NATIONAL UNIVERSITY OF COMPUTER & EMERGING SCIENCE
Computer Network Lab (CL3001)
Lab Session 13

Objective:

- Introduction to Access Control List (ACL)
- Types of ACL
- Advantages of ACL
- Rules of ACL
- ACL Implementation in Packet Tracer
- Lab Exercise

ACCESS CONTROL LIST (ACL)

1. Introduction to Access Control List (ACL):

Access-list (ACL) is a set of rules defined for controlling network traffic and reducing network attacks. ACLs are used to filter traffic based on the set of rules defined for the incoming or outgoing of the network. ACLs are mainly found in network devices with packet filtering capabilities including routers and switches.

Different ACLs have different working mechanisms based on what they do. For File system ACLs, they work by creating tables that inform the operating system of access privileges given for certain system subjects. Each object has a unique security property that acts as an identification factor in its access control list. Some privileges include read/write privileges, file execution, and several others.

Some popular operating systems utilizing this mechanism include Unix-based systems, Windows NT/2000, and Novell's Netware.

In the case of Networking ACLS, they are installed in networking devices (Routers and switches) with the sole purpose of filtering traffic. This is done by using pre-defined rules that decided which packets transferred. Source and destination IP addresses also play a major role in this decision.

Packet filtering improves network security by decreasing network traffic access, restricting device and user access to the involved network.

Access lists are sequential, and are made up of two major components; permit and deny statements. A name and a number are used to identify access lists.

ACL Features

1. The set of rules defined are matched serial wise i.e. matching starts with the first line, then 2nd, then 3rd, and so on.
2. The packets are matched only until it matches the rule. Once a rule is matched then no further comparison takes place and that rule will be performed.
3. There is an implicit denial at the end of every ACL, i.e., if no condition or rule matches then the packet will be discarded.

Once the access-list is built, then it should be applied to inbound or outbound of the interface:

Inbound access lists –
When an access list is applied on inbound packets of the interface then first the packets will be processed according to the access list and then routed to the outbound interface.

Outbound access lists –
When an access list is applied on outbound packets of the interface then first the packet will be routed and then processed at the outbound interface.

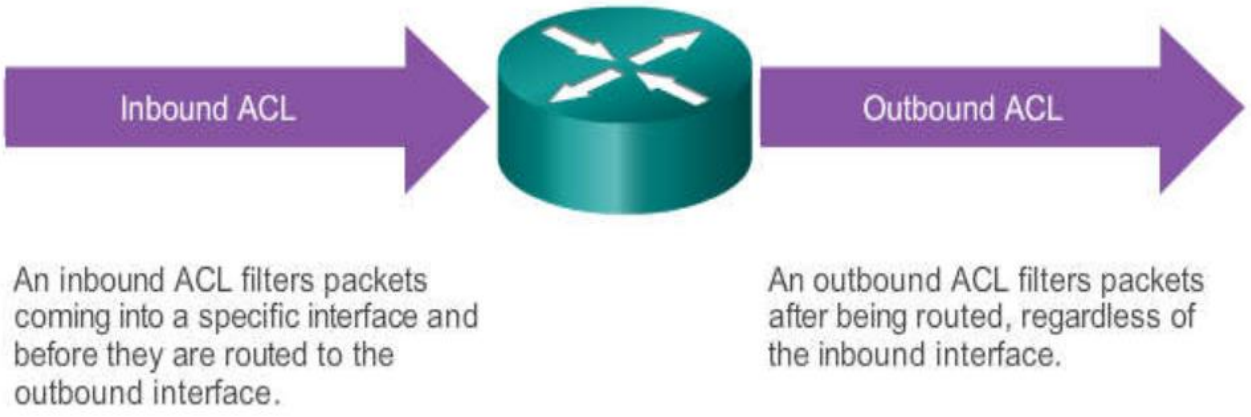

Fig-1: Inbound & Outbound

2. Types of ACL:

There are four types of ACLs that play different roles in a network including, Standard, Reflexive, Extended, and Dynamic:

1. Standard ACL

These are the Access-list that are made using the source IP address only. These ACLs permit or deny the entire protocol suite. They don't distinguish between the IP traffic such as TCP, UDP, HTTPS, etc. By using numbers 1-99 or 1300-1999, the router will understand it as a standard ACL and the specified address as the source IP address.

