

TECNOLOGIA DE REDES

MANUAL PACKET TRACER

CISCO

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 y listas de acceso. 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 ha añadido una zona DMZ con un Router y Switch DMZ donde se conectan un DNS-WEB Server y un FTP Server mejorando 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
- 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 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

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

GLOSARIO DE COMANDOS

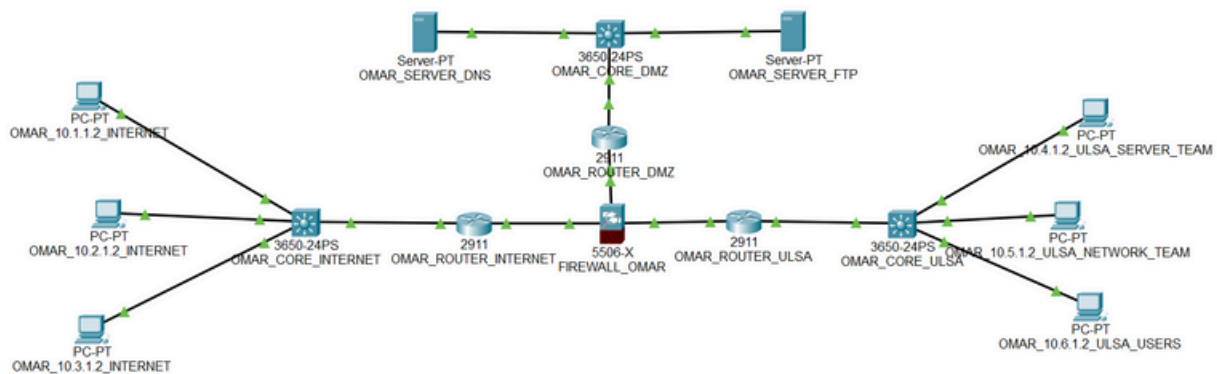
ANEXO DE COMANDOS UTILIZADAS DURANTE EL MANUAL

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. **ROUTER EIGRP 100**: Inicia el protocolo de enrutamiento EIGRP con el número de sistema autónomo 100.
12. **NETWORK [dirección IP]**: Define las redes a las que se aplica el protocolo EIGRP.
13. **REDISTRIBUTE CONNECTED**: Redistribuye las rutas conectadas directamente en el protocolo de enrutamiento EIGRP.
14. **no switchport**: Convierte la interfaz de capa 2 a capa 3, lo que permite asignar direcciones IP.
15. **nameif [nombre]**: Asigna un nombre a la interfaz (normalmente en dispositivos con firewall).
16. **security-level [nivel]**: Define el nivel de seguridad de una interfaz (usualmente en firewalls, como el ASA de Cisco).
20. **Username [nombre] password [contraseña]**: Crea un usuario local con su respectiva contraseña.
21. **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.
22. **access-group [nombre de lista] in interface [nombre interfaz]**: Aplica la lista de acceso a una interfaz específica.
24. **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 y 3 routers 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.

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.

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

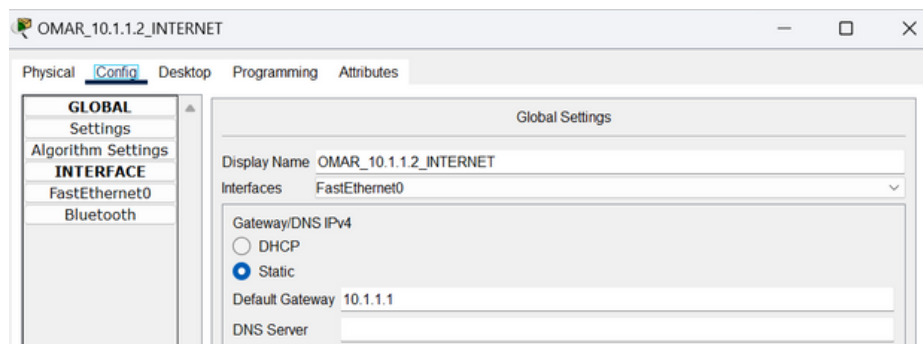
COMANDOS DE CADA DISPOSITIVO PARA CONECTAR LA RED

CONFIGURAR PC

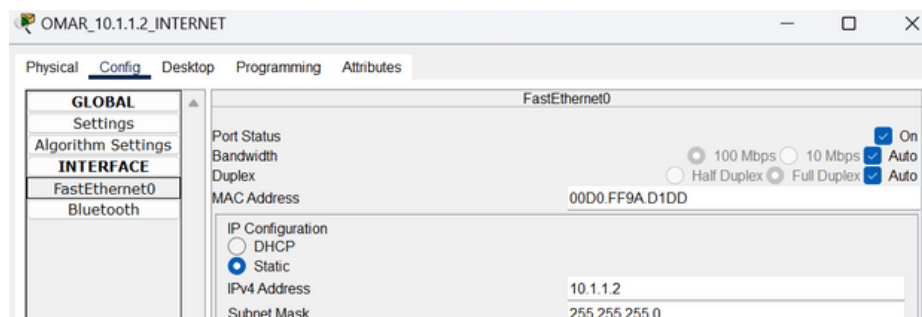
Para la configuración de los dispositivos nos basaremos en los detalles de la práctica. Las redes que usaremos serán en base a lo que nos pide la práctica de laboratorio. Comenzaremos con la configuración de las PCs, al ser una red espejo, no habrá necesidad de repetir la explicación por cada una de 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 los 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 y es un /24. De ser el caso de una 200, su direccionamiento sería el siguiente 10.2.1 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.



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.

