Namal Institute Mianwali

Computer Networks Laboratory Manual #13

Access Control List (ACL)

Course Title	Computer Networks	**Course Number**	CS – 331 L
Instructor	Shahzad Arif shahzad.arif@namal.edu.pk	**Lab Engineer**	Asad Majeed asad.majeed@namal.edu.pk
Submitted By	Muhammad Abrar Hussain	**Roll No.**	NIM-BSCS-2020-62
Lab No.	13	**Email**	Abrarhussain2020@namal.edu.pk

Access Control List

Access list provides the ability to control the traffic in the network. We can set up an access list according to our requirements. Access list filters out traffic based on the configuration.

Cisco router IOS has enough command through which we can control traffic effectively however special hardware like pix firewall or ASA firewalls have many extra security features.

Access list rules or conditions are read series wise so if any network that is denied earlier will not be permitted even after adding the permit statement e.g.

1. Deny 192.168.1.0 0.0.0.255
2. Permit host 192.168.1.5

In the above access list rules, we have denied the complete 192.168.1.0 network and in the second rule, we are permitting the host from the same network. As access-list rules are read in the series, the router will drop every packet from this network because it matches the deny rule. The router will read the second rule later but till then the traffic from that network is denied already so we have to be careful when setting up the rules for the access list.

Standard access-list vs. extended access-list

Standard access-list:

Standard access list only filters out traffic based on the source IP. This access list does not have any other way to filter traffic so this provides basic functionality.

Features of standard access list

1. A standard access list is very easy to configure.
2. It is very light on the processor so it does not overload the hardware.

Extended access list: Extended access lists can filter out traffic based on source IP, destination IP, protocols like TCP, UDP, ICMP, etc, and port numbers.

Feature of extended access list

1. It's not easy to configure as compared to the standard access list however it provides many filters that we can use to control traffic efficiently.
2. Requires more processor cycles due to the complexity of the defined rules.

Configuring Standard Access list in Cisco packet tracer

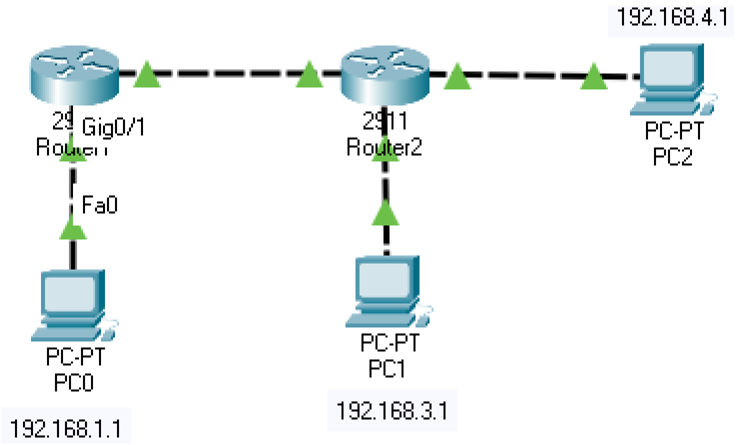


Figure: 1

In this Standard Access list configuration, we will block PC0 traffic from reaching router 2.

We are using the following commands to create an access list.

The standard access list can be given a number from 1-to 99 so we will give the number 1 to our access-list.

```
Router(config)#access-list 1 deny 192.168.1.1
Router(config)#access-list 1 permit any
```

While creating an access list, we have to make sure to use permit any command to allow other traffic that we don’t want to block because there is an invincible deny at the end of every access list so if this command is missed then the access-list will block all traffic.

Now, we have created the access list however it will not work until we apply this to the router’s interface. While enabling access-list on the router’s interface, we must make sure that it is being applied to the correct interface and in the right direction, otherwise standard list will not work because it filters traffic according to the source IP.

To apply, we have to use the following command.

```
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ip access-group 1 out
```

An access list is applied to the router’s interface in the inbound and outbound directions. We can only enable 1 access-list per interface and direction.

