



FACULTAD DE INGENIERÍA

Escuela de Computación

G10_DHCP_WLAN



COMPETENCIAS

- El estudiante configura el protocolo DHCP.
- El estudiante configura redes inalámbricas

MATERIALES Y EQUIPOS

- Computador con Simulador Packet-Tracer 8.2

INTRODUCCION

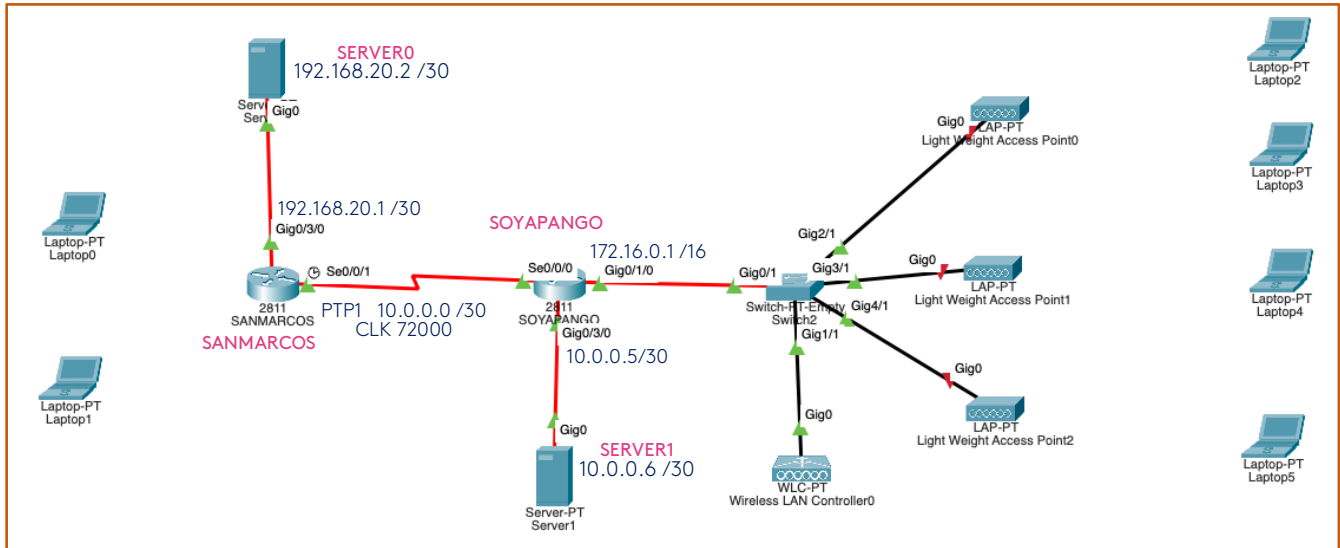
Todo dispositivo electrónico que se conecte a una red informática (cobre, fibra óptica o inalámbricamente) deberá recibir configuración TCP/IP (**direccionamiento IP**) para interactuar con los demás dispositivos conectados a dicha red.



El Protocolo DHCP es un protocolo de configuración Dinámica de Hosts, utilizado para asignar direcciones IP de forma automática a los dispositivos de red, evitando asignar manualmente las direcciones IP a cada dispositivo en la red. Además, DHCP permite la reutilización de direcciones IP, lo que significa que las direcciones IP pueden asignarse a diferentes dispositivos en diferentes momentos.

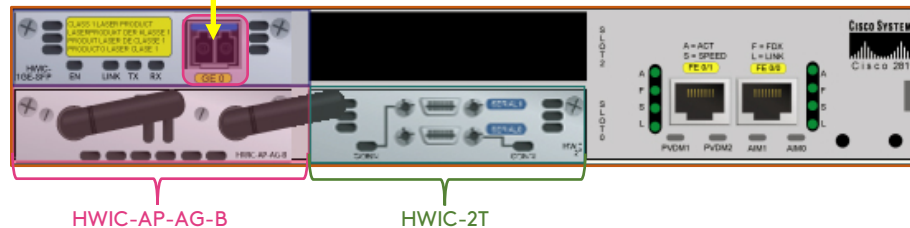
DHCP SERVER – WLAN ROUTER

1. Implemente la topología mostrada en la figura, haciendo uso de **switch PT-Empty** y **routers 2811** (configure los nombres y viñetas de los **routers** como se muestra)

