

PROYECTO INTEGRADOR

VARGAS MILLAN SAMUEL DAVID

DAZA DELGADILLO SEBASTIÁN

ALVARADO LEANDRO HAROLD RICARDO

CELIS GUTIERREZ CRISTIAN JESUS

UNIVERSIDAD PEDAGÓGICA Y TECNOLÓGICA DE COLOMBIA

FACULTAD DE INGENIERÍA

INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

TUNJA (COLOMBIA)

2024

## TABLA DE CONTENIDOS

<b>TABLA DE CONTENIDOS</b>	<b>2</b>
<b>1. Conocimiento previo y por adquirir</b>	<b>3</b>
<b>Selección del tema y planteamiento de la pregunta guía.</b>	<b>3</b>
Selección del Tema:	3
<b>Figura 1. Topología de red a realizar</b>	<b>4</b>
Pregunta Problema	4
<b>Formación de Equipo de colaborativos</b>	<b>4</b>
<b>Definición de Reto Principal</b>	<b>4</b>
Planificación	5
<b>Búsqueda y Recopilación de la Información</b>	<b>5</b>
Instalación y configuración de DHCP en ubuntu server.	5
Configuración de servidor isc-dhcp-server:	7
Instalación y configuración de WEB en ubuntu server.	7
Guía Básica para Instalación y Configuración de un Servidor Web en Ubuntu Server	7
Guía configuración servidor SSH	10
Configuración de servicios de red en entornos linux.	14
Configuración de la Red en Linux	14
Servicios de Red Comunes	15
a) Servidor DHCP	15
b) Servidor DNS	15
c) Servidor Web	15
d) Servidor de Archivos	15
e) Servidor SSH	15
f) Servidor de Correo	15
g) Servidor VPN	16
h) Servidor Proxy	16
Seguridad y Gestión de Servicios	16
Automatización y Gestión Avanzada	16
<b>Práctica con AP y Router</b>	<b>17</b>
Router:	17
AP Aerohive:	21
<b>Análisis y Síntesis</b>	<b>27</b>
1. Servidor DHCP (Dynamic Host Configuration Protocol)	27
2. Servidor WEB (Nginx)	27
3. Servidor DNS (Inferido de la sección 5.4)	28
4. Acceso Remoto Seguro (SSH)	28
5. Gestión General de Servicios	29
<b>Referencias</b>	<b>30</b>

## 1. Conocimiento previo y por adquirir

Conocimiento previo	Conocimiento por adquirir
<ul style="list-style-type: none"><li>• Conocimiento básico de comandos de terminal de linux.</li><li>• Direccionamiento IPv4</li><li>• Protocolos de red</li><li>• Topologías de red</li><li>• Desarrollo web básico</li><li>• Conocimientos en conectividad de redes básico.</li><li>• Manejo de switch para configurar adecuadamente la conectividad de red entre los dispositivos.</li><li>• Funcionamiento de DNS, DHCP y HTTP</li><li>• Instalación de un sistema operativo en hardware físico</li></ul>	<ul style="list-style-type: none"><li>• Instalación y configuración de DHCP.</li><li>• Instalación y configuración de WEB.</li><li>• Funcionamiento de un servidor web, como Apache o Nginx.</li><li>• Configuración del acceso remoto seguro al servidor utilizando el protocolo SSH.</li><li>• Gestión de procesos y servicios en Linux</li><li>• Configuración de servicios de red en entornos linux</li><li>• Configuración Access Point (AP)</li><li>• Direccionamiento IPV6</li></ul>

### Selección del tema y planteamiento de la pregunta guía.

#### Selección del Tema:

El proyecto se desarrollará en dos fases distintas. En la primera etapa, se instalará Ubuntu Server en un servidor proporcionado por la universidad, seguido de la configuración del acceso remoto seguro a través del servicio SSH. La segunda fase se enfocará en la instalación y configuración de servidores, los cuales se implementarán utilizando máquinas virtuales. Estos servidores proporcionarán servicios de DHCP, DNS y WEB. Esta fase incluirá tanto la instalación del sistema operativo Ubuntu Server como la configuración de la infraestructura de red necesaria. Además, se llevarán a cabo pruebas en los equipos de los clientes para asegurar el correcto funcionamiento de los servicios implementados. Para la correcta conexión de los servicios, se tendrá en cuenta la siguiente topología:

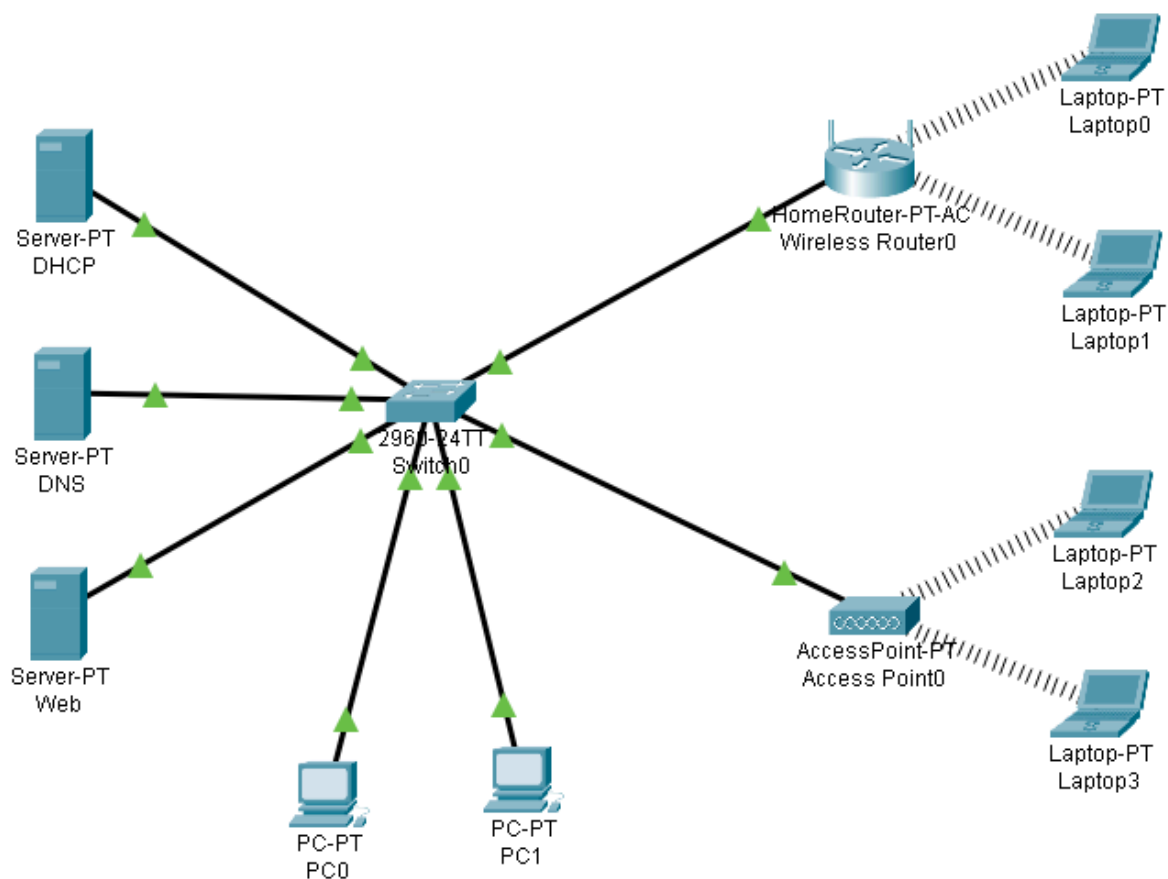


Figura 1. Topología de red a realizar

### Pregunta Problema

¿Cómo se puede diseñar e implementar una infraestructura de red básica utilizando servidores Ubuntu, que incluya la configuración de servidores DHCP y WEB, con el objetivo de hospedar y servir una página web básica?

