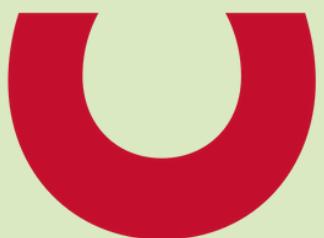


TECNOLOGIA DE REDES



OMAR ACUÑA 13097

ÍNDICE

- 01** CISCO PACKET TRACER
- 02** DESCRIPCIÓN DE PRÁCTICA
- 03** GLOSARIO DE CONCEPTOS Y COMANDOS
- 04** TOPOLOGÍA
- 05** CONFIGURACIÓN
- 06** RESULTADOS



CISCO PACKET TRACER



CISCO PACKET TRACER ES UNA HERRAMIENTA DE SIMULACIÓN DE REDES DESARROLLADA POR CISCO SYSTEMS, DISEÑADA PARA FACILITAR EL APRENDIZAJE Y LA ENSEÑANZA EN EL CAMPO DE LAS REDES INFORMÁTICAS. PERMITE A LOS USUARIOS DISEÑAR, CONFIGURAR Y SIMULAR REDES COMPLEJAS EN UN ENTORNO VIRTUAL SIN NECESIDAD DE HARDWARE FÍSICO. ESTA HERRAMIENTA ES FUNDAMENTAL TANTO PARA ESTUDIANTES COMO PARA PROFESIONALES QUE DESEAN PRACTICAR Y MEJORAR SUS HABILIDADES EN LA CONFIGURACIÓN Y ADMINISTRACIÓN DE REDES.

INTRODUCCIÓN:

Este manual guía la configuración de una red segmentada en múltiples VLANs utilizando Cisco Packet Tracer. El laboratorio refuerza conceptos como segmentación con VLANs, enrutamiento dinámico con EIGRP y seguridad con firewalls, listas de acceso, y administración remota mediante Telnet. La red se organiza en dos segmentos, cada uno con varias VLANs, un switch central, un router y un firewall para controlar el tráfico. Además, se incluye la configuración de un servidor DHCP para la asignación automática de direcciones IP, mejorando la gestión de red. También se ha añadido una zona DMZ con un router y un switch DMZ, donde se conectan un DNS-WEB Server y un FTP Server, incrementando la seguridad.

DESCRIPCIÓN DE LA PRÁCTICA

OBJETIVO:

El objetivo de este manual es proporcionar una guía paso a paso para configurar una red segmentada en VLANs utilizando Cisco Packet Tracer, centrándose en los siguientes aspectos clave:

- Conexión básica de dispositivos: Establecimiento de conexiones físicas y lógicas entre PCs, switches, routers y firewalls, asegurando la correcta distribución del tráfico en la red.
- Implementación de VLANs y enrutamiento: Configuración de múltiples VLANs en switches y el uso de subinterfaces en routers para permitir la comunicación inter-VLAN, gestionando adecuadamente el tráfico entre diferentes segmentos de red.
- Configuración de EIGRP: Implementación de EIGRP como protocolo de enrutamiento para facilitar la comunicación eficiente entre los routers, garantizando la distribución dinámica de rutas dentro de la red.
- Implementación de seguridad con firewalls: Configuración de listas de control de acceso (ACL) en el firewall para filtrar el tráfico entre las VLANs y proteger los segmentos de red de accesos no autorizados.
- Configuración de la zona DMZ: Creación de una nueva interfaz en el firewall conectada a un Router DMZ y un Switch DMZ, con un DNS-WEB Server y un FTP Server, para proporcionar mayor seguridad a los servicios expuestos a internet.
- Configuración de DHCP: Implementación de un servidor DHCP para la asignación automática de direcciones IP, simplificando la gestión de red y reduciendo errores en la configuración manual.
- Configuración de Telnet: Habilitación de Telnet en dispositivos clave para permitir la administración remota, facilitando el acceso y gestión desde ubicaciones externas.
- Verificación y solución de problemas: Uso de herramientas de diagnóstico y monitoreo para verificar la conectividad, identificar errores y asegurar el correcto funcionamiento de la red.

Al completar este manual, los usuarios adquirirán una comprensión profunda sobre cómo configurar y gestionar una red segmentada utilizando VLANs, enrutamiento EIGRP y seguridad basada en firewalls. Además, se reforzarán los conceptos clave de segmentación de tráfico, protocolos de enrutamiento dinámico, configuración de Telnet y DHCP, y la implementación de listas de control de acceso en un entorno de red.

DETALLES:

- Google

- 1 CORE Switch con 3 LANs

- IP .1 Gateway, IP .2 PC

- Vlan 100 – 10.1.1.1 255.255.255.0

- Vlan 200 – 10.2.1.1 255.255.255.0

- Vlan 300 – 10.3.1.1 255.255.255.0

- Switch a Router WAN1

- 11.11.11.0/30

- Router a Firewall WAN2

- 12.12.12.0/30

- ULSA

- 1 CORE Switch con 3 LANs

- IP .1 Gateway, IP .2 PC

- Vlan 400 – 10.4.1.1 255.255.255.0

- Vlan 500 – 10.5.1.1 255.255.255.0

- Vlan 600 – 10.6.1.1 255.255.255.0

- Switch a Router WAN1

- 14.14.14.0/30

- Router a Firewall WAN2

- 13.13.13.0/30

- ULSA DMZ

- 1 CORE Switch con 3 LANs

- IP .1 Gateway IP

- Vlan 700 – 10.7.x.1/24 – PC 10.7.x.7x

- Vlan 800 – 10.8.x.1/24 – PC 10.8.x.8x

- Vlan 900 – 10.9.x.1/24 – PC 10.9.x.9x

GLOSARIO DE DEFINICIONES

ANEXO DE DEFINICIONES UTILIZADAS DURANTE EL MANUAL

1. VLAN (Virtual Local Area Network):

Red lógica que agrupa dispositivos para segmentar el tráfico, mejorando el rendimiento y la seguridad

2. Gateway:

Dispositivo que conecta diferentes redes y actúa como punto de entrada o salida

3. Switch Core:

Switch central que maneja el tráfico entre VLANs y puede funcionar como enrutador

4. Subinterfaz:

Interfaz lógica en un router para manejar múltiples VLANs en una sola interfaz física

5. EIGRP (Enhanced Interior Gateway Routing Protocol):

Protocolo de enrutamiento dinámico que intercambia rutas entre routers en un sistema autónomo

6. ACL (Access Control List):

Lista de reglas que controla el tráfico permitido o denegado en una red

7. WAN (Wide Area Network):

Red que conecta redes locales en diferentes ubicaciones geográficas a través de enlaces de alta velocidad

8. Autonomous System (AS):

Conjunto de redes bajo una sola administración, identificado por un número único, utilizado en BGP

9. Firewalls:

Dispositivos que filtran el tráfico de red para proteger los recursos y controlar el acceso

11. DMZ (Demilitarized Zone):

Segmento de red aislado entre una red interna y externa donde se colocan servicios públicos, proporcionando mayor seguridad a la red interna

12. DNS-WEB Server:

Servidor dentro de la DMZ que gestiona peticiones DNS y aloja páginas web, permitiendo acceso público sin comprometer la red interna

13. FTP Server:

Servidor de archivos dentro de la DMZ que permite la transferencia de archivos a usuarios externos, manteniendo la seguridad de la red interna

14. Telnet:

Protocolo para acceder y controlar dispositivos remotamente por texto, sin cifrado.

15. DHCP:

Protocolo que asigna IPs automáticamente en una red.

GLOSARIO DE COMANDOS

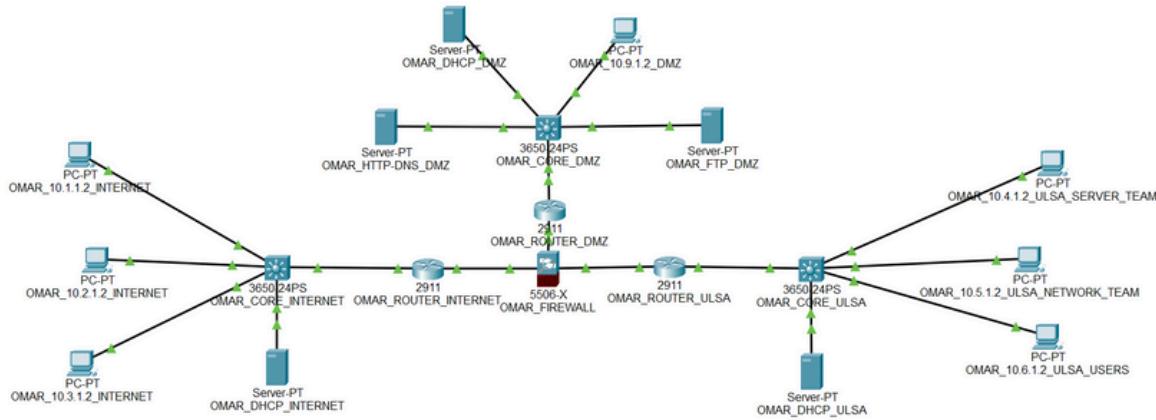
ANEXO DE COMANDOS UTILIZADAS DURANTE EL MANUAL

1. **enable:** Entra en el modo privilegiado del dispositivo.
2. **conf t:** Abre la configuración global en modo terminal.
3. **int Gi1/0/1, int Gi1/0/2, int Gi1/0/3, int Gi1/0/24, int Gi0/0, int Gi0/1, int Gi1/1, int Gi1/2:** Selecciona una interfaz específica del switch o router para configurar.
4. **description:** Añade una descripción a la interfaz para identificar su función.
5. **switchport mode access:** Configura la interfaz como puerto de acceso.
6. **switchport access vlan 100/200/300/400/500/600:** Asigna la interfaz a una VLAN específica
7. **no shut:** Habilita la interfaz (activa el puerto).
8. **ip routing:** Habilita el enrutamiento IP en el dispositivo.
9. **interface vlan 100/200/300/400/500/600:** Configura la interfaz VLAN con la que el switch o router interactúa.
10. **ip address [dirección IP] [máscara de subred]:** Asigna una dirección IP y máscara de subred a una interfaz.
11. **ip helper address:** Es un comando para redirigir paquetes de broadcast hacia un servidor específico en otra red.
12. **ROUTER EIGRP 100:** Inicia el protocolo de enrutamiento EIGRP con el número de sistema autónomo 100.
13. **NETWORK [dirección IP]:** Define las redes a las que se aplica el protocolo EIGRP.
14. **REDISTRIBUTE CONNECTED:** Redistribuye las rutas conectadas directamente en el protocolo de enrutamiento EIGRP.
15. **no switchport:** Convierte la interfaz de capa 2 a capa 3, lo que permite asignar direcciones IP.
16. **nameif [nombre]:** Asigna un nombre a la interfaz (normalmente en dispositivos con firewall).
17. **security-level [nivel]:** Define el nivel de seguridad de una interfaz (usualmente en firewalls, como el ASA de Cisco).a.
18. **Username [nombre] password [contraseña]:** Crea un usuario local con su respectiva contraseña.
19. **access-list INTERNET/ULSA extended permit/deny:** Crea una lista de acceso extendida que permite o deniega tráfico específico basado en la IP, protocolo, y puerto.
20. **access-group [nombre de lista] in interface [nombre interfaz]:** Aplica la lista de acceso a una interfaz específica.
21. **deny ip any any:** Deniega todo el tráfico IP.

TOPOLOGIA

ACOMODO DE LOS DISPOSITIVOS DE HARDWARE PARA EL FUNCIONAMIENTO DE LA RED

COLOCAR HARDWARE



En esta topología, se implementa una red que consta de 6 PCs, 3 cores, 3 routers, 3 servers DHCP y 2 servers interconectados con un Firewall de la siguiente manera para simular la conexión de distintas redes pertenecientes a INTERNET, ULSA (Universidad La Salle) y DMZ. Los dispositivos están configurados para permitir la comunicación entre diferentes subredes y la interconexión entre los routers mediante enlaces WAN.

Conexión de PCs a Cores:

- Pc1 (Internet) está conectada al core (Internet) mediante la interfaz FastEthernet 0 de la PC a la interfaz GigabitEthernet 1/0/1 del switch.
- Pc2 (Internet) está conectada al core (Internet) mediante la interfaz FastEthernet 0 de la PC a la interfaz GigabitEthernet 1/0/2 del switch.
- Pc3 (Internet) está conectada al core (Internet) mediante la interfaz FastEthernet 0 de la PC a la interfaz GigabitEthernet 1/0/3 del switch.
- Pc1 (ULSA) está conectada al core (ULSA) mediante la interfaz FastEthernet 0 de la PC a la interfaz GigabitEthernet 1/0/1 del switch.
- Pc2 (ULSA) está conectada al core (ULSA) mediante la interfaz FastEthernet 0 de la PC a la interfaz GigabitEthernet 1/0/2 del switch.
- Pc3 (ULSA) está conectada al core (ULSA) mediante la interfaz FastEthernet 0 de la PC a la interfaz GigabitEthernet 1/0/3 del switch.
- Pc4 (Dmz) está conectada al core (Dmz) mediante la interfaz FastEthernet 0 de la PC a la interfaz GigabitEthernet 1/0/3 del switch.

Conexión de Servers a Cores:

- Server1 (Dmz) está conectada al core (Dmz) mediante la interfaz FastEthernet 0 del server a la interfaz GigabitEthernet 1/0/1 del switch.
- Server2 (Dmz) está conectada al core (Dmz) mediante la interfaz FastEthernet 0 del server a la interfaz GigabitEthernet 1/0/2 del switch.
- Server (DHCP1) está conectada al core (Internet) mediante la interfaz FastEthernet 0 del server a la interfaz GigabitEthernet 1/0/4 del switch.
- Server (DHCP2) está conectada al core (ULSA) mediante la interfaz FastEthernet 0 del server a la interfaz GigabitEthernet 1/0/4 del switch.
- Server (DHCP3) está conectada al core (Dmz) mediante la interfaz FastEthernet 0 del server a la interfaz GigabitEthernet 1/0/4 del switch.

Conexión de Cores a Routers:

- Core (Internet) está conectado al router (Internet) mediante la interfaz GigabitEthernet 1/0/24 del core a la interfaz GigabitEthernet 0/0 del router.
- Core (ULSA) está conectado al router (ULSA) mediante la interfaz GigabitEthernet 1/0/24 del core a la interfaz GigabitEthernet 0/0 del router.
- Core (Dmz) está conectado al router (Dmz) mediante la interfaz GigabitEthernet 1/0/24 del core a la interfaz GigabitEthernet 0/0 del router.

Conexión al Firewall:

- Router (Internet) está conectado al firewall mediante la interfaz GigabitEthernet 0/1 del router (Internet) a la interfaz GigabitEthernet 1/1 del firewall.
- Router (ULSA) está conectado al firewall mediante la interfaz GigabitEthernet 0/1 del router (ULSA) a la interfaz GigabitEthernet 1/2 del firewall.
- Router (Dmz) está conectado al firewall mediante la interfaz GigabitEthernet 0/1 del router (Dmz) a la interfaz GigabitEthernet 1/3 del firewall.

CONFIGURACIÓN

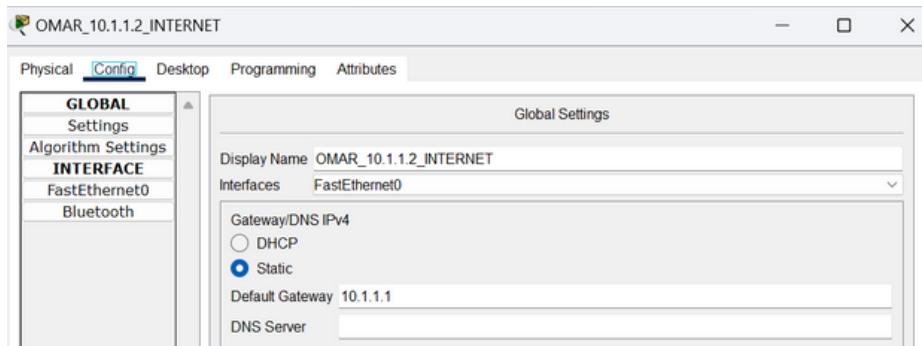
COMANDOS DE CADA DISPOSITIVO PARA CONECTAR LA RED

CONFIGURAR PC

Para la configuración de los dispositivos nos basaremos en los detalles de la práctica. Las redes que usaremos serán en base a lo que nos pide la práctica de laboratorio. Comenzaremos con la configuración de las PCs, al ser una rede espejo, no habrá necesidad de repetir la explicación por cada una de las PCs, simplemente repetiremos los pasos modificando según se requiera.

Para empezar la configuración de una PC, necesitamos conocer default gateway que utilizaremos al igual que conocer que IP y subnet mask llevará cada PC. Esto lo podemos saber analizando lo detalles de la práctica. Se nos menciona que cada puerto contiene una Vlan distinta, en este caso usaremos la 100, donde su direccionamiento es el siguiente 10.1.1.1 y es un /24. De ser el caso de una 200, su direccionamiento sería el siguiente 10.2.1.1 y también sería un /24.

