

[Banco de preguntas sobre informática](#)[Lista de comandos de iOS](#)[Libros electrónicos](#)[Calculadoras de IP »](#)[Donaciones](#)[Hogar](#) [CCNA »](#) [Seguridad »](#) [Operaciones cibernéticas »](#)[Banco de preguntas sobre informática](#) [Lista de comandos de iOS](#) [CCNA »](#)[CCNA Seguridad v2.0 »](#) [Ciberseguridad »](#) [Fundamentos de la creación de redes](#)[Calculadoras de subredes IP »](#) [Donación](#) [Contacto](#)

7.4.2 Laboratorio: Implementación de DHCPv4 (Respuestas)

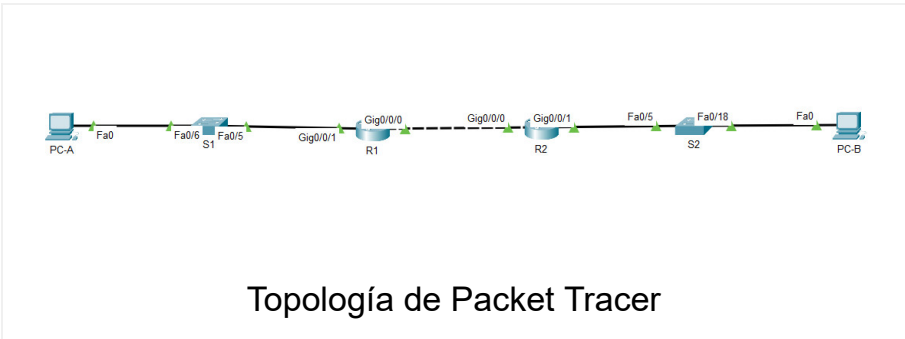
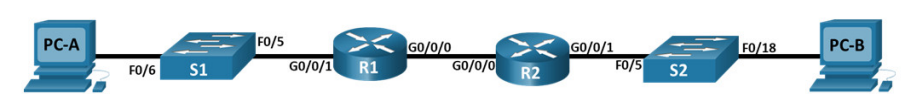
[30 de septiembre de 2020 |](#)[Última actualización: 19 de marzo de 2024 |](#)[Curso CCNA v7 n.º 2 |](#) [6 comentarios](#)

Respuestas del examen CCNA v7.0

[CCNA 1 - versión 7](#)[CCNA 2 - versión 7](#)[CCNA 3 - versión 7](#)[Examen de prueba del sistema](#)[Módulos 1 a 3:
Respuestas del examen
de comunicaciones y
conectividad de red](#)

Laboratorio: Implementación de DHCPv4 (versión para el instructor)

Topología



Topología de Packet Tracer

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de
R1	G0/0/0	10.0.0.1	255.255.2
	G0/0/1	N / A	N / A
	G0/0/1.100	192.168.1.1	255.255.2
	G0/0/1.200	192.168.1.65	255.255.255.224

básica

Módulos 4 a 7:
Respuestas del examen
de conceptos de
Ethernet

Módulos 8 - 10:
Respuestas del examen
de comunicación entre
redes

Módulos 11 a 13:
Respuestas del examen
de direccionamiento IP

Módulos 14 y 15:
Respuestas del examen
de comunicaciones de
aplicaciones de red

Módulos 16 y 17: Cómo
crear y proteger una red
pequeña Respuestas del
examen

[Habilidades de PT]
Práctica de evaluación
de habilidades de PT
(PTSA)

[Habilidades finales]
Examen de habilidades
finales de ITN (PTSA)

Examen final de
práctica de ITNv7

Respuestas del examen
final del curso CCNA 1
v7

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Puerta de enlace
	G0/0/1.1000	N / A	N / A	predeterminada
R2	G0/0/0	10.0.0.2	255.255.255.252	N / A
	G0/0/1	192.168.1.97	255.255.255.240	
S1	VLAN 200	192.168.1.66	255.255.255.224	192.168.1.65
S2	VLAN 1	192.168.1.98	255.255.255.240	192.168.1.97
PC-A	NIC	DHCP	DHCP	DHCP
TARJETA DE CIRCUITO IMPRESO	NIC	DHCP	DHCP	DHCP

Tabla VLAN

VLAN	Nombre	Interfaz asignada
1	N / A	T2: F0/18
100	Clientela	S1: F0/6
200	Gestión	S1: VLAN 200
999	Estacionamiento	S1: F0/1-4, F0/7-24, G0/1-2
1000	Nativo	N / A

Objetivos

- Parte 1: Construir la red y configurar los ajustes básicos del dispositivo
- Parte 2: Configurar y verificar dos servidores

Publicaciones relacionadas

16.1.2 Comprensión de paquetes con rutas estáticas

9.2.4 Comprueba tu comprensión – Respuestas HSRP

11.6.1 Packet Tracer – Configuración de seguridad del conmutador – Instrucciones Respuesta

3.6.1 Packet Tracer: Implementación de VLAN y enlaces troncales (Instrucciones Respuesta)

1.6.2 Packet Tracer: configuración de los parámetros básicos del enrutador: respuestas en modo físico

4.2.8 Laboratorio: Configurar el enrutamiento entre VLAN de Router-on-a-Stick (respuestas)

Plan de estudios de CCNA 2 v7.0: Módulo 15: Enrutamiento estático de IP

8.4.9 Verifique su comprensión: respuestas para configurar el servidor DHCPv6

7.4.4 Módulo de prueba: DHCPv4 (respuestas)

Respuestas del examen CCNA 2 v7 Módulos 7 a 9: Redes disponibles y confiables

Comentarios recientes

Respuestas completas del examen

DHCPv4 en R1

• Parte 3: Configurar y verificar un relé DHCP en R2

Antecedentes / Escenario

El Protocolo de configuración dinámica de host (DHCP) es un protocolo de red que permite a los administradores de red gestionar y automatizar la asignación de direcciones IP. Sin DHCP para IPv4, el administrador debe asignar y configurar manualmente las direcciones IP, los servidores DNS preferidos y las puertas de enlace predeterminadas. A medida que la red aumenta de tamaño, esto se convierte en un problema administrativo cuando los dispositivos se trasladan de una red interna a otra.

