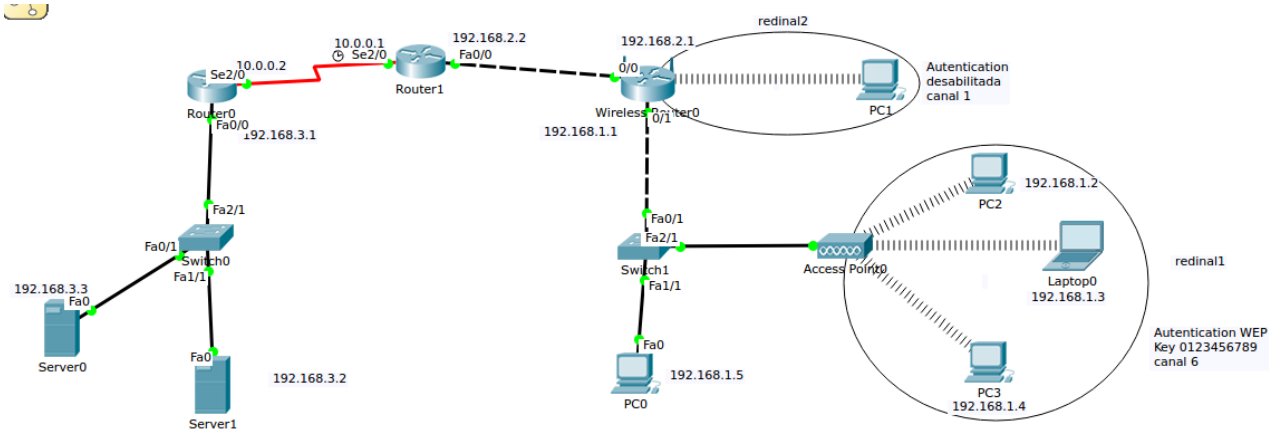
Práctica 8 Final
Nombre:

1. Construya la topología mostrada, configure los parámetros de red según se indica para las seis redes, complete la tabla de enrutamiento mostrada



Arquitectura mostrada

2. Llenar la siguiente tabla e identificar las redes utilizadas, deberá cambiar las tarjetas Ethernet por tarjetas inalámbricas de ser necesario

Dispositivo	*Interfaz*	*Red*	*Dirección IP*	*Máscara*	*Gateway*
Server 0	Fa0	192.168.3.0	192.168.3.3	255.255.255.0	192.168.3.1
Server 1	Fa0	192.168.3.0	192.168.3.2	255.255.255.0	192.168.3.1
Router 0	Fa0/0	192.168.3.0	192.168.3.1	255.255.255.0	192.168.3.1
Router 0	Se2/0	10.0.0.0	10.0.0.2	255.0.0.0	10.0.0.1
Router 1	Se2/0	10.0.0.0	10.0.0.1	255.0.0.0	10.0.0.2
Router 1	Fa0/0	192.168.2.0	192.168.2.2	255.255.255.0	192.168.2.1
Wireless Router	Fa0/0	192.168.2.0	192.168.2.1	255.255.255.0	192.168.2.2
Wireless Router	Fa0/1	192.168.1.0	192.168.1.1	255.255.255.0	192.168.1.1
PC0	W0	192.168.1.0	192.168.1.5	255.255.255.0	192.168.1.1
PC1	W0	192.168.1.0	DHCP(192.168.1.100)	255.255.255.0	192.168.1.1
PC2	W0	192.168.1.0	192.168.1.2	255.255.255.0	192.168.1.1

Laptop0	W0	192.168.1.0	192.168.1.3	255.255.255.0	192.168.1.1
PC3	W0	192.168.1.0	192.168.1.4	255.255.255.0	192.168.1.1