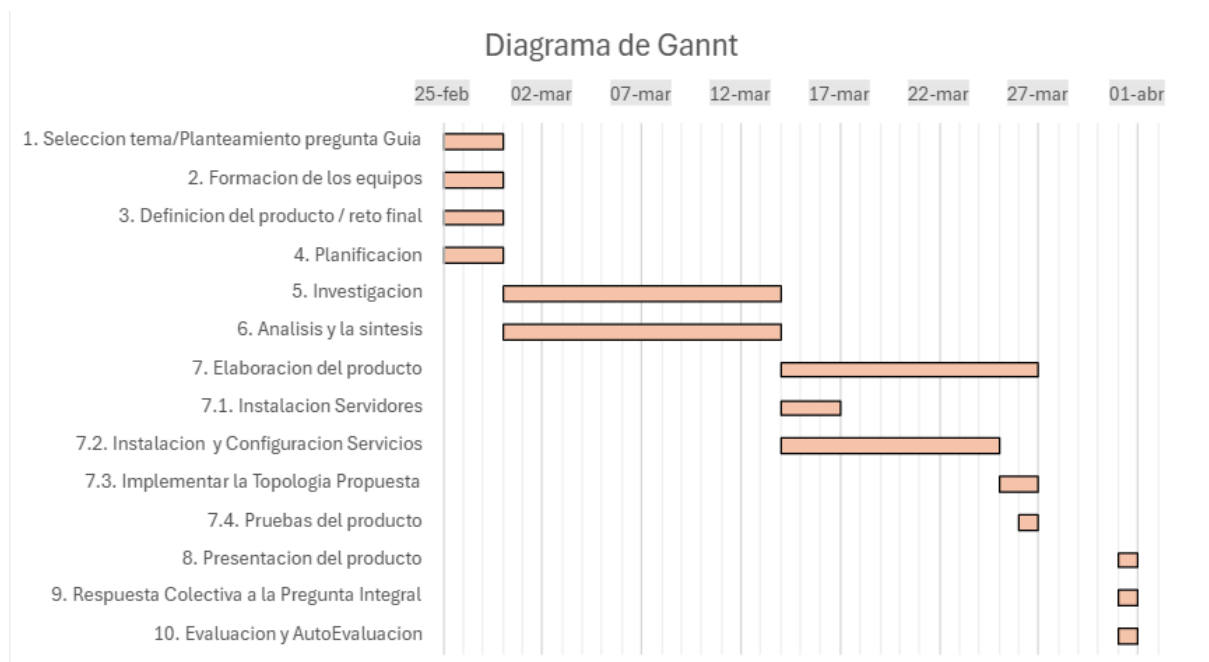
### Formación de Equipo de colaborativos

Harold Ricardo Alvarado Leandro  
 Sebastian Daza Delgadillo  
 Samuel David Vargas Millan  
 Cristian Jesus Celis Gutierrez

### Definición de Reto Principal

## Planificación

Nombre Actividad	Duracion En Horas	Responsable/s
1. Selecccion tema/Planteamiento pregunta Guia	2	Harold Alvarado
2. Formacion de los equipos	1	Cristian Celis
3. Definicion del producto / reto final	2	Sebastian Daza
4. Planificacion	1	Samuel Vargas
5. Investigacion	6	Harold Alvarado/Cristian Celis
6. Analisis y la sintesis	6	Samuel Vargas/Sebastian Daza
7. Elaboracion del producto	12	Harold Alvarado
7.1. Instalacion Servidores	2	Samuel Vargas
7.2. Instalacion y Configuracion Servicios	8	Harold Alvarado
7.3. Implementar la Topologia Propuesta	1	Cristian Celis
7.4. Pruebas del producto	1	Sebastian Daza
8. Presentacion del producto	3	Samuel Vargas
9. Respuesta Colectiva a la Pregunta Integral	1	Cristian Celis
10. Evaluacion y AutoEvaluacion	1	Sebastian Daza



## Búsqueda y Recopilación de la Información

### Instalación y configuración de DHCP en ubuntu server.

El Protocolo de Configuración Dinámica de Host (DHCP) permite asignar automáticamente direcciones IP y otros parámetros de configuración de red a dispositivos en una red.

La configuración común proporcionada por un servidor DHCP incluyen:

- Dirección IP y enmascaramiento de red

- Dirección IP de la pasarela por defecto al uso
- Direcciones IP de los servidores DNS a utilizar

Un servidor DHCP puede proporcionar ajustes de configuración utilizando los siguientes métodos:

**Asignación manual (dirección MAC):** Este método utiliza DHCP para identificar la dirección de hardware única de cada tarjeta de red conectada a la red, y luego suministra una configuración estática cada vez que el cliente DHCP hace una solicitud al servidor DHCP usando este dispositivo de red. Esto garantiza que una dirección en particular se asigne automáticamente a esa tarjeta de red, en función de su dirección MAC.

**Asignación dinámica (piscina de dirección):** En este método, el servidor DHCP asigna una dirección IP desde un grupo de direcciones (a veces también llamada rango o alcance) por un período de tiempo (conocido como un arrendamiento) configurado en el servidor, o hasta que el cliente informe al servidor que ya no necesita la dirección. De esta manera, los clientes reciben sus propiedades de configuración de forma dinámica y en un primer curso, primero servido. Cuando un cliente de DHCP ya no está en la red durante un período especificado, la configuración se expira y se vuelve a lanzar al fondo de direcciones para su uso por otros clientes de DHCP. Una vez que expire el período de arrendamiento, el cliente debe renegociar el contrato de arrendamiento con el servidor para mantener el uso de la misma dirección.

**Asignación automática:** Utilizando este método, el DHCP asigna automáticamente una dirección IP permanentemente a un dispositivo, persiguiéndola de un grupo de direcciones disponibles. Por lo general, DHCP se utiliza para asignar una dirección temporal a un cliente, pero un servidor DHCP puede permitir un tiempo de arrendamiento infinito.

Los dos últimos métodos se pueden considerar automáticos porque en cada caso el servidor DHCP asigna una dirección sin necesidad de intervención adicional. La única diferencia entre ellos es en cuánto tiempo se alquila la dirección IP; en otras palabras, si una dirección cliente varía con el tiempo.

**Servidores disponibles:** Ubuntu hace que dos servidores DHCP estén disponibles.

- isc-dhcp-server: Este servidor instala dhcpcd, el protocolo de configuración del host dinámico de demonio. Aunque Ubuntu aún apoya isc-dhcp-server, este software ya no es compatible con su proveedor.

- isc-kea: Kea fue creada por ISC (Internet Systems Consortium), para reemplazar isc-dhcp-server. Se apoya en los lanzamientos de Ubuntu a partir de 23.04.

### Configuración de servidor isc-dhcp-server:

Para instalar y configurar el servidor DHCP en Ubuntu Server, se siguen estos pasos:

- Instalación del servidor DHCP:  
Ejecutar: `sudo apt update && sudo apt install isc-dhcp-server`
- Luego de haber instalado el servidor DHCP, es necesario configurar el servidor para las necesidades particulares con las cuales se usará. Para ello se debe editar el archivo `/etc/dhcp/dhcpd.conf`.

```
subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.100 192.168.1.200;
    option routers 192.168.1.1;
    option domain-name-servers 8.8.8.8, 8.8.4.4;
}
```

La anterior configuración en el archivo `/etc/dhcp/dhcpd.conf` dará lugar a que el servidor DHCP dé a los clientes una dirección IP de la gama 192.168.1.100 - 192.168.1.200. También usará 192.168.1.1 como default-gateway, y usará 8.8.8.8 y 8.8.4.4 como servidores DNS.

