Dynamic NAT Configuration with Packet Tracer

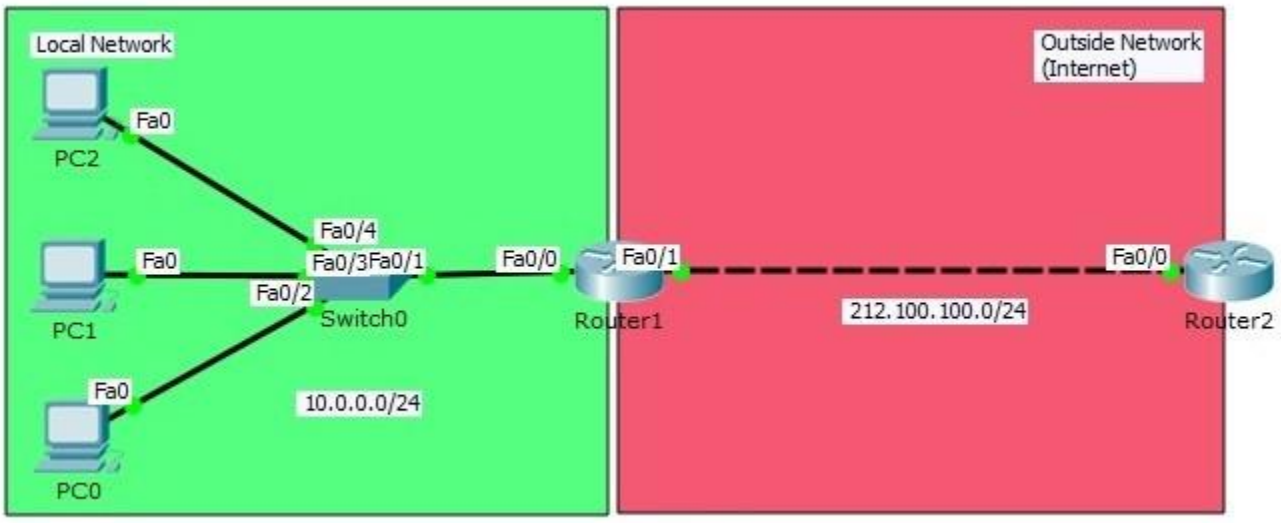


Table of Contents

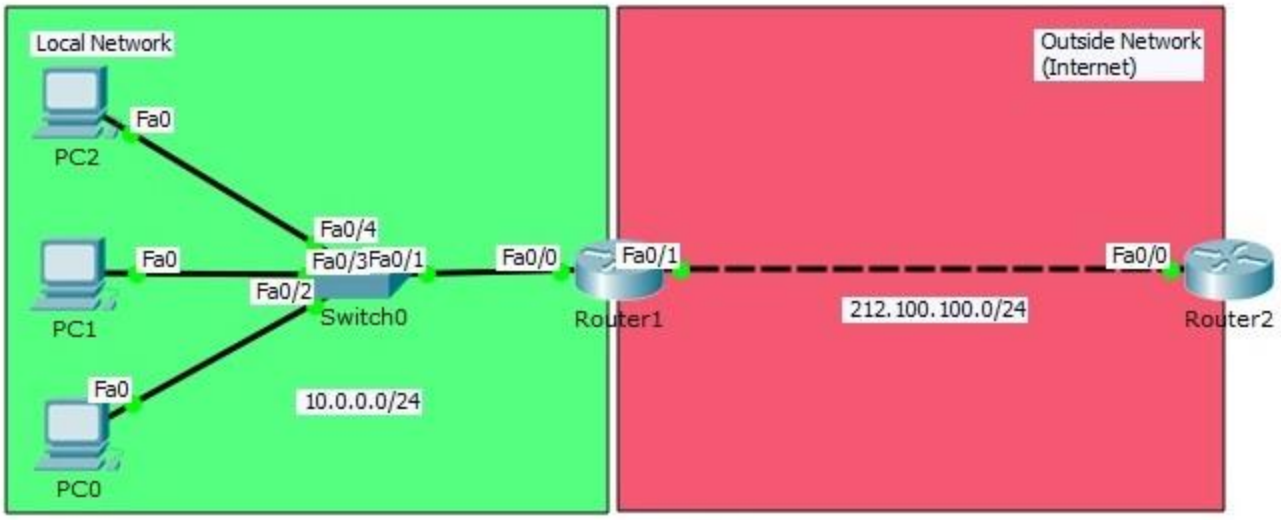
Packet Tracer Dynamic NAT Configuration Example

Before this article, we have talked about **Static NAT configuration**. Here, we will talk about another **types of NAT**, **Dynamic NAT** configuration on Packet Tracer. As in Static NAT, in the Dynamic NAT configuration, the interfaces must be identified as inside and outside again. Then we will define a Dynamic Address Pool on the NAT router. The ip address will be choosen in this pool to assign as source ip address.

We will use **Dynamic NAT topology** below for our **Dynamic NAT Configuration example**. And we will use Cisco Packet Tracer as a network simulation program.

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

You can also **DOWNLOAD** all the **Packet Tracer** examples with **.pkt** format in **Packet Tracer Labs** section.



Dynamic NAT (Network Address Translation) Configuration Topology

In our Dynamic NAT configuration topology on Packet Tracer, we will have two networks again, one local and one outside network. In local network, we have three PCs and we will provide internet access to these PCs. Our Dynamic NAT configuration topology on Packet Tracer will be a small simulation of real world office Internet access.

Interface IP Configurations

Firstly, before **Dynamic NAT configuration**, we will prepare our network with our IP configurations on PCS and routers. We will provide full connectivity end to end before starting our NAT Config.

Our PCs on Packet Tracer will be configured with below IP addresses.

PC0 : 10.0.0.2 255.255.255.0 GW:10.0.0.1
PC1 : 10.0.0.3 255.255.255.0 GW:10.0.0.1
PC2 : 10.0.0.4 255.255.255.0 GW:10.0.0.1

```
Router1(config)# interface FastEthernet0/0

Router1(config-if)# ip address 10.0.0.1 255.255.255.0

Router1(config-if)# no shutdown

Router1(config-if)# exit

Router1(config)# interface FastEthernet0/1

Router1(config-if)# ip address 212.100.100.2 255.255.255.0

Router1(config-if)# no shutdown

Router1(config-if)# exit

Router2(config)# interface FastEthernet0/0

Router2(config-if)# ip address 212.100.100.1 255.255.255.0

Router2(config-if)# no shutdown

Router2(config-if)# exit

Router2(config)# ip default-gateway 212.100.100.2
```

Firstly let's check the ping packet's source address when we are pinging from PC 1 to Router2. A2 you can seelowe b, the source address will be the PC 0 's IP address. To see the packet you must enable NAT debug mode on Router2 by **"debug ip nat"** command.Check the below screenshots.

