

## **Taller Protocolos de Seguridad**

Juan Pablo Morales, Jhonatan Steven Camacho, Enmanuel Toro Marin

Colegio de Ingeniería de Sistemas, Institución Universitaria Colegios de Colombia

Topologías de Red

Uriel Castañeda Sierra

15 de Noviembre de 2023

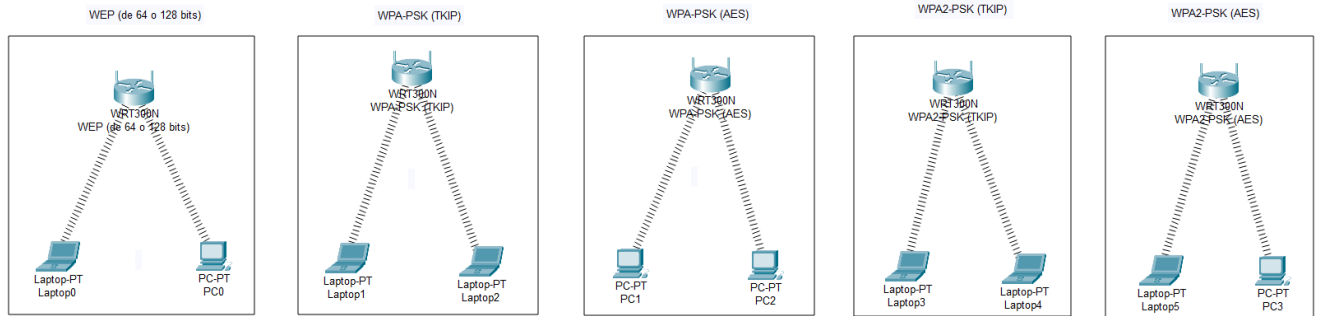
## Tabla de contenido

|   |    |
|---|----|
| Objetivos .....                           | 3  |
| Diseño global .....                       | 4  |
| Marco Teórico.....                        | 5  |
| Protocolos de seguridad inalámbrica ..... | 5  |
| WEP .....                                 | 5  |
| WPA.....                                  | 5  |
| WPA2.....                                 | 6  |
| Desarrollo de los Escenarios .....        | 7  |
| Modelo WEP (de 64 o 128 bits) .....       | 7  |
| Modelo WPA-PSK (TKIP) .....               | 10 |
| Modelo WPA-PSK (AES) .....                | 13 |
| Modelo WPA2-PSK (TKIP) .....              | 16 |
| Modelo WPA2-PSK (AES) .....               | 19 |
| Conclusiones .....                        | 22 |
| Referencias.....                          | 23 |

### **Objetivos**

- Identificar los diferentes protocolos de seguridad para redes inalámbricas.
- Comprender las características y cualidades de cada uno de los protocolos.
- Simular la configuración de los protocolos de seguridad en redes inalámbricas utilizando Packet Tracer.

## Diseño global



## **Marco Teórico**

### **Protocolos de seguridad inalámbrica**

Las redes inalámbricas (Wi-Fi) son cada vez más populares, ya que ofrecen una gran comodidad y flexibilidad. Sin embargo, también son más vulnerables a los ataques que las redes cableadas. Por ello, es importante implementar medidas de seguridad para proteger los datos que se transmiten a través de una red Wi-Fi.

Los protocolos de seguridad inalámbrica son los mecanismos que se utilizan para proteger los datos que se transmiten a través de una red Wi-Fi. Estos protocolos utilizan técnicas de cifrado para hacer que los datos sean ilegibles para los intrusos.

Los protocolos de seguridad inalámbrica más comunes son:

#### **WEP**

(Privacidad equivalente a privacidad equivalente por cable) : Es el protocolo de seguridad más antiguo y menos seguro. Utiliza un cifrado de 64 o 128 bits, que es relativamente fácil de descifrar.

Cifrado: 64 o 128 bits

Autenticación: No

Seguridad: Baja

#### **WPA**

(Acceso protegido Wi-Fi) : es una mejora del protocolo WEP. Utiliza un cifrado de 128 o 256 bits, que es más difícil de descifrar.

Cifrado: 128 o 256 bits

Autenticación: Protocolo de integridad de clave temporal (TKIP)

Seguridad: Mediana

## **WPA2**

(Acceso protegido Wi-Fi 2) : Es la versión más reciente y segura del protocolo WPA.

Utiliza un cifrado de 128 o 256 bits, y también incluye otras medidas de seguridad adicionales, como la autenticación de usuario.