OMAR_10.2.1.2_INTERNET

Physical **Config** Desktop Programming Attributes

GLOBAL

Settings

Algorithm Settings

INTERFACE

FastEthernet0

Bluetooth

Global Settings

Display Name OMAR_10.2.1.2_INTERNET

Interfaces FastEthernet0

Gateway/DNS IPv4

☐ DHCP

☒ Static

Default Gateway 10.2.1.1

DNS Server

OMAR_10.2.1.2_INTERNET

Physical **Config** Desktop Programming Attributes

GLOBAL

Settings

Algorithm Settings

INTERFACE

FastEthernet0

Bluetooth

FastEthernet0

Port Status ☒ On

Bandwidth ☒ Auto

Duplex ☒ Full Duplex

MAC Address 00D0.58EB.C459

IP Configuration

☐ DHCP

☒ Static

IPv4 Address 10.2.1.2

Subnet Mask 255.255.255.0

OMAR_10.3.1.2_INTERNET

Physical **Config** Desktop Programming Attributes

GLOBAL

Settings

Algorithm Settings

INTERFACE

FastEthernet0

Bluetooth

Global Settings

Display Name OMAR_10.3.1.2_INTERNET

Interfaces FastEthernet0

Gateway/DNS IPv4

☐ DHCP

☒ Static

Default Gateway 10.3.1.1

DNS Server

OMAR_10.3.1.2_INTERNET

Physical **Config** Desktop Programming Attributes

GLOBAL

Settings

Algorithm Settings

INTERFACE

FastEthernet0

Bluetooth

FastEthernet0

Port Status ☒ On

Bandwidth ☒ Auto

Duplex ☒ Full Duplex

MAC Address 0090.21ED.91DE

IP Configuration

☐ DHCP

☒ Static

IPv4 Address 10.3.1.2

Subnet Mask 255.255.255.0

OMAR_10.4.1.2_ULSA

Physical **Config** Desktop Programming Attributes

GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth

Global Settings

Display Name OMAR_10.4.1.2_ULSA

Interfaces FastEthernet0

Gateway/DNS IPv4
☐ DHCP
☒ Static
Default Gateway 10.4.1.1
DNS Server

OMAR_10.4.1.2_ULSA

Physical **Config** Desktop Programming Attributes

GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth

FastEthernet0

Port Status ☒ On
Bandwidth ☒ 100 Mbps ☐ 10 Mbps ☒ Auto
Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto
MAC Address 000B.BEDC.2D7A

IP Configuration
☐ DHCP
☒ Static
IPv4 Address 10.4.1.2
Subnet Mask 255.255.255.0

OMAR_10.5.1.2_ULSA

Physical **Config** Desktop Programming Attributes

GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth

Global Settings

Display Name OMAR_10.5.1.2_ULSA

Interfaces FastEthernet0

Gateway/DNS IPv4
☐ DHCP
☒ Static
Default Gateway 10.5.1.1
DNS Server

OMAR_10.5.1.2_ULSA

Physical **Config** Desktop Programming Attributes

GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth

FastEthernet0

Port Status ☒ On
Bandwidth ☒ 100 Mbps ☐ 10 Mbps ☒ Auto
Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto
MAC Address 00D0.BAAC.DD61

IP Configuration
☐ DHCP
☒ Static
IPv4 Address 10.5.1.2
Subnet Mask 255.255.255.0

OMAR_10.6.1.2_ULSA

Physical **Config** Desktop Programming Attributes

GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth

Global Settings

Display Name OMAR_10.6.1.2_ULSA

Interfaces FastEthernet0

Gateway/DNS IPv4
☐ DHCP
☒ Static
Default Gateway 10.6.1.1
DNS Server

OMAR_10.6.1.2_ULSA

Physical **Config** Desktop Programming Attributes

GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth

FastEthernet0

Port Status ☒ On
Bandwidth ☒ 100 Mbps ☐ 10 Mbps ☒ Auto
Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto
MAC Address 0060.7053.922C

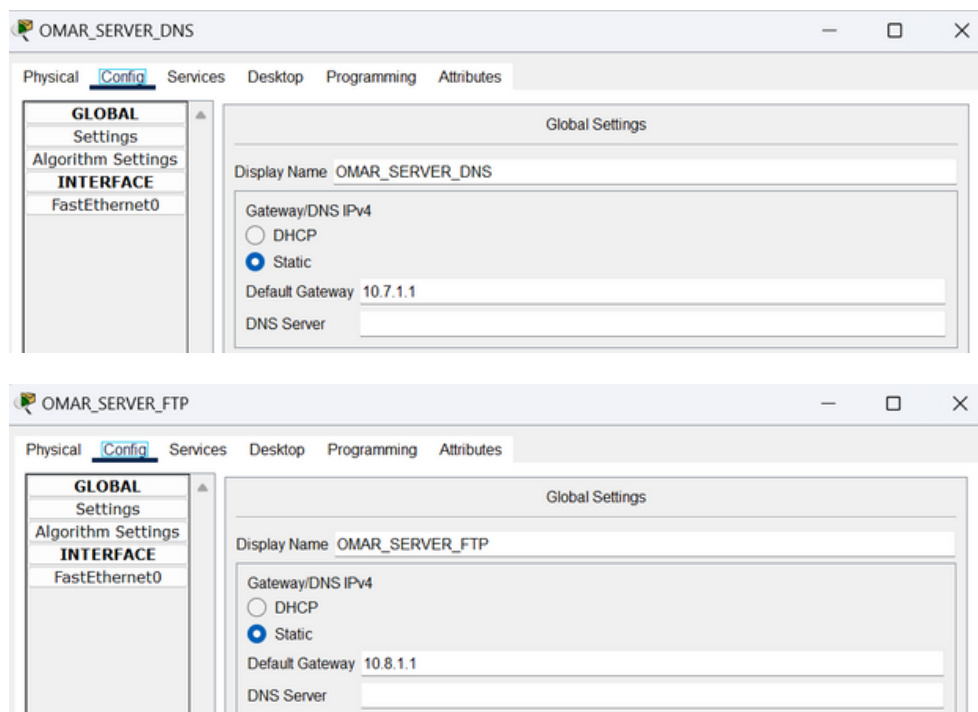
IP Configuration
☐ DHCP
☒ Static
IPv4 Address 10.6.1.2
Subnet Mask 255.255.255.0

CONFIGURACIÓN

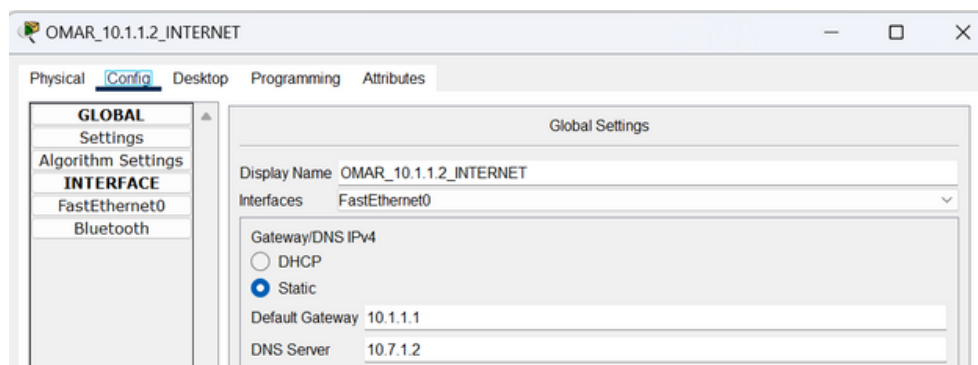
COMANDOS DE CADA DISPOSITIVO PARA CONECTAR LA RED

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.