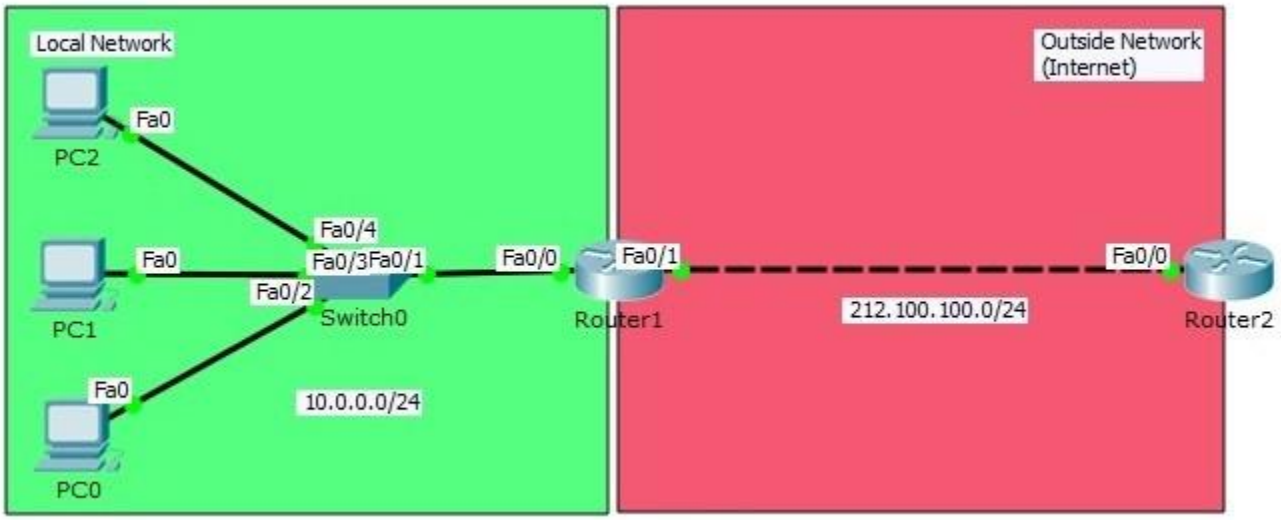
```
PC0> ping 212.100.100.1

Pinging 212.100.100.1 with 32 bytes of data:



Reply from 212.100.100.1: bytes=32 time=13ms TTL=254

Reply from 212.100.100.1: bytes=32 time=1ms TTL=254
```

```
Reply from 212.100.100.1: bytes=32 time=1ms TTL=254

Reply from 212.100.100.1: bytes=32 time=2ms TTL=254



Ping statistics for 212.100.100.1:

    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

    Minimum = 1ms, Maximum = 13ms, Average = 4ms
```

```
Router2# debug ip nat

IP NAT debugging is on

Router2#

ICMP: echo reply sent, src 212.100.100.1, dst 10.0.0.2



ICMP: echo reply sent, src 212.100.100.1, dst 10.0.0.2



ICMP: echo reply sent, src 212.100.100.1, dst 10.0.0.2



ICMP: echo reply sent, src 212.100.100.1, dst 10.0.0.2
```

Now let’s do the Dynamic NAT configuration on Router1.

PAT Configuration with Packet Tracer



Packet Tracer PAT Configuration Example

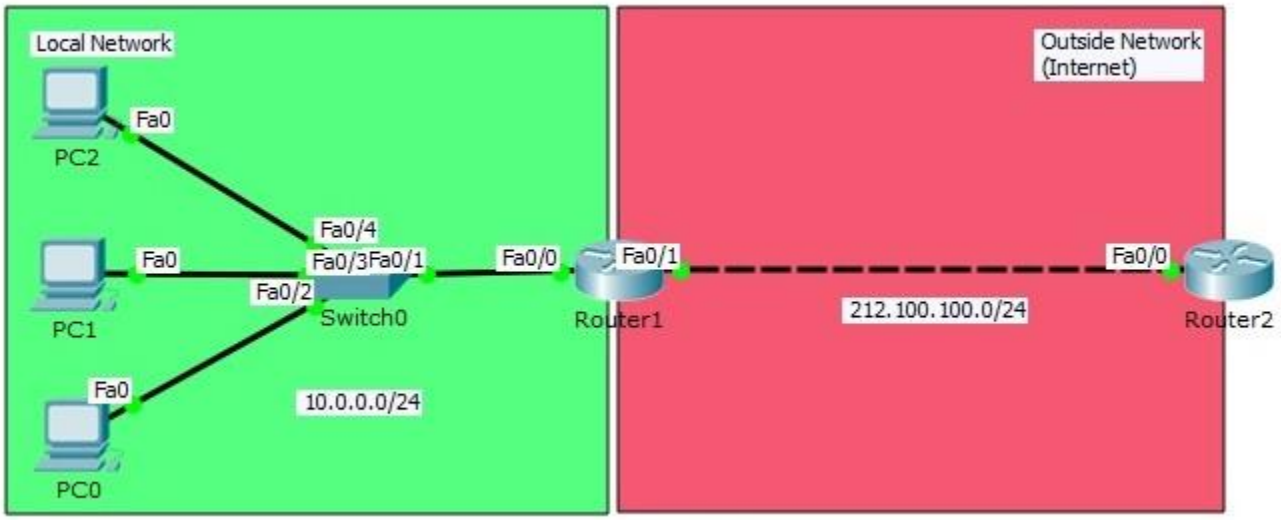
In some cases there can be hundreds of inside local addresses and at the same time your Global IP Addresses can be limited. At this time you can use **PAT** instead of Static and Dynamic **NAT** translation. Here, we will learn **PAT Configuration** with Cisco Packet tracer.

Here, with **PAT(Port Address Translation)**, we translate each PC to a unique port number of a single public address.

You can **DOWNLOAD Packet Tracer** example with **.pkt** format **HERE**.

You can also **DOWNLOAD** all the **Packet Tracer** examples with **.pkt** format in **Packet Tracer Labs** section.

Firstly we identify the interfaces as inside and outside as before static and dynamic **NAT configurations**. Here, we will use the same topology like **Dynamic NAT configuration** article. Because, for **PAT configuration**, we need a small change on the configuration.



PAT (Port Address Translation) Configuration Topology

Here, we will start with the IP address configurations firstly.

Our PCs on Packet Tracer will be configured with below IP addresses.

PC0 : 10.0.0.2 255.255.255.0 GW:10.0.0.1
PC1 : 10.0.0.3 255.255.255.0 GW:10.0.0.1
PC2 : 10.0.0.4 255.255.255.0 GW:10.0.0.1

```
Router1(config)# interface FastEthernet0/0

Router1(config-if)# ip address 10.0.0.1 255.255.255.0

Router1(config-if)# no shutdown

Router1(config-if)# exit

Router1(config)# interface FastEthernet0/1

Router1(config-if)# ip address 212.100.100.2 255.255.255.0

Router1(config-if)# no shutdown

Router1(config-if)# exit
```

```
Router2(config)# interface FastEthernet0/0

Router2(config-if)# ip address 212.100.100.1 255.255.255.0

Router2(config-if)# no shutdown

Router2(config-if)# exit

Router2(config)# ip default-gateway 212.100.100.2

Router2(config)# no ip routing
```

Now, let's do the classical NAT configuration and plus PAT configuration (overload).

```
Router1 (config)# int e0/0

Router1 (config-if)# ip nat inside

Router1 (config-if)# exit

Router1 (config)# int s0/0

Router1 (config-if)# ip nat outside

Router1 (config-if)# exit
```

After that we will use the below commands for PAT configuration:

```
Router1 (config)# access-list 10 permit 10.0.0.0 0.0.0.255

Router1 (config)# ip nat pool IPCISCO 50.50.50.80 50.50.50.80 netmask
255.255.255.0

Router1 (config)# ip nat inside source list 10 pool IPCISCO overload
```

Here, any match interface with access-list 10, will be translated with overload to the serial interface IP address. The secret key word of PAT configuration is "**overload**".