Cifrado: 128 o 256 bits

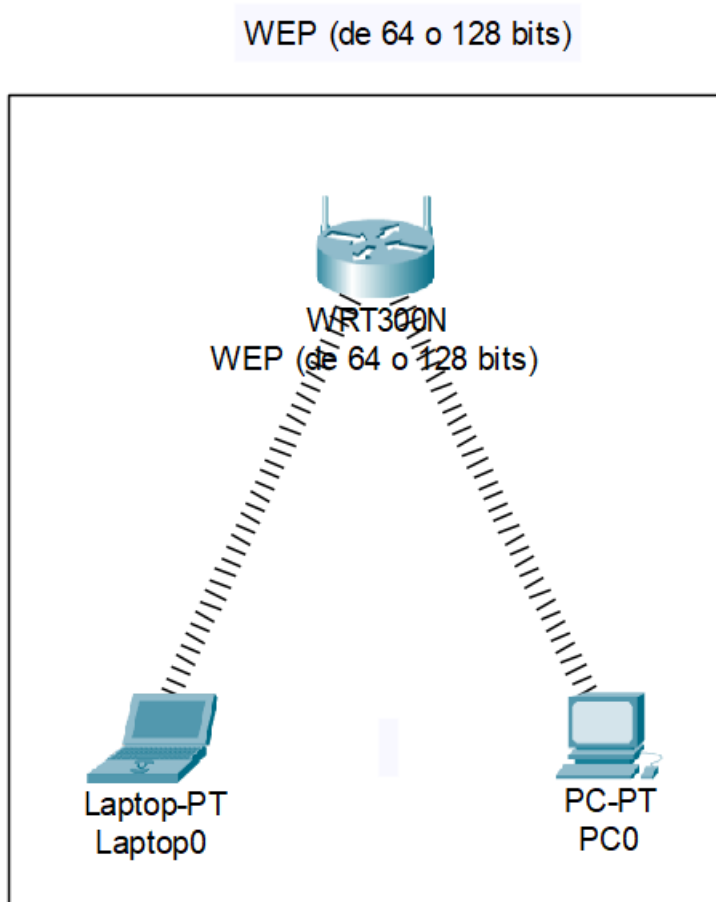
Autenticación: Protocolo de integridad de clave temporal (TKIP) o Estándar de cifrado avanzado (AES)

Seguridad: Alta

## Desarrollo de los Escenarios

### *Modelo WEP (de 64 o 128 bits)*

Diagrama del montaje:



## Configuracion del Router

WEP (de 64 o 128 bits)

Physical **Config** GUI Attributes

**GLOBAL**

- Settings
- Algorithm Settings

**INTERFACE**

- Internet
- LAN**
- Wireless

**LAN Settings**

IP Configuration

|              |               |
|--------------|---------------|
| IPv4 Address | 192.168.0.1   |
| Subnet Mask  | 255.255.255.0 |

☐ Top

WEP (de 64 o 128 bits)

Physical **Config** GUI Attributes

**GLOBAL**

- Settings
- Algorithm Settings

**INTERFACE**

- Internet
- LAN
- Wireless**

**Wireless Settings**

SSID: juan

2.4 GHz Channel: 1 - 2.412GHz

Coverage Range (meters): 250.00

Authentication

☐ Disabled ☒ WEP ☐ WPA-PSK ☐ WPA2-PSK ☐ WPA ☐ WPA2

WEP Key: ababababab

PSK Pass Phrase:

**RADIUS Server Settings**

IP Address:

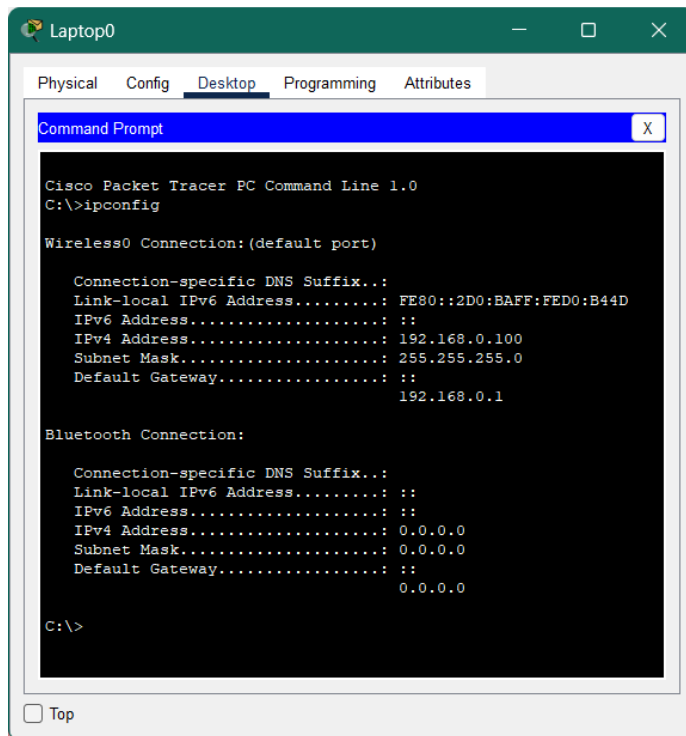
Shared Secret:

Encryption Type: 40/64-Bits (10 Hex digits)

☐ Top



## Configuración IP del computador



The screenshot shows a Cisco Packet Tracer window titled 'Laptop0' with tabs for Physical, Config, Desktop, Programming, and Attributes. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The command prompt shows the output of the 'ipconfig' command, displaying network configuration for both Wireless0 and Bluetooth connections. The Wireless0 connection is configured with an IPv4 address of 192.168.0.100 and a default gateway of 192.168.0.1. The Bluetooth connection is configured with all-zero values for IPv4 and the default gateway.

