

Practical 3**Configuring Extended ACLs: Configure, Apply and Verify an Extended Numbered ACL**

The Cisco Access Control List (ACL) are used for filtering traffic based on a given filtering criteria on a router or switch interface. Based on the conditions supplied by the ACL, a packet is allowed or blocked from further movement.

Cisco ACLs are available for several types of routed protocols including IP, IPX, AppleTalk, XNS, DECnet, and others. However, we will be discussing ACLs pertaining to TCP/IP protocol only.

ACLs for TCP/IP traffic filtering are primarily divided into two types:

- ☐ Standard Access Lists, and
- ☐ Extended Access Lists

Standard Access Control Lists:

Standard IP ACLs range from 1 to 99. A Standard Access List allows you to permit or deny traffic FROM specific IP addresses. The destination of the packet and the ports involved can be anything.

This is the command syntax format of a standard ACL.

access-list *access-list-number* {permit|deny} {host|source source-wildcard|any}

Standard ACL example:

access-list 10 permit 192.168.2.0 0.0.0.255

This list allows traffic from all addresses in the range 192.168.2.0 to 192.168.2.255

Note that when configuring access lists on a router, you must identify each access list uniquely by assigning either a name or a number to the protocol's access list.

There is an implicit deny added to every access list. If you entered the command:

show access-list 10

The output looks like:

access-list 10 permit 192.168.2.0 0.0.0.255 access-list 10 deny any

Extended Access Control Lists:

Extended IP ACLs allow you to permit or deny traffic from specific IP addresses to a specific destination IP address and port. It also allows you to have granular control by specifying controls for different types of protocols such as ICMP, TCP, UDP, etc within the ACL statements. Extended IP ACLs range from 100 to 199. In Cisco IOS Software Release 12.0.1, extended ACLs began to use additional numbers (2000 to 2699).

The syntax for IP Extended ACL is given below:

access-list *access-list-number* {deny | permit} *protocol* *source* *source-wildcard* *destination* *destination-wildcard* [*precedence* *precedence*]

Note that the above syntax is simplified, and given for general understanding only.

Extended ACL example:

access-list 110 - Applied to traffic leaving the office (outgoing)

access-list 110 permit tcp 92.128.2.0 0.0.0.255 any eq 80

ACL 110 permits traffic originating from any address on the 92.128.2.0 network. The 'any' statement means that the traffic is allowed to have any destination address with the limitation of going to port 80. The value of 0.0.0.0/255.255.255.255 can be specified as 'any'.

Applying an ACL to a router interface:

After the ACL is defined, it must be applied to the interface (inbound or outbound). The syntax for applying an ACL to a router interface is given below:

```
interface <interface> ip access-group {number|name} {in|out}
```

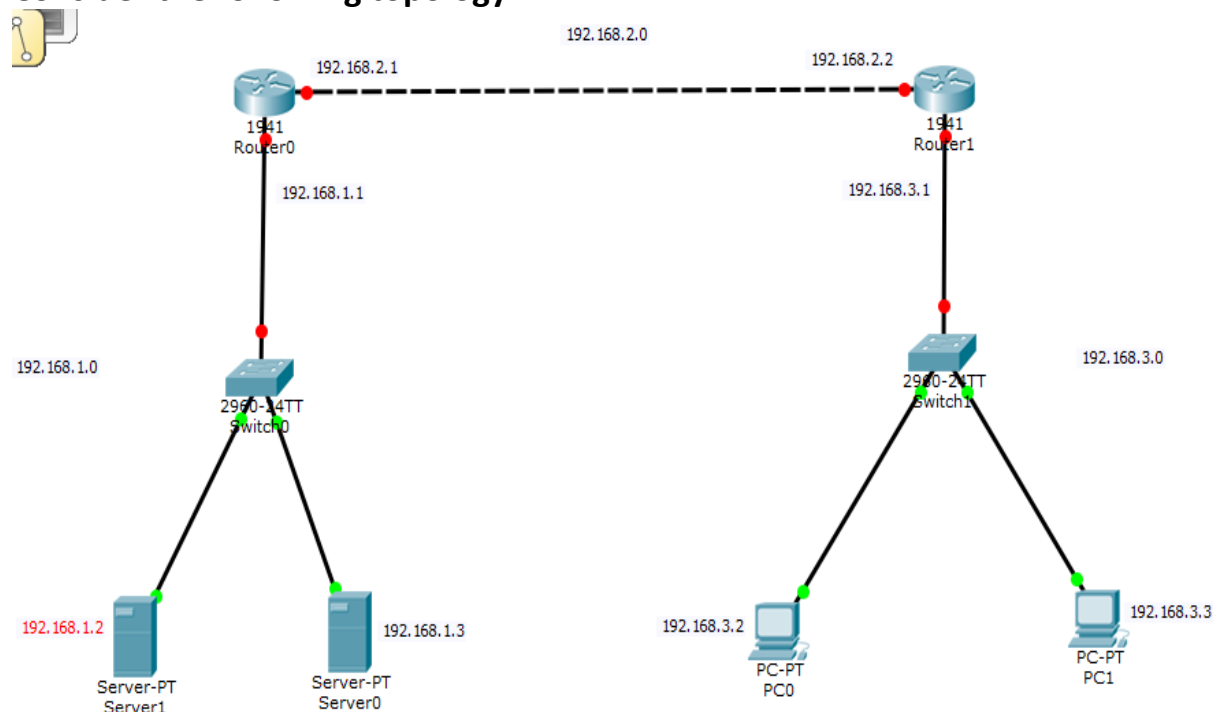
An Access List may be specified by a name or a number. "in" applies the ACL to the inbound traffic, and "out" applies the ACL on the outbound traffic.