Let's check the nat table on Router1.

```
Router1# show ip nat translations

Pro  Inside global     Inside local       Outside local      Outside
global

icmp 50.50.50.80:1     10.0.0.4:1         212.100.100.1:1
212.100.100.1:1

icmp 50.50.50.80:2     10.0.0.4:2         212.100.100.1:2
212.100.100.1:2

icmp 50.50.50.80:3     10.0.0.4:3         212.100.100.1:3
212.100.100.1:3

icmp 50.50.50.80:4     10.0.0.4:4         212.100.100.1:4
212.100.100.1:4
```

Static NAT Configuration with Packet Tracer

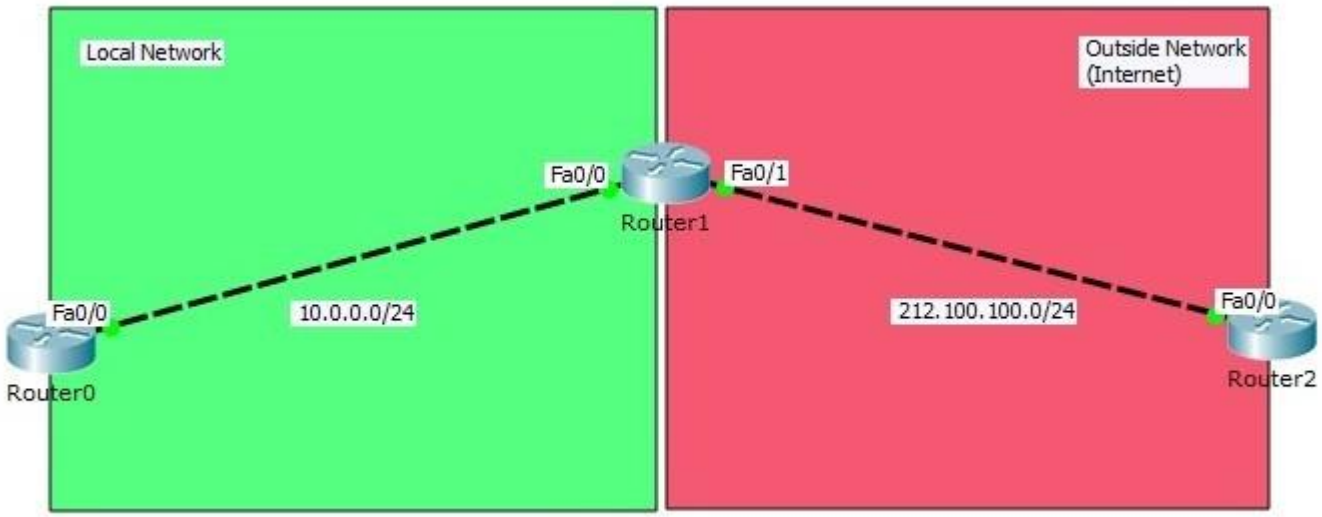


Table of Contents

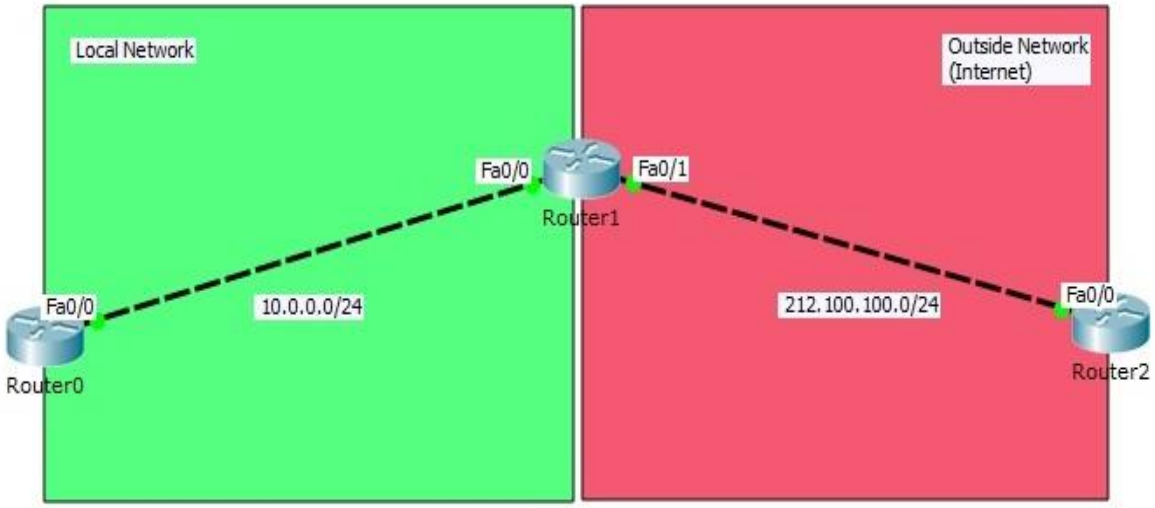
Packet Tracer Static NAT Configuration Example

In this example we will configure one of the **NAT types**, **Static NAT (Network Address Translation)** on Packet Tracer. For our Static NAT configuration, we will use the topology below.

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

You can also **DOWNLOAD** all the **Packet Tracer** examples with **.pkt** format in **Packet Tracer Labs** section.

In this NAT topology, we will configure Static NAT on Router1. We wwill use Router0 and Router2 as host devices(For example like PCS).



Interface Configurations

Static NAT (Network Address Translation) Configuration Topology

Here firstly we will configure interface IP addresses on three of these routers. And then we will write static route from both ends to others. For IP connectivity, lastly we will ping from one end to other end. After this verification, our Static NAT configuration topology is ready for our NAT configuration.
In Router0 we will use private block IP address, because we will think that this area is our local network. In Router2, we will use public block IP addresses. Router2 will be like any place on internet.

Inside Local : 10.0.0.1
Inside Global : 212.100.100.10

Outside Local : 212.100.100.1
Outside Global : 212.100.100.1

```
Router0(config)# interface FastEthernet0/0

Router0(config-if)# ip address 10.0.0.1 255.255.255.0

Router0(config-if)# no shutdown

Router0(config-if)# end

Router0# copy running-config startup-config
```

```
Router1(config)# interface FastEthernet0/0

Router1(config-if)# ip address 10.0.0.2 255.255.255.0

Router1(config-if)# no shutdown

Router1(config-if)# exit

Router1(config)# interface FastEthernet0/1

Router1(config-if)# ip address 212.100.100.2 255.255.255.0

Router1(config-if)# no shutdown

Router1(config-if)# end

Router1# copy running-config startup-config
```

```
Router2(config)# interface FastEthernet0/0
```

```
Router2(config-if)# ip address 212.100.100.1 255.255.255.0

Router2(config-if)# no shutdown

Router2(config-if)# end

Router2# copy running-config startup-config
```

We will also set "**no ip routing**" on host devices (router0 and router2) and configure the default gateway address of host devices.

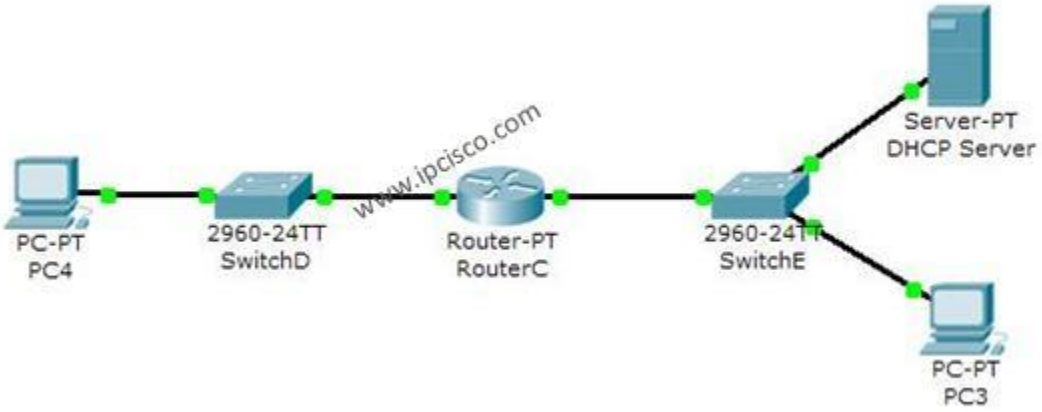
```
Router0(config)# no ip routing

Router0(config)# ip default-gateway 10.0.0.2
```

```
Router2(config)# no ip routing

Router2(config)# ip default-gateway 212.100.100.2
```

After IP connectivity, let's check the packets situation by openning debug with "**debug ip icmp**" command. Till now, we did not configure any NAT on Packet Tracer. We will only see the packets source and destintion before Static NAT.