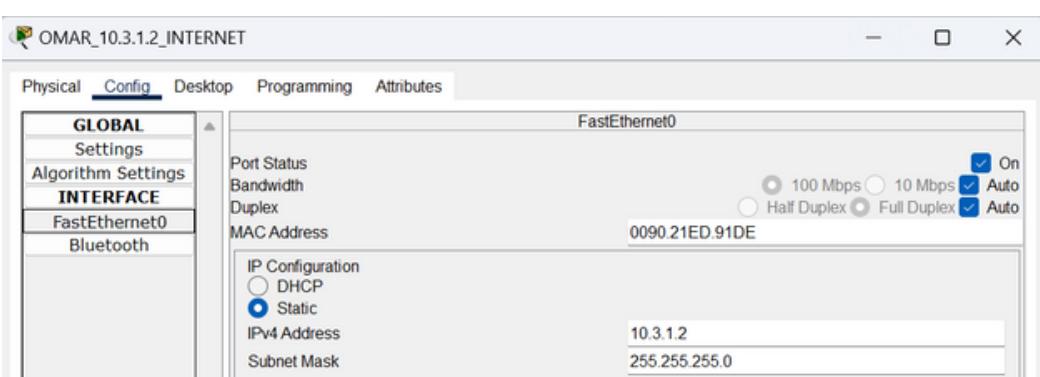
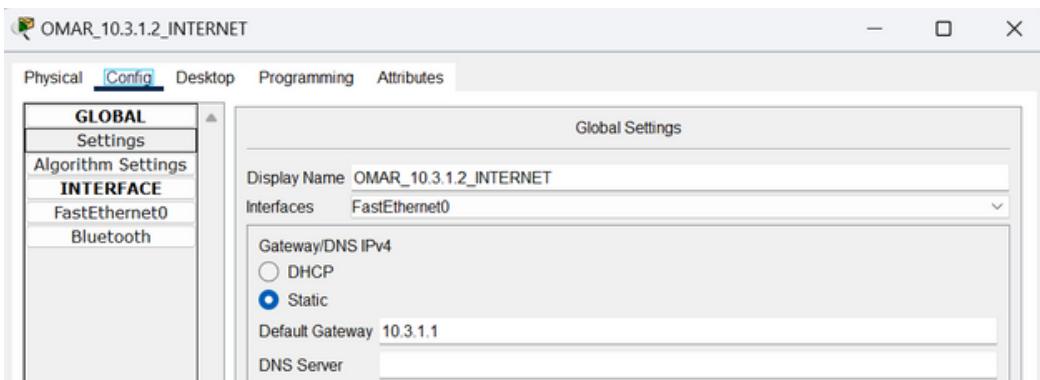
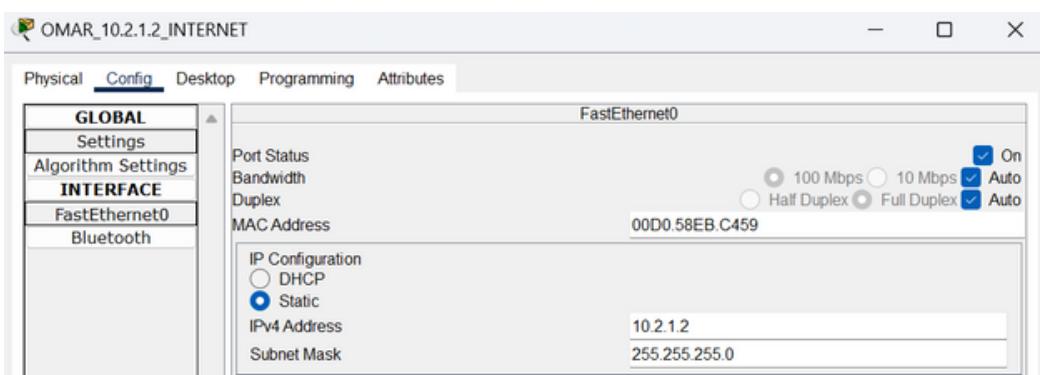
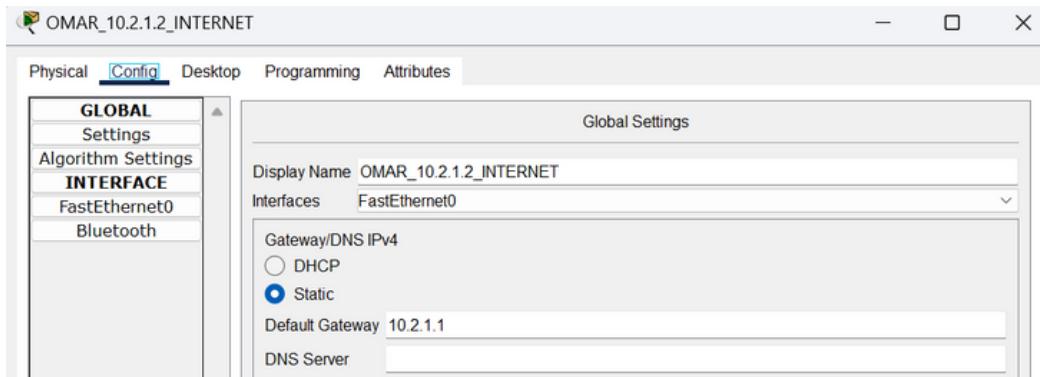
Como ya sabemos un default gateway es un dispositivo, generalmente un router, que permite a los dispositivos de una red local comunicarse con dispositivos en otras redes. Sirve como el punto de salida para el tráfico de datos que se dirige a una red diferente, facilitando la conexión a Internet u otras redes externas. Sabemos que el core en este caso se configura con la primer IP utilizable, por lo que el default gateway será 10.1.1.1.

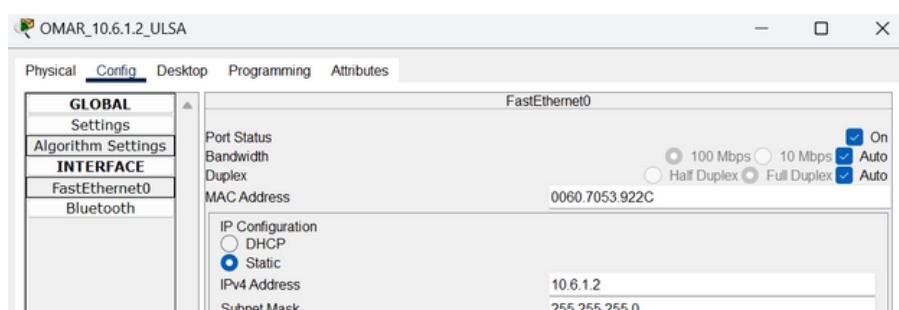
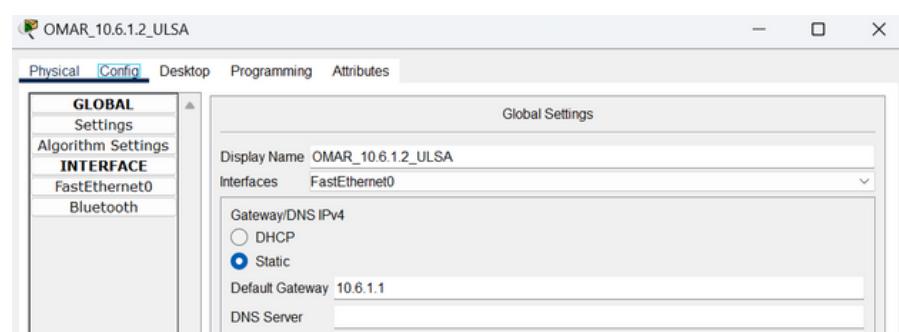
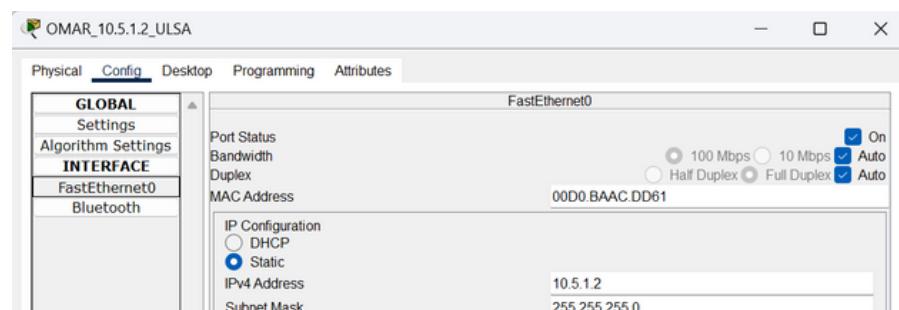
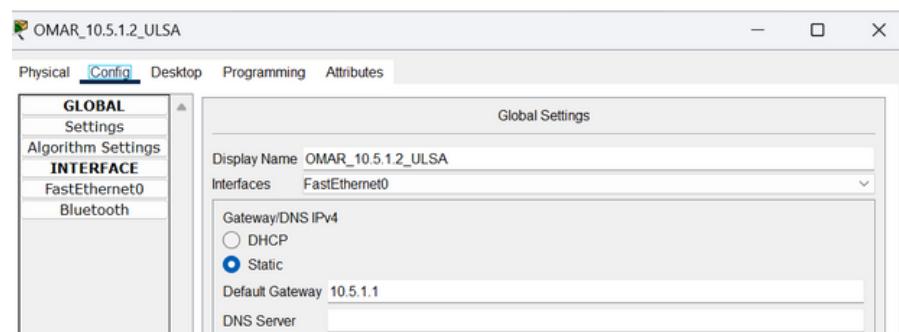
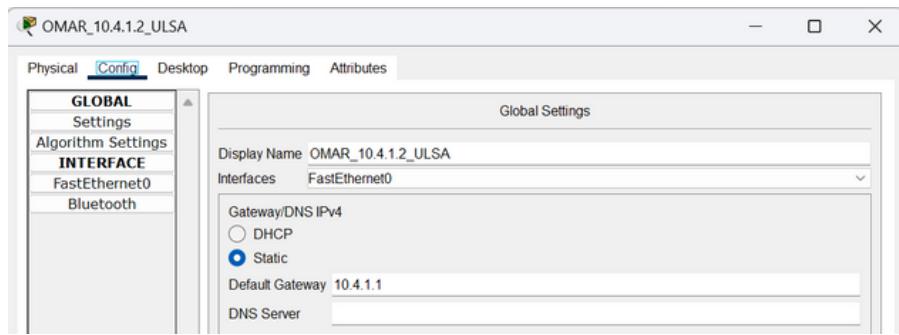


Ahora para seleccionar la IP al igual que la subnet mask, hace falta volver a revisar los detalles de la práctica, se nos menciona que las PCs deben usar un /24 y que podemos usar cualquier IP utilizable, sabiendo eso, la configuración sería la siguiente. 10.1.1.2 (La segunda IP utilizable). 255.255.255.0 (Usando el /24)



Repetiremos lo mismo para las otras seis PCs, donde cambiaremos únicamente el segundo octeto, el cual como mencionamos anteriormente, define la Vlan. Sabemos también que Internet usa la Vlan 100, 200 y 300 y Ulsa usa la Vlan 400, 500, 600.



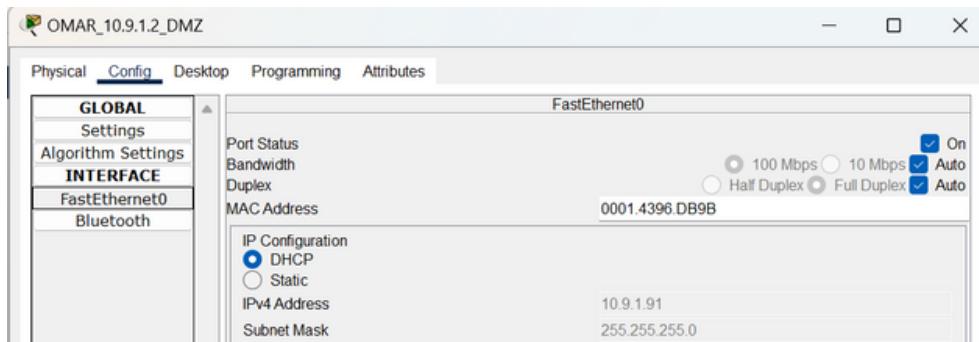
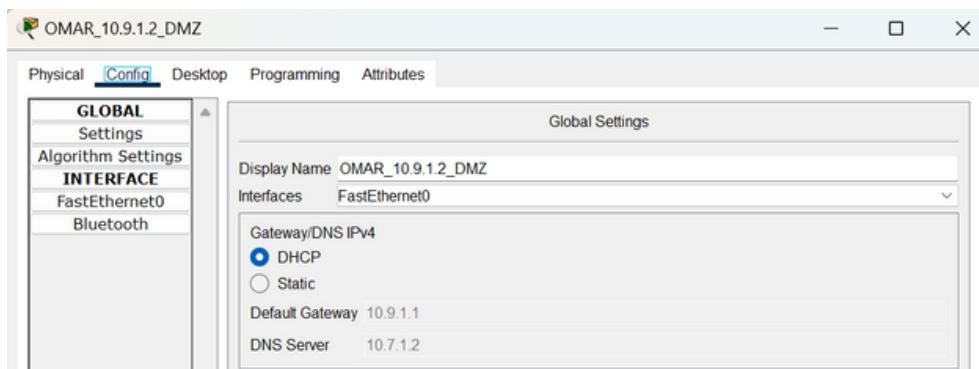


CONFIGURACIÓN

COMANDOS DE CADA DISPOSITIVO
PARA CONECTAR LA RED

CONFIGURAR PC

También podemos hacer clic en la opción de DHCP



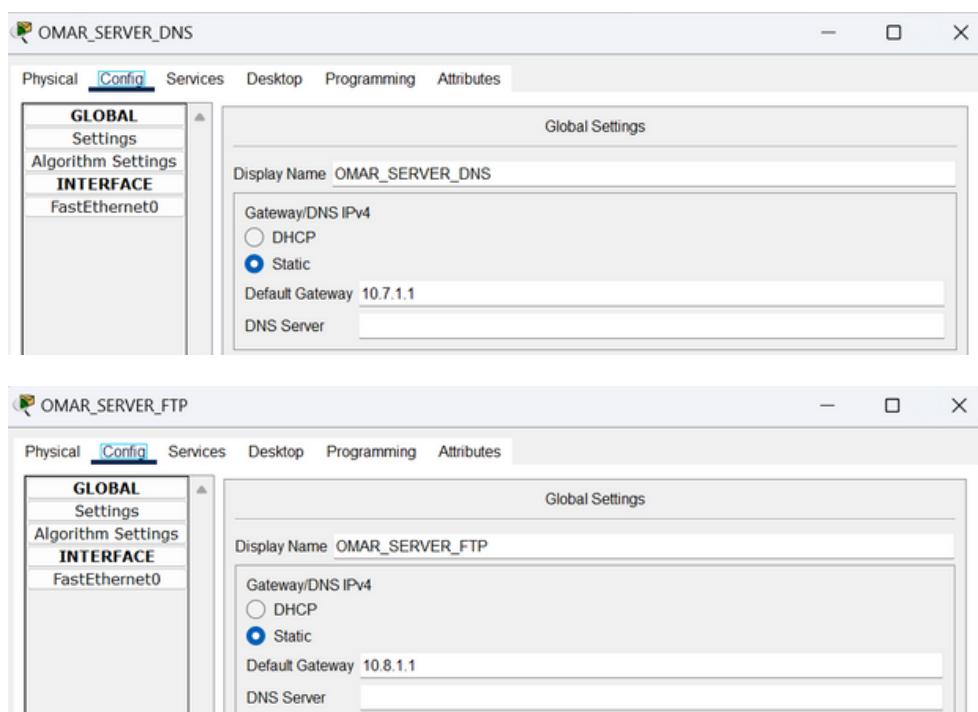
Debido a los nuevos servidores, se les asignarán IPs automáticas según estén configuradas las server pools.

CONFIGURACIÓN

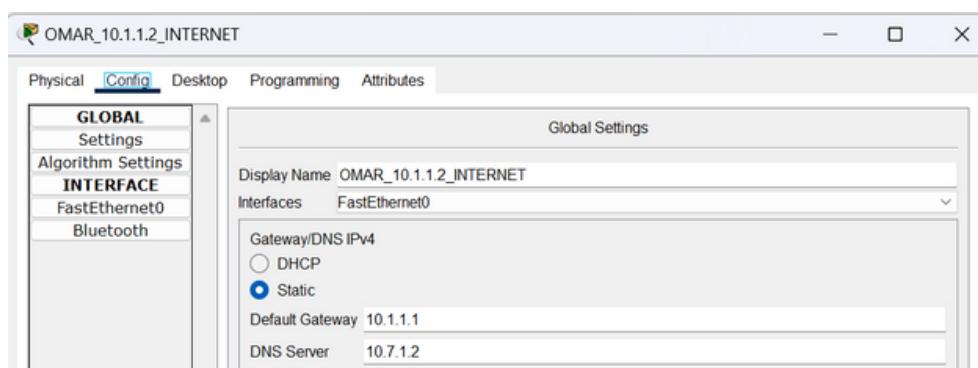
COMANDOS DE CADA DISPOSITIVO PARA CONECTAR LA RED

CONFIGURAR SERVERS

Para la configuración de los dispositivos nos basaremos en los detalles de la práctica. Las redes que usaremos serán en base a lo que nos pide la práctica de laboratorio. Comenzaremos con la configuración de los servers, primero usaremos la primer Ip utilizable para nuestro Default Gateway. Sabemos que los servers DMZ usan la Vlan 700 y 800.



En el caso de que queramos conectar una PC al DNS WEB SERVER deberemos de agregar en la configuración de DNS SERVER.

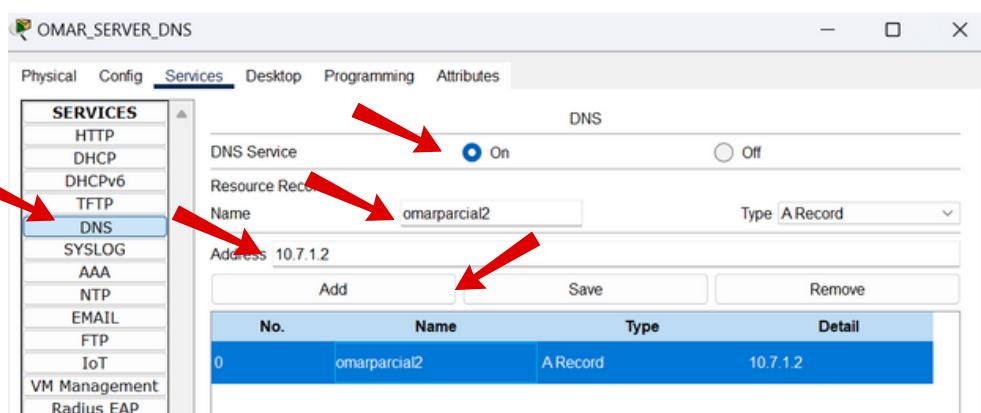


CONFIGURACIÓN

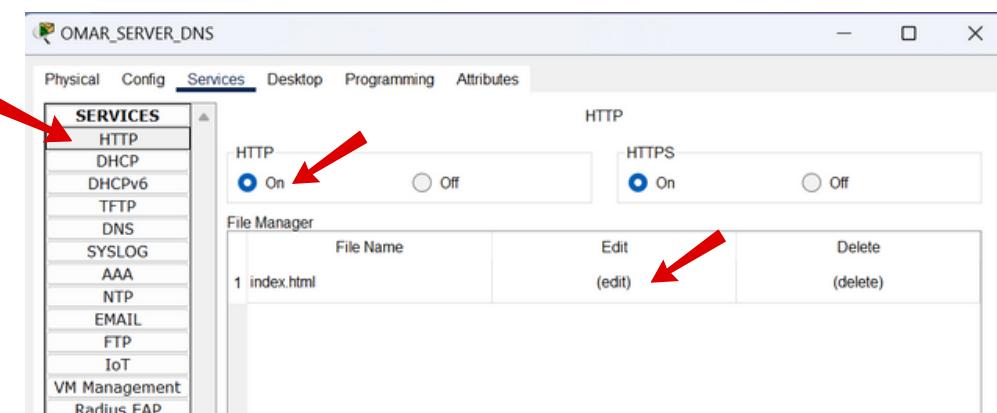
COMANDOS DE CADA DISPOSITIVO
PARA CONECTAR LA RED

CONFIGURAR SERVICIOS

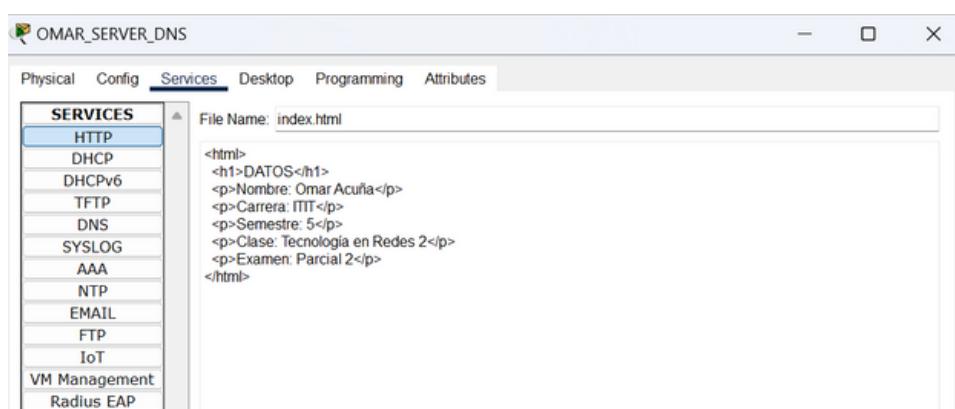
Comenzaremos con la configuración del DNS WEB SERVER.



