

# UNIVERSIDAD TÉCNICA DE COTOPAXI



## UNIDAD ACADÉMICA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

### CARRERA DE INGENIERIA EN INFORMATICA Y SISTEMAS COMPUTACIONALES

#### TESIS DE GRADO

Tema:

**“IMPLEMENTACIÓN Y CONFIGURACIÓN DE UNA RED INALÁMBRICA A TRAVÉS DE ACCESS POINT PARA EL LABORATORIO DE REDES DE LA CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI”**

Tesis presentada previa a la obtención del Título de Ingeniero en Informática y Sistemas Computacionales.

#### AUTORES:

Copara Teca Edwin Vinicio.

Toapanta Oña Mayra Elizabeth

#### DIRECTOR:

Ing. Corrales Beltrán Segundo MSc.

Latacunga - Ecuador

Julio del 2014

## AUTORIA

Los criterios emitidos en el presente trabajo de investigación **“IMPLEMENTACIÓN Y CONFIGURACIÓN DE UNA RED INALÁMBRICA A TRAVÉS DE ACCESS POINT PARA EL LABORATORIO DE REDES DE LA CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI”**, son de exclusiva responsabilidad de los autores.

Edwin Vinicio Copara Teca  
N° de C.C. 040106045-4

Mayra Elizabeth Toapanta Oña  
N° de C.C. 050263184-9

## **AVAL DEL DIRECTOR DE TESIS**

En calidad de Director del Trabajo de Investigación sobre el Tema: **“IMPLEMENTACIÓN Y CONFIGURACIÓN DE UNA RED INALÁMBRICA A TRAVÉS DE ACCESS POINT PARA EL LABORATORIO DE REDES DE LA CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI”** de los egresados: Edwin Vinicio Copara Teca y Mayra Elizabeth Toapanta Oña, Postulantes de la Carrera de Ingeniería en Informática y Sistemas Computacionales; considero que dicho Informe Investigativo cumple con los requerimientos metodológicos y aportes científico-técnicos suficientes para ser sometidos a la evaluación del Tribunal de Validación de Tesis que el Honorable Consejo Académico de la Unidad Académica de Ciencias de la Ingeniería y Aplicadas de la Universidad Técnica de Cotopaxi designe, para su correspondiente estudio y calificación.

Latacunga, Julio del 2014

El Director

Ing. Corrales Beltrán Segundo MSc.

## CERTIFICADO

La Carrera de Informática y Sistemas Computacionales de la Universidad Técnica de Cotopaxi, **CERTIFICA** que los egresados Edwin Vinicio Copara Teca con cédula de ciudadanía N°. 0401060454 y Mayra Elizabeth Toapanta Oña con cédula de ciudadanía N° 050263184-9, estudiantes de la Universidad Técnica de Cotopaxi, de la Unidad Académica de Ciencias de la de Ingeniería y Aplicadas, de la Carrera de Informática y Sistemas Computacionales, aplicaron la Tesis con el Tema: **“IMPLEMENTACIÓN Y CONFIGURACIÓN DE UNA RED INALÁMBRICA A TRAVÉS DE ACCESS POINT PARA EL LABORATORIO DE REDES DE LA CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI”**.

Trabajo que se implementó y se dejó en perfecto funcionamiento.

Es todo cuanto puedo certificar en honor a la verdad, los egresados Edwin Vinicio Copara Teca y Mayra Elizabeth Toapanta Oña, pueden hacer uso del presente certificado de la manera que estimen conveniente, siempre y cuando esto no perjudique directa o indirectamente a la Institución.

Atentamente,

Ing. Corrales Beltrán Segundo MSc.

C.C. 050240928-7

Coordinador Carrera de Ingeniería en Informática y Sistemas Computacionales

## **AVAL MIEMBROS DEL TRIBUNAL**

En calidad de Miembros del Tribunal de Grado aprueban el presente Informe de Investigación de acuerdo a las disposiciones reglamentarias emitidas por la Universidad Técnica de Cotopaxi y por la Unidad Académica de Ciencias de la Ingeniería y Aplicadas por cuanto los postulantes: Copara Teca Edwin Vinicio y Toapanta Oña Mayra Elizabeth, con el título de Tesis: **“IMPLEMENTACIÓN Y CONFIGURACIÓN DE UNA RED INALÁMBRICA A TRAVÉS DE ACCESS POINT PARA EL LABORATORIO DE REDES DE LA CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI”**, han considerado las recomendaciones emitidas oportunamente y reúne los méritos suficientes para ser sometido al acto de Defensa de Tesis.

Para constancia firma:

MSc. Víctor Hugo Armas  
Presidente Tribunal

Ing. Diana Marín  
Miembro del Tribunal

Ing. Víctor Medina  
Opositor

Ing. Corrales Beltrán Segundo MSc.  
Director de Tesis

## **AGRADECIMIENTO**

Agradecemos a **Dios** y a las personas que nos apoyaron durante toda la vida; a nuestros padres por su apoyo y esfuerzo constante.

A la Universidad Técnica de Cotopaxi, ya que nos abrió sus puertas para adquirir conocimientos y poderlos aplicar dentro del campo profesional.

Por último agradecemos a nuestro tutor de Tesis quien nos ayudó y orientó en todo momento.

*Copara Teca Edwin Vinicio  
Toapanta Oña Mayra Elizabeth*

## **DEDICATORIA**

Dedicamos este trabajo de investigación a nuestros familiares quienes nos han proporcionado fortaleza y apoyo moral, depositando en cada uno de nosotros su entera confianza.

A nuestros hijos Jeremmy André y Matías Josué, quienes son el motor y la inspiración más grande de nuestras vidas.

*Copara Teca Edwin Vinicio  
Toapanta Oña Mayra Elizabeth*

# ÍNDICE GENERAL

<b>ÍNDICE DE CONTENIDOS</b>	<b>PÁGS.</b>
Portada	i
Autoría	ii
Aval	iii
Aval Tribunal	iv
Certificado de implementación	v
Agradecimiento	vi
Dedicatoria	vii
Índice general	viii
Índice cuadros	xi
Índice gráfico	xi
Índice figuras	xii
Resumen	xiii
Abstract	xv
Certificación Abstract	Xvii
Introducción	xviii
<b>CAPITULO I</b>	
<b>1 Redes</b>	1
<b>1.1 Redes alámbricas</b>	1
1.1.1 Generalidades	1
<b>1.1.2 Topologías</b>	2
1.1.2.1 Bus	2
1.1.2.2 Anillo	3
1.1.2.3 Árbol	3
1.1.2.4 Malla	3
1.1.2.5 Estrella	3
1.1.2.6 Red Celular	3
<b>1.1.3 Medios de conexión</b>	4
1.1.3.1 Medios guiados	4



1.1.3.2 Medios no guiados	6
<b>1.2 Redes inalámbricas</b>	8
1.2.1 Introducción	8
1.2.2 Antecedentes	10
1.2.3 Ventajas y Desventajas de una red inalámbrica	11
<b>1.2.4 Clasificación de las redes inalámbricas</b>	12
1.2.4.1 Redes inalámbricas personales	12
1.2.4.2 Redes inalámbricas por consumo	13
1.2.5 Tipos de redes inalámbricas	14
1.2.6 Topologías de redes inalámbricas	23
<b>CAPITULO II</b>	
<b>2.1. BREVE CARACTERIZACIÓN DEL OBJETO DE ESTUDIO</b>	28
<b>2.2. DISEÑO DE LA INVESTIGACIÓN</b>	29
2.2.1 Tipo de investigación	29
2.3 Metodología	30
2.4 Unidad de estudio	31
<b>2.5 TÉCNICAS</b>	32
2.5.1 Percepción	32
2.5.2 Encuestas	32
2.5.3 Cuestionario	32
<b>2.7 ANÁLISIS E INTERPRETACIÓN DE RESULTADOS</b>	33
<b>CAPITULO III</b>	
<b>3 MARCO PROPOSITIVO</b>	43
3.1 Documento crítico	43
<b>3.2 DISEÑO DE LA PROPUESTA</b>	45
3.2.1 Fundamentación	45
3.2.2 Justificación	46
3.3 Objetivo	48
<b>3.4 DESARROLLO DE LA PROPUESTA</b>	48
3.4.1 Exposición de motivos	48
3.4.1.1 Dispositivos WLAN	48

3.4.1.2 Modos de operación inalámbrica	52
3.4.1.3 Seguridades inalámbricas	55
3.4.1.3.1 Mecanismos básicos de seguridad	55
<b>3.4.1.3.1.1 Cifrado</b>	56
3.4.1.3.1.1.1 Cifrado WEP	56
3.4.1.3.1.1.2 Cifrado WPA	59
3.4.1.3.1.1.2.1 Cifrado WPA-PSK	60
3.4.1.3.1.1.2.2 Cifrado WPA-EMPRESARIAL	61
<b>3.4.1.3.1.1.3 Cifrado WPA2</b>	62
3.4.1.3.1.1.3.1 Autenticación en sistema abierto	62
3.4.1.3.1.1.3.2 Autenticación con clave compartida	63
3.4.1.3.1.1.3.3 Autenticación EAP (IEEE 802.1X)	64
3.4.1.3.1.1.3.4 Autenticación IEEE 802.11i	66
3.4.1.3.1.1.3.4.1 TKIP (Temporary Key Integrity Protocol)	67
3.4.1.3.1.1.3.4.2 CCMP	68
3.4.1.3.1.1.3.4.2 WRAP	68
3.4.1.4 Guía de Instalación y configuración Access Point cisco WAP 321	69
3.4.1.4.1 Guía de inicio rápido	77
<b>3.5 CONCLUSIONES Y RECOMENDACIONES</b>	88
5.1 Conclusiones	88
5.2 Recomendaciones	89
<b>REFERENCIAS BIBLIOGRÁFICAS</b>	90
Bibliografía consultada	90
Bibliografía citada	90
Linografías	92
Textos legales	92
<b>ANEXOS</b>	93

## ÍNDICE CUADROS

Tabla N° 01 Topología de las redes	2
Tabla N° 02 Medios de conexión guiados	4
Tabla N° 03 Medios de conexión no guiados	7
Tabla N° 04 Cuadro resumen medios de transmisión	8
Tabla N° 05 Ventajas y desventajas de una red inalámbrica	11
Tabla N° 06 Tecnologías inalámbricas	19
Tabla N° 07 Topologías básicas de una red	20
Tabla N° 08 Presentación de datos de la encuesta	33
Tabla N° 09 Implementar y configurar laboratorio de redes	34
Tabla N° 10 Uso de dispositivos tecnológicos nuevos	35
Tabla N° 11 Mejorar actividades. enseñanza-aprendizaje	36
Tabla N° 12 Uso tecnología Wireless – ambiente real	37
Tabla N° 13 Implemente y configure Access Point	38
Tabla N° 14 Memoria técnica de Configuración Access Point	39
Tabla N° 15 Access Point interconecta redes.	40
Tabla N° 16 Mejorar nivel académico estudiantes	41

## ÍNDICE GRÁFICO

Grafico 01 Implementar y configurar laboratorio de redes	34
Grafico 02 Uso de dispositivos tecnológicos nuevos	35
Grafico 03 Mejorar actividades. enseñanza-aprendizaje	36
Grafico 04 Uso tecnología Wireless – ambiente real	37
Grafico 05 Implemente y configure Access Point	38
Grafico 06 Memoria técnica de configuración Access Point	39
Grafico 07 Access Point interconecta redes.	40
Grafico 08 Mejorar nivel académico estudiantes	41
Grafico 09 Resumen general	42

## ÍNDICE FIGURAS

Figura 01 Topología de las redes	4
Figura 02 Transmisión inalámbrica	6
Figura 03 Ámbito de uso de los tipos de redes inalámbricas	15
Figura 04 Red WLAN	16
Figura 05 Red WPAN	17
Figura 06 Red WWAN	18
Figura 07 Topologías de una red inalámbrica	20
Figura 08 Conexión de redes inalámbricas	22
Figura 09 Enlaces inalámbricos	22
Figura 10 Esquema modo de infraestructura	24
Figura 11 Esquema modo Ad-hoc	27
Figura 12 Access Point WAP Cisco 321	49
Figura 13 Conjunto de servicios básicos independientes	53
Figura 14 Conjunto de servicios básicos	54



**UNIVERSIDAD TÉCNICA DE COTOPAXI**  
**UNIDAD ACADÉMICA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS**  
**Latacunga – Ecuador**

---

**TEMA: “IMPLEMENTACIÓN Y CONFIGURACIÓN DE UNA RED INALÁMBRICA A TRAVÉS DE ACCESS POINT PARA EL LABORATORIO DE REDES DE LA CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI”**

**Autores:**

Copara Teca Edwin Vinicio.  
Toapanta Oña Mayra Elizabeth

**RESUMEN**

El vertiginoso avance tecnológico que vive la humanidad ha hecho imprescindible el uso permanente de computadoras en todas y cada una de las actividades de las personas, sea en su entorno laboral (oficinas, bancos, escuelas, empresas, industrias, etc.) o en el hogar. Por su naturaleza un computador (Pc-escritorio, laptop, tablet, ipon, ipad, celular), realizan y ejecutan de forma individual y personalizada la función para la que fueron creados; en ocasiones y a través del actual mundo globalizado es necesario la interacción, interconexión e intercambio de la información con otras computadoras, es decir hay que tomar en cuenta la clase de recursos de transmisión y recepción de datos que les permita comunicarse con otras computadoras y los dispositivos a los que puede acceder para lograr tal fin. De ahí, nace la importancia de tener una buena red, ya sea en los aspectos de medios de transmisión, protocolos de comunicación, **dispositivos externos**, entre otros. Dichos elementos permitirán un desempeño óptimo de los recursos, logrando una transmisión de datos más rápida, segura y plenamente fiable.

El presente trabajo se ocupa del análisis exhaustivo de los aspectos teóricos esenciales en la implementación y configuración de una red inalámbrica a través de un Punto de Acceso CISCO WAP 321 Wireless-N con configuración de un solo punto.

Es un dispositivo que permite la interconexión de varias redes de forma alámbrica o no, facilita la conexión de dispositivos fijos y móviles, logrando de esta manera que los alumnos del Alma Mater de Cotopaxi accedan de forma libre a la red; y, de manera específica los estudiantes de la Carrera de Informática y Sistemas Computacionales utilicen la Guía de Implementación y Configuración como medio esencial de manipulación y aprendizaje del dispositivo ACCESS POINT CISCO WAP 321, elemento usado en la aplicación práctica de los conocimientos teóricos y la ampliación de conocimientos bajo una situación de simulación real y desempeños auténticos indispensable en el mundo laboral.

Actualmente el ACCESS POINT CISCA WAP 321, tiene un sistema propio y básico de configuración, pero posee un sin número de funciones que garantizan un uso efectivo de todas sus bondades, lastimosamente no posee un guía específica de implementación, configuración y funcionamiento y al ser un dispositivo creado por empresas americanas sus bases vienen dadas en idioma inglés. De ahí nace la necesidad de elaborar una GUIA DE INSTLACION Y CONFIGURACION DEL ACCESS POINT CISCO WAP 321 DE UN SOLO PUNTO, como un elemento didáctico para la práctica de redes de los estudiantes de Informática y sistemas computacionales.



**UNIVERSIDAD TÉCNICA DE COTOPAXI**  
**UNIDAD ACADÉMICA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS**  
**Latacunga – Ecuador**

---

**TOPIC: “SETUP AND IMPLEMENTATION A WIRELESS ACCESS POINT THROUGH NETWORKING LABORATORY CAREER IN COMPUTER ENGINEERING AND COMPUTER SYSTEM OF THE TECHNICAL UNIVERSITY COTOPAXI”**

**Author:**

Copara Teca Edwin Vinicio.  
Toapanta Oña Mayra Elizabeth

**ABSTRACT**

The faster technological advancement that humanity has made imperative the permanent use of computers in all of the people activities, whether in the workplace (offices, banks, schools, businesses, industries, etc.) or household. By its nature a computer (PC- desktop, laptop, tablet, ipon, ipad, cell), made and executed individually customized function for which they were created, sometimes in a globalized world, where the interaction is necessary so you interconnection and exchange of information with other computers, have to take into account the resource class transmission and reception of data that allows them to communicate with other computers and devices that can access to achieve that purpose. So, the importance arises of having a network, either aspect of transmission media, communication protocols, external devices, among others. These elements allow optimal performance of resources, achieving faster transmission, fully secure and reliable data.

The present researching deals with the detailed analysis of the essential theoretical aspects in the implementation and configuration of a wireless network via an Access Point CISCO Wireless- N 321 WAP configuration with a single point.

A device that allows the interconnection of several networks in a wired or not, it makes connecting fixed and mobile devices, thus achieving students the Alma Mater of Cotopaxi log in freeform network; and specifically the students of the School of Computer Science and Computer Systems use the Setup and Implementation Guide as an essential means of handling and learning WAP ACCESS POINT CISCO 321 element device used in the practical application of theoretical knowledge and the expansion knowledge in a situation of actual simulation and real performance essential in the workplace.

Currently the ACCESS POINT CISCO WAP 321 has its own configuration and basic system, but has a number of features to ensure effective use of all its benefits, unfortunately does not have a specific guide implementation, configuration and operation and being a device created by American companies bases are given in English. Hence arises the need for a INSTALLATION GUIDE AND CONFIGURATION 321 ACCESS POINT CISCO WAP ONE ITEM, as a didactic element for practical networks students of Informatics and computer systems.





**UNIVERSIDAD TÉCNICA DE COTOPAXI**  
**UNIDAD ACADÉMICA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS**  
**Latacunga – Ecuador**

---

**CERTIFICACIÓN:**

Alison Mena Barthelotty, Docente del Centro de Idiomas de la Universidad Técnica de Cotopaxi y previo a la petición formulada por parte del Señor Copara Teca Edwin Vinicio portador de la cédula de ciudadanía N° 040106045-4 y la Señora Toapanta Oña Mayra Elizabeth portador de la cédula de ciudadanía N° 0502563184-9, estudiantes de la Carrera de Ingeniería en Informática y Sistemas Computacionales, AVALO, haber revisado y corregido el ABSTRACT del tema investigativo: **“IMPLEMENTACIÓN Y CONFIGURACIÓN DE UNA RED INALÁMBRICA A TRAVÉS DE ACCESS POINT PARA EL LABORATORIO DE REDES DE LA CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI”**. Es todo lo que puedo certificar en honor a la verdad y autorizo la utilización del presente documento en lo que estimen conveniente.

Alison Mena Barthelotty

C.C.050180125-2.

**ENGLISH – TEACHER**

## INTRODUCCIÓN

La red es una de las principales evoluciones de la tecnología, va cambiando de forma permanente a través del uso de medios y dispositivos cada vez más avanzados y que permiten una conexión e intercambio de información inalámbrica.

La red es un conjunto de dispositivos electrónicos inteligentes interconectados entre sí, esto quiere decir, máquinas que procesen y/o manipulen información.

En los últimos años las redes inalámbricas (WLAN, Wireless Local Area Network) han ganado muchos adeptos y popularidad ya sea en el sector público o en el sector privado. Las redes inalámbricas permiten a los usuarios acceder a información y a recursos en tiempo real sin necesidad de estar físicamente en un sólo lugar.

Una WLAN es un conjunto de Puntos de Acceso (AP (Access Point)) y clientes que se interconectan entre sí, formando una red, un punto de acceso en la red puede soportar un número ya determinado de computadoras y tiene un rango de alrededor de 30 metros, siempre se trata de que estos puntos de acceso sean colocados a una altura considerable, para evitar cualquier tipo de interferencia (muros, árboles, etc.).

Con WLAN la red por sí misma es móvil y elimina la necesidad de usar cables y establece nuevas aplicaciones añadiendo flexibilidad a la red y, lo más importante, incrementa la productividad y eficiencia en las actividades diarias de la empresa.

Un usuario dentro de una red inalámbrica puede transmitir y recibir voz, datos y video dentro de edificios, entre edificios o campus universitarios e inclusive sobre áreas metropolitanas a velocidades de hasta 54 Mbps.

En el **capítulo I** se realiza un análisis teórico de las redes, iniciamos dando un conocimiento básico sobre las redes físicas, así como las topologías, arquitectura y medios de conexión; posteriormente nos centramos en el estudio de las redes inalámbricas su clasificación, topologías y cifrados.

En el **capítulo II** se encuentra determinada la investigación de campo, en donde se definió la población a la cual se aplicó una encuesta y en donde los resultados obtenidos fueron analizados e interpretados discrecionalmente, dicha información fue obtenida de los alumnos de la Carrera de Ingeniería en Informática y Sistemas Computacionales, en relación al uso del Access Point como elemento indispensable de las redes inalámbricas.

En el **capítulo III** presentamos la propuesta investigativa, misma que va dirigida a la **“IMPLEMENTACIÓN Y CONFIGURACIÓN DE UNA RED INALÁMBRICA A TRAVÉS DE ACCESS POINT PARA EL LABORATORIO DE REDES DE LA CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI”**, la cual servirá como un elemento físico y lógico para las prácticas de redes, para esto se desarrolla una guía de implementación y configuración rápida, una guía administrativa del Access Point WAP CISCO 321 de un solo punto y un video tutorial de instalación y configuración. Así mismo tenemos las conclusiones y recomendaciones, las mismas que hacen su enfoque a elementos básicos y esenciales que se deben tener en cuenta en el uso de un Punto de Acceso.

# CAPITULO I

## REDES

### 1.1 REDES ALÁMBRICAS

#### 1.1.1 GENERALIDADES

Para el Ingeniero Luis Alvarado Cáceres (mayo 2013), en su obra Manual Redes de Computadora, dice: “Red de computadoras, es una colección interconectada de computadoras autónomas. Dos computadoras se consideran interconectadas cuando son capaces de intercambiar información” (p. 1)

Según el autor Luis Tarazona (2004), en su libro Redes de computadora, el hardware y el software detrás de la Tecnología de la Información, nos indican que una red es: “ Colección de computadores autónomos, interconectados a través de un medio físico cualquiera. La interconexión de computadores significa que éstos pueden intercambiar información” (p. 11)

Los investigadores concuerdan con las definiciones anteriores y definen a una red de computadoras como una serie de ordenadores y otros dispositivos conectados entre sí, esta conexión les permite comunicarse entre ellos, además de compartir información y recursos. Las redes varían en tamaño, pueden reducirse a una oficina o extenderse globalmente a nivel de una metrópoli y a nivel mundial.

Una red conectada en un área limitada se conoce como Red de área local (LAN/MAN), está contenida a menudo en una sola ubicación.

Una Red de área extensa (WAN) es un grupo de dispositivos, o varias LAN, conectados en una área geográficamente mayor, a menudo por medio de líneas

telefónicas u otro formato de cableado como puede ser una línea dedicada de alta velocidad, fibra óptica (intro continental o Inter, continental) o enlace vía satélite. Uno de los mayores ejemplos de WAN es el internet. Los dispositivos de una red se comunican entre sí transmitiendo información en grupos de pequeños impulsos eléctricos (conocidos como paquetes).

Cada paquete contiene la dirección del dispositivo transmisor (la dirección fuente) y la del receptor (dirección de destino). Los PCs y otro equipo de la red utilizan esta información para ayudar al paquete a llegar a su destino. Cuando dos dispositivos se intentan comunicar simultáneamente, ocurrirá una colisión entre los paquetes transmitidos, que los dispositivos transmisores detectan. Al detectar esta colisión, los dispositivos dejan de transmitir y hacen una pausa antes de volver a enviar los paquetes.

### 1.1.2 TOPOLOGÍAS

Según el criterio de los autores: José María Barceló Ordinas, Jordi Ñigo Grieria, Ramon Martí Escalé, Enric Peig Olivé y Xavier Perramon Tornil (2004) en su manual Software Libre hacen mención a que: “La topología de red es la disposición física en la que se conecta una red de ordenadores. Si una red tiene diversas topologías se la llama mixta.

Entre las topologías más comunes se tiene: bus, anillo, árbol, malla, estrella y topología de red celular.”

