



MANUAL

PACKET TRACER



Ian Alejandro Corral Marín
12130

TECNOLOGÍA DE REDES



INDICE

02-03 Introducción

04. Objetivo

05-06. Conceptos Clave

07. Glosario de comandos

08-09. Configuración de la Topología

10-30. Paso a Paso para Configurar las Redes

31-39. Resultados

40. Conclusión

01.

Introducción a Cisco Packet Tracer

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.



Este manual detalla la configuración de una topología de red en Cisco Packet Tracer que conecta las redes de ULSA, DMZ y Google. Busca garantizar una comunicación eficiente y controlada entre estos segmentos mediante el uso de VLANs, enrutamiento dinámico EIGRP, y un firewall que aplica estrictas políticas de seguridad.

Cada segmento desempeña un rol específico en la red. ULSA y Google están estructuradas en VLANs que segmentan el tráfico para mejorar la eficiencia y la seguridad. DMZ, por su parte, actúa como una zona intermedia donde se ubican servicios clave como FTP y DNS. Adicionalmente, cada zona cuenta con un servidor DHCP para asignar direcciones IP dinámicamente a ciertos dispositivos, facilitando la administración de la red.

El protocolo EIGRP se utiliza para propagar rutas dinámicas entre los diferentes segmentos, asegurando una conectividad fluida. Las listas de control de acceso (ACLs) y el firewall permiten o restringen el tráfico entre las redes, asegurando que solo los protocolos autorizados, como HTTP, FTP y DNS, puedan atravesar las restricciones. Además, se utilizan herramientas como ICMP (ping) para verificar la conectividad y validar que las configuraciones funcionan correctamente.

Este manual proporciona una guía detallada para la configuración de los dispositivos clave, desde los switches y routers hasta los servidores y el firewall, asegurando una comunicación segura, eficiente y confiable entre ULSA, DMZ y Google.

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

CORE SWITCH:

VLAN 100: 10.1.1.1/24 (GATEWAY),
PC 10.1.1.2

VLAN 200: 10.2.1.1/24 (GATEWAY),
PC 10.2.1.2

VLAN 300: 10.3.1.1/24 (GATEWAY),
PC 10.3.1.2

CONEXIONES:

SWITCH → ROUTER (WAN1):
11.11.11.0/30

ROUTER → FIREWALL (WAN2):
12.12.12.0/30

ULSA

CORE SWITCH:

VLAN 400: 10.4.1.1/24 (GATEWAY),
PC 10.4.1.2

VLAN 500: 10.5.1.1/24 (GATEWAY),
PC 10.5.1.2

VLAN 600: 10.6.1.1/24 (GATEWAY),
PC 10.6.1.2

CONEXIONES:

SWITCH → ROUTER (WAN1):
13.13.13.0/30

ROUTER → FIREWALL (WAN2):
14.14.14.0/30

ULSA DMZ

CORE SWITCH:

VLAN 700: 10.7.X.1/24 (GATEWAY),
PC 10.7.X.70

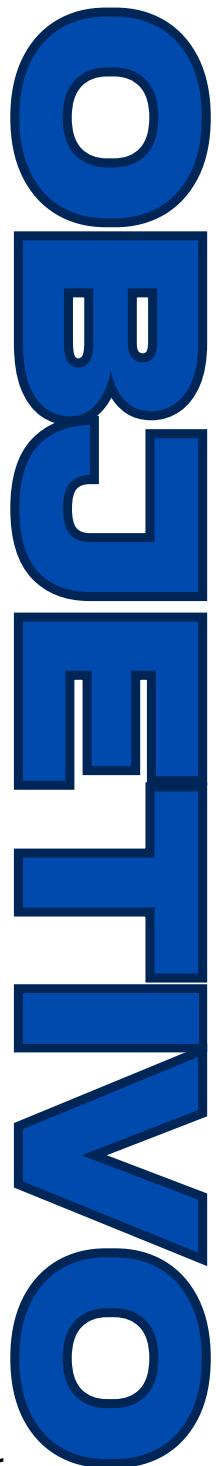
VLAN 800: 10.8.X.1/24 (GATEWAY),
PC 10.8.X.80

VLAN 900: 10.9.X.1/24 (GATEWAY),
PC 10.9.X.90

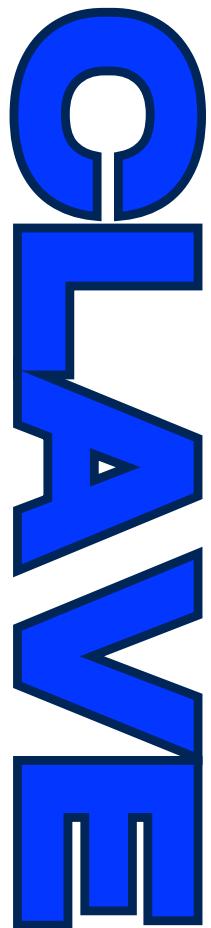
SWITCH → ROUTER (WAN1):
15.15.15.0/30

ROUTER → FIREWALL (WAN2):
16.16.16.0/30

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, así como tambien la asignacion de diferentes ips por medio de su Server DHCP correspondiente.



CONCEPTOS



- **Red:** Grupo de computadoras y dispositivos conectados para comunicarse e intercambiar información.
- **Router:** Dispositivo que conecta redes y dirige el tráfico entre ellas.
- **Switch:** Conecta múltiples dispositivos en una red y envía datos solo a los destinatarios correctos.
- **VLAN (Virtual LAN):** Red virtual dentro de un switch que organiza y segmenta dispositivos, mejorando la seguridad y eficiencia.
- **Dirección IP:** Identificador único para un dispositivo en la red, similar a una dirección postal.
- **Máscara de Subred:** Define qué parte de la dirección IP pertenece a la red y cuál a los dispositivos.
- **EIGRP:** Protocolo que permite a los routers compartir rutas y encontrar la mejor para enviar datos.
- **Firewall:** Controla el acceso a la red para protegerla contra amenazas.
- **DHCP:** Protocolo que asigna automáticamente direcciones IP a los dispositivos en la red.
- **Telnet:** Protocolo para acceder y administrar dispositivos de red de forma remota a través de línea de comandos.
- **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

CON
MAN
DO
C

- **enable:** Accede al modo privilegiado del dispositivo.
- **configure terminal (conf t):** Ingresa al modo de configuración global para realizar ajustes en el dispositivo.
- **show running-config:** Muestra la configuración actual en ejecución en el dispositivo.
- **username [nombre] password [contraseña]:** Crea un usuario local con su respectiva contraseña para autenticación.
- **interface [tipo] [número] (ej.: int Gi1/0/1):** Selecciona una interfaz específica para configurarla.
- **description [texto]:** Añade una descripción a la interfaz para identificar su función.
- **no shutdown (no shut):** Activa la interfaz.
- **switchport mode access:** Configura la interfaz como puerto de acceso.
- **switchport access vlan [VLAN_ID]:** Asigna la interfaz a una VLAN específica.
- **no switchport:** Convierte una interfaz de capa 2 a capa 3, lo que permite asignar direcciones IP.
- **ip address [dirección IP] [máscara de subred]:** Asigna una dirección IP y máscara de subred a una interfaz.
- **ip helper-address [dirección IP]:** Redirige paquetes de broadcast (como DHCP) hacia un servidor específico en otra red.
- **nameif [nombre]:** Asigna un nombre a la interfaz (usualmente en dispositivos con firewall).
- **security-level [nivel]:** Define el nivel de seguridad de una interfaz (en firewalls como ASA).
- **interface vlan [VLAN_ID]:** Configura la interfaz VLAN correspondiente.
- **ip routing:** Habilita el enrutamiento IP en el dispositivo.
- **router eigrp [AS_NUMBER]:** Inicia el protocolo de enrutamiento EIGRP con el número de sistema autónomo especificado.
- **network [dirección IP] [máscara comodín]:** Define las redes que EIGRP debe anunciar.
- **redistribute connected:** Redistribuye las rutas conectadas directamente en EIGRP.
- **ip route [destino] [máscara] [siguiente salto]:** Crea una ruta estática hacia una red específica.
- **access-list [nombre] extended permit/deny [protocolo] host [IP1] host [IP2] [puerto]:** Permite o deniega tráfico específico entre direcciones IP.
- **access-group [nombre] in interface [nombre interfaz]:** Aplica una lista de acceso a una interfaz en la dirección de entrada.
- **deny ip any any:** Deniega todo el tráfico no especificado en la lista de acceso.
- **nameif [nombre]:** Asigna un nombre a la interfaz para facilitar su identificación.
- **security-level [nivel]:** Configura el nivel de seguridad para una interfaz (usualmente para firewalls).

CONFIGURACIÓN

TUTORIAL
DE
REDES
EN
MANUAL
PACKET TRACER

Conexión de PCs a Cores:

- PCs de GOOGLE:
 - PC1, PC2 y PC3 conectados al core GOOGLE en las interfaces GigabitEthernet 1/0/1, 1/0/2 y 1/0/3 respectivamente.
- PCs de ULSA:
 - PC1, PC2 y PC3 conectados al core ULSA en las interfaces GigabitEthernet 1/0/1, 1/0/2 y 1/0/3 respectivamente.
- PC de DMZ:
 - PC4 conectada al core DMZ en la interfaz GigabitEthernet 1/0/3.

Conexión de Servers a Cores:

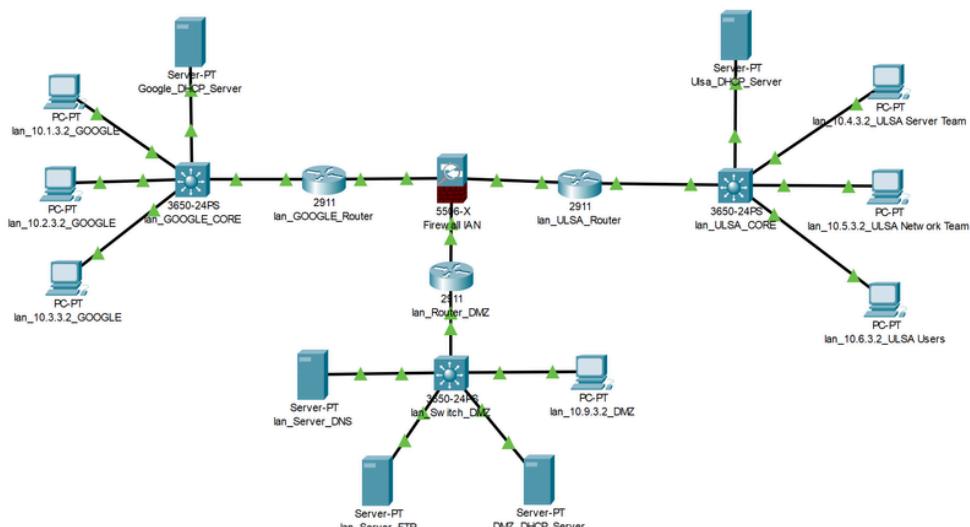
- Servers de DMZ:
 - Server1 y Server2 conectados al core DMZ en las interfaces GigabitEthernet 1/0/1 y 1/0/2.
- Servers DHCP:
 - Server DHCP1 conectado al core GOOGLE en la interfaz GigabitEthernet 1/0/4.
 - Server DHCP2 conectado al core ULSA en la interfaz GigabitEthernet 1/0/4.
 - Server DHCP3 conectado al core DMZ en la interfaz GigabitEthernet 1/0/4.

Conexión de Cores a Routers:

- Core GOOGLE al router GOOGLE: GigabitEthernet 1/0/24 del core al GigabitEthernet 0/0 del router.
- Core ULSA al router ULSA: GigabitEthernet 1/0/24 del core al GigabitEthernet 0/0 del router.
- Core DMZ al router DMZ: GigabitEthernet 1/0/24 del core al GigabitEthernet 0/0 del router.