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

Wireless0 Connection:(default port)

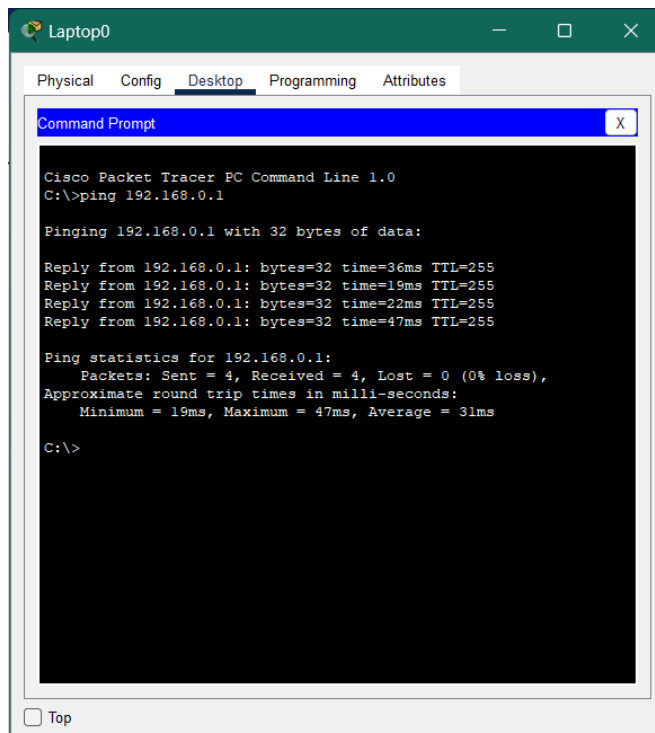
    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::2D0:BAFF:FED0:B44D
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 192.168.0.100
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::
                                192.168.0.1

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

C:\>
```

## Ping del computador al Router



The screenshot shows the same Cisco Packet Tracer window for 'Laptop0'. The 'Command Prompt' window now shows the output of the 'ping 192.168.0.1' command. It displays four successful replies from 192.168.0.1 with varying round-trip times (36ms, 19ms, 22ms, and 47ms). The ping statistics show that 4 packets were sent and received with 0% loss, and the average round-trip time is 31ms.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

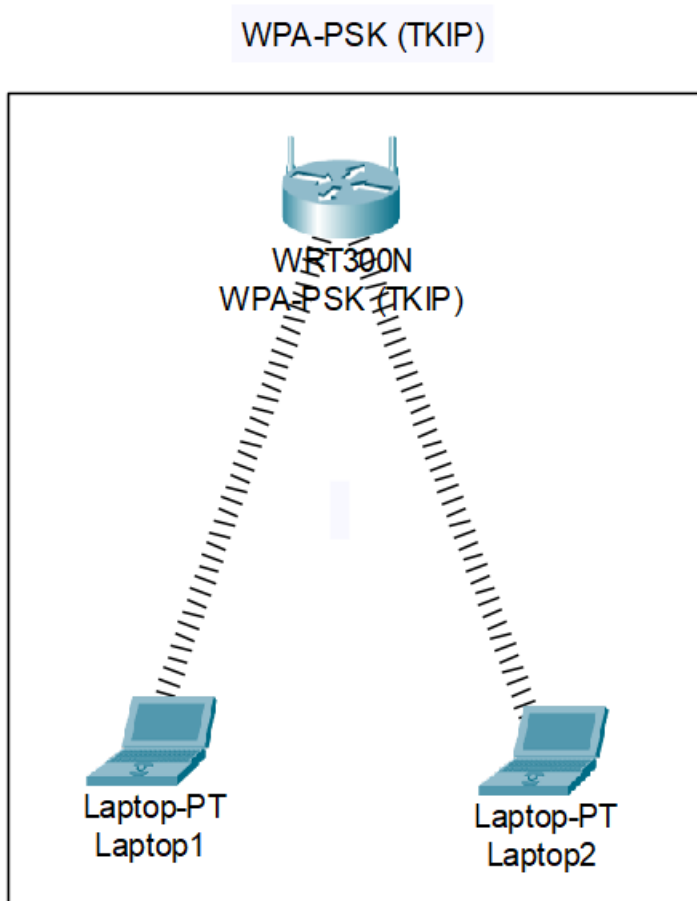
Reply from 192.168.0.1: bytes=32 time=36ms TTL=255
Reply from 192.168.0.1: bytes=32 time=19ms TTL=255
Reply from 192.168.0.1: bytes=32 time=22ms TTL=255
Reply from 192.168.0.1: bytes=32 time=47ms TTL=255

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 19ms, Maximum = 47ms, Average = 31ms

C:\>
```

***Modelo WPA-PSK (TKIP)***

Diagrama del montaje:



## Configuración del Router:

WPA-PSK (TKIP)

Physical **Config** GUI Attributes

**GLOBAL**

- Settings
- Algorithm Settings

**INTERFACE**

- Internet
- LAN**
- Wireless

**LAN Settings**

IP Configuration

|              |               |
|--------------|---------------|
| IPv4 Address | 192.168.2.1   |
| Subnet Mask  | 255.255.255.0 |

☐ Top

WPA-PSK (TKIP)

Physical **Config** GUI Attributes

**GLOBAL**

- Settings
- Algorithm Settings

**INTERFACE**

- Internet
- LAN
- Wireless**

**Wireless Settings**

SSID: juan2

2.4 GHz Channel: 1 - 2.412GHz

Coverage Range (meters): 250.00

Authentication

☐ Disabled ☐ WEP WEP Key:

☒ WPA-PSK ☐ WPA2-PSK PSK Pass Phrase: ababababab

☐ WPA ☐ WPA2

RADIUS Server Settings

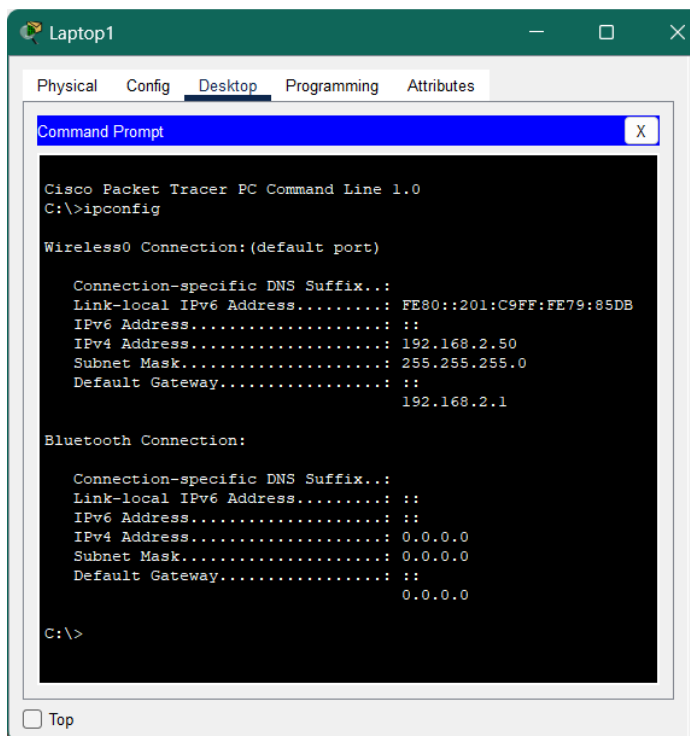
IP Address:

Shared Secret:

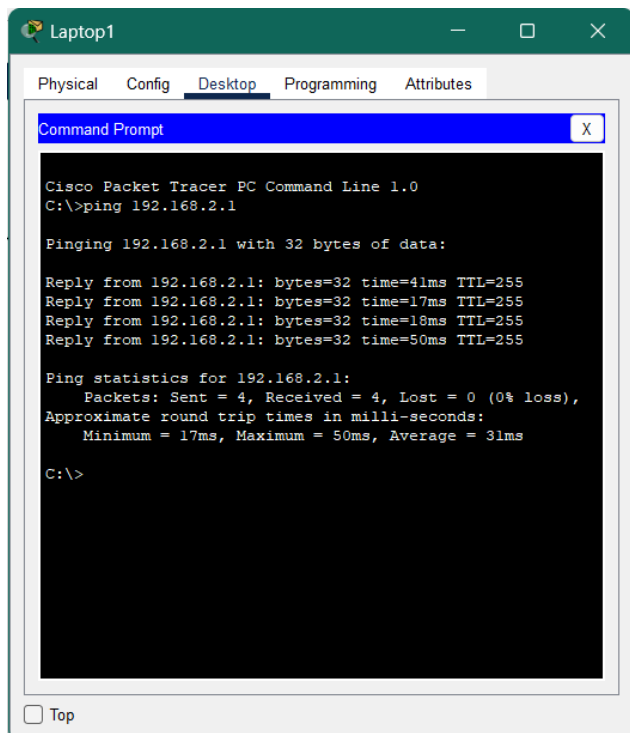
Encryption Type: TKIP

☐ Top

Configuración IP del computador:

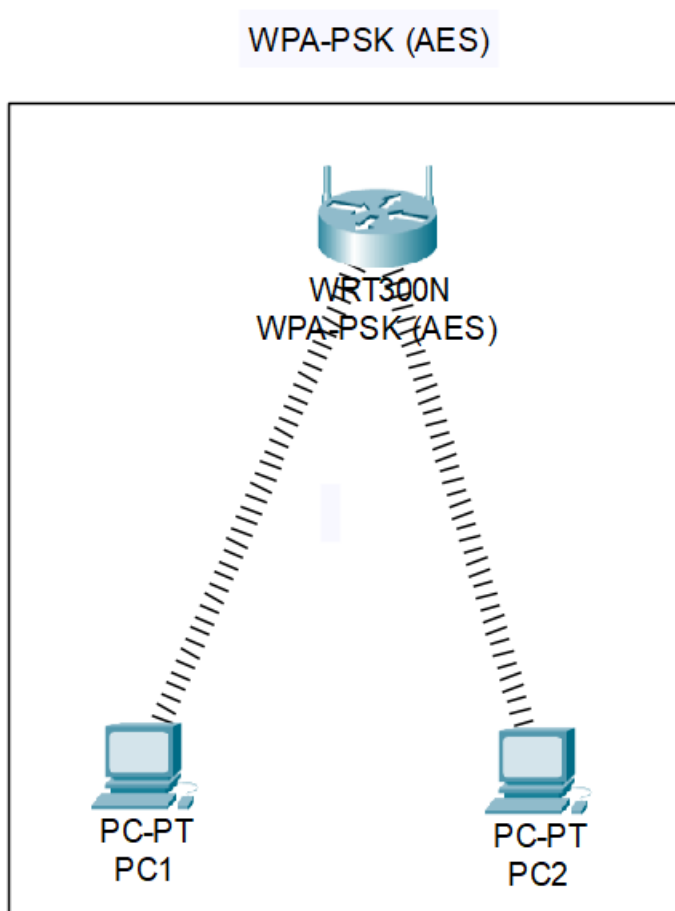


Ping del computador al router:



***Modelo WPA-PSK (AES)***

Diagrama del montaje:



## Configuración del router:

WPA-PSK (AES)

Physical **Config** GUI Attributes

**GLOBAL**

Settings

Algorithm Settings

**INTERFACE**

Internet

LAN

Wireless

**LAN Settings**

IP Configuration

|              |               |
|--------------|---------------|
| IPv4 Address | 192.168.3.1   |
| Subnet Mask  | 255.255.255.0 |

☐ Top

WPA-PSK (AES)

