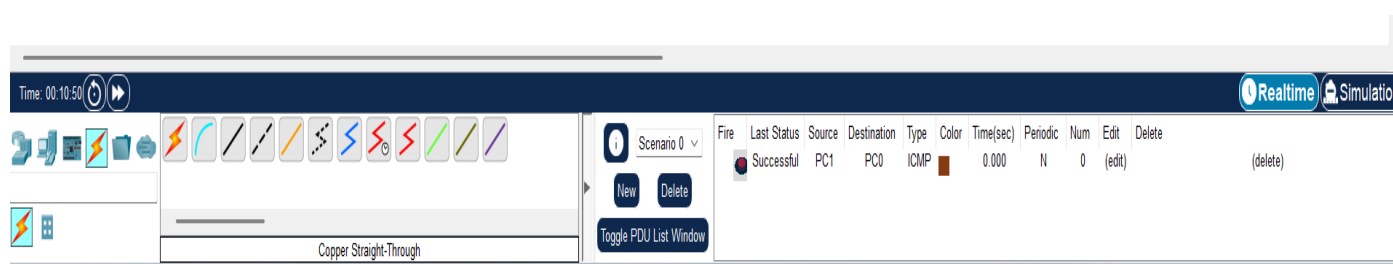
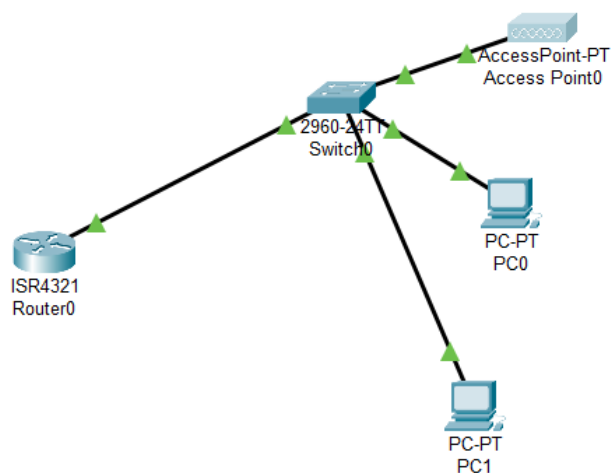


Rigoberto Márquez

Cisco Packet Tracer

Entrando a Packet Tracer y configurando:



Configuración para el router:

Router0

Physical **Config** CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0/0

GigabitEthernet0/0/1

GigabitEthernet0/0/0

Port Status ☒ On

Bandwidth ☐ 1000 Mbps ☒ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address 0010.11B4.0D01

IP Configuration

IPv4 Address 192.168.1.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Configurando el Acces Point:

Access Point0

Physical **Config** Attributes

GLOBAL

Settings

INTERFACE

Port 0

Port 1

Port 1

Port Status ☒ On

SSID Fam Marquez

2.4 GHz Channel 6

Coverage Range (meters) 140,00

Authentication

☐ Disabled ☐ WEP ☒ WPA2-PSK

WEP Key

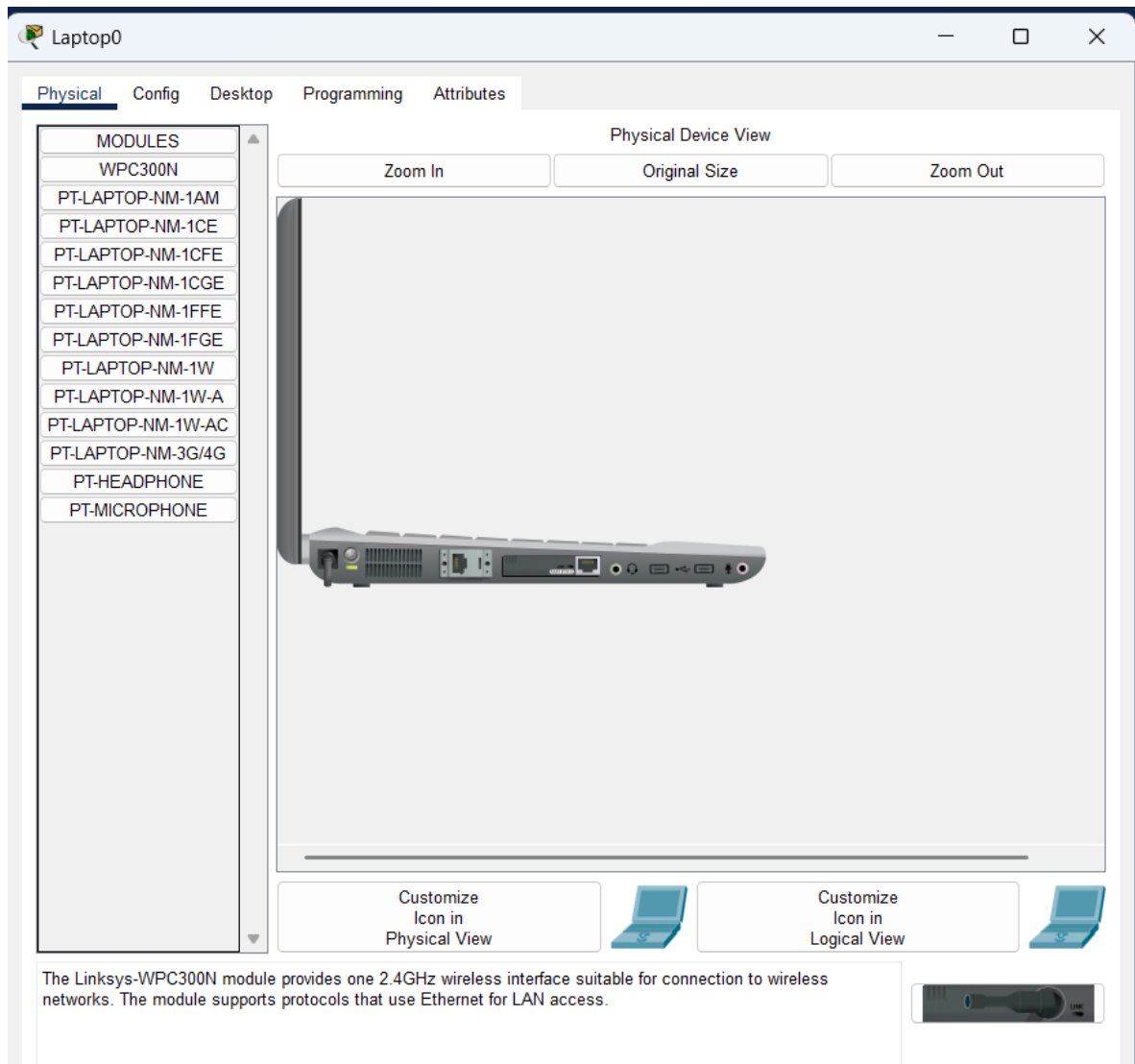
PSK Pass Phrase 12345678

User ID

Password

Encryption Type AES

Configuraciones de la laptop:



Habilitar wifi:

Physical Config Desktop Programming Attributes

Physical Device View

Zoom In Original Size Zoom Out

MODULES

- WPC300N
- PT-LAPTOP-NM-1AM
- PT-LAPTOP-NM-1CE
- PT-LAPTOP-NM-1CFE
- PT-LAPTOP-NM-1CGE
- PT-LAPTOP-NM-1FFE
- PT-LAPTOP-NM-1FGE
- PT-LAPTOP-NM-1W
- PT-LAPTOP-NM-1W-A
- PT-LAPTOP-NM-1W-AC
- PT-LAPTOP-NM-3G/4G
- PT-HEADPHONE
- PT-MICROPHONE

The Linksys-WPC300N module provides one 2.4GHz wireless interface suitable for connection to wireless networks. The module supports protocols that use Ethernet for LAN access.