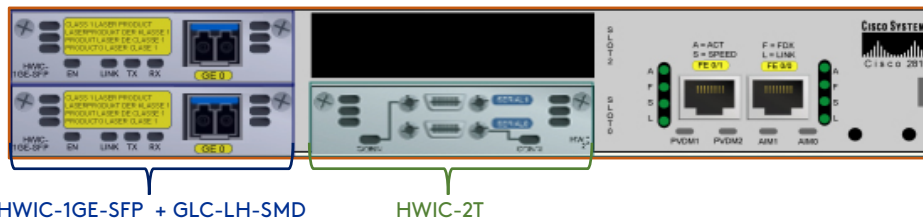


- En **router San Marcos** deberá instalar módulos HWIC mostrados en la figura

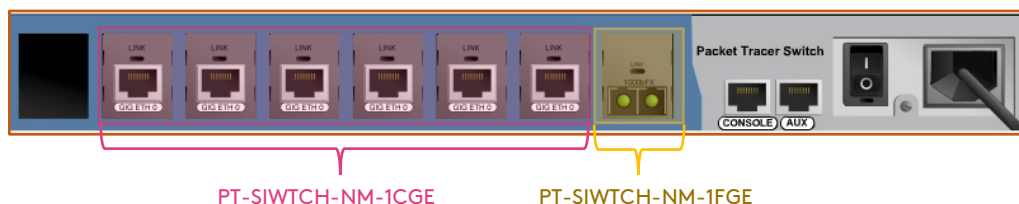
HWIC-1GE-SFP + GLC-LH-SMD



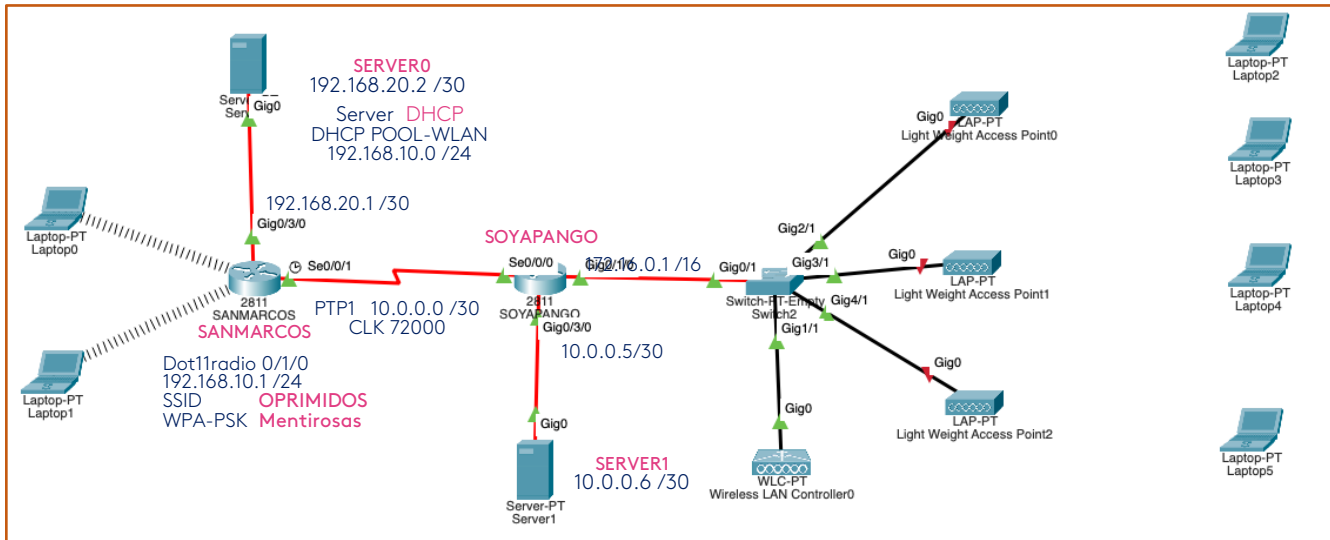
- En **router Soyapango** deberá instalar módulos HWIC mostrados en la figura



- En **switch PT-Empty** deberá instalar los módulos ethernet mostrados



2. Configure en **router SOYAPANGO** y **router SANMARCOS** las interfaces conforme a las redes en las que están conectados. Para la red PTP1 haga uso de la señal de reloj 72000



3. Deberá instalar en los servidores el módulo **PT-HOST-NM-1FGE** y configurarle las direcciones IP de forma manual (dirección IP, máscara, Gateway y DNS)
4. Configure en **server0** el servicio DHCP (**POOL-WLAN**) el cual será empleado en la red inalámbrica **OPRIMIDOS**. (El pool contara con 50 direcciones IPv4 otorgables)

Server0

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP**
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

Interface: GigabitEthernet0 Service: ☒ On ☐ Off

Pool Name: POOL-WLAN

Default Gateway: 192.168.10.1

DNS Server: 10.0.0.6

Start IP Address: 192.168.10.50

Subnet Mask: 255.255.255.0

Maximum Number of Users: 50

Add Save Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server
POOL-WLAN	192.168.10.1	10.0.0.6	192.168.10.50	255.255.255.0	50	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	192.168.20.0	255.255.25...	3	0.0.0.0

5. Configure la señal Wireless en la interfaz inalámbrica dot11radio 0/1/0 de **Router SanMarcos** y el reenvío de peticiones de direcciones IP.