In the above example, an access list is enabled on the gigabit Ethernet port of router 1 in the outbound direction as we want to block traffic from PC0 from reaching router 2.

Once the access list is enabled, we can check if it working appropriately by generating traffic. This can be checked by pinging the router from the host.

Following is the outcome when router 2 pinged from the host.

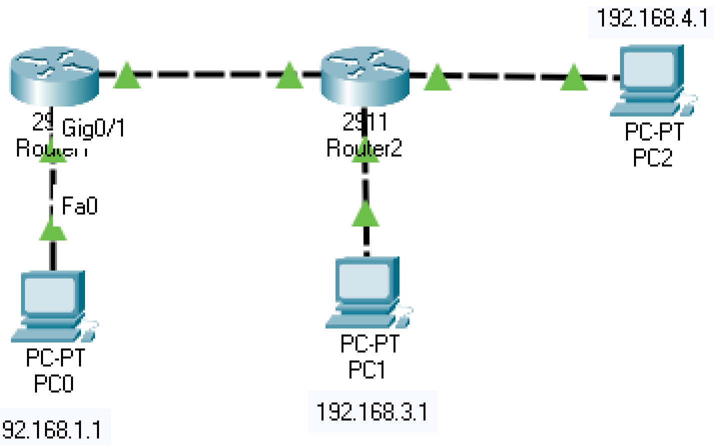
```
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.1.2: Destination host unreachable.
Reply from 192.168.1.2: Destination host unreachable.
Reply from 192.168.1.2: Destination host unreachable.
Reply from 192.168.1.2: Destination host unreachable.
```

We can use the following command to verify if the access list has blocked packets.

```
Router#show access-lists
Standard IP access list 1
10 deny host 192.168.1.1 (4 match(es))
20 permit any
```

As seen in the command output, deny condition has blocked the traffic from the host, 4 matches are for those ping packets that were sent to the router.

Configuring Extended Access list in Cisco packet tracer



As we have discussed, an extended access list can filter traffic on a protocol basis so we will block PC2 from pinging all other devices in the network.

We have used the following commands to create the access list

```
Router(config)#ip access-list extended 100
Router(config-ext-nacl)#deny icmp host 192.168.4.1 any
Router(config-ext-nacl)#permit ip any any
```

Numbers 100 to 199 are reserved for the extended list. We have chosen the number 100 and added two conditions to the list.

We have applied this access-list in the inbound direction on router 2.

Only ICMP traffic is blocked, this protocol is used for the ping functionality so now PC2 should not be able to ping any device in the network however rest of the traffic is permitted.

We can test the access-list by generating ICMP traffic using the ping command from PC2.

As expected, traffic is blocked by the router. Please check the ping result below

```
C:\>ping 192.168.4.2

Pinging 192.168.4.2 with 32 bytes of data:
```

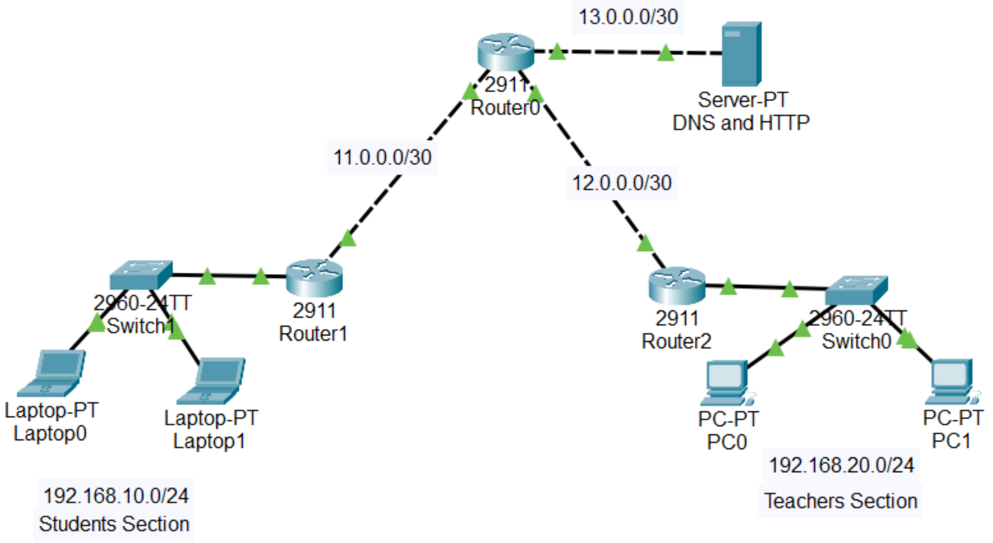
```
Reply from 192.168.4.2: Destination host unreachable.
Reply from 192.168.4.2: Destination host unreachable.
Reply from 192.168.4.2: Destination host unreachable.
Reply from 192.168.4.2: Destination host unreachable.

Ping statistics for 192.168.4.2:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),



C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.4.2: Destination host unreachable.
Reply from 192.168.4.2: Destination host unreachable.
Reply from 192.168.4.2: Destination host unreachable.
Reply from 192.168.4.2: Destination host unreachable.

Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Access list blocked 8 packets that were generated from PC2