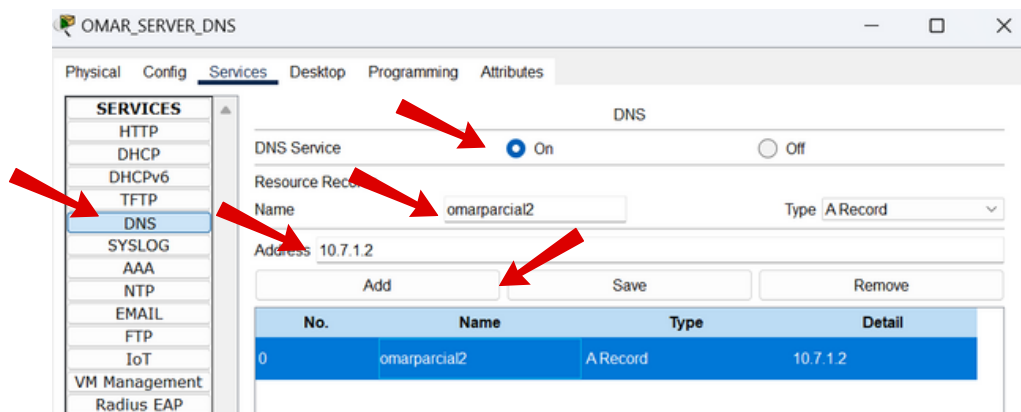


CONFIGURACIÓN

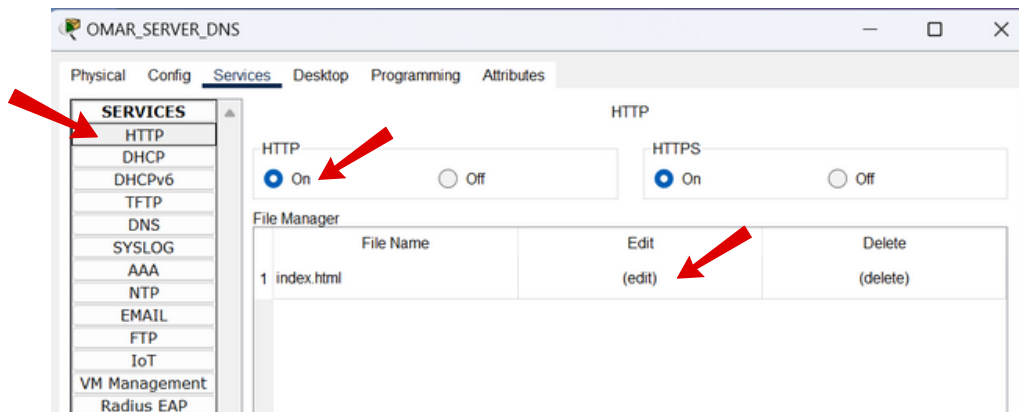
COMANDOS DE CADA DISPOSITIVO PARA CONECTAR LA RED

CONFIGURAR SERVICIOS

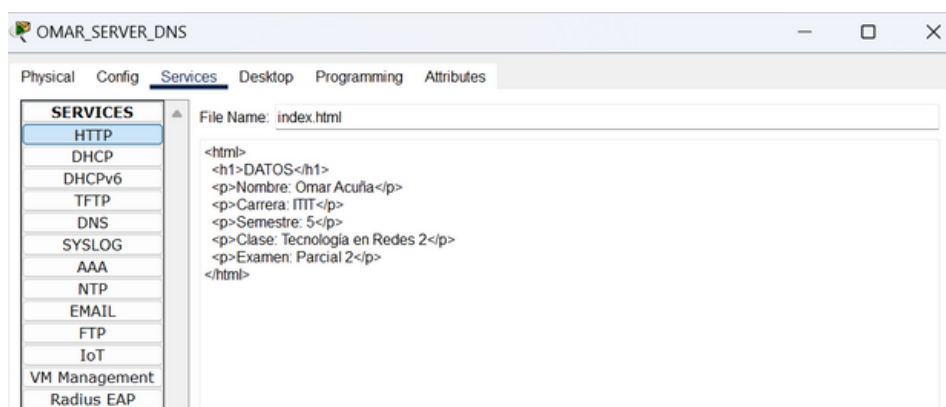
Comenzaremos con la configuración del DNS WEB SERVER.



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.

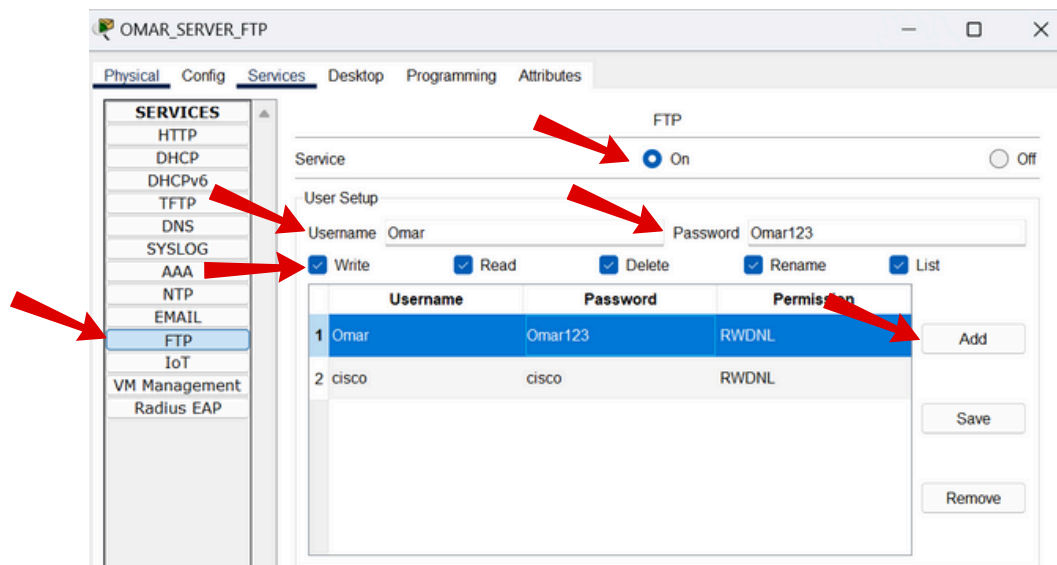


CONFIGURACIÓN

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

Habr  una lista de archivos accesibles a trav s de FTP.