En este escenario, la empresa ha crecido en tamaño y los administradores de red ya no pueden asignar direcciones IP a los dispositivos de forma manual. Su trabajo consiste en configurar el enrutador R1 para asignar direcciones IPv4 en dos subredes diferentes.

Nota: Los enrutadores que se utilizan en los laboratorios prácticos de CCNA son Cisco 4221 con Cisco IOS XE versión 16.9.4 (imagen universalk9). Los conmutadores que se utilizan en los laboratorios son Cisco Catalyst 2960s con Cisco IOS versión 15.2(2) (imagen lanbasek9). Se pueden utilizar otros enrutadores, conmutadores y versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y el resultado obtenido pueden variar con respecto a lo que se muestra en los laboratorios. Consulte la tabla de resumen de interfaces de enrutadores que se encuentra al final del laboratorio para conocer los identificadores de interfaz correctos.

Nota: Asegúrese de que los enrutadores y conmutadores se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, comuníquese con su instructor.

Nota para el instructor: consulte el Manual de laboratorio

final de [CCNA 1 v7.0: Introducción a las redes](#)

Uboo en [CCNA 1 v7 Módulos 14 y 15: Respuestas del examen de comunicaciones de aplicaciones de red](#)

[Respuestas completas del examen final](#) de SKA en CCNA 1 v7.0: Introducción a las redes

Ian sobre [6.1.5.3 Packet Tracer: control de dispositivos IoT \(respuestas\) – ITE v7](#)

KelvinLoty en [el laboratorio 129: Configuración de la autenticación WAN](#)



del instructor para conocer los procedimientos para inicializar y recargar dispositivos.

Recursos necesarios

- 2 enrutadores (Cisco 4221 con imagen universal Cisco IOS XE versión 16.9.4 o comparable)
- 2 conmutadores (Cisco 2960 con Cisco IOS versión 15.2(2), imagen lanbasek9 o comparable)
- 2 PC (Windows con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos Cisco IOS a través de los puertos de consola
- Cables Ethernet como se muestra en la topología

Instrucciones

Parte 1: Construir la red y configurar los ajustes básicos del dispositivo

En la Parte 1, configurará la topología de la red y configurará los ajustes básicos en los hosts y conmutadores de PC.

Paso 1: Establecer un esquema de direccionamiento

Subred la red 192.168.1.0/24 para cumplir con los siguientes requisitos:

- a. Una subred, "Subred A", que admite 58 hosts (la VLAN del cliente en R1).

Subred A:

192.168.1.0/26 (.1 -.63)

Registre la primera dirección IP en la tabla de direcciones para R1 G0/0/1.100. Registre la segunda dirección IP en la tabla de direcciones para S1 VLAN 200 e ingrese la puerta de enlace predeterminada asociada.



b. Una subred, “Subred B”, que admite 28 hosts (la VLAN de administración en R1).

Subred B:

192.168.1.64/27 (.65-.95)

Registre la primera dirección IP en la tabla de direcciones para R1 G0/0/1.200. Registre la segunda dirección IP en la tabla de direcciones para S1 VLAN 1 e ingrese la puerta de enlace predeterminada asociada.

c. Una subred, “Subred C”, que admite 12 hosts (la red del cliente en R2).

Subred C:

192.168.1.96/28 (.97-.111)

Registre la primera dirección IP en la tabla de direcciones para R2 G0/0/1.

Paso 2: Conecte la red como se muestra en la topología.

Conecte los dispositivos como se muestra en el diagrama de topología y realice el cableado según sea necesario.

Paso 3: Configure los ajustes básicos para cada enrutador.

a. Asignar un nombre de dispositivo al enrutador.

```
enrutador(config)# nombre de host R1
```

b. Deshabilite la búsqueda de DNS para evitar que el enrutador intente traducir comandos ingresados incorrectamente como si fueran nombres de host.

```
R1(config)# no ip domain-lookup
```

c. Asigne **la clase** como la contraseña cifrada de EXEC



privilegiado.

```
R1(config)# habilitar clase secreta
```

d. Asigne **Cisco** como contraseña de la consola y habilite el inicio de sesión.

```
R1(config)# línea consola 0  
R1(config-line)# contraseña cisco  
R1(config-line)# inicio de sesión
```

e. Asigne **Cisco** como contraseña de VTY y habilite el inicio de sesión.

```
R1(config)# línea vty 0 4  
R1(config-line)# contraseña cisco  
R1(config-line)# inicio de sesión
```

f. Cifrar las contraseñas en texto simple.

```
R1(config)# servicio de cifrado de contrase
```

g. Cree un banner que advierta a cualquier persona que acceda al dispositivo que el acceso no autorizado está prohibido.

```
R1(config)# banner motd $ ¡Solo usuarios au
```

h. Guarde la configuración en ejecución en el archivo de configuración de inicio.

```
R1# copiar configuración-en-ejecución confi
```

i. Configure el reloj del enrutador a la hora y fecha actuales.