```
Router#sh access-lists
Extended IP access list 100
10 deny icmp host 192.168.4.1 any (8 match(es))
20 permit ip any any
```

TASKS

Create the following network in the cisco packet tracer

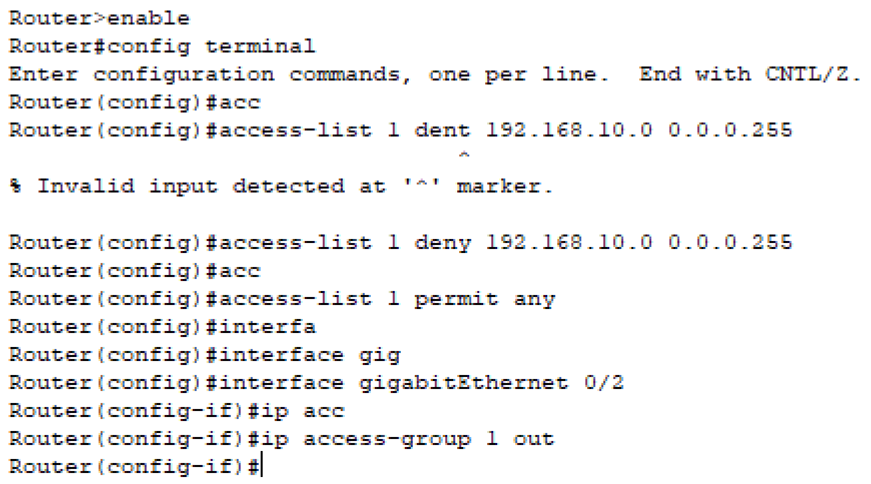


Do the following tasks

Task 1

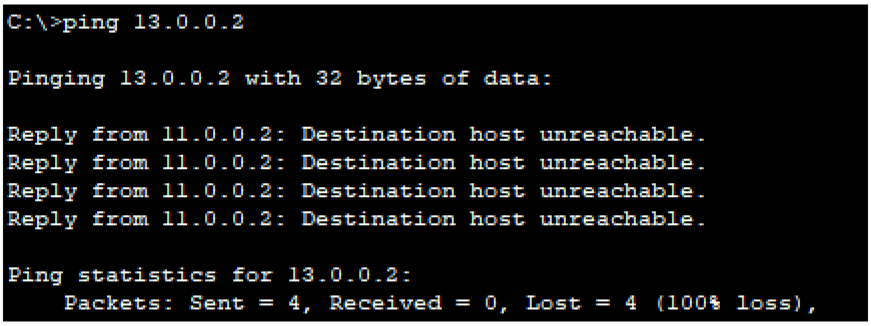
Use a standard access-list to block traffic from student's sections to the server but the students section pc should be able to ping Teacher's section PC.

Router CLI Snapshot:



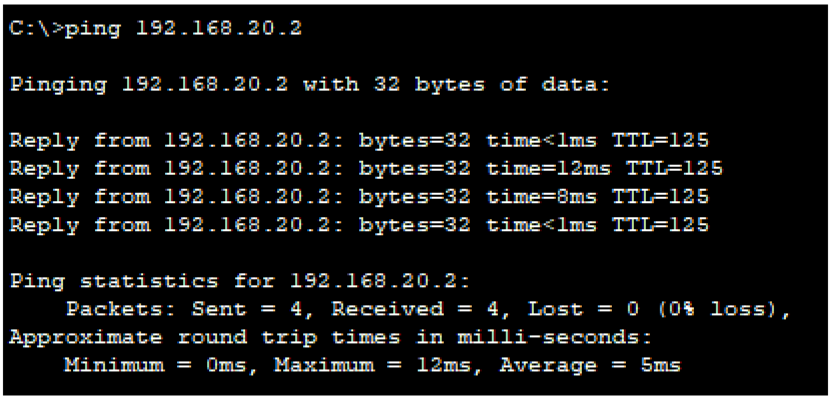
```
Router>enable
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#acc
Router(config)#access-list 1 dent 192.168.10.0 0.0.0.255
                                ^
% Invalid input detected at '^' marker.