CONFIGURACIÓN

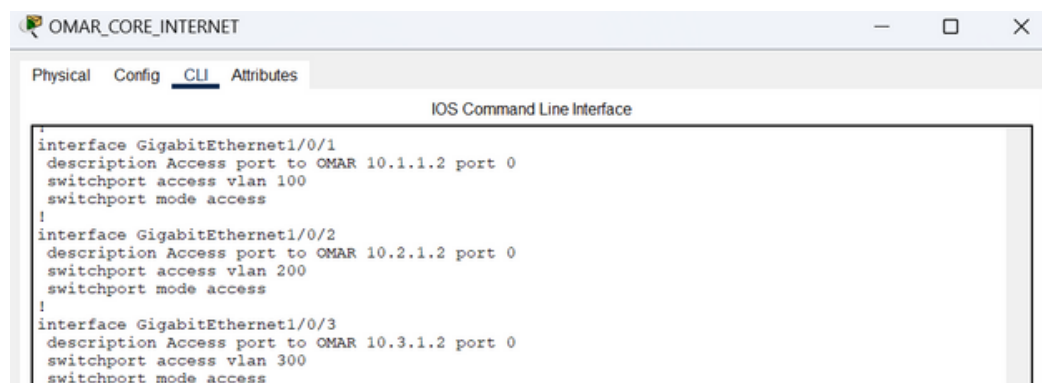
COMANDOS DE CADA DISPOSITIVO PARA CONECTAR LA RED

ACCESS PORTS DE TODOS LOS SWITCHES

```
INTERNET
>ENABLE
>CONF T
>INT Gi1/0/1
>DESCRIPTION
>SWITCHPORT MODE ACCESS
>SWITCHPORT ACCESS VLAN 100
>NO SHUT
```

```
INTERNET
>ENABLE
>CONF T
>INT Gi1/0/2
>DESCRIPTION
>SWITCHPORT MODE ACCESS
>SWITCHPORT ACCESS VLAN 200
>NO SHUT
```

```
INTERNET
>ENABLE
>CONF T
>INT Gi1/0/3
>DESCRIPTION
>SWITCHPORT MODE ACCESS
>SWITCHPORT ACCESS VLAN 300
>NO SHUT
```



- 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

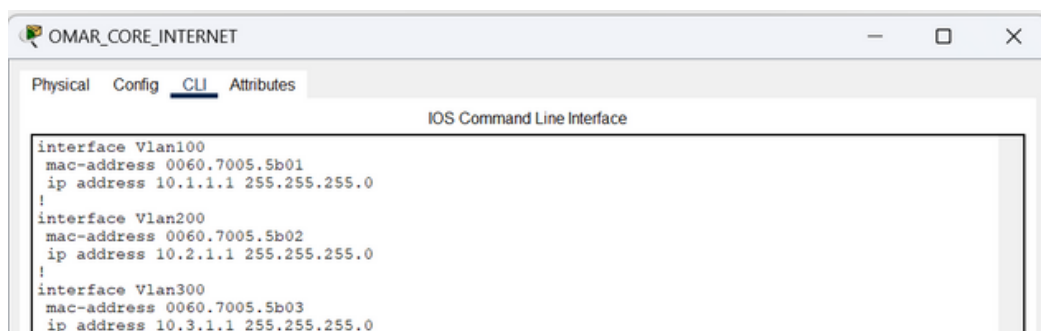
COMANDOS DE CADA DISPOSITIVO PARA CONECTAR LA RED

ACCESS PORTS DE TODOS LOS SWITCHES

```
INTERNET
>ENABLE
>CONF T
>IP ROUTING
>INTERFACE VLAN 100
>NO SHUT
>IP ADDRESS 10.1.1.1 255.255.255.0
```

```
INTERNET
>ENABLE
>CONF T
>IP ROUTING
>INTERFACE VLAN 200
>NO SHUT
>IP ADDRESS 10.2.1.1 255.255.255.0
```

```
INTERNET
>ENABLE
>CONF T
>IP ROUTING
>INTERFACE VLAN 300
>NO SHUT
>IP ADDRESS 10.3.1.1 255.255.255.0
```



- 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

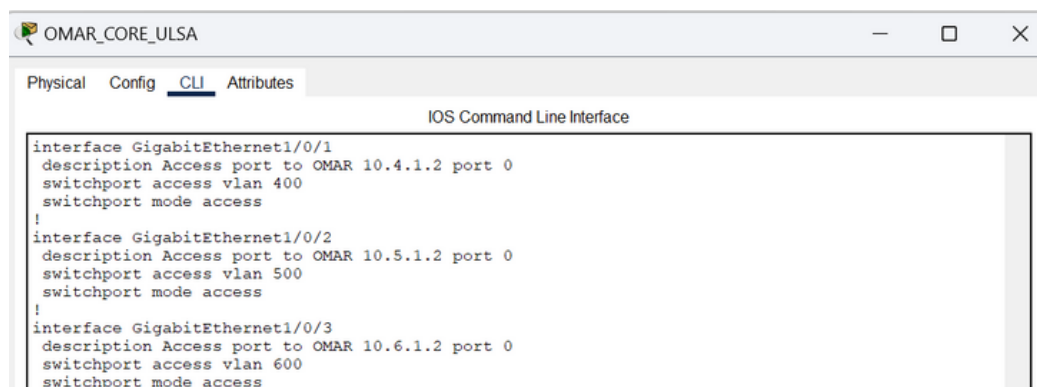
COMANDOS DE CADA DISPOSITIVO PARA CONECTAR LA RED

ACCESS PORTS DE TODOS LOS SWITCHES

```
ULSA
>ENABLE
>CONF T
>INT Gi1/0/1
>DESCRIPTION
>SWITCHPORT MODE ACCESS
>SWITCHPORT ACCESS VLAN 400
>NO SHUT
```

```
ULSA
>ENABLE
>CONF T
>INT Gi1/0/2
>DESCRIPTION
>SWITCHPORT MODE ACCESS
>SWITCHPORT ACCESS VLAN 500
>NO SHUT
```

```
ULSA
>ENABLE
>CONF T
>INT Gi1/0/3
>DESCRIPTION
>SWITCHPORT MODE ACCESS
>SWITCHPORT ACCESS VLAN 600
>NO SHUT
```



- 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

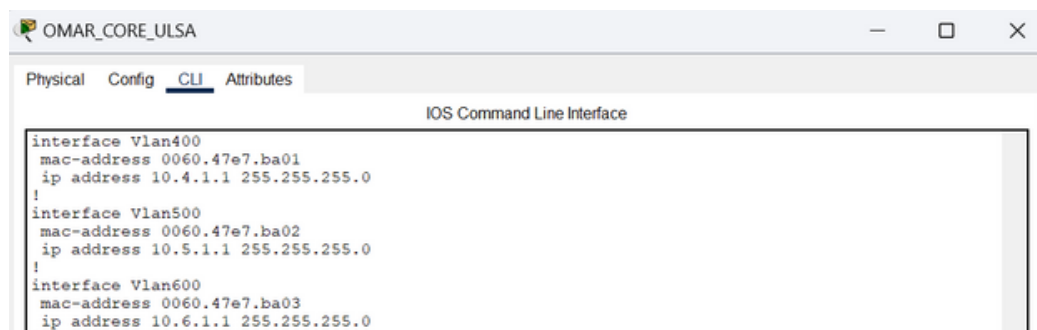
COMANDOS DE CADA DISPOSITIVO PARA CONECTAR LA RED

