MANUAL
PACKET TRACER

Ian Alejandro Corral Marín
12130

TECNOLOGÍA DE REDES

INDÌCE

Introducción a Cisco Packet Tracer

Cisco Packet Tracer es una herramienta de simulación de redes desarrollada por Cisco Systems. Está diseñada para ayudar a los estudiantes y profesionales a aprender y practicar la configuración de redes en un entorno virtual antes de implementarlas en el mundo real. A continuación, se presentan los puntos clave sobre Cisco Packet Tracer:

¿Qué es Cisco Packet Tracer?

Simulador de Redes: Packet Tracer permite a los usuarios crear y probar redes complejas sin necesidad de hardware físico. Puedes simular el comportamiento de dispositivos de red como routers, switches, PCs, servidores, y otros equipos de red.

INTRODUCCIÓN

MANUAL PACKET TRACER

En este manual se describe la configuración de una topología de red diseñada en Cisco Packet Tracer para interconectar las redes de ULSA, DMZ y Google. La topología está pensada para asegurar una comunicación eficiente y controlada entre estos segmentos de red mediante el uso de VLANs, enrutamiento EIGRP y la implementación de un firewall que gestiona las políticas de seguridad.

Cada segmento tiene una función clave dentro de la red. ULSA y Google están estructurados con VLANs que segmentan los dispositivos, mientras que DMZ actúa como una zona de acceso para servicios como FTP y DNS. La configuración incluye listas de control de acceso (ACLs) que permiten o deniegan el tráfico basado en los protocolos utilizados, como HTTP, FTP, y DNS, garantizando que cada red solo acceda a los servicios autorizados.

El enrutamiento EIGRP se encarga de la propagación de rutas entre las diferentes redes, mientras que las ACLs y el firewall aseguran que solo el tráfico permitido fluya entre las VLANs y los diferentes sitios. El uso de ICMP (ping) permite verificar la conectividad entre los dispositivos, y las pruebas de conectividad aseguran que la red funcione de manera eficiente y segura, sin comprometer las restricciones de acceso establecidas.

Este manual proporcionará una guía detallada de la configuración de cada dispositivo, desde los switches hasta los routers, servers y el firewall, permitiendo una implementación segura y confiable de la comunicación entre ULSA, DMZ y Google.

OBJETIVO

El objetivo de este manual es guiar la configuración de una red que conecte de manera segura las redes de Google, ULSA y la DMZ. Para ello, se implementarán las siguientes características clave:

- Google: Switch CORE con tres VLANs (100, 200 y 300), con gateways y conexiones hacia el router y firewall.
- ULSA: Switch CORE con tres VLANs (400, 500 y 600), con gateways y conexiones similares hacia su router y firewall.
- DMZ: VLAN 700 para el servidor DNS y VLAN 800 para el servidor FTP, accesibles bajo control de seguridad.

El enrutamiento entre los sitios se realizará con EIGRP 100, y las ACLs permitirán el acceso a servicios como HTTP, DNS, FTP, y ICMP de forma controlada, limitando el tráfico entre las VLANs según las políticas de seguridad establecidas.

CONCEPTOS CLAVE

·**Red:** Una red es un grupo de computadoras y dispositivos conectados entre sí que pueden comunicarse e intercambiar información.

•**Router:** Un router es un dispositivo que conecta diferentes redes y dirige el tráfico de datos entre ellas.

•**Switch:** Un switch es un dispositivo que conecta múltiples dispositivos en la misma red y envía datos solo a los dispositivos que los necesitan. Es como un conmutador que conecta llamadas telefónicas.

•**VLAN (Virtual LAN):** Una VLAN es una red virtual dentro de un switch que agrupa dispositivos como si estuvieran en la misma red física, aunque no lo estén. Ayuda a organizar y segmentar la red para mejorar la seguridad y la eficiencia.

•**IP Address (Dirección IP):** Una dirección IP es un identificador único para un dispositivo en una red, similar a una dirección postal para una casa.

•**Subnet Mask:** La máscara de subred se utiliza junto con la dirección IP para definir la red y los hosts (dispositivos) dentro de esa red. Es como un filtro que ayuda a identificar qué parte de la dirección IP corresponde a la red y cuál a los dispositivos.

•**EIGRP (Enhanced Interior Gateway Routing Protocol):** EIGRP es un protocolo de enrutamiento que ayuda a los routers a compartir información sobre las redes a las que están conectados, para que puedan encontrar la mejor ruta para enviar datos.

•**Firewall:** Sistema que controla el acceso a una red para protegerla contra amenazas.

•**LAN (Local Area Network):** Una LAN es una red que conecta dispositivos en un área pequeña, como una casa, oficina o edificio.
•**Interfaz:** Una interfaz es una conexión física o lógica a través de la cual los dispositivos de red pueden enviar y recibir datos.
•**Modo de Acceso:** En el contexto de un switch, el modo de acceso significa que la interfaz está configurada para conectarse a un solo dispositivo o red, y pertenece a una VLAN específica.
•**Redistribución de Rutas:** La redistribución de rutas es el proceso de compartir rutas de una fuente de enrutamiento (como EIGRP) con otra, para que las rutas se puedan usar en diferentes partes de la red.
•**DMZ (Zona Desmilitarizada):** Es una red perimetral que separa las redes internas de una empresa de las redes externas (como Internet), permitiendo que ciertos servicios (como DNS y FTP) sean accesibles desde fuera, mientras mantiene segura la red interna.
•**DNS (Domain Name System):** El sistema DNS traduce nombres de dominio (como www.ejemplo.com) a direcciones IP, lo que facilita la navegación en internet.
•**FTP (File Transfer Protocol):** Un protocolo que permite la transferencia de archivos entre un cliente y un servidor en una red. Se utiliza en el servidor FTP ubicado en la VLAN 800 en esta topología.
•**ICMP (Internet Control Message Protocol):** Protocolo utilizado para enviar mensajes de control y de error en la red, como el famoso comando "ping" para probar la conectividad entre dispositivos.
•**Lista de Control de Acceso (ACL):** Conjunto de reglas aplicadas en un firewall o router para permitir o bloquear tráfico específico según direcciones IP, protocolos, o puertos. En esta topología, las ACL se utilizan para controlar el acceso entre las VLANs de Google, ULSA y la DMZ.

GLOSARIO

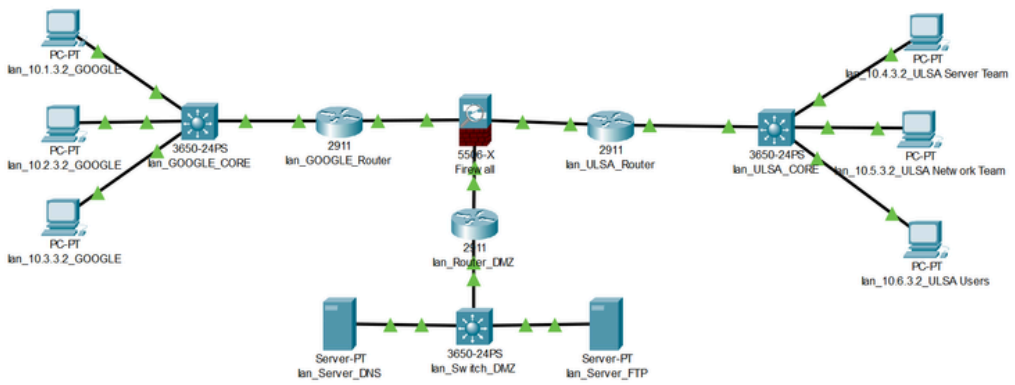
-enable: Entra en modo administrador del dispositivo.
-configure terminal: Entra en modo de configuración global.
-show running-config: Muestra la configuración actual del dispositivo Cisco.
-**interface vlan [VLAN_ID]:** Configura la interfaz VLAN para routing.
-no switchport: Cambia una interfaz de capa 2 (switching) a capa 3 (routing).
-ip address [IP_ADDRESS] [SUBNET_MASK]: Asigna una dirección IP a una interfaz.
-no shutdown: Activa la interfaz.
-switchport mode access: Configura una interfaz como puerto de acceso.
-switchport access vlan [VLAN_ID]: Asigna una interfaz a una VLAN específica.
-router eigrp [AS_NUMBER]: Inicia el proceso de EIGRP con el número de sistema autónomo especificado.
-network [NETWORK_ADDRESS] [WILDCARD_MASK]: Especifica qué redes EIGRP debe anunciar.
-redistribute connected: Permite redistribuir redes conectadas directamente en el proceso EIGRP.
- redistribute static: Permite redistribuir rutas estáticas en el proceso EIGRP.
- ip route [DESTINATION] [MASK] [NEXT_HOP]: Crea una ruta estática.
-access-list [NAME] extended permit tcp host [IP1] host [IP2] eq telnet: Permite tráfico Telnet desde [IP1] hacia [IP2] en una lista de acceso.
-access-list [NAME] extended deny ip any any: Niega cualquier otro tráfico no especificado en la lista de acceso.
-access-group [NAME] in interface [INTERFACE]: Aplica la lista de acceso a una interfaz en la dirección de entrada.

COMANDOS

INSTRUCCIONES

1. PC conectada a Switch en un puerto de acceso dentro de la VLAN correspondiente:
   - VLAN 100, 200, 300 para Google
   - VLAN 400, 500, 600 para ULSA
   - VLAN 700 y 800 para ULSA DMZ
2. Switch CORE conectado al Router por puertos de acceso dentro de las VLANs correspondientes.
3. Router con IP Gateway configurada para cada VLAN en una interfaz directa:
4. Conexión entre routers y firewall usando las IPs WAN asignadas:
   - Google Router a Firewall: 11.11.11.0/30 y 12.12.12.0/30.
   - ULSA Router a Firewall: 14.14.14.0/30 y 13.13.13.0/30.
   - ULSA DMZ Router a Firewall WAN2: 16.16.16.0/30.
   - Switch CORE a Router WAN1: 15.15.15.0/30.

