


REDES WIRELESS

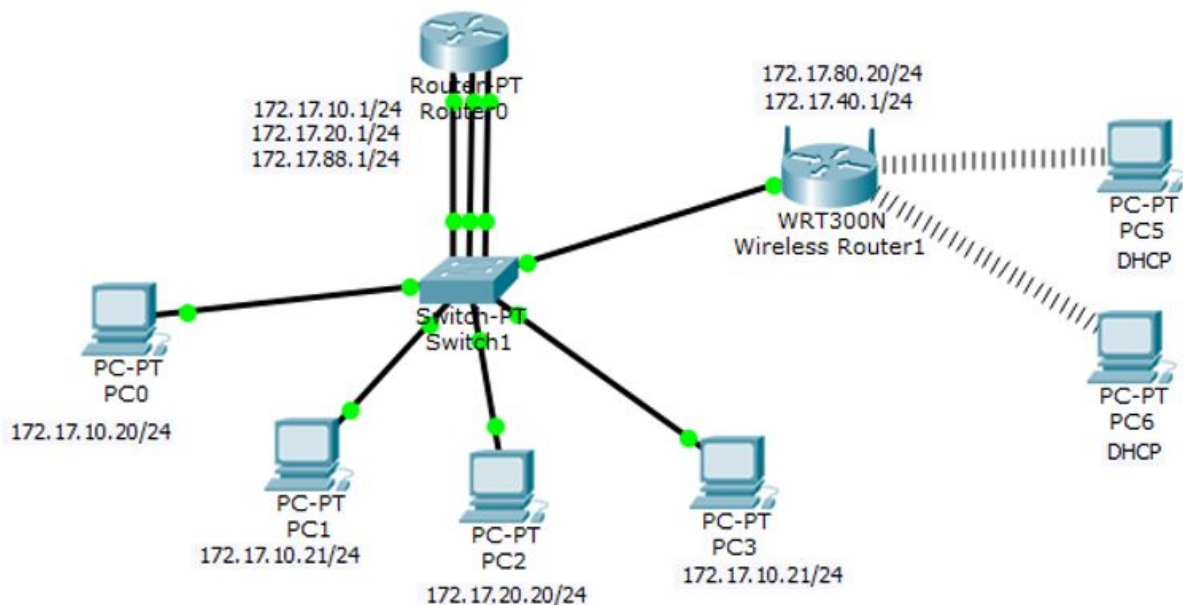
Final 9

Alumno:	Richard Alvarez Mamani		UNIVERSIDAD NACIONAL SAN AGUSTIN
Curso:	Redes y Comunicación de Datos		
Docente:	Lucy Angela Delgado Barra		

IV. ACTIVIDADES

4.1 Construya la topología mostrada, para ellos deberá

- Quitar del router todas las interfaces que no sean FastEthernet, luego llenar los slots libres hasta completar tres interfaces FastEthernet
- Completar en el Switch ocho interfaces FastEthernet
- Conecte las PC y el Router0
- Conecte el Wireless Router usando su puerto de Internet
- Configure las direcciones IP, máscaras y Gateway para PC0, PC1, PC2 y PC3, notar que están en diferentes redes
- Configure y encienda los tres puertos FastEthernet en el Router0



4.2 Configurar el router inalámbrico

a) Conexión a Internet

- Abra GUI

- Establecer **Internet Connection type** en **Static IP** y asignar la dirección IP 172.17.80.20/24
- b) Configuración de red
- En **Network** Setup opción **Router** IP establecer la dirección IP 172.17.40.1/24
 - Habilitar servidor DHCP
 - **Save Settings**
- c) Acceso y al router
- Seleccionar **Wireless** en la parte superior
- Colocar **Network Mode** en **Wireless-N Only**
 - Cambiar el **SSID** a EPIS_LAN
 - Deshabilitar el **SSID Broadcast**
 - **Save Settings**
- d) Seguridad
- Cambiar el **Security Mode** de **Disabled** a **WPA2 Personal**
 - Configurar **EPIS1234** como **Passphrase**
 - **Save Settings**

Network Mode:	Mixed ▼
Network Name (SSID):	EPISUNSA
Radio Band:	Auto ▼
Wide Channel:	Auto ▼
Standard Channel:	1 - 2.412GHz ▼
SSID Broadcast:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

