DISEÑO DE UNA RED INALÁMBRICA CORPORATIVA

Ing. Francisco Palacios Ortiz
Ing. Diana Espinoza Villón
Ing Fausto Orozco Lara

compAS
Grupo de Capacitación e investigación pedagógica

DISEÑO DE UNA RED INALÁMBRICA CORPORATIVA

PRIMERA EDICIÓN

Diseño de una red inalámbrica corporativa

Autores

ING. FRANCISCO PALACIOS ORTIZ
ING. DIANA ESPINOZA VILLÓN
ING. FAUSTO RAÚL OROZCO LARA

Primera edición, julio 2017

Libro sometido a revisión de pares académicos.

Edición
Diagramación
Diseño
Publicación
Maquetación.
Grupo Compás
Cámara Ecuatoriana del Libro - ISBN-E: 978-9942-760-31-9
Guayaquill - Ecuador

PRÓLOGO

Haciendo una descripción de la tecnología *"wireless"* sus cualidades, ventajas y desventajas, se promueve la introducción de esta tecnología a la red de la corporación Adsamed, tomando en consideración el diseño creado pensando en la infraestructura ya montada por la empresa, con características escalables y heterogéneas en toda su arquitectura, las mismas que permitirán a la empresa ir creciendo en usuarios a la medida de su demanda ya sea a corto, mediano o largo plazo.

En el presente libro se encuentran la mayoría de los aspectos de la red inalámbrica para la corporación Adsamed, la misma que en su primera instancia se implementará en la oficina matriz tomando en consideración los estándares y fabricantes de dispositivos que existen en el mercado.

ÍNDICE GENERAL

CAPÍTULO I: ESTADO DEL ARTE DE REDES INLÀMBRICAS 7

Evolución de las redes inalámbricas 8

Microondas 8

El infrarrojo 10

De Larga Distancia y De Corta Distancia 12

Ventajas de las WLAN Sobre Las Redes Fijas 16

Desventajas de las Redes Inalámbricas 17

El modelo OSI 19
Capas del modelo OSI 20

El modelo TCP/IP 25
Los protocolos de Internet 26

Topología 26
Topología en estrella 27
Topología en bus 27
Topología en anillo 28

Pseudotopología de las redes inalámbricas 30

CAPÍTULO II: ANÁLISIS DE REDES INALÁMBRICAS QUE EXISTEN EN EL MERCADO 31

Introducción 32

Wavelan de AT&T 34

Rangelan2 de Proxim inc. 35

Airlan de Soleteck 37

Netwave de Xircom inc. 38

Decidiendo por una WLAN 40

Funcionamiento 41

Modo infraestructurado 42

LAN inalámbrica con infraestructura ad-hoc 42

CAPÍTULO III: DISEÑO DE LA RED INALÀMBRICA PARA ADSAMED..... 61

Introducción..... 61

Componentes y operación de la LAN inalámbrica de ADSAMED. 61
Componentes de la red Inalámbrica de ADSAMED 68
Componentes de la red Inalámbrica de ADSAMED 69

Componentes relacionados con la WLAN de ADSAMED 72
Instalación y Configuración de Servidor RADIUS 73
Instalación de "Service Pack" 1 de Windows Server 2008 R2. 74
Instalación Network Policy Service NPS 77
Configuración en el Active Directory 81

Componentes relacionados con la seguridad de WLAN de ADSAMED 83

Configuración y verificación del acceso a la red inalámbrica de ADSAMED 103

Resolución de problemas de acceso al cliente inalámbrico. 103

CONCLUSIONES Y RECOMENDACIONES 101

Conclusiones 101

Recomendaciones 102

REFERENCIAS BIBLIOGRÀFICAS..... 108

GLOSARIO DE TÉRMINOS..... 111

CAPITULO 1

ESTADO DEL ARTE DE REDES INLÀMBRICAS

CAPITULO 1

ESTADO DEL ARTE DE REDES INLÀMBRICAS

Evolución de las redes inalámbricas

Las conexiones inalámbricas son mucho más que el sueño de aquellos que nunca consiguieron deshacer el lío entre los cables del televisor, el video y la consola. Aunque la más popular es el Wi-Fi (Fidelidad inalámbrica), hablar de redes inalámbricas supone también hablar de satélites, móviles, Internet y domótica entre otros.

Los expertos comenzaron a investigar en las redes inalámbricas hace ya más de 30 años, Las LAN inalámbricas se remontan a la publicación en 1979 de los resultados de un experimento realizado por ingenieros de IBM (*Internacional Bussines Machines*) en Suiza, consistente en utilizar enlaces infrarrojos para crear una red local en una fábrica. Estos resultados, pueden considerarse como el punto de partida en la línea evolutiva de esta tecnología.
Las investigaciones siguieron adelante tanto con infrarrojos como con microondas.

Microondas

Se denomina **microondas** a las ondas electromagnéticas definidas en un rango de frecuencias determinado; generalmente de entre 1 GHz y 300 GHz, es decir, longitudes de onda de entre 30 centímetros a 1 milímetro.

El rango de las microondas está incluido en las bandas de radiofrecuencia, concretamente en las de UHF (*ultra-high frequency* - frecuencia ultra alta) 0,3–3 GHz, SHF (*super-high frequency* - frecuencia súper alta) 3–30 GHz y EHF (*extremely-high frequency* - frecuencia extremadamente alta) 30–300 GHz. Otras bandas de radiofrecuencia incluyen ondas de menor frecuencia y mayor longitud de onda que las microondas.

La existencia de ondas electromagnéticas, de las cuales las microondas forman parte del espectro de alta frecuencia, fueron predichas por Maxwell en 1864 a partir de sus famosas Ecuaciones. En 1888, Heinrich Rudolf Hertz fue el primero en demostrar la existencia de ondas electromagnéticas.

Las microondas pueden ser generadas de varias maneras, generalmente divididas en dos categorías: dispositivos de estado sólido y dispositivos basados en tubos de vacío. Los dispositivos de estado sólido para microondas están basados en semiconductores de silicio o arseniuro de galio, e incluyen transistores de efecto campo (FET), transistores de unión bipolar (BJT), diodos Gunn (Diodo usado en la electrónica de alta frecuencia) y diodos IMPATT (Tiempo de Tránsito por Avalancha con Ionización por Choque). Se han desarrollado versiones especializadas de transistores estándar para altas velocidades que se usan comúnmente en aplicaciones de microondas.

En la figura 2.1 podemos observar la torre de telecomunicaciones en Wellington Nueva Zelanda mediante microondas el rango de frecuencias de microondas es utilizada para transmisiones de televisión (500–900 MHz, dependiendo de los países) o telefonía móvil (850–900 MHz y 1800–1900 MHz).

Figura 2.1: Torre de Telecomunicaciones de Wellington Nueva Zelanda
Fuente: www.rtve.es

El infrarrojo

El infrarrojo es un tipo de luz que no se puede ver con los ojos. Los ojos pueden solamente ver lo que se conoce como luz visible. La luz infrarroja nos brinda información especial que no se puede obtener de la luz visible. Nos muestra cuánto calor tiene alguna cosa y nos da información sobre la temperatura de un objeto. Todas las cosas tienen algo de calor e irradian luz infrarroja. Incluso las cosas que se pensaba que son muy frías, como un cubo de hielo, irradian algo de calor. Los objetos fríos irradian menos calor que los objetos calientes. Entre más caliente sea algo más es el calor irradiado y entre más frío es algo menos es el calor irradiado. Los objetos calientes brillan más luminosamente en el infrarrojo porque irradian más calor y más luz infrarroja. Los objetos fríos irradian menos calor y luz infrarroja, apareciendo menos brillantes en el infrarrojo. Cualquier cosa que tenga una temperatura irradia calor o luz infrarroja. En la Figura 1.2 las imágenes infrarrojas poseen colores diferentes estos colores son usados para representar diferentes temperaturas. Se puede encontrar cuál temperatura es representada por un color usando la escala color-temperatura a la derecha de las imágenes. Las temperaturas están en grados Fahrenheit.

En la figura 2.2. del lado izquierdo se muestra una imagen infrarroja de una taza de metal conteniendo una bebida muy caliente. Se Observa los anillos de color demostrando el calor proveniente del líquido a través de la taza de metal. Se puede observar esto también en la cuchara de metal. A la derecha está una imagen infrarroja de un cubo de hielo derritiéndose. Observa los anillos de color mostrando cómo el agua ya derretida se calienta mientras se desplaza alejándose del cubo. A pesar de que el cubo de hielo es frío, aún irradia calor, como se puede ver relacionado el color del cubo de hielo con su temperatura.

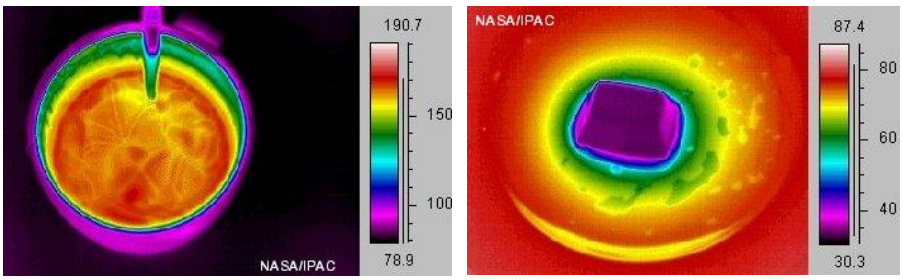


Figura 2.2: Taza de Metal y Cubo de Hielo en infrarrojo
Fuente: legacy.spitzer.caltech.edu

En los años 80 se asignaron las bandas ISM (*Industrial, Scientific and Medical*) 902-928 MHz, 2.4-2.4835 GHz, 5.725-5.85 GHz a las redes inalámbricas. Las bandas ISM son bandas de frecuencias para uso comercial y sin licencia (las utilizadas por los teléfonos inalámbricos domésticos DECT (Digital Enhanced Cordless Telecommunication), los microondas, o los dispositivos *Bluetooth*. A mediados del año 1997, el IEEE (Institute of Electrical and Electronics Engineers) hizo público el estándar 802.11 que definía las especificaciones para las WLAN (Wireless Local Area Nerwork), y poco después, salió a la luz el estándar IEEE 802.11.b que daría lugar posteriormente a la denominación Wi-Fi. El estándar 802.11 opera en las bandas de 2.4 GHz y 5 GHz. Cada uno de los 14 canales asignados al IEEE 802.11 tiene un ancho de banda de 22 MHz y la gama de frecuencias disponible va desde los 2.412 GHz hasta los 2.484 GHz.

Entre los estándares más utilizados en la banda de 2.4 GHz se encuentran el 802.11a: (5.1-5.2 GHz, 5.2-5.3 GHz, 5.7-5.8 GHz), velocidad de transmisión de 54 Mbps y OFDM *(Orthogonal Frequency Division Multiplexing, Multiplexado por División de Frecuencia Ortogonal)*, el 802.11b: (2,4-2,485 GHz), 11 Mbps y el 802.11g: (2,4-2,485 GHz), 54 Mbps. La modulación OFDM fue aprobada en el año 2003 para dar mayor velocidad con cierto grado de compatibilidad al equipamiento 802.11b. Otros estándares para comunicaciones inalámbricas son el IEEE 802.16 Wimax (Worldwide Interoperability for Microwave Access), HomeRF, Bluetooth, IEEE 802.15 para WPAN (Wireless Personal Área Networks) e HiperLAN. C.

En los últimos años las redes de área local inalámbricas WLAN, están ganando mucha popularidad, que se ve acrecentada conforme sus prestaciones aumentan y se descubren nuevas aplicaciones para ellas. Las WLAN permiten a sus usuarios acceder a información y recursos en tiempo real sin necesidad de estar físicamente conectados a un determinado lugar.

Con las 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 empresas donde está instalada. Un usuario dentro de una red WLAN puede transmitir y recibir voz, datos y vídeo dentro de edificios, entre edificios o "campus" universitarios e inclusive sobre áreas metropolitanas a velocidades de 11 Mbps, o superiores como el 802.11n.

Pero no solamente encuentran aplicación en las empresas, sino que su extensión en ambientes públicos, en áreas metropolitanas, como medio de acceso a Internet o para cubrir zonas de alta densidad de usuarios o puntos calientes "hot spots", en las próximas redes de última generación se ven como las soluciones de mayor interés durante los próximos años.

Muchos de los fabricantes de computadoras y equipos de comunicaciones como son los PDA *(Personal Digital Assistants)*, módems, terminales de punto de venta y otros dispositivos están introduciendo aplicaciones soportadas en las comunicaciones inalámbricas.

No se espera que las redes inalámbricas lleguen a remplazar a las redes cableadas, sin embargo se pueden mezclar las redes cableadas y las inalámbricas, y de esta manera generar una "Red Híbrida" y poder resolver los últimos metros hacia la estación de trabajo. Se puede considerar que el sistema cableado sea la parte principal y la inalámbrica le proporcione movilidad adicional al equipo y el operador se pueda desplazar con facilidad dentro de un almacén o una oficina. Existen dos amplias categorías de Redes Inalámbricas:

De Larga Distancia y De Corta Distancia

- **De Larga Distancia.-** Estas son utilizadas para transmitir la información en espacios que pueden variar desde una misma ciudad o hasta varios países circunvecinos, mejor conocido como Redes de Área Metropolitana MAN (***Metropolitan Area Network***).

Una **red de área metropolitana,** es una red de alta velocidad (banda ancha) que da cobertura en un área geográfica extensa, proporciona capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y vídeo, sobre medios de transmisión tales como fibra óptica y par trenzado, las redes MAN BUCLE, ofrecen velocidades de 10 Mbps, 20 Mbps, 45 Mbps, 75 Mbps, sobre pares de cobre y 100 Mbps, 1 Gbps y 10 Gbps mediante Fibra Óptica.

Las Redes MAN BUCLE, se basan en tecnologías "Bonding", de forma que los enlaces están formados por múltiples pares de cobre con el fin de ofrecer el ancho de banda necesario.

El concepto de red de área metropolitana representa una evolución del concepto de red de área local a un ámbito más amplio, cubriendo áreas mayores que en algunos casos no se limitan a un entorno metropolitano sino que pueden llegar a una cobertura regional e incluso nacional mediante la interconexión de diferentes redes de área metropolitana.

Este tipo de redes es una versión más grande que la LAN y que normalmente se basa en una tecnología similar a esta, La principal razón para distinguir una MAN con una categoría especial es que se ha adoptado un estándar para que funcione, que equivale a la norma IEEE.

Existen dos tipos de redes de larga distancia: Redes de Conmutación de Paquetes (públicas y privadas) y Redes Telefónicas Celulares.

- **Redes de Conmutación (públicas y privadas).-** Conmutación de Paquetes (Packet Switching en inglés) es el establecimiento, por parte de una red de comunicaciones, de un intercambio de bloques de información (o "paquetes") con un tamaño específico entre dos puntos, un emisor y un receptor. En el origen, extremo emisor, la información se divide en "paquetes" a los cuales se les indica la dirección del destinatario. Esto es, cada paquete contiene, además

de datos, un encabezado con información de control (prioridad y direcciones de origen y destino).

Los paquetes se transmiten a través de la red y, posteriormente, son reensamblados en el destino obteniendo así el mensaje original. En cada nodo de red, un paquete puede ser almacenado brevemente y encaminado dependiendo de la información de la cabecera. De esta forma, pueden existir múltiples vías o "caminos" de un punto a otro, siendo gestionado por la red el camino óptimo. Las redes basadas en la conmutación de paquetes evitan que mensajes de gran longitud signifiquen grandes intervalos de espera ya que limitan el tamaño de los mensajes transmitidos. La red puede transmitir mensajes de longitud variable pero con una longitud máxima.

Dominio Público

Una red de comunicaciones se denomina "Red Pública" cuando se utiliza, total o parcialmente, para la prestación de servicios de telecomunicaciones disponibles para el público. A este tipo de redes puede acceder cualquier usuario y comunicarse con cualquier otro que esté conectado a ella, sin ningún tipo de limitación.

Las Redes Públicas son de libre utilización por cualquier usuario que se abone a las mismas. Tienen grandes ventajas frente a las privadas en cuanto a economía de escala, aunque por el momento, sus prestaciones pueden resultar inferiores.

Las redes públicas de conmutación de circuitos proporcionan una buena eficiencia y resultan económicas solamente si existe una transmisión de datos prácticamente continua en dos sentidos. La transparencia de la conexión permite la transmisión de datos en cualquier código que acuerden los comunicantes.

Dominio Privado

Una red de comunicaciones pertenece al dominio privado (Red privada) cuando es ofertada únicamente para uso interno. Estas redes solas abarcan a los usuarios que pertenezcan a una determinada organización y solo se pueden comunicar con miembros de la misma organización.

Redes Telefónicas Celulares.- La red de telefonía celular o móvil, está formada por un sistema telefónico por el cual, mediante la combinación de redes de estaciones receptora - transmisoras de radio y centrales telefónicas de conmutación, se puede establecer la comunicación entre los teléfonos celulares o entre teléfonos celulares y teléfonos de línea fija.

El término celular, el cual se refiere a la **telefonía móvil**, tiene como origen el hecho de que las estaciones base, las encargadas de enlazar por radio a los teléfonos portátiles con los controladores de estaciones base, se encuentran dispuestas en forma de una malla, formando así celdas o células en la disposición de un panal de abejas.

De esta forma, cada estación se sitúa en un nudo de estas celdas y tiene asignado un conjunto de frecuencias de recepción y de transmisión propio. Como existe un número limitado de frecuencias, a partir de esta disposición se pueden reutilizar las mismas frecuencias en otras celdas, siempre y cuando no sean adyacentes, y así evitar interferencias entre ellas, en las redes como la CDMA este concepto es erróneo

Aunque decir teléfono móvil o teléfono celular es correcto, es más apropiado referirse a un teléfono celular que a un móvil, esto se debe a que un teléfono inalámbrico es también un teléfono móvil ya que se puede mover. Sería incluso más adecuado denominarlos “portátiles”, ya que así se estaría acentuando la idea de que no sólo se mueven por sí solos.

- **De Corta Distancia.-** Estas son utilizadas principalmente en redes corporativas cuyas oficinas se encuentran en uno o varios edificios que no se encuentran muy retirados entre sí, con velocidades del orden de 280 Kbps hasta los 2 Mbps.

Ventajas de las WLAN Sobre Las Redes Fijas

A continuación se detallan las ventajas:

- **Movilidad**

  Las redes inalámbricas proporcionan a los usuarios de una LAN acceso a la información en tiempo real en cualquier lugar dentro de la organización o el entorno público (zona limitada) en el que están desplegadas.

- **Simplicidad y rapidez en la instalación**

  La instalación de una WLAN es rápida y fácil y elimina la necesidad de tirar cables a través de paredes y techos.

- **Flexibilidad en la instalación**

  La tecnología inalámbrica permite a la red llegar a puntos de difícil acceso para una LAN cableada.

- **Costo de propiedad reducido**

  Mientras que la inversión inicial requerida para implementar la red inalámbrica puede ser más alta que el costo en hardware de una LAN, la inversión de toda la instalación y el costo durante el ciclo de vida puede ser significativamente inferior. Los beneficios a largo plazo son superiores en ambientes dinámicos que requieren acciones y movimientos frecuentes.

- **Escalabilidad**

  Los sistemas de WLAN pueden ser configurados en una variedad de topologías para satisfacer las necesidades de las instalaciones y aplicaciones específicas. Las configuraciones son muy fáciles de cambiar y además resulta muy fácil la incorporación de nuevos usuarios a la red.

- **Red Híbrida**

  Otra de las grandes ventajas que se deriva del empleo del Punto de Acceso es la posibilidad de enlazar una red inalámbrica con una red de cable Ethernet. Ambas redes, inalámbrica y de cable, quedarían de este modo integradas en una única red global, de manera que cualquier PC de la red de cable pueda comunicar con cualquier PC de la red inalámbrica y viceversa.

Desventajas de las Redes Inalámbricas

Evidentemente, como todo en la vida, no todo son ventajas, las redes inalámbricas también tiene puntos negativos en su comparación con las redes de cable.

Los principales inconvenientes de las redes inalámbricas son los siguientes:

- **Menor velocidad de transmisión.**

  IEEE 802.11n fue pensado para mejorar las tasas de datos y el alcance de la WLAN sin requerir energía adicional o asignación de la banda RF. 802.11n utiliza radios y antenas múltiples en los puntos finales, y cada uno transmite en la misma frecuencia para establecer "stream" (Protocolo de comunicación de capa de transporte) múltiples. La tecnología de entrada múltiple/salida múltiple (MIMO) divide un "stream" rápido de tasa de datos en múltiples canales de menor tasa y los transmite simultáneamente por las radios y antenas disponibles. Esto permite una tasa de datos teórica máxima de 248 Mbps por medio de dos "streams".

- **Mayor inversión inicial.**

  Para la mayoría de las configuraciones de la red local, el costo de los equipos de red inalámbricos es superior al de los equipos de red cableada aunque existen algunas soluciones más económicas.