Router(config)#access-list 1 deny 192.168.10.0 0.0.0.255
Router(config)#acc
Router(config)#access-list 1 permit any
Router(config)#interfa
Router(config)#interface gig
Router(config)#interface gigabitEthernet 0/2
Router(config-if)#ip acc
Router(config-if)#ip access-group 1 out
Router(config-if)#
```

Ping from Laptop0 to the server:



```
C:\>ping 13.0.0.2

Pinging 13.0.0.2 with 32 bytes of data:

Reply from 11.0.0.2: Destination host unreachable.
Reply from 11.0.0.2: Destination host unreachable.
Reply from 11.0.0.2: Destination host unreachable.
Reply from 11.0.0.2: Destination host unreachable.

Ping statistics for 13.0.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Ping from Laptop0 to the PC0:



```
C:\>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:

Reply from 192.168.20.2: bytes=32 time<1ms TTL=125
Reply from 192.168.20.2: bytes=32 time=12ms TTL=125
Reply from 192.168.20.2: bytes=32 time=8ms TTL=125
Reply from 192.168.20.2: bytes=32 time<1ms TTL=125

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 12ms, Average = 5ms
```

Task 2

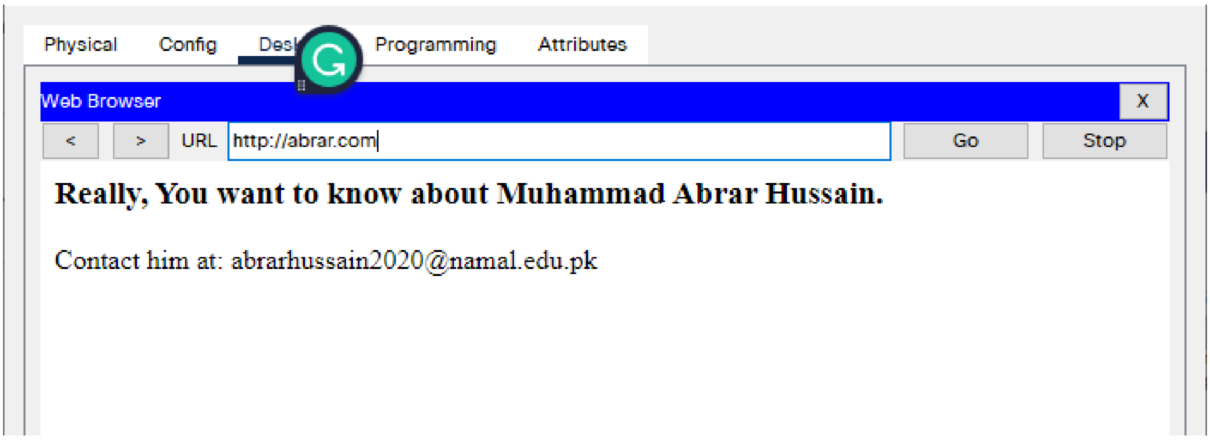
Use extended access-list to block DNS traffic generated from PC0.