5. Configurar el firewall para permitir o denegar el tráfico entre las VLANs según las reglas indicadas:
   - Configuración de zonas inside (ULSA), outside (Google), y DMZ (ULSA DMZ).
6. Implementar EIGRP 100 para redistribuir rutas entre los routers de Google y ULSA.
7. Verificar conectividad entre Google y ULSA, probando las reglas de acceso y el enrutamiento EIGRP.



CONFIGURACIÓN

- Conexión de PCs a Switches
  - PC1 (Google 10.1.1.2) se conecta al Switch1 (GOOGLE_CORE) desde la interfaz FastEthernet 0 de la PC a la interfaz GigabitEthernet 1/0/1 del switch.
  - PC2 (Google 10.2.1.2) se conecta al Switch1 (GOOGLE_CORE) desde la interfaz FastEthernet 0 de la PC a la interfaz GigabitEthernet 1/0/2 del switch.
  - PC3 (Google 10.3.1.2) se conecta al Switch1 (GOOGLE_CORE) desde la interfaz FastEthernet 0 de la PC a la interfaz GigabitEthernet 1/0/3 del switch.
  - PC4 (ULSA Server team 10.4.1.2) se conecta al Switch2 (ULSA_CORE) desde la interfaz FastEthernet 0 de la PC a la interfaz GigabitEthernet 1/0/1 del switch.
  - PC5 (ULSA Network Team 10.5.1.2) se conecta al Switch2 (ULSA_CORE) desde la interfaz FastEthernet 0 de la PC a la interfaz GigabitEthernet 1/0/2 del switch.
  - PC6 (ULSA Users 10.6.1.2) se conecta al Switch2 (ULSA_CORE) desde la interfaz FastEthernet 0 de la PC a la interfaz GigabitEthernet 1/0/3 del switch.

- Conexión de Switches a Routers
  - Switch1 (GOOGLE_CORE) se conecta al Router1 (Google) desde la interfaz GigabitEthernet 1/0/24 del switch a la interfaz GigabitEthernet 0/0 del router.
  - Switch2 (ULSA_CORE) se conecta al Router2 (ULSA) desde la interfaz GigabitEthernet 1/0/24 del switch a la interfaz GigabitEthernet 0/0 del router.

- Conexión entre Routers y Firewall
  - Router1 (Google) se conecta al ASA 5506-X Firewall desde la interfaz GigabitEthernet 0/1 del router a la interfaz GigabitEthernet 1/1 del firewall.
  - ASA 5506-X Firewall se conecta al Router2 (ULSA) desde la interfaz GigabitEthernet 1/2 del firewall a la interfaz GigabitEthernet 0/1 del router.

- Conexión de la DMZ
  - Server DNS se conecta al Switch DMZ desde la interfaz FastEthernet 0 del server a la interfaz GigabitEthernet 1/0/1 del switch.
  - Server FTP se conecta al Switch DMZ desde la interfaz FastEthernet 0 del server a la interfaz GigabitEthernet 1/0/2 del switch.
  - Switch DMZ se conecta al Router DMZ desde la interfaz GigabitEthernet 1/0/24 del switch a la interfaz GigabitEthernet 0/0 del router.
  - Router DMZ se conecta al ASA 5506-X Firewall desde la interfaz GigabitEthernet 0/1 del router a la interfaz GigabitEthernet 1/3 del firewall.

CONFIGURACIÓN

Reglas de Firewall para el flujo de trafico:

1.ULSA Server Team (10.4.x.x) solo debe alcanzar el DNS-WEB Server pero NO alcanzar el FTP Server

2.El DNS-WEB Server solo debe responder al Server Team

3.ULSA Network Team (10.5.x.x) solo debe alcanzar el FTP Server pero NO alcanzar el DNS-WEB Server

4.El FTP Server solo debe responder al Network Team

5.ULSA Users (10.6.x.x) solo debe salir a Google y NO deben alcanzar los Servers

6.Google LANs deben alcanzar ULSA Users y DNS-WEB Server pero NO el FTP Server

7.Todo lo no especificado debe ser bloqueado con un deny ip any any al final de cada lista de acceso

CONFIGURACIÓN

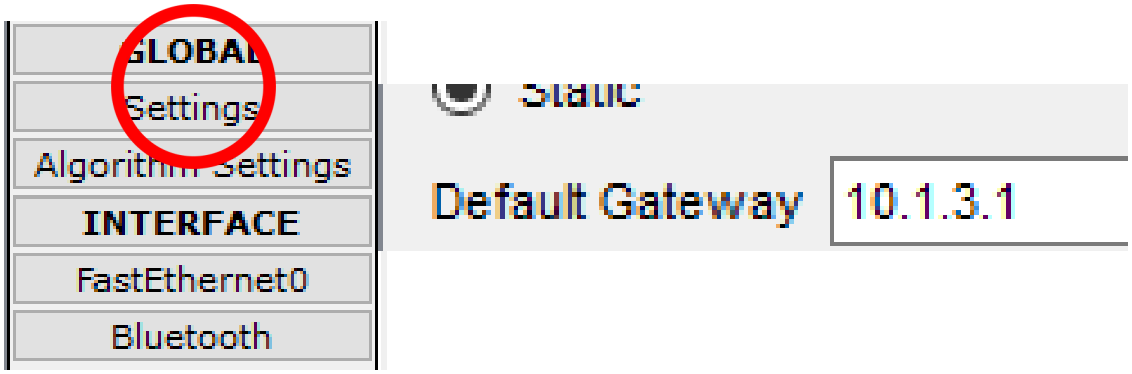
REDES

A continuación se explicara paso a paso la configuración y comandos que se deben realizar para el funcionamiento correcto de las redes en cada compañía (el tercer octeto sera siempre el número 3, ya que este fue proporcionado por el profesor):

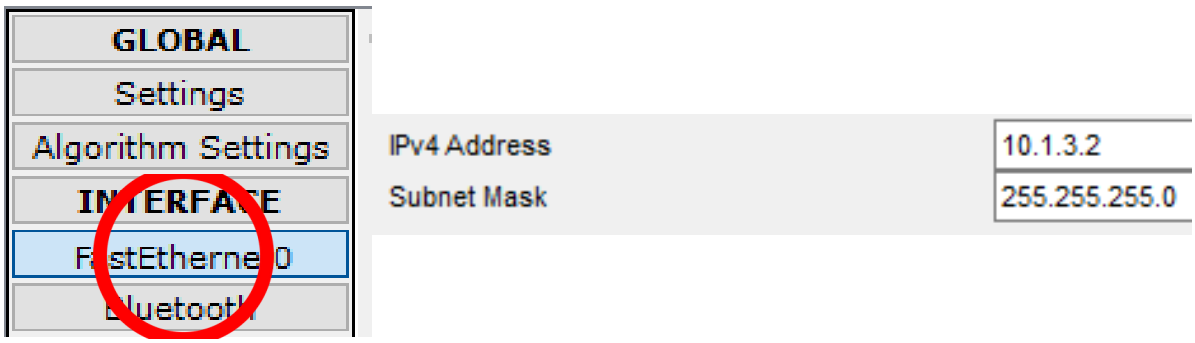
1. **Configuración de PCS y Servers:** Comenzaremos configurando cada Default Gateway, IP y Subnet Mask de las PC. Cada PC tiene un apartado de opciones, nos dirigiremos a la de **config** y cada imagen mostrara hacia donde ir.

En las **instrucciones de Topología** tenemos cada una de las configuraciones, el "default gateway" es un dispositivo de red, normalmente un router, que sirve como un punto de acceso o nodo de red que actúa como una ruta de paso para los dispositivos de una red local cuando necesitan comunicarse con dispositivos en otra red, típicamente fuera de su red local (LAN).

Como ejemplo tenemos la primer PC de Google que tiene una ruta 10.1.3.0/24 , por lo que usaremos **10.1.3.1 (el número que sigue despues del 10 depende de cada vlan, es decir en la siguiente PC sería 10.2.3.1 pues su vlan es 200, y así sucesivamente)**:

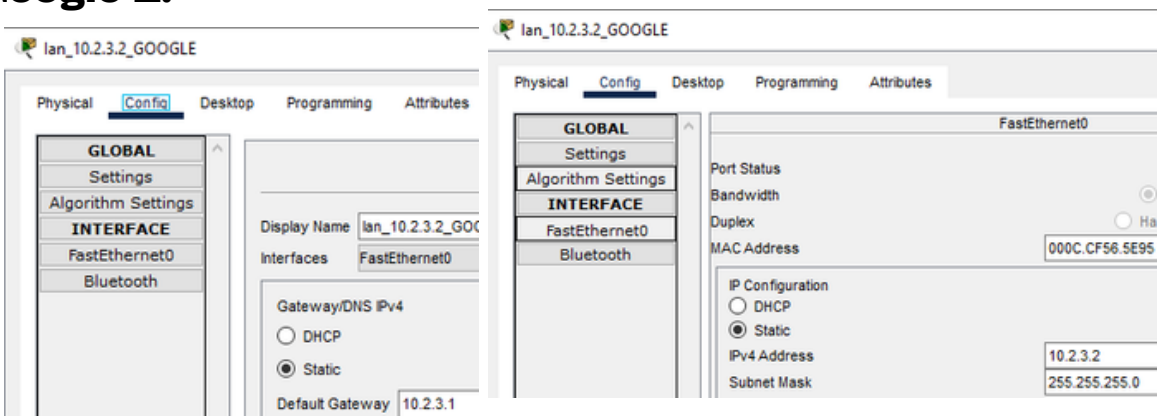


Ahora nos dirigiremos al apartado de FastEthernet en donde configuraremos la ip y la subnet mask, en las instrucciones se nos muestra que todas las subnets masks son /24 por lo que siempre será **255.255.255.0,** mientras que en la ip, la primer usable seria **10.1.3.2** :