Reloj R1# establecido a las 15:30:00 27 de

Nota: Utilice el signo de interrogación (?) para ayudar con la secuencia correcta de parámetros necesarios para ejecutar este comando.

Paso 4: Configurar el enrutamiento entre VLAN en R1

a. Active la interfaz G0/0/1 en el enrutador.

```
R1(config)# interfaz g0/0/1
R1(config-if)# no apagar
R1(config-if)# salir
```

b. Configure subinterfaces para cada VLAN según lo requiera la tabla de direcciones IP. Todas las subinterfaces utilizan encapsulación 802.1Q y se les asigna la primera dirección utilizable del conjunto de direcciones IP que haya calculado. Asegúrese de que la subinterfaz para la VLAN nativa no tenga una dirección IP asignada. Incluya una descripción para cada subinterfaz.

```
R1(config)# interfaz g0/0/1.100
R1(config-subif)# descripción Red de client
R1(config-subif)# encapsulación dot1q 100
R1(config-subif)# dirección IP 192.168.1.1
R1(config-subif)# interfaz g0/0/1.200
R1(config-subif)# encapsulación dot1q 200
R1(config-subif)# descripción Red de admini
R1(config-subif)# dirección IP 192.168.1.65
R1(config-subif)# interfaz g0/0/1.1000
R1(config-subif)# encapsulación dot1q 1000
R1(config-subif)# descripción VLAN nativa
```

c. Verifique que las subinterfaces estén operativas.

```
R1# muestra el resumen de la interfaz IP
¿Dirección IP de la interfaz correcta? Métc
```



```
GigabitEthernet0/0/0 sin asignar SÍ sin cor
GigabitEthernet0/0/1 sin asignar SÍ sin cor
Gi0/0/1.100 192.168.1.1 SI manual arriba a
Gi0/0/1.200 192.168.1.65 SI manual arriba a
Gi0/0/1.1000 sin asignar SÍ sin configurar
```

Paso 5: Configure G0/0/1 en R2, luego G0/0/0 y enrutamiento estático para ambos enrutadores

a. Configure G0/0/1 en R2 con la primera dirección IP de la subred C que calculó anteriormente.

```
R2(config)# interfaz g0/0/1
R2(config-if)# dirección IP 192.168.1.97 255.255.255.0
R2(config-if)# no apagar
R2(config-if)# salir
```

b. Configure la interfaz G0/0/0 para cada enrutador según la tabla de direcciones IP anterior.

```
R1(config)# interfaz g0/0/0
R1(config-if)# dirección IP 10.0.0.1 255.255.255.0
R1(config-if)# no apagar

R2(config)# interfaz g0/0/0
R2(config-if)# dirección IP 10.0.0.2 255.255.255.0
R2(config-if)# no apagar
```

c. Configure una ruta predeterminada en cada enrutador que apunte a la dirección IP de G0/0/0 en el otro enrutador.

```
R1(config)# ruta ip 0.0.0.0 0.0.0.0 10.0.0.2
R2(config)# ruta ip 0.0.0.0 0.0.0.0 10.0.0.1
```

d. Verifique que el enrutamiento estático esté funcionando haciendo ping a la dirección G0/0/1 de R2 desde R1.

```
R1# ping 192.168.1.97
```



e. Guarde la configuración en ejecución en el archivo de configuración de inicio.

```
R1# copiar configuración-en-ejecución confi
```

Paso 6: Configure los ajustes básicos para cada conmutador.

a. Asigne un nombre de dispositivo al conmutador.

```
conmutador(config)# nombre de host S1
```

b. Deshabilite la búsqueda de DNS para evitar que el enrutador intente traducir comandos ingresados incorrectamente como si fueran nombres de host.

```
S1(config)# no ip domain-lookup
```

c. Asigne **la clase** como la contraseña cifrada de EXEC privilegiado.

```
S1(config)# habilitar clase secreta
```

d. Asigne **Cisco** como contraseña de la consola y habilite el inicio de sesión.

```
S1(config)# línea consola 0  
S1(config-line)# contraseña cisco  
S1(config-line)# inicio de sesión
```

e. Asigne **Cisco** como contraseña de VTY y habilite el inicio de sesión.

```
S1(config)# línea vty 0 4  
S1(config-line)# contraseña cisco  
S1(config-line)# inicio de sesión
```



f. Cifrar las contraseñas en texto simple.

```
S1(config)# servicio de cifrado de contrase
```

g. Cree un banner que advierta a cualquier persona que acceda al dispositivo que el acceso no autorizado está prohibido.

```
S1(config)# banner motd $ ¡Solo usuarios au
```

h. Guarde la configuración en ejecución en el archivo de configuración de inicio.

```
S1(config)# exit  
S1# copy configuración-en-ejecución configu
```

i. Ajuste el reloj del interruptor a la hora y fecha actuales.

```
El reloj S1# está configurado a las 15:30:0
```

Nota: Utilice el signo de interrogación (?) para ayudar con la secuencia correcta de parámetros necesarios para ejecutar este comando.

j. Copie la configuración en ejecución a la configuración de inicio.

Paso 7: Crear VLAN en S1.

