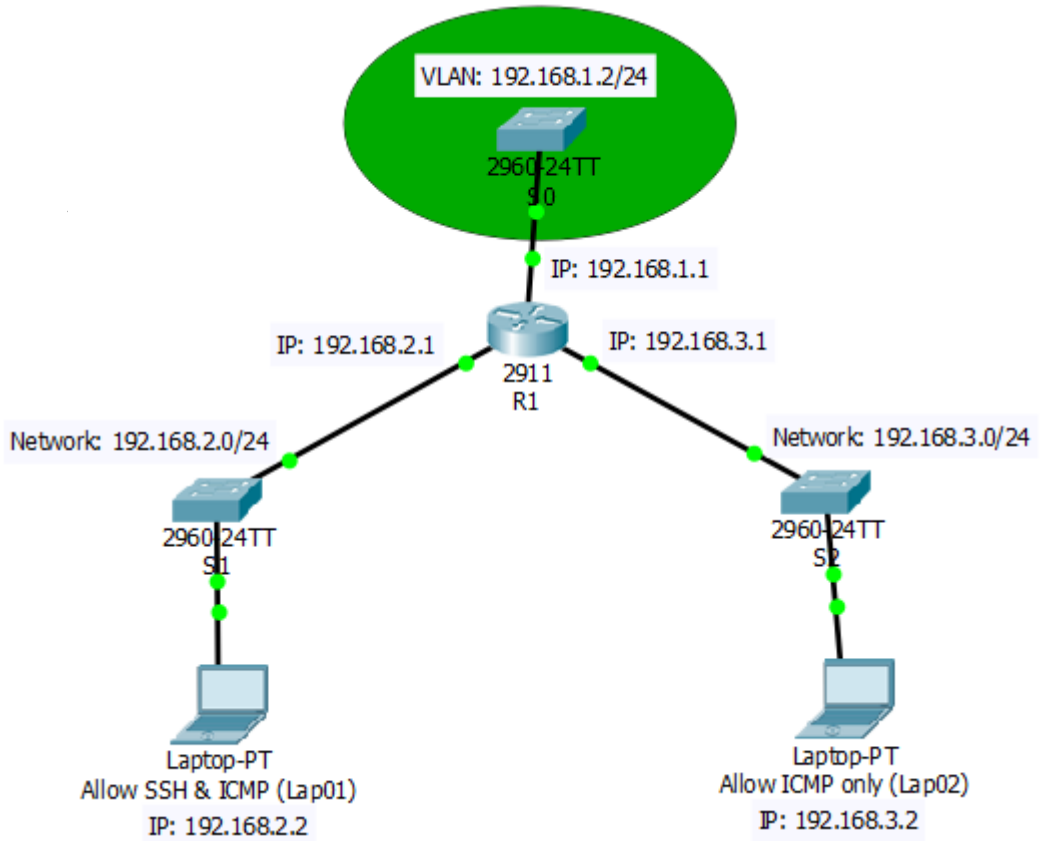
*LAB#06 (*Configuring Extended ACLs - Scenario 2*)*



Establish a network topology and configure it:

1- Set IP for Lap01 (Desktop -> IP configuration)
   a. IP address: 192.168.2.2
   b. Subnet Mask: 255.255.255.0
   c. Default Gateway: 192.168.2.1
2- Set IP for Lap02 (Desktop -> IP configuration)
   a. IP address: 192.168.3.2
   b. Subnet Mask: 255.255.255.0
   c. Default Gateway: 192.168.3.1
3- Set IP for the VLAN of switch S0 (CLI)
   a. S0(config)# interface vlan 1
   b. S0(config-if)# ip address 192.168.1.2 255.255.255.0
   c. S0(config-if)# no shutdown
   d. S0(config-if)# exit
   e. S0(config)# ip default-gateway 192.168.1.1
4- Set IPs for interfaces of router 2911 R1
   a. Config -> GigabitEthernet0/0
      i. Port Status: Check the “on” checkbox
      ii. IP address: 192.168.1.1
      iii. Subnet Mask: 255.255.255.0
   b. Config -> GigabitEthernet0/1

i. Port Status: Check the "on" checkbox
ii. IP address: 192.168.2.1
iii. Subnet Mask: 255.255.255.0

c. Config -> GigabitEthernet0/2
i. Port Status: Check the "on" checkbox
ii. IP address: 192.168.3.1
iii. Subnet Mask: 255.255.255.0