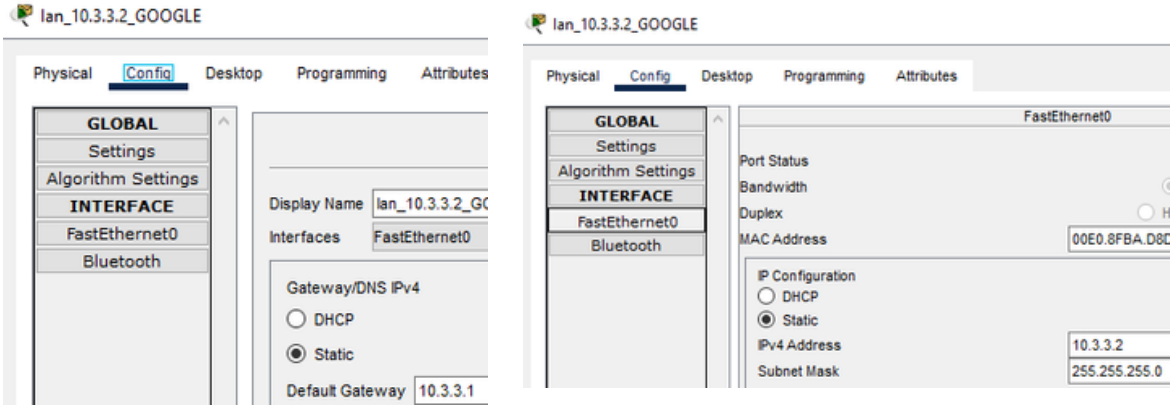


Repetiremos este proceso en cada PC:

Google 2:

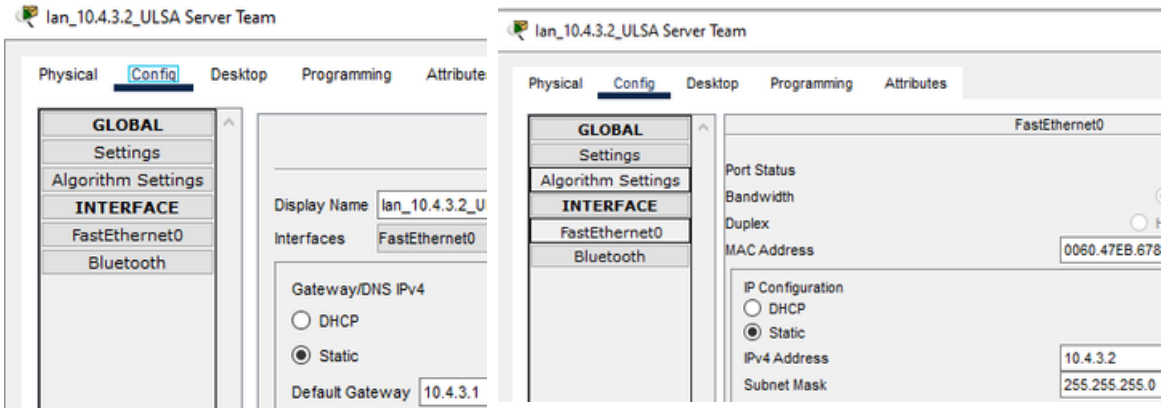


Google 3:

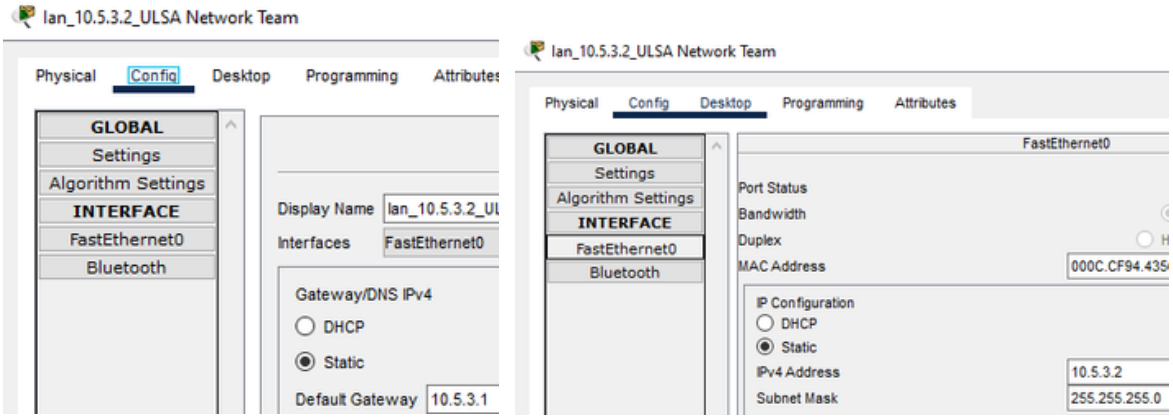


Ahora del lado derecho de ULSA:

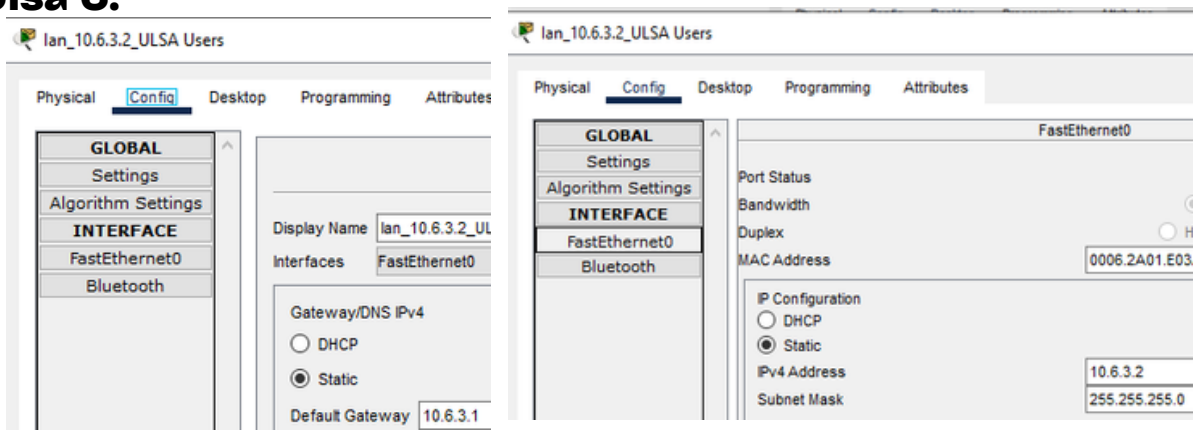
Ulsa 4:



Ulsa 5:

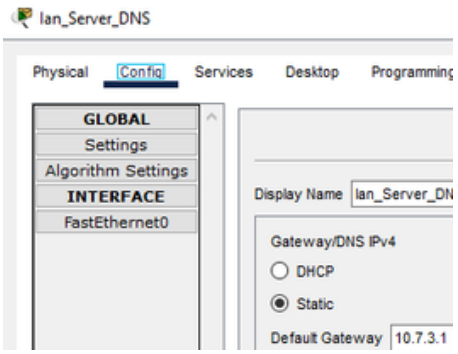


Ulsa 6:

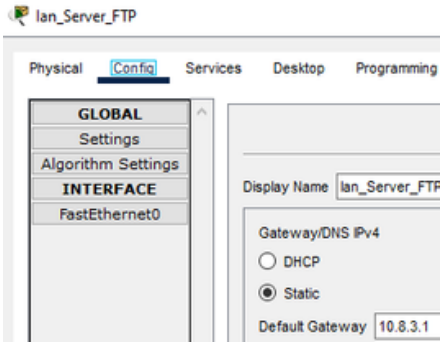


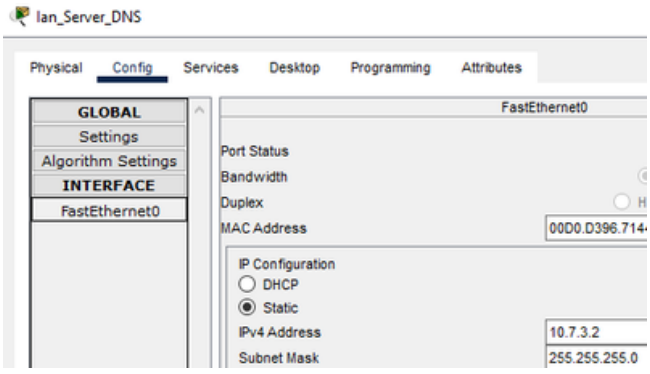
Ahora del lado derecho de ULSA DMZ:

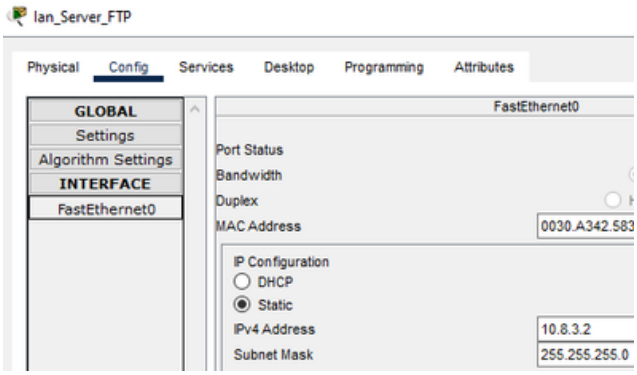
Server DNS:



Server FTP:







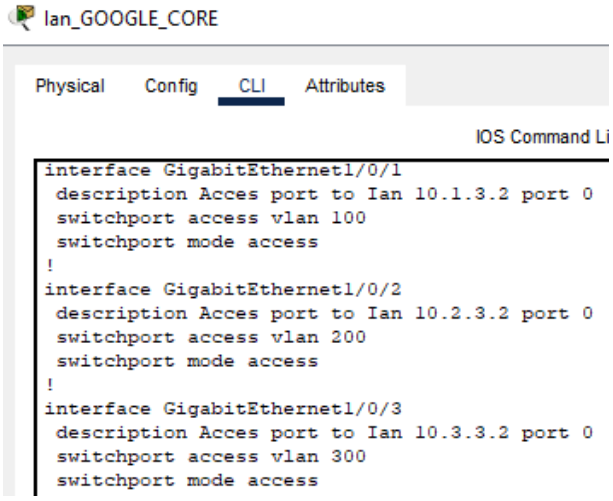
2. Configuración de Access Ports de todos lo Switches:

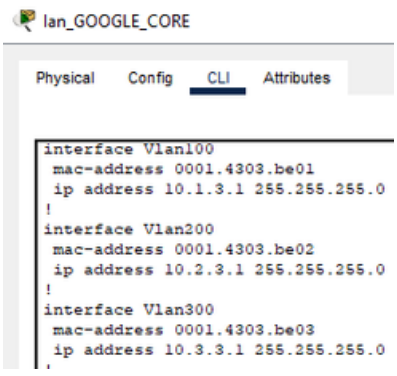
Entramos al apartado CLI de los switches para introducir cada comando.

