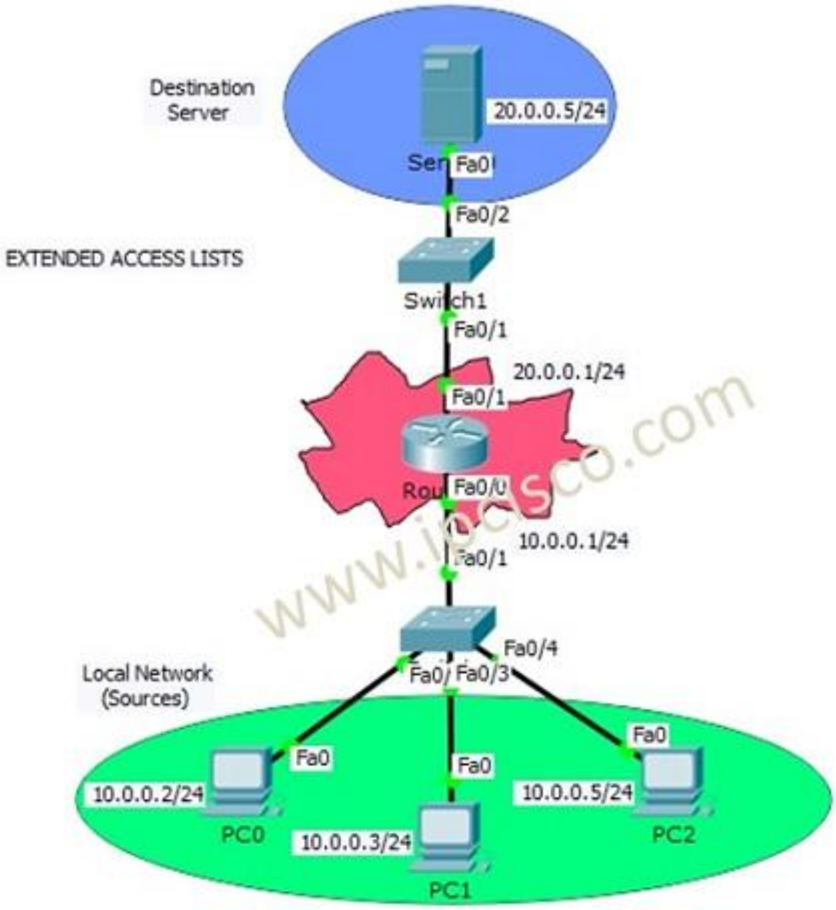
Assignment 3. Using a Network Simulator (e.g. packet tracer) Configure

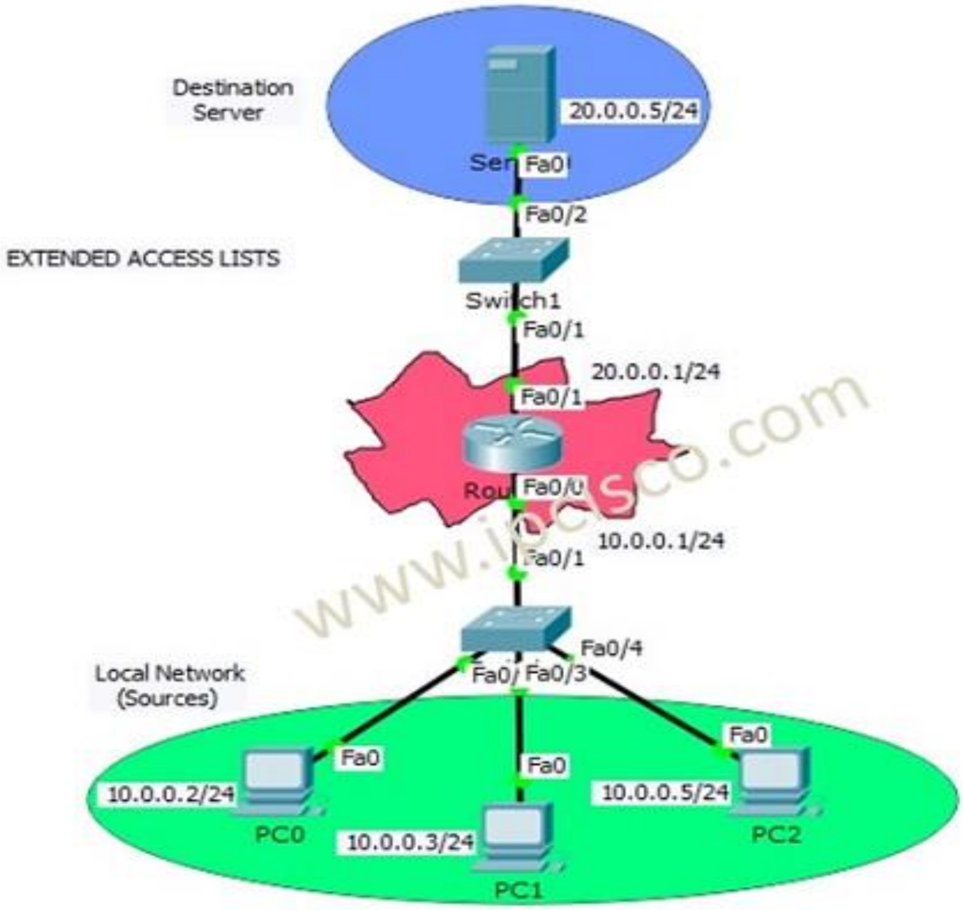
A router using router commands, Access Control lists – Standard & Extended.