Conexión al Firewall:

- Router GOOGLE al firewall: GigabitEthernet 0/1 del router a GigabitEthernet 1/1 del firewall.
- Router ULSA al firewall: GigabitEthernet 0/1 del router a GigabitEthernet 1/2 del firewall.
- Router DMZ al firewall: GigabitEthernet 0/1 del router a GigabitEthernet 1/3 del firewall.



CONFIGURACIÓN

T
O
T
O
F
O
R
A

Reglas de Firewall para el flujo de tráfico:

- Trafico debe cruzar el Firewall
- Deben existir access-list específicas para el trafico requerido
- Al final de cada lista de acceso incluir “deny ip any any”
- Google OUTSIDE debe tener acceso a ULSA INSIDE por Telnet
- ULSA INSIDE debe tener acceso a ULSA DMZ por DNS y HTTP
- ULSA INSIDE debe tener acceso a ULSA DMZ por FTP
- 3 DHCP Servers, uno en cada LAN debe dar IPs a las PCs locales
- Accesar via Telnet desde Google PC1 a ULSA INSIDE CORE Switch
- Ver pagina WEB de DMZ DNS-WEB Server desde ULSA INSIDE PC1
- Accesar via FTP desde ULSA PC2 a DMZ FTP Server
- Mostrar IPs de las 9 PCs obtenidas por DHCP (ipconfig)

CONFIGURACIÓN

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**

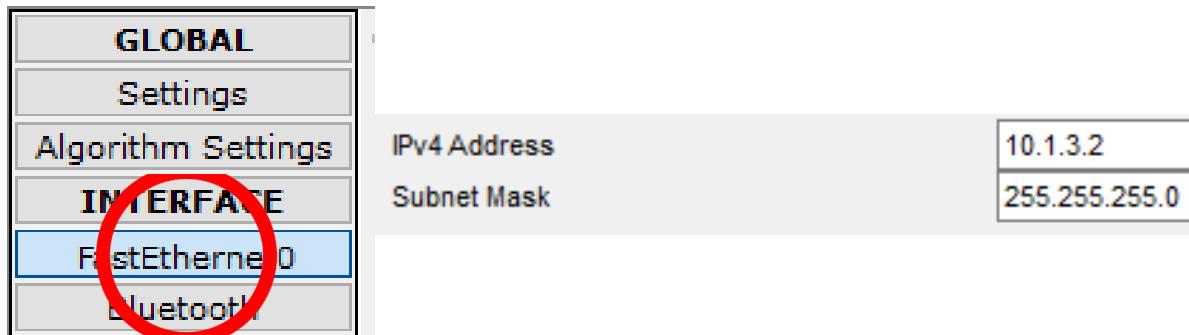
(el número que sigue despues del 10 depende de cada vlan, es decir en la siguiente PC seria 10.2.3.1 pues su vlan es 200, y así sucesivamente):



10.



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 sería **10.1.3.2** :



Repetiremos este proceso en cada PC:

Google 2:

This screenshot shows the configuration for the 'lan_10.2.3.2_GOOGLE' interface. The 'Config' tab is selected. In the 'GLOBAL' section, the 'Display Name' is 'lan_10.2.3.2_GOOGLE'. Under 'Interfaces', 'FastEthernet0' is selected. In the 'FastEthernet0' configuration panel, the 'IP Configuration' is set to 'Static', with 'IPv4 Address' set to '10.2.3.2' and 'Subnet Mask' set to '255.255.255.0'.

Google 3:

This screenshot shows the configuration for the 'lan_10.3.3.2_GOOGLE' interface. The 'Config' tab is selected. In the 'GLOBAL' section, the 'Display Name' is 'lan_10.3.3.2_GOOGLE'. Under 'Interfaces', 'FastEthernet0' is selected. In the 'FastEthernet0' configuration panel, the 'IP Configuration' is set to 'Static', with 'IPv4 Address' set to '10.3.3.2' and 'Subnet Mask' set to '255.255.255.0'.

Ahora del lado derecho de ULSA:

Ulsa 4:

The screenshot shows two windows side-by-side, both titled "lan_10.4.3.2_ULSA Server Team".

Left Window (Config tab):

- GLOBAL:** Settings, Algorithm Settings.
- INTERFACE:** FastEthernet0, Bluetooth.
- Display Name:** lan_10.4.3.2_U.
- Interfaces:** FastEthernet0.
- Gateway/DNS IPv4:** IP Configuration (Static selected), IP Address: 10.4.3.1.
- Default Gateway:** 10.4.3.1.

Right Window (Config tab):

- GLOBAL:** Settings, Algorithm Settings.
- INTERFACE:** FastEthernet0, Bluetooth.
- FastEthernet0:** Port Status, Bandwidth, Duplex, MAC Address: 0060.47EB.678.
- IP Configuration:** IP Address: 10.4.3.2, Subnet Mask: 255.255.255.0.

Ulsa 5:

The screenshot shows two windows side-by-side, both titled "lan_10.5.3.2_ULSA Network Team".

Left Window (Config tab):

- GLOBAL:** Settings, Algorithm Settings.
- INTERFACE:** FastEthernet0, Bluetooth.
- Display Name:** lan_10.5.3.2_U.
- Interfaces:** FastEthernet0.
- Gateway/DNS IPv4:** IP Configuration (Static selected), IP Address: 10.5.3.1.
- Default Gateway:** 10.5.3.1.

Right Window (Config tab):

- GLOBAL:** Settings, Algorithm Settings.
- INTERFACE:** FastEthernet0, Bluetooth.
- FastEthernet0:** Port Status, Bandwidth, Duplex, MAC Address: 000C.CF94.435.
- IP Configuration:** IP Address: 10.5.3.2, Subnet Mask: 255.255.255.0.

Ulsa 6:

The screenshot shows two windows side-by-side, both titled "lan_10.6.3.2_ULSA Users".

Left Window (Config tab):

- GLOBAL:** Settings, Algorithm Settings.
- INTERFACE:** FastEthernet0, Bluetooth.
- Display Name:** lan_10.6.3.2_U.
- Interfaces:** FastEthernet0.
- Gateway/DNS IPv4:** IP Configuration (Static selected), IP Address: 10.6.3.1.
- Default Gateway:** 10.6.3.1.

Right Window (Config tab):

- GLOBAL:** Settings, Algorithm Settings.
- INTERFACE:** FastEthernet0, Bluetooth.
- FastEthernet0:** Port Status, Bandwidth, Duplex, MAC Address: 0006.2A01.E03.
- IP Configuration:** IP Address: 10.6.3.2, Subnet Mask: 255.255.255.0.

Ahora del lado de DMZ:

DMZ 9:

lan_10.9.3.2_DMZ

Physical Config Desktop Programming Attributes

GLOBAL

- Settings
- Algorithm Settings
- INTERFACE**
- FastEthernet0
- Bluetooth

Display Name: lan_10.9.3.2_DMZ
Interfaces: FastEthernet0

Gateway/DNS IPv4:
 DHCP
 Static
Default Gateway: 10.9.3.1

lan_10.9.3.2_DMZ

Physical Config Desktop Programming Attributes

GLOBAL

- Settings
- Algorithm Settings
- INTERFACE**
- FastEthernet0
- Bluetooth

FastEthernet0

Port Status
Bandwidth
Duplex
MAC Address: 00E0.F794.C3E

IP Configuration:
 DHCP
 Static
IPv4 Address: 10.9.3.2
Subnet Mask: 255.255.255.0

NOTA: Tambien podemos oprimir en la parte de DHCP de cada PC o server pues como se menciono en la topología usaremos servers DHCP, los cuales asignan direcciones IP de forma automática dependiendo su configuración de serverPools la cual se vera más adelante como realizarla:

lan_10.9.3.2_DMZ

Physical Config Desktop Programming Attributes

GLOBAL

- Settings
- Algorithm Settings
- INTERFACE**
- FastEthernet0
- Bluetooth

Display Name: lan_10.9.3.2_DMZ
Interfaces: FastEthernet0

Gateway/DNS IPv4:
 DHCP
 Static

lan_10.9.3.2_DMZ

Physical Config Desktop Programming Attributes

GLOBAL

- Settings
- Algorithm Settings
- INTERFACE**
- FastEthernet0
- Bluetooth

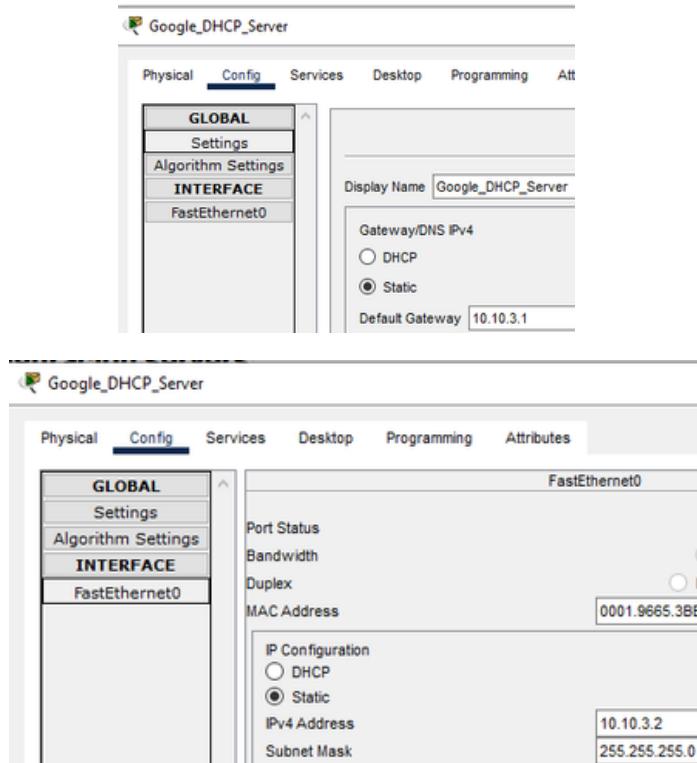
FastEthernet0

Port Status
Bandwidth
Duplex
MAC Address: 00E0.F794.C3E2

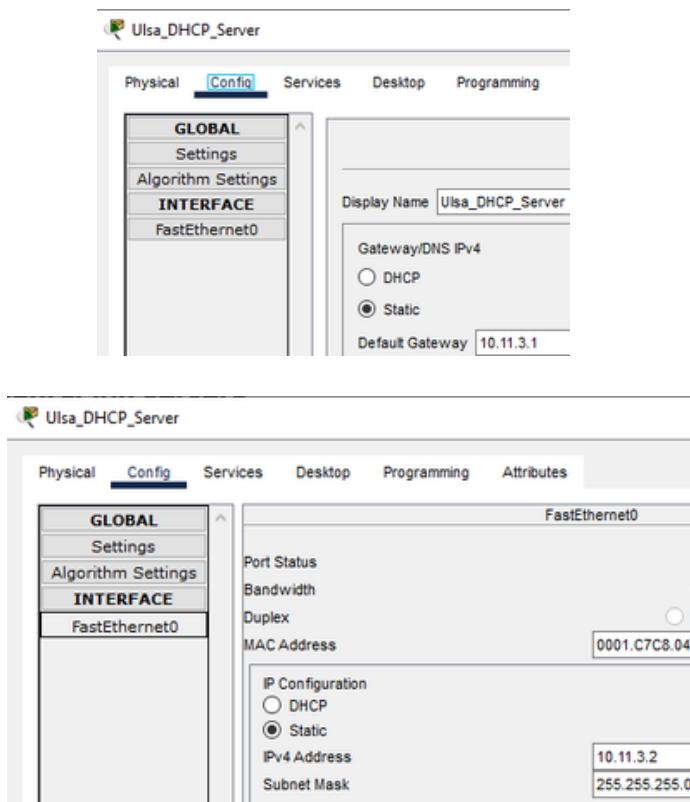
IP Configuration:
 DHCP
 Static
IPv4 Address: 10.9.3.94
Subnet Mask: 255.255.255.0