You can also **DOWNLOAD** all the **Packet Tracer** examples with **.pkt** format in **Packet Tracer Labs** section.

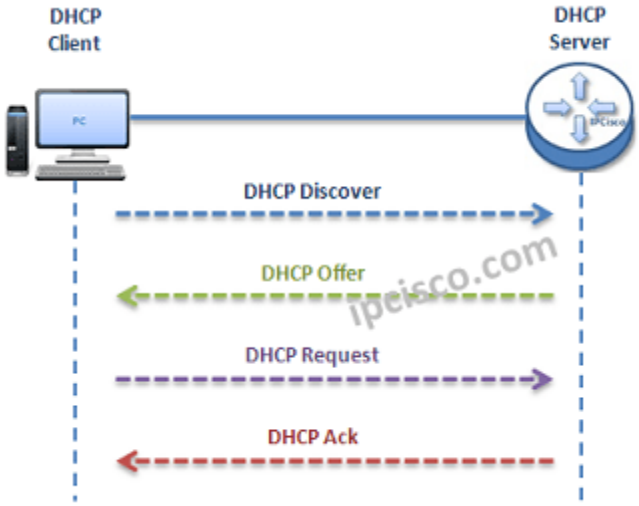
Router DHCP Configuration with Packet Tracer



In this **DHCP Cisco Packet Tracer** router example, we will focus on **DHCP Configuration in Cisco Packet Tracer**. In other words, we will see how to configure a **DHCP Server with Packet Tracer Router**. Before start up I want to give some basic information about **DHCP**.

As you know DHCP uses **UDP 67** and **UDP 68** ports. It has a messaging system for the communication between **DHCP Server** and **DHCP Client**. These messaging system's **messages** and their **types** are mentined below:

- **DHCP Discover (broadcast)**
- **DHCP Offer(broadcast)**
- **DHCP Request (broadcast)**
- **DHCP Ack (broadcast)**
- **DHCP Nak (unicast)**
- **DHCP Release (unicast)**
- **DHCP Decline (unicast)**
- **DHCP Inform (unicast)**



DHCP Messages

You can Reach **All Cisco Packet Tracer Labs** and **DOWNLOAD** the **Packet Tracer Examples** with **.pkt** format.

You can **DOWNLOAD** this lessons **Packet Tracer Example** with **.pkt** format **HERE.**

---

1. Firstly, a client sends a broadcast **"DHCP Discovery"** message that mentions that it need an ip address.
2. Then, the **DHCP servers** reply with configuration offers to the client by **"DHCP Offer"** unicast message
3. After that **DHCP client** sends a broadcast **"DHCP Request"** message to the network with the **"Transaction ID"** of the first **DHCP Server** that send **Offer**. The other **servers** understand that **client** wants to use the **server** that has the related **"Transaction ID"**.
4. Lastly, the **Server** sends a unicast **"Acknowledgement"** message to the **client** that mentions the ip assignment is successfully done or it send a refuse messaged named "**DHCP-NACK**".

To configure a Packet Tracer Router 's **DHCP**, we must follow some basic steps. For this configuration the important point is broadcast domains. If we have only one broadcast domain in our topology, our work is simpler, else we must get help from **"ip-helper address"** command.

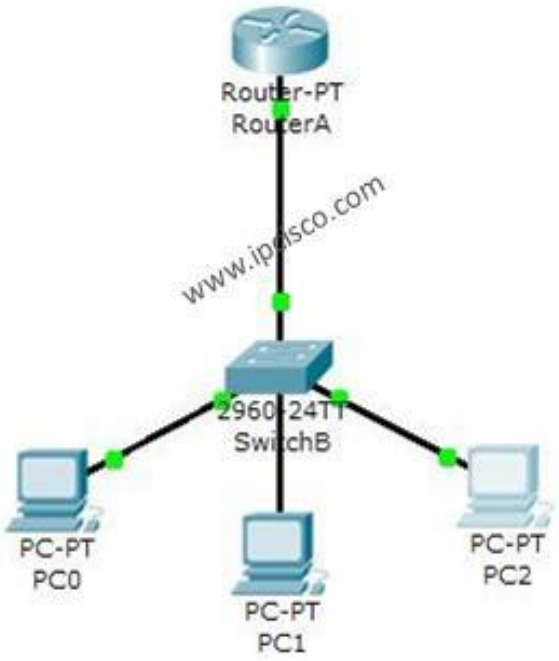
What is **ip helper address** command? **Ip helper address command** is the command that helps us to convince the router and make it pass the broadcast packets.

Now, let's go to our two different configuration topology and see how to configure a **server** in packet tracer for DHCP, **how to configure a DHCP Server in packet tracer**.

Table of Contents

DHCP Packet Tracer Config For One Broadcast Domain

Our one broadcast domain topology is like below. There is a router that will carry our **DHCP server** role beside its routing functionalities. And there is a switch for PCs.



DHCP Example Topology (One Broadcast Domain)

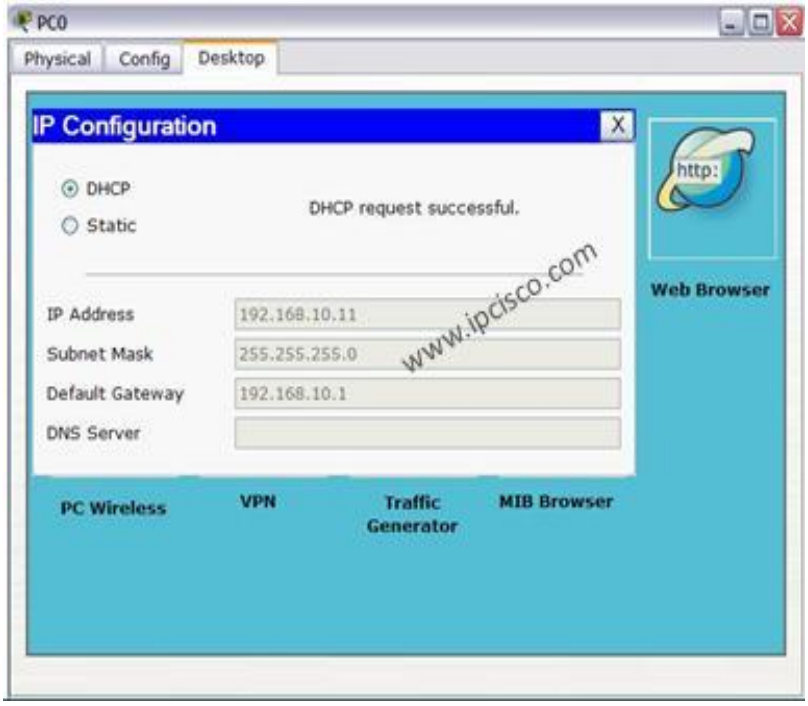
Firstly, let's see **How to Configure a DHCP Server** on a Packet Tracer Router for **One Broadcast Domain**. For this first case of our **DHCP Cisco packet tracer example**, the **One Broadcast Domain** topology that we will use, is like below. There is a router that will carry out **Server** role beside its routing functionalities. And there is a switch for PCs.