Physical **Config** GUI Attributes

**GLOBAL**

Settings

Algorithm Settings

**INTERFACE**

Internet

LAN

**Wireless**

**Wireless Settings**

SSID: juan2

2.4 GHz Channel: 1 - 2.412GHz

Coverage Range (meters): 250.00

Authentication

☐ Disabled ☐ WEP WEP Key

☒ WPA-PSK ☐ WPA2-PSK PSK Pass Phrase ababababab

☐ WPA ☐ WPA2

RADIUS Server Settings

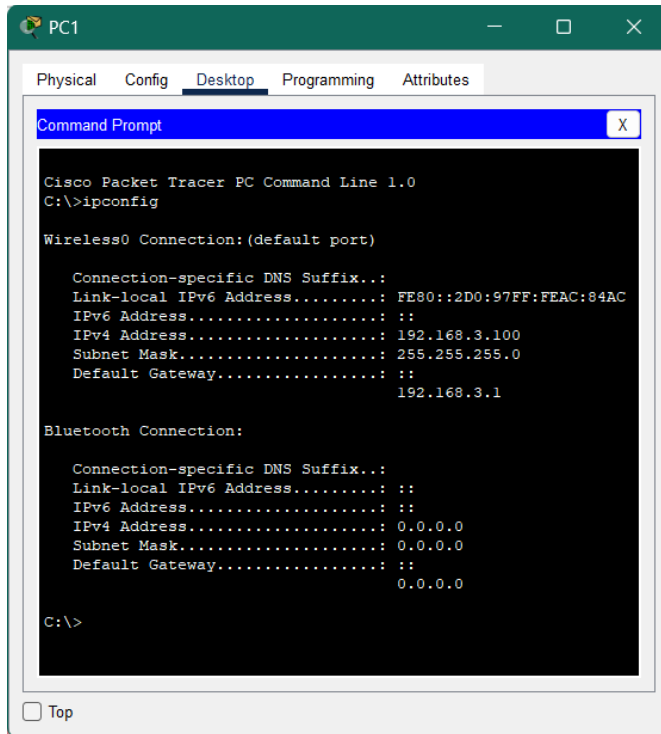
IP Address

Shared Secret

Encryption Type: AES

☐ Top

Configuración IP del computador:



The screenshot shows a Cisco Packet Tracer PC window titled 'PC1'. The 'Desktop' tab is selected, displaying a 'Command Prompt' window. The command prompt shows the output of the 'ipconfig' command, displaying network configuration for 'Wireless0' and 'Bluetooth' connections. The 'Wireless0' connection is active, showing an IPv4 address of 192.168.3.100 and a default gateway of 192.168.3.1. The 'Bluetooth' connection is inactive, showing 0.0.0.0 for all fields.

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

Wireless0 Connection:(default port)

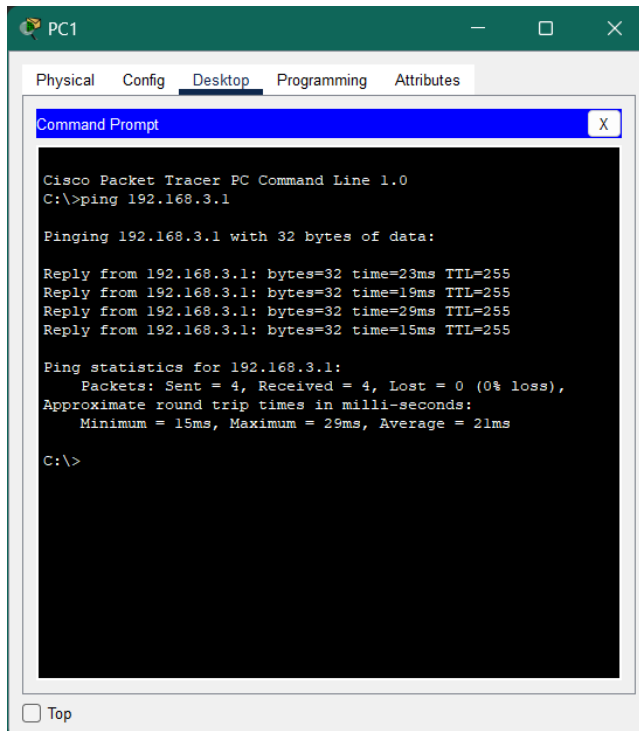
    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::2D0:97FF:FEAC:84AC
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 192.168.3.100
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::
                                192.168.3.1