Customize Icon in Physical View

Customize Icon in Logical View

El desktop de la laptop:

Laptop0

Physical Config Desktop Programming Attributes

Link Information Connect Profiles

No association with access point

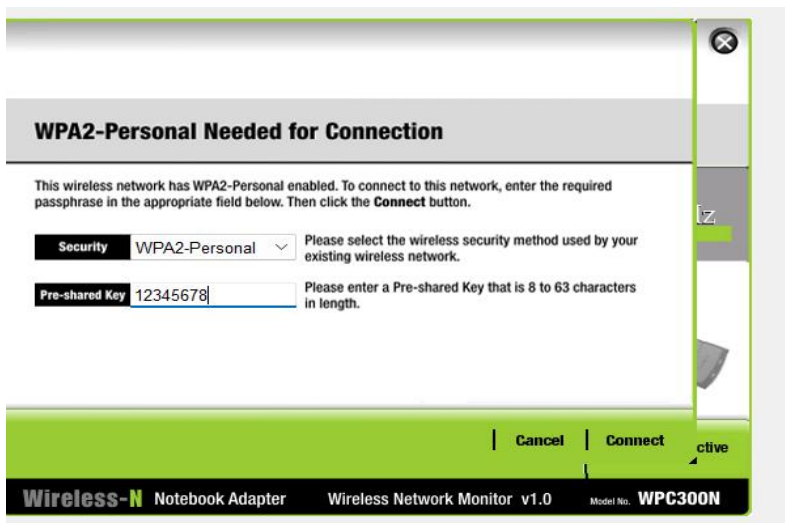
2.4GHz

Signal Strength Link Quality

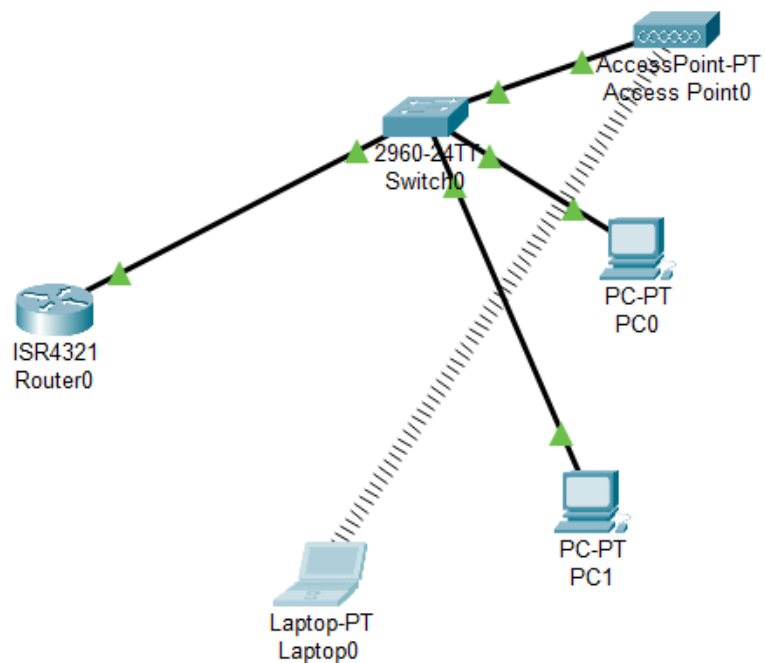
Wireless-N Notebook Adapter Wireless Network Monitor v1.0 Model No. WPC300N

Adapter is inactive



Conectándose a la red que creamos:

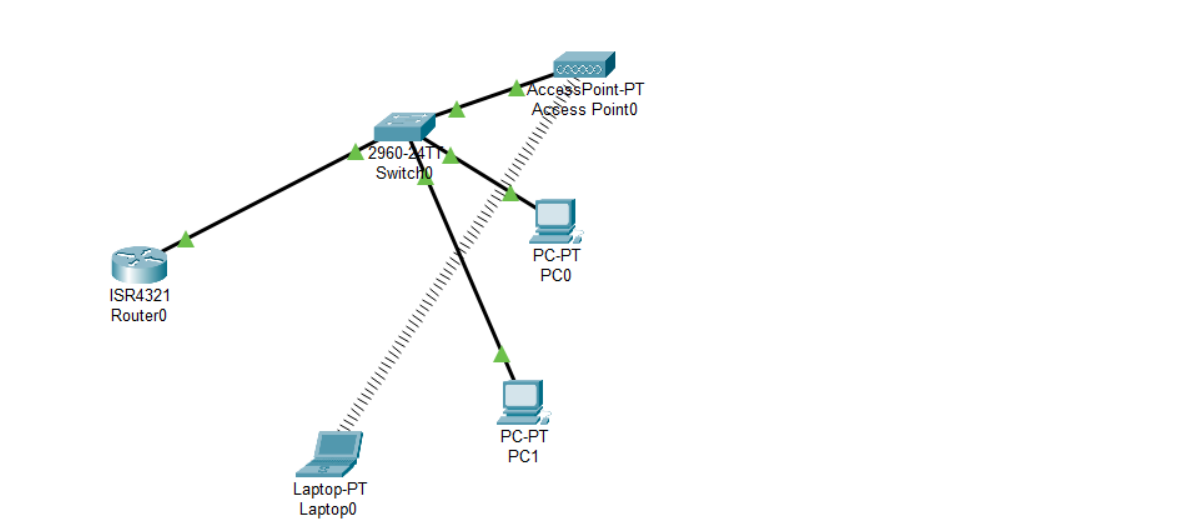


Mirar la conexión:





Ya la Laptop se puede comunicas con las pc:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Laptop0	PC1	ICMP		0.000	N	0	(edit)	