- **Seguridad.**

  Las redes inalámbricas tienen la particularidad de no necesitar una conexión por medio de un cable para conectarse a una red específica para funcionar. Esto fundamentalmente es una ventaja, pero se convierte en una desventaja

cuando se piensa que cualquier persona con una computadora portátil solo necesita estar dentro del área de cobertura de la red para poder intentar acceder a ella. Como el área de cobertura no está definida por paredes o por ningún otro medio físico, a los posibles intrusos no les hace falta estar dentro de un edificio o estar conectado a un cable. Además, el sistema de seguridad que incorporan las redes Wi-Fi no es de lo más fiables. A pesar de esto también es cierto que ofrece una seguridad válida para la inmensa mayoría de las aplicaciones y que ya hay disponible un nuevo sistema de seguridad (WPA) que hace a Wi-Fi mucho más confiable.

- **Interferencias**.

  Las redes inalámbricas funcionan utilizando el medio radio eléctrico 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. Además, todas las redes Wi-Fi funcionan en la misma banda de frecuencias incluida la de los vecinos. Este hecho hace que no se tenga la garantía de que el entorno radioelectrónico este completamente limpio 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. No obstante, 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. La tecnología que actualmente se está instalando y que ha adquirido una mayor popularidad es la conocida como Wi-Fi (IEEE 802.11b Ahora es la 802.11g). Sin embargo, ya existen tecnologías que ofrecen una mayor velocidad de transmisión como la 802.11n y unos mayores niveles de seguridad, es posible que, cuando se popularice esta nueva tecnología, se deje de comenzar la actual o, simplemente se deje de prestar tanto apoyo a la actual. Lo cierto es que las leyes del mercado vienen también marcadas por las necesidades del cliente y, aunque existe una incógnita, los

fabricantes no querrán perder el tirón que ha supuesto Wi-Fi y harán todo lo posible para que los nuevos dispositivos sean compatibles con los actuales.

El modelo OSI

El estándar internacional para Sistemas Abiertos de Interconexión, OSI (por su sigla en inglés: *Open Systems Interconnection*), se define en el documento ISO/IEC 7498-1, emanado de la *International Standards Organization* y la *International Electrotechnical Comission*.

El modelo OSI divide el tráfico de la red en una cantidad de capas, véase la figura 2.3. Cada capa es independiente de las capas que la rodean y cada una se apoya en los servicios prestados por la capa inferior mientras que proporciona sus servicios a la capa superior. La separación entre capas hace que sea fácil diseñar una ***pila de protocolos*** (*protocol stack*) muy elaborada y confiable, tal como la difundida pila **TCP/IP** (Protocolo de control de transmisión/Protocolo de Internet). Una pila de protocolos es una implementación real de un marco de comunicaciones estratificado. El modelo OSI no define los protocolos que van a usarse en una red en particular, sino que simplemente delega cada "trabajo" de comunicaciones a una sola capa dentro de una jerarquía bien definida.

Mientras que la especificación ISO/IEC 7498-1 determina cómo deberían interactuar las capas, los detalles de la implementación real se dejan al fabricante. Cada capa puede implementarse en el hardware (es más común para las capas inferiores), o en el software. Siempre y cuando la interfaz entre capas se adhiera al estándar, los instaladores son libres de usar cualquier medio a su disposición para construir su pila de protocolos. Esto quiere decir que cualquier capa de un fabricante A puede operar con la misma capa de un fabricante B (suponiendo que las especificaciones relevantes se implementen e interpreten correctamente).

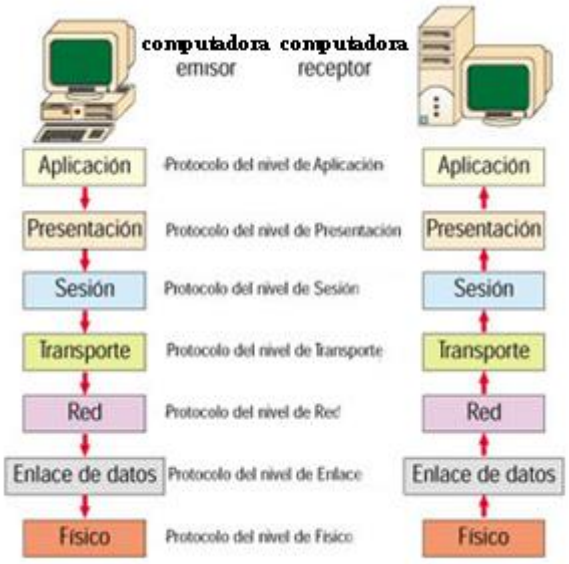


Figura 2.3: Capas del Modelo OSI
Creada por: Francisco Palacios.

Los niveles de la torre se comunican en dos direcciones:

- ✓ **Horizontal.** La comunicación horizontal sólo se da entre niveles homónimos. Se podría pensar –y de hecho es así– que todo el nivel constituye un único sistema distribuido que tiene un representante en cada uno de los equipos. Un protocolo de nivel *i* (en el que *i* es el identificador del nivel correspondiente) especifica el formato, el significado y la temporización de la información que circula entre los miembros de este sistema distribuido.

- ✓ **Vertical.** La comunicación vertical sólo se da entre niveles adyacentes de un mismo sistema. Este tipo de comunicación posee un carácter totalmente local; es decir, puede materializarse por mecanismos de software (llamadas a bibliotecas, comunicación entre procesos, etc.). De manera genérica, se denomina estos mecanismos *servicio de nivel i* (en el que *i* es el identificador del nivel que proporciona el servicio, e *i* + 1, el nivel que lo utiliza).

Capas del modelo OSI

La descripción de las diversas capas que componen este modelo es la siguiente:

- **Capa física**

  Es la encargada de transmitir los bits de información por la línea o medio utilizado para la transmisión. Se ocupa de las propiedades físicas y características eléctricas de los diversos componentes, de la velocidad de transmisión, si esta es unidireccional o bidireccional (simplex, dúplex).
  También de aspectos mecánicos de las conexiones y terminales, incluyendo la interpretación de las señales eléctricas.

  Como resumen de los cometidos de esta capa, se puede decir que se encarga de transformar un paquete de información binaria en una sucesión de impulsos adecuados al medio físico utilizado en la transmisión. Estos impulsos pueden ser eléctricos (transmisión por cable), electromagnéticos (transmisión Wireless) o luminosos (transmisión óptica). Cuando actúa en modo recepción el trabajo es inverso, se encarga de transformar estos impulsos en paquetes de datos binarios que serán entregados a la capa de enlace.

- **Capa de enlace**

  Puede decirse que esta capa traslada los mensajes hacia y desde la capa física a la capa de red. Especifica cómo se organizan los datos cuando se transmiten en un medio particular. Esta capa define como son los cuadros, las direcciones y las sumas de control de los paquetes Ethernet.

  Además del direccionamiento local, se ocupa de la detección y control de errores ocurridos en la capa física, del control del acceso a dicha capa y de la integridad de los datos y fiabilidad de la transmisión. Para esto agrupa la información a transmitir en bloques, e incluye a cada uno una suma de control que permitirá al receptor comprobar su integridad. Los datagramas recibidos son comprobados por el receptor. Si algún datagrama se ha corrompido se envía un mensaje de control al remitente solicitando su reenvío.

  La capa de enlace puede considerarse dividida en dos subcapas:

- **Control lógico de enlace LLC:** define la forma en que los datos son transferidos sobre el medio físico, proporcionando servicio a las capas superiores.

- **Control de acceso al medio MAC:** Esta subcapa actúa como controladora del hardware subyacente (el adaptador de red). De hecho el controlador de la tarjeta de red es denominado a veces "MAC driver", y la dirección física contenida en el hardware de la tarjeta es conocida como dirección principal y consiste en arbitrar la utilización del medio físico para facilitar que varios equipos puedan competir simultáneamente por la utilización de un mismo medio de transporte. El mecanismo CSMA/CD ("Carrier Sense Multiple Access with Collision Detection") utilizado en Ethernet es un típico ejemplo de esta subcapa.

- **Capa de Red**

  Esta capa se ocupa de la transmisión de los datagramas (paquetes) y de encaminar cada uno en la dirección adecuada tarea esta que puede ser complicada en redes grandes como Internet, pero no se ocupa para nada de los errores o pérdidas de paquetes. Define la estructura de direcciones y rutas de Internet. A este nivel se utilizan dos tipos de paquetes: paquetes de datos y paquetes de actualización de ruta. Como consecuencia esta capa puede considerarse subdividida en dos:

- **Transporte:** Encargada de encapsular los datos a transmitir (de usuario). Utiliza los paquetes de datos. En esta categoría se encuentra el protocolo **IP**.

- **Conmutación:** Esta parte es la encargada de intercambiar información de conectividad específica de la red. Los enrutadores son dispositivos que trabajan en este nivel y se benefician de estos paquetes de actualización de ruta. En esta categoría se encuentra el protocolo **ICMP** (Protocolo de mensajes

de control de Internet) responsable de generar mensajes cuando ocurren errores en la transmisión y de un modo especial de eco que puede comprobarse mediante ping (utilidad diagnóstica en redes).

Los protocolos más frecuentemente utilizados en esta capa son dos: X.25 e IP.

- **Capa de Transporte**

  Esta capa se ocupa de garantizar la fiabilidad del servicio, describe la calidad y naturaleza del envío de datos. Esta capa define cuando y como debe utilizarse la retransmisión para asegurar su llegada. Para ello divide el mensaje recibido de la capa de sesión en trozos (datagramas), los numera correlativamente y los entrega a la capa de red para su envío.

  Durante la recepción, si la capa de Red utiliza el protocolo **IP**, la capa de Transporte es responsable de reordenar los paquetes recibidos fuera de secuencia. También puede funcionar en sentido inverso multiplexando una conexión de transporte entre diversas conexiones de datos. Este permite que los datos provenientes de diversas aplicaciones compartan el mismo flujo hacia la capa de red.

  Un ejemplo de protocolo usado en esta capa es **TCP**, que con su homólogo **IP** de la capa de Red, configuran la suite **TCP/IP** utilizada en Internet, aunque existen otros como **UDP (**Protocolo de Datagrama de Usuario**)**, que es una capa de transporte utilizada también en Internet por algunos programas de aplicación.

- **Capa de Sesión**

  Es una extensión de la capa de transporte que ofrece control de diálogo y sincronización, aunque en realidad son pocas las aplicaciones que hacen uso de ella.

- **Capa de Presentación**

  Esta capa se ocupa de garantizar la fiabilidad del servicio, describe la calidad y naturaleza del envío de datos. Esta capa define cuando y como debe utilizarse la retransmisión para asegurar su llegada. Para ello divide el mensaje recibido de la capa de sesión en trozos (datagramas), los numera correlativamente y los entrega a la capa de red para su envío.

  Durante la recepción, si la capa de Red utiliza el protocolo IP, la capa de Transporte es responsable de reordenar los paquetes recibidos fuera de secuencia. También puede funcionar en sentido inverso multiplexando una conexión de transporte entre diversas conexiones de datos. Este permite que los datos provenientes de diversas aplicaciones compartan el mismo flujo hacia la capa de red.

  Esta capa se ocupa de los aspectos semánticos de la comunicación, estableciendo los arreglos necesarios para que puedan comunicar máquinas que utilicen diversa representación interna para los datos. Describe como pueden transferirse números de coma flotante entre equipos que utilizan distintos formatos matemáticos.

  En teoría esta capa presenta los datos a la capa de aplicación tomando los datos recibidos y transformándolos en formatos como texto imágenes y sonido. En realidad esta capa puede estar ausente, ya que son pocas las aplicaciones que hacen uso de ella.

- **Capa de Aplicación**

  Esta capa describe como hacen su trabajo los programas de aplicación (navegadores, clientes de correo, terminales remotos, transferencia de ficheros etc.). Esta capa implementa la operación con ficheros del sistema. Por un lado interactúan con la capa de presentación y por otro representan la interfaz con el usuario, entregándole la información y recibiendo los comandos que dirigen la comunicación.

Algunos de los protocolos utilizados por los programas de esta capa son **HTTP** (Protocolo de transferencia de hipertexto), **SMTP** (Simple Mail Transfer Protocol), **POP** (Protocolo de la oficina de correo), **IMAP** (protocolo de acceso a mensajes de Internet) etc.

El modelo TCP/IP

A diferencia del modelo OSI, el modelo TCP/IP no es un estándar internacional, y su definición varía. Sin embargo, es usado a menudo como un modelo práctico para entender y resolver fallas en redes Internet. La mayor parte de Internet usa TCP/IP, se puede plantear algunas premisas sobre las redes que las harán de más fácil comprensión. El modelo de redes TCP/IP describe las cinco capas que aparecen en la Tabla 1.1:

Capa	Nombre
5	Aplicación
4	Transporte
3	Internet
2	Enlace de Datos
1	Física

Tabla 2.1 Modelo TCP/IP
Creada por: Francisco Palacios.

En términos del modelo OSI, las capas cinco a siete quedan comprendidas en la capa superior (la Capa de Aplicación). Las primeras cuatro capas de ambos modelos son idénticas. Muchos ingenieros de redes consideran todo lo que está por encima de la capa cuatro como "sólo datos", que van a variar de aplicación a aplicación. Ya que las primeras tres capas son inter-operables para los equipos de casi todos los fabricantes, y la capa cuatro trabaja entre todos los anfitriones que usan TCP/IP, y todo lo que está por arriba de la capa cuatro es para aplicaciones específicas, este modelo simplificado funciona bien cuando se construyen o detectan fallas en redes TCP/IP. Se utiliza el modelo TCP/IP cuando se habla de redes en este libro.

Una manera de mirar al modelo TCP/IP es pensar en una persona que entrega una carta en un edificio de oficinas. Va a tener que interactuar primero con la calle (capa física), poner atención al tráfico de la misma (capa de enlace), doblar en los lugares correctos para conectarse con otras calles y arribar a la dirección correcta (capa Internet), ir al piso y oficina correcta (capa transporte), y finalmente encontrar el destinatario o recepcionista que puede recibir la carta (capa de aplicación). Una vez entregada la carta, el mensajero queda libre.

Las cinco capas pueden ser recordadas fácilmente usando la frase **F**avor **E**ntrar, **I**nmediatamente **T**omar el **A**scensor, para la secuencia de capas Física, **E**nlace de **D**atos, **I**nternet, **T**ransporte, y **A**plicación, o en inglés "*Please Don't Look In The Attic*," que se usa por "*Physical* / *Data Link* / *Internet* / *Transport* / *Application*".

Los protocolos de Internet

TCP/IP es la pila de protocolos más comúnmente usada en la Internet global. El acrónimo se lee en inglés ***Transmission Control Protocol***, e ***Internet Protocol***, respectivamente, pero en realidad se refiere a una familia completa de protocolos de comunicaciones relacionados. TCP/IP también se conoce como ***grupo de protocolo Internet***, y opera en las capas tres y cuatro del modelo TCP/IP.

Topología

Lo primero que caracteriza una red local es la manera en que se conectan las estaciones; es decir, la forma que adopta el medio compartido entre las mismas. Básicamente existen tres topologías posibles:

• Topología en estrella.

• Topología en bus.

• Topología en anillo

Topología en estrella

La topología en estrella consiste en conectar cada computadora a un punto central, que puede ser tan sencillo como una simple unión física de los cables. Véase figura 2.4

Cuando una computadora pone una trama en la red, ésta aparece de inmediato en las entradas del resto de computadoras.

Aunque se han definido estándares para este tipo de redes, en la actualidad ya casi no existen, puesto que no aportan ninguna ventaja sobre el resto y sí muchos inconvenientes.

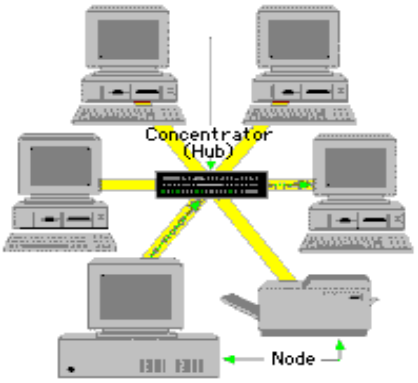


Figura 2.4: Topología tipo estrella
Fuente: www.blogextremo.com/conceptolanmedios

Topología en bus

La topología en bus consiste en un cable al que se unen todas las estaciones de la red. Todas las computadoras están pendientes de si hay actividad en el cable. Véase figura 2.5

En el momento en que una computadora pone una trama, todas las computadoras la cogen y miran si son el destinatario de la misma. Si es así, se la quedan, en caso contrario, la descartan.

Las primeras redes en bus utilizaban un cable coaxial grueso, conectores tipo BNC, y las computadoras se conectaban al mismo con un dispositivo denominado

transceptor (transceiver), que era exterior. Con posterioridad, apareció una nueva versión, con un cable más fino (*thin-ethernet*) y con unos transceptores más pequeños, de manera que se podían integrar en el adaptador de red y así no se veían.

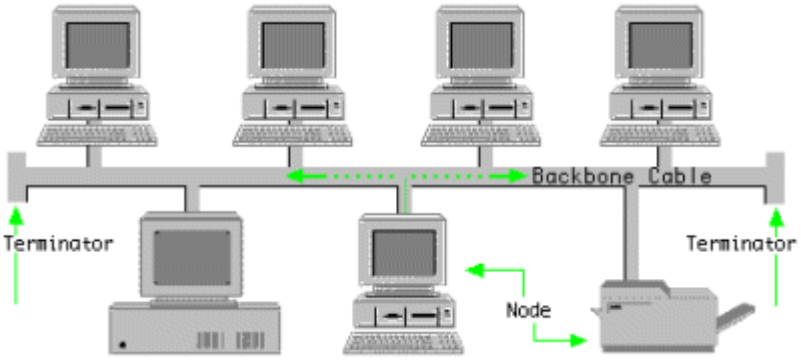


Figura 2.5: Topología tipo bus
Fuente: http://classunaed.blogspot.com/2011/03/descripcion-general-redes-lan

Topología en anillo

La topología en anillo consiste en conectar cada computadora a dos más, de manera que se forme un anillo. Cuando una computadora quiere enviar una trama a otro, ésta debe pasar por todas las computadoras que haya entre ellos: la circulación por el anillo es unidireccional. Véase figura 2.6

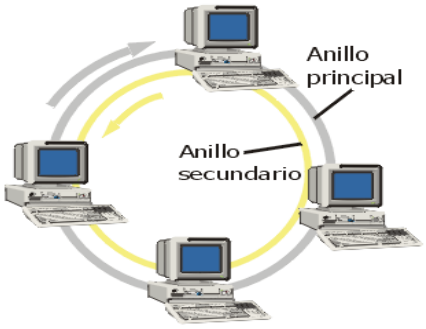


Figura 2.6: Topología tipo anillo
Fuente: http://porta-tlacuachasunidas.blogspot.com/2011/05/topologia-de-doble-anillo.html

El dispositivo que conecta la computadora al anillo es el repetidor, un circuito con tres conexiones:

- Conexión de entrada de tramas desde el anillo a la computadora (A).
- Conexión de salida de tramas desde la computadora al anillo (B).
- Conexión bidireccional, por la que pasan todas las tramas que entran y salen de la computadora. Véase figura. 2.7

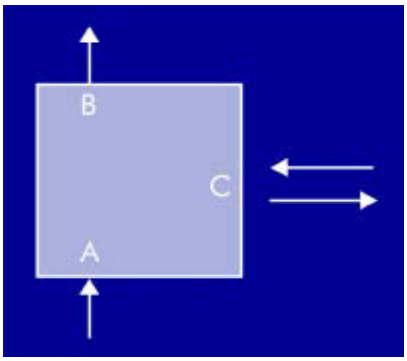


Figura 2.7 Repetidor
Fuente:http://www.uazuay.edu.ec/estudios/sistemas/teleproceso/apuntes_1/laninalambricas.htm

El repetidor tiene tres modos de trabajo:

- Modo escucha: el repetidor toma las tramas que le llegan por A y las pone simultáneamente en B y C, para que continúen por el anillo y para que el computadora reciba una copia de las mismas y la analice. Si es el destinatario de la trama, se la queda y, en caso contrario, la descarta.
- Modo transmisión: la computadora envía información a la red. Pone una trama en C, de manera que cruza el repetidor y sale por B hacia la computadora siguiente del anillo.

- Modo cortocircuito: las tramas que llegan por A se ponen directamente en B sin proporcionar una copia de las mismas la computadora. Este modo sirve para que el anillo continúe funcionando si la computadora correspondiente no está activa.

Pseudotopología de las redes inalámbricas

Hablar de topología en una red inalámbrica parece fuera de lugar, porque no se ve ningún medio de transmisión. Pero en realidad el "éter" por donde viajan las ondas se considera un medio de transmisión, y si lo compara con las tres topologías descritas, también se comparar a la topología en bus.

De hecho, las ondas electromagnéticas no necesitan ningún soporte físico para ser transmitidas. Se propagan en el vacío. Véase figura 2.8 Pero hasta que esto no fue demostrado, los científicos utilizaban el término "éter" para designar algo que se imaginaban que tenía que existir pero eran incapaces de ver. En un anillo o en una estrella en realidad existen 'n' medios independientes que conectan una estación a otra (o al punto central), mientras que en un bus tiene un sólo medio (un cable) al que se conectan todas las estaciones, de la misma manera que en una red inalámbrica tiene un solo medio (el aire) donde las estaciones ponen sus tramas

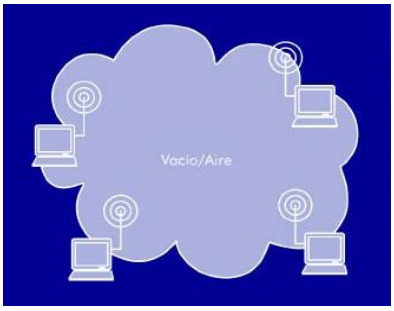


Figura 2.8: Ondas eletromagnéticas
Fuente:http://www.uazuay.edu.ec/estudios/sistemas/teleproceso/apuntes_1/laninalambricas.html

CAPITULO II

Análisis de Redes Inalámbricas que existen en el Mercado

CAPITULO II

Análisis de Redes Inalámbricas que existen en el Mercado

Introducción

Se analizaron adaptadores inalámbricos de AT&T, Proxim, Solectek y Xircom para conectar una computadora, a una LAN. Los cuatro ofrecen adaptadores inalámbricos orientados a usuarios con computadoras tipo portátil. Solectek también ofrece una versión de puerto paralelo, para que pueda conectar cualquier sistema de escritorio o portátil. La segunda parte de una solución inalámbrica en una LAN es el punto de acceso, el dispositivo que establece la conexión entre los adaptadores inalámbricos y la red alambrada. Se revisaron puntos de acceso de los mismos fabricantes.

