Módulo B

Cisco

Documentación SpainSkills22
Modalidad 39 Administración de sistemas en red

Daniel Ubalde Laguia

Configuring DHCP Server

This chapter describes how to configure DHCP server on the Cisco 910 Industrial Routers (*hereafter* referred to as the router).

This chapter consists of these sections:

Understanding DHCP

DHCP is widely used in LAN environments to dynamically assign host IP addresses from a centralized server, which significantly reduces the overhead of administration of IP addresses. DHCP also helps conserve the limited IP address space because IP addresses no longer need to be permanently assigned to hosts; only those hosts that are connected to the network consume IP addresses.

The DHCP server assigns IP addresses from specified address pools on a router or router to DHCP clients and manages them.

DHCP for IPv6 Address Assignment

DHCPv6 enables DHCP servers to pass configuration parameters, such as IPv6 network addresses, to IPv6 clients. The address assignment feature manages nonduplicate address assignment in the correct prefix based on the network where the host is connected. Assigned addresses can be from one or multiple prefix pools. Additional options, such as default domain and DNS name-server address, can be passed back to the client. Address pools can be assigned for use on a specific interface, on multiple interfaces, or the server can automatically find the appropriate pool.

Enabling DHCP Server

Beginning in privileged EXEC mode, follow these steps to enable the DHCP server on the router:

	Command	Purpose
1.	**configure terminal**	Enter global configuration mode.
2.	**service dhcp** *interface-type number*	Enable the DHCP server on the interface.
3.	**exit**	Return to privileged EXEC mode.
4.	**show running-config**	Verify your entries.
5.	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable the DHCP server, use the **no service dhcp** global configuration command.

Configuring DHCP Server

This section contains this configuration information:

Configuring DHCP Server

Beginning in privileged EXEC mode, follow these steps to configure DHCP server.

	Command	Purpose
1.	**configure terminal**	Enter global configuration mode.
2.	**ip dhcp pool**	Create a DHCP server address pool and enters DHCP pool configuration mode. **Note:** If you have changed the parameters of the DHCP server, you must perform a refresh using the **no service dhcp** *interface-type number* command and **service dhcp** *interface-type number* commands.
3.	**network** *network-number mask*	Specify the subnet network number and mask of the DHCP address pool.
4.	**domain-name** *domain*	Specify the domain name for the client.
5.	**dns-server** *address*	Specify the IP address of a DNS server that is available to a DHCP client.
6.	**default-router** *address*	Specify the IP address of the default router for a DHCP client.
7.	**exit**	Return to privileged EXEC mode.
8.	**service dhcp** *interface-type number*	Enable DHCP server on the interface.

The following example configures the DHCP server:

```
Router# configure terminal
Router(config)# ip dhcp included-address 192.168.1.101 192.168.1.150
Router(config)# ip dhcp pool
Router(dhcp-config)# network 192.168.1.0 255.255.255.0
Router(dhcp-config)# domain-name cisco.com
Router(dhcp-config)# dns-server 8.8.8.8
Router(dhcp-config)# default-router 192.168.1.1
Router(dhcp-config)# exit
Router(config)# service dhcp vlan1
```

Configuring Stateful DHCPv6 Server

Beginning in privileged EXEC mode, follow these steps to configure stateful DHCPv6 server.

	Command	Purpose
1.	**configure terminal**	Enter global configuration mode.
2.	**ip dhcp pool**	Create a DHCP server address pool and enters DHCP pool configuration mode. **Note:** If you have changed the parameters of the DHCP server, you must perform a refresh using the **no service dhcp** *interface-type number* command and **service dhcp** *interface-type number* commands.
3.	**address prefix** *ipv6-prefix*	Specify an address prefix for address assignment.
4.	**domain-name** *domain*	Specify the domain name for the DHCPv6 client.
5.	**dns-server** *ipv6-address*	Specify the DNS IPv6 servers available to a DHCPv6 client.
6.	**exit**	Return to privileged EXEC mode.
7.	**ipv6 dhcp included-address** *low-address high-address*	Specify the IP addresses that the DHCPv6 server should assign to DHCPv6 clients.
8.	**interface** *type number*	Specify an interface type and number, and enters the interface configuration mode.
9.	**ipv6 dhcp server**	Enable DHCPv6 on an interface.

The following example configures the stateful DHCPv6 server:

```
Router(config)# ipv6 dhcp pool
Router(config-dhcpv6)# address prefix 2001:DB8:1001::0/64
Router(config-dhcpv6)# domain-name cisco.com
Router(config-dhcpv6)# dns-server 2001:DB8:1001::1
Router(config-dhcpv6)# exit
Router(config)# ipv6 dhcp included-address 2001:DB8:1001::100 2001:DB8:1001::200
Router(config)# interface Vlan 1
Router(config-if)# ipv6 dhcp server
```

Configuring Stateless DHCPv6 Server

Beginning in privileged EXEC mode, follow these steps to configure stateless DHCPv6 server.

	Command	Purpose
1.	**configure terminal**	Enter global configuration mode.
2.	**ipv6 nd managed-config-flag**	Set the " managed address configuration flag" in IPv6 router advertisements.
3.	ipv6 nd prefix	Set the IPv6 prefix which is included in IPv6 Neighbor Discovery (ND) router advertisements.