2. Extended ACL

These are the ACL that uses source IP, Destination IP, source port, and Destination port. These types of ACL, we can also mention which IP traffic should be allowed or denied. These use range 100-199 and 2000-2699.

3. Reflexive ACL

Also known as IP session ACLs, Reflective ACLs use upper-layer session details to filter traffic.

4. Dynamic ACL

As the term suggests, Dynamic ACLs are reliable on extended ACLs, Telnet, and authentication. They grant users access to a resource only if the user authenticates the device through telnet.

Also, there are two categories of access-list:

1. ***Numbered access-list*** – These are the access list that cannot be deleted specifically once created i.e., if we want to remove any rule from an Access-list then this is not permitted in the case of the numbered access list. If we try to delete a rule from the access list then the whole access list will be deleted. The numbered access-list can be used with both standard and extended access lists.

2. ***Named access list*** – In this type of access list, a name is assigned to identify an access list. It is allowed to delete a named access list, unlike numbered access list. Like numbered access lists, these can be used with both standards and extended access lists.

3. Advantages of ACL:

- Improve network performance.
- Provides security as the administrator can configure the access list according to the needs and deny the unwanted packets from entering the network.
- Provides control over the traffic as it can permit or deny according to the need of the network.

4. Rules of ACL:

1. The standard Access-list is generally applied close to the destination (but not always).
2. The extended Access-list is generally applied close to the source (but not always).
3. We can assign only one ACL per interface per protocol per direction, i.e., only one inbound and outbound ACL is permitted per interface.
4. We can't remove a rule from an Access-list if we are using numbered Access-list. If we try to remove a rule then the whole ACL will be removed. If we are using named access lists then we can delete a specific rule.
5. Every new rule which is added to the access list will be placed at the bottom of the access list therefore before implementing the access lists, analyses the whole scenario carefully.
6. As there is an implicit deny at the end of every access list, we should have at least a permit statement in our Access-list otherwise all traffic will be denied.
7. Standard access lists and extended access lists cannot have the same name.

