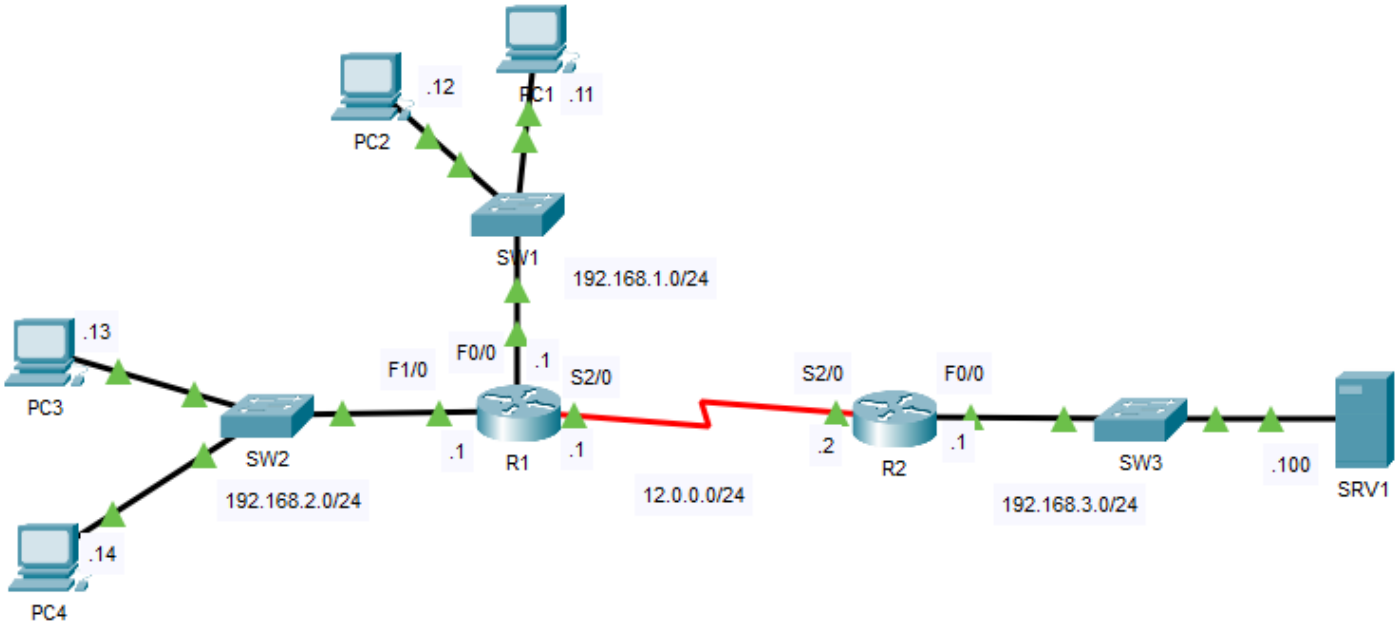
ACTIVITY 29 : Standards ACLs (ACLs Part 1)



Configure standard ACLs to achieve the following requirements:

1-Only computers in the 192.168.1.0/24 network can access SRV1

```
R2(config)#access-list 1 permit 192.168.1.0 0.0.0.255
R2(config)#interface f0/0
R2(config-if)#ip access-group 1 out
```

From PC1

```
C:\>ping 192.168.3.100

Pinging 192.168.3.100 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.100: bytes=32 time=1ms TTL=126
Reply from 192.168.3.100: bytes=32 time=1ms TTL=126
Reply from 192.168.3.100: bytes=32 time=1ms TTL=126
```

From PC3

```
C:\>ping 192.168.3.100

Pinging 192.168.3.100 with 32 bytes of data:

Reply from 12.0.0.2: Destination host unreachable.
Reply from 12.0.0.2: Destination host unreachable.
Reply from 12.0.0.2: Destination host unreachable.
Reply from 12.0.0.2: Destination host unreachable.
```