- De igual manera, es necesario editar el archivo `/etc/default/isc-dhcp-server` para especificar las interfaces dhcpd que escuchará:

```
INTERFACESv4="eth4"
```

Después de todo esto, se debe reiniciar el servicio dhcpd con el siguiente comando:  
`sudo systemctl restart isc-dhcp-server.service`

### Instalación y configuración de WEB en ubuntu server.

#### Guía Básica para Instalación y Configuración de un Servidor Web en Ubuntu Server

##### Arquitectura y propósito

Nginx es un servidor web de alto rendimiento, diseñado con una arquitectura event-driven y asíncrona. Esto le permite manejar múltiples conexiones simultáneas con un consumo muy bajo de recursos. Además, puede funcionar como proxy inverso, balanceador de carga y caché, lo que lo hace ideal para sitios con mucho tráfico.

### **Estructura de configuración:**

En Ubuntu, la configuración de Nginx se organiza principalmente en el directorio `/etc/nginx`.

Los bloques de servidor (server blocks) –equivalentes a los virtual hosts en Apache– se definen en archivos ubicados en `/etc/nginx/sites-available` y se habilitan creando enlaces simbólicos en `/etc/nginx/sites-enabled`.

Se configuran directivas como el puerto de escucha (por defecto 80 y 443), la raíz de documentos (por ejemplo, `/var/www/html`) y otros parámetros de seguridad o rendimiento.

### **Actualizar el sistema**

Antes de instalar cualquier paquete, es recomendable actualizar el sistema para asegurar de que se tienen las últimas versiones de los paquetes y parches de seguridad.

Ejecutando los siguientes comandos

Unset

```
sudo apt update  
sudo apt upgrade
```

### **Instalar Nginx**

Nginx es uno de los servidores web más populares y ampliamente utilizados.

Unset

```
sudo apt install nginx
```



## Configurar el Firewall

Si tienes un firewall habilitado, necesitarás permitir el tráfico HTTP y HTTPS.

```
Unset
sudo ufw allow 'Nginx Full'
```

Después iniciamos Nginx

```
Unset
sudo systemctl start nginx
```

## Funcionamiento y configuración de un servidor web, como Nginx en ubuntu server.

Verificar que Nginx está activo

```
Unset
sudo systemctl status nginx
```

El archivo principal se encuentra en [/etc/nginx/nginx.conf](#).

Los bloques de servidor (server blocks) se configuran en [/etc/nginx/sites-available/](#) y se habilitan con enlaces simbólicos en [/etc/nginx/sites-enabled/](#).

```
Unset
server {
    listen 80;
    listen [::]:80;
    root /var/www/dominio/html;
    index index.html index.htm;
    server_name dominio.com www.dominio.com;

    location / {
        try_files $uri $uri/ =404;
    }
}
```

```
}
```

Se habilita el dominio y se recarga nginx para hacer efectivas las configuraciones

```
Unset
sudo ln -s /etc/nginx/sites-available/dominio
    /etc/nginx/sites-enabled/
sudo nginx -t
sudo systemctl reload nginx
```

Finalmente, se debe asegurar que el firewall permitirá conexiones HTTP, se recarga de nuevo nginx y se puede proceder a probar

```
Unset
sudo ufw allow 'nginx full'
sudo ufw reload
```

## **Configuración del acceso remoto seguro al servidor utilizando el protocolo SSH.**

SSH ("Secure Shell") es un protocolo para acceder de forma segura a un ordenador desde otro. A pesar de su nombre, SSH permite ejecutar programas de línea de comandos y gráficos, transferir archivos e incluso crear redes privadas virtuales seguras en Internet.

Para usar SSH, se necesita instalar un cliente SSH en el ordenador desde el que se conecta y un servidor SSH en el ordenador al que se conecta. El proyecto OpenSSH mantiene el cliente y el servidor SSH para Linux más populares.

### **Guía configuración servidor SSH**

Para iniciar debemos instalar un servidor OpenSSH

Unset

```
sudo apt-get install openssh-server
```

Luego debemos hacer una copia de seguridad de su archivo `sshd_config` copiándolo a su directorio de inicio, o haciendo una copia de solo lectura en `/etc/ssh` haciendo:

Unset

```
sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.factory-defaults  
sudo chmod aw /etc/ssh/sshd_config.factory-defaults
```

Una vez que haya realizado una copia de seguridad de su archivo `sshd_config`, puede realizar cambios con cualquier editor de texto, por ejemplo;

Unset

```
sudo gedit /etc/ssh/sshd_config
```

Ejecuta el editor de texto estándar en Ubuntu 12.04 o posterior. En versiones anteriores, reemplaza "sudo" por "gksudo". Una vez realizados los cambios (consulta las sugerencias en el resto de esta página), puedes aplicarlos guardando el archivo y haciendo lo siguiente:

Unset

```
sudo restart ssh
```

Si recibe el error "No se puede conectar a Upstart", reinicie ssh con lo siguiente:

Unset

```
sudo systemctl restart ssh
```

## Gestión de procesos y servicios en Linux.

La gestión de procesos y servicios en Linux se puede realizar con los comandos `ps`, `top`, `htop`, `systemctl` y `service`.

- **Gestión de procesos**
  - `ps`: Lista procesos en ejecución
  - `top`: Muestra procesos ordenados por uso de CPU

- htop: Muestra procesos en tiempo real y tiene una interfaz visual
- pgrep: Busca procesos por nombre
- kill: Finaliza procesos por PID
- pkill: Finaliza procesos por nombre
- killall: Finaliza procesos en masa
- fg: Gestiona procesos en primer plano
- bg: Gestiona procesos en segundo plano
- nohup: Ejecuta procesos que continúan corriendo aunque el terminal se cierre

- **Gestión de servicios**

- systemctl: Inicia, detiene, verifica, habilita, o deshabilita servicios
- service: Gestiona servicios y procesos del sistema

Para administrar los servicios de Linux, es importante considerar el rendimiento, la seguridad y la funcionalidad del sistema.

Para gestionar el sistema operativo Linux, se puede utilizar una herramienta como Endpoint Central. Esta herramienta permite automatizar tareas de gestión de endpoints y gestionar distintos sistemas operativos desde una única consola.

## **Configuración de servicios de red en entornos linux.**

### **Configuración de la Red en Linux**

Para establecer y administrar la conectividad en Linux, se pueden utilizar diversas herramientas y configuraciones:

- **Configuración de Interfaces de Red:** Se pueden gestionar las conexiones con comandos como ip, ifconfig, nmcli y nmtui.
- **Direcciones IP Estáticas y Dinámicas:** Se pueden asignar direcciones IP manualmente en los archivos /etc/network/interfaces o /etc/netplan/, dependiendo de la distribución.
- **Enrutamiento y Rutas:** Con ip route es posible definir rutas estáticas y administrar el tráfico de red.
- **Configuración de DNS:** Se puede modificar el archivo /etc/resolv.conf o usar systemd-resolved para manejar la resolución de nombres de dominio.

### **Servicios de Red Comunes**

Algunos de los servicios más utilizados en entornos Linux incluyen:

#### **a) Servidor DHCP**

Un servidor DHCP permite asignar direcciones IP automáticamente a los dispositivos de la red. En Linux, se puede configurar con `isc-dhcp-server` o `dnsmasq`.

### **b) Servidor DNS**

Este servicio permite la resolución de nombres de dominio, facilitando la comunicación entre dispositivos en la red. Se pueden utilizar herramientas como `BIND` o `dnsmasq`, configurando las zonas y registros en `/etc/bind/named.conf.local`.

