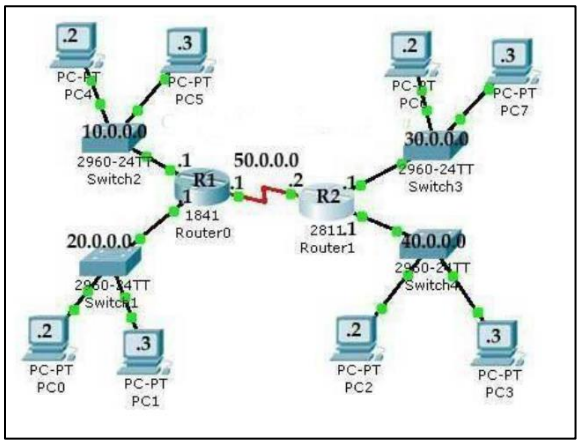
Student Name_____ Student Roll Num_____

LAB # 13: ACCESS CONTROL LIST Part-II

- **Extended ACL Implementation.**

Extended ACLs (100 – 199 and 2000 - 2699)

Over the time security becomes more challenging. To mitigate current security threats, advance filtering is required. Extended ACLs takes this responsibility. Extended ACLs can filter a packet based on its sources address, destination address, port number, protocol and much more. Extended Access List is an extension to the standard ACL. It equips the network administrator with greater authority to control network's security. Along with Extended ACL, we will use a RIP running topology.



Three basic steps to configure Extended Access List

• Use the access-list global configuration command to create an entry in an Extended ACL.

• Use the interface configuration command to select an interface to which apply the ACL.

• Use the ip access-group interface configuration command to activate the existing ACL on an interface.

Command to Configure Extended ACL

access-list access-list-number {permit | deny} protocol source source-wildcard

[operator port] destination destination-wildcard [operator port] [established] [log]

COMMAND PARAMETERS	DESCRIPTIONS
access-list	Main command
access-list-number	Identifies the list using a number in the ranges of 100–199 or 2000–2699.
permit | deny	Indicates whether this entry allows or blocks the specified address.
protocol	IP, TCP, UDP, ICMP, GRE, or IGRP.
Source and destination	Identifies source and destination IP addresses.
source-wildcard and destination-wildcard	The operator can be lt (less than), gt (greater than), eq (equal to), or neq (not equal to). The port number referenced can be either the source port or the destination port, depending on where in the ACL the port number is configured. As an alternative to the port number, well-known application names can be used, such as Telnet, FTP, and SMTP.
established	For inbound TCP only. Allows TCP traffic to pass if the packet is a response to an outbound-initiated session. This type of traffic has the acknowledgement (ACK) bits set. (See the Extended ACL with the Established Parameter example.)

Before we configure Extended Access list you should have knowledge of some important port numbers

Well-Known Port Numbers and IP Protocols

Port Number	IP Protocol
20 (TCP)	FTP data
21 (TCP)	FTP control
23 (TCP)	Telnet
25 (TCP)	Simple Mail Transfer Protocol (SMTP)
53 (TCP/UDP)	Domain Name System (DNS)
69 (UDP)	TFTP
80 (TCP)	HTTP

An extended ACL gives you much more power than just a standard ACL, you can create ACL to:

• Block host to host

• Block host to network

• Block Network to network

• Block telnet access for critical resources of company

• Limited ftp access for user

• Stop exploring of private network form ping

• Limited web access

• Configure established keyword

Block host to host

You are the network administrator at ABC Company. Your company hired a new employee and gave him a pc 10.0.0.3. your company's critical record remains in 40.0.0.3. So, you are asked to block the access of 40.0.0.3 from 10.0.0.3. While 10.0.0.3 must be able to connect with other computers of network to perform his task.

Decide where to apply ACL and in which directions.

