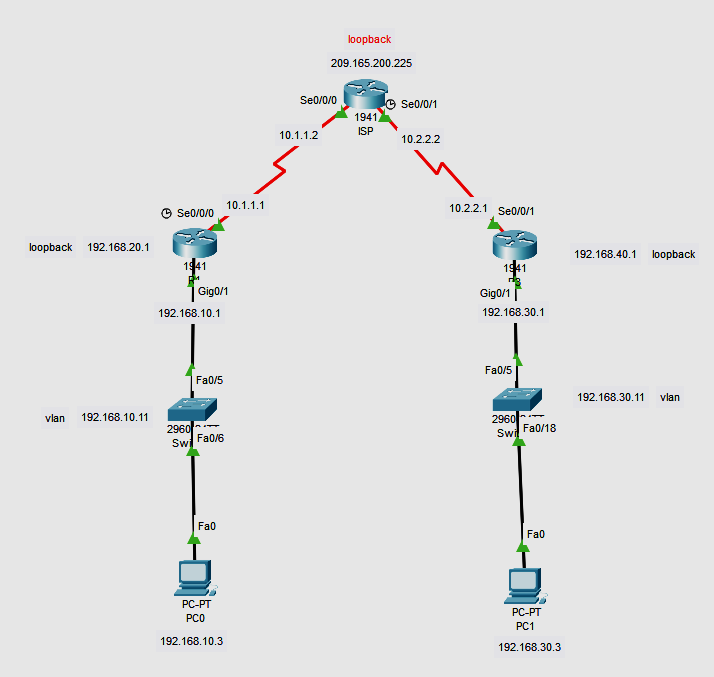
Implement IPv4 ACLs

1.Standard

2.Extended

**1.Standard**

Topology:



Addressing Table:

| **Device** | **Interface** | **IP Address** | **Subnet Mask** | **Default Gateway** |
| --- | --- | --- | --- | --- |
| R1 | G0/1 | 192.168.10.1 | 255.255.255.0 | N/A |
|  | Lo0 | 192.168.20.1 | 255.255.255.0 | N/A |
|  | S0/0/0 (DCE) | 10.1.1.1 | 255.255.255.252 | N/A |
| ISP | S0/0/0 | 10.1.1.2 | 255.255.255.252 | N/A |
|  | S0/0/1 (DCE) | 10.2.2.2 | 255.255.255.252 | N/A |
|  | Lo0 | 209.165.200.225 | 255.255.255.224 | N/A |
| R3 | G0/1 | 192.168.30.1 | 255.255.255.0 | N/A |
|  | Lo0 | 192.168.40.1 | 255.255.255.0 | N/A |
|  | S0/0/1 | 10.2.2.1 | 255.255.255.252 | N/A |
| S1 | VLAN 1 | 192.168.10.11 | 255.255.255.0 | 192.168.10.1 |
| S3 | VLAN 1 | 192.168.30.11 | 255.255.255.0 | 192.168.30.1 |
| PC-A | NIC | 192.168.10.3 | 255.255.255.0 | 192.168.10.1 |
| PC-C | NIC | 192.168.30.3 | 255.255.255.0 | 192.168.30.1 |

1. **Set Up the Topology and Initialize Devices**
   1. **Cable the network as shown in the topology.**
   2. **Initialize and reload the routers and switches.**

Router(config)#int Lo0

Router(config-if)#ip address 192.168.20.1 255.255.255.0

Router(config-if)#no shut

ISP(config)#int Lo0

ISP(config-if)#ip address 209.165.200.225 255.255.255.224

ISP(config-if)#no shut

ISP(config-if)#

R3(config)#int Lo0

R3(config-if)#ip address 192.168.40.1 255.255.255.0

R3(config-if)#no shut

R3(config-if)#

Step 2:

R1(config)# **router rip**

R1(config-router)# **version 2**

R1(config-router)# **network 192.168.10.0**

R1(config-router)# **network 192.168.20.0**

R1(config-router)# **network 10.1.1.0**

**ISP(config)# router rip**

**ISP(config-router)# version 2**

**ISP(config-router)# network 209.165.200.224**

**ISP(config-router)# network 10.1.1.0**

**ISP(config-router)# network 10.2.2.0**

R3(config)# **router rip**

R3(config-router)# **version 2**

R3(config-router)# **network 192.168.30.0**

R3(config-router)# **network 192.168.40.0**

R3(config-router)# **network 10.1.1.0**

S2(config)#int vlan 1

S2(config-if)#ip address 192.168.30.11 255.255.255.0

S2(config-if)#ip default-gateway 192.168.30.1

Switch(config)#int vlan 1

Switch(config-if)#ip address 192.168.10.11 255.255.255.0

Switch(config-if)#ip default-gateway 192.168.10.1

Switch(config)#

Step 3

R1(config)#access-list 1 remark Allow R3 LANs Access

R1(config)#access-list ?

<1-99> IP standard access list

<100-199> IP extended access list

R1(config)#access-list 1 permit 192.168.30.0 0.0.0.255

R1(config)#access-list 1 permit 192.168.40.0 0.0.0.255

R1(config)#access-list 1 deny?

deny

R1(config)#access-list 1 deny any

R1(config)#exit

R1(config)#int g0/1

R1(config-if)#ip access-group 1 out

R1(config-if)#exit

R1#show access-list 1

Standard IP access list 1

permit 192.168.30.0 0.0.0.255

permit 192.168.40.0 0.0.0.255

deny any

R1#show ip interface g0/1

GigabitEthernet0/1 is up, line protocol is up (connected)

Internet address is 192.168.10.1/24

Broadcast address is 255.255.255.255

Address determined by setup command

MTU is 1500 bytes

Helper address is not set

Directed broadcast forwarding is disabled

Outgoing access list is 1

Inbound access list is not set

Proxy ARP is enabled

Security level is default

Split horizon is enabled

ICMP redirects are always sent

ICMP unreachables are always sent

ICMP mask replies are never sent

IP fast switching is disabled

IP fast switching on the same interface is disabled

IP Flow switching is disabled

IP Fast switching turbo vector

IP multicast fast switching is disabled

IP multicast distributed fast switching is disabled

Router Discovery is disabled

R3#ping

Protocol [ip]:

Target IP address: 192.168.10.1

Repeat count [5]:

Datagram size [100]:

Timeout in seconds [2]:

Extended commands [n]: y

Source address or interface:

Type of service [0]:

Set DF bit in IP header? [no]:

Validate reply data? [no]:

Data pattern [0xABCD]:

Loose, Strict, Record, Timestamp, Verbose[none]:

Sweep range of sizes [n]:

Type escape sequence to abort.

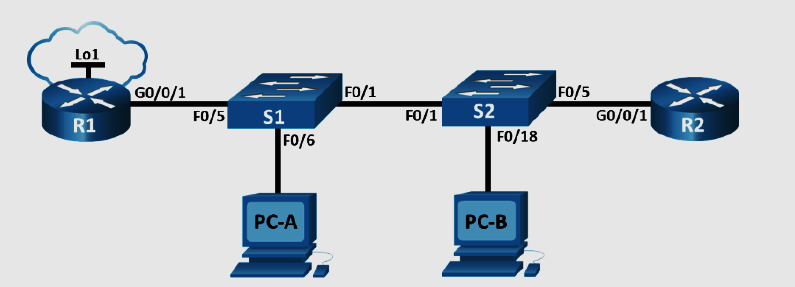
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:

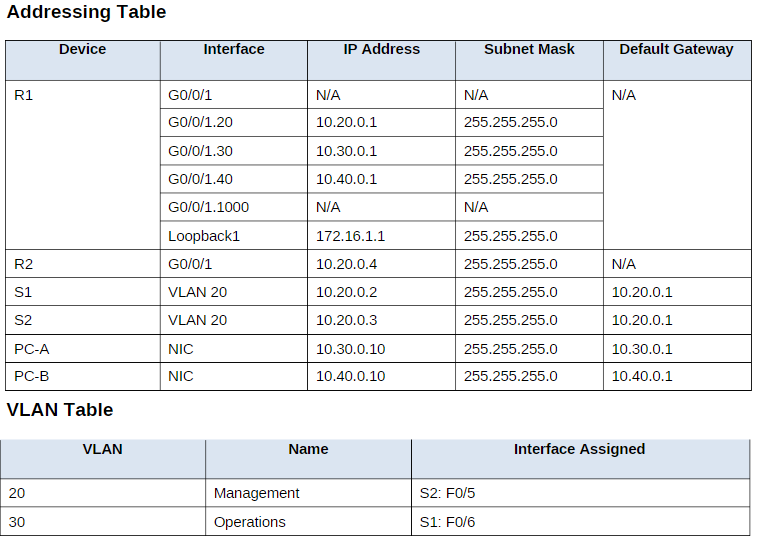
!!!!!