**Tabla 1:** Topologías de las redes

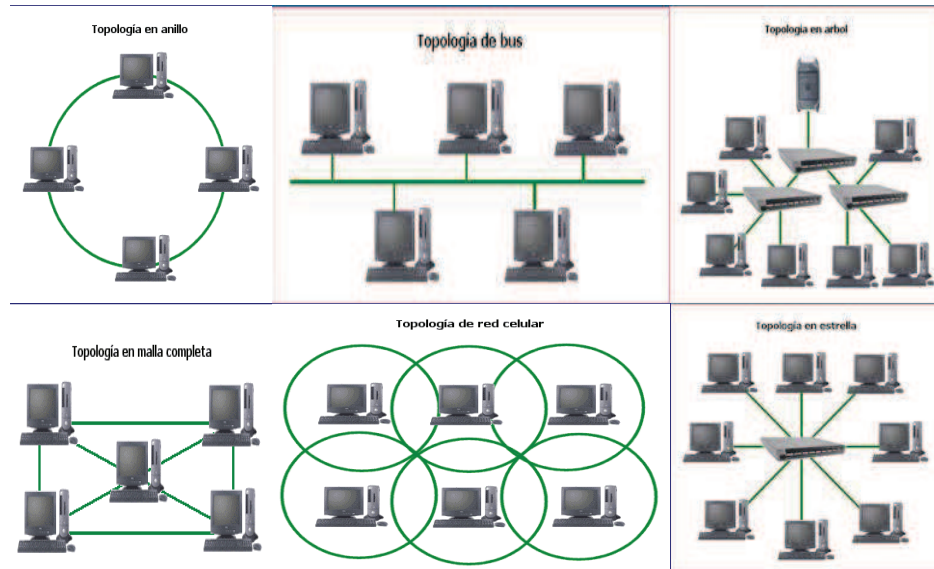
<b>Topologías</b>	<b>CARACTERÍSTICAS</b>	<b>VENTAJAS</b>	<b>DESVENTAJAS</b>
<b>BUS</b>	<ul style="list-style-type: none"> <li>- Las estaciones están conectadas a un único canal de comunicaciones</li> <li>- Sencillo de instalar la cantidad de cable utilizada es mínima</li> </ul>	<ul style="list-style-type: none"> <li>- El fallo de una estación no repercute en la red</li> </ul>	<ul style="list-style-type: none"> <li>- La ruptura de un cable puede dejarla totalmente inutilizada</li> <li>- Longitud (&lt;2000mts) poco segura, poco control de flujo.</li> </ul>

<b>ANILLO</b>	<ul style="list-style-type: none"> <li>- Las estaciones se conectan formando un anillo</li> <li>- Cada estación está conectada a la siguiente y la última está conectada a la primera, c/e tiene un receptor y un transmisor que hace la función de repetidor, pasando la señal a la siguiente estación del anillo.</li> </ul>	<ul style="list-style-type: none"> <li>- La comunicación se da por el paso de un token o testigo</li> </ul>	<ul style="list-style-type: none"> <li>- La ruptura de un cable puede dejarla totalmente inutilizada</li> </ul>
<b>MALLA</b>	<ul style="list-style-type: none"> <li>- Los nodos están colocados en forma de árbol parecida a una serie de redes en estrella interconectadas</li> </ul>	<ul style="list-style-type: none"> <li>- Es una variación de la red en bus, la falla de un nodo no implica interrupción en las comunicaciones.</li> <li>- Se comparte el mismo canal de comunicaciones.</li> <li>- Cuenta con un cable principal (<i>backbone</i>) al que hay conectadas redes individuales en bus</li> </ul>	<ul style="list-style-type: none"> <li>- Multiplicidad de conexiones</li> </ul>
<b>ARBOL</b>	<ul style="list-style-type: none"> <li>- Cada nodo está conectado a uno o más de los otros nodos, es posible llevar los mensajes de un nodo a otro por diferentes caminos.</li> </ul>	<ul style="list-style-type: none"> <li>- Si la red de malla está completamente conectada no puede existir absolutamente ninguna interrupción en las comunicaciones.</li> <li>- Cada servidor tiene sus propias conexiones con todos los demás servidores.</li> </ul>	<ul style="list-style-type: none"> <li>- Lleva un gran margen de complejidad</li> </ul>
<b>ESTRELLA</b>	<ul style="list-style-type: none"> <li>- Las estaciones están conectadas directamente al servidor u ordenador y todas las comunicaciones se hacen necesariamente a través del servidor</li> <li>- Todas las estaciones están conectadas por separado a un centro de comunicaciones, concentrador o nodo central, pero no están conectadas entre sí</li> </ul>	<ul style="list-style-type: none"> <li>- Mayor facilidad de supervisión y control de información (todos los mensajes pasan por el hub o concentrador).</li> <li>-El malfuncionamiento de un ordenador no afecta en nada a la red</li> </ul>	<ul style="list-style-type: none"> <li>- El costo del cableado puede llegar a ser muy alto.</li> <li>- Su punto débil consta en el concentrador ya que es el que sostiene la red en uno</li> </ul>
<b>CELULAR</b>	<ul style="list-style-type: none"> <li>- Está compuesta por áreas circulares o hexagonales, cada una de las cuales tiene un nodo individual en el centro.</li> <li>- Es un área geográfica dividida en regiones (celdas) para los fines de la tecnología inalámbrica.</li> <li>- En esta tecnología no existen enlaces físicos; si ondas electromagnéticas.</li> </ul>	<ul style="list-style-type: none"> <li>- No existe ningún medio tangible aparte de la atmósfera terrestre o el del vacío del espacio exterior (y los satélites)</li> </ul>	<ul style="list-style-type: none"> <li>- Las señales se encuentran presentes en cualquier lugar de la celda y, de ese modo, pueden sufrir disturbios y violaciones de seguridad.</li> </ul>

**Fuente:** Inv. Directa.

**Elaborado por:** Edwin Copara - Mayra Toapanta.

**Figura 1:** Topología de las redes




Fuente: [https://www.google.com.ec/search?q=topologias+de+red&biw=1024&bih=627&source=lnms&tbm=isch&sa=X&ei=Y8FOU4ebPJTRsASUvIH4Dg&ved=0CAYQ\\_AUoAQ](https://www.google.com.ec/search?q=topologias+de+red&biw=1024&bih=627&source=lnms&tbm=isch&sa=X&ei=Y8FOU4ebPJTRsASUvIH4Dg&ved=0CAYQ_AUoAQ)

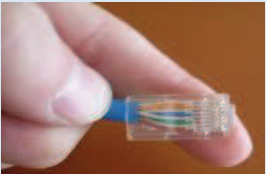



### 1.1.3 MEDIOS DE CONEXIÓN

#### 1.1.3.1 Medios Guiados

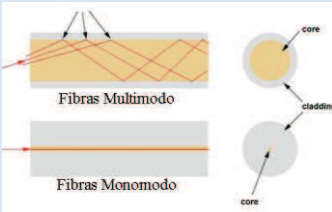
Según el criterio del Ingeniero Luis Alvarado Cáceres (mayo 2013), en su obra Manual Redes de Computadora, da a conocer los siguientes medios de conexión. (p. 44-57)

**Tabla 2:** Medios de conexión guiados.

MEDIOS	DETALLE	FIGURA
<b>Cable de par trenzado</b>	<p>Conocido como UTP (Unshielded Twisted Pair), suele ser la mejor opción para una PYME (Pequeñas y Medianas Empresas). La calidad del cable y consecuentemente, la cantidad de datos que es capaz de transmitir, varían en función de la categoría del cable</p> <p>El estándar para conectores de cable UTP es el RJ-45. Se trata de un conector de plástico similar al conector del cable</p>	

<p>Sin apantallar</p> <p>Con apantallamiento.</p>	<p>telefónico. La sigla RJ se refiere al estándar Registerd Jack, creado por la industria telefónica. Este estándar se encarga de definir la colocación de los cables en su pin correspondiente.</p> <p>Una de las desventajas del cable UTP es que es susceptible a las interferencias eléctricas. Para entornos con este tipo de problemas existe un tipo de cable que lleva apantallamiento, conocido como STP (Shielded Twisted Pair), esto significa protección contra interferencias eléctricas.</p>	 
<p><b>Cable coaxial</b></p>	<p>Contiene un conductor de cobre en su interior. Este va envuelto en un aislante para separarlo de un apantallado metálico con forma de rejilla que aísla el cable de posibles interferencias externas.</p> <p>Aunque la instalación de cable coaxial es mes complicada que la del UTP, éste tiene un alto grado de resistencia a las interferencias, también es posible conectar distancias mayores que con los cables de par trenzado.</p>	
<p><b>Cable de fibra óptica</b></p> <p><b>Multimodo</b></p>	<p>Consiste en un centro de cristal rodeado de varias capas de material protector. Lo que se transmite no son señales eléctricas sino luz, con lo que se elimina la problemática de las interferencias. Esto lo hace idea para entornos en los que haya gran cantidad de interferencias eléctricas. También se utiliza mucho en la conexión de redes entre edificios, debido a su inmunidad a la humedad y a la exposición solar.</p> <p>Es aquella que puede propagar más de un modo de luz. Una fibra multimodo puede tener más de mil modos de propagación de luz. Se usan comúnmente en aplicaciones de corta distancia, menores a 1 km. Su distancia máxima es de 2 km. y usa cañón láser de baja I.</p>	



<b>Monomodo</b>	<p>Es una fibra óptica en la que sólo se propaga un modo de luz. Se logra reduciendo el diámetro del núcleo de la fibra hasta un tamaño (8,3 a 10 micrones) que sólo permite un modo de propagación, su transmisión es en línea recta. Su distancia va desde 2.3 km. a 100 km. Máximo. A diferencia de las fibras multimodo, las fibras monomodo permiten alcanzar grandes distancias y transmitir elevadas tasas de bit.</p>	
-----------------	---	---

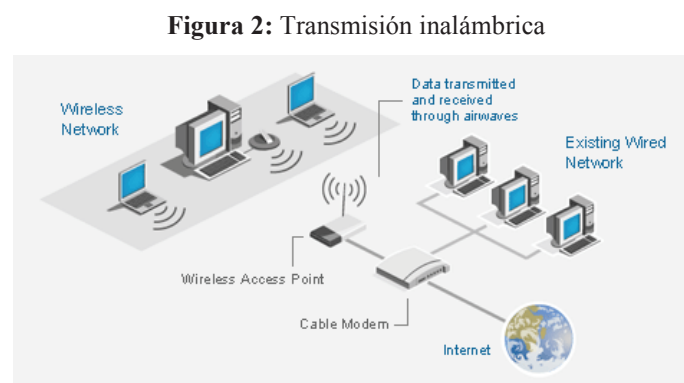
**Fuente:** Inv. Directa.

**Elaborado por:** Edwin Copara - Mayra Toapanta.

#### 1.1.4.2 No Guiados

#### Transmisión inalámbrica

No todas las redes se implementan sobre un cableado, algunas utilizan señales de radio de alta frecuencia o hacen infrarrojos para comunicarse. Cada punto de la red posee una antena desde la que emite y recibe. Para largas distancias se pueden utilizar teléfonos móviles o satélites.



**Fuente:** [http://www.innetrex.com/wireless\\_install.php](http://www.innetrex.com/wireless_install.php)

Este tipo de conexión está especialmente indicado para su uso con portátiles o para edificios viejos en los que es imposible instalar un cableado.

De acuerdo al criterio de William Stallings (2013), en su obra Comunicaciones y Redes de Computadoras, Capítulo IV Nivel Físico y Medios de Transmisión, da a conocer los siguientes medios de conexión no guiado. (p. 6-31)

**Tabla 3:** Medios de conexión no guiados.

MEDIOS	DETALLE	FIGURA
<p style="text-align: center;"><b>Infrarrojos</b></p>	<p>Poseen las mismas técnicas que las empleadas por la fibra óptica pero son por el aire, excelente opción para las distancias cortas, hasta los 2km generalmente.</p> <p>Las emisiones pueden ser de forma analógica o digital pero han de estar en la línea visible.</p> <p>Utilizan antenas parabólicas-Para conexiones a larga distancia, se utilizan conexiones intermedias punto a punto entre antenas parabólicas.</p>	
<p style="text-align: center;"><b>Satélite</b></p>	<p>Sus ventajas son la libertad geográfica, su alta velocidad, pero sus desventajas tienen como gran problema el retardo de las transmisiones debido a tener que viajar grandes distancias.</p> <p>El satélite recibe las señales y las amplifica o retransmite en la dirección adecuada. Para mantener la alineación del satélite con los receptores y emisores de la tierra, el satélite debe ser geoestacionario.</p> <p>Las microondas son unidireccionales y las ondas de radio omnidireccionales.</p> <p>Las microondas son más sensibles a la atenuación producida por la lluvia.</p>	

**Fuente:** Inv. Directa.

**Elaborado por:** Edwin Copara - Mayra Toapanta.

**Tabla 4:** Cuadro resumen medios de transmisión

<b>MEDIO DE TRANSMISION</b>	<b>ANCHO BANDA</b>	<b>CAPACIDAD MÁXIMA</b>	<b>CAPACIDAD USADA</b>	<b>OBSERVACIONES</b>
<b>Cable de pares</b>	250 KHz	10 Mbps	9600 bps	- Apenas usados hoy en día. - Interferencias, ruidos.
<b>Cable coaxial</b>	400 MHz	800 Mbps	10 Mbps	- Resistente a ruidos e interferencias - Atenuación.
<b>Fibra óptica</b>	2 GHz	2 Gbps	100 Mbps	- Pequeño tamaño y peso, inmune a ruidos e interferencias, atenuación pequeña. - Caras. Manipulación complicada.
<b>Microondas por satelital</b>	100 MHz	275 Gbps	20 Mbps	- Se necesitan emisores/receptores.
<b>Microondas terrestres</b>	50 GHz	500 Mbps		- Corta distancia y atenuación fuerte. - Difícil instalar.
<b>Láser</b>	100 MHz			- Poca atenuación. - Requiere visibilidad directa emisor/ receptor.

Fuente: Inv. Directa.

Elaborado por: Edwin Copara - Mayra Toapanta.

## 1.2 REDES INALÁMBRICAS

### 1.2.1 Introducción

Para el Ingeniero Luis Alvarado Cáceres (mayo 2013), en su obra Manual Redes de Computadora, Capítulo 8, Redes inalámbricas, dice que: “En estas redes los clientes se conectan a la red usando señales de radio en reemplazo del cobre, en parte o en toda la conexión entre el cliente y la central de conmutación.

Técnica de acceso muy utilizada en regiones donde las redes están aún en desarrollo. También en países de reciente apertura en competencia resulta ideal para un rápido despliegue de red” (p. 105)

Para Lilian Chamorro y Ermanno Pietrosevoli (2008), integrantes de la Asociación para el progreso de las comunicaciones, en su publicación, temas emergentes Redes inalámbricas para el desarrollo en América Latina y el Caribe, manifiestan que: “Las redes inalámbricas permiten la interconexión entre dos o más puntos, nodos o estaciones, por medio de ondas electromagnéticas que viajan a través del espacio llevando información de un lugar a otro. Para lograr el intercambio de información existen diferentes mecanismos de comunicación o protocolos que establecen reglas que permiten el flujo confiable de información entre nodos” (p, 3)

Para los investigadores las redes inalámbricas pueden proporcionar beneficios de conectividad en red sin las restricciones de estar ligadas a una ubicación o tejidas por cables. Las conexiones inalámbricas pueden ampliar o reemplazar una infraestructura cableada en situaciones en donde es costoso o está prohibido tender cables.

Las instalaciones temporales son un ejemplo de cuándo una red inalámbrica puede tener sentido o hasta ser requerida. Algunos tipos de edificios o códigos de construcción pueden prohibir el uso de cables, haciendo de las redes inalámbricas una alternativa importante.

Y por supuesto el fenómeno de "no tener cables nuevos" que se relaciona con una instalación inalámbrica, conjuntamente con la red de líneas telefónicas y hasta la red eléctrica, se ha vuelto un catalizador principal para las redes en el hogar y la experiencia de un hogar conectado. Los usuarios que cada vez son más móviles se vuelven un candidato evidente para una red inalámbrica.

El acceso móvil a redes inalámbricas se puede lograr utilizando computadoras portátiles y tarjetas de red inalámbricas. Esto permite al usuario viajar a distintas ubicaciones - salas de reuniones, pasillos, vestíbulos, cafeterías, salas de clases, etc. - y aún tener acceso a los datos en red. Sin un acceso inalámbrico, el usuario tendría que llevar molestos cables y encontrar un punto de red para conectarse.

Más allá del campo corporativo, el acceso a Internet y hasta los sitios corporativos podría estar disponible a través de puntos de redes inalámbricas en lugares públicos. Aeropuertos, restaurantes, estaciones de ferrocarril y áreas comunes en una ciudad pueden contar con este servicio. Cuando el profesional que viaja llega a su destino, quizás para reunirse con un cliente en su oficina corporativa, él podría tener acceso limitado a través de una red local inalámbrica. La red puede reconocer al usuario de otra empresa y crear una conexión que quede aislada de la red local corporativa, pero que proporcione acceso a Internet al visitante.

### **1.2.2 ANTECEDENTES**

La primera red de computadores inalámbrica registrada, data de 1971 en la Universidad de Hawai cuando se conectaron siete computadores desplegados en cuatro islas hawaianas, AlohaNet, trabajando alrededor de los 400 MHz.

El origen de las LAN inalámbricas (WLAN) se remonta a la publicación en 1979 de los resultados de un experimento realizado por ingenieros de IBM en Suiza, consistía en utilizar enlaces infrarrojos para crear una red local en una fábrica. Estos resultados, publicados en el volumen 67 de los Proceedings del IEEE, pueden considerarse como el punto de partida en la línea evolutiva de esta tecnología.

En mayo de 1985, y tras cuatro años de estudios, el FCC (Federal Communications Commission), la agencia federal del Gobierno de Estados Unidos encargada de regular y administrar en materia de telecomunicaciones, asignó las bandas SMS (Industrial, Scientific and Medical) 902-928 MHz, 2,400-2,483 GHz, 5,725-5,850 GHz a las redes inalámbricas basadas en "spread-spectrum".

La asignación de una banda de frecuencias propició una mayor actividad en el seno de la industria, ese respaldo hizo que las WLAN empezaran a dejar ya el laboratorio para iniciar el camino hacia el mercado. Desde 1985 hasta 1990 se

siguió trabajando ya más en la fase de desarrollo, hasta que en mayo de 1991 se publicaron varios trabajos referentes a WLAN operativas que superaban la velocidad de 1 Mbps, el mínimo establecido por el IEEE 802 para que la red sea considerada realmente una LAN.

### 1.2.3 VENTAJAS Y DESVENTAJAS DE UNA RED INALÁMBRICA

Según el criterio de varios autores, coinciden en que las redes inalámbricas proporcionan las siguientes ventajas y desventajas:

**Tabla 5:** Ventajas y desventajas de una red inalámbrica.

VENTAJAS	DESVENTAJAS
<b>Movilidad.-</b> Pueden situarse en cualquier punto dentro del área de cobertura de la red	<b>Menor ancho de banda.-</b> Las redes de cable trabajan a 100 Mbps, las redes inalámbricas Wi-Fi lo hacen a 11 Mbps. Existen estándares que alcanzan los 54 Mbps y soluciones propietarias que llegan a 100 Mbps, muy costosas
<b>Simplicidad y rapidez en la instalación.-</b> Es rápida, fácil y elimina la necesidad de tirar cables a través de paredes y techos.	<b>Seguridad.-</b> Cualquier persona con una computadora portátil solo necesita estar dentro del área de cobertura de la red para poder intentar acceder a ella.
<b>Flexibilidad en la instalación.-</b> Permite colocar una computadora de sobremesa en cualquier lugar sin tener que hacer el más mínimo cambio de configuración de la red.	<b>Interferencias.-</b> Las redes inalámbricas funcionan utilizando el medio radio electrónico en la banda de 2,4 GHz, no requiere de licencia administrativa para ser utilizada por lo que muchos equipos del mercado, como teléfonos inalámbricos, microondas, etc., utilizan esta misma banda de frecuencias.
<b>Ahorro de costos.-</b> permite ahorrar costos al compartir recursos, acceso a internet, impresoras, etc. Los beneficios a largo plazo son superiores en ambientes dinámicos que requieren acciones y movimientos frecuentes	<b>Calidad de servicio.-</b> Velocidades que no superan los 10 Mbps, frente a los 100 de una red normal. La tasa de error es alta alrededor de 10 <sup>-4</sup> frente a la 10 <sup>-10</sup> de las redes cableadas, 1 bit erróneo por cada 10.000 bits o de cada Megabit transmitido, 1 KM será erróneo.
<b>Escalabilidad y robustez.-</b> Facilidad de expandir la red después de su instalación. Puede aguantar percances inesperados	<b>Soluciones propietarias.-</b> Sólo funcionan en un entorno homogéneo y por lo tanto estando atado a ese fabricante. Problemas en el mantenimiento para la recuperación ante posibles fallos, se debe acudir de nuevo al mismo fabricante para comprar otra tarjeta, punto de enlace, etc.
<b>Poca planificación y diseño.-</b> Sólo hay que tener en cuenta el ámbito de cobertura de la red. Receptores pequeños y pueden integrarse dentro de un dispositivo y llevarlo en un bolsillo.	<b>Restricciones.-</b> Operan en un espacio del espectro radioeléctrico, saturado hoy en día, las redes deben amoldarse a las reglas que existan dentro de cada país.

**Fuente:** Inv. Directa.

**Elaborado por:** Edwin Copara - Mayra Toapanta.

## 1.2.4 CLASIFICACIÓN DE LAS REDES INALÁMBRICAS

Las redes inalámbricas pueden clasificarse en 2 tipos:

- Redes inalámbricas personales
- Redes inalámbricas por consumo

### 1.2.4.1 REDES INALÁMBRICAS PERSONALES

Se permite que la comunicación sea por 2 medios: Infrarrojos y Bluetooth

**Redes por infrarrojos.-** Permiten la comunicación entre dos nodos, usando una serie de leds infrarrojos para ello. Se trata de emisores/receptores de las ondas infrarrojas entre ambos dispositivos, cada dispositivo necesita "ver" al otro para realizar la comunicación, por ello es escasa su utilización a gran escala. Estas redes son muy limitadas dado su corto alcance, necesidad de "visión sin obstáculos" entre los dispositivos que se comunican y su baja velocidad (hasta 115 kbps). Se encuentran principalmente en ordenadores portátiles, PDAs (Agendas electrónicas personales), teléfonos móviles y algunas impresoras.

**Bluetooth.-** Es una frecuencia de radio de disponibilidad universal que conecta entre sí los dispositivos habilitados para Bluetooth® situados a una distancia de hasta 10 metros. Estándar de comunicación entre pequeños dispositivos de uso personal, como pueden ser los PDAs, teléfonos móviles de nueva generación y alguno que otro ordenador portátil., cámaras, impresoras, teclados, altavoces e incluso un ratón de ordenador. Su principal desventaja es que su puesta en marcha se ha ido retrasando desde hace años y la aparición del mismo ha ido plagada de diferencias e incompatibilidades entre los dispositivos de comunicación de los distintos fabricantes, que ha imposibilitado su rápida adopción. Opera dentro de la banda de los 2.4 GHz. por lo que puede presentar interferencias con Wi-Fi, sin embargo, en la versión 1.2 y mayores del estándar Bluetooth se ha actualizado su

especificación para que no haya interferencias en la utilización simultánea de ambas tecnologías.

Permite conectar de forma rápida y sencilla los dispositivos habilitados para Bluetooth entre sí y de este modo crear una red de área personal (PAN) en la que es posible combinar todas las herramientas de trabajo principales con todas las prestaciones de la oficina. El uso de una red de igual a igual Bluetooth permite intercambiar archivos en reuniones improvisadas con suma facilidad y ahorrar tiempo imprimiendo documentos sin necesidad de conectarse a una red fija o inalámbrica. Por ejemplo, imagine que acaba de terminar una reunión en la oficina de un cliente y necesita imprimir el informe de estado para realizar una acción inmediata. Con Bluetooth, puede imprimir el informe desde el escritorio mediante cualquier impresora habilitada para Bluetooth dentro del radio, sin cables, sin problemas y sin moverse siquiera.

#### **1.2.4.2 REDES INALÁMBRICAS POR CONSUMO**

##### **Redes CDMA (Code División Múltiple Access)**

CDMA (Acceso múltiple por división de código), estándar de telefonía móvil estadounidense, por ejemplo, con las versiones nuevas puede dar servicios de valor agregado muy competitivos frente a la oferta de cobre.

Hasta hace poco con las tecnologías inalámbricas no se podía transmitir fax o navegar por Internet.

Hoy es rentable y cómodo enviar y recibir fax y con las nuevas versiones de CDMA se pueden transmitir paquetes de datos, videos, con velocidades de hasta 128 Kbps, de forma inalámbrica.



Toda la industria se está moviendo hacia integrar lo inalámbrico sobre protocolos de Internet, en donde la voz es sólo un servicio más, porque se digitaliza, transformándose en una corriente de datos que se integra a la red.

