Configure Standard Access C
Step Guide

This tutorial explains how to configure, view, edit, upd s
control. Learn how to create and manage a standard acce

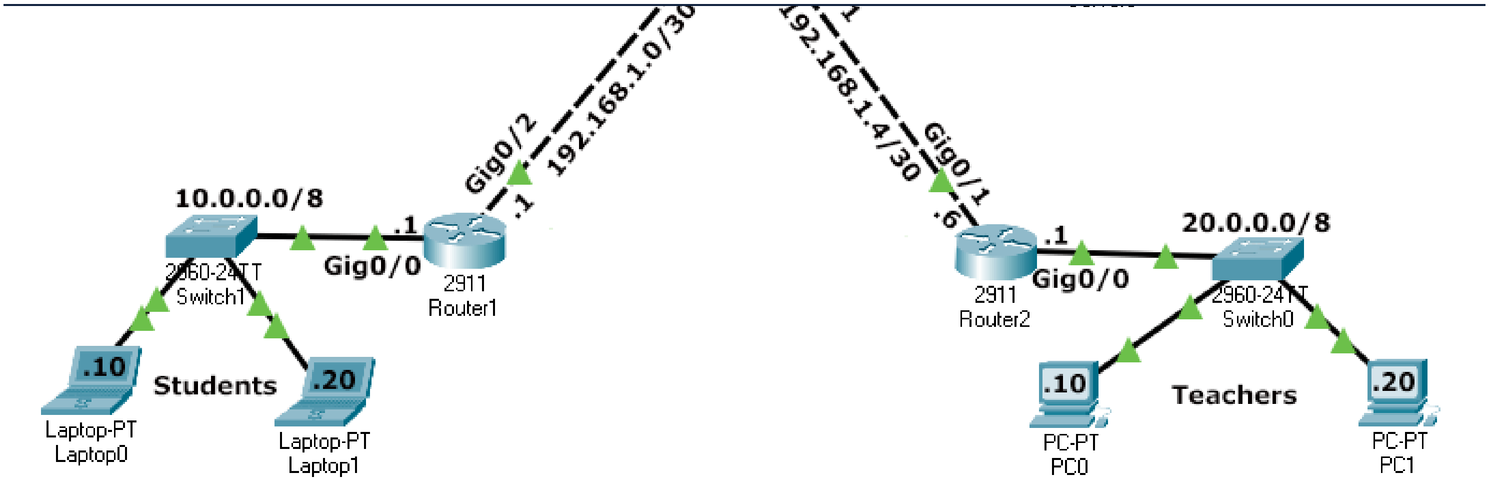
For this tutorial, I assume that you know what a standard o
create and implement a standard ACL. To learn access l e
previous parts of this tutorial.

This tutorial is the tenth part of the article **'Cisco Access**
parts of this article are the following.

Definition, purposes, benefits, and functions of ACL
Basic concepts and fundamentals of ACLs
How Access Lists work on Cisco routers
Types of access control lists explained
Wildcard masks in ACLs Explained
Rules and configuration guidelines for Cisco ACLs
Access Control List Explained with Examples
The ip access-list command options and arguments
Standard ACL Configuration Commands Explained
How to secure VTY access to the Router
Extended ACL Configuration Commands Explained
Configure Extended Access Control List Step by Step Guide
How to block ICMP Ping on Cisco Routers