3. Activar el protocolo RIP en cada router

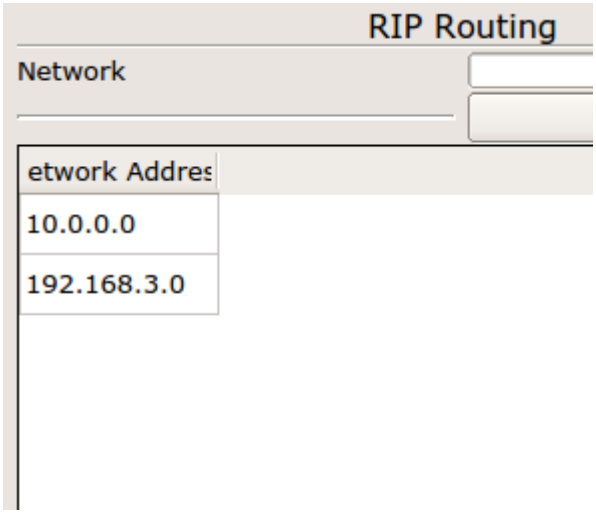


Tabla del router 0

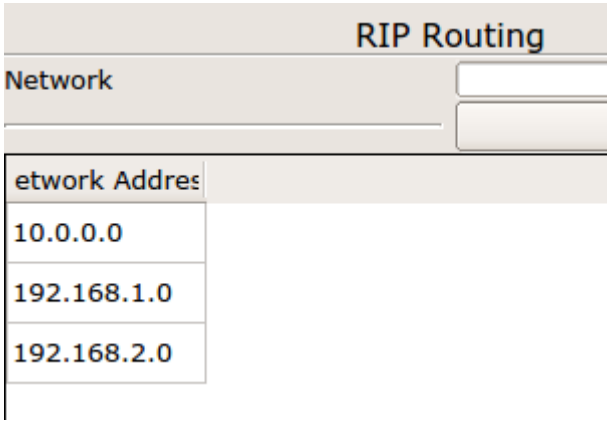


Tabla del router 1

Cuestionario

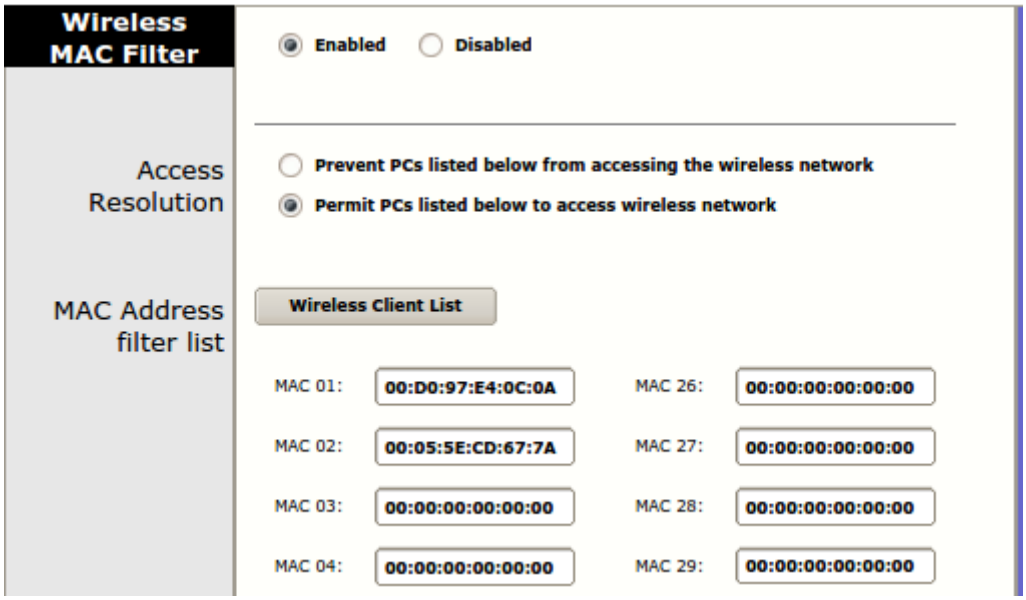
1. **Haga un resumen sobre los estándares 802.11**

Las redes LAN inalámbricas son cada vez más populares; los hogares, oficinas, cafeterías, bibliotecas, aeropuertos y demás sitios públicos se están equipando con este tipo de redes para conectar computadoras, dispositivos PDA y teléfonos inteligentes (smartphones) a Internet. Las redes LAN inalámbricas también se pueden usar para permitir que dos o más computadoras que estén cerca unas de otras se comuniquen sin necesidad de usar Internet. El principal estándar de LAN inalámbrica es 802.11 el cual define el uso de los dos niveles inferiores de la arquitectura o modelo OSI (capa física y capa de enlace de datos), especificando las normas de funcionamiento de una red de área local inalámbrica (WLAN).