Dejando aparte la conveniencia, se deben de considerar ciertos detalles como: el costo, el rendimiento y la facilidad de uso. Comparados con los adaptadores de LAN basados en cable, estos productos pueden parecer caros. Hoy en día, se pueden conseguir adaptadores de Ethernet por mucho menos de US$ 100.00 por nodo. Pero el costo de instalar el cable de red puede ser caro y a veces poco práctico, particularmente en los casos en que la red es sólo para uso temporal.

Aunque los sistemas inalámbricos no son tan veloces si son fáciles de instalar. Usando los puntos de acceso o los adaptadores inalámbricos que se instalan en un servidor, los usuarios pueden comunicarse con las redes alambradas existentes. Todos los productos mostraron buenos resultados, de 122 m a más de 305 m sin perder conexión en la prueba de distancia en exteriores.

Los productos analizados utilizan las dos técnicas para la distribución de la señal en el espectro:

- **Salto de Frecuencias**: utilizado por RangeLAN2 de Proxim y el Netwave de Xircom. Este método es una técnica en la cual los dispositivos receptores y emisores se mueven sincrónicamente en un patrón determinado de una

frecuencia a otra, brincando ambos al mismo tiempo y en la misma frecuencia predeterminada. Como en el método de secuencia directa, los datos deben ser reconstruidos en base del patrón de salto de frecuencia. Este método es variable para las redes inalámbricas, pero la asignación actual de las bandas ISM no es adecuada, debido a la competencia con otros dispositivos, como por ejemplo las bandas de 2.4 y 5.8 MHz que son utilizadas por hornos de Microondas.

- **Secuencia Directa:** Utilizada por El WaveLAN de AT&T y AirLAN de Solectek. En este método el flujo de bits de entrada se multiplica por una señal de frecuencia mayor, basada en una función de propagación determinada. El flujo de datos original puede ser entonces recobrado en el extremo receptor correlacionándolo con la función de propagación conocida. Este método requiere un procesador de señal digital para correlacionar la señal de entrada.

Como ya se mencionó, ambos enfoques ofrecen seguridad, elemento importante en la conectividad inalámbrica. Según las pruebas realizadas se puede considerar que los productos que usan la secuencia directa resultaron mejores en rendimiento y distancia.

Según se mueve la computadora, la señal del adaptador se puede cambiar o otro Punto de Acceso para continuar con la transmisión. Cuando una MC detecta que la señal se hace más débil y que se está alejando del alcance de un punto de acceso, el adaptador interroga a todos los otros puntos de acceso de la red para ver cuál está más cerca. Entonces, el adaptador, de forma transparente, se cambia de un punto de acceso a otro. Sólo el Proxim pudo moverse sin perder la conexión. El “NetWare” de “Xircom”, el “WaveLAN” de AT&T y el de AirLAN/Parallel de Solectek mostraron dificultad al moverse de un punto de acceso a otro.

Para conservar energía, AT&T, Proxim y Solectek tienen opciones de "sueño" que pueden configurarse para apagar el adaptador en el caso de que no haya transmisión

o recepción de datos. Sin embargo, el adaptador, envía un paquete de aviso para evitar que lo desconecten de la red.

Si se usa "NetWare" de "Novell", y se instala una red inalámbrica, se deben de aprovechar los VLM (Virtual Loadable Module). Existe un VLM de tecnología de ráfaga de paquete y éste aumenta el rendimiento del adaptador. Además, al conectarse sin alambres se notará que los archivos ejecutables, como el LOGIN.EXE de NetWare o un producto de procesamiento de texto, se demoran en arrancar. Si es posible, se deberá evitar correr archivos ejecutables grandes en la red inalámbrica. Lo recomendable es copiar los archivos ejecutables al disco duro de la MC para tener mejor rendimiento. De esta forma, solamente se transmitirán los archivos de datos.

Al diseñar la red inalámbrica que deba cubrir un área grande, se tienen que instalar tantos puntos de acceso, de tal forma que las áreas de cobertura se superpongan una con otra para eliminar cualquier zona muerta. Proxim y Solectek ofrecen ambos programas diagnósticos que le permiten probar la fortaleza y la calidad de la señal de radio entre una MC y un punto de acceso. Estas utilerías son buenas no solamente para la colocación de las antenas o puntos de acceso, sino que ayudan a diagnosticar los adaptadores que tengan problemas.

Wavelan de AT&T

El adaptador de PCMCIA AT&T, WaveLAN, junto con el puente WavePOINT tienen un buen rendimiento y fuertes opciones de administración. El cambiar las MC de un punto de acceso a otro no es fácil. WaveLAN no permite la movilidad.
El WaveLAN PCMCIA, está dividido en dos partes: una tarjeta tipo II, que opera en un rango de frecuencia de 902 a 928 MHz que se desliza en la ranura PCMCIA y una pequeña unidad de antena, que se agrega a la parte trasera del panel de vídeo de la computadora. Hay un cable flexible de 50 cm. que une a los dos componentes inalámbricos. La unidad de antena está completamente cubierta y se retira fácilmente. El rendimiento punto-a-punto de WaveLAN fue mejor que los otros productos. Sin embargo, el transferir Clientes de WaveLAN de un punto de acceso

a otro, no es fácil. La identificación de la red se escribe en la memoria no volátil del adaptador y no en un archivo de configuración será del arranque. Así que para cambiar la identificación del adaptador se debe ejecutar un servicio dedicado.
La "WaveLAN" resultó tener un buen rendimiento en cuanto a distancia, siendo aceptable de 30.48 a 304.8 m. Se pudo realizar una conexión pasando a través de dos paredes y una puerta de cristal con sólo una pequeña degradación de la señal.

La configuración de los puentes "WavePOINT" es de conectar-y-usar, excepto que posiblemente se tenga que cambiar uno o dos interruptores DIP en el exterior para adecuarlo a su tipo de medios. El puente incluye conectores RJ-45, BNC y AUI. Las opciones de administración de WaveLAN incluyen: control de acceso de una LAN alambrada, cumplimiento con SNMP, estadísticas sobre los paquetes, y mediciones de la señal. Las mediciones de la señal usan diagramas de barra para mostrar la fortaleza de la señal y la razón de señal-a-ruido. Para seguridad adicional en la red, hay opciones disponibles codificación de datos. WaveLAN también incluye administración de energía, que evita que el adaptador consuma más batería de la necesaria.

Rangelan2 de Proxim inc.
Proxim tiene el adaptador RangeLAN2/PCMCIA y el RangeLAN/Access Point. Esta solución tiene fuertes capacidades de movilidad, herramientas para diseñar redes inalámbricas. El RangeLAN/PCMCIA también incluye servicios de administración de energía para aprovechar la batería de la PC. Este es un adaptador para Ethernet compatible con el PCMCIA Tipo II que opera en el rango de frecuencias de 2,4 a 2,484 GHz. El RangeLAN2 Tiene una antena y un transmisor que se adhieren al dorso de la MC. La antena es liviana y fácilmente desmontable, al contrario de la de la antena paralela de Solectek.

El adaptador viene con manejadores de ODI y de NDIS y apoya todos los sistemas operativos importantes de red, incluyendo NetWare y LAN Manager, así como también cualquier sistema será de igual compatible con NDIS, incluyendo "Windows Workgroups" y "PowerLAN".

El rangeLAN2/Access Point, con un tamaño aproximadamente igual a la mitad de una computadora de escritorio, cubre la brecha entre la computadora móvil y un segmento alambrado de LAN. La antena del punto de acceso, que parece una palanca de juego, se conecta al dispositivo por un cable de 1.22 m de largo. No es tan pequeño o tan fácil de montar en la pared como la solución de "Xircom", que es de conectar-y-usar.

El RangeLAN2 realizó con satisfacción pruebas de rendimiento y fue el único producto en esta comparación con capacidades completas de movilidad. Los usuarios pueden moverse libremente por los pasillos de las oficinas sin tener brechas de transmisión siempre que las células de los puntos de acceso se superpongan. Una vez que las células se superponen, el software del adaptador detecta que se está alejando del rango del punto de acceso e interroga a los otros puntos de acceso para ver cuál tiene la señal más fuerte. Esto trabaja bien, dependiendo de la colocación de los puntos de acceso y las antenas a lo largo de la oficina.

RangeLAN2 requiere por lo menos que una estación de la red se configure como una Estación Base maestra, lo cual puede ser un problema en una red punto a punto. La Estación Base actúa como un mecanismo de sincronización de reloj para la frecuencia de salto de cada computadora móvil. Si la Estación Base deja de trabajar, entonces se necesita tener disponible una Estación Base alterna para controlar la dirección. Esto no es un gran problema cuando un servidor se configura como el amo, en un entorno punto a punto con usuarios móviles, se debe designar todas las computadoras fijas como Estaciones Bases alternas, sabiendo que el rendimiento disminuye.

En general, las excelentes capacidades de movilidad de RangeLAN2, sus herramientas de diseño, y su ejecución adecuada en las pruebas de rendimiento lo hacen una de las mejores soluciones inalámbricas de operación en redes del mercado de hoy.

Airlan de Soleteck

La única compañía que hoy ofrece soluciones de adaptador inalámbrico PCMCIA paralelo y de ISA, "Solectek" Corp., le permite tener bajo un mismo techo inalámbrico todas las necesidades del sistema. Los dos adaptadores que se probaron, el AirLAN/PCMCIA y el AirLAN/Parallel, proveen alcance y rendimiento superiores al promedio, pero sin habilidades de movilidad. Estos productos operan en el rango de frecuencias de 902 a 928 MHz. El AirLAN/PCMCIA es un adaptador del tipo II, compatible con PCMCIA, el AirLAN/Parallel es un adaptador paralelo que tiene una batería recargable. También se probó el Solectek AirLAN/Hub, El centro (Hub) es para las MC, que estén más allá de la distancia máxima que permite un servidor inalámbrico.

La antena del adaptador AirLAN/PCMCIA es liviana y fácil de quitar y se monta en un soporte al dorso de la PC. El adaptador AirLAN/Parallel también se monta en la cubierta, pero su tamaño no es tan cómodo, esto se debe principalmente a su batería recargable de níquel cadmio (con una vida de 10 horas). Los adaptadores AirLAN vienen con software de administración de energía que le ayuda a conservar la vida de la batería.

El adaptador AirLAN/Parallel trabajó más lento que el AirLAN/PCMCIA. Aunque la mayor diferencia estuvo en la prueba de alcance. El AirLAN/PCMCIA mantuvo su rendimiento a más de 1,000 pies, mientras el AirLAN/Parallel no pudo alcanzar los 700 pies.

Ambos adaptadores del AirLAN vienen con una herramienta de diagnóstico de punto-a-punto que permiten evaluar el enlace de radio frecuencia del adaptador. El software de diagnóstico puede ayudar a diseñar la red, ya que evalúa la razón de señal-a-ruido, la calidad de la señal y el nivel de la señal. Se puede usar esta información para ubicar los AirLAN/Hub donde sean más efectivos. Sin embargo, no se pudo ejecutar la prueba de punto-a-punto entre los dos adaptadores. (Solectek está trabajando en una solución).

La serie inalámbrica AirLAN de Solectek ofrece una solución para casi cualquier tipo de sistema: una PC de escritorio con un puerto paralelo, una PC tipo portátil paralelo, una PC tipo portátil con una ranura PCMCIA o hasta un sistema basado en pluma con un puerto paralelo o una ranura PCMCIA.

Netwave de Xircom inc.

Xircom no sólo se libra del cable en esta solución inalámbrica de LAN sino que el adaptador CreditCard también elimina la antena, ya que la incorpora en la propia tarjeta PCMCIA, dejando sólo una pequeña protuberancia. Este diseño único tiene sus ventajas y desventajas.

Por una parte, hace a este adaptador aun más portátil y flexible que las otras soluciones. Como no tiene una antena que cuelgue de su MC, hace más fácil moverse, especialmente si el usuario usa la pluma de computación.

El tamaño pequeño de la antena y la relativamente baja potencia de transmisión del adaptador limitan el alcance y las capacidades de transmisión. Puede ser necesario tener múltiples puntos de acceso para cubrir completamente la oficina. Xircom planea tener una mejora de software con movilidad completa. Como el RangeLAN2 de Proxim, Netwave usa salto de frecuencia y opera en el rango de frecuencias de 2.4 hasta 2.484 GHz para transmitir y recibir datos. El adaptador trabaja con el "Netwave Access Point" para conectar un cliente móvil o estacionario a la LAN o directamente con otros adaptadores "Netwave" en PC clientes en una LAN punto a punto. "Netwave" apoya múltiples sistemas operativos de la red, incluyendo NetWare y LAN Manager, así como también productos punto a punto como "Windows for Workgroups". Apoya tanto ODI como NDIS.

El "Access Point" crea una zona de servicio a su alrededor para proveer comunicaciones inalámbricas dentro de un radio de 50 m. Sin embargo, si la red excede el alcance del adaptador, se necesitara comprar por lo menos dos puntos de acceso y alambrarlos juntos para lograr la cobertura adicional.

Para dejar que los usuarios se muevan, se deberán colocar estratégicamente varios puntos de acceso para constituir una serie de zonas de servicio que se superponen una con la otra, creando una zona mayor de servicio. El "Access Point" es un dispositivo compacto y liviano. "Netwave" permite organizar la seguridad de varias maneras. Se puede segmentar la red en dominios, que incluyen diferentes números de dirección, para que sólo las MC de ese dominio puedan tener acceso a ese punto de acceso punto a punto.

La administración del punto de acceso es limitada: el software sólo se puede ejecutar en un sistema que ejecute IPX en un segmento alambrado de la red. El software de administración "Zona", le deja fijar contraseña, cambiar los números de dominio, agregar direcciones de usuario, mejorar el software, activar claves de codificación y dar un nombre a la unidad. "Netwave" ofrece flexibilidad, facilidad de uso y buenas opciones de seguridad. Véase figura 3.1 y figura 3.2

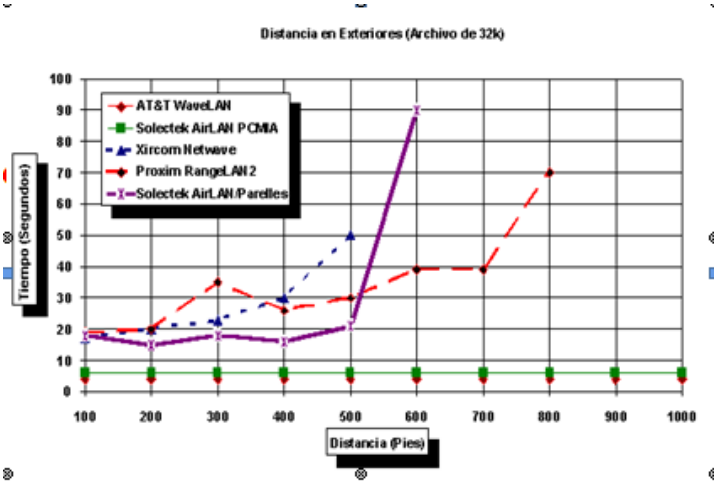


Figura 3.1: AT&T WaveLan
Fuente:http://www.elprisma.com/apuntes/ingenieria_de_sistemas/redesinalambricas/default8.asp

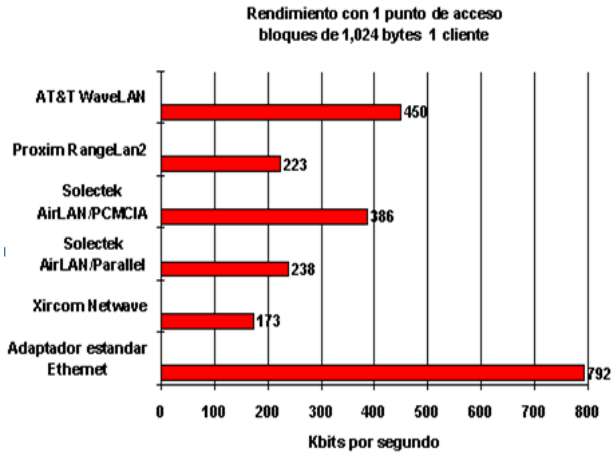


Figura 3.2: Rendimiento de AT&T WaveLan
Fuente: http://www.monografias.com/trabajos35/redes-inalambricas/redes-inalambricas2.shtml

Decidiendo por una WLAN

El medio ha sido bombardeado por diversas opciones, unas muy complicadas, otras muy caras, otras difíciles de instalar u otras que simplemente no funcionan. En este trabajo se expondrá solo una solución que haya sido probada, que sea sencilla y eficiente y que su alcance cubra todo el territorio de las empresas.

En la búsqueda de la solución ideal se ha escogido a *DLINK*, una empresa que ofrece soluciones de redes a todo nivel con soporte local. Es una empresa de Taiwán con 16 años de experiencia en redes físicas e inalámbricas.
Cuando se habla de WLAN realmente se tienen muchas opciones en el mercado por lo que ha sido necesario encontrar un buen y experimentado consultante para lograr la funcionalidad de la red necesaria.

Si se tienen los productos adecuados, crear una red inalámbrica no es nada complicado y si se tiene el soporte correcto aún menos. En una red típica basta con tener las tarjetas inalámbricas para las computadoras, ya sea USB, PCI o PCMCIA; los puntos de acceso (access points); y verificar que no hayan obstáculos muy grandes para logar la transmisión.

Lo más interesante está en que las WLAN siguen evolucionando y actualmente llegan a velocidades de 108 Mbps en el estándar 802.11g como en los productos AirPlus XtremeG de DLINK.

Funcionamiento

La Tarjeta PC de la computadora portátil recibe y transmite información digital a una frecuencia de radiofrecuencia de 2,4 GHz. La tarjeta convierte la señal de radio en datos digitales (en realidad, pequeños paquetes de información) que la PC puede comprender y procesar.

La tarjeta PCI se conecta a una computadora de escritorio y funciona de modo similar a la Tarjeta PC, con la diferencia de que es especial para computadoras Portátiles.

El punto de acceso de software permite que una PC conectada a una red “Ethernet” (un tipo de red de área local muy común) pueda desempeñarse como punto de acceso de hardware.

El punto de acceso del hardware recibe y transmite la información de forma similar a la tarjeta de la PC. Se conecta a la red “Ethernet” mediante un conector RJ-45 y maneja el tráfico entrante y saliente entre la red fija y los usuarios de la LAN INALÁMBRICA o "clientes", actuando así como un “hub” inalámbrico. En otras palabras, el punto de acceso de hardware se desempeña como un portal o rampa de ingreso, para que los usuarios inalámbricos puedan acceder a una LAN cableada.

Es importante destacar que, tal como ocurre en una autopista en horas de máximo tráfico, cuantos más usuarios se hallan en el punto de acceso, tanto más lento será el tráfico. El punto de acceso de hardware se conecta a un conmutador o encaminador, pero también puede conectarse directamente a un servidor mediante un adaptador de cable.

Modo infraestructurado

Cuando se selecciona el modo infraestructurado (en la PC mediante la utilidad de configuración), el usuario puede enviar y recibir señales de radio (información) a través de un punto de acceso, el cual puede ser mediante hardware o software. Este punto de acceso se conecta a una red convencional mediante un cable, recibe la señal de radio del cliente y la convierte a formato digital que la red y el servidor pueden comprender y procesar. Si el usuario solicita información (por ejemplo, una página web), el punto de acceso envía una señal de radio a la PC del usuario de la LAN INALÁMBRICA. Los puntos de acceso están ubicados en las conexiones de red donde cualquier computadora, impresora u otro dispositivo de red se conectaría mediante un cable RJ-45 (similar a un enchufe telefónico, pero ligeramente más grande). Véase figura 3.3

Figura 3.3: Modo infraestructurado
Fuente:http://www.uazuay.edu.ec/estudios/sistemas/teleproceso/apuntes_1/laninalambricas.htm

LAN inalámbrica con infraestructura ad-hoc

Modo de pares: Cuando se selecciona el modo entre pares (peer to peer), los usuarios se conectan a otras computadoras (ya sea portátiles o de mesa) equipadas con productos inalámbricos IEEE 802.11b de alta velocidad. Este modo se utiliza cuando no existen redes cableadas cuando un grupo de usuarios desea configurar

su propia red para colaborar y compartir archivos. En el extremo de servidor/red, el gerente de tecnología de la información debe instalar un paquete de software, que su departamento debe introducir en el servidor apropiado.