On routerA, firstly we will give an ip address to the router interface that is connected to the switch.Secondly that we will create a **DHCP pool** named IPD. In this pool we will mention ip addresses that will be given to the **DHCP clients**. After that we will assign the router's interface address as a default-router address for clients. And in the last part, we will exclude some addresses with "**ip dhcp excluded address**" command, that we don't want to use during this dynamic ip assignments. With "**ip dhcp excluded address**" command, the mentined addresses will not used in the pool.

```
RouterA# config terminal

RouterA(config)# interface fastEthernet 1/0

RouterA(config-if)# ip address 192.168.10.1 255.255.255.0

RouterA(config-if)# no shut



%LINK-5-CHANGED: Interface FastEthernet1/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed
state to up<
```

```
RouterA(config-if)# exit

RouterA(config)# ip dhcp pool IPD

RouterA(dhcp-config)# network 192.168.10.0 255.255.255.0

RouterA(dhcp-config)# default-router 192.168.10.1

RouterA(dhcp-config)# exit

RouterA(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.10

RouterA(config)# ip dhcp excluded-address 192.168.10.12 192.168.10.14
```

After this configuration, when we check the ip address of PC0, we will see the ip address **192.168.10.11** . Because it is the first available address in **DHCP pool**.

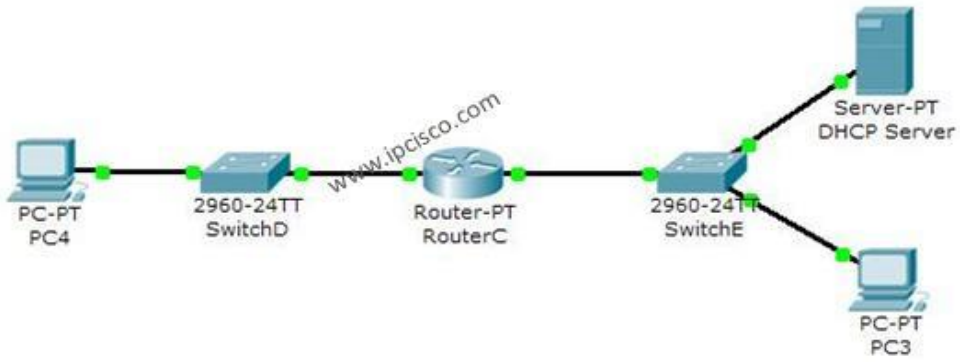


We can also check the pool information with Cisco "**show ip dhcp pool**" command.

Packet Tracer DHCP Config For Multiple Broadcast Domains

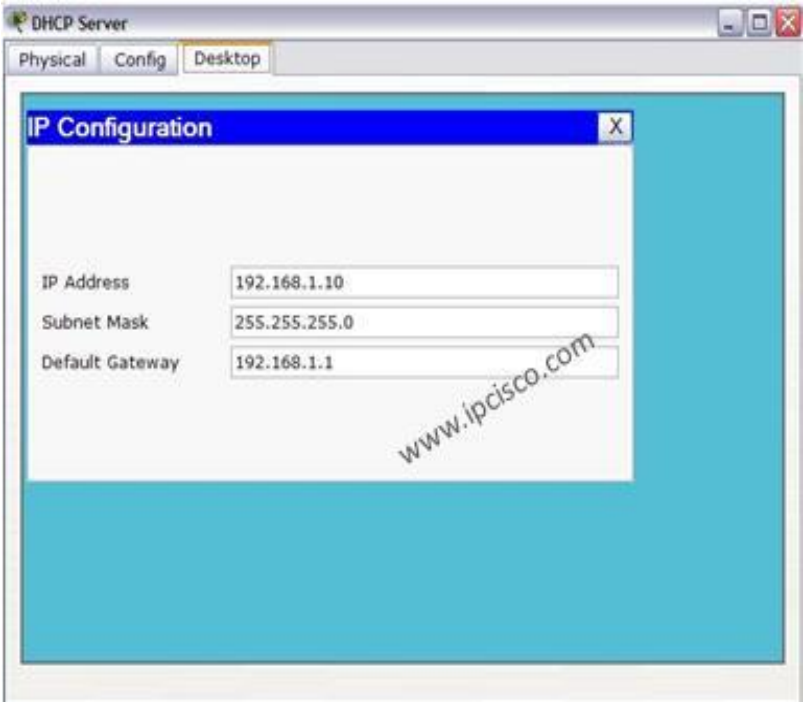
Our second case is **how to enable DHCP on router** for **multiple broadcast domains**. In our second Cisco packet tracer example, we will use ip helper, cisco command "**ip helper-address**". So, what is **ip helper address?**

Many **CCNAs** learn that routers do not pass broadcasts. But progress in **CCIE**, network engineers learn that it is not true. Because you can pass broadcast traffic for many protocols as DHCP by "**ip-helper address**" command. Here we will refer only the broadcast of **DHCP requests**. We can use a router as a **DHCP Server** again, but I use a separate DHCP Server instead of router in this topology.

