

# **Subnetting, MTK, ACL**

---

Práctica 7

Gonzalo Tudela Chavero

---

## ÍNDICE DE CONTENIDOS

---

Proceso de Trabajo .....	1
Ejercicio 1.....	2
Ejercicio 2.....	2
Simulación Packet Tracert.....	3
Configuración de los Routers: .....	4
Configuraciones IP:.....	5
Configuraciones DHCP:.....	5
Configuración DHCP Hosts: .....	6
Configuración de servidor DNS: .....	6
Configuración de servidor Web: .....	7
Código añadido a la web:.....	7
Configuración de las ACL (Access Control Lists): .....	8
ACL Extended para Mikrotik FA 1/0 numero 101(alumnos).....	8
ACL Extended para TP-Link FA 1/0 numero 101(profesores) .....	8
Comprobaciones ACL: .....	8
Ejercicio 3.....	13
Ejercicio 4.....	23

## ÍNDICE DE FIGURAS

---

Figura 1. Ejercicio 1, Esquema subredes VLSM. ....	2
Figura 2. Ejercicio 2, Esquema de la red en Visio.....	2
Figura 3. Ejercicio 2, esquema propuesto. ....	3
Figura 4. Ejercicio 2, RouterM interfaz FastEthernet 0/0, dirección IP+CIDR. ....	4
Figura 5. Ejercicio 2, RouterM interfaz FastEthernet 1/0, dirección IP+CIDR. ....	4
Figura 6. Ejercicio 2, RouterM interfaz FastEthernet 2/0, dirección IP+CIDR.....	4
Figura 7. Ejercicio 2, configuración DHCP parte1. ....	6
Figura 8. Ejercicio 2, configuración DHCP parte2 .....	6
Figura 9. Ejercicio 2, configuración servidor DNS.....	6
Figura 10. Ejercicio 2, configuración servidor web.....	7
Figura 11. Ejercicio 2, cambios en index.html.....	7
Figura 12. Ejercicio 2, comprobación DHCP en alumnos.....	9
Figura 13. Ejercicio 2, comprobación DHCP profesores. ....	9
Figura 14. Ejercicio 2, comprobación del funcionamiento DNS, TCP y HTTP en alumnos. ....	9
Figura 15. Ejercicio 2, alumnos solo hacen ping a su Gateway. ....	10
Figura 16. Ejercicio 2, profesor usuario solo ping a Alumnos. ....	11
Figura 17. Ejercicio 2, comprobación DNS,TCP,HTTP en profesor usuario.....	11
Figura 18. Ejercicio 2, comprobación profesor admin ICMP a resto de redes. ....	12
Figura 19. Ejercicio 2, comprobación profesor admin DNS,TCP,HTTP. ....	12
Figura 20. Ejercicio 3, laboratorio. ....	13
Figura 21. Ejercicio 3a, tablas de enrutamiento de Mikrotik. ....	13
Figura 22. Ejercicio 3b, Ping desde la red Servidores al resto de redes. ....	14
Figura 23. Ejercicio 3b, Ping desde la red Profesores al resto de redes. ....	15
Figura 24. Ejercicio 3b, Ping desde la red alumnos al resto de redes. ....	15
Figura 25. Ejercicio 3c, reglas firewall Mikrotik.....	16
Figura 26. Ejercicio 3d, filtrado del tráfico DHCP y paquetes capturados en la regla del firewall. ....	17
Figura 27. Ejercicio 3e, filtrado del tráfico DHCP y paquetes capturados en la regla del firewall. ....	18
Figura 28. Ejercicio 3f, ping al FQDN del servidor DNS desde el profesor admin. ....	19
Figura 29. Ejercicio 3g, ping al FQDN desde el profesor normal.....	20
Figura 30. Ejercicio 3h, ping a FQDN del servidor DNS desde un host Alumno.....	21
Figura 31. Ejercicio 3i, resultados Nmap.....	21
Figura 32. Ejercicio 3j, las reglas en el router impiden ver la diferencia con el comando anterior.....	22
Figura 33. Ejercicio 3k, página web visitada desde un host alumno. ....	22
Figura 34. Ejercicio 3k, página web funcionando desde un host profesor. ....	23

## Proceso de Trabajo

---

En un colegio se quiere implementar la siguiente arquitectura de red, partiendo de la dirección de red 172.16.0.0/24.

- Una red donde se encuentren los **servidores**: de momento se tiene un servidor DNS que gestiona la zona "lacomarca.local" y un servidor web accesible a través del protocolo "http". Se estima un **máximo de 15 servidores**. El FQDN del servidor DNS será "frodo.lacomarca.local". El FQDN del servidor web será "www.lacomarca.local".
- Una red de **alumnos** donde se prevé que a lo sumo haya un **total de 62 dispositivos**, uno por estudiante. Los alumnos no podrán escanear la red de los profesores ni de los servidores a través del envío de mensajes de tipo echo de ICMP (ICMP type 8). Los alumnos no podrán escanear la red de servidores ni la red de profesores. Esta red tendrá un servidor DHCP. Los alumnos serán clientes DNS del servidor "frodo.lacomarca.local" y podrán comunicarse con el servidor web a través del protocolo http y de la URL "http://www.lacomarca.local".
- Una red de **profesores** con un **máximo de 30 equipos**. Habrá un profesor administrador con el rol de "administrador" que será el único que pueda enviar mensajes de tipo "echo ICMP" a los servidores para ver si estos se encuentran levantados. su dirección IP es la 172.16.0.65/27. Los profesores podrán escanear la red de los alumnos para un descubrimiento de hosts activos, pero no podrán realizar esto con la red de los servidores. Esta red tendrá un servidor DHCP. Los profesores serán clientes DNS del servidor "frodo.lacomarca.local" y podrán comunicarse con el servidor web a través del protocolo http y de la URL "http://www.lacomarca.local".
- Se utilizará un router Mikrotik con tres interfaces de red de tipo FastEthernet, mínimo. El otro router será el router personal de cada alumno.
- Se utilizará RIPv1,2 para la creación y actualización del contenido de las tablas de rutas de los routers que forman la arquitectura de la red.

## Ejercicio 1

Realiza el esquema de direccionamiento necesario aprovechando al máximo el espacio de direccionamiento indicado. Indica en una tabla, la dirección de cada subred, el número de direcciones asignables, la máscara de subred, la dirección de broadcast en cada subred, así como el espacio de direccionamiento aprovechado.

Esquema subnetting VLSM Practica 07										
172.16.0.0/24										
Red Alumnos	62 host máx.	Espacio Aprov.	PARTE RED	SUBRED BITS	HOST BITS	MASK	RED + CIDR	Primer HOST	Ultimo HOST	BROADCAST
2 <sup>h-2</sup> >= 62	h=6 bit	100%	172.16.0	00	000000	255.255.255.192	172.16.0.0/26	172.16.0.1	172.16.0.62	172.16.0.63
64 direcciones	62 asignables			+1 bit						
				01						
Red Profesores	30 host máx.	Espacio Aprov.	PARTE RED	SUBRED BITS	HOST BITS	MASK	RED + CIDR	Primer HOST	Ultimo HOST	BROADCAST
2 <sup>h-2</sup> >= 30	h=5 bit	100%	172.16.0	010	00000	255.255.255.224	172.16.0.64/27	172.16.0.65	172.16.0.94	172.16.0.95
32 direcciones	30 asignables			+1 bit						
				011						
Red Servidores	15 host máx.	Espacio Aprov.	PARTE RED	SUBRED BITS	HOST BITS	MASK	RED + CIDR	Primer HOST	Ultimo HOST	BROADCAST
2 <sup>h-2</sup> >= 15	h=5 bit	50%	172.16.0	011	00000	255.255.255.224	172.16.0.96/27	172.16.0.97	172.16.0.126	172.16.0.127
32 direcciones	30 asignables			+1 bit						
				100						
Red Routers	2 host máx.	Espacio Aprov.	PARTE RED	SUBRED BITS	HOST BITS	MASK	RED + CIDR	Primer HOST	Ultimo HOST	BROADCAST
2 <sup>h-2</sup> >= 2	h=2 bit	100%	172.16.0	1000000	00	255.255.255.252	172.16.0.128/30	172.16.0.129	172.16.0.130	172.16.0.131
4 direcciones	2 asignables									

Figura 1. Ejercicio 1, Esquema subredes VLSM.

## Ejercicio 2

Realiza en Visio el esquema de la arquitectura de red que se plantea de la manera más detallada posible y posteriormente realiza una simulación en Packet Tracer. Las interfaces de los routers tendrán las direcciones más bajas de la subred, y los servidores las direcciones más altas.

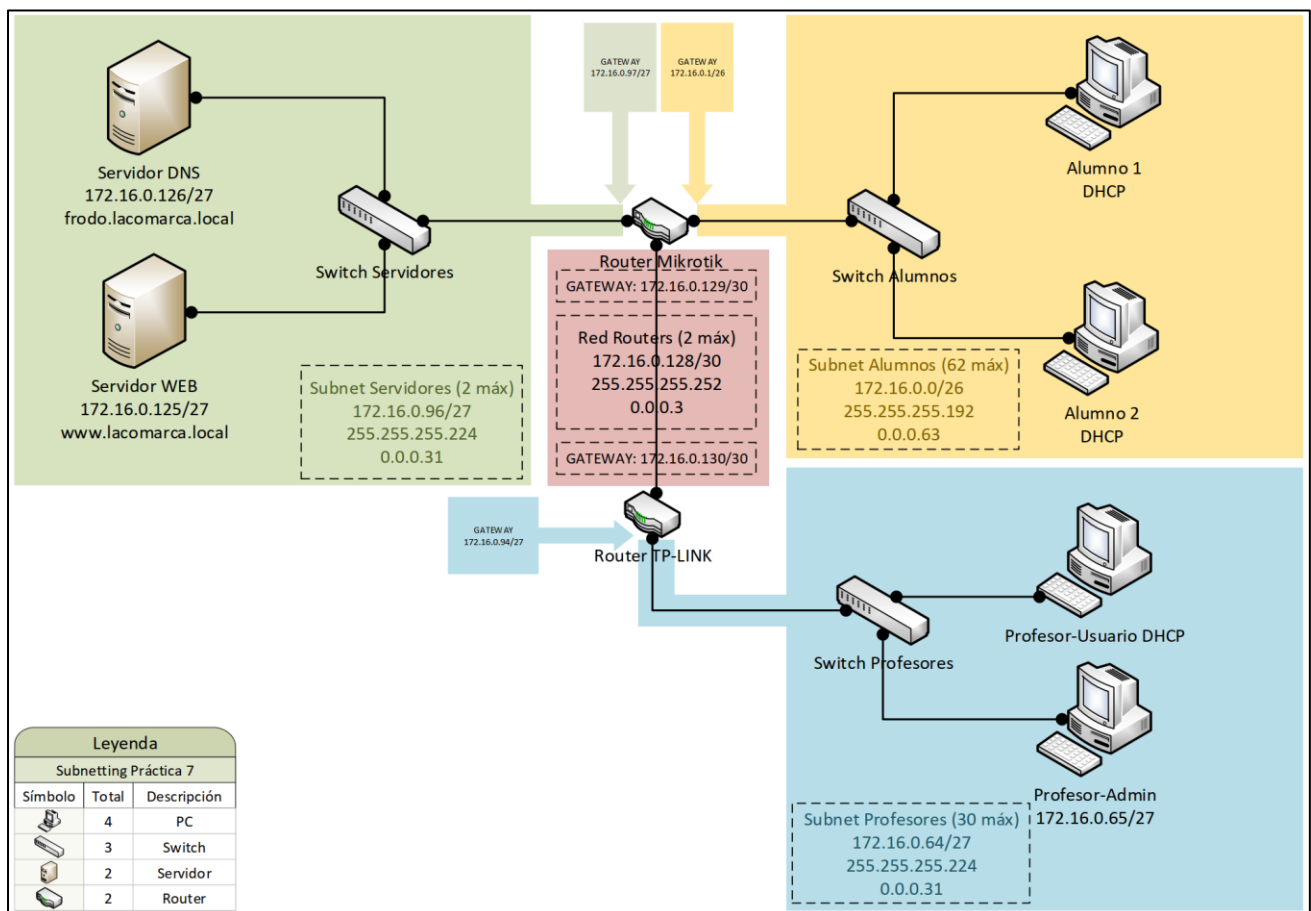


Figura 2. Ejercicio 2, Esquema de la red en Visio.

**Simulación Packet Tracer:** [Descarga el archivo de Packet Tracer v.7.2.1.0218 en este enlace a Google Drive.](#)

Cuando se hace click Google Drive lo identifica como un archivo multimedia, sencillamente descargarlo y abrirlo en Packet Tracer.

Para la simulación se realizó el siguiente esquema de red, en el que para ahorrar tiempo se han simplificado las redes a la mínima expresión, es decir, reduciendo el número de hosts que las componen al mínimo para poder hacer las comprobaciones.

Según este ejercicio **los routers tendrán las direcciones mas bajas de la subred, pero el proceso de trabajo indica que el host Profesor-Admin ocupará la dirección mas baja de su red** por lo que he asignado la mas alta de esa red al router, excluyendo ambas del pool DHCP como se puede ver más adelante.