The following example configures the stateless DHCPv6 server:

```
Router(config)# interface Vlan 1
```

```
Router(config-if)# ipv6 nd managed-config-flag
Router(config-if)# ipv6 nd prefix 2001:DB8:1001::0/64
```

Displaying DHCP Server Address Bindings

To display the DHCP server address binding information, use the privileged EXEC command in Table 4:

Table 4 Commands for Displaying DHCP Address Bindings

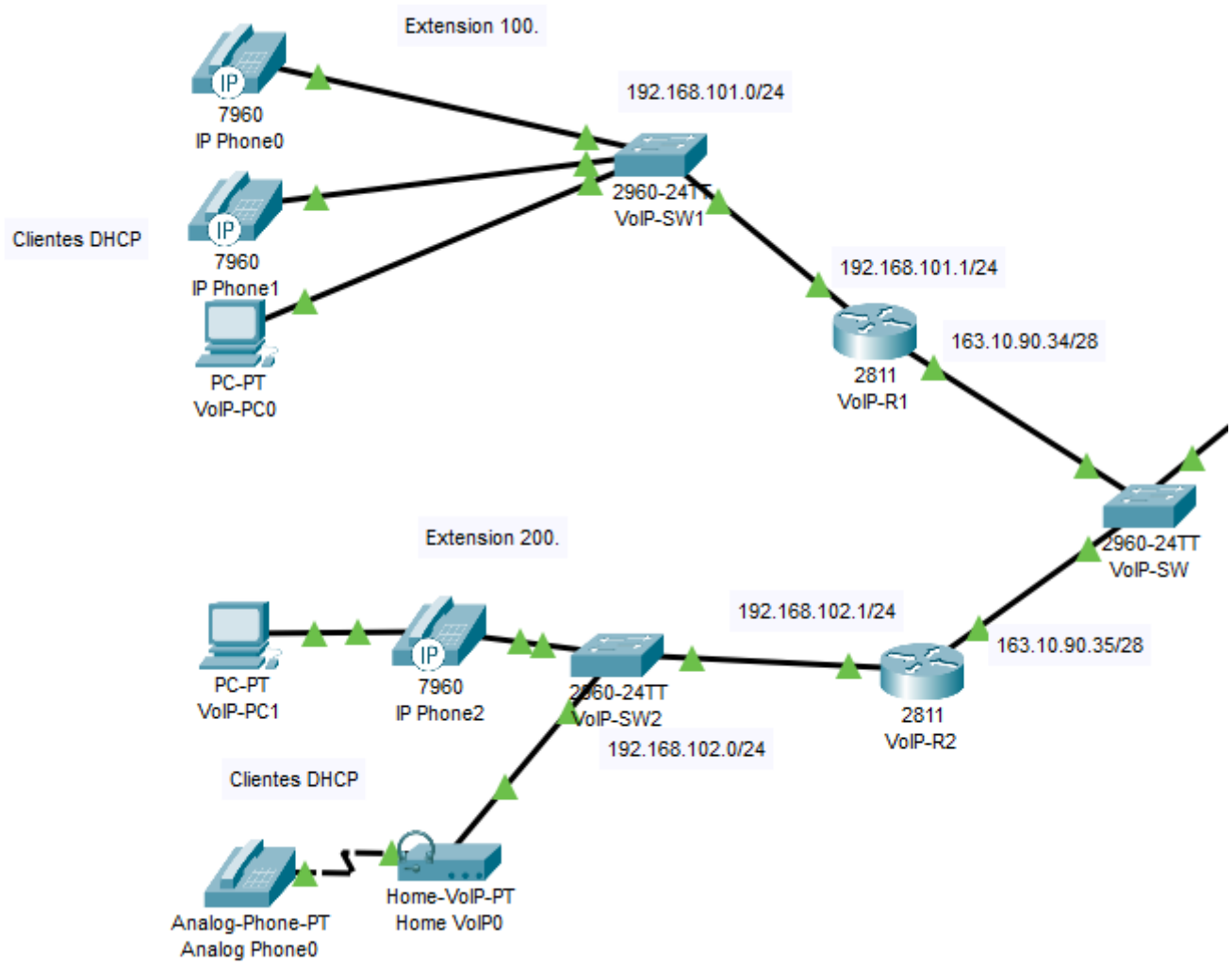
Command	Purpose
show ip dhcp binding	Display address bindings on the DHCP server.

The following example is a sample output of the **show ip dhcp binding** command:

```
Router# show ip dhcp binding

IP address    Hardware address     Lease expiration
10.0.1.60     88:75:56:27:32:01     2000/01/01 17:37:12
```

Config Dial-Peer Cisco



We hace to comunicate this two separated voice networks

- Network 1 have this phone numbers [1000, 1001, 1002]
- Network 2 have this phone numbers [2000, 2001]

To allow the comunication between them do the following:

In the router VoIP-R1

```
VoIP-R1(config)#dial-peer voice 1 voip
VoIP-R1(config-dial-peer)#destination-pattern 200.
VoIP-R1(config-dial-peer)#session ipv4:163.10.90.35
```

In the router VoIP-R2

```
VoIP-R2(config)#dial-peer voice 1 voip
VoIP-R2(config-dial-peer)#destination-pattern 100.
VoIP-R2(config-dial-peer)#session ipv4:163.10.90.34
```

Config RIP protocol CISCO Routers

RIP versions

There are three versions of routing information protocol – RIP Version1, RIP Version2, and RIPng.

RIPv1	RIPv2	RIPng
Sends update as breadcast	Sends update as multicast	Sends update sa multocast
Broadcast at 255.255.255.255	Multicast at 224.0.0.9	Milticast at FF02::9 (RIPng can only run on IPv6 networks)
Doesn't support authentification of updated messages	Supports authentification of RIPv2 update messages	-
Classful routing protocol	Classless protocol updated supports classful	Classless updates are sent

RIP v1 is known as Classful Routing Protocol because it doesn't send information of subnet mask in its routing update. **RIP v2** is known as Classless Routing Protocol because it sends information of subnet mask in its routing update.