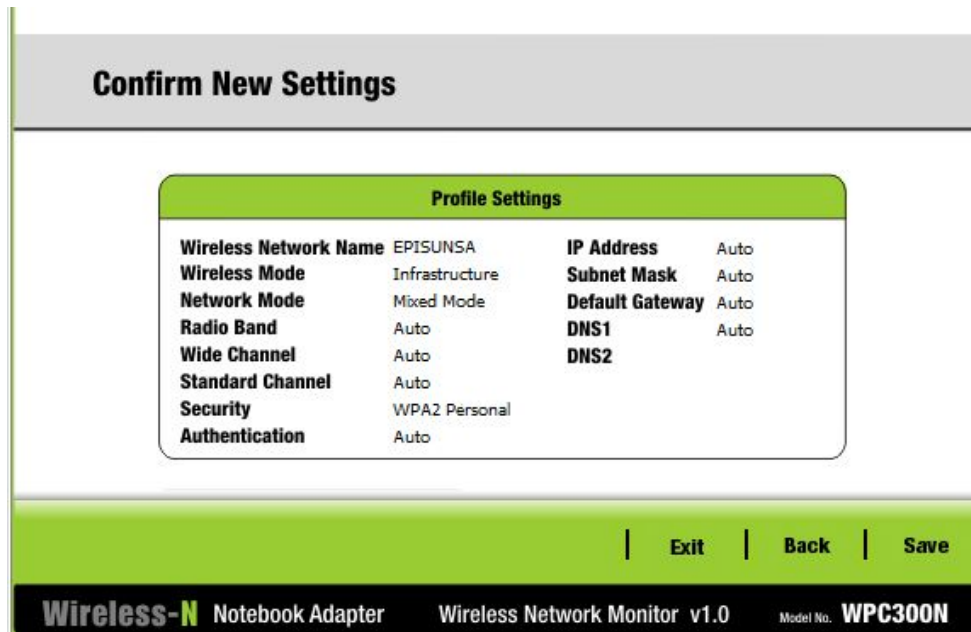
Wireless-N Broadband Router WRT300N	
Wireless 	Setup Wireless Security Access Restrictions Applications & Gaming Administration Status
	Basic Wireless Settings Wireless Security Wireless MAC Filter Advanced Wireless Settings
Wireless Security	<div> <div>Security Mode:</div> <div>WPA2 Personal ▼</div> </div> <div> <div>Encryption:</div> <div>AES ▼</div> </div> <div> <div>Passphrase:</div> <div>EPIS1234</div> </div> <div> <div>Key Renewal:</div> <div>3600</div> <div>seconds</div> </div>

Setup	Setup	Wireless	Security	Access Restrictions	Applications & Gaming	Admin
	Basic Setup		DDNS		MAC Address Clone	
Internet Setup						
Internet Connection type	Static IP					
	Internet IP Address: 172 . 17 . 80 . 20 Subnet Mask: 255 . 255 . 255 . 0 Default Gateway: 172 . 17 . 80 . 1 DNS 1: 0 . 0 . 0 . 0 DNS 2 (Optional): 0 . 0 . 0 . 0 DNS 3 (Optional): 0 . 0 . 0 . 0					
Optional Settings (required by some internet service providers)	Host Name:					
	Domain Name:					
	MTU: Size: 1500					
Network Setup						
Router IP	IP Address: 172 . 17 . 40 . 1 Subnet Mask: 255.255.255.0					
DHCP Server Settings	DHCP Server: <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled					
	Start IP Address: 172.17.40. 150					
	Maximum number of Users: 50					