Este paquete de software permite configurar, administrar y controlar el seguimiento del tráfico inalámbrico a través de la red.
Cada punto de acceso de hardware ofrece un caudal de hasta 11 Mbps.

Esta capacidad es adecuada para las siguientes actividades:

- 50 usuarios, en su mayoría inactivos, que ocasionalmente consultan mensajes de correo electrónico de texto.
- 25 usuarios principales que utilizan intensamente servicios de correo electrónico y cargan o descargan archivos de tamaño moderado.
- 10 a 20 usuarios que constantemente están conectados a la red y trabajan con archivos grandes.

Para aumentar la capacidad, pueden agregarse más puntos de acceso, lo que brinda a los usuarios mayor oportunidad de ingresar a la red. Es importante destacar que las redes se consideran optimizadas cuando los puntos de acceso corresponden a distintos canales.

Ejemplo:
Una compañía puede establecer 3 puntos de acceso (con un alcance de hasta 100 metros cada uno) en 3 oficinas adyacentes, cada uno configurado a un canal distinto. En teoría, esto permitiría que numerosos usuarios "compartiesen" una capacidad total de hasta 33 Mbps (si bien ningún usuario podría alcanzar velocidades superiores a 11 Mbps). En la realidad, dado que los clientes se comunican con el punto de acceso que les ofrece la señal más intensa, el ancho de banda no necesariamente se distribuye uniformemente entre todos los usuarios.
LAN troncal cableada como una Ethernet. Conecta varios servidores, estaciones de trabajo, o dispositivos de encaminamiento para conectar otra red Existe un Modulo de Control que funciona como interfaz con la LAN inalámbrica.

LAN inalámbrica de celda única

LAN inalámbrica de celdas múltiples Existen varios módulos de control interconectados por una LAN cableada. Cada modulo da servicio a varios sistemas finales inalámbricos dentro de su rango de transmisión.

Configuración y Estructuración de una LAN Inalámbrica

Para Configurar y estructurar una LAN Inalámbrica se debe disponer de un Punto de Acceso, que cumple el estándar IEEE 802.11, compuesto por un software de protocolo y una tarjeta para redes inalámbricas. Con este producto se facilita la configuración de redes inalámbricas en modo Infraestructura, proporcionando una mayor seguridad en el control de acceso a la red por parte de los equipos inalámbricos.

La especificación del IEEE ha elegido la banda ICM (uso Industrial, Científico y Médico) de 2.4 GHz para la definición del estándar de LAN Inalámbrica, lo que garantiza su validez global por ser una banda disponible a nivel mundial. La banda ICM es para uso comercial sin licencia, limitando la potencia de transmisión para las redes locales inalámbricas a 100 mW. La velocidad de enlace entre los equipos inalámbricos es de 2 Mbps, máxima velocidad definida en el estándar IEEE 802.11, con una modulación de señal de espectro expandido por secuencia directa (DSSS). Con esta técnica de modulación, cada bit de datos a transmitir, se sustituye por una secuencia de 11 bits equivalente y fácilmente reconocible por el receptor, de manera que aunque parte de la señal de transmisión se vea afectada por interferencias, el receptor aún puede reconstruir la información a partir de la señal recibida.

Punto de Acceso

Un punto de acceso inalámbrico “Access Point” (WAP o AP: Wireless Access Point) en redes de computadoras es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica. Normalmente un WAP también puede conectarse a una red cableada, y puede transmitir datos entre los

dispositivos conectados a la red cable y los dispositivos inalámbricos. Muchos WAP pueden conectarse entre sí para formar una red aún mayor, permitiendo realizar "roaming". Por otro lado, una red donde los dispositivos cliente se administran a sí mismo (sin la necesidad de un punto de acceso) se convierten en una red ad-hoc. Los puntos de acceso inalámbricos tienen direcciones IP asignadas, para poder ser configurados.

Son los encargados de crear la red, están siempre a la espera de nuevos clientes a los que dar servicios. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN y la LAN cableada.

Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos. Véase figura 3.4 Este o su antena normalmente se colocan en lato pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada.

El usuario final accede a la red WLAN a través de adaptadores. Estos proporcionan una interfaz entre el sistema de operación de red del cliente NOS (Network Operating System) y las ondas, mediante una antena inalámbrica.

Figura 3.4: Cliente y punto de acceso
Creada por: Francisco Palacios.

El Punto de Acceso está compuesto por:

- Una tarjeta LAN INALÁMBRICA (LAN Inalámbricas.)
- El Software de protocolo para redes LAN Inalámbricas 802.11.

Actúa como enlace entre la red inalámbrica y una red fija (Ethernet). Los únicos conectores son el de alimentación y el de cable fijo, conector 10Base-T (RJ-45). También existen dos antenas que se colocan en posición vertical durante el uso. Cumple con la norma IEEE 802.11b (Espectro de propagación de secuencias a alta velocidad). Véase figura. 3.5 Admite una temperatura entre 0 - 40ºC (temp. en operación) Humedad: 95% (sin condensación)

Figura 3.5 Wireless Inalámbrico

Funcionamiento general de una tarjeta para LAN inalámbricas:
Cumple con el estándar IEEE802.11. Alcance: 50 metros en oficinas densas, 100 metros en oficinas abiertas, 800 metros en exterior. Frecuencia intermedia: 280 MHz. Rango de frecuencias: 2,4 GHz (desde 2.412 MHz hasta 2.484 MHz). Antena: Externa omnidireccional. (Véase figura. 3.6)

Figura 3.6: Tarjeta para LAN

Creada por: Francisco Palacios.

Software para punto de acceso de red LAN inalámbrica:

El paquete "Punto de Acceso de Software" (SAP). Es un programa que se instala en una computadora equipada con una unidad de Punto de Acceso ofrece la funcionalidad de la misma. (Véase figura 3.7)

Figura 3.7: Software para LAN inalámbricas
Creada por: Francisco Palacios.

Usos de las LAN Inalámbricas

Acceso Nómada

- Permite un enlace no guiado entre un centro o servidor de LAN y un terminal de datos móvil con antena (computadora portátil).
- El usuario se puede desplazar con la computadora portátil y conectarse con servidores de LAN Inalámbricos desde distintos lugares.

Tarjeta para Notebook

La cual sirve para configurar a la Portátil para las LAN Inalámbricas, tiene antena integrada y puede transmitir a 11 Mbps (Véase figura. 3.8)

Figura 3.8: Tarjeta de LAN inalámbrica para portátiles
Creada por: Francisco Palacios.

Teniendo en cuenta que en la red de Infraestructurada el PC que lleva el control de acceso puede ser cualquier equipo de la red, el uso del Punto de Acceso permite ampliar las actuales redes de cable Ethernet sólo en base a la instalación de nuevos puntos con dispositivos inalámbricos, sin necesidad de seguir instalando cables de red. (Véase figura 3.9)

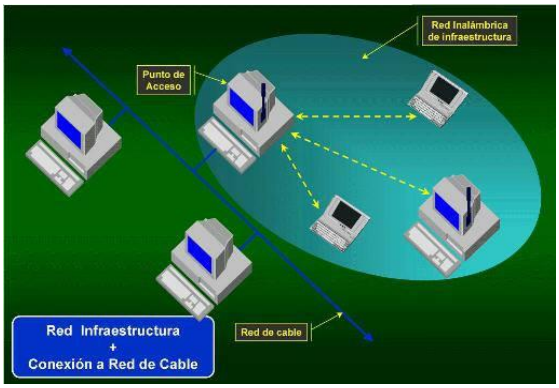


Figura 3.9 LAN inalámbrica con infraestructura y Conexión a una Red
Fuente:http://www.uazuay.edu.ec/estudios/sistemas/teleproceso/apuntes_1/laninalambricas.htm

El uso del Punto de Acceso, en la ampliación de redes de cable Ethernet existentes está especialmente indicado en enlaces entre plantas de un mismo edificio, entre edificios cercanos y/o entre locales próximos pero sin continuidad.
Para ello se usa el denominado Puente. El Puente o "Bridge" cumple el estándar IEEE802.11 y está compuesto por el software de protocolo para redes inalámbricas y una tarjeta de redes inalámbricas. (Véase figura 3.10). El Puente tiene como finalidad la unión entre dos redes de cables tradicionales (Ethernet), separadas por un cierto espacio físico, que hagan imposible o dificultosa su unión por cable.

El uso del Puente permite la fácil interconexión entre dos redes de cables situadas en locales cercanos, en pisos diferentes o hasta en edificios separados, ahorrando al usuario las costosas obras de infraestructura (zanjas, cableados, etc.,).

La solución que aporta la utilización del Puente frente a enlaces punto a punto o temporales, vía red telefónica conmutada, proporciona una velocidad superior en la

transferencia de datos (hasta 60 veces más), sin mayor costo que el uso del propio Puente.

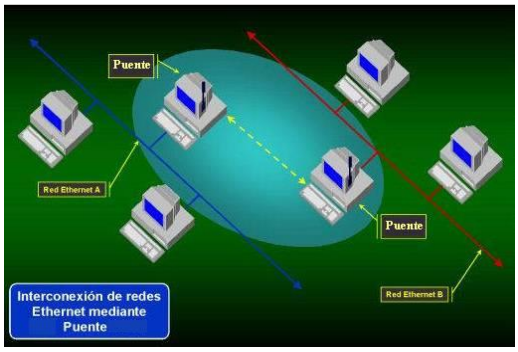


Figura 3.10: Interconexión de Redes Ethernet
Fuente:http://www.uazuay.edu.ec/estudios/sistemas/teleproceso/apuntes_1/laninalambricas.htm

Las Redes inalámbricas pueden ser configuradas en los siguientes entornos
Red "ad-hoc":

Es aquella en la que todas las computadoras (de sobremesa y/o portátiles) provistos de tarjetas de red inalámbrica pueden comunicarse entre sí directamente. Es una red igual (sin servidor central) establecida temporalmente para satisfacer una necesidad inmediata, formando así una red temporal. (Véase figura 3.11)

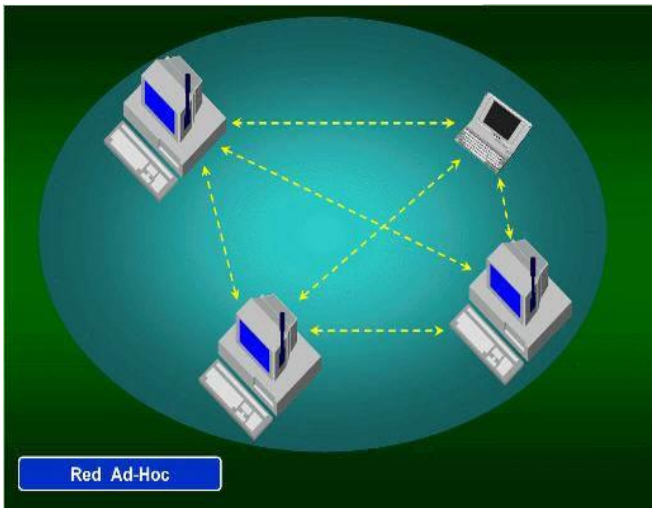


Figura 3.11: LAN inalámbrica
Fuente:http://www.uazuay.edu.ec/estudios/sistemas/teleproceso/apuntes_1/laninalambricas.html

Red Infraestructura.

Es aquella en la que todas las computadoras (de sobremesa y/o portátiles) provistos de tarjetas de red inalámbrica trabajan en orden jerárquico, por el que una de las computadoras de la red es el punto de enlace entre todas las PC de la misma red. Desde esa computadora se lleva el control de acceso, como medida de seguridad del resto de los equipos que forman parte de la red. (Véase figura 3.12) Para configurar la red de Infraestructura, se requiere que sobre la computadora elegida para llevar el control se instale un Punto de Acceso, conforme al estándar IEEE 802.11.

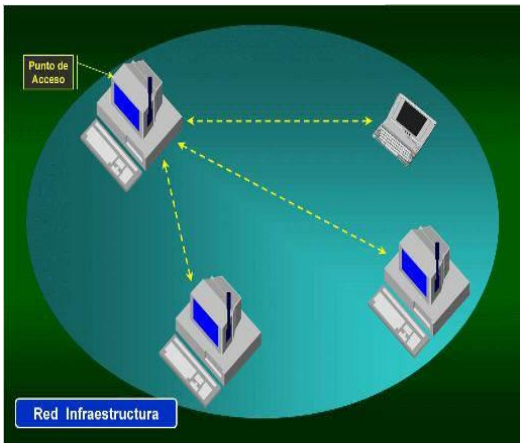


Figura 3.12: LAN inalámbrica
Fuente:http://www.uazuay.edu.ec/estudios/sistemas/teleproceso/apuntes_1/laninalambricas.htm

Aplicaciones típicas de LAN Inalámbrica

Enlace de áreas físicas independientes mediante Puntos de Acceso

El enlace entre redes inalámbricas situadas en diferentes plantas de un mismo edificio es un perfecto ejemplo del uso del Punto de Acceso para realizar el enlace entre redes inalámbricas independientes, mediante un mínimo cableado Ethernet, en aquellas situaciones de cobertura límite de las antenas debido a obstáculos importantes. (Véase figura 3.13)

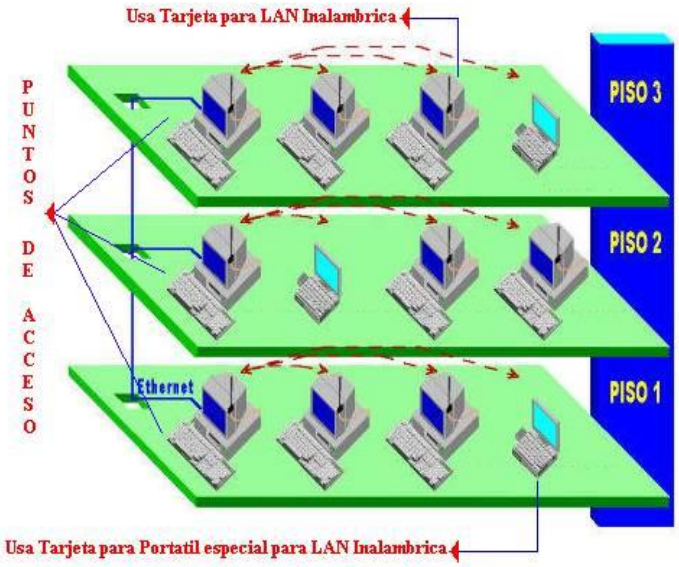


Figura 3.13 Interconexión de distintas LAN inalámbricas por medio de Red Ethernet.
Fuente:http://www.uazuay.edu.ec/estudios/sistemas/teleproceso/apuntes_1/laninalambricas.htm

Enlaces o Interconexión entre Edificios

En la conexión de redes LAN situadas en edificios vecinos, sean LAN cableadas o no, se usa un enlace no guiado entre los edificios, los dispositivos conectados son puentes o dispositivos de encaminamiento.

Este enlace punto a punto no es en sí una LAN, pero ésta aplicación se usa en las LAN Inalámbricas.

La combinación del Punto de Acceso y el Puente permite llevar a cabo el enlace entre dos áreas inalámbricas, cuando resulta imposible o demasiado caro realizar esta unión mediante un cable.

Para una situación similar entre dos redes Ethernet existentes, el punto de acceso que permite enlazar ambas redes inalámbricamente salvando vía radio los obstáculos que impedían su unión mediante un cable. (Véase figura 3.14)

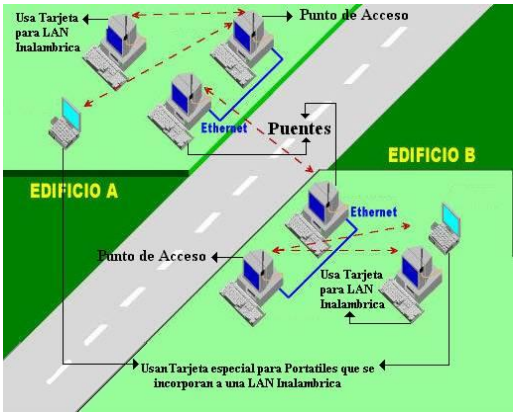


Figura 3.14: Interconexión de distintas LAN inalámbricas entre dos edificios Fuente:http://www.uazuay.edu.ec/estudios/sistemas/teleproceso/apuntes_1/laninalambricas.htm

Redes inalámbricas en la misma área física**:**

Dos o más redes inalámbricas, tanto en modo Ad-Hoc como en modo, pueden coexistir simultáneamente en la misma área física de cobertura de sus antenas, de forma totalmente transparente a los usuarios de cada una de las redes. Además, mediante una sencilla operación de asignación de canales en su configuración, ambas redes pueden operar a pleno rendimiento de su velocidad de transmisión a 2 Mbps. (Véase figura 3.15)

Requisitos de las LAN Inalámbricas:

Además de incluir los requisitos de cualquier otra red LAN, incluyendo:

- Alta capacidad
- Cobertura de pequeñas distancias
- Conectividad total de las estaciones conectadas.
- Capacidad de difusión

Existe un conjunto de necesidades específicas para entornos de LAN Inalámbricas:

- **Rendimiento:** El uso del protocolo MAC debe ser eficiente para maximizar la capacidad.

- **Número de Nodos:** pueden dar soporte a muchos nodos mediante el uso de varias celdas.

- **Conexión a la LAN Troncal:** se da la interconexión con estaciones situadas en una LAN troncal cableada. Se da soporte a las LAN Inalámbricas con infraestructura por medio de Módulos de control que conectan ambos tipos de LAN, a los usuarios nómadas y a las LAN Inalámbricas ad hoc.

- **Área de Servicio:** La superficie de cobertura tiene un diámetro típico entre 100 y 300 metros.

- **Consumo de Batería:** Cuando los usuarios móviles usan adaptadores sin cable necesitan una batería de larga vida.

- **Robustez en la transmisión y seguridad:** El diseño de una LAN inalámbrica debe permitir transmisiones fiables incluso en entornos ruidosos y debe ofrecer cierto nivel de seguridad contra escuchas.

- **Funcionamiento de red ordenada:** Es probable que dos o más redes operen en alguna zona donde sea posible la interferencia entre ella, esto frustra el funcionamiento del algoritmo MAC y pueden permitir accesos no autorizados a una LAN particular.

- **Funcionamiento sin licencia:** Los usuarios preferirían trabajar sobre LAN inalámbricas que no necesitan de una licencia para la banda de frecuencia usada por la red.

- **Sin intervención/nómada:** El protocolo MAC usado debería permitir a las estaciones móviles desplazarse de una celda a otra.

- **Configuración dinámica:** Los aspectos de direccionamiento MAC y de gestión de red de la LAN deberían permitir la inserción, eliminación y

traslado dinámicos y automáticos de sistemas finales sin afectar a otros usuarios.

Tipos de Comunicaciones inalámbricas por RF

Las transmisiones de datos entre equipos electrónicos sin cables se están aplicando cada vez más debido a los medios tecnológicos actuales, que son los circuitos integrados que permiten hacer un diseño sin tener demasiados conocimientos de RF, ni disponer de costosas instrumentaciones para RF, ya que estos dispositivos requieren pocos componentes externos y ningún tipo de ajuste en RF. Primero se usaron módulos de RF con componentes discretos unidireccionales y precisamente para no tener que depender del diseño de una circuitería en RF. Posteriormente con la aparición de circuitos transmisores completamente integrados con las funciones de emisor y receptor, en diferentes bandas de frecuencia que se fueron estandarizando en las diferentes zonas (Europa y USA), han permitido poderlos utilizar en los diferentes campos de aplicación industrial, comercial, y medico, como: control remoto, transmisión de datos en sensores o sistemas de adquisición de datos, en monitorización médica o de la salud, etc.

Las comunicaciones inalámbricas por RF se pueden dividir en las que no cumplen ningún protocolo estándar y las que cumplen un protocolo estándar, y en las normativas sobre sus distintas frecuencias de trabajo, que a la vez definen velocidad de transmisión o ancho de banda y campo de aplicación.

Componentes para crear una red WiFi (Wireless)

Módem/Enrutador.- *Módem* es un acrónimo de *MOdulador-DEModulador*; es decir, que es un dispositivo que transforma las señales digitales del la computadora en señal telefónica analógica y viceversa, con lo que permite a la computadora transmitir y recibir información por la línea telefónica.

Los chips que realizan estas funciones están casi tan estandarizados como los de las tarjetas de sonido; muchos fabricantes usan los mismos integrados, por ejemplo de

la empresa Rockwell, y sólo se diferencian por los demás elementos electrónicos o la carcasa.

Es, sin duda, el dispositivo más popular, ya que reúne en una sola carcasa tanto el módem ADSL (línea de abonado digital asimétrica) o Cable, el enrutador como el punto de acceso inalámbrico. Así que sirve para acceder a Internet y para crear una red local WiFi. El módem/enrutador debe ir conectado físicamente a una PC. (Véase figura 3.16)

Figura 3.16: Módem/enrutador
Creada por: Francisco Palacios.

Tipos de módems

La distinción principal que se suele hacer es entre módems internos y módems externos, si bien recientemente han aparecido unos módems llamados "módems software" o Winmódems, que han complicado un poco el panorama.

- **Internos**: consisten en una tarjeta de expansión sobre la cual están dispuestos los diferentes componentes que forman el módem. Existen para diversos tipos de conector:

    - **ISA**: debido a las bajas velocidades que se manejan en estos aparatos, durante muchos años se utilizó en exclusiva este conector, hoy en día en desuso.

- **PCI**: el formato más común en la actualidad.

