AUTORES:

Apellidos: Jiménez Bonilla. Nombres: Zully del Carmen.

Apellidos: Leaño Suárez. Nombres: Carlos Eduardo.

TÍTULO:

Redes Inalámbricas: Diseño e Implementación

CIUDAD:

Cartagena de Indias.

AÑO DE ELABORACIÓN:

2011

NÚMERO DE PÁGINAS:

65

INSTITUCIÓN:

Universidad Tecnológica de Bolívar.

FACULTAD:

Facultad de Ingeniería.

PROGRAMA:

Ingeniería de Sistemas.

TÍTULO OBTENIDO:

Ingeniero(a) de Sistemas

REDES INALÁMBRICAS: DISEÑO E IMPLEMENTACIÓN

ZULLY del CARMEN JIMÉNEZ BONILLA
CARLOS EDUARDO LEAÑO SUÁREZ

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SEMESTRE II DE 2011
CARTAGENA DE INDIAS

REDES INALÁMBRICAS: DISEÑO E IMPLEMENTACIÓN

ZULLY del CARMEN JIMÉNEZ BONILLA
CARLOS EDUARDO LEAÑO SUÁREZ

TRABAJO DE GRADO PARA OPTAR AL TÍTULO DE INGENIER(A) DE SISTEMAS

ISAAC ZÚÑIGA
DOCENTE TIEMPO COMPLETO UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SEMESTRE II DE 2011
CARTAGENA DE INDIAS

Nota de aceptación:

_____
_____
_____
_____
_____

_____

Firma del lector y tutor

Un trabajo dedicado a la familia, docentes y tutores
Quienes siempre nos han hecho ver todo
Posible…

ÍNDICE

Objetivos

Mostrar y analizar las tecnologías y estándares de configuración de redes inalámbricas, los dispositivos de conexión y las principales configuraciones de este tipo de soluciones.

Objetivos Específicos.

- Identificar los tipos de enlaces para la implementación de redes inalámbricas.
- Conocer las familias de estándares 802.11 (WLAN) y 802.15 (WPAN) y las aplicaciones en las organizaciones y en el hogar.
- Implementar y administrar la seguridad en redes inalámbricas.
- Elaborar un manual didáctico de implementación de redes inalámbricas.
- Comprender los aspectos relativos a la seguridad en redes inalámbricas y sus soluciones.
- Analizar el estándar 802.11n y sus ventajas

Breve descripción del problema

El tema principal es el diseño y la implementación de una red inalámbrica, dándole mayor enfoque al estándar **802.11n**, también conocido como **Wifi N**, y comprobar de esta manera la utilidad y eficiencia que se obtiene al utilizar el medio inalámbrico para nuestras comunicaciones.

Destacando también como con el paso del tiempo lo inestable de las redes inalámbricas hoy en día se está volviendo el común denominador del mercado de las telecomunicaciones.

Justificación

Así cómo pasa el tiempo, así de rápido van avanzado las investigaciones y los cambios que se van reflejando en el mundo de las telecomunicaciones son sorprendentes, por tal motivo, la investigación se encuentra enfocada hacia el rumbo y las tendencias de las Redes Inalámbricas enfocándonos en el diseño y la implementación de las misma, para poder aclarar muchas de las dudas y mitos que sobre estas existen.

Como también analizar e identificar el estándar **802.11n, su objetivo, sus ventajas y desventajas y los cambios que este ha generado en el concepto de red inalámbrica.**

Con una adecuada implementación de una configuración inalámbrica, las personas, medios o espacios, acortan distancias y establecen una conexión estable y segura, que brindara confiablidad a los usuarios que forman parte de la red.

Con la siguiente investigación, se aterrizan las funcionalidades para la configuración de una red inalámbrica, previamente implementadas en una sección de pruebas realizadas en los laboratorios de redes.

Metodología

La metodología utilizada paras el desarrollo de este trabajo de grado fue la siguiente:

Siguiendo una línea de seguimiento donde el primer paso fue la investigación de textos científicos (Papers, Libros Temáticos), procediendo a Documentas la bibliografía encontrada, para ponerla en práctica y finalizar con la retro alimentación del tutor.

Resaltando que en cualquier momento se podía interrumpir el proceso y regresar al paso anterior.

Estado del arte de las redes inalámbricas

1. Evolución

Desde los años 70 se vienen haciendo experimentos para lograr la conexión entre dispositivos de manera inalámbrica, pero fue en 1979 cuando la gente de IBM publicó los resultados de sus experimentos de conexión inalámbrica mediante infrarrojos en una fábrica suiza[1], este estudio se consideró como el punto de partida de las redes inalámbricas.

De ahí en adelante los estudios realizados en este campo fueron hechos utilizando altas frecuencias y fue cuando el FCC[2] asignó las bandas IMS[3] de 902 – 928 MHz, 2,4– 2,4835 GHz y 5,725 – 5,850 GHz a las redes inalámbricas basadas en Spread Spectrum[4]. Al hacerse la asignación de bandas de frecuencias, se vio favorecida la actividad en las empresas, ya cuando se tuvo este respaldo las redes inalámbricas empezaron a llegar a otros lados diferentes de los laboratorios, e iniciaron el camino hacia el mercado.

Entre 1985 y 1990 se realizaron trabajos de investigación más que todo orientados a la parte de desarrollo, hasta que en el año de 1991 se publicaron trabajos referentes a redes inalámbricas operativas cuya velocidad era un poco

[1] Volumen 67, Issue 11 de los IEEE Proceeding (Wireless in-house data communication via diffuse infrared radiation) pags.1474-1486.
[2] FCC, Federal Communication Comission, entidad encargada de regular y administrar en materia de telecomunicaciones en EE.UU.
[3] IMS, Industrial, Scientific and Medical. Es una banda para uso comercial sin licencia.
[4] Técnica de modulación empleada en telecomunicaciones para la transmisión de datos, por radiofrecuencia y digitales.

mayor de 1Mbps, el cual era el mínimo establecido por la IEEE 802 para que la red sea considerada una LAN.

Las ondas de radio fueron usadas de otra forma para crear lo que se conoce como Bluetooth[5] que eran ondas de radio corta, la ventaja de estos dispositivos es que requieren de poca energía para su funcionamiento. A pesar de que estas redes inalámbricas simplificaban la vida cotidiana siempre estaba presente la restricción de la distancia, para resolver esto se creó un nuevo estándar de conexión también usando ondas de radio llamado WiMAX[6] el cual permite la operatividad a grandes distancias (50 - 60 Km) y altas velocidades de transmisión de datos (superiores a 20Mbps).

Redes Inalámbricas Hoy Día

Actualmente las redes inalámbricas juegan un papel importante en el día a día de las personas, debido al creciente mercado de computadoras portátiles la necesidad de conectarse no solo a internet sino también estar en red con otras personas sin necesidad de cables ha ido aumentando debido a que muchos dependen de esto para realizar las actividades de su vida cotidiana (revisar el correo electrónico, buscar información para informes u otras asignaciones), ya que se puede dar el caso de que la actividad que las personas realizan no sea dentro de una oficina sino que le demande el estar desplazándose de un lugar a otro y

[5] Es una tecnología de ondas de radio de Corto Alcance, cuyo objetivo es simplificar las conexiones entre dispositivos informáticos.
[6] WiMAX, Worldwide Interoperability for Microwave Access

para eso necesitan el acceso a internet de una forma sencilla y sin la “atadura” de estar conectados mediante un cable.

En sus inicios, las redes inalámbricas eran de difícil acceso para todo el mundo por el alto costo que representaba el instalar un punto de acceso a la red, pero gracias a la evolución que ha ido teniendo la tecnología en el campo de dispositivos para facilitar la conexión inalámbrica ahora es común encontrar acceso a redes inalámbricas en lugares claves[7] y de forma gratuita.

En el mundo, existen muchas formas de conexión inalámbrica siendo la de radiofrecuencia la más popular ya que usa el estándar 802.11 de la IEEE, otra tecnología que también viene siendo muy usada es el Bluetooth ya que no solo los computadores la tienen sino que otros dispositivos ya cuentan con ella, como es el caso de los celulares, mouse, micrófonos, teclados, entre otros. La conexión mediante Bluetooth es usada con estos dispositivos ya que requiere poca energía para su funcionamiento.

Hoy en día, las redes inalámbricas son usadas en todas partes y hacen parte vital de la estructura de comunicaciones e informática de una empresa u organización, lo que se busca con ellas no es reemplazar las redes cableadas sino que son utilizadas como complemento de estas ya que hay lugares en donde estas no pueden tener acceso y debido a la facilidad de instalación de dispositivos para la conexión a la red los cuales ya funcionan con PoE[8].

[7] En Cartagena encontramos varios Puntos de Acceso públicos, uno de ellos es en el C.C Caribe Plaza, otro se encuentra ubicado en el centro de la ciudad en la plaza San Pedro Claver y otro en el Aeropuerto Rafael Núñez.
[8] PoE es Power over Ethernet, es decir, para que el dispositivo funcione no es necesario que este se conecte a la corriente debido a que el mismo cable le brinda la energía necesaria para que este funcione.

Otra aplicación de las redes inalámbricas es cuando se presenta el caso de la reconfiguración la topología de la red sin añadir costos adicionales, esta es una solución muy usada en entornos cuyo cambio es constante y los cuales necesitan de una estructura de red flexible que pueda adaptarse a los cambios que se vayan presentando.

2. ¿Que se está haciendo hoy en día con las redes inalámbricas y como se está haciendo?

El protocolo de conectividad inalámbrica WiFi no se encuentra estático y ya presenta una nueva versión que la IEEE ha liberado con la denominación 802.11n[9] la cual trae consigo la solución a una de las desventajas más grande de la tecnología WiFi y es el **aumento de la velocidad de conexión inalámbrica a una velocidad de 300**[10] **Mbps con un** alcance 70 metros interior, lo que hace más óptima y eficaz la conexión, si la comparamos con la velocidad de conexión del estándar 802.11g establecido en 54 Mbps

Las principales características promocionales del 802.11n son:

- MIMO (Multi-In, Multi-Out) generando canales de trafico simultáneos entre las diferentes antenas de los productos 802.11n.
- Canales de 20 y 40 Hz, los cuales permiten el incremento de la velocidad.

[9] http://www.tecnologiapyme.com/actualidad/aprobado-el-estandar-80211n-para-redes-inalambricas

[10] **300 Mbps.** Versión borrador, la versión final se espera que marque los **600 Mbps** como velocidad máxima posible.

- El uso de las bandas de 2,4 y 5 GHz simultáneamente, con esto se disminuirán los problemas ocasionados por las interferencias en la banda 2,4 GHz, y optimizara el uso de las bandas.

Tipos de tecnología Wi-Fi[11]:

Tecnología Wi-Fi	Banda de frecuencia	Máximo de ancho de banda o velocidad de datos
802.11a	5 GHz	54 Mbps
802.11b	2.4 GHz	11 Mbps
802.11g	2.4 GHz	54 Mbps
802.11n	**2,4 GHz, 5 GHz, 2,4 o 5 GHz (seleccionable), o 2,4 y 5 GHz (concurrente)**	450 Mbps

"El IEEE (Institute of Electrical and Electronics Engineers) está estudiando dos posibles tecnologías que podrían lograr que las conexiones WiFi alcanzaran velocidades Gigabit en 2012." Tomado de Revista **PC WORLD Digital**[12]

[11] http://www.wi-fi.org/certified_products.php
[12] http://www.idg.es/pcworld/

La tendencia de las redes inalámbricas apunta hacia la movilidad sin límites de espacio, es decir, que casi todo el territorio este cobijado de una buena cobertura, acompañada de seguridad y un canal con velocidad ilimitada.

3. *Presente – Futuro: Problemas Actuales*

DESVENTAJAS DE LAS REDES INALÁMBRICAS

A la hora de comparar las redes inalámbricas con las redes de alambicas encontramos que existen ciertos puntos en contra de las redes inalámbricas, los principales inconvenientes son:

Velocidad[13]: Las redes inalámbricas Wi-Fi[14] trabajan a 11 Mbps, pero existen estándares que alcanzan los 54 Mbps y soluciones propietarias que llegan a 100 Mbps, pero estos estándares están en los comienzos de su comercialización y tiene un precio superior al de los actuales equipos Wi-Fi; mientras que las redes cableadas ya llegaron hace unos cuantos años a los 100 Mbps.

Seguridad[15]: Las redes inalámbricas tienen la particularidad de no necesitar un medio físico para funcionar. Muchas redes Wi-Fi sufren accesos no debidos, gracias a la inexperiencia de quienes las instalaron y no configuraron correctamente los parámetros de seguridad, trayendo esto como consecuencia, que cualquier persona con dispositivos de menor jerarquía, como por ejemplo

[13] http://www.redsinfronteras.org/pdf/redes_wireless.pdf
[14] *Wireless Fidelity o* IEEE 802.11, es un sistema de envío de datos sobre redes computacionales que utiliza ondas de radio en lugar de cables.
[15] http://www.redsinfronteras.org/pdf/redes_wireless.pdf

Palms, PDA o pequeños dispositivos portátiles, solo necesita estar dentro del área de cobertura de la red para poder intentar acceder a ella.

Propensión a interferencias[16] **:** Las redes inalámbricas funcionan utilizando el medio radio electrónico en la banda de 2,4 GHz; Esta banda de frecuencias 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.

Esto trae como consecuencia que no se cuente con una frecuencia completamente limpia para que la red inalámbrica funcione a su más alto rendimiento. Cuantos mayores sean las interferencias producidas por otros equipos, menor será el rendimiento de la red. Aclarando que, el hecho de tener probabilidades de sufrir interferencias no quiere decir que se tengan. La mayoría de las redes inalámbricas funcionan perfectamente sin mayores problemas en este sentido.

Incertidumbre tecnológica[17]. La tecnología que actualmente se está instalando y que ha adquirido una mayor popularidad es la conocida como Wi-Fi. Sin embargo, ya existen tecnologías que ofrecen una mayor velocidad de transmisión y unos mayores niveles de seguridad, es posible que, cuando se acredite esta nueva tecnología, se deje de utilizar la actual.

Los productos que salen al mercado están marcados por las necesidades del cliente y, aunque existan incógnitas o dudas con respecto al uso de los que ya

[16] http://www.redsinfronteras.org/pdf/redes_wireless.pdf
[17] http://www.todo-linux.com/manual.todo-linux.com/redes/Manual%20redes%20inalambricas.pdf

están comercializados, los fabricantes no querrán perder el impulso que ha impuesto Wi-Fi y harán todo lo posible para que los nuevos dispositivos sean compatibles con los actuales.

Otros inconvenientes que presentan las redes inalámbricas son:

- Los puntos de acceso gratis podrían ser usados para robar información personal por usuarios maliciosos de la red Wi-Fi.
- La interoperabilidad entre marcas o desviaciones en los estándares puede causar limitaciones a las conexiones o bajar las velocidades de transmisión.

Enlaces para la implementación de redes inalámbricas.

Sabemos que 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[18] siempre es en dos sentidos (bidireccional), pero sabemos que 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.

Las redes inalámbricas son organizadas en estas tres configuraciones lógicas:

- Enlaces punto a punto
- Enlaces punto a multipunto
- Nubes multipunto a multipunto

Enlace Punto A Punto[19]

Este tipo de enlace son las que responden a un tipo de arquitectura de red en las que cada canal de datos se usa para comunicar únicamente dos nodos, los dispositivos en red actúan como socios iguales, o pares entre sí. Como pares,

[18] http://www.cybercom-cw.com.ar/pdf/Cybercom_WLAN_Paper.PDF
[19] http://www.cika.com/newsletter/archives/pp1.pdf
http://efrentelecom.com/enlaces%20punto%20a%20punto.pdf

cada dispositivo puede tomar el rol de esclavo o la función de maestro. En un momento, el dispositivo A, por ejemplo, puede hacer una petición de un mensaje/dato del dispositivo B, y este es el que le responde enviando el mensaje/dato al dispositivo A y viceversa.