2-PC4 cannot communicate with the 192.168.1.0/24 network.

```
R1(config)#access-list 1 deny host 192.168.2.14
R1(config)#access-list 1 permit any
R1(config)#interface f0/0
R1(config-if)#ip access-group 1 out
```

From PC4

```
C:\>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:

Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
```

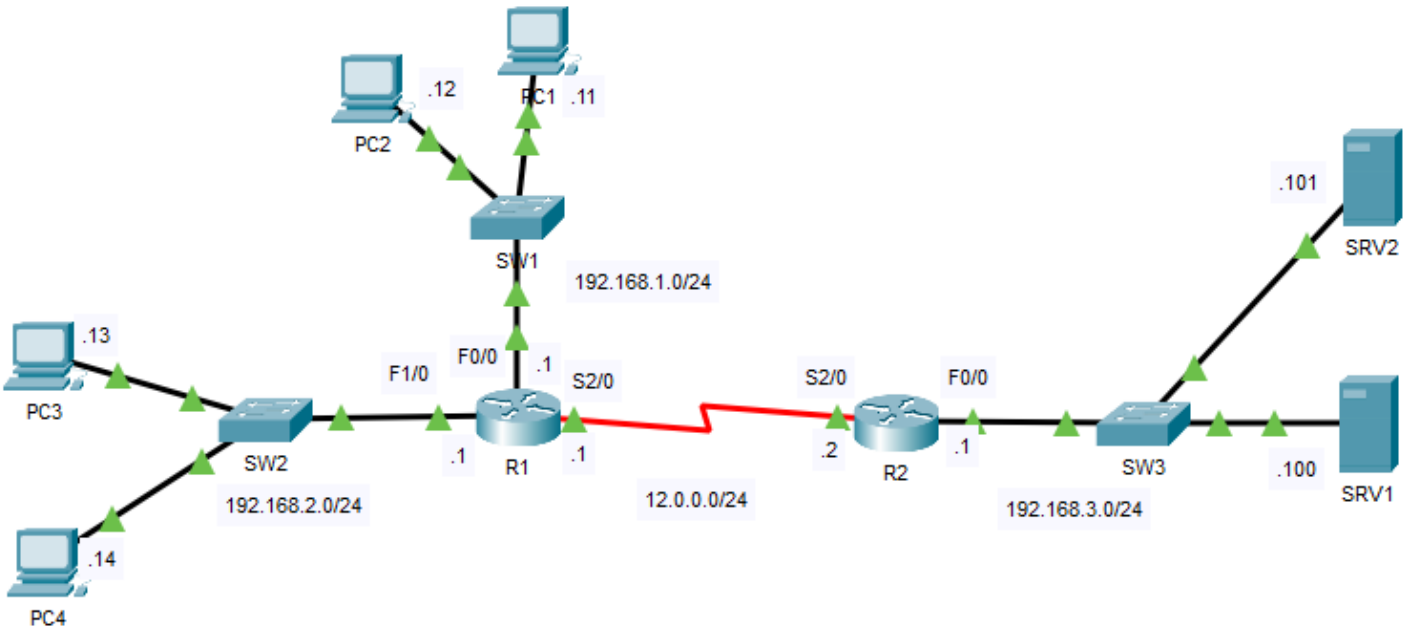
From PC3

```
C:\>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:

Reply from 192.168.1.11: bytes=32 time=1ms TTL=127
Reply from 192.168.1.11: bytes=32 time<1ms TTL=127
Reply from 192.168.1.11: bytes=32 time<1ms TTL=127
Reply from 192.168.1.11: bytes=32 time<1ms TTL=127
```

ACTIVITY 30 : Extended ACLs (ACLs Part 2)



Configure extended ACLs to achieve the following requirements:

---only PC1 can access SRV1

---only hosts on the 192.168.2.0/24 network can access SRV2

Let's configure the ACL on the single interface s2/0 as the network destination is the same:

Step 1: only PC1 can access SRV1

```
R1(config)#access-list 100 permit ip host 192.168.1.11 host 192.168.3.100
R1(config)#access-list 100 deny ip any host 192.168.3.100
```