Nota: S2 solo está configurado con configuraciones básicas.

a. Cree y nombre las VLAN requeridas en el conmutador 1 de la tabla anterior.

```
S1(config)# vlan 100  
S1(config-vlan)# nombre Clientes  
S1(config-vlan)# vlan 200  
S1(config-vlan)# nombre Administración
```



```
S1(config-vlan)# vlan 999  
S1(config-vlan)# nombre Estacionamiento  
S1(config-vlan)# vlan 1000  
S1(config-vlan)# nombre Nativo  
S1(config-vlan)# salir
```

b. Configure y active la interfaz de administración en S1 (VLAN 200) utilizando la segunda dirección IP de la subred calculada anteriormente. Además, configure la puerta de enlace predeterminada en S1.

```
S1(config)# interfaz vlan 200  
S1(config-if)# dirección ip 192.168.1.66 255.255.255.0  
S1(config-if)# no apagar  
S1(config-if)# salir  
S1(config)# puerta de enlace ip predeterminada 192.168.1.66
```

c. Configure y active la interfaz de administración en S2 (VLAN 1) utilizando la segunda dirección IP de la subred calculada anteriormente. Además, configure la puerta de enlace predeterminada en S2

```
S2(config)# interface vlan 1  
S2(config-if)# ip address 192.168.1.98 255.255.255.0  
S2(config-if)# no shutdown  
S2(config-if)# exit  
S2(config)# ip default-gateway 192.168.1.97
```

d. Assign all unused ports on S1 to the Parking_Lot VLAN, configure them for static access mode, and administratively deactivate them. On S2, administratively deactivate all the unused ports.

Note: The interface range command is helpful to accomplish this task with as few commands as necessary.

```
S1(config)# interface range f0/1 - 4, f0/7 - 10  
S1(config-if-range)# switchport mode access  
S1(config-if-range)# switchport access vlan 999
```



```
S1(config-if-range)# shutdown
S1(config-if-range)# exit
```

```
S2(config)# interface range f0/1 - 4, f0/6
S2(config-if-range)# switchport mode access
S2(config-if-range)# shutdown
S2(config-if-range)# exit
```

Step 8: Assign VLANs to the correct switch interfaces.

a. Assign used ports to the appropriate VLAN (specified in the VLAN table above) and configure them for static access mode.

```
S1(config)# interface f0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 100
```

b. Verify that the VLANs are assigned to the correct interfaces.

```
S1# show vlan brief
```

VLAN	Name	Status
1	default	active
100	Clients	active
200	Management	active
999	Parking_Lot	active
1000	Native	active
1002	fddi-default	active
1003	token-ring-default	active
1004	fddinet-default	active
1005	trnet-default	active



Why is interface F0/5 listed under VLAN 1?

Port 5 is in the default VLAN and has not been configured as an 802.1Q trunk.

Step 9: Manually configure S1's interface F0/5 as an 802.1Q trunk.

a. Change the switchport mode on the interface to force trunking.

```
S1(config)# interface f0/5
S1(config-if)# switchport mode trunk
```

b. Como parte de la configuración troncal, configure la VLAN nativa en 1000.

```
S1(config-if-range)# switchport trunk native 1000
```

c. Como otra parte de la configuración troncal, especifique que las VLAN 100, 200 y 1000 pueden cruzar el enlace troncal.

```
S1(config-if-range)# switchport trunk permitted vlan 100,200,1000
```

d. Guarde la configuración en ejecución en el archivo de configuración de inicio.

```
S1(config)# exit
S1# copy configuración-en-ejecución configuración-inicial
```

e. Verificar el estado del trunking.

```
S1# mostrar interfaces troncales
```

```
Estado de encapsulación del modo de puerto
Fa0/5 en trunking 802.1q 1000
```

```
Puertos VLAN permitidos en el trunk
```



```
Fa0/5 100,200,1000
```

```
Vlan de puerto permitidas y activas en el c
Fa0/5 100,200,1000
```

```
Puertos VLAN en estado de reenvío de árbol
Fa0/5 100,200,1000
```

En este punto, ¿qué dirección IP tendrían las PC si estuvieran conectadas a la red mediante DHCP?

Se autoconfigurarían con una dirección IP privada automática (APIPA) en el rango 169.254.xx.

Parte 2: Configurar y verificar dos servidores DHCPv4 en R1

En la Parte 2, configurará y verificará un servidor DHCPv4 en R1. El servidor DHCPv4 prestará servicio a dos subredes: la subred A y la subred C.

Paso 1: Configurar R1 con grupos de DHCPv4 para las dos subredes admitidas. A continuación, se proporciona solo el grupo de DHCP para la subred A

a. Excluya las primeras cinco direcciones utilizables de cada grupo de direcciones.

```
R1(config)# ip dhcp dirección excluida 192.
```

b. Cree el grupo DHCP (utilice un nombre único para cada grupo).

```
R1(config)# grupo de direcciones dhcp ip R1
```

c. Especifique la red que este servidor DHCP admite.

```
R1(dhcp-config)# red 192.168.1.0 255.255.25
```



d. Configure el nombre de dominio como ccna-lab.com

```
R1(dhcp-config) # nombre-de-dominio ccna-lab.com
```

e. Configure la puerta de enlace predeterminada adecuada para cada grupo de DHCP.

```
R1(dhcp-config) # enrutador predeterminado 192.168.1.1
```

f. Configure el tiempo de arrendamiento por 2 días, 12 horas y 30 minutos.

```
R1(dhcp-config) # arrendamiento 2 12 30
```

El software Packet Tracer no admite todos los comandos y funciones de IOS.

g. A continuación, configure el segundo grupo DHCPv4 utilizando el nombre de grupo R2_Client_LAN y la red calculada, enrutador predeterminado, y utilice el mismo nombre de dominio y tiempo de concesión del grupo DHCP anterior.

```
R1(config) # ip dhcp dirección-excluida 192.168.1.1  
R1(config) # ip dhcp pool R2_Client_LAN  
R1(dhcp-config) # red 192.168.1.96 255.255.255.240  
R1(dhcp-config) # enrutador-predeterminado 192.168.1.1  
R1(dhcp-config) # nombre-dominio ccna-lab.com  
R1(dhcp-config) # arrendamiento 2 12 30
```



Paso 2: Guarda tu configuración

Guarde la configuración en ejecución en el archivo de configuración de inicio.