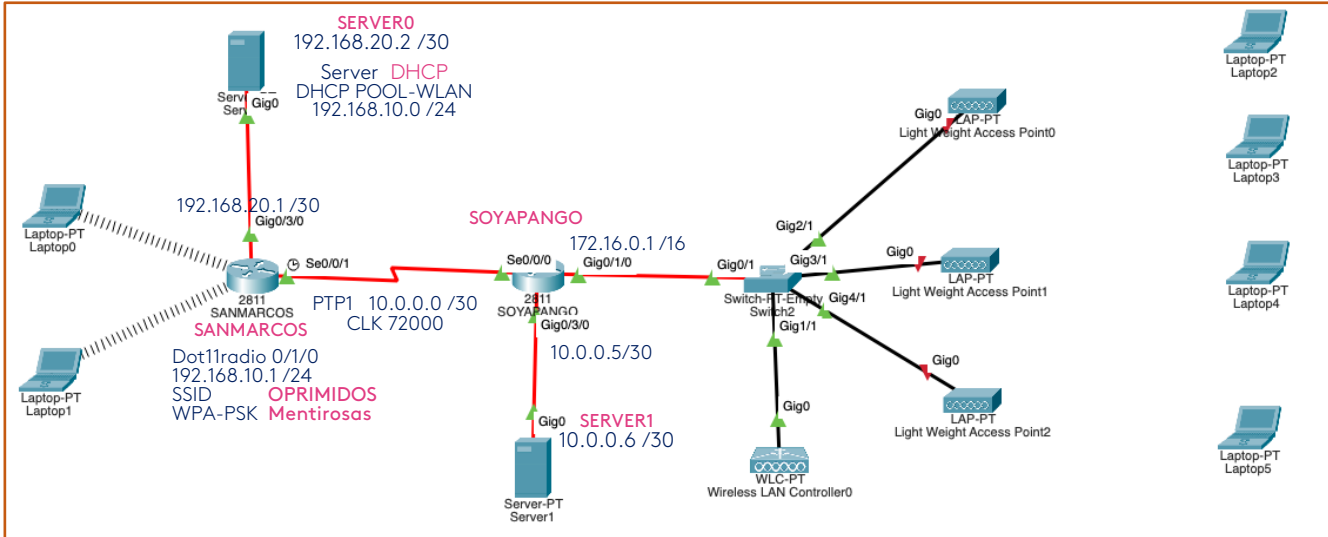
CLI - SANMARCOS	
SANMARCOS (config)# dot11 ssid OPRIMIDOS	Genera la wireless
SANMARCOS (config-ssid)# authentication open	Método de autenticación
SANMARCOS (config-ssid)# authentication key-management wpa	Cifrado WPA
SANMARCOS (config-ssid)# wpa-psk ascii 0 mentirosas	Contraseña
SANMARCOS (config-ssid)# guest-mode	Modo invitado activado
SANMARCOS (config-ssid)# exit	
SANMARCOS (config)# int dot11radio 0/1/0	Inter. inalámbrica
SANMARCOS (config-if)# ip address 192.168.10.1 255.255.255.0	Dirección IP
SANMARCOS (config-if)# ip helper-address 192.168.20.2	Reenvío de peticiones IP
SANMARCOS (config-if)# ssid OPRIMIDOS	Vincula SSID
SANMARCOS (config-if)# encryption mode ciphers aes-ccm	Encriptación AES
SANMARCOS (config-if)# no shutdown	Enciende la interfaz
SANMARCOS (config-if)# exit	
SANMARCOS (config)# do wr	

6. En **Laptop0** y **Laptop1**, coloque el módulo **PT-LAPTOP-NM-1W-AC** y configúrelos de la siguiente manera.

7. Revise las direcciones IP obtenidas de forma automática por **Laptop0** y **Laptop1**.

PROTOCOLO DE ENRUTAMIENTO EIGRP

8. Configure en **router SOYAPANGO** y **router SANMARCOS** el protocolo de enrutamiento **eigrp** y declare las redes en las que se encuentran conectados.



CLI -SANMARCOS

```

SANMARCOS (config)# router eigrp 10
SANMARCOS (config-router)# network 192.168.10.0 0.0.0.255
SANMARCOS (config-router)# network 192.168.20.0 0.0.0.3
SANMARCOS (config-router)# network 10.0.0.0 0.0.0.3
SANMARCOS (config-router)# no auto-summary
SANMARCOS (config-router)# passive-interface gi 0/3/0
SANMARCOS (config-router)# exit
SANMARCOS (config)# do wr

```

Protocolo EIGRP
 Declara la red inalámbrica
 Declara la red del servidor
 Declara la red PTP1
 no súper redes
 Interface pasiva
 Guarda la conf.

CLI -SOYAPANGO

```

SOYAPANGO (config)# router eigrp 10
SOYAPANGO (config-router)# network 172.16.0.0 0.0.255.255
SOYAPANGO (config-router)# network 10.0.0.0 0.0.0.3
SOYAPANGO (config-router)# network 10.0.0.4 0.0.0.3
SOYAPANGO (config-router)# no auto-summary
SOYAPANGO (config-router)# passive-interface gi 0/1/0
SOYAPANGO (config-router)# passive-interface gi 0/3/0
SOYAPANGO (config-router)# exit
SOYAPANGO (config)# do wr

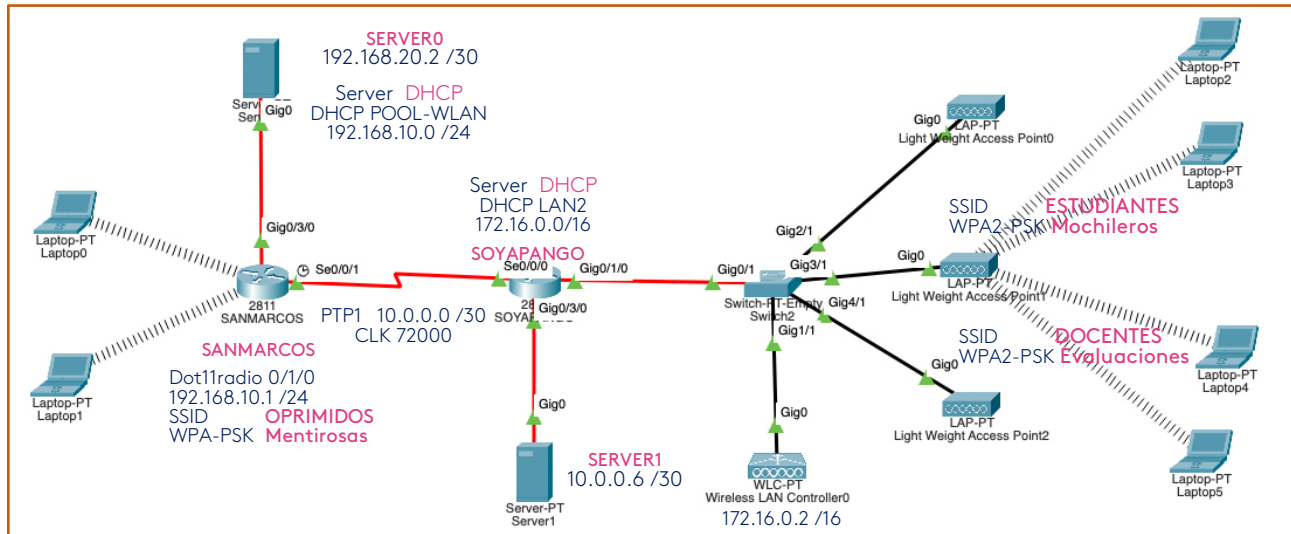
```