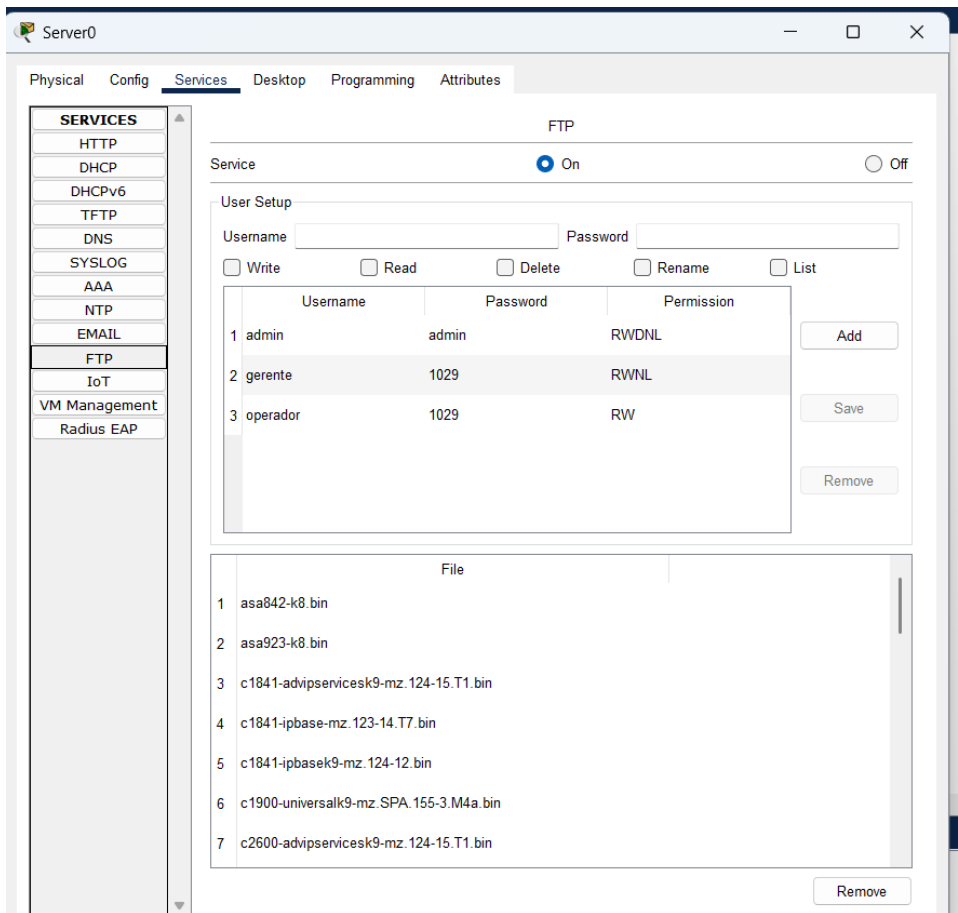


Scenario 0

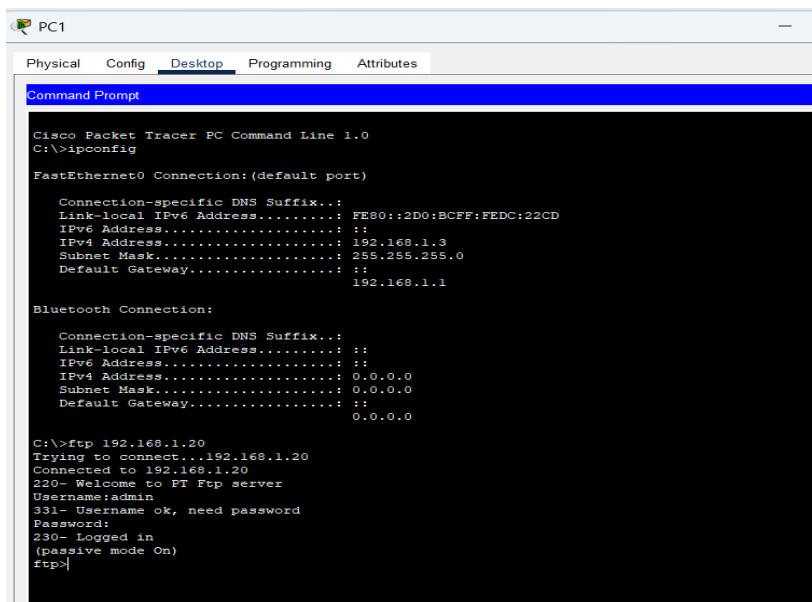
NewDelete

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Laptop0	PC1	ICMP		0.000	N	0	(edit)	(delete)

Crear servidor



Conexión al servidor ftp desde una de las pc



Listando:

```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
Trying to connect to 192.168.1.20
Connected to 192.168.1.20
220- Welcome to FT Ftp server
Username:admin
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir

Listing /ftp directory from 192.168.1.20:
0 : asa842-k8.bin 5571584
1 : asa923-k8.bin 30468096
2 : cl841-advipservicesk9-mz.124-15.T1.bin 33591768
3 : cl841-ipbase-mz.123-14.T7.bin 13832032
4 : cl841-ipbasek9-mz.124-12.bin 16599160
5 : cl900-universalk9-mz.SPA.155-3.M4a.bin 33591768
6 : c2600-advipservicesk9-mz.124-15.T1.bin 33591768
7 : c2600-i-mz.122-28.bin 5571584
8 : c2600-ipbasek9-mz.124-8.bin 13169700
9 : c2800nm-advipservicesk9-mz.124-15.T1.bin 50938004
10 : c2800nm-advipservicesk9-mz.151-4.M4.bin 33591768
11 : c2800nm-ipbase-mz.123-14.T7.bin 5571584
12 : c2800nm-ipbasek9-mz.124-8.bin 15522644
13 : c2900-universalk9-mz.SPA.155-3.M4a.bin 33591768
14 : c2950-i6q412-mz.121-22.EA4.bin 3058048
15 : c2950-i6q412-mz.121-22.EA8.bin 3117390
16 : c2960-lanbase-mz.122-25.FX.bin 4414921
17 : c2960-lanbase-mz.122-25.SEE1.bin 4670455
18 : c2960-lanbasek9-mz.150-2.SE4.bin 4670455
19 : c3560-advipservicesk9-mz.122-37.SE1.bin 8662192
20 : c3560-advipservicesk9-mz.122-46.SE.bin 10713279
21 : c800-universalk9-mz.SPA.152-4.M4.bin 33591768
22 : c800-universalk9-mz.SPA.154-3.M6a.bin 83029236
23 : cat3k_caa-universalk9.16.03.02.SPA.bin 505532849
24 : cgr1000-universalk9-mz.SPA.154-2.CG 159487552
25 : cgr1000-universalk9-mz.SPA.156-3.CG 184530138
26 : ir800-universalk9-bundle.SPA.156-3.M.bin 160968869
27 : ir800-universalk9-mz.SPA.155-3.M 61750062
28 : ir800-universalk9-mz.SPA.156-3.M 63753767
29 : ir800_yocto-1.7.2.tar 2877440
30 : ir800_yocto-1.7.2_python-2.7.3.tar 6912000
31 : pt1000-i-mz.122-28.bin 5571584
32 : pt3000-i6q412-mz.121-22.EA4.bin 3117390
ftp>
```