R1# **copiar configuración-en-ejecución confi**

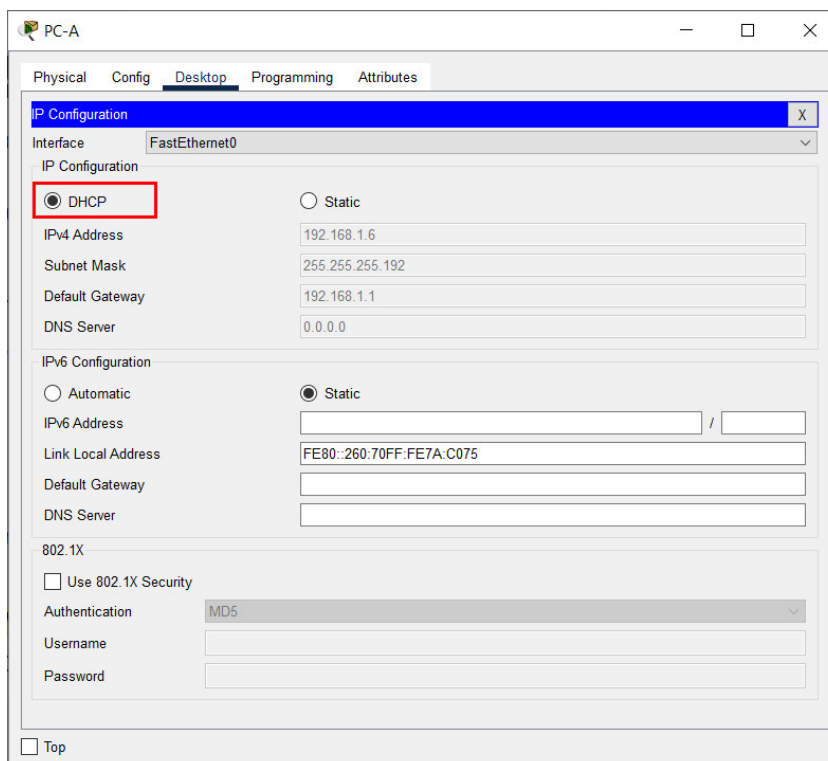
Paso 3: Verifique la configuración del servidor DHCPv4

- Emita el comando **show ip dhcp pool** para examinar los detalles del pool.
- Emita el comando **show ip dhcp bindings** para examinar las asignaciones de direcciones DHCP establecidas.
- Emita el comando **show ip dhcp server statistics** para examinar los mensajes DHCP.

Paso 4: Intente adquirir una dirección IP de DHCP en PC-A

- Abra un símbolo del sistema en la PC-A y emita el comando **ipconfig /renew**.

Packet Tracer: configura el host PC-A para recibir su dirección IP de un servidor DHCP.



- b. Una vez completado el proceso de renovación, emita el comando **ipconfig** para ver la nueva información de IP.
- c. Pruebe la conectividad haciendo ping a la dirección IP de la interfaz G0/0/1 de R1.

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Parte 3: Configurar y verificar un relé DHCP en R2

En la Parte 3, configurará R2 para retransmitir solicitudes DHCP desde la red de área local en la interfaz G0/0/1 al servidor DHCP (R1).

Paso 1: Configurar R2 como agente de retransmisión DHCP para la LAN en G0/0/1

- a. Configure el comando **ip helper-address** en G0/0/1 especificando la dirección IP G0/0/0 de R1.

```
R2(config)# interfaz g0/0/1
R2(config-if)# dirección-ip-auxiliar 10.0.0.1
```

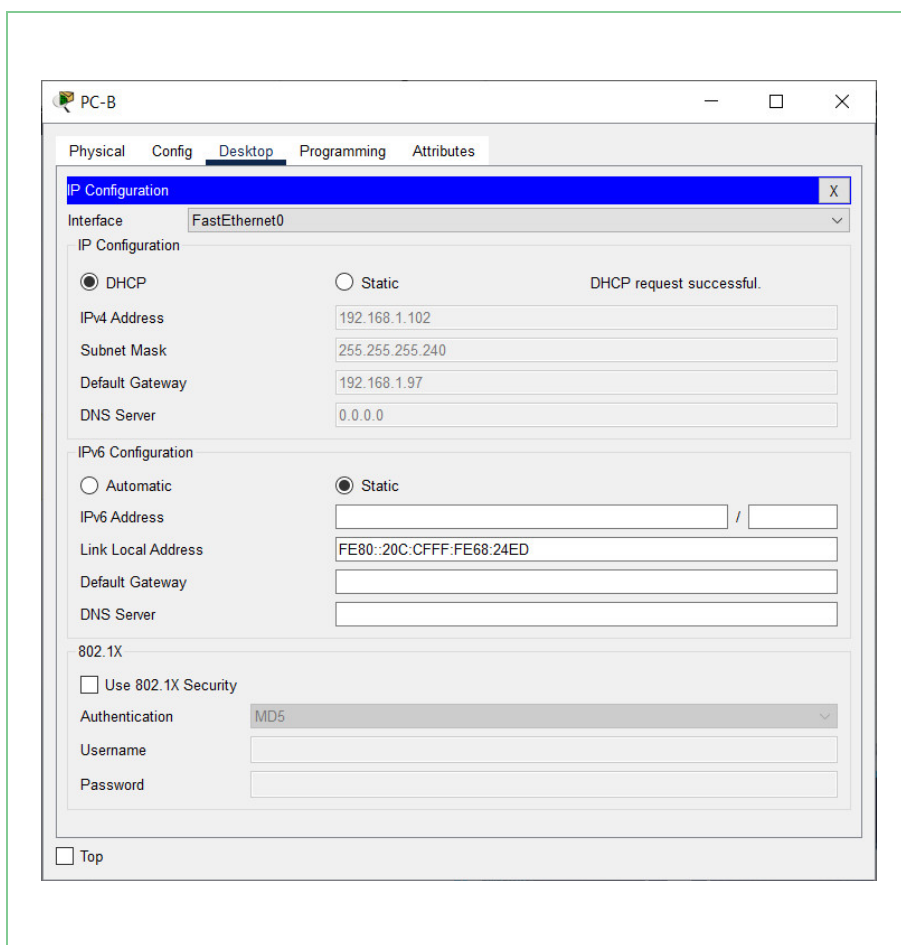
- b. Guarde su configuración.

```
R2(config-if)# fin
R2# wr
```