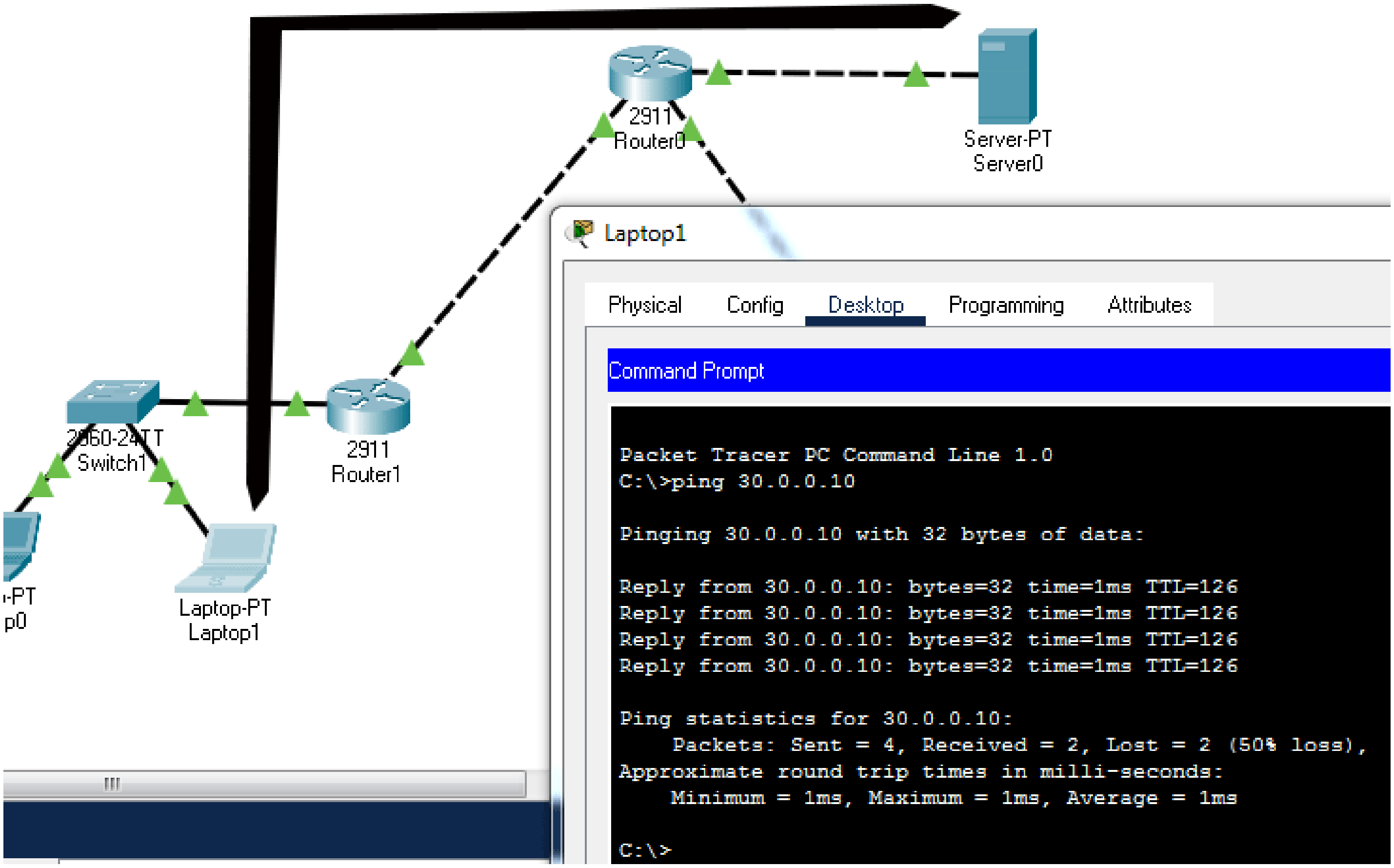
Setting up a practice lab

Create a packet tracer lab as shown in the following image.



Configure IP addresses as shown in the above image and enable RIPv2 protocol for routing and test connectivity between sections. To test connectivity between sections, you can use the **ping** command.

The following image shows how to use the **ping** command to test connectivity between **Laptop1** and **Server0**.



```
Packet Tracer PC Command Line 1.0
C:\>ping 30.0.0.10

Pinging 30.0.0.10 with 32 bytes of data:

Reply from 30.0.0.10: bytes=32 time=1ms TTL=126
Reply from 30.0.0.10: bytes=32 time=1ms TTL=126
Reply from 30.0.0.10: bytes=32 time=1ms TTL=126
Reply from 30.0.0.10: bytes=32 time=1ms TTL=126

Ping statistics for 30.0.0.10:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>
```

Objectives/requirements

Create and implement a standard access list that blocks the Students section from accessing the Server section.