### **c) Servidor Web**

Para alojar sitios web, Linux ofrece opciones como `Apache` y `Nginx`, cuyas configuraciones se encuentran en `/etc/apache2/sites-available/` y `/etc/nginx/sites-available/`.

### **d) Servidor de Archivos**

Para compartir archivos en la red, se pueden utilizar:

- **NFS**, ideal para entornos Linux y Unix.
- **Samba**, para compartir archivos con equipos Windows.

### **e) Servidor SSH**

El servicio `OpenSSH` permite conectarse de forma remota a servidores Linux de manera segura. Se configura mediante el archivo `/etc/ssh/sshd_config`.

### **f) Servidor de Correo**

Los servidores de correo como `Postfix` y `Dovecot` permiten gestionar el envío y la recepción de correos electrónicos en redes empresariales o personales.

### **g) Servidor VPN**

Servicios como `OpenVPN` y `WireGuard` facilitan conexiones seguras a redes privadas, protegiendo la información en tránsito.

### **h) Servidor Proxy**

Para gestionar el tráfico de red y mejorar la seguridad, se pueden usar servidores proxy como `Squid` o `NGINX` (en modo proxy inverso).

## **Seguridad y Gestión de Servicios**

Para garantizar la seguridad en los servicios de red, es fundamental implementar medidas de protección como:

- **Control de tráfico con firewalls:** Herramientas como firewallld, ufw o iptables permiten gestionar el acceso a la red.
- **Protección contra ataques:** Fail2Ban ayuda a bloquear intentos de acceso no autorizados.
- **Monitoreo de tráfico y servicios:** Con herramientas como netstat, ss, tcpdump y Wireshark se puede analizar la actividad en la red.
- **Gestión de logs:** Es recomendable revisar registros con journalctl y syslog para detectar posibles incidentes de seguridad.

## Automatización y Gestión Avanzada

Para optimizar la administración de los servicios de red, se pueden aplicar estrategias como:

- **Gestión con systemd:** systemctl permite iniciar, detener y administrar servicios en segundo plano.
- **Automatización con scripts:** Se pueden crear scripts en /etc/systemd/system/ para iniciar servicios automáticamente.
- **Balanceo de carga y alta disponibilidad:** Herramientas como HAProxy ayudan a distribuir el tráfico entre servidores y evitar sobrecargas.

## Direccionamiento IPv6

El direccionamiento en **IPv6** es el esquema utilizado para asignar identificadores únicos a dispositivos en una red que usa el **Protocolo de Internet versión 6 (IPv6)**. Este protocolo fue desarrollado para reemplazar **IPv4** debido al agotamiento de direcciones.

### Características del direccionamiento IPv6

Las direcciones **IPv6** tienen una longitud de **128 bits**, lo que permite una cantidad masiva de direcciones disponibles. Se representan en formato hexadecimal y están separadas por dos puntos (:).

2001:0db8:85a3:0000:0000:8a2e:0370:7334

Para simplificar, se pueden aplicar reglas de reducción:

**Omisión de ceros a la izquierda:**

2001:db8:85a3:0:0:8a2e:370:7334

**Sustitución de bloques de ceros por "::" (una sola vez en la dirección):**

2001:db8:85a3::8a2e:370:7334

## **Tipos de direcciones IPv6**

Existen tres categorías principales:

### **Direcciones Unicast**

Son direcciones únicas asignadas a una interfaz de un solo nodo. Se dividen en:

- **Global Unicast:** Direcciones enrutables en Internet, equivalentes a las IPv4 públicas.
- **Link-Local:** Direcciones utilizadas para comunicación dentro de un enlace, prefijo FE80::/10.
- **Unique Local:** Direcciones para redes privadas, prefijo FC00::/7.

### **Direcciones Multicast**

Se usan para enviar datos a múltiples destinatarios simultáneamente. Tienen el prefijo FF00::/8 y no existen direcciones **Broadcast** en IPv6.

### **Direcciones Anycast**

Son asignadas a múltiples dispositivos, y el tráfico se dirige al más cercano según la métrica de enrutamiento.

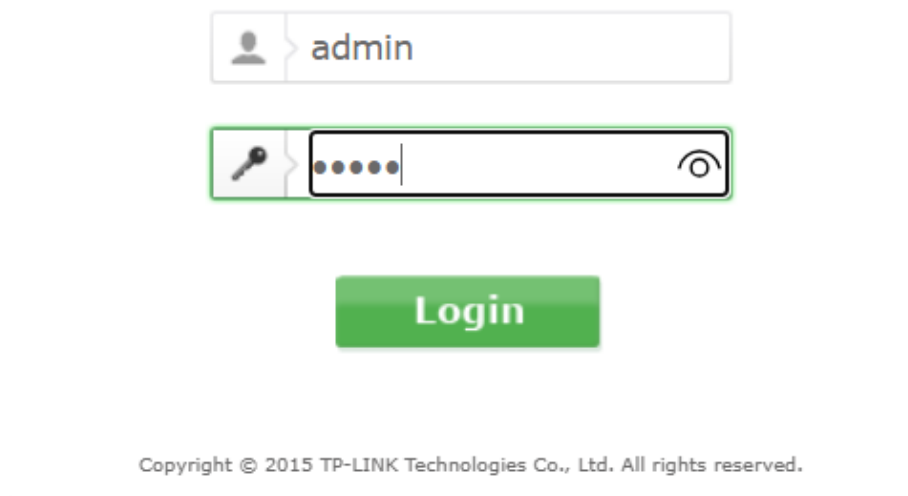
## **Configuración de direcciones IPv6**

Las direcciones pueden ser asignadas de tres formas:

1. **Estática:** Configurada manualmente por un administrador de red.
2. **Dinámica (DHCPv6):** Asignada por un servidor **DHCPv6**.

## Práctica con AP y Router

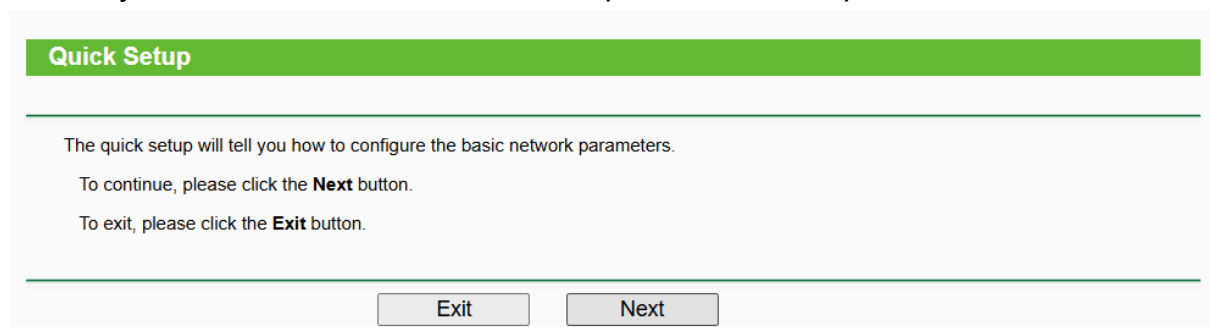
### Router:



The image shows the login interface of a TP-LINK router. It features two input fields: the first for the username, which contains the text 'admin', and the second for the password, which is masked with dots. A green 'Login' button is positioned below the password field. At the bottom of the page, a copyright notice reads: 'Copyright © 2015 TP-LINK Technologies Co., Ltd. All rights reserved.'

