Universidad Estatal a Distancia

Vicerrectoría Académica

Escuela De Ciencias Exactas y Naturales

Carrera de Bachillerato en Ingeniería Informática

Asignatura: Telemática y redes II

Código: 3076

Tarea #2

Estudiante:

Francisco Campos Sandi

114750560

Sede: San Vito

Grupo 04

Tutor: Mauricio Montoya Huertas

I Cuatrimestre 2025

**Contenido**

[Introducción 4](#_Toc192444148)

[Desarrollo 5](#_Toc192444149)

[Parte 1: Armado de la red y configuración 5](#_Toc192444150)

[Paso 1: Establecer el esquema de direccionamiento 5](#_Toc192444151)

[Tabla 1 Direccionamiento 6](#_Toc192444152)

[Tabla 2 VLAN 6](#_Toc192444153)

[Paso 2: Configuración de los parámetros básicos para cada router 7](#_Toc192444154)

[Paso 3: Configurar la interfaz f0/0 en el router R1 y las subinterfaces 8](#_Toc192444155)

[Paso 4: Configurarse en el R2 la f0/0, luego s0/0 y utilizar el protocolo de enrutamiento 9](#_Toc192444156)

[EIGRP para ambos router 9](#_Toc192444157)

[Paso 5: Configurar los básicos en cada switch 10](#_Toc192444158)

[Paso 6: Crear VLAN en el S1 11](#_Toc192444159)

[Paso 7: Asignación de las VLANs a las interfaces del switch 13](#_Toc192444160)

[Paso 8: Configuración de la interfaz e0 del switch S1 como enlace troncal 802.1Q 14](#_Toc192444161)

[Parte 2: Configuración y verificación de los servidores DHCPv4 en el router R1 15](#_Toc192444162)

[Paso 1: Configurar en R1 con grupos de DHCPv4 para las dos subredes. Sólo se configura con el protocolo DHCPv4 la subred A tomando los datos de la Parte 1 Paso 15](#_Toc192444163)

[Paso 2: Comprobación del servidor DHCPv4 16](#_Toc192444164)

[Paso 3: Configurar una dirección IP de DHCP en la PC-A 17](#_Toc192444165)

[Parte 3: Configuración y verificación de una retransmisión del DHCPv4 en el router R2 19](#_Toc192444166)

[Paso 1: Configurar R2 como agente de retransmisión DHCPv4 para la LAN en f0/0 19](#_Toc192444167)

[Paso 2: Intento de adquirir una dirección IP de DHCPv4 en PC-B 19](#_Toc192444168)

[Link del video 22](#_Toc192444169)

[https://youtu.be/KDUKEEu1LKM 22](#_Toc192444170)

[Script completo de cada Router 22](#_Toc192444171)

[Script completo de cada Switch 24](#_Toc192444172)

[Conclusión 27](#_Toc192444173)

[Referencias 28](#_Toc192444174)

**Tabla de ilustraciones**

[Ilustración 1 Topología tarea 2 5](#_Toc192444175)

[Ilustración 2 subinterfaces operativas 9](#_Toc192444176)

[Ilustración 3 ping de router a router 10](#_Toc192444177)

[Ilustración 4 VLANs estén asignadas a las interfaces 13](#_Toc192444178)

[Ilustración 5 estado del enlace troncal 14](#_Toc192444179)

[Ilustración 6 comando show ip dhcp pool 16](#_Toc192444180)

[Ilustración 7 comando show ip dhcp binding 17](#_Toc192444181)

[Ilustración 8 show ip dhcp server statistics para 17](#_Toc192444182)

[Ilustración 9 comando ip dhcp en PC-A 17](#_Toc192444183)

[Ilustración 10 comando show ip en PC-A 18](#_Toc192444184)

[Ilustración 11 ping de PC-A 18](#_Toc192444185)

[Ilustración 12 comando ip dhcp en PC-B 19](#_Toc192444186)

[Ilustración 13 Comando Show ip en PC-B 20](#_Toc192444187)

[Ilustración 14 Ping en PC-B 20](#_Toc192444188)

[Ilustración 15 Comando show ip dhcp binding en R1 21](#_Toc192444189)

[Ilustración 16 Comando show ip dhcp server statistics en R1 y R2 21](#_Toc192444190)

# Introducción

El presente corresponde una tarea sobre la configuración de una red dada además se debe trabajar utilizando subneteo con VLSM. Esta técnica permite dividir un espacio de direcciones IP en subredes de diferentes tamaños según la topología de red, lo que a su vez se puede aprovechar mejor el direccionamiento IP y garantizar una distribución eficiente de los recursos, algo fundamental en el diseño de redes.

Además del subneteo, en el presente trabajo se abordará la configuración de DHCP (Dynamic Host Configuration Protocol). Este protocolo es esencial en la automatización de la asignación de direcciones IP dentro de una red, evitando la necesidad de configurarlas manualmente en cada dispositivo. Con DHCP, se puede asegurar que cada equipo reciba una dirección válida sin conflictos, lo que facilita la administración y optimización del uso de direcciones IP.

La importancia de esta tarea consiste en reforzar los conocimientos sobre estándares y protocolos de redes, así permitiendo comprender cómo se comunican los dispositivos y cómo se configuran correctamente las direcciones IP. Además, se trabajará con el software GNS3 para simular las redes reales y aplicar lo aprendido en la configuración de routers, switches, VLANs y DHCP. De esta manera, se busca desarrollar habilidades prácticas que son esenciales en el mundo de las redes.