Step 2: only hosts on the 192.168.2.0/24 network can access SRV2

```
R1(config)#access-list 100 permit ip 192.168.2.0 0.0.0.255 host 192.168.3.101
R1(config)#access-list 100 deny ip any host 192.168.3.101
```

Step 3: Permit any other traffic

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

Step 4: Apply on s2/0

```
R1(config)#interface s2/0
R1(config-if)#ip access-group 100 out
```

Step 4: Test: - Only PC1 can access SRV1:

From PC1

```
C:\>ping 192.168.3.100

Pinging 192.168.3.100 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.100: bytes=32 time=1ms TTL=126
Reply from 192.168.3.100: bytes=32 time=1ms TTL=126
Reply from 192.168.3.100: bytes=32 time=1ms TTL=126
```

From PC3

```
C:\>ping 192.168.3.100

Pinging 192.168.3.100 with 32 bytes of data:

Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
```

From PC2:

```
C:\>ping 192.168.3.100

Pinging 192.168.3.100 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
```

- Only hosts on the 192.168.2.0/24 network can access SRV2
From PC3:

```
C:\>ping 192.168.3.101

Pinging 192.168.3.101 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.101: bytes=32 time=1ms TTL=126
Reply from 192.168.3.101: bytes=32 time=25ms TTL=126
Reply from 192.168.3.101: bytes=32 time=1ms TTL=126
```

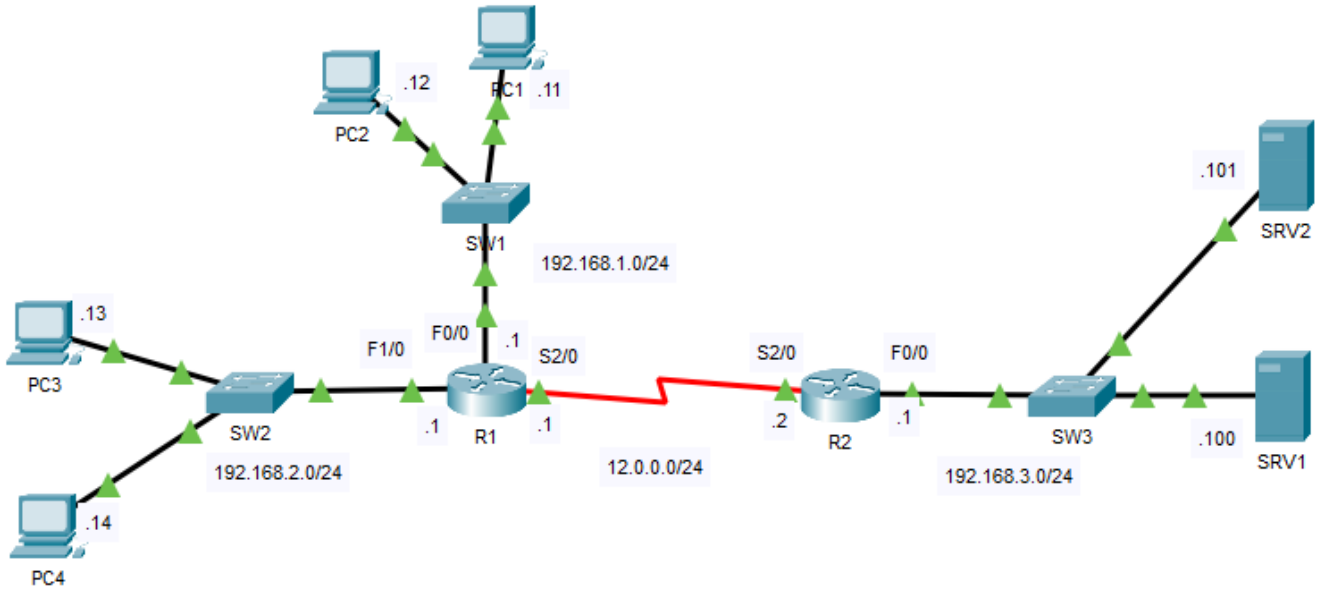
From PC1 and PC2:

```
C:\>ping 192.168.3.101

Pinging 192.168.3.101 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
```