Example: To apply the standard ACL created in the previous example, use the following commands:

```
Rouer(config)#interface serial0
```

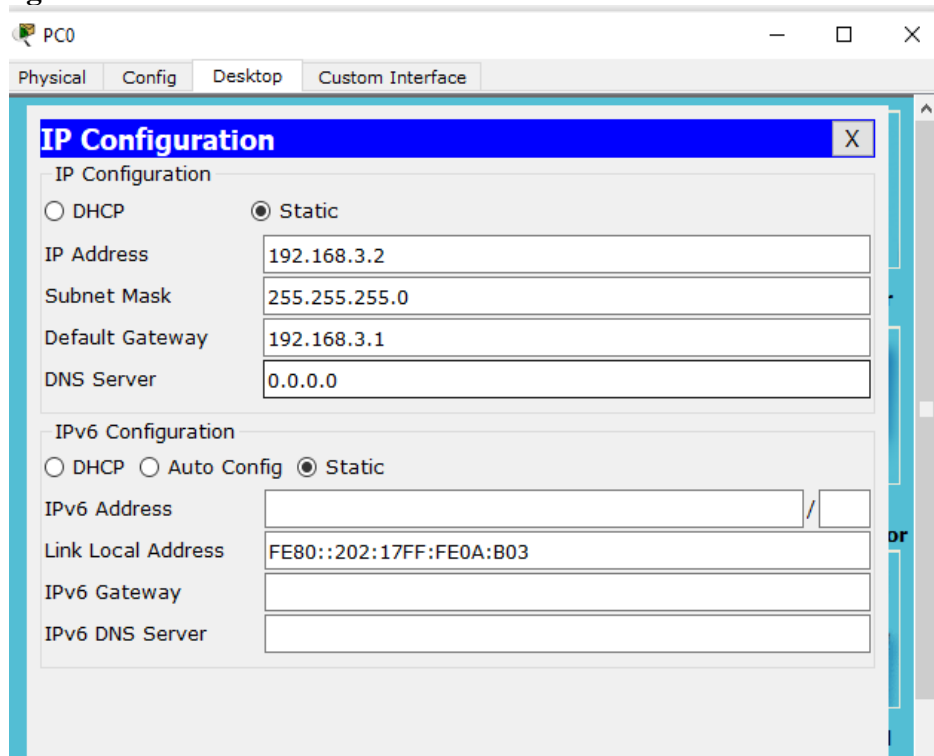
```
Rouer(config-if)#ip access-group 10 out
```

Consider the following topology



Topology Configuration

Configuring PC0

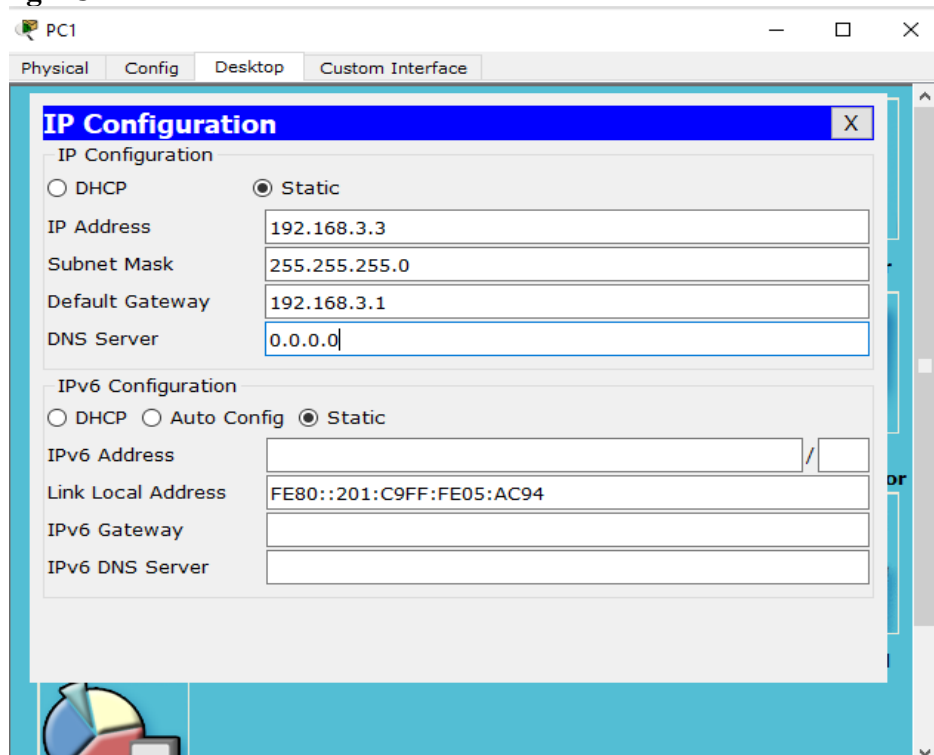


The screenshot shows the configuration window for PC0. The 'Config' tab is selected. The 'IP Configuration' section is expanded, showing the 'Static' radio button selected. The IP Address is 192.168.3.2, Subnet Mask is 255.255.255.0, Default Gateway is 192.168.3.1, and DNS Server is 0.0.0.0. The 'IPv6 Configuration' section is also expanded, showing the 'Static' radio button selected. The IPv6 Address is empty, Link Local Address is FE80::202:17FF:FE0A:B03, IPv6 Gateway is empty, and IPv6 DNS Server is empty.