El futuro es emigrar hacia Internet. Hoy en día todavía las velocidades de transmisión no hacen factible viajar sobre protocolos de Internet. El CDMA instalado en Latinoamérica no permite más de 64 Kb, en los próximos doce meses los operadores probablemente comenzarán a instalar las versiones nuevas de CDMA.

Las redes inalámbricas de hoy son competitivas en costo; y en pocos años serán competitivas en ancho de banda. Todas las tecnologías importantes están migrando hacia alcanzar mayores velocidades de transmisión de datos para aplicaciones fijas y móviles. Fijas hasta 2 Mg por segundo y móviles hasta 386 Kb por segundo. Esto se va a lograr en algunos años.

### **Redes GSM (Global System for Mobile)**

Estándar de telefonía móvil europeo y asiático, son los estándares que usa la telefonía móvil empleados alrededor de todo el mundo en sus diferentes variantes.

### **1.2.5 TIPOS DE REDES INALÁMBRICAS**

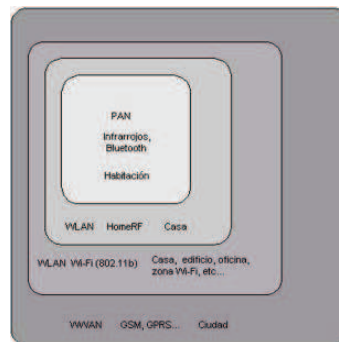
Para Wordpress (julio 2011), en la dirección electrónica <http://redesinalambricasfacci.wordpress.com/>, dice que: “Como se ha comentado anteriormente, conceptualmente la única diferencia existente entre las redes locales convencionales y las inalámbricas es la inexistencia en estas últimas de cableado entre los equipos. Por ello, para poner énfasis en esta característica, se presenta una clasificación de redes locales donde se añade la inicial W (del inglés, wireless, inalámbrico)”.

Para los investigadores, consideramos que en relación a los tipos de redes inalámbricas, se aplica lo mismo que las redes con cable, las redes inalámbricas se pueden clasificar en diferentes tipos, en función de las distancias a través de las que se pueden transmitir los datos.

Si clasificamos las redes por su alcance geográfico, tenemos tres tipos de redes inalámbricas:

- Wireless LAN (Local Área Network)
- Wireless PAN (Personal Área Network)
- Wireless WAN/MAN (Wide Area Network)

**Figura3:** Ámbito de uso de los tipos de redes inalámbricas



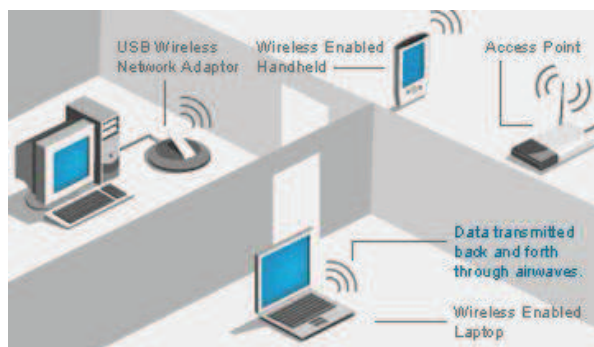
**Fuente:** <http://redesinalambricasfacci.files.wordpress.com/2011/07/1.jpg>

### **WLAN (Wireless Local Área Network - Red inalámbrica de ámbito local)**

Permiten conectar una red de computadores en una localidad geográfica, de manera inalámbrica para compartir archivos, servicios, impresoras, y otros recursos. Usualmente utilizan señales de radio, las cuales son captadas por PC-Cards o tarjetas PCMCIA conectadas a laptops o a slots PCI para PCMCIA de PCs de escritorio. Estas redes, soportan generalmente tasas de transmisión entre los 11 Mbps y 54Mbps (mega bits por segundo) y tienen un rango de entre 30 a 300 metros, con señales capaces de atravesar paredes.

Las WLAN pueden operar de dos formas distintas. En las WLAN de infraestructura, las estaciones inalámbricas (dispositivos con radiotarjetas de red o módems externos) se conectan a puntos de acceso inalámbrico que funcionan como puentes entre las estaciones y la red troncal existente. En las WLAN de igual a igual (ad hoc), varios usuarios dentro de un área limitada, como una sala de conferencias, pueden formar una red temporal sin utilizar puntos de acceso, si no necesitan obtener acceso a recursos de red.

**Figura 4: Red WLAN**

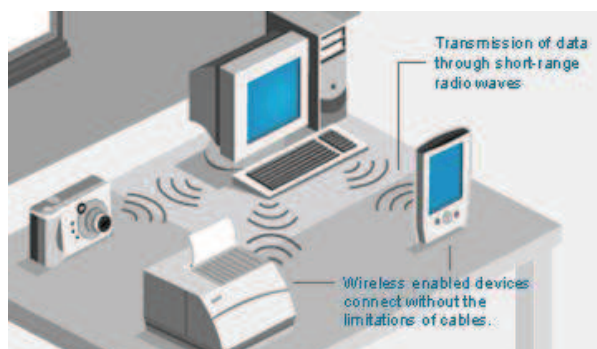


Fuente: [http://www.innetrex.com/wireless\\_install.php](http://www.innetrex.com/wireless_install.php)

### **WPAN (Wireless Personal Área Network - Red inalámbrica de ámbito personal)**

Tradicionalmente este tipo de redes se basan en infrarrojos, que permiten la comunicación inalámbrica ad hoc para dispositivos (ordenadores portátiles, PDAs, etc.) a baja velocidad y que se utilizan dentro de un espacio operativo personal (POS). Un POS es el espacio que rodea a una persona, hasta una distancia de 10 metros, que es relativamente cercano para comunicar y sincronizar información, hoy en día, como alternativa de comunicación está tomando auge el estándar Bluetooth, comúnmente utilizadas para interconectar dispositivos compatibles cerca de un lugar central, como un escritorio.

**Figura 5:** Red WPAN



**Fuente:** [http://www.innetrex.com/wireless\\_install.php](http://www.innetrex.com/wireless_install.php)

Bluetooth es una tecnología inalámbrica europea desarrollada por Ericsson que utiliza ondas de radio para transmitir datos a una distancia de hasta 30 pies. Los datos de Bluetooth se pueden transferir a través de paredes, bolsillos y maletines. El desarrollo de la tecnología de Bluetooth lo dirige el Grupo de interés general (SIG) de Bluetooth, que publicó la especificación de la versión 1.0 de Bluetooth en 1999. Otra posibilidad que tienen los usuarios para conectar dispositivos en un radio de acción muy cercano (1 metro o menos) es crear vínculos de infrarrojos.

Para normalizar el desarrollo de tecnologías WPAN, el IEEE ha establecido el grupo de trabajo 802.15 para las WPAN. Este grupo de trabajo está desarrollando una norma WPAN basada en la especificación de la versión 1,0 de Bluetooth. Los objetivos principales en esta norma preliminar son baja complejidad, bajo consumo de energía, interoperabilidad y coexistencia con redes de 802.11.

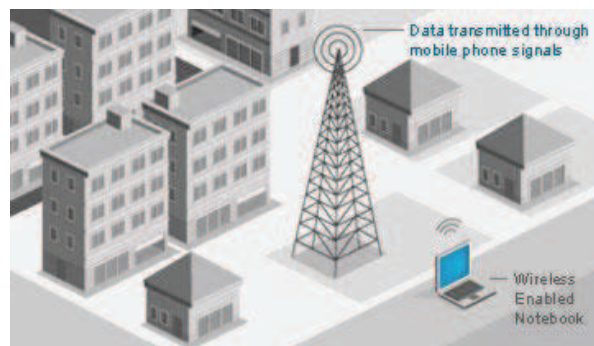
### **WWAN/MAN (Wireless Wide Área Network - Red inalámbrica de área extensa/metropolitana)**

Las tecnologías WWAN permiten a los usuarios establecer conexiones inalámbricas a través de redes remotas públicas o privadas. Estas conexiones pueden mantenerse a través de áreas geográficas extensas, como ciudades o países, mediante el uso de antenas de radio microondas en varias ubicaciones o

sistemas satélite que mantienen los proveedores de servicios inalámbricos. Estas redes son mucho más flexibles, económicas y fáciles de instalar.

Para que la comunicación satelital sea efectiva generalmente se necesita que los satélites permanezcan estacionarios con respecto a su posición sobre la tierra, si no es así, las estaciones en tierra los perderían de vista. Para mantenerse estacionario, el satélite debe tener un período de rotación igual que el de la tierra, y esto sucede cuando el satélite se encuentra a una altura de 35.784 Km.

**Figura 6:** Red WWAN



**Fuente:** [http://www.innetrex.com/wireless\\_install.php](http://www.innetrex.com/wireless_install.php)

Por su gran tamaño, estas redes son explotadas por las empresas de telefonía móvil. Las tecnologías WWAN actuales se conocen como sistemas de segunda generación (2G). Entre los sistemas 2G principales se incluyen Global System for Mobile Communications (GSM), Celular Digital Packet Data (CDPD) y Code División Múltiple Access (CDMA). Los esfuerzos van encaminados a la transición desde redes 2G. Algunas de las cuales tienen capacidades limitadas de movilidad y son incompatibles entre sí, a tecnologías de tercera generación (3G) que seguirían un estándar global y proporcionarían capacidades de movilidad internacional. Hasta la llegada de la telefonía móvil de tercera generación, el **UMTS**, la alternativa actual es el uso del **GPRS**, aunque su velocidad es bastante reducida.

## COMPARACIÓN TECNOLOGÍAS INALÁMBRICAS

A continuación se describe un cuadro de resumen de las tecnologías inalámbricas.

**Tabla 6:** Tecnologías inalámbricas

Tipo de red	WWAN (Wide)	WMAN (Metropolitan)	WLAN (Local)	WPAN (Personal)
Estándar	GSM/GPRS/ UMTS	IEEE 802.16	IEEE 802.11	IEEE 802.15
Certificación		WiMAX	WiFi	Bluetooth ZigBee
Velocidad	9.6/170/2000 Kb/s	15-134 Mb/s	1-2-11-54 Mb/s	721 Kb/s
Frecuencia	0.9/1.8/2.1 GHz	2-66 GHz	2.4 y 5 GHz Infrarrojos	
Rango	35 Km.	1.6 - 50 Km.	30 - 150 m.	10m.
Técnica radio	Varias	Varias	FHSS.DSSS. OFDM	FHSS
Itinerancia (roaming)	SI	SI (802.18e)	SI	NO
Equivalente a:	Conex. telef (modem)	ADSL.CATV	LAN	Cables de conexión

**Fuente:** [http://www.agenciaidea.es/c/document\\_library/get\\_file?uuid=9e84835b-e749-4b6c-a01d-f60d3399fae9&groupId=10157](http://www.agenciaidea.es/c/document_library/get_file?uuid=9e84835b-e749-4b6c-a01d-f60d3399fae9&groupId=10157) (pag. 19)

### 1.2.6 TOPOLOGÍAS DE REDES INALÁMBRICAS

Las redes LAN inalámbricas se construyen sobre la base de dos topologías básicas.

La topología de una red representa la disposición de los enlaces que conectan los nodos de una red.

Las redes pueden tomar muchas formas diferentes dependiendo de cómo están interconectados los nodos. Hay dos formas de describir la topología de una red: física o lógica.

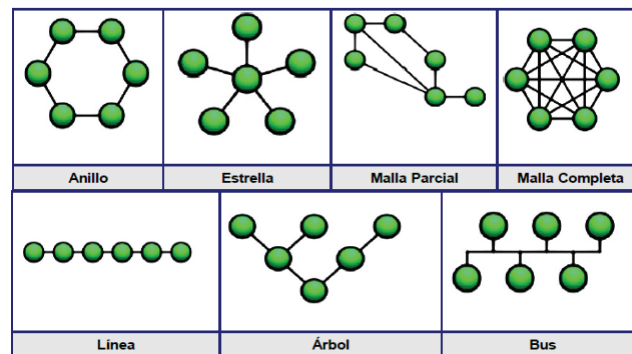
Para Sebastian Buettrich y Alberto Escudero Pascual es su obra: **“Topología e Infraestructura Básica de Redes Inalámbricas”**, hacen mención a que: “La topología física se refiere a la configuración de cables, antenas, computadores y otros dispositivos de red, mientras la topología lógica hace referencia a un nivel

más abstracto, considerando por ejemplo el método y flujo de la información transmitida entre nodos”

Los investigadores consideran acertada dicha tesis, pues es cierto que toda conexión, o interconexión se realiza de forma física y lógica, y así se realice una conexióna través de red inalámbrica, esto no implica que no existan ciertos componentes o dispositivos físicos de conexión y más aún una disposición lógica en el intercambio y priorización de la información generada o procesada.

A continuación se da una breve descripción de algunas topologías de red básicas:

**Figura 7:** Topologías de redes inalámbricas



Fuente: [www.wilac.net/tricalcar/](http://www.wilac.net/tricalcar/)

**Tabla 7:** Descripción Topologías básicas de una red

Topología	Descripción
<b>Bus o Barra</b>	Todos los nodos están conectados a un cable común o compartido. Las redes Ethernet normalmente usan esta topología.
<b>Estrella</b>	Cada nodo se conecta directamente a un concentrador central. En una topología de estrella todos los datos pasan a través del concentrador antes de alcanzar su destino. Esta es una topología común tanto en redes Ethernet como inalámbricas.
<b>Línea (o multi-concentrador)</b>	Un conjunto de nodos conectados en una línea. Cada nodo se conecta a sus dos nodos vecinos excepto el nodo final que tiene sólo un nodo vecino.
<b>Árbol</b>	Una combinación de las topologías de bus y estrella. Un conjunto de nodos configurados como estrella se conectan a una dorsal (backbone).
<b>Anillo</b>	Todos los nodos se conectan entre sí formando un lazo cerrado, de manera que cada nodo se conecta directamente a otros dos dispositivos. Típicamente la infraestructura es una dorsal (backbone) con fibra óptica.
<b>Malla completa</b>	Existe enlace directo entre todos los pares de nodos de la red. Una malla completa con n nodos requiere de $n(n-1)/2$ enlaces directos. Debido a esta característica, es una tecnología costosa pero muy confiable. Se usa principalmente para aplicaciones militares.
<b>Malla parcial</b>	Algunos nodos están organizados en una malla completa, mientras otros se conectan solamente a uno o dos nodos de la red. Esta topología es menos costosa que la malla completa pero por supuesto, no es tan confiable ya que el número de enlaces redundantes se reduce.

Fuente: [www.wilac.net/tricalcar/](http://www.wilac.net/tricalcar/)

## **TOPOLOGÍAS DE RED RELEVANTES EN CONEXIÓN DE REDES INALÁMBRICAS**

A continuación se hacen algunas observaciones generales que le ayudaran a entender cómo y por qué algunas topologías de red, pueden o no, ser aplicadas a redes inalámbricas. Estas observaciones pueden sonar triviales, pero su comprensión es fundamental para lograr la implementación de una red inalámbrica exitosa.

### **La comunicación inalámbrica no requiere un medio**

Obviamente la comunicación inalámbrica no requiere de cables pero tampoco necesita de algún otro medio, aire, éter u otra sustancia portadora. Una línea dibujada en el diagrama de una red inalámbrica, es equivalente a una (posible) conexión que se está realizando, no a un cable u otra representación física.

### **La comunicación inalámbrica siempre es en dos sentidos (bidireccional)**

No hay reglas sin excepción, en el caso de “sniffing” (monitoreo) completamente pasivo o eavesdropping (escucha subrepticia), la comunicación es no bidireccional. Esta bidireccionalidad existe bien sea que hablamos de transmisores o receptores, maestros o clientes.

### **Un radio es solo un radio y su rol posterior es determinado por el software**

Este software determina el comportamiento de las tarjetas de radio bajo las capas 1 y 2 del modelo OSI, por ejemplo en las capas física y de enlace. Teniendo en mente estas observaciones generales, podemos evaluar la relevancia de las topologías de red para redes inalámbricas.



**Figura 8:** Conexión de redes inalámbricas



Fuente: [www.wilac.net/tricalcar/](http://www.wilac.net/tricalcar/)

**Figura 9:** Enlaces inalámbricos

Topología	Representación visual	Relevancia en redes inalámbricas
Bus o Barra		No aplicable generalmente. Estudiando la topología de bus se puede notar que cada nodo se conecta a todos los demás nodos, en el punto donde un cable se conecta con otros cables. En el caso inalámbrico esta topología es equivalente a una red de malla completa operando en un canal único.
Estrella		Sí; esta es la topología estándar de una red inalámbrica.
Línea (multi-concentrador)		Sí; con dos o más elementos. Una línea de dos nodos es un enlace Punto a Punto.
Árbol		Sí; típicamente usado por ISP (Proveedores de servicio de Internet) inalámbricos.
Anillo		Sí; posible pero raro de encontrar.
Malla completa		Sí; pero la mayoría son mallas parciales.
Malla parcial		Sí.

Fuente: [www.wilac.net/tricalcar/](http://www.wilac.net/tricalcar/)

## TOPOLOGÍAS EN REDES INALÁMBRICAS

Podemos encontrar varios términos para estas topologías, los términos más usados son administrados y no administrados, alojadas y par a par, e infraestructura y "Ad Hoc". Estos términos están básicamente relacionados con las mismas distinciones básicas de topología. A continuación se va a describir las dos topologías o modos de funcionamiento de los dispositivos IEEE802.11: Infraestructura y "Ad Hoc".

### **Modo de infraestructura**

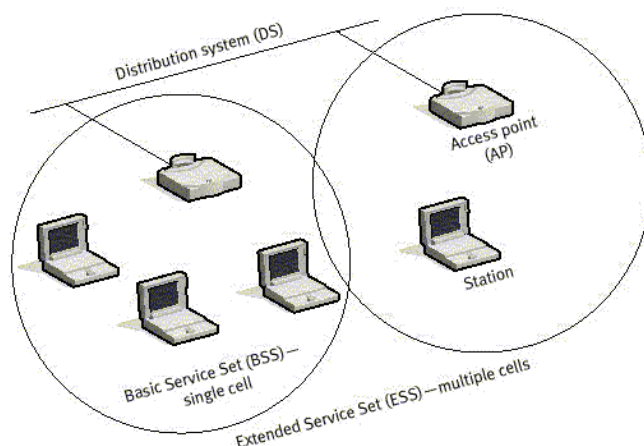
Se utiliza puntos de acceso (AP), estos dispositivos realizan una importante labor para el mantenimiento de la red simplificándolo en gran medida. Los puntos de acceso deberán proveer soporte de asociación y autenticación para que los dispositivos puedan conectarse con él permitir *roaming* para dispositivos procedentes de otros APs de la misma red. Además deberán aportar mecanismos de sincronización, control de energía y funciones de calidad de servicio.<sup>55</sup>

El punto de acceso (AP) da cobertura a toda una zona, esta zona se le conoce como BSS (Basic Service Set) o conjunto de servicios básicos, la cual se puede definir como el área geográfica en la cual una serie de dispositivos se interconectan entre sí por un medio aéreo.

Un sistema puede constar de una o varias células; en el caso pluricelular los diferentes AP se conectan entre sí mediante un *backbone* llamado DS (*Distribution System*), típicamente Ethernet, aunque en algunos casos también puede ser inalámbrico.

Además los APs podrían estar interconectados, o conectados a una red cableada, esto permite extender el alcance de la red, ya que donde no llegue el alcance de un AP llegará otro, para ello se hace necesario funciones de roaming entre celdas.

**Figura 10:** Esquema modo de infraestructura



**Fuente:** [http://88.12.10.114:8880/electron/franjagl/st/wireless/wifi\\_f.htm](http://88.12.10.114:8880/electron/franjagl/st/wireless/wifi_f.htm)

El punto de acceso coordina la transmisión y recepción de múltiples dispositivos inalámbricos dentro de una extensión específica; la extensión y el número de dispositivos dependen del estándar de conexión inalámbrica que se utilice y del producto. Si la zona es grande por lo general hay varios puntos de acceso lo que significa que hay varias estaciones base, en cambio sí la zona es pequeña como puede ser un hogar o un edificio con un solo punto de acceso bastaría.

Estando conectado a una red fija o una LAN, permitirá a los dispositivos móviles acceder a servicios de los LANs tradicionales, como intranets o recursos fijos.

Varios APs conectados forman un ESS o conjunto de servicios extendidos. Y la red que los conecta se le conoce como sistema de distribución. Este sistema de distribución podría estar montado sobre cualquier sistema, no siendo limitado a variantes de IEEE802.3.

### **Descripción de la modalidad Infraestructura.**

El dispositivo inteligente, denominado ESTACIÓN en el ámbito de las redes LAN inalámbricas, primero debe identificar los puntos de acceso y las redes disponibles. Este proceso se lleva a cabo mediante el control de las tramas de

señalización procedentes de los puntos de acceso que se anuncian a sí mismo o mediante el sondeo activo de una red específica con tramas de sondeo.

La estación elige una red entre las que están disponibles e inicia un proceso de autenticación con el punto de acceso. Una vez que el punto de acceso y la estación se han verificado mutuamente, comienza el proceso de asociación.

Esta asociación permite que el punto de acceso y la estación intercambien información y datos de capacidad. El punto de acceso puede utilizar esta información y compartirla con otros puntos de acceso de la red para distribuir la información de la ubicación actual de la estación en la red.

La estación sólo puede transmitir o recibir datos una vez terminada la asociación.

Esta modalidad obliga a que todo el tráfico que proceda de dispositivos inalámbricos pase por un punto de acceso antes de llegar a su destino en la red LAN con cable o inalámbrica.

El acceso a la red se administra mediante un protocolo que detecta las portadoras y evita las colisiones. Las estaciones tienen un período de tiempo en el cual sólo se limita a la escucha de las transmisiones, en esta parte del protocolo se detectan las portadoras.

Antes de transmitir, la estación debe esperar durante un periodo de tiempo específico después de que la red está despejada. Esta demora, junto con la transmisión por parte de la estación receptora de una confirmación de recepción correcta, representa la parte del protocolo que evita las colisiones.

En este tipo de modalidad (infraestructura) el emisor o el receptor es siempre el punto de acceso.

Es posible que algunas estaciones no se escuchen mutuamente, aunque ambas estén dentro del alcance del punto de acceso, se toman medidas especiales para

evitar las colisiones. Entre ellas, se incluye un intercambio de reserva, que puede tener lugar antes de transmitir un paquete, mediante un intercambio de tramas "petición para emitir" y "listo para emitir" y un vector de asignación de red que se mantiene en cada estación de la red. Aunque una estación no pueda oír la transmisión de la otra estación, oirá la transmisión de "listo para emitir" desde el punto de acceso y puede evitar transmitir durante ese intervalo.

El proceso de movilidad de un punto de acceso a otro no está completamente definido en el estándar. Sin embargo, la señalización y el sondeo que se utilizan para buscar puntos de acceso y un proceso de reasociación que permite a la estación asociarse a un punto de acceso diferente, junto con protocolos específicos de otros fabricantes entre puntos de acceso, proporciona una transición fluida.

La sincronización entre las estaciones de la red se controla mediante las tramas de señalización periódicas enviadas por el punto de acceso.

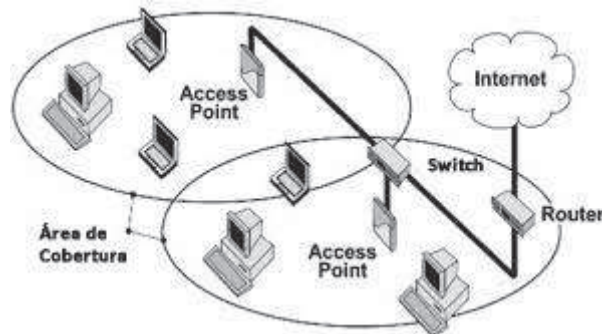
Estas tramas contienen el valor de reloj del punto de acceso en el momento de las transmisiones, por lo que sirve para comprobar la evolución en la estación receptora. La sincronización es necesaria por varias razones relacionadas con los protocolos y esquemas de modulación de las conexiones inalámbricas.

### **Descripción *Ad-Hoc*.**

Este modo utiliza mecanismos para crear redes "al vuelo", sin ningún tipo de infraestructura. Esto puede ser muy interesante de cara a redes de área personal, o para redes domésticas destinadas para usuarios con pocos conocimientos de comunicaciones. Este esquema en modo Ad-Hoc conocido también como Peer to Peer, consiste en un grupo de ordenadores que se comunican cada uno directamente con los otros a través de las señales de radio sin usar un punto de acceso y el alcance está dado por el alcance individual de cada máquina.