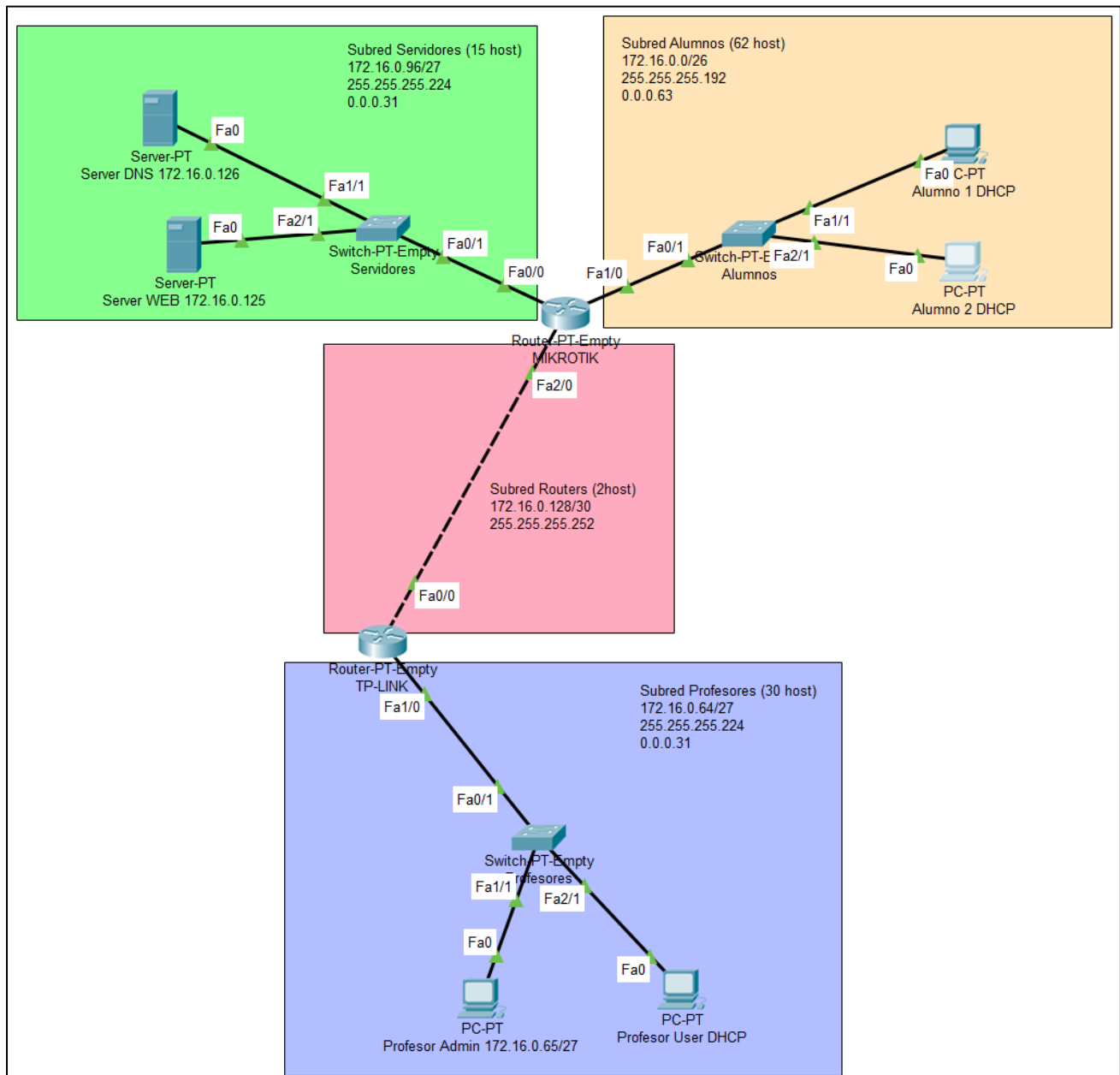


Figura 3. Ejercicio 2, esquema propuesto.

## Configuración de los Routers:

A continuación, se muestra la configuración del router encargado de las redes para servidores y alumnos, en el esquema anterior denominado con la etiqueta MIKROTIK y con nombre de host RouterM.

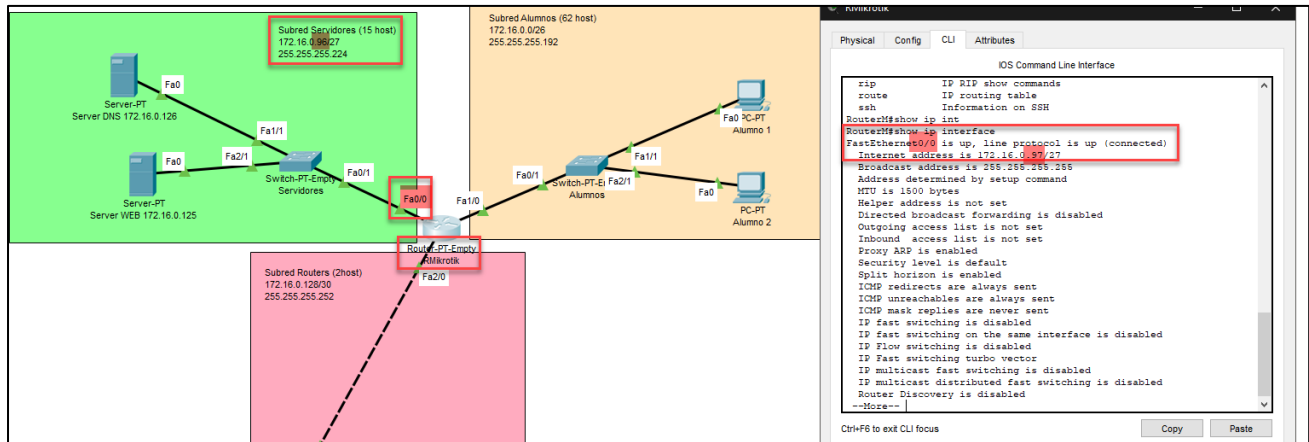


Figura 4. Ejercicio 2, RouterM interfaz FastEthernet 0/0, dirección IP+CIDR.

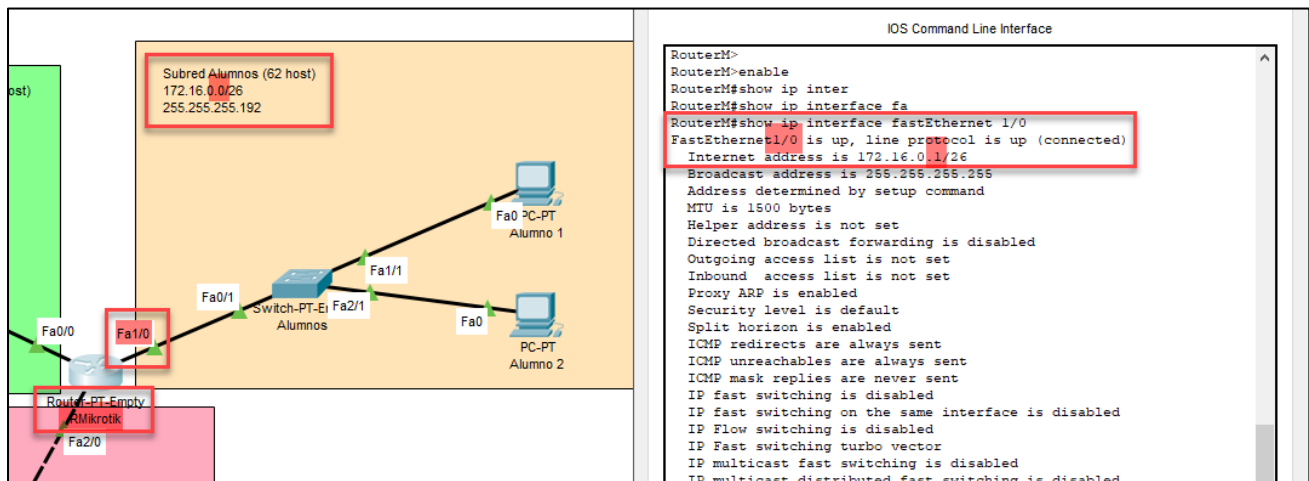


Figura 5. Ejercicio 2, RouterM interfaz FastEthernet 1/0, dirección IP+CIDR.

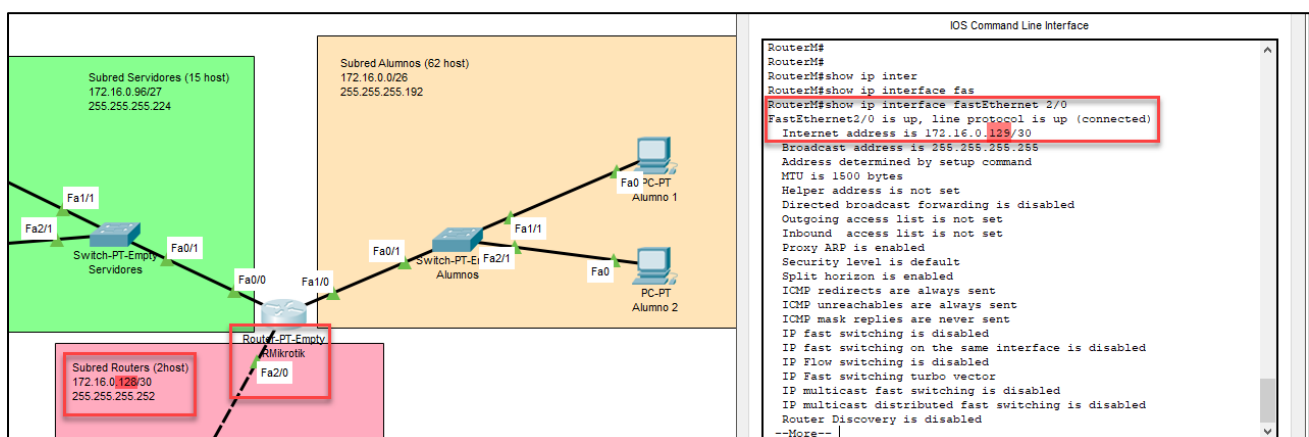


Figura 6. Ejercicio 2, RouterM interfaz FastEthernet 2/0, dirección IP+CIDR.

## Configuraciones IP:

El resto de las configuraciones de las interfaces de red se realiza mediante los siguientes comandos, en los que sustituimos los valores de tipo, numeración, IP y mascara por los adecuados en cada caso según el esquema de red.

```
interface "tipo" "numeración"
ip address "dirección ip" "mascara de red"
```

## Configuraciones DHCP:

**Configuración del servicio DHCP para "Router Mikrotik" en la interfaz 1/0 con la intención de servir direcciones en la subred Alumnos.**

Damos un nombre a un grupo de direcciones que entregará el servicio DHCP.

```
ip dhcp pool alumnos
```

Configuramos la red con la que trabajará nuestro servicio DHCP.

```
net 172.16.0.0 255.255.255.192
```

Establecemos la puerta de enlace (Gateway) que serviremos a los clientes del pool alumnos.

```
default-router 172.16.0.1
```

Establecemos la ip del servidor DNS que vamos a servir a los clientes del pool alumnos.

```
dns-server 172.16.0.126
```

Establecemos un nombre de dominio.

```
domain-name alumnos
```

Excluimos de los préstamos que hará el servicio la propia IP de la puerta de enlace.

```
ip dhcp excluded-address 172.16.0.1 172.16.0.1
```

**Configuración del servicio DHCP para "Router TP-Link" en la interfaz 1/0 con la intención de servir direcciones en la subred Profesores.**

Damos un nombre a un grupo de direcciones que entregará el servicio DHCP.

```
ip dhcp pool profesores
```

Configuramos la red con la que trabajará nuestro servicio DHCP.

```
net 172.16.0.64 255.255.255.224
```

Establecemos la puerta de enlace (Gateway) que serviremos a los clientes del pool alumnos.

```
default-router 172.16.0.94
```

Establecemos la ip del servidor DNS que vamos a servir a los clientes del pool alumnos.

```
dns-server 172.16.0.125
```

Establecemos un nombre de dominio.

```
domain-name profesores
```

Excluimos de los préstamos la Gateway (.66) y el Profesor Admin (.65) que cuentan con IP fija.

```
ip dhcp excluded-address 172.16.0.65 172.16.0.66
```



### Configuración DHCP Hosts:

Todos los hosts en los que se requiere configuración DHCP han quedado configurados como en las siguientes figuras.

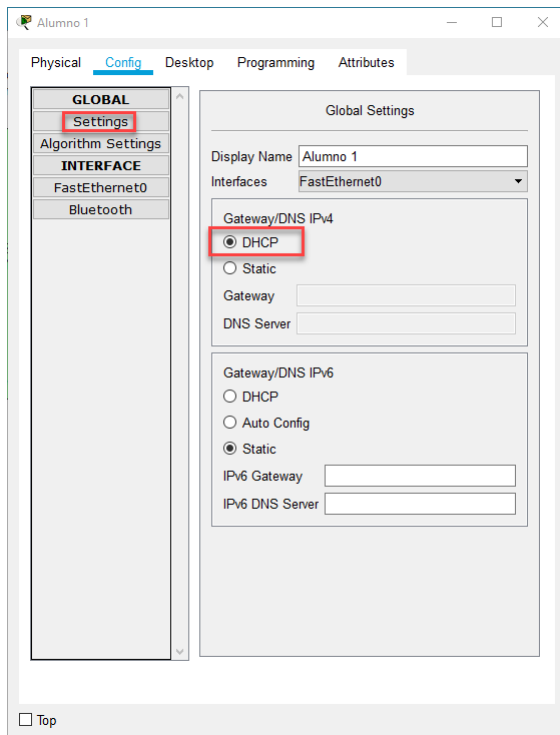


Figura 7. Ejercicio 2, configuración DHCP parte1.