Protocolo EIGRP
 Declara la red inalámbrica
 Declara red PTP1
 Declara la red del servidor
 no súper redes
 Interface pasiva
 Interface pasiva
 Guarda la conf.

9. Haga pruebas de conectividad entre los dispositivos configurados en este momento. **¡Todas las pruebas deben ser exitosas!**

DHCP ROUTER – WLAN WCONTROLLER

10. Configure en **router soyapango** el servicio DHCP (**LAN2**) el cual será empleado en las redes inalámbricas **DOCENTES** y **ESTUDIANTES**.



CLI -SOYAPANGO

```
SOYAPANGO (config)# ip dhcp excluded-address 172.16.0.1 172.16.0.50
```

Excluye el rango

```
SOYAPANGO (config)# ip dhcp pool LAN2
```

Pool de IP LAN2

```
SOYAPANGO (dhcp-config)# network 172.16.0.0 255.255.0.0
```

red y mascara

```
SOYAPANGO (dhcp-config)# default-router 172.16.0.1
```

Default Gateway

```
SOYAPANGO (dhcp-config)# dns-server 10.0.0.6
```

Dirección DNS

```
SOYAPANGO (dhcp-config)# exit
```

```
SOYAPANGO (config)# do wr
```

Guarda la configu.

11. Configure de forma manual el direccionamiento IP del **controlador wireless** para poder administrarlo.

Wireless LAN Controller0	
GLOBAL	Physical Config Attributes
Settings	
Wireless LANs	
AP Groups	
DHCP	
INTERFACE	
GigabitEthernet0	
Management	IP Configuration IPv4 Address: 172.16.0.2 Subnet Mask: 255.255.0.0 Default Gateway: 172.16.0.1 DNS Server: 10.0.0.6

12. Siempre en el controlador de red inalámbrico, configure las redes inalámbricas **ESTUDIANTES Y DOCENTES**, exactamente como se muestra.

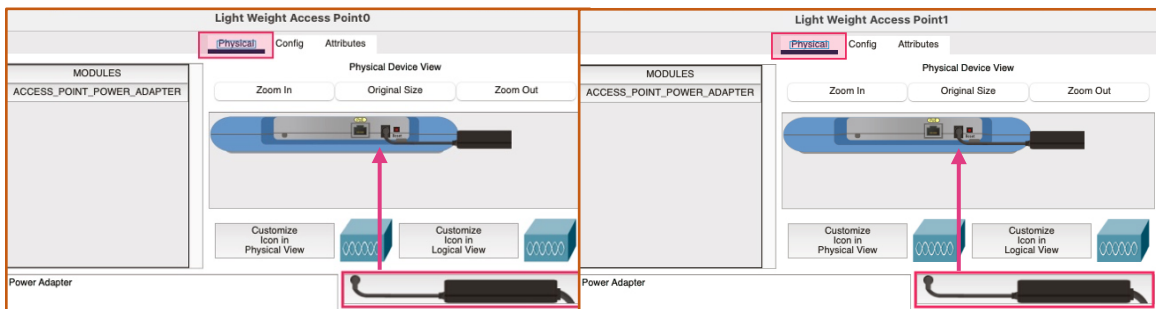
Wireless LAN Controller0 Configuration - WIFI-DOCENTES

- GLOBAL** > **Config** > **Wireless LANs**
- Select WLAN:** WIFI-DOCENTES
- Name:** WIFI-DOCENTES, **SSID:** DOCENTES
- Authentication:**
 - ☒ WPA2-PSK, **PSK Pass Phrase:** Evaluaciones
 - ☐ WPA, ☐ WPA2
- Encryption Type:** AES
- Central Control:**
 - ☒ Local switching, local authentication
 - ☐ Central switching, central authentication
 - ☐ Local switching, central authentication
- Buttons:** New, Remove, Save

Wireless LAN Controller0 Configuration - WIFI-ESTUDIANTES

- GLOBAL** > **Config** > **Wireless LANs**
- Select WLAN:** WIFI-ESTUDIANTES
- Name:** WIFI-ESTUDIANTES, **SSID:** ESTUDIANTES
- Authentication:**
 - ☒ WPA2-PSK, **PSK Pass Phrase:** Mochileros
 - ☐ WPA, ☐ WPA2
- Encryption Type:** AES
- Central Control:**
 - ☒ Local switching, local authentication
 - ☐ Central switching, central authentication
 - ☐ Local switching, central authentication
- Buttons:** New, Remove, Save