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

C:\>
```

Ping del computador al router:



The screenshot shows the same PC1 Command Prompt window, but now displaying the output of the 'ping 192.168.3.1' command. The output shows four successful replies from 192.168.3.1 with varying round trip times (23ms, 19ms, 29ms, 15ms). The ping statistics summary at the bottom indicates 4 packets sent, 4 received, 0% loss, and an average round trip time of 21ms.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.1

Pinging 192.168.3.1 with 32 bytes of data:

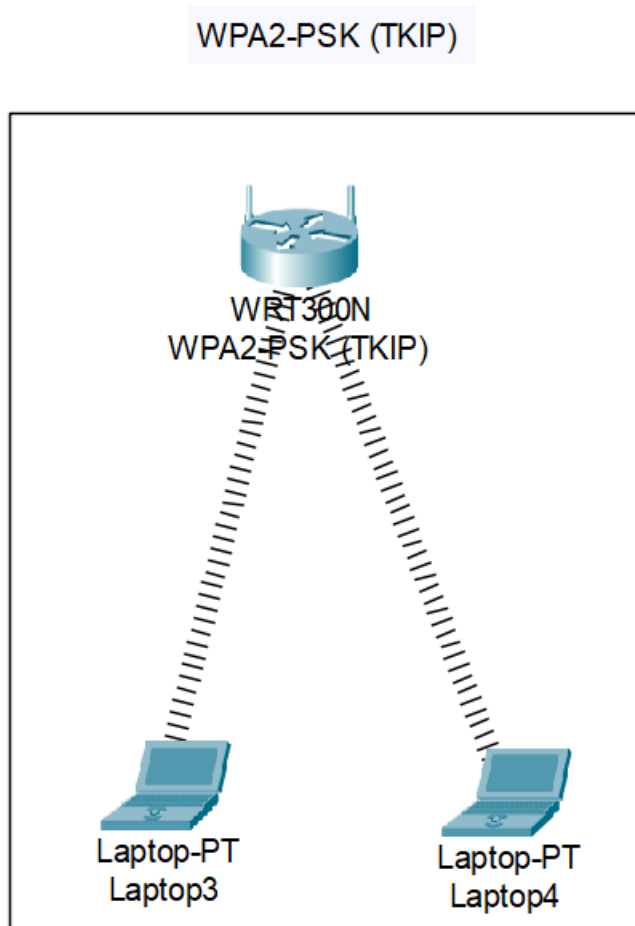
Reply from 192.168.3.1: bytes=32 time=23ms TTL=255
Reply from 192.168.3.1: bytes=32 time=19ms TTL=255
Reply from 192.168.3.1: bytes=32 time=29ms TTL=255
Reply from 192.168.3.1: bytes=32 time=15ms TTL=255

Ping statistics for 192.168.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 15ms, Maximum = 29ms, Average = 21ms

C:\>
```

**Modelo WPA2-PSK (TKIP)**

Diagrama del montaje:





## Configuración del router:

WPA2-PSK (TKIP)

Physical **Config** GUI Attributes

**GLOBAL**

Settings

Algorithm Settings

**INTERFACE**

Internet

LAN

Wireless

**LAN Settings**

IP Configuration

IPv4 Address 192.168.5.1

Subnet Mask 255.255.255.0

☐ Top

WPA2-PSK (TKIP)

Physical **Config** GUI Attributes

**GLOBAL**

Settings

Algorithm Settings

**INTERFACE**

Internet

LAN

**Wireless**

**Wireless Settings**

SSID juan4

2.4 GHz Channel 1 - 2.412GHz

Coverage Range (meters) 250.00

Authentication

☐ Disabled ☐ WEP WEP Key

☐ WPA-PSK ☒ WPA2-PSK PSK Pass Phrase ababababab

☐ WPA ☐ WPA2

RADIUS Server Settings

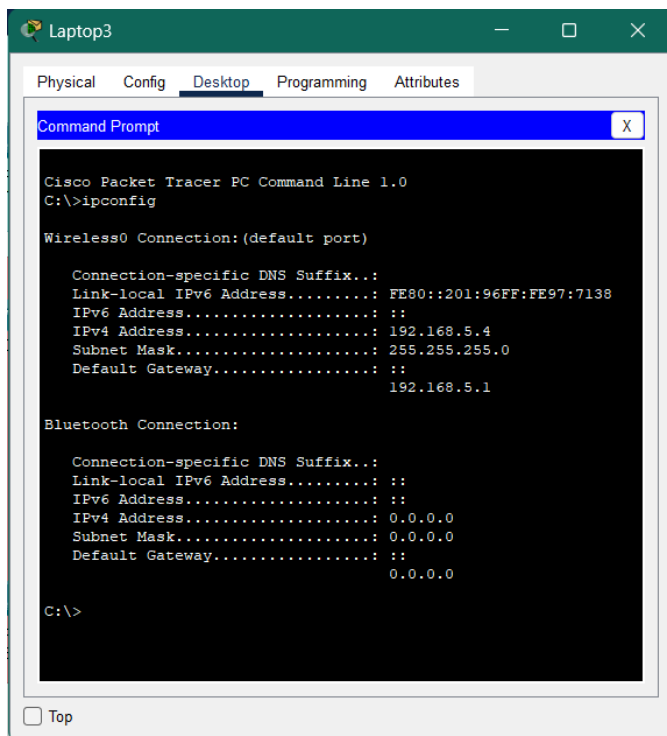
IP Address

Shared Secret

Encryption Type TKIP

☐ Top

Configuración IP del computador:



The screenshot shows the 'Laptop3' window in Cisco Packet Tracer, with the 'Desktop' tab selected. A 'Command Prompt' window is open, displaying the output of the 'ipconfig' command. The output shows the configuration for the 'Wireless0' and 'Bluetooth' connections. The 'Wireless0' connection is active, showing an IPv4 address of 192.168.5.4 and a subnet mask of 255.255.255.0. The 'Bluetooth' connection is inactive, showing all-zero values for IP addresses and subnet mask.