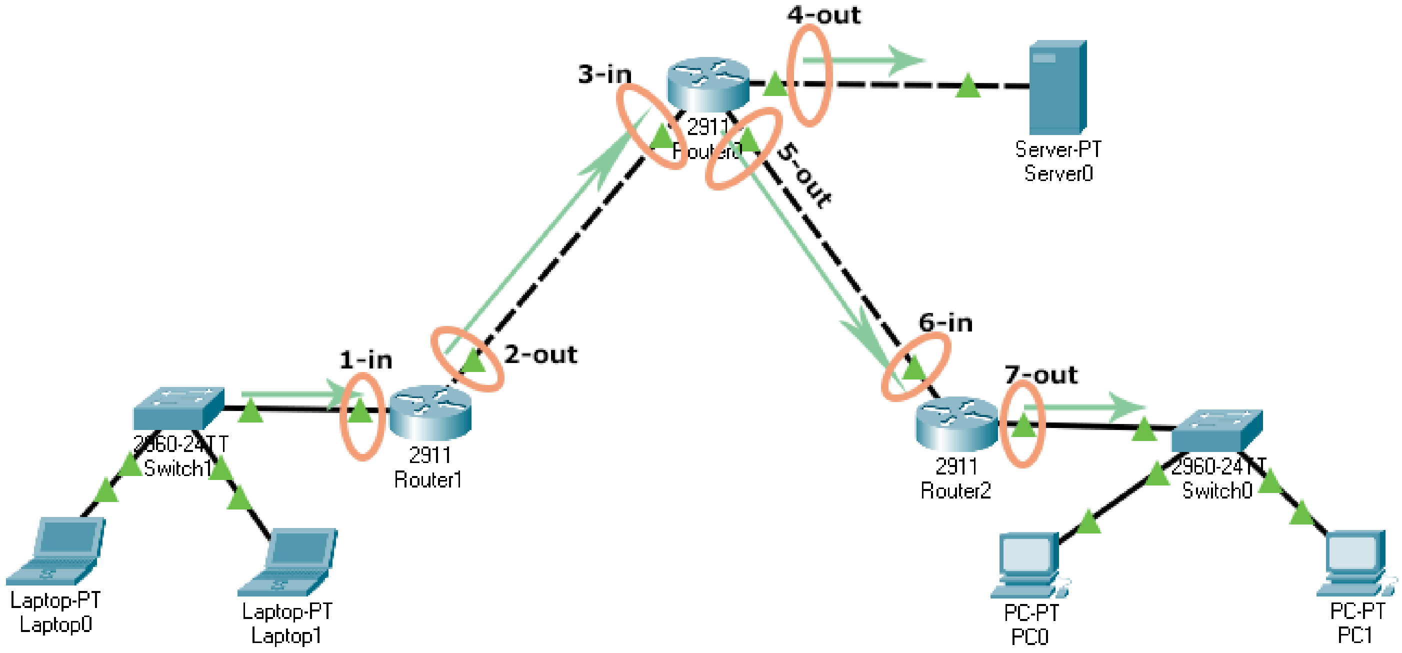
Understanding requirements

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.

Selecting location and direction for the ACL

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.



The following table lists the above locations and the effect of the ACL on each location.

Location	Interface	Direction	Effect
1	Router1's	In	The Students section will not be able to access the

3	Router0's Gig0/2	In	The Students section will not be able to access the Server and Teachers section.
4	**Router0's Gig0/0**	**Out**	**The Students 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 Students 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 Students 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 Students section will not be able to access the Teachers section but it will be able to access the Server section.

As you can see in the above table, the correct location for our ACL is Router0's Gig0/0 and the correct direction is the out.