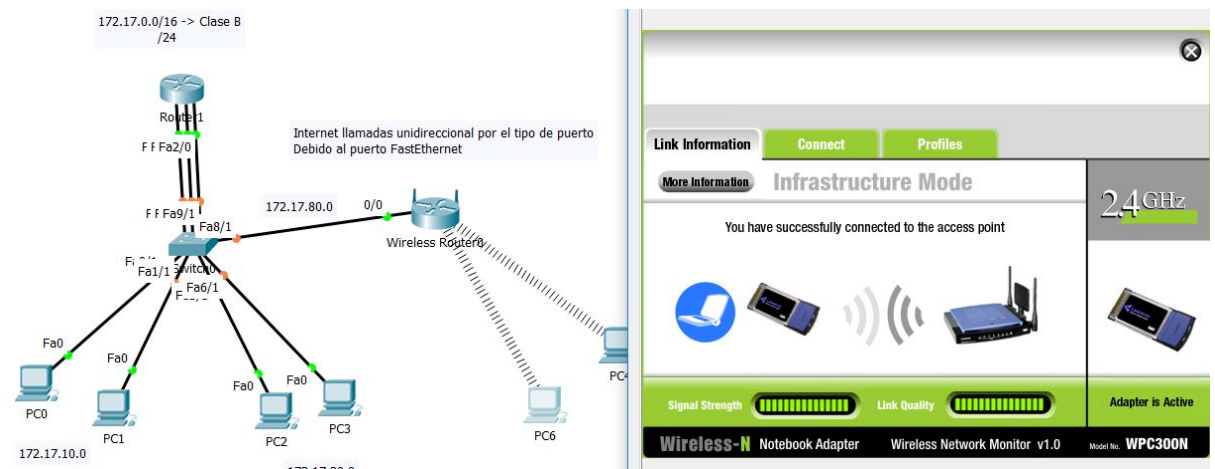
4.3 Configuración del cliente inalámbrico (PC5)

- En Desktop selecciones **PC Wireless**
- En **Profiles** seleccionar **New**
- Asignarle el nombre **EPIS Access**
- Seleccionar **Advanced Setup** e introducir el SSID **EPIS_LAN** en el campo **Wireless Network Name**, presione **Next**
- Elegir **Obtain Network setting automatically (DHCP)** para la configuración de la red y presione **Next**
- En **Wireless Security** seleccionar **WPA2-Personal** este será el método de cifrado, presione **Next**
- Introducir la frase de contraseña o **Passphrase EPIS1234** y presione **Next**
- Guardar con **Save** y presione **Connect to Network**
- Verificar la calidad de la señal con los indicadores **Signal Strength** y **Line Quality**