Configuración servers:

GOOGLE DHCP:

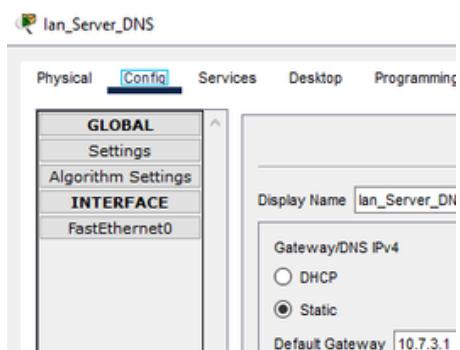


ULSA DHCP:

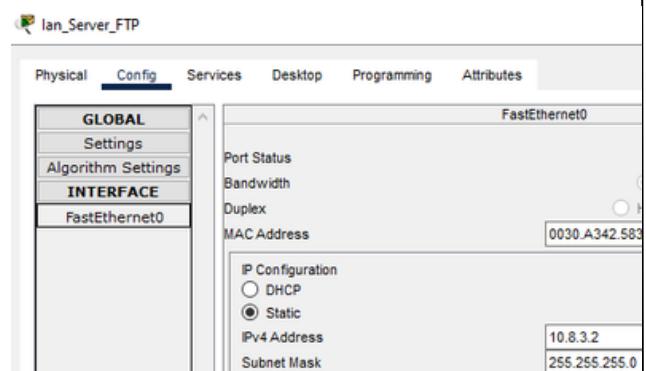
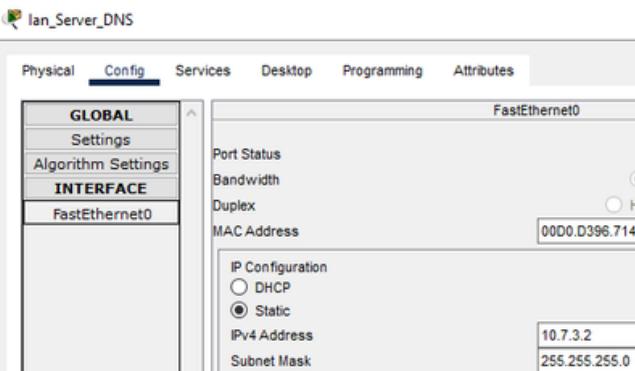
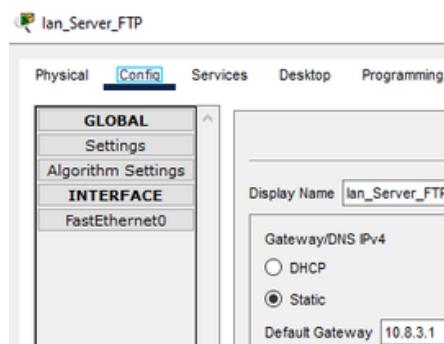


Del lado de DMZ se encuentran 3:

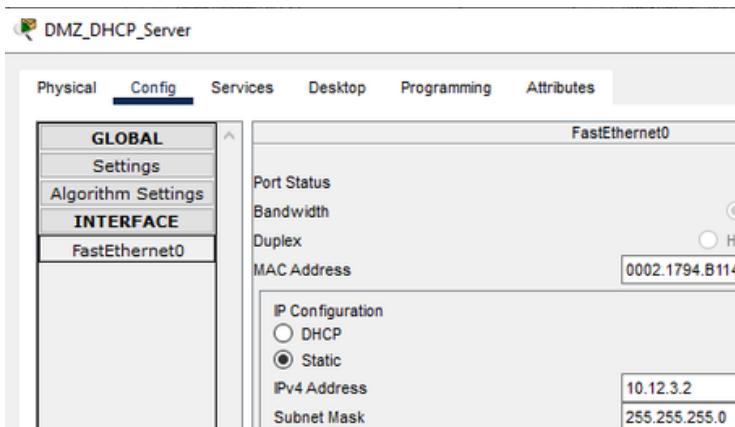
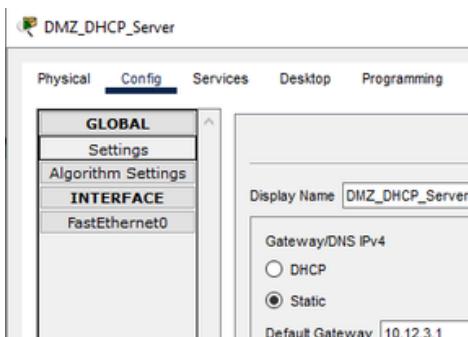
Server DNS:



Server FTP:



DMZ DHCP:



2. Configuración de Access Ports de todos los 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
>ip helper-address 10.10.3.2
>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
>ip helper-address 10.10.3.2
>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
>ip helper-address 10.10.3.2
>no shut
```

```
>enable
>conf t
>int Gi1/0/4
>description
>switchport mode Access
>Switchport access vlan 1000
```

```
>int vlan 1000
>ip address 10.10.3.1 255.255.255.0
>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 deseas.

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.

ip helper-address: Redirige paquetes de broadcast (como DHCP) hacia un servidor específico en otra red.

no shut: Habilita la interfaz, permitiendo el paso de tráfico.

Ian_GOOGLE_CORE

Physical	Config	CLI	Attributes
IOS Command Line Interface			
<pre>interface GigabitEthernet1/0/1 description Access port to Ian 10.1.3.2 port 0 switchport access vlan 100 switchport mode access ! interface GigabitEthernet1/0/2 description Access port to Ian 10.2.3.2 port 0 switchport access vlan 200 switchport mode access ! interface GigabitEthernet1/0/3 description Access port to Ian 10.3.3.2 port 0 switchport access vlan 300 switchport mode access ! interface GigabitEthernet1/0/4 description Access port to Google DHCP Server 10.10.3.2 port 0 switchport access vlan 1000 switchport mode access</pre>			

Ian_GOOGLE_CORE

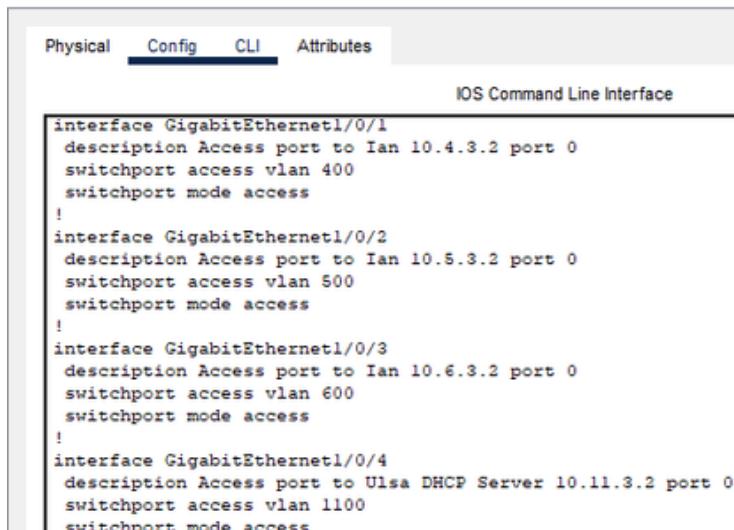
Physical	Config	CLI	Attributes
IOS Command Line Interface			
<pre>interface Vlan100 mac-address 0001.4303.be01 ip address 10.1.3.1 255.255.255.0 ip helper-address 10.10.3.2 ! interface Vlan200 mac-address 0001.4303.be02 ip address 10.2.3.1 255.255.255.0 ip helper-address 10.10.3.2 ! interface Vlan300 mac-address 0001.4303.be03 ip address 10.3.3.1 255.255.255.0 ip helper-address 10.10.3.2 ! interface Vlan1000 mac-address 0001.4303.be04 ip address 10.10.3.1 255.255.255.0</pre>			

Repetiremos este proceso en el switch de Ulsa Y DMZ:

Switch Ulsa:

```
>enable                                         >enable  
>conf t                                         >conf t  
>int Gi1/0/1                                     >int Gi1/0/2  
>description                                    >description  
>switchport mode Access                         >switchport mode Access  
>Switchport access vlan 400                      >Switchport access vlan 500  
  
>int vlan 400                                     >int vlan 500  
>ip address 10.4.3.1 255.255.255.0             >ip address 10.5.3.1 255.255.255.0  
>ip helper-address 10.11.3.2                     >ip helper-address 10.11.3.2  
    >no shut  
  
>enable                                         >enable  
>conf t                                         >conf t  
>int Gi1/0/3                                     >int Gi1/0/4  
>description                                    >description  
>switchport mode Access                         >switchport mode Access  
>Switchport access vlan 600                      >Switchport access vlan 1100  
  
>int vlan 600                                     >int vlan 1100  
>ip address 10.6.3.1 255.255.255.0            >ip address 10.11.3.1 255.255.255.0  
>ip helper-address 10.11.3.2                     >no shut  
    >no shut
```

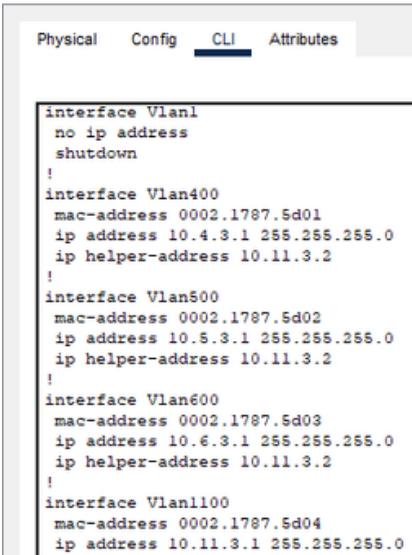
Ian_Ulsa_CORE



IOS Command Line Interface

```
interface GigabitEthernet1/0/1
description Access port to Ian 10.4.3.2 port 0
switchport access vlan 400
switchport mode access
!
interface GigabitEthernet1/0/2
description Access port to Ian 10.5.3.2 port 0
switchport access vlan 500
switchport mode access
!
interface GigabitEthernet1/0/3
description Access port to Ian 10.6.3.2 port 0
switchport access vlan 600
switchport mode access
!
interface GigabitEthernet1/0/4
description Access port to Ulsa DHCP Server 10.11.3.2 port 0
switchport access vlan 1100
switchport mode access
```

Ian_Ulsa_CORE



IOS Command Line Interface

```
interface Vlan1
no ip address
shutdown
!
interface Vlan400
mac-address 0002.1787.5d01
ip address 10.4.3.1 255.255.255.0
ip helper-address 10.11.3.2
!
interface Vlan500
mac-address 0002.1787.5d02
ip address 10.5.3.1 255.255.255.0
ip helper-address 10.11.3.2
!
interface Vlan600
mac-address 0002.1787.5d03
ip address 10.6.3.1 255.255.255.0
ip helper-address 10.11.3.2
!
interface Vlan1100
mac-address 0002.1787.5d04
ip address 10.11.3.1 255.255.255.0
```

Switch DMZ:

```
>enable
>conf t
>int Gig1/0/1
>description
>switchport mode Access
>Switchport access vlan 700

>int vlan 700
>ip address 10.7.3.1 255.255.255.0
>ip helper-address 10.12.3.2
>no shut

>enable
>conf t
>int Gig1/0/2
>description
>switchport mode Access
>Switchport access vlan 800

>int vlan 800
>ip address 10.8.3.1 255.255.255.0
>ip helper-address 10.12.3.2
>no shut

>enable
>conf t
>int Gig1/0/3
>description
>switchport mode Access
>Switchport access vlan 900

>int vlan 900
>ip address 10.9.3.1 255.255.255.0
>ip helper-address 10.12.3.2
>no shut

>enable
>conf t
>int Gig1/0/4
>description
>switchport mode Access
>Switchport access vlan 1200

>int vlan 1200
>ip address 10.12.3.1 255.255.255.0
>no shut
```

