Contents

1 Configuring Cisco router for the first time

This tutorial is for those of you that have never touched a Cisco router before. I'll show you what happens when you boot a `Cisco` router and how to apply a basic configuration so that you can login remotely. In this example I'm using a `Cisco 1941` router but any other model will give you similar results.

First we will connect our blue Cisco console cable to our router and start `Putty` (`sudo putty`) so that we can connect to it:

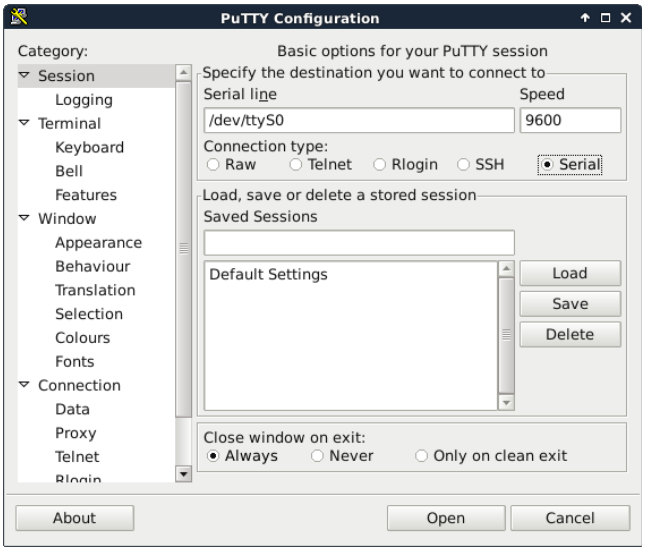


Figure 1: Serial connection using putty

Make sure you select `Serial` and set the speed at `9600`. The `COM` port might be different for you, especially if you are using a USB to Serial adapter. Make sure to check this number in the Windows device manager. In the case where you are using USB to Serial adapter to connect the router to your computer make sure you select `Serial` and set the `serial line` box to `/dev/ttyACM0`. As soon as you switch on the power of your router you will see something like this on your terminal screen:

```
Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of
      memory.
Processor board ID FCZ1941705Y
2 Gigabit Ethernet interfaces
1 terminal line
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
255488K bytes of ATA System CompactFlash 0 (Read/Write)
```

So what does all of this mean?

The first thing you see is the router model, in my example we are looking at a `Cisco 1941/K9`. This router has *2 Gigabit interfaces* and *1 terminal line interface*. Now you have an idea what your router is capable of.

The first thing we'll do is erase that default configuration so we can start with a clean one:

```
Router>en
Router#erase startup-config
```

```
Erasing the nvram filesystem will remove all configuration
     files! Continue? [confirm]
[OK]
Erase of nvram: complete
*Dec 10 16:16:12.683: %SYS-7-NV_BLOCK_INIT: Initialized the
     geometry of nvram
```

This deletes our configuration but we still have to reboot the router to make sure it's not active anymore:

```
Router#reload
Proceed with reload? [confirm]

*Dec 10 16:20:42.455: %SYS-5-RELOAD: Reload requested by
     console. Reload Reason: Reload Command.
```

If the router asks you to save the system configuration, make sure you answer with **no**. It will take some time for the router to reload and once it's ready you will see the following screen:

```
        --- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes
     /no]: no
```

The router asks you if you want to follow a wizard that lets you configure some basic items like setting a hostname, IP address and changing the default passwords. We are not going to do this. We'll configure everything ourselves. Make sure you answer with **no** and you'll see the following screen:

```
Router>
```

You are now in user mode but you are only allowed to use a few commands now. You can recognize the user mode because of the `>` symbol. What we need is privileged or enabled mode which allows us to do anything on the router. This is how to do it:

```
Router>enable
Router#
```

The `#` symbol tells us that we are in privileged mode. You are now allowed to do anything on your router. Let's start by looking at the interfaces that this router has. Check the status of the interfaces on the router with the show ip interface brief command.

```
Router#show ip interface brief
Interface                  IP-Address      OK? Method Status
                Protocol
Embedded-Service-Engine0/0 unassigned      YES unset
     administratively down down
GigabitEthernet0/0         unassigned      YES unset
     administratively down down
GigabitEthernet0/1         unassigned      YES unset
     administratively down down
```

Here you can see the interfaces that this router has. For now we'll just work with the `GigabitEthernet0/0` interface.

1. Explain the result of that command?

2 Lab 1: Set static route

2.1 Connect your router to your PC

Let consider the following topology:

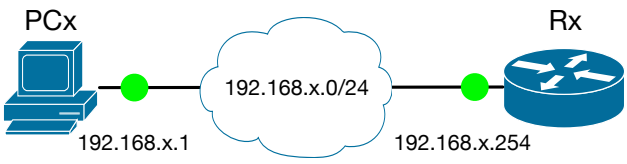


Figure 2: Network topology

In this topology we connect your PC to you router. We start by changing the name of your router. We chose `Rx`, where x is the number oy your router as a new router name. In this case we should move the privilage mode and than use the command hostname to change the name of your router as following:

```
Router>enable
Router#configure terminal
Router(config)#hostname Rx
Rx(config)#
```

Now let's look at the interfaces that this router has. We whant to activate the GigabitEthernet0/0 interface and connect our computer to it. In this case, we'll give to that interface an IP address. First we need to go to the configure mode which is where we can make changes:

```
Rx#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Rx(config)#
```

Now we move to the interface level, activate it and configure an IP address on it:

```
Rx(config)#interface gigabitEthernet 0/0
Rx(config-if)#ip address 192.168.x.254 255.255.255.0
Rx(config-if)#no shutdown
Rx(config-if)#exit
Rx(config)#exit
```

Now you have to connect your computer to that interface and configure your computer to be in the same subnet as the router.