IP Configuration	
<input type="radio"/> DHCP <input checked="" type="radio"/> Static	
IP Address	192.168.3.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.3.1
DNS Server	0.0.0.0

IPv6 Configuration	
<input type="radio"/> DHCP <input type="radio"/> Auto Config <input checked="" type="radio"/> Static	
IPv6 Address	
Link Local Address	FE80::202:17FF:FE0A:B03
IPv6 Gateway	
IPv6 DNS Server	

Configuring PC1



The screenshot shows the configuration window for PC1. The 'Config' tab is selected. The 'IP Configuration' section is expanded, showing the 'Static' radio button selected. The IP Address is 192.168.3.3, Subnet Mask is 255.255.255.0, Default Gateway is 192.168.3.1, and DNS Server is 0.0.0.0. The 'IPv6 Configuration' section is also expanded, showing the 'Static' radio button selected. The IPv6 Address is empty, Link Local Address is FE80::201:C9FF:FE05:AC94, IPv6 Gateway is empty, and IPv6 DNS Server is empty.

IP Configuration	
<input type="radio"/> DHCP <input checked="" type="radio"/> Static	
IP Address	192.168.3.3
Subnet Mask	255.255.255.0
Default Gateway	192.168.3.1
DNS Server	0.0.0.0

IPv6 Configuration	
<input type="radio"/> DHCP <input type="radio"/> Auto Config <input checked="" type="radio"/> Static	
IPv6 Address	
Link Local Address	FE80::201:C9FF:FE05:AC94
IPv6 Gateway	
IPv6 DNS Server	

Configuring Router0

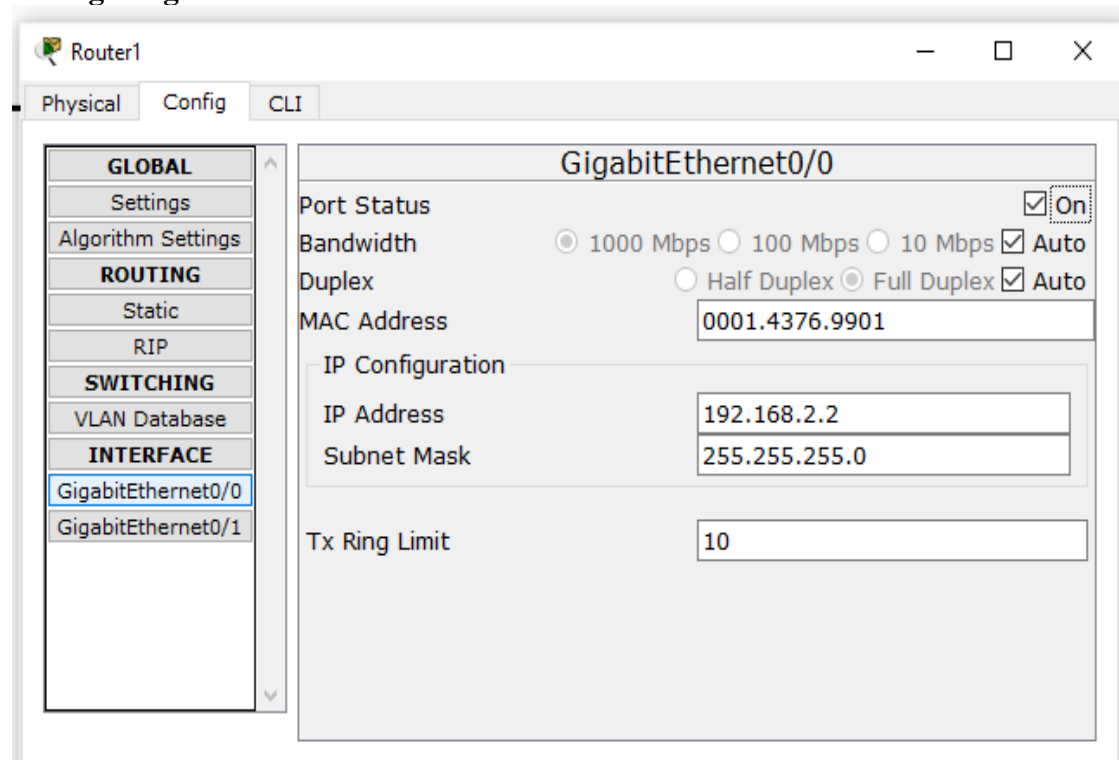
The screenshot shows the configuration window for Router0, specifically for the GigabitEthernet0/0 interface. The left sidebar contains a tree view with categories: GLOBAL, ROUTING, SWITCHING, and INTERFACE. Under INTERFACE, GigabitEthernet0/0 is selected. The main panel displays the configuration for this interface. The Port Status is checked and set to On. Bandwidth is set to 1000 Mbps, Duplex is set to Half Duplex, and MAC Address is 00D0.582D.C101. The IP Configuration section shows IP Address 192.168.1.1 and Subnet Mask 255.255.255.0. The Tx Ring Limit is set to 10.