*Figura 1: Inicio de sesión router*

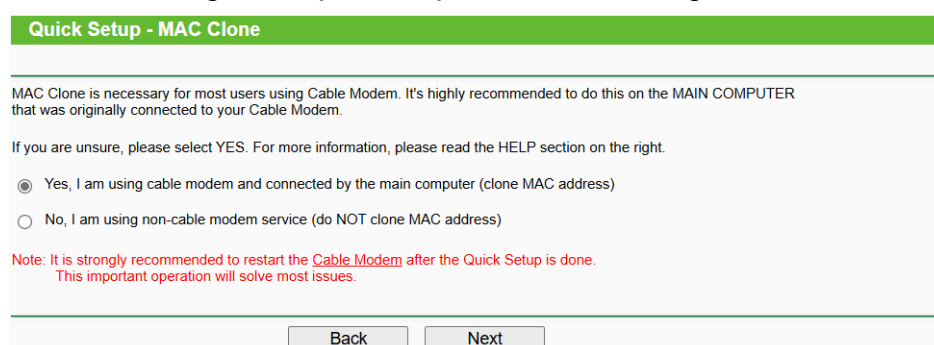
Para iniciar debemos ingresar a la interfaz de configuración del router ingresando usuario y contraseña en este caso **admin** para ambos campos



The image displays the 'Quick Setup' screen of the router's configuration interface. It has a green header with the text 'Quick Setup'. Below the header, there is a paragraph explaining that the quick setup will guide the user through basic network parameters. It then instructs the user to click the 'Next' button to continue or the 'Exit' button to exit. At the bottom, there are two buttons: 'Exit' and 'Next'.

*Figura 2: Asistente de configuración*

Le damos a siguiente para empezar con la configuración



The image shows the 'Quick Setup - MAC Clone' screen. It has a green header with the text 'Quick Setup - MAC Clone'. Below the header, there is a paragraph explaining that MAC Clone is necessary for most users using Cable Modem and is highly recommended to be done on the main computer. It then asks the user to select 'Yes' if they are using a cable modem and connected by the main computer, or 'No' if they are using a non-cable modem service. At the bottom, there are two buttons: 'Back' and 'Next'.

*Figura 3: Asistente de configuración*



Ya que estamos conectados por cable ethernet seleccionamos la opción que indica que estamos usando este método para conectarnos al router

**Quick Setup - Dual Band Selection**

This router supports dual band, please choose the frequency that you would like to work with:

☒ Concurrently with 2.4GHz and 5GHz (802.11a/b/g/n)

☐ Only work in 2.4GHz (802.11b/g/n)

☐ Only work in 5GHz (802.11a/n)

To turn off the wireless radio, you can switch the Wireless On/Off button located on the back panel of the device to the OFF position.

Back Next

Figura 4: Asistente de configuración

Aquí seleccionamos que vamos a usar 2.4 GHz y 5ghz para así configurar ambas opciones

**Quick Setup - Wireless 2.4GHz**

Wireless Radio: Enable

Wireless Network Name: RouterG03 (Also called the SSID)

Region: Colombia

Warning: Ensure you select a correct country to conform local law. Incorrect settings may cause interference.

Band: 2.4GHz

Mode: 11bgn mixed

Channel Width: Auto

Channel: Auto

Wireless Security:

☐ Disable Security

☒ Enable Security(WPA-PSK/WPA2-PSK)

PSK Password: Redes305 (You can enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)

☐ No Change

Back Next

Figura 4: Asignación nombre y contraseña de red 2.4GHz

Vamos a configurar la frecuencia de 2.4 GHz le asignamos como nombre de red(SSID) RouterG03 en la región de Colombia y la contraseña Redes305 las

demás opciones las dejamos como están por defecto.

**Quick Setup - Wireless 5GHz**

**Wireless Radio:** Enable

**Wireless Network Name:** RouterG03-5G (Also called the SSID)

**Region:** Colombia

**Warning:** Ensure you select a correct country to conform local law. Incorrect settings may cause interference.

**Band:** 5GHz

**Mode:** 11an mixed

**Channel Width:** Auto

**Channel:** Auto

**Wireless Security:**

☐ Disable Security

☒ Enable Security(WPA-PSK/WPA2-PSK)

**PSK Password:** Redes305  
(You can enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)

☐ No Change

Back Next

*Figura 5: Asignación nombre y contraseña de red 5GHz*

Vamos a configurar la frecuencia de 5 GHz le asignamos como nombre de red(SSID) RouterG03-5G en la región de Colombia y la contraseña Redes305 las demás opciones las dejamos como están por defecto.

**Quick Setup - Finish**

**Congratulations! The Router is now connecting you to the Internet. For detail settings, please click other menus if necessary.**

The change of wireless config will not take effect until the Router reboot.

Back Reboot

*Figura 6: Opción de reiniciar el router*

Después de haber configurado ambas frecuencias de red procedemos a reiniciar el router

para que las direcciones ip que se asignen a los equipos conectados al router debemos desactivar la opción de DHCP server

**DHCP Settings**

DHCP Server: ☒ Disable ☐ Enable

Start IP Address: 192.168.0.100

End IP Address: 192.168.0.199

Address Lease Time: 120 minutes (1~2880 minutes, the default value is 120)

Default Gateway: 192.168.0.1 (optional)

Default Domain: (optional)

Primary DNS: 0.0.0.0 (optional)

Secondary DNS: 0.0.0.0 (optional)

Save

*Figura 6: Desactivar opción DHCP*

Después accedemos a la consola de comandos e ingresamos ipconfig y nos damos de cuenta que la dirección ip que nos asignó esta en el rango de la red de la universidad es decir el que nos está asignando la dirección ip es el servidor DHCP de la universidad

```

Adaptador de LAN inalámbrica Conexión de área local* 2:

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

Adaptador de LAN inalámbrica Wi-Fi:

    Sufijo DNS específico para la conexión. . : uptc.edu.co
    Vínculo: dirección IPv6 local. . . : fe80::8344:8a0d:34e8:fa95%13
    Dirección IPv4. . . . . : 10.4.73.45
    Máscara de subred . . . . . : 255.255.252.0
    Puerta de enlace predeterminada . . . . : 10.4.72.1
  
```

*Figura 6: Dirección ip asignada por la universidad*

Por último hacemos un ping entre dos dispositivos conectados al router y vemos que tienen comunicación entre sí

```

C:\Users\samue>ping 10.4.74.238

Haciendo ping a 10.4.74.238 con 32 bytes de datos:
Respuesta desde 10.4.74.238: bytes=32 tiempo=12ms TTL=128
Respuesta desde 10.4.74.238: bytes=32 tiempo=13ms TTL=128
Respuesta desde 10.4.74.238: bytes=32 tiempo=16ms TTL=128
Respuesta desde 10.4.74.238: bytes=32 tiempo=12ms TTL=128

Estadísticas de ping para 10.4.74.238:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 12ms, Máximo = 16ms, Media = 13ms

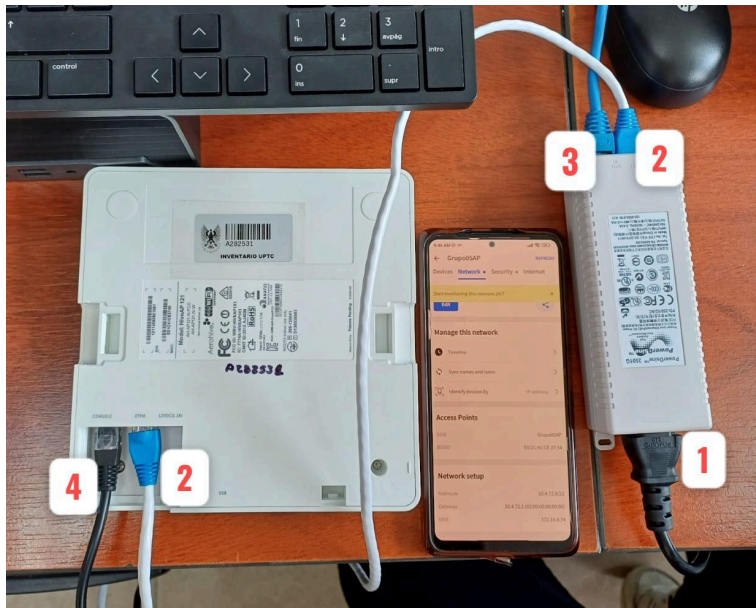
C:\Users\samue>
  