Elegimos el servicio DNS. Comenzamos haciendo clic en el botón de On, Asignamos un nombre de la página web y agregamos la Address IP del servidor, en este caso usamos la segunda IP utilizable, por ultimo hacemos clic en Add.



Elegimos el servicio HTTP. Hacemos clic en On. Luego encontraremos varios archivos HTML, donde podemos editarlos para poner la información que queremos que aparezca en nuestra página web.

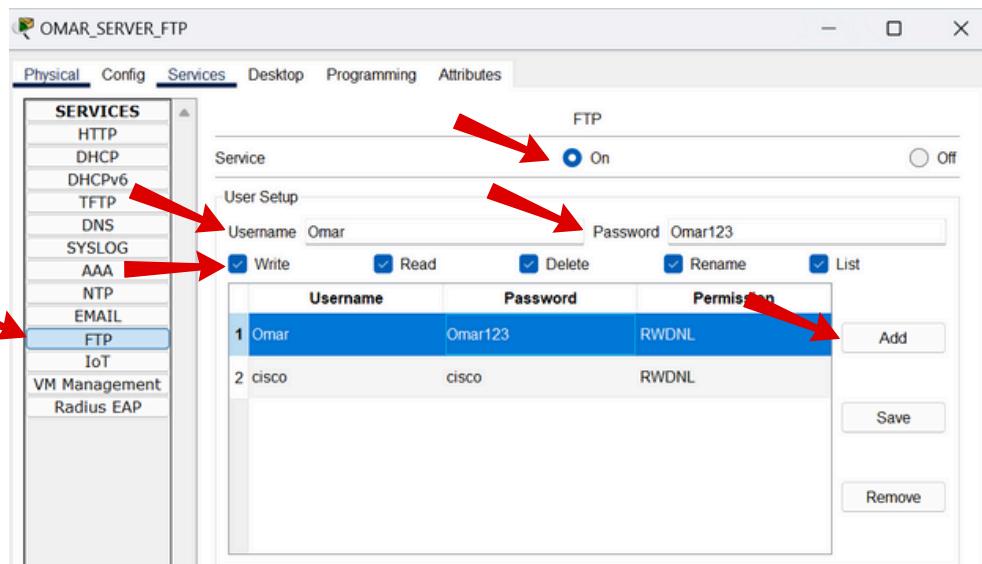


CONFIGURACIÓN

COMANDOS DE CADA DISPOSITIVO
PARA CONECTAR LA RED

CONFIGURAR SERVICIOS

Comenzaremos con la configuración del SERVER FTP.



Elegimos el servicio FTP. Hacemos clic en On. Agregamos un Username y su respectiva Password, marcamos todas las casillas, tanto Write, Read, Delete, Rename, List y finalmente hacemos clic en Add.

File
1 asa842-k8.bin
2 asa923-k8.bin
3 c1841-advipservicesk9-mz.124-15.T1.bin
4 c1841-ipbase-mz.123-14.T7.bin
5 c1841-ipbasek9-mz.124-12.bin
6 c1900-universalk9-mz.SPA.155-3.M4a.bin
7 c2600-advipservicesk9-mz.124-15.T1.bin

Habrá una lista de archivos accesibles atreves de FTP.

CONFIGURACIÓN

COMANDOS DE CADA DISPOSITIVO PARA CONECTAR LA RED

CONFIGURAR SERVERS

Para la configuración de los dispositivos nos basaremos en los detalles de la práctica. Las redes que usaremos serán en base a lo que nos pide la práctica de laboratorio. Comenzaremos con la configuración de los servers, primero usaremos la primer ip utilizable para nuestro Default Gateway. Sabemos que los servers DHCP usan la Vlan 1000, 1100 y 1200.

The image displays three separate windows for configuring DHCP servers:

- OMAR_DHCP_INTERNET:** The Default Gateway is set to 10.10.1.1.
- OMAR_DHCP_ULSA:** The Default Gateway is set to 10.11.1.1.
- OMAR_DHCP_DMZ:** The Default Gateway is set to 10.12.1.1.

CONFIGURACIÓN

COMANDOS DE CADA DISPOSITIVO PARA CONECTAR LA RED

CONFIGURAR SERVERS

Usaremos la segunda ip utilizable por cada vlan y una subnet mask /24 como nos pide el laboratorio.

The image displays three separate windows from a network configuration tool, each showing the configuration of a FastEthernet0 interface:

- OMAR_DHCP_INTERNET:** The IP address is set to 10.10.1.2 and the subnet mask to 255.255.255.0.
- OMAR_DHCP_ULSA:** The IP address is set to 10.11.1.2 and the subnet mask to 255.255.255.0.
- OMAR_DHCP_DMZ:** The IP address is set to 10.12.1.2 and the subnet mask to 255.255.255.0.

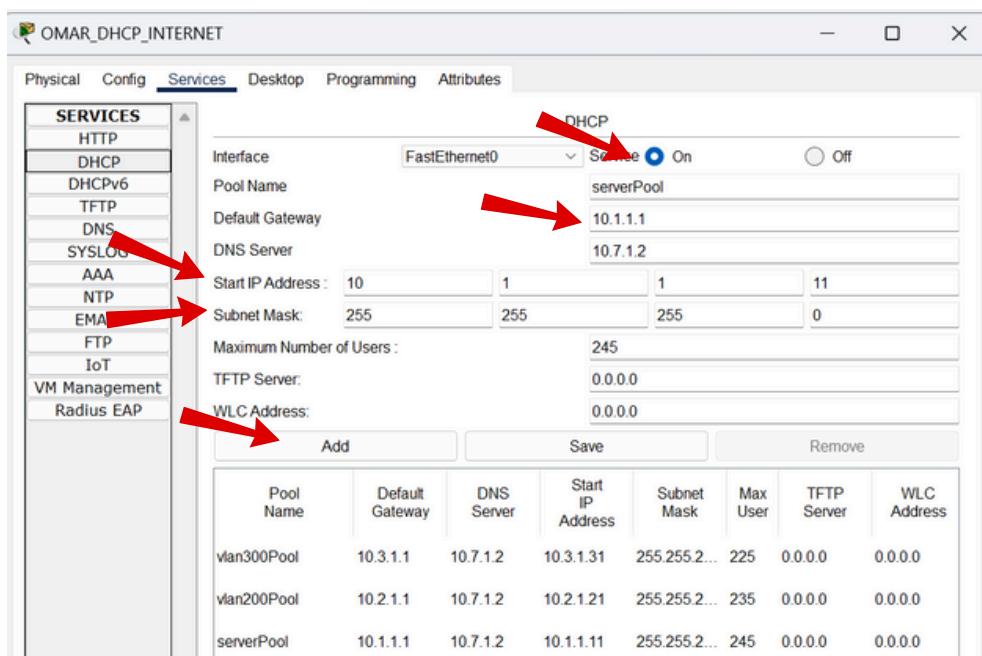
In all three configurations, the MAC address is listed as 0003.E492.7650, the bandwidth is set to 100 Mbps, and the duplex mode is set to Auto. The port status is On.

CONFIGURACIÓN

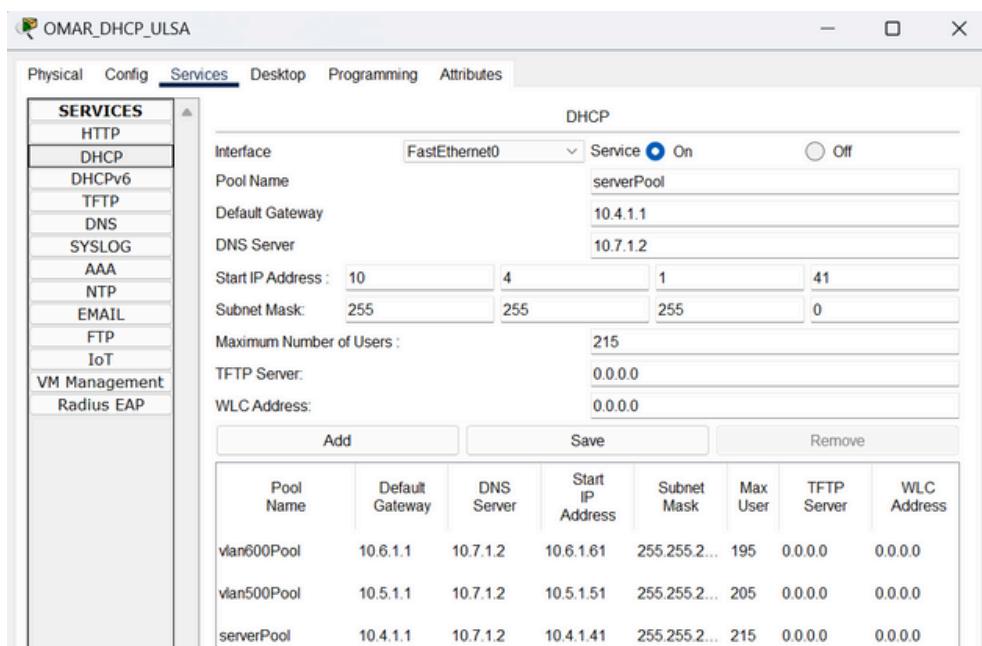
COMANDOS DE CADA DISPOSITIVO PARA CONECTAR LA RED

CONFIGURAR SERVICIOS

Comenzaremos con la configuración del SERVER DHCP.



Elegimos el servicio DHCP. Hacemos clic en On. Agregamos un Pool Name, en este caso el DNS Server será solo en caso de que exista, Elegimos la start ip address según nos indica el laboratorio por cada la Vlan y una subnet mask /24. El número de usuario máximo se ajustara automáticamente y al finalizar damos clic en add o save según corresponda. Repetimos por cada server.



CONFIGURACIÓN

COMANDOS DE CADA DISPOSITIVO
PARA CONECTAR LA RED

CONFIGURAR SERVICIOS

The screenshot shows a software interface for managing network services. The title bar reads "OMAR_DHCP_DMZ". The top menu bar includes "Physical", "Config", "Services", "Desktop", "Programming", and "Attributes". The "Services" tab is currently selected. On the left, a sidebar lists various service types under the heading "SERVICES": HTTP, DHCP, DHCPv6, TFTP, DNS, SYSLOG, AAA, NTP, EMAIL, FTP, IoT, VM Management, and Radius EAP. The "DHCP" service is selected. The main configuration area for "DHCP" includes the following fields:

DHCP							
Interface	FastEthernet0	Service	<input checked="" type="radio"/> On	<input type="radio"/> Off			
Pool Name	serverPool						
Default Gateway	10.7.1.1						
DNS Server	10.7.1.2						
Start IP Address :	10	7	1	71			
Subnet Mask:	255	255	255	0			
Maximum Number of Users :	185						
TFTP Server:	0.0.0.0						
WLC Address:	0.0.0.0						

Below these fields are three buttons: "Add", "Save", and "Remove". A table below the buttons displays existing DHCP pool configurations:

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
vlan900Pool	10.9.1.1	10.7.1.2	10.9.1.91	255.255.2...	165	0.0.0.0	0.0.0.0
vlan800Pool	10.8.1.1	10.7.1.2	10.8.1.81	255.255.2...	175	0.0.0.0	0.0.0.0
serverPool	10.7.1.1	10.7.1.2	10.7.1.71	255.255.2...	185	0.0.0.0	0.0.0.0

CONFIGURACIÓN

COMANDOS DE CADA DISPOSITIVO PARA CONECTAR LA RED

ACCESS PORTS DE TODOS LOS SWITCHES

INTERNET	INTERNET	INTERNET	INTERNET
>ENABLE	>ENABLE	>ENABLE	>ENABLE
>CONF T	>CONF T	>CONF T	>CONF T
>INT Gi1/0/1	>INT Gi1/0/2	>INT Gi1/0/3	>INT Gi1/0/4
>DESCRIPTION	>DESCRIPTION	>DESCRIPTION	>DESCRIPTION
>SWITCHPORT MODE ACCESS	>SWITCHPORT MODE ACCESS	>SWITCHPORT MODE ACCESS	>SWITCHPORT MODE ACCESS
>SWITCHPORT ACCESS VLAN 100	>SWITCHPORT ACCESS VLAN 200	>SWITCHPORT ACCESS VLAN 300	>SWITCHPORT ACCESS VLAN 1000
>NO SHUT	>NO SHUT	>NO SHUT	>NO SHUT

```
OMAR_CORE_INTERNET
Physical Config CLI Attributes
IOS Command Line Interface
interface GigabitEthernet1/0/1
description Access port to OMAR 10.1.1.2 port 0
switchport access vlan 100
switchport mode access
!
interface GigabitEthernet1/0/2
description Access port to OMAR 10.2.1.2 port 0
switchport access vlan 200
switchport mode access
!
interface GigabitEthernet1/0/3
description Access port to OMAR 10.3.1.2 port 0
switchport access vlan 300
switchport mode access
!
interface GigabitEthernet1/0/4
description Access Port to DHCP SERVER port 0
switchport access vlan 1000
switchport mode access
```

- 1.enable: Entra en modo privilegiado.
- 2.conf t: Entra en el modo de configuración global.
- 3.int Gi: Selecciona la interfaz GigabitEthernet.
- 4.description: Añade una descripción a la interfaz para identificar su propósito.
- 5.switchport mode access: Configura la interfaz en modo de acceso, permitiendo que solo una VLAN pase por la interfaz.
- 6.switchport access vlan: Asigna la interfaz a la VLAN, permitiendo el tráfico de esta VLAN.
- 7.no shut: Habilita la interfaz, permitiendo el paso de tráfico.

CONFIGURACIÓN

COMANDOS DE CADA DISPOSITIVO
PARA CONECTAR LA RED

ACCESS PORTS DE TODOS LOS SWITCHES

INTERNET	INTERNET	INTERNET
>ENABLE	>ENABLE	>ENABLE
>CONF T	>CONF T	>CONF T
>IP ROUTING	>IP ROUTING	>IP ROUTING
>INTERFACE VLAN 100	>INTERFACE VLAN 200	>INTERFACE VLAN 300
>NO SHUT	>NO SHUT	>NO SHUT
>IP ADDRESS 10.1.1.1 255.255.255.0	>IP ADDRESS 10.2.1.1 255.255.255.0	>IP ADDRESS 10.3.1.1 255.255.255.0
>IP HELPER-ADDRESS 10.10.1.2	>IP HELPER-ADDRESS 10.10.1.2	>IP HELPER-ADDRESS 10.10.1.2
INTERNET		
>ENABLE		
>CONF T		
>IP ROUTING		
>INTERFACE VLAN 1000		
>NO SHUT		
>IP ADDRESS 10.10.1.1 255.255.255.0		

```
OMAR_CORE_INTERNET
Physical Config CLI Attributes
IOS Command Line Interface
interface Vlan100
mac-address 0060.7005.5b01
ip address 10.1.1.1 255.255.255.0
ip helper-address 10.10.1.2
!
interface Vlan200
mac-address 0060.7005.5b02
ip address 10.2.1.1 255.255.255.0
ip helper-address 10.10.1.2
!
interface Vlan300
mac-address 0060.7005.5b03
ip address 10.3.1.1 255.255.255.0
ip helper-address 10.10.1.2
!
interface Vlan1000
mac-address 0060.7005.5b04
ip address 10.10.1.1 255.255.255.0
```

- 1.enable: Entra en modo privilegiado.
- 2.conf t: Entra en el modo de configuración global.
- 3.ip routing: Habilita el enrutamiento IP en el dispositivo.
- 4.interface vlan: Selecciona la interfaz VLAN para configurarla.
- 5.no shut: Habilita la interfaz VLAN, permitiendo el paso de tráfico.
- 6.ip address: Asigna la dirección IP con la máscara de red

CONFIGURACIÓN

COMANDOS DE CADA DISPOSITIVO PARA CONECTAR LA RED

ACCESS PORTS DE TODOS LOS SWITCHES

ULSA	ULSA	ULSA	ULSA
>ENABLE	>ENABLE	>ENABLE	>ENABLE
>CONF T	>CONF T	>CONF T	>CONF T
>INT Gi1/0/1	>INT Gi1/0/2	>INT Gi1/0/3	>INT Gi1/0/4
>DESCRIPTION	>DESCRIPTION	>DESCRIPTION	>DESCRIPTION
>SWITCHPORT MODE ACCESS	>SWITCHPORT MODE ACCESS	>SWITCHPORT MODE ACCESS	>SWITCHPORT MODE ACCESS
>SWITCHPORT ACCESS VLAN 400	>SWITCHPORT ACCESS VLAN 500	>SWITCHPORT ACCESS VLAN 600	>SWITCHPORT ACCESS VLAN 1100
>NO SHUT	>NO SHUT	>NO SHUT	>NO SHUT

The screenshot shows a Windows-style application window titled "OMAR_CORE_ULA". The tab bar at the top has "Physical", "Config", "CLI" (which is selected), and "Attributes". Below the tabs is a title bar "IOS Command Line Interface". The main area contains the following configuration script:

```
!
interface GigabitEthernet1/0/1
description Access port to OMAR 10.4.1.2 port 0
switchport access vlan 400
switchport mode access
!
interface GigabitEthernet1/0/2
description Access port to OMAR 10.5.1.2 port 0
switchport access vlan 500
switchport mode access
!
interface GigabitEthernet1/0/3
description Access port to OMAR 10.6.1.2 port 0
switchport access vlan 600
switchport mode access
!
interface GigabitEthernet1/0/4
description Access port to DHCP SERVER port 0
switchport access vlan 1100
switchport mode access
```

- 1.enable: Entra en modo privilegiado.
- 2.conf t: Entra en el modo de configuración global.
- 3.int Gi: Selecciona la interfaz GigabitEthernet.
- 4.description: Añade una descripción a la interfaz para identificar su propósito.
- 5.switchport mode access: Configura la interfaz en modo de acceso, permitiendo que solo una VLAN pase por la interfaz.
- 6.switchport access vlan: Asigna la interfaz a la VLAN, permitiendo el tráfico de esta VLAN.
- 7.no shut: Habilita la interfaz, permitiendo el paso de tráfico.