Los ordenadores de la red inalámbrica que quieren comunicarse entre ellos necesitan usar el mismo canal de radio y configurar un identificador específico de Wi-Fi denominado SSID (*Service Set Identifier*), en "Modo Ad Hoc".

**Figura 11:** Esquema modo de ad-hoc



**Fuente:** <http://www.monografias.com/trabajos90/modos-funcionamiento-redes-wifi/modos-funcionamiento-redes-wifi.shtml>

Esta topología es práctica en lugares en los que pueden reunirse pequeños grupos de equipos que no necesitan acceso a otra red. Ejemplos de entornos en los que podrían utilizarse redes inalámbricas ad hoc serían un domicilio sin red con cable o una sala de conferencias donde los equipos se reúnen con regularidad para intercambiar ideas.

### **Descripción general del funcionamiento de la modalidad Ad- Hoc.**

Este modo no tiene punto de acceso. Se puede decir que en este tipo de estructura sólo hay dispositivos inalámbricos presentes, las tareas de señalización y la sincronización son controladas por una estación.

La red ad-hoc tiene varios inconvenientes comparada con las redes infraestructura, uno de ellos es que este tipo de red no permite la posibilidad de transmitir tramas entre dos estaciones que no se oyen mutuamente.

## CAPITULO II

### 2.1 BREVE CARACTERIZACIÓN DEL OBJETO DE ESTUDIO

Las redes constituyen actualmente una de las principales tecnologías actualizadas más necesarias, refiere a un conjunto muy amplio de dispositivos tecnológicos electrónicos más utilizados, con características de interconexión inteligentes.

Dichas redes pueden desarrollarse en ámbitos locales (privadas), generalmente a través de conexión alámbricas, concentradores y enrutadores es decir pequeñas redes empresariales o personales, tenemos redes de área extendida, usadas por empresas en una extensión más amplia.

Una red inalámbrica LAN, es un sistema flexible de transmisión de datos implementados como una extensión, o como alternativa, de una red cableada. Utiliza tecnología de radio frecuencia, transmite y recibe datos utilizando como medio el aire, minimizando la necesidad de una conexión de cable, permitiendo la combinación conectividad y movilidad.

Una red de computadoras local inalámbrica es un sistema de comunicación de datos que utiliza tecnología de radiofrecuencia. En esta red se transmite y recibe datos sobre aire, minimizando la necesidad de conexiones alámbricas, es decir, combinan la conectividad de datos con la movilidad de usuarios.

La disponibilidad de la tecnología inalámbrica y de las redes (LAN) inalámbricas puede ampliar la libertad del usuario en red, resolver distintos problemas asociados con redes de cableado físico y en algunos casos, hasta reducir los costos de implementar redes. Sin embargo, junto con esta libertad, las redes inalámbricas conllevan también un nuevo conjunto de retos. Hoy en día, existen varias soluciones para redes inalámbricas disponibles con distintos niveles de

estandarización e interoperabilidad. Dos soluciones que actualmente son líderes en la industria son Home RF y Wi-Fi™ (IEEE 802.11b).

De estas dos, las tecnologías 802.11 cuentan con amplio apoyo en la industria y tienen la intención de resolver las necesidades empresariales del hogar y hasta de puntos de conexión públicos a redes inalámbricas. La alianza Wireless Ethernet Compatibility Alliance está trabajando para proporcionar la certificación de cumplimiento con los estándares 802.11, contribuyendo a garantizar la interoperabilidad entre las soluciones de los múltiples proveedores.

El amplio soporte de la industria para apoyar la interoperabilidad y el sistema operativo atienden algunos de los retos de implementación de las redes inalámbricas. Aun así, las redes inalámbricas presentan retos nuevos en cuanto a seguridad, roaming y configuración. El resto de este documento analiza estos retos y presenta algunas de las posibles soluciones, enfocándose en la forma en que Windows XP desempeñará un papel importante, proporcionando estas soluciones con soporte para cero configuraciones, seguridad 802.1x y otras innovaciones.

## **2.2 DISEÑO DE LA INVESTIGACIÓN**

### **2.2.1 Tipo de investigación**

Se ha considerado en la investigación realizada un tipo investigativo de orden descriptivo, cuasi experimental y post facto, en razón de las siguientes consideraciones:

Es de orden descriptivo ya que fue utilizada durante la recopilación bibliográfica en el desarrollo del Capítulo I, así como en la conceptualización de los elementos de red inalámbrica, y de igual forma en la identificación de los procesos de instalación y configuración del dispositivo inalámbrico Access Point Cisco WAP



321, el cual mantiene una configuración originaria de fábrica; dicha información fue tomada como base para el desarrollo de la guía de instalación y configuración básica, además del manual administrativo.

Es de carácter cuasi experimental ya que inicialmente el Access Point Cisco WAP 321 presenta una configuración inicial de fábrica, ésta fue empleada y adaptada en función de las necesidades y requerimientos del espacio físico y el área de cobertura. Dicha información obtenida permitió realizar una configuración a medida del dispositivo, además de elaborar una guía de instalación rápida adecuada y un manual administrativo funcional del Access Point Cisco WAP 321.

La investigación realizada es de tipo post facto ya que no manipulamos las variables de forma indiscriminada, sino que partimos de información previa ya existente adaptada al medio real de aplicación, es decir de conformidad a los requerimientos determinados y el espacio y radio de frecuencia del laboratorio de Redes de la Carrera de Informática y Sistemas Computacionales, los instigadores no influimos de ninguna forma en las variables y sus efectos ya que nos limitamos a la percepción de la configuración ya existente.

### **2.3 METODOLOGÍA.**

En la presente investigación los Tesistas aplicaron los siguientes métodos: científico, inductivo, analítico, sintético y estadístico.

Es científico ya que partimos de un problema real, mismo que fue resuelto a través de nuestra propuesta, generamos soluciones a la falta de interconexión de redes a través de dispositivos inalámbricos. Generamos premisas y conclusiones funcionales de aplicabilidad lo cual permitió desarrollar una guía adecuada de instalación y configuración básica y un manual administrativo del dispositivo ACCESS POINT CISCO WAP 321.

Aplicamos el método inductivo como base de recolección informativa de carácter empírica en el desarrollo del Capítulo I, ya que nos permitió obtener información generalizada a partir de principios básicos de manipulación del dispositivo seleccionada para la red inalámbrica y admitió generar el marco teórico adecuado de la investigación.

Se utilizó el método analítico al momento de valorar las respuestas obtenidas de los alumnos de Ingeniería en Sistemas en la encuesta aplicada, ya que dichas respuestas permitieron determinar los elementos esenciales de implementación y configuración acordes a sus necesidades académicas y laborales.

La investigación aplicó el método sintético para generar una propuesta adecuada, la cual se determinó en el desarrollo de una memoria técnica adecuada para una red inalámbrica a través de Access Point y tanto el análisis como la síntesis, permite determinar propuestas puntuales que se reflejan posteriormente en una norma general de configuración, misma que viene dada por la guía rápida de instalación y configuración, además del manual administrativo del dispositivo ACCEESS POINT CISCO WAP 321

Finalmente se aplicó el método estadístico para presentar los resultados obtenidos, de la investigación en cuadros estadísticos a través del análisis de frecuencias, mismos que son representados en diagramas o pasteles de fácil comprensión, los cuales permitirán determinar la necesidad de la propuesta y hacerla efectiva.

## **2.4 UNIDAD DE ESTUDIO**

La investigación realizada se centra en aspectos no discriminativos de las variables y sus efectos, en el análisis directo de elementos físicos y técnicos de conexión tomando como base directa las Redes de Información, desarrollando un estudio de factibilidad para su instalación, implementación, administración, mantenimiento y seguridad a través de dispositivos inalámbricos; de forma

prioritaria el estudio investigativo tratará sobre la conexión y configuración de una red inalámbrica a través de un Acces Point Cisco WAP 321 de un solo punto y el desarrollo de una guía de instalación y configuración al igual que un manual administrativo del dispositivo.

## **2.5 TÉCNICAS E INSTRUMENTOS**

**2.5.1 Percepción.-** Los investigadores palpamos a través de nuestros sentidos las características de funcionalidad del ACCESS POINT CISCO WAP 321, nos permitió generar premisas de manipulación, instalación y configuración multidisciplinaria en función de las necesidades académicas, de la disponibilidad física de espacio y del espectro radioeléctrico requerido.

Dicha técnica fue utilizada en el desarrollo de los Capítulos I y II, ya que fue necesario observar la realidad de nuestro medio y correlacionarlo con las existentes dentro de los avances tecnológicos en América Latina y el mundo; y, proponer alternativas de solución a la problemática existente.

**2.5.2 Encuesta.-** Fue aplicada a una población de 195 alumnos de la Carrera de Ciencias de la Ingeniería y Aplicadas, con la finalidad de obtener información relevante sobre la necesidad de dotar al laboratorio de Redes de dispositivos tecnológicos modernos, mismos que serán usados en los procesos de enseñanza aprendizaje de la materia.

**2.5.3. Cuestionario:** Se desarrolló un cuestionario constante de ocho preguntas cerradas las cuales permitieron obtener información acerca de la necesidad de dotar a la Carrera de Informática y Sistemas Computacionales de un punto de conexión que permita interconectar redes y dispositivos de forma inalámbrica; al mismo tiempo la necesidad imperiosa de que éstos sean utilizados como medios

didácticos de aprendizaje y como elementos de práctica permanente, para lo cual es necesario contar con una guía de instalación y un manual administrativo del ACCESS POINT CISCO WAP 321.

## 2.7 ANÁLISIS E INTERPRETACIÓN DE RESULTADOS DE LA INVESTIGACIÓN DE CAMPO

A continuación se presenta los resultados de las encuestas realizadas a los estudiantes de la Unidad Académica de Ciencias de la Ingeniería y Aplicadas, Carrera de Ingeniería en Informática y Sistemas Computacionales de la Universidad Técnica de Cotopaxi, con una muestra de ciento noventa y cinco personas (195), en relación a la **“IMPLEMENTACIÓN Y CONFIGURACIÓN DE UNA RED INALÁMBRICA A TRAVÉS DE ACCESS POINT PARA EL LABORATORIO DE REDES DE LA CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI”**

**Tabla 8.** Presentación de datos de la encuesta

OPCIÓN	FRECUENCIA		%	
	SI	NO	SI	NO
<b>Pregunta 1</b>	187	8	96%	4%
<b>Pregunta 2</b>	187	8	96%	4%
<b>Pregunta 3</b>	179	16	92%	8%
<b>Pregunta 4</b>	168	27	86%	14%
<b>Pregunta 5</b>	181	14	93%	7%
<b>Pregunta 6</b>	183	12	94%	6%
<b>Pregunta 7</b>	181	14	93%	7%
<b>Pregunta 8</b>	189	6	97%	3%

Fuente: Inv. Directa.

Elaborado por: Edwin Copara - Mayra Toapanta.

**PREGUNTA N° 1** ¿Está usted de acuerdo con que se implemente y configure un laboratorio de práctica de redes en la Carrera de Informática y Sistemas Computacionales de la Universidad Técnica de Cotopaxi a través de dispositivos tecnológicos modernos para el estudio práctico de la materia?

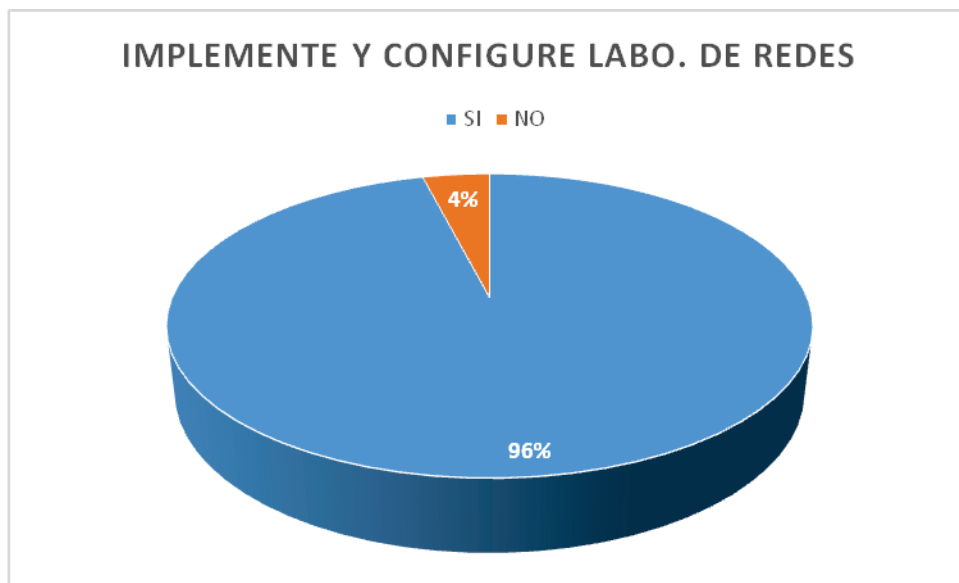
**Tabla 9:** Implementar y configurar Lab. Redes

OPCIONES	N°	%
SI	187	96
NO	8	4
TOTAL	195	100

Fuente: Inv. Directa.

Elaborado por: Edwin Copara - Mayra Toapanta.

**GRAFICO N° 01**



Fuente: Inv. Directa.

Elaborado por: Edwin Copara - Mayra Toapanta.

### **Análisis e interpretación**

De la información recolectada el 4% de la muestra opina no estar de acuerdo con la implementación de un laboratorio para la práctica de redes, mientras que un 96% considera necesario la implementar y configurar un laboratorio de redes a través de dispositivos tecnológicos modernos con el fin de llevar a cabo actividades educativas adecuadas.

**PREGUNTA N° 2** ¿El uso de dispositivos tecnológicos nuevos en el laboratorio de redes permitirá que el estudio de la informática y sistemas computacionales, amplíe y ponga en práctica los conocimientos teóricos adquiridos?

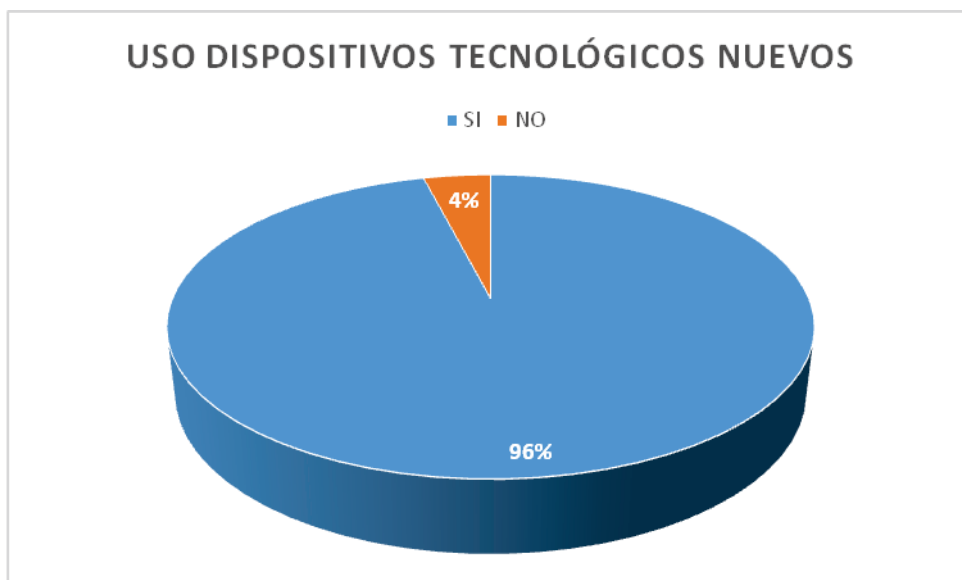
**Tabla 10:** Uso de dispositivos tecnológicos nuevos

OPCIONES	N°	%
SI	187	96
NO	8	4
TOTAL	195	100

Fuente: Inv. Directa.

Elaborado por: Edwin Copara - Mayra Toapanta.

**GRAFICO N° 02**



Fuente: Inv. Directa.

Elaborado por: Edwin Copara - Mayra Toapanta.

### **Análisis e interpretación**

A través del análisis de la colección de datos obtenidos 4% de la muestra considera que la implementación de dispositivos tecnológicos nuevos no contribuyen a la formación práctica del estudiantado, mientras que un 96% opina que la implementación de dispositivos tecnológicos modernos en el laboratorio de redes permitirá llevar a cabo actividades educativas prácticas de configuración de redes.

**PREGUNTA N° 3** ¿Los procesos de enseñanza aprendizaje son adquiridos de mejor forma a través de las prácticas de laboratorio bajo un ambiente real y de desempeños auténticos?

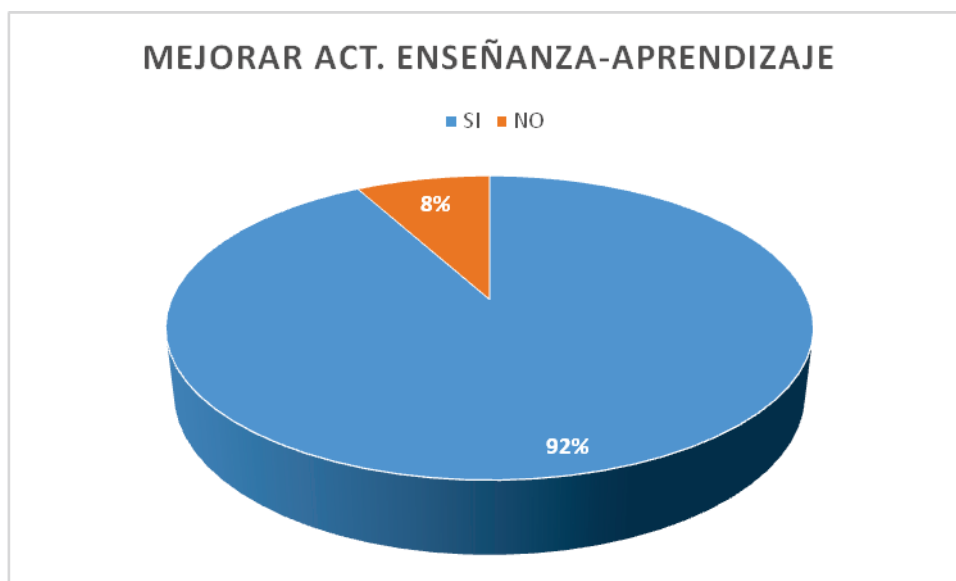
**Tabla 11:** Mejorar Act. Enseñanza-aprendizaje

OPCIONES	N°	%
SI	179	92
NO	16	8
TOTAL	195	100

Fuente: Inv. Directa.

Elaborado por: Edwin Copara - Mayra Toapanta.

**GRAFICO N° 03**



Fuente: Inv. Directa.

Elaborado por: Edwin Copara - Mayra Toapanta.

### **Análisis e interpretación**

Luego de revisar las frecuencias obtenidas se puede notar que el 92% de la muestra considera que las prácticas de laboratorio mejoran los procesos de enseñanza aprendizaje, mientras tan solo el 16% considera que los desempeños auténticos no mejorarían los procesos de aprendizaje.

**PREGUNTA N° 4** ¿El uso de tecnologías Wireless permitirá que los conocimientos adquiridos se desenvuelvan en ambientes reales acorde a los avances tecnológicos y su adaptación a la evolución informático?

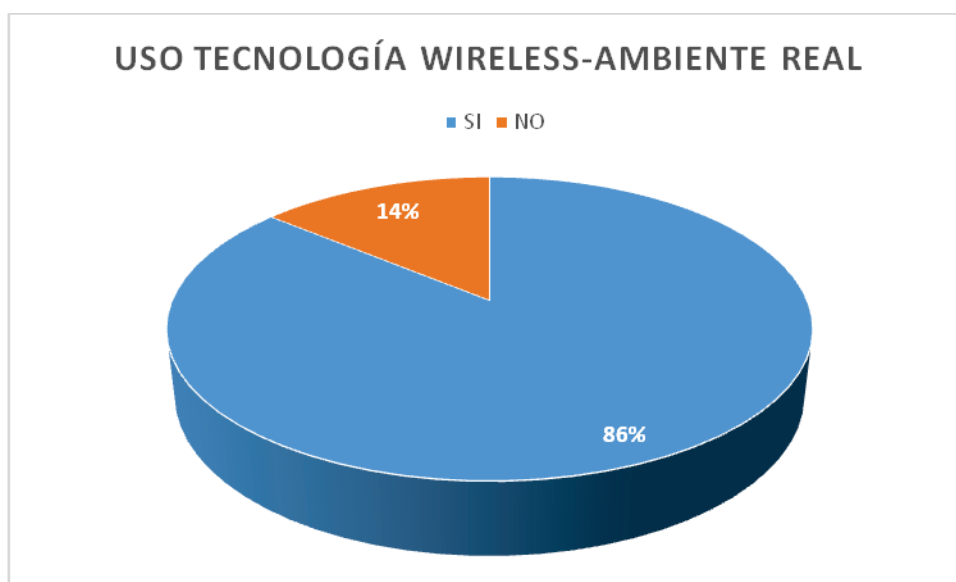
**Tabla 12:** Uso tecnología Wireless – ambiente real

OPCIONES	N°	%
SI	168	86
NO	27	14
TOTAL	195	100

Fuente: Inv. Directa.

Elaborado por: Edwin Copara - Mayra Toapanta.

**GRAFICO N° 04**



Fuente: Inv. Directa.

Elaborado por: Edwin Copara - Mayra Toapanta.

### **Análisis e interpretación**

De los datos obtenidos, se desprende que el 14% de los encuestados hacen mención a que el uso de nuevas tecnologías como los Wireless no mejorarían la calidad educativas y la simulación de ambientes reales; pero el 86% considera que el uso de Wireless en prácticas de laboratorio los involucra en procesos de aprendizaje actualizados y acorde a los avances actuales.



**PREGUNTA N° 5** ¿Está usted de acuerdo con que se implemente y configure una red inalámbrica a través de Access Point?

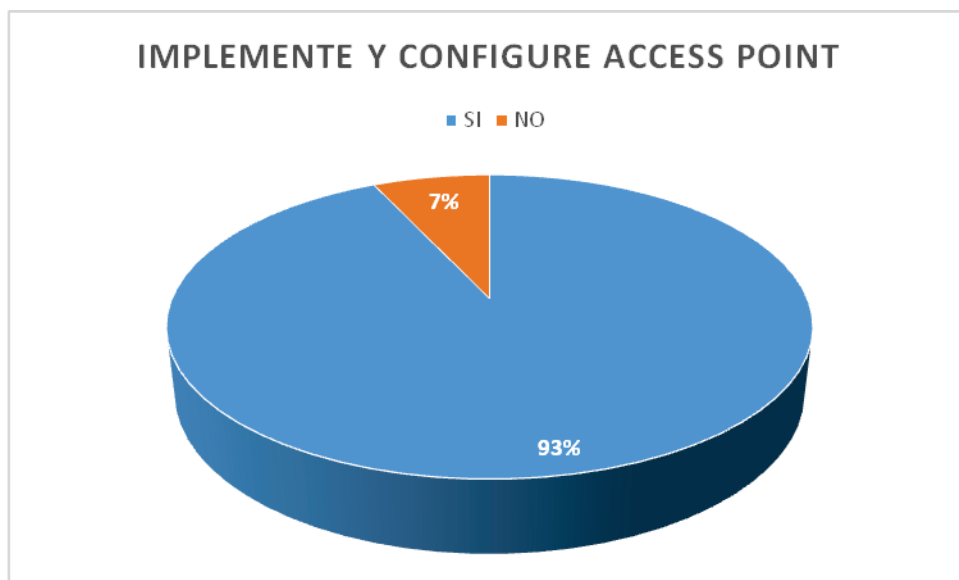
**Tabla 13:** Implemente y configure Access Point

OPCIONES	N°	%
SI	181	93
NO	14	7
TOTAL	195	100

Fuente: Inv. Directa.

Elaborado por: Edwin Copara - Mayra Toapanta.

**GRAFICO N° 05**



Fuente: Inv. Directa.

Elaborado por: Edwin Copara - Mayra Toapanta.

### **Análisis e interpretación**

De los datos obtenidos, se observa que el 93% del total de encuestados piensa que se debe configurar una red inalámbrica a través de Access Point, mientras que tan solo un 7% no considera que sea necesario configurar una red inalámbrica por intermedio de un Access Point.

**PREGUNTA N° 6** ¿Es necesario contar con una memoria técnica y/o guía de instalación y configuración de un **ACCESS POINT CISCO WAP321** (configuración de un solo punto)?