```

*Figura 7: Ping entre dos dispositivos conectados al router*

### AP Aerohive:

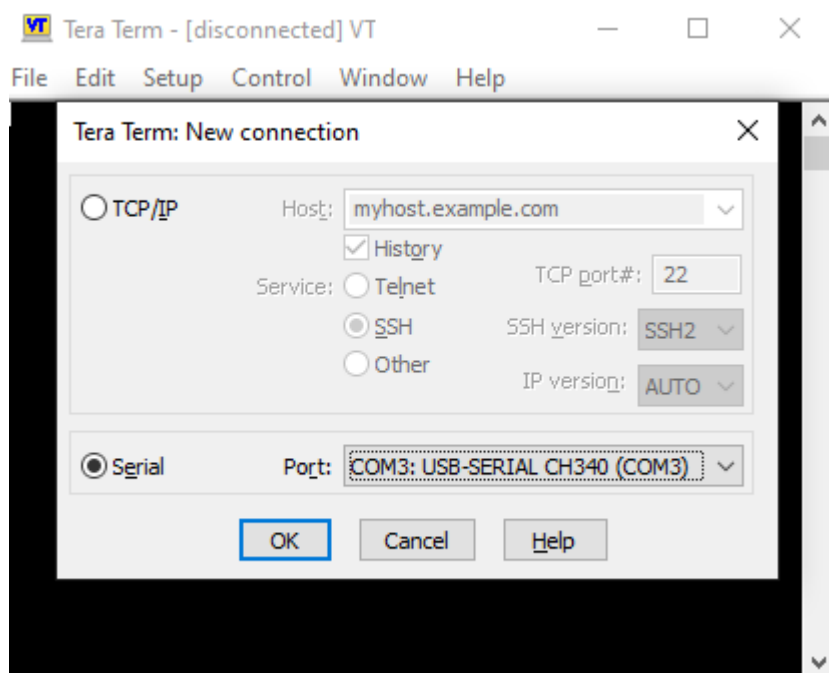
Inicialmente se realiza la conexión cableada de los puertos correspondientes del AP para realizar su configuración como se muestra en la *Figura 7*:

1. Conexión cable alimentación ac-poe.
2. Conexión patch cort puerto poe (data power out) a puerto eth0 ap aerohive.
3. Conexión patch cort puerto poe (data in) a puerto de red.
4. Conexión usb serial pc, a puerto console ap aerohive.



*Figura 8. Conexiones alámbricas numeradas para la configuración del AP.*

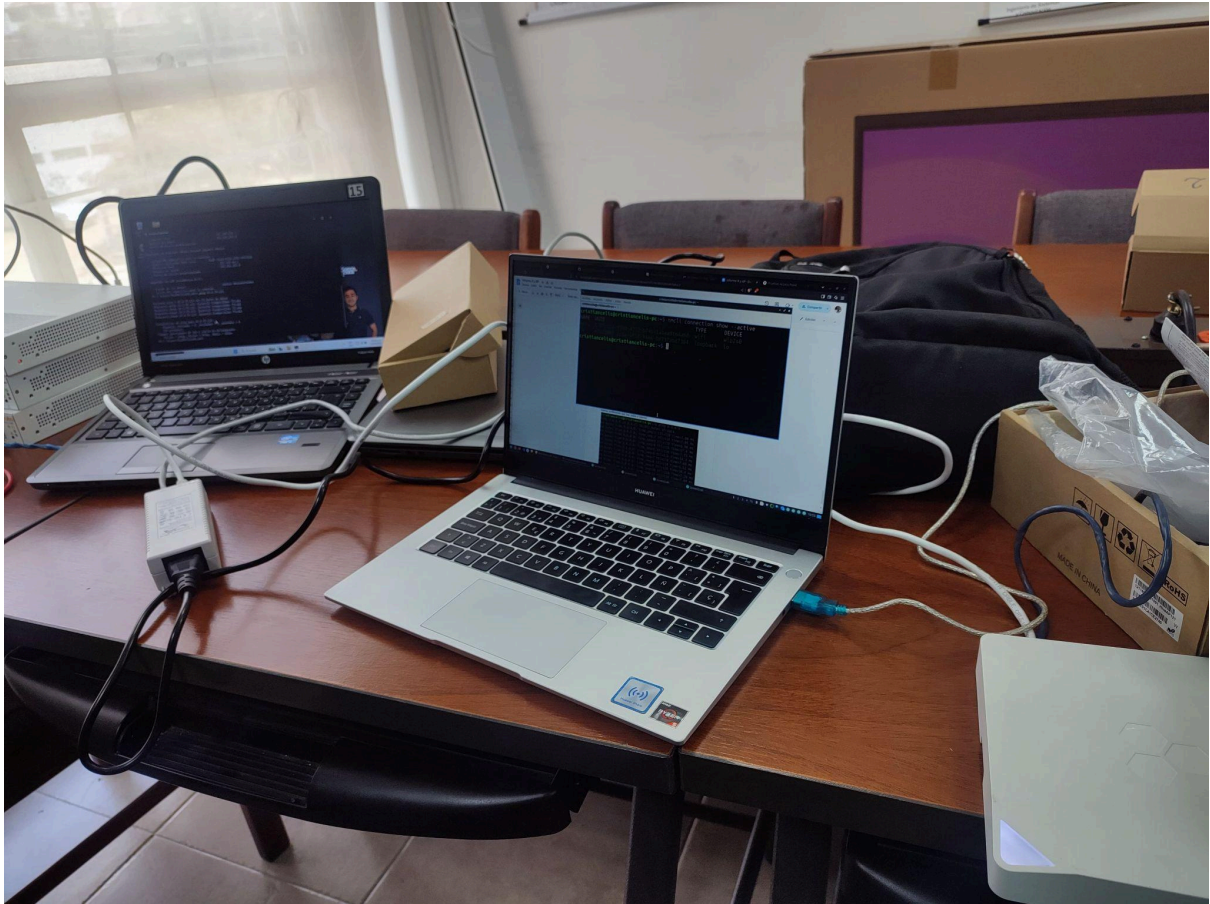
Seguidamente se hace la instalación del programa Tera Term para realizar la configuración por CLI del Access Point. Al ejecutar el programa se observa una interfaz en la cuál es necesario realizar una conexión de forma serial para empezar a configurar el AP, como se muestra en la *Figura 8*.



*Figura 9. Conexión serial mediante Tera Term al Access Point.*

Antes de realizar la configuración del AP, es necesario realizar un **reseteo**, con el fin de eliminar configuraciones anteriores realizadas en el mismo. Esto se puede hacer usando un clip para mantener presionado el botón en forma de alfiler durante 10-20 segundos.

A continuación se muestra, en la figura 9 se observan dos computadoras y un Access Point para realizar la práctica. La computadora ubicada a la izquierda está conectada a un Switch que a su vez está conectado a la red de la universidad, y la otra computadora se encuentra conectada por puerto USB al Access Point para su configuración.