La importancia de este trabajo radica en que aprender a configurar correctamente una red es clave para garantizar su buen funcionamiento. Conocer cómo funciona el subneteo con VLSM permite optimizar el uso de direcciones IP y evitar desperdicio de recursos. Además, comprender la segmentación de redes, el enrutamiento y la configuración de equipos como servidores DHCP ayuda a diseñar infraestructuras más eficientes y seguras.

En el presente trabajo se abordarán los fundamentos y la terminología básica en redes de computadoras, con un enfoque especial en el direccionamiento IP y la automatización de configuraciones mediante DHCP. Estos conceptos son esenciales para entender cómo se asignan las direcciones en una red y cómo se pueden organizar mejor los dispositivos conectados.

# Desarrollo

Parte 1: Armado de la red y configuración **de los parámetros básicos de los dispositivos**

## Paso 1: Establecer el esquema de direccionamiento

**Ilustración 1 Topología tarea 2**

Subnetear al subred 192.168.1.0/24 para cumplir con los siguientes requerimientos:

a. Una subred “Subred A” que permita 58 Hosts en la red ver (Figura 1 (Topología)) Subred A: **192.168.1.0/26**

Registre la primera direccion IP con su respectiva mascara de red en la Tabla 1 (Direccionamiento) para R1 f0/0.1

Registre la segunda direccion IP con su respectiva mascara de red en la Tabla 1 (Direccionamiento) para S1 VLAN 200 e introduzca su respectivo Default Gateway

b. Una subred “Subred B” que permita 28 Hosts en la red ver (Figura 1 (Topología)) Subred B: **192.168.1.64/27**

Registre la primera direccion IP con su respectiva mascara de red en la Tabla 1 (Direccionamiento) para R1 f0/0.2

Registre la segunda direccion IP con su respectiva mascara de red en la Tabla 1 (Direccionamiento) para S1 VLAN 1 e introduzca su respectivo Default Gateway

c. Una subred “Subred C” que permita 12 Hosts en la red ver (Figura 1 (Topología)) Subred C: **192.168.1.96/28**

Registre la primera direccion IP con su respectiva mascara de red en la Tabla 1 (Direccionamiento) para R2 f0/0

Registre la segunda direccion IP con su respectiva mascara de red en la Tabla 1 (Direccionamiento) para S2 VLAN 1 e introduzca su respectivo Default Gateway

**Esquema de direccionamiento**

Se realiza con apoyo de la calculadora (*Online IP Subnet Calculator and CIDR Calculator*, s. f.)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Descripción de la  subred | Cantidad  de Hosts | Dirección de  red | Mascara de  red | Broadcast | Primera  Dirección IP | Ultima  Dirección IP |
| Sub Red A | 58 | 192.168.1.0/26 | 255.255.255.192 | 192.168.1.63 | 192.168.1.1 | 192.168.1.62 |
| Sub Red B | 28 | 192.168.1.64/27 | 255.255.255.224 | 192.168.1.95 | 192.168.1.65 | 192.168.1.94 |
| Sub Red C | 12 | 192.168.1.96/28 | 255.255.255.240 | 192.168.1.111 | 192.168.1.97 | 192.168.1.110 |

## Tabla 1 Direccionamiento

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Dispositivos** | **Interfaz** | **Dirección IP** | **Mascara de**  **Subred** | **Puerta de Enlace**  **Predeterminada**  **(Default Gateway)** |
| R1 | s0/0 | 10.0.0.1 | 255.255.255.252 | N/D |
| f0/0 | No corresponde | No corresponde |
| f0/0.100 | 192.168.1.1 | 255.255.255.192 |
| f0/0.200 | 192.168.1.65 | 255.255.255.224 |
| R2 | s0/0 | 10.0.0.2 | 255.255.255.252 | N/D |
| f0/0 | 192.168.1.97 | 255.255.255.240 |
| S1 | VLAN 200 | 192.168.1.66 | 255.255.255.224 | 192.168.1.65 |
| VLAN 1 | 192.168.1.2 | 255.255.255.192 | 192.168.1.1 |
| S2 | VLAN 1 | 192.168.1.98 | 255.255.255.240 | 192.168.1.97 |
| PC-A | NIC | DHCP | DHCP | DHCP |
| PC-B | NIC | DHCP | DHCP | DHCP |

## Tabla 2 VLAN

|  |  |  |
| --- | --- | --- |
| **VLAN** | **Nombre** | **Interfaz Asignada** |
| 1 | No corresponde | S2: e1 |
| 100 | Estudiantes | S1: e1 |
| 200 | Clases | S1: VLAN 200 |
| 999 | Dirección | S1: e2-7 |
| 1000 | Nativa | N/D |