Por ejemplo:

Una empresa puede tener una conexión *Frame Relay* [20]o una conexión VSAT[21] dentro de la sede1, pero difícilmente podrá justificar otra conexión de la misma índole a un edificio muy importante fuera de la sede. Si el Nodo 1 tiene una visión libre de obstáculos al Nodo 2, una conexión punto a punto puede ser utilizada para unirlos. Ésta puede complementar o incluso remplazar enlaces discados existentes.

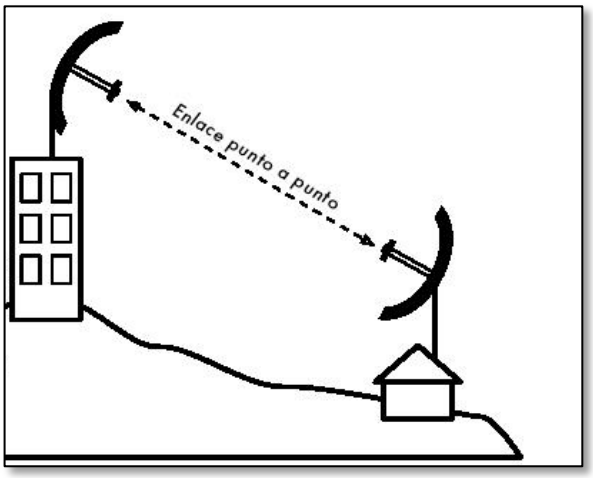


Figura1[22].: Enlace Punto a Punto

[20] Tecnología de conmutación rápida de tramas, basada en estándares internacionales, que puede utilizarse como un protocolo de transporte y como un protocolo de acceso en redes públicas o privadas proporcionando servicios de comunicaciones.

[21] (Very Small Aperture Terminals) son redes privadas de comunicación de datos vía satélite para intercambio de información punto-punto o, punto-multipunto (broadcasting) o interactiva.

[22] http://www.eslared.org.ve/tricalcar/04_es_topologia-e-infraestructura_guia_v02%5B1%5D.pdf

Utilizando el hardware adecuado se pueden hacer enlaces punto a punto seguros de más de treinta kilómetros.

Enlaces Punto A Multipunto[23]

El enlace Punto a Multipunto es donde varios nodos están hablando con un punto de acceso central, este tipo de enlace es ideal para locaciones gubernamentales, municipalidades, operadores e ISPs los cuales puede utilizar redes inalámbricas que cubren toda la ciudad. Es también recomendable para campus universitarios y empresas con numerosas edificaciones dispersadas sobre un área de tamaño significativo.

El enlace Punto a Multipunto puede funcionar como un segmento principal de red de banda ancha para hots, outdoor access points y switches DSL. Las compañías de telecomunicaciones encontrarán al enlace Punto a Multipunto atractivo porque puede ser usado para distribuir redes de fibra óptica y actuar como segmento principal de red de banda ancha para switches and routers DSL.

Hay diferentes tipos de conexiones punto a multipunto:

- *Estrella*: Un host conectado a varias terminales remotas.
- *Bus*: Un medio de comunicación común conectado a muchas estaciones remotas.
- *Anillo*: Todas las terminales conectadas a un mismo cable. Si una falla hay problemas con todas.

[23] http://www.ehas.org/uploads/file/difusion/academico/PFC/MarcBanhos_PFC.pdf

- *Malla*: Es el tipo de conexión utilizado en las centrales telefónicas. Todas las terminales interconectadas entre sí.

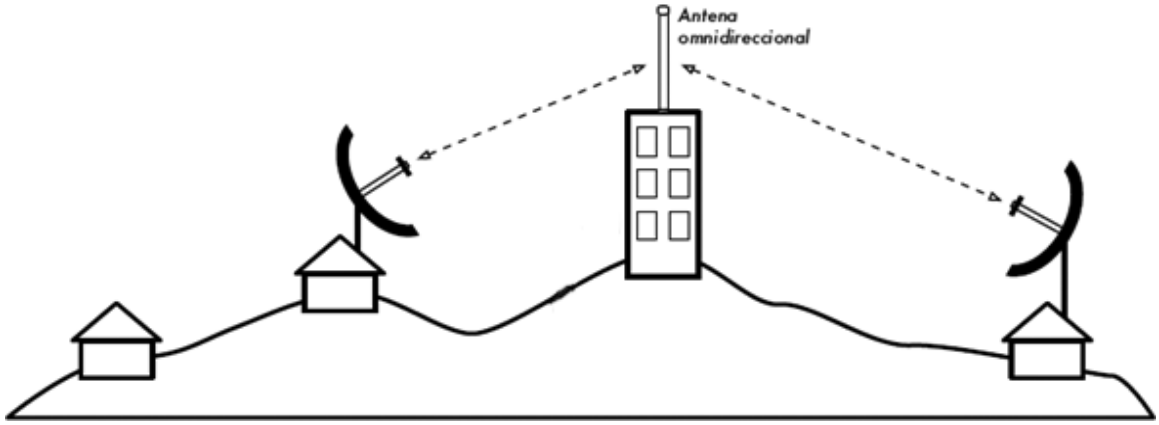


Figura 2. : Enlace Punto A Multipunto

Multipunto A Multipunto[24]

La red multipunto a multipunto, el cual también es denominado red **ad hoc** o en malla (**mesh**). En una red multipunto a multipunto, no hay una autoridad central. Cada nodo de la red transporta el tráfico de tantos otros como sea necesario, y todos los nodos se comunican directamente entre sí.

El beneficio de este diseño de red es que aún si ninguno de los nodos es alcanzable desde el punto de acceso central, igual pueden comunicarse entre sí. Las buenas implementaciones de redes **mesh** son auto-reparables, detectan automáticamente problemas de enrutamiento y los corrigen. Extender una red **mesh** es tan sencillo como agregar más nodos. Si uno de los nodos en la "nube" tiene acceso a Internet, esa conexión puede ser compartida por todos los clientes.

24 http://ingeborda.com.ar/biblioteca/Biblioteca%20Internet/Articulos%20Tecnicos%20de%20Consulta/Redes%20de%20Datos/Diseno%20de%20Redes%20Inalambricas.pdf

Dos grandes desventajas de esta topología son el aumento de la complejidad y la disminución del rendimiento. La seguridad de esta red también es un tema importante, ya que todos los participantes pueden potencialmente transportar el tráfico de los demás. La resolución de los problemas de las redes multipunto a multipunto tiende a ser complicada, debido al gran número de variables que cambian al moverse los nodos.

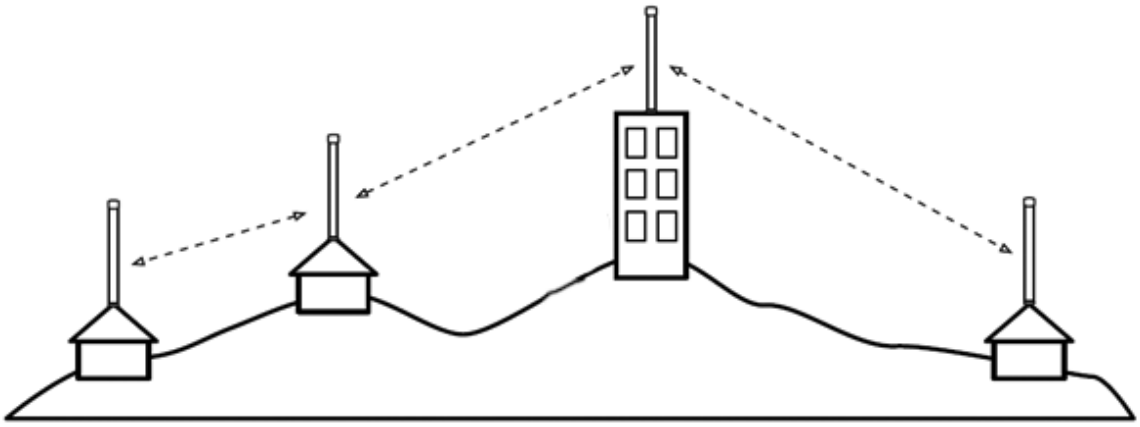


Figura 3.: Enlace Multipunto a Multipunto

Protocolo de Comunicación: TCP/IP

Con las diferentes tipos de enlaces vistos anteriormente, se puede montar, diseñar o estructura redes de gran tamaño, y utilizando una mezcla de cada tipo de enlace, sin olvidar que para entablar una comunicación entre las redes, es decir entre los ordenadores estaba a estar sujeta a un **Protocolo**[25]**,** el modelo **TCP/IP**,

[25] Conjunto de normas que regulan la comunicación (establecimiento, mantenimiento y cancelación) entre los distintos componentes de una red informática

es la columna vertebral para armar una comunicación entre redes, debido a que comprende el conjunto de protocolos que permiten que sucedan las conversaciones en Internet.

TCP/IP está basado en un modelo de referencia de cuatro niveles. Todos los protocolos que pertenecen al conjunto de protocolos **TCP/IP** se encuentran en los tres niveles superiores de este modelo.

Tal como se muestra en la siguiente ilustración, cada nivel del modelo TCP/IP corresponde a uno o más niveles del modelo de referencia Interconexión de sistemas abiertos (*OSI, Open Systems Interconnection*) de siete niveles, propuesto por la Organización internacional de normalización *(ISO, International Organization for Standardization).*

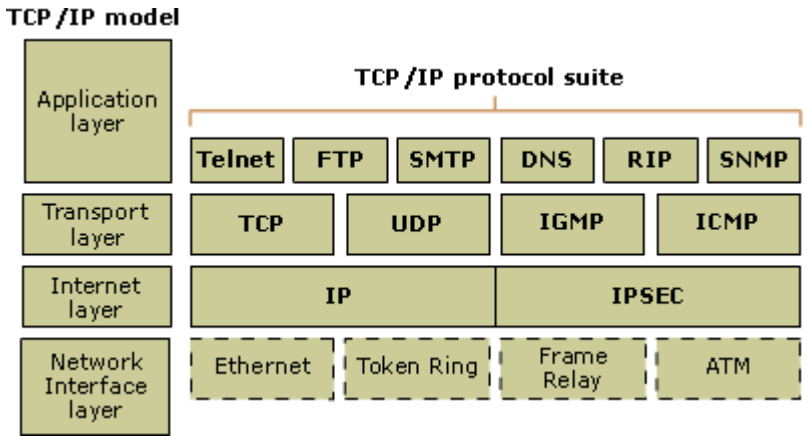


Figura 4.: Modelo TCP/IP[26]

[26] http://technet.microsoft.com/es-es/library/cc786900(WS.10).aspx

Para proveer conectividad física, los dispositivos de redes inalámbricas deben operar en la misma porción del espectro de radio, es decir, que los radios 802.11a se comunican con otro radio 802.11a en frecuencias de 5GHz, y que los radios 802.11b/g hablan con otros 802.11b/g en 2,4GHz, pero un dispositivo 802.11a no puede interoperar con uno 802.11b/g, puesto que usan porciones completamente diferentes del espectro electromagnético, concluyendo que las tarjetas inalámbricas deben concordar en un canal común, para lograr una comunicación o transferencia de datos.

Los dispositivos de las Redes Inalámbricas **802.11a/b/g/n** puede operar en uno de los cuatro modos posibles:[27]

[27] http://standards.ieee.org/getieee802/download/802.11p-2010.pdf
http://standards.ieee.org/about/get/802/802.11.html
http://www.wi-fi.org/brand.php

Cuando implementamos un enlace punto a punto, o punto a multipunto, un radio opera en modo maestro, mientras que los otros operan en modo administrado. En una red multipunto a multipunto, todos los radios operan en modo ad hoc de manera que puedan comunicarse directamente.

Estándar IEEE 802.11 (WLAN)

Estándar inicialmente creado en 1997 por la IEEE (Institute of Electrical and Electronics Engineers) por desgracia este solamente soportaba una transferencia de 2 Mbps la cual no era suficiente para la gran mayoría de aplicaciones.

En Julio de 1999 la IEEE expande este estándar creando la especificación 802.11b la cual llegaba a velocidades de 11 Mbps la cual es comparable a las velocidades que ofrecía el Ethernet tradicional. 802.11b usa la frecuencia de radio no regulada (2.4 GHz), la cual al momento de fabricación reduce costos, al ser esta frecuencia no regulada se pueden presentar interferencias entre otros dispositivos electrónicos que también la usan (teléfonos inalámbricos, hornos microondas).

802.11a es otra especificación de este estándar, el cual fue creado al mismo tiempo que 802.11b pero como la mencionada anteriormente ganó popularidad más rápido, se tiene la errónea idea que 802.11a fue creada después. Pero debido a su alto costo de producción solo era aplicado en negocios donde era mejor aprovechada que la 802.11b que es mayormente usada en el hogar, hablando más técnicamente la 802.11a alcanza velocidades hasta de 54 Mbps y trabaja en una frecuencia regulada que ronda los 5 GHz pero a su vez esto trae su desventaja, ya que en comparación con la 802.11b es inferior en rango y además tiene más dificultad en pasar a través de las paredes.

En los años 2002 y 2003 un nuevo estándar apareció en el mercado 802.11g el cual combinaba lo mejor del 802.11a y 802.11b, es decir, llega a velocidades de 54 Mbps y trabaja a la frecuencia de 2.4 GHz para mayor rango, además es compatible con 802.11b esto significa que los Access Points funcionaran con 802.11b y viceversa.

Ventajas y Desventajas de cada estándar:

- 802.11b Ventajas
    - Tiene un bajo costo.
    - El rango de la señal es bueno y no es obstruido con facilidad.

- 802.11b Desventajas
    - La velocidad máxima no es muy rápida.
    - Puede presentar mucha interferencia con los aparatos caseros.

- 802.11a Ventajas
    - La velocidad máxima es rápida.
    - Al encontrarse en una frecuencia regulada evita la interferencia con otros aparatos caseros.

- 802.11a Desventajas
    - Tiene un costo muy alto.
    - La señal es más fácil de obstruir y tiene poco rango.

- 802.11b Ventajas
    - Velocidad máxima muy rápida y un muy buen rango de señal y no es fácilmente obstruida.
    - El rango de la señal es bueno y no es obstruido con facilidad.

- 802.11g Desventajas
    - Es más caro que el 802.11b.
    - Puede presentar interferencia con los aparatos caseros.

Estándar IEEE 802.15[28](WPAN)

Este estándar se especializa en las redes inalámbricas de área personal (*Wireless Personal Area Network* WPAN) o redes inalámbricas de corta distancia. Las redes WPAN permiten a aparatos portables y móviles tales como PCs, PDAs, Celulares, comunicarse e interoperar entre sí. Este estándar se encuentra dividido en 9 grupos de trabajo, de los cuales los últimos cuatro se encuentran aún en revisión.

IEEE 802.15.1[29]

Este grupo de trabajo fue aprobado el 15 de abril de 2002 y es un recurso adicional para la implementación de dispositivos Bluetooth. Además también define las especificaciones de la capa física y el control de acceso al medio de las conexiones inalámbricas con dispositivos fijos, portables y en movimiento dentro o entrando espacios de operación personal.