CONFIGURACIÓN

COMANDOS DE CADA DISPOSITIVO
PARA CONECTAR LA RED

ACCESS PORTS DE TODOS LOS SWITCHES

```
ULSA
>ENABLE
>CONF T
>IP ROUTING
>INTERFACE VLAN 400
>NO SHUT
>IP ADDRESS 10.4.1.1 255.255.255.0
>IP HELPER-ADDRESS 10.11.1.2
```

```
ULSA
>ENABLE
>CONF T
>IP ROUTING
>INTERFACE VLAN 500
>NO SHUT
>IP ADDRESS 10.5.1.1 255.255.255.0
>IP HELPER-ADDRESS 10.11.1.2
```

```
ULSA
>ENABLE
>CONF T
>IP ROUTING
>INTERFACE VLAN 600
>NO SHUT
>IP ADDRESS 10.6.1.1 255.255.255.0
>IP HELPER-ADDRESS 10.11.1.2
```

```
ULSA
>ENABLE
>CONF T
>IP ROUTING
>INTERFACE VLAN 1100
>NO SHUT
>IP ADDRESS 10.11.1.1 255.255.255.0
```

```
OMAR_CORE_ULSA
Physical Config CLI Attributes
IOS Command Line Interface

interface Vlan400
mac-address 0060.47e7.ba01
ip address 10.4.1.1 255.255.255.0
ip helper-address 10.11.1.2
!
interface Vlan500
mac-address 0060.47e7.ba02
ip address 10.5.1.1 255.255.255.0
ip helper-address 10.11.1.2
!
interface Vlan600
mac-address 0060.47e7.ba03
ip address 10.6.1.1 255.255.255.0
ip helper-address 10.11.1.2
!
interface Vlan1100
mac-address 0060.47e7.ba04
ip address 10.11.1.1 255.255.255.0
```

- 1.enable: Entra en modo privilegiado.
- 2.conf t: Entra en el modo de configuración global.
- 3.ip routing: Habilita el enrutamiento IP en el dispositivo.
- 4.interface vlan: Selecciona la interfaz VLAN para configurarla.
- 5.no shut: Habilita la interfaz VLAN, permitiendo el paso de tráfico.
- 6.ip address: Asigna la dirección IP con la máscara de red

CONFIGURACIÓN

COMANDOS DE CADA DISPOSITIVO PARA CONECTAR LA RED

ACCESS PORTS DE TODOS LOS SWITCHES

DMZ	DMZ	DMZ	DMZ
>ENABLE	>ENABLE	>ENABLE	>ENABLE
>CONF T	>CONF T	>CONF T	>CONF T
>INT Gi1/0/1	>INT Gi1/0/2	>INT Gi1/0/3	>INT Gi1/0/4
>DESCRIPTION	>DESCRIPTION	>DESCRIPTION	>DESCRIPTION
>SWITCHPORT MODE ACCESS	>SWITCHPORT MODE ACCESS	>SWITCHPORT MODE ACCESS	>SWITCHPORT MODE ACCESS
>SWITCHPORT ACCESS VLAN 700	>SWITCHPORT ACCESS VLAN 800	>SWITCHPORT ACCESS VLAN 900	>SWITCHPORT ACCESS VLAN 1200
>NO SHUT	>NO SHUT	>NO SHUT	>NO SHUT

```
OMAR_CORE_DMZ
Physical Config CLI Attributes
IOS Command Line Interface
interface GigabitEthernet1/0/1
description Access port to OMAR DNS port 0
switchport access vlan 700
switchport mode access
!
interface GigabitEthernet1/0/2
description Access port to OMAR FTP port 0
switchport access vlan 800
switchport mode access
!
interface GigabitEthernet1/0/3
description Access port to OMAR 10.9.1.2 port 0
switchport access vlan 900
switchport mode access
!
interface GigabitEthernet1/0/4
description Access port to DHCP SERVER port 0
switchport access vlan 1200
switchport mode access
```

- 1.enable: Entra en modo privilegiado.
- 2.conf t: Entra en el modo de configuración global.
- 3.int Gi: Selecciona la interfaz GigabitEthernet.
- 4.description: Añade una descripción a la interfaz para identificar su propósito.
- 5.switchport mode access: Configura la interfaz en modo de acceso, permitiendo que solo una VLAN pase por la interfaz.
- 6.switchport access vlan: Asigna la interfaz a la VLAN, permitiendo el tráfico de esta VLAN.
- 7.no shut: Habilita la interfaz, permitiendo el paso de tráfico.

CONFIGURACIÓN

COMANDOS DE CADA DISPOSITIVO PARA CONECTAR LA RED

ACCESS PORTS DE TODOS LOS SWITCHES

```
DMZ                                         DMZ                                         DMZ
>ENABLE                                     >ENABLE                                     >ENABLE
>CONF T                                      >CONF T                                      >CONF T
>IP ROUTING                                 >IP ROUTING                                >IP ROUTING
>INTERFACE VLAN 700                         >INTERFACE VLAN 800                         >INTERFACE VLAN 900
>NO SHUT                                     >NO SHUT                                    >NO SHUT
>IP ADDRESS 10.7.1.1 255.255.255.0        >IP ADDRESS 10.8.1.1 255.255.255.0        >IP ADDRESS 10.9.1.1 255.255.255.0
>IP HELPER-ADDRESS 10.12.1.2                 >IP HELPER-ADDRESS 10.12.1.2                 >IP HELPER-ADDRESS 10.12.1.2

                                         DMZ
                                         >ENABLE
                                         >CONF T
                                         >IP ROUTING
                                         >INTERFACE VLAN 1200
                                         >NO SHUT
                                         >IP ADDRESS 10.12.1.1 255.255.255.0
```

```
OMAR_CORE_DMZ
Physical Config CLI Attributes
IOS Command Line Interface

interface Vlan700
mac-address 0001.4386.2701
ip address 10.7.1.1 255.255.255.0
ip helper-address 10.12.1.2
!
interface Vlan800
mac-address 0001.4386.2702
ip address 10.8.1.1 255.255.255.0
ip helper-address 10.12.1.2
!
interface Vlan900
mac-address 0001.4386.2703
ip address 10.9.1.1 255.255.255.0
ip helper-address 10.12.1.2
!
interface Vlan1200
mac-address 0001.4386.2704
ip address 10.12.1.1 255.255.255.0
```

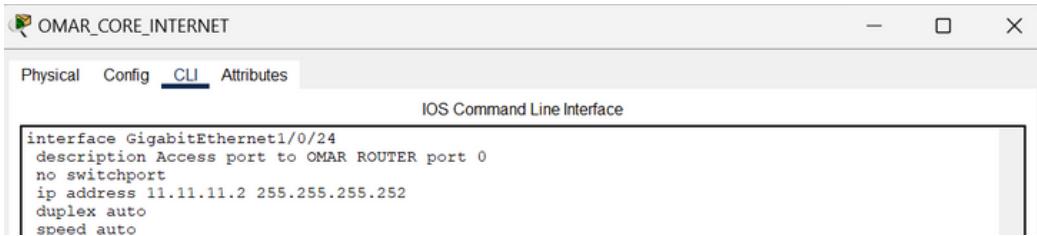
- 1.enable: Entra en modo privilegiado.
- 2.conf t: Entra en el modo de configuración global.
- 3.ip routing: Habilita el enrutamiento IP en el dispositivo.
- 4.interface vlan: Selecciona la interfaz VLAN para configurarla.
- 5.no shut: Habilita la interfaz VLAN, permitiendo el paso de tráfico.
- 6.ip address: Asigna la dirección IP con la máscara de red

CONFIGURACIÓN

COMANDOS DE CADA DISPOSITIVO
PARA CONECTAR LA RED

EIGRP PORTS DE TODOS LOS SWITCHES

```
INTERNET
>ENABLE
>CONF T
>INT Gi1/0/24
>DESCRIPTION
>NO SWITCHPORT
>NO SHUT
>IP ADDRESS 11.11.11.2 255.255.255.252
```



```
OMAR_CORE_INTERNET
Physical Config CLI Attributes
IOS Command Line Interface
interface GigabitEthernet1/0/24
description Access port to OMAR ROUTER port 0
no switchport
ip address 11.11.11.2 255.255.255.252
duplex auto
speed auto
```

- 1.enable: Entra en modo privilegiado.
- 2.conf t: Entra en el modo de configuración global.
- 3.int Gi: Selecciona la interfaz GigabitEthernet para configurarla.
- 4.description: Añade una descripción a la interfaz para identificar su propósito.
- 5.no switchport: Configura la interfaz para modo enrutado, deshabilitando las funciones de switch.
- 6.no shut: Habilita la interfaz, permitiendo el paso de tráfico.
- 7.ip address: Asigna la dirección IP junto con la máscara de red.

```
INTERNET
>ENABLE
>CONF T
>ROUTER EIGRP 100
>NETWORK 11.11.11.11
>REDISTRIBUTE CONNECTED
```



```
OMAR_CORE_INTERNET
Physical Config CLI Attributes
IOS Command Line Interface
router eigrp 100
redistribute connected
network 11.0.0.0
auto-summary
```

- 1.enable: Entra en modo privilegiado.
- 2.conf t: Entra en el modo de configuración global.
- 3.router eigrp 100: Activa el protocolo de enrutamiento EIGRP en el Autonomous System 100.
- 4.network: Incluye la red en el proceso de EIGRP para que sea anunciada.
- 5.redistribute connected: Redistribuye las rutas conectadas directamente a través del protocolo EIGRP.

CONFIGURACIÓN

COMANDOS DE CADA DISPOSITIVO PARA CONECTAR LA RED

EIGRP PORTS DE TODOS LOS SWITCHES

```
ULSA
>ENABLE
>CONF T
>INT Gi1/0/24
>DESCRIPTION
>NO SWITCHPORT
>NO SHUT
>IP ADDRESS 13.13.13.2 255.255.255.252
```



```
OMAR_CORE_ULSA
Physical Config CLI Attributes
IOS Command Line Interface
interface GigabitEthernet1/0/24
description Access port to OMAR ROUTER port 0
no switchport
ip address 13.13.13.2 255.255.255.252
duplex auto
speed auto
```

- 1.enable: Entra en modo privilegiado.
- 2.conf t: Entra en el modo de configuración global.
- 3.int Gi: Selecciona la interfaz GigabitEthernet para configurarla.
- 4.description: Añade una descripción a la interfaz para identificar su propósito.
- 5.no switchport: Configura la interfaz para modo enrutado, deshabilitando las funciones de switch.
- 6.no shut: Habilita la interfaz, permitiendo el paso de tráfico.
- 7.ip address: Asigna la dirección IP junto con la máscara de red.

```
ULSA
>ENABLE
>CONF T
>ROUTER EIGRP 100
>NETWORK 13.13.13.13
>REDISTRIBUTE CONNECTED
```



```
OMAR_CORE_ULSA
Physical Config CLI Attributes
IOS Command Line Interface
router eigrp 100
redistribute connected
network 13.0.0.0
auto-summary
```

- 1.enable: Entra en modo privilegiado.
- 2.conf t: Entra en el modo de configuración global.
- 3.router eigrp 100: Activa el protocolo de enrutamiento EIGRP en el Autonomous System 100.
- 4.network: Incluye la red en el proceso de EIGRP para que sea anunciada.
- 5.redistribute connected: Redistribuye las rutas conectadas directamente a través del protocolo EIGRP.

CONFIGURACIÓN

COMANDOS DE CADA DISPOSITIVO PARA CONECTAR LA RED

EIGRP PORTS DE TODOS LOS SWITCHES

```
DMZ
>ENABLE
>CONF T
>INT Gi1/0/24
>DESCRIPTION
>NO SWITCHPORT
>NO SHUT
>IP ADDRESS 15.15.15.2 255.255.255.252
```



```
interface GigabitEthernet1/0/24
no switchport
ip address 15.15.15.2 255.255.255.252
duplex auto
speed auto
```

- 1.enable: Entra en modo privilegiado.
- 2.conf t: Entra en el modo de configuración global.
- 3.int Gi: Selecciona la interfaz GigabitEthernet para configurarla.
- 4.description: Añade una descripción a la interfaz para identificar su propósito.
- 5.no switchport: Configura la interfaz para modo enrutado, deshabilitando las funciones de switch.
- 6.no shut: Habilita la interfaz, permitiendo el paso de tráfico.
- 7.ip address: Asigna la dirección IP junto con la máscara de red.

```
DMZ
>ENABLE
>CONF T
>ROUTER EIGRP 100
>NETWORK 15.15.15.15
>REDISTRIBUTE CONNECTED
```



```
router eigrp 100
redistribute connected
network 15.0.0.0
auto-summary
```

- 1.enable: Entra en modo privilegiado.
- 2.conf t: Entra en el modo de configuración global.
- 3.router eigrp 100: Activa el protocolo de enrutamiento EIGRP en el Autonomous System 100.
- 4.network: Incluye la red en el proceso de EIGRP para que sea anunciada.
- 5.redistribute connected: Redistribuye las rutas conectadas directamente a través del protocolo EIGRP.

CONFIGURACIÓN

COMANDOS DE CADA DISPOSITIVO
PARA CONECTAR LA RED

EIGRP PORTS DE TODOS LOS ROUTERS

```
INTERNET
>ENABLE
>CONF T
>INT GI0/0
>DESCRIPTION
>NO SHUT
>IP ADDRESS 11.11.11.1 255.255.255.252
```

The screenshot shows a window titled "OMAR_ROUTER_INTERNET" with tabs for Physical, Config, CLI, and Attributes. The CLI tab is selected, displaying the IOS Command Line Interface. Inside the interface, the configuration command for the GigabitEthernet0/0 interface is shown:

```
interface GigabitEthernet0/0
description Access port to OMAR CORE port 24
ip address 11.11.11.1 255.255.255.252
duplex auto
speed auto
```

- 1.enable: Entra en modo privilegiado.
- 2.conf t: Entra en el modo de configuración global.
- 3.int Gi: Selecciona la interfaz GigabitEthernet para configurarla.
- 4.description: Añade una descripción a la interfaz para identificar su propósito.
- 5.no shut: Habilita la interfaz, permitiendo el paso de tráfico.
- 6.ip address: Asigna la dirección IP junto con la máscara de red.

```
ULSA
>ENABLE
>CONF T
>INT GI0/0
>DESCRIPTION
>NO SHUT
>IP ADDRESS 13.13.13.1 255.255.255.252
```

The screenshot shows a window titled "OMAR_ROUTER_ULSA" with tabs for Physical, Config, CLI, and Attributes. The CLI tab is selected, displaying the IOS Command Line Interface. Inside the interface, the configuration command for the GigabitEthernet0/0 interface is shown:

```
interface GigabitEthernet0/0
description Access port to OMAR CORE port 24
ip address 13.13.13.1 255.255.255.252
duplex auto
speed auto
```

- 1.enable: Entra en modo privilegiado.
- 2.conf t: Entra en el modo de configuración global.
- 3.int Gi: Selecciona la interfaz GigabitEthernet para configurarla.
- 4.description: Añade una descripción a la interfaz para identificar su propósito.
- 5.no shut: Habilita la interfaz, permitiendo el paso de tráfico.
- 6.ip address: Asigna la dirección IP junto con la máscara de red.

CONFIGURACIÓN

COMANDOS DE CADA DISPOSITIVO
PARA CONECTAR LA RED

EIGRP PORTS DE TODOS LOS ROUTERS

```
DMZ
>ENABLE
>CONF T
>INT GI0/0
>DESCRIPTION
>NO SHUT
>IP ADDRESS 15.15.15.1 255.255.255.252
```

The screenshot shows a window titled "OMAR_ROUTER_DMZ" with tabs for "Physical", "Config", "CLI" (which is selected), and "Attributes". Below the tabs is the text "IOS Command Line Interface". The CLI area contains the following configuration commands:

```
interface GigabitEthernet0/0
description Access port to OMAR CORE port 24
ip address 15.15.15.1 255.255.255.252
duplex auto
speed auto
```

- 1.enable: Entra en modo privilegiado.
- 2.conf t: Entra en el modo de configuración global.
- 3.int Gi: Selecciona la interfaz GigabitEthernet para configurarla.
- 4.description: Añade una descripción a la interfaz para identificar su propósito.
- 5.no shut: Habilita la interfaz, permitiendo el paso de tráfico.
- 6.ip address: Asigna la dirección IP junto con la máscara de red.