Questions

1. Propose a configuration for your PC (IP adress, Mask and Gateway)
2. Check the status of the interfaces on router.
3. Test connectivity by pinging from each PC to the default gateway that has been configured for your host

Finally, we have to save the running configuration to the startup configuration file as following:

```
Rx#copy running-config startup-config
```

The last command save the current configuration in order to be used at the next router reboot. The restarting router can be done either with the `reload` command or with a `shutdown`. In this case, the current configuration will be lost if it was not registered. During the startup, the router uses the startup configuration as a default configuration.

2.2 Configure static route between two routers

2.2.1 Topology configuration

You must establish a network that enables communication between PCs `x` and `y`, in two different subnets, as illustrated in the following figure. We assume that these two PCs are located on different geographical sites, each haves router. Communication is thus carried out through the public network `200.0.xy.0/24` (inter-network router).

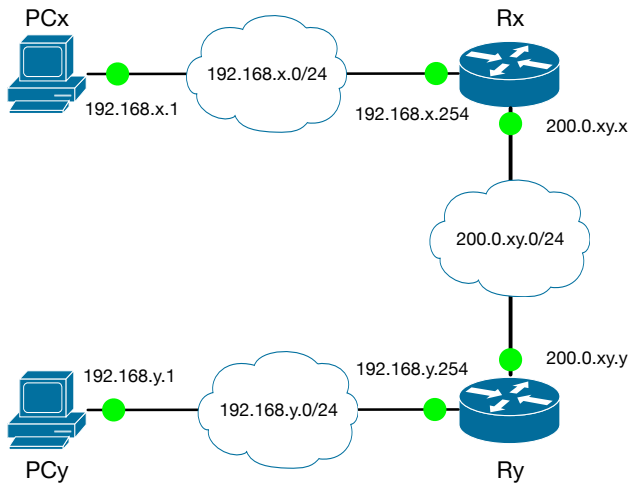


Figure 3: Network topology

Questions

1. Using the console set the configuration of the second router interface `FastEthernet0/0` or `GigaEthernet0/1` depending on your router.

2. Use the router show commands to check its parameters.

3. Save the new configuration, otherwise it will be lost if you restart your router.

4. Ping the IP address of the `PCy`. What is the result?

5. Make a `traceroute`[1] between the PC `x` and the PC `y`. What is the result? The packets are there dropped? In which device?

6. Check the router interfaces using the command `show ip interface brief`. This command displays a summary of the command `show ip interfaces`. Are all the interfaces actives?

7. Check the routing table of your router using the command `show ip route`. Comment the result of that command? Why you can not ping the PC `y`?

[1] `traceroute` command is a network diagnostic tool for displaying the route (path) and measuring transit delays of packets between your PC to a given destination across an IP network (`traceroute @Destination_IP_Address`.

2.2.2 Configure the static route

Routers forward packets using the route informations from route table entries that you manually configure or using dynamic routing algorithms. Using static routes we have to manually define paths between two routers. In our example, we have to add a static route between the routers Rx and Ry. Basically, we need to add a new entry in the routing table of router Rx where we specify that the next hop to reach the network 192.168.y.0/24 is the router Ry. This operatio is done as follwoing:

```
Rx>enable
Rx#configure terminal
Rx(config)#ip route 192.168.y.0 255.255.255.0 200.0.xy.y
Rx(config)#exit
Rx#
```

Questions

1. Ping the IP address of the PCy. What is the result?

2. Display the routing table of your router. Discuss the difference between the current routing table and the last routing table?

3. What is the administrative distance?

2.3 Connect 4 sub-networks using static routes

With other groups realize an interconnection of four subnets, as illustrated in the last figure. Since, we have only two IP interfaces in our routers you have to use the switch interface of your router to connect the the other routers. Basically, you have to create a vlan on your swith. In order to assign an IP adress to a specific switch interface on your router, you have to proceed as following:

```
Rx>enable
Rx#configure terminal
Rx(config)#interface FastEthernet0/0/0
Rx(config-if)# switchport access vlan 1
Rx(config-if)# no ip address
Rx(config-if)# no shutdown
Rx(config)#exit
Rx#
```

Now you can use the `vlan 1` interface as a classical ethernet interface and assign an IP address to the `vlan 1` interface.

Questions

1. Configure all the interfaces and add all the necessary static routes so that all the PCs can ping between each other.

2. Display the routing table of your router. Discuss the difference between the current routing table and the last routing table?