ACTIVITY 31: Named ACLs (ACLs Part 3)



Configure named standard ACLs to achieve the following requirements:

1-Hosts in the 192.168.1.0/24 and 192.168.2.0/24 networks can't communicate with each other

```
R1(config)#ip access-list standard NO1TO2
R1(config-std-nacl)#deny 192.168.1.0 0.0.0.255
R1(config-std-nacl)#permit any
R1(config-std-nacl)#interface f1/0
R1(config-if)#ip access-group NO1TO2 out
```

From PC1:

```
C:\>ping 192.168.2.13

Pinging 192.168.2.13 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
```

From SRV2:

```
C:\>ping 192.168.2.13

Pinging 192.168.2.13 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.13: bytes=32 time=1ms TTL=126
Reply from 192.168.2.13: bytes=32 time=1ms TTL=126
Reply from 192.168.2.13: bytes=32 time=1ms TTL=126
```

2-Hosts in the 192.168.2.0/24 network cannot access the 192.168.3.0/24 network

```
R2(config)#ip access-list standard NO2TO3
R2(config-std-nacl)#deny 192.168.2.0 0.0.0.255
R2(config-std-nacl)#permit any
R2(config-std-nacl)#interface f0/0
R2(config-if)#ip access-group NO2TO3 out
```

From PC3:

```
C:\>ping 192.168.3.101

Pinging 192.168.3.101 with 32 bytes of data:

Reply from 12.0.0.2: Destination host unreachable.
Reply from 12.0.0.2: Destination host unreachable.
Reply from 12.0.0.2: Destination host unreachable.
Reply from 12.0.0.2: Destination host unreachable.
```

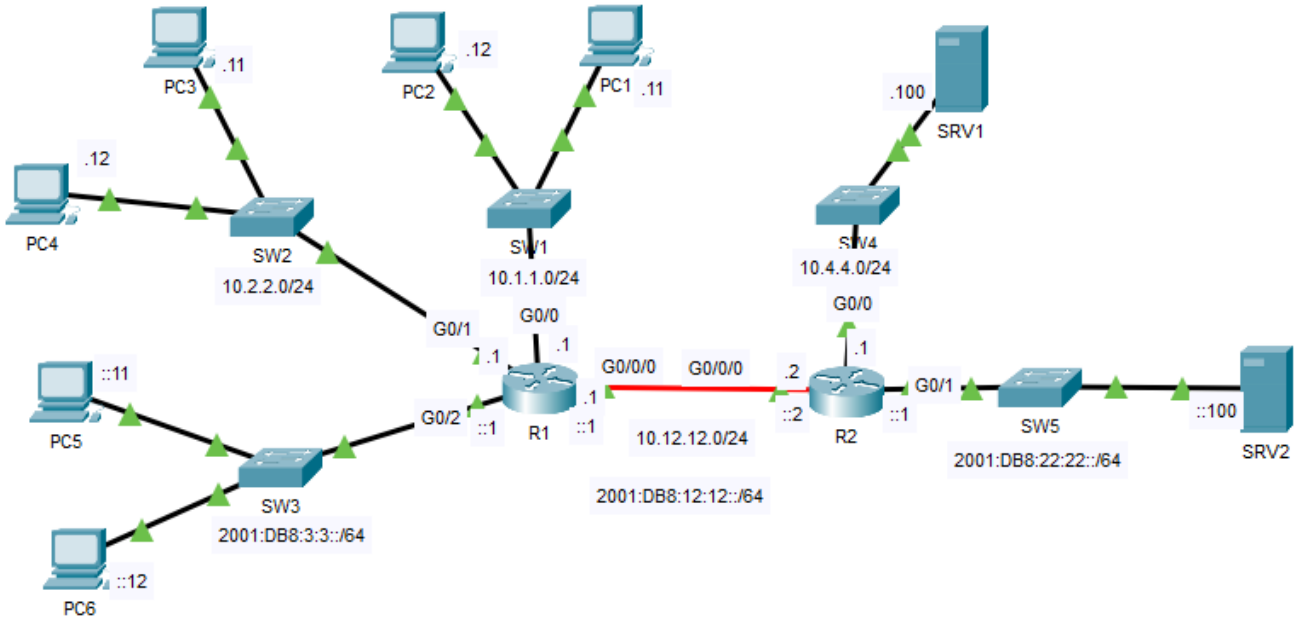
From PC1:

```
C:\>ping 192.168.3.101

Pinging 192.168.3.101 with 32 bytes of data:

Reply from 192.168.3.101: bytes=32 time=14ms TTL=126
Reply from 192.168.3.101: bytes=32 time=1ms TTL=126
Reply from 192.168.3.101: bytes=32 time=2ms TTL=126
Reply from 192.168.3.101: bytes=32 time=1ms TTL=126
```