GigabitEthernet0/0	
Port Status	<input checked="" type="checkbox"/> On
Bandwidth	<input checked="" type="radio"/> 1000 Mbps <input type="radio"/> 100 Mbps <input type="radio"/> 10 Mbps <input checked="" type="checkbox"/> Auto
Duplex	<input checked="" type="radio"/> Half Duplex <input type="radio"/> Full Duplex <input checked="" type="checkbox"/> Auto
MAC Address	00D0.582D.C101
IP Configuration	
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Tx Ring Limit	10

The screenshot shows the configuration window for Router0, specifically for the GigabitEthernet0/1 interface. The left sidebar is the same as the previous screenshot, but GigabitEthernet0/1 is now selected. The main panel displays the configuration for this interface. The Port Status is checked and set to On. Bandwidth is set to 1000 Mbps, Duplex is set to Half Duplex, and MAC Address is 00D0.582D.C102. The IP Configuration section shows IP Address 192.168.2.1 and Subnet Mask 255.255.255.0. The Tx Ring Limit is set to 10.

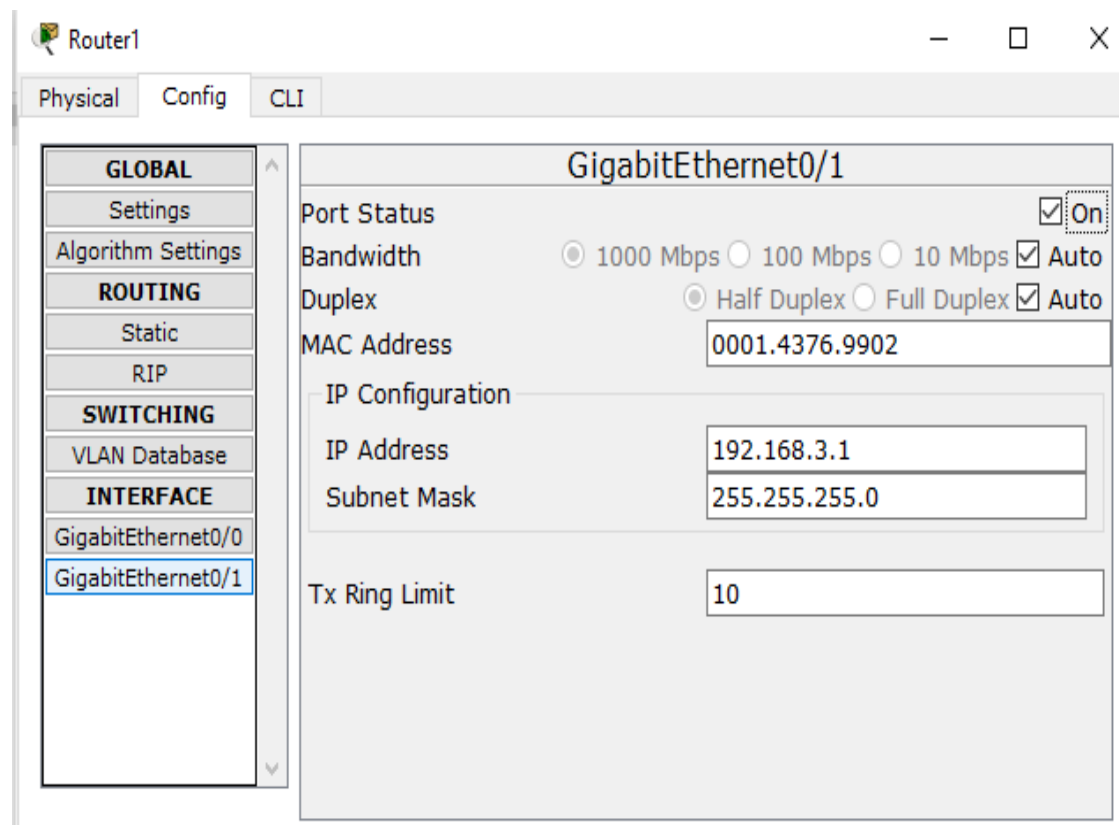
GigabitEthernet0/1	
Port Status	<input checked="" type="checkbox"/> On
Bandwidth	<input checked="" type="radio"/> 1000 Mbps <input type="radio"/> 100 Mbps <input type="radio"/> 10 Mbps <input checked="" type="checkbox"/> Auto
Duplex	<input checked="" type="radio"/> Half Duplex <input type="radio"/> Full Duplex <input checked="" type="checkbox"/> Auto
MAC Address	00D0.582D.C102
IP Configuration	
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Tx Ring Limit	10