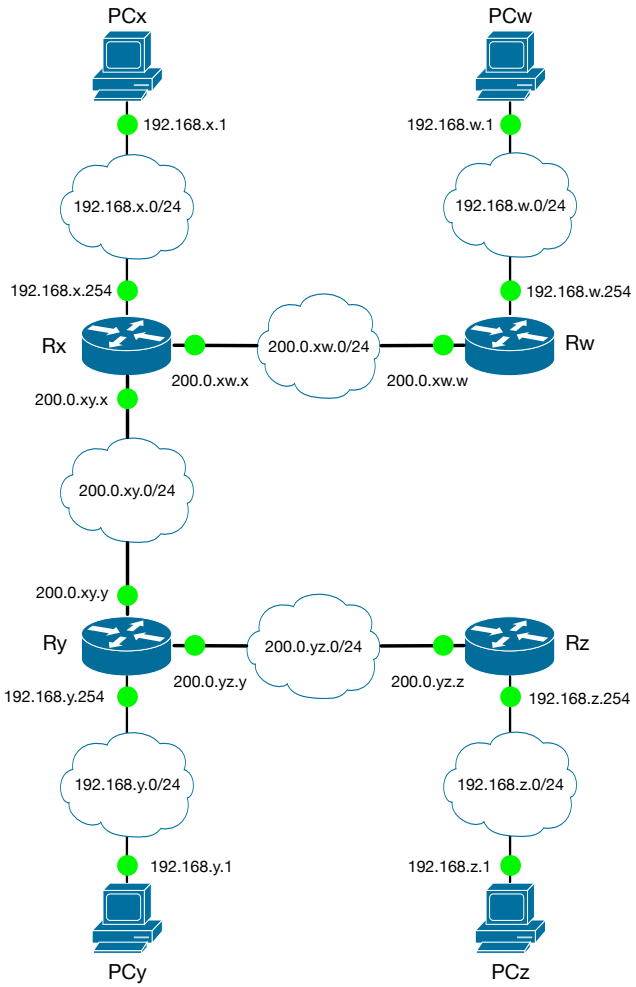


Figure 4: Network topology

3 Lab 2: Dynamic routing protocol (RIPv2 – Routing Information Protocol version 2)

RIP is a distance vector routing protocol and the simplest routing protocol to start with. We'll start by paying attention to the distance vector class. What does the name distance vector mean?

- Distance: How far away, in routing world we use metrics which we discussed in class.
- Vector: Which direction, in routing world we care about which interface and the IP-address of the next router to send it to.

RIPv2 support a maximum hop count value of 15. Any router farther than 15 hops away is considered to be unreachable. The main enhancement of RIPv2 over its ancestor is the fact that it first sends the subnet mask with the updates; hence it is considered to be a classless routing protocol in the sense that it is able to distinguish among different subnets – which is something that is not found in RIPv1. The main characteristics of RIPv2 are:

- Transmits the subnet mask with routes updates
- Supports plain text and MD5 authentification
- Uses multicast routing updates
- Uses external routes tags

3.1 Configure RIP on a Cisco router

Start by establishing the network topology illustrated in the following figure. All PCs are located on different geographical sites, each haves router. Communication is carried out through the public network `200.0.xy.0/24` (inter-network router).

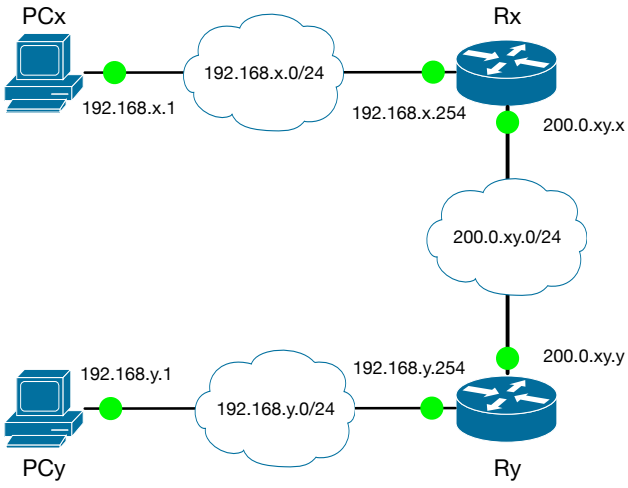


Figure 5: Network topology

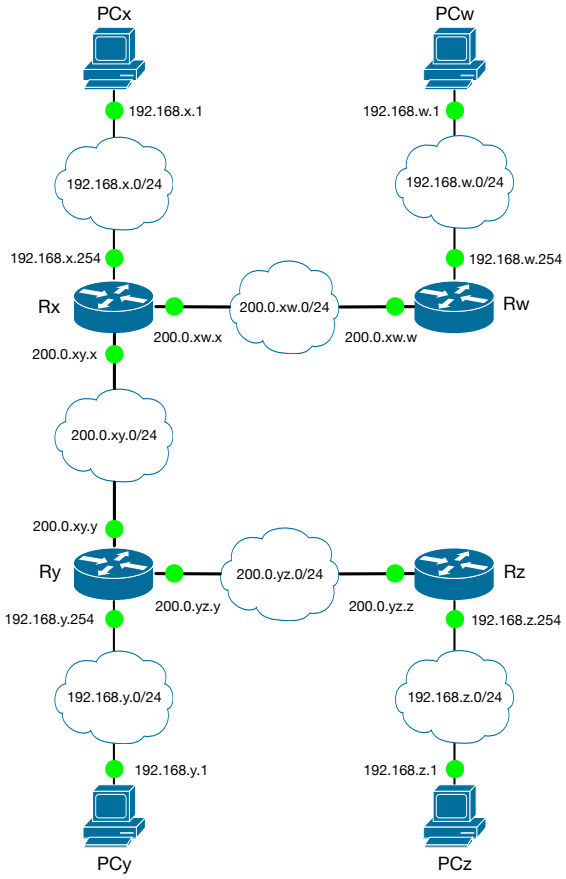


Figure 6: RIPv2 with 4 routers topology

Questions

1. Configure all the interfaces for the PCs and the routers.
2. Display and analyse the routing table of your router.

Let's configure on each routers RIPv2 as following:

```
Rx>enable
Rx#configure terminal
Rx(config)#router rip
Rx(config)#version 2
Rx(config-router)#network 192.168.x.0
Rx(config-router)#network 200.0.xy.0
Rx(config-router)#exit
Rx(config)#exit
Rx#
```

Questions

1. On `PCx` ping the IP address of the `PCy` and on `PCy` ping the IP address of `PCx`. What are the results?
2. Display and comment the routing table of your router.