ACTIVITY 71: IPv4 and IPv6 ACLs with telnet :



Configure and apply the following access lists:

1- Standard Numbered ACL: PC4 cannot access the 10.4.4.0/24 network

```
R2(config)#access-list 1 deny host 10.2.2.12
R2(config)#access-list 1 permit any
R2(config)#interface g0/0
R2(config-if)#ip access-group 1 out
```

From PC4

```
C:\>ping 10.4.4.100

Pinging 10.4.4.100 with 32 bytes of data:

Reply from 10.12.12.2: Destination host unreachable.
Reply from 10.12.12.2: Destination host unreachable.
Reply from 10.12.12.2: Destination host unreachable.
Reply from 10.12.12.2: Destination host unreachable.
```

From PC2:

```
C:\>ping 10.4.4.100

Pinging 10.4.4.100 with 32 bytes of data:

Request timed out.
Reply from 10.4.4.100: bytes=32 time<1ms TTL=126
Reply from 10.4.4.100: bytes=32 time<1ms TTL=126
Reply from 10.4.4.100: bytes=32 time<1ms TTL=126
```

2- IPv6 ACL: PC5 cannot access the 2001:DB8:22:22::/64 network

```
R1(config)#ipv6 access-list NOPC5
R1(config-ipv6-acl)#deny ipv6 host 2001:db8:3:3::11 2001:db8:22:22::/64
R1(config-ipv6-acl)#permit ipv6 any any
R1(config-ipv6-acl)#interface g0/2
R1(config-if)#ipv6 traffic-filter NOPC5 in
```

From PC5:

```
C:\>ping 2001:db8:22:22::100

Pinging 2001:db8:22:22::100 with 32 bytes of data:

Reply from 2001:DB8:3:3::1: Destination host unreachable.
Reply from 2001:DB8:3:3::1: Destination host unreachable.
Reply from 2001:DB8:3:3::1: Destination host unreachable.
Reply from 2001:DB8:3:3::1: Destination host unreachable.
```

From PC6:

```
C:\>ping 2001:db8:22:22::100

Pinging 2001:db8:22:22::100 with 32 bytes of data:

Reply from 2001:DB8:22:22::100: bytes=32 time<1ms TTL=126
Reply from 2001:DB8:22:22::100: bytes=32 time<1ms TTL=126
Reply from 2001:DB8:22:22::100: bytes=32 time<1ms TTL=126
Reply from 2001:DB8:22:22::100: bytes=32 time<1ms TTL=126
```

3- Extended Named ACL: PC3 cannot communicate with PC1

```
R1(config)#ip access-list extended NOPC3TOPC1
R1(config-ext-nacl)#deny ip host 10.2.2.11 host 10.1.1.11
R1(config-ext-nacl)#permit ip any any
R1(config-ext-nacl)#interface g0/1
R1(config-if)#ip access-group NOPC3TOPC1 in
```