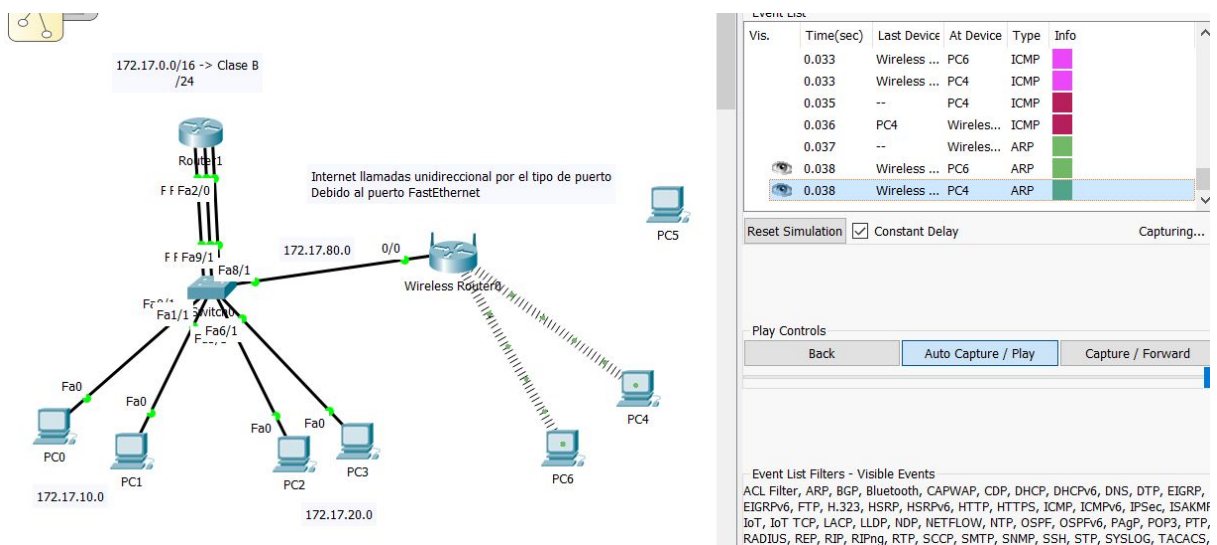
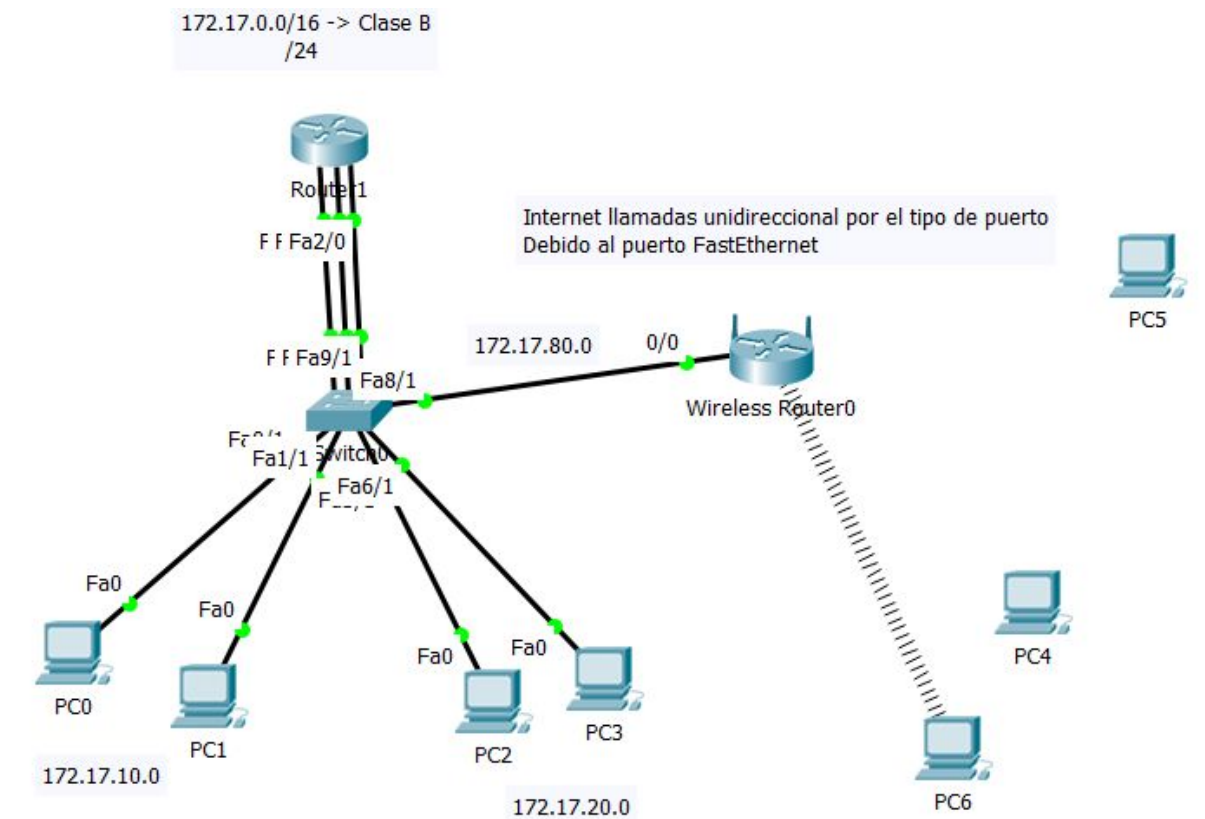
- Seleccione **More Information** para obtener el resumen de la conexión, anote la dirección IP obtenida dinámicamente
- Cerrar **PC Wireless**