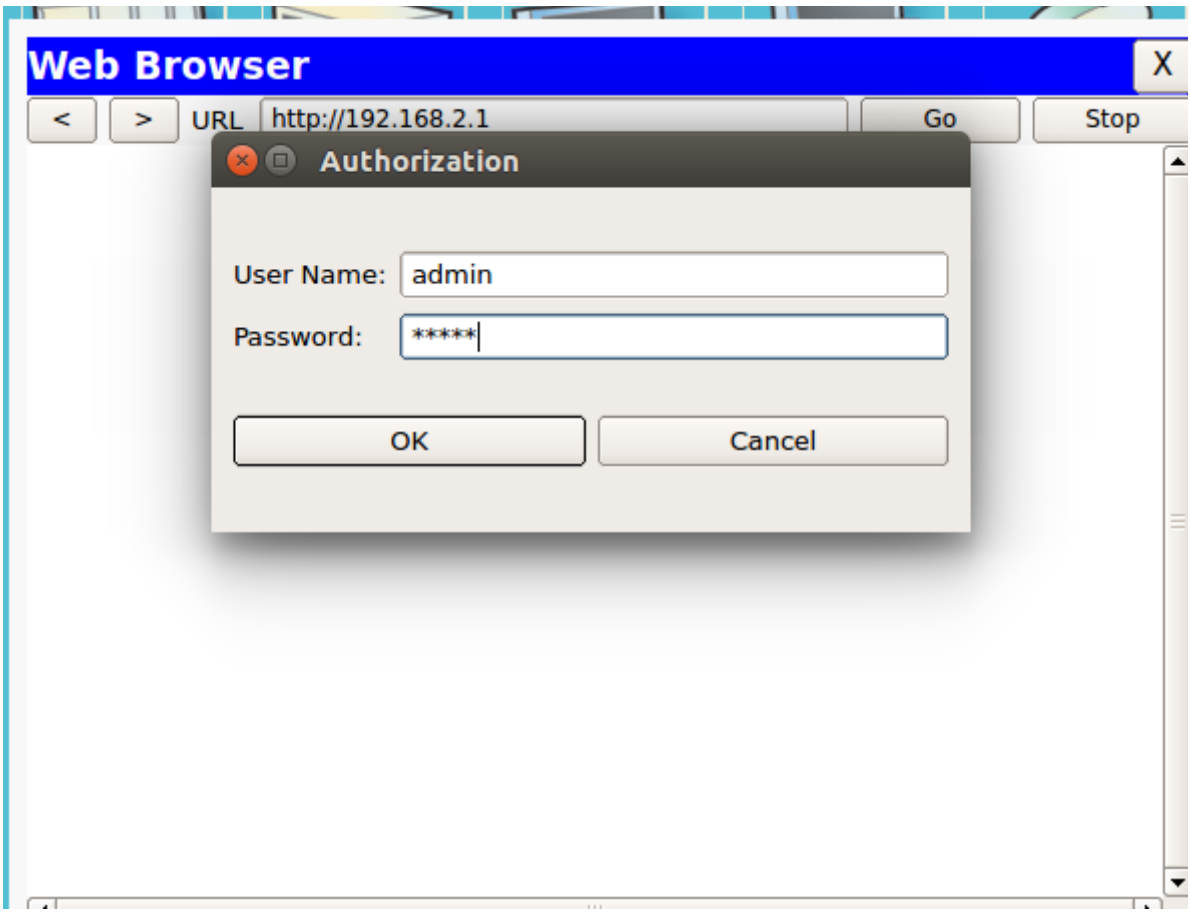
La primera versión de la norma se publicó en 1997 por el Institute of Electrical and Electronics Engineers (Instituto de Ingenieros Eléctricos y Electrónicos) o IEEE, el cual actualmente se encarga de su mantenimiento. Las especificaciones de este estándar proporcionan la base para los productos con redes inalámbricas que hacen uso de la marca Wi-Fi. a versión original del estándar IEEE 802.11 publicada en 1997 especifica dos velocidades de transmisión teóricas de 1 y 2 mega bit por segundo (Mbit/s) que se transmiten por señales infrarrojas (IR) en la banda ISM a 2,4 GHz. IR sigue siendo parte del estándar, pero no hay implementaciones disponibles.