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
```

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

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



- 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

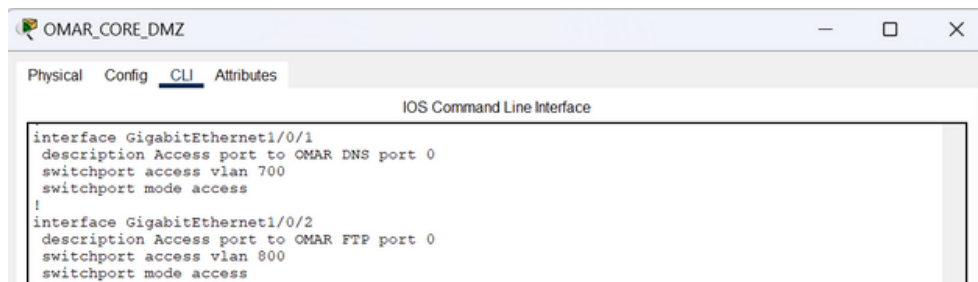
CONFIGURACIÓN

COMANDOS DE CADA DISPOSITIVO PARA CONECTAR LA RED

ACCESS PORTS DE TODOS LOS SWITCHES

```
DMZ
>ENABLE
>CONF T
>INT Gi1/0/1
>DESCRIPTION
>SWITCHPORT MODE ACCESS
>SWITCHPORT ACCESS VLAN 700
>NO SHUT
```

```
DMZ
>ENABLE
>CONF T
>INT Gi1/0/2
>DESCRIPTION
>SWITCHPORT MODE ACCESS
>SWITCHPORT ACCESS VLAN 800
>NO SHUT
```



- 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

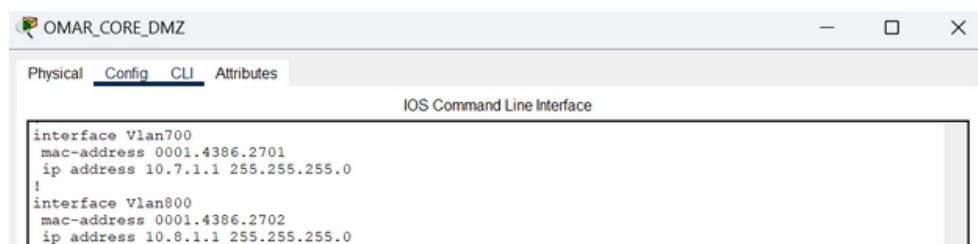
ACCESS PORTS DE TODOS LOS SWITCHES

DMZ

```
>ENABLE
>CONF T
>IP ROUTING
>INTERFACE VLAN 700
>NO SHUT
>IP ADDRESS 10.7.1.1 255.255.255.0
```

DMZ

```
>ENABLE
>CONF T
>IP ROUTING
>INTERFACE VLAN 800
>NO SHUT
>IP ADDRESS 10.8.1.1 255.255.255.0
```



- 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
```



- 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
```



- 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
```



- 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
```



- 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

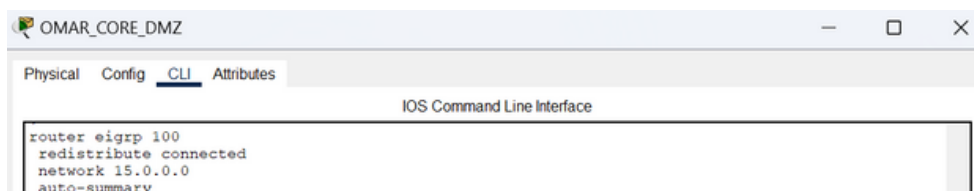
EIGRP PORTS DE TODOS LOS SWITCHES

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



- 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
```



- 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
```



- 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
```



- 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
```



- 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
```



- 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
```



- 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
```



- 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
>NWTWORK 14.14.14.14
>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

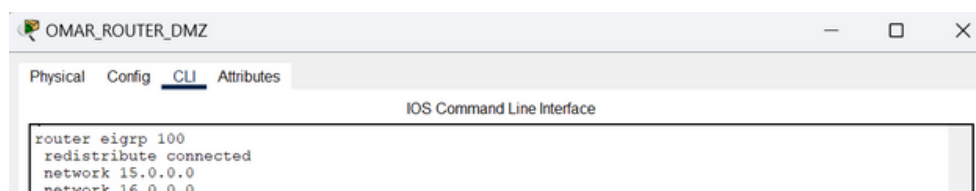
EIGRP PORTS DE TODOS LOS ROUTERS

```
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
>NWTWORK 16.16.16.16
>REDISTRIBUTE CONNECTED
```



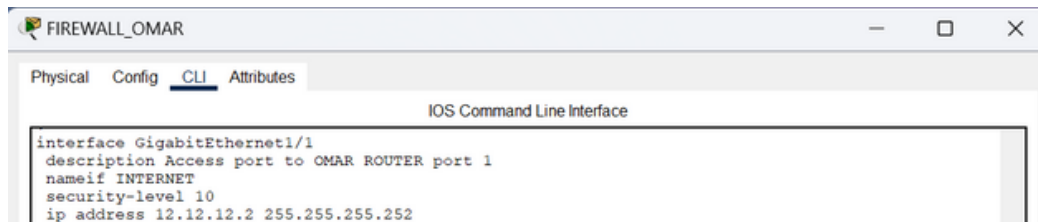
- 1.enable: Entra en modo privilegiado.
- 2.conf t: Entra en el modo de configuración global.
- 3.router eigrp 100: Activa el protocolo de enrutamiento EIGRP en el Autonomous System 100.
- 4.network: Incluye la red en el proceso de EIGRP para que sea anunciada.
- 5.redistribute connected: Redistribuye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



- 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
```



- 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

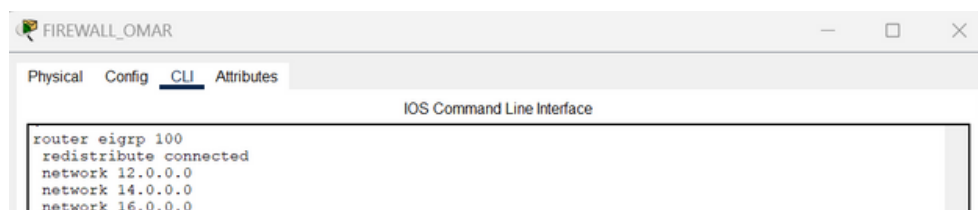
EIGRP PORTS DEL FIREWALL

```
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
```



- 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
```



- 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 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 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 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 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 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 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.
- 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.
- 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.
- Bloquea todo el tráfico no autorizado.