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

```
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.

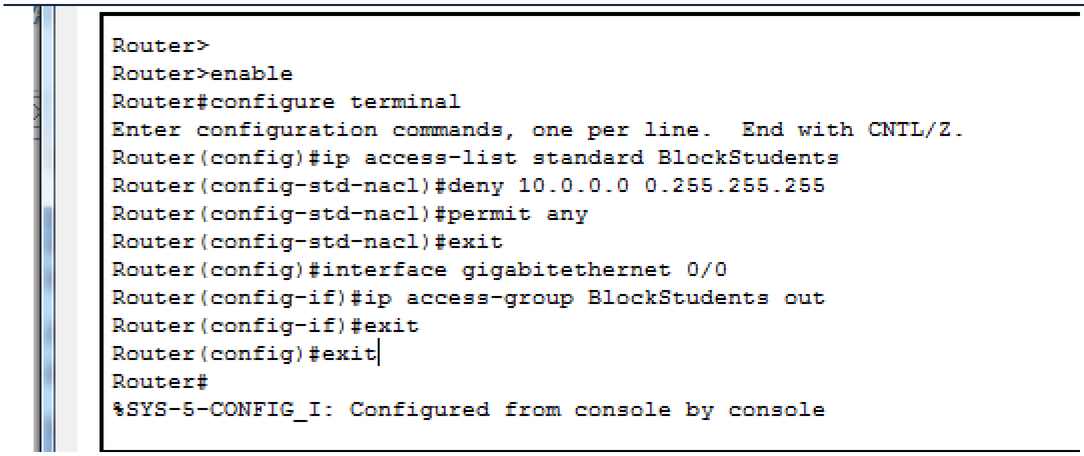
Creating a standard ACL

Access the command prompt of Router0 and run the following commands.

```
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.

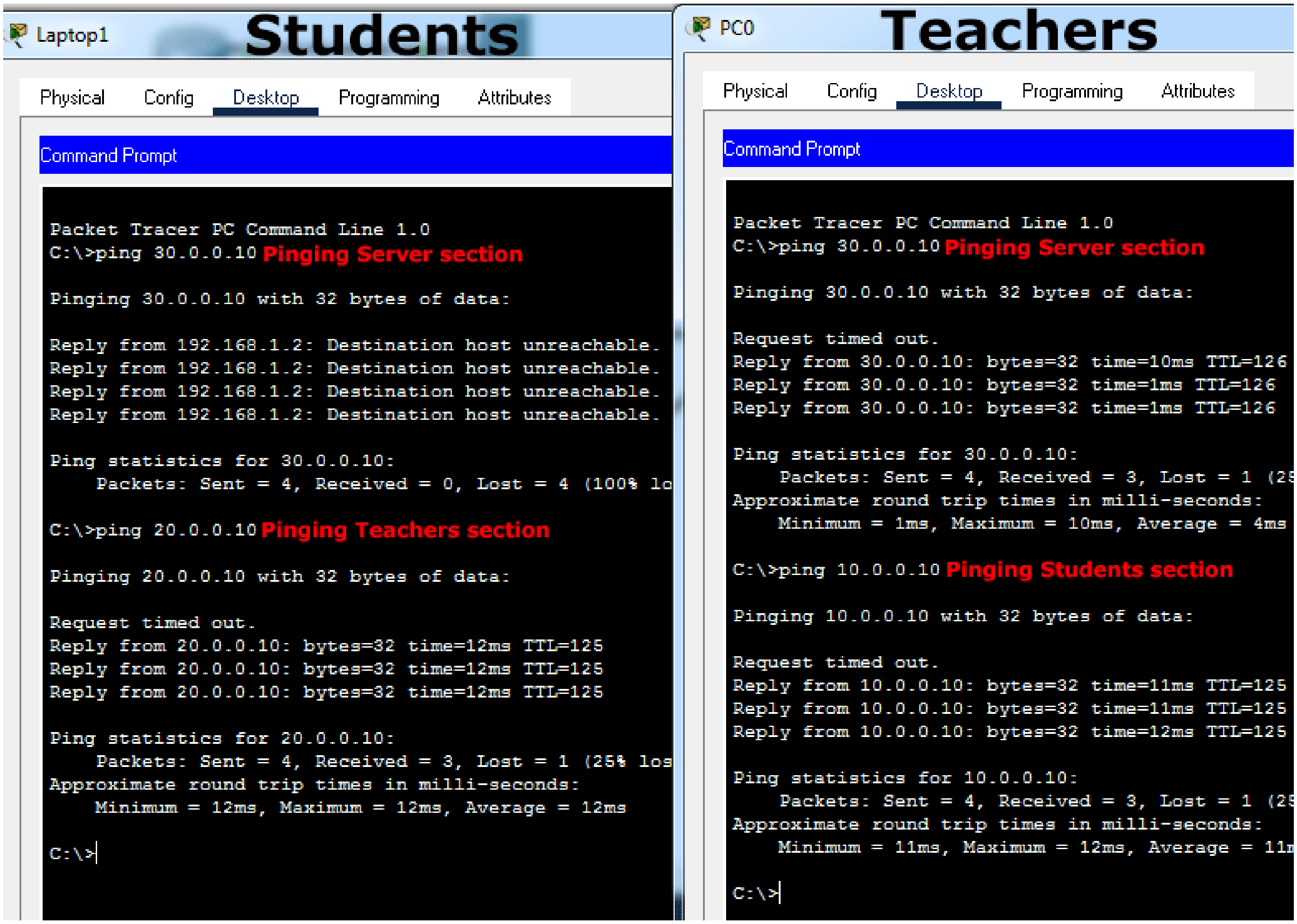
The following image shows how to run the above commands on the command prompt of the router.



```
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#
%SYS-5-CONFIG_I: Configured from console by console
```