> Use debug command to get the details:

```
# debug ip rip
```

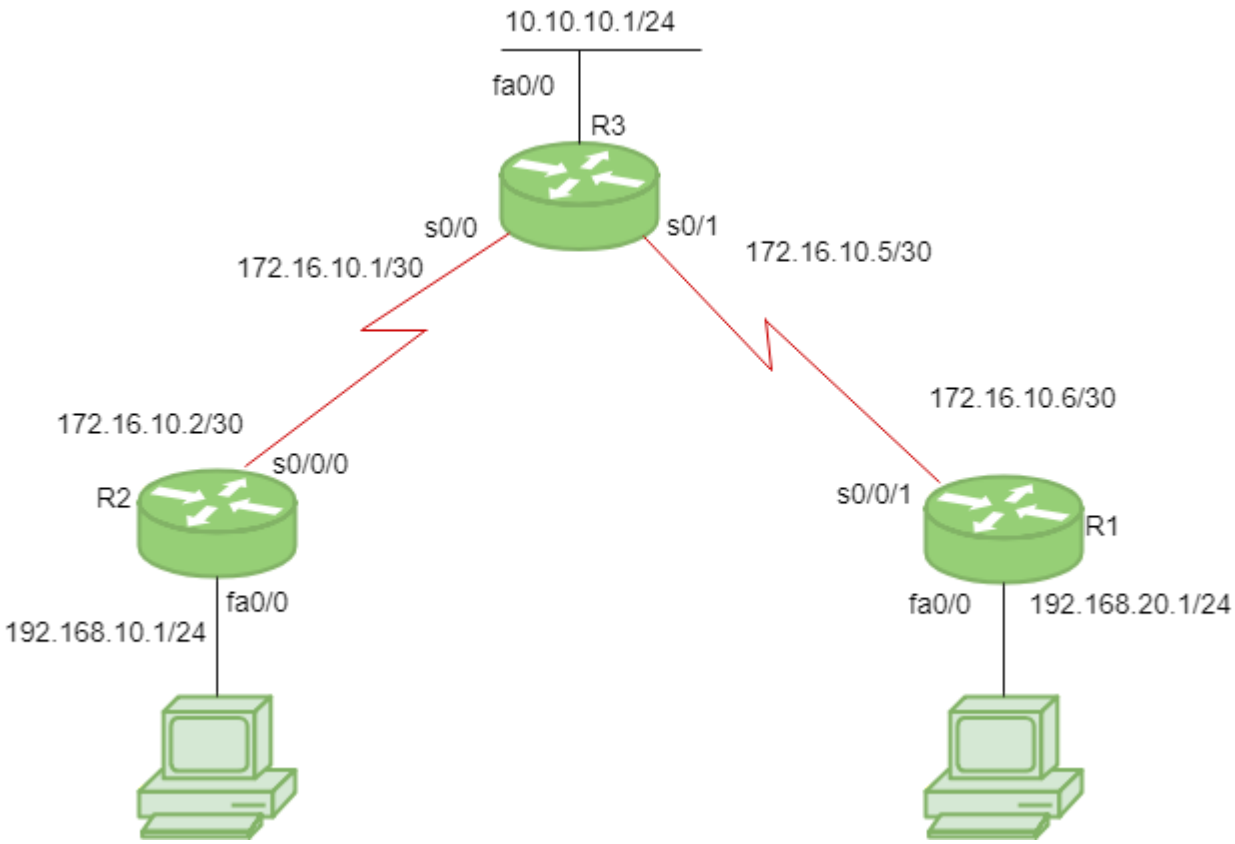
> Use this command to show all routes configured in router, say for router R1:

```
R1# show ip route
```

> Use this command to show all protocols configured in router, say for router R1:

```
R1# show ip protocols
```

Configuration:



Consider the above-given topology which has 3-routers R1, R2, R3. R1 has IP address 172.16.10.6/30 on s0/0/1, 192.168.20.1/24 on fa0/0. R2 has IP address 172.16.10.2/30 on s0/0/0, 192.168.10.1/24 on fa0/0. R3 has IP address 172.16.10.5/30 on s0/1, 172.16.10.1/30 on s0/0, 10.10.10.1/24 on fa0/0.

Configure RIP for R1:

```
R1(config)# router rip
R1(config-router)# network 192.168.20.0
R1(config-router)# network 172.16.10.4
R1(config-router)# version 2
R1(config-router)# no auto-summary
```

> **Note:** no auto-summary command disables the auto-summarisation. If we don't select any auto-summary, then the subnet mask will be considered as classful in Version 1.

Configuring RIP for R2:

```
R2(config)# router rip
R2(config-router)# network 192.168.10.0
R2(config-router)# network 172.16.10.0
R2(config-router)# version 2
R2(config-router)# no auto-summary
```

Similarly, Configure RIP for R3:

```
R3(config)# router rip
R3(config-router)# network 10.10.10.0
R3(config-router)# network 172.16.10.4
R3(config-router)# network 172.16.10.0
R3(config-router)# version 2
R3(config-router)# no auto-summary
```

RIP timers:

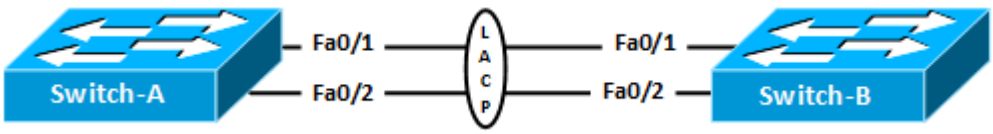
- **Update timer:** The default timing for routing information being exchanged by the routers operating RIP is 30 seconds. Using an Update timer, the routers exchange their routing table periodically.
- **Invalid timer:** If no update comes until 180 seconds, then the destination router considers it invalid. In this scenario, the destination router mark hop counts as 16 for that router.
- **Hold down timer:** This is the time for which the router waits for a neighbor router to respond. If the router isn't able to respond within a given time then it is declared dead. It is 180 seconds by default.
- **Flush time:** It is the time after which the entry of the route will be flushed if it doesn't respond within the flush time. It is 60 seconds by default. This timer starts after the route has been declared invalid and after 60 seconds i.e time will be 180 + 60 = 240 seconds.