From PC3:

```
C:\>ping 10.1.1.11

Pinging 10.1.1.11 with 32 bytes of data:

Reply from 10.2.2.1: Destination host unreachable.
Reply from 10.2.2.1: Destination host unreachable.
Reply from 10.2.2.1: Destination host unreachable.
Reply from 10.2.2.1: Destination host unreachable.
```

From PC4

```
C:\>ping 10.1.1.11

Pinging 10.1.1.11 with 32 bytes of data:

Request timed out.
Reply from 10.1.1.11: bytes=32 time<1ms TTL=127
Reply from 10.1.1.11: bytes=32 time<1ms TTL=127
Reply from 10.1.1.11: bytes=32 time<1ms TTL=127
```

4- IPv6 ACL: PC6 can telnet to R2, but other devices using IPv6 cannot (Telnet password = ccna)

```
R2(config)#ipv6 access-list TELNET
R2(config-ipv6-acl)#permit tcp host 2001:db8:3:3::12 any eq 23
R2(config-ipv6-acl)#line vty 0 15
R2(config-line)#ipv6 access-class TELNET in
```

From PC6:

```
C:\>telnet 2001:db8:12:12::2
Trying 2001:DB8:12:12::2 ...Open


User Access Verification

Password:
R2#
```

```
C:\>ping 2001:db8:12:12::2

Pinging 2001:db8:12:12::2 with 32 bytes of data:

Reply from 2001:DB8:12:12::2: bytes=32 time<1ms TTL=254
Reply from 2001:DB8:12:12::2: bytes=32 time<1ms TTL=254

Ping statistics for 2001:DB8:12:12::2:
```

From PC5:

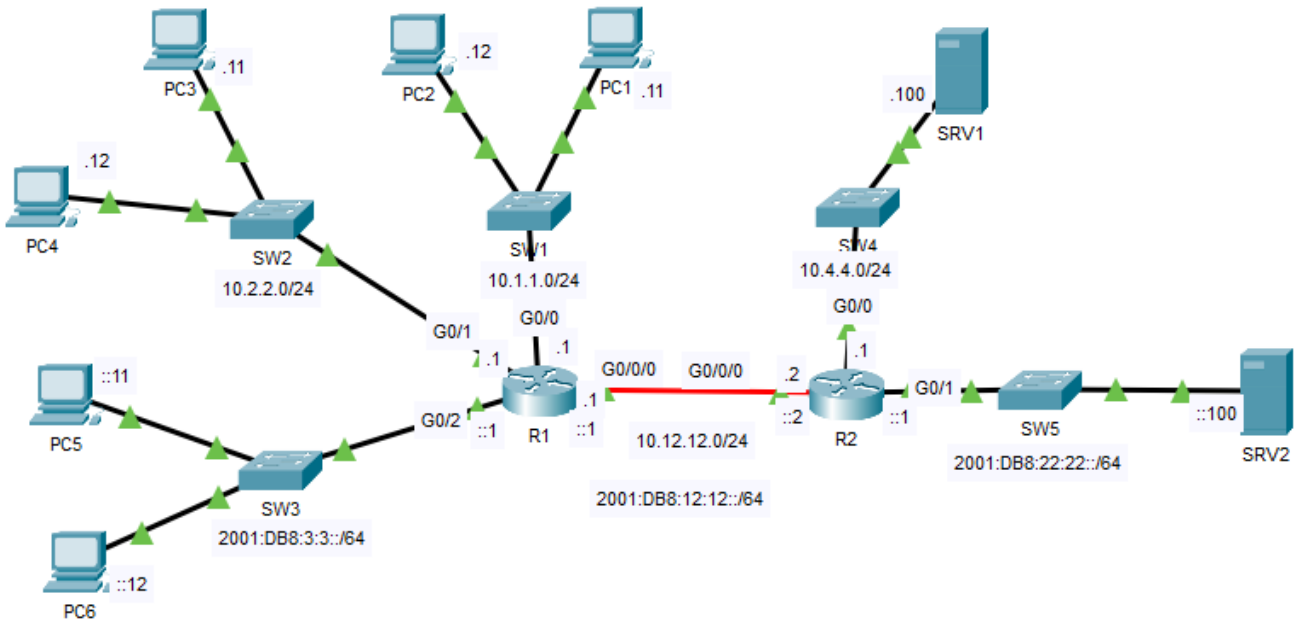
```
C:\>telnet 2001:db8:12:12::2
Trying 2001:DB8:12:12::2 ...
% Connection refused by remote host
C:\>
```

```
C:\>ping 2001:db8:12:12::2

Pinging 2001:db8:12:12::2 with 32 bytes of data:

Reply from 2001:DB8:12:12::2: bytes=32 time<1ms TTL=254
Reply from 2001:DB8:12:12::2: bytes=32 time<1ms TTL=254
```