# Paso 2: Configuración de los parámetros básicos para cada router

a) Asignar el nombre a cada router como se ve en la Figura 1

|  |  |
| --- | --- |
| R1 | R2 |
| enable  configure terminal  hostname R1 | enable  configure terminal  hostname R2 |

b) Deshabilite el DNS en cada router para que evite traducir los comandos mal introducidos como si fueran nombres de Hosts

|  |  |
| --- | --- |
| R1 | R2 |
| no ip domain lookup | no ip domain lookup |

c) Asigne **gns** como contraseña cifrada del modo EXEC privilegiado en cada router

|  |  |
| --- | --- |
| R1 | R2 |
| enable secret gns | enable secret gns |

d) Asigne **gnstres** como la contraseña de la consola y active el inicio de sesión en cada router

|  |  |
| --- | --- |
| R1 | R2 |
| line console 0  password gnstres  login | line console 0  password gnstres  login |

e) Asigne **gnstres** como la contraseña VTY y active el inicio de sesión en cada router

|  |  |
| --- | --- |
| R1 | R2 |
| line vty 0 4  password gnstres  login | line vty 0 4  password gnstres  login |

f) En cada router cifre las contraseñas de texto sin formato

|  |  |
| --- | --- |
| R1 | R2 |
| service password-encryption | service password-encryption |

g) En cada router cree un aviso que advierta a todo el que acceda al dispositivo que el

“**Acceso no Autorizado Está Prohibido**”

|  |  |
| --- | --- |
| R1 | R2 |
| banner motd $ Acceso no Autorizado Está Prohibido$ | banner motd $ Acceso no Autorizado Está Prohibido$ |

h) Ajustar en los router el reloj con la hora y la fecha del momento de configuración

|  |  |
| --- | --- |
| R1 | R2 |
| clock set 19:28:00 27 Feb 2025 | clock set 19:28:00 27 Feb 2025 |

i) Guarde la configuración en cada router

|  |  |
| --- | --- |
| R1 | R2 |
| copy running-config startup-config | copy running-config startup-config |

**Nota:** Utilice el signo de interrogación (?) para poder determinar la secuencia correcta de parámetros necesarios para ejecutar los comandos.

# Paso 3: Configurar la interfaz f0/0 en el router R1 y las subinterfaces

a) Encienda la interfaz f0/0 en el router, no se configura solo en enciende

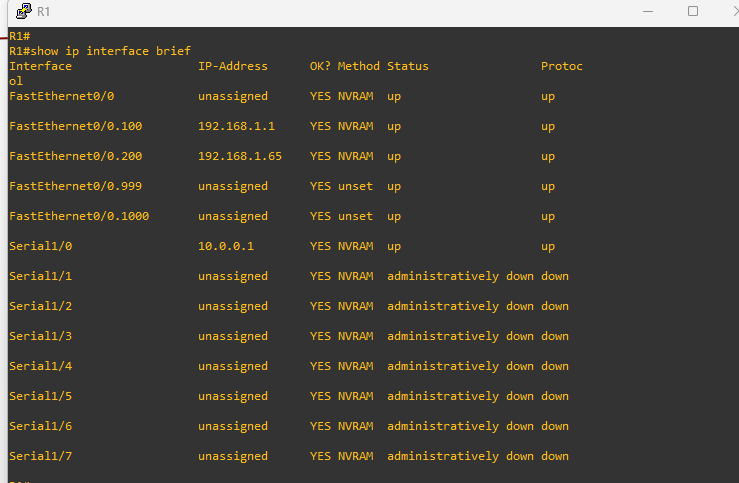
|  |
| --- |
| R1 |
| interface fa0/0  no shutdown  exit |

b) Configure las subinterfaces según lo muestra la Tabla 1 Direccionamiento. Todas las subinterfaces usando encapsulación 802.1Q y se les asigna la primera dirección IP utilizable de cada grupo de direcciones IP que se calcularon el Paso 1. Incluya una descripción para cada subinterfaz.

|  |
| --- |
| R1 |
| interface fastethernet 0/0.100  encapsulation dot1q 100  ip address 192.168.1.1 255.255.255.192  description Estudiantes  exit  interface fastethernet 0/0.200  encapsulation dot1q 200  ip address 192.168.1.65 255.255.255.224  description Clases  exit  wr  interface fastethernet 0/0.999  encapsulation dot1q 999  description Direccion  exit  end  do wr  interface fastethernet 0/0.1000  encapsulation dot1q 1000 native  description Nativo  exit  do wr |

c) Verifique que las subinterfaces estén operativas

|  |  |
| --- | --- |
| R1 | R2 |
| show ip interface brief | show ip interface brief |

****

**Ilustración 2 subinterfaces operativas**

# Paso 4: Configurarse en el R2 la f0/0, luego s0/0 y utilizar el protocolo de enrutamiento

# EIGRP para ambos router

a) Configure f0/0 en R2 con la primera dirección IP de las subred C que se calculó en la

Tabla 1

|  |
| --- |
| R2 |
| interface fastethernet 0/0  no shutdown  ip address 192.168.1.97 255.255.255.240  description Subred C  exit  do wr |

b) Configure la interfaz s0/0 para cada router según la Tabla 1

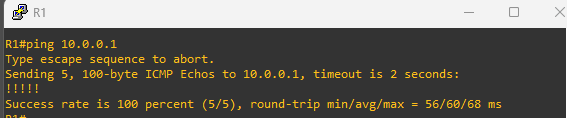
|  |  |
| --- | --- |
| R1 | R2 |
| interface serial 1/0  ip address 10.0.0.1 255.255.255.252  no shutdown  description Hacia R2  exit  do wr | interface serial 1/0  ip address 10.0.0.2 255.255.255.252  no shutdown  description Hacia R1  exit  do wr |

c) Configure el protocolo EIGRP en cada router para poder tener comunicación de un extremo a otro de la topología (Incluya las direcciones IP correspondientes)

|  |  |
| --- | --- |
| R1 | R2 |
| show ip route connected  router eigrp 1  network 10.0.0.0 0.0.0.3  network 192.168.1.0 0.0.0.63  network 192.168.1.64 0.0.0.31  no auto-summary  exit  do wr | show ip route connected  router eigrp 1  network 10.0.0.0 0.0.0.3  network 192.168.1.96 0.0.0.15  no auto-summary  exit  do wr |

d) Realice un ping de router a router para ver si hay comunicación

|  |
| --- |
| R1 |
| ping 10.0.0.1 |



**Ilustración 3 ping de router a router**

e) Guarde la configuración en cada router

|  |  |
| --- | --- |
| R1 | R2 |
| copy running-config startup-config | copy running-config startup-config |