Ian_Switch_DMZ

Physical Config **CLI** Attributes

IOS Command Line Interface

```
interface GigabitEthernet1/0/1
description Access port to Ian DNS port 0
switchport access vlan 700
switchport mode access
!
interface GigabitEthernet1/0/2
description Access port to Ian FTP port 0
switchport access vlan 800
switchport mode access
!
interface GigabitEthernet1/0/3
description Access port to Ian 10.9.3.2 port 0
switchport access vlan 900
switchport mode access
!
interface GigabitEthernet1/0/4
description Access port to DMZ DHCP Server 10.12.3.2 port 0
switchport access vlan 1200
switchport mode access
```

Ian_Switch_DMZ

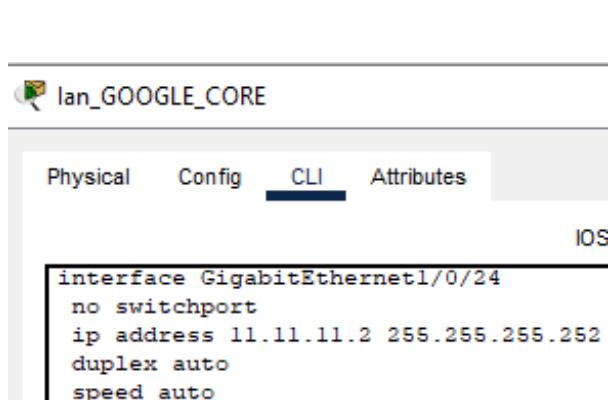
Physical Config **CLI** Attributes

```
interface Vlan700
mac-address 00d0.58ee.8e01
ip address 10.7.3.1 255.255.255.0
ip helper-address 10.12.3.2
!
interface Vlan800
mac-address 00d0.58ee.8e02
ip address 10.8.3.1 255.255.255.0
ip helper-address 10.12.3.2
!
interface Vlan900
mac-address 00d0.58ee.8e03
ip address 10.9.3.1 255.255.255.0
ip helper-address 10.12.3.2
!
interface Vlan1200
mac-address 00d0.58ee.8e04
ip address 10.12.3.1 255.255.255.0
```

3. Port EIGRP de Switches:

Switch Google:

```
>enable  
>conf t  
>int Gig1/0/24  
>description  
>No switchport  
>ip address 11.11.11.2 255.255.255.252  
    >no shut  
  
>enable  
>conf t  
>Ip routing  
>Router eigrp 100  
>Redistribute connected  
    >Network 11.11.11.1
```

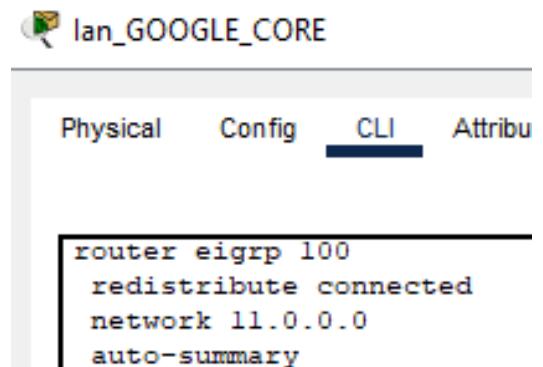


lan_GOOGLE_CORE

Physical Config CLI Attributes

IOS

```
interface GigabitEthernet1/0/24
no switchport
ip address 11.11.11.2 255.255.255.252
duplex auto
speed auto
```



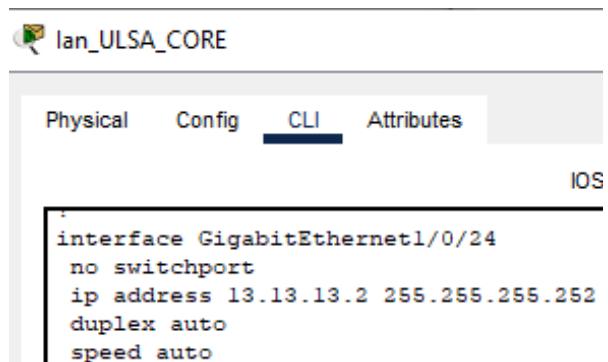
lan_GOOGLE_CORE

Physical Config CLI Attributes

```
router eigrp 100
redistribute connected
network 11.0.0.0
auto-summary
```

Switch Ulsa:

```
>enable  
>conf t  
>int Gig1/0/24  
>description  
>No switchport  
>ip address 13.13.13.2 255.255.255.252  
    >no shut  
  
>enable  
>conf t  
>Ip routing  
>Router eigrp 100  
>Redistribute connected  
    >Network 13.13.13.13
```

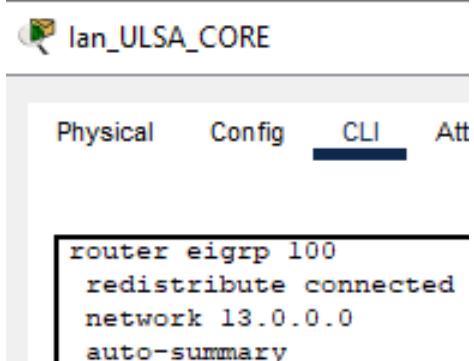


lan_ULSA_CORE

Physical Config CLI Attributes

IOS

```
interface GigabitEthernet1/0/24
no switchport
ip address 13.13.13.2 255.255.255.252
duplex auto
speed auto
```



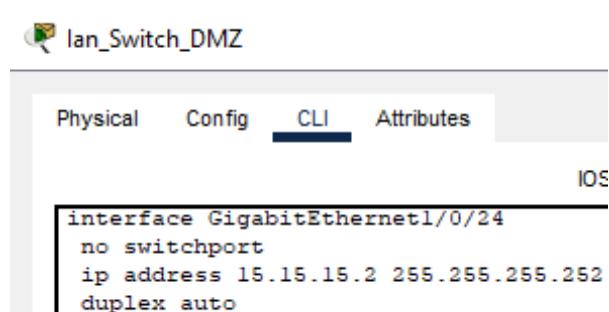
lan_ULSA_CORE

Physical Config CLI Attributes

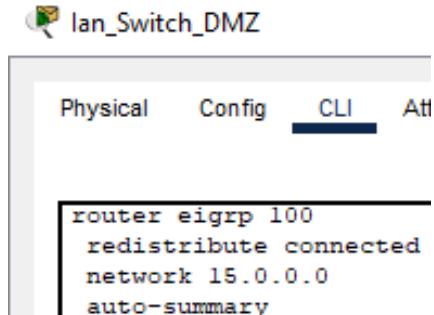
```
router eigrp 100
redistribute connected
network 13.0.0.0
auto-summary
```

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 connected  
>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 connected  
>Network 11.11.11.11  
>Network 12.12.12.12
```

```
lan_GOOGLE_Router  
Physical Config CLI Attributes  
IOS Command  
interface GigabitEthernet0/0  
description Acces port to Ian Core port 24  
ip address 11.11.11.1 255.255.255.252  
duplex auto  
speed auto  
!  
interface GigabitEthernet0/1  
description Acces port to FIREWALL port 1  
ip address 12.12.12.1 255.255.255.252  
duplex auto  
speed auto  
!  
lan_GOOGLE_Router  
Physical Config CLI Attr  
IOS Command  
router eigrp 100  
redistribute connected  
network 11.0.0.0  
network 12.0.0.0
```

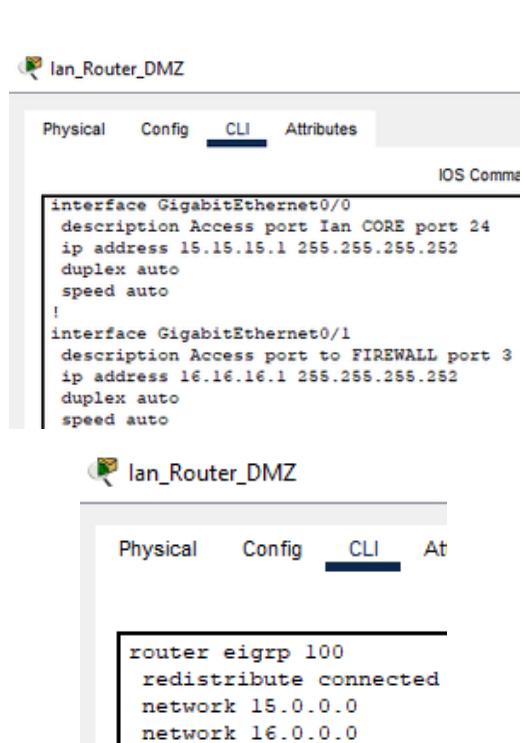
Router Ulsa:

```
>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 connected  
>Network 13.13.13.13  
>Network 14.14.14.14
```

```
lan_ULSA_Router  
Physical Config CLI Attributes  
IOS Command  
interface GigabitEthernet0/0  
description Access port to Ian Core port 24  
ip address 13.13.13.1 255.255.255.252  
duplex auto  
speed auto  
!  
interface GigabitEthernet0/1  
description Access port to FIREWALL port 2  
ip address 14.14.14.1 255.255.255.252  
duplex auto  
speed auto  
!  
lan_ULSA_Router  
Physical Config CLI Attr  
IOS Command  
router eigrp 100  
redistribute connected  
network 13.0.0.0  
network 14.0.0.0
```

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 connected  
>Network 15.15.15.15  
>Network 16.16.16.16
```



The image shows two screenshots of a Cisco IOS CLI interface. The top screenshot displays the configuration for two interfaces: GigabitEthernet0/0 and GigabitEthernet0/1. The bottom screenshot shows the configuration of a redistribute statement under the Router EIGRP 100 process.

```
lan_Router_DMZ  
Physical Config CLI Attributes  
IOS Comm  
interface GigabitEthernet0/0  
description Access port Ian CORE port 24  
ip address 15.15.15.1 255.255.255.252  
duplex auto  
speed auto  
!  
interface GigabitEthernet0/1  
description Access port to FIREWALL port 3  
ip address 16.16.16.1 255.255.255.252  
duplex auto  
speed auto  
  
lan_Router_DMZ  
Physical Config CLI At  
router eigrp 100  
redistribute connected  
network 15.0.0.0  
network 16.0.0.0
```

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.

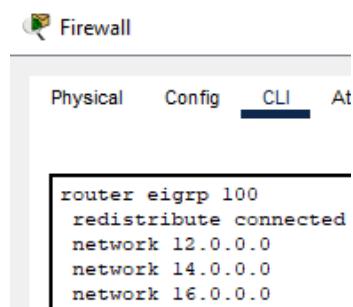
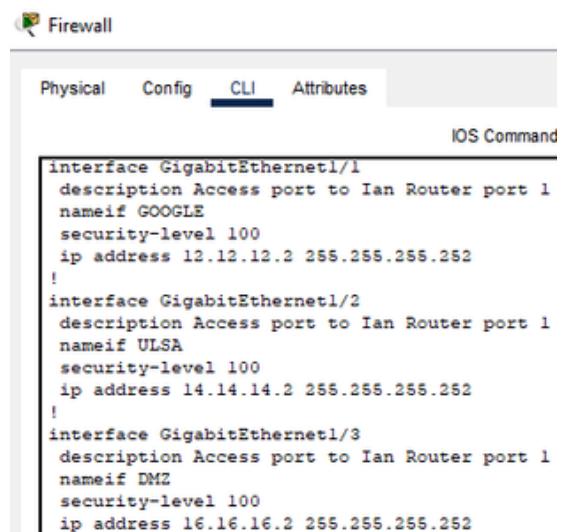
ip routing: Habilita el enrutamiento IP en el dispositivo para que pueda enrutar paquetes entre diferentes redes.