El estándar original también define el protocolo CSMA/CA (Múltiple acceso por detección de portadora evitando colisiones) como método de acceso. Una parte importante de la velocidad de transmisión teórica se utiliza en las necesidades de esta codificación para mejorar la calidad de la transmisión bajo condiciones ambientales diversas, lo cual se tradujo en dificultades de interoperabilidad entre equipos de diferentes marcas. Estas y otras debilidades fueron corregidas en el estándar 802.11b, que fue el primero de esta familia en alcanzar amplia aceptación entre los consumidores. (CSMA/CA: Es un protocolo de control de redes utilizado para evitar colisiones entre los paquetes de datos (comúnmente en redes inalámbricas, ya que estas no cuenta con un modo práctico para transmitir y recibir simultáneamente)).

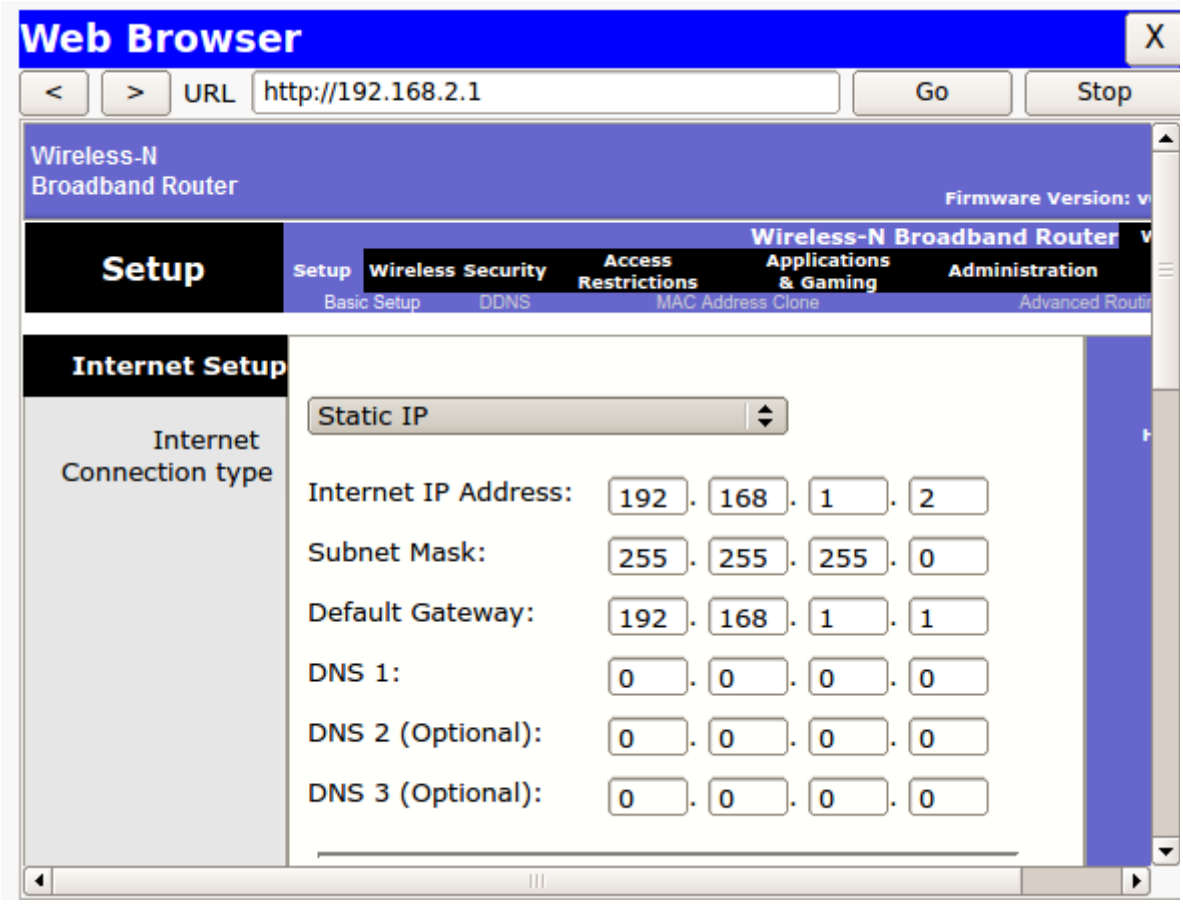
2. **Configure en el router inalámbrico el filtrado de PCs a través de la dirección MAC de modo que permita solo el acceso de las PC2 y PC3. Muestre las pruebas del caso. (accesar desde el navegador usando 192.168.2.1 user name: admin – password: EPIS123 (escenario 2)**