Borrando un archivo con los permisos de admin:

```
230- Logged in
(passive mode On)
ftp>delete asa842-k8.bin

Deleting file asa842-k8.bin from 192.168.1.20: ftp>
[Deleted file asa842-k8.bin successfully ]
ftp>dir

Listing /ftp directory from 192.168.1.20:
0 : asa923-k8.bin 30468096
1 : cl841-advipservicesk9-mz.124-15.T1.bin 33591768
2 : cl841-ipbase-mz.123-14.T7.bin 13832032
3 : cl841-ipbasek9-mz.124-12.bin 16599160
4 : cl900-universalk9-mz.SPA.155-3.M4a.bin 33591768
5 : c2600-advipservicesk9-mz.124-15.T1.bin 33591768
6 : c2600-i-mz.122-28.bin 5571584
7 : c2600-ipbasek9-mz.124-8.bin 13169700
8 : c2800nm-advipservicesk9-mz.124-15.T1.bin 50938004
```


Vemos que si usamos otro usuario que tiene otros permisos distintos nos niegan ciertas cosas. En este caso, borrar algo.

```
C:\>ftp 192.168.1.20
Trying to connect...192.168.1.20
Connected to 192.168.1.20
220- Welcome to PT Ftp server
Username:gerente
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>delete pt1000-i-mz.122-28.bin

Deleting file pt1000-i-mz.122-28.bin from 192.168.1.20: ftp>
%Error ftp://192.168.1.20/pt1000-i-mz.122-28.bin (No such file or directory Or Permission denied)
550-Requested action not taken. permission denied).

ftp>
```

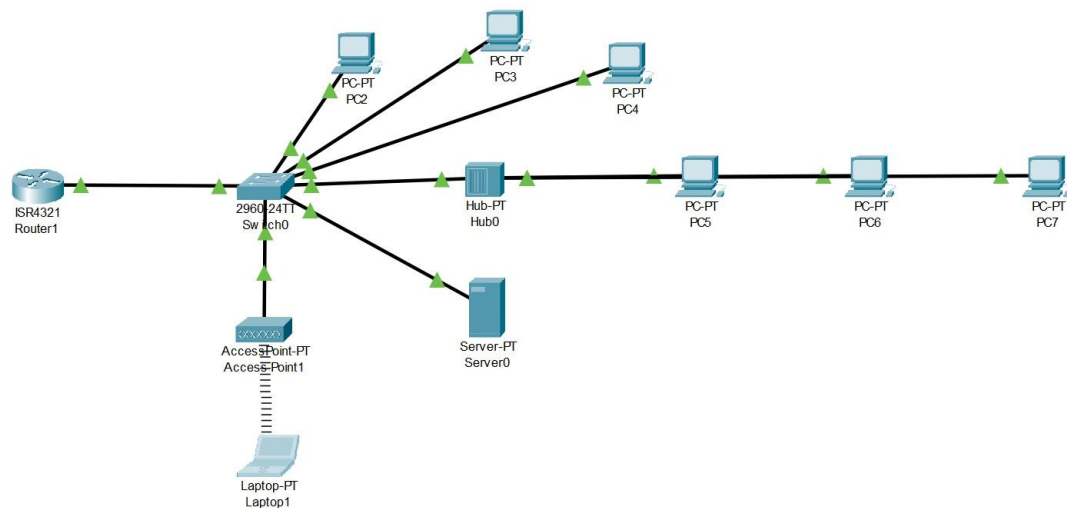
Vemos que el usuario operador no tiene permisos de listar.

```
ftp>
ftp 192.168.1.20
Trying to connect...192.168.1.20
Connected to 192.168.1.20
220- Welcome to PT Ftp server
Username:operador
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir

Listing /ftp directory from 192.168.1.20:
%Error ftp://192.168.1.20/ (No such file or directory Or Permission denied)
550-Requested action not taken. permission denied).

ftp>
```

Finalmente:



Apuntes:

Existen varios tipos de autenticación, cada uno con sus propias características y niveles de seguridad:

Autenticación basada en contraseña

Autenticación de dos factores

Autenticación biométrica

Autenticación basada en certificados

Tipos de autenticación

¿Qué es RADIUS?

