Practical 3: Configuring Extended ACLs

IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Gig0/0	172.22.34.1	255.255.255.192	-
	Gig0/1	172.22.34.65	255.255.255.224	-
	Gig0/2	172.22.34.97	255.255.255.240	-
Server	Fa0	172.22.34.62	255.255.255.192	172.22.34.1
PC1	Fa0	172.22.34.66	255.255.255.224	172.22.34.65
PC2	Fa0	172.22.34.98	255.255.255.240	172.22.34.97

a. Extended Numbered ACL

1. In R1

```
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

R1(config)#int Gig0/1

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

R1(config-if)#exit
```

2. In PC1

Ping from PC1 to Server and it should be successful

FTP from PC2 to Server should be successful with username and password both ***cisco***. Exit FTP using *quit* command

```
ftp> quit
```

Ping from PC1 to PC2 will be unsuccessful

b. Extended Named ACL

1. In R1

```
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

R1(config-ext-nacl)#exit

R1(config)#int Gig0/2

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

R1(config-if)#exit
```

2. In PC2

Ping from PC2 to Server. It should be successful

FTP from PC2 to Server will fail.

Open Web Browser in PC2 and enter 172.22.34.62 and it should display cisco website