Verifying

To verify the ACL, we can test connectivity between sections. The Students 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.



```
Packet Tracer PC Command Line 1.0
C:\>ping 30.0.0.10 Pinging Server section

Pinging 30.0.0.10 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.

Ping statistics for 30.0.0.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% lo

C:\>ping 20.0.0.10 Pinging Teachers section

Pinging 20.0.0.10 with 32 bytes of data:

Request timed out.
Reply from 20.0.0.10: bytes=32 time=12ms TTL=125
Reply from 20.0.0.10: bytes=32 time=12ms TTL=125
Reply from 20.0.0.10: bytes=32 time=12ms TTL=125

Ping statistics for 20.0.0.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% los
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 12ms, Average = 12ms

C:\>
```

```
Packet Tracer PC Command Line 1.0
C:\>ping 30.0.0.10 Pinging Server section

Pinging 30.0.0.10 with 32 bytes of data:

Request timed out.
Reply from 30.0.0.10: bytes=32 time=10ms TTL=126
Reply from 30.0.0.10: bytes=32 time=1ms TTL=126
Reply from 30.0.0.10: bytes=32 time=1ms TTL=126

Ping statistics for 30.0.0.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 10ms, Average = 4ms

C:\>ping 10.0.0.10 Pinging Students section

Pinging 10.0.0.10 with 32 bytes of data:

Request timed out.
Reply from 10.0.0.10: bytes=32 time=11ms TTL=125
Reply from 10.0.0.10: bytes=32 time=11ms TTL=125
Reply from 10.0.0.10: bytes=32 time=12ms TTL=125

Ping statistics for 10.0.0.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 12ms, Average = 11

C:\>
```