Configuring Router1



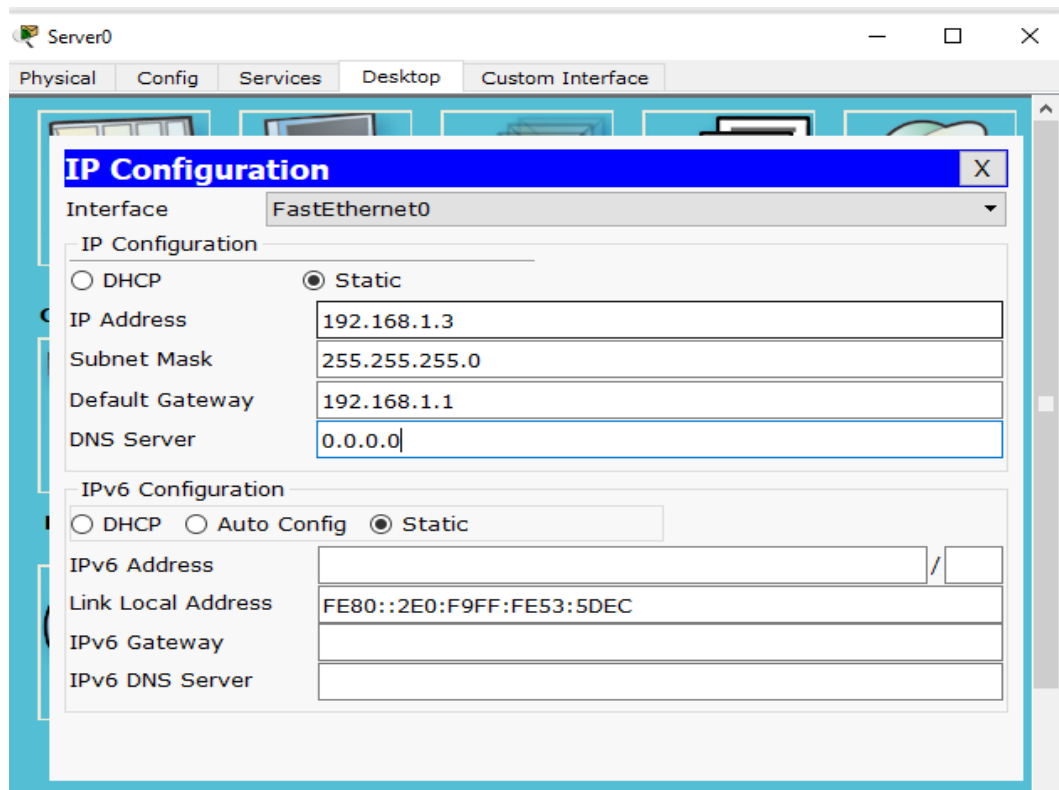
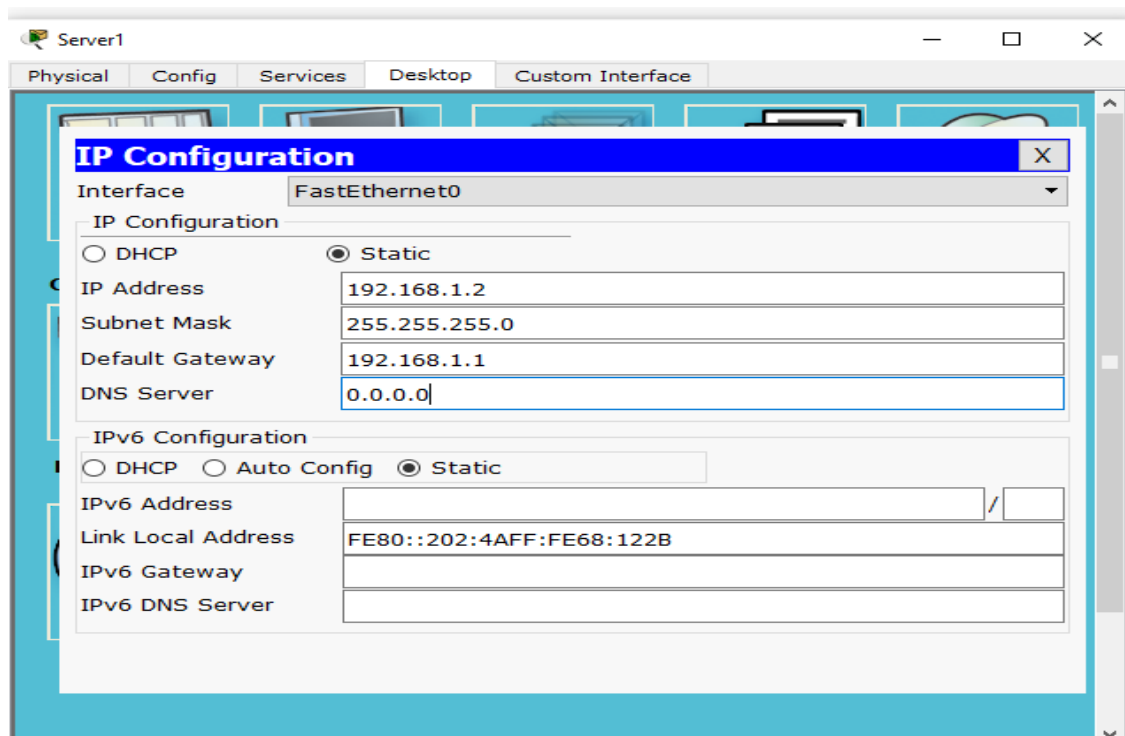
The screenshot shows the configuration window for Router1, specifically for the GigabitEthernet0/0 interface. The window has tabs for Physical, Config, and CLI. The left sidebar shows a tree view with categories: GLOBAL, Settings, Algorithm Settings, ROUTING, Static, RIP, SWITCHING, VLAN Database, and INTERFACE. Under INTERFACE, GigabitEthernet0/0 is selected. The main area displays the configuration for GigabitEthernet0/0. The Port Status is checked and set to On. Bandwidth is set to 1000 Mbps, 100 Mbps, or 10 Mbps, with Auto selected. Duplex is set to Half Duplex or Full Duplex, with Auto selected. The MAC Address is 0001.4376.9901. The IP Configuration section shows the IP Address as 192.168.2.2 and the Subnet Mask as 255.255.255.0. The Tx Ring Limit is set to 10.