3.2 Connect 4 sub-networks using RIPv2

With a neighboring groups realize the interconnection of four subnets, as illustrated in the following figure.

Questions

1. Configure all the interfaces for the PCs and the routers.

2. The PCs are they able to ping each other?

3. Display and comment the routing table of your router.

One of the most important notion in routing protocol is the **Administrative Distance** (AD). Administrative distance is an arbitrary numerical value assigned to a routing protocol, a static route or a directly-connected route based on its perceived **quality of routing**. The administrative distance value is often used by `Cisco` routers to determine the "**best**" route that should be used when multiple paths to the same destination exist. *A routing protocol with a lower administrative distance is considered "better" and is given priority over routing protocols with higher administrative distances.* The "better" route is selected by the router and is inserted into the router's routing table to be used to route traffic. The following table lists the default administrative distances for various routing protocols used on Cisco routers:

Connected	0
Static	1
RIP	120
OSPF	110

Questions

1. Now unplug one of your subnets and display the routing table. What do you notice?

3.3 RIPv2 messages Analysis

Reconnect all the subnets and wait 2 minutes for routing tables to regain their initial configuration. As introduced in the class, each RIP router sends a copy of its routing table on all its interfaces. Among them we have the interface that connects the router to your PC. Thus, your PC will also receive the routing table of your router. In the following we will capture this traffic in order to analyse the RIPv2 frames. In order to analyse the RIPv2 frames we needs to run the `wireshark` tool on your PC in `sudo` mode and start capturing the traffic received by your PC.

1. Using the wireshark tool analyse the paquet that your are receiving from your router. What is the IP source address that are used for the RIPv2 messages? What information do you receive?

2. What is the routing domaine?

3.4 Add redundant route

Now, we want to connect router `Rx` and router `Rz`. In this case, we add a serial cable between `Rx` and `Rz`. This new link provide a redundant route to your networks.

Suppose that `Rx` is the DCE and `Rz` the DTE, and a bitrate of **56kps** is desired, then the routers are configured as follows:

```
Rx(config)#interface serial 1/0
Rx (config-if)#ip address 200.0.xz.x 255.255.255.0
Rx (config-if)#clock rate 56000
Rx (config-if)#no shutdown
Rx(config-if)#end
```

and

```
Rz(config)#interface serial 1/0
Rx (config-if)#ip address 200.0.xz.z 255.255.255.0
Rz (config-if)#no shutdown
Rz(config-if)#end
```

1. List and record the contents of your routing tables.

2. Now to reach the network `y` from the `x`, which path is choosen? Is there an alternative route? Is this a good choice?

3. If we unplug the link between the network `z` and the network `x`, What do you observe on your routing tables? The communication between the network `z` and `x` is it re-established?

4 Lab 3: Dynamic routing protocol (OSPF – Open Shortest Path First)

OSPF is a link-state routing protocol and it's one of the routing protocols you need to understand if you want to do the Cisco CCNA exam. In this lab we will explain the basics of OSPF to learn how and why it works. OSPF protocol belongs to the Link-state routing protocols family. Link-state routing protocols are like your navigation system, they have a complete map of the network. If you have a full map of the network you can just calculate the shortest path to all the different destinations out there. This is cool because if you know about all the different paths it's impossible to get a loop since you know everything! The downside is that this is more CPU intensive than a distance vector routing protocol. It's just like your navigation system... if you calculate a route from Paris to Lyon it's going to take a bit longer than when you calculate a route from one street to another street in the same city.

Basically, link-state routing protocols operate by sending link-state advertisements (LSA) to all other link-state routers. All the routers need to have these link-state advertisements so they can build their link-state database or LSDB. Basically all the link-state advertisements are a piece of the puzzle which builds the LSDB.

4.1 Configure OSPF on a Cisco router

As in RIPv2 Lab, start by establishing the network topology illustrated in the following figure 4.1. All PCs are located on different geographical sites, each haves router.

Questions

1. Configure all the interfaces for the PCs and the routers.
2. Display and analyse the routing table of your router.

Let's configure on each routers OSPF as following:

```
Rx>enable
Rx#configure terminal
Rx(config)#router ospf 1
Rx(config-router)#network 192.168.x.0 0.0.0.255 area 0
Rx(config-router)#network 200.0.xy.0 0.0.0.255 area 0
Rx(config-router)#exit
Rx(config)#exit
Rx#
```

Questions

1. The PCs are they able to ping each other?
2. Display and comment the routing table of your router.
3. Now unplug one of your subnets and display the routing table. What do you notice?