- **AMR**: sólo en algunas placas muy modernas; baratos pero poco recomendables por su bajo rendimiento.

La principal ventaja de estos módems reside en su mayor integración con la computadora, ya que no ocupan espacio sobre la mesa y toman su alimentación eléctrica de la propia computadora. Además, suelen ser algo más barato debido a carecer de carcasa y transformador, especialmente si son PCI (aunque en este caso son casi todos del tipo "módem software".

Por contra, son algo más complejos de instalar y la información sobre su estado sólo puede obtenerse mediante software.

- **Externos**: son similares a los anteriores pero metidos en una carcasa que se coloca sobre la mesa o la computadora. La conexión con la computadora se realiza generalmente mediante uno de los puertos **serie o "COM"**, por lo que se usa la UART de la computadora, que deberá ser capaz de proporcionar la suficiente velocidad de comunicación; actualmente ya existen modelos para puerto **USB**, de conexión y configuración aún más sencillas.

  La ventaja de estos módems reside en su fácil transportabilidad entre computadoras, además puede (saber el estado el módem (marcando, con/sin línea, transmitiendo...) mediante unas luces que suelen tener en el frontal. Por el contrario, son un trasto más, necesitan un enchufe para su transformador y la UART debe ser una 16550 o superior para que el rendimiento de un módem de 28.800 bps o más sea el adecuado.

- **Módems PC-Card**: son módems que se utilizan en portátiles; su tamaño es similar al de una tarjeta de crédito algo más gruesa, pero sus capacidades pueden ser igual o más avanzadas que en los modelos normales.

- **Módems software, HSP o Winmódems:** son módems en los cuales se han eliminado varias piezas electrónicas, generalmente chips especializados, de manera que el microprocesador de la computadora debe suplir su función mediante software. Lo normal es que utilicen como conexión una ranura PCI (o una AMR), aunque no todos los módems PCI son de este tipo.

  La ventaja resulta evidente: menos piezas, más baratos. Las desventajas, que necesitan microprocesadores muy potentes (como poco un Pentium 133 MHz), que su rendimiento depende del número de aplicaciones abiertas (nada de multitarea mientras el módem funciona o se volverá una auténtica tortuga) y que el software que los maneja sólo suele estar disponible para Windows 95/98, de ahí el apelativo de *Winmódems*. Evidentemente, resultan poco recomendables pero son baratos...

- **Módems completos**: los módems clásicos no HSP, bien sean internos o externos. En ellos el rendimiento depende casi exclusivamente de la velocidad del módem y de la UART, no del microprocesador.

Punto de acceso

Los puntos de acceso son meras "emisoras" de señales WiFi y se utilizan para crear una red inalámbrica. El punto de acceso también debe estar conectado a una PC mediante un cable de red. (Véase figura 3.17)

Figura 3.17: Punto de Acceso
Creada por: Francisco Palacios.

Tarjetas de conexión.

Una **tarjeta de red** o **adaptador de red** permite la comunicación con aparatos conectados entre si y también permite compartir recursos entre dos o más computadoras (discos duros, CD-ROM, impresoras, etc). A las tarjetas de red también se les llama **NIC** (por *network interface card*; en español "tarjeta de interfaz de red"). Hay diversos tipos de adaptadores en función del tipo de cableado o arquitectura que se utilice en la red (coaxial fino, coaxial grueso, Token Ring, etc.), pero actualmente el más común es del tipo Ethernet utilizando una interfaz o conector RJ-45.

Aunque el término tarjeta de red se suele asociar a una tarjeta de expansión insertada en una ranura interna de un computador o impresora, se suele utilizar para referirse también a dispositivos integrados (del inglés *embedded*) en la placa madre del equipo, como las interfaces presentes en las videoconsolas Xbox o las computadoras portátiles. Igualmente se usa para expansiones con el mismo fin que en nada recuerdan a la típica tarjeta con chips y conectores soldados, como la interfaz de red para la Sega Dreamcast, las PCMCIA, o las tarjetas con conector y factor de forma CompactFlash y Secure Digital SIO utilizados en PDA.

Cada tarjeta de red tiene un número de identificación único de 48 bits, en hexadecimal llamado dirección MAC (no confundir con Apple Macintosh). Estas direcciones hardware únicas son administradas por el IEEE (Institute of Electronic

and Electrical Engineers) Los tres primeros octetos del número MAC son conocidos como OUI e identifican a proveedores específicos y son designados por la IEEE.

Se denomina también NIC al circuito integrado de la tarjeta de red que se encarga de servir como interfaz de Ethernet entre el medio físico (por ejemplo un cable coaxial) y el equipo (por ejemplo una computadora personal o una impresora). Es un circuito integrado usado en computadoras o periféricos tales como las tarjetas de red, impresoras de red o sistemas integrados (*embebed* en inglés), para conectar dos o más dispositivos entre sí a través de algún medio, ya sea conexión inalámbrica, cable UTP, cable coaxial, fibra óptica, etc.

Figura 3.18: Tarjetas de Conexión
Creada por: Francisco Palacios.

Los riesgos ligados a una red Wi-Fi

Las ondas Wi-Fi atraviesan los muros de su empresa. Si su red no está protegida, esto presenta varios riesgos:

- intrusión de una persona no autorizada a su red
- confidencialidad: perdida de confidencialidad de la información que circula en su red
- ataques y deterioro de la red de su empresa

Por lo tanto, es indispensable prohibir el acceso a la red a personas que no tengan permiso y limitar el nivel de acceso de los usuarios para evitar cualquier modificación que pueda poner fuera de servicio al servidor.

Proteja su red Wi-Fi

Para evitar intrusiones o actos maliciosos, es necesario:

- Identificar a los usuarios conectados
- Proteger el intercambio de datos a través de la red Wi-Fi mediante el cifrado de datos.
- Asegurarse de que todos los dispositivos estén protegidos.

Los datos que transitan en la red están protegidos por

Protocolos de seguridad inalámbrica: los cifrados WEP (Wired Equivalent rivacy) o WAP (Wi-fi Protected Access). Estos cifran la información que transita en la red Wi-Fi, para que los usuarios externos no puedan acceder a ella. Únicamente las personas que tienen permiso y el código de acceso a la red pueden acceder a los datos.

Los nuevos equipos inalámbricos por lo general ofrecen todas las garantías para evitar intrusiones en la red de la empresa. Cuando un usuario desee conectarse a la red inalámbrica deberá ingresar el código WEP o WAP, asignado a cada punto de acceso. Estos códigos son constituidos por una serie de 13 a 26 caracteres, números y letras.

Seguridades de Redes Inalámbricas

La infiltración no autorizada en redes inalámbricas de por sí ya es grave en una instalación residencial (en casa), mucho más peligroso es en una instalación corporativa. Y desgraciadamente, cuando se analiza el entorno corporativo (queda claro que las redes cerradas son más bien escasas).

Sin pretender hacer algo ilegal, se puede comprobar la cantidad de redes abiertas que se pueden encontrar sin más que utilizar el programa "Network Stumbler" o la función Site "Survey" o escaneo de redes de la PDA con Wi-Fi o de la portátil mientras se pasea por el vecindario, el hogar o por la zona de trabajo.

Las pocas medidas de seguridad permiten que un "intruso" irrumpa en la red y acceda a la información o la maneje a su antojo. Por este motivo, existen protocolos de seguridad que hacen más segura la red WLAN, el nivel de seguridad depende del tipo y la función de la red, pues la necesidad es diferente en la casa que en la empresa. Otro factor es garantizar que las redes WLAN tengan las mismas garantías de seguridad de las redes cableadas. Para tener una red inalámbrica más o menos segura es necesario que exista un mecanismo de encriptación de los datos que viajan por el aire y uno de autenticación.

Conseguir una red Wi-Fi más segura

El protocolo 802.11 implementa encriptación WEP, pero no se debe mantener el protocolo WEP como la única estrategia de seguridad ya que no es del todo segura.

Existen aplicaciones para Linux y Windows como "AiroPeek", "AirSnort", "AirMagnet" o WEPCrack) que, escaneando el suficiente número de paquetes de información de una red Wi-Fi, son capaces de obtener las claves WEP utilizadas y permitir el acceso de intrusos a red empresarial o privada. Más que hablar de la gran regla de la seguridad se puede hablar de una serie de estrategias que, aunque no definitivas de forma individual, en su conjunto pueden mantener la red oculta o protegida de ojos ajenos y mal intencionados.

Asegurar el Punto de Acceso

Cambiar la contraseña por defecto.

Todos los fabricantes establecen un "password" por defecto de acceso a la administración del Punto de Acceso. Al usar un fabricante la misma contraseña para todos sus equipos, es fácil o posible que el observador la conozca.

Evitar las contraseñas como fecha de nacimiento, el nombre de la pareja, etc.

Además se deben intercalar letras con números**.**

Aumentar la seguridad de los datos transmitidos

Usa encriptación WEP/WPA.

Activa en el Punto de Acceso la encriptación WEP. Mejor de 128 bits que de 64 bits, cuanto mayor sea el número de bits mejor.

Los Puntos de Acceso más recientes permiten escribir una frase a partir de la cual se generan automáticamente las claves. Es importante que en esta frase intercales mayúsculas con minúsculas y números, evites utilizar palabras incluidas en el diccionario y secuencias contiguas en el teclado (como "qwerty", "fghjk" o "12345").También establece en la configuración WEP la clave que se utilizará de las cuatro generadas (Key 1, Key 2, Key 3 o Key 4).

Después de configurar el AP tendrás que configurar los accesorios o dispositivos Wi-Fi de la red. En éstos tendrás que marcar la misma clave WEP (posiblemente puedas utilizar la frase anterior) que has establecido para el AP y la misma clave a utilizar (Key 1, Key 2, Key 3 o Key 4).

Algunos Puntos de Acceso más recientes soportan también encriptación WPA (Wi-Fi Protected Access), encriptación dinámica y más segura que WEP.

Ocultar la red Wi-Fi:

Cambia el SSID por defecto.

Suele ser algo del estilo a "default", "wireless", "101", "linksys" o "SSID". En vez de "MiAP", "APManolo" o el nombre de la empresa es preferible escoger algo menos atractivo para el observador, como puede ser "Broken", "Down" o "Desconectado". Si no se llama la atención del observador hay menos posibilidades de que éste intente entrar en la red.

Desactiva el "broadcasting" SSID.

El "broadcasting" SSID permite que los nuevos equipos que quieran conectarse a la red Wi-Fi identifiquen automáticamente los datos de la red inalámbrica, evitando así la tarea de configuración manual. Al desactivarlo será necesario introducir manualmente el SSID en la configuración de cada nuevo equipo que se quiera conectar. Si el observador conoce el SSID (por ejemplo si está publicado en alguna web de acceso libre) no conseguirá nada con la desactivación del "broadcasting" SSID.

Activa el filtrado de direcciones MAC.

Con esto se evita que se conecten, Activando en el AP el filtrado de direcciones MAC de los dispositivos Wi-Fi que actualmente tengas funcionando. Al activar el filtrado MAC dejarás que sólo los dispositivos con las direcciones MAC especificadas se conecten a la red Wi-Fi.

Por un lado es posible conocer las direcciones MAC de los equipos que se conectan a la red con tan sólo "escuchar" con el programa adecuado, ya que las direcciones MAC se transmiten "en lenguaje abierto", sin encriptar, entre el Punto de Acceso y el equipo.

Además, aunque en teoría las direcciones MAC son únicas para cada dispositivo de red y no pueden modificarse, hay comandos o programas que permiten simular temporalmente por software una nueva dirección MAC para una tarjeta de red.

Establece el número máximo de dispositivos que pueden conectarse.

Si el AP lo permite, se puede establecer el número máximo de dispositivos que pueden conectarse al mismo tiempo al Punto de Acceso.

Desactiva DHCP.

Desactiva el DHCP en el enrutador ADSL y en el AP.

En la configuración de los dispositivos/accesorios Wi-Fi se tendrá que introducir a mano la dirección IP, la puerta de enlace, la máscara de subred y el DNS primario y secundario.

Si el observador conoce "el formato" y el rango de las IP que se usa en la red, no se consigue nada la desactivación del DHCP.

Desconecta el AP cuando no se esté usando.

Desconecta el Punto de Acceso de la alimentación cuando no se esté usando o no se vayas a hacer durante una temporada. El AP almacena la configuración y no se necesitará introducirla de nuevo cada vez que lo conectes.

Cambia las claves WEP regularmente.

Por ejemplo semanalmente o cada 2 ó 3 semanas. Antes se dijo que existen aplicaciones capaces de obtener la clave WEP de la red Wi-Fi mediante el análisis los datos transmitidos por la misma. Pueden ser necesarios entre 1 y 4 Gb de datos para romper una clave WEP, dependiendo de la complejidad de las claves.

Cuando se llegue a este caudal de información transmitida es recomendable cambiar las claves.

Hay que recordar que se tendrá que poner la misma clave WEP en el Punto de Acceso y en los dispositivos que se vayan a conectar a ésta.

CAPITULO III

DISEÑO DE LA RED INALÀMBRICA PARA ADSAMED

DISEÑO DE LA RED INALÀMBRICA PARA ADSAMED

Introducción.

El proyecto presentado es la conformación de la red inalámbrica para la corporación **ADSAMED** que tiene como sede principal la oficina matriz en la ciudad de Quito, esta nueva arquitectura inalámbrica basada en la investigación realizada anteriormente se implementará en primera instancia en la oficina Matriz de la ciudad de Guayaquil. Esta tecnología brindará óptima calidad de servicios de telecomunicaciones como son: voz, datos y video con un ancho de banda especifico de acuerdo a la tecnología utilizada para este proyecto, la misma que abarcara todo el edificio principal garantizando la mejor disponibilidad y confiabilidad de los servicios ofrecidos por la Empresa.

Cabe indicar que al ser la red inalámbrica una alternativa de conectividad a la red cableada no se garantiza que llegue a tener la misma capacidad en ancho de banda y velocidad que la red cableada pero ayudará en gran medida a los problemas de conectividad que actualmente tienen los usuarios dentro de la organización dado que las redes comerciales típicas hacen uso extensivo de las redes conectadas por cable.

Las conexiones físicas se realizan entre sistemas de computación, sistemas de teléfono y otros dispositivos periféricos a conmutadores ubicados en los armarios de cableado ante ello administrar una infraestructura de cableado es bastante desafiante. Considere qué sucede cuando un trabajador decide que prefiere ubicar su sistema de computación en otro lugar de su oficina, o cuando un administrador quiere llevar su computadora portátil a la sala de conferencias y conectarse a la red desde allí. En una red conectada por cable, necesitará mover el cable de conexión de la red a una nueva ubicación en la oficina del trabajador y asegurarse de que exista una conexión de red disponible en la sala de conferencias. Cada vez son más comunes las redes inalámbricas para evitar estos cambios físicos.

En este capítulo se desarrollará un diseño de red inalámbrica de área local (WLAN) para la corporación ADSAMED ofreciendo un entorno de red flexible, para ello se utilizarán los distintos estándares inalámbricos que están disponibles hoy en día y las características que cada estándar ofrece, sus componentes de hardware que son usualmente necesarios en una infraestructura inalámbrica, además como operara la WLAN y cómo asegurarla.

Finalmente, se propondrá una simulación configurando un punto de acceso inalámbrico y un cliente inalámbrico de esta forma se probará el diseño propuesto para este edificio.

Componentes y operación de la LAN inalámbrica de ADSAMED.

Las LAN inalámbricas 802.11 extienden las infraestructuras LAN Ethernet 802.3 para proporcionar opciones adicionales de conectividad. Sin embargo, se utilizan componentes y protocolos adicionales para completar las conexiones inalámbricas. En una LAN Ethernet 802.3 cada cliente tiene un cable que conecta la NIC del cliente a un conmutador. El conmutador es el punto en el que el cliente obtiene acceso a la red. A diferencia de la red cableada la LAN inalámbrica, cada cliente utiliza un adaptador inalámbrico para obtener acceso a la red a través de un dispositivo inalámbrico como un enrutador inalámbrico o punto de acceso (AP).

En la figura 4.1 se muestra como el adaptador inalámbrico en el cliente se comunica con el enrutador inalámbrico o punto de acceso mediante señales RF Una vez conectados a la red, los clientes inalámbricos pueden acceder a los recursos de la red como si estuvieran conectados a la red mediante cable.

Componentes de la red Inalámbrica de ADSAMED

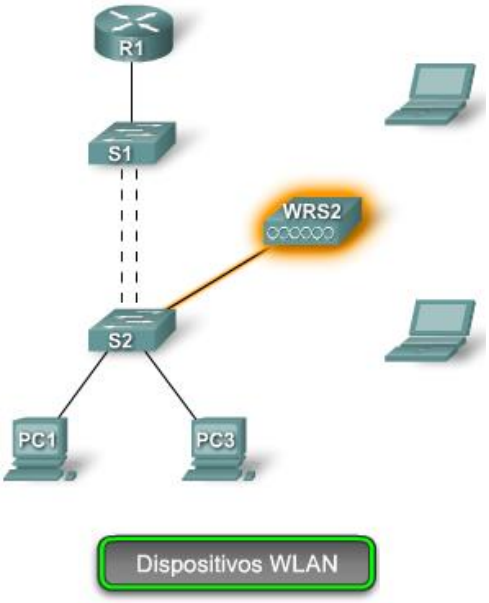


Figura 4.1: Dispositivos WLAN (adaptador inalámbrico en el cliente se comunica con el enrutador inalámbrico)
Creada por: Francisco Palacios.

En el gráfico 4.1 se puede apreciar que en una LAN inalámbrica, cada cliente utiliza un adaptador inalámbrico para obtener acceso a la red a través de un dispositivo inalámbrico como un enrutador inalámbrico o punto de acceso.

También se puede apreciar que el dispositivo AP está conectado a un conmutador el mismo que está conectado en cascada a otro y estos están conectados a una LAN por un sector y a una WAN por otro, de tal manera que se pueda formar una red hibrida conectando varias computadoras por medio del cableado estructurado.

Esta misma arquitectura será utilizada en el diseño propuesto para ADSAMED, tomando en cuenta especificaciones técnicas y estándares proporcionados por cada uno de los fabricantes de los componentes que se deberán utilizar para el desarrollo de este diseño.

Los equipos AP que se utilizarán son de fabricación de la empresa CISCO, los mismos fueron escogidos por su alta confiabilidad y funcionalidad.

En la figura 4.2 se observa el adaptador inalámbrico en el cliente el mismo que se comunica con el enrutador inalámbrico o punto de acceso mediante señales RF. Una vez conectados a la red, los clientes inalámbricos pueden acceder a los recursos de la red como si estuvieran conectados a la red mediante cable.

Componentes de la red Inalámbrica de ADSAMED

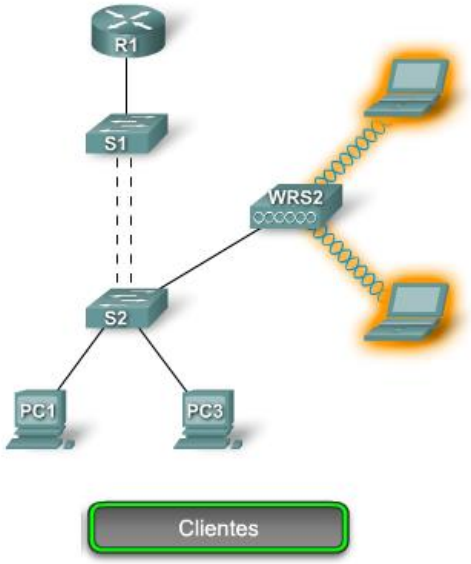
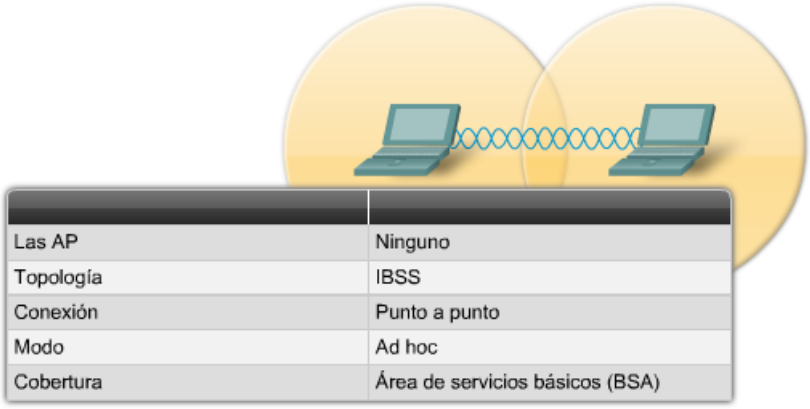


Figura 4.2 Clientes WLAN (Comunicación con enrutador inalámbrico desde los clientes inalámbricos)
Creada por: Francisco Palacios.

Tomando en cuenta que en los primeros capítulos se revisó los distintos modos de topología y conociendo la complejidad de implementar cada uno de ellos se tomo en consideración varios factores que ayudarán en este capítulo puesto que es el más importante de todo el proyecto de tesis por ende se muestra de forma resumida de forma resumida los diferentes modos que se podrían haber utilizado pero que considerando la magnitud y la escalabilidad del proyecto se tomo la decisión de optar por uno en particular.