13. Conecte los adaptadores de energía a los puntos de acceso inalámbricos **LAP-PT** (conecte los 3 adaptadores)



14. En **Laptop2**, **Laptop3**, **Laptop4** y **5**, coloque el módulo **PT-LAPTOP-NM-1W-AC** y conecte 2 laptops en la red **ESTUDIANTES** y 2 laptops en la red **DOCENTES**

Laptop2 Configuration - Wireless0

- GLOBAL** > **Config** > **Wireless0**
- Port Status:** ☒ On
- Bandwidth:** 300 Mbps
- Algorithm Settings:** 000C.CFE0.976A
- MAC Address:** 000C.CFE0.976A
- SSID:** ESTUDIANTES
- Authentication:**
 - ☒ WPA2-PSK, **PSK Pass Phrase:** Mochileros
 - ☐ WPA, ☐ WPA2
- User ID:** , **Password:**
- Encryption Type:** AES

Laptop5 Configuration - Wireless0

- GLOBAL** > **Config** > **Wireless0**
- Port Status:** ☒ On
- Bandwidth:** 300 Mbps
- Algorithm Settings:** 0090.0CE4.8CD0
- MAC Address:** 0090.0CE4.8CD0
- SSID:** DOCENTES
- Authentication:**
 - ☒ WPA2-PSK, **PSK Pass Phrase:** Evaluaciones
 - ☐ WPA, ☐ WPA2
- User ID:** , **Password:**
- Encryption Type:** AES

15. Revise las direcciones IP obtenidas de forma automática por [Laptop2](#), [Laptop3](#), [Laptop4](#) y [Laptop5](#).

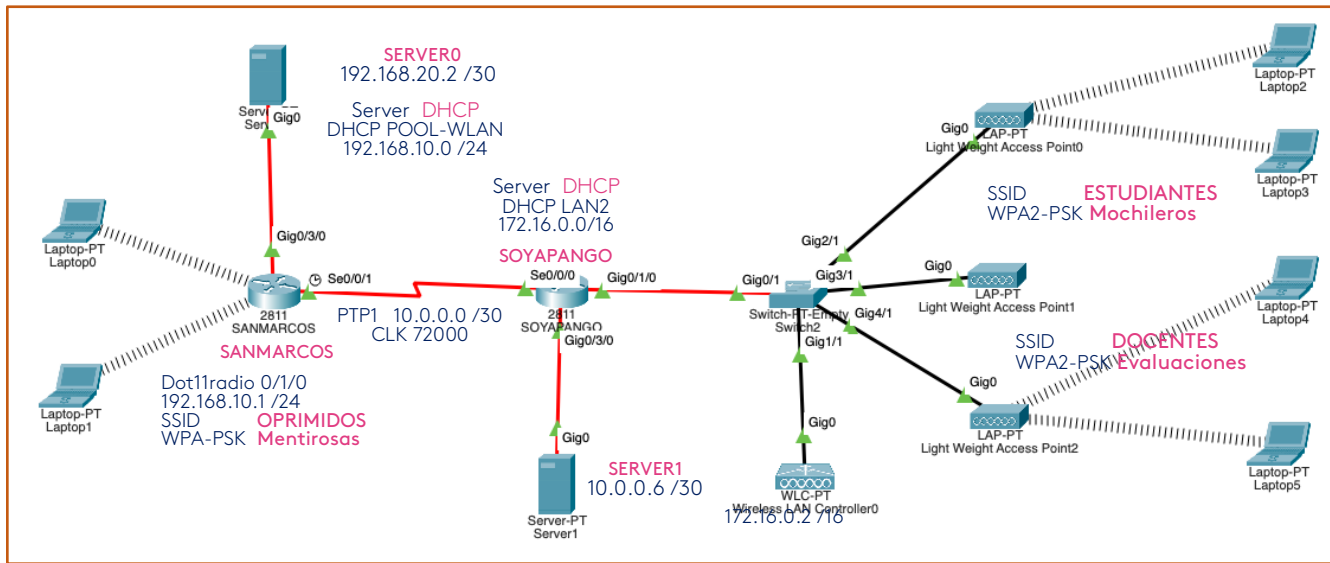
Laptop2					Laptop5				
Physical	Config	Desktop	Programming	Attributes	Physical	Config	Desktop	Programming	Attributes
IP Configuration					IP Configuration				
<input checked="" type="radio"/> DHCP <input type="radio"/> Static					<input checked="" type="radio"/> DHCP <input type="radio"/> Static				
IPv4 Address: 172.16.0.56					IPv4 Address: 172.16.0.54				
Subnet Mask: 255.255.0.0					Subnet Mask: 255.255.0.0				
Default Gateway: 172.16.0.1					Default Gateway: 172.16.0.1				
DNS Server: 10.0.0.6					DNS Server: 10.0.0.6				

16. Haga pruebas de conectividad entre todos los dispositivos (pruebas de ping),
¡todas deberán ser exitosas!

Laptop5					Laptop5				
Physical	Config	Desktop	Programming	Attributes	Physical	Config	Desktop	Programming	Attributes
<pre>C:\>ping 192.168.10.51 Pinging 192.168.10.51 with 32 bytes of data: Reply from 192.168.10.51: bytes=32 time=46ms TTL=126 Reply from 192.168.10.51: bytes=32 time=51ms TTL=126 Reply from 192.168.10.51: bytes=32 time=42ms TTL=126 Reply from 192.168.10.51: bytes=32 time=36ms TTL=126</pre>					<pre>C:\>ping 192.168.20.2 Pinging 192.168.20.2 with 32 bytes of data: Reply from 192.168.20.2: bytes=32 time=40ms TTL=126 Reply from 192.168.20.2: bytes=32 time=54ms TTL=126 Reply from 192.168.20.2: bytes=32 time=39ms TTL=126 Reply from 192.168.20.2: bytes=32 time=44ms TTL=126</pre>				