Modifying /updating a standard ACL statement

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

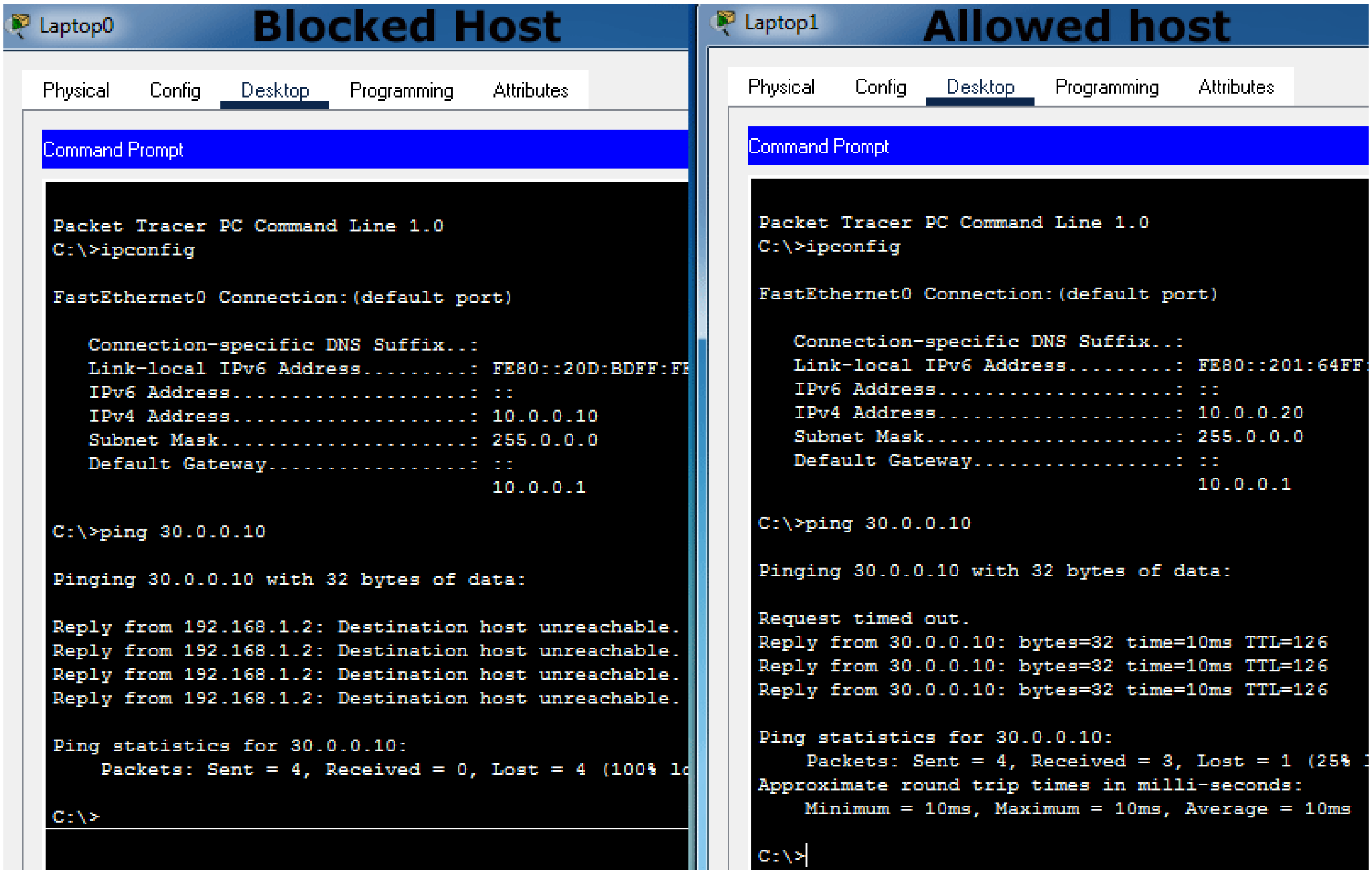
Insert the modified, updated, or the new statement with the sequence number of the old statement

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 Students 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 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.



```
Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::20D:BDFF:FE
   IPv6 Address....................: ::
   IPv4 Address....................: 10.0.0.10
   Subnet Mask.....................: 255.0.0.0
   Default Gateway.................: ::
                                     10.0.0.1

C:\>ping 30.0.0.10

Pinging 30.0.0.10 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.

Ping statistics for 30.0.0.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% lo

C:\>
```

```
Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::201:64FF:
   IPv6 Address....................: ::
   IPv4 Address....................: 10.0.0.20
   Subnet Mask.....................: 255.0.0.0
   Default Gateway.................: ::
                                     10.0.0.1

C:\>ping 30.0.0.10

Pinging 30.0.0.10 with 32 bytes of data:

Request timed out.
Reply from 30.0.0.10: bytes=32 time=10ms TTL=126
Reply from 30.0.0.10: bytes=32 time=10ms TTL=126
Reply from 30.0.0.10: bytes=32 time=10ms TTL=126

Ping statistics for 30.0.0.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% l
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 10ms, Average = 10ms

C:\>
```

Updated Packet Tracer Lab

The following link provides the updated packet tracer lab of this example.

Download updated Packet Tracer Lab with ACL Configuration

Deleting a standard ACL

To delete a standard ACL, use the following command in global configuration mode.

```
Router(config)no ip access-list standard ACL_#
```

Replace **ACL_#** with the ACL name or number.

The following command deletes the **BlockStudents** ACL.

```
Router(config)no ip access-list standard BlockStudents
```

That's all for this tutorial. In the next tutorial, we will learn how to use a standard access list to secure VTY lines on a router.

Step by Step Guide

Standard ACL Configuration Commands Explained

Extended ACL Configuration Commands Explained

About Privacy Policy Terms and Conditions