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 connected  
>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.

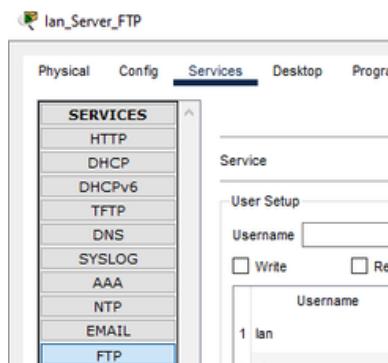
network [dirección IP de red] [wildcard mask]:

Anuncia una red en el proceso de enrutamiento.

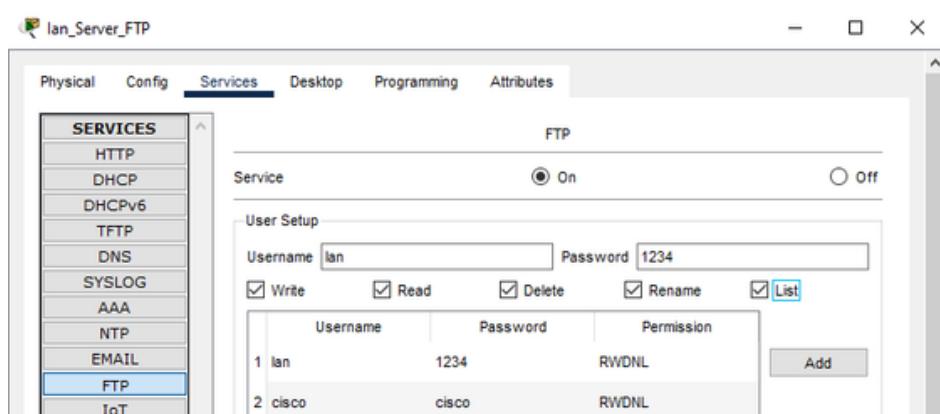
no shut: Habilita la interfaz, permitiendo el paso de tráfico.

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:

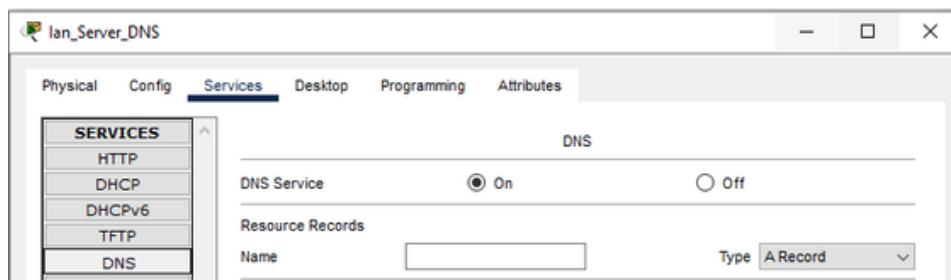


Ahí nos dirigiremos al apartado de Username, ponemos el nombre que queramos y para la password igual, seleccionamos las opciones que se ven en la captura, oprimimos el botón Add y se agregaría nuestro usuario y contraseña, la cual la usaremos más adelante para acceder al server y descargar un archivo:

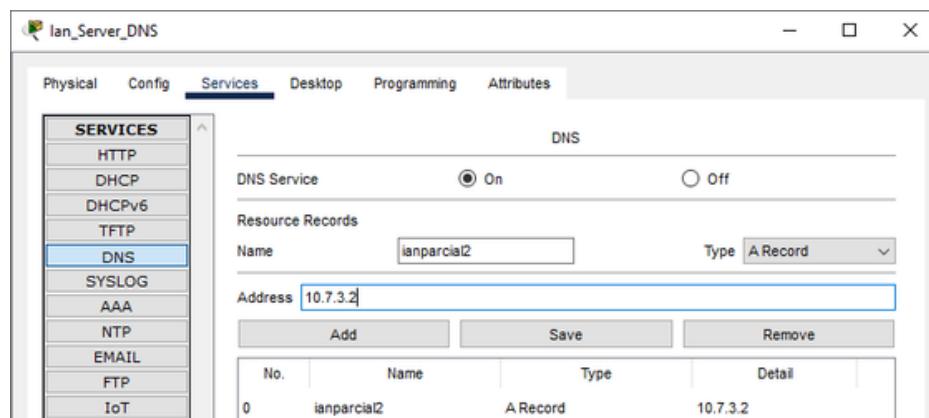


7. Configuración servicio Server DNS:

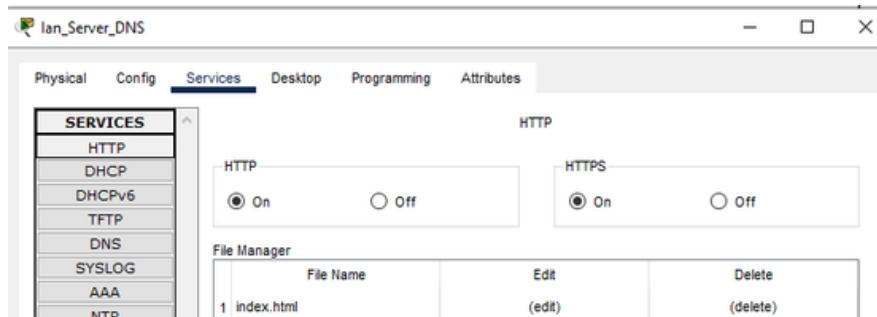
Para poder hacer la configuración correcta del Server tendremos que acceder al apartado de servicios y luego al apartado de DNS:



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

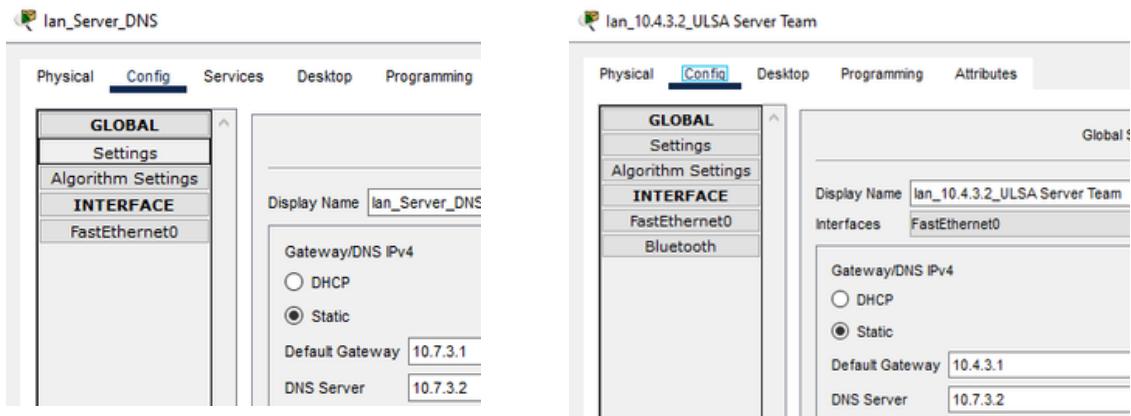


Vamos a la parte de HTTP donde con editaremos un documento index.html, esto para poner información de ejemplo y comprobar en nuestra página que puede ser visible:



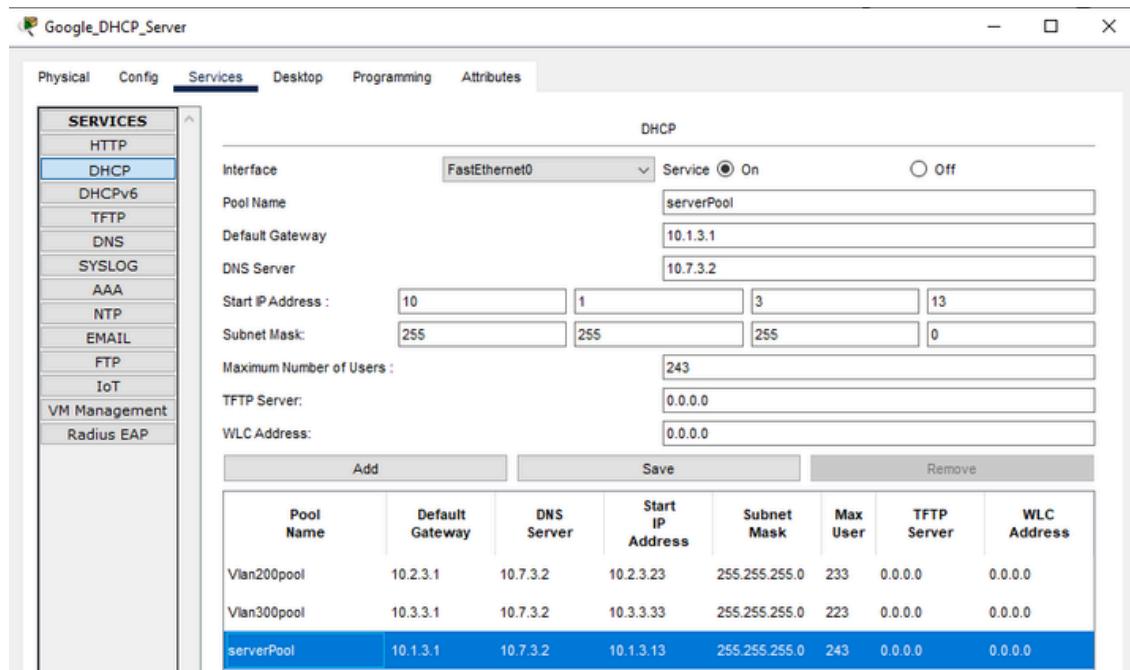
```
<html>
<h1>DATOS</h1>
<p>Nombre: Ian Alejandro Corral
Marín</p>
<p>Carrera: ITIT</p>
<p>Semestre: 5</p>
<p>Clase: Tecnología en Redes 2</p>
<p>Examen: Parcial 2</p>
</html>
```

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:



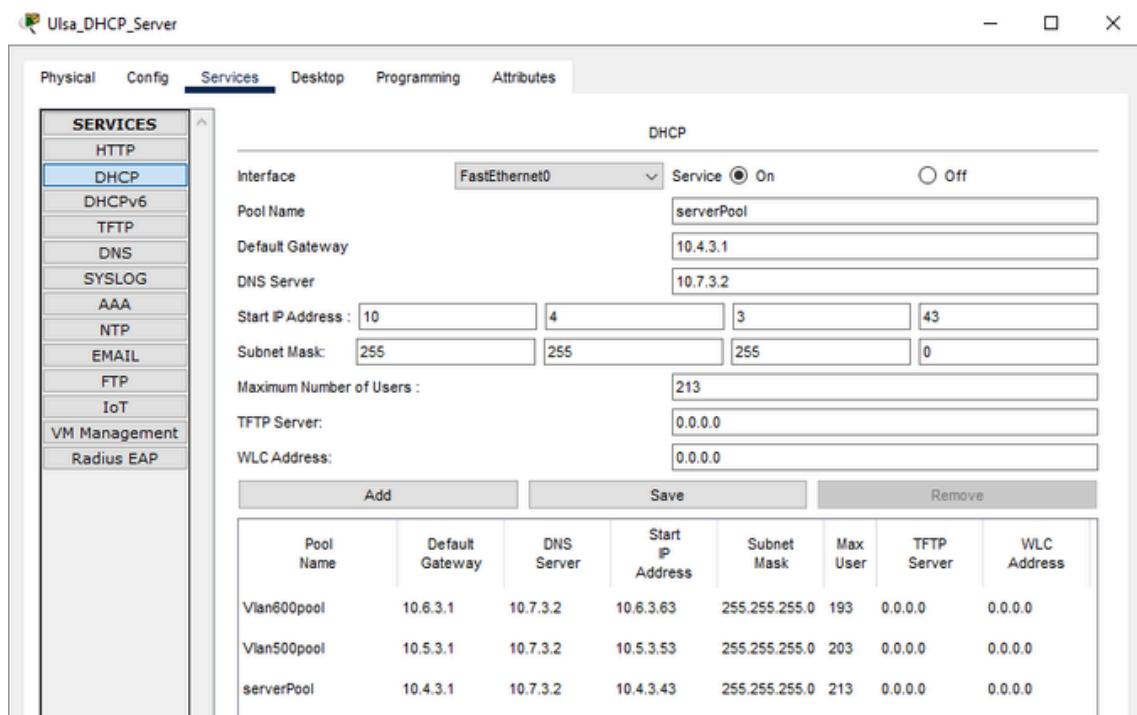
8. Configuración servicio Servers DHCP:

Nos dirigiremos nuevamente al apartado de servicios pero ahora en DHCP, aquí como podemos ver en la imagen agregaremos 3 diferentes “Pools” los cuales son conjunto de direcciones ip con un rango específico para cada vlan, las cuales se asignan automáticamente

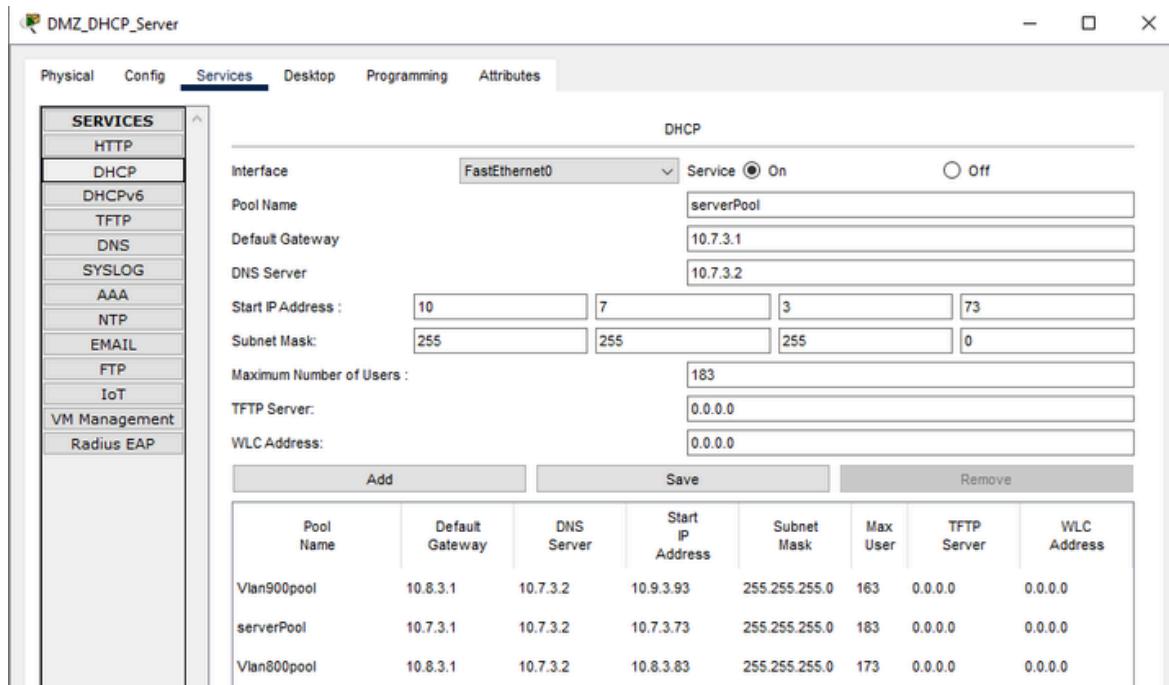


Aquí hacemos las configuraciones necesarias, DG: en el que queramos iniciar, el DNS server conectado, la ip address inicial, su subnet mask y el numero maximo de usuarios sera aplicado de forma automatica, esto para cada vlan.

ULSA DHCP:



DMZ DHCP:



9. 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 permit tcp host 10.5.3.2 host 15.15.15.2 eq telnet
>access-list ULSA extended permit tcp host 13.13.13.2 eq telnet host 10.1.3.2
                                         >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 permit tcp host 15.15.15.2 eq telnet host 10.5.3.2
                                         >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 permit tcp host 10.1.3.2 host 13.13.13.2 eq telnet
                                         >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
```

Firewall IAN

Physical Config **CLI** Attributes

IOS Command Line Interface

```
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 permit tcp host 10.5.3.2 host 15.15.15.2 eq telnet
access-list ULSA extended permit tcp host 13.13.13.2 eq telnet host 10.1.3.2
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 permit tcp host 15.15.15.2 eq telnet host 10.5.3.2
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 permit tcp host 10.1.3.2 host 13.13.13.2 eq telnet
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

HTTP (TCP): Permite tráfico web (puerto 80) desde 10.4.3.2 hacia 10.7.3.2.

DNS (UDP): Permite tráfico DNS (puerto 53) desde 10.4.3.2 hacia 10.7.3.2.

FTP (TCP): Permite tráfico FTP (puerto 21) desde 10.5.3.2 hacia 10.8.3.2.

Rango de Puertos (TCP): Permite tráfico desde 10.5.3.2 hacia 10.8.3.2 en los puertos comprendidos entre 1024 y 1100.

ICMP (Ping): Permite pings (ICMP) desde 10.6.3.2 hacia las siguientes direcciones:

11.11.11.2

10.1.3.2

10.2.3.2

10.3.3.2

Telnet (TCP): Permite acceso Telnet (puerto 23) desde 10.5.3.2 hacia 15.15.15.2.

Permite acceso Telnet desde 13.13.13.2 hacia 10.1.3.2.

Denegar Todo: Todo el tráfico IP no especificado se bloquea de manera explícita.

Access List DMZ

HTTP (TCP): Permite tráfico web (puerto 80) desde 10.7.3.2 hacia 10.4.3.2.

DNS (UDP): Permite tráfico DNS (puerto 53) desde 10.7.3.2 hacia 10.4.3.2.

FTP (TCP): Permite tráfico FTP (puerto 21) desde 10.8.3.2 hacia 10.5.3.2.

Rango de Puertos (TCP): Permite tráfico desde 10.8.3.2 hacia 10.5.3.2 en los puertos comprendidos entre 1024 y 1100.

HTTP (TCP): Permite tráfico web (puerto 80) desde 10.7.3.2 hacia las siguientes direcciones:

10.1.3.2

10.2.3.2

10.3.3.2

DNS (UDP): Permite tráfico DNS (puerto 53) desde 10.7.3.2 hacia las siguientes direcciones:

10.1.3.2

10.2.3.2

10.3.3.2

Telnet (TCP): Permite tráfico Telnet (puerto 23) desde 15.15.15.2 hacia 10.5.3.2.

Denegar Todo: Todo el tráfico IP no especificado se bloquea de manera explícita.

Access List GOOGLE

ICMP (Ping): Permite pings (ICMP) entre las siguientes direcciones:

Desde 11.11.11.2 hacia 10.6.3.2.

Desde 10.1.3.2, 10.2.3.2 y 10.3.3.2 hacia 10.6.3.2.

HTTP (TCP): Permite tráfico web (puerto 80) desde:

10.1.3.2, 10.2.3.2 y 10.3.3.2 hacia 10.7.3.2.

DNS (UDP): Permite tráfico DNS (puerto 53) desde:

10.1.3.2, 10.2.3.2 y 10.3.3.2 hacia 10.7.3.2.

Telnet (TCP): Permite tráfico Telnet (puerto 23) desde 10.1.3.2 hacia 13.13.13.2.

Denegar Todo: Todo el tráfico IP no especificado se bloquea de manera explícita.

Aplicación de las Listas de Acceso

ULSA: Aplicada en la interfaz ULSA como lista de control de acceso entrante.

GOOGLE: Aplicada en la interfaz GOOGLE como lista de control de acceso entrante.

DMZ: Aplicada en la interfaz DMZ como lista de control de acceso entrante.

10. Show ip Route de todos los switches:

Switch GOOGLE:

```

Ian_GOOGLE_CORE#sh 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       10.1.3.0 is directly connected, Vlan100
C       10.2.3.0 is directly connected, Vlan200
C       10.3.3.0 is directly connected, Vlan300
D EX    10.4.3.0 [170/256026624] via 11.11.11.1, 02:45:13, GigabitEthernet1/0/24
D EX    10.5.3.0 [170/256026624] via 11.11.11.1, 02:45:13, GigabitEthernet1/0/24
D EX    10.6.3.0 [170/256026624] via 11.11.11.1, 02:45:13, GigabitEthernet1/0/24
D EX    10.7.3.0 [170/256026624] via 11.11.11.1, 02:45:13, GigabitEthernet1/0/24
D EX    10.8.3.0 [170/256026624] via 11.11.11.1, 02:45:13, GigabitEthernet1/0/24
D EX    10.9.3.0 [170/256026624] via 11.11.11.1, 02:45:13, GigabitEthernet1/0/24
C       10.10.3.0 is directly connected, Vlan1000
D EX    10.11.3.0 [170/256026624] via 11.11.11.1, 02:45:13, GigabitEthernet1/0/24
D EX    10.12.3.0 [170/256026624] via 11.11.11.1, 02:45:13, 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, 02:45:13, GigabitEthernet1/0/24
      13.0.0.0/30 is subnetted, 1 subnets
D       13.13.13.0 [90/3584] via 11.11.11.1, 02:45:13, GigabitEthernet1/0/24
      14.0.0.0/30 is subnetted, 1 subnets
D       14.14.14.0 [90/3328] via 11.11.11.1, 02:45:13, GigabitEthernet1/0/24
      15.0.0.0/30 is subnetted, 1 subnets
D       15.15.15.0 [90/3584] via 11.11.11.1, 02:45:13, GigabitEthernet1/0/24
      16.0.0.0/30 is subnetted, 1 subnets
D       16.16.16.0 [90/3328] via 11.11.11.1, 02:45:13, GigabitEthernet1/0/24

```

Redes C:

Directamente conectadas al router por interfaces físicas (e.g., VLAN o GigabitEthernet).

Redes: 10.1.3.0/24, 10.2.3.0/24, 10.3.3.0/24, 10.10.3.0/24, 11.0.0.0/30, 11.0.0.4/30, 11.0.0.8/30.

Redes D EX:

Aprendidas por EIGRP externo, redistribuidas desde otro protocolo o router.

Redes: 10.9.3.0/24, 10.4.3.0/24, 10.5.3.0/24, 10.6.3.0/24, 16.0.0.0/8.

Switch ULSA:

```

Ian_ULSA_CORE#SH 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  10.1.3.0 [170/256026624] via 13.13.13.1, 02:51:15, GigabitEthernet1/0/24
D EX  10.2.3.0 [170/256026624] via 13.13.13.1, 02:51:15, GigabitEthernet1/0/24
D EX  10.3.3.0 [170/256026624] via 13.13.13.1, 02:51:15, GigabitEthernet1/0/24
C   10.4.3.0 is directly connected, Vlan400
C   10.5.3.0 is directly connected, Vlan500
C   10.6.3.0 is directly connected, Vlan600
D EX  10.7.3.0 [170/256026624] via 13.13.13.1, 02:51:15, GigabitEthernet1/0/24
D EX  10.8.3.0 [170/256026624] via 13.13.13.1, 02:51:15, GigabitEthernet1/0/24
D EX  10.9.3.0 [170/256026624] via 13.13.13.1, 02:51:15, GigabitEthernet1/0/24
D EX  10.10.3.0 [170/256026624] via 13.13.13.1, 02:51:15, GigabitEthernet1/0/24
C   10.11.3.0 is directly connected, Vlan1100
D EX  10.12.3.0 [170/256026624] via 13.13.13.1, 02:51:15, GigabitEthernet1/0/24
    11.0.0.0/30 is subnetted, 1 subnets
D   11.11.11.0 [90/3584] via 13.13.13.1, 02:51:15, GigabitEthernet1/0/24
    12.0.0.0/30 is subnetted, 1 subnets
D   12.12.12.0 [90/3328] via 13.13.13.1, 02:51:15, 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, 02:51:15, GigabitEthernet1/0/24
    15.0.0.0/30 is subnetted, 1 subnets
D   15.15.15.0 [90/3584] via 13.13.13.1, 02:51:15, GigabitEthernet1/0/24
    16.0.0.0/30 is subnetted, 1 subnets
D   16.16.16.0 [90/3328] via 13.13.13.1, 02:51:15, GigabitEthernet1/0/24

```

Redes C:

Directamente conectadas al router por interfaces físicas (e.g., VLAN o GigabitEthernet).