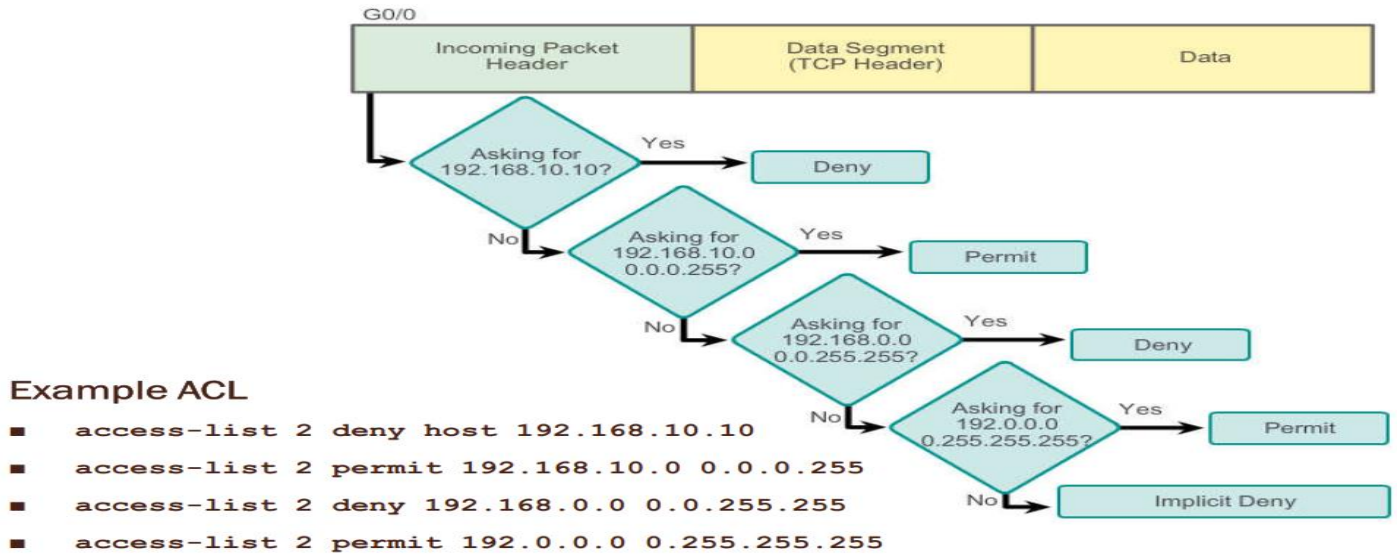

Fig-2: Flow of ACL checking packet

5. ACL Implementation in Packet Tracer:

Create the network topology given in figure 3. Implement IP addresses scheme and configure RIPv2 in routers. Then ping server from laptop 1 to test the connectivity.

