Practical 3

Configure extended ACLs - Scenario 1

Addressing Table

Device	Interface	IP Addresses	Subnet Mask	Default Gateway
R1	G 0/0	172.22.34.65	255.255.255.224	N/A
	G0/1	172.22.34.97	255.255.255.240	N/A
	G0/2	172.22.34.1	255.255.255.192	N/A
Server	NIC	172.22.34.62	255.255.255.192	172.22.34.1
PC1	NIC	172.22.34.66	255.255.255.224	172.22.34.65
PC2	NIC	172.22.34.98	255.255.255.240	172.22.34.97

Part 1 - Configure, apply and verify an extended numbered ACL

Step 1 - Configure an ACL to permit FTP and ICMP

R1(config) - access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp

R1(config) - access-list 100 Permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62

Step 2 - Apply the ACL on correct interface to filter traffic

R1(config)# interface g 0/0
R1(config-if)# ip access-group 100 in

Step 3: Verify the ACL implementation

1] Pinging PC1 to Server
PC3 ping 172.22.34.62

2] PC3 ping 172.22.34.62

3] Exit the ping device of the server ping > quit

4] Pinging PC1 to PC2
PC3 ping 172.22.34.98

Part 2 - Configure, apply and verify an Extended Named ACL

Step 1 - Configure an ACL to permit HTTP access and ICMP

R1 (config)# ip access-list extended HTTP-ONLY
R1 (config-ext-nacl)# permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www

R1 (config-ext-nacl)# permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62

Step 2 - Apply the ACL on correct interface

R1 (config)# int g 0/1
R1 (config-if)# ip access-group HTTP-ONLY in

Step 3 - Verify the ACL implementation

a) Ping from PC2 to server
PC> ping 172.22.34.62 # should success

b) ftp 172.22.34.62 # should be fail

c) On web browser of PC2. Enter the ip address of server and connection should be successful.