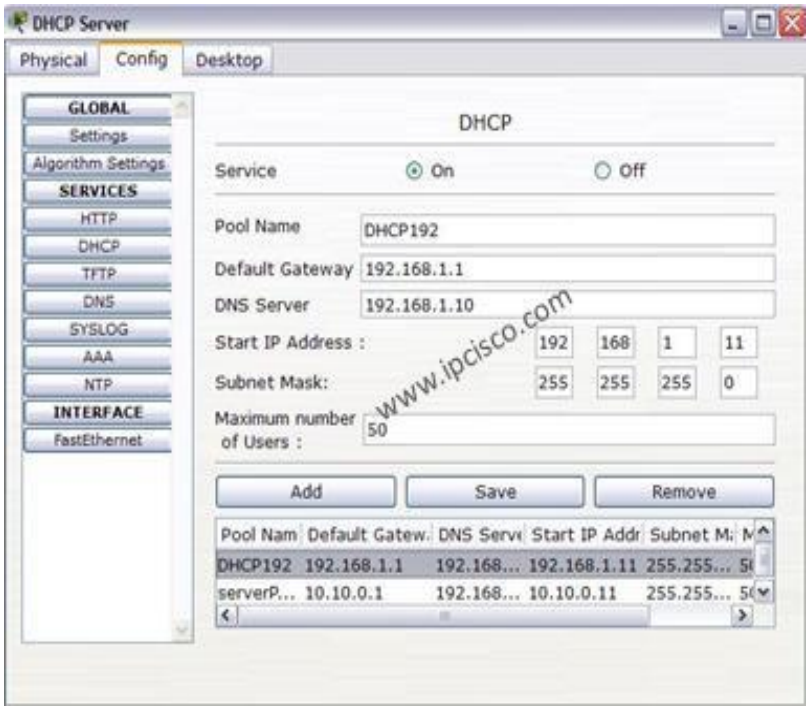


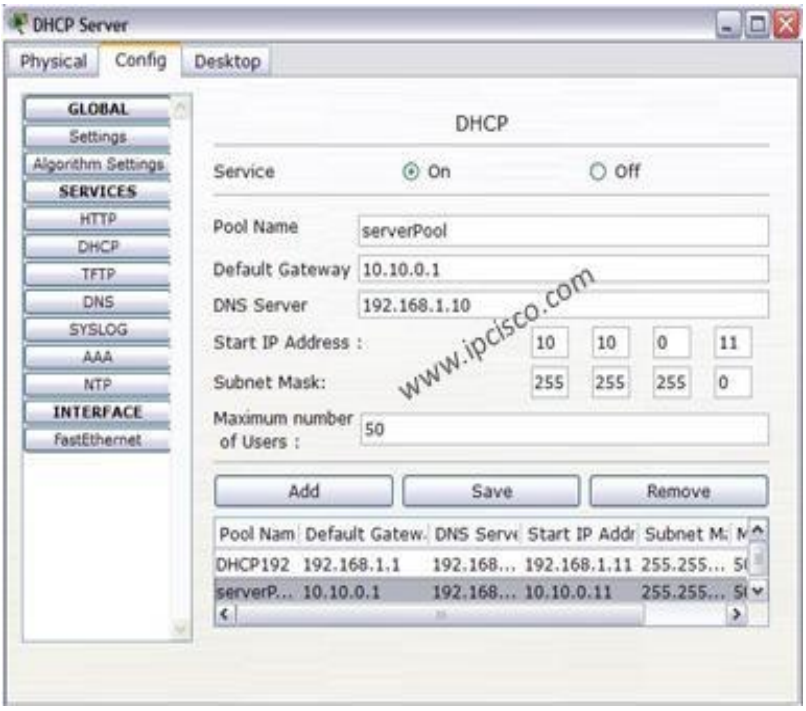
DHCP Example Topology (Multiple Broadcast Domains)

In the first place we will configure the **DHCP Server** for its **DHCP pools** and its ip configuration. The ip address is 192.168.1.10 and the default gateway will be the routers interface's ip address that is face to DHCP server.



For the subnets 192.168.1.0 and 10.10.0.0 there must be two **DHCP pool**.The below screenshot is showing how these assignments will be done in **DHCP Server**.





In the Packet Tracer router the following configuration will be done for two different subnet **DHCP** achivement:

```
RouterC # config terminal

RouterC(config)# interface fa0/0

RouterC(config-if)# ip address 10.10.0.1 255.255.255.0

RouterC(config-if)# ip helper-address 192.168.1.10

RouterC(config-if)# no shutdown

RouterC(config-if)# exit

RouterC(config)# interface fa1/0

RouterC(config-if)# ip address 192.168.1.1 255.255.255.0

RouterC(config-if)# ip helper-address 192.168.1.10

RouterC(config-if)# no shutdown
```

```
RouterC(config-if)# end

RouterC# copy run start
```

After this configuration, we can try **dynamic ip assignment** on PC by selecting the **dynamic option** on ip configuration screen like below.

Extended Access List Configuration With Packet Tracer

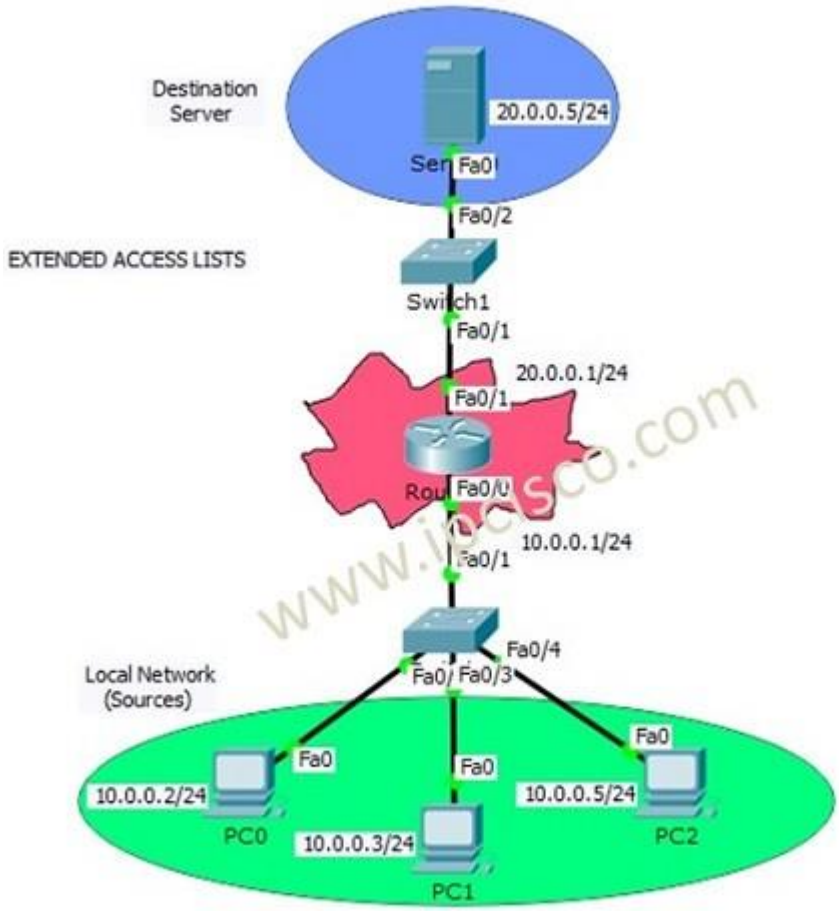
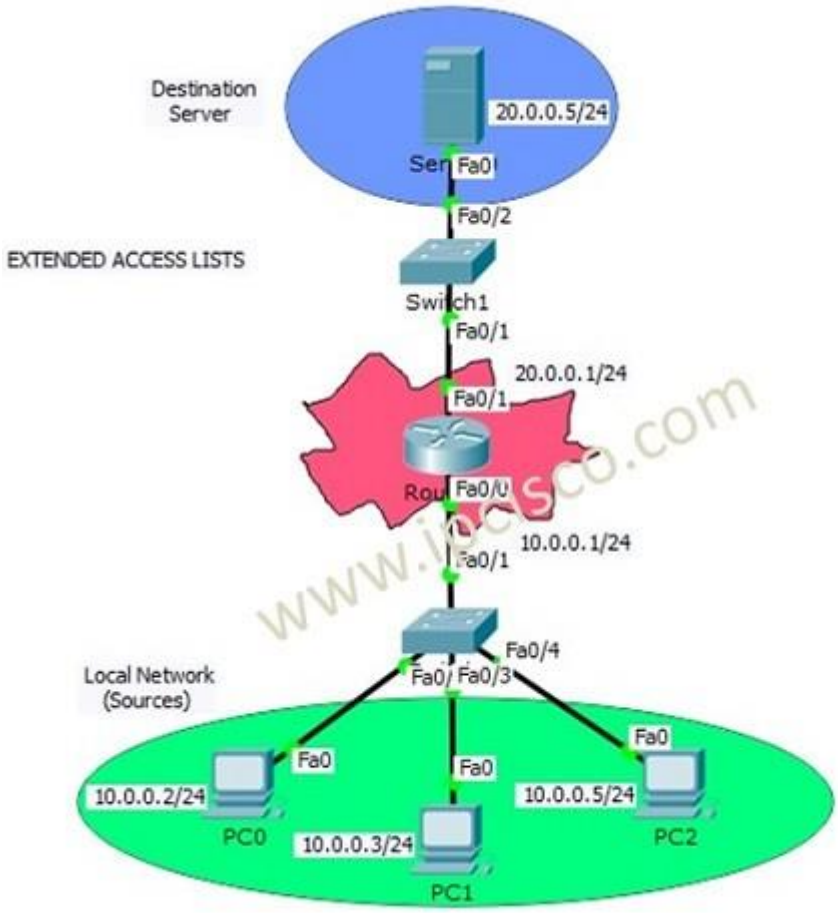


Table of Contents

- Packet Tracer Extended Access Lists Configuration
  - Extended Access-List Configuration

Packet Tracer Extended Access Lists Configuration

In this lesson we will focus on **Cisco Extended ACL 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 **Cisco Extended ACL Configuration** 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 **Cisco Extended ACL Configuration**.