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

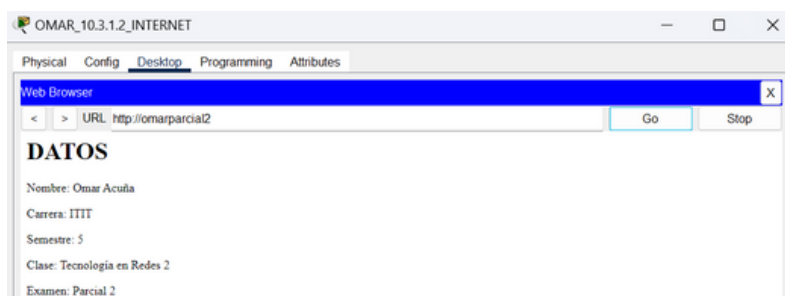
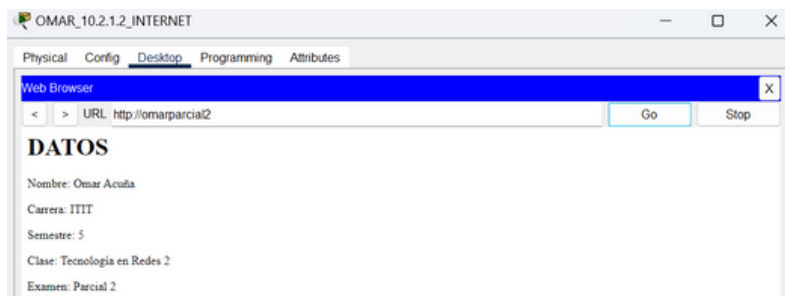
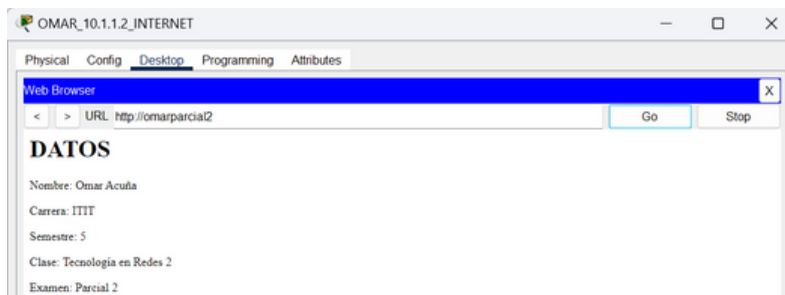
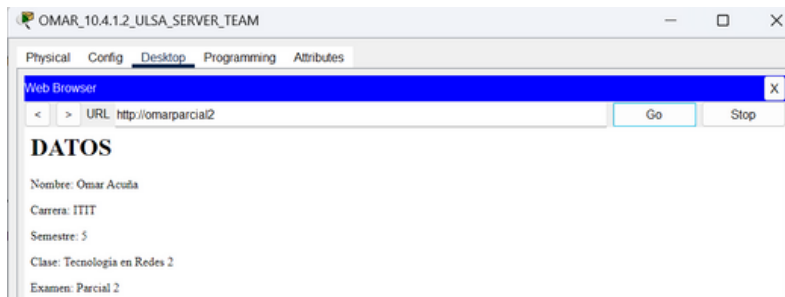
- ULSA a la interfaz ULSA.
- DMZ a la interfaz DMZ.
- INTERNET a la interfaz INTERNET.