Extended Access List Configuration With Packet Tracer



Extended Access Lists Configuration With Packet Tracer

In this lesson we will focus on **Extended Access Lists Configuration** with **Cisco Packet Tracer**. We will use the below topology for our packet tracer configuration.



You can **DOWNLOAD** the **Cisco Packet Tracer** example with **.pkt** format at the **End of This Lesson**.

Like **Standard ACL** configuration example, we will use one router, one destination server and 3 PCS in common. The switches in the topology will onlu used for port need.

Extended ACLs are a little complex if we compare with Standard ACLs. With **Extended ACLs**, we can restrict or allow specific things like **destination, protocol** or **port**.

In this Extended ACL example, we will **allow/deny ICMP protocol** through the server. As you know, ICMP is ping protocol. Here, PC0 and PC1 will be allowed and PC2 will be denied.

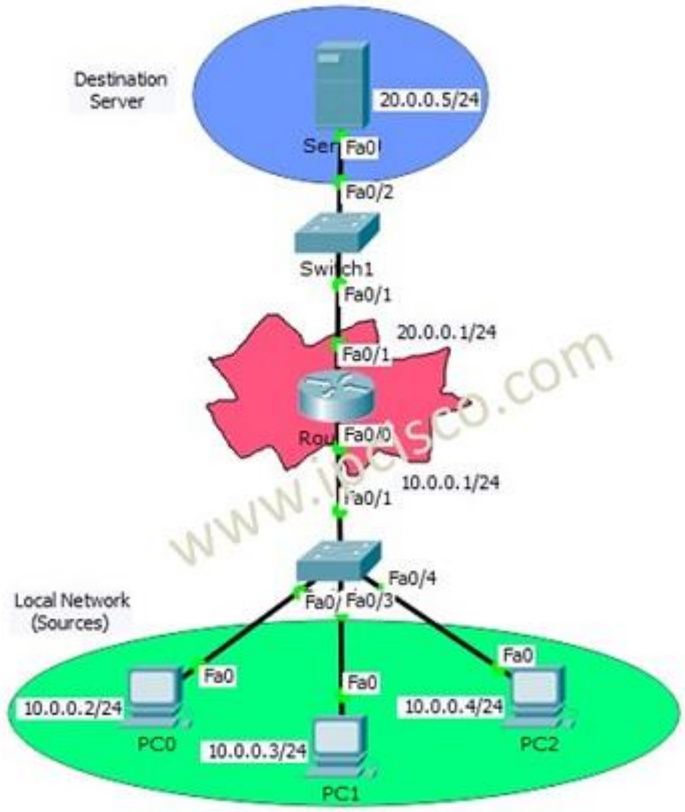
Extended Access-List Configuration

Let’s start to configure router for our Extended ACL.