GigabitEthernet0/0	
Port Status	<input checked="" type="checkbox"/> On
Bandwidth	<input type="radio"/> 1000 Mbps <input type="radio"/> 100 Mbps <input type="radio"/> 10 Mbps <input checked="" type="checkbox"/> Auto
Duplex	<input type="radio"/> Half Duplex <input checked="" type="radio"/> Full Duplex <input checked="" type="checkbox"/> Auto
MAC Address	0001.4376.9901
IP Configuration	
IP Address	192.168.2.2
Subnet Mask	255.255.255.0
Tx Ring Limit	10

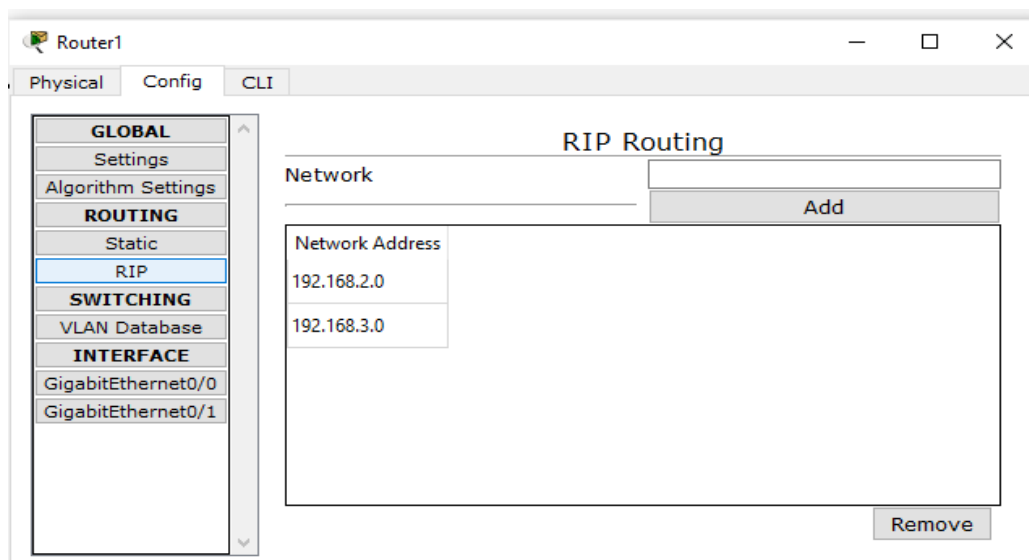
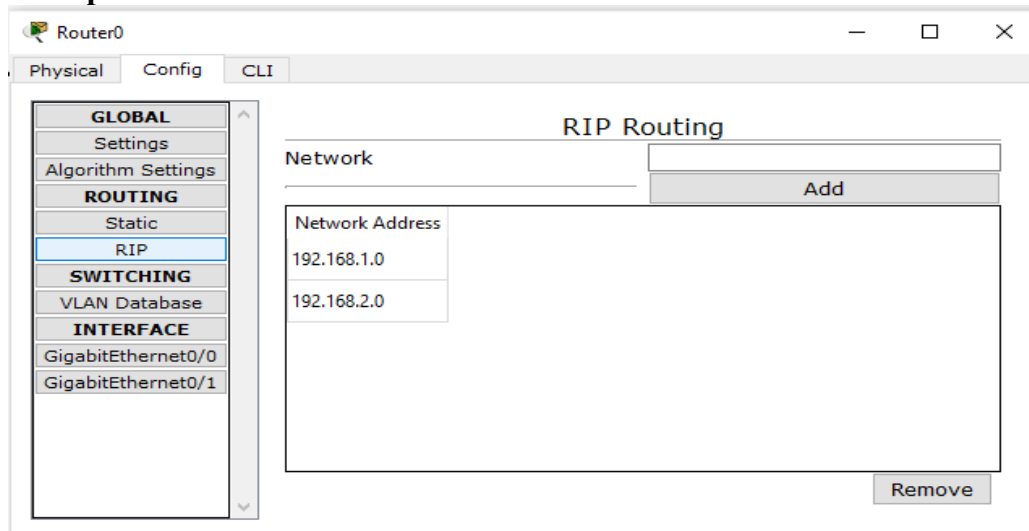


The screenshot shows the configuration window for Router1, specifically for the GigabitEthernet0/1 interface. The window has tabs for Physical, Config, and CLI. The left sidebar shows a tree view with categories: GLOBAL, Settings, Algorithm Settings, ROUTING, Static, RIP, SWITCHING, VLAN Database, and INTERFACE. Under INTERFACE, GigabitEthernet0/1 is selected. The main area displays the configuration for GigabitEthernet0/1. The Port Status is checked and set to On. Bandwidth is set to 1000 Mbps, 100 Mbps, or 10 Mbps, with Auto selected. Duplex is set to Half Duplex or Full Duplex, with Auto selected. The MAC Address is 0001.4376.9902. The IP Configuration section shows the IP Address as 192.168.3.1 and the Subnet Mask as 255.255.255.0. The Tx Ring Limit is set to 10.