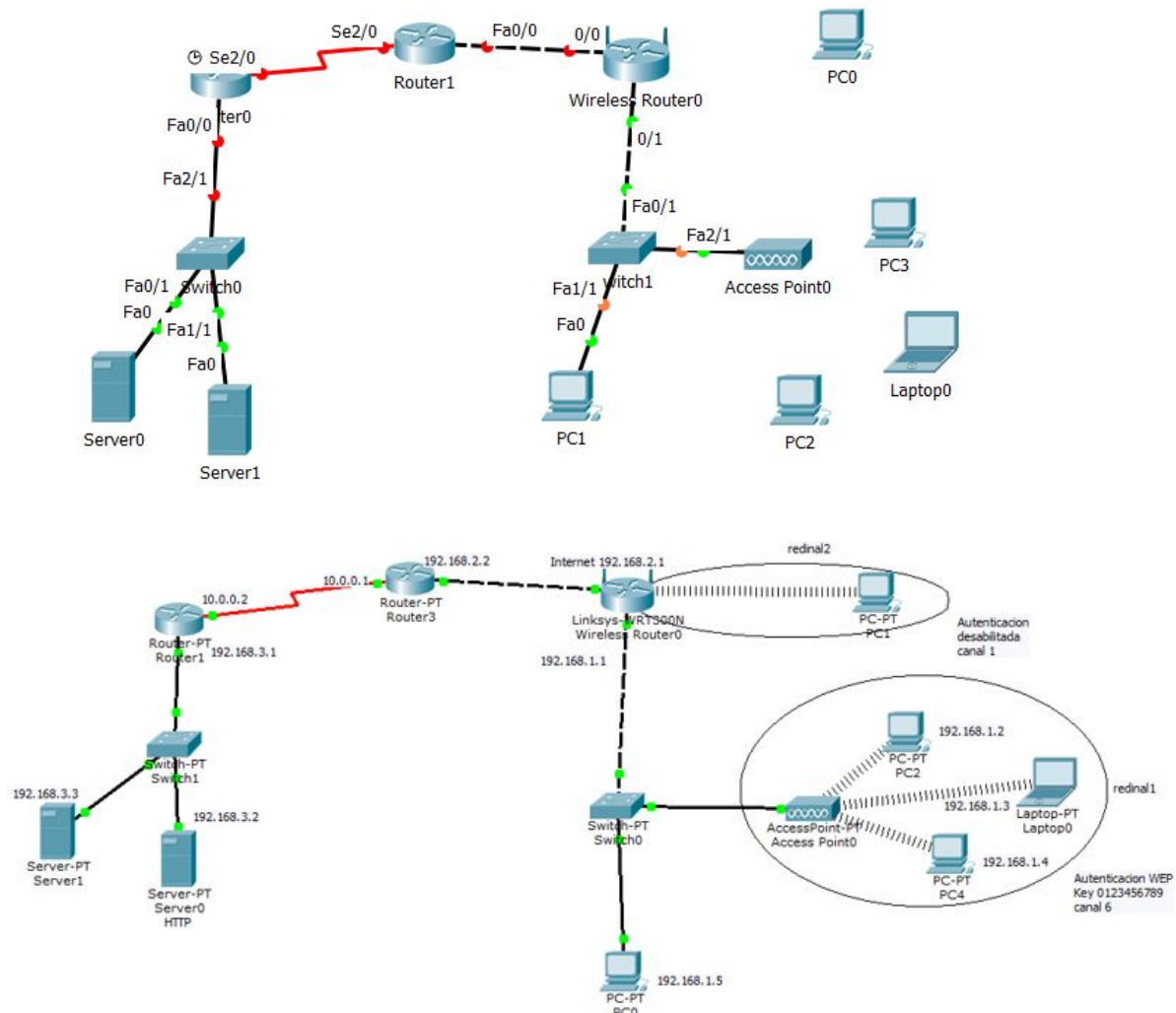
4.4 Configurar la conexión de PC6



- #### 4.5
- Verificar la conexión entre los elementos de la arquitectura, observe la diferencia del tráfico y paquetes cuando se comunican elementos de la misma red y de redes diferentes



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



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

The screenshot shows a network simulation software interface. On the left, there is a network diagram with various devices and their connections. On the right, there is an 'Event List' window showing a table of events. The table has columns for Time(sec), Last Device, At Device, Type, and Info. The events listed are:

Time(sec)	Last Device	At Device	Type	Info
1.197	Switch0	Server0	STP	
1.197	Switch0	Router0	STP	
1.197	Switch0	Server1	STP	
1.298	Switch1	PC1	STP	
1.299	Switch1	Access...	STP	
1.299	Switch1	PC1	STP	
1.299	Switch1	Wireless...	STP	

Below the event list, there are 'Play Controls' and 'Event List Filters - Visible Events'.

<i>Dispositivo</i>	<i>Interfaz</i>	<i>Red</i>	<i>Dirección IP</i>	<i>Máscara</i>	<i>Gateway</i>
PC0	Wireless	192.168.1.0	192.168.1.100	255.255.255.0	192.168.1.1
PC3	Wireless	192.168.1.0	192.168.1.2	255.255.255.0	192.168.1.1
Laptop 0	Wireless	192.168.1.0	192.168.1.3	255.255.255.0	192.168.1.1
PC2	Wireless	192.168.1.0	192.168.1.4	255.255.255.0	192.168.1.1
PC1	FastEthernet	192.168.1.0	192.168.1.5	255.255.255.0	192.168.1.1
Server0	FastEthernet	192.168.3.0	192.168.3.3	255.255.255.0	192.168.3.1

6 Activar el protocolo RIP en cada router

7 Configure los servidores solicitados, pruebe los servicios brindados y genere intercambio de correos electrónicos

V. CONCLUSIONES

PRIMERA: El router wireless permite una sólo dirección para conservar su velocidad.