El IEEE 802.15.1 está basado en regulaciones para Europa, Japón y Norte América, en Europa la aprobación del estándar se dio mediante la European Telecommunications Standard Institute (ETSI) en los documentos "EN 300 328, ETS 300-826" y al autoridad que dio la aprobación fue la National Type Approval Authorities. En Japón fue aprobado mediante la Association of Radio Industries and Businesses (ARIB) el documento es el "ARIB STD-T66" y la autoridad fue el Ministry of Post and Telecommunications (MPT) y para Norte América en el caso

[28] http://www.ieee802.org/15/about.html
[29] http://www.ieee802.org/15/pub/TG1.html

de Estados Unidos la aprobación se dio mediante la Federal Communications Commission (FCC) en los documentos "CFR47, Part 15, Sections 15.205, 15.209, 15.247, and 15.249" y la autoridad fue tambien la FCC, en el caso de Canadá la aprobación se dio mediante la Industry Canada (IC) en los documentos GL36 y la autoridad fue la misma IC.

IEEE 802.15.2[30]

Este grupo de trabajo se basa en la coexistencia en las WPAN con otros dispositivos inalámbricos que operen en frecuencias no licenciadas.

IEEE 802.15.3[31]

Este grupo de trabajo se enfoca en establecer los estatus y trabajar en la publicación de un nuevo estándar de alta velocidad para las WPAN. Otro punto a favor en este grupo de trabajo es que además de ofrecer una alta velocidad de transmisión también está siendo diseñado para que el consumo de energía sea bajo. Además de lo mencionado anteriormente, este grupo de trabajo se encuentra dividido en 3 subgrupos de los cuales actualmente solo se encuentran 2 en trabajo ya que el subgrupo **802.15.3a** ha sido retirado[32] ya a que habían dos propuestas distintas establecidas por dos alianzas diferentes y debido a que no se pudo llegar a un acuerdo se decidió retirarlo. El subgrupo **802.15.3b**[33] trabaja para mejorar la implementación e interoperabilidad de MAC, y el subgrupo **802.15.3c**[34] trabaja

[30] http://www.ieee802.org/15/pub/TG2.html
[31] http://www.ieee802.org/15/pub/TG3.html
[32] http://standards.ieee.org/board/nes/projects/802-15-3a.pdf
[33] http://www.ieee802.org/15/pub/TG3b.html
[34] http://www.ieee802.org/15/pub/TG3c.html

para desarrollar una capa física alternativa (PHY) basada en onda milimétrica, la cual operará en la banda no licenciada que se encuentra en el rango de 57-64 GHZ además la velocidad de transferencia va desde 1Gbps para acceso a internet y streaming y 2Gbps para aplicaciones en tiempo real.

IEEE 802.15.4[35]

Este grupo de trabajo se enfoca en la investigación de una solución de baja transmisión de datos para sistemas con baterías de larga o corta duración y complejidad baja, se encuentra operando en una banda no licenciada e internacional. Aplicaciones potenciales son encontradas en los sensores, juguetes interactivos, controles remotos. Además de esto, este grupo se encuentra dividido en siete subgrupos, de los cuales los tres últimos (802.15.4e, 802.15.4f, 802.15.4g) se encuentran en revisión. El primer subgrupo **802.15.4a**[36] cuyo principal interés consiste en proveer mayor capacidad de comunicación y precisión (rango y localización) en distancias de un metro y mayores que requieran alta productividad y bajo costo de energía. El segundo subgrupo **802.15.4b**[37] fue creado para desarrollar un proyecto para revisar y mejorar el estándar, en lo cual se destaca la resolución de ambigüedades y reducción de complejidades innecesarias, incrementar la seguridad en el uso de claves de seguridad entre otros. El tercer subgrupo **802.15.4c**[38] se encuentra trabajando en definir una corrección de capa física (PHY) para las regulaciones en China donde se abrieron

[35] http://www.ieee802.org/15/pub/TG4.html
[36] http://www.ieee802.org/15/pub/TG4a.html
[37] http://www.ieee802.org/15/pub/TG4b.html
[38] http://www.ieee802.org/15/pub/TG4c.html

las bandas 314-316 MHz, 430-434 MHz, y 779-787 MHz para usos de WPANs dentro de China. El cuarto subgrupo **802.15.4d**[39] se encuentra en una corrección al estándar **802.15.4-2006**, la corrección consiste en definir una nueva capa física (PHY) y tales cambios a la MAC son necesarios para soportar la nueva asignación de frecuencias (950MHz - 956 MHz) en Japón.

IEEE 802.15.5[40]

Este grupo se encuentra trabajando en determinar los mecanismos necesarios que deben estar presentes en las capas física (PHY) y en la capa de control de acceso al medio (MAC) de las WPANs para permitir las redes en mallas.

[39] http://www.ieee802.org/15/pub/TG4d.html
[40] http://www.ieee802.org/15/pub/TG5.html

Implementar y administrar la seguridad en redes inalámbricas

Una de las muchas ventajas que tiene una conexión inalámbrica es que la transmisión de datos se realiza por medio de ondas que cada estación de trabajo móvil remite para acceder a la información que está circulando dentro del mismo entorno, con la gran ventaja de que ya no es necesario contactarse por medio de un cableado de red.

Pero como en todo servicio ó aplicación informático existen vulnerabilidades de seguridad, es necesario tomar medidas estrictas para evitar cualquier tipo de eventualidad negativa. Así como un usuario en una empresa o una persona en su domicilio quieren ingresar a Internet usando su propia conexión inalámbrica, hay personas con fines inescrupulosos o que por curiosidad acceden clandestinamente a una red inalámbrica para tratar de encontrar o sacar alguna información importante que esté circulando en ella.

Las redes inalámbricas actuales incorporan funciones completas de seguridad, y cuando estas redes cuentan con una protección adecuada, las compañías y las personas pueden aprovechar con confianza las ventajas que ofrecen.

"*Los proveedores están haciendo un gran trabajo para mejorar las funciones de seguridad, y los usuarios están obteniendo conocimiento de la seguridad inalámbrica"*, afirma Richard Webb, analista de orientación para redes de área local inalámbricas (LAN) de Infonetics Research.

Tener un mejor conocimiento de los elementos de la seguridad de LAN inalámbricas y el empleo de algunas de las mejores prácticas puede ser de gran ayuda para ayudarle a beneficiarse de las ventajas de las redes inalámbricas.

Los métodos de ataques normales han tomado gran amplitud, así como también han aparecido otros métodos de protección a este tipo de conexiones. A pesar de que siempre existen riesgos y vulnerabilidades, también existen soluciones y mecanismos de seguridad que pueden evitar un ataque a una red inalámbrica.

Elementos de la seguridad inalámbrica[41]

Para proteger una red inalámbrica, hay tres acciones que pueden ayudar:

- ***Proteger los datos durante su transmisión mediante el cifrado:*** el cifrado[42] es como un código secreto. Traduce los datos a un lenguaje indescifrable que sólo el destinatario indicado comprende. El cifrado requiere que tanto el remitente como el destinatario tengan una clave para decodificar los datos transmitidos. El cifrado más seguro utiliza claves muy complicadas, o algoritmos, que cambian con regularidad para proteger los datos.

- ***Desalentar a los usuarios no autorizados mediante autenticación:*** los nombres de usuario y las contraseñas son la base de la autenticación, pero otras herramientas pueden hacer que la autenticación sea más segura y

[41] http://www.coit.es/publicac/publbit/bit138/3com.pdf
[42] Cifrado: Método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido. Sinónimo de Criptografía.

confiable. La mejor autenticación es la que se realiza por usuario, por autenticación mutua entre el usuario y la fuente de autenticación.

- ***Impedir conexiones no oficiales mediante la eliminación de puntos de acceso dudosos:*** un empleado que goza de conexión inalámbrica en su hogar podría comprar un punto de acceso barato y conectarlo al punto de red sin pedir permiso. A este punto de acceso se le denomina dudoso, y la mayoría de estos puntos de acceso los instalan empleados, no intrusos maliciosos. Buscar la existencia de puntos de acceso dudosos no es difícil. Existen herramientas que pueden ayudar, y la comprobación puede hacerse con una computadora portátil y con software en un pequeño edificio, o utilizando un equipo de administración que recopila datos de los puntos de acceso.

Soluciones de seguridad inalámbrica[43]

Existen tres soluciones disponibles para proteger el cifrado y la autenticación de LAN inalámbrica:

- Acceso protegido Wi-Fi – WPA.
- Acceso protegido Wi-Fi 2 - WPA2.
- Conexión de redes privadas virtuales - VPN.

[43] http://www.saulo.net/pub/inv/SegWiFi-art.htm

WPA – WPA2

Luego de desaparecer WEP[44], en 2003 se propone el Acceso Protegido a Wi-Fi (WPA, por sus iniciales en inglés) y luego queda certificado como parte del estándar IEEE 802.11i, con el nombre de WPA2 (en 2004).

WPA y WPA2 son protocolos diseñados para trabajar con y sin un servidor de manejo de llaves. Si no se usa un servidor de llaves, todas las estaciones de la red usan una "llave previamente compartida" (PSK - Pre-Shared-Key-, en inglés), El modo PSK se conoce como WPA o WPA2-Personal.

Cuando se emplea un servidor de llaves, al WPA2 se le conoce como WPA2-Corporativo (o WPA2- Enterprise, en inglés). En WPA-Corporativo, se usa un servidor IEEE 802.1X para distribuir las llaves.

Una mejora notable en el WPA" sobre el viejo WEP es la posibilidad de intercambiar llaves de manera dinámica mediante un protocolo de integridad temporal de llaves (TKIP -Temporal Key Integrity Protocol).

WPA2 vs. WPA

1. El reemplazo del algoritmo Michael por una código de autenticación conocido como el protocolo "Counter-Mode/CBC-Mac " (CCMP), que es considerado criptográficamente seguro.
2. El reemplazo del algoritmo RC4 por el "Advanced Encryption Standard (AES)" conocido también como Rijndael.

[44] WEP y sus extensiones (WEP+, WEP2) son al día de hoy obsoletas. WEP está basado en el algoritmo de encripción RC4, cuyas implementaciones en el estándar IEEE 802.11 se consideran inadecuadas.

VPN[45]

VPN brinda seguridad eficaz para los usuarios que acceden a la red por vía inalámbrica mientras están de viaje o alejados de sus oficinas. Con VPN, los usuarios crean un "túnel" seguro entre dos o más puntos de una red mediante el cifrado, incluso si los datos cifrados se transmiten a través de redes no seguras como la red de uso público Internet. Los empleados que trabajan desde casa con conexiones de acceso telefónico o de banda ancha también pueden usar VPN.

Así funciona

La comunicación entre los dos extremos de la red privada a través de la red pública se hace estableciendo túneles virtuales entre esos dos puntos y usando sistemas de encriptación y autentificación que aseguren la confidencialidad e integridad de los datos transmitidos a través de esa red pública. Debido al uso de estas redes públicas, generalmente Internet, es necesario prestar especial atención a las cuestiones de seguridad para evitar accesos no deseados.

La tecnología de túneles (Tunneling) es un modo de envío de datos en el que se encapsula un tipo de paquetes de datos dentro del paquete de datos propio de algún protocolo de comunicaciones, y al llegar a su destino, el paquete original es desempaquetado volviendo así a su estado original.

[45] Virtual Private Network - http://www.cisco.com/en/US/products/ps5743/Products_Sub_Category_Home.html

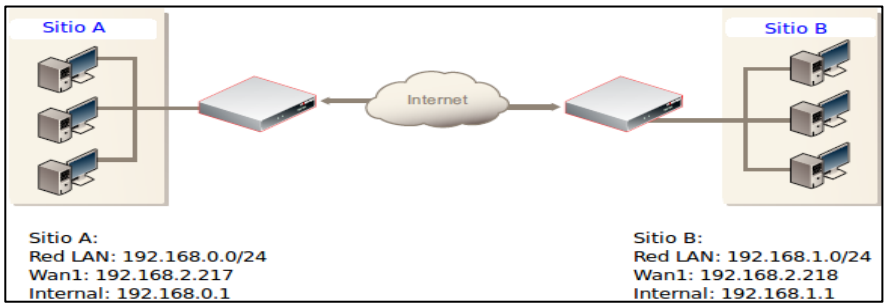
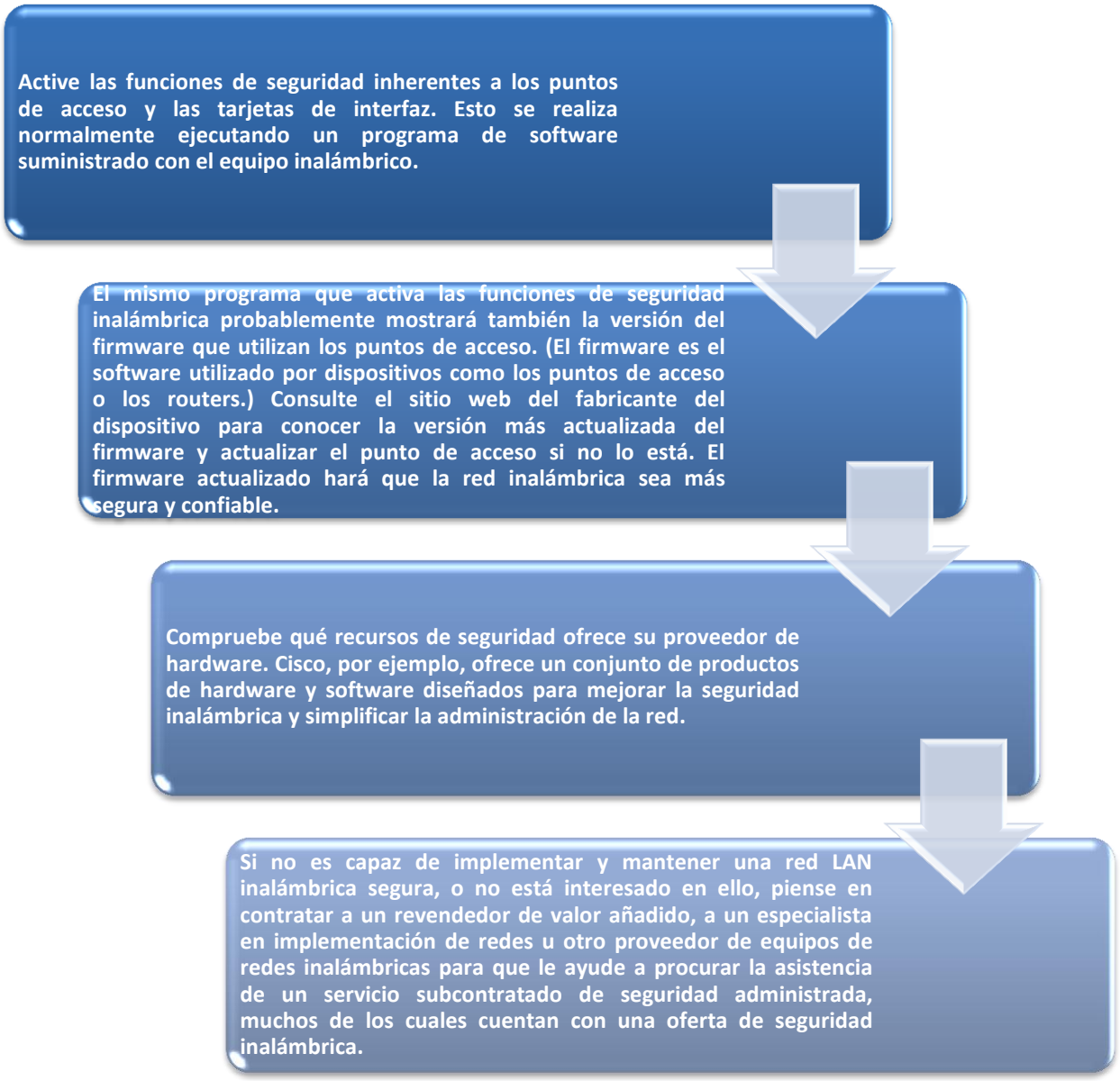


Figura 5 Funcionamiento de VPN

Pasos básicos para implementar la seguridad una red LAN inalámbrica[46]



[46] http://www.eslared.org.ve/tricalcar/12_es_seguridad-inalambrica_guia_v01[1].pdf

"La seguridad es definitivamente un elemento que se debe planificar, igual que la administración de la red, la disponibilidad de acceso y cobertura, etc.", Ask, de Jupiter.