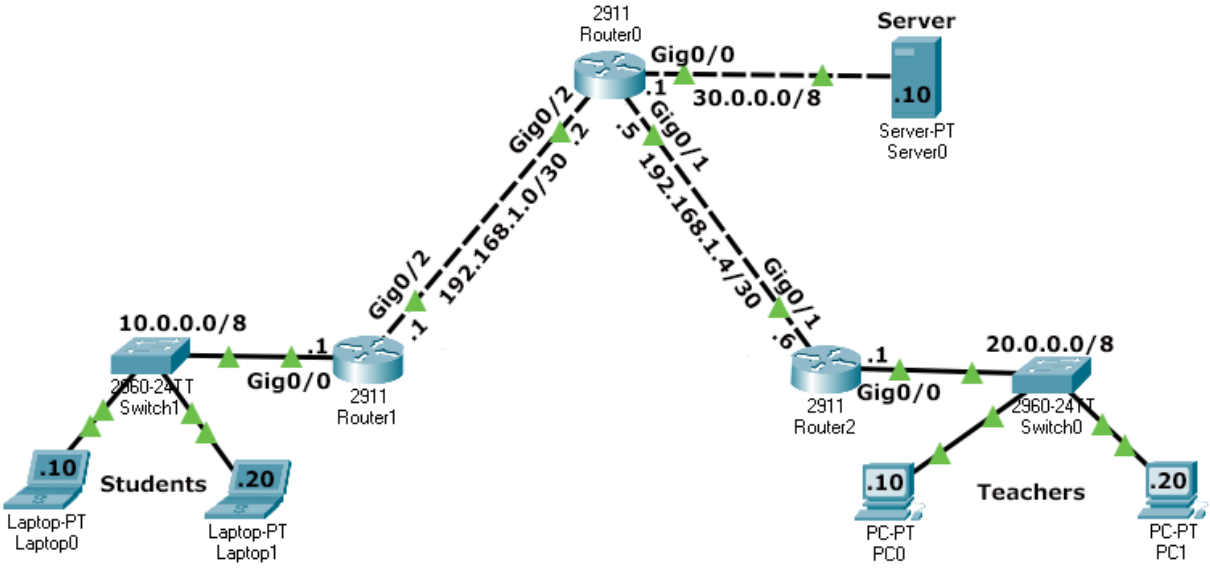

Fig-3: Network Topology showing Student & teacher subnets

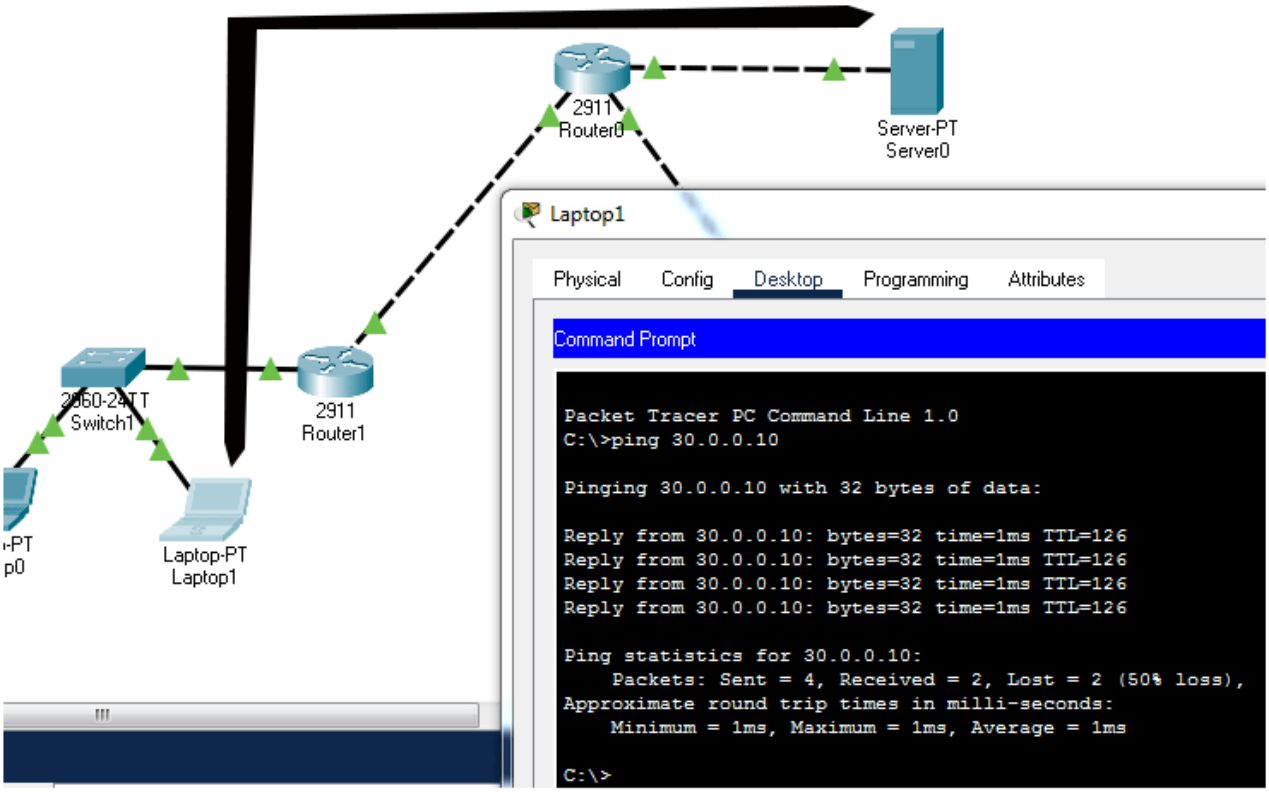

Fig-4: Connectivity between laptop 1 & server

Create and implement a standard access list that blocks the student's section from accessing the Server section.

The students section uses IP subnet 10.0.0.0/8. All packets originating from this section have an IP address from this subnet. If we create a standard ACL with a deny statement for this subnet, all packets having an IP address from this subnet in their source address will be dropped.

A router's interface uses the ACL to filter traffic passing through it. An incorrectly implemented ACL can block entire traffic passing through it. Before creating and implementing an ACL, we have to select the correct interface and the correct direction for the ACL.

In our network, we have seven locations where we can implement the ACL. The following image shows these locations and the direction in which they can be used to filter traffic.