Laptop0					Laptop0				
Physical	Config	Desktop	Programming	Attributes	Physical	Config	Desktop	Programming	Attributes
<pre>C:\>ping 172.16.0.57 Pinging 172.16.0.57 with 32 bytes of data: Reply from 172.16.0.57: bytes=32 time=49ms TTL=126 Reply from 172.16.0.57: bytes=32 time=54ms TTL=126 Reply from 172.16.0.57: bytes=32 time=51ms TTL=126 Reply from 172.16.0.57: bytes=32 time=51ms TTL=126</pre>					<pre>C:\>ping 10.0.0.6 Pinging 10.0.0.6 with 32 bytes of data: Reply from 10.0.0.6: bytes=32 time=48ms TTL=126 Reply from 10.0.0.6: bytes=32 time=18ms TTL=126 Reply from 10.0.0.6: bytes=32 time=8ms TTL=126 Reply from 10.0.0.6: bytes=32 time=8ms TTL=126</pre>				

GRUPOS WLAN WCONTROLLER



17. En el controlador Wireless, genere los grupos para asociar las redes inalámbricas **ESTUDIANTES** y **DOCENTES** con puntos de acceso como se muestra

GLOBAL

Physical

Config

Attributes

Settings

Wireless LANs

AP Groups

DHCP

INTERFACE

GigabitEthernet0

Management

1

2

3

Select AP Group

Name

GRUPO ESTUDIANTES

Wireless LANs

Each Wireless LAN can belong to multiple AP groups.

In AP Group	Name	SSID
<input type="checkbox"/>	WIFI-DOCENTES	DOCENTES
<input checked="" type="checkbox"/>	WIFI-ESTUDIANTES	ESTUDIANTES

Access Points

In AP Group	Name	MAC Address	Status
<input checked="" type="checkbox"/>	Light Weight Access Point0	0006.2ABA.5301	Online
<input checked="" type="checkbox"/>	Light Weight Access Point1	000C.8513.6601	Online
<input type="checkbox"/>	Light Weight Access Point2	0001.42E4.8501	Online

New Remove Save

GLOBAL

Physical

Config

Attributes

Settings

Wireless LANs

AP Groups

DHCP

INTERFACE

GigabitEthernet0

Management

1

2

3

Select AP Group

Name

GRUPO DOCENTES

Wireless LANs

Each Wireless LAN can belong to multiple AP groups.

In AP Group	Name	SSID
<input checked="" type="checkbox"/>	WIFI-DOCENTES	DOCENTES
<input type="checkbox"/>	WIFI-ESTUDIANTES	ESTUDIANTES

Access Points

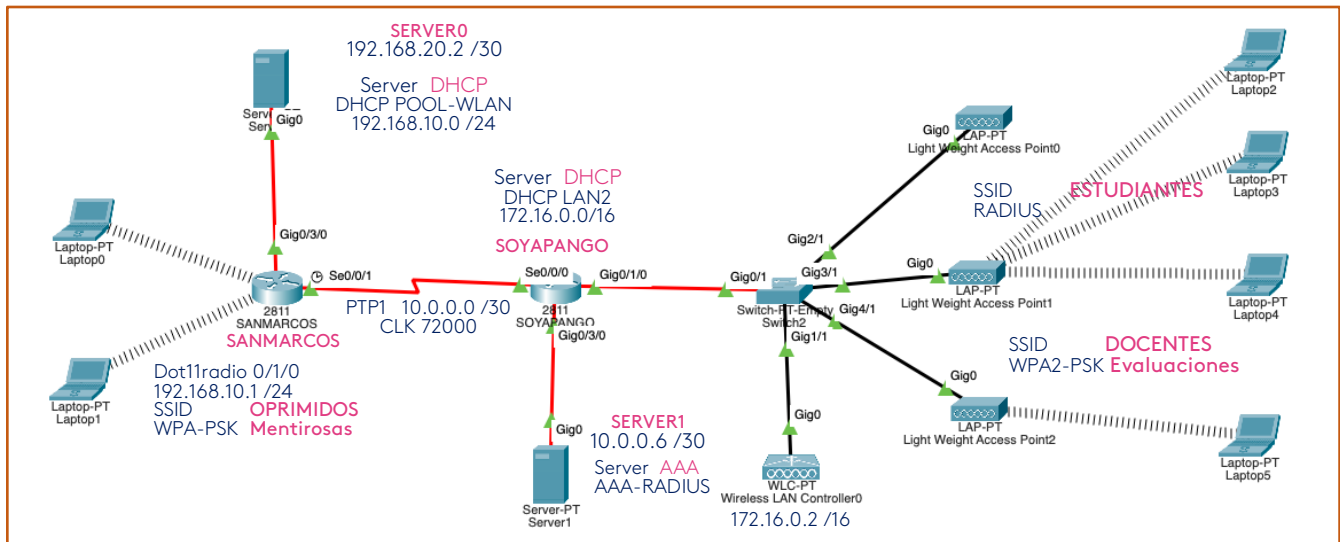
In AP Group	Name	MAC Address	Status
<input type="checkbox"/>	Light Weight Access Point0	0006.2ABA.5301	Online
<input type="checkbox"/>	Light Weight Access Point1	000C.8513.6601	Online
<input checked="" type="checkbox"/>	Light Weight Access Point2	0001.42E4.8501	Online

New Remove Save

18. Observe el cambio de conexiones en las redes inalámbricas

PROTOCOLO AAA (RADIUS) – WLAN WCONTROLLER

RADIUS (Remote Authentication Dial-In User Service) es un protocolo de red que se utiliza para la autenticación, autorización y contabilidad de usuarios que acceden a la topología por medio de una red inalámbrica.