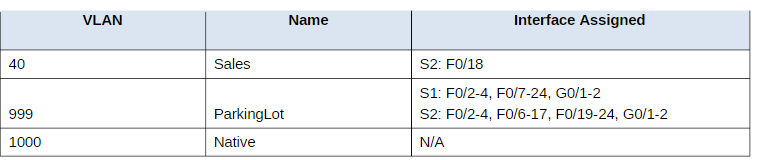
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/16/23 ms

**2.Extended**

**Topology:**







**Part 1: Build the Network and Configure Basic Device Settings.**

#### *Step 1: Cable the network as shown in the topology.*

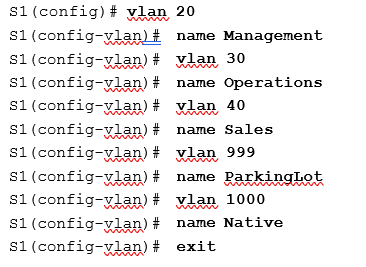
Attach the devices as shown in the topology diagram, and cable as necessary.

#### *Step 2: Configure basic settings for each router.*

#### *Step 3: Configure basic settings for each switch.*

## **Part 2: Configure VLANs on the Switches**

**Step 1: Create VLANs on both switches**

****

**Do the same for s2**

Assign all unused ports on the switch to the Parking Lot VLAN, configure them for static access mode, and administratively deactivate them.

**Note**: The interface range command is helpful to accomplish this task with as few commands as necessary.

#### *Step 2: Assign VLANs to the correct switch interfaces.*

## **Part 3: Configure Trunking**

**step 1: Manually configure trunk interface F0/1.**

S1(config)# **interface f0/1**

S1(config-if)# **switchport mode trunk**

S1(config-if)# **switchport trunk native vlan 1000**

S1(config-if)# **switchport trunk allowed vlan 20,30,40,1000**

###### S1# show interfaces trunk

#### *Step 2: Manually configure S1’s trunk interface F0/5.*

Configure S1’s interface F0/5 with the same trunk parameters as F0/1. This is the trunk to the router.

S1(config)# **interface f0/5**

###### S1(config-if)#switchport mode trunk

S1(config-if)# **switchport trunk native vlan 1000**

S1(config-if)# **switchport trunk allowed vlan 20,30,40,1000**

Save the running configuration to the startup configuration file.

###### S1# copy running-config startup-config

Issue the **show interfaces trunk** command to verify trunking.

## **Part 4: Configure Routing**

#### *Step 1: Configure Inter-VLAN Routing on R1.*

Activate interface G0/0/1 on the router.

R1(config)# **interface g0/0/1**

R1(config-if)# **no shutdown**

Configure sub-interfaces for each VLAN as specified in the IP addressing table. All sub-interfaces use 802.1Q encapsulation. Ensure the sub-interface for the native VLAN does not have an IP address assigned. Include a description for each sub-interface.

R1(config)# **interface g0/0/1.20**

R1(config-subif)# description Management Network

###### R1(config-subif)# encapsulation dot1q 20

R1(config-subif)# description Operations Network

R1(config-subif)#ip address 10.30.0.1 255.255.255.0

R1(config-subif)# interface g0/0/1.40

R1(config-subif)# encapsulation dot1q 40

R1(config-subif)# description Sales Network

R1(config-subif)#ip address 10.40.0.1 255.255.255.0

R1(config-subif)# interface g0/0/1.1000

R1(config-subif)# encapsulation dot1q 1000 native

R1(config-subif)# description Native VLAN

Configure interface Loopback 1 on R1 with addressing from the table above.

R1(config)# interface Loopback 1

R1(config-if)# ip address 172.16.1.1 255.255.255.0

Use the **show ip interface brief** command to verify the sub-interfaces are operational.