GigabitEthernet0/1	
Port Status	<input checked="" type="checkbox"/> On
Bandwidth	<input type="radio"/> 1000 Mbps <input type="radio"/> 100 Mbps <input type="radio"/> 10 Mbps <input checked="" type="checkbox"/> Auto
Duplex	<input checked="" type="radio"/> Half Duplex <input type="radio"/> Full Duplex <input checked="" type="checkbox"/> Auto
MAC Address	0001.4376.9902
IP Configuration	
IP Address	192.168.3.1
Subnet Mask	255.255.255.0
Tx Ring Limit	10

Configuring Server0**Configuring Server1**

Set the RIP protocol on both the Routers as follows



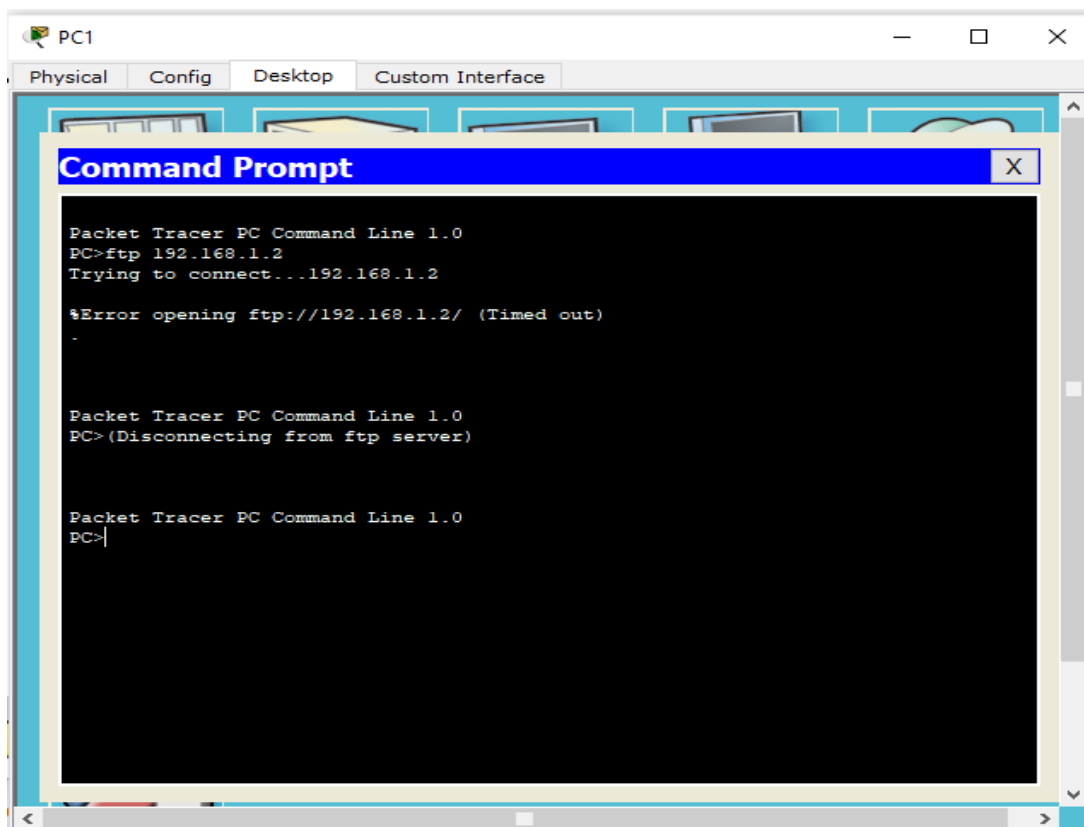
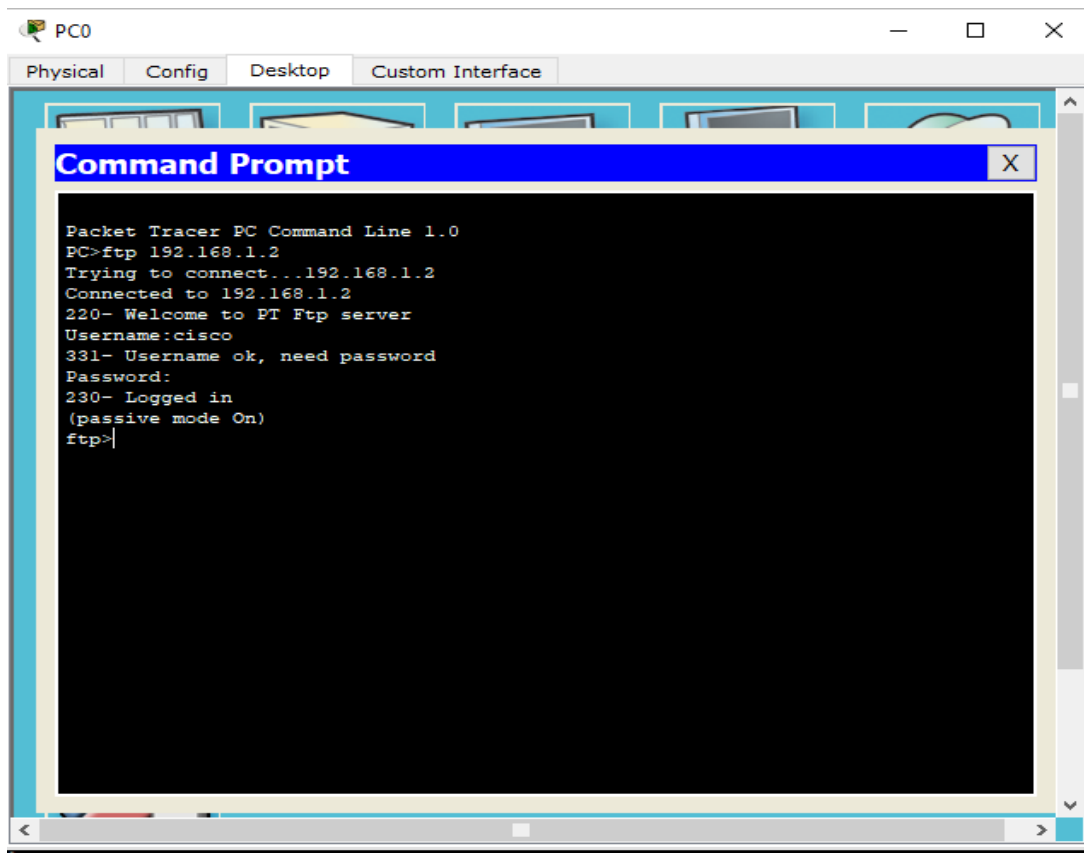
Check the connectivity by using the ping command