Filtrado por MAC



Administración por el Web Browser



Administración por el Web Browser

3. **Describa la diferencia entre los diferentes tipos de seguridad soportados además de WEP**

WEP: (Wired Equivalent Privacy): Cifrado que apareció en 1999. Era el más utilizado en el mundo y su uso ha disminuido paulatinamente debido a su debilidad. Cuando entró en vigor, se le descubrieron muchos fallos y agujeros, por lo que tuvo que ir evolucionando con el tiempo. Pese a las mejoras, revisiones de los algoritmos y aumento de tamaño de las contraseñas, se ha demostrado, continuamente, que es un cifrado poco fiable y fácil de explotar. Los sistemas que funcionan con WEP deben estar totalmente actualizados y con sistemas de seguridad alternativos.

WPA: (WiFi Protected Access): Este cifrado fue la respuesta automática al WEP y sus vulnerabilidades cada vez más frecuentes. Empezó a usarse de forma oficial hacia el año 2003. Las claves usadas por WPA son de 256 bits, el doble de los 128 bits usados por WEP. Las principales mejoras y avances respecto al cifrado WEP son: Usar el doble de bits para las claves, comprobación de contenido e integridad de mensajes, para evitar intercepción de tráfico, y el protocolo de clave temporal TKIP. Todo esto evita que un router sea atacado de forma tan sencilla como ocurría con el uso de WEP.

WPA2: Una de las principales diferencias entre WPA y WPA2 es el uso del algoritmo AES; este es un tipo de cifrado por bloques, adoptado como estándar de cifrado por los EE.UU., el cual permite claves más largas y más seguras y, además, la implementación del CCMP (Modo de contador cifrado bloqueo de encadenamiento protocolo de código de autenticación de mensajes) que es un protocolo mejorado de encriptación, que sustituye a TKIP.

4. **Defina WLAN**

Las redes inalámbricas de área local, WLAN por sus siglas en inglés Wirless Local Area Network, son redes que comúnmente cubren distancias de los 10 a los 100 de metros. Esta pequeña cobertura contiene una menor potencia de transmisión que a menudo permite el uso de bandas de frecuencia sin licencia. Debido a que las LANs a menudo son utilizadas para comunicaciones de una relativa alta capacidad de datos, normalmente tienen índices de datos más altos. Por ejemplo 802.11, una tecnología WLAN, tiene un ámbito nominal de 100 metros e índices de transmisión de datos de hasta 11Mbps. Los dispositivos que normalmente utilizan WLANs son los que tienen una plataforma más robusta y abastecimiento de potencia como son las computadoras personales en particular.

Sus características más destacadas son:

- Movilidad: permite transmitir información en tiempo real en cualquier lugar de la organización o empresa a cualquier usuario. Esto supone mayor productividad y posibilidades de servicio.

- Facilidad de instalación: al no usar cables, se evitan obras para tirar cable por muros y techos, mejorando así el aspecto y la habitabilidad de los locales, y reduciendo el tiempo de instalación. También permite el acceso instantáneo a usuarios temporales de la red.

- Flexibilidad: puede llegar donde el cable no puede, superando mayor número de obstáculos, llegando a atravesar paredes. Así, es útil en zonas donde el cableado no es posible o es muy costoso: parques naturales, reservas o zonas escarpadas.