CONFIGURACIÓN

COMANDOS DE CADA DISPOSITIVO PARA CONECTAR LA RED

EIGRP PORTS DE TODOS LOS ROUTERS

```
INTERNET
>ENABLE
>CONF T
>INT GI0/1
>DESCRIPTION
>NO SHUT
>IP ADDRESS 12.12.12.1 255.255.255.252
```



The screenshot shows a window titled "OMAR_ROUTER_INTERNET" with tabs for Physical, Config, CLI, and Attributes. The CLI tab is selected, displaying the command-line interface. The interface "GigabitEthernet0/1" is configured with the following parameters:

```
interface GigabitEthernet0/1
description Access port to FIREWALL port 1
ip address 12.12.12.1 255.255.255.252
duplex auto
speed auto
```

- 1.enable: Entra en modo privilegiado.
- 2.conf t: Entra en el modo de configuración global.
- 3.int Gi: Selecciona la interfaz GigabitEthernet para configurarla.
- 4.description: Añade una descripción a la interfaz para identificar su propósito.
- 5.no shut: Habilita la interfaz, permitiendo el paso de tráfico.
- 6.ip address: Asigna la dirección IP junto con la máscara de red.

```
INTERNET
>ENABLE
>CONF T
>ROUTER EIGRP 100
>NETWORK 11.11.11.11
>NETWORK 12.12.12.12
>REDISTRIBUTE CONNECTED
```



The screenshot shows a window titled "OMAR_ROUTER_INTERNET" with tabs for Physical, Config, CLI, and Attributes. The CLI tab is selected, displaying the command-line interface. The EIGRP protocol is configured with the following parameters:

```
router eigrp 100
redistribute connected
network 11.0.0.0
network 12.0.0.0
```

- 1.enable: Entra en modo privilegiado.
- 2.conf t: Entra en el modo de configuración global.
- 3.router eigrp 100: Activa el protocolo de enrutamiento EIGRP en el Autonomous System 100.
- 4.network: Incluye la red en el proceso de EIGRP para que sea anunciada.
- 5.redistribute connected: Redistribuye las rutas conectadas directamente a través del protocolo EIGRP.

CONFIGURACIÓN

COMANDOS DE CADA DISPOSITIVO
PARA CONECTAR LA RED

EIGRP PORTS DE TODOS LOS ROUTERS

```
ULSA
>ENABLE
>CONF T
>INT Gi0/1
>DESCRIPTION
>NO SHUT
>IP ADDRESS 14.14.14.1 255.255.255.252
```

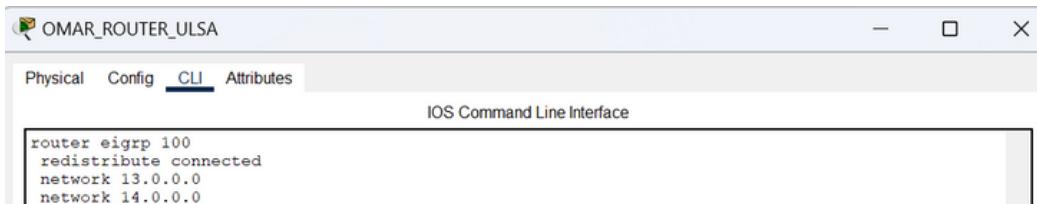


The screenshot shows a Cisco IOS CLI window titled "OMAR_ROUTER_ULSA". The tab bar at the top has "Physical", "Config", "CLI" (which is selected), and "Attributes". Below the tabs is the text "IOS Command Line Interface". The main area contains the following configuration command:

```
interface GigabitEthernet0/1
description Access port to FIREWALL port 2
ip address 14.14.14.1 255.255.255.252
duplex auto
speed auto
```

- 1.enable: Entra en modo privilegiado.
- 2.conf t: Entra en el modo de configuración global.
- 3.int Gi: Selecciona la interfaz GigabitEthernet para configurarla.
- 4.description: Añade una descripción a la interfaz para identificar su propósito.
- 5.no shut: Habilita la interfaz, permitiendo el paso de tráfico.
- 6.ip address: Asigna la dirección IP junto con la máscara de red.

```
ULSA
>ENABLE
>CONF T
>ROUTER EIGRP 100
>NETWORK 13.13.13.13
>NETWORK 14.14.14.14
>REDISTRIBUTE CONNECTED
```



The screenshot shows a Cisco IOS CLI window titled "OMAR_ROUTER_ULSA". The tab bar at the top has "Physical", "Config", "CLI" (which is selected), and "Attributes". Below the tabs is the text "IOS Command Line Interface". The main area contains the following configuration command:

```
router eigrp 100
redistribute connected
network 13.0.0.0
network 14.0.0.0
```

- 1.enable: Entra en modo privilegiado.
- 2.conf t: Entra en el modo de configuración global.
- 3.router eigrp 100: Activa el protocolo de enrutamiento EIGRP en el Autonomous System 100.
- 4.network: Incluye la red en el proceso de EIGRP para que sea anunciada.
- 5.redistribute connected: Redistribuye las rutas conectadas directamente a través del protocolo EIGRP.

CONFIGURACIÓN

COMANDOS DE CADA DISPOSITIVO
PARA CONECTAR LA RED

EIGRP PORTS DE TODOS LOS ROUTERS

```
DMZ
>ENABLE
>CONF T
>INT GI0/1
>DESCRIPTION
>NO SHUT
>IP ADDRESS 16.16.16.1 255.255.255.252
```



- 1.enable: Entra en modo privilegiado.
- 2.conf t: Entra en el modo de configuración global.
- 3.int Gi: Selecciona la interfaz GigabitEthernet para configurarla.
- 4.description: Añade una descripción a la interfaz para identificar su propósito.
- 5.no shut: Habilita la interfaz, permitiendo el paso de tráfico.
- 6.ip address: Asigna la dirección IP junto con la máscara de red.

```
DMZ
>ENABLE
>CONF T
>ROUTER EIGRP 100
>NETWORK 15.15.15.15
>NETWORK 16.16.16.16
>REDISTRIBUTE CONNECTED
```



- 1.enable: Entra en modo privilegiado.
- 2.conf t: Entra en el modo de configuración global.
- 3.router eigrp 100: Activa el protocolo de enrutamiento EIGRP en el Autonomous System 100.
- 4.network: Incluye la red en el proceso de EIGRP para que sea anunciada.
- 5.redistribute connected: Redistribuye las rutas conectadas directamente a través del protocolo EIGRP.

CONFIGURACIÓN

COMANDOS DE CADA DISPOSITIVO
PARA CONECTAR LA RED

EIGRP PORTS DEL FIREWALL

```
FIREWALL
>ENABLE
>CONF T
>INT GI1/1
>DESCRIPTION
>NAMEIF INTERNET
>SECURITY-LEVEL 10
>NO SHUT
>IP ADDRESS 12.12.12.2 255.255.255.252
```

The screenshot shows a software interface titled "FIREWALL_OMAR". At the top, there are tabs for "Physical", "Config", "CLI" (which is selected), and "Attributes". Below the tabs, it says "IOS Command Line Interface". The CLI window contains the following configuration command:

```
interface GigabitEthernet1/1
description Access port to OMAR ROUTER port 1
nameif INTERNET
security-level 10
ip address 12.12.12.2 255.255.255.252
```

- 1.enable: Entra en modo privilegiado.
- 2.conf t: Entra en el modo de configuración global.
- 3.int Gi: Selecciona la interfaz GigabitEthernet para configurarla.
- 4.description: Añade una descripción a la interfaz para identificar su propósito.
- 5.nameif: Asigna un nombre a la interfaz.
- 6.security-level: Establece el nivel de seguridad de la interfaz.
- 7.no shut: Habilita la interfaz, permitiendo el paso de tráfico.
- 8.ip address: Asigna la dirección con la máscara de red.

```
FIREWALL
>ENABLE
>CONF T
>INT GI1/2
>DESCRIPTION
>NAMEIF ULSA
>SECURITY-LEVEL 100
>NO SHUT
>IP ADDRESS 14.14.14.2 255.255.255.252
```

The screenshot shows a software interface titled "FIREWALL_OMAR". At the top, there are tabs for "Physical", "Config", "CLI" (which is selected), and "Attributes". Below the tabs, it says "IOS Command Line Interface". The CLI window contains the following configuration command:

```
interface GigabitEthernet1/2
description Access port to OMAR ROUTER port 1
nameif ULSA
security-level 100
ip address 14.14.14.2 255.255.255.252
```

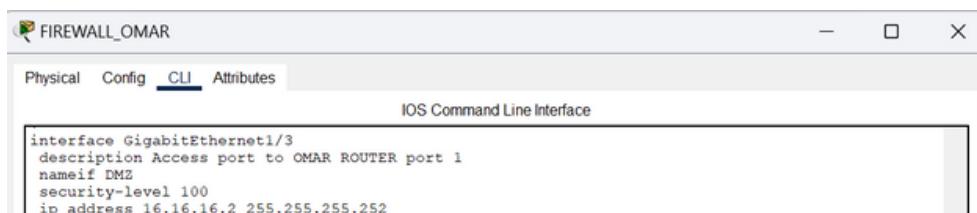
- 1.enable: Entra en modo privilegiado.
- 2.conf t: Entra en el modo de configuración global.
- 3.int Gi: Selecciona la interfaz GigabitEthernet para configurarla.
- 4.description: Añade una descripción a la interfaz para identificar su propósito.
- 5.nameif: Asigna un nombre a la interfaz.
- 6.security-level: Establece el nivel de seguridad de la interfaz.
- 7.no shut: Habilita la interfaz, permitiendo el paso de tráfico.
- 8.ip address: Asigna la dirección con la máscara de red.

CONFIGURACIÓN

COMANDOS DE CADA DISPOSITIVO PARA CONECTAR LA RED

EIGRP PORTS DEL FIREWALL

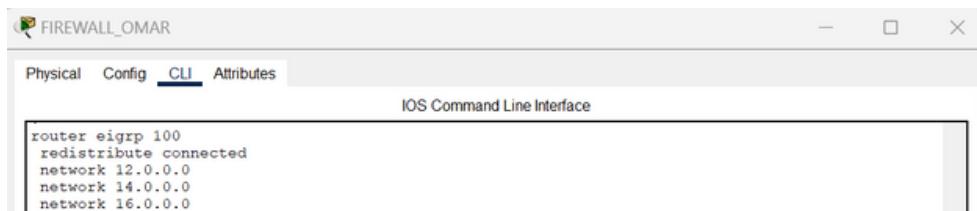
```
FIREWALL
>ENABLE
>CONF T
>INT Gi1/3
>DESCRIPTION
>NAMEIF DMZ
>SECURITY-LEVEL 100
>NO SHUT
>IP ADDRESS 16.16.16.2 255.255.255.252
```



```
interface GigabitEthernet1/3
description Access port to OMAR ROUTER port 1
nameif DMZ
security-level 100
ip address 16.16.16.2 255.255.255.252
```

- 1.enable: Entra en modo privilegiado.
- 2.conf t: Entra en el modo de configuración global.
- 3.int Gi: Selecciona la interfaz GigabitEthernet para configurarla.
- 4.description: Añade una descripción a la interfaz para identificar su propósito.
- 5.nameif: Asigna un nombre a la interfaz.
- 6.security-level: Establece el nivel de seguridad de la interfaz.
- 7.no shut: Habilita la interfaz, permitiendo el paso de tráfico.
- 8.ip address: Asigna la dirección con la máscara de red.

```
FIREWALL
>ENABLE
>CONF T
>ROUTER EIGRP 100
>NETWORK 12.12.12.12
>NETWORK 14.14.14.14
>NETWORK 16.16.16.16
>REDISTRIBUTE CONNECTED
```



```
router eigrp 100
redistribute connected
network 12.0.0.0
network 14.0.0.0
network 16.0.0.0
```

- 1.enable: Entra en modo privilegiado.
- 2.conf t: Entra en el modo de configuración global.
- 3.router eigrp 100: Activa el protocolo de enrutamiento EIGRP en el Autonomous System 100.
- 4.network: Incluye la red en el proceso de EIGRP para que sea anunciada.
- 5.redistribute connected: Redistribuye las rutas conectadas directamente a través del protocolo EIGRP.

CONFIGURACIÓN

COMANDOS DE CADA DISPOSITIVO PARA CONECTAR LA RED

ACCESS LISTS DEL FIREWALL

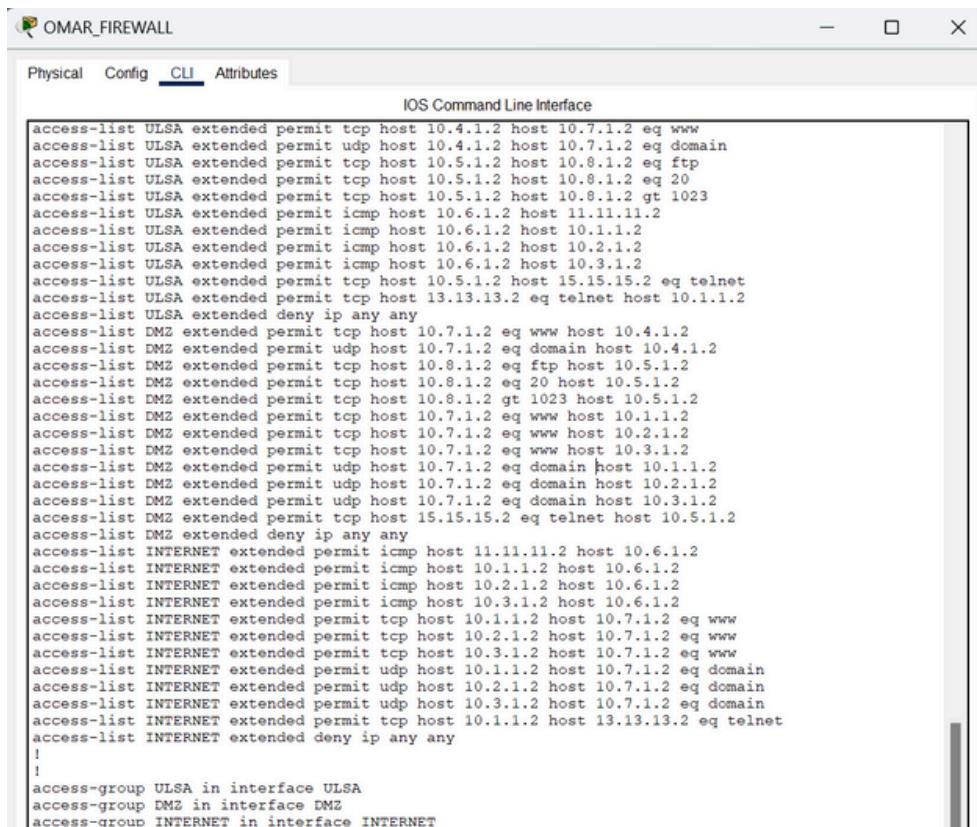
```
ACCESS-LIST ULSA EXTENDED PERMIT TCP HOST 10.4.1.2 HOST 10.7.1.2 EQ WWW
ACCESS-LIST ULSA EXTENDED PERMIT UDP HOST 10.4.1.2 HOST 10.7.1.2 EQ DOMAIN
ACCESS-LIST ULSA EXTENDED PERMIT TCP HOST 10.5.1.2 HOST 10.8.1.2 EQ FTP
ACCESS-LIST ULSA EXTENDED PERMIT TCP HOST 10.5.1.2 HOST 10.8.1.2 EQ 20
ACCESS-LIST ULSA EXTENDED PERMIT TCP HOST 10.5.1.2 HOST 10.8.1.2 GT 1023
ACCESS-LIST ULSA EXTENDED PERMIT ICMP HOST 10.6.1.2 HOST 11.11.11.2
ACCESS-LIST ULSA EXTENDED PERMIT ICMP HOST 10.6.1.2 HOST 10.1.1.2
ACCESS-LIST ULSA EXTENDED PERMIT ICMP HOST 10.6.1.2 HOST 10.2.1.2
ACCESS-LIST ULSA EXTENDED PERMIT ICMP HOST 10.6.1.2 HOST 10.3.1.2
ACCESS-LIST ULSA EXTENDED PERMIT TCP HOST 10.5.1.2 HOST 15.15.15.2 EQ TELNET
ACCESS-LIST ULSA EXTENDED PERMIT TCP HOST 13.13.13.2 EQ TELNET HOST 10.1.1.2
ACCESS-LIST ULSA EXTENDED DENY IP ANY ANY
ACCESS-LIST DMZ EXTENDED PERMIT TCP HOST 10.7.1.2 EQ WWW HOST 10.4.1.2
ACCESS-LIST DMZ EXTENDED PERMIT UDP HOST 10.7.1.2 EQ DOMAIN HOST 10.4.1.2
ACCESS-LIST DMZ EXTENDED PERMIT TCP HOST 10.8.1.2 EQ FTP HOST 10.5.1.2
ACCESS-LIST DMZ EXTENDED PERMIT TCP HOST 10.8.1.2 EQ 20 HOST 10.5.1.2
ACCESS-LIST DMZ EXTENDED PERMIT TCP HOST 10.8.1.2 GT 1023 HOST 10.5.1.2
ACCESS-LIST DMZ EXTENDED PERMIT TCP HOST 10.7.1.2 EQ WWW HOST 10.1.1.2
ACCESS-LIST DMZ EXTENDED PERMIT TCP HOST 10.7.1.2 EQ WWW HOST 10.2.1.2
ACCESS-LIST DMZ EXTENDED PERMIT TCP HOST 10.7.1.2 EQ WWW HOST 10.3.1.2
ACCESS-LIST DMZ EXTENDED PERMIT UDP HOST 10.7.1.2 EQ DOMAIN HOST 10.1.1.2
ACCESS-LIST DMZ EXTENDED PERMIT UDP HOST 10.7.1.2 EQ DOMAIN HOST 10.2.1.2
ACCESS-LIST DMZ EXTENDED PERMIT UDP HOST 10.7.1.2 EQ DOMAIN HOST 10.3.1.2
ACCESS-LIST DMZ EXTENDED PERMIT TCP HOST 15.15.15.2 EQ TELNET HOST 10.5.1.2
ACCESS-LIST DMZ EXTENDED DENY IP ANY ANY
ACCESS-LIST INTERNET EXTENDED PERMIT ICMP HOST 11.11.11.2 HOST 10.6.1.2
ACCESS-LIST INTERNET EXTENDED PERMIT ICMP HOST 10.1.1.2 HOST 10.6.1.2
ACCESS-LIST INTERNET EXTENDED PERMIT ICMP HOST 10.2.1.2 HOST 10.6.1.2
ACCESS-LIST INTERNET EXTENDED PERMIT ICMP HOST 10.3.1.2 HOST 10.6.1.2
ACCESS-LIST INTERNET EXTENDED PERMIT TCP HOST 10.1.1.2 HOST 10.7.1.2 EQ WWW
ACCESS-LIST INTERNET EXTENDED PERMIT TCP HOST 10.2.1.2 HOST 10.7.1.2 EQ WWW
ACCESS-LIST INTERNET EXTENDED PERMIT TCP HOST 10.3.1.2 HOST 10.7.1.2 EQ WWW
ACCESS-LIST INTERNET EXTENDED PERMIT UDP HOST 10.1.1.2 HOST 10.7.1.2 EQ DOMAIN
ACCESS-LIST INTERNET EXTENDED PERMIT UDP HOST 10.2.1.2 HOST 10.7.1.2 EQ DOMAIN
ACCESS-LIST INTERNET EXTENDED PERMIT UDP HOST 10.3.1.2 HOST 10.7.1.2 EQ DOMAIN
ACCESS-LIST INTERNET EXTENDED PERMIT TCP HOST 10.1.1.2 HOST 13.13.13.2 EQ TELNET
ACCESS-LIST INTERNET EXTENDED DENY IP ANY ANY

ACCESS-GROUP ULSA IN INTERFACE ULSA
ACCESS-GROUP DMZ IN INTERFACE DMZ
ACCESS-GROUP INTERNET IN INTERFACE INTERNET
```

