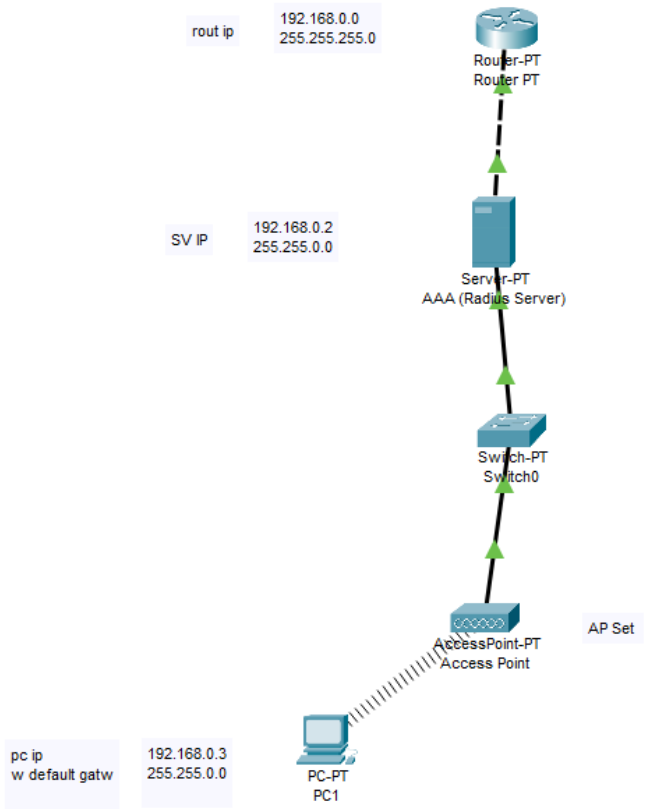
Laboratorio #5 Realizado por Adrian Molano

Fecha: 23/06/2025

En este ejercicio se implementa una red WiFi para una empresa mediana utilizando Packet Tracer. La topología incluye:

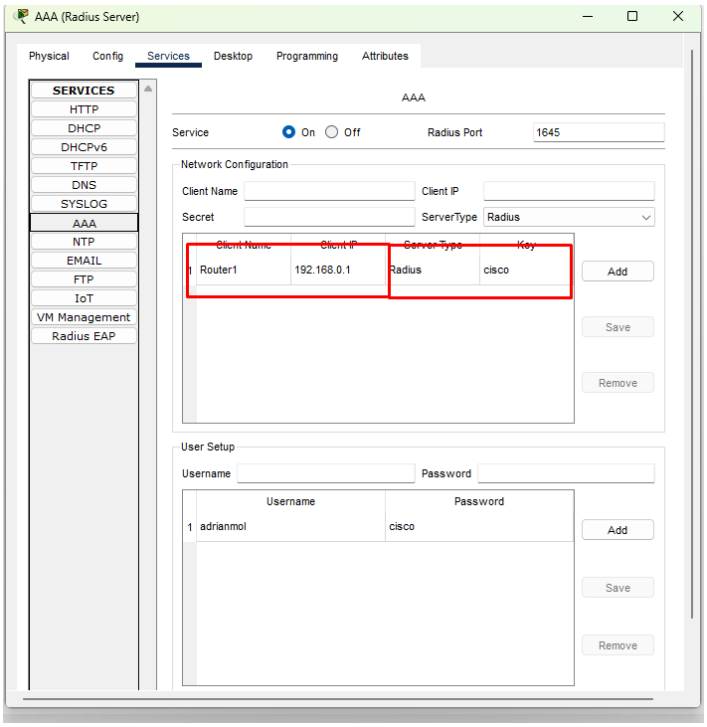
- 1 Router (puerta de enlace con DHCP)
- 1 Switch
- 1 Punto de Acceso WiFi
- 1 Servidor RADIUS (para autenticar usuarios)
-

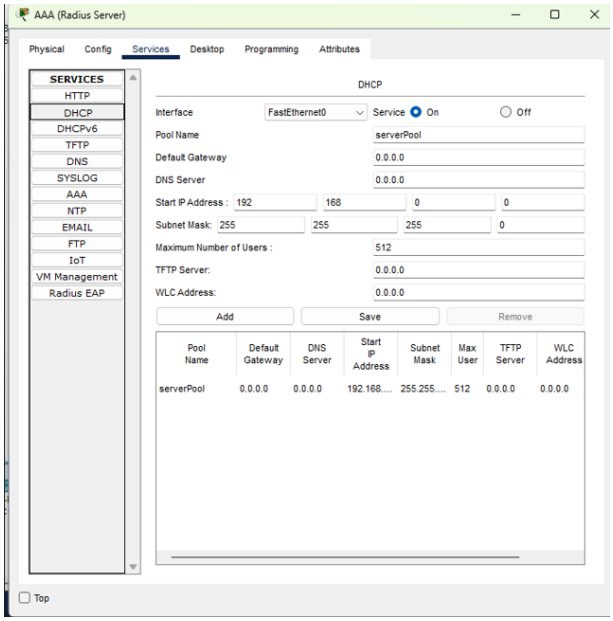


Configuración del servidor RADIUS

Se configuró el servidor para autenticar usuarios mediante RADIUS:

- **Servicio RADIUS activado** en Services → AAA.
- Usuario creado: adrianmol/cisco
- Dirección IP del servidor RADIUS: 192.168.0.2
- Clave compartida entre RADIUS y AP: cisco123





En esta configuración se ha habilitado el esquema de autenticación centralizada mediante AAA y RADIUS.

Primero, se activó el servicio AAA en el router con el comando aaa new-model. Luego, se registró el servidor RADIUS en el router indicando su IP y la clave compartida, que en este caso es “cisco”. Después, se configuró AAA para autenticar las sesiones de login utilizando el grupo RADIUS definido.

A continuación, se aplicó este método de autenticación AAA a las líneas VTY, que corresponden al acceso remoto por Telnet o SSH, mediante el comando login authentication AAA. Finalmente, se guardó la configuración en la memoria NVRAM del router utilizando write memory.

En resumen, se implementó un esquema AAA que utiliza un servidor RADIUS para autenticar a los usuarios que acceden remotamente al router por las líneas VTY, mejorando la seguridad y centralizando la gestión de usuarios.

RADIUS vs. TACACS+

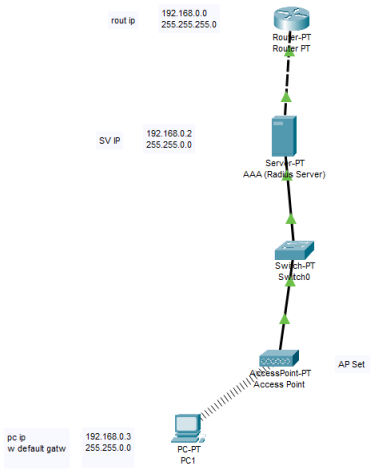
- **RADIUS:**
  Usa UDP, autentica usuarios y es ideal para WiFi y usuarios remotos. **(el mas adecuado)**
- **TACACS+:**
  Usa TCP, separa autenticación, autorización y contabilidad. Ideal para administración de equipos de red.

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#aaa new-model
Router(config)#radius-server host 192.168.0.2 key cisco
Router(config)#aaa authentication login AAA group radius
Router(config)#line vty 0 4
Router(config-line)#login authentication AAA
Router(config-line)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
exit
```

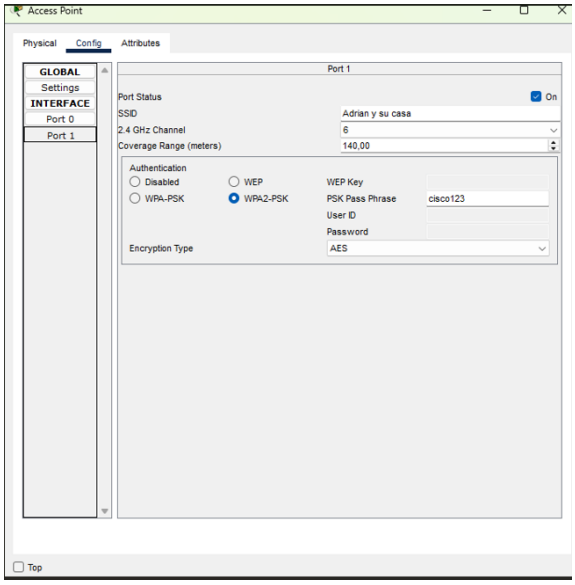
Testeo de pingeo entre las ip's

Fueron organizadas de esta manera DHCP // IP static desde el router al Wireless pc

- Router 192.168.0.1
- Server 192.168.0.2
- PC 192.168.0.3
- El AP y el Servidor compartían contraseña de cifrado "cisco"



Conexión Exitosa entre el AP y el dispositivo, cabe aclarar que toco añadirle un modulo WMP300N para poder conectarlo directamente.



Riesgos y contramedidas

Riesgos:

- Interceptación de tráfico inalámbrico
- Ataques Evil Twin
- Contraseñas débiles (en WPA2-PSK)

Contramedidas:

- Usar WPA2-Enterprise/Personal para evitar PSK
- Autenticación centralizada por RADIUS
- Usar EAP-TLS si es posible
- Configuración de VLANs y filtrado MAC