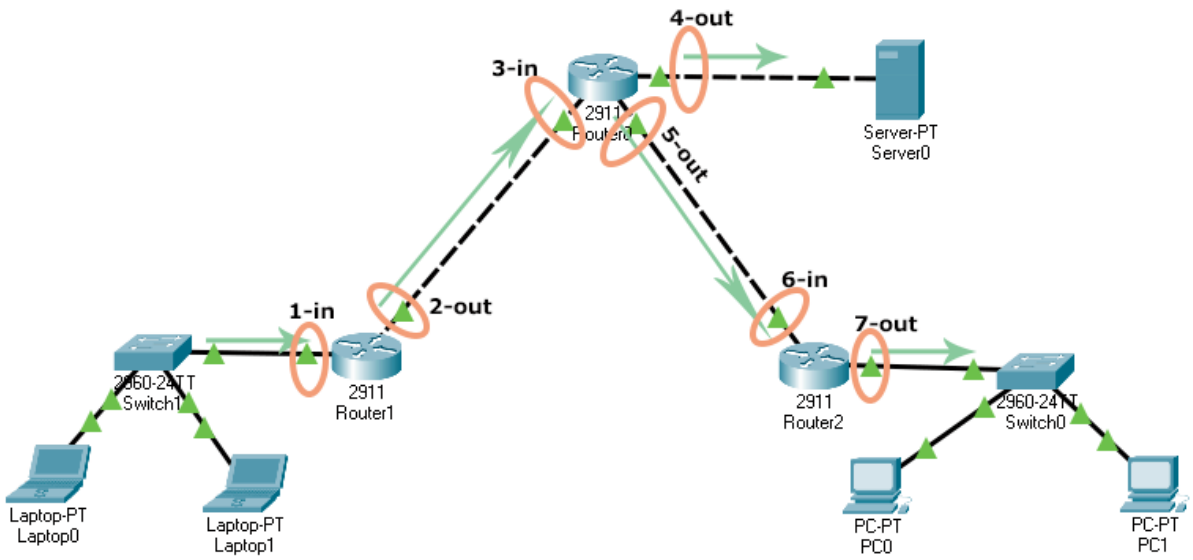

Fig-5: Network Topology showing all inbound & outbound

Location	Interface	Direction	Effect
1	Router1's Gig0/0	In	The student's section will not be able to access the Server and the Teachers section.
2	Router1's Gig0/2	Out	The student's section will not be able to access the Server and Teachers section.
3	Router0's Gig0/2	In	The student's section will not be able to access the Server and Teachers section.
4	**Router0's Gig0/0**	**Out**	**The student's section will not be able to access the Server section but it will be able to access the Teachers section.**
5	Router0's Gig0/1	Out	The student's section will not be able to access the Teachers section but it will be able to access the Server section.
6	Router1's Gig0/1	In	The student's section will not be able to access the Teachers section but it will be able to access the Server section.
7	Router1's Gig0/0	Out	The student's section will not be able to access the Teachers section but it will be able to access the Server section.

Table-1: Shows location & impact of ACL

Standard ACL configuration commands

We have two commands to create a standard access list. These commands are 'access-list' and 'ip access-list'. The 'ip access-list' command has an advantage over the 'access-list' command. It allows us to update or modify statements. We have already learned how to use the 'access-list' command to create a standard access list in the previous part of this tutorial. In this part, let's use the 'ip access-list' command.

The 'ip access-list' is a global configuration mode command. To create a standard access list, it uses the following syntax.

Router(config)# ip access-list standard ACL_#

In the above syntax, the ACL_# is the name or number of the standard ACL. When you hit the enter key after entering this command, the command prompt changes and you enter standard ACL configuration mode.

Router(config-std-acl)#

In standard ACL configuration mode, you can use the following syntax to create statements.

Router(config)# ip access-list standard ACL_name
Router(config-std-acl)# permit|deny source_IP_address [wildcard_mask]

An ACL does nothing until it is applied to an interface. To apply a standard ACL to an interface, enter the interface configuration mode of the interface and use the following command.

Router(config)# interface type [slot_#]port_#
Router(config-if)# ip access-group ACL_# in|out

Once an ACL is activated on an interface, the interface processes all packets through it.

Now applying ACL on Router 0.

Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip access-list standard BlockStudents
Router(config-std-nacl)#deny 10.0.0.0 0.255.255.255
Router(config-std-nacl)#permit any
Router(config-std-nacl)#exit
Router(config)#interface gigabitethernet 0/0
Router(config-if)#ip access-group BlockStudents out
Router(config-if)#exit
Router(config)#exit
Router#

Let's discuss the above commands. We used the first two commands to enter global configuration mode. The next command creates a standard ACL named **BlockStudents**. In ACL configuration mode, we added two statements. The first statement denies all traffic from the 10.0.0.0/8 subnet. The second statement allows all other traffic. We used the next commands to exit ACL configuration mode and enter interface configuration mode. The next command applies the **BlockStudents** ACL in the out direction. The last two commands exit interface configuration mode and global configuration mode, respectively.
To verify the ACL, we can test connectivity between sections. The student's section should not be able to access the Server section but it should be able to access the Teachers section. The Teachers section should be able to access both the Server and the Students section. You can use the ping command to test connectivity. The following image shows this testing.

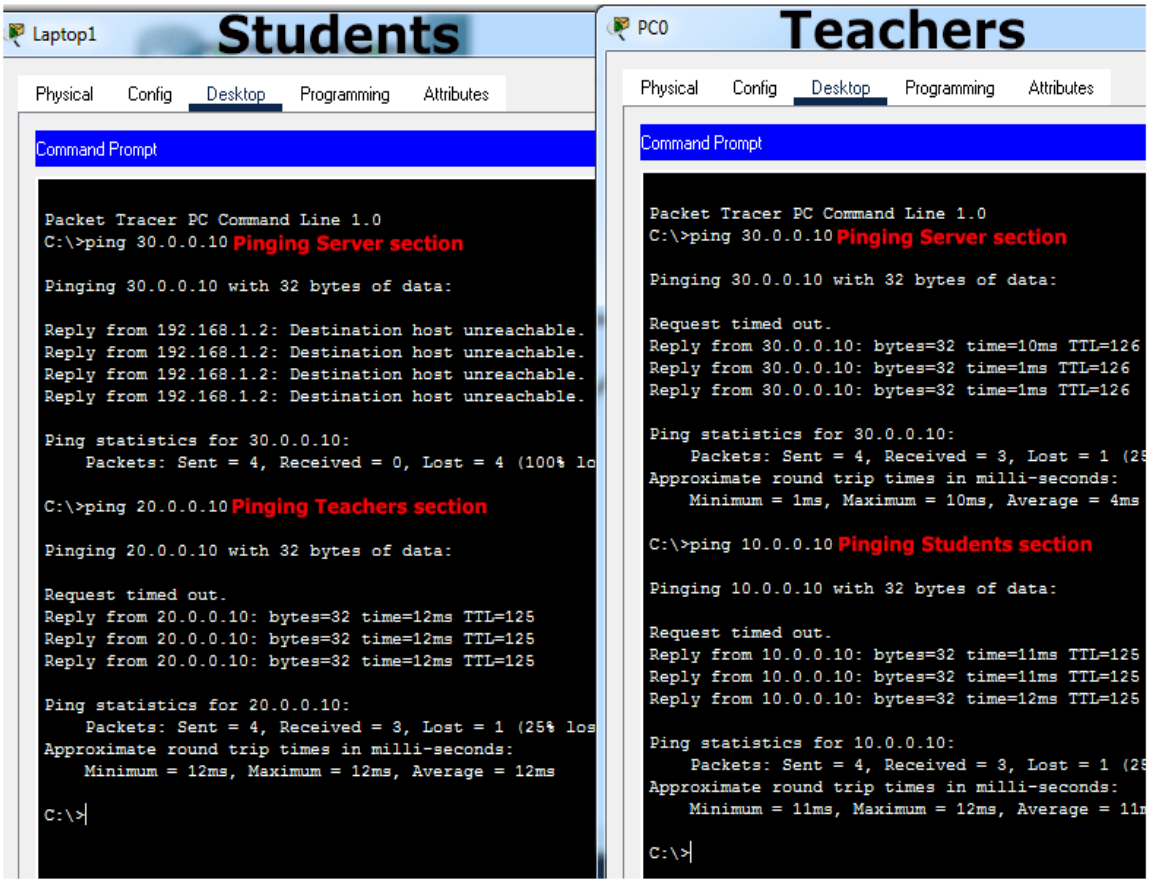

Fig-6: Verifying ACL

To modify or update a standard ACL statement, use the following steps.