ACTIVITY 72: ACL Troubleshooting:



The following ACLs have been configured:

1- Standard Numbered ACL: PC4 cannot access the 10.4.4.0/24 network

2- IPv6 ACL: PC5 cannot access the 2001:DB8:22:22::/64 network

3- Extended Named ACL: PC3 cannot communicate with PC1

4- IPv6 ACL: PC6 can telnet to R2, but other devices using IPv6 cannot (Telnet password = ccna)

However, the network is not functioning as intended. There are misconfigurations in three of the ACLs. Troubleshoot and fix the errors.

1- From PC4 :

```
C:\>ping 10.4.4.100

Pinging 10.4.4.100 with 32 bytes of data:

Request timed out.
Reply from 10.4.4.100: bytes=32 time<1ms TTL=126
Reply from 10.4.4.100: bytes=32 time=10ms TTL=126
Reply from 10.4.4.100: bytes=32 time<1ms TTL=126
```

PC4 can ping 10.4.4.0/24, so let's see the ACL configuration on R2 :

```
R2#show ip access-lists
Standard IP access list 1
    10 permit any (4 match(es))
    20 deny host 10.2.2.12
IPv6 access list TELNET
    permit tcp host 2001:DB8:3:3::12 any eq telnet
```

As we see, the general statement "permit any" comes before the specific one. Let's arrange it:

```
R2(config)#no access-list 1
R2(config)#access-list 1 deny host 10.2.2.12
R2(config)#access-list 1 permit any
```

Now, PC4 cant's ping 10.4.4.0/24 but PC3 can:

```
C:\>ping 10.4.4.100

Pinging 10.4.4.100 with 32 bytes of data:

Reply from 10.12.12.2: Destination host unreachable.
Reply from 10.12.12.2: Destination host unreachable.
Reply from 10.12.12.2: Destination host unreachable.
Reply from 10.12.12.2: Destination host unreachable.
```

```
C:\>ping 10.4.4.100

Pinging 10.4.4.100 with 32 bytes of data:

Reply from 10.4.4.100: bytes=32 time<1ms TTL=126
Reply from 10.4.4.100: bytes=32 time<1ms TTL=126
Reply from 10.4.4.100: bytes=32 time=14ms TTL=126
Reply from 10.4.4.100: bytes=32 time<1ms TTL=126
```

2- From PC5:

```
C:\>ping 2001:db8:22:22::100

Pinging 2001:db8:22:22::100 with 32 bytes of data:

Reply from 2001:DB8:22:22::100: bytes=32 time=3ms TTL=126
Reply from 2001:DB8:22:22::100: bytes=32 time<1ms TTL=126
Reply from 2001:DB8:22:22::100: bytes=32 time<1ms TTL=126
Reply from 2001:DB8:22:22::100: bytes=32 time<1ms TTL=126
```

As we can see, PC5 can ping the host in the network. Let's check the ACL config on R1:

```
R1#show ip access-lists
Extended IP access list G0/1_IN
    10 deny ip host 10.2.2.11 host 10.1.1.11
    20 permit ip any any (12 match(es))
IPv6 access list G0/2_IN
    deny ipv6 host 2001:DB8:3:3::11 2001:DB8:22:22::/64
    permit ipv6 any any (4 match(es))
```