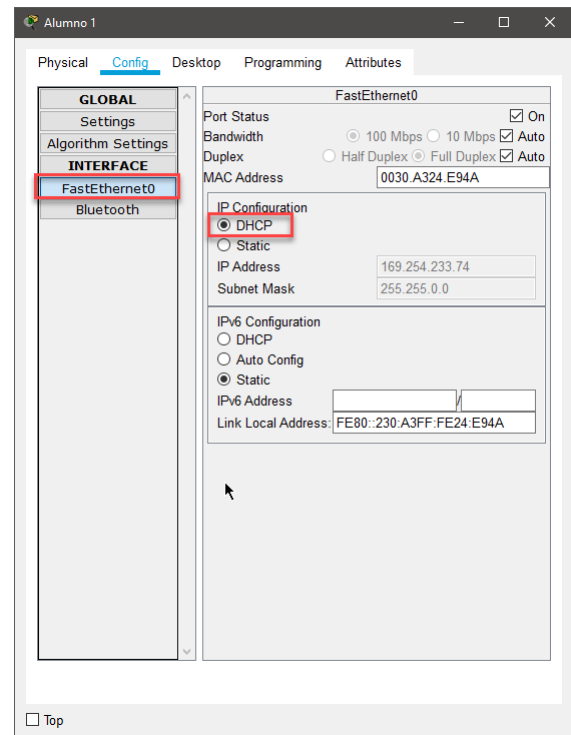


Figura 8. Ejercicio 2, configuración DHCP parte2

### Configuración de servidor DNS:

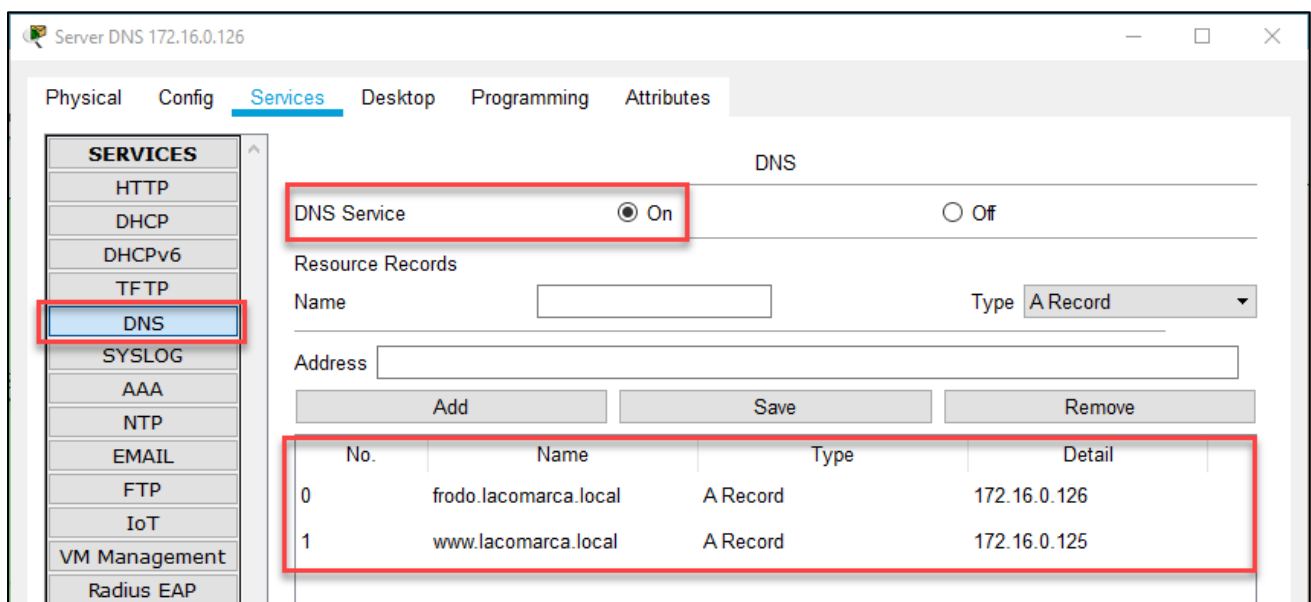


Figura 9. Ejercicio 2, configuración servidor DNS.

### Configuración de servidor Web:

Se ha añadido una etiqueta `<h1>Salesianos Server</h1>` al código de la pagina web para comprobar que es en efecto la web que servimos.

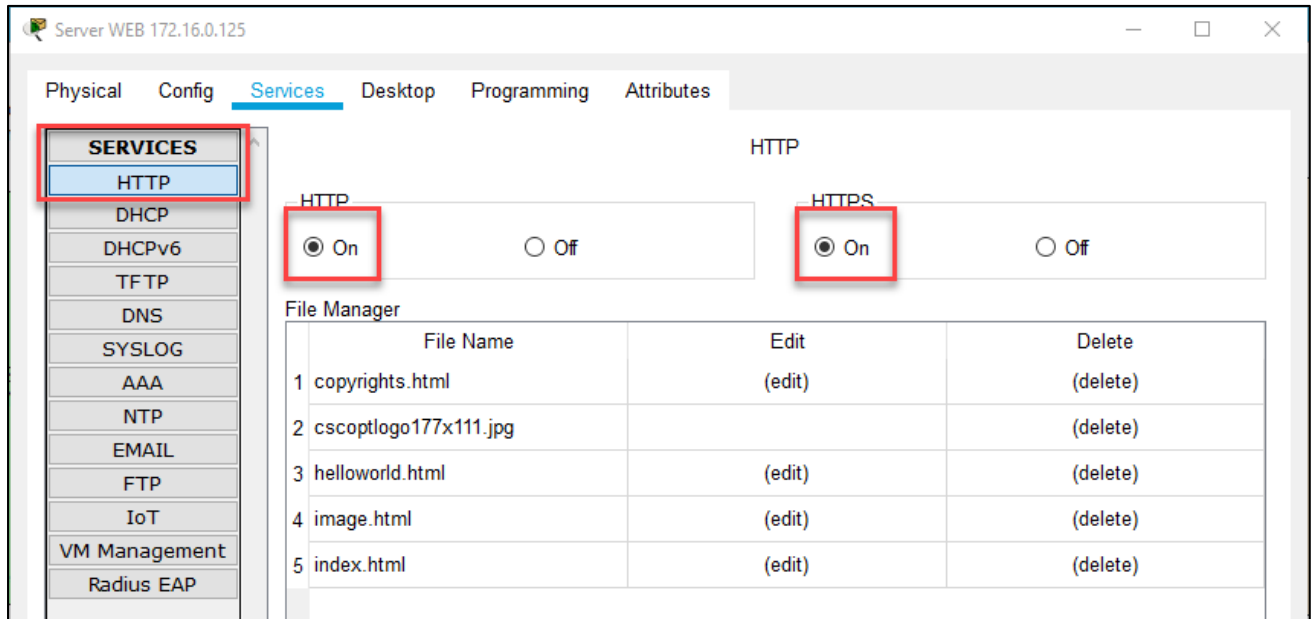


Figura 10. Ejercicio 2, configuración servidor web.

### Código añadido a la web:

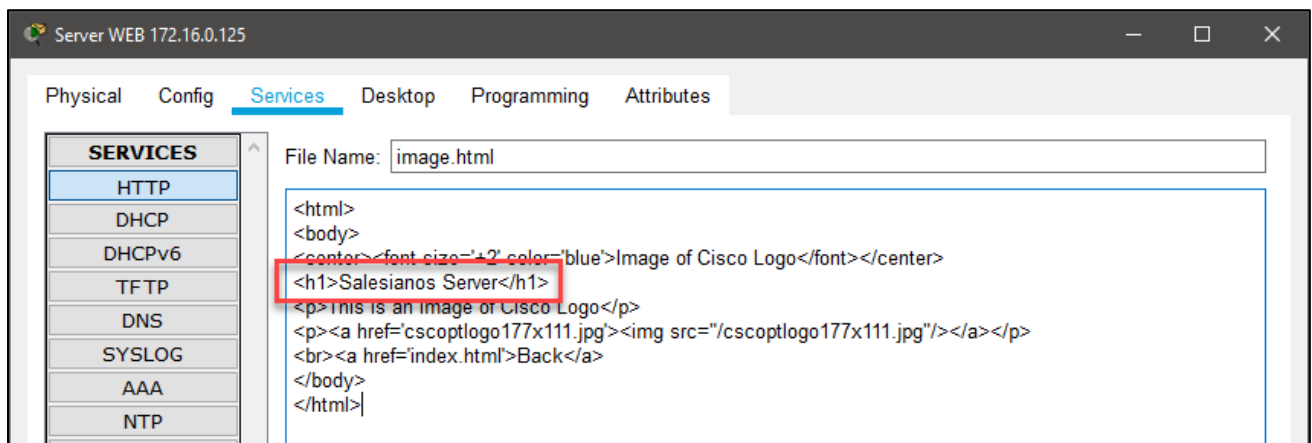


Figura 11. Ejercicio 2, cambios en index.html.

**Configuración de las ACL (Access Control Lists):**

Las ACL's afectan a los alumnos y a los profesores y se crearan mediante su forma extendida lo mas cerca del origen del tráfico, es decir en las puertas de enlace de las redes alumnos y profesores.

**Alumnos:**

- a. Permitir DHCP (UDP's 68 y 67)
- b. Permitir DNS (UDP 53)
- c. Permitir HTTP (TCP, 80)
- d. Denegar peticiones ICMP a Profesores y Servidores

**Profesores:**

- a. Permitir DHCP (UDP's, 68 y 67)
- b. Permitir DNS (UDP, 53)
- c. Permitir HTTP (TCP, 80)
- d. Permitir peticiones ICMP a Alumnos
- e. Permitir peticiones ICMP a Servidores (solo el administrador).

Estas listas de control de acceso son creadas para cumplir lo que se solicita, pero no están complementadas con sus "inversas" en los destinos, que controlarían el sentido opuesto de la comunicación, para así ganar en seguridad.

Se observa inmediatamente la falta de control en la subred de servidores, lo que permitiría que equipos intrusos en esta red podrían obtener información de toda la infraestructura.

**Las ACL aplicadas son las siguientes:****ACL Extended para Mikrotik FA 1/0 numero 101 (alumnos)**

```
5 permit icmp 172.16.0.0 0.0.0.63 host 172.16.0.1 - permite ICMP a gateway
10 permit icmp 172.16.0.0 0.0.0.63 any 0 - permitir respuestas ICMP a cualquier destino
20 permit udp host 0.0.0.0 host 255.255.255.255 range 67 68 - permite DHCP a equipos sin IP
30 permit udp 172.16.0.0 0.0.0.63 host 172.16.0.126 eq 53 - permite comunicacion con servidor dns
40 permit tcp 172.16.0.0 0.0.0.63 host 172.16.0.125 eq 80 - permite tcp 80 con servidor web
50 deny icmp 172.16.0.0 0.0.0.63 172.16.0.96 0.0.0.31 8 - denegar peticiones ICMP a red servidores
60 deny icmp 172.16.0.0 0.0.0.63 172.16.0.64 0.0.0.31 8 - denegar peticiones ICMP a red profesores
```

**ACL Extended para TP-Link FA 1/0 numero 101 (profesores)**

```
5 permit icmp 172.16.0.64 0.0.0.31 host 172.16.0.66 - permite ICMP a gateway
10 permit icmp 172.16.0.64 0.0.0.31 any 0 permite respuestas ICMP a cualquier destino
20 permit udp host 0.0.0.0 host 255.255.255.255 range 67 68 - permite DHCP a equipos sin IP
30 permit udp 172.16.0.64 0.0.0.31 host 172.16.0.126 eq 53 - permite comunicacion con servidor dns
40 permit tcp 172.16.0.64 0.0.0.31 host 172.16.0.125 eq 80 - permite tcp 80 con servidor web
50 permit icmp host 172.16.0.65 172.16.0.96 0.0.0.31 - permite ICMP completo profesor admin a servidores
60 permit icmp 172.16.0.64 0.0.0.31 172.16.0.0 0.0.0.63 8 - permitir peticiones ICMP a red alumnos
70 deny icmp 172.16.0.64 0.0.0.31 172.16.0.96 0.0.0.31 8 - denegar peticiones ICMP a red servidores
```

**Comprobaciones ACL:**

A continuación, se muestran capturas de pantalla de las pruebas para verificar las ACL.