- Use the 'show access-lists' command to view the sequence number of the statement.
- Enter standard ACL configuration mode
- Delete the existing statement with the 'no [*sequence number*]' command
- Insert the modified, updated, or the new statement with the sequence number of the old statement

Let's take an example. Suppose, instead of blocking the entire subnet we only want to block a single host (10.0.0.10/8) from the student's section. For this, access the CLI prompt of Router0 and run the following commands.

Router>
Router#show access-lists
Standard IP access list BlockStudents
10 deny 10.0.0.0 0.255.255.255
20 permit any
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip access-list standard BlockStudents
Router(config-std-nacl)#no 10
Router(config-std-nacl)#10 deny 10.0.0.10 0.0.0.0
Router(config-std-nacl)#exit
Router(config)#exit
Router#
Router#show access-lists

Standard IP access list BlockStudents
10 deny host 10.0.0.10
20 permit any
Router#

Let's understand the above commands.

First, we checked the sequence number of the statement that we had used to block the entire Students section. As we can in the above output, the sequence number of the statement is 10. After it, we entered the ACL configuration mode of the ACL. In ACL configuration mode, we deleted the current statement with the 'no *sequence_number_of_statement*' command. In the end, we inserted the new statement at the place of the existing statement.

Since the ACL is already active on the interface, the interface starts using the new statement as soon as it is added. To verify the change, send ping requests again from the blocked host and the allowed host. The following image shows this testing.