CONFIGURACIÓN

COMANDOS DE CADA DISPOSITIVO PARA CONECTAR LA RED

ACCESS LISTS DEL FIREWALL



```
access-list ULSA extended permit tcp host 10.4.1.2 host 10.7.1.2 eq www
access-list ULSA extended permit udp host 10.4.1.2 host 10.7.1.2 eq domain
access-list ULSA extended permit tcp host 10.5.1.2 host 10.8.1.2 eq ftp
access-list ULSA extended permit tcp host 10.5.1.2 host 10.8.1.2 eq 20
access-list ULSA extended permit tcp host 10.5.1.2 host 10.8.1.2 gt 1023
access-list ULSA extended permit icmp host 10.6.1.2 host 11.11.11.2
access-list ULSA extended permit icmp host 10.6.1.2 host 10.1.1.2
access-list ULSA extended permit icmp host 10.6.1.2 host 10.2.1.2
access-list ULSA extended permit icmp host 10.6.1.2 host 10.3.1.2
access-list ULSA extended permit tcp host 10.5.1.2 host 15.15.15.2 eq telnet
access-list ULSA extended permit tcp host 13.13.13.2 eq telnet host 10.1.1.2
access-list ULSA extended deny ip any any
access-list DMZ extended permit tcp host 10.7.1.2 eq www host 10.4.1.2
access-list DMZ extended permit udp host 10.7.1.2 eq domain host 10.4.1.2
access-list DMZ extended permit tcp host 10.8.1.2 eq ftp host 10.5.1.2
access-list DMZ extended permit tcp host 10.8.1.2 eq 20 host 10.5.1.2
access-list DMZ extended permit tcp host 10.8.1.2 gt 1023 host 10.5.1.2
access-list DMZ extended permit tcp host 10.7.1.2 eq www host 10.1.1.2
access-list DMZ extended permit tcp host 10.7.1.2 eq www host 10.2.1.2
access-list DMZ extended permit tcp host 10.7.1.2 eq www host 10.3.1.2
access-list DMZ extended permit udp host 10.7.1.2 eq domain host 10.1.1.2
access-list DMZ extended permit udp host 10.7.1.2 eq domain host 10.2.1.2
access-list DMZ extended permit udp host 10.7.1.2 eq domain host 10.3.1.2
access-list DMZ extended permit tcp host 15.15.15.2 eq telnet host 10.5.1.2
access-list DMZ extended deny ip any any
access-list INTERNET extended permit icmp host 11.11.11.2 host 10.6.1.2
access-list INTERNET extended permit icmp host 10.1.1.2 host 10.6.1.2
access-list INTERNET extended permit icmp host 10.2.1.2 host 10.6.1.2
access-list INTERNET extended permit icmp host 10.3.1.2 host 10.6.1.2
access-list INTERNET extended permit tcp host 10.1.1.2 host 10.7.1.2 eq www
access-list INTERNET extended permit tcp host 10.2.1.2 host 10.7.1.2 eq www
access-list INTERNET extended permit tcp host 10.3.1.2 host 10.7.1.2 eq www
access-list INTERNET extended permit udp host 10.1.1.2 host 10.7.1.2 eq domain
access-list INTERNET extended permit udp host 10.2.1.2 host 10.7.1.2 eq domain
access-list INTERNET extended permit udp host 10.3.1.2 host 10.7.1.2 eq domain
access-list INTERNET extended permit tcp host 10.1.1.2 host 13.13.13.2 eq telnet
access-list INTERNET extended deny ip any any
!
!
access-group ULSA in interface ULSA
access-group DMZ in interface DMZ
access-group INTERNET in interface INTERNET
```

1. access-list ULSA: Permite o deniega tráfico entre dispositivos en la red ULSA.

- Permite HTTP y DNS desde ULSA SERVERS 10.4.1.2 a DNS WEB SERVER 10.7.1.2.
- Permite FTP y puertos relacionados desde ULSA NETWORK TEAM 10.5.1.2 a FTP SERVER 10.8.1.2.
- Permite ping (ICMP) desde ULSA USERS 10.6.1.2 a PC's GOOGLE.
- Permite TELNET desde ULSA NETWORK 10.5.1.2 a DMZ Switch Core 15.15.15.2
- Permite TELNET desde ULSA Switch Core 13.13.13.2 a PC GOOGLE 10.1.1.2
- Bloquea cualquier otro tráfico.

2. access-list DMZ: Controla el tráfico hacia la DMZ.

- Permite HTTP y DNS desde DNS WEB SERVER 10.7.1.2 a ULSA USERS 10.4.1.2.
- Permite FTP y puertos relacionados desde FTP SERVER 10.8.1.2. a ULSA NETWORK TEAM 10.5.1.2.
- Permite HTTP y DNS desde DNS WEB SERVER 10.7.1.2 a PC's GOOGLE.
- Permite TELNET desde DMZ Switch Core 15.15.15.2 a ULSA NETWORK 10.5.1.2
- Bloquea todo el tráfico no permitido.

3. access-list INTERNET: Controla el tráfico de y hacia la red externa.

- Permite ping (ICMP) desde PC's GOOGLE a ULSA USERS 10.6.1.2.
- Permite HTTP y DNS desde PC's GOOGLE a DNS WEB SERVER 10.7.1.2.
- Permite TELNET desde PC GOOGLE 10.1.1.2 a ULSA Switch Core 13.13.13.2
- Bloquea todo el tráfico no autorizado.

4. access-group: Asocia las listas de acceso (ACL) a las interfaces correspondientes:

- ULSA a la interfaz ULSA.
- DMZ a la interfaz DMZ.
- INTERNET a la interfaz INTERNET.

RESULTADOS

COMPROBACIÓN DE LA CORRECTA FUNCIÓN DE LA PRÁCTICA

SWITCHES

SHOW IP ROUTE de los Switches

```
OMAR_CORE_INTERNET#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

      10.0.0.0/24 is subnetted, 12 subnets
C        10.1.1.0 is directly connected, Vlan100
C        10.2.1.0 is directly connected, Vlan200
C        10.3.1.0 is directly connected, Vlan300
D  EX   10.4.1.0 [170/256026624] via 11.11.11.1, 00:00:56, GigabitEthernet1/0/24
D  EX   10.5.1.0 [170/256026624] via 11.11.11.1, 00:00:56, GigabitEthernet1/0/24
D  EX   10.6.1.0 [170/256026624] via 11.11.11.1, 00:00:56, GigabitEthernet1/0/24
D  EX   10.7.1.0 [170/256026624] via 11.11.11.1, 00:00:56, GigabitEthernet1/0/24
D  EX   10.8.1.0 [170/256026624] via 11.11.11.1, 00:00:56, GigabitEthernet1/0/24
D  EX   10.9.1.0 [170/256026624] via 11.11.11.1, 00:00:56, GigabitEthernet1/0/24
C        10.10.1.0 is directly connected, Vlan1000
D  EX   10.11.1.0 [170/256026624] via 11.11.11.1, 00:00:56, GigabitEthernet1/0/24
D  EX   10.12.1.0 [170/256026624] via 11.11.11.1, 00:00:56, GigabitEthernet1/0/24
      11.0.0.0/30 is subnetted, 1 subnets
C        11.11.11.0 is directly connected, GigabitEthernet1/0/24
      12.0.0.0/30 is subnetted, 1 subnets
D        12.12.12.0 [90/3072] via 11.11.11.1, 00:00:56, GigabitEthernet1/0/24
      13.0.0.0/30 is subnetted, 1 subnets
D        13.13.13.0 [90/3584] via 11.11.11.1, 00:00:56, GigabitEthernet1/0/24
      14.0.0.0/30 is subnetted, 1 subnets
D        14.14.14.0 [90/3328] via 11.11.11.1, 00:00:56, GigabitEthernet1/0/24
      15.0.0.0/30 is subnetted, 1 subnets
D        15.15.15.0 [90/3584] via 11.11.11.1, 00:00:56, GigabitEthernet1/0/24
      16.0.0.0/30 is subnetted, 1 subnets
D        16.16.16.0 [90/3328] via 11.11.11.1, 00:00:56, GigabitEthernet1/0/24
```

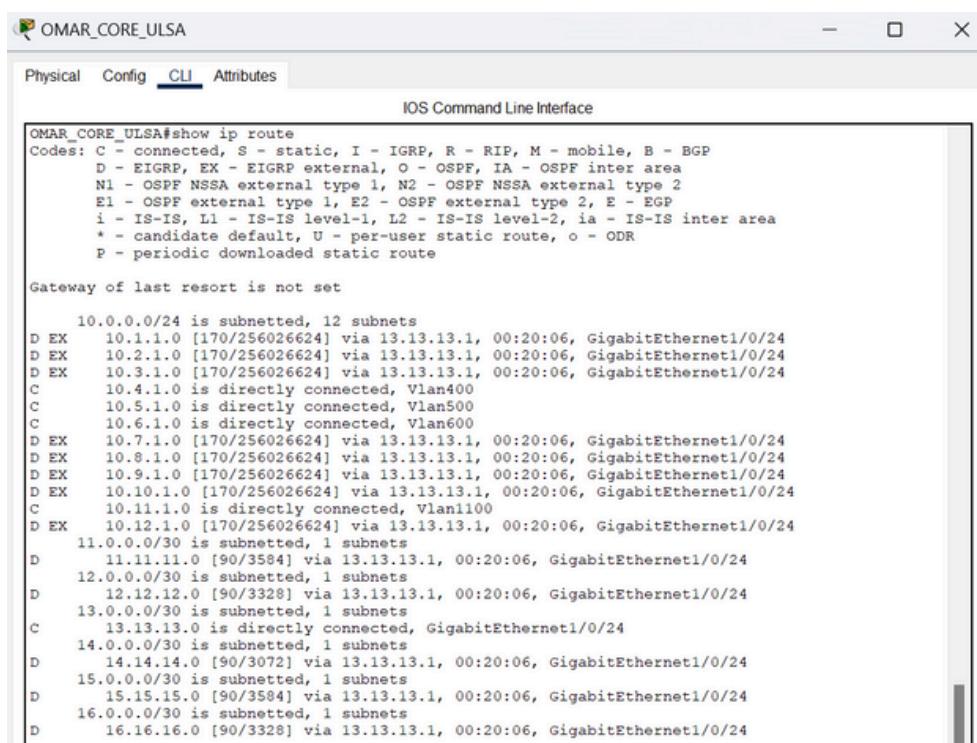
- C - 10.(1-2-3).1.0 Cuenta con 3 Vlans que están directamente conectadas al Switch.
D - 10.(4-5-6-7-8-9).1.0 Cuenta con las 6 siguientes Vlans que están conectadas al Switch mediante EIGRP external.
C - 10.10.1.0 Cuenta con la Vlan destinada para los DHCP servers que está directamente conectada al Switch.
D - 10.(11-12).1.0 Cuenta con las siguientes Vlans destinadas para los DHCP servers mediante EIGRP external.
C - 11.0.0.0 Cuenta con la red Wan que está directamente conectada al Switch.
D - (12-13-14-15-16).0.0.0 Cuenta con las siguientes Wan's que están conectadas al Switch mediante EIGRP.

RESULTADOS

COMPROBACIÓN DE LA CORRECTA FUNCIÓN DE LA PRÁCTICA

SWITCHES

SHOW IP ROUTE de los Switches



```
OMAR_CORE_ULSA
Physical Config CLI Attributes
IOS Command Line Interface

OMAR_CORE_ULSA#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/24 is subnetted, 12 subnets
D EX  10.1.1.0 [170/256026624] via 13.13.13.1, 00:20:06, GigabitEthernet1/0/24
D EX  10.2.1.0 [170/256026624] via 13.13.13.1, 00:20:06, GigabitEthernet1/0/24
D EX  10.3.1.0 [170/256026624] via 13.13.13.1, 00:20:06, GigabitEthernet1/0/24
C   10.4.1.0 is directly connected, Vlan400
C   10.5.1.0 is directly connected, Vlan500
C   10.6.1.0 is directly connected, Vlan600
D EX  10.7.1.0 [170/256026624] via 13.13.13.1, 00:20:06, GigabitEthernet1/0/24
D EX  10.8.1.0 [170/256026624] via 13.13.13.1, 00:20:06, GigabitEthernet1/0/24
D EX  10.9.1.0 [170/256026624] via 13.13.13.1, 00:20:06, GigabitEthernet1/0/24
D EX  10.10.1.0 [170/256026624] via 13.13.13.1, 00:20:06, GigabitEthernet1/0/24
C   10.11.1.0 is directly connected, Vlan1100
D EX  10.12.1.0 [170/256026624] via 13.13.13.1, 00:20:06, GigabitEthernet1/0/24
11.0.0.0/30 is subnetted, 1 subnets
D   11.11.11.0 [90/3584] via 13.13.13.1, 00:20:06, GigabitEthernet1/0/24
12.0.0.0/30 is subnetted, 1 subnets
D   12.12.12.0 [90/3328] via 13.13.13.1, 00:20:06, GigabitEthernet1/0/24
13.0.0.0/30 is subnetted, 1 subnets
C   13.13.13.0 is directly connected, GigabitEthernet1/0/24
14.0.0.0/30 is subnetted, 1 subnets
D   14.14.14.0 [90/3072] via 13.13.13.1, 00:20:06, GigabitEthernet1/0/24
15.0.0.0/30 is subnetted, 1 subnets
D   15.15.15.0 [90/3584] via 13.13.13.1, 00:20:06, GigabitEthernet1/0/24
16.0.0.0/30 is subnetted, 1 subnets
D   16.16.16.0 [90/3328] via 13.13.13.1, 00:20:06, GigabitEthernet1/0/24
```

C - 10.(4-5-6).1.0 Cuenta con 3 Vlans que están directamente conectadas al Switch.

D - 10.(1-2-3-7-8-9).1.0 Cuenta con las 6 siguientes Vlans que están conectadas al Switch mediante EIGRP external.

C - 10.11.1.0 Cuenta con la Vlan destinada para los DHCP servers que está directamente conectada al Switch.

D - 10.(10-12).1.0 Cuenta con las siguientes Vlans destinadas para los DHCP servers mediante EIGRP external.

C - 13.0.0.0 Cuenta con la red Wan que está directamente conectada al Switch.

D - (11-12-14-15-16).0.0.0 Cuenta con las siguientes Wan's que están conectadas al Switch mediante EIGRP.

RESULTADOS

COMPROBACIÓN DE LA CORRECTA FUNCIÓN DE LA PRÁCTICA

SWITCHES

SHOW IP ROUTE de los Switches

```
Switch#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

  10.0.0.0/24 is subnetted, 12 subnets
D EX   10.1.1.0 [170/256026624] via 15.15.15.1, 00:22:47, GigabitEthernet1/0/24
D EX   10.2.1.0 [170/256026624] via 15.15.15.1, 00:22:47, GigabitEthernet1/0/24
D EX   10.3.1.0 [170/256026624] via 15.15.15.1, 00:22:47, GigabitEthernet1/0/24
D EX   10.4.1.0 [170/256026624] via 15.15.15.1, 00:22:47, GigabitEthernet1/0/24
D EX   10.5.1.0 [170/256026624] via 15.15.15.1, 00:22:47, GigabitEthernet1/0/24
D EX   10.6.1.0 [170/256026624] via 15.15.15.1, 00:22:47, GigabitEthernet1/0/24
C     10.7.1.0 is directly connected, Vlan700
C     10.8.1.0 is directly connected, Vlan800
C     10.9.1.0 is directly connected, Vlan900
D EX   10.10.1.0 [170/256026624] via 15.15.15.1, 00:22:47, GigabitEthernet1/0/24
D EX   10.11.1.0 [170/256026624] via 15.15.15.1, 00:22:47, GigabitEthernet1/0/24
C     10.12.1.0 is directly connected, Vlan1200
    11.0.0.0/30 is subnetted, 1 subnets
D     11.11.11.0 [90/3584] via 15.15.15.1, 00:22:47, GigabitEthernet1/0/24
    12.0.0.0/30 is subnetted, 1 subnets
D     12.12.12.0 [90/3328] via 15.15.15.1, 00:22:47, GigabitEthernet1/0/24
    13.0.0.0/30 is subnetted, 1 subnets
D     13.13.13.0 [90/3584] via 15.15.15.1, 00:22:47, GigabitEthernet1/0/24
    14.0.0.0/30 is subnetted, 1 subnets
D     14.14.14.0 [90/3328] via 15.15.15.1, 00:22:47, GigabitEthernet1/0/24
    15.0.0.0/30 is subnetted, 1 subnets
C     15.15.15.0 is directly connected, GigabitEthernet1/0/24
    16.0.0.0/30 is subnetted, 1 subnets
D     16.16.16.0 [90/3072] via 15.15.15.1, 00:22:47, GigabitEthernet1/0/24
```

C - 10.(7-8-9).1.0 Cuenta con 3 Vlans que están directamente conectadas al Switch.

D - 10.(1-2-3-4-5-6).1.0 Cuenta con las 6 siguientes Vlans que están conectadas al Switch mediante EIGRP external.

C - 10.12.1.0 Cuenta con la Vlan destinada para los DHCP servers que está directamente conectada al Switch.

D - 10.(10-11).1.0 Cuenta con las siguientes Vlans destinadas para los DHCP servers mediante EIGRP external.

C - 15.0.0.0 Cuenta con la red Wan que está directamente conectada al Switch.

D - (11-12-13-14-16).0.0.0 Cuenta con las siguientes Wan's que están conectadas al Switch mediante EIGRP.