> Note that all these times are adjustable. Use this command to change the timers:

```
R1(config-router)#  timers basic
R1(config-router)#  timers basic 20   80    80    90
```

Configure LACP EtherChannel in Cisco IOS Switch

The physical switch ports running LACP protocol can be either in **active** or **passive** mode. In **active mode**, the port actively tries to form LACP EtherChannel with remote switch port. Whereas, in **passive mode**, the port just waits for remote switch port to initiate LACP negotiation. The diagram below shows a simple scenario with two Cisco switches, Switch-A and Switch-B. The switches are connected with two switch ports Fa0/1 and Fa0/2. We can bundle these two switch ports into one logical EtherChannel using Link Aggregation Control Protocol (LACP) protocol. The links between the switches are TRUNKS so we have to **configure TRUNK** in the LACP bundled port as well.



Let's start configuring LACP in Switch-A. It is better to start the configuration after shutting down the switch ports to avoid any negotiation issues while configuring LACP.

```
Switch-A(config)#interface range fastEthernet 0/1 - 2
Switch-A(config-if-range)#channel-group 1 mode active
Switch-A(config-if-range)#channel-protocol lacp
```

The command **channel-group 1 mode active** means the physical interfaces Fa0/1 and Fa0/2 will be member of logical EtherChannel interface **Port-Channel 1** and the physical ports will actively try to negotiate with remote switch ports to form LACP EtherChannel interface. Here is same configuration for Switch-B.

```
Switch-B(config)#interface range fastEthernet 0/1 - 2
Switch-B(config-if-range)#channel-group 1 mode active
Switch-B(config-if-range)#channel-protocol lacp
```

To verify the EtherChannel, type **show etherchannel summary** as shown below.

```
Switch-A#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

1      Po1(SU)           LACP   Fa0/1(P) Fa0/2(P)
```

Above output shows, Port-Channel Po1 has been created, the protocol is LACP and ports Fa0/1 and Fa0/2 are member of the Port-Channel 1 interface. Regarding flags, **Po1(SU)** – S means it is operating at layer 2 and **U** means it is in use. Similarly, flags regarding ports **Fa0/1(P) and Fa0/2(P)** – **P** means these physical ports are member of port-channel 1 (Po1) interface.

You can also verify creation of Port-Channel interface by issuing, **show ip interface brief** command,

```
Switch-A#show ip interface brief | inc Po1
Interface              IP-Address      OK? Method Status                Protocol

Port-channel 1         unassigned      YES unset  up                    up
```

So, Port-Channel interface running LACP protocol has been created. Now, to configure the EtherChannel interface as TRUNK port type following commands as shown below,

```
Switch-A(config)#interface port-channel 1
Switch-A(config-if)#switchport trunk encapsulation dot1q
Switch-A(config-if)#switchport mode trunk
```

Repeat same commands in Switch-B as well.

```
Switch-B(config)#interface port-channel 1
Switch-B(config-if)#switchport trunk encapsulation dot1q
Switch-B(config-if)#switchport mode trunk
```

Review the EtherChannel configuration. Use **show running-config** command in user Exec mode.

```
interface FastEthernet0/1
 channel-protocol lacp
 channel-group 1 mode active
 switchport mode trunk
!
interface FastEthernet0/2
 channel-protocol lacp
 channel-group 1 mode active
 switchport mode trunk
!
interface Port-channel 1
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

You can now verify the TRUNK port using **show interfaces trunk** command as shown below,

```
Switch-A#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1
Fa0/2       on           802.1q         trunking      1
Po1         on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/2       1-1005
Po1         1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,30
Fa0/2       1,10,20,30
Po1         1,10,20,30

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,30
Fa0/2       1,10,20,30
Po1         1,10,20,30
```

As you can see above, **Po1** is trunking with 802.1q protocol. In this way you can configure LACP EtherChannel in Cisco Switch.

Dynamic NAT and PAT overload

Configure the router's inside interface

```
Router(config)#interface fa0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
```

Configure the router's outside interface

```
Router(config)#interface eth0/0/0
Router(config-if)#ip nat outside
Router(config-if)#exit
```

Configure an ACL that has a list of the inside source addresses that will be translated.

```
Router(config)#access-list 1 permit 192.168.0.0 0.0.0.255
```

> NOTE:The access list configured above matches all hosts from the 192.168.0.0/24 subnet.

Configure the pool of global IP addresses

```
Router(config)#ip nat pool MY_POOL 4.4.4.1 4.4.4.5 netmask 255.255.255.0
```

> NOTE: The pool configured above consists of 5 addresses: 4.4.4.1, 4.4.4.2, 4.4.4.3, 4.4.4.4, and 4.4.4.5.

Enable dynamic NAT