4.2 OSPF messages Analysis

4.3 Add redundant route

As in the RIPv2 Lab, we want to connect router `Rx` and router `Rz`. Add a serial cable between `Rx` and `Rz`. This new link provide a redundant route to your networks. We also want to limit the bitrate between the two router to **56kps**

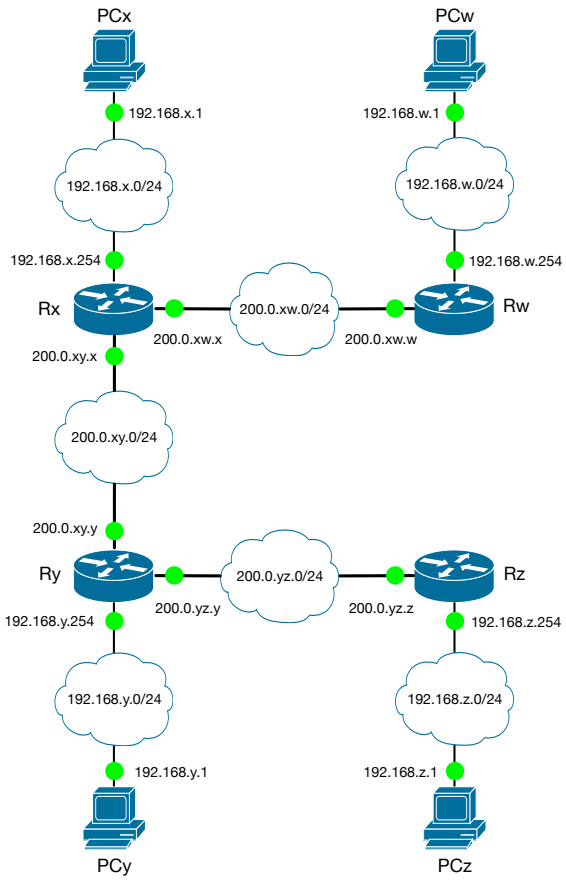


Figure 7: OSPF with 4 routers topology

Questions

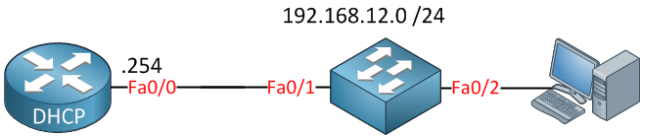
1. List and record the contents of your routing tables.
2. To reach the network `y` from the `x`, which path is choosen? Is there an alternative route? This route is it the same as in the RIPv2 Lab? Is this a good choice?
3. If we unplug the link between the network `z` and the network `y`, what do you observe on your routing tables? The communication between the network `z` and `y` is it re-established?

5 Lab 4: DHCP

IP addresses can be configured statically or dynamically. The static configuration is made by the administrator on each device. However, the dynamic method uses **DHCP** (*Dynamic Host Configuration Protocol*) in order to provide to the devices all the required configuration. In the following, we will show how we could configure the DHCP server on a Cisco router.

5.1 Basic DHCP Server configuration on Cisco

Cisco IOS routers and layer 3 switches can be configured as DHCP server. Let's use the following topology to configure a basic DHCP Server:



As we can see, we have one router that we will call **DHCP**. The router and computer are connected to each other either by using a switch or directely from the router interface. The most import thing is that both the router and the PC have to be in the same VLAN at this stage. We will use the `192.168.12.0/24` subnet for this first configuration. The first step is to configure the ip address of the router on the interface `fastEthernet 0/0`, as following:

```
DHCP(config)#interface fastEthernet 0/0
DHCP(config-if)#no shutdown
DHCP(config-if)#ip address 192.168.12.254 255.255.255.0
```

Next, we can configure the DHCP server. Here, we use the `ip dhcp pool` command in order to create a DHCP pool and give it a name (here `PoolOnRx`). This DHCP pool will use network `192.168.12.0/24`. Basically this is all you have to do to get DHCP server going, there is no need to start a service or something.

```
DHCP(config)#ip dhcp pool PoolOnRx
DHCP(dhcp-config)#network 192.168.12.0 255.255.255.0
```

Now let's start a DHCP request from the PC client as following:

```
[$]sudo dhclient -v eth1
[sudo] password for achir:
Internet Systems Consortium DHCP Client 4.2.4
Copyright 2004-2012 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth1/00:1f:f3:8b:95:69
Sending on  LPF/eth1/00:1f:f3:8b:95:69
Sending on  Socket/fallback
DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 3 (
     xid=0x1f591868)
DHCPREQUEST of 192.168.12.1 on eth1 to 255.255.255.255 port 67
      (xid=0x6818591f)
DHCPOFFER of 192.168.12.1 from 192.168.12.254
DHCPACK of 192.168.12.1 from 192.168.12.254
bound to 192.168.12.1 -- renewal in 39791 seconds.
```

We can finally verify that we have DHCP clients using the following command on the router:

```
DHCP#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration
     Type
                    Hardware address/
                    User name
192.168.12.1        001f.f38b.9569          Dec 12 2015 02:52 PM
     Automatic
```

As we can see, we have a DHCP client and it received IP address `192.168.12.1`.

In addition to the IP address, we may also use DHCP to hand out some other useful things like a default gateway, DNS server and more. Let's see how we can do this:

```
DHCP(config)#ip dhcp pool PoolOnRx
DHCP(dhcp-config)#default-router 192.168.12.254
DHCP(dhcp-config)#dns-server 208.67.222.222
```

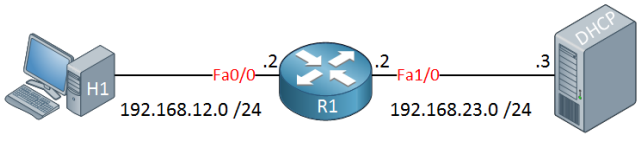
Above we configured IP adress `192.168.12.254` as default gateway for the DHCP clients with the `default-router` command. We can also specify the DNS server using the command `dns-server`.