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

Wireless0 Connection:(default port)

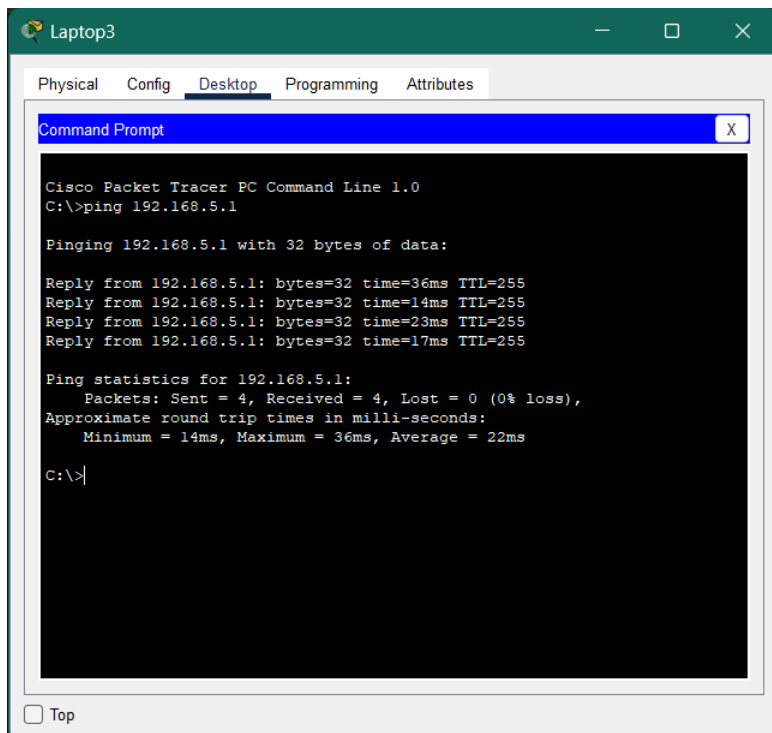
Connection-specific DNS Suffix.:
Link-local IPv6 Address.....: FE80::201:96FF:FE97:7138
IPv6 Address.....: ::
IPv4 Address.....: 192.168.5.4
Subnet Mask.....: 255.255.255.0
Default Gateway.....: ::
                               192.168.5.1

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

C:\>
```

Ping del computador al router:



The screenshot shows the 'Laptop3' window in Cisco Packet Tracer, with the 'Desktop' tab selected. A 'Command Prompt' window is open, displaying the output of the 'ping 192.168.5.1' command. The output shows four successful replies from 192.168.5.1 with varying response times (36ms, 14ms, 23ms, 17ms) and a TTL of 255. The ping statistics show 4 packets sent, 4 received, and 0% loss, with an average round trip time of 22ms.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.5.1

Pinging 192.168.5.1 with 32 bytes of data:

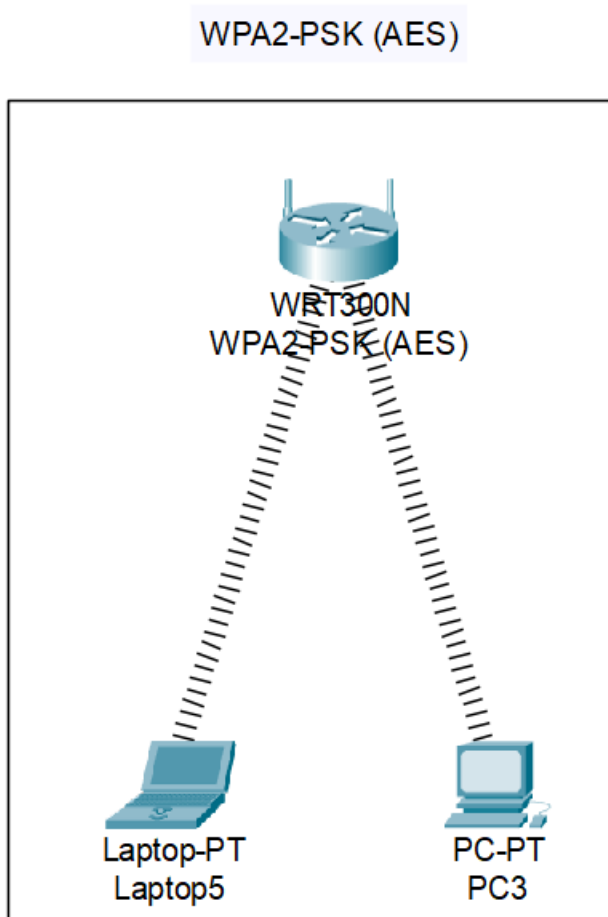
Reply from 192.168.5.1: bytes=32 time=36ms TTL=255
Reply from 192.168.5.1: bytes=32 time=14ms TTL=255
Reply from 192.168.5.1: bytes=32 time=23ms TTL=255
Reply from 192.168.5.1: bytes=32 time=17ms TTL=255

Ping statistics for 192.168.5.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 14ms, Maximum = 36ms, Average = 22ms

C:\>
```

**Modelo WPA2-PSK (AES)**

Diagrama del montaje:



## Configuración del router:

WPA2-PSK (AES)

Physical **Config** GUI Attributes

**GLOBAL**

Settings

Algorithm Settings

**INTERFACE**

Internet

LAN

Wireless

**LAN Settings**

IP Configuration

IPv4 Address 192.168.6.1

Subnet Mask 255.255.255.0

☐ Top

WPA2-PSK (AES)