```
Router(config)#ip nat inside source list 1 pool MY_POOL
```

To make that with overload (PAT) we have to add `overload` at the end of the command

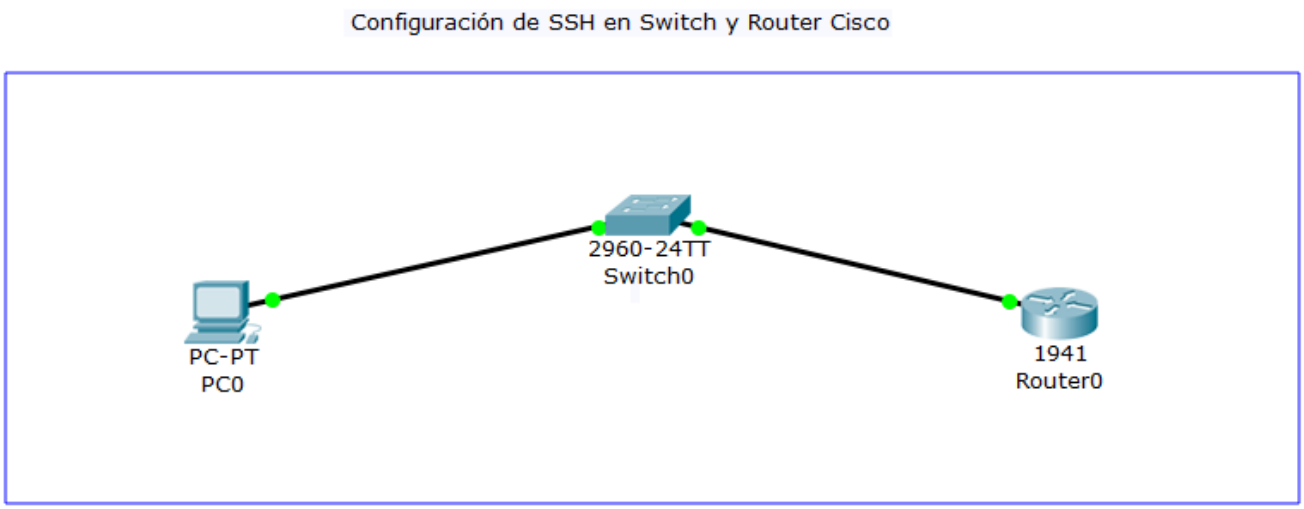
```
Router(config)#ip nat inside source list 1 pool MY_POOL overload
```

> NOTE: The command above instructs the router to translate all addresses specified in the access list 1 to the pool of global addresses called MY_POOL.

Save config

```
do wr
```

Habilitar SSH en Switch Cisco



1. Configuración de IP de administración

```
Switch#conf t
Switch(config)#interface vlan 10
Switch(config-if)#ip address 192.168.10.10 255.255.255.0
Switch(config-if)#no shutdown
```

2. Configuración de default Gateway apuntando al Router

```
Switch(config)#ip default-gateway 192.168.10.1
```

3. Configuración de hostname y nombre de dominio

```
Switch(config)#hostname eclassvirtual-sw
eclassvirtual-sw(config)#ip domain-name eclassvirtual.com
```

4. Generación de llaves RSA

```
eclassvirtual-sw(config)# crypto key generate rsa
```

5. Cambiar SSH versión 1 a la 2 (la versión 2 es más segura)

```
eclassvirtual-sw(config)#ip ssh version 2
```

6. Configuración de Line VTY

```
eclassvirtual-sw(config)# line vty 0 15
eclassvirtual-sw(config-line)# transport input ssh
eclassvirtual-sw(config-line)# login local
```

7. Crear nombre de usuario y password

```
eclassvirtual-sw(config)# username kerjox privilege 15 secret cisco123
```

8. Habilitar enable secret

```
eclassvirtual-sw(config)# enable secret cisco123
```

9. Realizar pruebas de SSH desde el PC

```
C:\>ssh -l eclassvirtual 192.168.10.10 Open Password:
```

10. Revisión de conexión SSH en el Switch

```
eclassvirtual-sw# show ssh
```

Habilitar SSH en Router Cisco

```
Router#conf t
Router(config)#hostname eclassvirtual-router
eclassvirtual-router(config)#interface g0/0
eclassvirtual-router(config-if)#ip address 192.168.0.1 255.255.255.0
eclassvirtual-router(config-if)#no shutdown
eclassvirtual-router(config-if)#exit
eclassvirtual-router(config)#ip domain-name cisco.com
eclassvirtual-router(config)#username eclassvirtual privilege 15 secret cisco123
eclassvirtual-router(config)#crypto key generate rsa
eclassvirtual-router(config)#ip ssh version 2
eclassvirtual-router(config)#enable secret cisco123
eclassvirtual-router(config)#line vty 0 15
eclassvirtual-router(config-line)#transport input ssh
eclassvirtual-router(config-line)#login local
eclassvirtual-router#show ip ssh C:\>ssh -l eclassvirtual 192.168.0.1 Open Password:
```

Packet Tracer 8.1.1 tutorial - IP telephony basic configuration

Last Updated: Tuesday, 22 February 2022 07:32
Published: Sunday, 19 September 2010 12:12
Written by PacketTracerNetwork

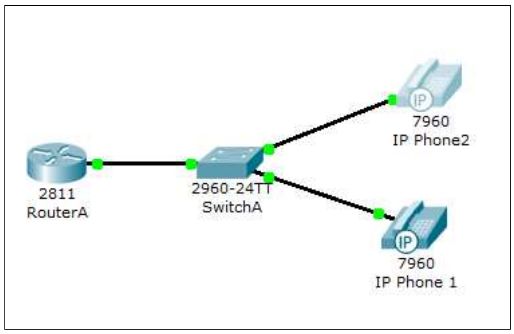
Tutorial description

This tutorial is designed to help you to configure the **voice over ip (voip) features available in Packet Tracer 8.1.1**

It will show you the steps required to :

- Configure Call Manager Express™ on a 2811 router,
- Use the various telephony devices
- Setup dial peers
- Connect Cisco™ IP phones as well as analogue phone on the network.

Network diagram



Note : Connect only IP Phone 1 at the beginning of the lab. IP Phone 2 must be disconnected.

Tasks 1 : Configure interface FastEthernet 0/0 and DHCP server on RouterA (2811 router)

Configure the FastEthernet 0/0 interface with 192.168.10.1/24 ip address. Don't forget to enable the interface with the no shutdown command !