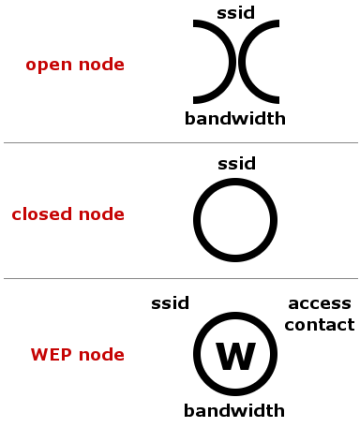
Aspectos relativos a la seguridad en redes inalámbricas y sus soluciones

El poder acceder a las redes inalámbricas, además de ser su mayor atracción es a la vez su mayor debilidad, debido a que cualquier equipo que se encuentre dentro del rango de esta puede acceder a ella lo cual visto desde la perspectiva de una empresa es peligroso, ya que puede ser usada para cometer muchas actividades delictivas.

Es por eso que a la hora de configurar una red inalámbrica debemos tener en cuenta que el cifrado WEP (Wired Equivalent Privacy) en estos tiempos es obsoleto, puesto que ya existen muchas formas de acceder a ella por su baja calidad de protección y si a esto le agregamos que todo el tráfico es visible y accesible por un atacante y además WEP no ofrece ni autenticación, ni confidencialidad ni integridad, estamos dejando nuestra red expuesta a muchas formas de ataque.

Antes de una red ser atacada, los hackers o crackers que vayan a realizar dicha actividad, primero deben identificar cual es el rango de la red, si tiene o no seguridad activada, lo cual lo hacen de varias formas entre las más populares están el “*Warchalking*” y el “*Wardriving*”.

Warchalking es un lenguaje de símbolos que normalmente son escritos con tiza en los muros o aceras cuyo objetivo es el de informar de un punto de acceso inalámbrico en ese punto, los símbolos usados son los siguientes:

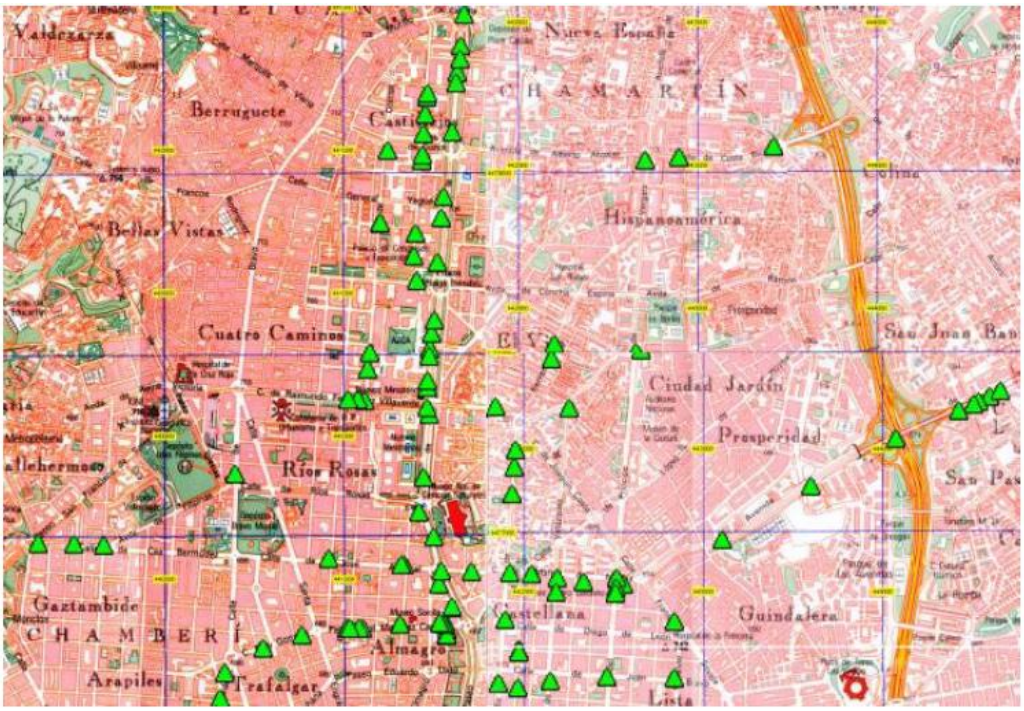


En donde el primer símbolo indica que hay un nodo abierto, arriba va el nombre de la red y abajo el ancho de banda a la que esta trabaja.

El segundo símbolo indica que es un nodo cerrado.

Y el tercer símbolo indica que está protegido pero mediante cifrado WEP

Wardriving se enfoca en lo mismo, lo cual es encontrar puntos de red inalámbricas pero este es realizado desde un automóvil, también se necesita un portátil con una tarjeta inalámbrica y un receptor GPS



La imagen de arriba nos muestra los lugares donde fueron hallados puntos de red inalámbricos, y las de abajo son antenas de fabricación casera.

Existes dos tipos de ataques a las redes inalámbricas, los ataques pasivos y los ataques activos. Los ataques pasivos se enfocan más que todo al monitoreo y análisis de la red y los ataques activos están más enfocados en atentar de cierta forma contra la red, ya sea ingresando a ella o negándole el servicio.

Dentro de los ataques pasivos tenemos:

- Sniffing: Es una técnica que permite "escuchar" todo lo que se transmite en una red, y en redes inalámbricas el tráfico puede ser espiado con mucha más facilidad que en las redes cableadas. Es necesario disponer de un portátil con tarjeta de red inalámbrica y el software que se encarga de esto, el cual circula de manera gratuita en internet.
- Análisis de Tráfico: En donde el cual el atacante obtiene información solamente examinando el tráfico de la red, por ejemplo, a qué hora están habilitados ciertos equipos, durante cuánto tiempo y cuanta es la cantidad de tráfico que envían.

Dentro de los ataques activos tenemos:

- Modificación: El atacante manipula los mensajes transmitidos (borra, añade o reordena). Dentro de estos tenemos el ataque "*Man-in-the-middle*".
- Denegación de servicio: Se generan interferencias las cuales producen errores en la transmisión lo que ocasiona que la velocidad se reduzca drásticamente e inclusive que la red deje de funcionar.
- Suplantación: Mediante un *Sniffer* se obtienen direcciones MAC válidas, mediante el análisis de tráfico se sabe a qué hora se conecta el usuario por el cual

se quiere hacer pasar, otra forma es instalando APs *Rogue* (falsos) con el objetivo de que usuarios legítimos se conecten a este AP en vez del real.

- Reactuación: Se inyectan en la red paquetes interceptados mediante un sniffer y con el cual se pueden repetir acciones u operaciones que habían sido realizadas por un usuario de la red.

Analizar el estándar 802.11n y sus ventajas

El estándar 802.11n es una propuesta que se hizo para modificar el estándar 802.11-2007 y consiste en mejorar el rendimiento de la red e inclusive proporcionar más velocidad de transmisión de datos que 802.11b y 802.11g de 54Mbps a 600Mbps. Actualmente la capa física aguanta hasta los 300Mbps y usando 2 flujos espaciales en un canal de 40MHz.

Este estándar está basado en los anteriores de la familia 802.11 la diferencia radica en que se le agrega *Multiple-Input Multiple-Output* (*MIMO*), la unión de interfaces de red (*Channel Bonding*) y además le agrega tramas a la capa MAC.

MIMO utiliza múltiples antenas tanto transmisoras como receptoras que mejoran el desempeño, manejar más información (cuidando la coherencia de la misma), que utilizando una sola antena. Esta tecnología depende de señales multiruta, una señal multiruta es una señal reflejada que llega al receptor un tiempo después de que la señal de la Línea de Visión (*LoS* por sus siglas en inglés) ha sido recibida. Redes 802.11 a/b/g al no ser basadas en *MIMO* identifican a las señales multiruta como si fuesen interferencia esto trae como consecuencia que el receptor no sea capaz de recuperar el mensaje de dicha señal.

Las ventajas que posee este estándar son:

- Mejor Rendimiento: Al incrementar la velocidad de transmisión de datos de 54Mbps a 600Mbps, lo cual permitirá en una red local hacer video streaming en HD sin ningún problema, la copia de archivos en red será muchísimo más rápida, entre otros.

- Mayor Alcance: Al utilizar 2 flujos espaciales de 40Mhz puede llegar a cubrir un espacio de 70 metros o superior con una buena velocidad de transmisión de datos.

- Retro compatibilidad: Será compatible con estándares anteriores, lo cual significa que no hay que adquirir otro dispositivo para redes 802.11 a/b/g si se desea trabajar con ellas

- El uso de las bandas de 2.4 Ghz y 5 Ghz simultáneamente.

Conclusiones

- Desarrollo de tecnologías inalámbricas ha permitido el desarrollo de nuevos conceptos como el de “Conectividad Total”.
- El estudio y desarrollo total de WiMax, (analizando las ventajas que se muestran el siguiente recuadro) porque puede ser una solución a la brecha digital en los países en vías de desarrollo.

- Desarrollo del WiFi está en pleno proceso y aún debe mejorar el aspecto de seguridad.
- Redes de datos inalámbricas están y seguirán creciendo de ahí la importancia de su estudio.

	WiMAX 802.16	**Wi-Fi 802.11**
Velocidad	124 Mbit/s	11-54 Mbit/s
Cobertura	40-70 km	300 m
Licencia	Si/No	No
Ventajas	Velocidad y Alcance	Velocidad y Precio
Desventajas	Interferencias?	Bajo alcance

Conclusión metodología

Se puede concluir que la metodología aplicada para la realización de este trabajo fue muy optima y nos arrojó excelentes resultados, debido a que nos brinda la oportunidad de aplicar los conceptos básicos obtenido en la investigación de cada tema, permitiendo que el estudiante afiance sus habilidades en la configuración y montaje de una red inalámbrica, así como también permite la comprobación de los conceptos técnicos y la mejora de los mismo.

Resaltando la participación del tutor como guía de los conceptos aprendidos y en la aprobación de las practicas realizadas.

Recomendaciones para los usuarios

La ubicación

Uno de los factores principales que determinan el éxito de un despliegue de una red inalámbrica es dónde se sitúa el router inalámbrico. Para conseguir una adecuada instalación, ofreciendo una óptima cobertura inalámbrica, se debe estudiar con detalle el lugar a cubrir y los obstáculos a evitar.

En primer lugar se debe conocer qué cobertura se desea ofrecer. Puede que no importe la existencia de zonas sin cobertura (como pasillos, entrada, etc.) y sin embargo se prefiera ofrecer una mejor cobertura en otras zonas más utilizadas (salón, cuartos de estudio, terraza, etc.).

El alcance de la señal de una red Wi-Fi dependerá de la potencia del router, la potencia del cliente o dispositivo Wi-Fi con el que se va a conectar y los obstáculos que la señal tenga que atravesar. La velocidad de la conexión depende directamente de la distancia existente entre el router inalámbrico y el cliente conectado.

Los router que se encuentran equipados con antenas omnidireccionales en el plano que ofrecen un círculo de cobertura alrededor de la antena.

Es importante tener en cuenta que justo debajo del mismo router inalámbrico la cobertura obtenida es pequeño. Las señales de radio se propagan hacia fuera de la antena de una manera circular, a menos que se encuentre con paredes, puertas, muebles, etc... que puedan obstruir la propagación de la señal. Esta

señal todavía puede continuar pero no con suficiente energía como para ofrecer un rendimiento en largas distancias.

Se aconseja situar la antena perpendicular al equipo para obtener una cobertura circular alrededor de él. Si se sitúa justamente debajo del router, es muy probable que tampoco se disponga de cobertura. Para resolver problemas, se aconseja mover la antena buscando una posición que mejore su cobertura dependiendo de la situación del router y el equipo cliente.

Ubicación de un Router en una vivienda:

Ubicado de esta manera se tendrá mayor cobertura.

La seguridad

Asignar un SSID (*Service Set IDentifier*, Identificador del conjunto de servicios) único a la red: este es el nombre que será visible a quienes buscan una red inalámbrica disponible. Hay que comunicar la frase secreta de WPA2,

de un modo seguro a las personas autorizadas que se conectarán a esta red (clientes), o configurar manualmente los parámetros de acceso de dichos clientes, y especificarles que se conecten únicamente con el nombre especificado.

Monitorizar la aparición de nuevos puntos de acceso en las proximidades, y recordar a los clientes móviles los peligros de conectarse a un punto de acceso equivocado o malicioso. Estos, podrían incluir piratas informáticos leyendo el tráfico desde y hacia los clientes, e incluso tomando el control de una red cableada si el cliente está conectado simultáneamente a una red local Ethernet.

Habilitar el filtrado de IP y MAC en la configuración del router, el filtrado MAC permite incluir manualmente los adaptadores de red con sus números de identificación específicos en una lista de dispositivos autorizados. De este modo, cualquier identificador que no se encuentre en la lista, tendrá prohibido el acceso a la red. El filtrado IP utiliza el mismo principio: solo se les permitirá la conexión a los clientes con los números de IP autorizados, pero para esto es necesario desactivar el servidor DHCP (*Dynamic Host Configuration Protocol*, Protocolo de configuración dinámica de servidores) en el router, y asignar manualmente los números IP permitidos.

Además, podría ser útil definir el número de clientes que se pueden conectar al router, limitando los números de subred al mínimo necesario, y especificar intervalos de tiempo durante los cuales el dispositivo de conexión permitirá que el cliente acceda a la red. Esta última opción podría no estar disponible en algunos los routers.

Limitar el rango de la distribución de señal del punto de acceso, de modo que los clientes puedan conectarse solo hasta cierta distancia: pasado el límite establecido no habrá señal disponible. Esta funcionalidad está disponible únicamente en algunos dispositivos.

Considerar la ocultación de SSID, opción presente en la página de configuración del router, de modo que la red no aparezca en la lista de redes disponibles cuando los clientes realizan una nueva búsqueda. Así, se aplicarán todos los parámetros configurados previamente en el cliente, y los ordenadores que ya han sido asociados con el SSID, tendrán la capacidad de continuar detectando esta estación.

Glosario de términos

ADSL: es un tipo de línea DSL (Digital Subscriber Line, "línea de suscripción digital"). Es una tecnología de acceso a Internet de banda ancha, lo que implica una velocidad superior a una conexión tradicional por módem en la transferencia de datos

ANTENA: Es un dispositivo diseñado con el objetivo de emitir o recibir ondas electromagnéticas hacia el espacio libre. Una antena transmisora transforma voltajes en ondas electromagnéticas, y una receptora realiza la función inversa.

ATENUACION: En telecomunicación, se denomina atenuación de una señal, sea esta acústica, eléctrica u óptica, a la pérdida de potencia sufrida por la misma al transitar por cualquier medio de transmisión.

BLUETOOTH: Es una especificación industrial para Redes Inalámbricas de Área Personal (WPANs) que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia.