Questions

1. Using the last commands, cofigure the DHCP Server on your router and connect two different PCs using a switch.
2. Using the documentation provided by Cisco online, list a set of option that we could add in order to add other options to PC configuration?
3. Explain the mechanism for assigning an IP address by DHCP, based on the analysis of the frames exchanged between the PC and the DHCP server from the start a DHCP request from the PC to the complete assignment of the configuration. Use the Wireshark software to support your analysis.

5.2 DHCP Relay Agent

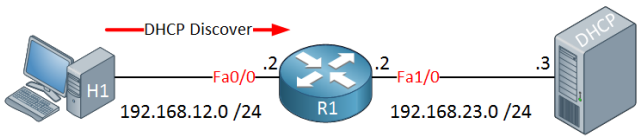
DHCP is often used for hosts to automatically assign IP addresses and uses 4 different packets to do so. Since a host doesn't have an IP address to start with, we use broadcast messages on the network that hopefully end up at a DHCP server. The problem with broadcast is that this means that the DHCP server has to be in the **same broadcast domain since routers do not forward broadcast packets**. Take a look at the following picture:



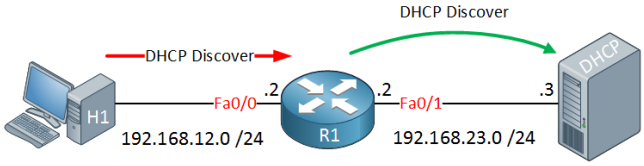
On the left side we have a client (**H1**), in the middle a router (R1) and on the right side is our DHCP server. The client wants to get an IP address through DHCP and will send broadcast a `DHCP discover` message. The router, doing its job will not forward broadcast traffic so the DHCP discover will never reach the DHCP server.

So **how can we solve this?** We have to use the **DHCP Relay Agent** feature. In short, the router will forward

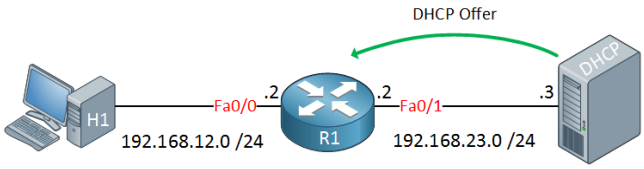
`DHCP requests` from the client towards the DHCP server and when the DHCP server responds it will forward the messages back to the client, as following:



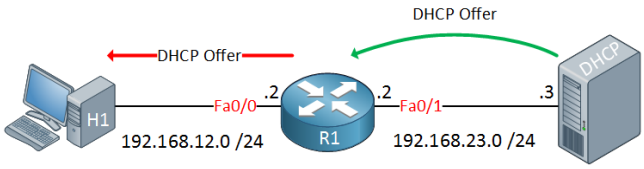
The first thing that happens is that our client will broadcast a `DHCP discover` message, the router will receive this message since its in the same broadcast domain as the client. Here's what happens next:



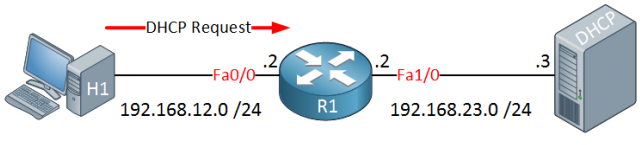
The router receives the `DHCP discover` message on its `FastEthernet 0/0` interface and will normally just discard this packet. With the **DHCP relay agent** feature enabled, it will do something else. It will forward the `DHCP discover` message as a unicast packet and also inserts a field called `giaddr` (*Gateway IP Address*) in the DHCP packet. It will insert IP address `192.168.12.2` in this field since we received the `DHCP discover` on the `FastEthernet 0/0` interface. This `giaddr` field is required by the DHCP server or it won't know from which pool it has to select an IP address. Also, the source IP address of this unicast packet will be `192.168.12.2`.



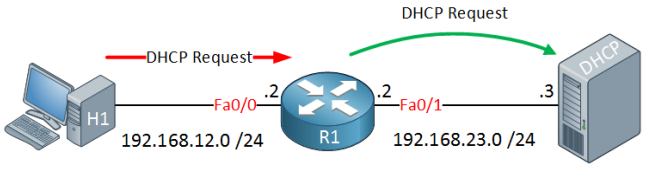
The DHCP server has received the `DHCP discover` message and in return will send a `DHCP offer` message. This will be sent as a unicast packet to the router.



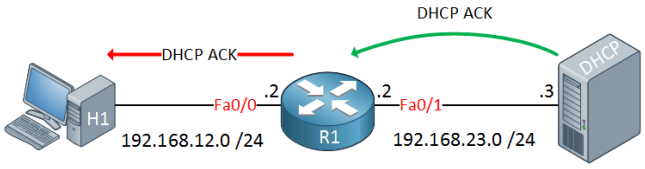
The router, being a good relay will forward the `DHCP offer` on its `FastEthernet0/0` interface as a broadcast.



The client likes the content of the `DHCP offer` message and will create a `DHCP request` which is broadcasted. The router hears this broadcast and will do this:



Just like the initial `DHCP discover` message, this `DHCP request` will be forwarded as a unicast packet. Once again the giaddr field is inserted with IP address `192.168.12.2`. The DHCP server receives the `DHCP request` and will process it.