The config seems to be OK but let's check the interface config on the running-config:

```
interface GigabitEthernet0/2
 no ip address
 ipv6 traffic-filter G0/2_IN out
 duplex auto
 speed auto
 ipv6 address 2001:DB8:3:3::1/64
 ipv6 eigrp 100
!
```

The traffic-filter should be in not out. Let's reconfigure it:

```
R1(config)#interface g0/2
```

```
R1(config-if)#no ipv6 traffic-filter G0/2_IN out
R1(config-if)#ipv6 traffic-filter G0/2_IN in
```

Let's test it on PC5, then PC6:

```
C:\>ping 2001:db8:22:22::100

Pinging 2001:db8:22:22::100 with 32 bytes of data:

Reply from 2001:DB8:3:3::1: Destination host unreachable.
Reply from 2001:DB8:3:3::1: Destination host unreachable.
Reply from 2001:DB8:3:3::1: Destination host unreachable.
Reply from 2001:DB8:3:3::1: Destination host unreachable.
```

```
C:\>ping 2001:db8:22:22::100

Pinging 2001:db8:22:22::100 with 32 bytes of data:

Reply from 2001:DB8:22:22::100: bytes=32 time<1ms TTL=126
Reply from 2001:DB8:22:22::100: bytes=32 time<1ms TTL=126
Reply from 2001:DB8:22:22::100: bytes=32 time=2ms TTL=126
Reply from 2001:DB8:22:22::100: bytes=32 time<1ms TTL=126
```

3- From PC3:

```
C:\>ping 10.1.1.11

Pinging 10.1.1.11 with 32 bytes of data:

Reply from 10.2.2.1: Destination host unreachable.
Reply from 10.2.2.1: Destination host unreachable.
Reply from 10.2.2.1: Destination host unreachable.
Reply from 10.2.2.1: Destination host unreachable.
```

From PC4:

```
C:\>ping 10.1.1.11

Pinging 10.1.1.11 with 32 bytes of data:

Request timed out.
Reply from 10.1.1.11: bytes=32 time<1ms TTL=127
Reply from 10.1.1.11: bytes=32 time<1ms TTL=127
Reply from 10.1.1.11: bytes=32 time<1ms TTL=127
```

Everything is OK, there is no troubleshooting to do.

4- Let's check on PC6 then PC5:

```
C:\>telnet 2001:db8:12:12::2
Trying 2001:DB8:12:12::2 ...Open


User Access Verification

Password:
R2#
```

```
C:\>telnet 2001:db8:12:12::2
Trying 2001:DB8:12:12::2 ...Open


User Access Verification

Password:
R2#
```

As we see it, PC5 can telnet R2, but it shouldn't. So, let's see the configuration on R2:

```
R2#show ip access-lists
Standard IP access list 1
    10 deny host 10.2.2.12 (4 match(es))
    20 permit any (4 match(es))
IPv6 access list TELNET
    permit tcp host 2001:DB8:3:3::12 any eq telnet
```

As we see with the IPv6 ACL, everything seems to be OK. Let's check the line on the running-config:

```
line vty 0 4
 password ccna
 login
 transport input telnet
 privilege level 15
line vty 5 15
 password ccna
 login
 transport input telnet
 privilege level 15
!
```

As we see, the ACL is not set on the line vty 0 15. Let's configure it:

```
R2(config)#line vty 0 15
R2(config-line)#ipv6 access-class TELNET in
```

Let's recheck on PC6, then PC5:

```
C:\>telnet 2001:db8:12:12::2
Trying 2001:DB8:12:12::2 ...Open


User Access Verification

Password:
R2#
```

```
C:\>
C:\>telnet 2001:db8:12:12::2
Trying 2001:DB8:12:12::2 ...
% Connection refused by remote host
C:\>
```

Now everything is perfect.