Las redes inalámbricas pueden operar sin puntos de acceso; a esto se lo conoce como topología ad hoc. Las estaciones clientes que están configuradas para operar en modo ad hoc se puede apreciar mediante el ejemplo que se muestra en la figura 4.3 en donde se configuran los parámetros inalámbricos entre ellas. El estándar

IEEE 802.11 se refiere a una red ad hoc como un BSS (Conjunto de Servicios Básicos) IBSS (Conjunto de Servicios Básicos Independientes).



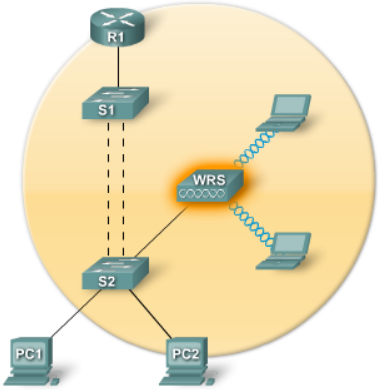
Las AP	Ninguno
Topología	IBSS
Conexión	Punto a punto
Modo	Ad hoc
Cobertura	Área de servicios básicos (BSA)

Figura 4.3: Topología Ad Hoc (Redes Inalámbricas que operan sin punto de acceso)
Creada por: Francisco Palacios.

Los puntos de acceso proporcionan una infraestructura que agrega servicios y mejora el alcance para los clientes. Un punto de acceso simple en modo infraestructura administra los parámetros inalámbricos y la topología es simplemente un BSS. El área de cobertura para un IBSS y un BSS es el área de servicios básicos BSA (Área de servicios básicos).

Cuando un BSS simple no proporciona la suficiente cobertura RF, se pueden unir uno o más a través de un sistema de distribución simple hacia un ESS (Conjunto de servicios extendidos) tal como se ha considerado en el ejemplo de la figura 4.4 y 4.5.

En un ESS, un BSS se diferencia de otro mediante el identificador BSS / BSSID (Dirección MAC del punto de Acceso), que sirve al BSS. El área de cobertura ESA (Área de servicio extendida) es el área en donde operara estos servicios extendidos. A continuación se muestra el ejemplo en la figura 4.4 y 4.5



Las AP	Uno
Topología	BSS
Conexión	Cliente a AP
Modo	Infraestructura
Cobertura	Área de servicios básicos (BSA)

Figura 4.4 BSS (Conjunto de servicios básicos extendidos mediante áreas de cobertura extendida)
Creada por: Francisco Palacios.

Cuando un BSS simple no proporciona la suficiente cobertura RF, se pueden unir uno o más a través de un sistema de distribución simple hacia un conjunto de servicios extendidos (ESS). En un ESS, un BSS se diferencia de otro mediante el identificador BSS (BSSID), al BSS. El área de cobertura es el área de servicio extendida (ESA).

Las AP	Más de una
Topología	ESS
Conexión	Cliente a AP
Modo	Infraestructura
Cobertura	Área de servicio extendida (ESA)

Figura 4.5 ESS (Conjunto de servicios extendidos mediante áreas de cobertura extendida por medio de BSSID)
Creada por: Francisco Palacios.

En resumen se puede definir mediante la figura 4.6 la tabla de modos de topologías existentes en el medio las cuales se podrá utilizar en este diseño o en otro propuesto por algún maestrante.

Resumen de las topologías WLAN

Dispositivos inalámbricos	Modo de topología	Topología del bloque del edificio	Área de cobertura
No hay puntos de acceso	Ad hoc	Conjunto de servicios básicos independientes (IBSS)	Área de servicios básicos (BSA)
Un punto de acceso	Infraestructura	Conjunto de servicios básicos (BSS)	Área de servicios básicos (BSA)
Más de un punto de acceso	Infraestructura	Conjunto de servicios extendidos (ESS)	Área de servicio extendida (ESA)

Figura 4.6: Topologías WLAN (Modos de Topología existentes para las WLAN)
Creada por: Francisco Palacios.

Una vez identificado estos escenarios se propondrá utilizar el diseño de red inalámbrica de tipo infraestructurada ESS, puesto que esta arquitectura tecnológica es la ideal para la necesidad de redes inalámbricas de la corporación Adsamed.

Componentes relacionados con la WLAN de ADSAMED

Para este diseño se escogió varios componentes como tres servidores Windows server 2008 R2, los mismos que servirán para la conexión a la red inalámbrica de invitados o de usuarios autenticados en nuestra red.

Estos servidores serán utilizados con diferentes roles y cada uno tendrá configuraciones especiales. Los dos primeros servidores tendrán instalados los servicios de controlador de dominio DNS y un “active directory” (Servicio de directorio activo en una red distribuida) quien será el encargado de proporcionar la autentificación de los usuarios del dominio y los que no se encuentren en el dominio para el caso de los usuarios invitados.

Cabe indicar que estos servidores funcionan el uno como servidor principal de dominio y el segundo como secundario, esto se realiza con la finalidad de proporcionar redundancia para el caso de que el servidor de dominio principal falle.

En el tercer servidor estará instalado el rol del servidor RADIUS el mismo que permitirá conectarse a través de la red inalámbrica este tiene la funcionalidad de

consultar al "active directory" y conceder o denegar el permiso a nuestra red a usuarios autentificados.

Para los usuarios invitados que normalmente existen en la red como por ejemplo, proveedores, consultores, visitantes, etc. Se ha considerado otro grupo de acceso para evitar que usuarios no autentificados ingresen a la red sin autorización.

Instalación y Configuración de Servidor RADIUS

Para entender más al detalle el rol del servidor radius en la figura 4.7 se muestra el siguiente esquema en el mismo se detalla gráficamente los dispositivos implementados como el servidor radius, el AP, el conmutador de configuración y los equipos a conectarse por medio de las tarjetas inalámbricas de las computadoras que utilicen esta conexión.

ESQUEMA

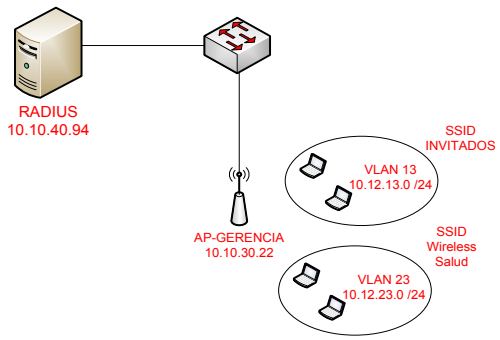


Figura 4.7: Esquema de Servidor Radius (Funcionamiento del rol del servidor radius en la red wlan de Adsamed)
Creada por: Francisco Palacios.

Para comenzar con la instalación del servidor Radius se debe tener instalado Windows Server Estándar 2008 R2 de 64 bits, este permitirá instalar los servicios del servidor Radius, en la figura 4.8 se muestra las características de dicho servidor que se encuentra instalado en una máquina virtual dentro de la empresa.

.

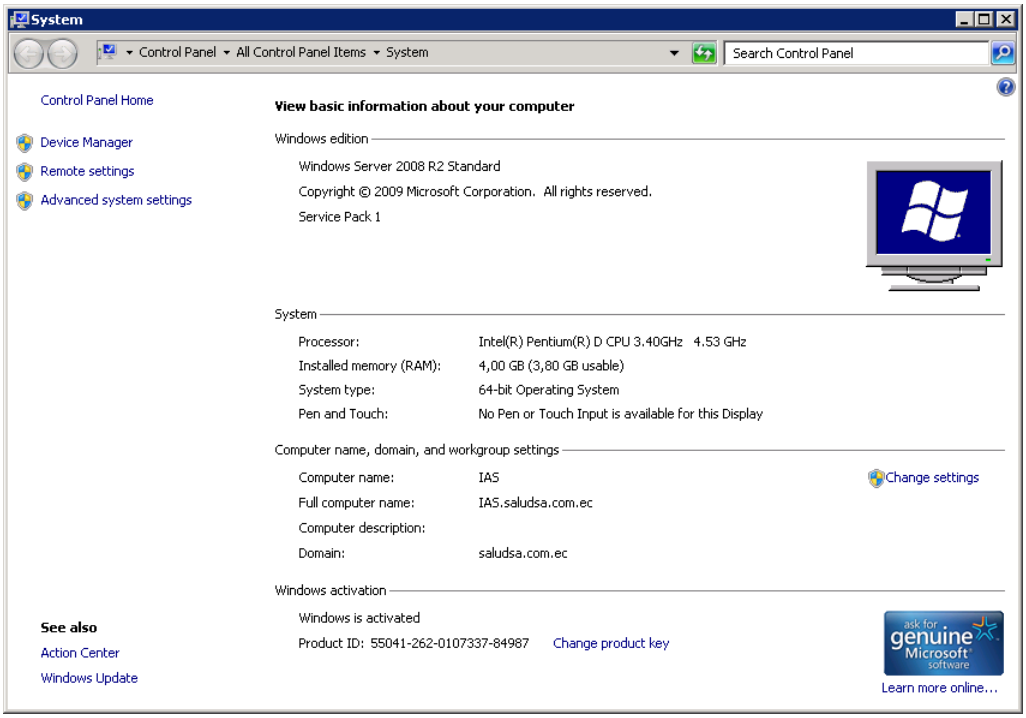


Figura 4.8: Servidor Radius (características de servidor radius instalado en una máquina virtual)
Creada por: Francisco Palacios.

Instalación de "Service Pack" 1 de Windows Server 2008 R2.

Uno de los requisitos de la instalación del servidor Radius es la instalación del **"service pack"** 1 de Windows server 2008 R2 de Microsoft tal como se muestra en la figura 4.9, este instalador se descarga del internet y luego se procede a ejecutarlo, el paquete tiene la siguiente denominación "windows6.1-KB976932-X64.exe".

En la figura 4.9 se muestra la ejecución del paquete "windows6.1-KB976932-X64.exe" por primera vez, aquí nos muestra el botón "Run" que se debe presionar para comenzar con la instalación.

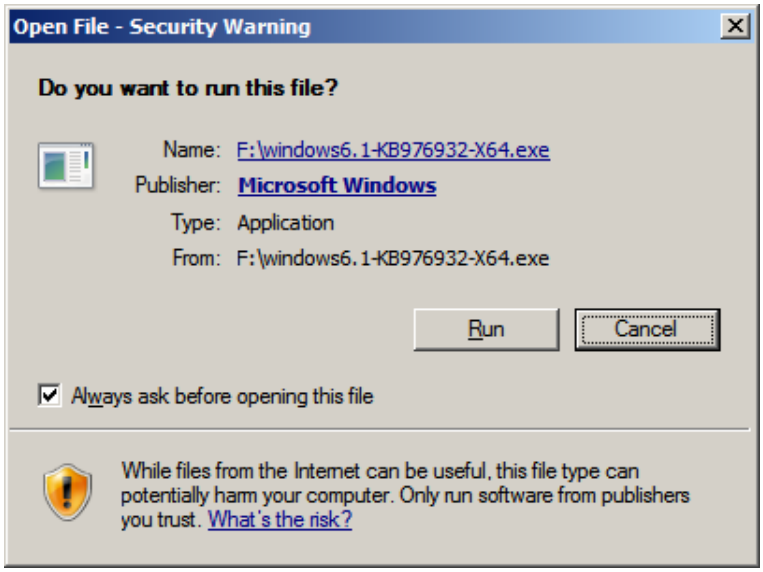


Figura 4.9: Servipack 1 (Requisito indispensable para la instalación del servidor radius)
Creada por: Francisco Palacios.

A continuación se observa la figura 4.10 en donde se presiona el botón **"Next"** para continuar la instalación del **"service pack"** 1.

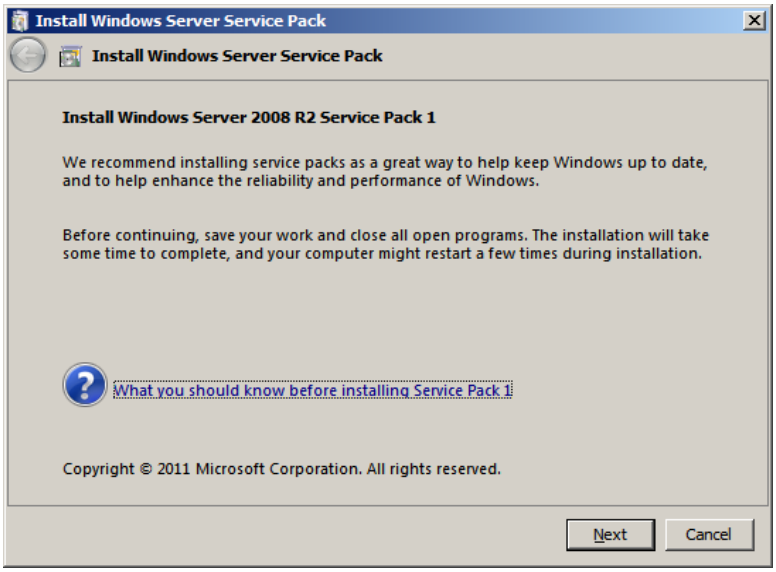


Figura 4.10: Instalador Run (Instalación del paquete de windows6.1-KB976932-X64.exe)
Creada por: Francisco Palacios.

En la figura 4.11 se muestra el avance del progreso de la instalación.

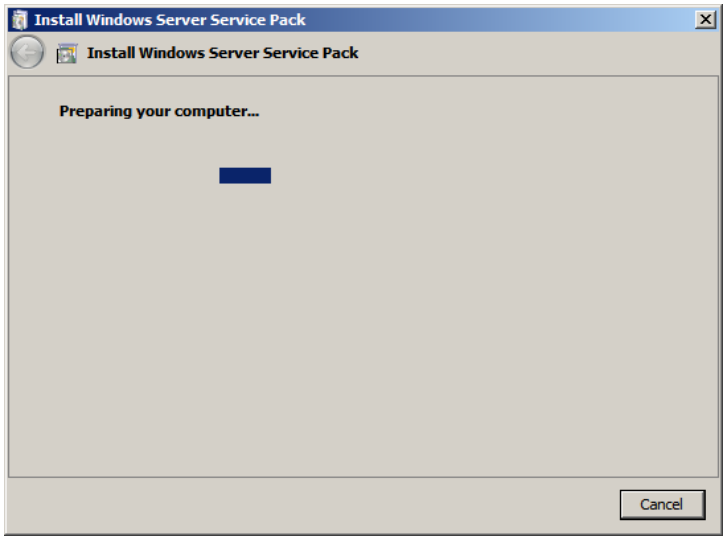


Figura 4.11: Boton Next (Continuación de la instalación del Servipack 1)
Creada por: Francisco Palacios.

Luego de la instalación es necesario verificar que se encuentre activada la opción **"Automatically restart the computer"**, y presionar **"Install"**, tal como se muestra en la figura 4.12 y cuando se termine esta instalación el equipo se reiniciara automáticamente.

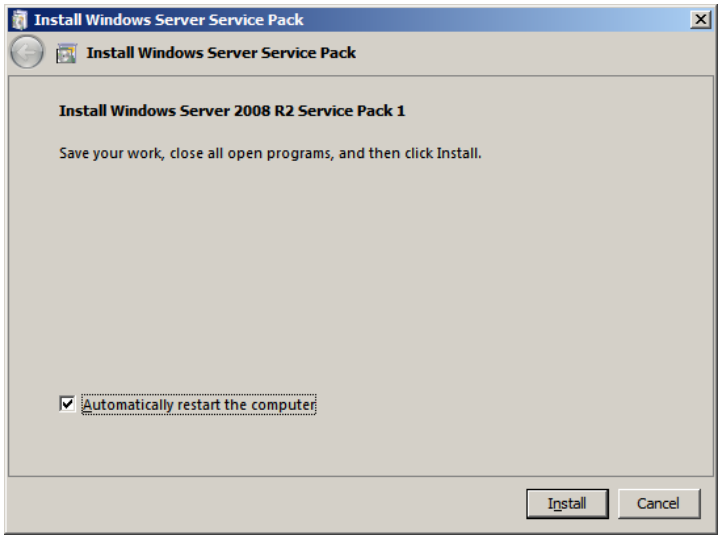


Figura 4.12: Windows Service Pack (Continuación de evento de instalación de servipack 1)
Creada por: Francisco Palacios.

En la figura 4.13 se mostrara la continuación de la instalación antes de que culmine esta etapa.

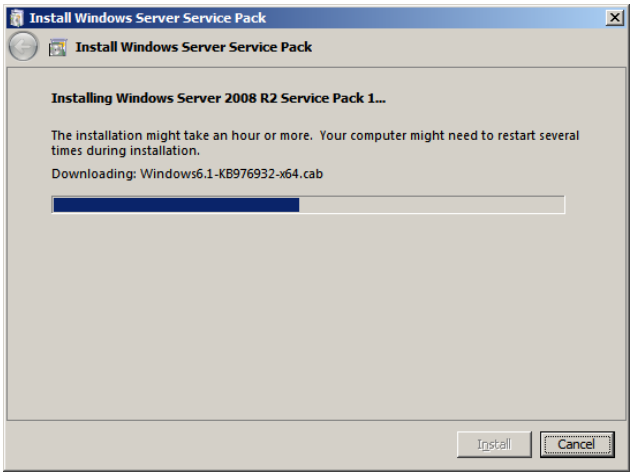


Figura 4.13: Windows Service Pack (Continuación de evento de instalación de servipack 1)
Creada por: Francisco Palacios.

Una vez realizado el proceso de instalación del **"service pack" 1** se abra terminado el primer paso de la instalación del rol de servidor Radius

Instalación Network Policy Service NPS

Para continuar con el proceso de configuración e instalación el siguiente paso es instalar el rol de servidor radius, la instalación se muestra a continuación. Se procede abrir la ventana de "Add Roles Wizard", en esta ventana se escoge la opción "Server Roles" en el lado izquierdo y luego se escoge la opción **"Network Policy and Access Services"**, luego de esto se procede a presionar el botón **"Next"** en la parte inferior de la ventana tal como se observa en la figura 4.14.

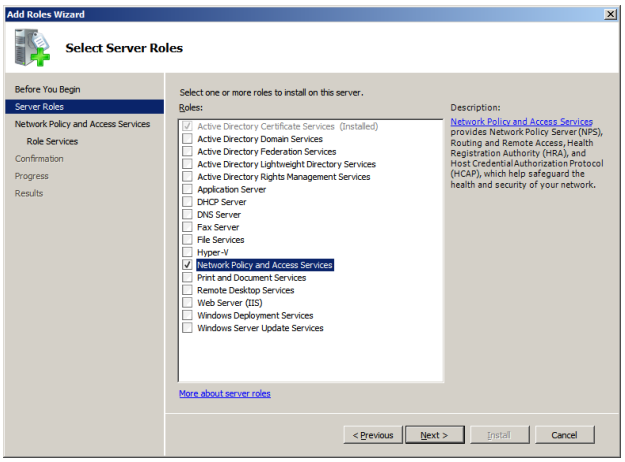


Figura 4.14: Add Roles Wizard (Ventana de roles en servidor radius)
Creada por: Francisco Palacios.

Una vez concluido el proceso anterior se procede abrir del lado izquierdo el enlace que dice **"Network Policy and Access Services"** como se observa en la figura 4.15 y en este se escoge del lado derecho la opción **"Network Policy Server"** y se presiona el botón **"Next"** de esta manera queda instalado el nuevo rol del servidor.

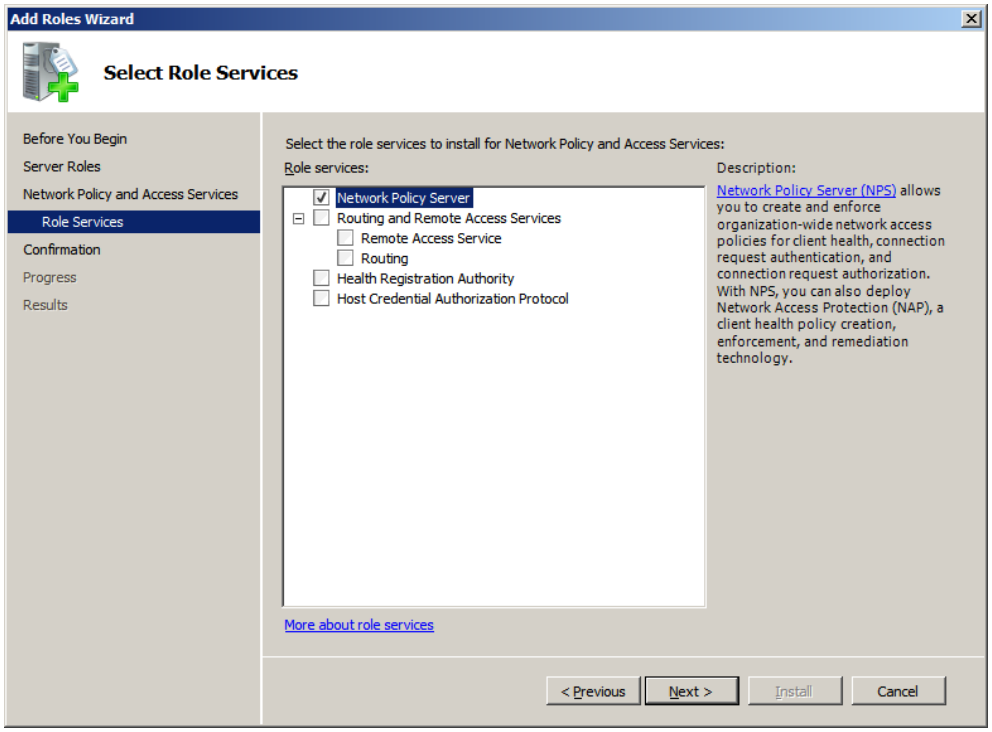


Figura 4.15: Network Policy Server (Instalación del Nuevo Rol)
Creada por: Francisco Palacios.