Redes: 10.4.3.0/24, 10.5.3.0/24, 10.9.3.0/24.

Redes D EX:

Aprendidas por EIGRP externo, redistribuidas desde otro protocolo o router.

Redes: 10.1.3.0/24, 10.2.3.0/24, 10.3.3.0/24, 11.0.0.0/30, 12.0.0.0/30, 14.14.14.0/30, 16.16.16.0/16.

Switch DMZ:

```

Ian_Switch_DMZ#SH 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  10.1.3.0 [170/256026624] via 15.15.15.1, 02:51:26, GigabitEthernet1/0/24
D EX  10.2.3.0 [170/256026624] via 15.15.15.1, 02:51:26, GigabitEthernet1/0/24
D EX  10.3.3.0 [170/256026624] via 15.15.15.1, 02:51:26, GigabitEthernet1/0/24
D EX  10.4.3.0 [170/256026624] via 15.15.15.1, 02:51:26, GigabitEthernet1/0/24
D EX  10.5.3.0 [170/256026624] via 15.15.15.1, 02:51:26, GigabitEthernet1/0/24
D EX  10.6.3.0 [170/256026624] via 15.15.15.1, 02:51:26, GigabitEthernet1/0/24
C  10.7.3.0 is directly connected, Vlan700
C  10.8.3.0 is directly connected, Vlan800
C  10.9.3.0 is directly connected, Vlan900
D EX  10.10.3.0 [170/256026624] via 15.15.15.1, 02:51:26, GigabitEthernet1/0/24
D EX  10.11.3.0 [170/256026624] via 15.15.15.1, 02:51:26, GigabitEthernet1/0/24
C  10.12.3.0 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, 02:51:26, GigabitEthernet1/0/24
12.0.0.0/30 is subnetted, 1 subnets
D  12.12.12.0 [90/3328] via 15.15.15.1, 02:51:26, GigabitEthernet1/0/24
13.0.0.0/30 is subnetted, 1 subnets
D  13.13.13.0 [90/3584] via 15.15.15.1, 02:51:26, GigabitEthernet1/0/24
14.0.0.0/30 is subnetted, 1 subnets
D  14.14.14.0 [90/3328] via 15.15.15.1, 02:51:26, 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, 02:51:26, GigabitEthernet1/0/24

```

Redes C:

Directamente conectadas al router por interfaces físicas (e.g., VLAN o GigabitEthernet).

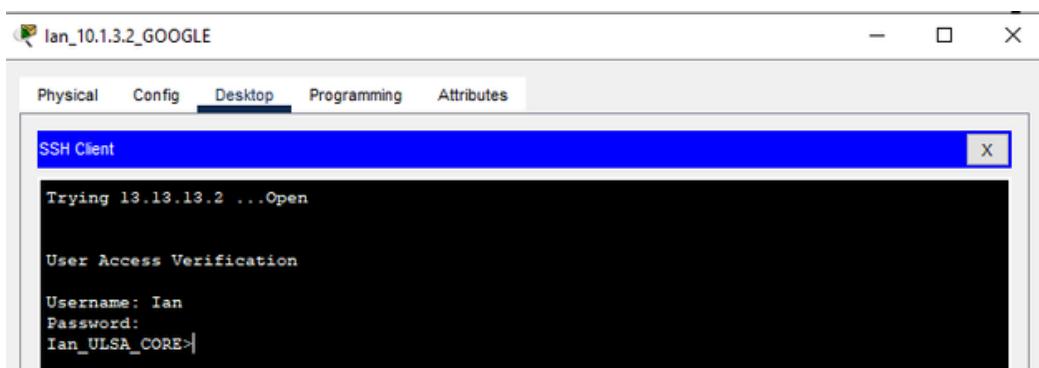
Redes: 10.7.3.0/24, 10.8.3.0/24, 10.9.3.0/24.

Redes D EX:

Aprendidas por EIGRP externo, redistribuidas desde otro protocolo o router.

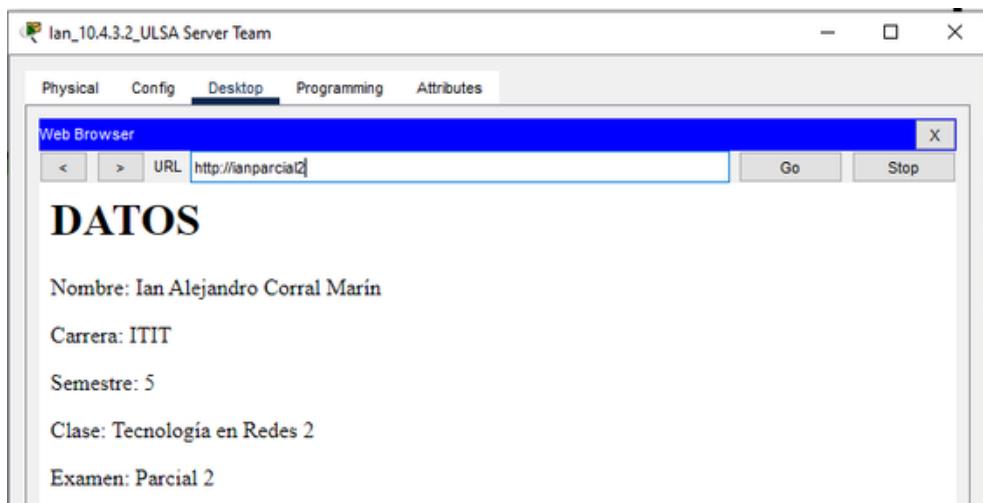
Redes: 10.1.3.0/24, 10.2.3.0/24, 10.3.3.0/24, 11.0.0.0/30, 12.0.0.0/30, 14.14.14.0/30, 16.16.16.0/16.

11. PC GOOGLE 1 accesando a Switch ULSA por Telnet:

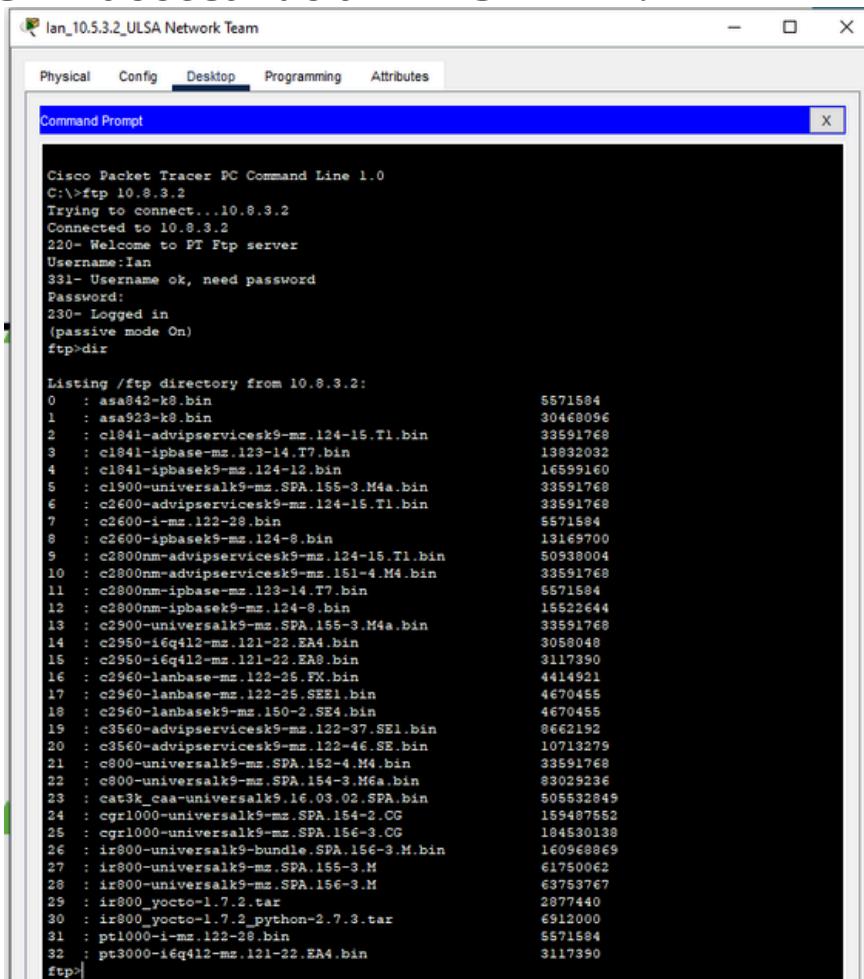


3D PRINTING FOR SAFETY

12. PC ULSA 1 accediendo a página web desde el DNS WEB SERVER:



13. PC ULSA 2 accedendo a FTP SERVER:



MANUAL PACKET TRACER

14. Nueve ips obtenidas por Servers

DHCP:

GOOGLE:

lan_10.1.3.2_GOOGLE

Physical Config Desktop Programming Attributes

Command Prompt

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::20A:F3FF:FE17:CD04
IPv6 Address.....: :::
IPv4 Address.....: 10.1.3.14
Subnet Mask.....: 255.255.255.0
Default Gateway.....: :::
                           10.1.3.1

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
```

lan_10.2.3.2_GOOGLE

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::20C:CFEE:FE56:5E95
IPv6 Address.....: :::
IPv4 Address.....: 10.2.3.24
Subnet Mask.....: 255.255.255.0
Default Gateway.....: :::
                           10.2.3.1

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
```

lan_10.3.3.2_GOOGLE

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::2E0:8FFF:FEBA:D8D2
IPv6 Address.....: :::
IPv4 Address.....: 10.3.3.34
Subnet Mask.....: 255.255.255.0
Default Gateway.....: :::
                           10.3.3.1

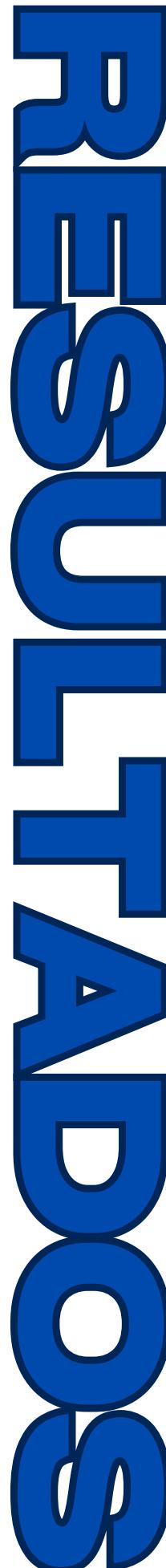
Bluetooth Connection:

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
```

MANUAL PACKET TRACER

MANUAL
PACKET
TRACER

ULSA:



lan_10.4.3.2_ULSA Server Team

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::260:47FF:FE0B:6784
IPv6 Address.....: :::
IPv4 Address.....: 10.4.3.44
Subnet Mask.....: 255.255.255.0
Default Gateway.....: :::
10.4.3.1

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
```

lan_10.5.3.2_ULSA Network Team

Physical Config Desktop Programming Attributes

Command Prompt

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::20C:CFFF:FE94:4356
IPv6 Address.....: :::
IPv4 Address.....: 10.5.3.53
Subnet Mask.....: 255.255.255.0
Default Gateway.....: :::
10.5.3.1