RESULTADOS

COMPROBACIÓN DE LA CORRECTA FUNCIÓN DE LA PRÁCTICA

DNS WEB SERVER

PC'S ALCANZANDO AL DNS WEB SERVER

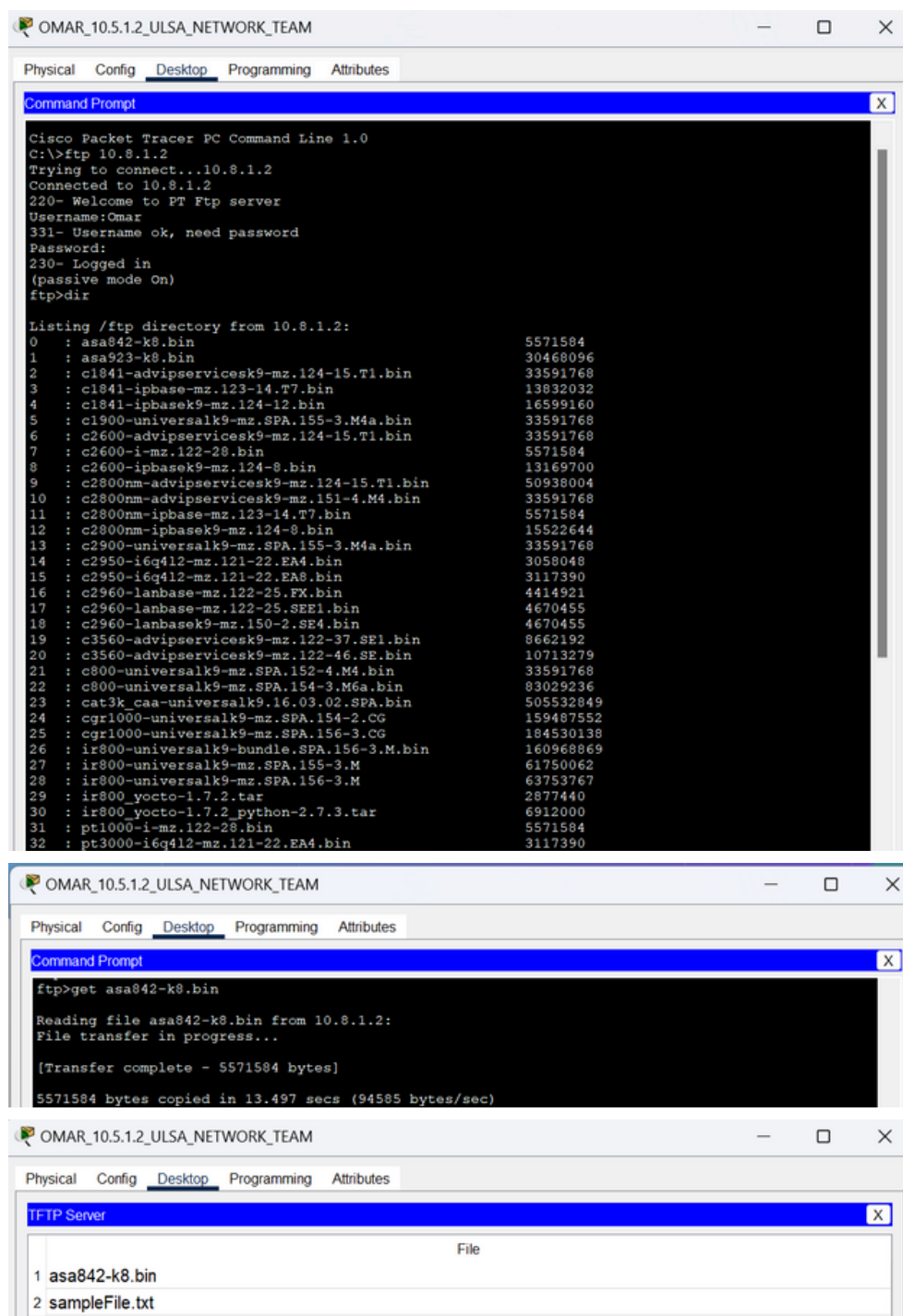


RESULTADOS

COMPROBACIÓN DE LA CORRECTA FUNCIÓN DE LA PRÁCTICA

FTP SERVER

PC ALCANZANDO AL FTP SERVER Y DESCARGANDO ARCHIVO

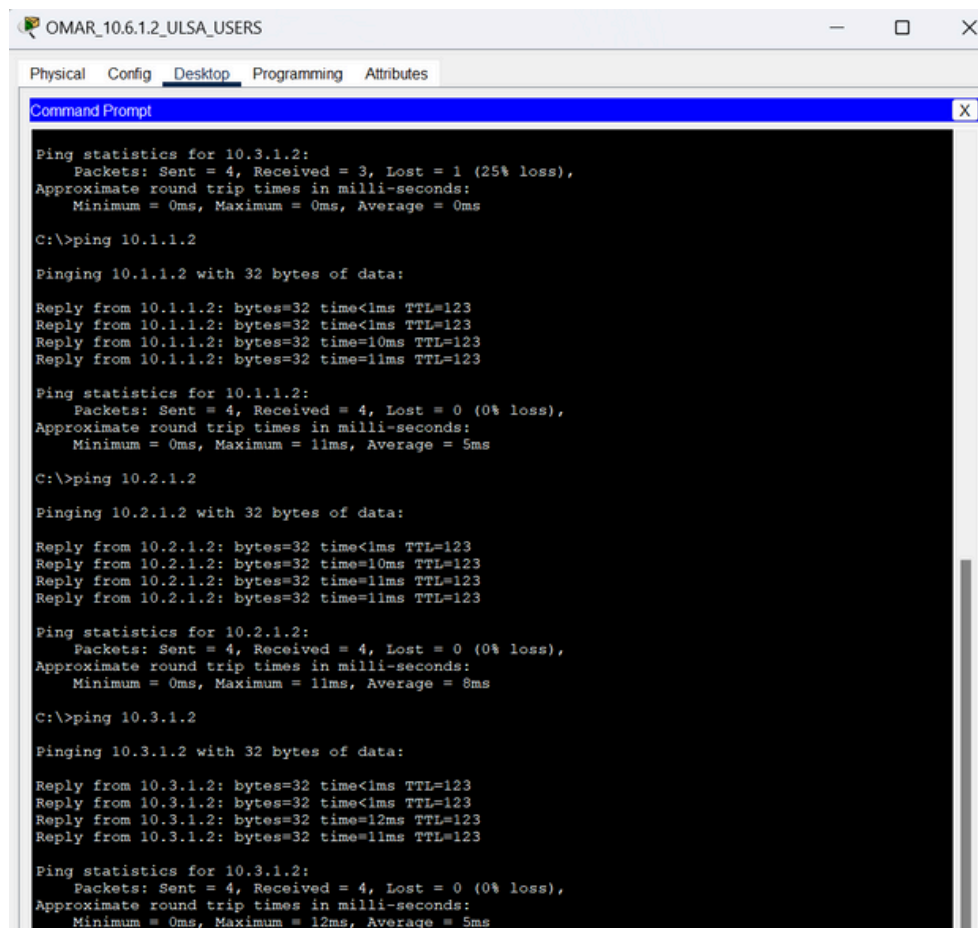


RESULTADOS

COMPROBACIÓN DE LA CORRECTA FUNCIÓN DE LA PRÁCTICA

ULSA USERS

PC USERS ALCANZANDO A GOOGLE Y VICEVERSA.



```
OMAR_10.6.1.2_ULSA_USERS
Physical Config Desktop Programming Attributes
Command Prompt
Ping statistics for 10.3.1.2:
  Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.1.1.2

Pinging 10.1.1.2 with 32 bytes of data:

Reply from 10.1.1.2: bytes=32 time<1ms TTL=123
Reply from 10.1.1.2: bytes=32 time<1ms TTL=123
Reply from 10.1.1.2: bytes=32 time=10ms TTL=123
Reply from 10.1.1.2: bytes=32 time=11ms TTL=123

Ping statistics for 10.1.1.2:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 5ms

C:\>ping 10.2.1.2

Pinging 10.2.1.2 with 32 bytes of data:

Reply from 10.2.1.2: bytes=32 time<1ms TTL=123
Reply from 10.2.1.2: bytes=32 time=10ms TTL=123
Reply from 10.2.1.2: bytes=32 time=11ms TTL=123
Reply from 10.2.1.2: bytes=32 time=11ms TTL=123

Ping statistics for 10.2.1.2:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 8ms

C:\>ping 10.3.1.2

Pinging 10.3.1.2 with 32 bytes of data:

Reply from 10.3.1.2: bytes=32 time<1ms TTL=123
Reply from 10.3.1.2: bytes=32 time<1ms TTL=123
Reply from 10.3.1.2: bytes=32 time=12ms TTL=123
Reply from 10.3.1.2: bytes=32 time=11ms TTL=123

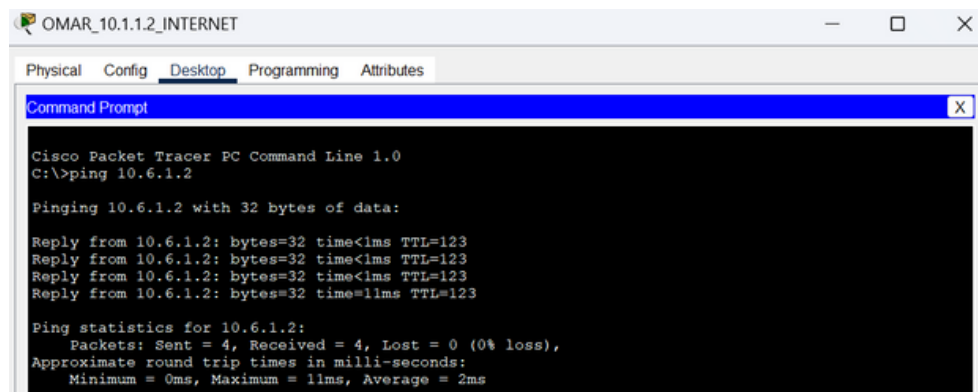
Ping statistics for 10.3.1.2:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 12ms, Average = 5ms
```

RESULTADOS

COMPROBACIÓN DE LA CORRECTA FUNCIÓN DE LA PRÁCTICA

ULSA USERS

PC USERS ALCANZANDO A GOOGLE Y VICEVERSA.