5. **Identifique los posibles tipos de autenticación en las redes inalámbricas, que significa cada tipo**

La mayoría de las redes inalámbricas utilizan algún tipo de configuración de seguridad. Estas configuraciones de seguridad definen la autentificación (el modo en que el dispositivo en sí se identifica en la red) y la encriptación (el modo en que los datos se cifran a medida que se envían por la red). Si no especifica correctamente estas opciones cuando esté configurando su dispositivo inalámbrico Brother, no podrá conectar con la red inalámbrica. Por lo tanto, estas opciones deben configurarse con cuidado. Consulte la siguiente información para ver los métodos de autentificación y encriptación que admite su dispositivo inalámbrico Brother.

Métodos de autentificación

La impresora Brother admite los siguientes métodos:

- Sistema abierto: Se permite el acceso a la red a dispositivos inalámbricos sin ninguna autentificación.
- Clave compartida: Todos los dispositivos que acceden a la red inalámbrica comparten una clave predeterminada secreta. El equipo inalámbrico Brother utiliza claves WEP como claves predeterminadas.
- WPA-PSK/WPA2-PSK Activa una clave precompartida de acceso protegido Wi-Fi (WPA-PSK/WPA2-PSK), que permite al equipo inalámbrico Brother asociarse con puntos de acceso utilizando el cifrado TKIP para WPA-PSK o AES para WPA-PSK y WPA2-PSK (WPA-Personal).
- WPA-PSK/WPA2-PSK: Activa una clave precompartida de acceso protegido Wi-Fi (WPA-PSK/WPA2-PSK), que permite al equipo inalámbrico Brother asociarse con puntos de

acceso utilizando el cifrado TKIP para WPA-PSK o AES para WPA-PSK y WPA2-PSK (WPA-Personal).

- LEAP: Cisco Systems, Inc. ha desarrollado el protocolo Cisco LEAP (Protocolo ligero de autentificación extensible), que utiliza identificaciones de usuario y contraseñas para la autenticación.

Métodos de encriptación

La encriptación se utiliza para proteger los datos que se envían por la red inalámbrica. El equipo inalámbrico Brother admite los siguientes métodos de encriptación:

- Ninguna: No se utiliza ningún método de encriptación.
- WEP: Al utilizar WEP (Privacidad equivalente a cableado), los datos se transmiten y se reciben con una clave segura.
- TKIP: TKIP (Protocolo de integridad de clave temporal) proporciona una clave por paquete que mezcla una comprobación de integridad de mensajes y un mecanismo que vuelve a crear claves.
- AES: AES (Estándar de encriptación avanzado) es un potente estándar de encriptación autorizado por Wi-Fi.
- CKIP: El protocolo de integridad de clave original para LEAP de Cisco Systems, Inc.

6. **Describa las características de los siguientes tipos de antenas:**

- **De rejilla**: La antena parabólica de rejilla está diseñada para propagar el sistema de espectro. Funciona en la banda de los 2,4-2,5 GHz y una intensidad direccional de 24 dBi. Su superficie incorpora un reflector de acero soldado que permite obtener el mejor rendimiento. Sus características incluyen una elevada ganancia, amplia cobertura, peso ligero, estructura compacta y excelente resistencia al viento. Se utiliza en exteriores y su rango de alcance es de hasta 56 Km.

- **Yagi:** Una aplicación práctica de este tipo de antenas, es el de las antenas tipo yagi-uda (directivas), ampliamente utilizadas, por ejemplo, para la recepción de señales de televisión en la banda de UHF, ya que poseen una gran directividad, tanto mayor cuanto mayor sea el número de elementos pasivos (parásitos) que incorpore y así su ganancia es la adecuada para recibir el nivel de señal suficiente para que pueda ser amplificado sin problemas. La antena Yagi es pues una antena capaz de concentrar la mayor parte de la energía radiada de manera localizada, aumentando así la potencia emitida hacia el receptor o recibida desde la fuente y evitando interferencias introducidas por fuentes no deseadas.