Physical **Config** GUI Attributes

**GLOBAL**

Settings

Algorithm Settings

**INTERFACE**

Internet

LAN

**Wireless**

**Wireless Settings**

SSID juan5

2.4 GHz Channel 1 - 2.412GHz

Coverage Range (meters) 250.00

Authentication

☐ Disabled ☐ WEP WEP Key

☐ WPA-PSK ☒ WPA2-PSK PSK Pass Phrase ababababab

☐ WPA ☐ WPA2

RADIUS Server Settings

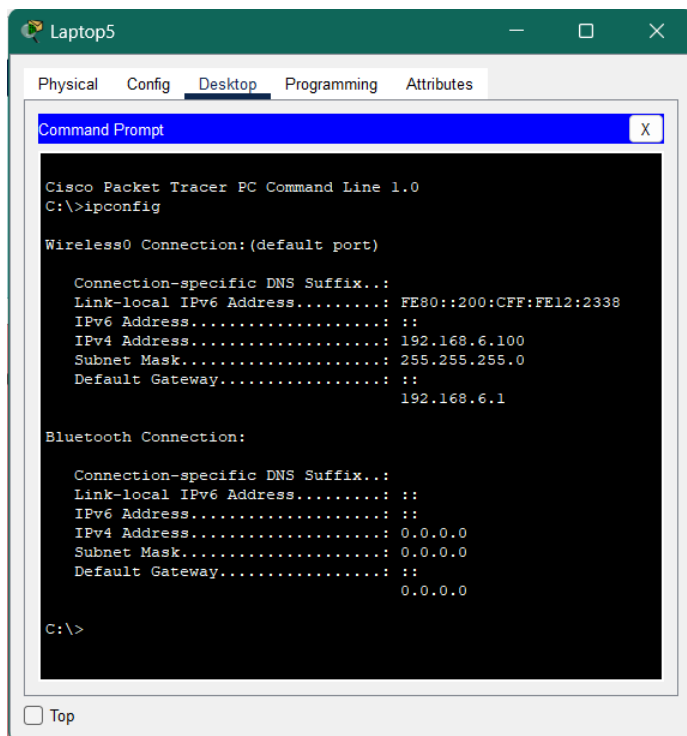
IP Address

Shared Secret

Encryption Type AES

☐ Top

Configuración IP del computador:



The screenshot shows a 'Laptop5' window with tabs for Physical, Config, Desktop, Programming, and Attributes. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The command prompt shows the output of the 'ipconfig' command, displaying network configuration for both Wireless0 and Bluetooth connections. The Wireless0 connection is configured with an IPv4 address of 192.168.6.100, a subnet mask of 255.255.255.0, and a default gateway of 192.168.6.1. The Bluetooth connection is currently unconfigured with 0.0.0.0 values.

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

Wireless0 Connection:(default port)

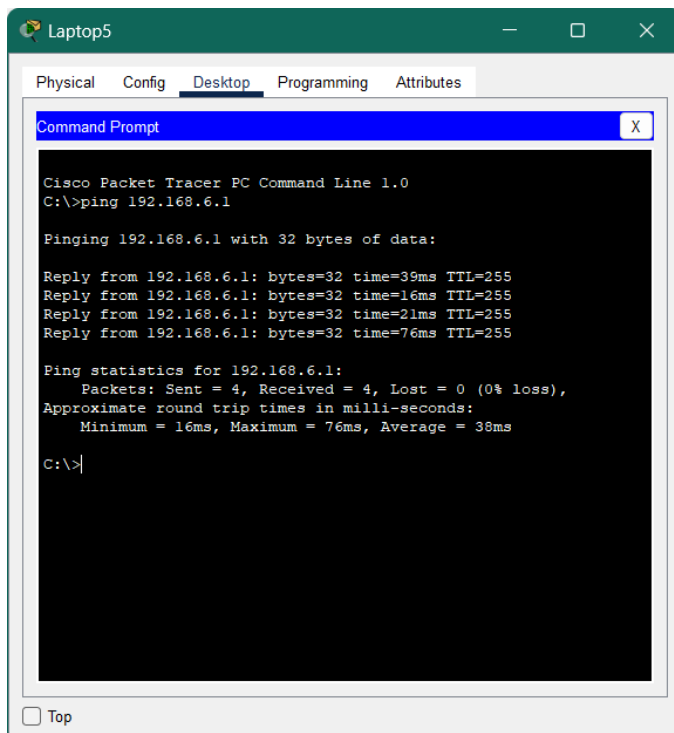
Connection-specific DNS Suffix.:
Link-local IPv6 Address.....: FE80::200:CFF:FE12:2338
IPv6 Address.....: ::
IPv4 Address.....: 192.168.6.100
Subnet Mask.....: 255.255.255.0
Default Gateway.....: ::
                        192.168.6.1

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

C:\>
```

Ping del computador al router:



The screenshot shows the same 'Laptop5' window with the 'Command Prompt' displaying the output of the 'ping 192.168.6.1' command. The ping is successful, showing four replies from 192.168.6.1 with varying response times (39ms, 16ms, 21ms, 76ms) and a TTL of 255. The statistics show 4 packets sent, 4 received, and 0% loss.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.6.1

Pinging 192.168.6.1 with 32 bytes of data:

Reply from 192.168.6.1: bytes=32 time=39ms TTL=255
Reply from 192.168.6.1: bytes=32 time=16ms TTL=255
Reply from 192.168.6.1: bytes=32 time=21ms TTL=255
Reply from 192.168.6.1: bytes=32 time=76ms TTL=255

Ping statistics for 192.168.6.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 16ms, Maximum = 76ms, Average = 38ms

C:\>
```

## **Conclusiones**

Los protocolos de seguridad inalámbrica son esenciales para proteger los datos que se transmiten a través de una red Wi-Fi. Es importante elegir el protocolo de seguridad adecuado para las necesidades de la red. Para redes domésticas o pequeñas, el protocolo WPA suele ser suficiente. Para redes empresariales o con datos sensibles, el protocolo WPA2 es la mejor opción.

## Referencias

Ghimiray, D. (2023, February 23). *Seguridad de Wi-Fi: WEP frente a WPA o WPA2*.

Seguridad De Wi-Fi: WEP Frente a WPA O WPA2. <https://www.avast.com/es-es/c-wep-vs-wpa-or-wpa2>