A continuación las siguientes tres ventanas figura 4.16, 4.17, 4.18, muestran la confirmación de instalación del nuevo rol y el progreso de la misma, cabe recalcar que esto es parte del proceso de instalación del servidor Radius, recordar también que este servicio o rol es el que nos permitirá conectarnos a nuestra red inalámbrica a través de los permisos que se tenga en el servidor de nombres DNS.

Luego de finalizada esta instalación se mostraran los resultados de la misma y se procede a verificar que dicha instalación haya sido exitosa mediante el mensaje de "**Installation Succeeded"**, que significa que la instalación del nuevo rol en este servidor no tuvo problemas con lo cual se finaliza presionando el botón **"close".**

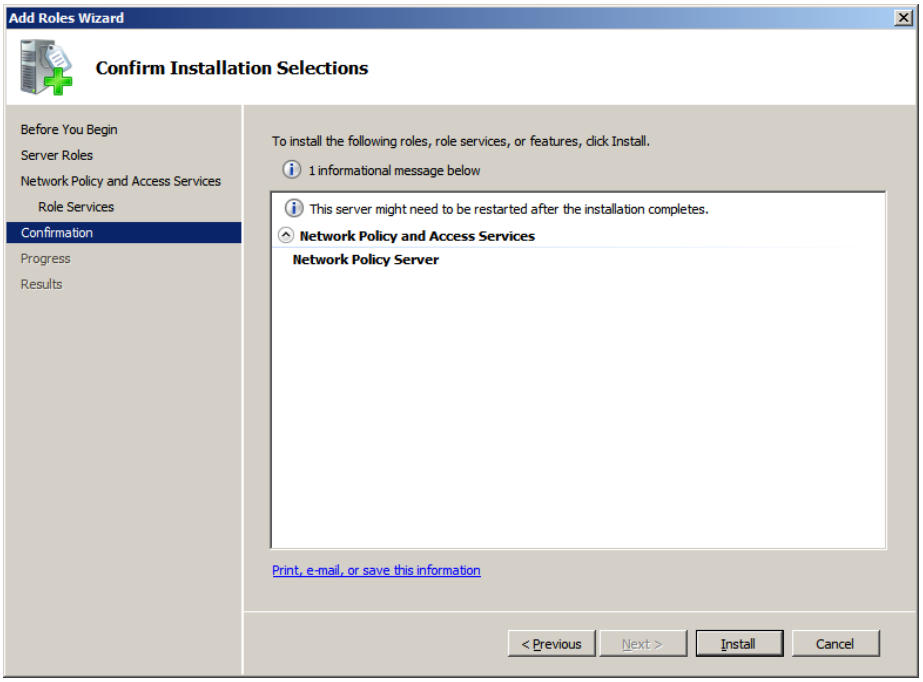


Figura 4.16: Confirm Installation Selections (Confirmación de la instalación del nuevo rol)
Creada por: Francisco Palacios.

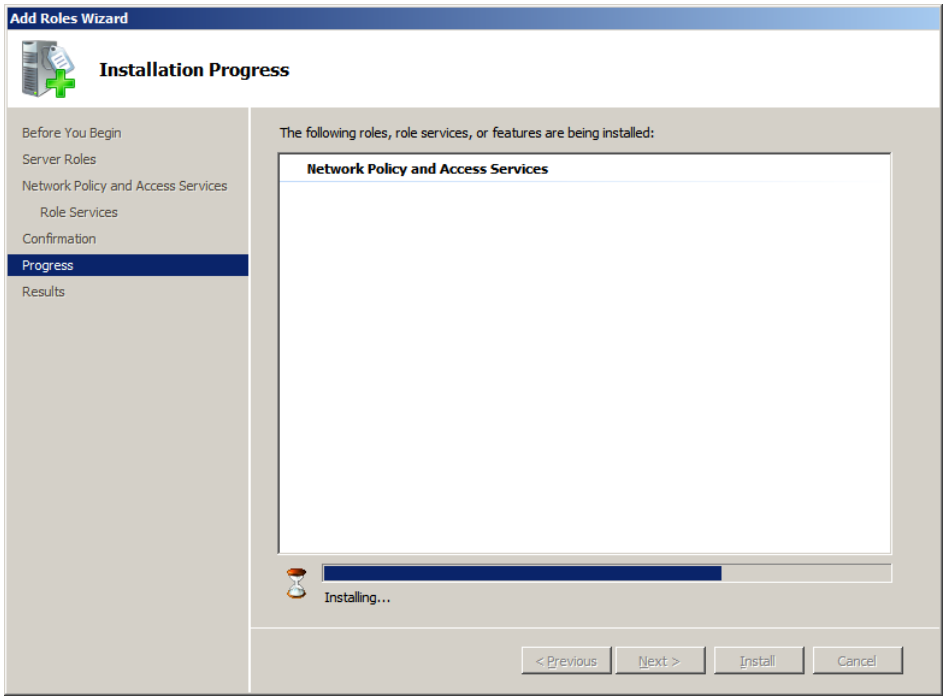


Figura 4.17: Installation Progress (Progreso de instalación del nuevo rol)
Creada por: Francisco Palacios.

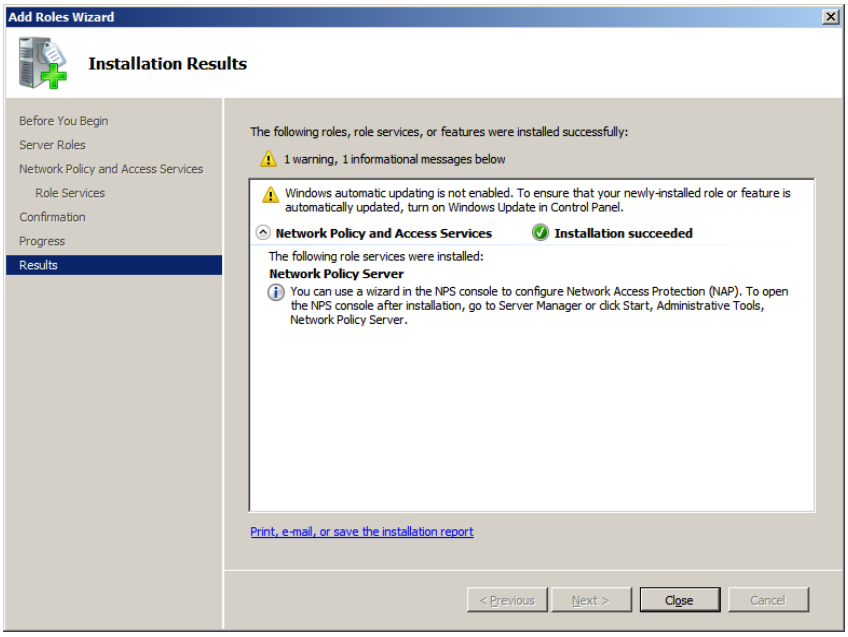


Figura 4.18: Installation Results (Información de resultados de la instalación)
Creada por: Francisco Palacios.

Al finalizar la instalación se podrá observar el nuevo rol ya instalado en el servidor Windows server 2008 R2 tal como se muestra en la figura 4.19.

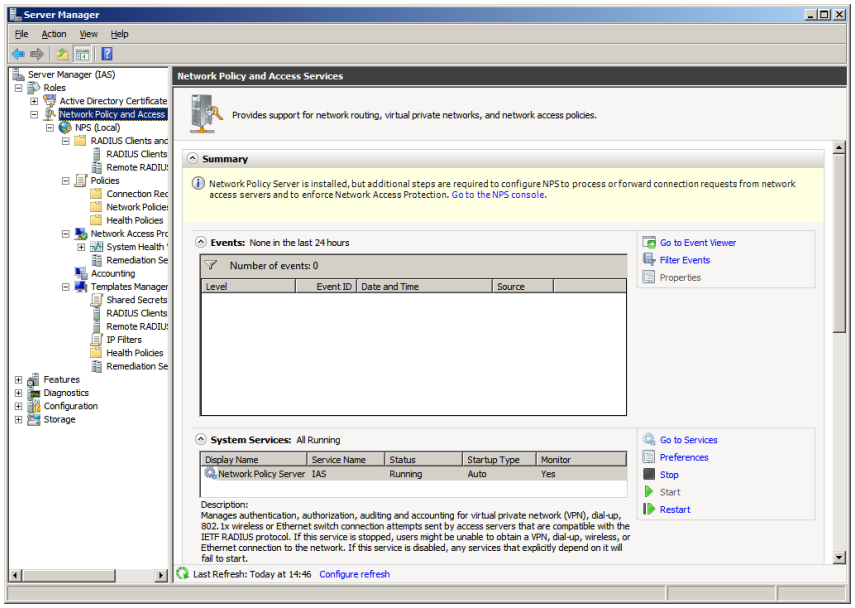


Figura 4.19: Rol Instalado (Rol de Servidor Radius instalado en Windows Server 2008 R2)
Creada por: Francisco Palacios.

Configuración en el Active Directory

En el Active Directory de la empresa se agrega al servidor Radius (IAS.saludsa.com.ec) al grupo de "Servidores RAS e IAS" tal como se muestra en el ejemplo de la figura 4.20 y 4.21. Para que estos cambios surjan efecto es necesario reiniciar el servidor Radius para que tenga estos permisos.

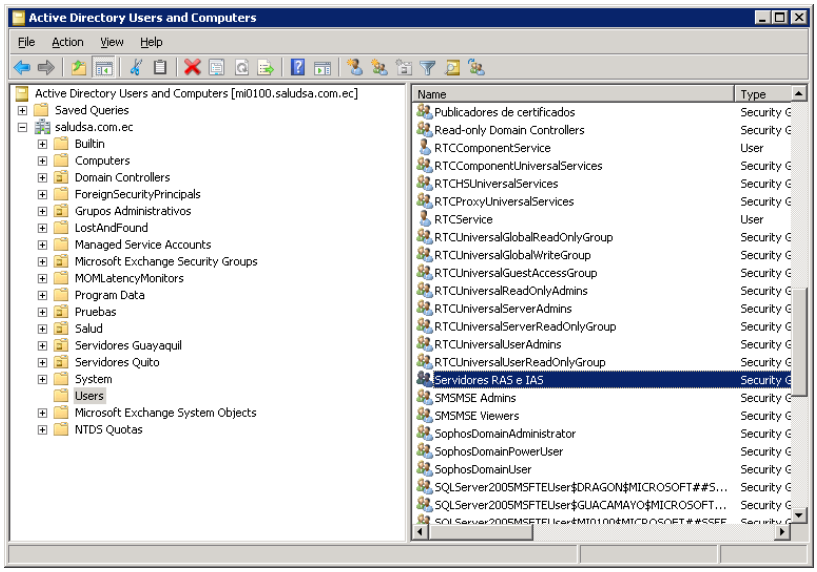


Figura 4.20: Active Directory (Asignación de servidor Radius al grupo Ras e IAS)
Creada por: Francisco Palacios.

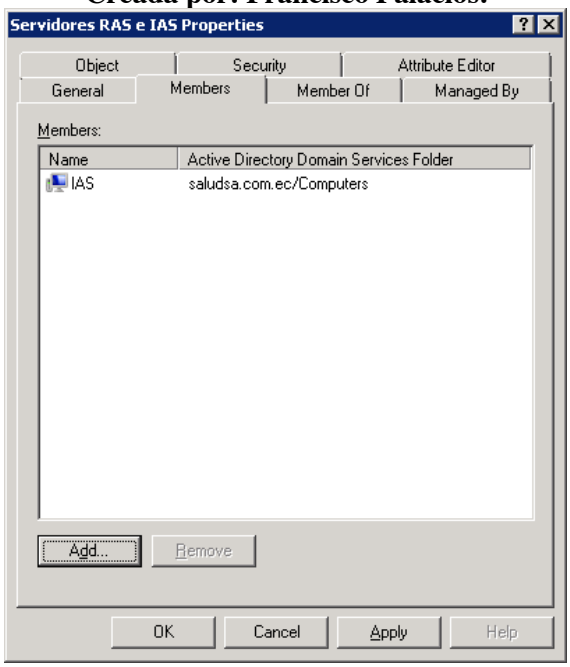


Figura: 4.21 RAS e IAS (Asignación de servidor Radius al grupo Ras e IAS)
Creada por: Francisco Palacios.

Luego de agregar al servidor Radius al grupo de servidores RAS e IAS se crea un grupo "Usuarios Wireless", el cual permitirá colocar todos los usuarios que necesiten conectarse a la red de manera segura a través de la conexión inalámbrica, este proceso se muestra en la figura 4.22 que a continuación se observa.

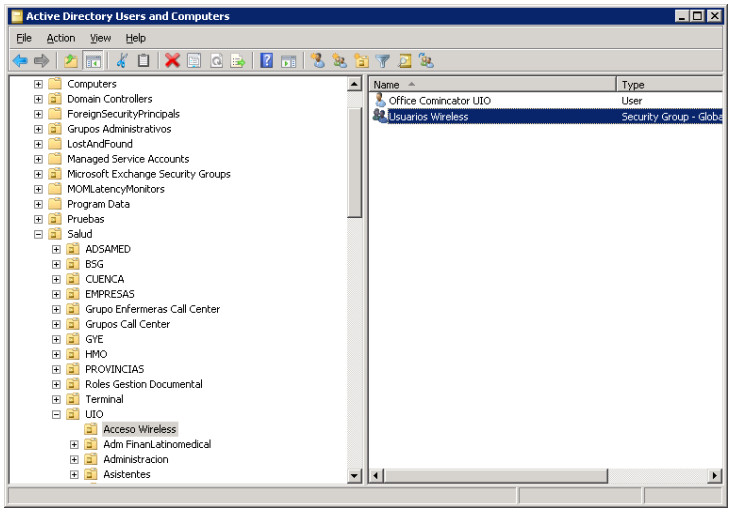


Figura 4.22: User Wireless (Grupo de usuarios autenticados)
Creada por: Francisco Palacios.

Todos los usuarios que formen parte de este grupo se podrán autenticar con el servidor Radius en la figura 4.23 se puede apreciar los usuarios asignados a este grupo.

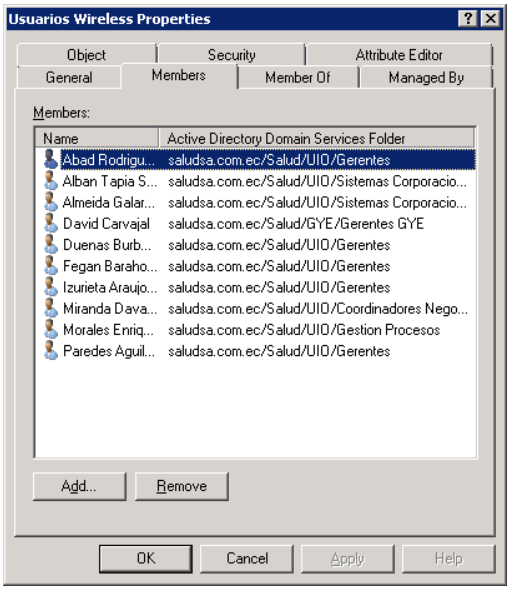


Figura 4.23: Propiedades de los usuarios wireless (Usuarios autenticados mediante active directory)
Creada por: Francisco Palacios.

Componentes relacionados con la seguridad de WLAN de ADSAMED
Configuración en Entidad Certificadora

Dentro del servidor Radius se procede a configurar la entidad certificadora esto se lo realiza con la finalidad de que cada vez que un usuario necesite conectarse a la red inalámbrica al mismo se le otorgue un certificado de conexión automático a fin de garantizar la seguridad en la conexión.

La siguiente ventana muestra en donde configurar dicha entidad certificadora y cómo hacerlo, para lo cual se procede a presionar el botón derecho en "Certificate Templates" y seleccionar "Manage". Este proceso se puede observar en la figura 4.24 que se muestra a continuación.

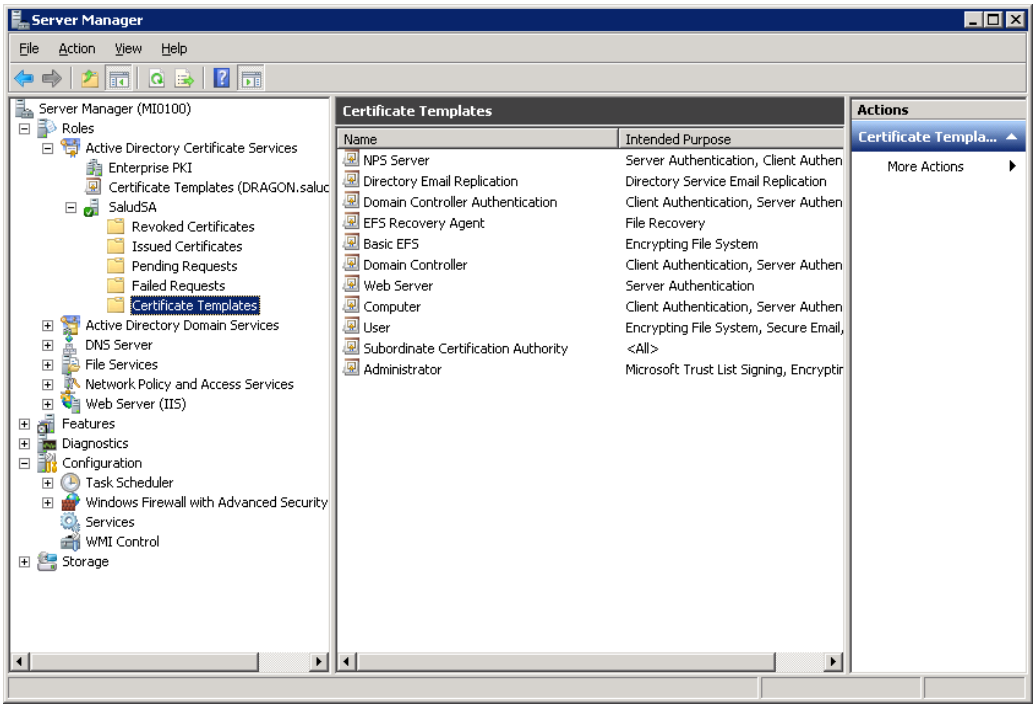


Figura 4.24: Certificate Templates (Entidad certificadora para conexión de usuarios)
Creada por: Francisco Palacios.

Luego de haber seleccionado "Manage" se procede a seleccionar "Servidor RAS e IAS" del lado derecho de la ventana y se procede a presionar el botón derecho del "mouse" y se selecciona la opción "Duplicate". Una vez que se nos muestre dicha ventana hay que verificar que aparezca la opción "Windows Server 2008

Enterprise" tal como se muestra en el siguiente figura 4.25.

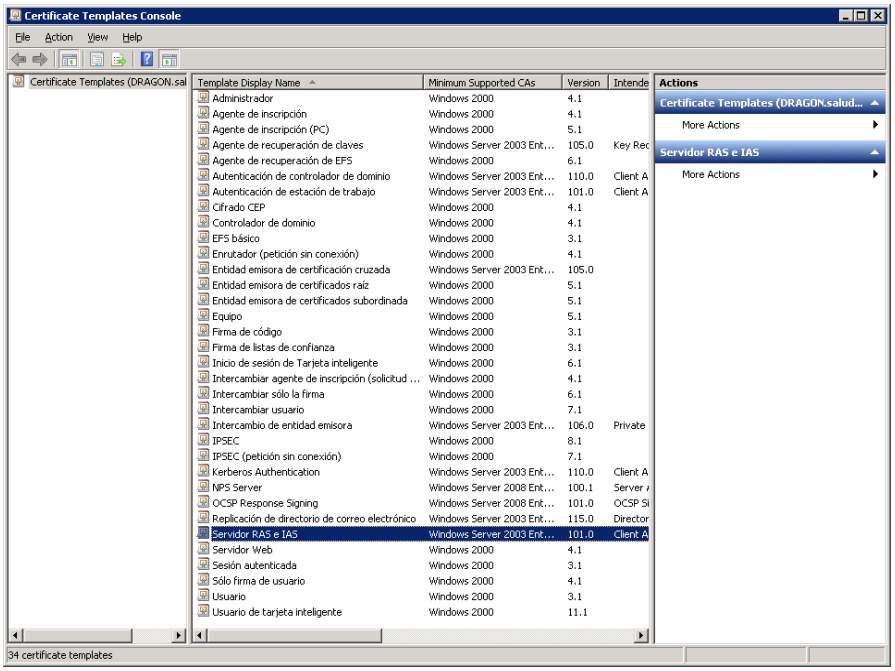


Figura 4.25: Certificate Templates Console (Configuración de Entidad certificadora para conexión de usuarios)
Creada por: Francisco Palacios.

A continuación la figura 4.26 que nos muestras la ventana de verificación que se menciono en el texto anterior y la opción "Windows Server 2008 Enterprise" y luego de ello se presiona OK.