19. Configure en **server0** el protocolo AAA (**Radius**) el cual será empleado en la red inalámbrica **ESTUDIANTES**.

Server1

SERVICES

Physical Config **Services** Desktop Programming Attributes

AAA

Service ☒ On ☐ Off Radius Port 1645

Network Configuration

Client Name Client IP

Secret ServerType Radius

	Client Name	Client IP	Server Type	Key
1	UDB-REC104	172.16.0.2	Radius	BERRINCHE

Add Save

User Setup

Username Password

	Username	Password
1	Kelly	Shortyparty
2	Maluma	Feliceslos4
3	Yanira	Corazonbello

Add Save Remove

Protocolo AAA

- Establecer conexión cifrada por contraseña (BERRINCHE) entre server1 y el controlador wireless
- Crear usuarios y sus respectivas contraseñas en el servidor para que puedan tener acceso hacia toda la topología desde la red inalámbrica.

Cuando un usuario intenta conectarse a una red inalámbrica, el dispositivo de red solicita al usuario sus credenciales de autenticación, nombre de usuario y contraseña. El dispositivo de red envía estas credenciales a un servidor RADIUS para su verificación.

- Si las credenciales son válidas el usuario tiene acceso a la red.
- Si las credenciales son incorrectas el usuario no puede acceder a la red.

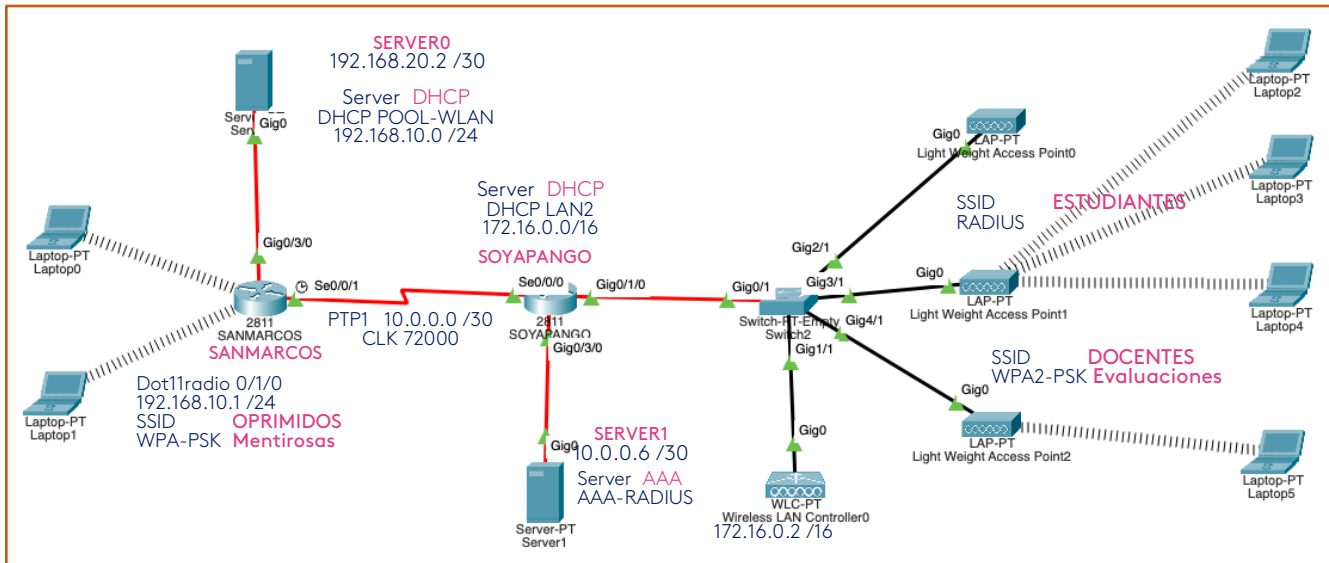
20. En el controlador Wireless, configure la red inalámbrica **ESTUDIANTES** para que el acceso a la topología sea con autenticación y validación **Radius**.

Protocolo AAA

- Establecer conexión cifrada por contraseña (BERRINCHE) entre server1 y el controlador Wireless.
- La red inalámbrica estudiantes será validada y autenticada con el servidor AAA

21. Configure los ordenadores **Laptop2**, **Laptop3** y **Laptop4** con los usuarios **AAA-radius** configurados en el **server1**.