# Paso 5: Configurar los básicos en cada switch

a) Asignar el nombre a cada router como se ve en la Figura 1

|  |  |
| --- | --- |
| S1 | S2 |
| enable  configure terminal  hostname S1 | enable  configure terminal  hostname S2 |

b) Deshabilite el DNS en cada router para que evite traducir los comandos mal introducidos como si fueran nombres de Hosts

|  |  |
| --- | --- |
| S1 | S2 |
| no ip domain-lookup | no ip domain-lookup |

c) Asigne **gns** como contraseña cifrada del modo EXEC privilegiado en cada router

|  |  |
| --- | --- |
| S1 | S2 |
| enable secret gns | enable secret gns |

d) Asigne **gnstres** como la contraseña de la consola y active el inicio de sesión en cada router

|  |  |
| --- | --- |
| S1 | S2 |
| line console 0  password gnstres  login | line console 0  password gnstres  login |

e) Asigne **gnstres** como la contraseña VTY y active el inicio de sesión en cada router

|  |  |
| --- | --- |
| S1 | S2 |
| line vty 0 4  password gnstres  login | line vty 0 4  password gnstres cisco  login |

f) En cada router cifre las contraseñas de texto sin formato

|  |  |
| --- | --- |
| S1 | S2 |
| service password-encryption | service password-encryption |

g) En cada router cree un aviso que advierta a todo el que acceda al dispositivo que el

“**Acceso no Autorizado Está Prohibido**”

|  |  |
| --- | --- |
| S1 | S2 |
| banner motd # Acceso no Autorizado Está Prohibido # | banner motd # Acceso no Autorizado Está Prohibido # |

h) Ajustar en los router el reloj con la hora y la fecha del momento de configuración

|  |  |
| --- | --- |
| S1 | S2 |
| clock set 19:28:00 27 Feb 2025 | clock set 19:28:00 27 Feb 2025 |

i) Guarde la configuración en cada switch

|  |  |
| --- | --- |
| S1 | S2 |
| copy running-config startup-config | copy running-config startup-config |

# Paso 6: Crear VLAN en el S1

a) Cree y asigne el nombre a cada VLAN tal como se muestra en la Tabla 2

|  |
| --- |
| S1 |
| vlan database  vlan 100 name Estudiantes  vlan 200 name Clases  vlan 999 name Direccion  vlan 1000 name Nativa  exit  copy running-config startup-config |

b) Configure y active las interfaces de administración en S1 (VLAN 200 y VLAN 1) utilizando la segunda dirección IP de la subred calculada en el Paso 1, recuerde establecer su respectivo default gateway ver Tabla 1

|  |
| --- |
| S1 |
| interface vlan 100  ip address 192.168.1.2 255.255.255.192  no shutdown  description Estudiantes  exit  ip default-gateway 192.168.1.1  interface vlan 200  ip address 192.168.1.66 255.255.255.224  no shutdown  description Clases  exit |

c) Configure y active la interfaz de administración en S2 (VLAN 1) utilizando la segunda dirección IP de la subred calculada en el Paso 1, recuerde establecer su respectivo default gateway ver Tabla 1

|  |
| --- |
| S1 |
| interface vlan 1  ip address 192.168.1.98 255.255.255.240  no shutdown  description Subred C  exit  ip default-gateway 192.168.1.97  do wr |

d) Asigne los demás puertos no utilizados en S1 a la VLAN de Dirección, configurándolos en modo acceso y desactívalos administrativamente, en el S2 desactive todos los puertos que no están siendo utilizados.

**Nota**: El comando que se debe utilizar para este punto es el **interface range**

|  |
| --- |
| S1 |
| interface range fastethernet 1/2 - 9  switchport mode access  switchport access vlan 999  exit  do wr  interface range fastethernet 1/10 - 15  switchport mode access  switchport access vlan 999  do wr |

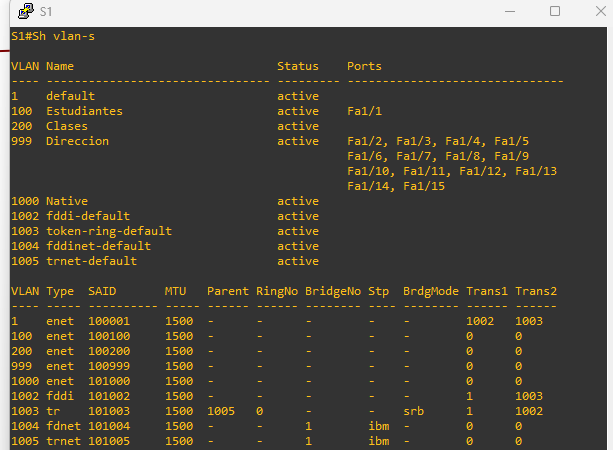
# Paso 7: Asignación de las VLANs a las interfaces del switch