RADIUS es un protocolo de red que se utiliza principalmente para autenticar, autorizar y contabilizar a usuarios y dispositivos que se conectan a una red. Su nombre, en español, significa "Servicio de usuario de marcación remota para autenticación". A pesar de su nombre, su uso se ha extendido más allá de las conexiones dial-up y ahora se utiliza en una amplia variedad de escenarios de red .

¿Cómo funciona RADIUS?

La operación de RADIUS se basa en un modelo cliente-servidor:

- 1.Solicitud de acceso
- 2.Envío de solicitud al servidor RADIUS
- 3.Autenticación
- 4.Autorización
- 5.Contabilidad

Tipos de autenticación

TACACS+ (Terminal Access Controller Access-Control System Plus)

TACACS+ es un protocolo de red de autenticación, autorización y contabilidad (AAA) que proporciona un nivel de seguridad y granularidad más alto que RADIUS. Se utiliza principalmente para autenticar y autorizar el acceso a dispositivos de red como routers, switches y servidores. A diferencia de RADIUS, TACACS+ separa las funciones de autenticación, autorización y contabilidad en servicios independientes, lo que ofrece una mayor flexibilidad y seguridad.

Funcionamiento de TACACS+

El funcionamiento de TACACS+ se basa en un modelo cliente-servidor similar a RADIUS, pero con algunas diferencias clave:

1. Solicitud de acceso
2. Envío de solicitud al servidor TACACS+
3. Autenticación
4. Autorización
5. Contabilidad

Tipos de autenticación

Cifrado

El cifrado es una técnica que convierte los datos en un formato ininteligible para cualquier persona que no tenga la clave de descifrado. En el contexto de los protocolos de autenticación, el cifrado se utiliza para proteger la confidencialidad de los datos transmitidos, como nombres de usuario y contraseñas.

- **Tipos de cifrado:**
 - Cifrado simétrico
 - Cifrado asimétrico
- **Protocolos de cifrado:**
 - TLS/SSL: Es el estándar de facto para el cifrado de comunicaciones en Internet. Se utiliza para proteger la comunicación entre un cliente y un servidor.
 - IPsec: Es un conjunto de protocolos que proporciona seguridad a nivel de red, incluyendo cifrado, autenticación e integridad de datos.

Seguridad en redes inalámbricas (WEP, WPA, WPA2)

redes inalámbricas

El Protocolo TKIP (Temporal Key Integrity Protocol)

TKIP es una parte fundamental de WPA. Su función principal es proporcionar integridad de datos y protección contra ataques de repetición.

- **Generación de claves de sesión:** TKIP genera una clave de sesión única para cada paquete de datos, lo que dificulta enormemente los ataques de descifrado.
- **MIC (Message Integrity Check):** TKIP incluye un código de autenticidad de mensaje (MIC) que se adjunta a cada paquete. Este MIC permite verificar la integridad de los datos y detectar cualquier modificación realizada por un atacante.
- **Replays:** TKIP utiliza un mecanismo de protección contra repeticiones para evitar que los atacantes retransmitan paquetes antiguos.

¿Cómo funciona TKIP?

Generación de la clave de sesión: Se genera una clave de sesión única para cada paquete, utilizando la clave maestra compartida y un valor de inicialización (IV).

Cálculo del MIC: Se calcula un MIC para el paquete de datos utilizando la clave de sesión y se adjunta al paquete.

Transmisión del paquete: El paquete cifrado y con el MIC se transmite a través del enlace inalámbrico.

Verificación del MIC: El receptor calcula su propio MIC para el paquete y lo compara con el MIC recibido. Si los MIC coinciden, el paquete se considera auténtico y se descifra.

Seguridad en redes inalámbricas (WEP, WPA, WPA2)

redes inalámbricas

Análisis Detallado

- **WEP:** Como ya hemos visto, WEP es el protocolo más antiguo y menos seguro. Sus claves estáticas, el algoritmo de cifrado débil RC4 y la falta de protección de integridad lo hacen extremadamente vulnerable a ataques.
- **WPA:** WPA representó un gran avance respecto a WEP, introduciendo claves temporales y el protocolo TKIP para mejorar la seguridad. Sin embargo, TKIP aún presentaba algunas vulnerabilidades, y RC4 seguía siendo un algoritmo de cifrado relativamente débil.
- **WPA2:** WPA2 es el sucesor de WPA y se considera el estándar de oro en seguridad Wi-Fi. El uso de AES y CCMP proporciona una protección mucho más robusta contra ataques, y el protocolo de autenticación es más seguro.