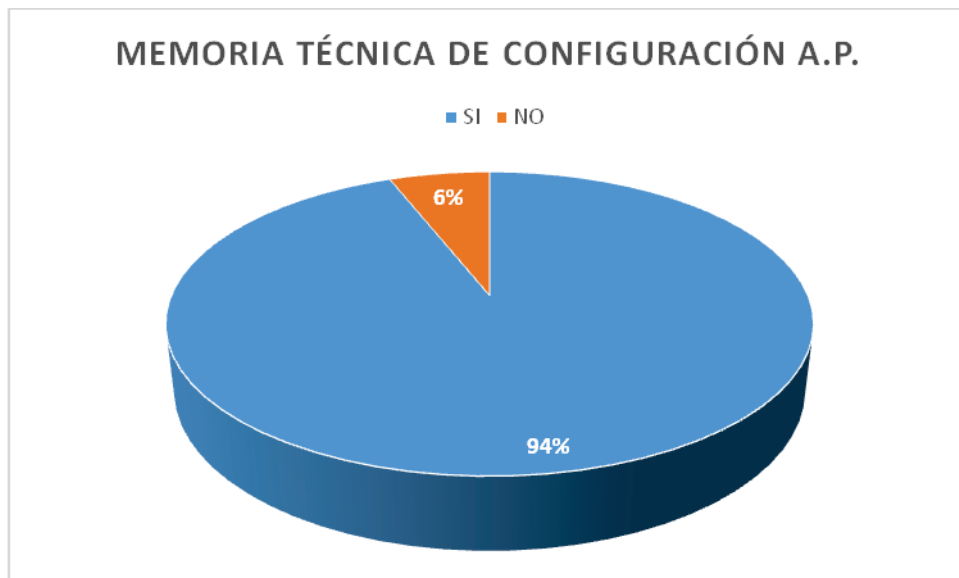
**Tabla 14:** Memoria técnica de Configuración AP

OPCIONES	N°	%
SI	183	94
NO	12	6
TOTAL	195	100

Fuente: Inv. Directa.

Elaborado por: Edwin Copara - Mayra Toapanta.

**GRAFICO N° 06**



Fuente: Inv. Directa.

Elaborado por: Edwin Copara - Mayra Toapanta.

### **Análisis e interpretación**

El 94% de la muestra considera primordial contar con una memoria técnica de configuración de un solo punto de un Access Point; únicamente el 6% de los encuestados piensa que no es necesario ningún manual de configuración para el funcionamiento de un Access Point.

**PREGUNTA N° 7** ¿La implementación y configuración de una red inalámbrica a través de Access Point permitirá interconectar las redes y asegurar el enrutamiento de los paquetes de información entre redes?

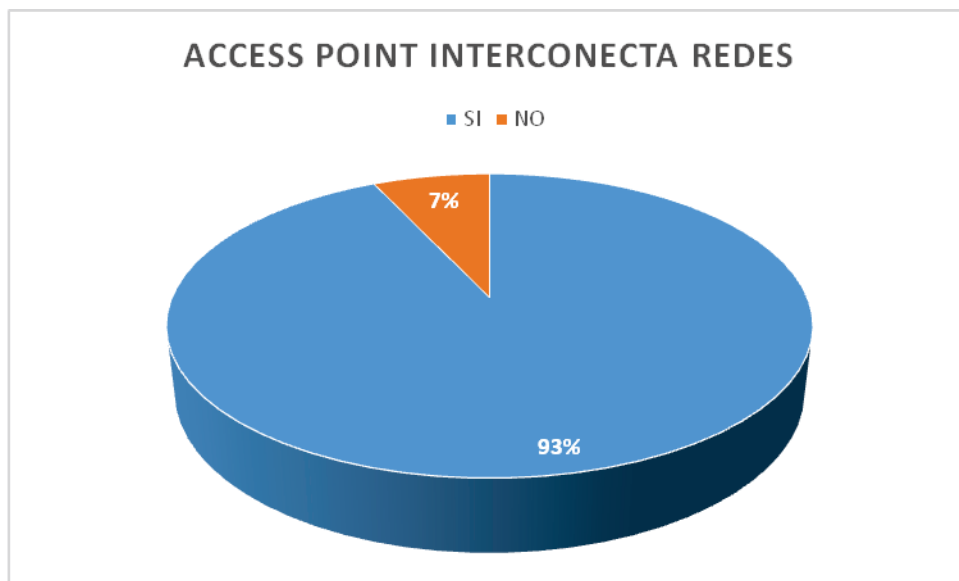
**Tabla 15:** Access Point interconecta redes.

OPCIONES	N°	%
SI	181	93
NO	14	7
TOTAL	195	100

Fuente: Inv. Directa.

Elaborado por: Edwin Copara - Mayra Toapanta.

**GRAFICO N° 07**



Fuente: Inv. Directa.

Elaborado por: Edwin Copara - Mayra Toapanta.

### **Análisis e interpretación**

Luego de revisar las frecuencias obtenidas se puede notar que el 93% de los encuestados se pronuncian en relación a que una red inalámbrica a través de Access Point permitirá interconectar varias redes, mientras que tan solo un 7% considera que no permitirá una interconexión entre redes.

**PREGUNTA N° 8** ¿Considera usted que la implementación y configuración de una red inalámbrica para los procesos prácticos de enseñanza aprendizaje, mejoraría el nivel académico de los estudiantes de Ingeniería en Informática y sistemas Computacionales?

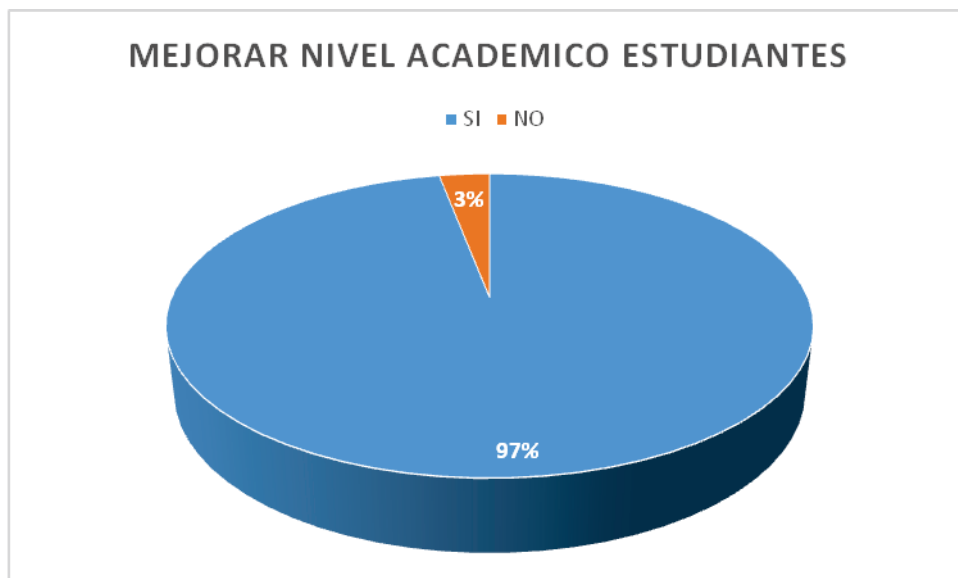
**Tabla 16:** Mejorar nivel académico estudiantes

OPCIONES	N°	%
SI	189	97
NO	6	3
TOTAL	195	100

Fuente: Inv. Directa.

Elaborado por: Edwin Copara - Mayra Toapanta.

**GRAFICO N° 08**



Fuente: Inv. Directa.

Elaborado por: Edwin Copara - Mayra Toapanta.

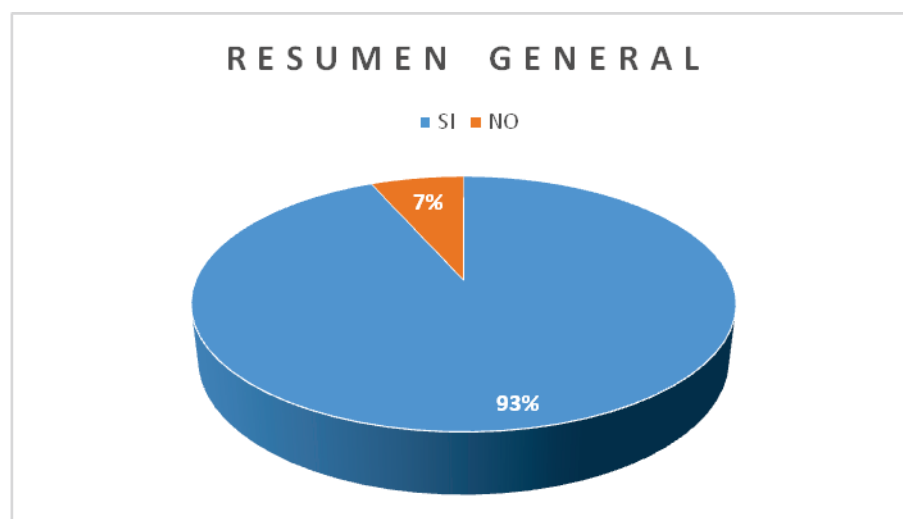
### **Análisis e interpretación**

A través de la investigación de campo realizada se observa que el 97% de las personas sondeadas reflexionan que la implementación y configuración de una red inalámbrica para los procesos prácticos de enseñanza-aprendizaje permitirá mejorar el nivel académico estudiantil y exclusivamente solo un 3% especula en razón de que no mejoraría su rendimiento académico.

Al realizar un análisis completo sobre la investigación de campo efectuada en relación a la propuesta sobre la **“IMPLEMENTACIÓN Y CONFIGURACIÓN DE UNA RED INALÁMBRICA A TRAVÉS DE ACCESS POINT PARA EL LABORATORIO DE REDES DE LA CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI”**, podemos indicar que el 93% de los encuestados, es decir 182 personas nos dan el sustento necesario para hablar con firmeza y determinación *que la aplicación práctica de conocimientos en un laboratorio de redes, mejoraría notablemente los procesos de enseñanza aprendizaje y desarrollaría en el estudiante un conjunto de habilidades, destrezas y competencias profesionales necesarias e indispensables en el mundo laboral actual*, de tal manera que hacemos efectiva nuestra propuesta de implementar y configurar una red inalámbrica a través de Access Point CISCO WAP 321 y la elaboración de una Guía de Configuración del dispositivo.

De esta manera tener la certeza que la propuesta que presentamos tendrá la aceptación requerida, para esto daremos a conocer el sustento legal, social y educativo.

**GRAFICO N° 09**



Fuente: Inv. Directa.

Elaborado por: Edwin Copara - Mayra Toapanta.

## CAPÍTULO III

### 3. MARCO PROPOSITIVO

#### 3.1 Documento Crítico

Las redes inalámbricas actualmente tienen un avance vertiginoso en los procesos de comunicación. La aplicación práctica de los conocimientos teóricos adquiridos, constituye el cimiento de un adecuado desarrollo profesional.

Llevar a cabo prácticas en un ambiente real acorde a los nuevos y actuales avances tecnológicos constituye una formación educativa de calidad. El uso de redes inalámbricas es constante y permanente; conocer de forma práctica su configuración, constituye un elemento esencial en los procesos de intercambio de información. Dentro del mercado existe una gran variedad de dispositivos tecnológicos que permite lograr este fin, sus costos son accesibles y sus beneficios incomparables. Las actuales normas de educación de calidad requiere de principios y parámetros de aprendizaje más sofisticados y que garanticen un conocimiento pleno y bajo medidas de criticidad y desempeños auténticos.

La Universidad Técnica de Cotopaxi, Alma Mater de la Provincia, es una institución que oferta la Carrera de Informática y Sistemas Computacionales, esta carrera forma parte de la Unidad Académica de Ciencias de la Ingeniería y Aplicadas, por ende del desarrollo técnico y tecnológico del país. La LOES a través de la Secretaria Nacional de Educación Superior, Ciencia Tecnología e Innovación (SENESCYT), actual institución reguladora de la calidad educativa de las Universidades buscan el mejoramiento continuo de los procesos educativos, de tal forma es prioritario contar con laboratorios de práctica en las diferentes asignaturas que forman parte de la malla curricular, de ahí la necesidad de implementar un laboratorio de redes conforme a los avances tecnológicos actuales, por tal razón proponemos implementar y configurar una red inalámbrica

a través de un Access Point CISCO WAP 321 de un solo punto para el laboratorio de redes de la Carrera de Sistemas y contribuir de esta manera con el desarrollo académico estudiantil y el mejoramiento institucional.

Es necesario que los estudiantes de informática y sistemas computacionales cuenten con espacios adecuados para la práctica de los conocimientos adquiridos. Siempre se debe llevar de la mano los conocimientos teóricos con los prácticos ya que de esta forma se estaría formando profesionales de calidad y capacitados para afrontar los retos actuales e involucrarse activamente en los procesos de desarrollo del país.

La aplicación de redes inalámbricas de comunicación es un aspecto cotidiano, va creciendo a la par de la sociedad y ésta no puede quedarse al margen de su evolución; una adecuada configuración de elementos de conexión brindará la posibilidad de incorporarse a los nuevos modelos tecnológicos de dispositivos y permitirá capacitar adecuadamente al estudiante informático en los procesos de uso y configuración de dispositivos de conexión. El uso de un laboratorio de redes adecuado a los procesos prácticos de aprendizaje tendrá una utilidad permanente y funcional y dotará al estudiante de los elementos necesarios en su formación profesional y futura inserción laboral.

La adecuación física y lógica de una red inalámbrica a través de Access Point beneficia directamente a los estudiantes de informática y sistemas computacionales, en la cimentación de sus conocimientos teórico-prácticos y brindará la posibilidad de llevar a cabo procesos de investigación y experimentación práctica de los modelos de comunicación y configuración de redes inalámbricas. Se requiere de la participación activa de los beneficiarios (comunidad universitaria), ya que ellos son los llamados a conocer de los procedimientos de transformación y mejoramiento de los procesos educativos a través de la implementación y configuración de redes a través de Access Point.

## **3.2. DISEÑO DE LA PROPUESTA**

### **3.2.1 Fundamentación**

La propuesta se fundamentó en los resultados de la investigación; así como también en las disposiciones legales y constitucionales expuestas en la Constitución de la República y la Ley Orgánica de Educación Superior.

La implementación y configuración de una red inalámbrica a través de un Access Point CISCO WAP 321 de un solo punto, se efectuó en razón de los actuales avances tecnológicos y la necesidad de la universidad de contar con un laboratorio de práctica de redes bajo la premisa constitucional de lograr una educación de calidad con calidez.

Los Docentes y Autoridades universitarias, tienen la facultad y la obligación de ir formando su criterio acerca de la necesidad de fortalecer los procesos de enseñanza-aprendizaje a través del uso de laboratorios equipados con los actuales avances tecnológicos, desde el instante que entra en contacto y tiene un acercamiento con dicho medio, para al final confrontar todos los conocimientos técnico-teóricos receptados, previo una valoración de eficiencia y eficacia de las mismas, lo que constituye una plena depuración de ellas de conformidad a los principios constitucionales de educación de calidad y calidez, para luego tomar una decisión que garantice su efectividad; es decir hablamos de una verdadera educación y formación profesional para que sean y puedan ser incorporados al mundo laboral con bases y conocimientos de las tecnologías actuales.

Para desarrollo de ésta investigación se ordenó y compendió la información obtenida en el medio nacional e internacional, analizando los avances tecnológicos y necesidades actuales, los cuales son sumamente necesarios en la formación profesional del Ingeniero en Informática y Sistemas Computacionales, por lo que consideramos que nuestra propuesta es de gran interés en el proceso académico y de formación profesional.



### **3.2.2 Justificación**

La implementación del proyecto expuesto anteriormente en el presente documento, tuvo como fin implementar y configurar una Red Inalámbrica a través de un Access Point CISCO WAP 321 de un solo punto para el laboratorio de redes la Unidad Académica CIYA de la Universidad Técnica de Cotopaxi, cuyo objetivo fundamental fue promover y fortalecer los conocimientos teórico-prácticos adquiridos bajo un ambiente de simulación real y desempeños auténticos, al mismo tiempo la vinculación universidad - empresa en todos sus ejes de acción, desde fomentar el desarrollo de proyectos de investigación formativa y generativa de carácter multi e inter-disciplinarios, lo cual permitirá llegar al mundo laboral de una forma más capacitada y profesional, optimizando los recursos bajo una premisa de cooperación, innovación y emprendimiento.

Es necesario que los profesionales en Informática y Sistemas Computacionales cumplan un currículo y perfil profesional acorde a las nuevas tecnologías y avances actuales, en donde se prime el conocimiento práctico respecto al uso, implementación y configuración de dispositivos de conexión de redes inalámbricas como el Access Point CISCO WAP321 de un solo punto, puesto que los conocimientos teóricos deben guardar concordancia con la práctica con la finalidad de generar un conocimiento más eficiente y eficaz, lo que permita un mejor desempeño profesional y una adecuada inserción laboral.

Es de interés general que se garantice el uso y manipulación de medios tecnológicos para el proceso de enseñanza-aprendizaje, ya que esto logrará una ampliación de conocimientos bajo un ambiente de simulación real y de desempeños auténticos, así como los de evitar que en el campo laboral se vulneren accesos no autorizados por personas ajenas al entorno laboral por el desconocimiento sobre la implementación y configuración de dispositivos de conexión inalámbrica como el Access Point.

La propuesta beneficiará a todos quienes forman parte de la Unidad Académica CIYA y de forma especial a los docentes y alumnos de la Carrera de Informática y Sistemas Computacionales ya que dentro de su futuro laboral es imperioso el conocimiento de implementar y configurar una conexión inalámbrica a través de Access Point, ya que son elementos de uso permanente en la actualidad tanto a nivel personal como empresarial.

De las averiguaciones efectuadas por los tesisistas la actual Ley Orgánica de Educación Superior y la Constitución de la República buscan que la educación superior sea de calidad y calidez, bajo las directrices interpuestas en el proyecto de desarrollo nacional y del buen vivir, lo cual hace que la propuesta investigativa y de aplicación sea muy necesaria en la Universidad Técnica de Cotopaxi, ya que permitirá que la institución cuente con espacios de práctica profesional tan necesarios en las instituciones de educación superior y de forma especial en el alma Mater de Cotopaxi.

Por lo que la propuesta se enviste de mucha originalidad, como un aporte social y de fortalecimiento institucional dada la importancia de adecuar el actual equipamiento institucional al avance tecnológico vigente a nuestra realidad.

Es factible la presentación de esta propuesta porque se cuenta con los respaldos de la investigación, las conclusiones y recomendaciones; así como también con los aportes técnicos y tecnológicos, a la vez que se efectuará la enunciación de una guía adecuada de instalación rápida.

### **3.3 OBJETIVO**

- Dotar de una red inalámbrica y una guía de instalación y configuración del Access Point Cisco WAP 321, como herramienta de investigación y práctica educativa en la Unidad Académica CIYA de la Universidad Técnica de Cotopaxi en el año 2014, para mejorar los procesos de enseñanza aprendizaje bajo un ambiente de simulación real y desempeños auténticos.

### **3.4. DESARROLLO DE LA PROPUESTA**

#### **3.4.1. Exposición de Motivos**

##### **3.4.1.1 DISPOSITIVOS WLAN**

### **COMPONENTES DE REDES INALÁMBRICAS**

#### **PUNTO DE ACCESO**

Un punto de acceso es un “concentrador” inalámbrico. El transmisor/receptor conecta entre sí los nodos de la red inalámbrica y normalmente también sirve de puente entre ellos y la red cableada. Un conjunto de puntos de acceso (coordinados) se pueden conectar unos con otros para crear una gran red inalámbrica.

Desde el punto de vista de los clientes inalámbricos (como las computadoras portátiles o las estaciones móviles), un punto de acceso provee un cable virtual entre los clientes asociados. Este “cable inalámbrico” conecta tanto a los clientes entre sí, como los clientes con la red cableada.

**Figura 12:** Access Point WAP Cisco 321



**Fuente:** Guía Cisco WAP 321

Un punto de acceso debe distinguirse de un enrutador inalámbrico, que es muy común en el mercado actual.

Un enrutador inalámbrico es una combinación entre un punto de acceso y un enrutador, y puede ejecutar tareas más complejas que las de un punto de acceso. Considere un enrutador inalámbrico como un puente (entre la red inalámbrica y la red Ethernet) y un enrutador (con características de enrutamiento IP).

En una red inalámbrica se pueden encontrar trabajando juntos dispositivos inalámbricos como puntos de acceso, enrutadores y puentes.

Los enrutadores y los puentes se pueden encargar de interconectar dos redes (por ejemplo Internet y su red local, o dos redes locales). Los enrutadores a diferencia de los puentes pueden hacer más eficiente el transporte de paquetes entre las redes debido al uso de tablas de enrutamiento que permiten determinar la mejor ruta que puede seguir un paquete de datos para llegar a su destino, además un enrutador inalámbrico se encargara de realizar la traducción de direcciones de red (NAT) o enmascaramiento.

Los puntos de acceso podrán captar las señales de los enrutadores y clientes, amplificándolas para dar una mayor cobertura a la red. A pesar de que los puntos

de acceso son “transparentes” para los otros dispositivos de la red, siempre se les debe asignar una dirección IP que permita su configuración.

Esto aplica a todos los dispositivos de la red, los cuales para ser gestionados requieren tener asignada una dirección IP.

## **ENMASCARAMIENTO**

El enmascaramiento o NAT (Network address traduction) permite comunicar computadores de una red interna, que no tienen una dirección conocida, a una red externa como Internet. Los paquetes que provienen de un equipo de la red interna, que tiene un rango de direcciones privadas en la red local, son pasados a un enrutador que modifica la información de la dirección IP y el número de puerto de los datagramas para que parezca que fueron generados por el mismo, enviándolos a Internet con una dirección IP conocida. Al recibir una respuesta del host remoto, el enrutador devuelve la modificación realizada al paquete, para que llegue correctamente a su destino dentro de la red interna.

El enmascaramiento es una práctica común para redes que usan IPv4, pero con IPv6 ya no será necesario.

## **PUENTEAR VS. ENRUTAR**

Un *puente* es un dispositivo que permite interconectar diferentes redes, independientemente del protocolo que cada una utilice. Esto ocurre debido a que un puente trabaja en los niveles 1 y 2 del modelo OSI (físico y datos respectivamente), utilizando la dirección MAC1 de los dispositivos, para definir la red de donde proviene y hacia dónde se dirige un paquete de datos.

Un *enrutador* permite también interconectar varias redes, pero a diferencia de un puente, estas deben utilizar el mismo protocolo. Un enrutador trabaja en las 3 primeras capas del modelo OSI y utiliza las direcciones de red de los equipos que toma de la capa 3 (de red), las cuales corresponden a un protocolo específico.

Si se desea interconectar dos redes que utilizan el mismo protocolo (p.e. IP) es recomendable utilizar un *enrutador* ya que este tiene la capacidad de optimizar las rutas recorridas por los paquetes para llegar a su destino utilizando tablas de enrutamiento que se actualizan constantemente aumentando su eficiencia.

Se recomienda el uso de *puentes* cuando no es posible crear subredes IP o cuando el protocolo de su red no permite enrutamiento (**NetBIOS, o DECnet**).

Un puente es más fácil de configurar pero puede afectar el rendimiento de su red.

Los clientes se conectan a un punto de acceso mediante su nombre. Este mecanismo de identificación se conoce como SSID-Service Set Identifier (Identificador del Conjunto de Servicio) y debe ser el mismo para todos los miembros de una red inalámbrica específica. Todos los punto de acceso y clientes que pertenecen a un mismo ESS -Extended Service Set- (Conjunto de Servicio extendido) se deben configurar con el mismo ID (ESSID).

Cuando hablamos de SSID pensamos en la etiqueta de un punto (socket) de Ethernet. Conectarse a una red inalámbrica con SSID “x” es equivalente a conectar su computador a un punto de red sobre una pared identificado con la etiqueta “x”. Para más detalles mire la unidad “Configuración de puntos de acceso”.

### **3.4.1.2 MODOS DE OPERACIÓN INALÁMBRICA**

#### **CLIENTES INALÁMBRICOS**

Un cliente inalámbrico es cualquier estación inalámbrica que se conecta a una red de área local (LAN–Local Área Network) inalámbrica para compartir sus recursos. Una estación inalámbrica se define como cualquier computador con una tarjeta adaptadora de red inalámbrica instalada que transmite y recibe señales de Radio Frecuencia (RF).

Algunos de los clientes inalámbricos más comunes son las computadoras portátiles, PDAs, equipos de vigilancia y teléfonos inalámbricos de VoIP.