For Extended ACLs, we can use **Extended Access-List Number** range **100 to 199**. Here, we will use 100.

```
Router # configure terminal

Router (config)# ip access-list extended 100
Router (config-ext-nacl)# permit  icmp  10.0.0.0  0.0.0.3 host 20.0.0.5

Router (config-ext-nacl)# deny  icmp host 10.0.0.5 host 20.0.0.5 host-unreachable

Router (config-ext-nacl)# end

Router # copy run start
```

Standard Access List Configuration With Packet Tracer



Standard Access List Configuration With Packet Tracer

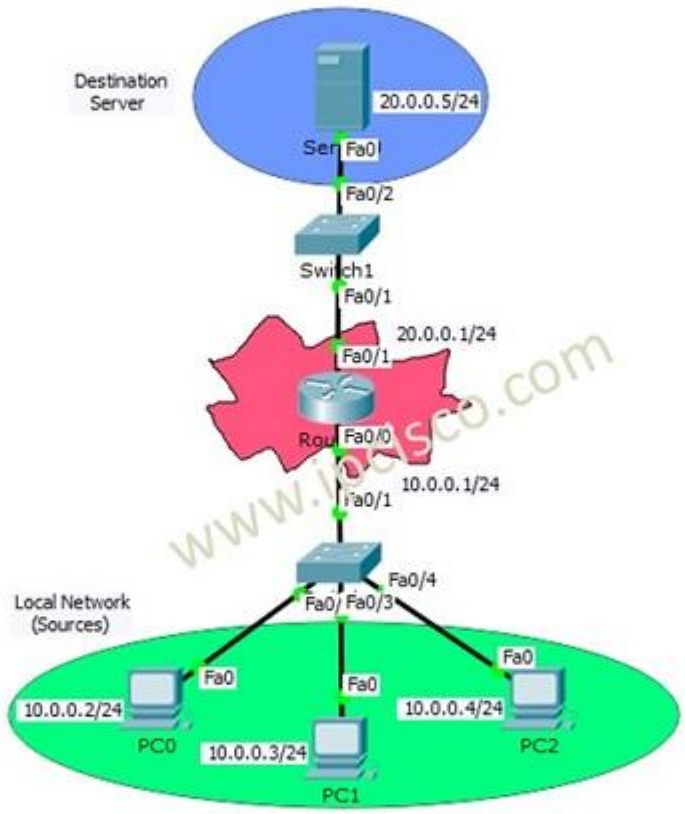
In this lsson we will see the Standard Access-List and how to configure **Standart Access-List** in Packet Tracer.
There are **three types Access Lists** in common. Thse access list types are :

– Standard Access List
– Extended Access List
– Named Access List

You can **DOWNLOAD** the **Cisco Packet Tracer** example with **.pkt** format at the **End of This Lesson**.

Standard Access-Lists are the simplest one. With Standard Access-List you can check only the source of the IP packets. On the other hand, with **Extended Access-Lists**, you can check source, destination, specific port and protocols. Lastly, with **Named Access-Lists**, you can use names instead of the numbers used in standard and extended ACLs. It do not have too much difference, but it is different with its named style.

In this lesson, we will focus on **Standart Access-List Configuration** with **Cisco Paket Tracer**. We will focus on the below topology.



Here, with our **Standard Access-List**, we will prohibit PC2 to access the server. But PC0 and PC1 can still access the server.

For our Standard Access-List, we can use the **ACL Number** 1 to 99. These numbers can be **100 to 199**, if you use extended ACLs.

Standard Access-List Configuration

Let’s start to write Standard Access-List. We will configure the Standard Access-List on router .

```
Router # configure terminal

Router (config)# ip access-list standard 1

Router (config-std-nacl)# permit  10.0.0.2  0.0.0.0
Router (config-std-nacl)# permit  10.0.0.3  0.0.0.0
```

With this ACL configuration that we have written, we permit PC0 and PC1 to access the server. At the end of ACLs, there is an “**Implicit Deny**”. These Implicit Deny, prohibits the other IP addresses. Because of the fact that we did not, allow PC2’s IP address, it is autoamtically denied and can not access the server.

Here, there is no need to write but to show how to write deny, I will write the deny command also. As Is aid before, for this scenario, it is not necesary. But, you can write.

```
Router (config-std-nacl)# deny  10.0.0.4  0.0.0.0

Router (config-std-nacl)# end

Router #  copy run start
```