**EXTENDED ACL**

Extended ACLs are always applied near to source. Extended ACLs uses both source and destination. It is used to filter or block the traffic of host and network as well as many services can be blocked with the extended ACLs , like Telnet, WWW etc.

**Task 1:**

**Go to R3 and Run the following Commands to configure Telnet service:**

R3>en

R3#

R3#

R3#confi t

Enter configuration commands, one per line. End with CNTL/Z.

R3(config)#line vty 0 15

**Note:** The virtual terminal or “VTY” lines are virtual lines that allow connecting to the device using telnet. Cisco devices can have up to 16 VTY lines. You can determine how many VTY lines you have by issuing “line vty 0?” from global configuration mode.

R3(config-line)#password ccna

R3(config-line)#login

R3(config-line)#exit

R3(config)#enable secret ccnp

**Task 2:**

**Go to PC0 command prompt to check the working of telnet:**

Packet Tracer PC Command Line 1.0

C:\> telnet 20.0.0.2

Trying 20.0.0.2 ...Open

User Access Verification

Password:

R3>

R3>enable

Password:

R3#sh ip route

**Task 3:**

**Control the telnet access through Extended ACL**

Note: Extended ACL configure at near to source router, Go to R1 fa0/0 for configuration:

R1>en

R1#config t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#access-list ?

<1-99> IP standard access list

<100-199> IP extended access list

R1(config)#access-list 100 deny ?

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

R1(config)#access-list 100 deny tcp host 192.168.1.2 host 20.0.0.2 ?

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

<cr>

R1(config)#access-list 100 deny tcp host 192.168.1.2 host 20.0.0.2 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)

R1(config)#access-list 100 deny tcp host 192.168.1.2 host 20.0.0.2 eq 23

R1(config)#access-list 100 deny tcp host 192.168.1.2 host 192.168.3.1 eq telnet

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

// any for the source & any for the destination, permit any for the host , any for the destination

**Now apply the ACL rules nearest the source fa0/0**

R1(config)#int fa0/0

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

R1(config-if)#

**Now check the working of Telnet from PC 0**

C:\>telnet 20.0.0.2

Trying 20.0.0.2...

% Connection timed out; remote host not responding