CLIENTE: Es una aplicación informática que se utiliza para acceder a los servicios que ofrece un servidor, normalmente a través de una red de telecomunicaciones.

DNS: Es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado al internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignados a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres inteligibles para los humanos en identificadores binarios asociados con los

equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

HARDWARE: Corresponde a todas las partes físicas y tangibles de una computadora: sus componentes eléctricos, electrónicos, electromecánicos y mecánicos[,]sus cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado

GATEWAYS: (puerta de enlace) Es un dispositivo, con frecuencia un ordenador, que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.

MICROONDAS: A las ondas electromagnéticas definidas en un rango de frecuencias determinado.

PROTOCOLO DE INTERNET: (IP, Internet Protocol) Es un protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados.

PROTOCOLO DE RED: Es un conjunto de reglas usadas por computadoras para comunicarse unas con otras a través de una red. Un protocolo es una convención o estándar que controla o permite la conexión, comunicación, y transferencia de datos entre dos puntos finales.

RADIOFRECUENCIA: (RF) También denominado espectro de radiofrecuencia o RF, se aplica a la porción menos energética del espectro electromagnético, y corresponde a un ciclo por segundo. Las ondas electromagnéticas de esta región

del espectro se pueden transmitir aplicando la corriente alterna originada en un generador a una antena.

SERVIDOR: Es una computadora que, formando parte de una red, provee servicios a otras computadoras denominadas clientes.[

SOFTWARE: Se refiere al equipamiento lógico o soporte lógico de una computadora digital, y comprende el conjunto de los componentes lógicos necesarios para hacer posible la realización de tareas específicas

WPA: (Wi-Fi Protected Access) Adopta la autentificación de usuarios mediante el uso de un servidor, donde se almacenan las credenciales y contraseñas de los usuarios de la red. Para no obligar al uso de tal servidor para el despliegue de redes.

Bibliografía

ENGLS, Adams., Introducción a Redes Inalámbricas, 344 págs., 2008

FERNANDEZ QUISPE, Edson y otros, Tesis en computación e informática, INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO HUAYCAN, Redes inalámbricas en el ISTP Huaycán, 84 págs, 2002.

GARCÍA SERRANO, Alberto. Redes Wi-Fi, 344 págs., 2009

GÓMEZ LÓPEZ, J., Guía de campo de Wi-Fi, 214 págs., 2009

OLIVA, N., Castro. Sistemas de Cableado Estructurado, 224 págs., 2009

REID, Neil y SEID, Row, Manual de Redes inalámbricas, 384 págs., 2001

ROLDÁN M., David, Comunicaciones inalámbricas, 384 págs., 2001

TANENBAUM, Andrew, Redes De Computadoras, 145 págs., 3Ed.2008

[En línea] Consultado en

ttp://es.wikipedia.org/wiki/Redes_inal%C3%A1mbricas.(03.agosto.2011) .Parr 2

[En línea] Consultado en

http://es.wikipedia.org/wiki/Red_de_computadoras.(12.agosto.2011) .Parr 1

[En línea] Consultado en

http://es.wikipedia.org/wiki/Red_de_%C3%A1rea_local.(20.julio.2011) .Parr 2

[En línea] Consultado en

http://www.monografias.com/Computacion/Redes/.(01.julio.2011) .Parr 2

[En línea] Consultado en

http://www.monografias.com/trabajos28/manual-redes/manual-

redes.shtml/.(29.mayo.2011) .Parr 2

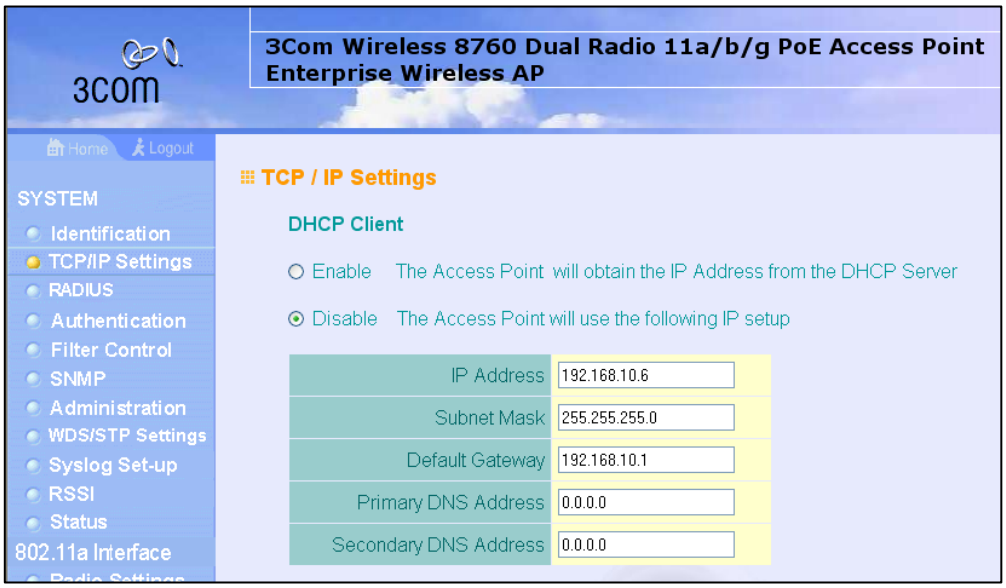
Anexos

Prácticas Implementación de Redes Inalámbricas

Configuración Red Infraestructura (Un Access Point)

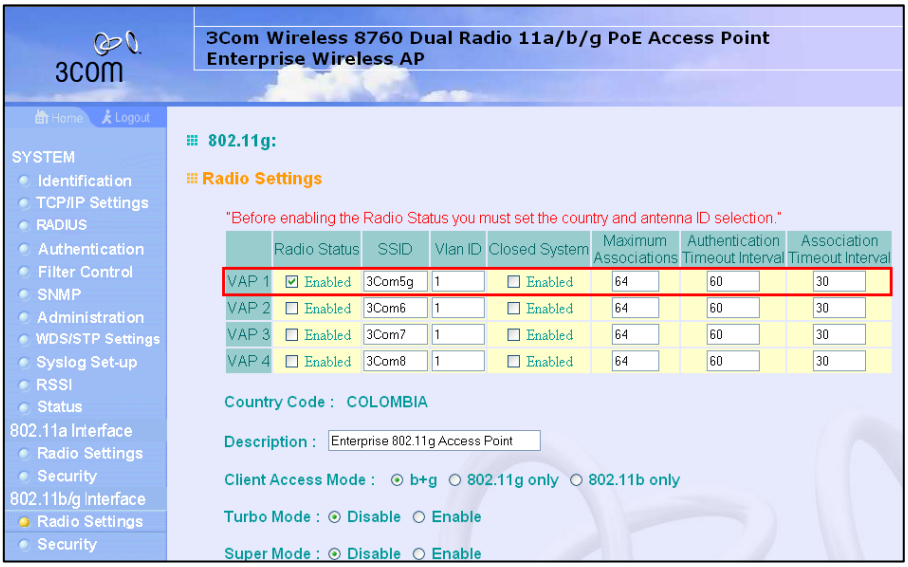
1. Se configura el Access Point (AP)

Por defecto, la dirección IP del AP es 169.254.2.1 y se entra al AP con el nombre de usuario *admin* y la contraseña *password*, luego se va a TCP/IP Settings y desactivamos (disable) el Cliente DHCP y configuramos manualmente la dirección IP del AP como se ve a continuación:



Luego damos clic en *Apply* (que se encuentra al final de la página) para guardar los cambios y el AP ya cuenta con esta dirección IP.

Además le colocamos el nombre a la SSID:



2. Configuramos una pequeña red LAN con varios equipos y un switch (CISCO CATALYST 2960 series) los equipos que vayan a estar en la red con sus direcciones IP.

EQUIPO 1: IP 192.168.10.4

Mascara 255.255.255.0

Puerta Enlace: 192.168.10.1

EQUIPO 2: IP 192.168.10.5

MASCARA 255.255.255.0

Puerta Enlace: 192.168.10.1

AP: IP 192.168.10.6

MOVIL: IP 192.168.10.11

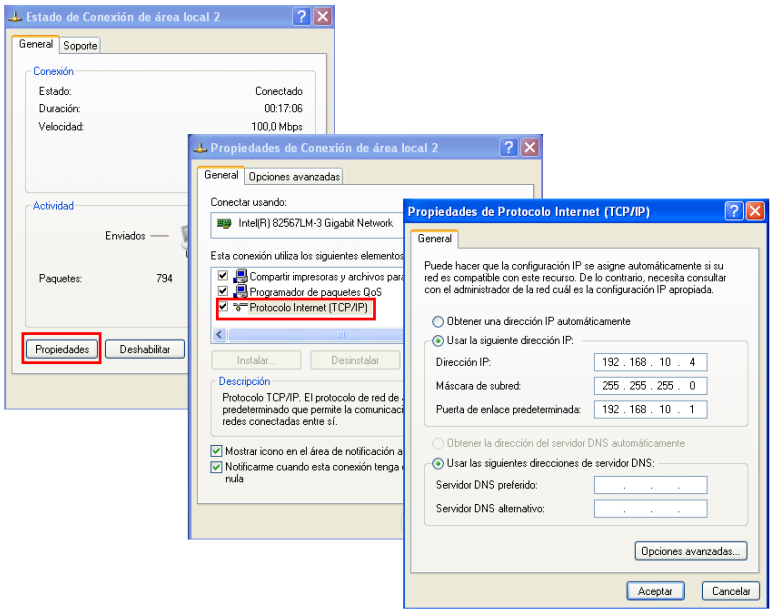
PORTATIL: IP 192.168.10.8

MASCARA 255.255.255.0

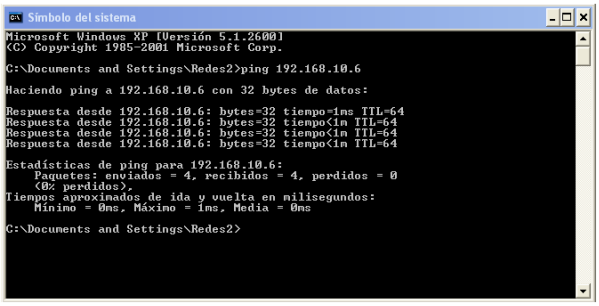
Puerta Enlace: 192.168.10.1

3. Se hace la prueba de interconectividad con el comando *ping* desde la línea de comandos:

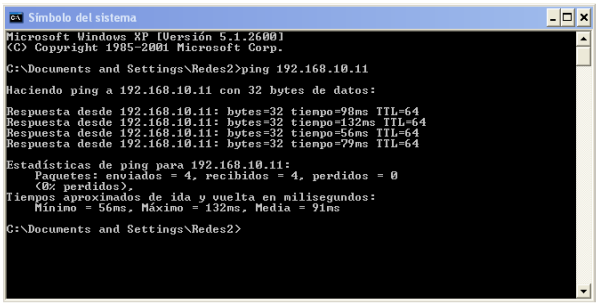
Desde el equipo PC#1 que cuenta con la siguiente configuración:



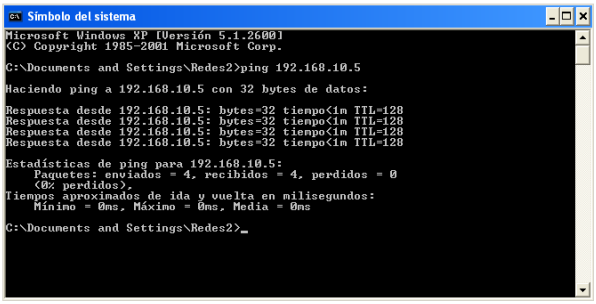
PING AP 3COM IP 192.168.10.6



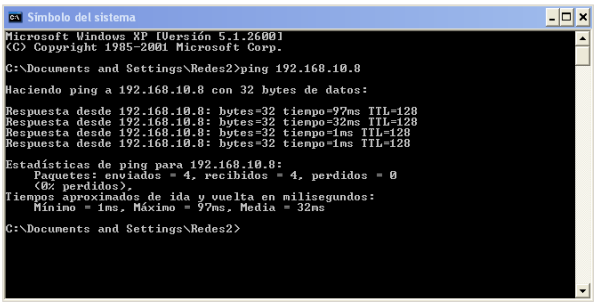
PING DISPOSITIVO MOVIL IP 192.168.10.11



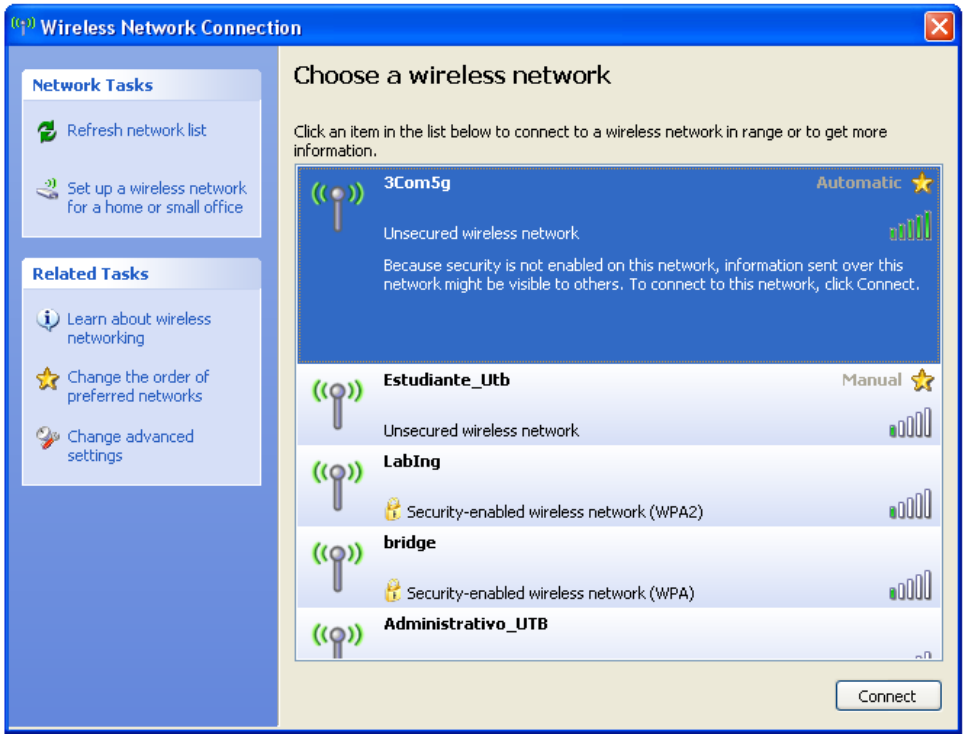
PING EQUIPO PC #2 IP 192.168.10.5



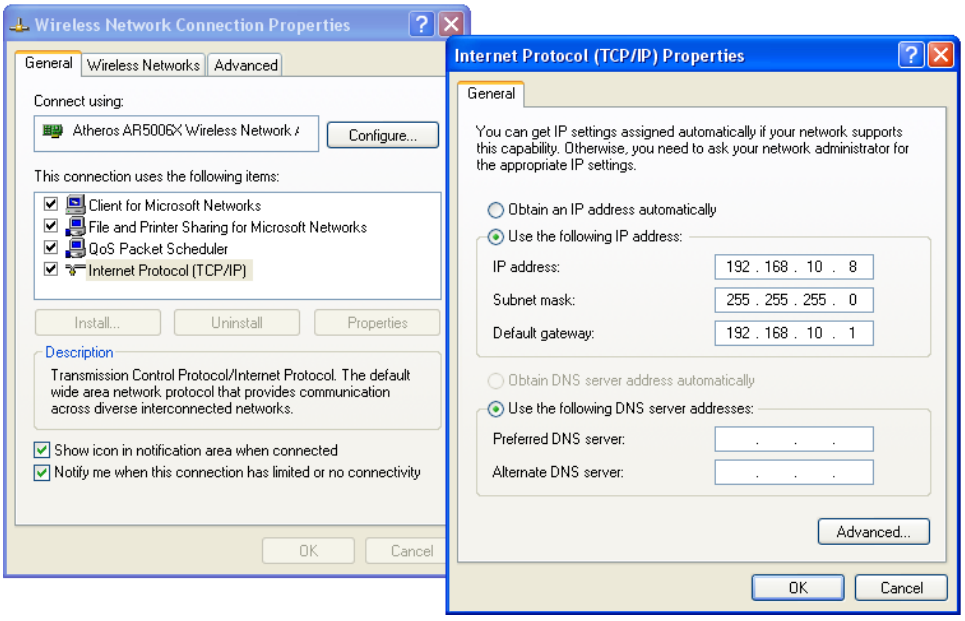
PING EQUIPO PORTATIL IP 192.168.10.8



Nos conectamos al AP desde el equipo portátil

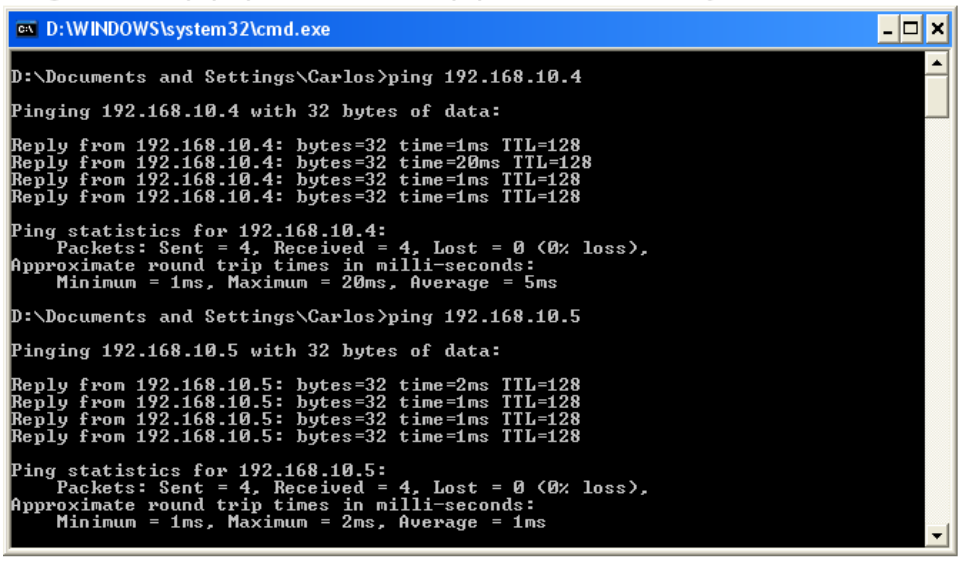


Cuya configuración es la siguiente:



Luego de conectar a la red hacemos la prueba de interconectividad desde el equipo portátil hacia los equipos cableados.

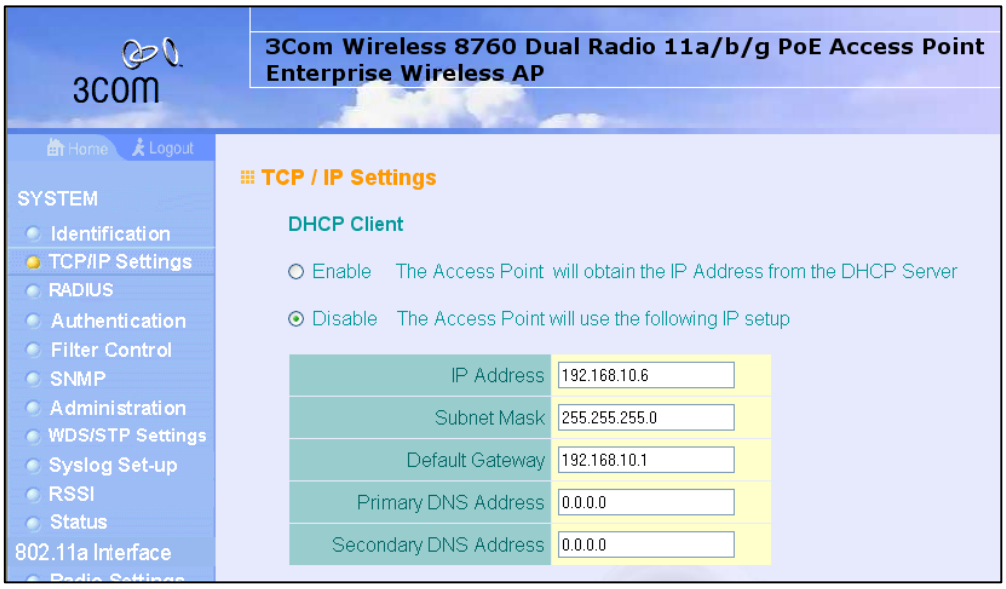
Ping desde el equipo portátil hacia los equipos cableados PC#1 y PC#2



Configuración Red Infraestructura con seguridad (Un Access Point)

1. Se configura el Access Point (AP)

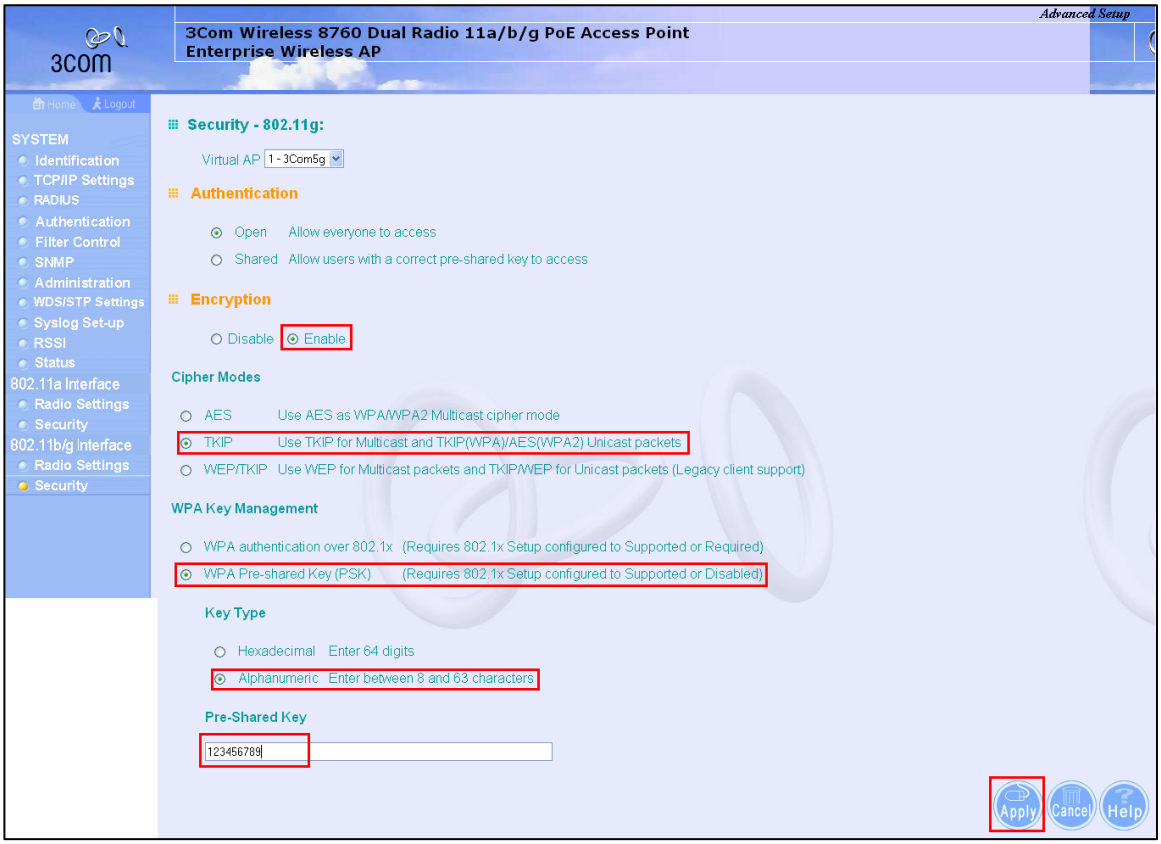
Por defecto, la dirección IP del AP es 169.254.2.1 y se entra al AP con el nombre de usuario *admin* y la contraseña *password*, luego se va a TCP/IP Settings y desactivamos (disable) el Cliente DHCP y configuramos manualmente la dirección IP del AP como se ve a continuación:



Luego damos clic en *Apply* (que se encuentra al final de la página) para guardar los cambios y el AP ya cuenta con esta dirección IP.

Además le colocamos el nombre a la SSID:

2. Configuramos el AP para que pida autenticación a la hora de conectarse con él:



3. Configuramos una pequeña RED LAN con varios equipos y un switch (CISCO CATALYST 2960 series) los equipos que vayan a estar en la red con sus direcciones IP.

EQUIPO 1: IP 192.168.10.4

MASCARA 255.255.255.0

Puerta Enlace: 192.168.10.1

AP: IP 192.168.10.6

MOVIL: IP 192.168.10.11

EQUIPO 2: IP 192.168.10.5

MASCARA 255.255.255.0

Puerta Enlace: 192.168.10.1

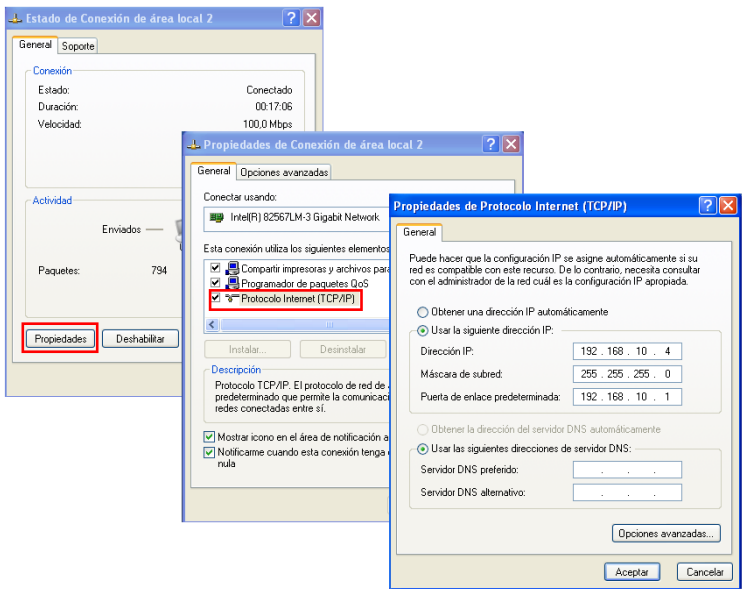
PORTATIL: IP 192.168.10.8

MASCARA 255.255.255.0

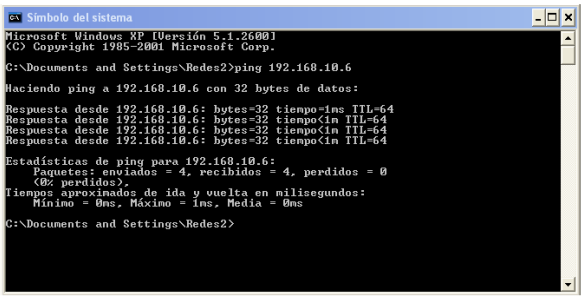
Puerta Enlace: 192.168.10.1

4. Se hace la prueba de interconectividad con el comando *ping* desde la línea de comandos:

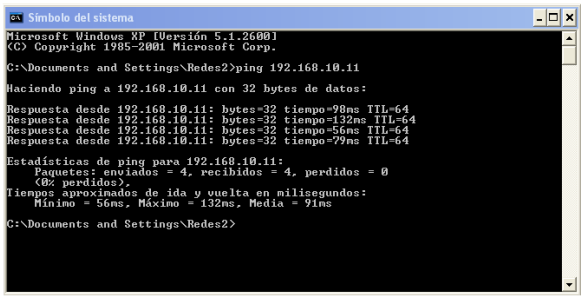
Desde el equipo PC#1 que cuenta con la siguiente configuración:



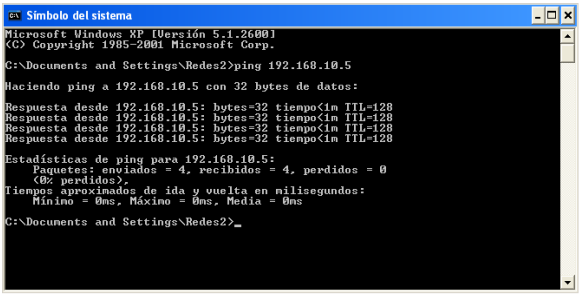
PING AP 3COM IP 192.168.10.6



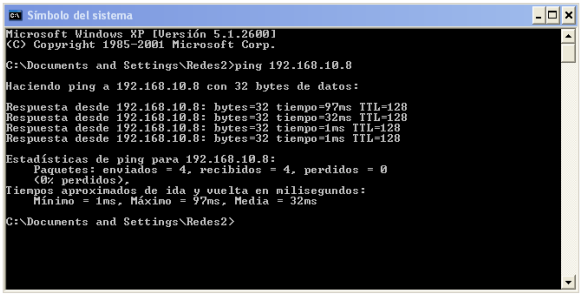
PING DISPOSITIVO MOVIL IP 192.168.10.11



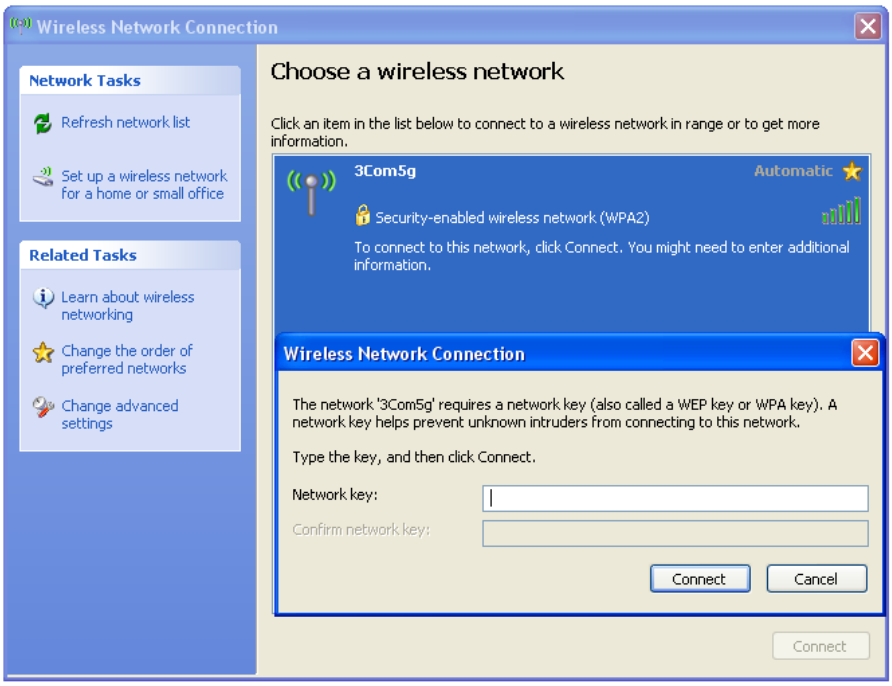
PING EQUIPO PC #2 IP 192.168.10.5



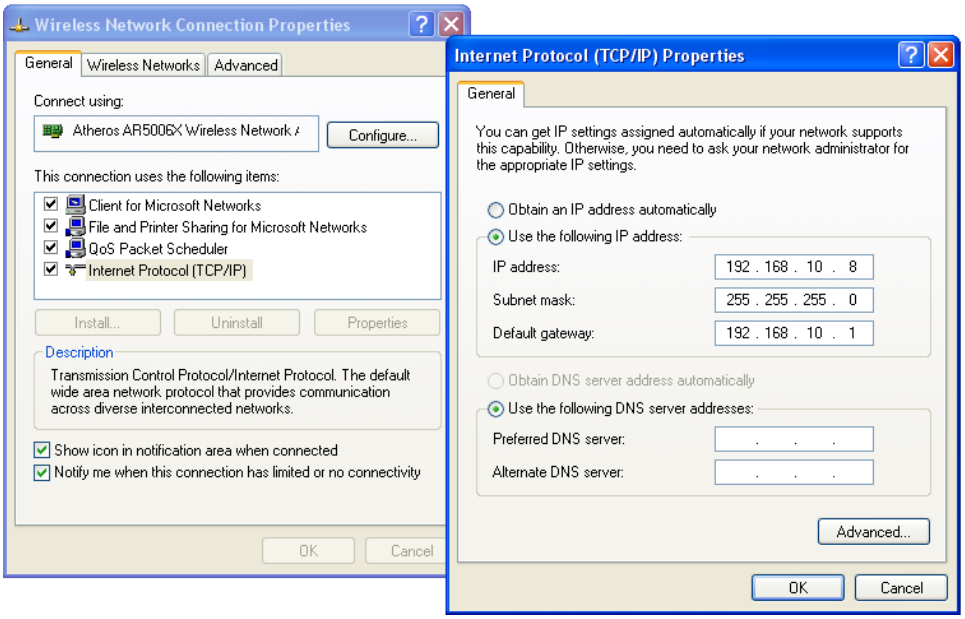
PING EQUIPO PORTATIL IP 192.168.10.8



Nos conectamos al AP desde el equipo portátil, pero esta vez nos pide una contraseña:

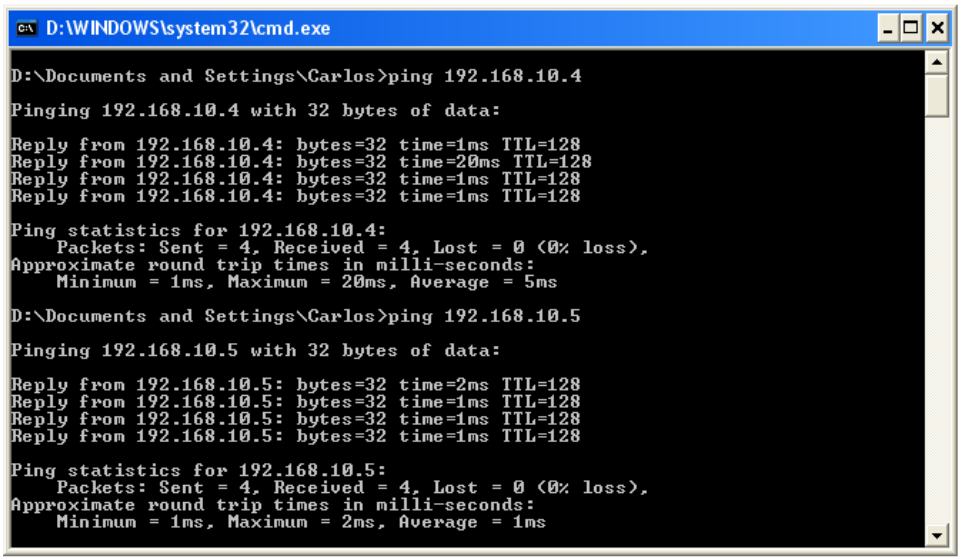


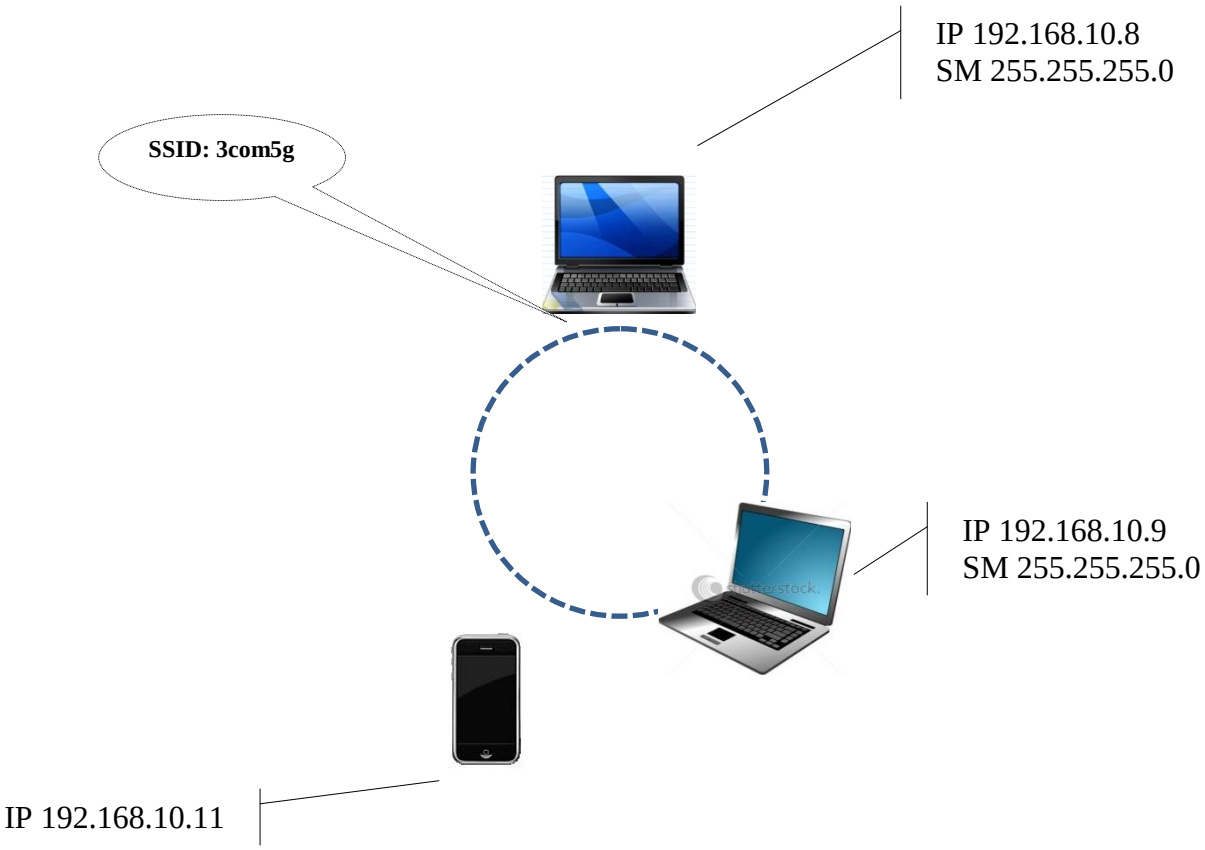
Cuya configuración es la siguiente:



Luego de conectar a la red hacemos la prueba de interconectividad desde el equipo portátil hacia los equipos cableados.

Ping desde el equipo portátil hacia los equipos cableados PC#1 y PC#2





PRACTICA

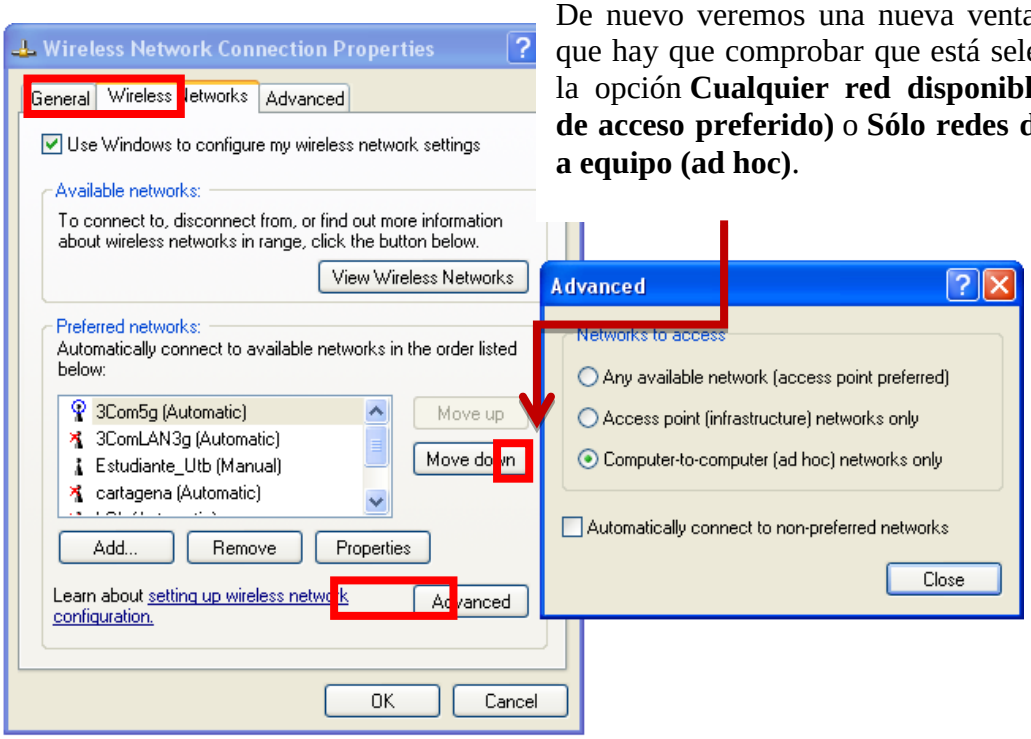
Configuración ***RED AD HOC***

El primer paso es instalar un adaptador inalámbrico y los drivers en todos los equipos que estarán conectados a la ***RED AD HOC.***

Para empezar, debemos localizar el icono **Mis sitios de red** en el escritorio de nuestro ordenador. Una vez localizado (normalmente suele encontrarse debajo o muy próximo al icono **Mi PC**), hacemos clic con el botón derecho del ratón y nos apareara el menú contextual en el que elegiremos la opción **Propiedades**, luego, en la ventana que aparece volvemos a hacer clic con el botón derecho del ratón

sobre el icono **Conexiones de red inalámbricas** y también seleccionamos la opción **Propiedades**.

Seleccionamos la pestaña **Redes Inalámbricas**, cuando estemos ubicados en esta seleccionaremos **Opciones Avanzadas.**



De nuevo veremos una nueva ventana, en la que hay que comprobar que está seleccionada la opción **Cualquier red disponible (punto de acceso preferido)** o **Sólo redes de equipo a equipo (ad hoc)**.

Nota: Si ya tenemos conexiones inalámbricas creadas previamente elegimos la que va hacer nuestra red Ad Hoc, en caso contrario se debe crear la conexión, siguiendo los siguientes pasos:

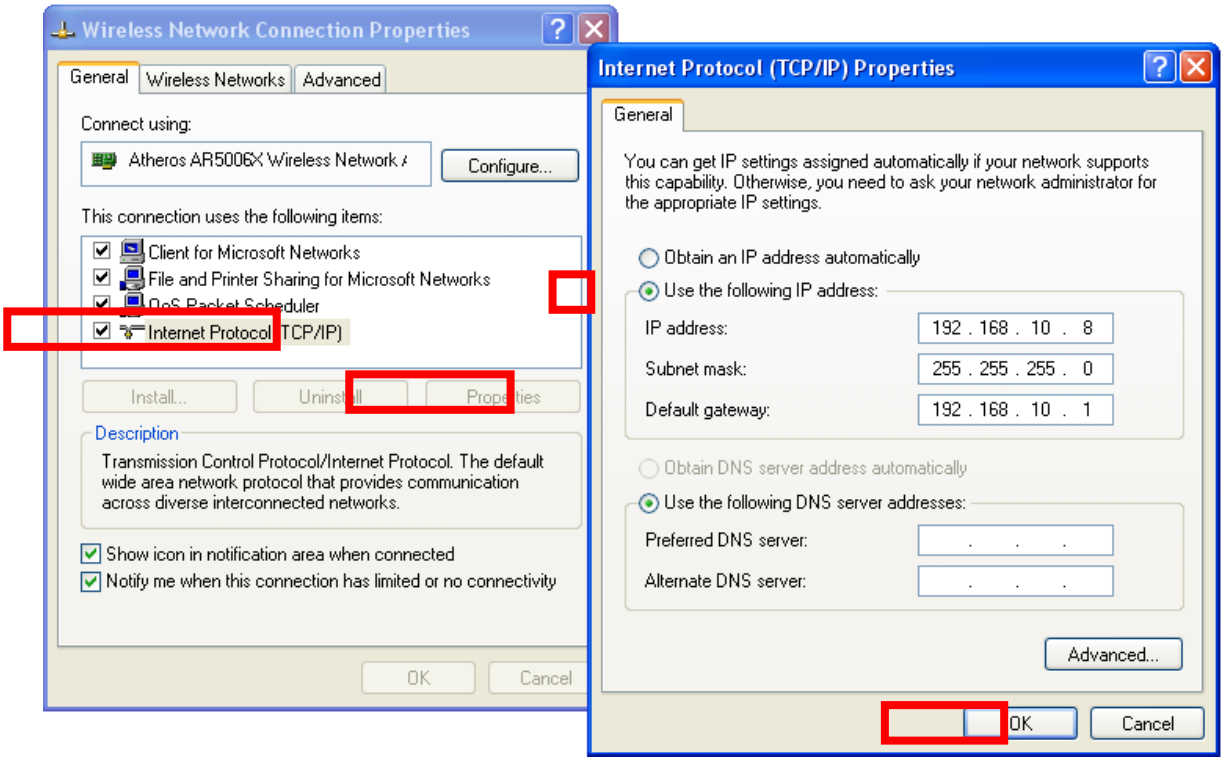
1. Damos clic en el botón **Agregar** de la primera ventana, aparecerá la ventana de **Propiedades de red inalámbrica**

2. Asignamos un nombre a la red en la casilla **Nombre de red (SSID)**, que en este caso la hemos llamado **Red 1**

La casilla (*Esta es una red de tipo (AD-HOC). No utilizan puntos de acceso inalámbrico*), debe estar marcada.

Procedemos a asignar las IP a los equipos que van hacer parte de la red, utilizaremos las IP asignadas en la primera grafica IP en el rango 192.168.0.201 al 192.168.0.203, con mascara de red 255.255.255.0.