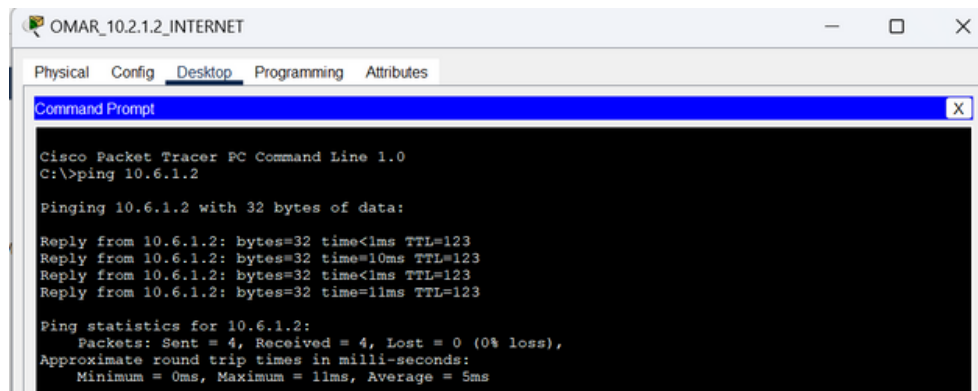


```
OMAR_10.1.1.2_INTERNET
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.6.1.2

Pinging 10.6.1.2 with 32 bytes of data:

Reply from 10.6.1.2: bytes=32 time<1ms TTL=123
Reply from 10.6.1.2: bytes=32 time<1ms TTL=123
Reply from 10.6.1.2: bytes=32 time<1ms TTL=123
Reply from 10.6.1.2: bytes=32 time=11ms TTL=123

Ping statistics for 10.6.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 2ms
```

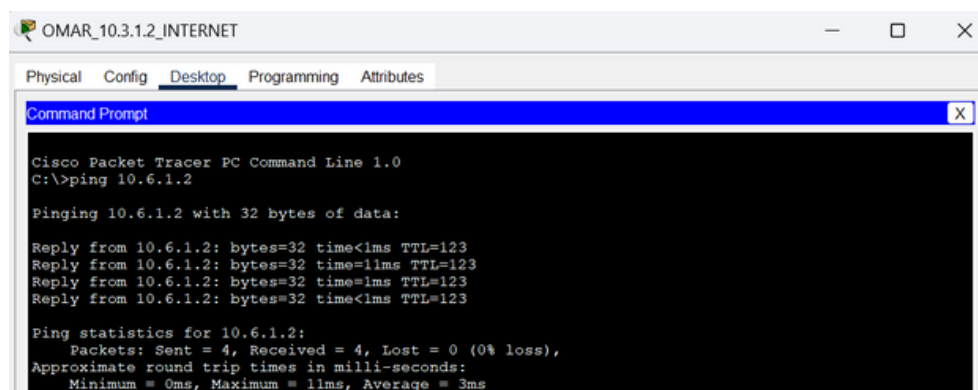


```
OMAR_10.2.1.2_INTERNET
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.6.1.2

Pinging 10.6.1.2 with 32 bytes of data:

Reply from 10.6.1.2: bytes=32 time<1ms TTL=123
Reply from 10.6.1.2: bytes=32 time=10ms TTL=123
Reply from 10.6.1.2: bytes=32 time<1ms TTL=123
Reply from 10.6.1.2: bytes=32 time=11ms TTL=123

Ping statistics for 10.6.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 5ms
```



```
OMAR_10.3.1.2_INTERNET
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.6.1.2

Pinging 10.6.1.2 with 32 bytes of data:

Reply from 10.6.1.2: bytes=32 time<1ms TTL=123
Reply from 10.6.1.2: bytes=32 time=11ms TTL=123
Reply from 10.6.1.2: bytes=32 time=1ms TTL=123
Reply from 10.6.1.2: bytes=32 time<1ms TTL=123

Ping statistics for 10.6.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 3ms
```

CONCLUSIÓN



LA TOPOLOGÍA PRESENTADA DEMUESTRA UNA ESTRUCTURA DE RED BIEN ORGANIZADA QUE ASEGURA LA INTERCONEXIÓN EFICIENTE DE DISTINTAS REDES, COMO INTERNET, ULSA Y DMZ, MANTENIENDO AL MISMO TIEMPO UN ALTO NIVEL DE SEGURIDAD. AL CONECTAR PCS Y SERVIDORES A SUS RESPECTIVOS CORES Y ROUTERS, Y CENTRALIZAR LA SEGURIDAD MEDIANTE UN FIREWALL, SE LOGRA UN CONTROL EFECTIVO DEL TRÁFICO ENTRE LAS SUBREDES.

LA DISPOSICIÓN DE LOS ROUTERS Y EL FIREWALL GARANTIZA NO SOLO LA COMUNICACIÓN FLUIDA ENTRE LAS REDES INTERNAS Y EXTERNAS, SINO TAMBIÉN LA PROTECCIÓN ADECUADA FRENTE A AMENAZAS EXTERNAS. ESTA INTEGRACIÓN DE MÚLTIPLES REDES A TRAVÉS DE ENLACES WAN REFUERZA LA CAPACIDAD DE LA TOPOLOGÍA PARA MANEJAR COMUNICACIONES COMPLEJAS DE MANERA CONFIABLE.

EN CONCLUSIÓN, LA RED DISEÑADA NO SOLO FACILITA LA CONECTIVIDAD ENTRE DIFERENTES DOMINIOS, SINO QUE TAMBIÉN IMPLEMENTA MEDIDAS DE SEGURIDAD ESENCIALES PARA PROTEGER LOS RECURSOS CRÍTICOS. LA INCLUSIÓN DE LA DMZ Y EL USO DE UN FIREWALL CENTRALIZADO DEMUESTRAN UN ENFOQUE SÓLIDO HACIA LA PROTECCIÓN Y GESTIÓN DEL TRÁFICO DE RED, CUMPLIENDO CON LOS REQUISITOS DE INTERCONEXIÓN Y SEGURIDAD DE UNA INFRAESTRUCTURA MODERNA.