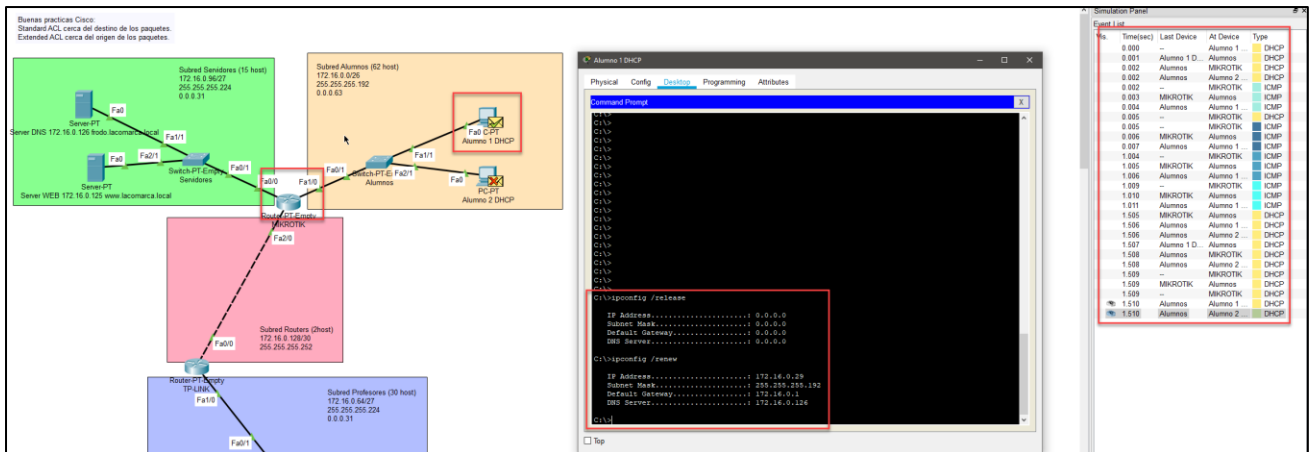


Figura 12. Ejercicio 2, comprobación DHCP en alumnos.

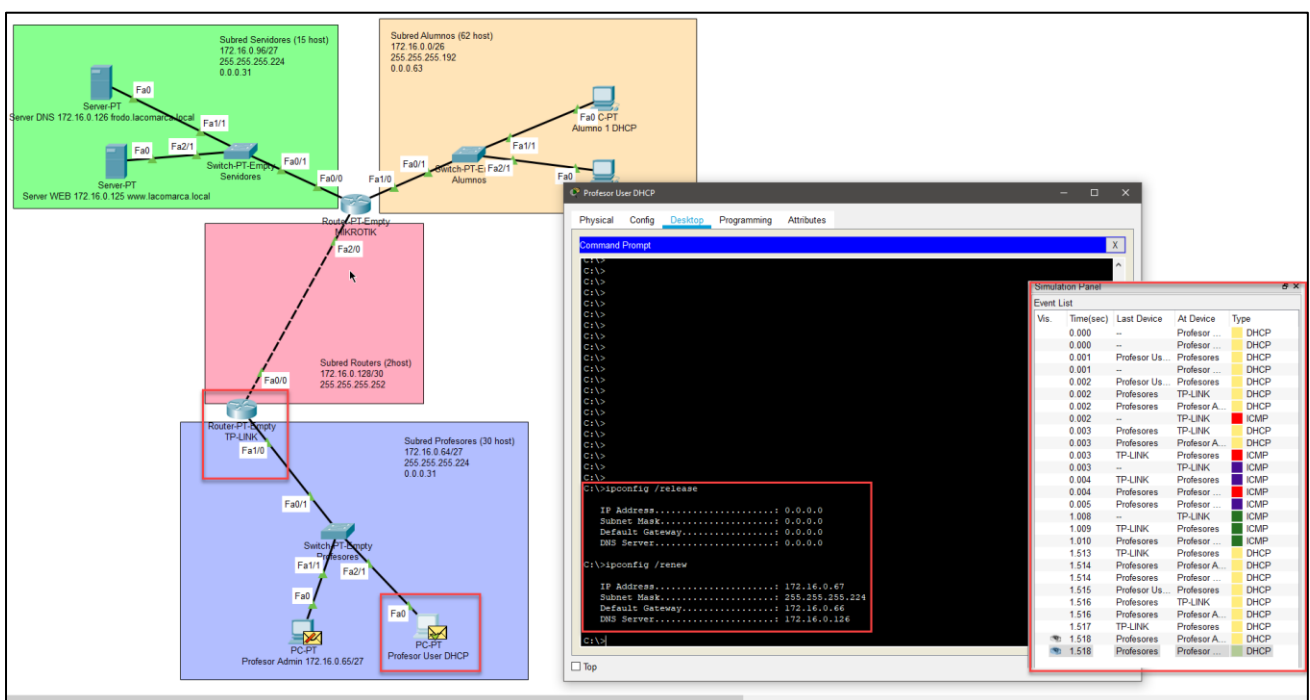


Figura 13. Ejercicio 2, comprobación DHCP profesores.

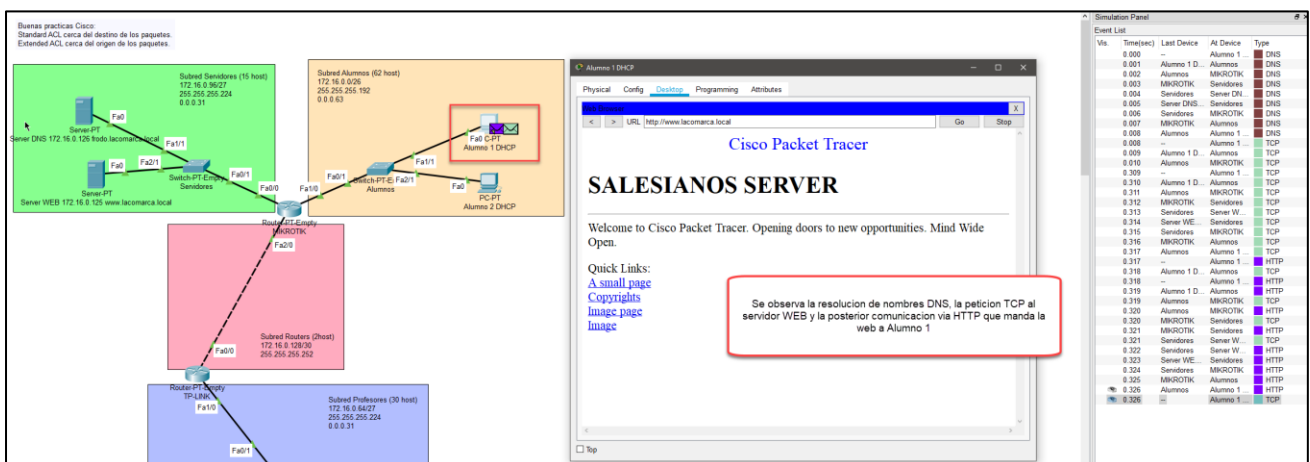
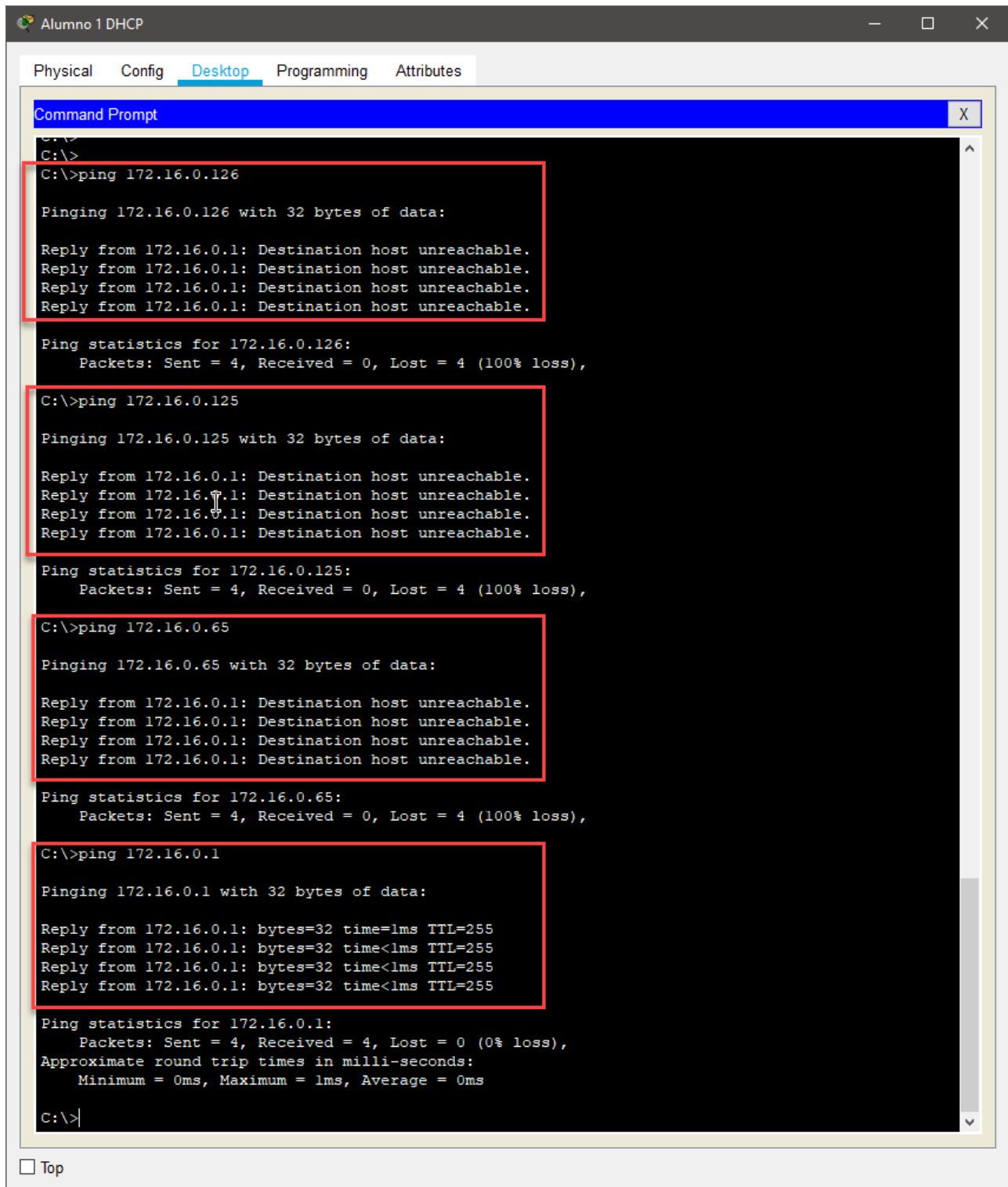


Figura 14. Ejercicio 2, comprobación del funcionamiento DNS, TCP y HTTP en alumnos.



The screenshot shows a Packet Tracer interface with a 'Command Prompt' window open. The window has tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes', with 'Desktop' selected. The Command Prompt displays the results of four ping commands executed from the C:\> prompt. Each command is followed by a red rectangular highlight box. The first three commands (ping 172.16.0.126, ping 172.16.0.125, and ping 172.16.0.65) all result in 'Destination host unreachable' for all four attempts, with a 100% loss. The fourth command (ping 172.16.0.1) results in successful replies for all four attempts, with 0% loss and round trip times of 1ms.

```
Alumno 1 DHCP
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>ping 172.16.0.126

Pinging 172.16.0.126 with 32 bytes of data:

Reply from 172.16.0.1: Destination host unreachable.
Reply from 172.16.0.1: Destination host unreachable.
Reply from 172.16.0.1: Destination host unreachable.
Reply from 172.16.0.1: Destination host unreachable.

Ping statistics for 172.16.0.126:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 172.16.0.125

Pinging 172.16.0.125 with 32 bytes of data:

Reply from 172.16.0.1: Destination host unreachable.
Reply from 172.16.0.1: Destination host unreachable.
Reply from 172.16.0.1: Destination host unreachable.
Reply from 172.16.0.1: Destination host unreachable.

Ping statistics for 172.16.0.125:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 172.16.0.65

Pinging 172.16.0.65 with 32 bytes of data:

Reply from 172.16.0.1: Destination host unreachable.
Reply from 172.16.0.1: Destination host unreachable.
Reply from 172.16.0.1: Destination host unreachable.
Reply from 172.16.0.1: Destination host unreachable.

Ping statistics for 172.16.0.65:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 172.16.0.1

Pinging 172.16.0.1 with 32 bytes of data:

Reply from 172.16.0.1: bytes=32 time=1ms TTL=255
Reply from 172.16.0.1: bytes=32 time<1ms TTL=255
Reply from 172.16.0.1: bytes=32 time<1ms TTL=255
Reply from 172.16.0.1: bytes=32 time<1ms TTL=255

Ping statistics for 172.16.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>|
```

☐ Top

Figura 15. Ejercicio 2, alumnos solo hacen ping a su Gateway.