Snapshot of the Router CLI:

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip access-list extended 130
Router(config-ext-nacl)#deny udp host 192.168.20.2 any
Router(config-ext-nacl)#permit ip any any
Router(config-ext-nacl)#exit
Router(config)#interface gigabitEthernet 0/2
Router(config-if)#ip access-group 130 out
Router(config-if)#exit
Router(config)#
```

Snapshot of the PC0 Browser accessing HTTP server with Domain Name:

- **Before implementing the extended control list**

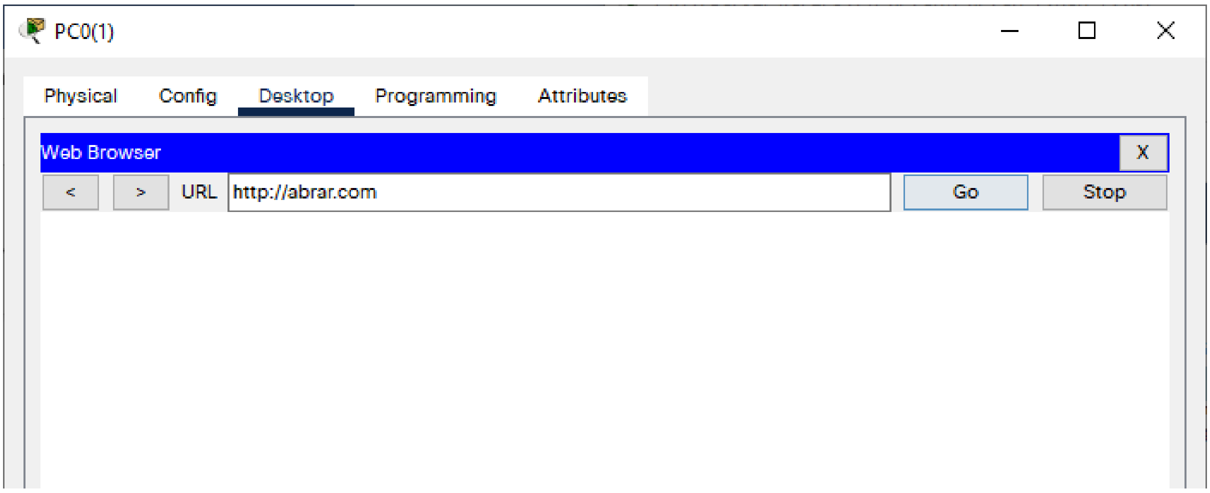


URL http://abrar.com

Really, You want to know about Muhammad Abrar Hussain.

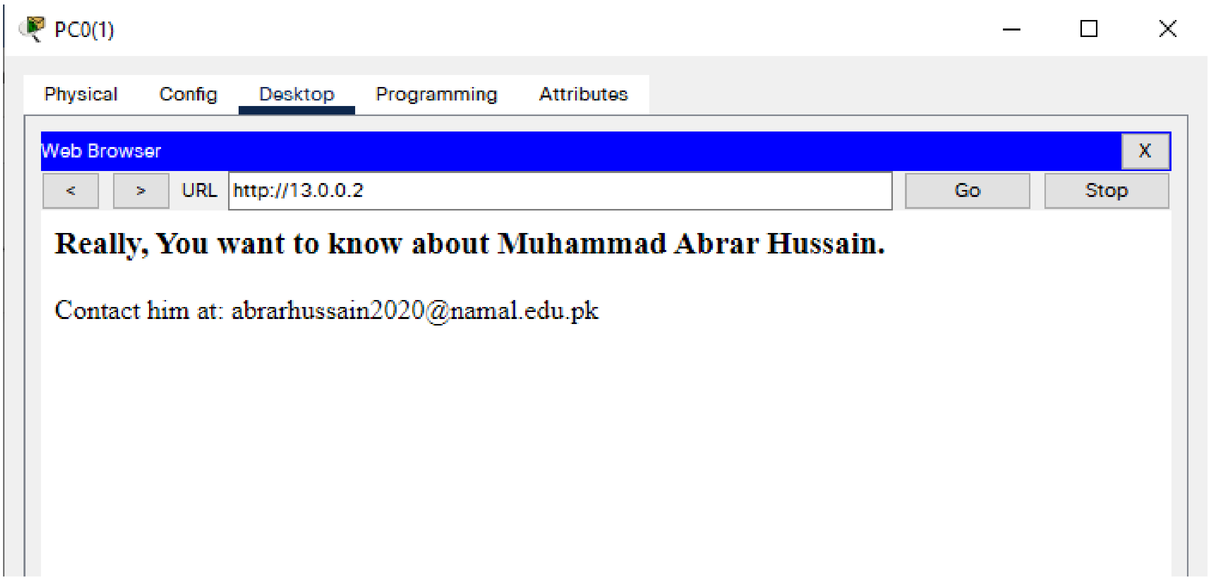
Contact him at: abrarhussain2020@namal.edu.pk