*Figura 10. Computadoras y access point.*

Para realizar la configuración, se ingresa al dispositivo mediante la línea de comandos usando las credenciales de fábrica (usuario: admin, contraseña: aerohive). Al aparecer el mensaje del asistente de configuración se escribe “yes”, se selecciona “no” y se presiona Enter. Luego, se asigna el nombre al AP (AP-01) y se elige un número entre 1 y 127. Seguidamente, se configura el usuario “adminAP” con la contraseña “MiClaveSegura!”. Finalmente, se establece la conexión del AP a Internet de forma dinámica mediante DHCP, asignando también la fecha y hora vía NTP a través de DHCP. Esto se observa a continuación en la figura 10.



```

Use the Aerohive Initial Configuration Wizard? <yes|no>:yes
----- Welcome to the HiveAP Initial CLI Configuration Wizard -----

To exit this dialog without saving any changes, enter <ctrl-C> at any time.
You can restart the wizard by entering the following from the CLI command prompt: wizard startup.

(Note: If you enter ctrl-c, there should be a confirmation window to proceed or quit without saving changes.)

Help:
<ctrl-b> - Go back to previous configuration entry
<ctrl-n> - Go to next configuration entry
<ctrl-r> - Restart Initial CLI Configuration Wizard from the beginning
<ctrl-c> - Exit without saving

Values in brackets [ ] are default values
Type <enter> to accept the entered or default value

-----

Press <enter> to continue...

Ready to use the Aerohive HiveManager to manage this HiveAP? <[yes]|no>:no

Enter the hostname for the HiveAP [AH-00-11-10]:AP-01

Enter the location for the HiveAP, 1-127 chars [change_net]:Oficina

The HiveAP uses its management interface <ngt0> for all IP communications such as SSH, SNMP, SYSLOG, RADIUS, etc... The IP address of the
P or configured statically.
Configure the ngt0 interface using:
1. DHCP
2. Static IP Assignment
Enter option <[1] or 2>:1

The root admin has full management privileges for the HiveAP. Therefore, it is important that the name and password remain a secret.
Enter the root admin name, 3-20 chars [admin]:adminAP
Enter the root admin password, 5-32 chars []:
Confirm the root admin password []:

DNS
1. Obtain DNS server addresses via DHCP
2. Configure DNS server addresses manually
Enter option <[1] or 2>:1

```

*Figura 11. Configuración inicial access point.*

Al finalizar la configuración se asigna una contraseña de autenticación para la red WLAN creada, seleccionando las opciones correspondientes y digitando la contraseña “Redes305”, así como el nombre de red (SSID) ApG3. Se visualiza el resumen de la configuración y se escribe “yes” para guardar los cambios. Finalmente, se reinicia el AP y se espera aproximadamente 5 minutos hasta que la conexión se establezca y el LED blanco se encienda, indicando que todo quedó configurado correctamente. Como se aprecia en la figura 11.

```

If you have multiple HiveAPs that are within the same subnet or VLAN, you create a Hive by configuring the HiveAPs with the same Hive name
municate with each other using the Aerohive collective control protocols to allow fast roaming, coordinated radio frequency management, be
ies.
Enter the name for the Hive, 1-32 chars [myHive]:Hive-01

In order for devices in the Hive to communicate with each other, they must use the same shared secret.
Enter 8-63 ASCII characters for the shared secret []:
Confirm the shared secret []:

The SSID (Service Set Identifier) is the name that wireless clients associate with to connect to the wireless LAN.
Enter and SSID name, 1-32 chars [ssid0]:ApG3

In order to establish communications between the HiveAP and wireless clients, you must select the keying, authentication and encryption me
If you require an option that is not displayed, you can configure the SSID through the CLI or Aerohive.
Wireless LAN Security Protocols for the SSID:
1. open -Set security to open, no encryption or authentication
2. upa-auto-8021x -Set the key management and authentication protocol to allow WPA or WPA2 with 802.1X (EAP) and allow the encryp
3. upa-auto-psk -Set the key management and authentication protocol to allow WPA or WPA2 with a preshared key and allow the enc
Enter the number of the security protocol suite to use for this SSID [1]:3

Key type:
1. ASCII Passphrase
2. Hexadecimal Key
Enter option <[1] or 2>:1

Enter an 8-63 character passphrase:
Confirm passphrase:

Display a summary of the CLI commands that will be configured <[yes|no]:yes
*****
hostname AP-01
snmp location Oficina
admin root-admin adminAP password 5s6qE9RoyJLnHrs9xJFese//Ra/
Hive Hive-01
interface mgmt0 Hive Hive-01
Hive Hive-01 password 9fKSHoQBxOKesvXtFh$dzJ9nojuU3vSNhkTBrH6PlqHnPsrnVeH5PU0u3BrVoaJ4K0uZz1
ssid ApG3
interface wifi0 ssid ApG3
ssid ApG3 security protocol-suite upa-auto-psk ascii-key LxJK3IsgoiiSo2Zyu3rnk41LefRJyvavQGvQg
*****

```

Figura 12. Configuración final access point.

Finalizada la configuración, y esperados 5 minutos, se prueba la conexión inalámbrica al Access Point con SSID ApG3. En la siguiente figura se muestran las conexiones activas, y la conexión mostrada tiene como nombre ApG3, probando que la conexión se realizó de manera exitosa.

```

cristiancelis@cristiancelis-pc:~$ nmcli connection show --active
NAME    UUID                                  TYPE      DEVICE
ApG3    b767cc1d-f9d0-4722-b74b-1a1ea9164a60 wifi       wlp2s0

```

Figura 13. Conexión inalámbrica a dispositivo access point por nombre de red ApG3.

Posteriormente, se obtiene la dirección IP de la máquina. En la figura 13 se observa que la ip obtenida es **10.4.75.123**, dirección que se encuentra dentro del rango de la red de la universidad, por lo que se asignó correctamente.



```
cristiancelis@cristiancelis-pc:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue sta
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: wlp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdi
    link/ether 64:6c:80:a0:a1:19 brd ff:ff:ff:ff:ff:ff
    inet 10.4.75.123/22 brd 10.4.75.255 scope global dyna
        valid_lft 507sec preferred_lft 507sec
    inet6 fe80::7110:abd1:3c95:c584/64 scope link noprefi
        valid_lft forever preferred_lft forever
```

*Figura 14. Ip obtenida al ejecutar el comando "ip a"*

A continuación se realiza un ping a una IP Externa, como es la de Google (8.8.8.8). Demostrando que la conexión es exitosa y confirmando que hay salida a internet

```
cristiancelis@cristiancelis-pc:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=118 time=7.00 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=7.01 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=118 time=6.98 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=118 time=17.6 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=118 time=7.73 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=118 time=14.3 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=118 time=7.68 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=118 time=5.63 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=118 time=10.4 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=118 time=7.26 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=118 time=7.04 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=118 time=6.83 ms
```

*Figura 15. Resultado ping 8.8.8.8 (Google)*

Finalmente, se procede a hacer ping de la computadora conectada al Switch, a la computadora conectada inalámbricamente al access point. Esta prueba resulta exitosa como se observa a continuación en la figura 15.

```
PS C:\Users\TELEMATICA305_A47> ping 10.4.75.123

Haciendo ping a 10.4.75.123 con 32 bytes de datos:
Respuesta desde 10.4.75.123: bytes=32 tiempo=288ms TTL=64
Respuesta desde 10.4.75.123: bytes=32 tiempo=109ms TTL=64
Respuesta desde 10.4.75.123: bytes=32 tiempo=432ms TTL=64
Respuesta desde 10.4.75.123: bytes=32 tiempo=221ms TTL=64
```