```
RouterA>enable
RouterA#configure terminal
RouterA(config)#interface FastEthernet0/0
RouterA(config-if)#ip address 192.168.10.1 255.255.255.0
RouterA(config-if)#no shutdown
```

The DHCP server is needed to provide each IP phone connected to the network with an IP adress and the TFTP server location.

```
RouterA(config)#ip dhcp pool VOICE #Create DHCP pool named VOICE
RouterA(dhcp-config)#network 192.168.10.0 255.255.255.0 #DHCP network network 192.168.10 with /24 mask#
RouterA(dhcp-config)#default-router 192.168.10.1 #The default router IP address#
RouterA(dhcp-config)#option 150 ip 192.168.10.1 #Mandatory for voip configuration.
```

After configuring the ISR router, wait a moment and check that 'IP Phone 1' has received an IP address by placing your cursor over the phone until a configuration summary appears.

Tasks 2 : Configure the Call Manager Express telephony service on RouterA

You must now configure the Call Manager Express telephony service on RouterA to enable voip on your network.

```
RouterA(config)#telephony-service #Configuring the router for telephony services#
RouterA(config-telephony)#max-dn 5 #Define the maximum number of directory numbers#
RouterA(config-telephony)#max-ephones 5 #Define the maximum number of phones#
RouterA(config-telephony)#ip source-address 192.168.10.1 port 2000 #IP Address source#
RouterA(config-telephony)#auto assign 4 to 6 #Automatically assigning ext numbers to buttons#
RouterA(config-telephony)#auto assign 1 to 5 #Automatically assigning ext numbers to buttons#
```

Task 4 : Configure a voice vlan on SwitchA

Apply the following configuration on SwitchA interfaces. This configuration will separate voice and data traffic in different vlans on SwitchA. data packets will be carried on the access vlan.

```
SwitchA(config)#interface range fa0/1 - 5 #Configure interface range#
SwitchA(config-if-range)#switchport mode access
SwitchA(config-if-range)#switchport voice vlan 1 #Define the VLAN on which voice packets will be handled#
```

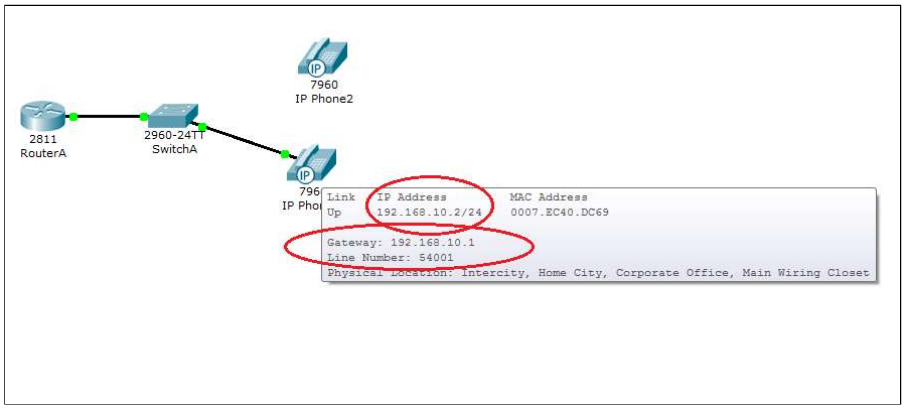
Task 5 : Configure the phone directory for IP Phone 1

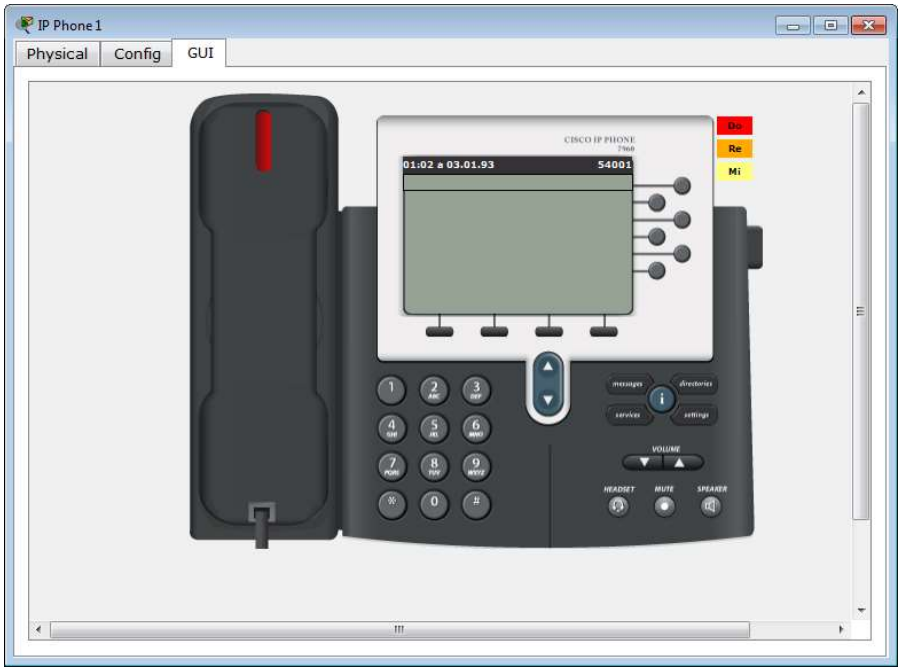
Although 'IP Phone 1' is already connected to SwitchA, it needs additionnal configuration before beeing able to communicate. You need to configure RouterA CME to assign a phone number to this IP phone.