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
```

lan_10.6.3.2_ULSA Users

Physical Config Desktop Programming Attributes

Command Prompt

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

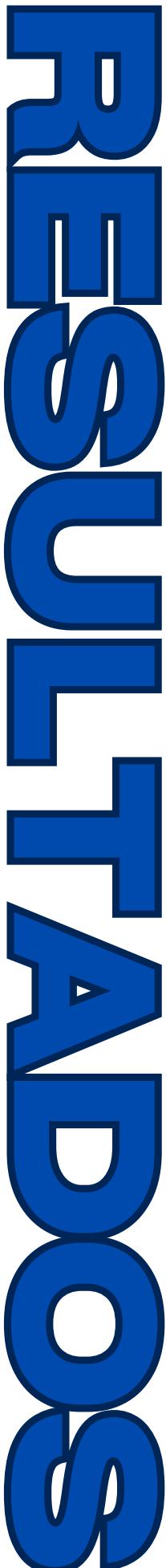
FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::206:2AFF:FE01:E03A
IPv6 Address.....: :::
IPv4 Address.....: 10.6.3.63
Subnet Mask.....: 255.255.255.0
Default Gateway.....: :::
10.6.3.1

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
```

DMZ:



lan_Server_DNS

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::2D0:D3FF:FE96:7144
IPv6 Address.....: :::
IPv4 Address.....: 10.7.3.73
Subnet Mask.....: 255.255.255.0
Default Gateway.....: :::
10.7.3.1
```

lan_Server_FTP

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:FE42:5836
IPv6 Address.....: :::
IPv4 Address.....: 10.8.3.83
Subnet Mask.....: 255.255.255.0
Default Gateway.....: :::
10.8.3.1
```

lan_10.9.3.2_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::2E0:F7FF:FE94:C3E2
IPv6 Address.....: :::
IPv4 Address.....: 10.9.3.93
Subnet Mask.....: 255.255.255.0
Default Gateway.....: :::
10.8.3.1

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
```

JO
M
G
E
C
H
A
D
O
@

15. Show access-list del

Firewall:

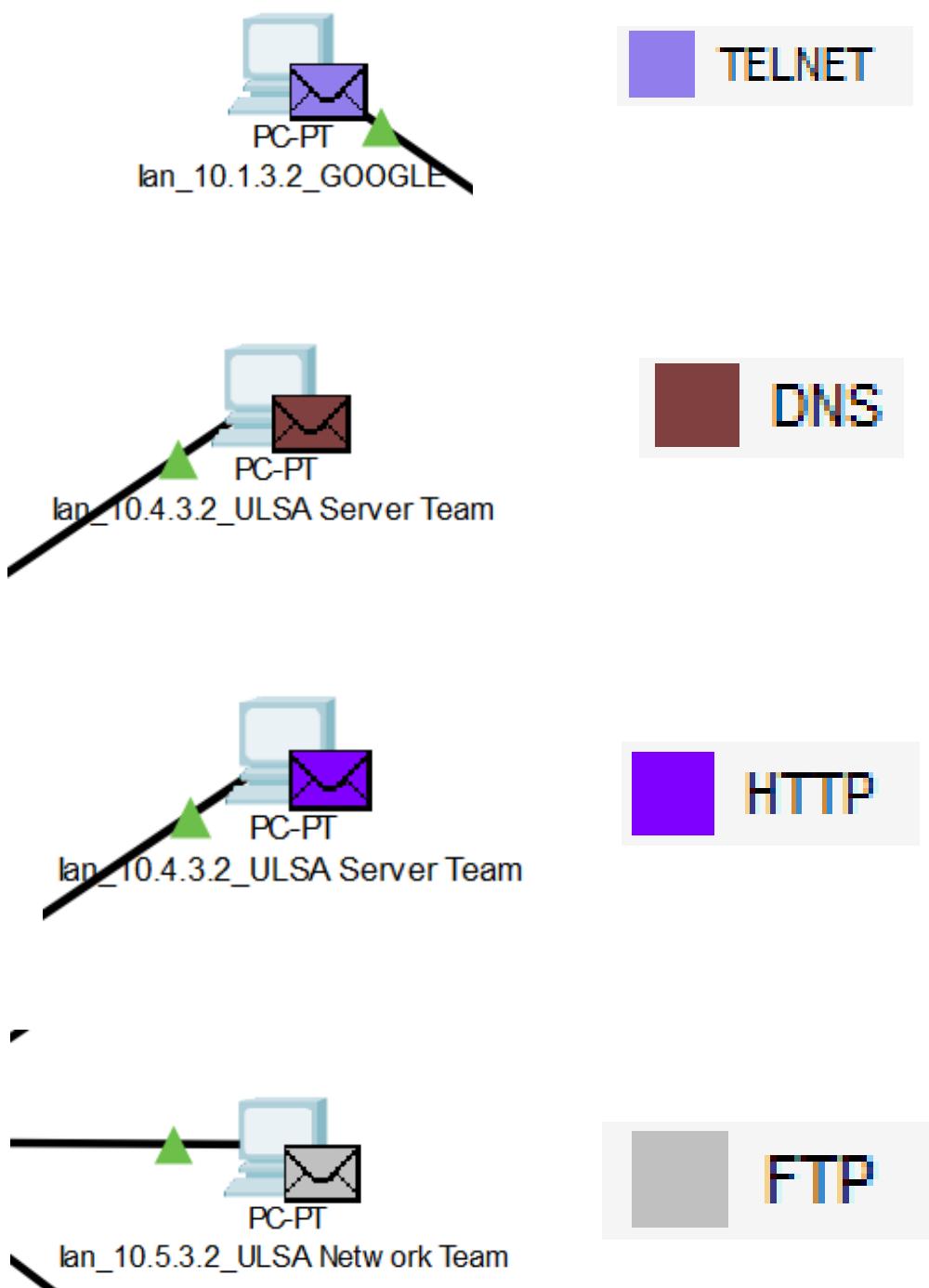
Firewall IAN

Physical Config CLI Attributes

IOS Command Line Interface

```
firewall#sh access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval 300
access-list ULSA; 11 elements; name hash: 0x495a42a0
access-list ULSA line 1 extended permit tcp host 10.4.3.2 host 10.7.3.2 eq www(hitcnt=1) 0xa547cadc
access-list ULSA line 2 extended permit udp host 10.4.3.2 host 10.7.3.2 eq domain(hitcnt=3) 0x7666156c
access-list ULSA line 3 extended permit tcp host 10.5.3.2 host 10.8.3.2 eq ftp(hitcnt=2) 0x532c14b1
access-list ULSA line 4 extended permit tcp host 10.5.3.2 host 10.8.3.2 range 1024 1100(hitcnt=1) 0x41cd0a02b
access-list ULSA line 5 extended permit icmp host 10.6.3.2 host 11.11.11.2(hitcnt=0) 0xe9775444
access-list ULSA line 6 extended permit icmp host 10.6.3.2 host 10.1.3.2(hitcnt=0) 0xd6ee2ceb
access-list ULSA line 7 extended permit icmp host 10.6.3.2 host 10.2.3.2(hitcnt=0) 0xd1e7d6dd
access-list ULSA line 8 extended permit icmp host 10.6.3.2 host 10.3.3.2(hitcnt=0) 0xb2221d27
access-list ULSA line 9 extended permit tcp host 10.5.3.2 host 15.15.15.2 eq telnet(hitcnt=0) 0xb05a3aea
access-list ULSA line 10 extended permit tcp host 13.13.13.2 eq telnet host 10.1.3.2(hitcnt=2) 0x4eac001d
access-list ULSA line 11 extended deny ip any any(hitcnt=0) 0xcb9a2be4
access-list DMZ; 12 elements; name hash: 0xe6d7b8ab
access-list DMZ line 1 extended permit tcp host 10.7.3.2 eq www host 10.4.3.2(hitcnt=1) 0xd4da8e53
access-list DMZ line 2 extended permit udp host 10.7.3.2 eq domain host 10.4.3.2(hitcnt=1) 0x37a4e74e
access-list DMZ line 3 extended permit tcp host 10.8.3.2 eq ftp host 10.5.3.2(hitcnt=1) 0x40e7d06c
access-list DMZ line 4 extended permit tcp host 10.8.3.2 range 1024 1100 host 10.5.3.2(hitcnt=1) 0xa820961e
access-list DMZ line 5 extended permit tcp host 10.7.3.2 eq www host 10.1.3.2(hitcnt=0) 0x88d6d992
access-list DMZ line 6 extended permit tcp host 10.7.3.2 eq www host 10.2.3.2(hitcnt=0) 0x1781b23b
access-list DMZ line 7 extended permit tcp host 10.7.3.2 eq www host 10.3.3.2(hitcnt=0) 0x67ad9688
access-list DMZ line 8 extended permit udp host 10.7.3.2 eq domain host 10.1.3.2(hitcnt=0) 0xc11a2601
access-list DMZ line 9 extended permit udp host 10.7.3.2 eq domain host 10.2.3.2(hitcnt=0) 0xdb808dea
access-list DMZ line 10 extended permit udp host 10.7.3.2 eq domain host 10.3.3.2(hitcnt=0) 0xa08bd6e8
access-list DMZ line 11 extended permit tcp host 15.15.15.2 eq telnet host 10.5.3.2(hitcnt=0) 0x34b5411b
access-list DMZ line 12 extended deny ip any any(hitcnt=0) 0xa93ca3d6
access-list GOOGLE; 12 elements; name hash: 0x02054035
access-list GOOGLE line 1 extended permit icmp host 11.11.11.2 host 10.6.3.2(hitcnt=0) 0xc18aa337
access-list GOOGLE line 2 extended permit icmp host 10.1.3.2 host 10.6.3.2(hitcnt=0) 0x25c70bd8
access-list GOOGLE line 3 extended permit icmp host 10.2.3.2 host 10.6.3.2(hitcnt=0) 0xc14adb1
access-list GOOGLE line 4 extended permit icmp host 10.3.3.2 host 10.6.3.2(hitcnt=0) 0xa80acd9
access-list GOOGLE line 5 extended permit tcp host 10.1.3.2 host 10.7.3.2 eq www(hitcnt=0) 0x66b629ca
access-list GOOGLE line 6 extended permit tcp host 10.2.3.2 host 10.7.3.2 eq www(hitcnt=0) 0x91a0d83c
access-list GOOGLE line 7 extended permit tcp host 10.3.3.2 host 10.7.3.2 eq www(hitcnt=0) 0x166156aa
access-list GOOGLE line 8 extended permit udp host 10.1.3.2 host 10.7.3.2 eq domain(hitcnt=0) 0x23b9d189
access-list GOOGLE line 9 extended permit udp host 10.2.3.2 host 10.7.3.2 eq domain(hitcnt=0) 0xa04258cb
access-list GOOGLE line 10 extended permit udp host 10.3.3.2 host 10.7.3.2 eq domain(hitcnt=0) 0x7ba74137
access-list GOOGLE line 11 extended permit tcp host 10.1.3.2 host 13.13.13.2 eq telnet(hitcnt=2) 0x275d1878
access-list GOOGLE line 12 extended deny ip any any(hitcnt=0) 0xba649718
```

16. Simulación de todos los paquetes viajando:



CONEXIÓN

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, ULSA y la DMZ, 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 y una conectividad robusta.

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

Se incorpora además un servidor DHCP que automatiza la asignación de direcciones IP dentro de las VLANs, simplificando la administración de la red y asegurando que cada dispositivo reciba una configuración válida. Este servidor está configurado para gestionar rangos específicos de direcciones IP por cada segmento de la red, optimizando el uso de recursos y reduciendo el riesgo de conflictos.

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

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, automatizando la gestión de direcciones IP con DHCP y protegiendo el tráfico entre sus segmentos mediante un firewall.