Recomendación

Siempre que sea posible, utiliza WPA2. Es el protocolo más seguro y compatible con la mayoría de los dispositivos modernos. Si tu router no admite WPA2, WPA es una mejor opción que WEP. Sin embargo, debes tener en cuenta que WPA también tiene sus limitaciones y puede ser vulnerable a ciertos tipos de ataques.

Consideraciones Adicionales

- **WPA3:** Es el protocolo más reciente y ofrece un nivel de seguridad aún mayor que WPA2. Sin embargo, la compatibilidad con WPA3 puede ser limitada en algunos dispositivos.
- **Configuraciones de seguridad:** Además del protocolo de seguridad, es importante configurar correctamente tu red Wi-Fi. Utiliza contraseñas fuertes, oculta el SSID (nombre de la red) y mantén tu firmware actualizado.

En resumen, WPA2 es la mejor opción para la mayoría de los usuarios. Ofrece un equilibrio óptimo entre seguridad y rendimiento y es compatible con una amplia gama de dispositivos.

Seguridad en redes inalámbricas (WEP, WPA, WPA2)

redes inalámbricas

Mejores prácticas para la seguridad en redes inalámbricas

- Uso de WPA3, ocultación del SSID, filtrado de MAC.

1. Utilizar WPA3:

- **La última generación:** WPA3 es el protocolo de seguridad Wi-Fi más reciente y robusto. Ofrece características avanzadas de seguridad, como la autenticación simultánea de prueba (Simultaneous Authentication of Equals, SAE), que es más resistente a ataques de fuerza bruta.
- **Protección mejorada:** WPA3 proporciona una protección significativamente mayor contra ataques como los de diccionario y los de fuerza bruta, lo que hace que sea mucho más difícil para los atacantes comprometer la seguridad de tu red.

2. Ocultar el SSID (Nombre de Red):

- **Disminuir la visibilidad:** Al ocultar el SSID, tu red no aparecerá en la lista de redes disponibles para los dispositivos cercanos. Esto dificulta que los atacantes encuentren tu red y la intenten hackear.
- **No es una protección completa:** Ocultar el SSID es una medida de seguridad adicional, pero no es suficiente por sí sola. Los atacantes aún pueden encontrar tu red utilizando herramientas de escaneo de redes.

3. Filtrado de MAC:

- **Control de acceso:** El filtrado de MAC (Media Access Control) te permite especificar las direcciones MAC de los dispositivos que pueden conectarse a tu red. Esto puede ser útil para bloquear dispositivos no autorizados.
- **Limitaciones:** El filtrado de MAC no es una medida de seguridad infalible, ya que las direcciones MAC pueden ser falsificadas. Además, puede ser engorroso mantener una lista actualizada de direcciones MAC, especialmente en entornos con muchos dispositivos.

Seguridad en redes inalámbricas (WEP, WPA, WPA2)

redes inalámbricas

Ataques de Diccionario contra WPA/WPA2

Aunque WPA y WPA2 son mucho más seguros que WEP, aún son vulnerables a ataques de diccionario, especialmente si se utilizan contraseñas débiles.

- ¿Cómo funciona? Los atacantes utilizan una lista de palabras comunes, combinaciones de palabras y frases para intentar adivinar la contraseña de la red.
- **Contramedidas:**
 - **Contraseñas fuertes:** Utiliza contraseñas largas y complejas que combinen mayúsculas, minúsculas, números y símbolos. Evita usar palabras de diccionario, nombres propios o fechas de nacimiento.
 - **Gestores de contraseñas:** Utiliza un gestor de contraseñas para generar y almacenar contraseñas seguras de forma segura.
 - **Autenticación de dos factores:** Si tu router lo permite, habilita la autenticación de dos factores para agregar una capa adicional de seguridad.
 - **Limitar intentos de conexión:** Configura tu router para bloquear las conexiones después de un número determinado de intentos fallidos.