As we are configuring extended access list. With extended access list we can filter the packed as soon as it is generated. So, we will place our access list on F0/0 of Router1841 the nearest port of 10.0.0.3

To configure Router:

```
R1>enable
R1#configure terminal
R1(config)#access-list 101 deny ip host 10.0.0.3 40.0.0.3 0.0.0.0
R1(config)#access-list 101 permit ip any any
R1(config)#interface fastEthernet 0/0
R1(config-if)#ip access-group 101 in
R1(config-if)#exit
R1(config)#
```

Verify by doing ping from 10.0.0.3 to 40.0.0.3. It should be request time out. Also, ping other computers of network including 40.0.0.2. ping should be successfully.

Block host to network

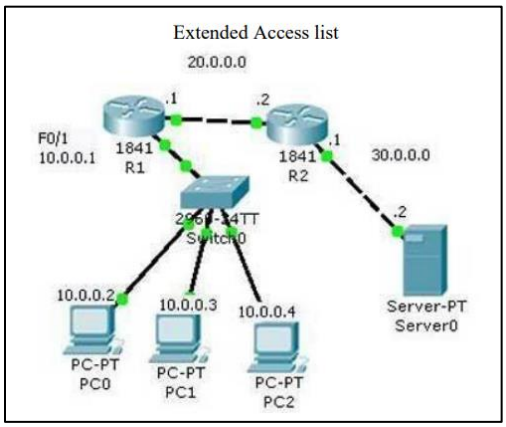
Now we will block the 10.0.0.3 from gaining access on the network 40.0.0.0. (if you are doing this practical after configuring pervious example don't forget to remove the last access list 101. With no access-list command. Or just close the packet tracer without saving and reopen it to be continue with this example.)

```
R1(config)#access-list 102 deny ip host 10.0.0.3 40.0.0.0 0.255.255.255
R1(config)#access-list 102 permit ip any any
R1(config)#interface fastEthernet 0/0
R1(config-if)#ip access-group 102 in
R1(config-if)#exit
```

Application based Extended Access list

In pervious example, we filter ip based traffic. Now we will filter application-based traffic. Using the extended access-list we can create far more complex statements. Considering the following network topology as an example:

Student Name_____ Student Roll Num_____



Grant FTP access to limited user

You want to grant ftp access only to 10.0.0.2. no other user need to provide ftp access on server. So you want to create a list to prevent FTP traffic that originates from the subnet 10.0.0.0/8, going to the 30.0.0.2 server, from traveling in on Ethernet interface E0/1 on R1.

```
R1(config)#access-list 103 permit tcp host 10.0.0.2 30.0.0.2 0.0.0.0 eq 20
R1(config)#access-list 103 permit tcp host 10.0.0.2 30.0.0.2 0.0.0.0 eq 21
R1(config)#access-list 103 deny tcp any any eq 20
R1(config)#access-list 103 deny tcp any any eq 21
R1(config)#access-list 103 permit ip any any
R1(config)#interface fastethernet 0/1
R1(config-if)#ip access-group 103 in
R1(config-if)#exit
```

Filtering TCP Traffic

You can use TCP established to deny all traffic into your network except for incoming traffic that was first initiated from inside your network. This is commonly used to block all originating traffic from the Internet into a company's network except for Internet traffic that was first initiated from users inside the company. The following configuration would accomplish this for all TCP-based traffic coming in to interface serial 0/0/0 on the router:

```
R1(config)#access-list 101 permit tcp any any established
R1(config)#interface serial 0/0/0
R1(config-if)#ip access-group 101 in
R1(config-if)#exit
```

We host our web server on 30.0.0.2. But we do not want to allow external user to ping our server as it could be used as denial of services.

To test this access list ping from 10.0.0.2 to 30.0.0.2 it should be request time out. Now open the web browser and access 30.0.0.2 it should be successfully retrieved.

Student Name_____ Student Roll Num_____

LAB TASK

-ACL to block Network on a host

Block all traffic to 40.0.0.3 from the Network of 10.0.0.0 To accomplish this write an extended access list.

Verify using ping from 10.0.0.3 and 10.0.0.2 to 40.0.0.3. It should request time out. Also, ping computers of another network, ping should be successfully.

-ACL to Block Network on a Network

Block the network of 10.0.0.0 from gaining access on the network 40.0.0.0.