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**

You can also **DOWNLOAD** all the **Packet Tracer** examples with **.pkt** format in **Packet Tracer Labs** section.

Standard Access List Configuration With Packet Tracer

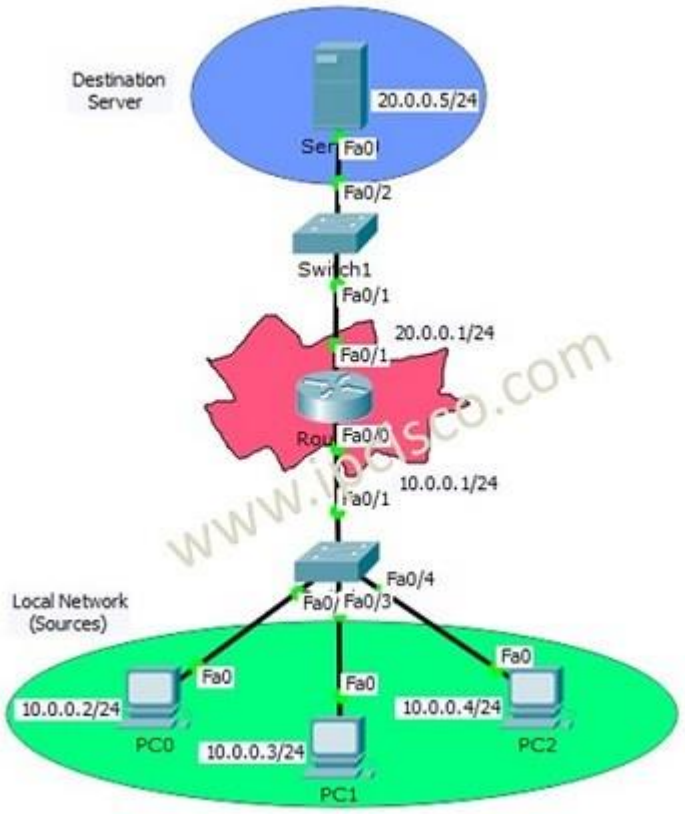


Table of Contents

Packet Tracer Standard Access List Configuration

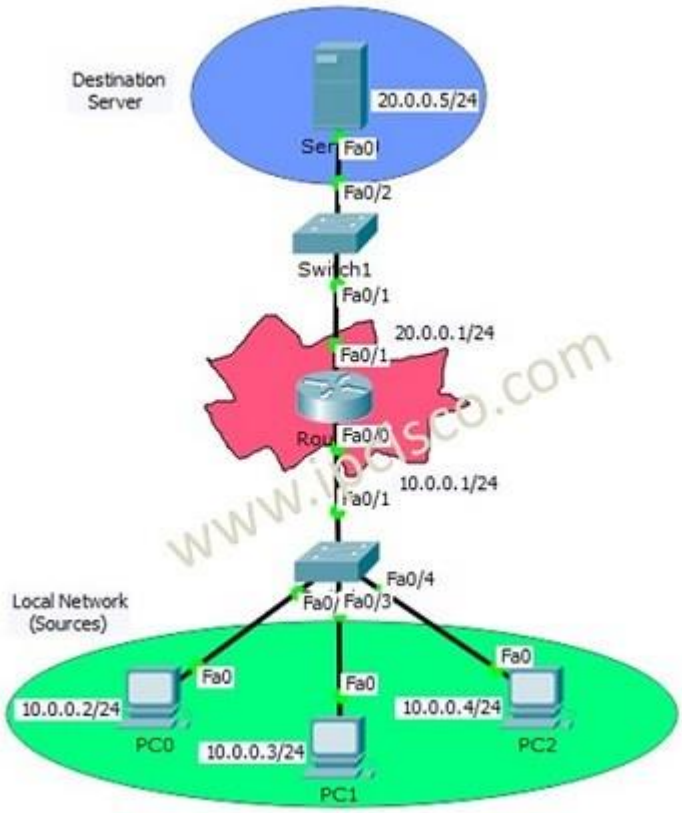
In this lesson we will see **Cisco Standard ACL Configuration** and how to configure **Standart Access-List** in Packet Tracer.
There are **three types Access Lists** in common. Thse access list types are :

- **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 Packet 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 do**Cisco Standard ACL Configuration**. 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.

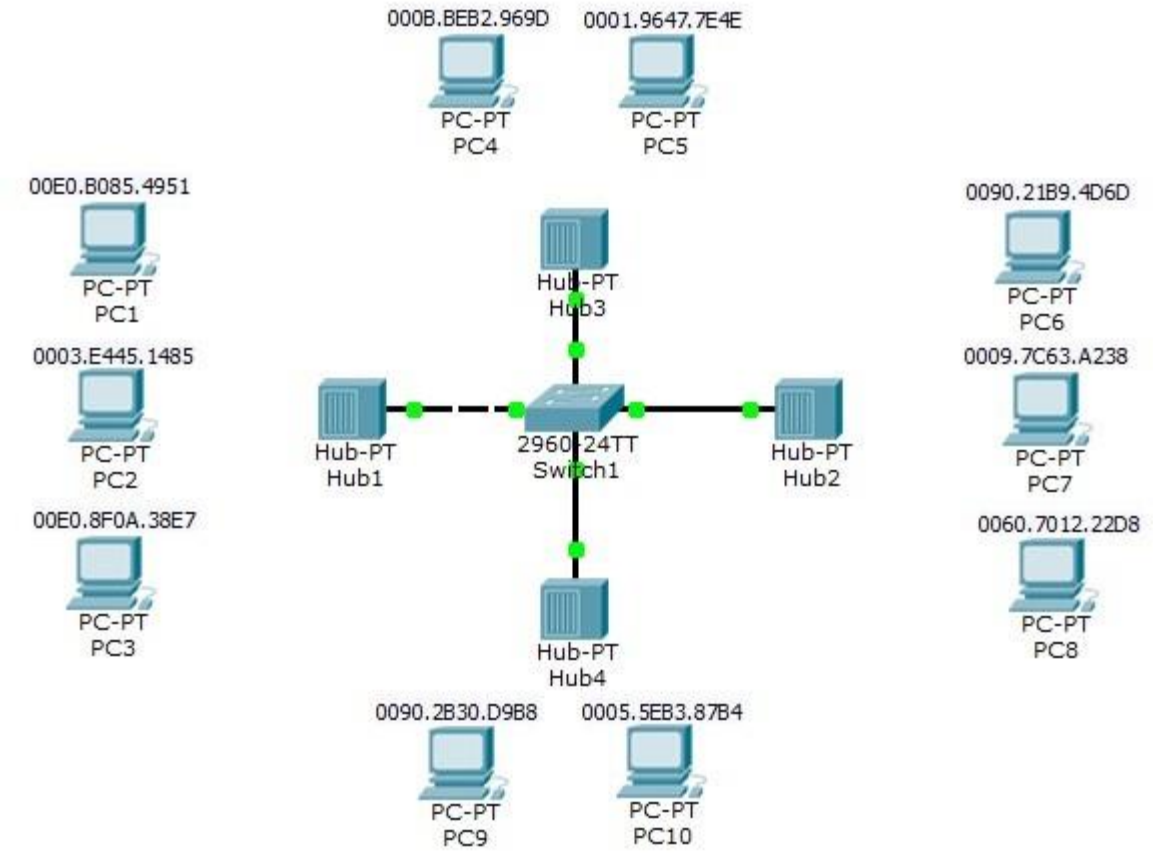
Here, there is no need to write but to show how to write deny, I will write the deny command also. As I said before, for this scenario, it is not necesary. But, you can write.