#### **MODOS DE OPERACIÓN DE REDES INALÁMBRICAS**

El conjunto de estándares 802.11 definen dos modos fundamentales para redes inalámbricas:

1. Ad hoc
2. Infraestructura

Es importante comprender que no siempre, los modos se ven reflejados directamente en la topología.

Por ejemplo, un enlace punto a punto puede ser implementado en modo *ad hoc* o Infraestructura y nos podríamos imaginar una red en estrella construida por conexiones *ad hoc*. El modo puede ser visto como la configuración individual de la tarjeta inalámbrica de un nodo, más que como una característica de toda una infraestructura.

## MODO AD HOC (IBSS)

El modo ad hoc, también conocido como punto a punto, es un método para que los clientes inalámbricos puedan establecer una comunicación directa entre sí. Al permitir que los clientes inalámbricos operen en modo ad hoc, no es necesario involucrar un punto de acceso central. Todos los nodos de una red ad hoc se pueden comunicar directamente con otros clientes.

Cada cliente inalámbrico en una red *ad hoc* debería configurar su adaptador inalámbrico en modo *ad hoc* y usar los mismos SSID y “numero de canal” de la red.

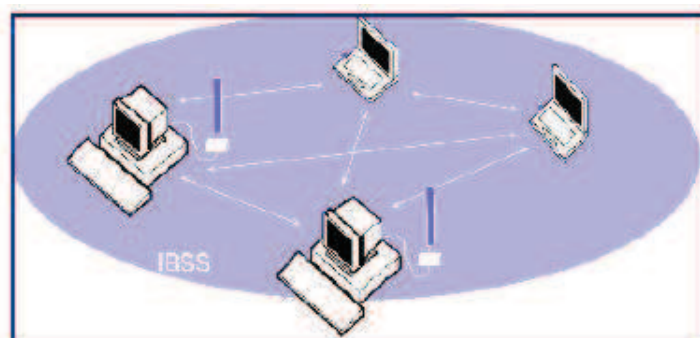
Una red *ad hoc* normalmente está conformada por un pequeño grupo de dispositivos dispuestos cerca unos de otros. En una red *ad hoc* el rendimiento es menor a medida que el número de nodos crece.

Para conectar una red *ad hoc* a una red de área local (LAN) cableada o a Internet, se requiere instalar una Pasarela o *Gateway* especial.

El termino latino *ad hoc* significa “para esto” pero se usa comúnmente para describir eventos o situaciones improvisadas y a menudo espontaneas.

En redes IEEE 802.11 el modo *ad hoc* se denota como Conjunto de Servicios Básicos Independientes (IBSS -Independent Basic Service Set).

**Figura 13:** Conjunto de servicios básicos independientes



**Fuente:** [www.wilac.net/tricalcar/](http://www.wilac.net/tricalcar/)



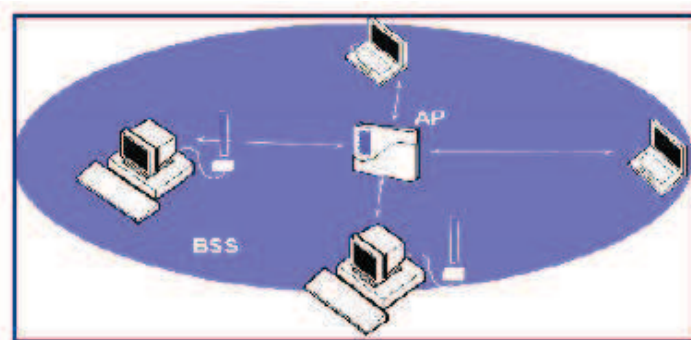
## INFRAESTRUCTURA (BSS)

Contrario al modo *ad hoc* donde no hay un elemento central, en el modo de infraestructura hay un elemento de “coordinación”: un punto de acceso o estación base. Si el punto de acceso se conecta a una red Ethernet cableada, los clientes inalámbricos pueden acceder a la red fija a través del punto de acceso. Para interconectar muchos puntos de acceso y clientes inalámbricos, todos deben configurarse con el mismo SSID. Para asegurar que se maximice la capacidad total de la red, no configure el mismo canal en todos los puntos de acceso que se encuentran en la misma área física.

Los clientes descubrirán (a través del escaneo de la red) cual canal esta usando el punto de acceso de manera que no se requiere que ellos conozcan de antemano el número de canal.

En redes IEEE 802.11 el modo de infraestructura es conocido como Conjunto de Servicios Básicos (BSS – Basic Service Set). También se conoce como Maestro y Cliente.

**Figura 14:** Conjunto de servicios básicos



**Fuente:** [www.wilac.net/tricalcar/](http://www.wilac.net/tricalcar/)

### **3.4.1.3 SEGURIDAD PARA LAS REDES INALÁMBRICAS**

Desde sus comienzos, 802.11 ha proporcionado algunos mecanismos de seguridad básicos para impedir que esta libertad mejorada sea una posible amenaza. Por ejemplo, los puntos de acceso (o conjuntos de puntos de acceso) 802.11 se pueden configurar con un identificador del conjunto de servicios (SSID). La tarjeta NIC también debe conocer este SSID para asociarlo al AP y así proceder a la transmisión y recepción de datos en la red. Esta seguridad, si se llegase a considerar como tal, es muy débil debido a estas razones:

- Todas las tarjetas NIC y todos los AP conocen perfectamente el SSID
- El SSID se envía por ondas de manera transparente (incluso es señalizado por el AP)
- La tarjeta NIC o el controlador pueden controlar localmente si se permite la asociación en caso de que el SSID no se conozca
- No se proporciona ningún tipo de cifrado a través de este esquema

#### **3.4.1.3.1 MECANISMOS BÁSICOS DE SEGURIDAD EN REDES INALÁMBRICAS**

Incluye dos aspectos básicos: autenticación y cifrado.

El cifrado se utiliza para codificar, los datos de las tramas inalámbricas antes de que se envíen a la red inalámbrica. Además se requiere que los clientes inalámbricos se autenticuen antes de que se les permita unirse a la red inalámbrica.

### **3.4.1.3.1.1 Cifrado**

Están disponibles los siguientes tipos de cifrado para su uso con las redes 802.11:

- WEP
- WPA
- WPA2

#### **3.4.1.3.1.1.1 Cifrado WEP (Wired Equivalent Privacy)**

Privacidad Equivalente por Cable (WEP), es un sistema que forma parte del estándar 802.11 desde sus orígenes. Es el sistema más simple de cifrado y lo admiten en la totalidad de los adaptadores inalámbricos. El cifrado WEP se realiza en la capa MAC del adaptador de red inalámbrico o en el punto de acceso, utilizando claves compartidas de 64 o 128 bits, es la suma de una clave WEP de 104 bits y otro número empleado durante el proceso de cifrado denominado vector de inicialización (un número de 24 bits). Asimismo, algunos puntos de acceso inalámbricos recientes admiten el uso de una clave de cifrado inalámbrico de 152 bits. Se trata de una clave WEP de 128 bits sumada al vector de inicialización de 24 bits. Los cuadros de diálogo de configuración de Windows XP no admiten claves WEP de 128 bits.

Cada clave consta de dos partes, una de las cuáles la tiene que configurar el usuario/administrador en cada uno de los adaptadores o puntos de acceso de la red. La otra parte se genera automáticamente y se denomina vector de inicialización (IV). El objetivo del vector de inicialización es obtener claves distintas para cada trama.

WEP utiliza una clave compartida y secreta para cifrar los datos del nodo emisor. El nodo receptor utiliza la misma clave WEP para descifrar los datos. Para el modo de infraestructura, la clave WEP debe estar configurada en el punto de

acceso inalámbrico y en todos los clientes inalámbricos. Para el modo Ad hoc, la clave WEP debe estar configurada en todos los clientes inalámbricos.

Cuando tenemos activo el cifrado WEP en cualquier dispositivo inalámbrico, bien sea una adaptador de red o un punto de acceso, estamos forzando que el emisor cifre los datos y el CRC de la trama 802.11. El receptor recoge y la descifra. Para no incurrir en errores de concepto, cuando el punto de acceso recoge una trama y la envía a través del cable, la envía sin cifrar. El cifrado se lleva a cabo partiendo de la clave compartida entre dispositivos que, como indicamos con anterioridad, previamente hemos tenido que configurar en cada una de las estaciones. En realidad un sistema WEP almacena cuatro contraseñas y mediante un índice indicarnos cuál de ellas vamos a utilizar en las comunicaciones.

El proceso de cifrado WEP agrega un vector de inicialización (IV) aleatorio de 24 bits concatenándolo con una clave compartida para generar la llave de cifrado.

Observamos como al configurar WEP tenemos que introducir un valor de 40 bits (cinco dígitos hexadecimales), que junto con los 24 bits del IV obtenemos la clave de 64 bits. El vector de inicialización podría cambiar en cada trama transmitida. WEP usa la llave de cifrado para generar la salida de datos que serán, los datos cifrados más 32 bits para la comprobación de la integridad, denominada ICV (integrity check value). El valor ICV se utiliza en la estación receptora donde se recalcula y se compara con el del emisor para comprobar si ha habido alguna modificación y tomar una decisión, que puede ser rechazar el paquete.

Para cifrar los datos WEP utiliza el algoritmo RC4, que básicamente consiste en generar un flujo de bits a partir de la clave generada, que utiliza como semilla, y realizar una operación XOR entre este flujo de bits y los datos que tiene que cifrar. El valor IV garantiza que el flujo de bits no sea siempre el mismo. WEP incluye el IV en la parte no cifrada de la trama, lo que aumenta la inseguridad. La estación receptora utiliza este IV con la clave compartida para descifrar la parte cifrada de la trama.

Lo más habitual es utilizar IV diferentes para transmitir cada trama aunque esto no es un requisito de 801.11. El cambio del valor IV mejora la seguridad del cifrado WEP dificultando que se pueda averiguar la contraseña capturando tramas, aunque a pesar de todo sigue siendo inseguro.

Una clave WEP basada en una palabra (como un nombre de compañía en el caso de una pequeña empresa o el apellido si se trata de una red doméstica) o en una frase fácil de recordar se puede averiguar fácilmente. Después de que el usuario malintencionado haya determinado la clave WEP, puede descifrar las tramas cifradas con WEP, cifrar tramas WEP correctamente y comenzar a atacar la red.

Aunque la clave WEP sea aleatoria, todavía se puede averiguar si se recopila y analiza una gran cantidad de datos cifrados con la misma clave. Por lo tanto, se recomienda cambiar la clave WEP por una nueva secuencia aleatoria periódicamente, por ejemplo, cada tres meses.

### **Debilidades de WEP**

Las debilidades de WEP se basan en que, por un lado, las claves permanecen estáticas y por otro lado los 24 bits de IV son insuficientes y se transmiten sin cifrar. Aunque el algoritmo RC4 no esté considerado de los más seguros, en este caso la debilidad de WEP no es culpa de RC4<sub>5</sub> sino de su propio diseño.

Si tenemos un vector de inicialización de 24 bits tendremos  $2^{24}$  posibles IV distintos y no es difícil encontrar distintos paquetes generados con el mismo IV. Sí la red tiene bastante tráfico, estas repeticiones se dan con cierta frecuencia. Un atacante puede recopilar suficientes paquetes similares cifrados con el mismo IV y utilizarlos para determinar el valor del flujo de bits y de la clave compartida. El valor del IV se transmite sin cifrar por lo que es público. Esto puede parecer muy complicado, pero hay programas que lo hacen automáticamente y en horas o días

averiguan la contraseña compartida. No olvidemos que aunque la red tenga poco tráfico el atacante puede generarlo mediante ciertas aplicaciones.

Una vez que alguien ha conseguido descifrar la contraseña WEP tiene el mismo acceso a la red que si pudiera conectarse a ella mediante cable. Si la red está configurada con un servidor DHCP, entonces el acceso es inmediato, y si no tenemos servidor DHCP pues al atacante le puede llevar cinco minutos más.

Vista la debilidad real de WEP lo ideal es que se utilizaran claves WEP dinámicas, que cambiarán cada cierto tiempo lo que haría materialmente imposible utilizar este sistema para asaltar una red inalámbrica, pero 802.11 no establece ningún mecanismo que admita el intercambio de claves entre estaciones. En una red puede ser tedioso, simplemente inviable, ir estación por estación cambiando la contraseña y en consecuencia es habitual que no se modifiquen, lo que facilita su descifrado.

Algunos adaptadores sólo admiten cifrado WEP por lo que a pesar de su inseguridad puede ser mejor que nada. Al menos evitaremos conexiones y desconexiones a la red si hay varias redes inalámbricas disponibles.

#### **3.4.1.3.1.1.2 CIFRADO WPA**

WPA es la abreviatura de Wifi Protect Access, y consiste en un mecanismo de control de acceso a una red inalámbrica, pensado con la idea de eliminar las debilidades de WEP. También se le conoce con el nombre de TSN (Transition Security Network).

WPA utiliza TKIP (Temporal Key Integrity Protocol) para la gestión de las claves dinámicas mejorando notablemente el cifrado de datos, incluyendo el vector de inicialización. En general WPA es TKIP con 8021X. Por lo demás WPA funciona de una manera parecida a WEP pero utilizando claves dinámicas, utiliza el

algoritmo RC4 para generar un flujo de bits que se utilizan para cifrar con XGR y su vector de inicialización (IV) es de 48 bits. La modificación dinámica de claves puede hacer imposible utilizar el mismo sistema que con WEP para abrir una red inalámbrica con seguridad WPA.

Además WPA puede admitir diferentes sistemas de control de acceso incluyendo la validación de usuario-contraseña, certificado digital u otro sistema o simplemente utilizar una contraseña compartida para identificarse.

Consta de 2 clases de cifrado:

- WPA-PSK
- WPA EMPRESARIAL

#### **3.4.1.3.1.1.2.1 WPA-PSK**

Es el sistema más simple de control de acceso tras WEP, a efectos prácticos tiene la misma dificultad de configuración que WEP, una clave común compartida, sin embargo, la gestión dinámica de claves aumenta notoriamente su nivel de seguridad. PSK se corresponde con las iniciales de PreShared Key y viene a significar clave compartida previamente, es decir, a efectos del cliente basa su seguridad en una contraseña compartida.

WPA-PSK usa una clave de acceso de una longitud entre 8 y 63 caracteres, que es la clave compartida. Al igual que ocurría con WEP, esta clave hay que introducirla en cada una de las estaciones y puntos de acceso de la red inalámbrica. Cualquier estación que se identifique con esta contraseña, tiene acceso a la red.

Las características de WPA-PSK lo definen como el sistema, actualmente, más adecuado para redes de pequeñas oficinas o domésticas, la configuración es muy simple, la seguridad es aceptable y no necesita ningún componente adicional.

### **Debilidades de WPA-PSK**

La principal debilidad de WPA-PSK es la clave compartida entre estaciones. Cuando un sistema basa su seguridad en una contraseña siempre es susceptible de sufrir un ataque de fuerza bruta, es decir ir comprobando contraseñas, aunque dada la longitud de la contraseña y si está bien elegida no debería plantear mayores problemas.

#### **3.4.1.3.1.1.2 WPA EMPRESARIAL**

En redes corporativas resultan imprescindibles otros mecanismos de control de acceso más versátiles y fáciles de mantener, como por ejemplo los usuarios de un sistema identificado con nombre/contraseña o la posesión de un certificado digital. Evidentemente el hardware de un punto de acceso no tiene la capacidad para almacenar y procesar toda esta información, por lo que es necesario recurrir a otros elementos de la red cableada para que comprueben unas credenciales. Ahora bien, parece complicado que un cliente se pueda validar ante un componente de la red por cable si todavía no tenemos acceso a la red, parece el problema del huevo y la gallina. En este punto es donde entra en juego el IEEE 802.1X, que describimos a continuación, para permitir el tráfico de validación entre un cliente y una máquina de la red local. Una vez que se ha validado a un cliente es cuando WPA inicia TKIP para utilizar claves dinámicas.

Los clientes WPA tienen que estar configurados para utilizar un sistema concreto de validación que es completamente independiente del punto de acceso. Los sistemas de validación WPA pueden ser, entre otros, EAP-TLS, PEAP, EAP-TTLS que describimos más adelante.



### **3.4.1.3.1.1.3 CIFRADO WPA2**

WPA2, es una certificación de producto que otorga Wi-Fi Alliance y certifica que los equipos inalámbricos son compatibles con el estándar 802.11i. WPA2 admite las características de seguridad obligatorias adicionales del estándar 802.11i que no están incluidos para productos que admitan WPA. Con WPA2, el cifrado se realiza mediante AES (estándar de cifrado avanzado), que también reemplaza WEP por un algoritmo de cifrado más seguro. Al igual que TKIP para WPA, AES proporciona la determinación de una clave de cifrado de unidifusión de inicio exclusiva para cada autenticación y el cambio sincronizado de la clave de cifrado de unidifusión para cada trama. Debido a que las claves AES se determinan automáticamente, no es necesario configurar una clave de cifrado para WPA2. WPA2 es la forma más eficaz de seguridad inalámbrica.

### **Autenticación**

Están disponibles los siguientes tipos de autenticación para utilizarlos con las redes 802.11:

- Sistema abierto
- Clave compartida
- IEEE 802.1X
- SEE802.11i

#### **3.4.1.3.1.1.3.1 Autenticación en 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.

Para el modo de infraestructura, aunque algunos puntos de acceso inalámbricos permiten configurar una lista de direcciones de hardware permitidas para la autenticación de sistema abierto, resulta bastante sencillo para un usuario malintencionado capturar las tramas enviadas en la red inalámbrica para determinar la dirección de hardware de los nodos inalámbricos permitidos y, a continuación, utilizar la dirección de hardware para realizar la autenticación de sistema abierto y unirse a su red inalámbrica.

Para el modo ad hoc, no existe equivalencia para la configuración de la lista de direcciones de hardware permitidas en Windows XP. Por lo tanto, se puede utilizar cualquier dirección de hardware para realizar la autenticación de sistema abierto y unirse a su red inalámbrica basada en el modo ad hoc.

#### **3.4.1.3.1.3.2 Autenticación con Clave compartida**

La autenticación de clave compartida comprueba que el cliente inalámbrico que se va a unir a 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 utilizan la misma clave compartida. Para el modo ad hoc, todos los clientes inalámbricos de la red inalámbrica ad hoc utilizan la misma clave compartida.

De todas las formas, la mayoría de las instalaciones 802.1x otorgan cambios automáticos de claves de encriptación usadas solo para la sesión con el cliente, no dejando el tiempo necesario para que ningún sniffer sea capaz de obtener la clave.

Para el control de admisión 802.1X utiliza un protocolo de autenticación denominado EAP y para el cifrado de datos CCMP y esto es lo que se conoce

como RSN (Robust Secure Network) o también WPA2. No todo el hardware admite CCMP.

#### **3.4.1.3.1.1.3.3 EAP (IEEE 802.1X)**

Hemos visto que 802.1X utiliza un protocolo de autenticación llamado EAP (Extensible Authentication Protocol) que admite distintos métodos de autenticación como certificados, tarjetas inteligentes, ntlm, Kerberos, Idap, etc. En realidad EAP actúa como intermediario entre un solicitante y un motor de validación permitiendo la comunicación entre ambos.

El proceso de validación está conformado por tres elementos, un solicitante que quiere ser validado mediante unas credenciales, un punto de acceso y un sistema de validación situado en la parte cableada de la red. Para conectarse a la red, el solicitante se identifica mediante una credencial que pueden ser un certificado digital, una pareja nombre/usuario u otros datos. Junto con las credenciales, el cliente solicitante tiene que añadir también qué sistema de validación tiene que utilizar. Evidentemente no podemos pretender que el punto de acceso disponga del sistema de validación. Por ejemplo, si queremos utilizar como credenciales los usuarios de un sistema, será el punto de acceso el que tendrá que preguntar al sistema si las credenciales son correctas. En general EAP actúa de esta forma, recibe una solicitud de validación y la remite a otro sistema que sepa cómo resolverla y que formará parte de la red cableada. De esta forma vemos como el sistema EAP permite un cierto tráfico de datos con la red local para permitir la validación de un solicitante. El punto de acceso rechaza todas las tramas que no estén validadas, que provengan de un cliente que no se ha identificado, salvo aquellas que sean una solicitud de validación. Estos paquetes EAP que circulan por la red local se denominan EAPQL (EAP over LAN). Una vez validado, el punto de acceso admite todo el tráfico del cliente.

El sistema de autenticación puede ser un servidor RADIUS situado en la red local. Los pasos que sigue el sistema de autenticación 802.1X son:

- El cliente envía un mensaje de inicio EAP que inicia un intercambio de mensajes para permitir autenticar al cliente.
- El punto de acceso responde con un mensaje de solicitud de identidad EAP para solicitar las credenciales del cliente.
- El cliente envía un paquete respuesta EAP que contiene las credenciales de validación y que es remitido al servidor de validación en la red local, ajena al punto de acceso.
- El servidor de validación analiza las credenciales y el sistema de validación solicitado y determina si autoriza o no el acceso. En este punto tendrán que coincidir las configuraciones del cliente y del servidor, las credenciales tienen que coincidir con el tipo de datos que espera el servidor.
- El servidor puede aceptar o rechazar la validación y le envía la respuesta al punto de acceso.
- El punto de acceso devuelve un paquete EAP de acceso o de rechazo al cliente.
- Si el servidor de autenticación acepta al cliente, el punto de acceso modifica el estado del puerto de ese cliente como autorizado para permitir las comunicaciones.

De lo que hemos visto, el protocolo 802.1X tiene un mecanismo de autenticación independiente del sistema de cifrado. Si el servidor de validación 802.1X está configurado adecuadamente, se puede utilizar para gestionar el intercambio dinámico de claves, e incluir la clave de sesión con el mensaje de aceptación. El

punto de acceso utiliza las claves de sesión para construir, firmar y cifrar el mensaje de clave EAP que se manda tras el mensaje de aceptación. El cliente puede utilizar el contenido del mensaje de clave para definir las claves de cifrado aplicables. En los casos prácticos de aplicación del protocolo 802.1X, el cliente puede cambiar automáticamente las claves de cifrado con la frecuencia necesaria para evitar que haya tiempo suficiente como para poder averiguarla.

Existen múltiples tipos de EAP, algunos son estándares y otros son soluciones propietarias de empresas. Entre los tipos de EAP podemos citar:

**EAP-TLS:** Es un sistema de autenticación fuerte basado en certificados digitales, tanto del cliente como del servidor, es decir, requiere una configuración PKI (Public Key Infraestructura) en ambos extremos. TLS (transport Layer Security) es el nuevo estándar que sustituye a SSL (Secure Socket Layer).

**EAP-TTLS:** El sistema de autenticación se basa en una identificación de un usuario y contraseña que se transmiten cifrados mediante TLS, para evitar su transmisión en texto limpio. Es decir se crea un túnel mediante TLS para transmitir el nombre de usuario y la contraseña. A diferencia de EAP-TLS sólo requiere un certificado de servidor.

**PEAP:** El significado de PEAP se corresponde con Protected EAP y consiste en un mecanismo de validación similar a EAP-TTLS, basado en usuario y contraseña también protegidos.

#### **3.4.1.3.1.1.3.4 Autenticación IEEE 802.11i**

Se ha visto que con WEP utilizamos claves estáticas que son relativamente fáciles de averiguar. La solución al problema que plantea WEP consiste en establecer un sistema dinámico de claves sin necesidad de intervención del administrador y con este propósito se establece el estándar IEEE 802.11 i.

El estándar IEEE 802.11 i incluye protocolos de gestión de claves y mejoras de cifrado y autenticación con IEEE 802.1X.

Podemos citar 3 tipos de autenticación en el estándar IEE 802.11:

- TKIP
- CCMP
- WRAP

#### **3.4.1.3.1.1.3.4.1 TKIP (Temporary Key Integrify Protocol)**

Es un protocolo de gestión de claves dinámicas admitido por cualquier adaptador que permite utilizar una clave distinta para cada paquete transmitido. La clave se construye a partir de la clave base, la dirección MAC de la estación emisora y del número de serie del paquete como vector de inicialización.

Cada paquete que se transmite utilizando TKIP incluye un número de serie único de 48 bits que se incrementa en cada nueva transmisión para asegurar que todas las claves son distintas. Esto evita "ataques de colisión" que se basan en paquetes cifrados con la misma clave.

Por otro lado al utilizar el número de serie del paquete como vector de inicialización (IV), también evitamos IV duplicados. Además, si se inyectara un paquete con una contraseña temporal que se hubiese podido detectar, el paquete estaría fuera de secuencia y sería descartado.