SEGUNDA: Los Access Point son puentes que nos ayudan a conectar equipos Wireless, y formar una red inalámbrica.

TERCERA: Para la configuración de wireless es posible hacer de modo infraestructura mode o adhoc mode. (config o GUI)

CUARTA: Hablar de Wireless es hablar del Bluetooth de menos rango.

QUINTA Con respecto a LAN implicaría saber sobre los estándares 802.11 siendo algo manejable, pero con respecto a MAN sería el 802.16 donde hay problemas latentes y las redes Ad Hoc y los problemas de enrutamiento.

SEXTA: Entre las autenticaciones que se manejan la EAP, es la de mayor seguridad, pero también es posible tener redes de autenticación para empresas.

VI. CUESTIONARIO.

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

- **Sistema Abierto**

La autenticación de sistema abierto no es realmente una autenticación, porque todo lo que hace es identificar un nodo inalámbrico mediante su dirección de hardware de adaptador inalámbrico. Una dirección de hardware es una dirección asignada al adaptador de red durante su fabricación y se utiliza para identificar la dirección de origen y de destino de las tramas inalámbricas.

- **Clave Compartida**

La autenticación de clave compartida comprueba que el cliente inalámbrico que se va a unir la red inalámbrica conoce una clave secreta. Durante el proceso de autenticación, el cliente inalámbrico demuestra que conoce la clave secreta sin realmente enviarla.

Para el modo de infraestructura, todos los clientes inalámbricos y el punto de acceso inalámbrico utiliza la misma clave compartida.

- **WPA-PSK**

Lo más habitual en una red WiFi doméstica con seguridad WPA es que la autenticación se base en PSK, que son las siglas de Pre Shared Key (clave compartida previamente), es decir, la seguridad de la red WiFi se basa en un secreto compartido (la contraseña de la red WiFi), que conocen sus usuarios y el punto de acceso.

Para simplificarlo, una red WiFi WPA-PSK dispone de una contraseña conocida por todos y cada uno de los clientes que se conectan a la red WiFi. Es la configuración de red más utilizada en los routers WiFi que los ISPs facilitan con sus conexiones de ADSL/Cable/Fibra óptica.

- **WPA2-PSK**

Por supuesto que una red puede ser WPA2-PSK. WPA2 es el nuevo estándar de seguridad WiFi que incorpora algunas mejoras para hacerlo más resistente a algunos ataques conocidos. con WPA2 las contraseñas se pueden seguir intercambiando cómo un secreto compartido (PSK) en las redes domésticas.

- **LEAP**

LEAP es un mecanismo de autenticación de Cisco utilizado como parte de un sistema de autenticación IEEE 802.1x, generalmente considerado como el estándar emergente para la autenticación de red. A mediados de 2003, aparecieron diversas herramientas capaces de generar ataques de diccionarios contra LEAP. "Husmeando" la sesión de autenticación, adivinan la contraseña a partir de una base de datos de nombres y términos. Contra estos ataques, las recomendaciones de Cisco fueron, en un primer momento, utilizar contraseñas difíciles de adivinar, así como emplear otro tipo de EAP, como Protected EAP (PEAP), desarrollo conjunto de Cisco, Microsoft y RSA.

6.2. Describa las características de los siguientes tipos de antenas:

- **De rejilla**

Antena rejilla parabólica TL-ANT2424B está diseñado para el sistema de espectro ensanchado, opera en la banda de 2.4-2.5 GHz y proporciona un funcionamiento direccional 24dBi. El diseño de la superficie con reflector de acero soldado, para tener el mejor rendimiento. Esta antena cuenta con alta ganancia, larga cobertura, peso ligero, estructura compacta y excelente resistencia al viento. Se utiliza para los exteriores y el rango es de hasta 56 km.

- **Yagi**

Son similares a las antenas de televisión, también tienen gran alcance y no es tan complejo orientarlas.