a) Asigne el puerto de la VLAN apropiada tal como se muestra en la Tabla 2 y configúrelos en modo acceso

|  |
| --- |
| S1 |
| interface fastethernet 1/1  switchport mode access  switchport access vlan 100  exit |

b) Verifique que las VLANs estén asignadas a las interfaces correctas

|  |
| --- |
| S1 |
| Sh vlan-s |



**Ilustración 4 VLANs estén asignadas a las interfaces**

# Paso 8: Configuración de la interfaz e0 del switch S1 como enlace troncal 802.1Q

a) Cambie el modo del switchport en la interfaz para formar la conexión troncal

|  |
| --- |
| S1 |
| interface fastethernet 1/0  switchport mode trunk |

b) Como parte de la configuración troncal, establezca la VLAN Nativa en 1000 como se muestra la Tabla 2

|  |
| --- |
| S1 |
| switchport trunk native vlan 1000 |

c) Como otra parte de la configuración troncal, especifique que las VLAN 100, 200 y

1000 pueden cruzar el enlace troncal

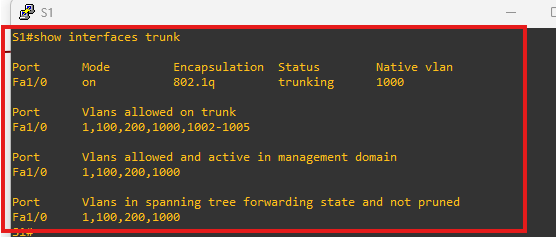
|  |
| --- |
| S1 |
| switchport trunk allowed vlan 1,100,200,1000,1002-1005 |

d) Guarde la configuración en ejecución

|  |
| --- |
| S1 |
| exit  copy running-config startup-config |

e) Verificar el estado del enlace troncal

|  |
| --- |
| S1 |
| show interfaces trunk |

****

**Ilustración 5 estado del enlace troncal**

## Parte 2: Configuración y verificación de los servidores DHCPv4 en el router R1

En esta parte vamos a configurar y verificar el servidor de DHCPv4 en R1, donde el servidor

DHCPv4 dará servicio a las subredes A y C

### Paso 1: Configurar en R1 con grupos de DHCPv4 para las dos subredes. Sólo se configura con el protocolo DHCPv4 la subred A tomando los datos de la Parte 1 Paso

**1**

a) Excluya las primeras cinco direcciones IP utilizables de la subred A ver **Parte 1 Paso**

**1 punto a**

|  |
| --- |
| R1 |
| enable  configure termimal  ip dhcp excluded-address 192.168.1.1 192.168.1.5 |

b) Cree el grupo DHCPv4 con el siguiente nombre **R1\_cliente\_LAN**

|  |
| --- |
| R1 |
| ip dhcp pool R1\_cliente\_LAN |

c) Configure la direccion red para el servidor DHCPv4

|  |
| --- |
| R1 |
| red 192.168.1.0 255.255.255.192 |

d) Configure el nombre de dominio con el siguiente **gnstres-lab.net**

|  |
| --- |
| R1 |
| domain-name gnstres-lab.net |

e) Configure el default Gateway

|  |
| --- |
| R1 |
| default-router 192.168.1.1 |

f) Configure el tiempo de concesión con el siguiente parámetro 2 días 12 horas 30 minutos

|  |
| --- |
| R1 |
| lease 2 12 30 |

g) Seguidamente vamos a configurar el segundo grupo DHCPv4 utilizando el nombre de **R2\_Cliente\_LAN**, con la red calcula en la **Parte 1 Paso 1 punto c**, excluyendo las primeras cinco direcciones IP, configurando la dirección de red y su respectiva mascara, utilice el mismo nombre de dominio **gnstres-lab.net** y el mismo tiempo de concesión **2 12 30**

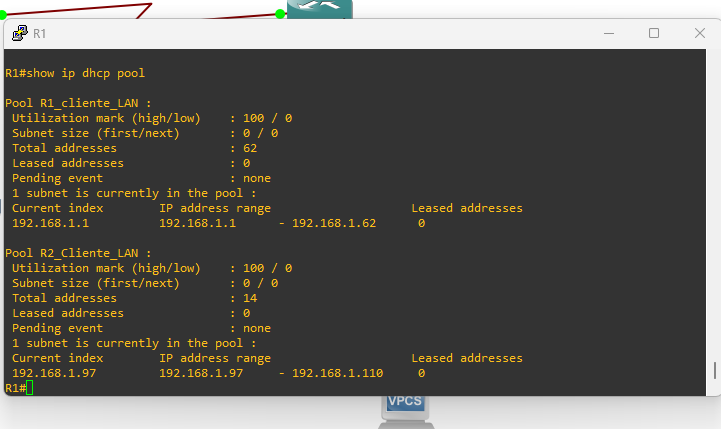
|  |
| --- |
| R1 |
| ip dhcp excluded-address 192.168.1.97 192.168.1.101  ip dhcp pool R2\_Cliente\_LAN  network 192.168.1.96 255.255.255.240  desfault-router 192.168.1.97  domain-name gnstres-lab.net  dns-server 8.8.8.8  lease 2 12 30  exit  do wr |