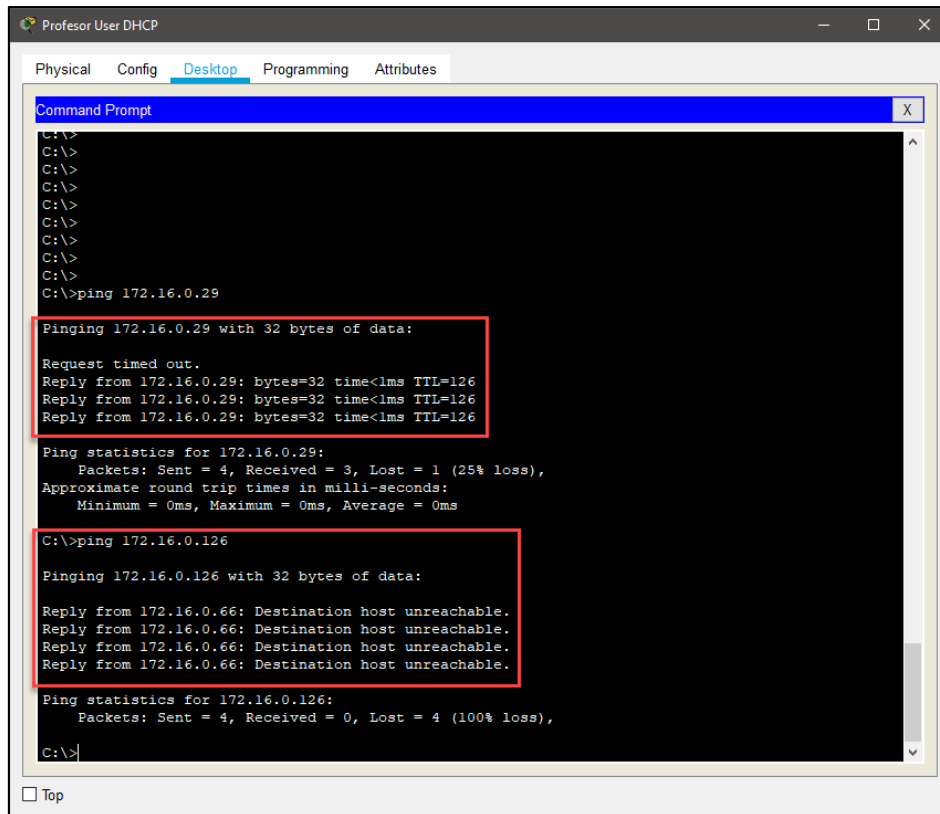


Figura 16. Ejercicio 2, profesor usuario solo ping a Alumnos.

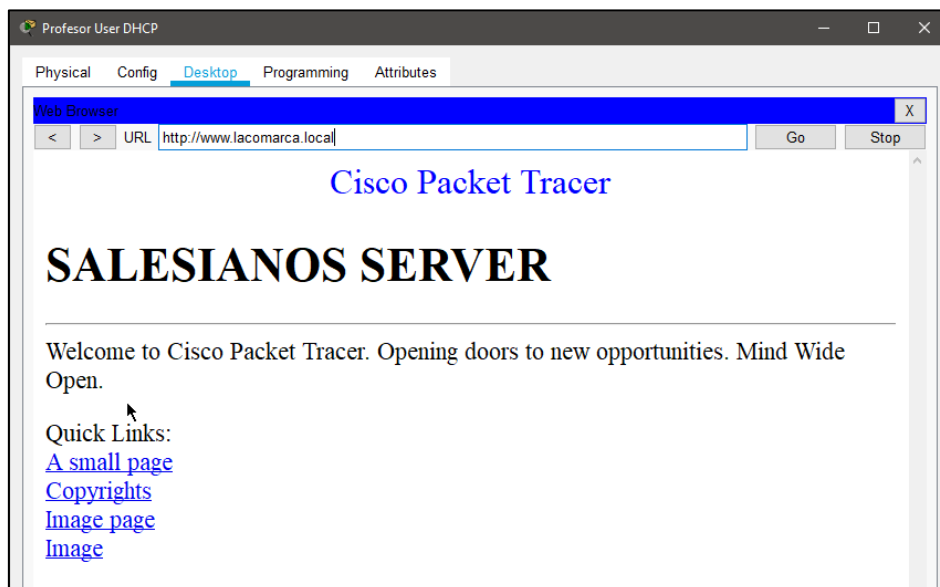


Figura 17. Ejercicio 2, comprobación DNS,TCP,HTTP en profesor usuario.

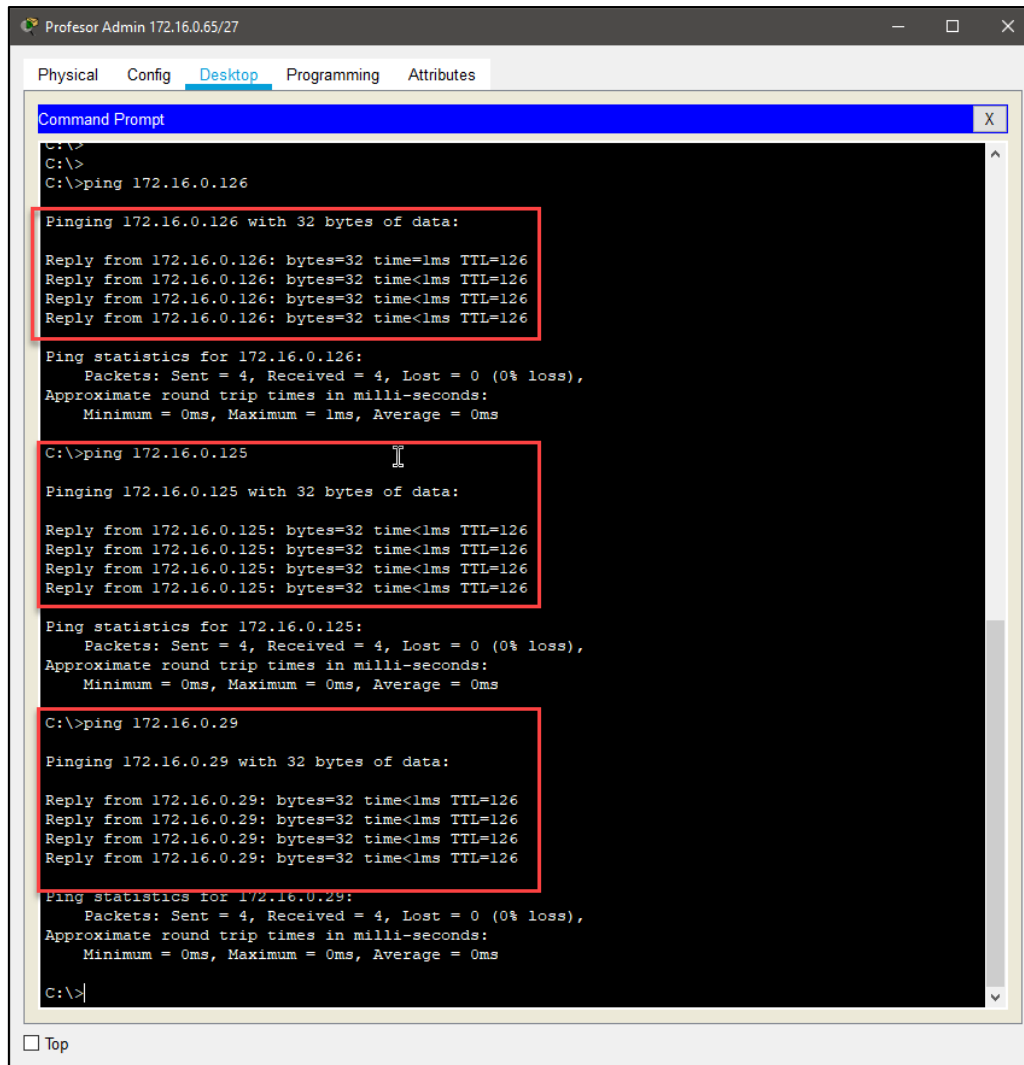


Figura 18. Ejercicio 2, comprobación profesor admin ICMP a resto de redes.

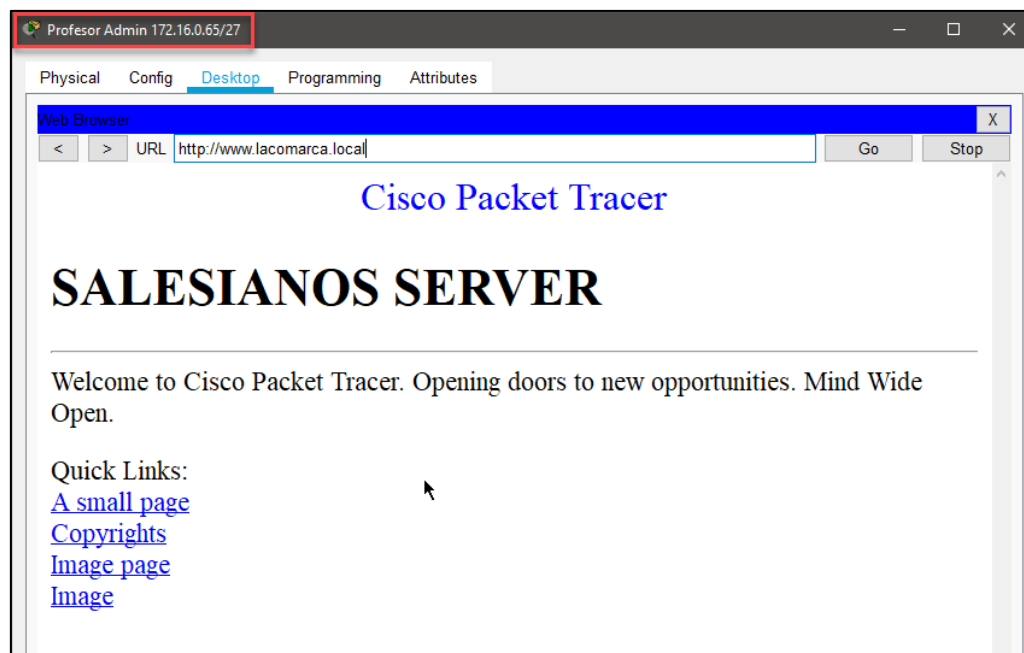


Figura 19. Ejercicio 2, comprobación profesor admin DNS,TCP,HTTP.

## Ejercicio 3

Implementa la red anterior con la condición de que el Servidor DNS sea Windows Server 2016/2012/2008. Salvo la subred de comunicación entre los routers y la red de servidores, las dos subredes restantes tendrán su propio servidor DHCP. Realiza las siguientes pruebas:

La implementación se ha realizado con un Windows Server 2016 instalado en un SSD en un equipo de escritorio al que se le ha conectado un router Mikrotik hexS.

En este router se ha montado toda la red, ya que por error se conectó el transformador de corriente de este (24v) al router secundario, un TP-LINK que solo soportaba 12v, por lo cual la red de profesores ha tenido que incorporarse al Mikrotik quedando fuera la parte de enrutamiento mediante RIP v2, aunque el resto ha seguido las pautas de trabajo.



Figura 20. Ejercicio 3, laboratorio.

- a. Indica el contenido de las tablas de enrutamiento de los routers, así como la configuración de enrutamiento de cada uno de ellos.

A continuación, se muestran las tablas de enrutamiento.

```
[admin@MikroTik] > ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
#      DST-ADDRESS      PREF-SRC      GATEWAY      DISTANCE
0 ADS  0.0.0.0/0             192.168.1.1   1
1 ADC  172.16.0.0/26         172.16.0.1   Alumnos      0
2 ADC  172.16.0.64/27        172.16.0.65  Profesores   0
3 ADC  172.16.0.96/27        172.16.0.97  Servidores   0
4 ADC  192.168.1.0/24        192.168.1.28 WAN          0
[admin@MikroTik] >
```

Figura 21. Ejercicio 3a, tablas de enrutamiento de Mikrotik.



- b. Demuestra que todos los hosts de todas las subredes pueden comunicarse entre sí.

```

C:\Windows\system32\cmd.exe

C:\Users\gon>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet 2:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::882b:b94e:371f:adec%10
    Dirección IPv4. . . . . : 172.16.0.126
    Máscara de subred . . . . . : 255.255.255.224
    Puerta de enlace predeterminada . . . . . : 172.16.0.97

Adaptador de túnel isatap.{8599D05E-6773-4635-89E8-F297A1D3A80C}:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . . :

C:\Users\gon>ping 172.16.0.29

Haciendo ping a 172.16.0.29 con 32 bytes de datos:
Respuesta desde 172.16.0.29: bytes=32 tiempo<1m TTL=127
Respuesta desde 172.16.0.29: bytes=32 tiempo<1m TTL=127
Respuesta desde 172.16.0.29: bytes=32 tiempo=1ms TTL=127
Respuesta desde 172.16.0.29: bytes=32 tiempo<1m TTL=127

Estadísticas de ping para 172.16.0.29:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms

C:\Users\gon>ping 172.16.0.66

Haciendo ping a 172.16.0.66 con 32 bytes de datos:
Respuesta desde 172.16.0.66: bytes=32 tiempo<1m TTL=127
Respuesta desde 172.16.0.66: bytes=32 tiempo<1m TTL=127
Respuesta desde 172.16.0.66: bytes=32 tiempo<1m TTL=127
Respuesta desde 172.16.0.66: bytes=32 tiempo<1m TTL=127

Estadísticas de ping para 172.16.0.66:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\gon>

```

Figura 22. Ejercicio 3b, Ping desde la red Servidores al resto de redes.

```

C:\WINDOWS\system32\cmd.exe

C:\Users\Gon>ping 172.16.0.29

Haciendo ping a 172.16.0.29 con 32 bytes de datos:
Respuesta desde 172.16.0.29: bytes=32 tiempo<1m TTL=127
Respuesta desde 172.16.0.29: bytes=32 tiempo=1ms TTL=127
Respuesta desde 172.16.0.29: bytes=32 tiempo<1m TTL=127
Respuesta desde 172.16.0.29: bytes=32 tiempo<1m TTL=127

Estadísticas de ping para 172.16.0.29:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 1ms, Media = 0ms

C:\Users\Gon>ping 172.16.0.126

Haciendo ping a 172.16.0.126 con 32 bytes de datos:
Respuesta desde 172.16.0.126: bytes=32 tiempo<1m TTL=127
Respuesta desde 172.16.0.126: bytes=32 tiempo<1m TTL=127
Respuesta desde 172.16.0.126: bytes=32 tiempo<1m TTL=127
Respuesta desde 172.16.0.126: bytes=32 tiempo<1m TTL=127

Estadísticas de ping para 172.16.0.126:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\Gon>