```
RouterA(config)#ephone-dn 1 #Defining the first directory entry#
RouterA(config-ephone-dn)#number 54001 #Assign the phone number to this entry#
```

Task 5 : Verify the configuration

Ensure that the IP Phone receives an IP Address and a the phone number 54001 from RouterA (this can take a short while).





Task 6 : Configure the phone directory for IP Phone 2

Connect IP Phone 2 to SwitchA and power the phone ON using the power adapter (Physical tab).

```
RouterA(config)#ephone-dn 2 #Defining the first directory entry#
RouterA(config-ephone-dn)#number 54002 #Assign the phone number to this entry#
```

Task 7 : Verify the configuration

Ensure that the IP Phone 2 receives an IP Address and a the phone number 54002 from RouterA (this can take a short while). Same procedure as task n°5.

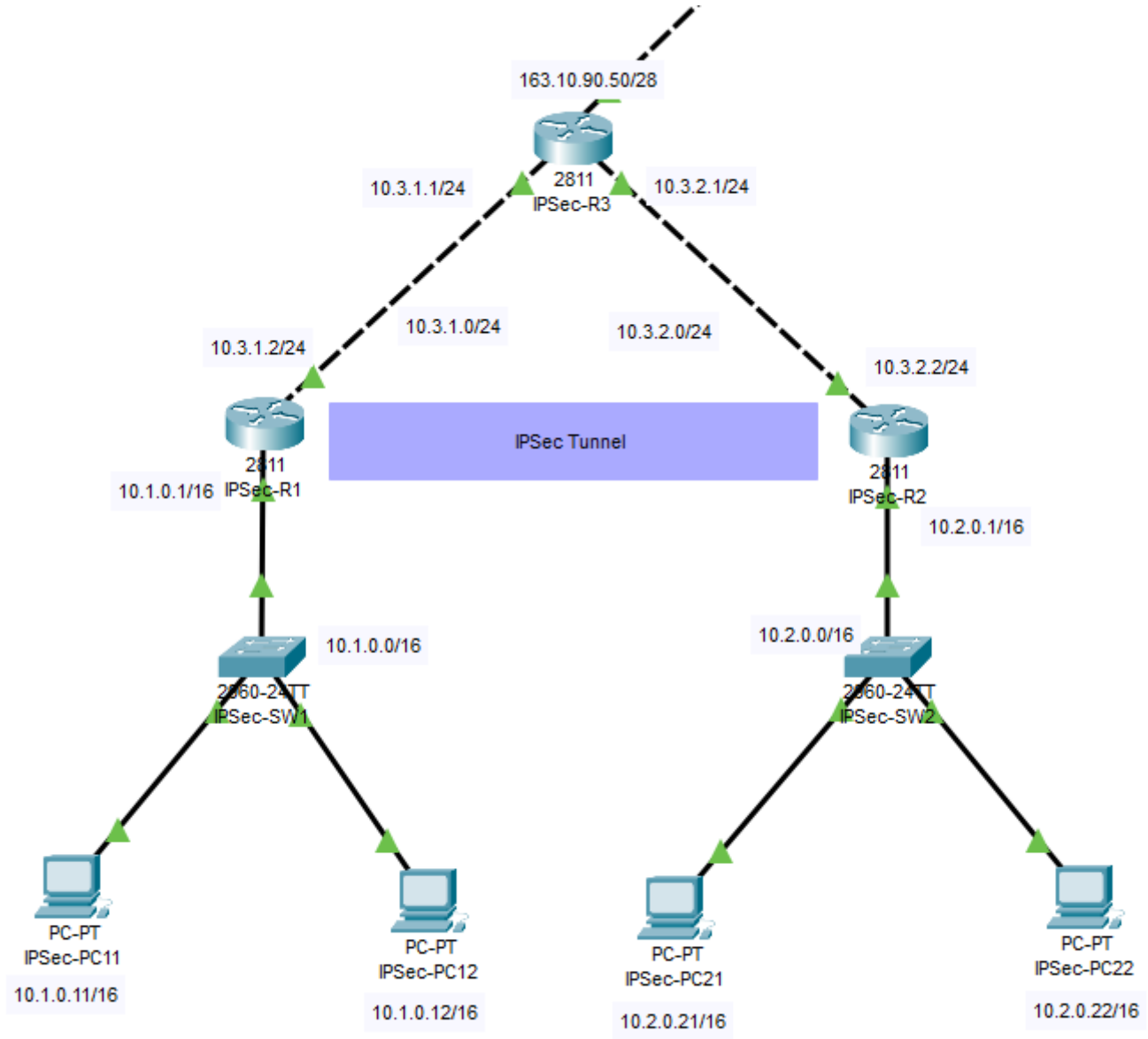
Dial 54001 and check if IP phone 1 correctly receives the call.

IPSec Cisco

Requirements

- You should have conectivity between the two routers you are going to make the tunnel

Configuration



ACL

IPSec-R1

```
R1(config)#access-list 100 permit ip 10.1.0.0 0.0.255.255 10.2.0.0 0.0.255.255
```

IPSec-R2

```
R2(config)#access-list 100 permit ip 10.2.0.0 0.0.255.255 10.1.0.0 0.0.255.255
```

ISAKMP polity (PHASE1) ISAKMP key

IPSec-R1