22. Nuevamente haga pruebas de conectividad desde las laptops las redes inalámbricas **DOCENTES** y **ESTUDIANTES**. hacia los servidores y las laptops de la red **OPRIMIDOS**

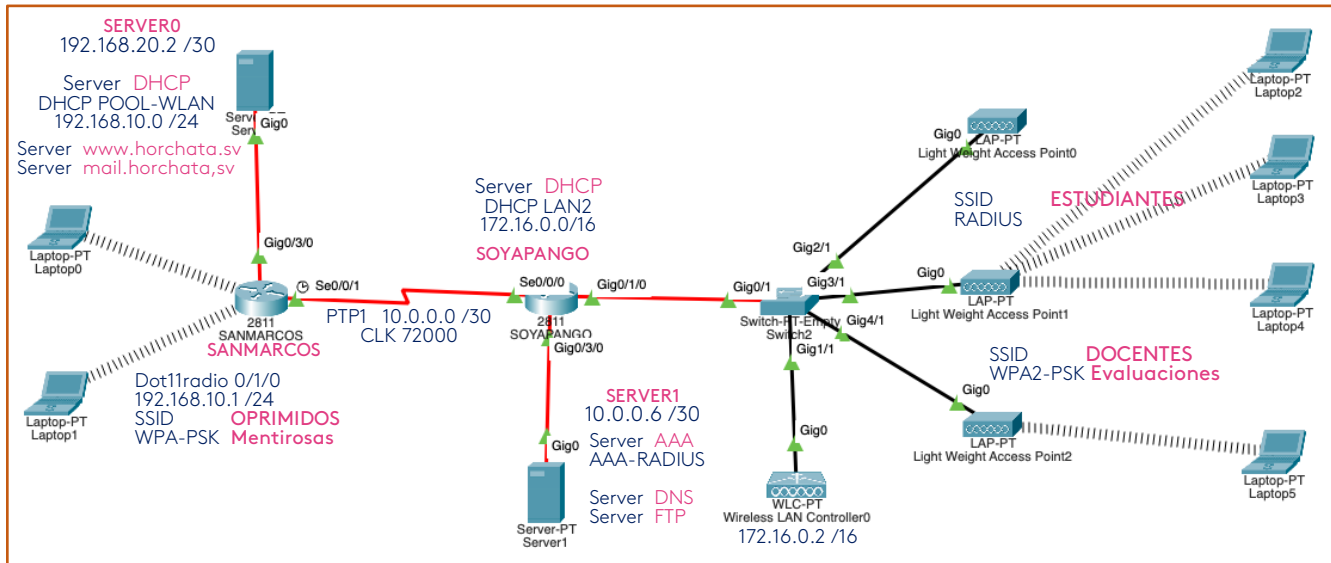


Laptop5	Laptop5
<pre> C:\>ping 192.168.10.51 Pinging 192.168.10.51 with 32 bytes of data: Reply from 192.168.10.51: bytes=32 time=46ms TTL=126 Reply from 192.168.10.51: bytes=32 time=51ms TTL=126 Reply from 192.168.10.51: bytes=32 time=42ms TTL=126 Reply from 192.168.10.51: bytes=32 time=36ms TTL=126 </pre>	<pre> C:\>ping 192.168.20.2 Pinging 192.168.20.2 with 32 bytes of data: Reply from 192.168.20.2: bytes=32 time=40ms TTL=126 Reply from 192.168.20.2: bytes=32 time=54ms TTL=126 Reply from 192.168.20.2: bytes=32 time=39ms TTL=126 Reply from 192.168.20.2: bytes=32 time=44ms TTL=126 </pre>

Laptop2	Laptop2
<pre> C:\>ping 192.168.20.2 Pinging 192.168.20.2 with 32 bytes of data: Reply from 192.168.20.2: bytes=32 time=8ms TTL=126 Reply from 192.168.20.2: bytes=32 time=8ms TTL=126 Reply from 192.168.20.2: bytes=32 time=5ms TTL=126 Reply from 192.168.20.2: bytes=32 time=7ms TTL=126 </pre>	<pre> C:\>ping 192.168.10.50 Pinging 192.168.10.50 with 32 bytes of data: Reply from 192.168.10.50: bytes=32 time=27ms TTL=126 Reply from 192.168.10.50: bytes=32 time=49ms TTL=126 Reply from 192.168.10.50: bytes=32 time=18ms TTL=126 Reply from 192.168.10.50: bytes=32 time=17ms TTL=126 </pre>

TAREA COMPLEMENTARIA

1. Asegure la comunicación entre los routers Soyapango y San Marcos, haciendo uso de autenticación md5 en la red PTP1



2. Una vez establecida la comunicación entre todas redes, active el servicio DNS en **server1** y asigne nombre a los dispositivos de la siguiente manera.

Wireless controller	Server0	Server
wlc	www.horchata.sv	ftp.horchata.sv

3. Deberá realizar pruebas de conexión desde **Laptop4** a los nombres de los dispositivos.
4. Levante/active el servicio FTP en **server1**, deberá crear dos usuarios/clientes y configurar como se muestra a continuación.
 Usuario: Rosalia Password: Motomami (Todos los permisos)
 Usuario: su-apellido Password: Nambechele (Todos los permisos)
5. Levante/active el servicio de **correo electrónico** en **server0**, con el dominio **horchata.sv**, utilice como servidor entrante y saliente el puntero configurado en DNS **www.horchata.sv**
 Usuario: ozuna Password: criminal **Laptop1**
 Usuario: benito Password: yonaguni **Laptop3**

6. En `server0` Habilite el servicio HTTP en el servidor y personalice la página www.horchata.sv de tal manera que aparezcan sus apellidos, carnet, grupo de laboratorio y el escudo del Barcelona.
7. En `router soyapango` configure el servicio SSH para las 15 líneas digitales, password: **perversa** Dominio: **horchata.sv**, key **rsa**, **2048**, SSH v2, user: **tilin**, privilegios 15