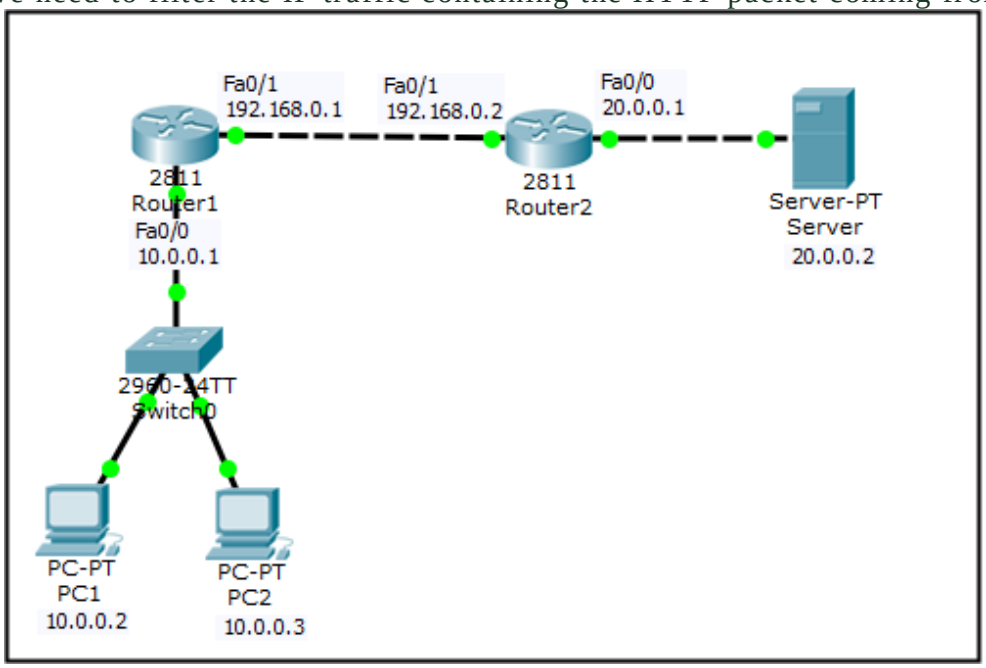
Extended ACL

How to Configure Extended Access List on Router

Steps to Configure Extended ACL

To configure an Extended ACL, we will use the following network topology. In this example, we will deny host 10.0.0.2 from accessing the Web server (20.0.0.2). To do so, we need to filter the IP traffic containing the HTTP packet coming from 10.0.0.2 host.



In order to prevent host 10.0.0.2 to access the Web server (20.0.0.2), you need to execute the following commands on Router2.

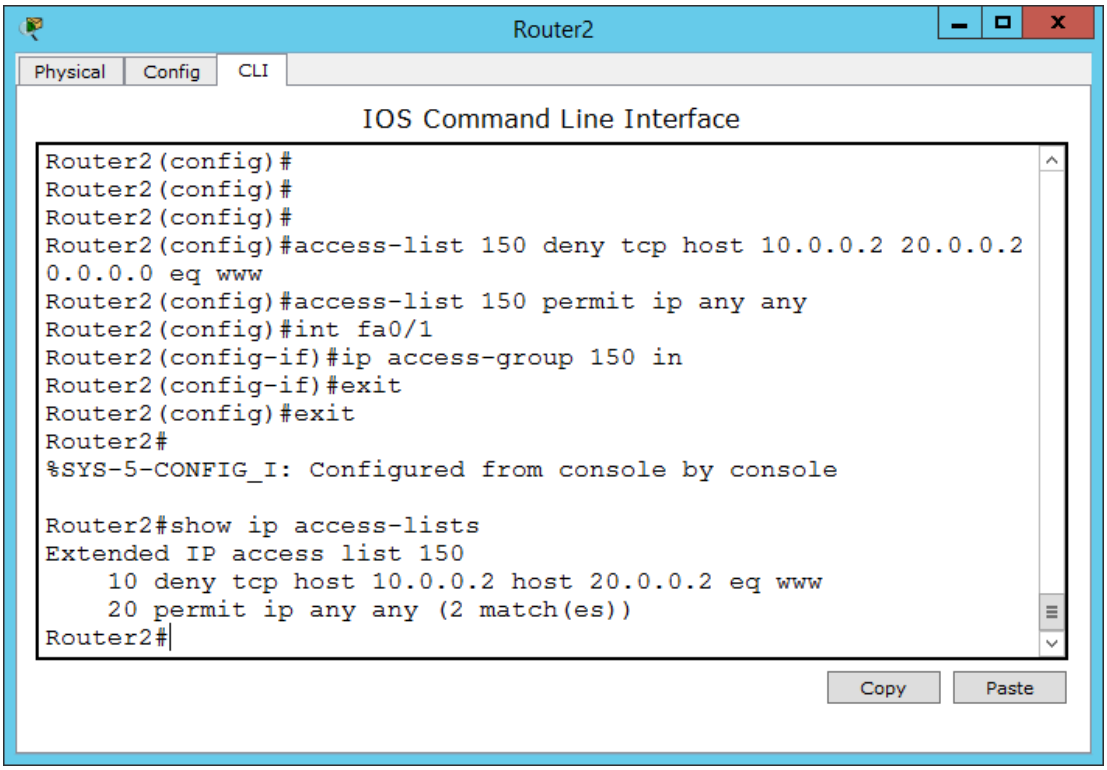
```
Router2(config)#access-list 150 deny tcp host 10.0.0.2 host
20.0.0.2 0.0.0.0 eq www
Router2(config)#access-list 150 permit tcp host 10.0.0.3 host 20.0.0.2
0.0.0.0 eq ftp
Router2(config)#access-list 150 deny icmp host 10.0.0.3 host 20.0.0.2
0.0.0.0

Router2(config)#access-list 150 permit ip any any
Router2(config)#int fa0/1
Router2(config-if)#ip access-group 150 in
Router2(config-if)#exit
Router2(config)#exit
```

Once you applied an ACL on the desired interface (in this case fa0/1), you can view the configured access lists by executing the following command.

```
Router2#show ip access-lists
```

4. The following figure shows how to configure an extended ACL on a Cisco router.



Verify Access Control List Configuration

1. To verify your configuration, open the Web browser on PC1, type http://20.0.0.2, and press Enter. You should not be able to access the Web server as shown in the following figure.

2. Now move on to PC2 and try to access the Web server, this time you should be able to access the Webserver.

That's all you need to know to configure an Extended ACL on Cisco router. In this post, we have learned how to configure Extended ACl on Cisco Routers using the numbered method. In the next posts, we will learn how to configure Extended ACL using the named ACL method. If you found this article helpful, please share with others too. Sharing this article will not cost you anything.