h) Guarde las configuraciones en ejecución dentro del router

|  |
| --- |
| R1 |
| copy running-config startup-config |

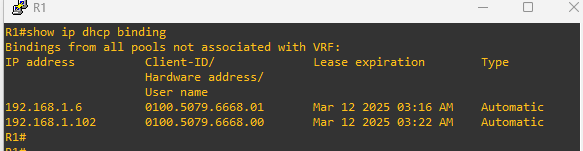
## Paso 2: Comprobación del servidor DHCPv4

a) Ejecutemos el comando **show ip dhcp pool** para ver los detalles del pool

****

**Ilustración 6 comando show ip dhcp pool**

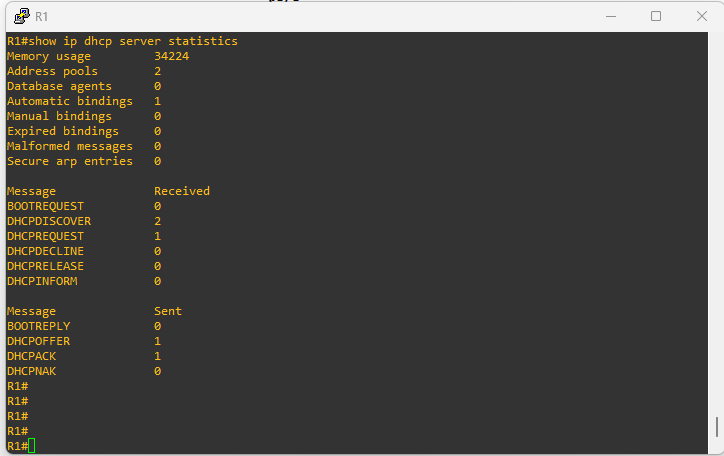
b) Ejecutemos el comando **show ip dhcp binding** para ver los detalles de las asignaciones de direcciones DHCP establecidas

****

**Ilustración 7 comando show ip dhcp binding**

c) Ejecutemos el comando **show ip dhcp server statistics** para ver los mensajes del

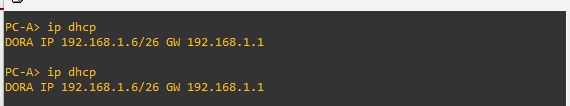
DHCP.

****

**Ilustración 8 show ip dhcp server statistics para**

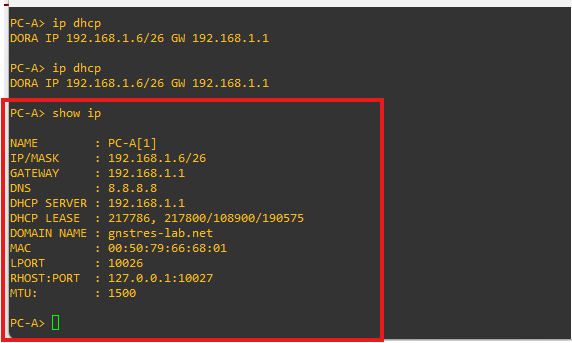
## Paso 3: Configurar una dirección IP de DHCP en la PC-A

a) En el símbolo de sistema de la PC-A vamos a introducir el comando **ip dhcp**

****

**Ilustración 9 comando ip dhcp en PC-A**

b) Una vez realizado el comando anterior vamos a ejecutar el comando **show ip** para ver la nueva información de IP que nos muestra la PC

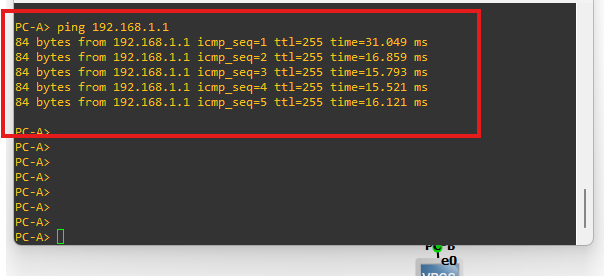
****

**Ilustración 10 comando show ip en PC-A**

c) Realizamos un **ping** para comprobar que la dirección IP de la PC-A llega la dirección

IP de la interfaz f0/0 del router R1

|  |
| --- |
| PC-A |
| ping 192.168.1.1 |

****

**Ilustración 11 ping de PC-A**

# Parte 3: Configuración y verificación de una retransmisión del DHCPv4 en el router R2

En esta parte, vamos a configurar en el router R2 la retransmisión del protocolo DHCPv4 desde la red de área local en la interfaz f0/0 al servidor DHCPv4 del router R1

## Paso 1: Configurar R2 como agente de retransmisión DHCPv4 para la LAN en f0/0

a) Introduzca el comando **ip helper-address** en f0/0 especificando la dirección IP de la interfaz s0/0 de R1

|  |
| --- |
| R2 |
| interface fastethernet 0/0  ip helper-address 10.0.0.1  exit  do wr |