Switch Google:

```
>enable
>conf t
>int Gi1/0/1
>description
>switchport mode Access
>Switchport access vlan 100

>int vlan 100
>ip address 10.1.3.1 255.255.255.0
>no shut

>enable
>conf t
>int Gi1/0/2
>description
>switchport mode Access
>Switchport access vlan 200

>int vlan 200
>ip address 10.2.3.1 255.255.255.0
>no shut

>enable
>conf t
>int Gi1/0/3
>description
>switchport mode Access
>Switchport access vlan 300

>int vlan 300
>ip address 10.3.3.1 255.255.255.0
>no shut
```

enable: Entra en modo privilegiado.
conf t: Entra en el modo de configuración global.
int Gi1/0/1: Selecciona la interfaz GigabitEthernet 1/0/1 o la que desees.
description [texto]: Añade una descripción a la interfaz para identificar su propósito.
switchport mode access: Configura la interfaz en modo de acceso, permitiendo que solo una VLAN pase por la interfaz.
switchport access vlan : Asigna la interfaz a la VLAN, permitiendo el tráfico de esta VLAN.
int vlan [número]: Selecciona la interfaz de una VLAN específica, permitiendo su configuración.
ip address [dirección IP] [máscara de subred]: Asigna una dirección IP y su máscara de subred a la interfaz, lo que permite que esta participe en la red.
no shut: Habilita la interfaz, permitiendo el paso de tráfico.





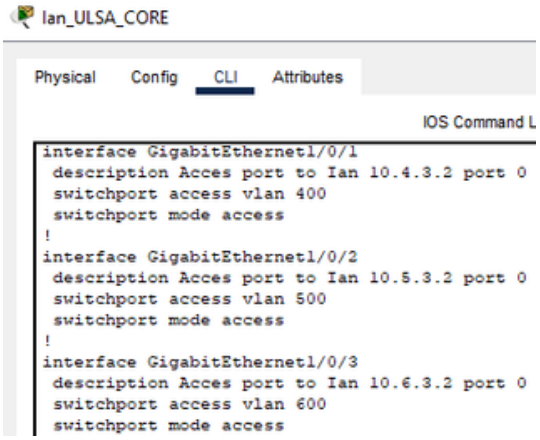
Repetiremos este proceso en el switch de Ulsa Y DMZ:

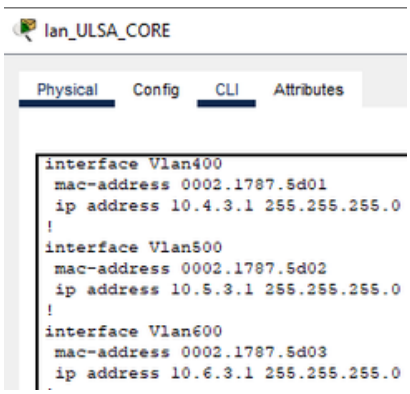
Switch Ulsa:

```
>enable
>conf t
>int Gi1/0/1
>description
>switchport mode Access
>Switchport access vlan 400

>int vlan 400
>ip address 10.4.3.1 255.255.255.0
>no shut
```

```
>enable
>conf t
>int Gi1/0/2
>description
>switchport mode Access
>Switchport access vlan 500

>int vlan 500
>ip address 10.5.3.1 255.255.255.0
>no shut
```

```
>enable
>conf t
>int Gi1/0/3
>description
>switchport mode Access
>Switchport access vlan 600

>int vlan 600
>ip address 10.6.3.1 255.255.255.0
>no shut
```

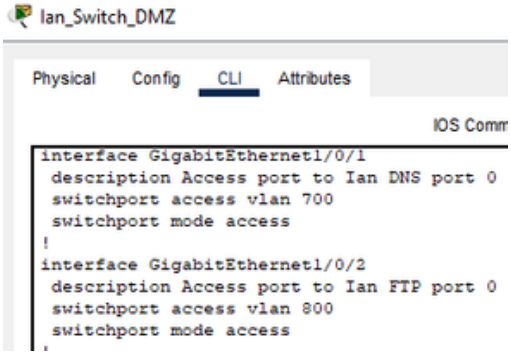


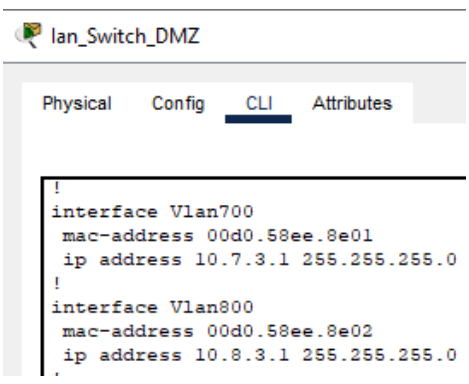


Switch Ulsa DMZ:

```
>enable
>conf t
>int Gi1/0/1
>description
>switchport mode Access
>Switchport access vlan 700

>int vlan 700
>ip address 10.7.3.1 255.255.255.0
>no shut
```

```
>enable
>conf t
>int Gi1/0/2
>description
>switchport mode Access
>Switchport access vlan 800

>int vlan 800
>ip address 10.8.3.1 255.255.255.0
>no shut
```

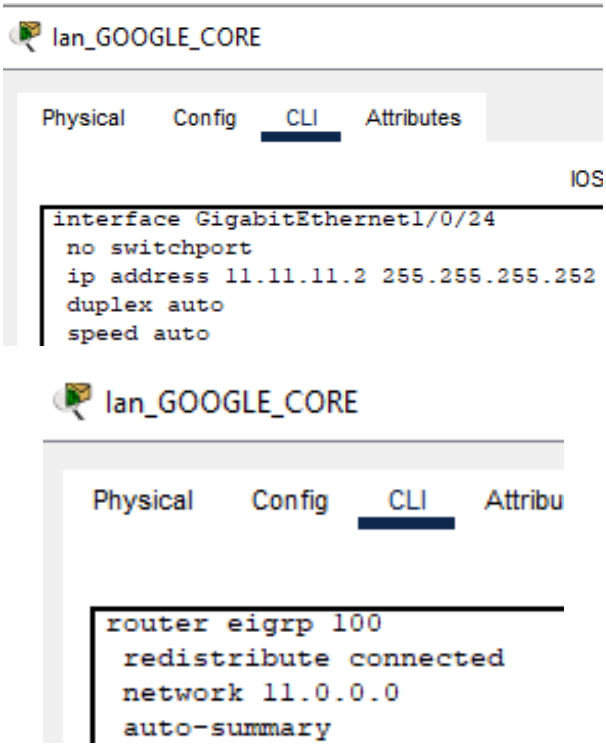




3. Port EIGRP de Switches:

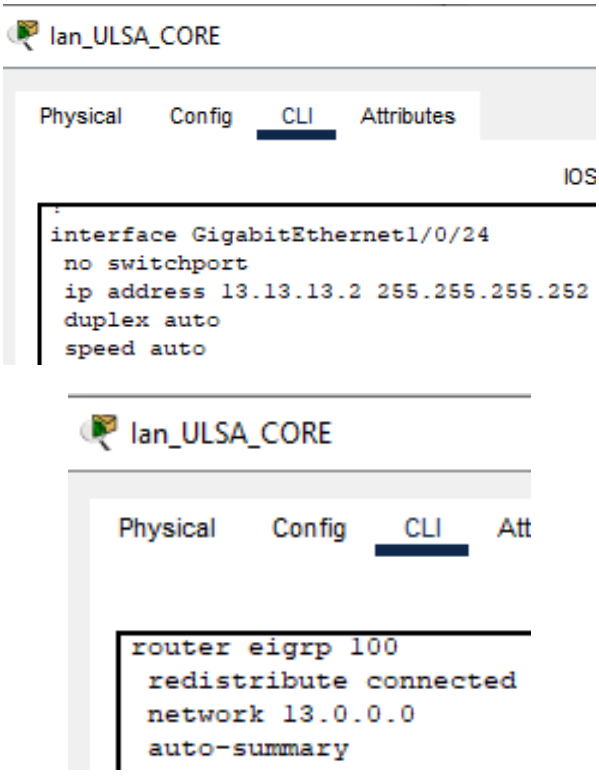
Switch Google:

```
>enable
>conf t
>int Gi1/0/24
>description
>No switchport
>ip address 11.11.11.2 255.255.255.252
>no shut

>enable
>conf t
>Ip routing
>Router eigrp 100
>Redistribute conneceted
>Network 11.11.11.1
```