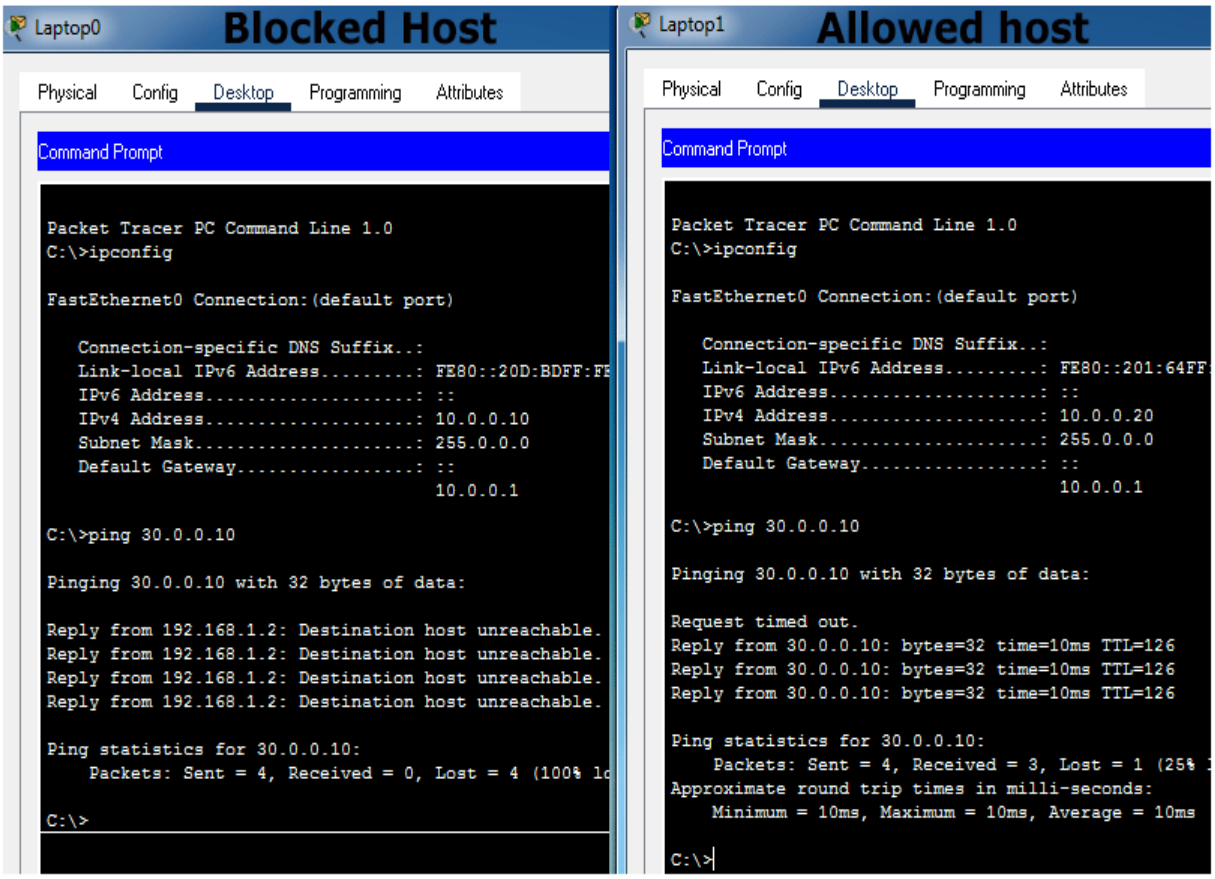

Fig-7: Verifying Modify ACL

6. Lab Exercise:

Create the given network Topology in figure 8. Apply IP given IP scheme which is shown in table II. Where xx are your student ID two digits.

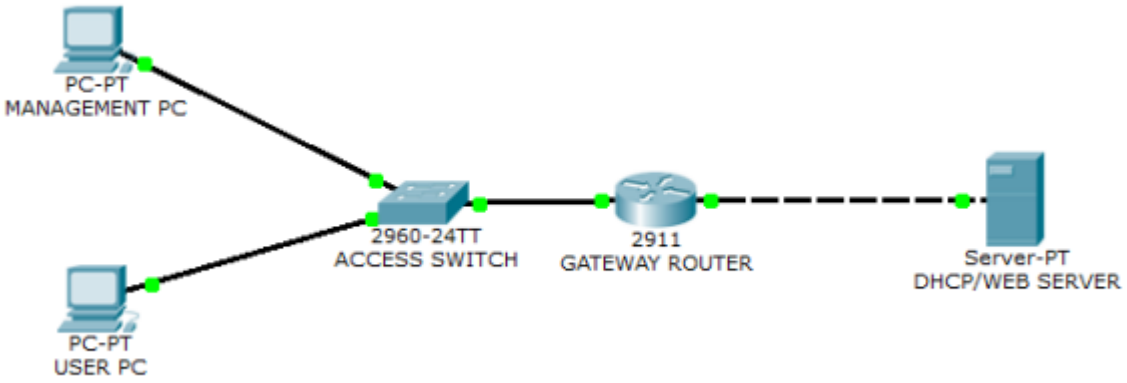

Fig-8: Network Topology for Task

Addressing Table			
Device	**IP Address**	**Subnet Mask**	**Default-Gateway**
Management PC	xx.1.0.1	255.255.255.0	xx.1.0.254
User PC	xx.1.0.2	255.255.255.0	xx.1.0.254
Gateway Router G0/0	xx.1.0.254	255.255.255.0	
Gateway Router G0/1	xx.2.0.254	255.255.255.0	
DHCP / WEB server	xx.2.0.1	255.255.255.0	xx.2.0.254

Table-II: Addressing scheme of above network topology

Q1) Configure the network and verify the connection between PCs & server.

Q2) Create a standard named ACL (such as TEL) to limit access of Telnet of router by any other devices only Management PC can access router Telnet.

Q3) Create an extended ACL to only limit the web traffic to pass and block other services by server.