- **Parabólicas:** En este tipo de antenas la señal emitida/recibida no sale/entra directamente en/del elemento captador, sino que se emite/recoge por/en el mismo una vez reflejada en un elemento pasivo que concentra la señal. En el caso de una antena receptora, su funcionamiento se basa en la reflexión de las ondas electromagnéticas, por la cual las ondas que inciden paralelamente al eje principal se reflejan y van a parar a un punto denominado foco que está centrado en el paraboloide. En cambio, si se trata de una antena emisora, las ondas que emanan del foco (dispositivo de emisión) se ven reflejadas y salen en dirección paralela al eje de la antena. Básicamente, existen tres tipos básicos de antenas con reflector.

- **De panel plano:** Las antenas de panel plano como su nombre lo dice son un panel con forma cuadrada o rectangular. y están configuradas en un formato tipo patch. Las antenas tipo Flat Panel son muy direccionales ya que la mayoría de su potencia radiada es una sola dirección ya sea en el plano horizontal o vertical. En el patrón de elevación y en el patrón de

azimuth se puede ver la directividad de la antena Flat Panel. Las antenas Flat Panel pueden ser fabricadas en diferentes valores de ganancia de acuerdo a su construcción. Esto puede proveer excelente directividad y considerable ganancia.

- **Omnidireccionales:** Definimos las antenas omnidereccionales como aquella que es capaz de radiar energía prácticamente en todas direcciones. El uso habitual hace que las antenas omnidireccionales no emitan exactamente en todas direcciones, sino que tiene una zona donde irradia energía por igual (por ejemplo el plano horizontal). Por ejemplo no nos puede interesar emitir o recibir señal de la parte que está exactamente encima de la antena, imaginémonos la antena de radio del coche: difícilmente tendremos la fuente de señal exactamente encima de la antena, así que favorecemos la emisión o recepción en otras direcciones (como puede ser el plano horizontal) en detrimento de otras (el plano vertical).

7. **En la opción Network Mode que opciones de modo de red existen, explique la diferencia**

8. **Defina SSID**

El SSID (*Service Set Identifier*) es una secuencia de 0-32 octetos incluida en todos los paquetes de una red inalámbrica para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres, que la mayoría de las veces son alfanuméricos (aunque el estándar no lo especifica, así que puede consistir en cualquier carácter). Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID.

9. **Qué es encriptación y que algoritmos admite la seguridad del router inalámbrico**

La encriptación se utiliza para proteger los datos que se envían por la red inalámbrica. El equipo inalámbrico Brother admite los siguientes métodos de encriptación:

- Ninguna: No se utiliza ningún método de encriptación.
- WEP: Al utilizar WEP (Privacidad equivalente a cableado), los datos se transmiten y se reciben con una clave segura.
- TKIP: TKIP (Protocolo de integridad de clave temporal) proporciona una clave por paquete que mezcla una comprobación de integridad de mensajes y un mecanismo que vuelve a crear claves.
- AES: AES (Estándar de encriptación avanzado) es un potente estándar de encriptación autorizado por Wi-Fi.
- CKIP**:** El protocolo de integridad de clave original para LEAP de Cisco Systems, Inc.

6.10 **Explique cómo es posible que PC1 y PC5 se comunique perteneciendo a redes diferentes**

Porque existe un router (Router 0) que hace una internetwork. Los mensajes de PC1 primero pasan por el router que los rutea hacia la red de PC5 y viceversa.

CONCLUSIONES

- La tecnología Wifi es muy usada actualmente en muchos ámbitos. Por esta razón es necesario tener niveles, protocolos y algoritmos de seguridad para proteger la información que se transporta mediante esta tecnología.
- La seguridad actualmente debe ser revisada, ya que la mayoria de los niveles de seguridad pueden ser burlados de alguna forma.

Bibliografía

- Redes de computadoras, ANDREW S. TANENBAUM y DAVID J. WETHERALL, Quinta edición, PEARSON EDUCACIÓN, México.
- Camargo, J. L. "Modelo de Cobertura para Redes Inalámbricas de Interiores." *Proyecto Final de Carrera, Universidad de Sevilla* (2009).
- Huidobro, J. M. "Antenas de Telecomunicaciones." *Revista Digital, CEDRO* (2013).