- **After implementing the standard control list**



URL http://abrar.com

Snapshot of the PC0 Browser accessing HTTP server with IP Address:

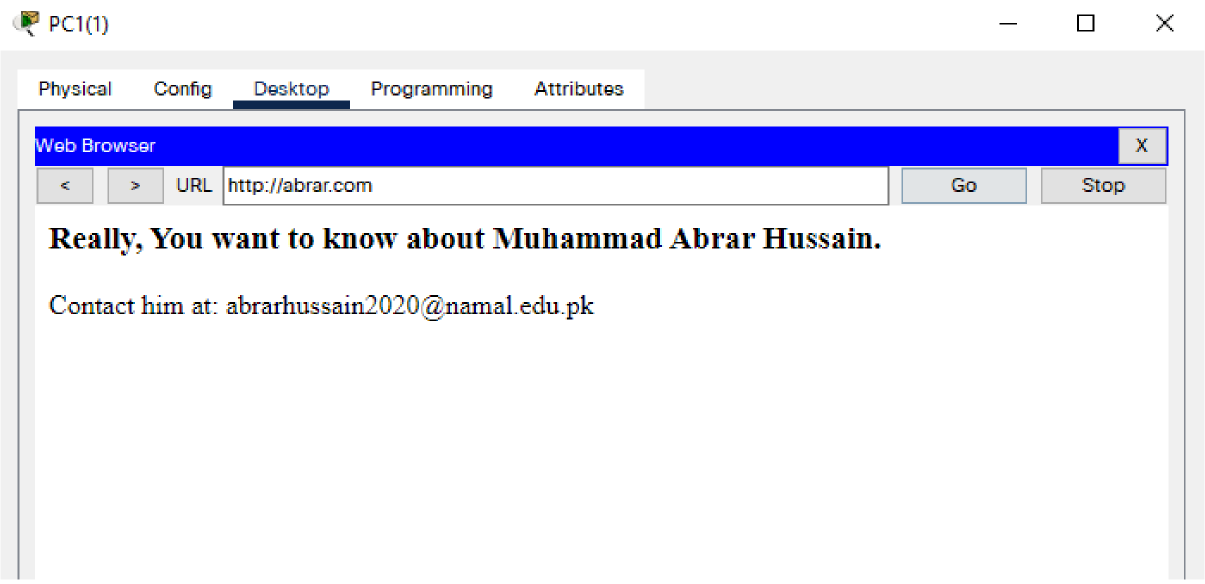


http://13.0.0.2

Really, You want to know about Muhammad Abrar Hussain.

Contact him at: abrarhussain2020@namal.edu.pk

Snapshot of the PC1 Browser accessing HTTP server with Domain Name:



http://abrar.com

Really, You want to know about Muhammad Abrar Hussain.

Contact him at: abrarhussain2020@namal.edu.pk

Upload the lab manual and .pkt file to QoBE.

Rubrics Sheet

Lab Exercise	Marks
Implementing Standard Control List	5
Implementing Extended Control List	5