Router (config-std-nacl)# **deny 10.0.0.4 0.0.0.0**
Router (config-std-nacl)# **end**
Router # **copy run start**

Applying Standard Access-List to the Interface

After creating ACLs, we need to apply this ACL to the **interface**. For **Standard Access-List**, it is better to apply this ACL, close to the destination. So, for this configuration, we will apply our standard acceess list to the fastethernet 0/1 interface of the router.In other words, we will add ACL to the server face of the router.

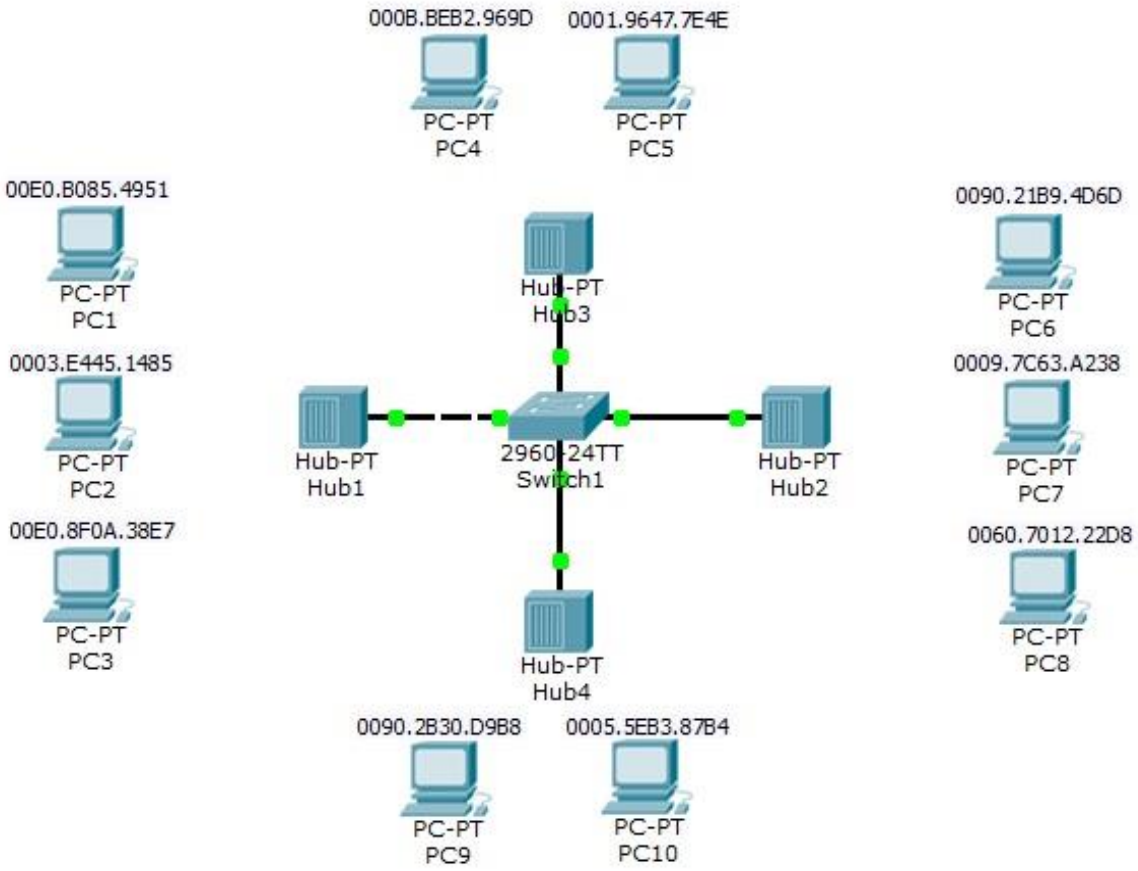
Switch Port Security Configuration with Cisco Packet Tracer



In this article, we will focus on detailed **Port Security Configuration**. For our **Port Security Configuration**, we will use the below topology. In this topology we will make examples for the configuration cases on Port Security.

You can **DOWNLOAD** the **Packet Tracer** example with **.pkt** format **HERE**.

You can download all Cisco Packet Tracer Labs on **Cisco Packet Tracer Labs** Page.



Switch Port Security Topology

Here we will use four scenario on four switch port. According to these scenarios, the below **Port Security** configuration will be done:

1.port

– max MAC 2
– 1 static MAC (PC1)
– 1 dynamic MAC (PC2)
– 1 violation (PC3)
– violation type shutdown

Switch(config)# **interface fastEthernet 0/1**
Switch(config-if)# **switchport mode access**
Switch(config-if)# **switchport port-security**
Switch(config-if)# **switchport port-security maximum 2**
Switch(config-if)# **switchport port-security mac-address 00E0.B085.4951**
Switch(config-if)# **switchport port-security mac-address 0003.e445.1485**
Switch(config-if)# **switchport port-security violation shutdown**

2.port

– max MAC 2
– 2 dynamic MAC (PC6,PC7)
– 1 violation (PC8)
– violation type restrict

Switch(config)# **interface fastEthernet 0/2**
Switch(config-if)# **switchport mode access**
Switch(config-if)# **switchport port-security**
Switch(config-if)# **switchport port-security maximum 2**
Switch(config-if)# **switchport port-security mac-address sticky**
Switch(config-if)# **switchport port-security violation restrict**

Basic Cisco Router Security Configuration

Table of Contents

How to Secure a Cisco Router Basically?

Security is an important concern for a network engineer. How can a network engineer provide security of a router? In this **Basic Cisco Router Security Configuration** lesson, we will talk about, how to **Secure a Router**. We sill see the **Router Security Steps** one by one. Let's start.

Would you like to learn **Basic Cisco Router Configuration**?

Disabling Unused Ports

For a router basic security configuration, the first step is **shutdowning** all the **unused ports**. If you are using a port, it needs to be up. But if you don't use any ports, then always disable (administratively down) these unused ports.

Shutdowning, in other words, disabling a port is very easy. You can do it with "**shutdown**" command under that interface.

```
Router(config)# interface fastethernet 0/0
Router(config-if)# shutdown
```

Enable and Enable Secret Passwords

The second important router security step is **passwords**. You should use passwords on your router.
Here, there are two passwords: **Enable** and **enable secret password**.

Enable password stores the password in clear text format. So, it is easy to see it. But ,enable secret password stores password in encrypted mode. So, it is more secure.

To **encrypt** all passwords in a router/switch, you can use "**service pasword-encryption**" command.
Let's see how to configure this paswords on a router.

```
Router(config)# enable password 12345
Router(config)# enable secret 12345
Router(config)# service password-encryption
```

Configuring Telnet Access Password

Telnet is not a secure way of connecting to a router. But if you use telnet to connect a router, you should use telnet password.

To configure **Telnet Access** with password, you can use the below commands.

```
Router (config)# line vty 0 4
Router(config-line)# password 12345
Router(config-line)# login
```

Here, firstly we enter the **line vty mode** and then set the password string with password keyword. After that, we enter login command to activate it.

Configuring Console Access Password

Like telnet, you also need to configure **Console Access** password for a secure router. To do this, firstly you need to enter line **console mode** and then set the **password string**. Again, with the login keyword, you can activate it.

To configure **Console Access** with password, you can use the below commands.

```
Router(config)# line console 0
Router(config-line)# password 12345
Router(config-line)# login
```

Configuring Auxiliary Port Access Password

Aux Port Access password is rarely used. But like telnet and console, you can configure its password in line aux mode.

To configure **Aux Port Access** with password, you can use the below commands.