Como ya sabemos esto lo hacemos en la ventana **Propiedades de Conexiones de red inalámbricas,** damos clic sobre el **Protocolo de Internet (TCP/IP)** y luego sobre el botón Propiedades. Nos debe quedar algo como la siguiente gráfica:

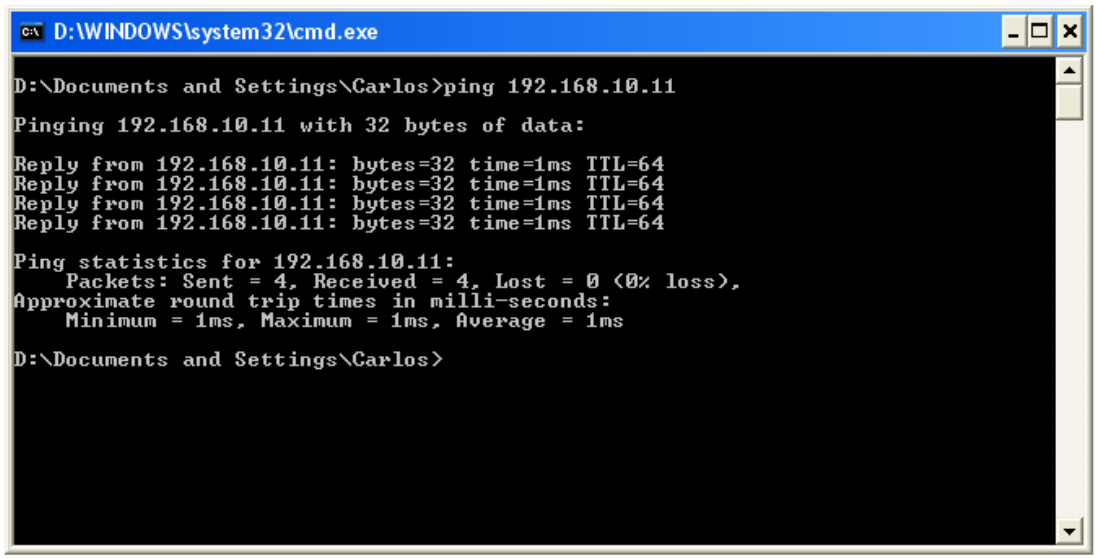


El paso anterior lo haremos en todos los computadores y dispositivos que conforman la red.

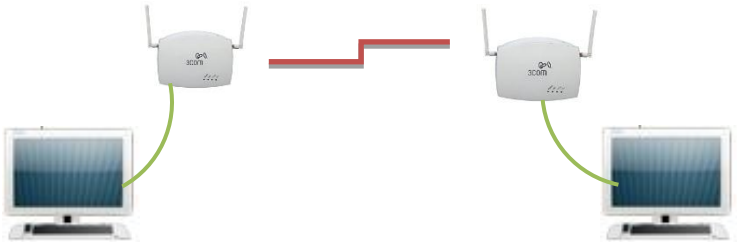
Realizado esto ya dispondremos de nuestra *Red Wifi AD Hoc* y podremos compartir archivos, documentos y realizar trabajos en grupo.

Para verificar esto hacemos ping cíclico es decir cada PC, hacemos hará ping a los otros para ver si existe comunicación entre ellos, como lo ilustramos a continuación:

Hacemos ping desde el equipo con IP **192.168.10.8**, hacia el dispositivo movil, y obtenemos lo siguiente:


D:\WINDOWS\system32\cmd.exe
D:\Documents and Settings\Carlos>ping 192.168.10.11
Pinging 192.168.10.11 with 32 bytes of data:
Reply from 192.168.10.11: bytes=32 time=1ms TTL=64
Reply from 192.168.10.11: bytes=32 time=1ms TTL=64
Reply from 192.168.10.11: bytes=32 time=1ms TTL=64
Reply from 192.168.10.11: bytes=32 time=1ms TTL=64
Ping statistics for 192.168.10.11:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 1ms, Average = 1ms
D:\Documents and Settings\Carlos>

Configuración Red Infraestructura (Wireless Bridge – Modo Bridge)



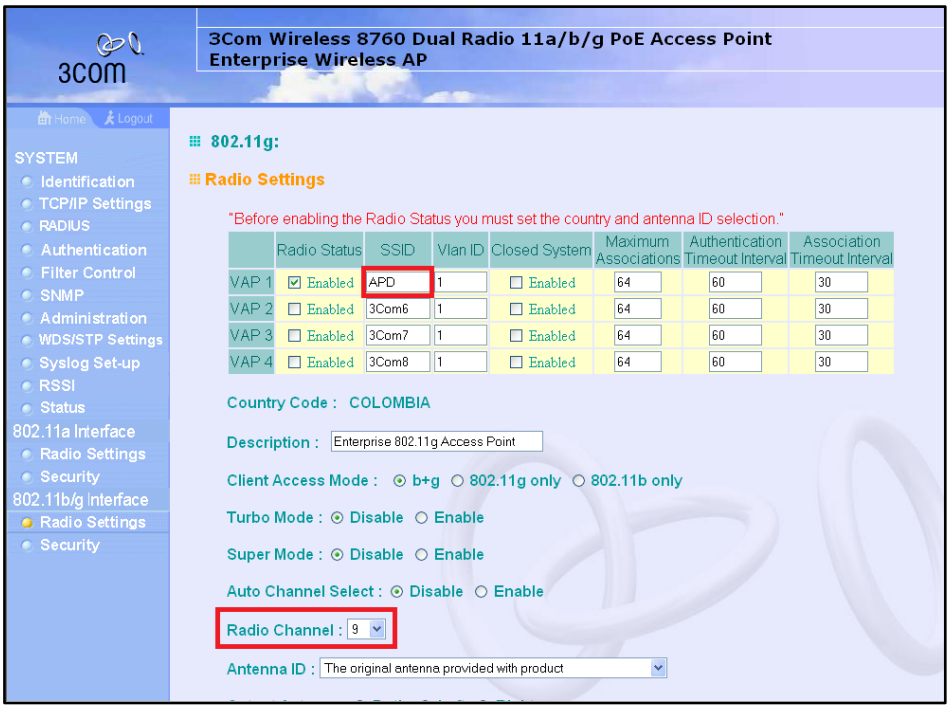
PRACTICA

---

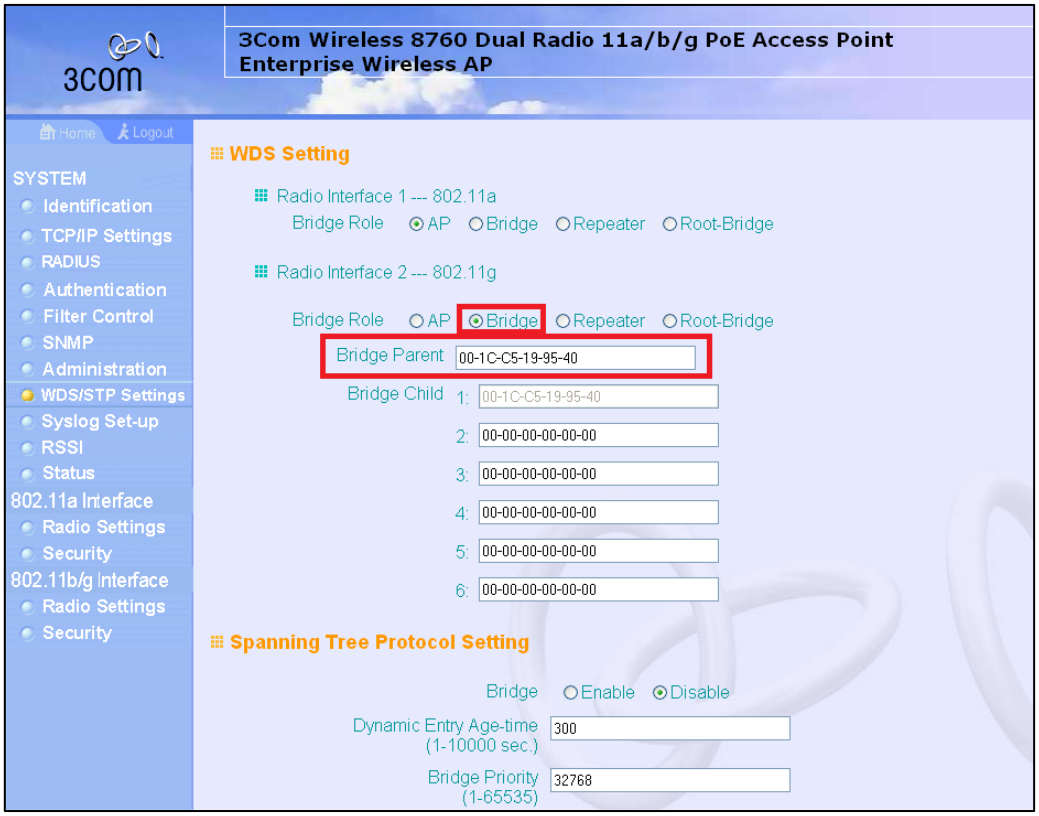
1. Se configura el Access Point (AP)

Por defecto, la dirección IP del AP es 169.254.2.1 y se entra al AP con el nombre de usuario *admin* y la contraseña *password*, luego se va a TCP/IP Settings y desactivamos (disable) el Cliente DHCP y configuramos manualmente la dirección IP del AP como se ha realizado en las practicas anteriores.

En esta práctica los AP utilizaran los mismo SSID y CHANNE, procedemos a configurarlos, como se muestra en la gráfica (en *este caso mostraremos la configuración del AP con IP:192.168.10.6)*:



Luego en el panel de WDS/STP settings, configuramos el funcionamiento del AP en modo BRIDGE, y le asignamos la dirección MAC del AP remoto, como se muestra en la grafica:



Nota: Para la configuración de los equipos seguimos utilizando la implementada en la práctica *Configuración Red Infraestructura (Un Access Point)*, A continuación se detalla la configuración de todos los equipos que intervienen en la práctica.

AP1

IP: 192.068.10.6

SSID: APD

CHANNEL: 9

MAC:00-1C-C5-A5-B6-80

AP2

IP: 192.068.10.20

SSID: APD

CHANNEL: 9

MAC: 00-1C-C5-19-95-40

EQUIPO 1

IP: 192.168.10.6

MASCARA 255.255.255.0

Puerta Enlace: 192.168.10.1

EQUIPO 2

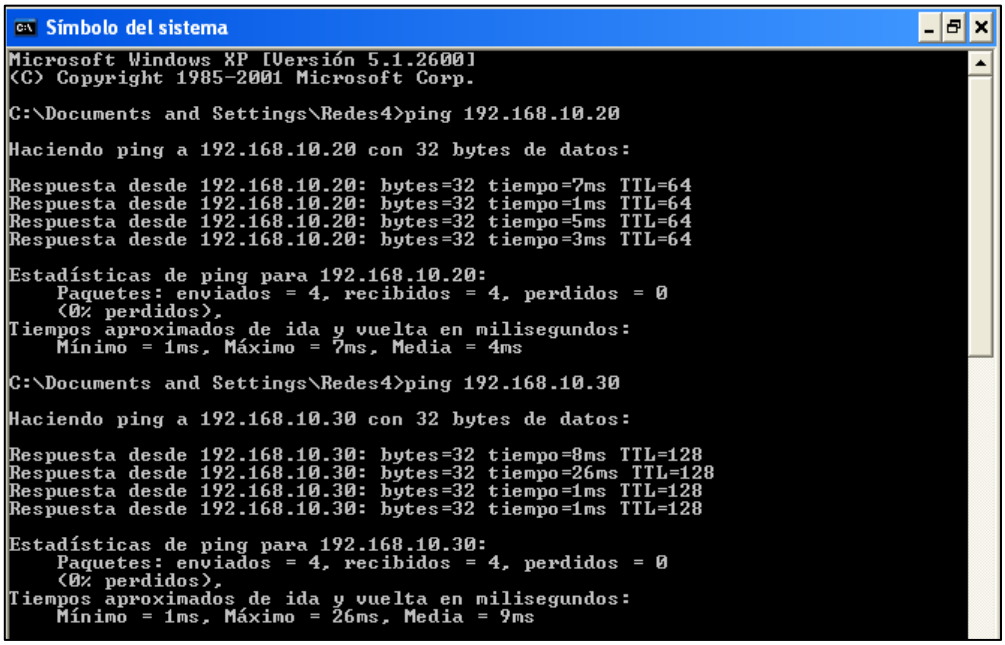
IP: 192.168.10.30

MASCARA 255.255.255.0

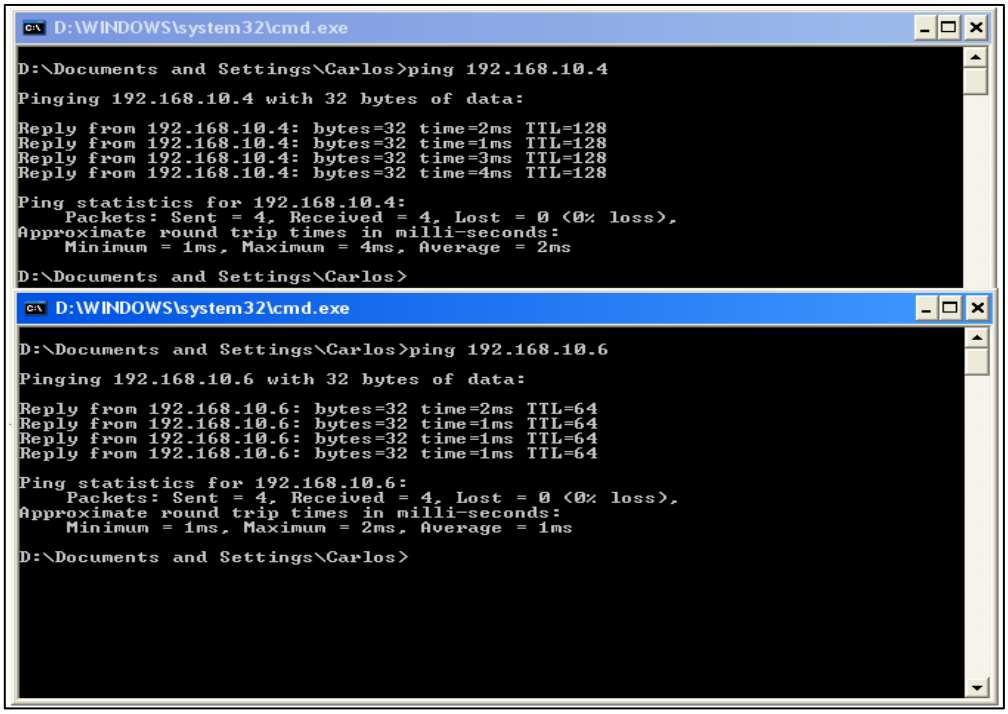
Puerta Enlace: 192.168.10.1

Luego de configurados todos los equipos hacemos la prueba de conectividad:

Hacemos ping desde el **EQUIPO1**, hacia el AP con IP: 192.168.10.20 y el equipo: 192.168.10.30



Hacemos ping desde el **EQUIPO2**, hacia el AP con IP: 192.168.10.6 y el equipo : 192.168.10.4


D:\WINDOWS\system32\cmd.exe
D:\Documents and Settings\Carlos>ping 192.168.10.4
Pinging 192.168.10.4 with 32 bytes of data:
Reply from 192.168.10.4: bytes=32 time=2ms TTL=128
Reply from 192.168.10.4: bytes=32 time=1ms TTL=128
Reply from 192.168.10.4: bytes=32 time=3ms TTL=128
Reply from 192.168.10.4: bytes=32 time=4ms TTL=128
Ping statistics for 192.168.10.4:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 4ms, Average = 2ms
D:\Documents and Settings\Carlos>
D:\WINDOWS\system32\cmd.exe
D:\Documents and Settings\Carlos>ping 192.168.10.6
Pinging 192.168.10.6 with 32 bytes of data:
Reply from 192.168.10.6: bytes=32 time=2ms TTL=64
Reply from 192.168.10.6: bytes=32 time=1ms TTL=64
Reply from 192.168.10.6: bytes=32 time=1ms TTL=64
Reply from 192.168.10.6: bytes=32 time=1ms TTL=64
Ping statistics for 192.168.10.6:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 2ms, Average = 1ms
D:\Documents and Settings\Carlos>