Paso 2: Intente adquirir una dirección IP de DHCP en PC-B

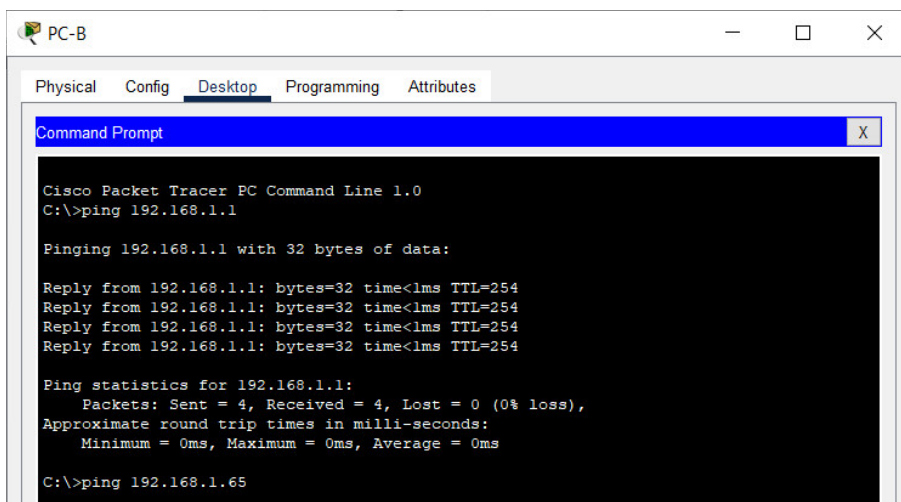


a. Abra un símbolo del sistema en PC-B y emita el comando **ipconfig /renew** .



b. Una vez completado el proceso de renovación, emita el comando **ipconfig** para ver la nueva información de IP.

c. Pruebe la conectividad haciendo ping a la dirección IP de la interfaz G0/0/1 de R1.



```
Pinging 192.168.1.65 with 32 bytes of data:

Reply from 192.168.1.65: bytes=32 time<1ms TTL=254
Reply from 192.168.1.65: bytes=32 time<1ms TTL=254
Reply from 192.168.1.65: bytes=32 time<1ms TTL=254
Reply from 192.168.1.65: bytes=32 time<1ms TTL=254

Ping statistics for 192.168.1.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

☐ Top

d. Emita el **comando show ip dhcp binding** en R1 para verificar los enlaces DHCP.

e. Emita el comando **show ip dhcp server statistics** en R1 y R2 para verificar los mensajes DHCP.

Configuraciones del dispositivo – Final

Interruptor S1

S1# **mostrar ejecución**

Configuración del edificio...

Configuración actual: 3194 bytes

!

versión 15.2

Sin almohadilla de servicio

Servicio de marcas de tiempo de depuración

Servicio de marcas de tiempo de registro de
servicio de cifrado de contraseñas

!

nombre de host S1

!

marcador de inicio de arranque

marcador de fin de bota

!

habilitar secreto 5 \$1\$b/Df\$ndTHDMqOPLb0hgz

!

No aaa nuevo modelo

enrutamiento mtu del sistema 1500

!

!



```
No hay búsqueda de dominio IP
!
!
modo de árbol de expansión rapid-pvst
árbol de expansión extiende el id del siste
!
Política de asignación interna de VLAN asce
!
!
Interfaz FastEthernet0/1
Acceso al puerto de conmutación VLAN 999
Acceso al modo switchport
cerrar
!
Interfaz FastEthernet0/2
Acceso al puerto de conmutación VLAN 999
Acceso al modo switchport
cerrar
!
Interfaz FastEthernet0/3
Acceso al puerto de conmutación VLAN 999
Acceso al modo switchport
cerrar
!
Interfaz FastEthernet0/4
Acceso al puerto de conmutación VLAN 999
Acceso al modo switchport
cerrar
!
Interfaz FastEthernet0/5
El enlace troncal switchport permite VLAN
VLAN nativa del puerto troncal del switchp
modo switchport trunk
!
Interfaz FastEthernet0/6
Acceso al puerto de conmutación VLAN 100
Acceso al modo switchport
!
Interfaz FastEthernet0/7
Acceso al puerto de conmutación VLAN 999
Acceso al modo switchport
cerrar
!
```



```
Interfaz FastEthernet0/8
Acceso al puerto de conmutación VLAN 999
Acceso al modo switchport
cerrar
!
Interfaz FastEthernet0/9
Acceso al puerto de conmutación VLAN 999
Acceso al modo switchport
cerrar
!
Interfaz FastEthernet0/10
Acceso al puerto de conmutación VLAN 999
Acceso al modo switchport
cerrar
!
Interfaz FastEthernet0/11
Acceso al puerto de conmutación VLAN 999
Acceso al modo switchport
cerrar
!
Interfaz FastEthernet0/12
Acceso al puerto de conmutación VLAN 999
Acceso al modo switchport
cerrar
!
interface FastEthernet0/13
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/14
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/15
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/16
switchport access vlan 999
switchport mode access
```