Last but not least, the DHCP server will send a `DHCP ACK` in response to the `DHCP request`. This is sent to the router by using unicast and our router will broadcast it on its `FastEthernet 0/0` interface so the client receives it. The client now has an IP address and our mission is a great success.

Now you know how the DHCP relay agent works, let's take a look at the configuration.

5.3 Basic DHCP relay agent configuration on Cisco

In order to configure the DHCP relay on the router we have to:

- Create the Pool on the DHCP server. If this DHCP Server has to configure several Subnets, than we have to create one pool by Subnet.
- On each router connected to one Subnet we must configure the Remote Router using the `ip helper-address ...` command to enable the transmission of DHCP messages from the subnet to the DHCP server using unicast communictions. According to the last example, this command should be configured as following:

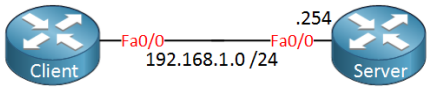
```
R1(config)#interface fastethernet 0/0
R1(config-if)#ip helper-address 192.168.23.3
```

Questions

1. Connect all the routers of the Lab room in order to form one signle network. You could use RIPv2 as routing protocol.
2. Among all the routers, select one router acting as DHCP Server and configure all the other routers to act as DHCP Relays.

5.4 DHCP Client on Cisco

DHCP server is often used on Cisco IOS routers so you supply hosts with an IP address. We can also use **DHCP client** on our routers which is useful if your ISP uses dynamic IP addresses for customers. We will see in the following how to configure your router as DHCP client.



- DHCP Server: Let's create a pool for our local subnet and include a default route:

```
Server(config)#ip dhcp pool MY_POOL
Server(dhcp-config)#network 192.168.1.0 /24
Server(dhcp-config)#default-router 192.168.1.254
```

- DHCP Client: You only need one command on the interface to use DHCP:

```
Client(config)#interface FastEthernet 0/0
Client(config-if)#ip address dhcp
Client(config-if)#no shutdown
```

  After a few seconds you will see this:

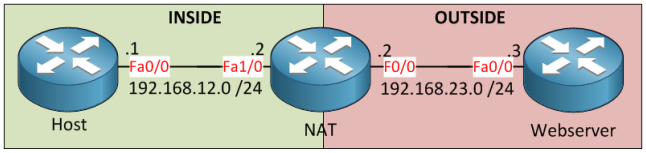
```
Client#
%DHCP-6-ADDRESS_ASSIGN: Interface FastEthernet0/0 assigned
      DHCP address 192.168.1.1, mask 255.255.255.0,
     hostname Client
```

6 Lab 5: NAT/PAT

Without network address translation (**NAT**) or port address translation (**PAT**) you probably wouldn't be able to access the internet from your computer or at least you'll be the only one in the house having internet access...in this lab we want to give you an explanation of why and how we use **NAT/PAT** for Internet access.

6.1 How to configure Static NAT/PAT on Cisco IOS Router

Let's take a look at how to configure static NAT no a Cisco router. Here's the topology I will use:



Above you see **2 PCs** called `Host` and `Webserver` and one router noted as `NAT`. Imagine our host is on our LAN and the webserver is somewhere on the Internet. Our `NAT` router in the middle is our connection to the Internet.

First we have to configure all the address of all the interfaces as given in the figure above.

Both PCs can use router `NAT` as their default gateway. Let's see if they can reach each other. In this case try to ping the Host PC from the Webserver PC and the Webserver PC from the Home PC.

1. Ping the IP address of each PC from the other PC. What is the result?
2. Start wireshark on the Webserver PC and indicate, for the received IP packets, which IP address is used as source address?

Now let's configure `NAT` so you can see the difference:

```
NAT(config)#interface fastEthernet 1/0
NAT(config-if)#ip nat inside
NAT(config-if)#exit
NAT(config)#interface fastEthernet 0/0
NAT(config-if)#ip nat outside
```

Now we would like to tell to the router `NAT` how to perform address translation and mention which IP addresses (source or destination) to re-write in packets moving between the inside and the outside interfaces. Here we go:

```
NAT(config)# ip nat inside source static 192.168.12.1
    192.168.23.2
```

Here, we are telling to the router `NAT` to permform Nat on packets commung into the router on the inside interface `Fa1/0`. More specifically the router would identify which of these packets have a source IP address `192.168.12.1` and would change it to `192.168.23.2` before forwarding the packet out the outside interface `Fa0/0`. Simularly, return packets comming from outside interface `Fa0/0` would undergo translation of the destination IP address.

Let's now verify if Nat is actually working as it is supposed to work. There are a couple of very useful CISCO IOS commands that can be used to do just that. Command `show ip nat statistics` display the number of **static dynamic NAT** translations, inside and outside interfaces, and the number of hits and misses.

```
NAT#show ip nat statistics
```

Command `show ip nat translations` displays the IP addresses for NAT translations.

Let's now go to the PC and ping the Server before running the command `show ip nat translations` again. Is there any difference?