```

Figura 23. Ejercicio 3b. Ping desde la red Profesores al resto de redes.

```

C:\WINDOWS\system32\cmd.exe

Microsoft Windows [Versión 10.0.17763.503]
(c) 2018 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Gon>ping 172.16.0.126

Haciendo ping a 172.16.0.126 con 32 bytes de datos:
Respuesta desde 172.16.0.126: bytes=32 tiempo<1m TTL=127
Respuesta desde 172.16.0.126: bytes=32 tiempo=1ms TTL=127
Respuesta desde 172.16.0.126: bytes=32 tiempo<1m TTL=127
Respuesta desde 172.16.0.126: bytes=32 tiempo<1m TTL=127

Estadísticas de ping para 172.16.0.126:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 1ms, Media = 0ms

C:\Users\Gon>ping 172.16.0.66

Haciendo ping a 172.16.0.66 con 32 bytes de datos:
Respuesta desde 172.16.0.66: bytes=32 tiempo<1m TTL=127
Respuesta desde 172.16.0.66: bytes=32 tiempo<1m TTL=127
Respuesta desde 172.16.0.66: bytes=32 tiempo<1m TTL=127
Respuesta desde 172.16.0.66: bytes=32 tiempo<1m TTL=127

Estadísticas de ping para 172.16.0.66:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms

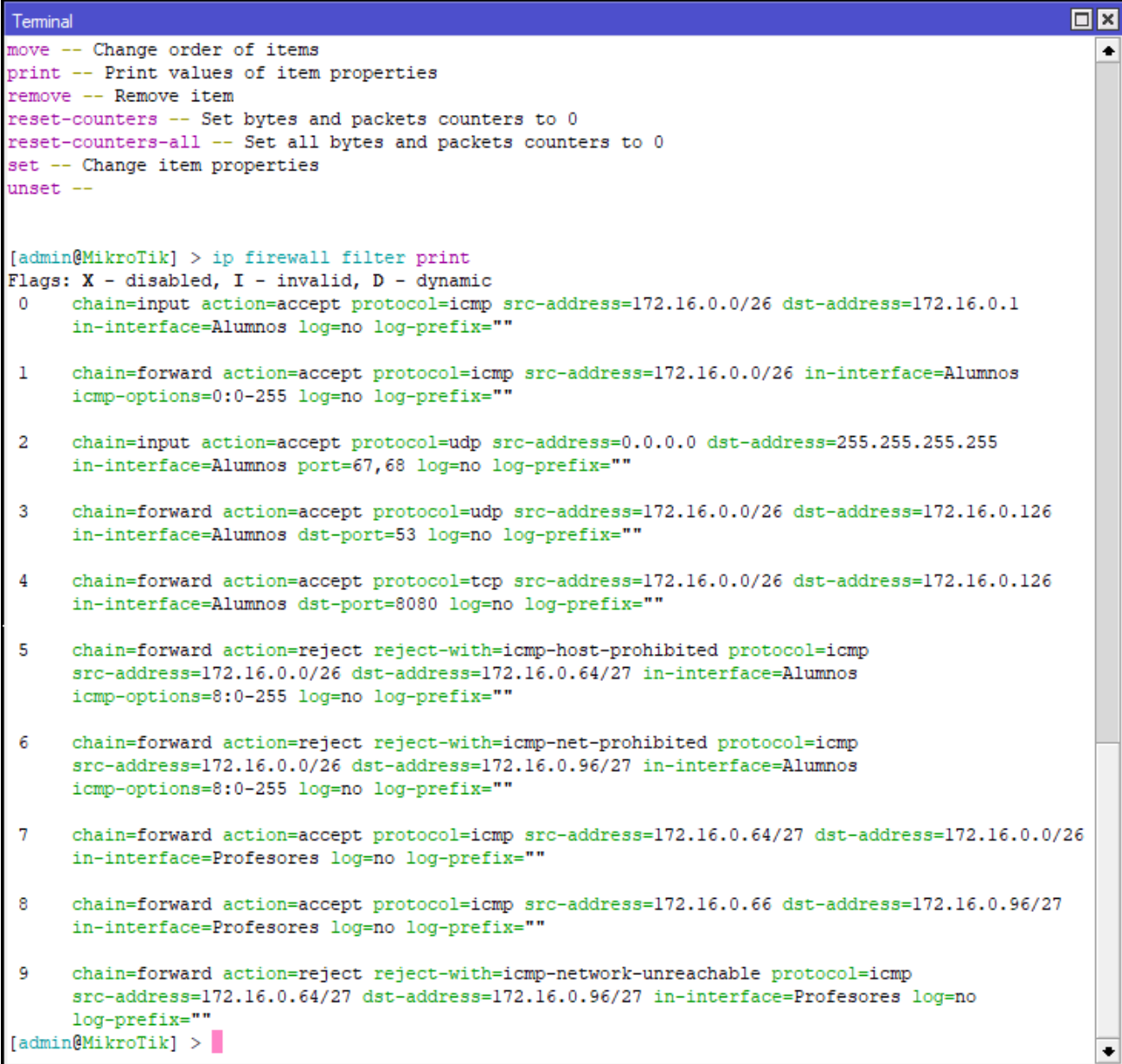
C:\Users\Gon>

```

Figura 24. Ejercicio 3b, Ping desde la red alumnos al resto de redes.

- c. En el router Mikrotik, aplica las políticas restrictivas que se ajusten al enunciado de la práctica.

La lista de reglas queda como se puede ver en la siguiente figura:



```

Terminal
move -- Change order of items
print -- Print values of item properties
remove -- Remove item
reset-counters -- Set bytes and packets counters to 0
reset-counters-all -- Set all bytes and packets counters to 0
set -- Change item properties
unset --

[admin@MikroTik] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
 0 chain=input action=accept protocol=icmp src-address=172.16.0.0/26 dst-address=172.16.0.1
  in-interface=Alumnos log=no log-prefix=""

 1 chain=forward action=accept protocol=icmp src-address=172.16.0.0/26 in-interface=Alumnos
  icmp-options=0:0-255 log=no log-prefix=""

 2 chain=input action=accept protocol=udp src-address=0.0.0.0 dst-address=255.255.255.255
  in-interface=Alumnos port=67,68 log=no log-prefix=""

 3 chain=forward action=accept protocol=udp src-address=172.16.0.0/26 dst-address=172.16.0.126
  in-interface=Alumnos dst-port=53 log=no log-prefix=""

 4 chain=forward action=accept protocol=tcp src-address=172.16.0.0/26 dst-address=172.16.0.126
  in-interface=Alumnos dst-port=8080 log=no log-prefix=""

 5 chain=forward action=reject reject-with=icmp-host-prohibited protocol=icmp
  src-address=172.16.0.0/26 dst-address=172.16.0.64/27 in-interface=Alumnos
  icmp-options=8:0-255 log=no log-prefix=""

 6 chain=forward action=reject reject-with=icmp-net-prohibited protocol=icmp
  src-address=172.16.0.0/26 dst-address=172.16.0.96/27 in-interface=Alumnos
  icmp-options=8:0-255 log=no log-prefix=""

 7 chain=forward action=accept protocol=icmp src-address=172.16.0.64/27 dst-address=172.16.0.0/26
  in-interface=Profesores log=no log-prefix=""

 8 chain=forward action=accept protocol=icmp src-address=172.16.0.66 dst-address=172.16.0.96/27
  in-interface=Profesores log=no log-prefix=""

 9 chain=forward action=reject reject-with=icmp-network-unreachable protocol=icmp
  src-address=172.16.0.64/27 dst-address=172.16.0.96/27 in-interface=Profesores log=no
  log-prefix=""
[admin@MikroTik] >

```

Figura 25. Ejercicio 3c, reglas firewall Mikrotik.

- d. Desde un host de la red de profesores, realiza una petición al servidor DHCP. Filtra el tráfico de red perteneciente únicamente al servicio DHCP e indica los comandos empleados.

El filtrado de las comunicaciones se realiza a través de Winbox estableciendo filtros para solo ver comunicaciones originarias de la red profesores.

The screenshot displays the Mikrotik WinBox Firewall configuration interface. The top window shows the 'Connections' tab with a list of active connections. The bottom window shows the 'Filter Rules' tab with a list of rules.

**Connections Window:**

Src. Address	Det. Address	Protocol	Connec...	Timeout	TCP State	Orig./Repl. Rate	Orig./Repl. Bytes
C 172.16.0.65	172.16.0.94	1 (icmp)		00:00:08		0 bps/0 bps	56 B/0 B
C 172.16.0.65.520	224.0.0.9.520	17 (udp)		00:00:09		0 bps/0 bps	132 B/0 B
C 172.16.0.94.68	172.16.0.65.67	17 (udp)		00:00:04		0 bps/0 bps	328 B/0 B
C 172.16.0.94.137	172.16.0.95.137	17 (udp)		00:00:09		0 bps/0 bps	288 B/0 B
SC 172.16.0.94.50999	172.16.0.126.53	17 (udp)		00:00:02		0 bps/0 bps	430 B/86 B
SAC 172.16.0.94.51690	172.16.0.126.53	17 (udp)		00:02:53		0 bps/0 bps	310 B/186 B
SAC 172.16.0.94.52543	172.16.0.126.53	17 (udp)		00:02:53		0 bps/0 bps	310 B/310 B
SC 172.16.0.94.55635	172.16.0.126.53	17 (udp)		00:00:02		0 bps/0 bps	300 B/60 B
C 172.16.0.94.56307	172.16.0.126.53	17 (udp)		00:00:09		0 bps/0 bps	86 B/0 B
C 172.16.0.94.56335	172.16.0.126.53	17 (udp)		00:00:09		0 bps/0 bps	69 B/0 B
C 172.16.0.94.58683	172.16.0.126.53	17 (udp)		00:00:03		0 bps/0 bps	228 B/0 B
SC 172.16.0.94.59573	172.16.0.126.53	17 (udp)		00:00:01		0 bps/0 bps	60 B/60 B
C 172.16.0.94.61361	172.16.0.126.53	17 (udp)		00:00:03		0 bps/0 bps	172 B/0 B

**Filter Rules Window:**

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Src. Ad...	Dst. Ad...	ICMP Options/IC...	Bytes	Packets
0	accept	input	172.16.0.0/26	172.16.0.1	1 (icmp)			Alumnos							0 B	0
1	accept	forward	172.16.0.0/26		1 (icmp)			Alumnos						0 (echo reply)	0 B	0
2	accept	input	172.16.0.0/26	172.16.0.1	17 (udp)	68	67	Alumnos							660 B	2
3	accept	input	172.16.0.64/27	172.16.0.65	17 (udp)	68	67	Profeso...							344 B	1
4	accept	forward	172.16.0.0/26	172.16.0.126	17 (udp)		53	Alumnos							6.2 KiB	96
5	accept	forward	172.16.0.0/26	172.16.0.126	6 (tcp)		8080	Alumnos							0 B	0
6	accept	forward	172.16.0.64/27	172.16.0.0/26	1 (icmp)			Profeso...							0 B	0
7	accept	forward	172.16.0.66	172.16.0.96/27	1 (icmp)			Profeso...							0 B	0
8	reject	forward	172.16.0.0/26	172.16.0.64/27	1 (icmp)			Alumnos					8 (echo request)	0 B	0	0
9	reject	forward	172.16.0.0/26	172.16.0.96/27	1 (icmp)			Alumnos					8 (echo request)	0 B	0	0
10	reject	forward	172.16.0.64/27	172.16.0.96/27	1 (icmp)			Profeso...							896 B	10

11 items (1 selected)

Figura 26. Ejercicio 3d, filtrado del tráfico DHCP y paquetes capturados en la regla del firewall.

- e. Desde un host que se encuentre en la red de alumnos, realiza una petición al servidor DHCP. Filtra el tráfico de red perteneciente únicamente al servicio DHCP e indica los comandos empleados.

El filtrado de las comunicaciones para este caso también se realizó a través de Winbox estableciendo filtros para solo ver comunicaciones originarias de la red alumnos.

The image consists of two screenshots from the Mikrotik WinBox interface, showing firewall rule configuration and connection tracking.

**Top Screenshot: Firewall Rule Configuration**

The 'Filter Rules' tab is active. A list of 10 rules is shown. Rule 2 is selected and highlighted in red. It is an 'accept' rule for the 'input' chain, filtering traffic from the 'Alumnos' interface (172.16.0.0/26) to the 'Profeso...' interface (172.16.0.0/26) using protocol 17 (UDP) on port 68. The rule is named '0 (echo reply)'.