```
shutdown
!
interface FastEthernet0/17
  switchport access vlan 999
  switchport mode access
  shutdown
!
interface FastEthernet0/18
  switchport access vlan 999
  switchport mode access
  shutdown
!
interface FastEthernet0/19
  switchport access vlan 999
  switchport mode access
  shutdown
!
interface FastEthernet0/20
  switchport access vlan 999
  switchport mode access
  shutdown
!
interface FastEthernet0/21
  switchport access vlan 999
  switchport mode access
  shutdown
!
interface FastEthernet0/22
  switchport access vlan 999
  switchport mode access
  shutdown
!
interface FastEthernet0/23
  switchport access vlan 999
  switchport mode access
  shutdown
!
interface FastEthernet0/24
  switchport access vlan 999
  switchport mode access
  shutdown
!
interface GigabitEthernet0/1
```



```
switchport access vlan 999
switchport mode access
shutdown
!
interface GigabitEthernet0/2
switchport access vlan 999
switchport mode access
shutdown
!
interface Vlan1
no ip address
shutdown
!
interface Vlan200
ip address 192.168.1.66 255.255.255.224

ip default-gateway 192.168.1.65
!
ip http server
ip http secure-server
!
banner motd ^C Authorized Users Only! ^C
!
line con 0
password 7 060506324F41
login
line vty 0 4
password 7 060506324F41
login
line vty 5 15
login
!
vlan 100
name Clients
vlan 200
name Management
vlan 999
name Parking_Lot
vlan 1000
name Native
exit
!
end
```



Switch S2

```
S2# show run
```

```
Building configuration...
```

```
Current configuration : 2323 bytes
```

```
!
```

```
version 15.2
```

```
no service pad
```

```
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
```

```
service password-encryption
```

```
!
```

```
hostname S2
```

```
!
```

```
boot-start-marker
```

```
boot-end-marker
```

```
!
```

```
enable secret 5 $1$86v.$3mG1aMq7hcn2P0ZDNa2
```

```
!
```

```
no aaa new-model
```

```
system mtu routing 1500
```

```
!
```

```
!
```

```
no ip domain-lookup
```

```
!
```

```
!
```

```
spanning-tree mode rapid-pvst
```

```
spanning-tree extend system-id
```

```
!
```

```
vlan internal allocation policy ascending
```

```
!
```

```
!
```

```
interface FastEthernet0/1
```

```
    switchport mode access
```

```
    shutdown
```

```
!
```

```
interface FastEthernet0/2
```

```
    switchport mode access
```

```
    shutdown
```

```
!
```

```
interface FastEthernet0/3
```



```
switchport mode access
shutdown
!
interface FastEthernet0/4
switchport mode access
shutdown
!
interface FastEthernet0/5
!
interface FastEthernet0/6
switchport mode access
shutdown
!
interface FastEthernet0/7
switchport mode access
shutdown
!
interface FastEthernet0/8
switchport mode access
shutdown
!
interface FastEthernet0/9
switchport mode access
shutdown
!
interface FastEthernet0/10
switchport mode access
shutdown
!
interface FastEthernet0/11
switchport mode access
shutdown
!
interface FastEthernet0/12
switchport mode access
shutdown
!
interface FastEthernet0/13
switchport mode access
shutdown
!
interface FastEthernet0/14
switchport mode access
```



```
shutdown
!
interface FastEthernet0/15
  switchport mode access
  shutdown
!
interface FastEthernet0/16
  switchport mode access
  shutdown
!
interface FastEthernet0/17
  switchport mode access
  shutdown
!
interface FastEthernet0/18
!
interface FastEthernet0/19
  switchport mode access
  shutdown
!
interface FastEthernet0/20
  switchport mode access
  shutdown
!
interface FastEthernet0/21
  switchport mode access
  shutdown
!
interface FastEthernet0/22
  switchport mode access
  shutdown
!
interface FastEthernet0/23
  switchport mode access
  shutdown
!
interface FastEthernet0/24
  switchport mode access
  shutdown
!
interface GigabitEthernet0/1
  switchport mode access
  shutdown
```



```
!  
interface GigabitEthernet0/2  
  switchport mode access  
  shutdown  
!  
interface Vlan1  
  ip address 192.168.1.98 255.255.255.240  
!  
ip default-gateway 192.168.1.97  
ip http server  
ip http secure-server  
!  
banner motd ^C Authorized Users Only! ^C  
!  
line con 0  
  password 7 045802150C2E  
  login  
line vty 0 4  
  password 7 045802150C2E  
  login  
line vty 5 15  
  login  
!  
end
```

Router R1

```
R1# show run  
Building configuration...  
  