En cuanto a la clave base, se genera a partir del identificador de asociación, un valor que crea el punto de acceso cada vez que se asocia una estación. Además del identificador de asociación, para generar la clave base se utilizan las

direcciones MAC de la estación y del punto de acceso, la clave de sesión y un valor aleatorio.

Como veremos más adelante, la clave de sesión puede ser estática y compartida (PSK) por toda la red o bien, mediante 802.1X, transmitirla por un canal seguro.

#### **3.4.1.3.1.1.3.4.2 CCMP**

CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) es un nuevo protocolo que utiliza AES como algoritmo criptográfico y proporciona integridad y confidencialidad.

CCMP se basa en el modo CCM del algoritmo de cifrado AES y utiliza llaves de 128 bits con vectores de inicialización de 48 bits.

CCMP consta del algoritmo de privacidad que es el "Counter Mode" (CM) y del algoritmo de integridad y autenticidad que es el "Cipher Block Chaining Message Authentication Code" (CBC-MAC).

CCMP es obligatorio sobre RSN (Robust Secure Network).

#### **3.4.1.3.1.1.3.4.3 WRAP**

Existe un sistema de cifrado opcional denominado WRAP (Wireless Robust Authentication Protocol) que puede sustituir a CCMP.

### 3.4.1.4 GUÍA DE INSTALACIÓN Y CONFIGURACIÓN

#### PUNTO DE ACCESO CISCO WAP321 WIRELESS-N



#### CON CONFIGURACIÓN DE UN SOLO PUNTO



283935

#### PUNTO DE ACCESO WIRELESS-N WAP321 DE BANDA SELECCIONABLE CON POE

#### INFORMACIÓN GENERAL & GUÍA DE INICIO RÁPIDO

#### CONECTIVIDAD WIRELESS-N SEGURA, FÁCIL DE IMPLEMENTAR Y ASEQUIBLE



## **DESCRIPCIÓN GENERAL**

En un lugar de trabajo cada vez más móvil, ofrecer una conectividad inalámbrica segura y de alta velocidad a los empleados y los usuarios temporales es lo más importante. El punto de acceso Cisco WAP321 Wireless-N con configuración de un solo punto es una manera fácil y asequible de mejorar el rendimiento y el alcance de su red de pequeña empresa con tecnología inalámbrica avanzada 802.11n. Esta solución flexible es ideal para conectar hasta 10 empleados en un solo punto de acceso. Con la tecnología de implementación de un punto de varios accesos sin controlador de la configuración de un solo punto, la red LAN inalámbrica puede ampliarse hasta cuatro WAP321 para ofrecer una cobertura más amplia y admitir a usuarios adicionales a medida que cambian las necesidades empresariales.

Diseñado para las aplicaciones con rendimiento intenso de la actualidad, Cisco WAP321 utiliza la tecnología inalámbrica 802.11n para entregar un alto rendimiento y un alcance extendido en toda su oficina. Cuenta con funciones de calidad de servicio (QoS) integradas que le permiten priorizar el tráfico según el ancho de banda, lo que permite la implementación de voz sobre IP (VoIP) de calidad empresarial y aplicaciones de video.

Cisco WAP321 es sencillo de configurar y usar, está basada en un asistente intuitivo para un funcionamiento en minutos. Un diseño elegante y compacto con opciones de montaje flexibles permite integrar el punto de acceso sin problemas a cualquier entorno de pequeña empresa. La compatibilidad con PoE permite que el dispositivo sea fácil de instalar sin necesidad de enchufes de alimentación por separado o un nuevo y costoso cableado.

Para mejorar la confiabilidad y proteger la información comercial sensible, Cisco WAP321 admite Privacidad equiparable a la de redes cableadas (WEP) y Acceso protegido Wi-Fi (WPA2), que cifran todas sus transmisiones inalámbricas con un potente cifrado. Además, la autenticación 802.1X RADIUS ayuda a mantener lejos a los usuarios no autorizados. Para las organizaciones que necesitan ofrecer un acceso inalámbrico seguro a los empleados, los clientes y los partners,

proporciona también compatibilidad para redes virtuales separadas, con opciones de configuración granular que permite brindar el nivel de acceso adecuado para diferentes usuarios.

La configuración de un solo punto, ofrece un método centralizado exclusivo para administrar y controlar los servicios inalámbricos en varios puntos de acceso. Mediante un punto de acceso en la red LAN, usted tiene una sola vista de toda la WLAN para replicar la configuración, la seguridad y la administración en todos los puntos de acceso.

Con Cisco WAP321, usted puede extender la red inalámbrica de clase empresarial sumamente segura en la oficina, con la confiabilidad y flexibilidad para satisfacer las necesidades empresariales en constante cambio.

La Figura 1 muestra una configuración típica con este punto de acceso inalámbrico. Las Figuras 2 y 3 muestran la parte frontal y posterior, respectivamente, del punto de acceso Cisco WAP321 Wireless-N con configuración de un solo punto.

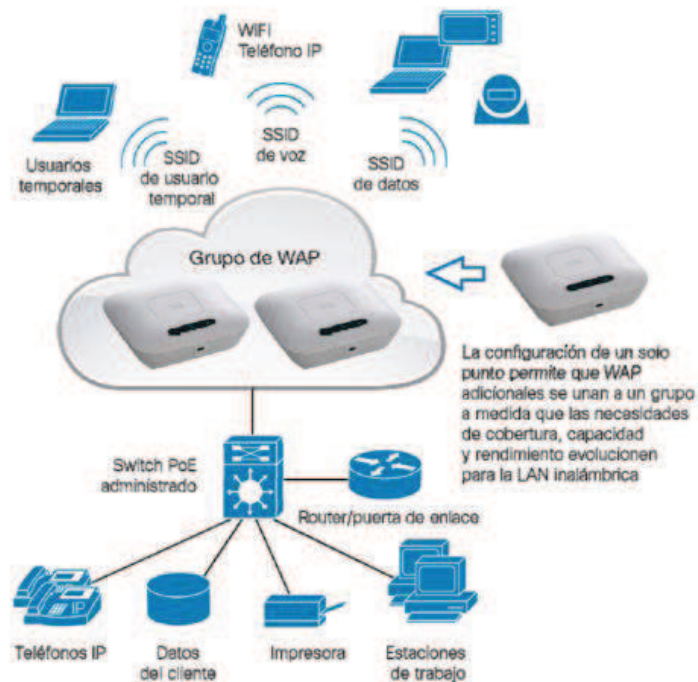
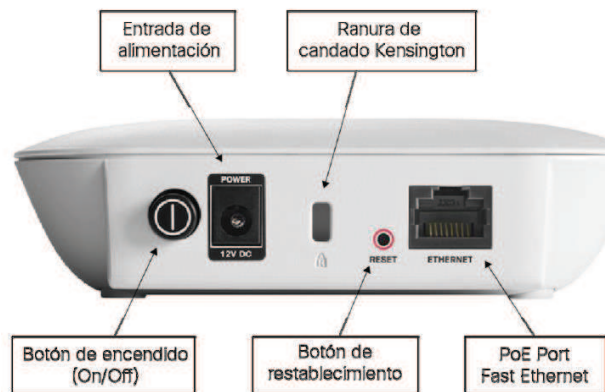


Figura 1. Configuración típica



**Figura 2.** Panel frontal del punto de acceso Cisco WAP321 Wireless-N con configuración de un solo punto



**Figura 3.** Panel posterior del punto de acceso Cisco WAP321 Wireless-N con configuración de un solo

## **FUNCIONALIDADES**

- Las redes inalámbricas sumamente seguras y de alta velocidad 802.11n entregan un mayor rendimiento y mayor alcance para aplicaciones con un uso intensivo del ancho de banda.
- La instalación y la configuración mediante asistentes permiten una implementación rápida y simple.

- La tecnología de administración e implementación de un punto de varios accesos sin controlador de la configuración de un solo punto permite que la configuración sea sencilla.
- La seguridad sólida, que incluye WPA2, 802.1x con autenticación RADIUS segura y detección de puntos de acceso dudosos ayuda a proteger la información confidencial de la empresa.
- La compatibilidad con PoE permite una instalación fácil sin el costoso cableado adicional.
- El modo puente grupo de trabajo permite expandir la red mediante la conexión inalámbrica a una segunda red Ethernet.
- El compacto y elegante diseño con antenas internas y los diversos kits de armado hacen que puedan instalarse en el techo, la pared o en un escritorio.
- La calidad de servicio inteligente prioriza el tráfico de red para ayudar a mantener en funcionamiento las aplicaciones de red más importantes.
- El modo suspendido con ahorro de energía y las funciones de control de puertos ayudan a maximizar la eficiencia energética.
- El acceso sumamente seguro de los usuarios temporales permite una conectividad inalámbrica segura para todos los visitantes.
- La compatibilidad con IPv6 permite implementar futuras aplicaciones de redes y sistemas operativos sin las costosas actualizaciones.

## ESPECIFICACIONES

La Tabla 1 menciona las especificaciones, el contenido del paquete y los requisitos mínimos del punto de acceso Cisco WAP121 Wireless-N con configuración de un solo punto.

**Tabla 1.** Especificaciones

Especificaciones	Descripción
Estándares	IEEE 802.11n, 802.11g, 802.11b, 802.3af, 802.3u, 802.1X (autenticación de seguridad), 802.1Q (VLAN), 802.1D (Árbol de expansión), 802.11i (seguridad WPA2), 802.11e (QoS inalámbrica), IPv4 (RFC 791), IPv6 (RFC 2460)
Puertos	Detección automática de Ethernet rápida de LAN, enchufe de CC
Switch	Botón de encendido (encendido/apagado)
Botones	Botón de alimentación (encendido/apagado), botón de restablecimiento
Tipo de cableado	Categoría 5e o superior
Antenas	Antenas internas optimizadas para su colocación en la pared, el cielo o el escritorio
Indicadores LED	Alimentación, WLAN, LAN
Sistema operativo	Linux
<b>Interfaces físicas</b>	
Puertos	Ethernet 10BASE-T/100BASE-TX, alimentación CC de 12 V con compatibilidad para PoE 802.3af
Fuente de alimentación	Enchufe de alimentación externo 12 V 0,5 A CC (Energy Star 2.0 conforme con el Nivel de eficacia 5) y PoE 802.3af
Botones	Botón de alimentación (encendido/apagado); botón de restablecimiento
Ranura de bloqueo	Ranura para candado Kensington
Indicador LED	Alimentación, inalámbrico, Ethernet
<b>Especificaciones físicas</b>	
Dimensiones físicas (An x Prof. x Al)	4,89 x 4,89 x 1,38 in. (124,17 x 124,17 x 35 mm)
Peso	0,37 lb o 168 g
<b>PoE</b>	
PoE	802.3af
Alimentación máxima PoE	6W
<b>Capacidades de red</b>	
Compatibilidad con redes VLAN	Sí
Cantidad de VLAN	1 VLAN de administración más 4 VLAN para identificador de conjunto de servicios (SSID)
Varios SSID	4
Suplicante 802.1X	Sí
SSID o asignación del VLAN	Sí
Selección automática de canales	Sí

Especificaciones	Descripción
Árbol de expansión	SI
Equilibrio de carga	SI
IPv6	SI <ul style="list-style-type: none"> <li>• Compatibilidad de host IPv6</li> <li>• IPv6 RADIUS, syslog, protocolo de tiempo de red (NTP), etc.</li> </ul>
Capa 2	VLANS basadas en 802.1Q, 4 VLANS activas más 1 VLAN de administración
<b>Seguridad</b>	
WPA/WPA2/WEK	SI, incluida la autenticación de empresa
Control de acceso	SI, lista de control de acceso de administración (ACL) más MAC ACL
Administración segura	HTTPS
Wi-Fi Protected Setup (WPS)	SI (WPS blando, sin botón de hardware)
Difusión SSID	SI
Detección de puntos de acceso dudosos	SI
<b>Montaje y seguridad física</b>	
Varias opciones de montaje	Instalación en escritorio; soporte de montaje incluido para montaje sencillo en el cielo o en la pared.
Candado de seguridad físico	Ranura para candado Kensington
<b>Calidad de servicio</b>	
Calidad de servicio (QoS)	Multimedia Wi-Fi y especificación de tráfico (WMM TSPEC)
<b>sistema</b>	
Rendimiento inalámbrico	Hasta 300 Mbps de velocidad de datos (el rendimiento en el mundo real puede variar)
Soporte de usuarios recomendado	Hasta 16 usuarios conectados o 10 usuarios activos.
<b>Configuración</b>	
Interfaz de usuario web	Interfaz de usuario web integrada para una configuración simple basada en navegador (HTTP/HTTPS)
<b>Administración de punto de varios accesos</b>	
Configuración de un solo punto	SI
Máximo de puntos de acceso por grupo	4
Clientes activos por grupo	40
<b>Administración</b>	
Protocolos de administración	Navegador web, protocolo simple de administración de redes (SNMP) v3, Bonjour
Administración remota	SI
Registro de eventos	Syslog local, remoto, alertas de correo electrónico
Diagnósticos de red	Registros y captura de paquetes
Actualización de firmware web	Firmware que se puede actualizar mediante el navegador web, archivo de configuración importado/exportado
Protocolo de configuración dinámica de host (DHCP)	Cliente DHCP
Host IPv6	SI
<b>Tecnología inalámbrica</b>	
Frecuencia	2,4 GHz de una sola banda
Tipo de modulación y radio	Radio simple, multiplexado de división de frecuencia ortogonal (OFDM)
WLAN	802.11n
Canales operativos	1 a 13 (según el país) Canales 1 al 11 (FCC) Canales 1 al 13 (ETSI)



Especificaciones	Descripción
Aislamiento Inalámbrico	Aislamiento Inalámbrico entre clientes
Antenas externas	Ninguno
Antenas Internas	Antenas Internas PIFA fijas
Ganancia de antena en dBi	2 dBi cada antena
Alimentación de salida transmitida	<ul style="list-style-type: none"> <li>• 802.11b @ 11 Mbps: 17 dBm</li> <li>• 802.11g @ 54 Mbps: 13 dBm</li> <li>• 802.11n @ HT20HT40, MCS15: 13 dBm</li> </ul>
Sensibilidad del receptor	<ul style="list-style-type: none"> <li>• 802.11b: 11 Mbps a -86 dBm</li> <li>• 802.11g: 54 Mbps a -71 dBm</li> <li>• 802.11n: 300 Mbps a -64 dBm</li> </ul>
Sistema de distribución Inalámbrica (WDS)	SI
Roaming	SI
Varios SSID	4
Asignación de VLAN Inalámbrica	SI
Seguridad de WLAN	SI
WMM	SI, con ahorro de energía automático sin programar y perfil de voz
<b>Modos de funcionamiento</b>	
Punto de acceso	Modos de punto de acceso, puente WDS, modo de puente de grupo de trabajo
<b>Condiciones del entorno</b>	
Alimentación	12 V, 0,5 A entrada CC y PoE conforme a IEEE802.3af
Certificaciones	FCC clase B, CE, IC, Wi-Fi
Temperatura de funcionamiento	De 0° a 40 °C (32° a 104 °F)
Temperatura de almacenamiento	De -20° a 70 °C (-4° a 158 °F)
Humedad de funcionamiento	De 10 a 85%, sin condensación
Humedad de almacenamiento	De 5 a 90%, sin condensación
Tiempo medio entre fallas (MTBF)	531.189 horas
<b>Contenido del paquete</b>	
<ul style="list-style-type: none"> <li>• Punto de acceso Cisco WAP121 Wireless-N con configuración de un solo punto</li> <li>• Kit de montaje en cielo/pared</li> <li>• Guía del usuario en CD-ROM</li> <li>• Guía de inicio rápido</li> <li>• Cables de red Ethernet</li> <li>• Fuente de alimentación de 12 V, 0,5 A</li> </ul>	
<b>Requisitos mínimos</b>	
<ul style="list-style-type: none"> <li>• Adaptador Inalámbrico 802.11b, 802.11g, 802.11n con protocolo TCP/IP instalado en cada PC</li> <li>• Switch/router con compatibilidad con PoE o inyector PoE cuando se usa con PoE</li> <li>• Configuración basada en la web: navegador web habilitado con Java</li> </ul>	
<b>Garantía</b>	
Punto de acceso	Limitada de por vida
Fuente de alimentación	1 año de garantía

### 3.4.1.4.1 GUÍA DE INICIO RÁPIDO

Cisco WAP321 es un punto de acceso de 2,4 GHz o 5,0 GHz 802.11n de radio única con banda seleccionable; Cisco WAP321 es una variante de banda única de 2,4 GHz de Cisco WAP321. Esta guía está diseñada para familiarizarlo con la disposición general del punto de acceso, a la vez que describe cómo debe implementar el dispositivo en la red y cómo configurarlo. El punto de acceso tiene más características y funcionalidades de lo que se describe en esta guía. Para obtener más información, consulte la Guía de administración.

Antes de comenzar la instalación, asegúrese de contar con los siguientes equipos y servicios:

- Una computadora compatible con los siguientes exploradores:
  - Internet Explorer v7.0 o posterior
  - Chrome v5.0 o posterior – Firefox v3.0 o posterior
  - Safari v3.0 o posterior
  
- Herramientas para instalar el hardware
- Uno o más switches de red Ethernet
- Fuente de alimentación ininterrumpida (UPS) para contar con energía de respaldo para los dispositivos principales.

#### **Características de los puntos de acceso Wireless-N WAP321 de Cisco**

##### **Panel frontal**

El panel frontal de los dispositivos posee tres luces: Energía, WLAN y LAN. Para ver una descripción completa de los colores de las luces y sus indicaciones, consulte “Verificación de la instalación del hardware”. Hay una ranura para el



conector de seguridad Kensington debajo de las luces. Panel posterior El panel posterior de los dispositivos posee:

- Power Button (Botón de encendido): use este botón para encender o apagar el dispositivo. No se aplica al usar PoE.
- Power Jack (Toma de alimentación): use esta toma siempre y cuando no esté usando PoE.
- Kensington Lock Slot (Ranura del conector de seguridad Kensington): úsela para conectar un cable y un conector de seguridad al dispositivo.
- Reset (Reinicio): consulte “Reinicio de los dispositivos o retorno a las configuraciones predeterminadas de fábrica” para obtener información sobre el botón de reinicio.
- RJ-45 Ethernet Port (Puerto Ethernet RJ-45): use este puerto de detección automática Gigabit Ethernet (802.3) para conectarse a dispositivos de red, como computadoras, routers o switches. Cisco recomienda usar Cat5 o un cable de mayor calidad para la conectividad Gigabit. Puede usar el puerto Ethernet para alimentar su dispositivo con PoE.

### CONFIGURACIÓN PREDETERMINADA

Parámetros	Valor predeterminado
Nombre de usuario	cisco
Contraseña	cisco
Dirección IP de la red LAN	Dirección DHCP asignada por el servidor
Reserva de IP de la red LAN	192.168.1.245
Mascara de subred	255.255.255.0

## **Conexión de los puntos de acceso Wireless-N de Cisco WAP321**

Para conectar el dispositivo a la red:

**PASO1** Conecte el cable Ethernet al puerto Ethernet de un switch o router.

**PASO2** Conecte el otro extremo del cable de red Ethernet al puerto Ethernet del punto de acceso inalámbrico.

**PASO3** Si PoE lo provee, para Cisco WAP321 enchufe el adaptador de energía para suministrar energía al dispositivo.

Después de la instalación, todas las luces deberían activarse. Consulte Verificación de la instalación del hardware, para obtener más información sobre las diferentes luces de cada switch.

### **Verificación de la instalación del hardware**

Para verificar la instalación del hardware, realice las siguientes tareas:

- Verifique las conexiones de los cables.
- Controle el estado de las luces del indicador.

Etiqueta	Actividad	Descripción
Encendido	Desact.	La energía está desactivada
	Verde permanente	La energía está activada. Funcionamiento normal al usar un adaptador de energía externo.
	Ambar permanente	La energía está activada. Funcionamiento normal con PoE.
	Parpadeo	Arranque/actualización de firmware
WLAN	Desact.	El acceso inalámbrico está desactivado para redes inalámbricas de 2,4 GHz y 5 GHz
	Verde permanente	La banda inalámbrica de 2,4 GHz está activada.
	Ambar permanente	La banda inalámbrica de 5 GHz está activada.
	Parpadeo	Transmisión y recepción de datos
	Parpadeo rápido (2 veces la velocidad de parpadeo)	Wi-Fi Protected Setup (WPS) se está sincronizando.
LAN	Desact.	Sin enlace Ethernet
	Verde permanente	El enlace Ethernet está activado. <ul style="list-style-type: none"> <li>El enlace FE se detecta para Cisco WAP121</li> <li>El enlace GE se detecta para Cisco WAP321</li> </ul>
	Ambar permanente	El enlace Ethernet está activado. <ul style="list-style-type: none"> <li>El enlace FE se detecta para Cisco WAP321</li> </ul>
	Parpadeo	Transmisión y recepción de datos

## Inicio de la configuración

Para configurar los puntos de acceso inalámbrico, siga estos pasos para poder acceder al Asistente y luego a la utilidad de configuración web desde la computadora.

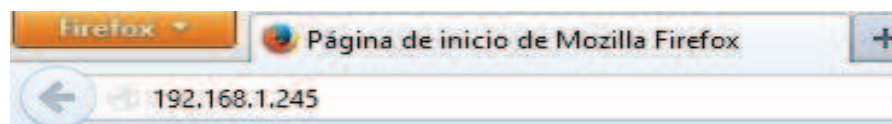
**PASO1** Conecte el punto de acceso inalámbrico a la misma red (subred de IP) que tenga la computadora. La configuración predeterminada de fábrica de la dirección de IP de los puntos de acceso es DHCP. Asegúrese de que el servidor DHCP esté funcionando y que pueda alcanzarse.

Consulte “Dirección IP incorrecta” en la página 10 para obtener información referida a la resolución de problemas, o en caso de que no posea un servidor DHCP.

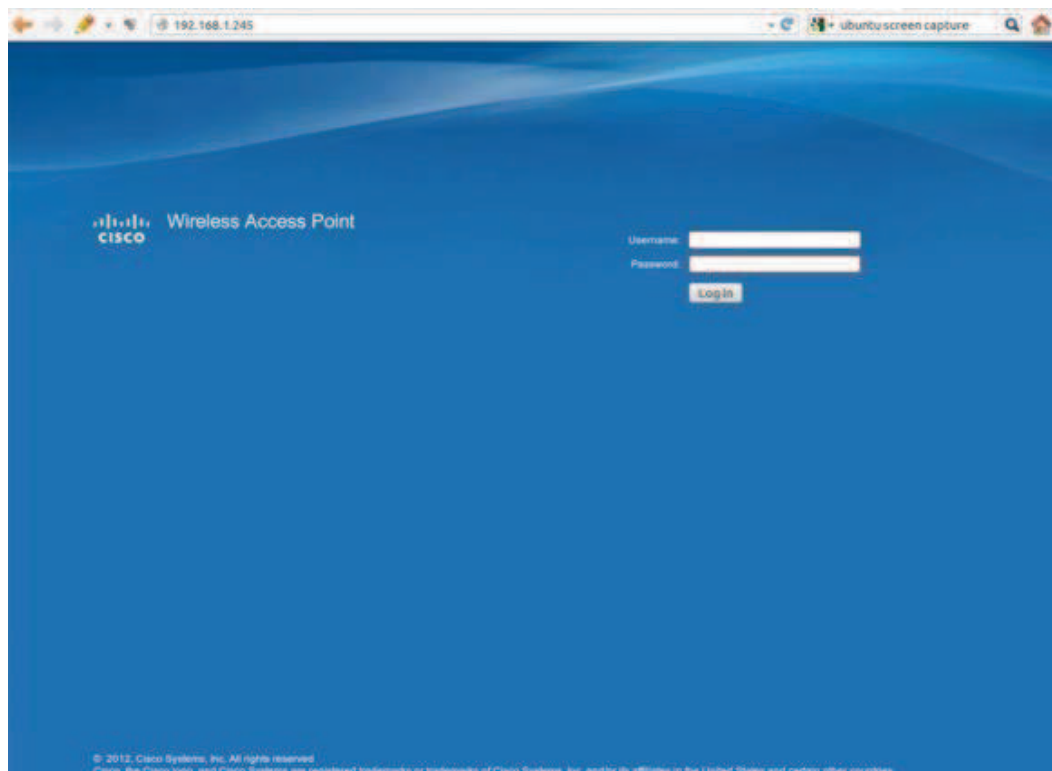
**PASO2** Localice la dirección IP del punto de acceso inalámbrico.