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

Click on Router1 go to CLI tab and press enter and enter the following commands: -

```
Router>en
Router#conf t
Router(config)# access-list 100 permit tcp host 192.168.3.2 host 192.168.1.2 eq ftp
Router(config)# interface GigabitEthernet0/0
Router(config)# ip access-group 100 out
Router(config-line)#exit
Router(config)#
```

Now verify the ftp (ftp 192.168.1.2) command from both the PCs, one would be successful (PC0) and other (PC1) would fail.



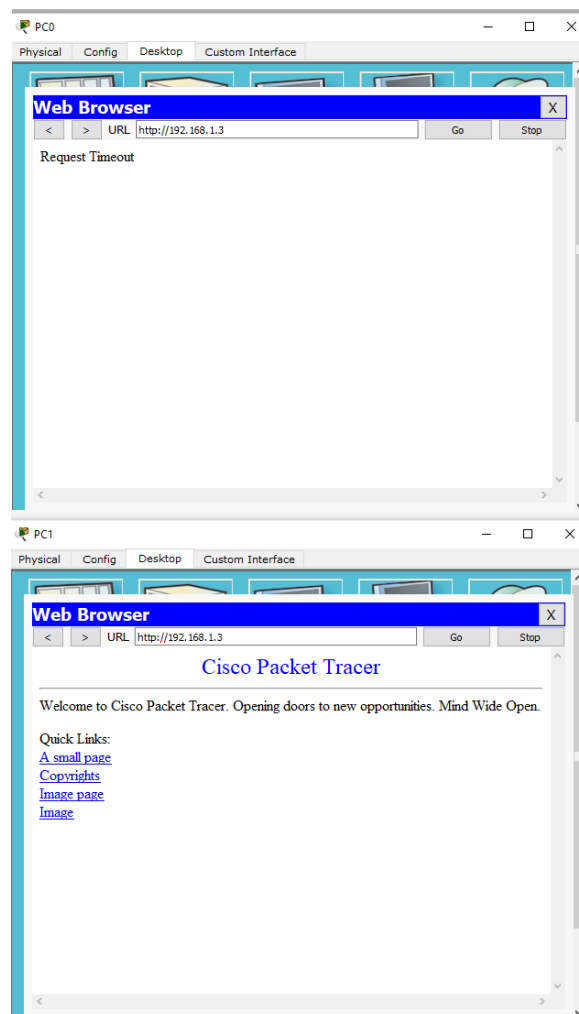
Part 2: Configure, Apply and Verify an Extended Named ACL

We use the same topology for this case

Click on Router1 go to CLI tab and press enter and enter the following commands: -

```
Router>en
Router#conf t
Router(config)# ip access-list extended DALMIA
Router(config-ext-nacl)# permit tcp host 192.168.3.3 host 192.168.1.3 eq www
Router(config-ext-nacl)#exit
Router(config)#
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip access-group DALMIA out
Router(config-if)#exit
Router(config)#
```

Now verify the www (192.168.1.3) command from both the PCs browser, one would be successful (PC1) and other (PC0) would fail.



Hence Extended Numbered ACLs as well as Extended Named ACLs have been verified