###### R1# show ip interface brief

#### *Step 2: Configure the R2 interface g0/0/1 using the address from the table and a default route with the next hop 10.20.0.1*

R2(config)# **interface g0/0/1**

R2(config-if)# ip address 10.20.0.4 255.255.255.0

R2(config-if)# **no shutdown**

R2(config-if)# **exit**

R2(config)# **ip route 0.0.0.0 0.0.0.0 10.20.0.1**

## **Part 5: Verify Connectivity**

#### *Step 1: Configure PC hosts.*

Refer to the Addressing Table for PC host address information.

## **Part 6: Configure and Verify Extended Access Control Lists.**

When basic connectivity is verified, the company requires the following security policies to be implemented

**Policy 1**: The Sales Network is not allowed to SSH to the Management Network (but other SSH is allowed).

**Policy 2**: The Sales Network is not allowed to access IP addresses in the Management network using any

web protocol (HTTP/HTTPS). The Sales Network is also not allowed to access R1 interfaces using any web protocol. All other web traffic is allowed (note – Sales can access the Loopback 1 interface on R1).**Policy 3**

**Policy 4**: The Operations network is not allowed to send ICMP echo-requests to the Sales network. ICMP echo requests to other destinations are allowed.

Step 1: Analyze the network and the security policy requirements to plan ACL implementation.

Answers may vary. The requirements listed above require two extended access lists to be implemented. Following the guidance of placing extended access lists as close to the source of the traffic to be filtered as possible, these ACLs will go on interfaces G0/0/0.30 and G0/0/0.40.

#### *Step 2: Develop and apply extended access lists that will meet the security policy statements.*

###### Answers may vary. The ACLs should be similar to the following:

R1(config)# access-list 101 remark ACL 101 fulfills policies 1, 2, and 3

| R1(config)# | access-list | 100 | deny | tcp | 10.40.0.0 | 0.0.0.255 | 10.20.0.0 | 0.0.0.255 eq 22 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| R1(config)# | access-list | 100 | deny | tcp | 10.40.0.0 | 0.0.0.255 | 10.20.0.0 | 0.0.0.255 eq 80 |
| R1(config)# | access-list | 100 | deny | tcp | 10.40.0.0 | 0.0.0.255 | 10.30.0.0 | 0.0.0.0 eq 443 |
| R1(config)# | access-list | 100 | deny | tcp | 10.40.0.0 | 0.0.0.255 | 10.40.0.0 | 0.0.0.0 eq 80 |
| R1(config)# | access-list | 100 | deny | tcp | 10.40.0.0 | 0.0.0.255 | 10.20.0.0 | 0.0.0.255 eq 443 |
| R1(config)# | access-list | 100 | deny | tcp | 10.40.0.0 | 0.0.0.255 | 10.30.0.0 | 0.0.0.0 eq 80 |
| R1(config)# | access-list | 100 | deny | tcp | 10.40.0.0 | 0.0.0.255 | 10.40.0.0 | 0.0.0.0 eq 443 |

R1(config)# access-list 100 deny icmp 10.40.0.0 0.0.0.255 10.20.0.0 0.0.0.255 echo

R1(config)# access-list 100 deny icmp 10.40.0.0 0.0.0.255 10.30.0.0 0.0.0.255 echo

R1(config)# access-list 100 permit ip any any

R1(config)# interface g0/0/1.40

R1(config-subif)# ip access-group 100 in

R1(config)# access-list 102 deny icmp 10.30.0.0 0.0.0.255 10.40.0.0 0.0.0.255 echo

R1(config)# access-list 102 permit ip any any

R1(config)# interface g0/0/1.30

R1(config-subif)# ip access-group 101 in

**Step 3: Verify security policies are being enforced by the deployed access lists.**

Run the following tests. The expected results are shown in the table:

From Protocol Destination Result

| PC-A | Ping | 10.40.0.10 | Fail |
| --- | --- | --- | --- |
| PC-A | Ping | 10.20.0.1 | Success |
| PC-B | Ping | 10.30.0.10 | Fail |
| PC-B | Ping | 10.20.0.1 | Fail |
| PC-B | Ping | 172.16.1.1 | Success |
| PC-B | HTTPS | 10.20.0.1 | Fail |
| **PC-B** | **HTTPS** | **172.16.1.1** | **Success** |