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Src. Ad...	Dst. Ad...	ICMP Options/IC...	Bytes	Packets
0	accept	input	172.16.0.0/26	172.16.0.1	1 (icmp)			Alumnos						0 (echo reply)	0 B	0
1	accept	forward	172.16.0.0/26	172.16.0.126	1 (icmp)			Alumnos							0 B	0
2	accept	input	172.16.0.0/26	172.16.0.1	17 (udp)	68	67	Alumnos							330 B	1
3	accept	forward	172.16.0.0/26	172.16.0.126	17 (udp)		53	Alumnos							0 B	0
4	accept	forward	172.16.0.0/26	172.16.0.126	6 (tcp)		8080	Alumnos							0 B	0
5	reject	forward	172.16.0.0/26	172.16.0.64/27	1 (icmp)			Alumnos					8 (echo request)		0 B	0
6	reject	forward	172.16.0.0/26	172.16.0.96/27	1 (icmp)			Alumnos					8 (echo request)		0 B	0
7	accept	forward	172.16.0.64/27	172.16.0.0/26	1 (icmp)			Profeso...							0 B	0
8	accept	forward	172.16.0.66	172.16.0.96/27	1 (icmp)			Profeso...							0 B	0
9	reject	forward	172.16.0.64/27	172.16.0.96/27	1 (icmp)			Profeso...							0 B	0

10 items (1 selected)

**Bottom Screenshot: Connection Tracking**

The 'Tracking' tab is active. It shows a list of connections. The connection from 172.16.0.29.68 to 172.16.0.1.67 is selected and highlighted in red. It is a UDP connection on port 17.

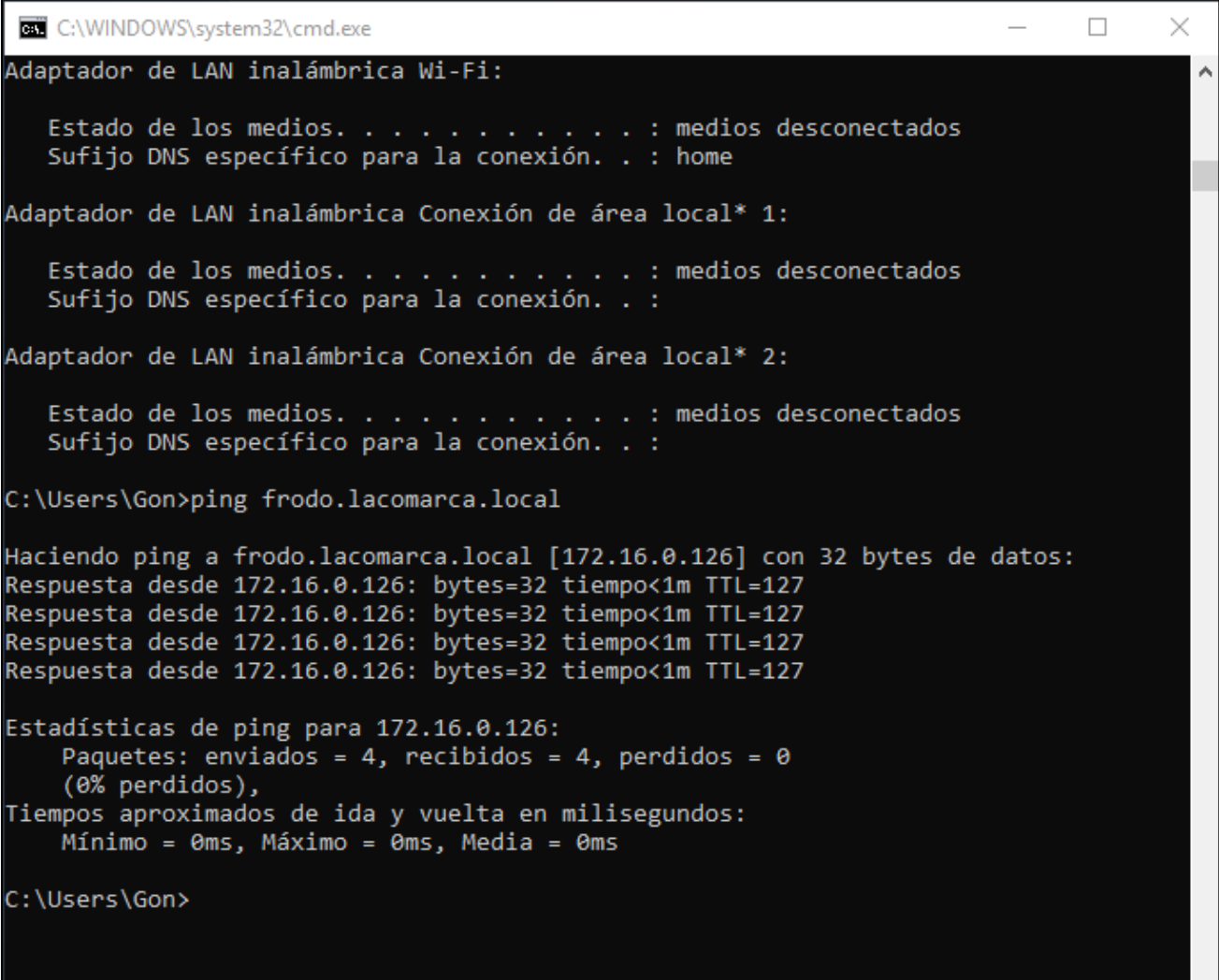
	Src. Address	/	Dst. Address	Protocol	Connecti...	Timeout	TCP State	Orig./Repl. Rate	Orig./Repl. Bytes
C	172.16.0.1	/	224.0.0.22	2 (icmp)		00:06:14	0 bps/0 bps	1560 B/0 B	
C	172.16.0.29.68	/	172.16.0.1.67	17 (udp)		00:00:00	0 bps/0 bps	330 B/0 B	
SC	172.16.0.29.52943	/	172.16.0.126.53	17 (udp)		00:00:08	0 bps/0 bps	310 B/62 B	
SAC	172.16.0.29.55333	/	172.16.0.126.53	17 (udp)		00:02:11	0 bps/0 bps	248 B/248 B	
SAC	172.16.0.29.56544	/	172.16.0.126.53	17 (udp)		00:01:45	0 bps/0 bps	124 B/124 B	
C	172.16.0.29.64139	/	172.16.0.126.53	17 (udp)		00:00:09	520 bps/0 bps	325 B/0 B	

6 items out of 16 (1 selected) | Max Entries: 472320

Figura 27. Ejercicio 3e, filtrado del tráfico DHCP y paquetes capturados en la regla del firewall.

- f. Desde el host 172.16.0.65/27, envía un mensaje de tipo "echo ICMP" al servidor de DNS utilizando su FQDN.

Como el método de trabajo exige que la dirección mas baja sea la de la puerta de enlace, el equipo administrador de la red de profesores tiene la IP 172.16.0.66 en lugar de la .65. que corresponde a la puerta de enlace de esa red.



```
C:\WINDOWS\system32\cmd.exe

Adaptador de LAN inalámbrica Wi-Fi:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . : home

Adaptador de LAN inalámbrica Conexión de área local* 1:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :

Adaptador de LAN inalámbrica Conexión de área local* 2:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :

C:\Users\Gon>ping frodo.lacomarca.local

Haciendo ping a frodo.lacomarca.local [172.16.0.126] con 32 bytes de datos:
Respuesta desde 172.16.0.126: bytes=32 tiempo<1m TTL=127
Respuesta desde 172.16.0.126: bytes=32 tiempo<1m TTL=127
Respuesta desde 172.16.0.126: bytes=32 tiempo<1m TTL=127
Respuesta desde 172.16.0.126: bytes=32 tiempo<1m TTL=127

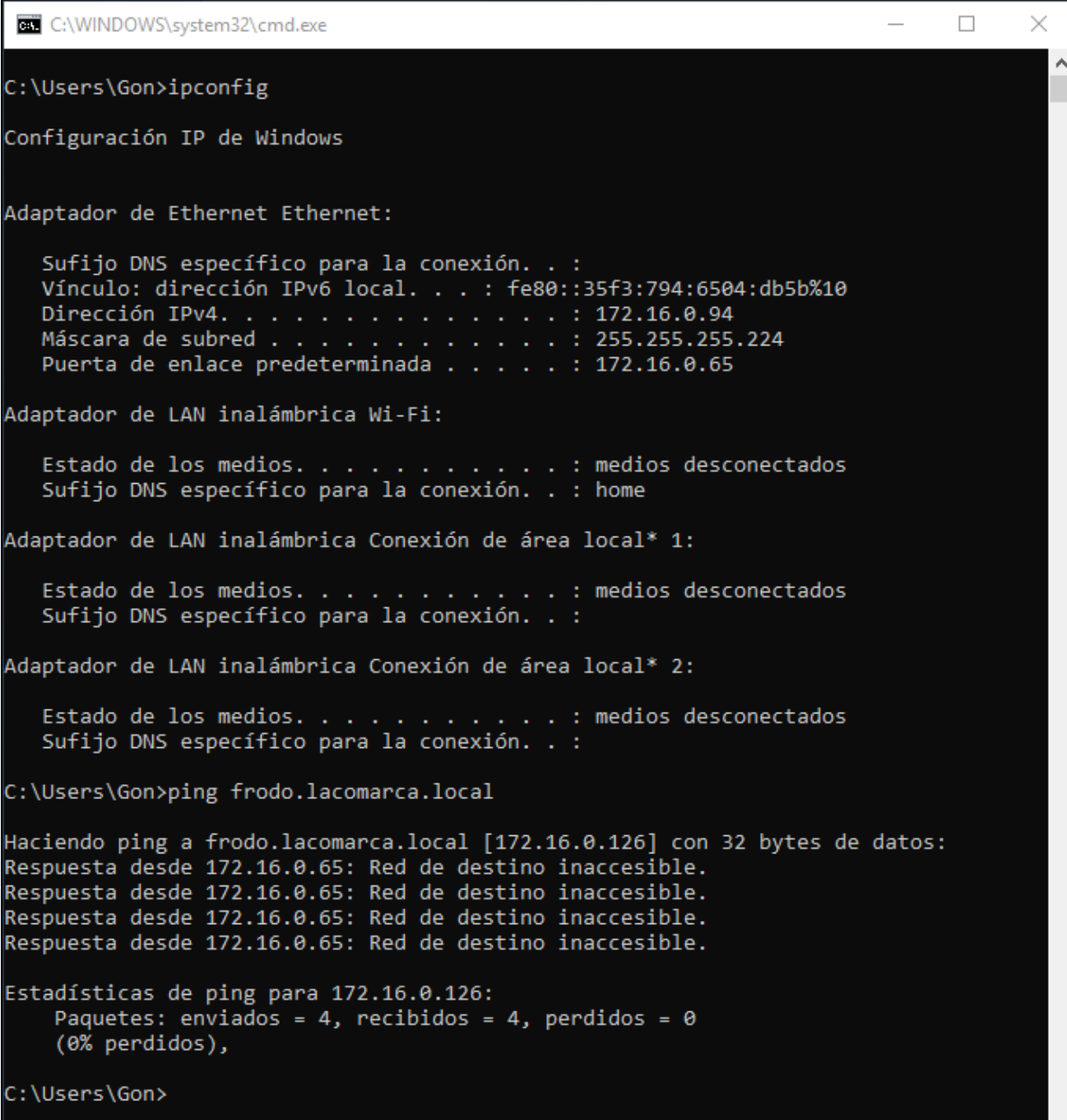
Estadísticas de ping para 172.16.0.126:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\Gon>
```

Figura 28. Ejercicio 3f, ping al FQDN del servidor DNS desde el profesor admin.

- g. Realiza el apartado anterior pero ahora desde un host que se encuentre en la red de profesores pero que no sea el anterior.