- **Parabólicas**

Concentrar toda la energía en un haz pequeño con una antena parabólica (como el tan familiar plato de televisión por satélite) produce una relación señal a ruido mucho más alta, pero las antenas transmisora y receptora deben estar bien alineadas entre sí. Además, esta direccionalidad permite que varios transmisores alineados en una

fila se comuniquen sin interferencia con varios receptores en fila, siempre y cuando se sigan algunas reglas de espaciado.

- **Pringles**

Construir una antena guía-ondas o la pringles. Consiste en agregarle unos directores para concentrar aún más la señal (Dbm) o agregarle un embudo o adicionarle otra lata para duplicar su longitud, etc, etc, etc. Todo esto con la finalidad de lograr elevar su ganancia (Dbi).

La ganancia de esta antena está entre los 10 y 12 dB.

- **De panel**

Las antenas de panel en su versión más básica consisten en una placa o lámina conductora que adopta distintas formas y tamaños en función de la señal que quiera transmitir. El patrón de radiación puede variar sustancialmente atendiendo a la forma de la placa y a sí se coloca en solitario o formando un conjunto, pero con carácter general todas son muy direccionales, radiando casi en su totalidad en el plano horizontal o en el vertical.

- **Omnidireccionales**

“Envían” la información teóricamente a los 360 grados por lo que es posible establecer comunicación independientemente del punto en el que se esté, ya que no requieren orientarlas.

6.3 En la opción Network Mode que opciones de modo de red existen, explique la diferencia

- **MIXED**

Quiere decir que puedes conectar tantas tarjetas que van a 11mb la b y a 54mb la g, y que no precisamente todas tienen que ser del mismo modo.

- **BG-MIXED**

Quiere decir que puedes conectar tantas tarjetas que van a 11mb la b y a 54mb la g, y que no precisamente todas tienen que ser del mismo modo, podrá tener dos b y una g, etc., y cada una se conectará con su protocolo correspondiente.

- **WIRELESS-G ONLY**

Es de 54mbps.

- **WIRELESS-B ONLY**

Wireless B solamente. Los enrutadores inalámbricos B y los puntos de acceso no son capaces de comunicarse con dispositivos Wireless G solo, por lo que los dispositivos inalámbricos G siempre incluyen una forma de volver a la B inalámbrica si el enrutador lo solicita. Tenga en cuenta que tener un solo dispositivo que solo sea compatible con Wireless B en una red Wireless G ralentizaría toda la red. Por lo tanto, aunque es posible,

no es recomendable mezclar los dispositivos Wireless G y Wireless B en una red.

6.4 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.

6.5 Qué es encriptación y que algoritmos admite la seguridad del router inalámbrico

- Encriptación

Encriptar es protegerla mediante una clave, de manera que sólo los ordenadores cuya configuración coincida con la del router tengan acceso. Es necesaria para mantener segura nuestra red frente a los intrusos, que en el caso de redes domésticas, muy bien pueden ser nuestros “adorables” vecinos.

Cifrado mediante claves simétricas y claves asimétricas.

Algoritmos

o Algoritmos de cifrado asimétrico

Este problema no se va a presentar en los algoritmos asimétricos porque cada usuario tiene una pareja de claves, una pública y la otra privada, independientemente del número de canales seguros que queramos establecer. Únicamente debe proteger la clave privada.

o Algoritmos de cifrado simétrico

DES

El DES (Data Encryption Standard o Estándar de Encriptación de Datos) es el nombre del documento FIPS (Federal Information Processing Standard) 46-1 del Instituto Nacional de Estándares y Tecnología (NIST) del Departamento de Comercio de Estados Unidos. Fue publicado en 1977. En este documento se describe el DEA (Data Encryption Algorithm o Algoritmo de Encriptación de Datos). Es el algoritmo de cifrado simétrico más estudiado, mejor conocido y más empleado del mundo.

Triple-DES

Consiste en encriptar tres veces una clave DES. Esto se puede hacer de varias maneras:

- DES-EEE3: Tres encriptaciones DES con tres claves distintas.
- DES-EDE3: Tres operaciones DES con la secuencia encriptar-desencriptar-encriptar con tres claves diferentes.
- DES-EEE2 y DES-EDE2: Igual que los anteriores pero la primera y tercera operación emplean la misma clave.