RESULTADOS

COMPROBACIÓN DE LA CORRECTA FUNCIÓN DE LA PRÁCTICA

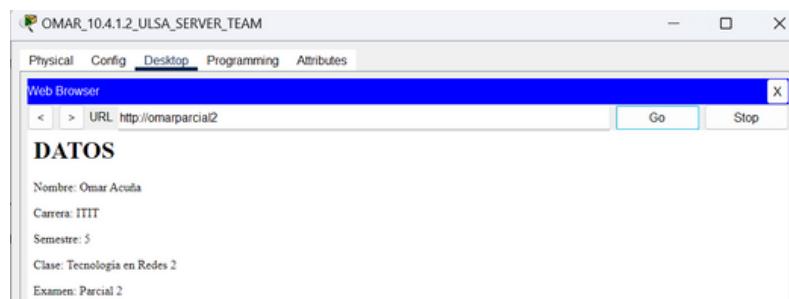
TELNET – DNS WEB SERVER

PC GOOGLE ALCANZANDO AL SWITCH ULSA MEDIANTE TELNET



```
Trying 13.13.13.2 ...Open
User Access Verification
Username: Omar3
Password: OMAR_CORE_ULSA>
```

PC ALCANZANDO AL DNS WEB SERVER

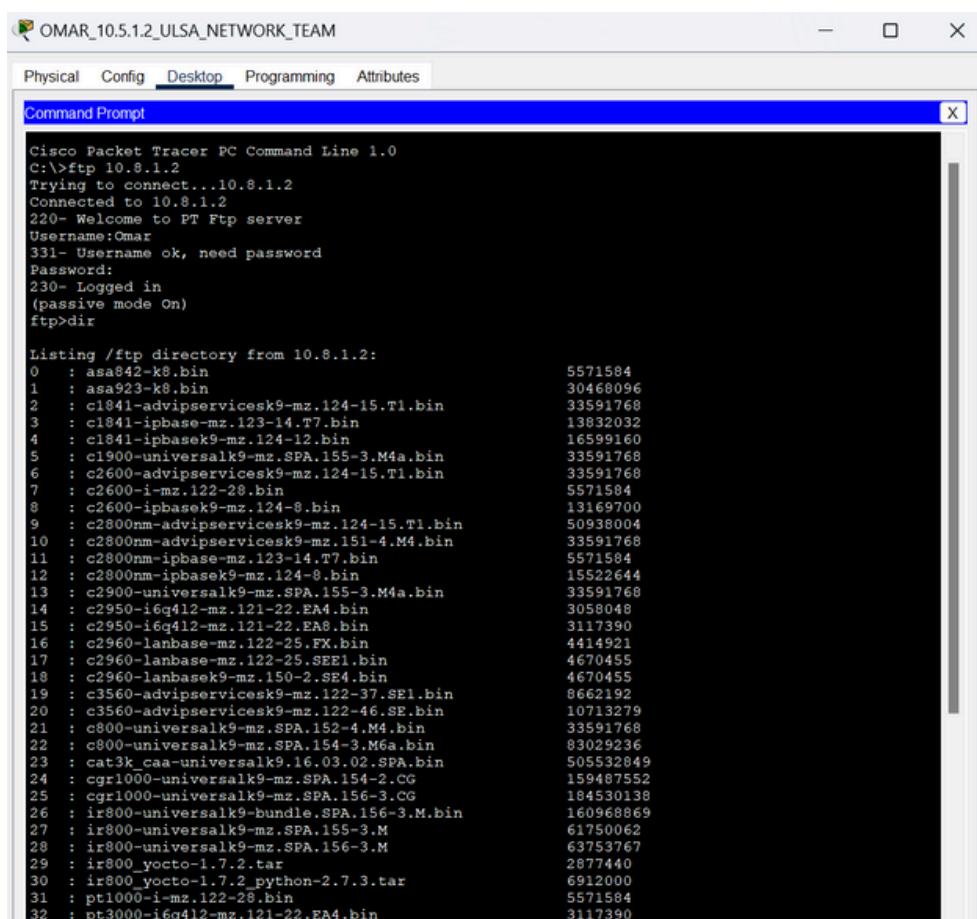


RESULTADOS

COMPROBACIÓN DE LA CORRECTA FUNCIÓN DE LA PRÁCTICA

FTP SERVER

PC ALCANZANDO AL FTP SERVER



The screenshot shows a Cisco Packet Tracer window titled "OMAR_10.5.1.2_ULSA_NETWORK_TEAM". It displays a Command Prompt window with the following output:

```
Cisco Packet Tracer PC Command Line 1.0
C:>ftp 10.8.1.2
Trying to connect...10.8.1.2
Connected to 10.8.1.2
220- Welcome to PT Ftp server
Username:Omar
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir

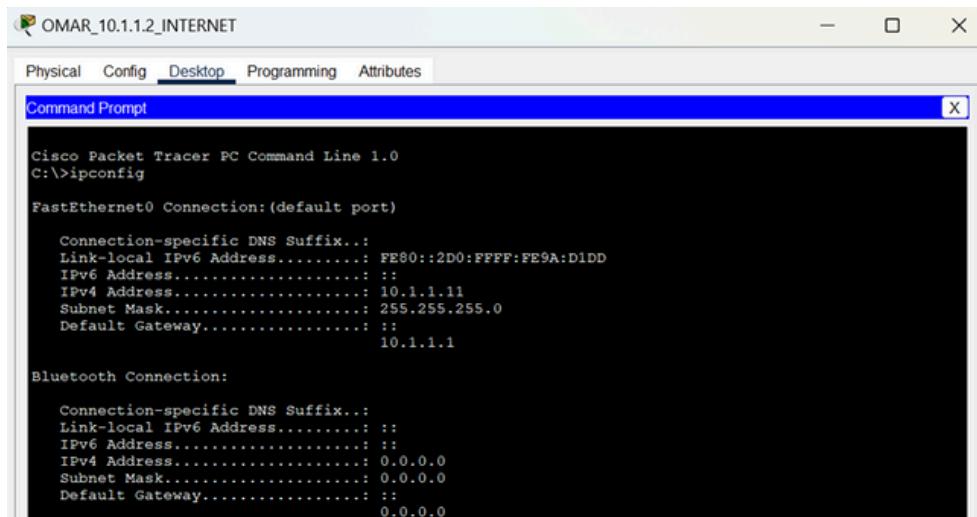
Listing /ftp directory from 10.8.1.2:
0 : asa842-k8.bin          5571584
1 : asa923-k8.bin          30468096
2 : c1841-advp�servicesk9-mz.124-15.T1.bin   33591768
3 : c1841-ipbasek9-mz.123-14.T7.bin      13832032
4 : c1841-ipbasek9-mz.124-12.bin      16599160
5 : c1900-universalk9-mz.SPA.155-3.M4a.bin    33591768
6 : c2600-advp�servicesk9-mz.124-15.T1.bin   33591768
7 : c2600-i-mz.122-28.bin      5571584
8 : c2600-ipbasek9-mz.124-8.bin      13169700
9 : c2800nm-advp�servicesk9-mz.124-15.T1.bin  50938004
10 : c2800nm-advp�servicesk9-mz.151-4.M4.bin  33591768
11 : c2800nm-ipbasek9-mz.123-14.T7.bin      5571584
12 : c2800nm-ipbasek9-mz.124-8.bin      15522644
13 : c2900-universalk9-mz.SPA.155-3.M4a.bin    33591768
14 : c2950-i6q412-mz.121-22.EA4.bin      3058048
15 : c2950-i6q412-mz.121-22.EA8.bin      3117390
16 : c2960-lanbase-mz.122-25.FX.bin      4414921
17 : c2960-lanbase-mz.122-25.SE1.bin      4670455
18 : c2960-lanbasek9-mz.150-2.SE4.bin      4670455
19 : c3560-advp�servicesk9-mz.122-37.SE1.bin  8662192
20 : c3560-advp�servicesk9-mz.122-46.SE.bin   10713279
21 : c800-universalk9-mz.SPA.152-4.M4.bin    33591768
22 : c800-universalk9-mz.SPA.154-3.M6a.bin    83029236
23 : cat3k_caa-universalk9.16.03.02.SPA.bin  505532849
24 : cgr1000-universalk9-mz.SPA.154-2.CG    159487552
25 : cgr1000-universalk9-mz.SPA.156-3.CG    184530138
26 : ir800-universalk9-bundle.SPA.156-3.M.bin 160968869
27 : ir800-universalk9-mz.SPA.155-3.M       61750062
28 : ir800-universalk9-mz.SPA.156-3.M       63753767
29 : ir800_yocto-1.7.2.tar                 2877440
30 : ir800_yocto-1.7.2_python-2.7.3.tar    6912000
31 : pt1000-i-mz.122-28.bin      5571584
32 : pt3000-i6q412-mz.121-22.EA4.bin    3117390
```

RESULTADOS

COMPROBACIÓN DE LA CORRECTA FUNCIÓN DE LA PRÁCTICA

DHCPSERVER

IPS OBTENIDAS



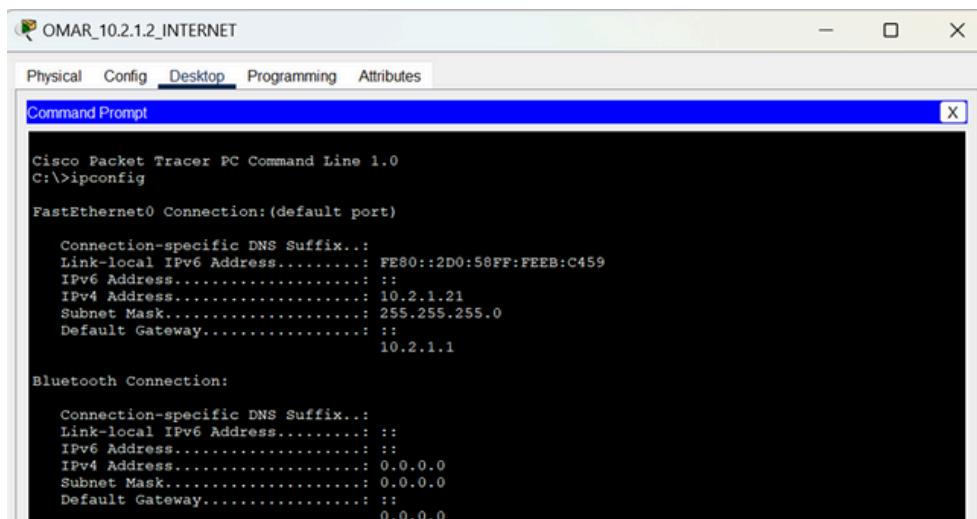
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::2D0:FFFF:FE9A:D1DD
IPv6 Address.....: ::
IPv4 Address.....: 10.1.1.11
Subnet Mask.....: 255.255.255.0
Default Gateway.....: ::
10.1.1.1

Bluetooth Connection:

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: ::
IPv6 Address.....: ::
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: ::
0.0.0.0
```



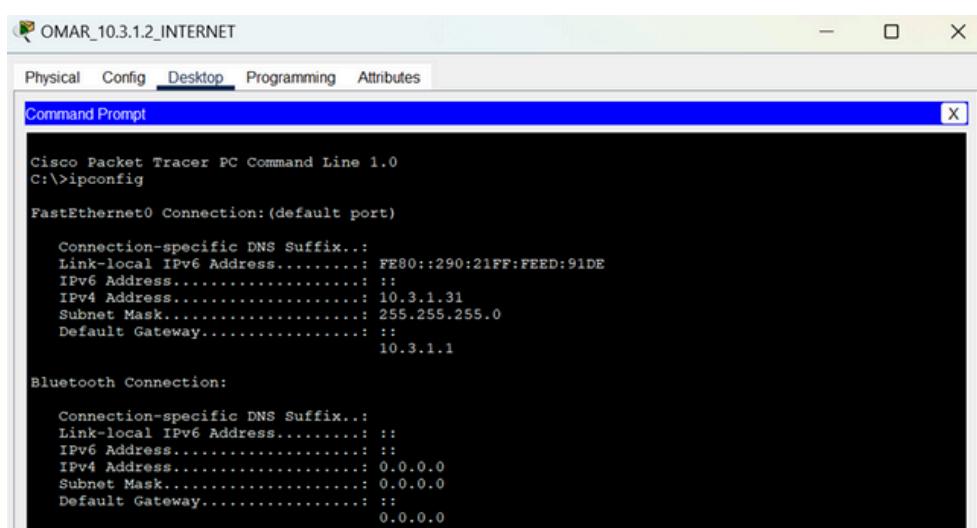
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::2D0:58FF:FE8B:C459
IPv6 Address.....: ::
IPv4 Address.....: 10.2.1.21
Subnet Mask.....: 255.255.255.0
Default Gateway.....: ::
10.2.1.1

Bluetooth Connection:

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: ::
IPv6 Address.....: ::
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: ::
0.0.0.0
```



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::290:21FF:FEED:91DE
IPv6 Address.....: ::
IPv4 Address.....: 10.3.1.31
Subnet Mask.....: 255.255.255.0
Default Gateway.....: ::
10.3.1.1

Bluetooth Connection:

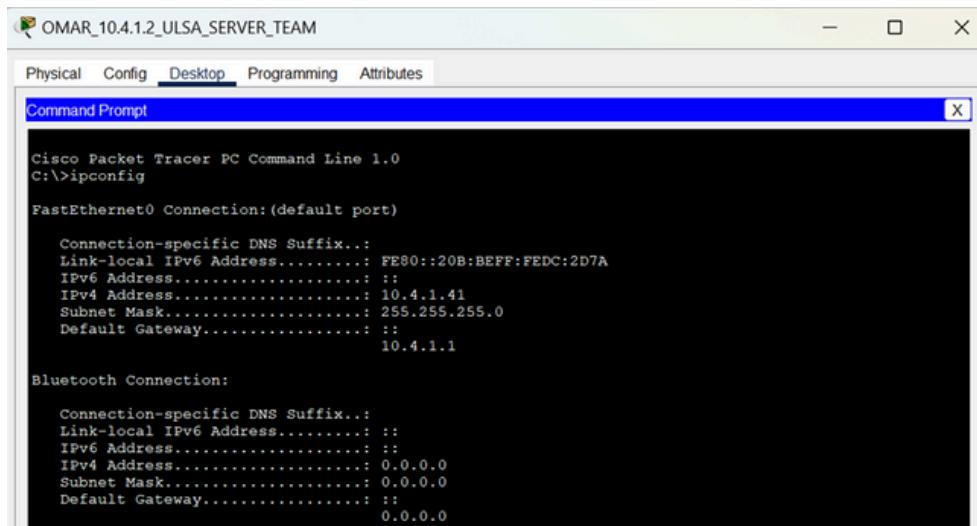
Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: ::
IPv6 Address.....: ::
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: ::
0.0.0.0
```

RESULTADOS

COMPROBACIÓN DE LA CORRECTA FUNCIÓN DE LA PRÁCTICA

DHCPSERVER

IPS OBTENIDAS



```
Cisco Packet Tracer PC Command Line 1.0
C:>ipconfig

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::20B:BEFF:FE00:2D7A
IPv6 Address.....: ::

IPv4 Address.....: 10.4.1.41
Subnet Mask.....: 255.255.255.0
Default Gateway.....: ::

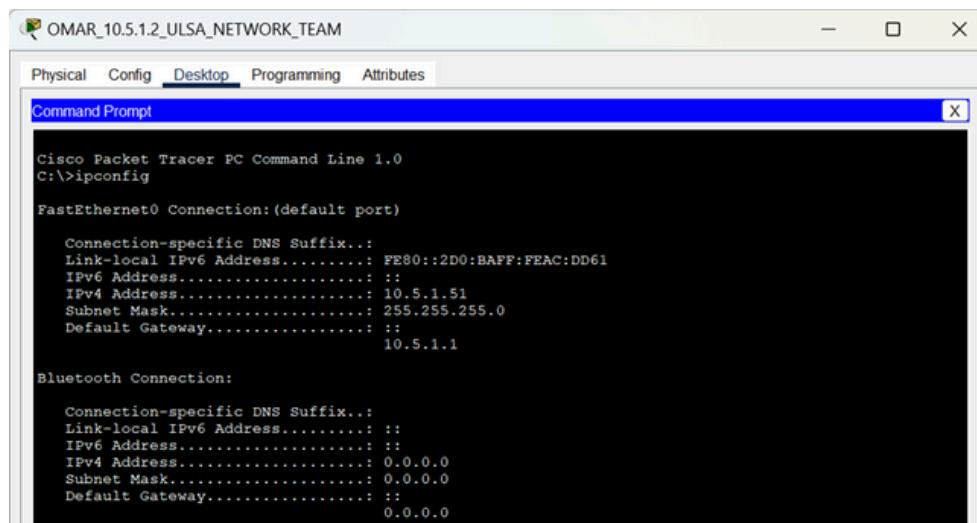
10.4.1.1

Bluetooth Connection:

Connection-specific DNS Suffix..:
Link-local IPv6 Address.....: ::
IPv6 Address.....: ::

IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: ::

0.0.0.0
```



```
Cisco Packet Tracer PC Command Line 1.0
C:>ipconfig

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix..:
Link-local IPv6 Address.....: FE80::2D0:BAFF:FEAC:DD61
IPv6 Address.....: ::

IPv4 Address.....: 10.5.1.51
Subnet Mask.....: 255.255.255.0
Default Gateway.....: ::

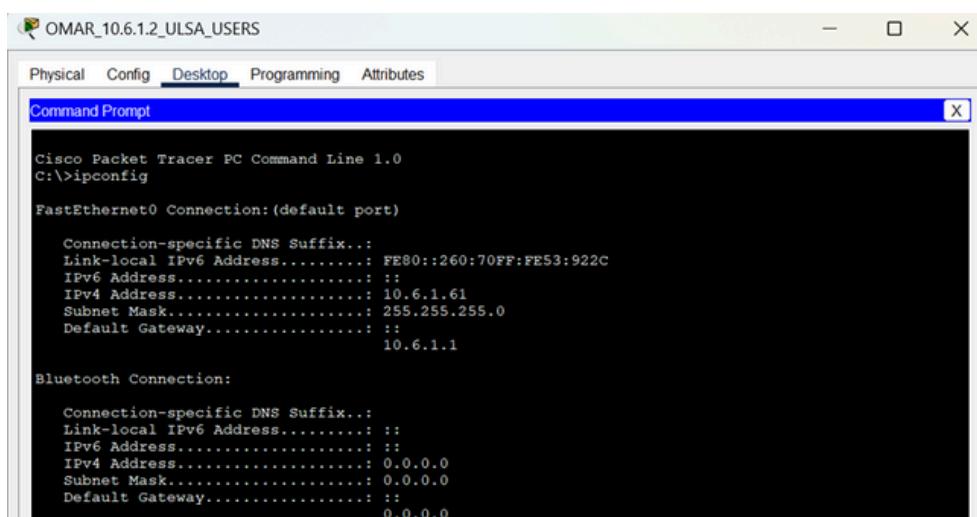
10.5.1.1

Bluetooth Connection:

Connection-specific DNS Suffix..:
Link-local IPv6 Address.....: ::
IPv6 Address.....: ::

IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: ::