Figura 16. Ping exitoso entre computadoras utilizadas para la práctica

## Analisis y Sintesis

### 1. Servidor DHCP (Dynamic Host Configuration Protocol)

- Elección del software DHCP:
  - **isc-dhcp-server** vs. **isc-kea**:
    - *isc-dhcp-server* ya no es compatible en las versiones más recientes, pero aún soportado en versiones antiguas de Ubuntu.
    - *isc-kea* es la opción moderna (para Ubuntu 23.04+), diseñada para entornos escalables y con soporte activo.
  - **Compatibilidad**: Verificar la versión de Ubuntu Server para elegir el software adecuado.
- Métodos de asignación de IP:
  - **Asignación manual (MAC)**: Ideal para dispositivos críticos (servidores, impresoras) que requieren IP fija. Requiere mantener un registro actualizado de direcciones MAC.
  - **Asignación dinámica (pool)**: Optimiza el uso de direcciones IP en redes con dispositivos móviles. Definir rangos (**range**) y tiempos de arrendamiento (**lease time**) acordes al tamaño de la red.
  - **Asignación automática**: Útil para redes con alta rotación de dispositivos, pero puede generar conflictos si no se gestionan las IPs expiradas.
- Parámetros críticos en **dhcpd.conf**:
  - **Subnet y máscara**: Deben coincidir con la topología de la red física.
  - **Gateway y DNS**: Proporcionar la dirección del router y servidores DNS (externos como 8.8.8.8 o internos si se implementa DNS local).
  - **Interfaces activas**: Configurar **INTERFACESv4** en **/etc/default/isc-dhcp-server** para evitar que el servicio escuche en interfaces no deseadas.

### 2. Servidor WEB (Nginx)

- **Arquitectura y rendimiento:**
  - La arquitectura asíncrona de Nginx lo hace ideal para alto tráfico, pero requiere ajustes en la configuración para optimizar recursos (ej: `worker_processes`, `keepalive_timeout`).
  - **Server Blocks:** Organizar sitios web en `/etc/nginx/sites-available` y habilitarlos mediante enlaces simbólicos. Esto permite hostear múltiples dominios en un solo servidor.
- **Configuración básica:**
  - **Raíz del sitio:** Definir `root` correctamente (ej: `/var/www/dominio/html`) y permisos de archivos (evitar usar `root` como propietario).
  - **Puertos y SSL:** Configurar escucha en puerto 80 (HTTP) y 443 (HTTPS). Implementar certificados SSL/TLS (Let's Encrypt) para seguridad.
- **Firewall y seguridad:**
  - Habilitar solo los puertos necesarios (`ufw allow 'Nginx Full'`).
  - Restringir acceso a directorios sensibles (ej: `.git`, `.env`) mediante reglas en `location` dentro de los bloques de servidor.
  - Actualizar Nginx regularmente para mitigar vulnerabilidades.
- **Pruebas y mantenimiento:**
  - Usar `sudo nginx -t` para validar la sintaxis antes de recargar.
  - Monitorear logs (`/var/log/nginx/access.log` y `error.log`) para detectar errores o ataques.

### 3. Servidor DNS (Inferido de la sección 5.4)

- **Elección de software:**
  - **BIND** para configuraciones avanzadas (ej: zonas primarias/secundarias).
  - **dnsmasq** para redes pequeñas o integración con DHCP.
- **Integración con DHCP:**
  - El servidor DHCP debe proporcionar la dirección del servidor DNS a los clientes (mediante `option domain-name-servers` en `dhcpd.conf`).
  - Configurar zonas (forward/reverse) en `/etc/bind/named.conf.local` para resolver nombres de dominio internos.
- **Seguridad:**
  - Restringir consultas recursivas a redes internas.
  - Implementar DNSSEC para autenticación de respuestas.

### 4. Acceso Remoto Seguro (SSH)

- **Autenticación por clave:**
  - Deshabilitar `PasswordAuthentication` para evitar ataques de fuerza bruta.
  - Usar claves SSH ed25519 o RSA de 4096 bits.
- **Configuración avanzada:**

- Cambiar el puerto predeterminado (22) para reducir ataques automatizados.
- Limitar usuarios permitidos (`AllowUsers` en `sshd_config`).
- Usar `ufw limit ssh` para mitigar ataques de denegación de servicio.
- **Túneles y reenvíos:**
  - Desactivar `X11Forwarding` y `AllowTcpForwarding` si no son necesarios.

## 5. Gestión General de Servicios

- **Interdependencias:**
  - El servidor DHCP depende de una configuración de red estática en el servidor (IP fija en la interfaz).
  - El servidor WEB y DNS deben tener IPs fijas (asignadas manualmente vía DHCP o estáticamente en Netplan).
- **Monitoreo:**
  - Usar `systemctl status <servicio>` para verificar el estado de DHCP, Nginx, SSH, etc.
  - Configurar alertas para reinicios inesperados o caídas.
- **Backup y recuperación:**
  - Respalidar archivos críticos (`dhcpd.conf`, `nginx.conf`, `sshd_config`, zonas DNS).
  - Usar herramientas como `rsync` o `tar` para backups automatizados.

La implementación exitosa requiere un equilibrio entre funcionalidad, seguridad y mantenibilidad. Priorizar:

1. **Planificación de red:** Subredes, rangos DHCP, y asignación estática/dinámica.
2. **Seguridad por capas:** Firewalls, autenticación sin contraseña (SSH), y actualizaciones periódicas.
3. **Integración de servicios:** DHCP debe asignar DNS correcto; DNS debe resolver nombres internos/externos.
4. **Documentación y pruebas:** Registrar configuraciones y validar escenarios de fallos (ej: agotamiento de IPs, caída de servicios).

## Referencias

- APACHE SOFTWARE FOUNDATION. *Documentación de Apache HTTP Server* [en línea]. Disponible en: <https://httpd.apache.org/docs/>.
- CANONICAL. *Instalar y configurar Nginx* [en línea]. Ubuntu Tutorials. Disponible en: <https://ubuntu.com/tutorials/install-and-configure-nginx>.
- CANONICAL. *Acerca de DHCP* [en línea]. Documentación de Ubuntu Server. Disponible en: <https://documentation.ubuntu.com/server/explanation/networking/about-dhcp/index.html>.
- CANONICAL. *Instalación del servidor DHCP ISC* [en línea]. Documentación de Ubuntu Server. Disponible en: <https://documentation.ubuntu.com/server/how-to/networking/install-isc-dhcp-server/#install-isc-dhcp-server>
- CANONICAL. *Configuración de OpenSSH* [en línea]. Ubuntu Help. Disponible en: <https://help.ubuntu.com/community/SSH/OpenSSH/Configuring>.
- APACHE SOFTWARE FOUNDATION. *Documentación de Apache HTTP Server* [en línea]. Disponible en: <https://httpd.apache.org/docs/>.
- CANONICAL. *Instalar y configurar Nginx (Resumen)* [en línea]. Ubuntu Tutorials. Disponible en: <https://ubuntu.com/tutorials/install-and-configure-nginx#1-overview>.
- CANONICAL. *SSH en Ubuntu* [en línea]. Ubuntu Help. Disponible en: <https://help.ubuntu.com/community/SSH>.
- DIGITALOCEAN. *Uso de systemctl para administrar servicios y unidades en systemd* [en línea]. Disponible en: <https://www.digitalocean.com/community/tutorials/how-to-use-systemctl-to-manage-systemd-services-and-units>.
- LINUX-CONSOLE. *Cómo instalar Fedora Server*. [en línea]. Disponible en: <https://es.linux-console.net/?p=1438>.
- Internet Engineering Task Force (IETF). (2017). *RFC 8200 - Internet Protocol, Version 6 (IPv6) Specification*. [en línea]. Disponible en: <https://www.rfc-editor.org/rfc/rfc8200>