5- Test connectivity.
a. Ping from Lap01 to Lap02
b. Ping from Lap01 & Lap02 to switch S0

Enable SSH on switch S0

1. Switch> enable
2. Switch# configure terminal
3. Switch (config)# username **Admin** secret **cisco1**
4. Switch (config)# enable secret **cisco**
5. Switch (config)# hostname S0
6. S0(config)# ip domain-name bfci.com
7. S0(config)# crypto key generate rsa
8. How many bits in the modulus [512]: 1024
9. S0(config)# line vty 0 4
10. S0(config-line)# login local

Part 1: Configure, Apply and Verify an Extended Numbered ACL

Step 1: Configure an ACL to permit SSH for Network 192.168.2.0

1. `R1(config)#` **access-list ?**
```
<1-99> IP standard access list
<100-199> IP extended access list
```
2. `R1(config)#` **access-list 199 ?**
```
deny Specify packets to reject
permit Specify packets to forward
remark Access list entry comment
```
3. `R1(config)#` **access-list 199 permit ?**
```
ahp Authentication Header Protocol
eigrp Cisco's EIGRP routing protocol
esp Encapsulation Security Payload
gre Cisco's GRE tunneling
icmp Internet Control Message Protocol
ip Any Internet Protocol
ospf OSPF routing protocol
tcp Transmission Control Protocol
udp User Datagram Protocol
```
4. `R1(config)#` **access-list 199 permit tcp ?**
```
A.B.C.D Source address
any Any source host
```

```
host A single source host
```

5. `R1(config)#` **access-list 199 permit tcp 192.168.2.0 0.0.0.255 ?**
   ```
   A.B.C.D Source wildcard bits
   ```
6. `R1(config)#` **access-list 199 permit tcp 192.168.2.0 0.0.0.255 host 192.168.1.2 ?**
   ```
   dscp Match packets with given dscp value
   eq Match only packets on a given port number
   established established
   gt Match only packets with a greater port number
   lt Match only packets with a lower port number
   neq Match only packets not on a given port number
   precedence Match packets with given precedence value
   range Match only packets in the range of port numbers
   ```
7. `R1(config)#` **access-list 199 permit tcp 192.168.2.0 0.0.0.255 host 192.168.1.2 eq ?**
   ```
   <0-65535> Port number
   ftp File Transfer Protocol (21)
   pop3 Post Office Protocol v3 (110)
   smtp Simple Mail Transport Protocol (25)
   telnet Telnet (23)
   www World Wide Web (HTTP, 80)
   ```
8. `R1(config)#` **access-list 199 permit tcp 192.168.2.0 0.0.0.255 host 192.168.1.2 eq 22**
9. All other traffic is denied, by default.

Step 2: Apply the ACL on the correct interface to filter traffic.

1. `R1(config)#` **interface gigabitEthernet 0/0**
2. `R1(config-if)#` **ip access-group 199 out**

Step 3: Verify the ACL implementation

1. Ping from **Lap01 & Lap02** to **Switch S0**. The pings will be unsuccessful.
2. SSH from **Lap01** to **S0**. The username **Admin** and password **cisco**.
   `PC>` **ssh –l Admin 192.168.1.2**
   Password: cisco

Step 4: Configure an ACL to permit ICMP (Ping) for all

1. `R1(config)#` **access-list ?**
   ```
   <1-99> IP standard access list
   <100-199> IP extended access list
   ```
2. `R1(config)#` **access-list 199 ?**
   ```
   deny Specify packets to reject
   permit Specify packets to forward
   remark Access list entry comment
   ```
3. `R1(config)#` **access-list 199 permit ?**
   ```
   ahp Authentication Header Protocol
   eigrp Cisco's EIGRP routing protocol
   esp Encapsulation Security Payload
   gre Cisco's GRE tunneling
   icmp Internet Control Message Protocol
   ip Any Internet Protocol
   ospf OSPF routing protocol
   ```

```
tcp Transmission Control Protocol
udp User Datagram Protocol
```

4. `R1(config)#` **access-list 199 permit icmp ?**

```
A.B.C.D Source address
any Any source host
host A single source host
```

5. `R1(config)#` **access-list 199 permit icmp any any**
6. All other traffic is denied, by default.

Step 6: Verify the ACL implementation

1. Ping from **Lap01 and Lap02** to **S0 and each other**. The pings will be successful.
2. SSH from **Lap02** to **S0**. The username **Admin** and password **cisco**.

   `PC>` **ssh –l Admin 192.168.1.2**

   Connection timed out; remote host not responding