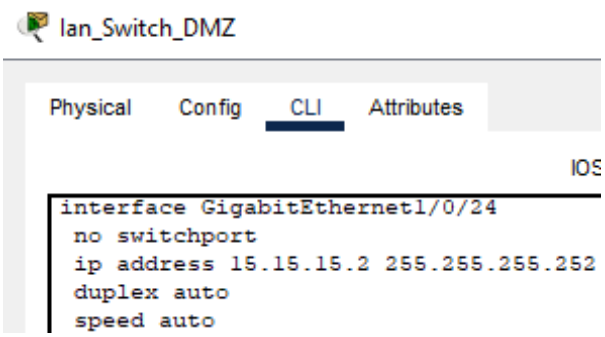
Switch Ulsa:

```
>enable
>conf t
>int Gi1/0/24
>description
>No switchport
>ip address 13.13.13.2 255.255.255.252
>no shut

>enable
>conf t
>Ip routing
>Router eigrp 100
>Redistribute conneceted
>Network 13.13.13.13
```

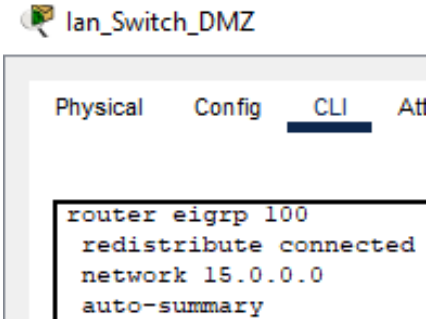


Switch Ulsa DMZ:

```
>enable
>conf t
>int Gi1/0/24
>description
>No switchport
>ip address 15.15.15.2 255.255.255.252
>no shut
```




```
>enable
>conf t
>Ip routing
>Router eigrp 100
>Redistribute conneceted
>Network 11.11.11.1
```

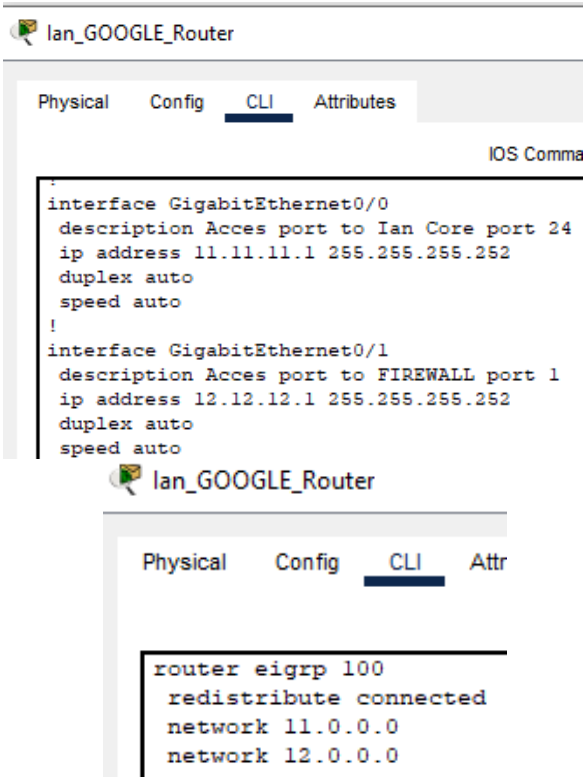


conf t: Configuración global.
int Gi1/0/24: Selecciona la interfaz GigabitEthernet 1/0/24.
description [texto]: Añade una descripción a la interfaz para identificar su propósito.
ip address [dirección IP] [máscara de subred]: Asigna una dirección IP y su máscara de subred a la interfaz, lo que permite que esta participe en la red.
ip routing: Habilita el enrutamiento IP en el dispositivo para que pueda enrutar paquetes entre diferentes redes.
router eigrp 100: Inicia el proceso de enrutamiento EIGRP (Enhanced Interior Gateway Routing Protocol) con el número de sistema autónomo 100.
redistribute connected: Redistribuye las rutas de las interfaces conectadas directamente en el proceso de enrutamiento EIGRP.
network [dirección IP de red] [wildcard mask]: Anuncia una red en el proceso de enrutamiento.
no shut: Habilita la interfaz, permitiendo el paso de tráfico.

4. Configuración de Access ports y Port EIGRP de Routers:

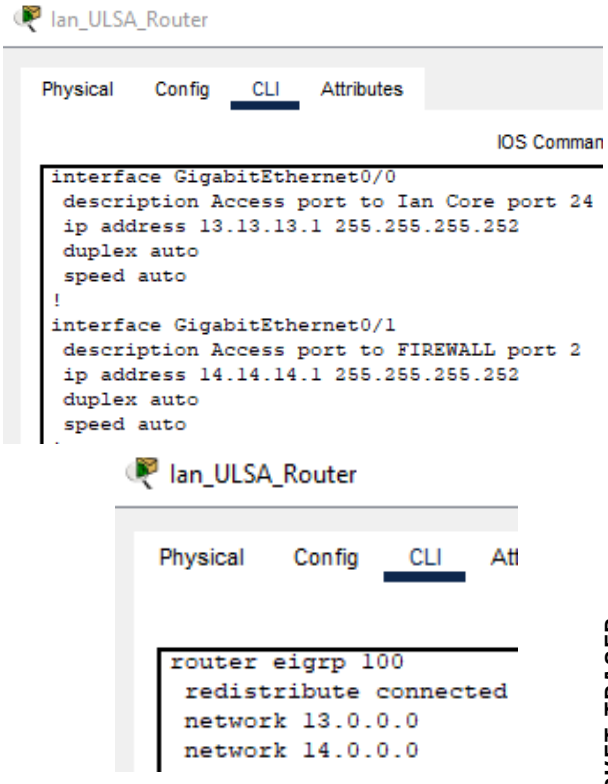
Router Google:

```
>enable
>conf t
>int Gi0/0
>description
>ip address 11.11.11.1 255.255.255.252
>int Gi0/1
>description
>ip address 12.12.12.1 255.255.255.252
>no shut

>enable
>conf t
>Ip routing
>Router eigrp 100
>Redistribute conneceted
>Network 11.11.11.11
>Network 12.12.12.12
```



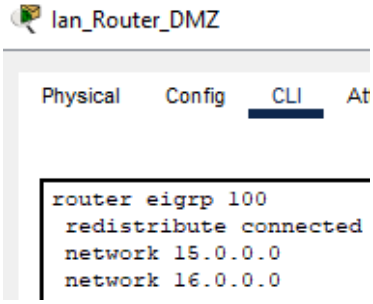
Router Ulsa:

```
>enable
>conf t
>int Gi0/0
>description
>ip address 13.13.13.1 255.255.255.252
>int Gi0/1
>description
>ip address 14.14.14.1 255.255.255.252
>no shut

>enable
>conf t
>Ip routing
>Router eigrp 100
>Redistribute conneceted
>Network 13.13.13.13
>Network 14.14.14.14
```



Router Ulsa DMZ:

```
>enable
>conf t
>int Gi0/0
>description
>ip address 15.15.15.1 255.255.255.252
>int Gi0/1
>description
>ip address 16.16.16.1 255.255.255.252
>no shut

>enable
>conf t
>Ip routing
>Router eigrp 100
>Redistribute conneceted
>Network 15.15.15.15
>Network 16.16.16.16
```

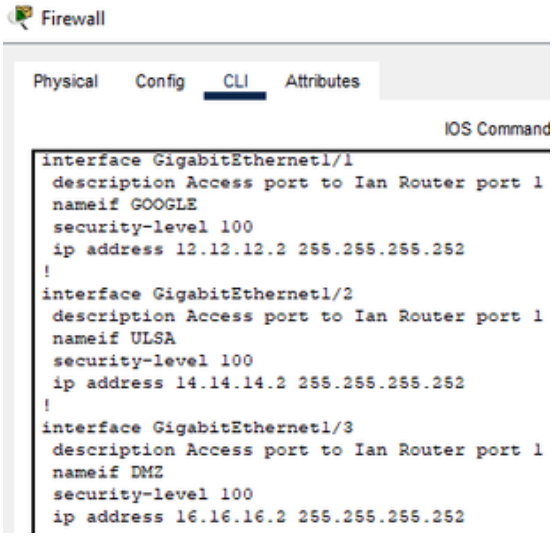


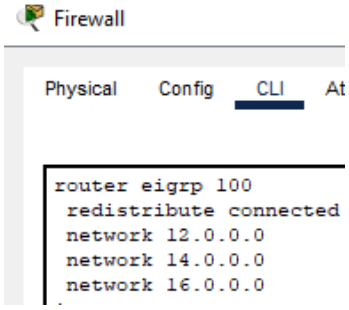
conf t: Configuración global.
int Gi0/0: Selecciona la interfaz GigabitEthernet 0/0 o la que quisiera seleccionarse.
description [texto]: Añade una descripción a la interfaz para identificar su propósito.
ip address [dirección IP] [máscara de subred]: Asigna una dirección IP y su máscara de subred a la interfaz, lo que permite que esta participe **en la red.**
ip routing: Habilita el enrutamiento IP en el dispositivo para que pueda enrutar paquetes entre diferentes redes.
no shut: Habilita la interfaz, permitiendo el paso de tráfico.