Ahora enviamos la misma solicitud, pero desde la posición de un profesor normal, su ip ahora viene dada por el DHCP.



```

C:\WINDOWS\system32\cmd.exe

C:\Users\Gon>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::35f3:794:6504:db5b%10
    Dirección IPv4. . . . . : 172.16.0.94
    Máscara de subred . . . . . : 255.255.255.224
    Puerta de enlace predeterminada . . . . . : 172.16.0.65

Adaptador de LAN inalámbrica Wi-Fi:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . : home

Adaptador de LAN inalámbrica Conexión de área local* 1:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :

Adaptador de LAN inalámbrica Conexión de área local* 2:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :

C:\Users\Gon>ping frodo.lacomarca.local

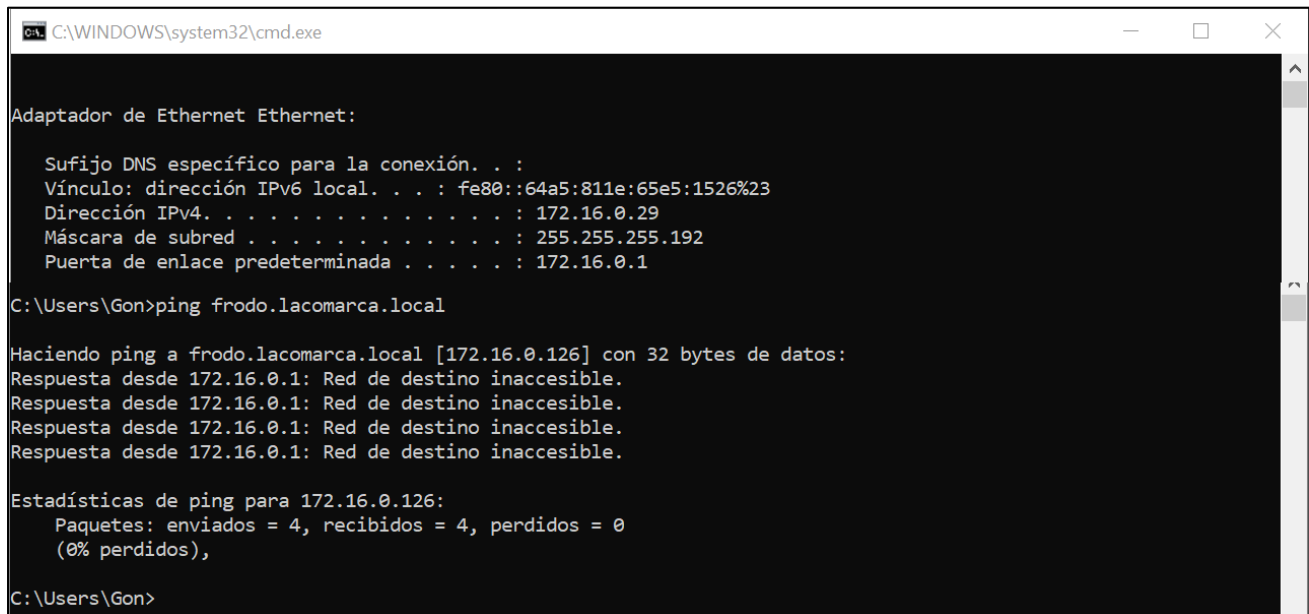
Haciendo ping a frodo.lacomarca.local [172.16.0.126] con 32 bytes de datos:
Respuesta desde 172.16.0.65: Red de destino inaccesible.
Respuesta desde 172.16.0.65: Red de destino inaccesible.
Respuesta desde 172.16.0.65: Red de destino inaccesible.
Respuesta desde 172.16.0.65: Red de destino inaccesible.

Estadísticas de ping para 172.16.0.126:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),

C:\Users\Gon>
  
```

Figura 29. Ejercicio 3g, ping al FQDN desde el profesor normal.

h. Realiza el apartado anterior pero ahora desde un host que se encuentre en la red de alumnos.



```

C:\WINDOWS\system32\cmd.exe

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . . : fe80::64a5:811e:65e5:1526%23
    Dirección IPv4. . . . . : 172.16.0.29
    Máscara de subred . . . . . : 255.255.255.192
    Puerta de enlace predeterminada . . . . . : 172.16.0.1

C:\Users\Gon>ping frodo.lacomarca.local

Haciendo ping a frodo.lacomarca.local [172.16.0.126] con 32 bytes de datos:
Respuesta desde 172.16.0.1: Red de destino inaccesible.
Respuesta desde 172.16.0.1: Red de destino inaccesible.
Respuesta desde 172.16.0.1: Red de destino inaccesible.
Respuesta desde 172.16.0.1: Red de destino inaccesible.

Estadísticas de ping para 172.16.0.126:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),

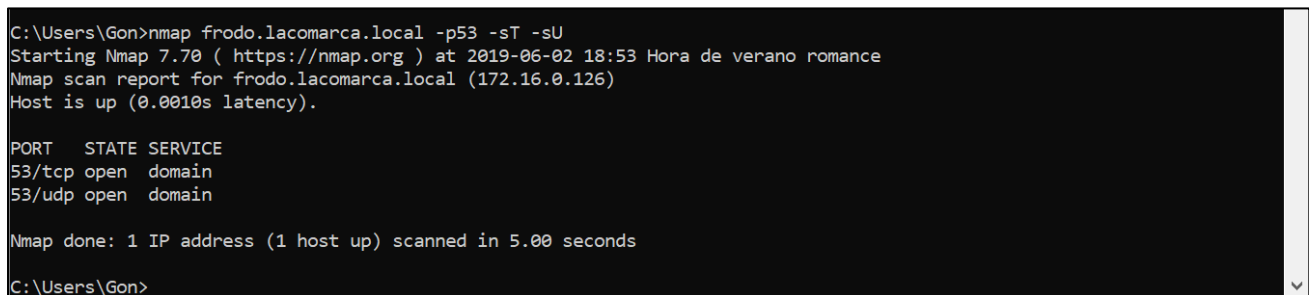
C:\Users\Gon>
  
```

Figura 30. Ejercicio 3h, ping a FQDN del servidor DNS desde un host Alumno.

i. Desde un host que se encuentre en la red de alumnos ejecuta el siguiente comando: "nmap FQDN\_DNS\_Server -p53 -sT -sU". Investiga qué significan los flags anteriores de nmap. ¿Qué resultados obtienes?

Los flags utilizados piden a nmap que escanee el puerto 53 tanto tcp como udp.

El resultado es el siguiente:



```

C:\Users\Gon>nmap frodo.lacomarca.local -p53 -sT -sU
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-02 18:53 Hora de verano romance
Nmap scan report for frodo.lacomarca.local (172.16.0.126)
Host is up (0.0010s latency).

PORT      STATE SERVICE
53/tcp    open  domain
53/udp    open  domain

Nmap done: 1 IP address (1 host up) scanned in 5.00 seconds
C:\Users\Gon>
  
```

Figura 31. Ejercicio 3i, resultados Nmap.



- j. Realiza el apartado anterior, pero esta vez utilizando el flag "-Pn". ¿Qué diferencia aprecias analizando el tráfico de red con el apartado anterior?

Al existir reglas que permiten las comunicaciones DNS(udp 53) y tcp sin puerto de origen, estos puertos aparecen abiertos, véase la Figura 25. Ejercicio 3c, reglas firewall Mikrotik.

El flag -Pn que trata los hosts como si estuvieran ya online (no hace host Discovery) no ha tenido el efecto deseado para comparar con el anterior.

```
C:\Users\Gon>nmap frodo.lacomarca.local -p53 -sT -sU -Pn
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-02 19:02 Hora de verano romance
Nmap scan report for frodo.lacomarca.local (172.16.0.126)
Host is up (0.0018s latency).

PORT      STATE SERVICE
53/tcp    open  domain
53/udp    open  domain

Nmap done: 1 IP address (1 host up) scanned in 4.79 seconds
C:\Users\Gon>
```

Figura 32. Ejercicio 3j, las reglas en el router impiden ver la diferencia con el comando anterior.

- k. Desde un host de la red de profesores y desde otro host de la red alumnos, abre un navegador y realiza la petición "http://www.lacomarca.local".

Página web desde el host en alumnos.

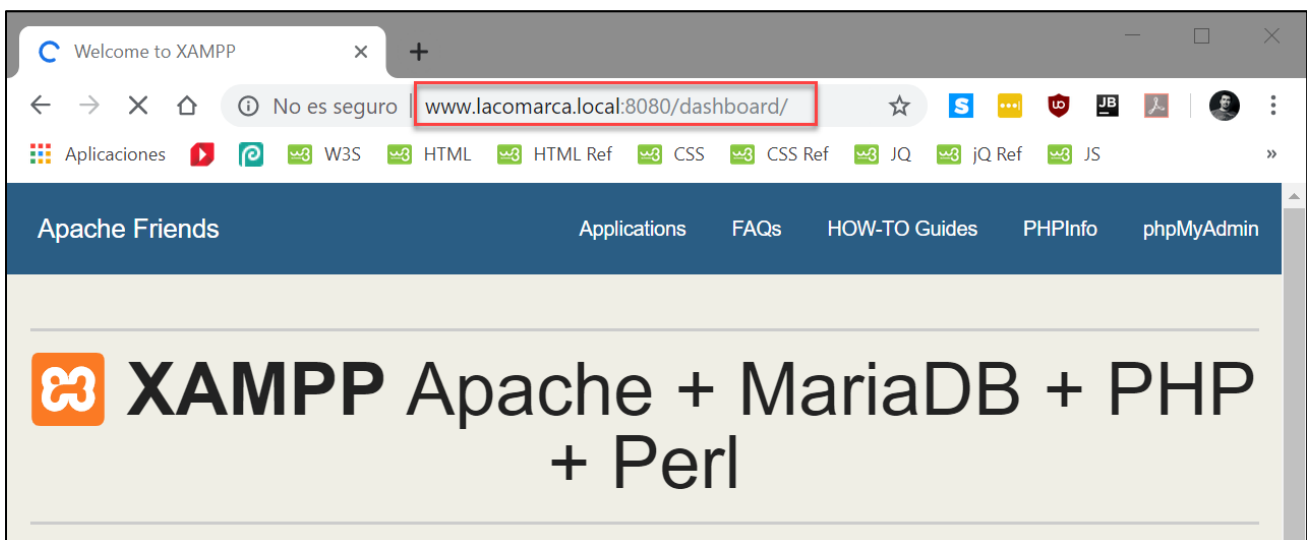


Figura 33. Ejercicio 3k, página web visitada desde un host alumno.

Página web visitada desde un host profesor.

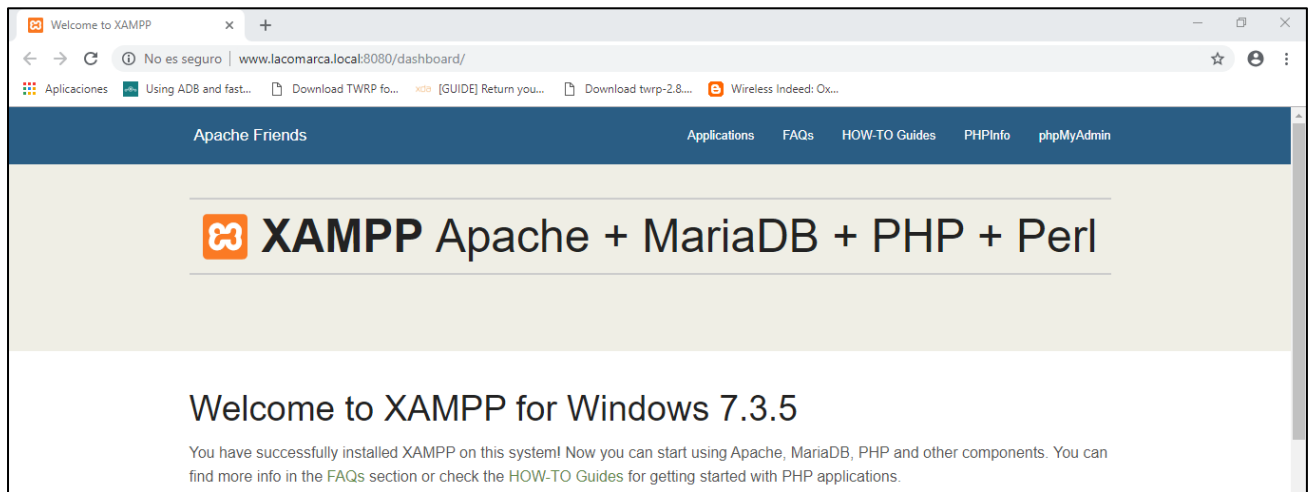


Figura 34. Ejercicio 3k, página web funcionando desde un host profesor.

## Ejercicio 4

**Indica las dificultades que han aparecido a lo largo de la práctica.**

Hasta el ejercicio 2 la complicación viene dada por las ACL ya que un mínimo fallo en cualquier dirección puede echar a perder la configuración, esta, al ser secuencial y exclusiva (una vez que algo es denegado ya no sigue la secuencia) es una tarea delicada que ha requerido de diversas correcciones ya que al intentar ahorrar tiempo y copiar las partes útiles entre ACL's siempre quedan errores.

La simulación con todos los requisitos de DHCP, DNS, TCP, UDP, RIPv2... ha llevado un proceso de investigación y búsqueda de información en la documentación de CISCO, así como información sobre los puertos y funcionamiento de los diversos protocolos.

Sin duda la parte más difícil ha sido la implementación en una red real ya que surgieron problemas a la hora de instalar Windows Server en una máquina real sin virtualización, por culpa de la controladora SATA del equipo y algún tipo de problema en el particionamiento que realiza Windows Server y esta, descubrir que el problema se solucionaba particionando completamente la unidad sin crear particiones más pequeñas por un problema de compatibilidad con esa controladora en particular me llevo 3 horas, lo cual retraso bastante el avance.

La instalación de Windows Server es bastante sencilla y la creación del servidor DNS en principio no tuvo ningún problema por la experiencia obtenida en la práctica de Implantación de Sistemas Operativos.

Los problemas reales han llegado al trabajar con el router mikrotik y la inmensa cantidad de opciones, así como la metodología para crear las reglas del firewall que al ser tan abierta al contrario que con cisco que es completamente metódica ha supuesto unas 6 horas de dedicación y experimentación, no hay comparación entre la simulación que hace Packet Tracer del router de Cisco con la tremenda cantidad de opciones y posibilidades que ofrece el hardware de Mikrotik.

Los continuos fallos en el direccionamiento y consultas de los datos de las redes y las puertas de enlace también ha supuesto un hándicap a la hora de trabajar.

Toda la parte de las reglas del firewall ha sido creada "con alfileres" lo justo para que funcione sin tener intención ninguna de pulir o crear un entorno seguro como demuestra la prueba con nmap en el ejercicio 3, en la que la segunda propuesta y la primera no obtuvieron resultados diferentes por la forma en la que el firewall estaba configurado, sin embargo, las reglas que solicitaba el ejercicio se cumplieron.