- a. Se puede acceder a los puntos de acceso inalámbrico y administrarlos con las herramientas y los servicios de red de Cisco Small Business, incluida Cisco FindIT Network Discovery Utility, que le permite detectar automáticamente todos los dispositivos Cisco Small Business compatibles que se encuentren en el mismo segmento de red local que la computadora. Puede disponer de una vista instantánea de cada dispositivo o abrir la utilidad de configuración del producto para ver y configurar las opciones. Para obtener más información, visite [www.cisco.com/go/findit](http://www.cisco.com/go/findit).
- b. Los puntos de acceso inalámbrico se habilitan para Bonjour y en forma automática transmiten sus servicios y detectan los servicios anunciados por otros dispositivos habilitados para Bonjour. En caso de que posea un explorador habilitado para Bonjour, tal como Microsoft Internet Explorer con un complemento para Bonjour, o el explorador Apple Mac Safari, podrá encontrar el punto de acceso inalámbrico en su red local sin conocer la dirección IP. Puede descargar el explorador completo Bonjour para Internet Explorer desde el sitio web de Apple. Visite: <http://www.apple.com/bonjour/>.
- c. Acceda al router o servidor DHCP para ubicar la dirección IP asignada por dicho servidor; consulte las instrucciones del servidor DHCP para obtener información.

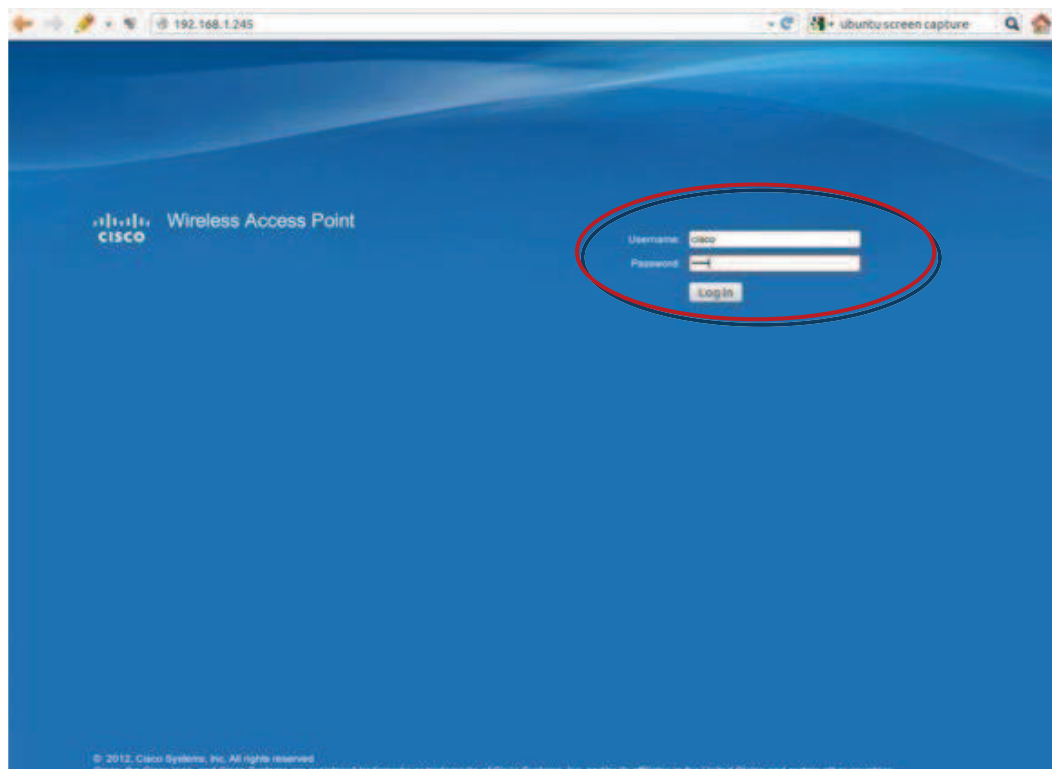
**PASO3** Inicie un explorador web, tal como Internet Explorer o Mozilla Firefox.



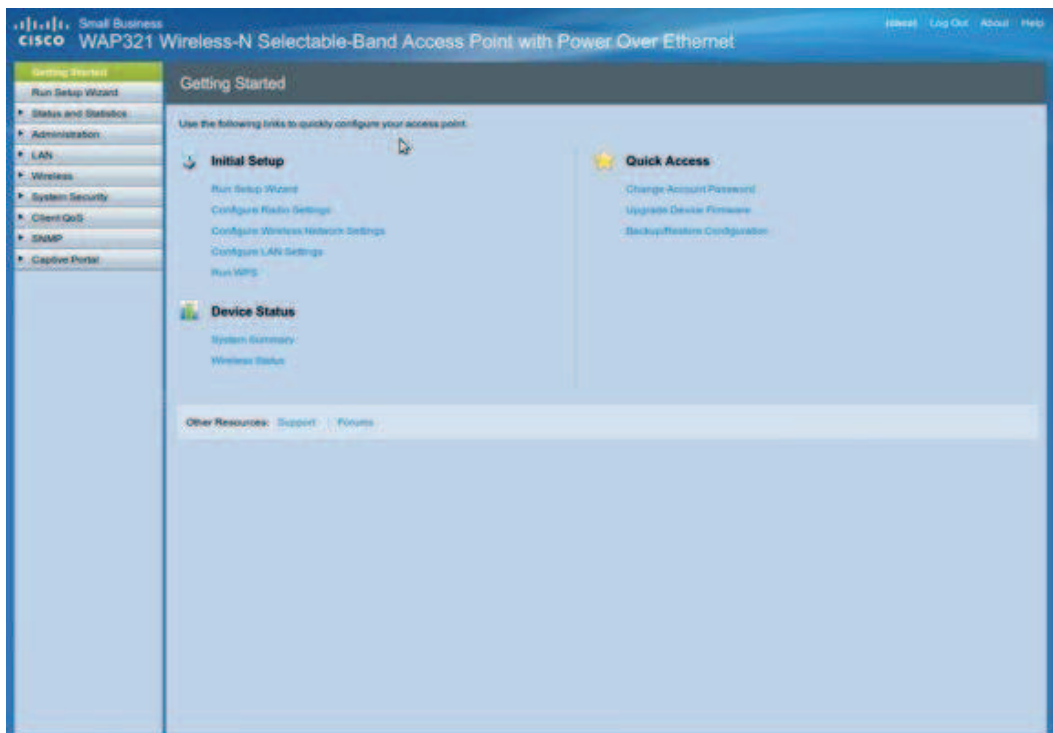
**PASO4** En el campo Dirección, ingrese la dirección de DHCP predeterminada y presione la tecla Enter (Intro).



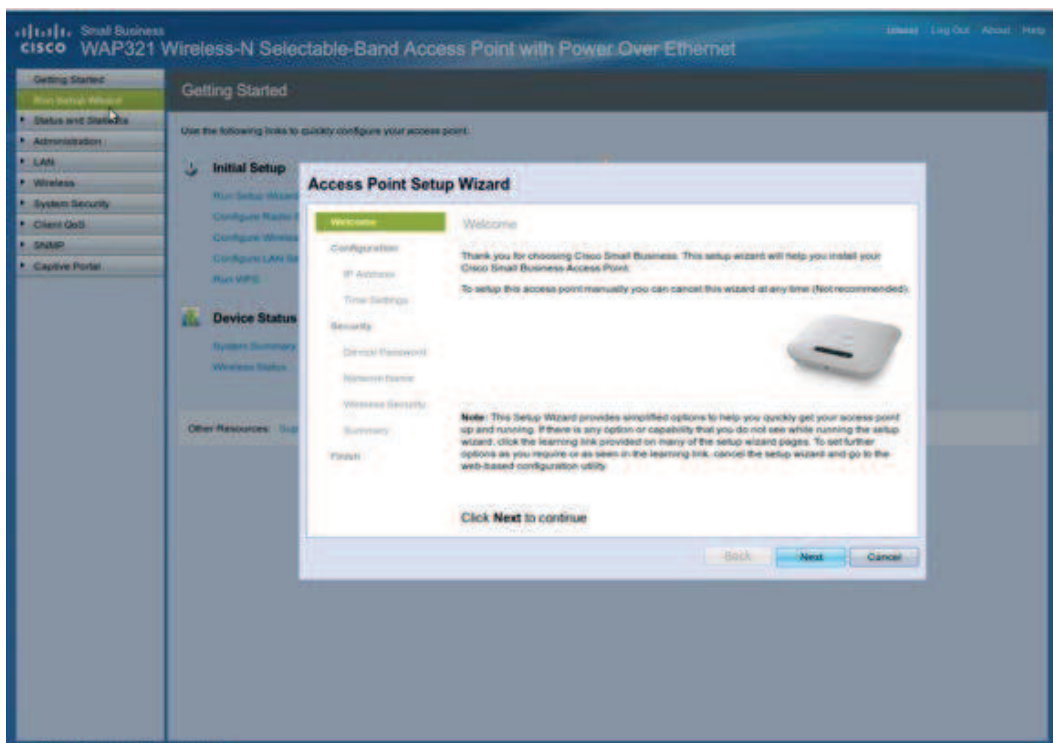
**PASO5** Ingrese el nombre de usuario predeterminado de cisco y la contraseña de cisco en los campos Nombre de usuario y Contraseña.



**PASO6** Haga clic en Login (Iniciar sesión). Aparecerá el Asistente de configuración del punto de acceso inalámbrico.



**PASO7** Siga las instrucciones de dicho asistente para finalizar la instalación del dispositivo WAP. Para configuraciones más avanzadas, vea la Guía de administración.



## **Pasos siguientes sugeridos**

En caso de que aparezca algún error durante la instalación, pruebe los siguientes procedimientos de resolución de problemas:

### **Resolución de problemas**

En caso de que no pueda ver la utilidad de configuración, puede probar la capacidad de la computadora para comunicarse con el dispositivo mediante el comando ping. Para usar el comando ping en una computadora que ejecute Windows:

**PASO1** Verifique que Cisco WAP321 esté encendido y que las luces indiquen los enlaces apropiados.

**PASO2** Localice la dirección IP del dispositivo. Aunque existen diferentes formas de localizar la dirección IP del dispositivo, este procedimiento utilizará Cisco FindIT.

- a. Si usted ya ha descargado Cisco FindIT, abra Mozilla Firefox e inicie Cisco FindIT. Para obtener más información sobre la descarga de Cisco FindIT, visite [www.cisco.com/go/findit](http://www.cisco.com/go/findit).
- b. En la pantalla de Cisco FindIT, coloque el mouse sobre el nombre del dispositivo. La dirección IP del dispositivo aparece junto con el resto de la información del dispositivo.

**PASO3** Abra una ventana de comando al utilizar Start (Inicio) > Run (Ejecutar) y escriba cmd.

**PASO4** En la ventana Command (Comando), escriba ping y la dirección IP del dispositivo. En este ejemplo, nosotros hicimos ping en 192.0.2.10. Si tuvo éxito, usted debería obtener una respuesta similar a la siguiente: Pinging

192.0.2.10 with 32 bytes of data: Reply from 192.0.2.10: bytes=32 time<1ms TTL=128 Si falla, usted debería obtener una respuesta similar a la siguiente: Pinging 192.0.2.10 with 32 bytes of data: Request timed out.

### **Posible causa de falla**

#### **Sin alimentación**

- Encienda el switch y la computadora si están apagados.
- Si el punto de acceso está utilizando PoE, asegúrese de que el switch PoE esté encendido y que las luces indiquen que el enlace existe. Consulte “Verificación de la instalación del hardware”
- Verifique que el botón de encendido esté activado; solo se aplica si no está usando PoE.
- Verifique que los dispositivos de la red no estén enchufados en una salida de switch.

#### **Mala conexión Ethernet**

- Controle el estado de las luces del indicador. Consulte “Verificación de la instalación del hardware” en la página 80.
- Revise los conectores del cable Ethernet para asegurarse de que estén firmemente conectados al switch y a la computadora.



- Verifique que el switch conectado tenga la negociación automática habilitada. El punto de acceso y el switch necesitan el mismo conjunto de parámetros de negociación.

### **Mala imagen**

Después de una nueva instalación de firmware, si la luz de encendido parpadea rápidamente, comuníquese con Asistencia técnica de sistemas.

### **Dirección IP incorrecta**

La causa más probable de falla de conectividad es una dirección IP incorrecta. El explorador web puede estar apuntando a la dirección IP errónea o la computadora podría estar configurada con una dirección IP que no está en la misma subred que el dispositivo.

Debido a que la configuración de dirección IP predeterminada de fábrica es DHCP, asegúrese de que el servidor DHCP esté funcionando y que pueda alcanzarse. Es posible que deba desconectar y volver a conectar los dispositivos para que detecten las nuevas direcciones IP del servidor DHCP. Luego puede enviar una consulta al servidor DHCP para obtener la nueva dirección IP. Consulte Paso 2 de “Inicio de la configuración” en la página 85 para obtener más información sobre cómo encontrar la dirección DHCP.

Si los puntos de acceso inalámbrico no reciben una respuesta del DHCP (no existe ningún servidor de DHCP en su red) después de 60 segundos, los puntos de acceso se reservarán en la siguiente dirección IP estática predeterminada. 192.168.1.245 con una máscara predeterminada de 255.255.255.0. Para llegar a esa dirección IP, asegúrese de que la computadora esté en la red 192.168.1.xxx.

**Reinicio de los dispositivos o retorno a las configuraciones predeterminadas de fábrica Para reiniciar el dispositivo:**

- Si el dispositivo usa un adaptador de energía, use el botón de encendido para reiniciarlo. El botón de encendido solo funciona cuando el dispositivo usa un adaptador de energía.
- Desconecte la conexión Ethernet durante tres segundos y vuelva a conectarla.
- Si el dispositivo usa PoE, con la energía encendida, presione el botón de reinicio con un sujetapapeles doblado durante menos de tres segundos o hasta que las luces se apaguen.
  - Cuando todas las luces se apaguen, suelte el botón de reinicio.
  - Suelte el botón de reinicio apenas se hayan apagado las luces o las configuraciones predeterminadas de fábrica se restaurarán y perderá sus configuraciones.

Para reiniciar el dispositivo a las configuraciones predeterminadas de fábrica:

- Para restaurar las configuraciones predeterminadas de fábrica del dispositivo, con la energía encendida, presione y mantenga presionado el botón de reinicio con un sujetapapeles doblado durante más de 10 segundos.
  - Todas las luces se apagarán.
  - Suelte el botón de reinicio cuando la luz de encendido se active.

## **3.5. CONCLUSIONES Y RECOMENDACIONES**

### **3.5.1 CONCLUSIONES:**

1. La evolución tecnológica en dispositivos de conexión inalámbrica, han modificado los métodos de trabajo personal y empresarial, ya que presentan facilidades en la movilidad de la información, facilidad de instalación, flexibilidad y comodidad, de ahí la necesidad de contar con una red inalámbrica a través de un Access Point en el laboratorio de redes la Carrera de Sistemas.
2. Las redes inalámbricas constituyen la alternativa más viable para extender una red tradicional a lugares donde las conexiones físicas no lo permitan. La investigación realizada permitió determinar la tendencia de crecimiento y la amplitud de aplicaciones que tienen las redes inalámbricas en los procesos de enseñanza-aprendizaje e interconexión de redes.
3. Al implementar una red inalámbrica a través de un Access Point Cisco WAP 321, es necesario tener en cuenta los estándares y tecnologías actuales, que permitan optimizar dinero y tiempo pero sobre todo logrando y evitando problemas de incompatibilidad de hardware y/o software.
4. El IEEE es el cuerpo estandarizador para las TICs, en relación a la implementación del Access Point Cisco WAP 321, es necesario enfocarse y aplicar la estandarización IEEE 802.11 que es la familia de los estándares para “Ethernet Inalámbrica”.

### 3.5.2. RECOMENDACIONES

1. Se recomienda no sustituir las redes tradicionales (alámbricas), por las redes inalámbricas (WLAN), ya que éstas constituyen únicamente un complemento.
2. Se deben adquirir los equipos necesarios para una conexión inalámbrica, en nuestro caso para una WLAN de una misma casa fabricante, ya que pese a que existen normas básicas preestablecidas, no nos garantizan la compatibilidad entre equipos de diferentes casas fabricantes, para nuestro caso CISCO.
3. Es necesario analizar y seleccionar cual es el sistema de red local inalámbrica más conveniente a implantar, para así poder identificar con claridad factores tales como ancho de banda y velocidad de transferencia necesarios, número de usuarios e intensidad de uso, limitaciones geográficas (radio cobertura, existencia de paredes y ventanas, ubicación y alimentación de puntos de acceso, etc.), atención de dispositivos móviles con posibilidades de relevo entre puntos de acceso, presupuesto disponible y así seleccionar equipos que satisfagan las necesidades de la aplicación.
4. Las claves de ingreso al Access Point que tienen por defecto deben ser cambiadas, puesto que la mayoría de marcas del mercado vienen con las mismas para todos los modelos, con lo cual se puede acceder a cualquiera de ellos, haciendo un acceso remoto a la red y poniéndolas en riesgo a la misma.
5. Es necesario por seguridad e incremento de la vida útil de los dispositivos apagar y desconectar la línea de alimentación de energía cuando los tiempos de inactividad son prolongados.
6. Se recomienda por lo menos aplicar una política de seguridad WEP con cifrado de 128 bits hexadecimal.

## BIBLIOGRAFÍA

### CONSULTADA

- **KENDAL & KENDAL**, “Análisis y Diseño de Sistemas”, Tercera Edición.
- **Hacker Friendly LLC (2008)**, <http://hackerfriendly.com/>,”Redes Inalámbricas en los países de desarrollo”, Tercera edición
- **Bruce Alexander**, “Wireless Network Site Surveying and Installation, 802.11., Cisco Press. ISBN #1-587-05164-8
- **Tanenbaum Andrew S**, (2002), “**Computer Networks.**”, ISBN 0130661023, Clásico en redes de computadoras en general.
- **Rob Flickenger**, “Implementación de redes inalámbricas”, Building Wireless Community Networks, Publicado: O'Relly; Segunda edición (Junio de 2003), ISBN: 0-596-00502-4
- **Javier Espín del Pozo y José Luis Ruiz Ludeña** (2009), “Topologías-red2”, <http://www.monografias.com/trabajos53/topologias-red/topologias-red2.shtml>.

### CITADA.

- **Sebastian Buettrich** wire.less.dk, Alberto Escudero Pascual - IT +46 Traducido por Colnodo, “Topología e Infraestructura Básica de Redes Inalámbricas”, TRICALCAR, [www.wilac.net/tricalcar](http://www.wilac.net/tricalcar) – Versión final. Octubre 2007.

- **Ing. Luis Alvarado Cáceres (2013)**, “Manual Redes de Computadora”, [http://yoprofesor.ecuadorsap.org/wp-content/uploads/2013/05/manual\\_redes.pdf](http://yoprofesor.ecuadorsap.org/wp-content/uploads/2013/05/manual_redes.pdf) - Ultimo acceso 27 abril 2014, 11:48 A.M.
- **Luis Tarazona DIP UNEXPO Barquisimeto (2004)**, ELT-51123 “Redes de computadora, el hardware y el software detrás de la Tecnología de la información”,[http://www.el.bqto.unexpo.edu.ve/~ltarazona/redes/redesc01\\_2.pdf](http://www.el.bqto.unexpo.edu.ve/~ltarazona/redes/redesc01_2.pdf) - Ultimo acceso 27 abril 2014, 12:20 P.M.
- José María Barceló Ordinas, Jordi Íñigo Griera, Ramon Martí Escalé, Enric Peig Olivé y Xavier Perramon Tornil (2004), “Software Libre”, Primera edición: marzo 2004, Fundació per a la Universitat Oberta de Catalunya,[http://ocw.uoc.edu/computer-science-technology-and-multimedia/computer-networks/computer-networks/XP06\\_M2105\\_01496.pdf](http://ocw.uoc.edu/computer-science-technology-and-multimedia/computer-networks/computer-networks/XP06_M2105_01496.pdf) - Ultimo acceso 27 abril 2014, 15:45 P.M
- **Lilian Chamorro y Ermanno Pietrosevoli (2008)**, Asociación para el progreso de las comunicaciones (APC), “Redes inalámbricas para el desarrollo en América Latina y el Caribe”, Temas Emergentes Serie (2008),[https://www.apc.org/es/system/files/APC\\_RedesInalambricasParaElDesarrolloLAC\\_20081223.pdf](https://www.apc.org/es/system/files/APC_RedesInalambricasParaElDesarrolloLAC_20081223.pdf) - Ultimo acceso 27 abril 2014, 15:39 P.M.
- **Eramis BUENO SÁNCHEZ (2003)**, “La Investigación Científica Teoría y Metodología”, Universidad Autónoma de Zacatecas, Unidad Académica de Ciencias sociales, <http://exordio.qfb.umich.mx/archivos%20pdf%20de%20trabajo%20umsh/LIBROS%2014/libmetod.pdf> - Ultimo acceso 27 abril 2014, 18:43 P.M.

## **VIRTUAL**

### **Redes inalámbricas a través de Access Point**

- <http://clubensayos.com/imprimir/Tesis-De-RedesInalambricas/717.html>- Ultimo acceso 20 de junio 2013, 19:53 P.M.
- [http://www.univo.edu.sv:8081/tesis/018116/018116\\_Cap5.pdf](http://www.univo.edu.sv:8081/tesis/018116/018116_Cap5.pdf) - Ultimo acceso 20 de junio 2013, 19:55 P.M
- <http://bibdigital.epn.edu.ec/bitstream/15000/4390/1/CD-4002.pdf> - Ultimo acceso 7 de junio 2013, 16h27 P.M.
- [http://www.innetrex.com/wireless\\_install.php](http://www.innetrex.com/wireless_install.php) - Ultimo acceso 16 de abril 2014, 20h20 P.M.
- <http://redesinalambricasfacci.files.wordpress.com> - Ultimo acceso 16 de abril 2014, 20h45 P.M.

## **NORMATIVA LEGAL**

- Constitución de la República del Ecuador 2008, Corporación de Estudios y Publicaciones, actualizada a mayo del 2012
- Ley Organiza de Educación Superior.

**ANEXO 1.** Manual Administrativo de Configuración Access Point CISCO WAP321.

**ANEXO 2.** Encuesta dirigida a alumnos de la Carrera de Ingeniería en Informática y Sistemas Computacionales.





## UNIVERSIDAD TÉCNICA DE COTOPAXI

UNIDAD ACADÉMICA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

### CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

#### ENCUESTA

La presente encuesta tiene como objetivo conocer la opinión que tienen los estudiantes de la Carrera de Informática y Sistemas computacionales en relación a la **IMPLEMENTACIÓN Y CONFIGURACIÓN DE UNA RED INALÁMBRICA A TRAVÉS DE ACCESS POINT**.

Esperamos su colaboración, respondiendo con sinceridad el presente cuestionario, recuerde que la encuesta es anónima. Lea usted con atención y conteste a las preguntas con un "X" en una sola alternativa.

1. ¿Está usted de acuerdo con que se implemente y configure un laboratorio de práctica de redes en la Carrera de Informática y Sistemas Computacionales de la Universidad Técnica de Cotopaxi a través de dispositivos tecnológicos modernos para el estudio práctico de la materia?  
 Si                       No
2. ¿El uso de dispositivos tecnológicos nuevos en el laboratorio de redes permitirá que el estudio de la informática y sistemas computacionales, amplíe y ponga en práctica los conocimientos teóricos adquiridos?  
 Si                       No
3. ¿Los procesos de enseñanza aprendizaje son adquiridos de mejor forma a través de las prácticas de laboratorio bajo un ambiente real y de desempeños auténticos?  
 Si                       No
4. ¿El uso de tecnologías Wireless permitirá que los conocimientos adquiridos se desenvuelvan en ambientes reales acorde a los avances tecnológicos y su adaptación a la evolución informático?  
 Si                       No
5. ¿Está usted de acuerdo con que se implemente y configure una red inalámbrica a través de Access Point?  
 Si                       No
6. ¿Es necesario contar con una memoria técnica y/o guía de instalación y configuración de un **ACCESS POINT CISCO WAP321** (configuración de un solo punto)?  
 Si                       No
7. ¿La implementación y configuración de una red inalámbrica a través de Access Point permitirá interconectar las redes y asegurar el enrutamiento de los paquetes de información entre redes?  
 Si                       No
8. ¿Considera usted que la implementación y configuración de una red inalámbrica para los procesos prácticos de enseñanza aprendizaje, mejoraría el nivel académico de los estudiantes de Ingeniería en Informática y Sistemas Computacionales?  
 Si                       No

**GRACIAS POS SU COLABORACIÓN**