5. Configuración Ports Firewall y EIGRP:

Firewall:

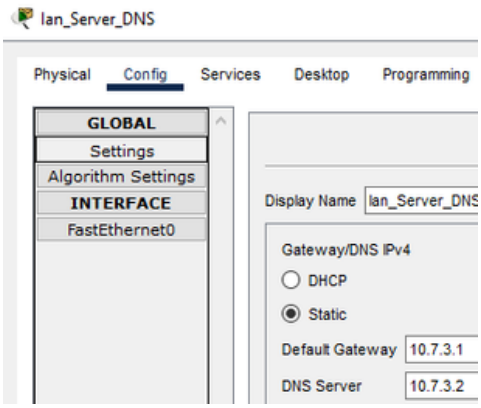
```
>enable
>conf t
>int Gi1/1
>description
>ip address 12.12.12.2 255.255.255.252
>nameif GOOGLE
>Security-level
>int Gi1/2
>description
>ip address 14.14.14.2 255.255.255.252
>nameif ULSA
>security-level
>int Gi1/3

>ip address 16.16.16.2 255.255.255.252
>nameif DMZ
>security-level
>description
>no shut

>enable
>conf t
>Router eigrp 100
>Redistribute conneceted
>Network 12.12.12.12
>Network 14.14.14.14
>Network 16.16.16.16
```

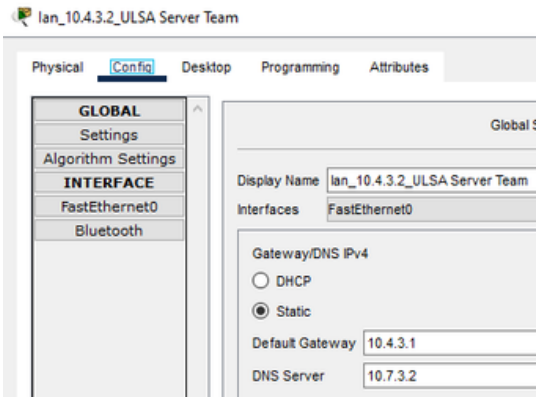




conf t: Configuración global.
int Gi1/1: Selecciona la interfaz GigabitEthernet 1/1 o la que quisiera seleccionarse.
description [texto]: Añade una descripción a la interfaz para identificar su propósito.
ip address [dirección IP] [máscara de subred]: Asigna una dirección IP y su máscara de subred a la interfaz, lo que permite que esta participe en la red.
router eigrp 100: Inicia el proceso de enrutamiento EIGRP (Enhanced Interior Gateway Routing Protocol) con el número de sistema autónomo 100.
redistribute connected: Redistribuye las rutas de las interfaces conectadas directamente en el proceso de enrutamiento EIGRP.
network [dirección IP de red] [wildcard mask]: Anuncia una red en el proceso de enrutamiento.
no shut: Habilita la interfaz, permitiendo el paso de tráfico.

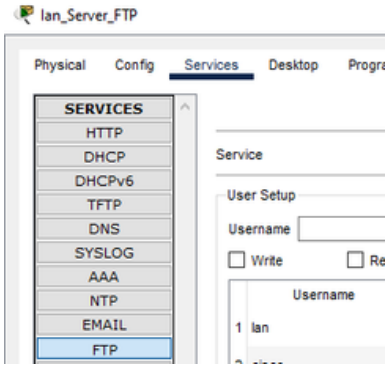
Ahora esta misma ip la tenemos que poner primero en la parte de DNS de el servidor, y despues de las Pcs, que queramos que se muestre la pagina como ejemplo pondre la principal que es la de Ulsa server team:



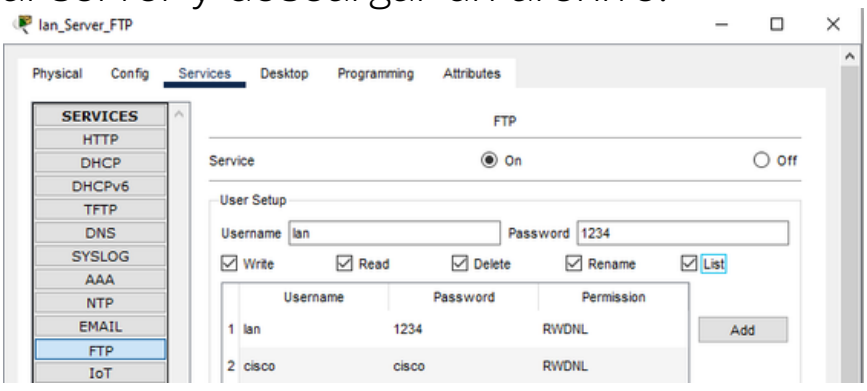


6. Configuración servicio Server FTP:

Para poder hacer la configuración correcta del Server tendremos que acceder al apartado de servicios y luego al apartado de FTP:

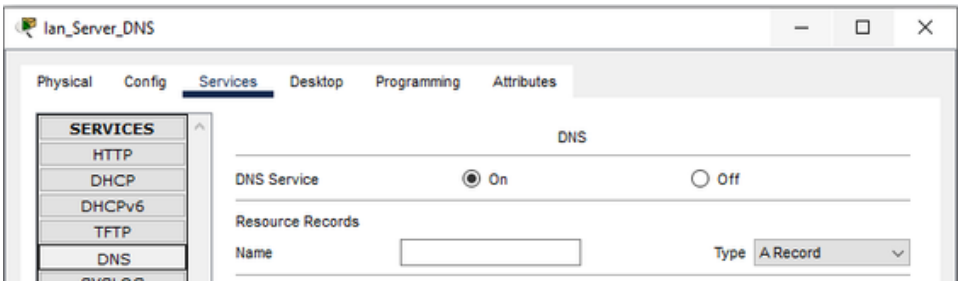


Ahí nos dirigiremos al apartado de Username, ponemos el nombre que queramos y para la password igual, seleccionamos las opciones que se ven en la captura, oprimimos el boton Add y se agregaria nuestro usuario y contraseña, la cual la usaremos más adelante para acceder al server y descargar un archivo:

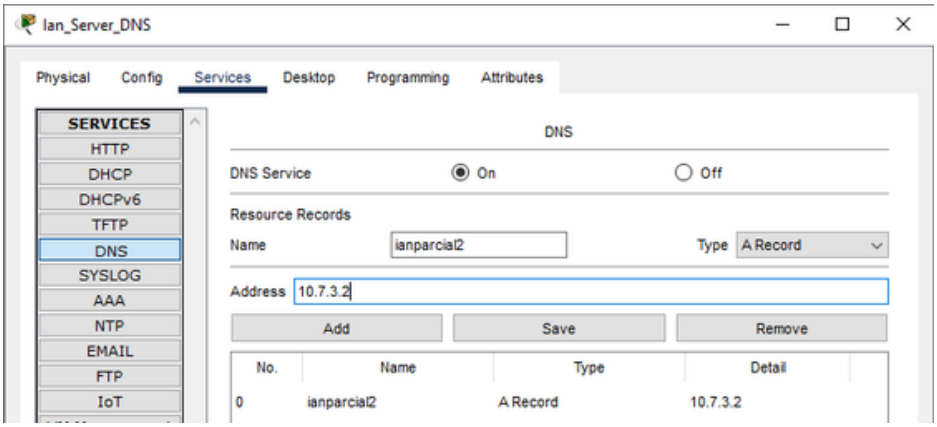


6. Configuración servicio Server DNS:

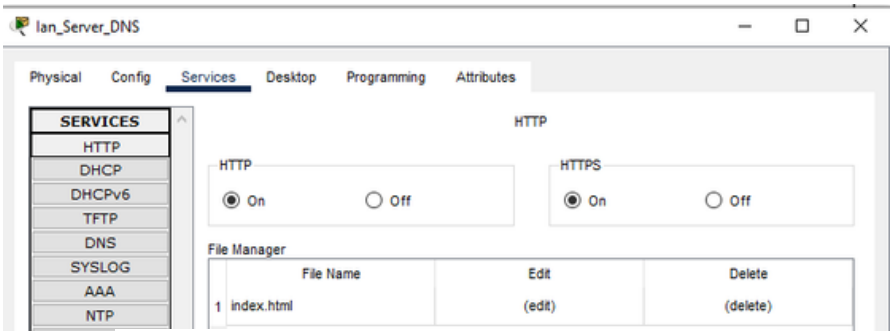
Para poder hacer la configuración correcta del Server tendremos que acceder al apartado de servicios y luego al apartado de DNS:



Ahí nos dirigiremos a la parte de Name para crear nuestra pagina web que usaremos como ejemplo de busqueda en las Pcs remotas solicitadas, ponemos el nombre de nuestra página y en el aparatado de Address ponemos la misma ip del server en este caso 10.7.3.2, oprimimos el boton de ADD y ya quedaría agregada esta DNS para la página web:



Vamos a la parte de HTTP donde con editaremos un documento index.html, esto para poner información de ejemplo y comprobar en nuestra página que puede ser visible:

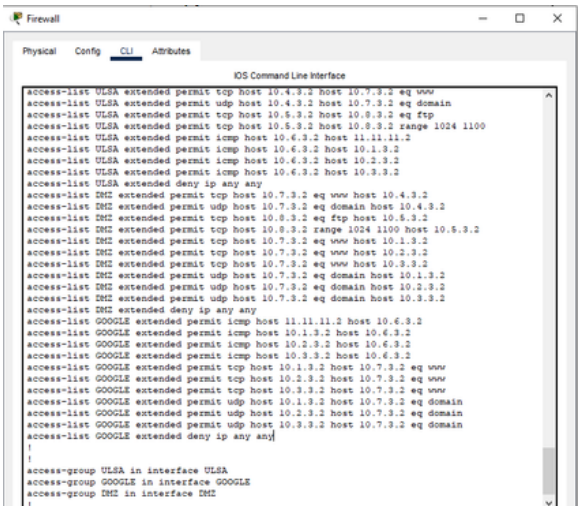



```
<html>
<h1>DATOS</h1>
<p>Nombre: Ian Alejandro Corral
Marín</p>
<p>Carrera: ITIT</p>
<p>Semestre: 5</p>
<p>Clase: Tecnología en Redes 2</p>
<p>Examen: Parcial 2</p>
</html>
```