```
IPSec-R1(config)#crypto osakmp polity 10
                  encryptation aes 256
                  authentication pre-share
                  group 5

IPSec-R1(config)#crypto isakmp key <secret_pass> address 10.3.2.2
```

IPSec-R2

```
IPSec-R2(config)#crypto osakmp polity 10
                  encryptation aes 256
                  authentication pre-share
                  group 5

IPSec-R2(config)#crypto isakmp key <secret_pass> address 10.3.1.2
```

IPSec transform set (PHASE2)

IPSec-R1 & IPSec-R2

```
IPSec-R1(config)#crypto ipsec transform-set <name> esp-aes 256 esp-sha-hmac
```

Crypto map (tie it together)

IPSec-R1

```
IPSec-R1(config)#crypto map <name> 10 ipsec-isakmp
                 set peer 10.3.2.2
                 set pfs group5
                 set security-association lifetime seconds 900
                 set transform-set <name-of-the-transform-set-created-prevoiusly>
                 match address <number-of-access-list-created-previously>
```

IPSec-R2

```
IPSec-R2(config)#crypto map <name> 10 ipsec-isakmp
                 set peer 10.3.1.2
                 set pfs group5
                 set security-association lifetime seconds 900
                 set transform-set <name-of-the-transform-set-created-prevoiusly>
                 match address <number-of-access-list-created-previously>
```

Assign crypto map to WAN interface

IPSec-R1

```
IPSec-R1(config)#interface FastEthernet 0/0
                 crypto map <name-of-the-crypto-map>
```

IPSec-R2

```
IPSec-R2(config)#interface FastEthernet 0/0
                 crypto map <name-of-the-crypto-map>
```

Router on a Stick Cisco 1841

If the router doesnt have an expansion modules of interfaces such as HWIC-4ESW, we need to go this way due to the 2 FastEthernet integrated ports dont suport Trunk and also it meens no VTP.

We need Inter-VLAN routing between clients of the vlans.

Switch Vlans

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/24
11   redA                              active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10
22   redB                              active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20
99   administracion                    active    Fa0/23
100  servidores                        active    Fa0/21, Fa0/22
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Router config

We are going to set up the subinterfaces

```
RouterLab2(config)# int FastEthernet 0/0.11        # 11 because is the vlan 11
(optional) you could put other number
RouterLab2(config-subif)#encapsulation dot1Q 11        # 11 because is the vlan 11
(¡Important!) Here no
RouterLab2(config-subif)#ip address 192.168.11.1 255.255.255.0
```

Repeat the process whit the other vlans

Finally execute the following commands to power on the interface

```
RouterLab2(config)# int FastEthernet 0/0
RouterLab2(config-if)#no shutdown
```

Packet Tracer - Configurar NAT estática

Objetivos

Parte 1: probar el acceso sin NAT

Parte 2: configurar NAT estática

Parte 3: probar el acceso con NAT

Situación

En las redes IPv4 configuradas, los clientes y los servidores utilizan direcciones privadas. Antes de que los paquetes con direccionamiento privado puedan cruzar Internet, deben traducirse a direccionamiento público. Los servidores a los que se puede acceder desde fuera de la organización generalmente tienen asignadas una dirección IP estática pública y una privada. En esta actividad, configurará NAT estática para que los dispositivos externos puedan acceder a un servidor interno en su dirección pública.

Instrucciones

Parte 1: Probar el acceso sin NAT

Paso 1: Intente conectarse a Server1 desde Simulation Mode.

a. Cambiar al modo de simulación.

b. Desde **PC**1 o **L1**, use el navegador web para intentar conectarse a la página web del **Servidor1** en 172.16.16.1. Continúe haciendo clic en el botón **Capturar hacia adelante** , observe cómo los paquetes nunca salen de la nube de Internet. Los intentos deberían fallar.

c. Salga del modo de **simulación**.

d. Desde **PC1**, hacer ping a la interfaz **R1**S0/0/0 (209.165.201.2). El ping debe ser correcto.

Paso 2: Vea la tabla de routing del R1 y la configuración en ejecución.

a. Vea la configuración en ejecución en el **R1**. Observe que no hay comandos que se refieran a NAT. Una forma fácil de confirmar esto es ejecutar el siguiente comando:

```
R1# show run | include name
```

b. Verifique que la tabla de routing no tenga entradas que se refieran a las direcciones IP utilizadas por la **PC1** y la **L1**.

c. Verifique que el **R1** no utilice NAT.

```
R1# show ip nat translations
```

Parte 2: Configurar NAT estática

Paso 1: Configure las instrucciones de NAT estática.

Consulte la topología. Cree una traducción de NAT estática para asignar la dirección interna del **Servidor1** a su dirección externa.

```
R1(config)# ip nat inside source static 172.16.16.1 64.100.50.1
```

Paso 2: Configure las interfaces.

a. Configure la interfaz **G0/**0 como una interfaz interna.

```
R1(config)# interface g0/0
R1(config-if)# ip nat inside
```

b. Configure la interfaz pública s0/0/0 como una interfaz externa.

Parte 3: Probar el acceso con NAT

Paso 1: Verifique la conectividad a la página web de Server1.

a. Abra el símbolo del sistema en la **PC1** o la **L1**, e intente hacer ping a la dirección pública del **Servidor1**. Los pings se deben realizar correctamente.

b. Verifique que tanto la **PC1** como la **L1** ahora puedan acceder a la página web del **Servidor1**.

Paso 2: Vea las NAT.

Utilice los siguientes comandos para verificar la configuración de NAT estática en **R1**:

```
show running-config
show ip nat translations
show ip nat statistics
```