Dependiendo del método elegido, el grado de seguridad varía; el método más seguro es el DES-EEE3.

AES

El AES (Advanced Encryption Standard o Estándar Criptográfico Avanzado) es un algoritmo de cifrado por bloques destinado a reemplazar al DES como estándar.

En la actualidad se han aceptado 15 propuestas de estándar de las que saldrán 5

candidatos para una revisión más completa. El proceso no parece que vaya a terminar hasta pasado el año 2000.

RC2

El RC2 es un algoritmo de cifrado por bloques de clave de tamaño variable diseñado por Ron Rivest de RSA Data Security (la RC quiere decir Ron's Code o Rivest's Cipher).

El algoritmo trabaja con bloques de 64 bits y entre dos y tres veces más rápido que el DES en software. Se puede hacer más o menos seguro que el DES contra algoritmos de fuerza bruta eligiendo el tamaño de clave apropiadamente.

El algoritmo está diseñado para reemplazar al DES.

RC4

El RC4 es un algoritmo de cifrado de flujo diseñado por Ron Rivest para RSA Data Security. Es un algoritmo de tamaño de clave variable con operaciones a nivel de byte. Se basa en el uso de una permutación aleatoria y tiene un periodo estimado de más de 10100. Además, es un algoritmo de ejecución rápida en software.

El algoritmo se emplea para encriptación de ficheros y para encriptar la comunicación en protocolos como el SSL (TLS).

RC5

El RC5 es un algoritmo parametrizable con tamaño de bloque variable, tamaño de clave variable y número de rotaciones variable. Los valores más comunes de los parámetros son 64 o 128 bits para el tamaño de bloque, de 0 a 255 rotaciones y claves de 0 a 2048 bits. Fue diseñado en 1994 por Ron Rivest. El RC5 tiene 3 rutinas: expansión de la clave, encriptación y desencriptación. En la primera rutina la clave proporcionada por el usuario se expande para llenar una tabla de claves cuyo tamaño depende del número de rotaciones. La tabla se emplea en la encriptación y desencriptación. Para la encriptación sólo se emplean tres operaciones: suma de enteros, o-exclusiva de bits y rotación de variables.

6.6 Explique cómo es posible que PC1 y PC5 se comuniquen perteneciendo a redes diferentes

Por el DHCP, ya que posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van quedando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

El mismo gateway brindada por el DHCP.

6.7 Describa las principales especificaciones de un Access point (AP)

- Difunde un SSID (service set identifier) ó también llamado nombre de la red inalámbrica, el cuál es visible desde los dispositivos wireless y les permite autenticarse por medio de una contraseña o un PIN (personal identification number).
 - Permiten interactuar con todo tipo de dispositivos inalámbricos (smartphone, netbook, laptop, PDA, tablet, etc.).
- Su tecnología de comunicación es a base de ondas de radio capaces de traspasar obstáculos, sin embargo entre cada uno de ellos, la señal pierde fuerza y se reduce la cobertura.

- Cuenta con un alcance máximo de distancia radial, la cual puede ser de hasta 100 m.
- Integra GUI (graphic user interface), para ser administrado mediante navegador de Internet (simplemente escribiendo en la barra de direcciones la dirección IPv4 del access point y autenticando con usuario / contraseña).

VII. BIBLIOGRAFÍA

[1] *RedesInalámbricas*

<http://todoenredesinalmbricas.blogspot.pe/2008/06/sistema-abierto.html>

[2] *Cisco responde con un nuevo protocolo a los problemas de seguridad de LEAP*

<http://www.networkworld.es/actualidad/cisco-responde-con-un-nuevo-protocolo-a-los-problemas-de-seguridad-de-leap>

[3] *Antena Yagi*

<http://www.neoteo.com/antena-yagi/>

[4] *Antena Parabólica*

https://es.wikipedia.org/wiki/Antena_parab%C3%B3lica

[5] *Diferencia entre Wireless B y Wireless G*

<http://www.differencebetween.net/technology/communication-technology/difference-between-wireless-b-and-wireless-g>

[6] *Encriptar*

https://www.adslayuda.com/wag54g-seguridad_inalambrica_encryption.html

[7] *SSID*

<https://es.wikipedia.org/wiki/SSID>

[8] *Acces Point*

http://www.informaticamoderna.com/Access_point.htm