface fa0/1

cdp enable

exit

interface fa0/3

switchport mode access

switchport mode vlan1

exit

end

wr

**SW2:**

enable

configure terminal

vlan 30

name SALES

exit

vlan 20 name SERVER exit

interface fa0/3

switchport mode access

switchport access vlan 20

exit

interface fa0/4

switchport mode access

switchport access vlan 30

exit

interface fa0/2

no cdp enable

exit

interface fa0/3

no cdp enable

exit

interface fa0/4

no cdp enable

exit

interface fa0/1

cdp enable

exit

end

wr

**R1**:

enable

configure terminal

interface FastEthernet0/0.1

encapsulation dot1Q 1 native

ip address 10.10.1.1 255.255.255.0

exit

interface FastEthernet0/1.20

encapsulation dot1Q 20

ip address 10.20.1.1 255.255.255.0

exit

interface FastEthernet0/1.30

encapsulation dot1Q 30

ip address 10.30.1.1 255.255.255.0

exit

interface FastEthernet0/0

no shutdown

exit

interface FastEthernet0/1

no shutdown

exit

end

write memory

**LAB7:**

All physical cabling is in place. A company plans to deploy 16 site. The sites will utilize both IPv4 and IPv6 networks.

Subnet 172.16.0.0/16 to meet the subnet requirements and maximize the number of hosts

. Using the second subnet

1. Assign the first usable IP address to f0/1 on Sw101

2. Assign the last usable IP address to f0/1 on Sw102

Subnet 2001:DB8::/50 to meet requirements and maximize the number of hosts

.Using the second subnet

1. Assign an IPv6 GUA using a unique 64-Bit interface identifier on f0/1 on Sw101

2. Assign an IPv6 GUA using a unique 64-Bit interface identifier on f0/1 on Sw102

A green and black dotted line

AI-generated content may be incorrect.

**SW-101:**

en

configure terminal

sdm prefer dual-ipv4-and-ipv6 default

exit

reload

enable

configure terminal

interface Fa0/1

no switchport

ip address 172.16.16.1 255.255.240.0

ipv6 address 2001:DB8:0:1::1/64

no shutdown

exit

end

wr

**SW-102:**

en

configure terminal

sdm prefer dual-ipv4-and-ipv6 default

exit reload enable

configure terminal

interface Fa0/1

no switchport

ip address 172.16.31.254 255.255.240.0

ipv6 address 2001:DB8:0:1::2/64

no shutdown exit

end

wr

**LAB8:**

All physical cabling between the two switch is installed. Configure the network connectivity between the switches using the designated VLANs and interfaces.

1. Configure VLAN 12 named Compute and VLAN 34 named Telephony where required for each task.

2. Configure F0/2 on SW2 to use the existing VLAN name Available.

3. Configure the connection between the switches using access ports.

4. Configure f0/1 on SW1 using data and voice VLANs.

5. Configure f0/2 on SW2 so that the Cisco proprietary neighbor discovery protocol is turned off for the designated interface only.

A diagram of a computer network

AI-generated content may be incorrect.

**Sw0:**

en

configure terminal

vlan 12

name Compute

vlan 34

name Telephony

interface Fa0/1

switchport mode access

switchport access vlan 12

interface Fa0/2

switchport mode access

switchport access vlan 12

switchport voice vlan 34

spanning-tree portfast

end

wr

**Sw1:**

enable

configure terminal

vlan 12

name Compute

vlan 34

name Telephony

interface Fa0/1

switchport mode access

switchport access vlan 12

interface Fa0/2

switchport mode access

switchport access vlan 12

no cdp enable

end

write memory

**LAB9:**

Refer to the topology. All physical cabling is in place. Configure local users accounts, modify the Name ACL (NACL),

and configure DHCP Snooping. The current contents of the NACL must remain intact.

. Configure a local account on Sw103 with telnet access only on virtual ports 0-4. Use the following information:

1. Username: devnet

2. Password: access8cli

3. Algorithm type:SHA256

. Using the minimum number of ACEs, modify the existing NACL "INTERNET\_ACL" to control network traffic destined for the internet, and apply the ACL on R1:

1. Allow HTTPS from 172.16.0.0/16

2. Allow Telnet only for VLAN 101

3. Restrict all other traffic and log the ingress interface, source MAC address, the packet's source and destination IP address, and ports

. Configure Sw101:

1. Enable DHCP Snooping for VLAN 101

2. Disable DHCP Option-82 data insertion

3. Enable DHCP Snooping MAC address verification

**R0:**

en

configure terminal

interface GigabitEthernet0/0

ip address 172.16.1.1 255.255.255.0

no shutdown

interface GigabitEthernet0/1

ip address 172.16.2.1 255.255.255.0

no shutdown

interface GigabitEthernet0/2

ip address 192.168.1.1 255.255.255.0

no shutdown

ip access-list extended INTERNET ACL

permit tcp 172.16.0.0 0.0.255.255 any eq 443

permit tcp 172.16.1.0 0.0.0.255 any eq telnet

deny ip any any

interface GigabitEthernet0/2

ip access-group INTERNET ACL out

end

wr

**SW1:**

enable

configure terminal

vlan 101

name VLAN101

interface Vlan101

ip address 172.16.1.11 255.255.255.0

no shutdown

interface Fa0/1

switchport trunk encapsulation dot1q

switchport mode trunk

no shutdown

interface Fa0/2

switchport trunk encapsulation dot1q

switchport mode trunk

no shutdown

interface Fa0/3

switchport trunk encapsulation dot1q

switchport mode trunk no shutdown

enable secret algorithm-type scrypt

username devnet secret access8cli

line vty 0 4

login local

transport input telnet

end

write memory

**SW2:**

enable

configure terminal

vlan 101

name VLAN101

interface Vlan101

ip address 172.16.2.11 255.255.255.0

no shutdown

interface Fa0/1

switchport trunk encapsulation dot1q

switchport mode trunk

no shutdown

interface Fa0/2

switchport trunk encapsulation dot1q

switchport mode trunk

no shutdown

interface Fa0/3

switchport trunk encapsulation dot1q

switchport mode trunk no shutdown

end

write memory

**SW3:**

enable

configure terminal

vlan 101

name VLAN101

interface Vlan101

ip address 172.16.1.13 255.255.255.0

no shutdown

interface Fa0/1

switchport mode trunk

no shutdown

interface Fa0/2

switchport trunk encapsulation dot1q

switchport mode trunk

no shutdown

interface Fa0/3

switchport mode access

switchport access vlan 101

no shutdown

ip dhcp snooping

ip dhcp snooping vlan 101

no ip dhcp snooping information option

ip dhcp snooping verify mac-address

interface Fa0/1

ip dhcp snooping trust

end

write memory

**SW4:**

en

configure terminal

vlan 101

name VLAN101

interface Vlan101

ip address 172.16.2.14 255.255.255.0

no shutdown

interface Fa0/1

switchport trunk encapsulation dot1q

switchport mode trunk

no shutdown interface Fa0/2

switchport trunk encapsulation dot1q

switchport mode trunk

no shutdown

interface Fa0/3

switchport mode access

switchport access vlan 101

no shutdown

end

write memory

**LAB10:**

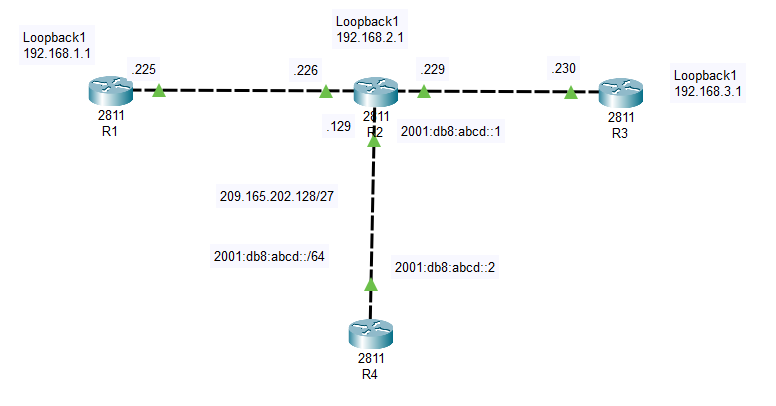
Connectivity between four routers has been established. IP connectivity must be configured in

the order presented to complementation. No dynamic routing protocols are included.

1. Configure static routing using host routes to establish connectivity from router R3 to the router R1 Loopback address using the source IP of 209.165.200.230

2. Configure an IPv4 default route on router R2 destined for router R4.

3. Configure an IPv6 default route on router R2 destined for router R4



**Rl:**

en

configure terminal

hostname R1

interface Loopbackl

ip address 192.168.1.1 255.255.255.255

interface FastEthernet0/0

ip address 209.165.202.225 255.255.255.252

no shutdown

end

wr

**R2:**

enable

configure terminal

hostname R2

interface FastEthernet0/0

ip address 209.165.202.226 255.255.255.252

no shutdown

interface FastEthernet0/1

ip address 209.165.202.229 255.255.255.252

no shutdown

interface FastEthernet1/0

ip address 209.165.202.129 255.255.255.192

no shutdown

ipv6 address 2001:db8:abcd::l/64

ip route 0.0.0.0 0.0.0.0 209.165.202.130

ipv6 route ::/0 2001:db8:abcd::2

end

wr

**R3:**

en

conf t

hostname R3

interface Loopbackl

ip address 192.168.3.1 255.255.255.255

interface FastEthernet0/0

ip address 209.165.202.230 255.255.255.252

no shutdown

ip route 192.168.1.1 255.255.255.255 209.165.202.229

end

wr

**R4:**

en

configure terminal

hostname R4

interface FastEthernet0/0

ip address 209.165.202.130 255.255.255.192

no shutdown

ipv6 address 2001:db8:abcd::2/64

end

wr