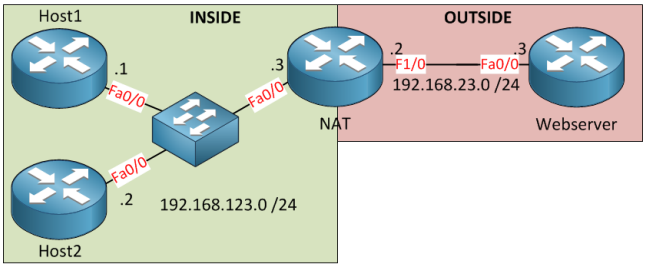
We just configured and verified a simple NAT scenario translating only the source of destination (not both at the same time) IP addresses of packets moving between inside and outside interfaces. This sort of NAT configuration is called **static NAT** as a single inside local IP address is statically mapped to a signgle outside local IP address. Another important feature of **NAT** is static Port Address Translation (**PAT**). Static **PAT** is designed to allow one-to-one mapping between local and global addresses. A common use of a **static PAT** is to allow Internet users from the public network to access a Web server located in the provate network.

Let's assume we intend to host a Web server on the inside on the PC `Host`. In this case the following configuration line would allow us to do just that:

```
NAT(config)#ip nat inside source static tcp 192.168.12.1 80
    192.168.23.2 80
```

This configuration line performs the static address translation from the Web server.

6.2 How to configure Dynamic NAT/PAT on Cisco IOS Router



Dynamic NAT is another **NAT** (Network Address Translation) technology which allows the address translation of a private IP address to a pool of public IP addresses configured on the `NAT` router. **Dynamic NAT** is mostly used when inside computers configured with private IP addresses needs to access outside public internet.

The main difference between **Static NAT** and **Dynamic NAT** is that `Static NAT` allows a remote host to connect to an inside private IP addresses configured computer and `Dynamic NAT` allows a group of private IP addresses to connect to public internet, using the public IP address pool (a range of public IP addresses). The configured public IP address pool typically has fewer addresses than the inside private IP addresses.

Dynamic NAT is is typically used for providing internet access to a private network. But the problem with **Dynamic NAT** is that the number of public IP addresses in the NAT

pool may not be sufficiant for mapping large number of computers configured with private IP addresses.

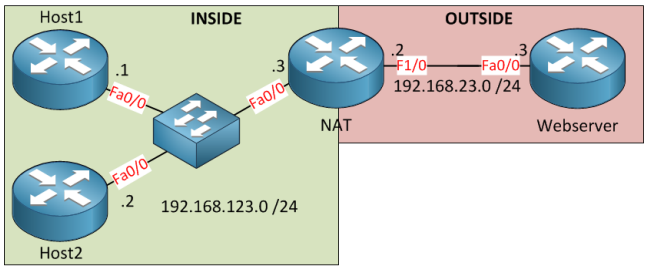
To configure **Dynamic NAT** on a Cisco router, first you need to create an access list to identify the group of private inside IPv4 addresses, which are allowed for NAT translation. That can be done by creating a standard IP access list.

Then you have to create a pool of public IP addresses (which your ISP (internet service provider) has allocated to you).

Finally, you must configure NAT using "`ip nat`" command. Finally you must specify which is inside interface and which is outside interface.

```
NAT>enable
NAT#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
NAT(config)#access-list 10 permit 192.168.123.0 0.0.0.255
NAT(config)#ip nat pool mypool 192.168.23.230 192.168.23.239
     netmask 255.255.255.0
NAT(config)#ip nat inside source list 10 pool mypool
NAT(config)#interface fastEthernet 0/0
NAT(config-if)#ip nat inside
NAT(config-if)#exit
NAT(config)#int fastEthernet 0/1
NAT(config-if)#ip nat outside
NAT(config-if)#exit
NAT(config)#exit
NAT#
```

6.3 How to configure PAT (Port Address Translation or NAT overload) in a Cisco Router



Static NAT is type of Network Address Translation (NAT) which is a one-to-one IP address mapping (one private IP address to one public IP address) and **Dynamic NAT** is a type NAT using many public IP addresses in a NAT address pool. **Static NAT** and **Dynamic NAT** therefore cannot be used providing internet access to inside users, because both require large number of IP public addresses.

PAT (*Port Address Translation or NAT overload*) is another Network Address Translation technology, which can be used to provide internet access to inside users. In **PAT**, several inside private IP addresses can be translated to one or a few outside public IP addresses. The main advantage of **PAT** is that it can be used efficiently for large number of inside private IP addresses even with a single public IP address.

PAT uses unique source port number translation, instead of IP address translation. Port Numbers are **16-bit binary numbers** and we have **65535** port numbers available. **PAT** uses port numbers on Inside Global IP address to distinguish between translations. **PAT** will try to keep the original source port from the inside private IP address. If this source port is already allocated to some other inside computer, **PAT** will allocate another port number.

To configure **PAT** on a Cisco router, first you need to create an access list to identify the group of private inside IP addresses, which are allowed for NAT translation. That can be done by creating a standard IP access list.

After that, you must configure **NAT** using "`ip nat`" command. Finally, you must specify which is inside interface and which is outside interface.

The main difference between configuring `Dynamic NAT` and `PAT` is the use of keywork "`overload`".

The configuration commands to configure PAT is shown below:

```
NAT>enable
NAT#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
NAT(config)#access-list 1 permit 192.168.123.0 0.0.0.255
NAT(config)#ip nat inside source list 1 interface fastEthernet
      1/0 overload
NAT(config)#interface fastEthernet 0/0
NAT(config-if)#ip nat inside
NAT(config-if)#exit
NAT(config)#int fastEthernet 0/1
NAT(config-if)#ip nat outside
NAT(config-if)#exit
NAT(config)#exit
NAT#
```