0.0.0.0
```



```
Cisco Packet Tracer PC Command Line 1.0
C:>ipconfig

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix..:
Link-local IPv6 Address.....: FE80::260:70FF:FE53:922C
IPv6 Address.....: ::

IPv4 Address.....: 10.6.1.61
Subnet Mask.....: 255.255.255.0
Default Gateway.....: ::

10.6.1.1

Bluetooth Connection:

Connection-specific DNS Suffix..:
Link-local IPv6 Address.....: ::
IPv6 Address.....: ::

IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: ::

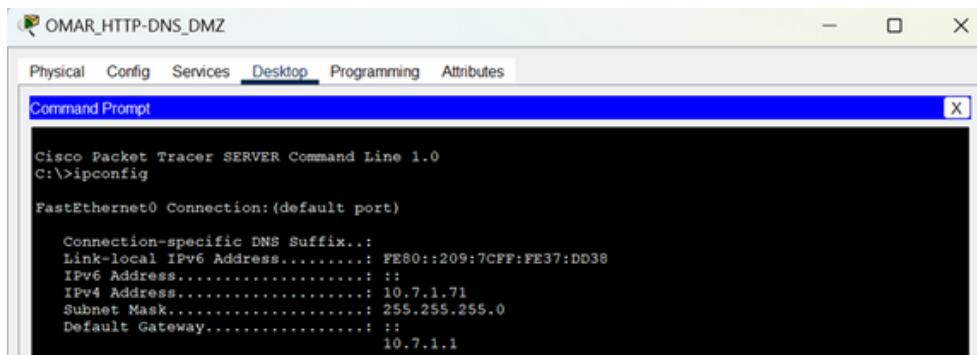
0.0.0.0
```

RESULTADOS

COMPROBACIÓN DE LA CORRECTA FUNCIÓN DE LA PRÁCTICA

DHCPSERVER

IPS OBTENIDAS



OMAR_HTTP-DNS_DMZ

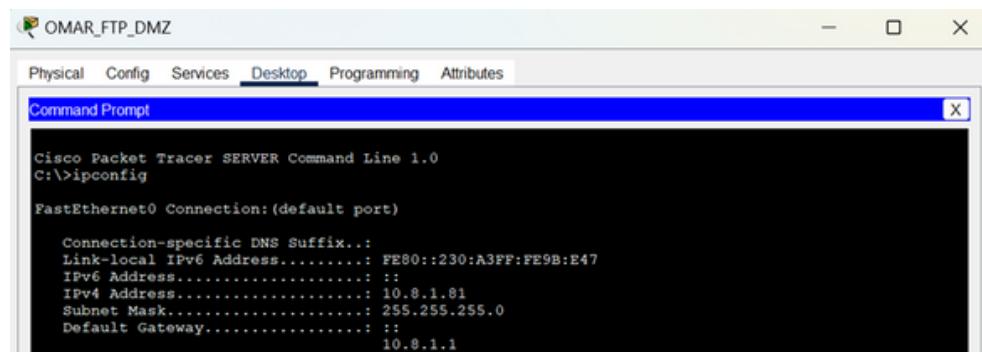
Physical Config Services Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer SERVER Command Line 1.0
C:>ipconfig

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::209:7CFF:FE37:DD38
IPv6 Address.....: :::
IPv4 Address.....: 10.7.1.71
Subnet Mask.....: 255.255.255.0
Default Gateway.....: :::
10.7.1.1
```



OMAR_FTP_DMZ

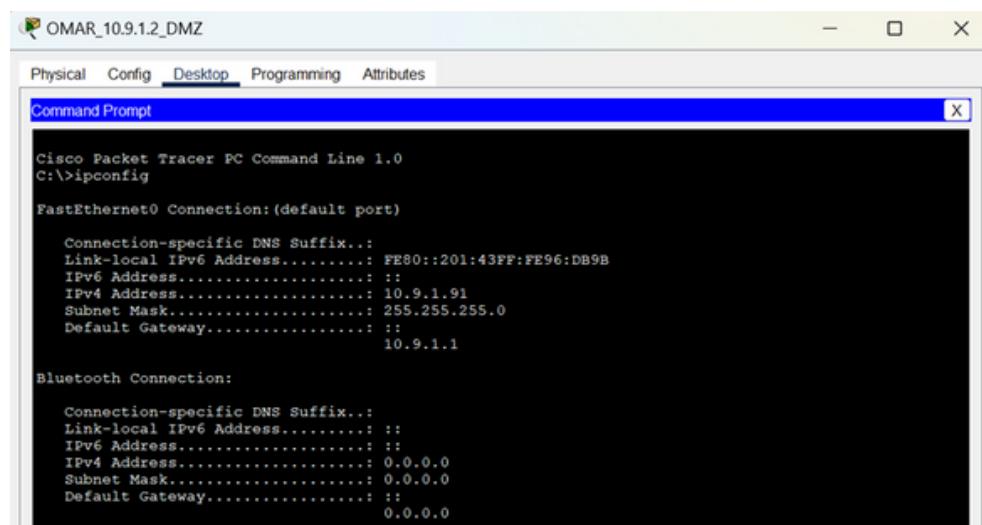
Physical Config Services Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer SERVER Command Line 1.0
C:>ipconfig

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::230:A3FF:FE9B:E47
IPv6 Address.....: :::
IPv4 Address.....: 10.8.1.81
Subnet Mask.....: 255.255.255.0
Default Gateway.....: :::
10.8.1.1
```



OMAR_10.9.1.2_DMZ

Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:>ipconfig

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::201:43FF:FE96:DB9B
IPv6 Address.....: :::
IPv4 Address.....: 10.9.1.91
Subnet Mask.....: 255.255.255.0
Default Gateway.....: :::
10.9.1.1

Bluetooth Connection:

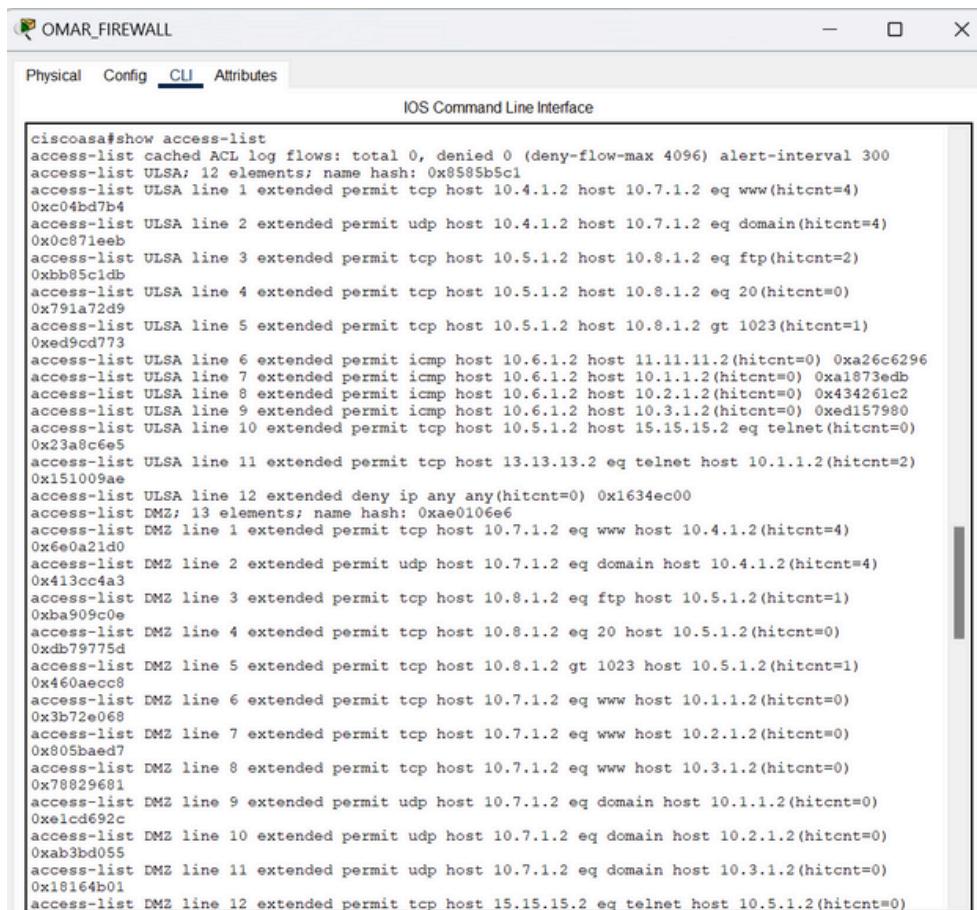
Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: :::
IPv6 Address.....: :::
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: :::
0.0.0.0
```

RESULTADOS

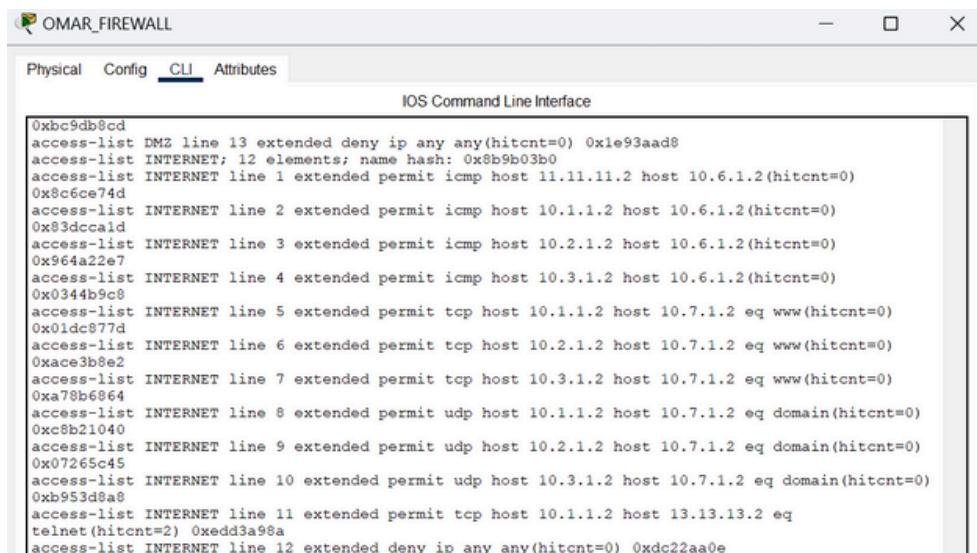
COMPROBACIÓN DE LA CORRECTA FUNCIÓN DE LA PRÁCTICA

FIREWALL

SHOW ACCESS-LIST Y HIT COUNT



```
ciscoasa#show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval 300
access-list ULSA; 12 elements; name hash: 0x8585b5c1
access-list ULSA line 1 extended permit tcp host 10.4.1.2 host 10.7.1.2 eq www(hitcnt=4)
0xc04bd7b4
access-list ULSA line 2 extended permit udp host 10.4.1.2 host 10.7.1.2 eq domain(hitcnt=4)
0x0c871eeb
access-list ULSA line 3 extended permit tcp host 10.5.1.2 host 10.8.1.2 eq ftp(hitcnt=2)
0xbb85c1db
access-list ULSA line 4 extended permit tcp host 10.5.1.2 host 10.8.1.2 eq 20(hitcnt=0)
0x791a72d9
access-list ULSA line 5 extended permit tcp host 10.5.1.2 host 10.8.1.2 gt 1023(hitcnt=1)
0xed9cd773
access-list ULSA line 6 extended permit icmp host 10.6.1.2 host 11.11.11.2(hitcnt=0) 0xa26c6296
access-list ULSA line 7 extended permit icmp host 10.6.1.2 host 10.1.1.2(hitcnt=0) 0xa1873edb
access-list ULSA line 8 extended permit icmp host 10.6.1.2 host 10.2.1.2(hitcnt=0) 0x434261c2
access-list ULSA line 9 extended permit icmp host 10.6.1.2 host 10.3.1.2(hitcnt=0) 0xed157980
access-list ULSA line 10 extended permit tcp host 10.5.1.2 host 15.15.15.2 eq telnet(hitcnt=0)
0x23a8c6e5
access-list ULSA line 11 extended permit tcp host 13.13.13.2 eq telnet host 10.1.1.2(hitcnt=2)
0x151009ae
access-list ULSA line 12 extended deny ip any any(hitcnt=0) 0x1634ec00
access-list DMZ; 13 elements; name hash: 0xae0106e6
access-list DMZ line 1 extended permit tcp host 10.7.1.2 eq www host 10.4.1.2(hitcnt=4)
0x6e0a21d0
access-list DMZ line 2 extended permit udp host 10.7.1.2 eq domain host 10.4.1.2(hitcnt=4)
0x413cc4a3
access-list DMZ line 3 extended permit tcp host 10.8.1.2 eq ftp host 10.5.1.2(hitcnt=1)
0xba909c0e
access-list DMZ line 4 extended permit tcp host 10.8.1.2 eq 20 host 10.5.1.2(hitcnt=0)
0xdb79775d
access-list DMZ line 5 extended permit tcp host 10.8.1.2 gt 1023 host 10.5.1.2(hitcnt=1)
0x460aec08
access-list DMZ line 6 extended permit tcp host 10.7.1.2 eq www host 10.1.1.2(hitcnt=0)
0xb3b72e068
access-list DMZ line 7 extended permit tcp host 10.7.1.2 eq www host 10.2.1.2(hitcnt=0)
0x805baed7
access-list DMZ line 8 extended permit tcp host 10.7.1.2 eq www host 10.3.1.2(hitcnt=0)
0x78829681
access-list DMZ line 9 extended permit udp host 10.7.1.2 eq domain host 10.1.1.2(hitcnt=0)
0x1cd692c
access-list DMZ line 10 extended permit udp host 10.7.1.2 eq domain host 10.2.1.2(hitcnt=0)
0xab3bd055
access-list DMZ line 11 extended permit udp host 10.7.1.2 eq domain host 10.3.1.2(hitcnt=0)
0x18164b01
access-list DMZ line 12 extended permit tcp host 15.15.15.2 eq telnet host 10.5.1.2(hitcnt=0)
```



```
0xbc9db8cd
access-list DMZ line 13 extended deny ip any any(hitcnt=0) 0x1e93aad8
access-list INTERNET; 12 elements; name hash: 0xb9b03b0
access-list INTERNET line 1 extended permit icmp host 11.11.11.2 host 10.6.1.2(hitcnt=0)
0x8c6ce74d
access-list INTERNET line 2 extended permit icmp host 10.1.1.2 host 10.6.1.2(hitcnt=0)
0x83dccald
access-list INTERNET line 3 extended permit icmp host 10.2.1.2 host 10.6.1.2(hitcnt=0)
0x964a22e7
access-list INTERNET line 4 extended permit icmp host 10.3.1.2 host 10.6.1.2(hitcnt=0)
0x0344b9c8
access-list INTERNET line 5 extended permit tcp host 10.1.1.2 host 10.7.1.2 eq www(hitcnt=0)
0x01dc877d
access-list INTERNET line 6 extended permit tcp host 10.2.1.2 host 10.7.1.2 eq www(hitcnt=0)
0xace3b8e2
access-list INTERNET line 7 extended permit tcp host 10.3.1.2 host 10.7.1.2 eq www(hitcnt=0)
0xa78b6864
access-list INTERNET line 8 extended permit udp host 10.1.1.2 host 10.7.1.2 eq domain(hitcnt=0)
0xc85b21040
access-list INTERNET line 9 extended permit udp host 10.2.1.2 host 10.7.1.2 eq domain(hitcnt=0)
0x07265c45
access-list INTERNET line 10 extended permit udp host 10.3.1.2 host 10.7.1.2 eq domain(hitcnt=0)
0xb953d8a8
access-list INTERNET line 11 extended permit tcp host 10.1.1.2 host 13.13.13.2 eq
telnet(hitcnt=2) 0xedd3a98a
access-list INTERNET line 12 extended deny ip any any(hitcnt=0) 0xdc22aa0e
```

RESULTADOS

COMPROBACIÓN DE LA CORRECTA
FUNCIÓN DE LA PRÁCTICA

SIMULACIÓN

MOSTRAR PAQUETES VIAJANDO



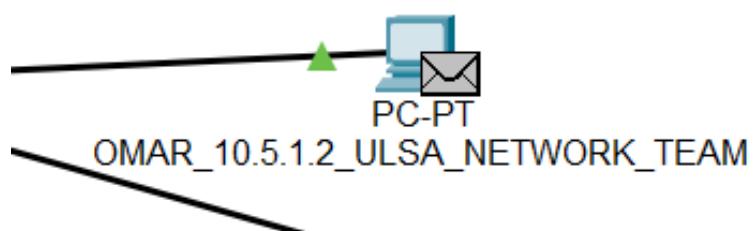
■ TELNET



■ DNS



■ HTTP



■ FTP

CONCLUSIÓN



LA TOPOLOGÍA PRESENTADA GARANTIZA UNA INTERCONEXIÓN EFICIENTE ENTRE REDES COMO INTERNET, ULSA Y DMZ, MANTENIENDO UN ALTO NIVEL DE SEGURIDAD. LA CONEXIÓN DE PCS Y SERVIDORES A SUS RESPECTIVOS CORES Y ROUTERS, JUNTO CON UN FIREWALL CENTRALIZADO, ASEGURA UN CONTROL EFICAZ DEL TRÁFICO ENTRE SUBREDES Y LA PROTECCIÓN FREnte A AMENAZAS EXTERNAS.

LA DISPOSICIÓN DE ROUTERS Y FIREWALLS NO SOLO FACILITA LA COMUNICACIÓN FLUIDA ENTRE REDES INTERNAS Y EXTERNAS, SINO QUE TAMBIÉN REFUERZA LA SEGURIDAD DE LA INFRAESTRUCTURA. LA INTEGRACIÓN DE TELNET PERMITE UNA ADMINISTRACIÓN REMOTA EFICIENTE, MIENTRAS QUE EL SERVIDOR DHCP OPTIMIZA LA ASIGNACIÓN AUTOMÁTICA DE DIRECCIONES IP, SIMPLIFICANDO LA GESTIÓN DE RED.

EN CONCLUSIÓN, LA TOPOLOGÍA DISEÑADA COMBINA CONECTIVIDAD, SEGURIDAD Y ADMINISTRACIÓN EFICIENTE. LA INCLUSIÓN DE LA DMZ, EL FIREWALL CENTRALIZADO, Y LAS CONFIGURACIONES DE TELNET Y DHCP REFLEJAN UN ENFOQUE INTEGRAL HACIA LA PROTECCIÓN, INTERCONEXIÓN Y GESTIÓN DEL TRÁFICO, CUMPLIENDO CON LAS DEMANDAS DE UNA RED MODERNA Y SEGURA.