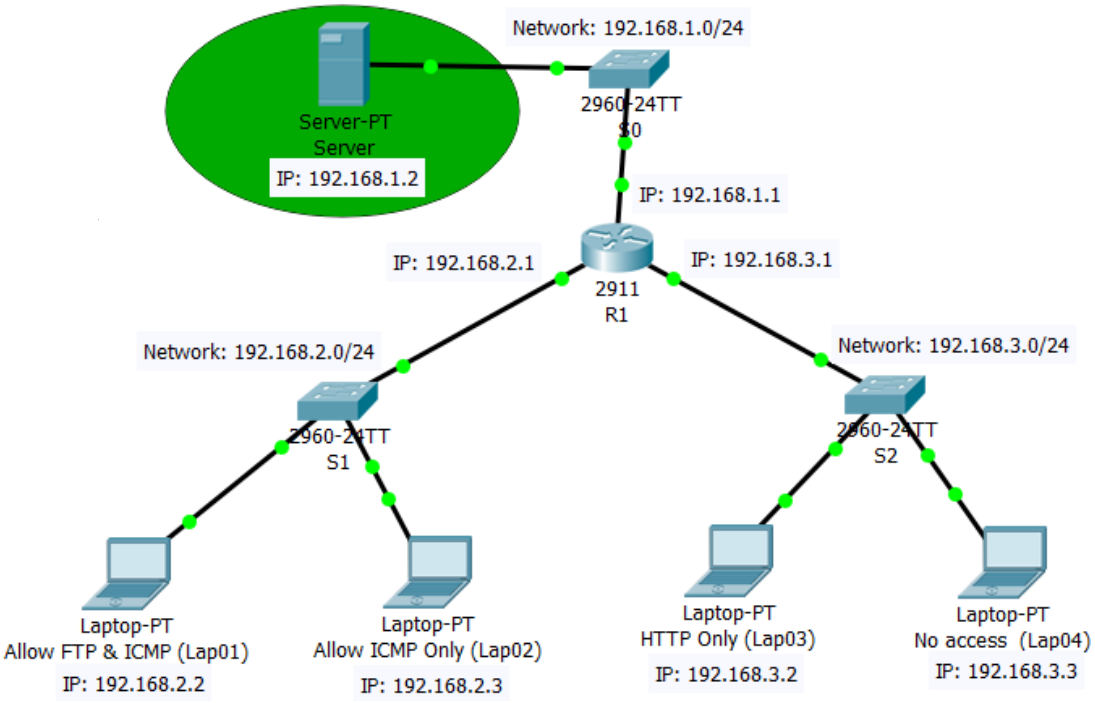
*LAB#06 (*Configuring Extended ACLs - Scenario 1*)*



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: 192.168.2.3
   b. Subnet Mask: 255.255.255.0
   c. Default Gateway: 192.168.2.1
3- Set IP for Lap03 (Desktop -> IP configuration)
   a. IP address: 192.168.3.2
   b. Subnet Mask: 255.255.255.0
   c. Default Gateway: 192.168.3.1
4- Set IP for Lap04 (Desktop -> IP configuration)
   a. IP address: 192.168.3.3
   b. Subnet Mask: 255.255.255.0
   c. Default Gateway: 192.168.3.1
5- Set IP for the Server (Desktop -> IP configuration)
   a. IP address: 192.168.1.2
   b. Subnet Mask: 255.255.255.0
   c. Default Gateway: 192.168.1.1
6- 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

7- Test connectivity.
   a. Ping from Lap01, Lap02, Lap03 & Lap04 to the Server.
   b. Ping from Lap01, Lap02, Lap03 & Lap04 to each other.

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

Step 1: Configure an ACL to permit FTP for Lap01

1. `R1(config)#` **access-list ?**
   ```
   <1-99> IP standard access list
   <100-199> IP extended access list
   ```
2. `R1(config)#` **access-list 100 ?**
   ```
   deny Specify packets to reject
   permit Specify packets to forward
   remark Access list entry comment
   ```
3. `R1(config)#` **access-list 100 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 100 permit tcp ?**
   ```
   A.B.C.D Source address
   any Any source host
   host A single source host
   ```
5. `R1(config)#` **access-list 100 permit tcp host 192.168.2.2 ?**
   ```
   A.B.C.D Source wildcard bits
   ```
6. `R1(config)#` **access-list 100 permit tcp host 192.168.2.2 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 100 permit tcp host 192.168.2.2 host 192.168.1.2 eq ?**

*LAB#06 (*Configuring Extended ACLs - Scenario 1*)*

```
<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 100 permit tcp host 192.168.2.2 host 192.168.1.2 eq ftp**
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 0/1**
2. `R1(config-if)#` **ip access-group 100 in**

Step 3: Verify the ACL implementation

1. Ping from **Lap01, Lap02, Lap03 & Lap04** to **Server**. The pings will be unsuccessful.
2. FTP from **Lap01** to **Server**. The username and password are both **cisco**.
   `PC>` **ftp 192.168.1.2**
3. Exit the FTP service of the **Server**.
   `ftp>` **quit**

Step 4: Configure an ACL to permit ICMP (Ping) for Lap01 & Lap02

1. `R1(config)#` **access-list ?**
   ```
   <1-99> IP standard access list
   <100-199> IP extended access list
   ```
2. `R1(config)#` **access-list 100 ?**
   ```
   deny Specify packets to reject
   permit Specify packets to forward
   remark Access list entry comment
   ```
3. `R1(config)#` **access-list 100 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 100 permit icmp ?**
   ```
   A.B.C.D Source address
   any Any source host
   host A single source host
   ```
5. `R1(config)#` **access-list 100 permit icmp 192.168.2.0 0.0.0.255 ?**
   ```
   A.B.C.D Source wildcard bits
   ```
6. `R1(config)#` **access-list 100 permit icmp 192.168.2.0 0.0.0.255 any**
7. All other traffic is denied, by default.

Step 5: Apply the ACL on the correct interface to filter traffic.

1. `R1(config)#` **interface gigabitEthernet 0/1**
2. `R1(config-if)#` **ip access-group 100 in**

*LAB#06 (*Configuring Extended ACLs - Scenario 1*)*

Step 6: Verify the ACL implementation

1. Ping from **Lap01 and Lap02** to **Server and the other devices**. The pings will be successful.
2. FTP from **Lap01** to **Server**. The username and password are both **cisco**.
   `PC>` **ftp 192.168.1.2**
3. Exit the FTP service of the **Server**.
   `ftp>` **quit**
4. FTP from **Lap02** to **Server**. The username and password are both **cisco**.
   `PC>` **ftp 192.168.1.2**
5. It will not be reached.

Part 2: Configure, Apply and Verify an Extended Named ACL

Step 1: Configure an ACL to permit HTTP access for Lap03

1. `R1(config)#` **ip access-list ?**
   `extended` Extended Access List
   `standard` Standard Access List
2. `R1(config)#` **ip access-list extended HTTP_ONLY**
3. `R1(config-ext-nacl)#` **permit tcp host 192.168.3.2 ?**
4. `R1(config-ext-nacl)#` **permit tcp 192.168.3.2 host 192.168.1.2 eq www**
5. All other traffic is denied, by default.

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

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

Step 3: Verify the ACL implementation.

1. Open the web browser on **Lap03** and enter the IP address of **Server** as the URL. The connection should be successful.

2. There is not any access for **LAP04.**