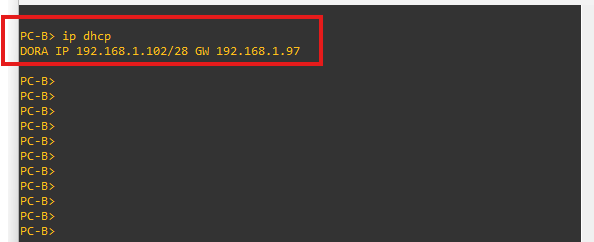
b) Guarde la configuración de ejecución dentro del router

|  |
| --- |
| R2 |
| exit  copy running-configuration startup-configuration |

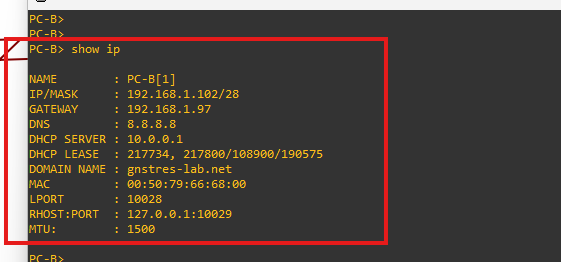
## Paso 2: Intento de adquirir una dirección IP de DHCPv4 en PC-B

a) En el símbolo de sistema de la PC-B vamos a introducir el comando **ip dhcp**

|  |
| --- |
| PC-B |
| ip dhcp  save |

****

**Ilustración 12 comando ip dhcp en PC-B**

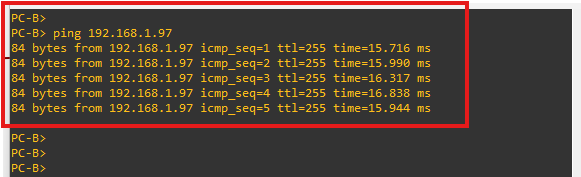
****b) Una vez realizado el comando anterior vamos a ejecutar el comando **Show ip** para ver la nueva información de IP que nos muestra la PC

**Ilustración 13 Comando Show ip en PC-B**

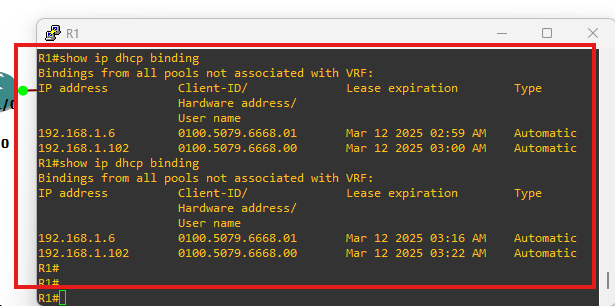
|  |
| --- |
| R2 |
| Show ip |

c) Realizamos un **ping** para comprobar que la dirección IP de la PC-A llega la direcciónIP de la interfaz f0/0 del router R1

|  |
| --- |
| PC-A |
| ping 192.168.1.97 |

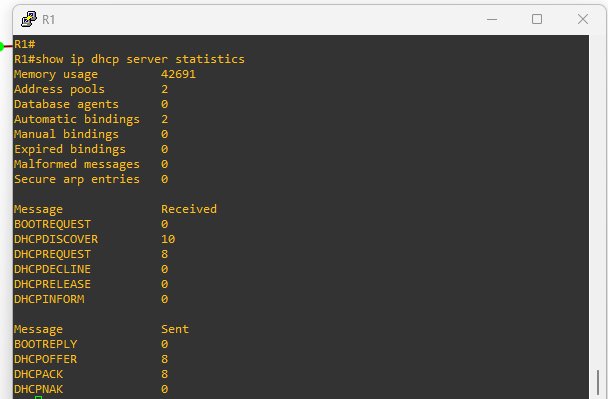


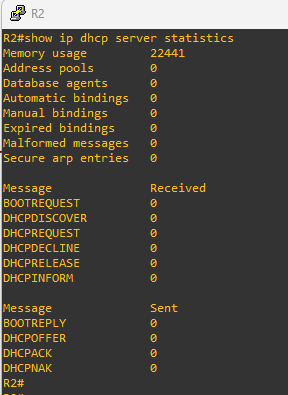
**Ilustración 14 Ping en PC-B**

d) Ejecute el comando **show ip dhcp binding** en el router R1 para verificar los enlaces de DHCP

**Ilustración 15 Comando show ip dhcp binding en R1**

e) Ejecute el comando **show ip dhcp server statistics** server en los router R1 y R2 para verificar los mensajes de DHCP