6. Configuración de todas las ACCESS-LIST:

Siguiendo las reglas de firewall para el flujo de tráfico mostradas al inicio del documento es como se configuraran todas las listas de acceso:

```
>enable
>conf t
>access-list ULSA extended permit tcp host 10.4.3.2 host 10.7.3.2 eq www
>access-list ULSA extended permit udp host 10.4.3.2 host 10.7.3.2 eq domain
>access-list ULSA extended permit tcp host 10.5.3.2 host 10.8.3.2 eq ftp
>access-list ULSA extended permit tcp host 10.5.3.2 host 10.8.3.2 range 1024
1100
>access-list ULSA extended permit icmp host 10.6.3.2 host 11.11.11.2
>access-list ULSA extended permit icmp host 10.6.3.2 host 10.1.3.2
>access-list ULSA extended permit icmp host 10.6.3.2 host 10.2.3.2
>access-list ULSA extended permit icmp host 10.6.3.2 host 10.3.3.2
>access-list ULSA extended deny ip any any
>access-list DMZ extended permit tcp host 10.7.3.2 eq www host 10.4.3.2
>access-list DMZ extended permit udp host 10.7.3.2 eq domain host 10.4.3.2
>access-list DMZ extended permit tcp host 10.8.3.2 eq ftp host 10.5.3.2
>access-list DMZ extended permit tcp host 10.8.3.2 range 1024 1100 host
10.5.3.2
>access-list DMZ extended permit tcp host 10.7.3.2 eq www host 10.1.3.2
>access-list DMZ extended permit tcp host 10.7.3.2 eq www host 10.2.3.2
>access-list DMZ extended permit tcp host 10.7.3.2 eq www host 10.3.3.2
>access-list DMZ extended permit udp host 10.7.3.2 eq domain host 10.1.3.2
>access-list DMZ extended permit udp host 10.7.3.2 eq domain host 10.2.3.2
access-list DMZ extended permit udp host 10.7.3.2 eq domain host 10.3.3.2
>access-list DMZ extended deny ip any any
>access-list GOOGLE extended permit icmp host 11.11.11.2 host 10.6.3.2
>access-list GOOGLE extended permit icmp host 10.1.3.2 host 10.6.3.2
>access-list GOOGLE extended permit icmp host 10.2.3.2 host 10.6.3.2
>access-list GOOGLE extended permit icmp host 10.3.3.2 host 10.6.3.2
>access-list GOOGLE extended permit tcp host 10.1.3.2 host 10.7.3.2 eq www
>access-list GOOGLE extended permit tcp host 10.2.3.2 host 10.7.3.2 eq www
>access-list GOOGLE extended permit tcp host 10.3.3.2 host 10.7.3.2 eq www
>access-list GOOGLE extended permit udp host 10.1.3.2 host 10.7.3.2 eq domain
>access-list GOOGLE extended permit udp host 10.2.3.2 host 10.7.3.2 eq domain
>access-list GOOGLE extended permit udp host 10.3.3.2 host 10.7.3.2 eq domain
>access-list GOOGLE extended deny ip any any
>access-group ULSA in interface ULSA
>access-group GOOGLE in interface GOOGLE
>access-group DMZ in interface DMZ
```



Access List ULSA:

1. HTTP (TCP): Permite tráfico desde `10.4.3.2` a `10.7.3.2`.
2. DNS (UDP): Permite tráfico desde `10.4.3.2` a `10.7.3.2`.
3. FTP (TCP): Permite tráfico desde `10.5.3.2` a `10.8.3.2`.
4. Rango de puertos (TCP): Permite tráfico desde `10.5.3.2` a `10.8.3.2` en puertos `1024-1100`.
5. ICMP (Ping): Permite pings desde `10.6.3.2` a varias IPs (`11.11.11.2`, `10.1.3.2`, `10.2.3.2`, `10.3.3.2`).
6. Denegar todo: Todo el tráfico IP no especificado se deniega.

Access List DMZ:

1. HTTP (TCP): Permite tráfico desde `10.7.3.2` a `10.4.3.2`.
2. DNS (UDP): Permite tráfico desde `10.7.3.2` a `10.4.3.2`.
3. FTP (TCP): Permite tráfico desde `10.8.3.2` a `10.5.3.2`.
4. Rango de puertos (TCP): Permite tráfico desde `10.8.3.2` a `10.5.3.2` en puertos `1024-1100`.
5. HTTP y DNS a otras IPs: Permite tráfico desde `10.7.3.2` a `10.1.3.2`, `10.2.3.2`, y `10.3.3.2`.
6. Denegar todo: Todo el tráfico IP no especificado se deniega.

Access List GOOGLE:

1. ICMP (Ping): Permite pings desde `11.11.11.2` y `10.x.3.2` a `10.6.3.2`.
2. HTTP (TCP): Permite tráfico desde `10.x.3.2` a `10.7.3.2`.
3. DNS (UDP): Permite tráfico desde `10.x.3.2` a `10.7.3.2`.
4. Denegar todo: Todo el tráfico IP no especificado se deniega.

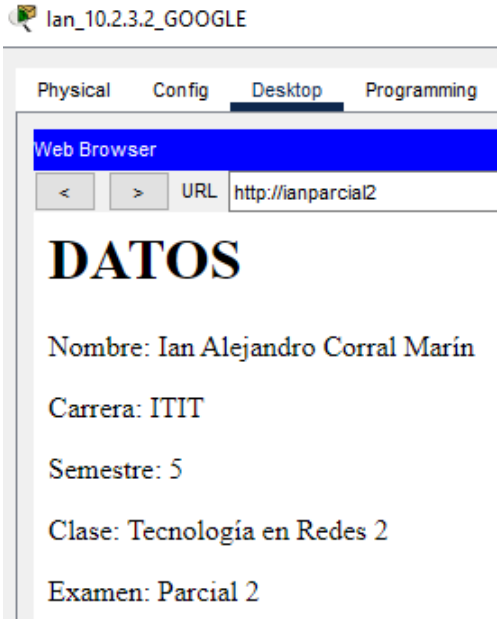
Aplicación de las listas de acceso:

- Las listas se aplican a las interfaces `ULSA`, `GOOGLE` y `DMZ`.

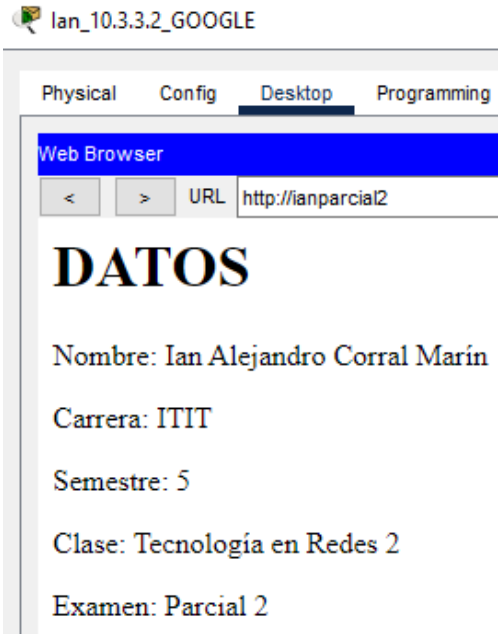
Por último para comprobar que funciono correctamente vamos a accesar a la pagina web desde GOOGLE y desde Ulsa Server Team:

Google 1:

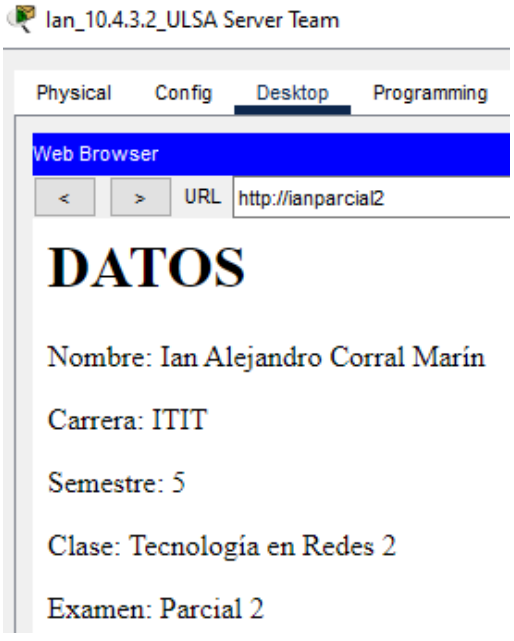
Google 2:



Google 3:

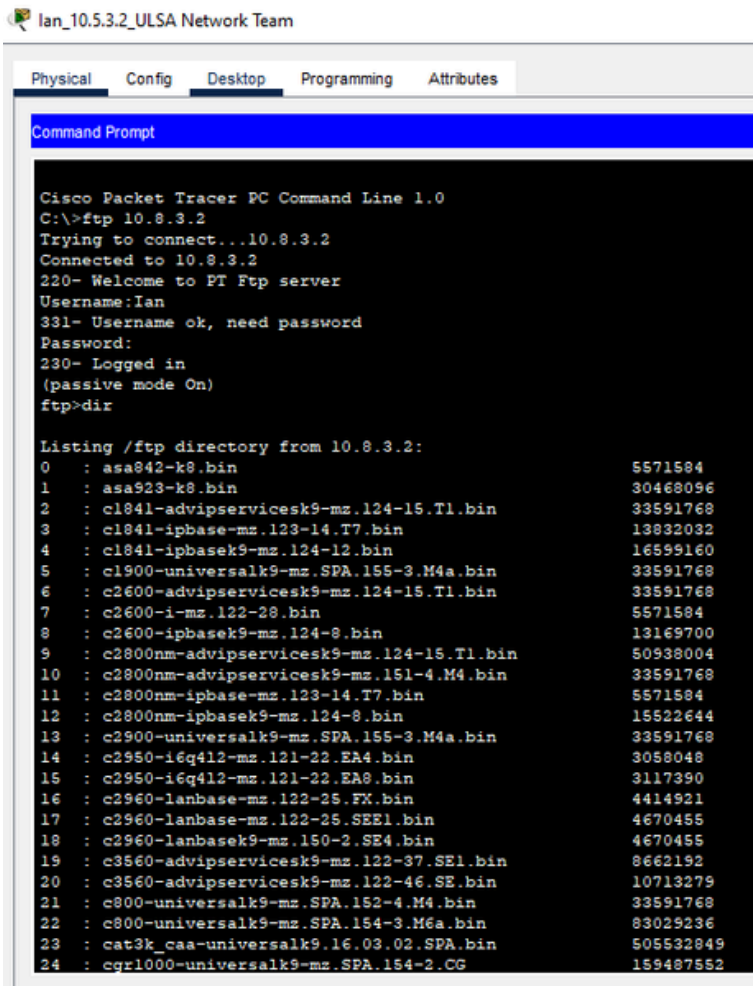


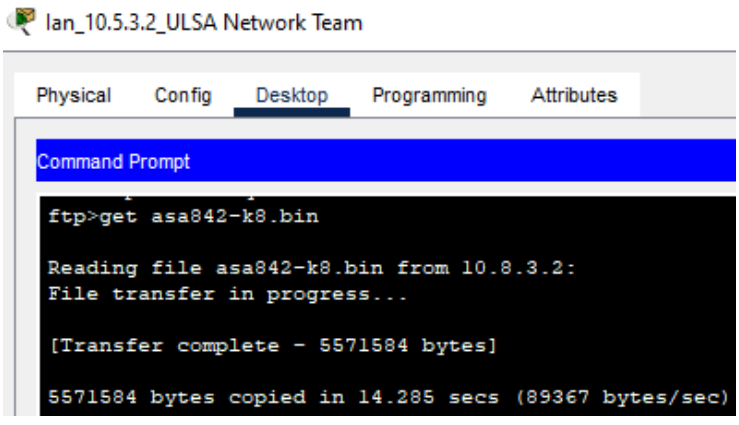
Ulsa Server Team:

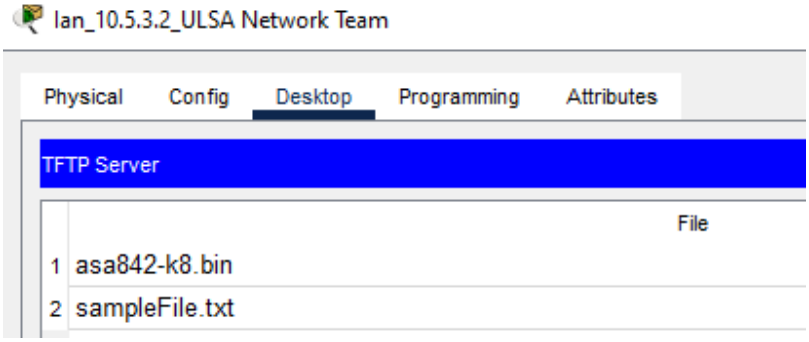


Ahora entraremos al FTP Server desde Ulsa Network Team con nuestro usuario y contraseña creado anteriormente, y descargaremos alguno de los documentos que se encuentren en el server:

Ulsa Network Team:





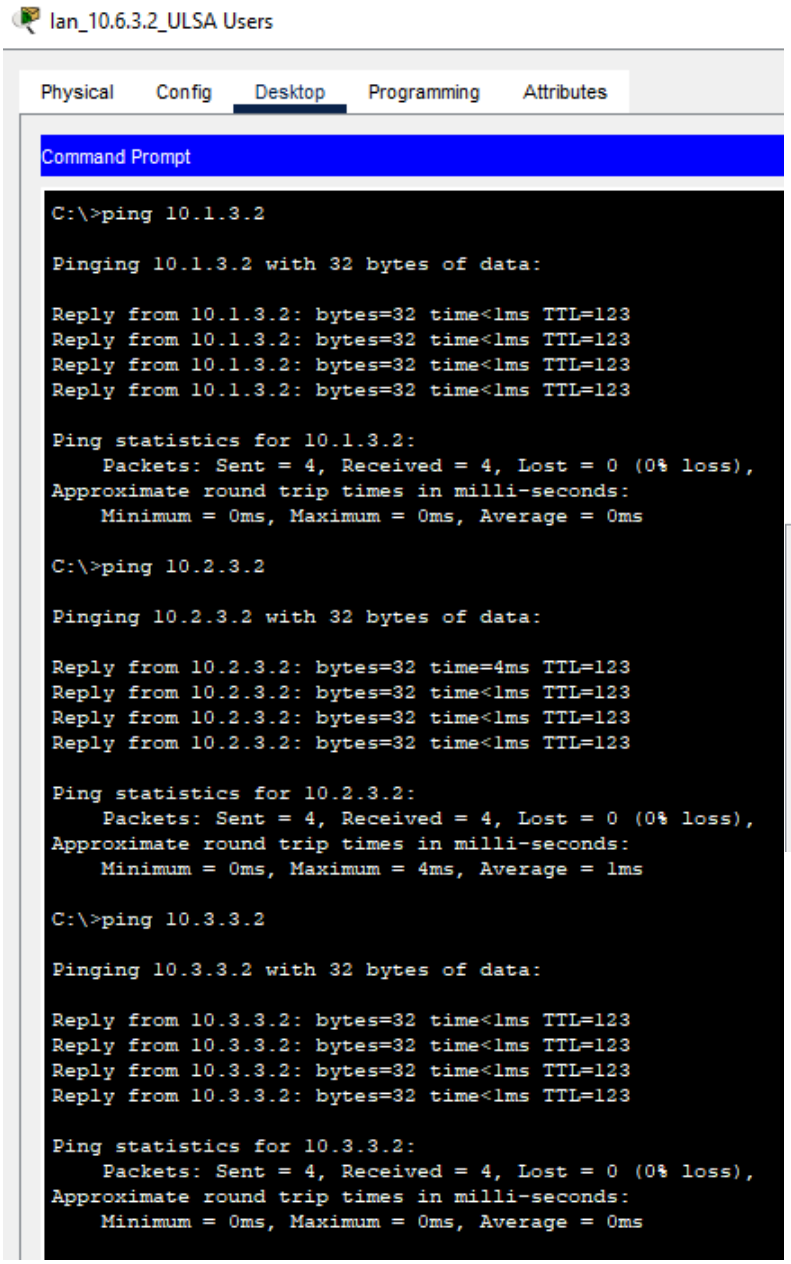


PC users alcanza a todo GOOGLE y viceversa:

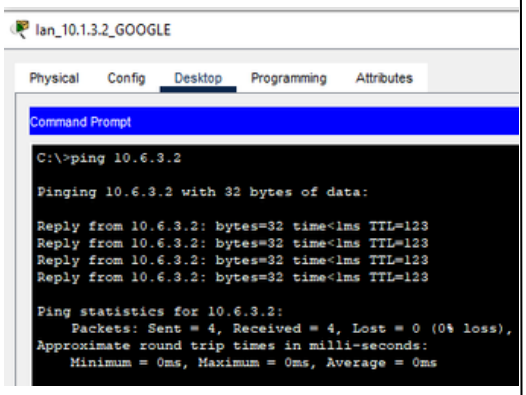
RESULTADOS

MANUAL PACKET TRACER

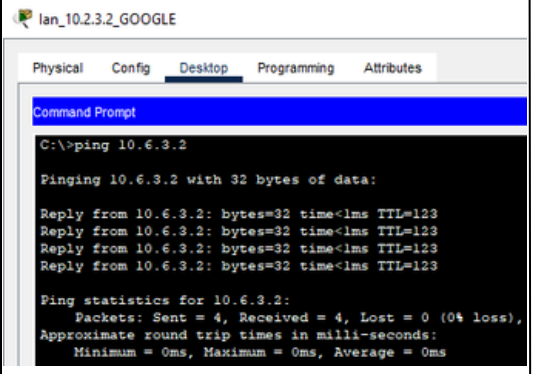
Ulsa Users:



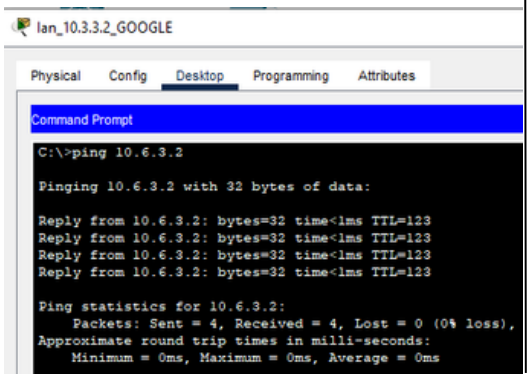
Google 1:



Google 2:



Google 3:



CONCLUSIÓN

Este manual detalla la configuración de una topología de red en Packet Tracer que conecta las redes de Google, ULSA y la DMZ, con el objetivo de establecer una conectividad eficiente y segura. La red incluye switches CORE, VLANs y un firewall para gestionar y proteger el tráfico de red.

La estructura de la red se segmenta en tres áreas principales: Google y ULSA, cada una con un switch CORE y varias VLANs que optimizan la comunicación. La interconexión entre estas áreas se realiza mediante routers y el protocolo de enrutamiento EIGRP 100, asegurando la propagación dinámica de rutas.

Un aspecto esencial de esta configuración es el firewall, que controla el tráfico entre las VLANs, aplicando reglas de acceso que limitan las conexiones entre Google y ULSA a aquellas que están autorizadas. Cada VLAN cuenta con su propio gateway, facilitando una segmentación clara del tráfico.

Asimismo, se gestionan servicios como HTTP, DNS, FTP e ICMP, asegurando que el tráfico sea manejado conforme a las políticas de seguridad.

En resumen, este manual proporciona una guía práctica para configurar una red empresarial segura y eficiente que conecta las redes de Google y ULSA, optimizando la comunicación y protegiendo el tráfico entre sus segmentos.