Current configuration : 2225 bytes  
!  
version 16.9  
service timestamps debug datetime msec  
service timestamps log datetime msec  
service password-encryption  
no platform punt-keepalive disable-kernel-c  
!  
hostname R1  
!  
boot-start-marker
```



```
boot-end-marker
!
!
vrf definition Mgmt-intf
!
  address-family ipv4
  exit-address-family
!
  address-family ipv6
  exit-address-family
!
enable secret 5 $1$lzpq$ribRztM6WUv/dsnQ7x2
!
no aaa new-model
!
!
no ip domain-lookup
ip dhcp excluded-address 192.168.1.1 192.168.1.96
ip dhcp excluded-address 192.168.1.97 192.168.1.254
!
ip dhcp pool R1_Client_LAN
  network 192.168.1.0 255.255.255.192
  domain-name ccna-lab.com
  default-router 192.168.1.1
  lease 2 12 30
!
ip dhcp pool R2_Client_LAN
  network 192.168.1.96 255.255.255.240
  default-router 192.168.1.97
  domain-name ccna-lab.com
  lease 2 12 30
!
!
subscriber templating
!
multilink bundle-name authenticated
!
spanning-tree extend system-id
!
!
redundancy
  mode none
!
```



```
!  
interface GigabitEthernet0/0/0  
ip address 10.0.0.1 255.255.255.252  
negotiation auto  
!  
interface GigabitEthernet0/0/1  
no ip address  
negotiation auto  
!  
interface GigabitEthernet0/0/1.100  
description Connected to Client Network  
encapsulation dot1Q 100  
ip address 192.168.1.1 255.255.255.192  
!  
interface GigabitEthernet0/0/1.200  
description Connected to Management Networ  
encapsulation dot1Q 200  
ip address 192.168.1.65 255.255.255.224  
!  
interface GigabitEthernet0/0/1.1000  
description Connected to Native VLAN  
encapsulation dot1Q 1000 native  
!  
interface Serial0/1/0  
!  
interface Serial0/1/1  
!  
Interfaz GigabitEthernet0  
Gestión de reenvío de VRF-intf  
Sin dirección IP  
cerrar  
negociación automática  
!  
protocolo de reenvío de IP nd  
Sin servidor IP http  
Sin IP http servidor seguro  
interfaz de origen tftp ip GigabitEthernet(  
ruta ip 0.0.0.0 0.0.0.0 10.0.0.2  
!  
!  
plano de control  
!  
banner motd ^C ;Solo usuarios autorizados!
```



```
!  
línea con 0  
  contraseña 7 01100F175804  
  acceso  
  bits de parada 1  
línea auxiliar 0  
  bits de parada 1  
línea vty 0 4  
  contraseña 7 02050D480809  
  acceso  
!  
fin
```

Enrutador R2

R2# **mostrar ejecución**

Configuración del edificio...

Configuración actual: 1501 bytes

!

versión 16.9

Servicio de marcas de tiempo de depuración

Servicio de marcas de tiempo de registro de

servicio de cifrado de contraseñas

Sin plataforma punt-keepalive deshabilitar-

!

nombre de host R2

!

marcador de inicio de arranque

marcador de fin de bota

!

!

Definición de VRF Mgmt-intf

!

familia de direcciones ipv4

dirección de salida de la familia

!

familia de direcciones ipv6

dirección de salida de la familia

!

habilitar secreto 5 \$1\$swCy\$LDg9k0nMAN5Cxn9

!



```
No aaa nuevo modelo
!
No hay búsqueda de dominio IP
!
!
Plantillas de suscriptores
!
nombre de paquete multitenlace autenticado
!
árbol de expansión extiende el id del sistema
!
!
redundancia
    modo ninguno
!
!
Interfaz GigabitEthernet0/0/0
dirección ip 10.0.0.2 255.255.255.252
    negociación automática
!
Interfaz GigabitEthernet0/0/1
    dirección ip 192.168.1.97 255.255.255.240
    dirección de ayuda ip 10.0.0.1
negociación automática
!
Interfaz Serial0/1/0
!
Interfaz Serial0/1/1
!
Interfaz GigabitEthernet0
    Gestión de reenvío de VRF-intf
    Sin dirección IP
    cerrar
    negociación automática
!
protocolo de reenvío de IP nd
Sin servidor IP http
Sin IP http servidor seguro
interfaz de origen tftp ip GigabitEthernet0/0/0
ruta ip 0.0.0.0 0.0.0.0 10.0.0.1
!
!
plano de control
```




```
!  
banner motd ^C ;Solo usuarios autorizados!  
!  
línea con 0  
    contraseña 7 05080F1C2243  
    acceso  
    bits de parada 1  
línea auxiliar 0  
    bits de parada 1  
línea vty 0 4  
    contraseña 7 104D000A0618  
    acceso  
!  
fin
```

Descargar archivo PDF y PKT Completado

100% Puntuación:



[7.4.2 Packet Tracer -
Laboratorio: Implementación de
DHCPv4](#)

1 archivo(s) 283,65 KB

Descargar

← Artículo anterior

**6.4.2 Laboratorio:
Implementación de
Etherchannel
(Respuestas)**

Siguiente artículo →

**8.5.1 Laboratorio:
Configurar DHCPv6
(Respuestas)**



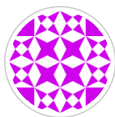
Suscribir



Join the discussion

B *I* U         

6 COMENTARIOS



Adrián  Hace 1 mes

Hay un problema si usas isr 2321, todos los comandos no funcionan y dan como resultado una falla.

 Responder



latchumy  Hace 9 meses

bien

 Responder



nadie importante  Hace 2 años

Para aquellos que tienen dificultades como yo, Packet Tracer no admite algunos comandos DHCP y deberán negociar esto con su profesor o utilizar GNS3 para realizar esta tarea.

 Responder



Yassine  Hace 2 años

No puedo descargar archivos PDF y PKT, ¿podría ayudarme señor?

 Responder





Javinder  Hace 3 años

¿¿¿dónde está mi descarga????!!

 Responder



Mohamed Harún  Hace 4 años

¡Excelente!

 Responder

Derechos de autor de [ITExamAnswers.net](https://itexamanswers.net) © 2025.

[política de privacidad](#)

[Contacto](#)