**Ilustración 16 Comando show ip dhcp server statistics en R1 y R2**

# Link del video

## <https://youtu.be/KDUKEEu1LKM>

## Script completo de cada Router

|  |  |
| --- | --- |
| R1 | R2 |
| enable  configure terminal  hostname R1  no ip domain-lookup  enable secret gns  line console 0  password gnstres  login  exit  line vty 0 15  password gnstres  login  exit  service password-encryption  banner motd $Acceso no Autorizado Esta Prohibido$  do wr  service password-encryption  do wr  exit  clock set 19:28:00 27 Feb 2025  interface fastethernet 0/0  no shutdown  interface fastethernet 0/0.100  encapsulation dot1q 100  ip address 192.168.1.1 255.255.255.192  description Estudiantes  exit  interface fastethernet 0/0.200  encapsulation dot1q 200  ip address 192.168.1.65 255.255.255.224  description Clases  exit  do wr  interface fastethernet 0/0.999  encapsulation dot1q 999  description Direccion  exit  do wr  interface fastethernet 0/0.1000  encapsulation dot1q 1000 native  description Nativa  exit  do wr  interface serial 1/0  ip address 10.0.0.1 255.255.255.252  no shutdown  description Hacia R2  exit  do wr  router eigrp 1  network 10.0.0.0 0.0.0.3  network 192.168.1.0 0.0.0.63  network 192.168.1.64 0.0.0.31  no auto-summary  exit  do wr  ip dhcp excluded-address 192.168.1.1 192.168.1.5  ip dhcp pool R1\_cliente\_LAN  network 192.168.1.0 255.255.255.192  default-router 192.168.1.1  domain-name gnstres-lab.net  dns-server 8.8.8.8  lease 2 12 30  exit  ip dhcp excluded-address 192.168.1.97 192.168.1.101  ip dhcp pool R2\_Cliente\_LAN  network 192.168.1.96 255.255.255.240  default-router 192.168.1.97  domain-name gnstres-lab.net  dns-server 8.8.8.8  lease 2 12 30  exit  do wr  copy running-config startup-config  ##HACER CAPTURA Y MOSTRAR VIDEO  show ip interface brief | enable  configure terminal  hostname R2  no ip domain-lookup  enable secret gns  line console 0  password gnstres  login  exit  line vty 0 15  password gnstres  login  exit  service password-encryption  banner motd $Acceso no Autorizado Esta Prohibido$  do wr  service password-encryption  do wr  exit  end  clock set 19:28:00 27 Feb 2025  configure terminal  interface fastethernet 0/0  no shutdown  ip address 192.168.1.97 255.255.255.240  description Subred C  exit  do wr  interface serial 1/0  ip address 10.0.0.2 255.255.255.252  no shutdown  description Hacia R1  exit  do wr  router eigrp 1  network 10.0.0.0 0.0.0.3  network 192.168.1.96 0.0.0.15  no auto-summary  exit  do wr  interface fastethernet 0/0  ip helper-address 10.0.0.1  exit  do wr  copy running-config startup-config |

## Script completo de cada Switch

|  |  |
| --- | --- |
| S1 | S2 |
| enable  configure terminal  hostname S1  no ip domain-lookup  enable secret gns  line console 0  password gnstres  login  exit  line vty 0 15  password gnstres  login  exit  service password-encryption  banner motd $Acceso no Autorizado Esta Prohibido$  do wr  service password-encryption  do wr  exit  clock set 19:28:00 27 Feb 2025  end  vlan database  vlan 100 name Estudiantes  vlan 200 name Clases  vlan 999 name Direccion  vlan 1000 name Native  exit  configure terminal  interface vlan 100  ip address 192.168.1.2 255.255.255.192  no shutdown  description Estudiantes  exit  ip default-gateway 192.168.1.1  do wr  interface vlan 200  ip address 192.168.1.66 255.255.255.224  no shutdown  description Clases  exit  do wr  interface range fastethernet 1/2 - 9  switchport mode access  switchport access vlan 999  exit  do wr  interface range fastethernet 1/10 - 15  switchport mode access  switchport access vlan 999  exit  interface fastethernet 1/1  switchport mode access  switchport access vlan 100  exit  interface fastethernet 1/0  switchport mode trunk  switchport trunk native vlan 1000  switchport trunk allowed vlan 1,100,200,1000,1002-1005  exit  do wr  copy running-config startup-config | enable  configure terminal  hostname S2  no ip domain-lookup  enable secret gns  line console 0  password gnstres  login  exit  line vty 0 15  password gnstres  login  exit  service password-encryption  banner motd $Acceso no Autorizado Esta Prohibido$  do wr  service password-encryption  do wr  exit  clock set 19:28:00 27 Feb 2025  interface vlan 1  ip address 192.168.1.98 255.255.255.240  no shutdown  description Subred C  exit  ip default-gateway 192.168.1.97  do wr  interface range fastethernet 1/2 - 9  shutdown  exit  do wr  interface range fastethernet 1/10 - 15  shutdown  exit  do wr  copy running-config startup-config |

# Conclusión

En conclusión, la elaboración de esta tarea ha permitido desarrollar un conocimiento sólido sobre subneteo con VLSM y la configuración de redes, direccionamiento IP y así mejorar el uso de los recursos disponibles. Se ha trabajado en la importancia del diseño adecuado en las subredes en función de las necesidades específicas de cada segmento dentro de la topología de red, lo cual esencial para la escalabilidad y eficiencia en entornos reales.

Por otro lado, se ha adquirido una comprensión clara sobre la configuración y administración de dispositivos clave como routers, switches y PCs, además de la implementación de DHCP para la asignación dinámica de direcciones IP. A través del uso de GNS3, se han aplicado comandos esenciales para configurar redes funcionales, asegurando que cada dispositivo pueda comunicarse correctamente dentro de la infraestructura establecida. También se han incorporado medidas de seguridad fundamentales, como la asignación de contraseñas y la inclusión de banners de advertencia, con el objetivo de proteger la red contra accesos no autorizados y fortalecer su estabilidad.

Finalmente, este proceso de aprendizaje ha demostrado la importancia del diseño estructurado de una red, la correcta segmentación y la configuración precisa de los dispositivos para lograr una conectividad eficiente y segura. El uso de subneteo con VLSM optimiza el direccionamiento IP, mientras que la implementación de DHCP facilita la administración de la red. Estos ejercicios prácticos, combinados con los fundamentos teóricos, proporcionan una base esencial para comprender el funcionamiento de las redes y su papel fundamental en la comunicación entre distintos dispositivos en un mundo cada vez más interconectado.

# Referencias

Comer, D. E. (2015). REDES DE COMPUTACION E INTERNET, 6th Edition. [[VitalSource Bookshelf version]]. Retrieved from vbk://9786073233248

*Online IP Subnet Calculator and CIDR Calculator*. (s. f.). Recuperado 21 de febrero de 2025, de https://www.subnet-calculator.com/