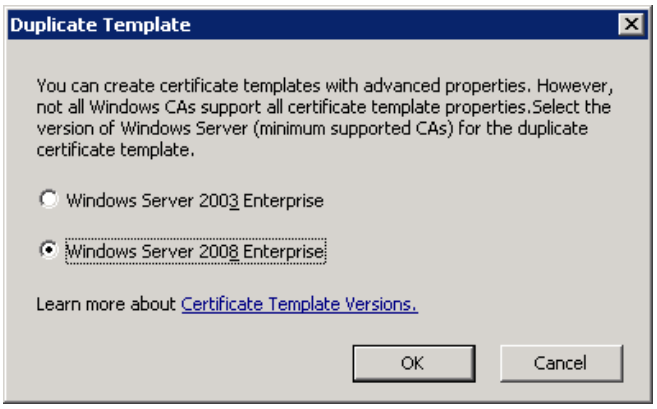


Figura 4.26: Duplicate Template (Ventana de verificación del Sistema Operativo del certificado)
Creada por: Francisco Palacios.

Para continuar con el proceso se debe colocar un nombre para el nuevo certificado tal como se muestra en la figura 4.27 que se detalla a continuación.

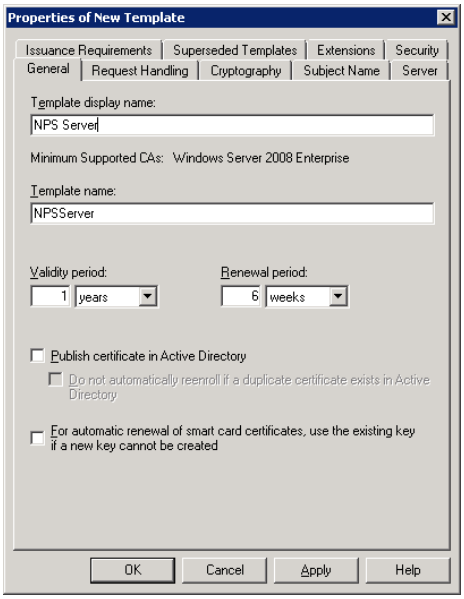


Figura 4.27: New Template (Nombre de Certificado)
Creada por: Francisco Palacios.

Luego de haber realizado el proceso anterior en la pestaña "Security" se agrega la política al grupo "Servidores RAS e IAS", y se verifica que se encuentren asignados los atributos "Enroll" y "Autoenroll" tal como se muestra en la figura 4.28.

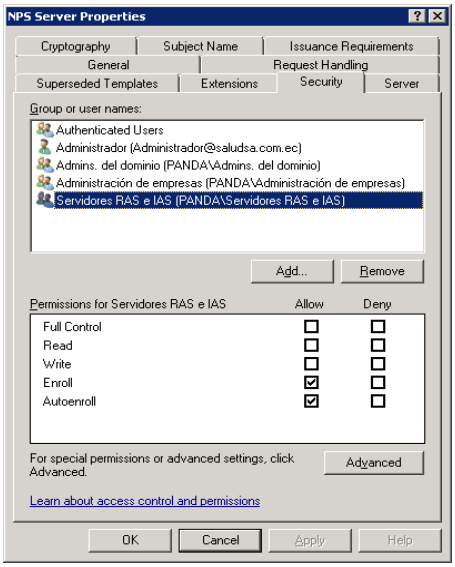


Figura 4.28: Servidor RAS e IAS (Propiedades de los servidores RAS e IAS)
Creada por: Francisco Palacios.

Configuración Cliente Radius

En la opción NPS que se encuentra del lado izquierdo de la ventana, se procede a seleccionar con el botón izquierdo del "mouse" en "RADIUS clients" y se selecciona "New" tal como se ve en la figura 4.29.

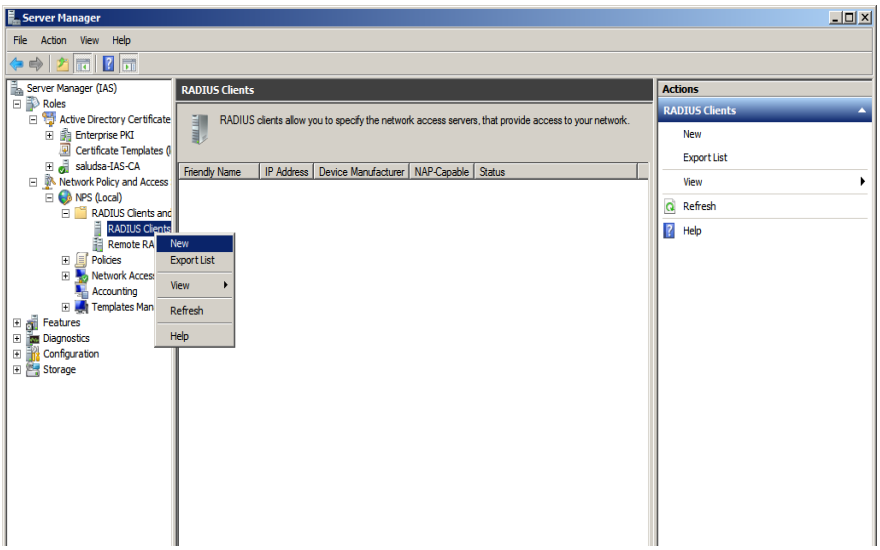


Figura 4.29: NPS (Configuración de servicio para clientes radius)
Creada por: Francisco Palacios.

En la figura 4.30 Se muestra la configuración en donde se especifica un nombre para el cliente Radius y la dirección IP (10.X.X.X) del Access Point, esta IP se la coloca dependiendo de la asignación que nos otorgue los administradores de red de la empresa, además hay que establecer una contraseña secreta (XXXXXXXXXXX) para establecer la comunicación entre el Servidor Radius y el cliente (AP).

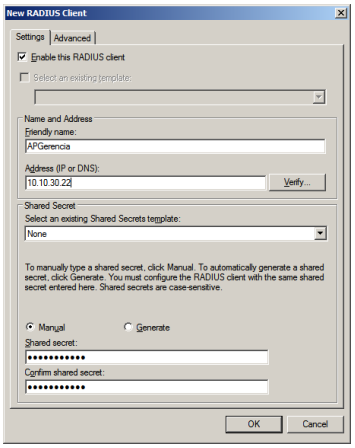


Figura 4.30: Radius Cliente (Nombre del cliente radius)
Creada por: Francisco Palacios.

Adicional a las configuraciones que se revisó anteriormente en la ventana anterior en las opciones avanzadas se puede especificar "Vendor name" del cliente Radius (Cisco), que es el nombre del fabricante del AP. En la figura 4.31 se ilustra el ejemplo.

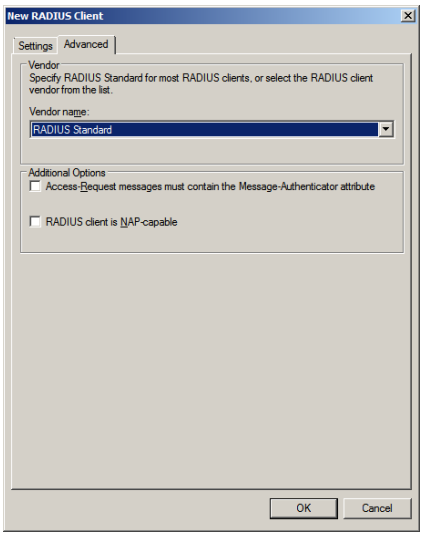


Figura 4.31: Radius Client (Nombre del fabricante del AP)
Creada por: Francisco Palacios.

Una vez finalizado de revisar todo este proceso se procede a presionar OK y se abra terminado con esta etapa.

Solicitud de Certificado a la Entidad Certificadora

En este proceso en el servidor se procede a ejecutar el comando "Run"en la barra de inicio del Sistemas Operativo Windows 2008 Server y luego se escribe el comando "mmc" para abrir una consola local de administración tal como se observa en la figura 4.32.

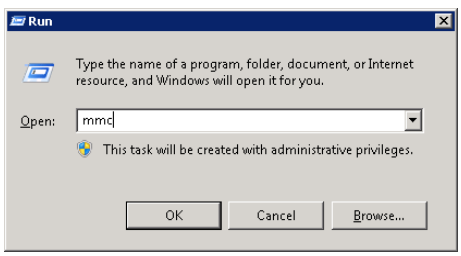


Figura 4.32: Run (Ejecución del mmc para consola de administración)
Creada por: Francisco Palacios.

En la consola que se observa en la figura 4.33 se procede a escoger la opción File y luego la opción Add/Remove Snap-in".

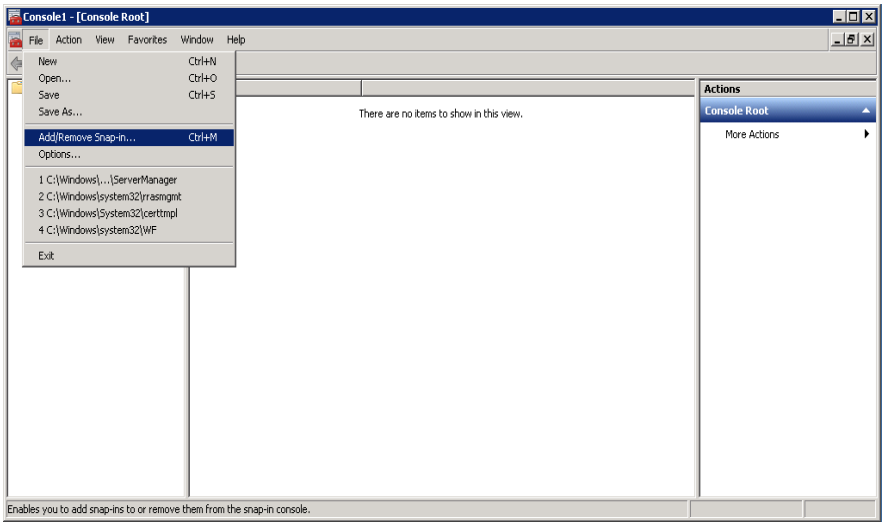


Figura 4.33: Console Root (Consola de administración)
Creada por: Francisco Palacios.

Una vez terminado el proceso anterior se procede con la opción **"Certificates"** y luego la opción **"Add"** que se encuentra a un costado del menú en la figura 4.34 en donde se encuentra la opción anterior.

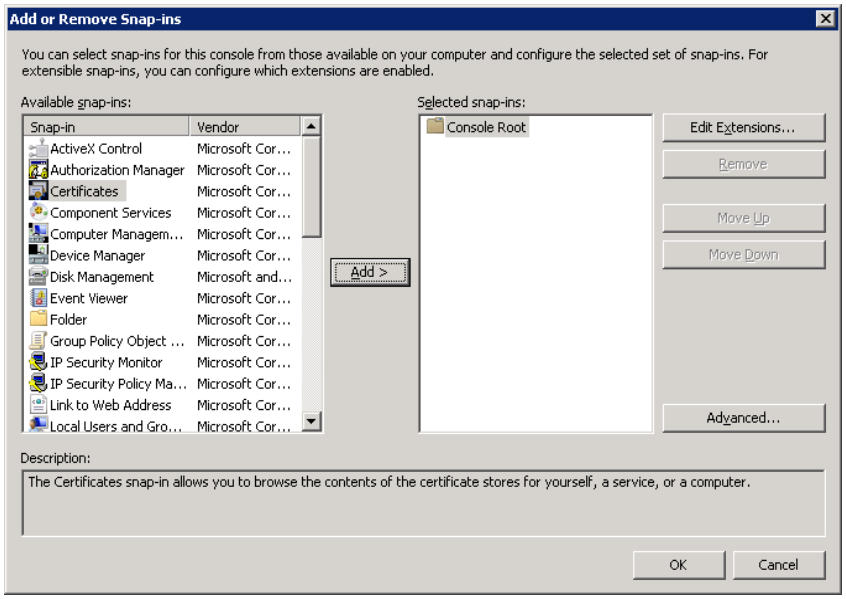


Figura 4.34: Add Remove Snap Ins (Configuración de certificados)
Creada por: Francisco Palacios.

En la figura 4.35 se escoge la tercera opción dentro de la entidad certificadora la llamada **"Computer Account"** y luego se presiona "Next" para continuar con el proceso.

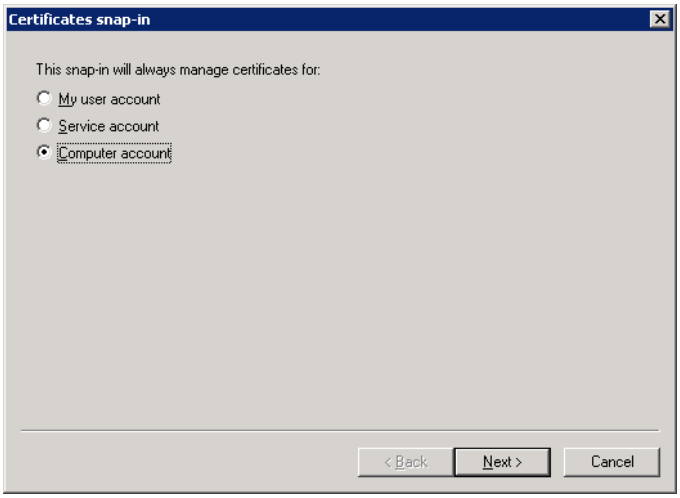


Figura 4.35: Certificates snap in (Cuentas de Computador)
Creada por: Francisco Palacios.

En la figura 4.36 que se muestra a continuación se escoge la opción **"Local computer: (the computer this console is running on)"** y luego se presiona "Next".

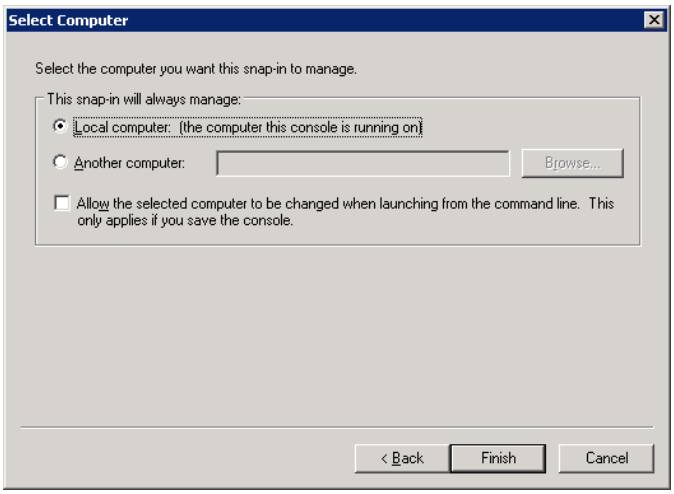


Figura 4.36: Select Computer (Para computadoras locales de la red)
Creada por: Francisco Palacios.

En la figura 4.37 se puede visualizar que se ha agregado la instancia "Certificates (Local computer)".

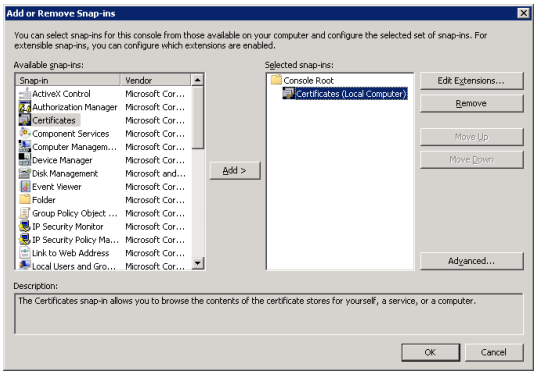


Figura 4.37: Certificates Local Computer
Creada por: Francisco Palacios.

Para continuar con el proceso de instalación y configuración se procede a presionar el botón derecho del "mouse" sobre Personal y luego en "**All Tasks"** para terminar seleccionando la opción **"Request New Certificate"**, tal como se aprecia en la figura 4.38.

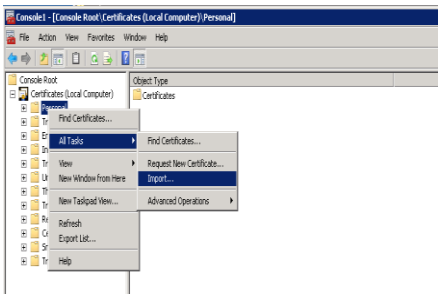


Figura 4.38: Request New Certificate
Creada por: Francisco Palacios.

Luego se procede a presionar "Next" como se ve en la figura 4.39 en la primera pantalla del "wizard".

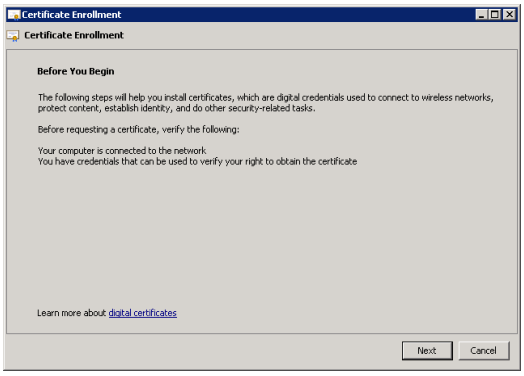


Figura 4.39: Certificate Enrollment
Creada por: Francisco Palacios.

Luego se deja por defecto la configuración que viene a continuación y se presiona "next" tal como se muestra en la figura 4.40

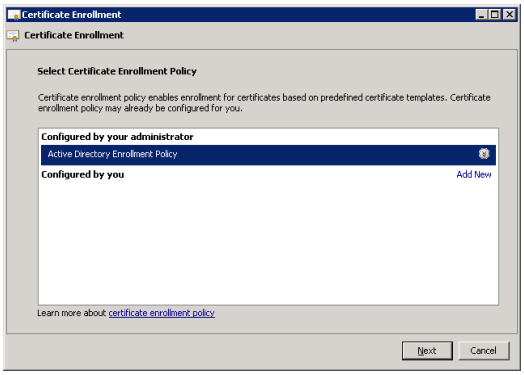


Figura 4.40: Active Directory Enrollment Policy
Creada por: Francisco Palacios.

En la figura 4.41 se escoge el certificado que se requiere para realizar la petición, en este caso es el **"NPS Server"**, el cual fue creado previamente en la Entidad Certificadora, luego de esto se presiona **"Enroll"**.

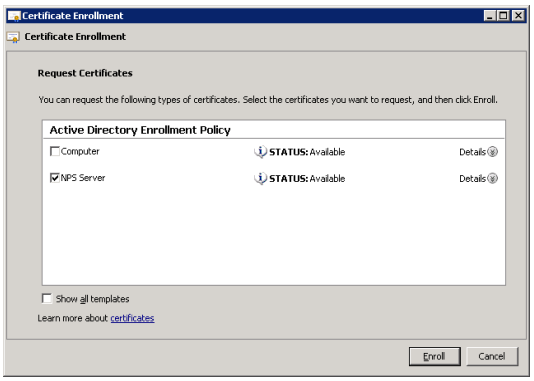


Figura 4.41: NPS Server (Certificado NPS Server)
Creada por: Francisco Palacios.

En la figura 4.42 se puede observar en la pestaña “Personal → Certificates” que ya se encuentra agregado el certificado que sé solicito.

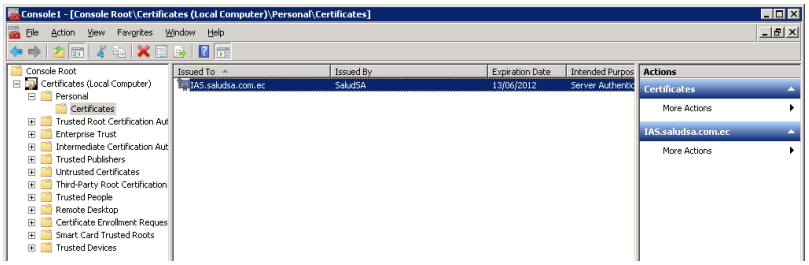


Figura 4.42: Certificado Agregado en server radius
Creada por: Francisco Palacios.

Configuración de “Wireless Access Policies”

En el rol NAS del servidor Windows server 2008 se selecciona en el menú principal **“Standard Configuration”**, en esta parte se debe seleccionar el “wizard” de configuración de “RADIUS server for 802.1x Wireless o Wired Connections”. Finalmente se selecciona “Configure 802.1x”, esto se puede apreciar en la figura 4.43 que se muestra a continuación.

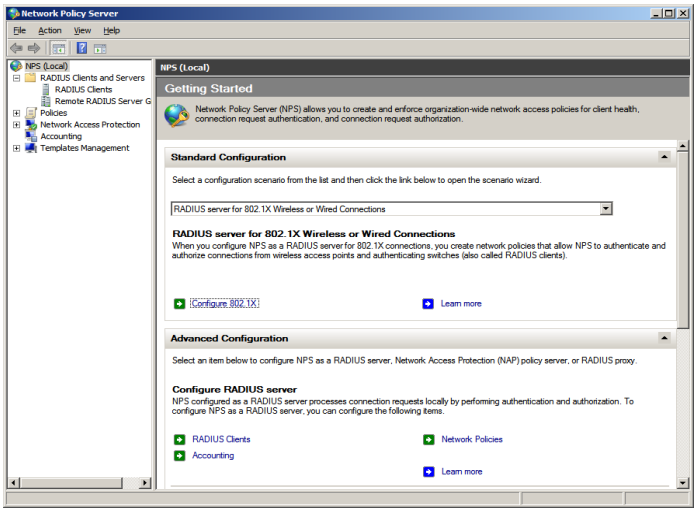


Figura 4.43: Network Policy Server
Creada por: Francisco Palacios.

A continuación se selecciona si esta política será para una red alámbrica o inalámbrica, en este caso se selecciona **“Secure Wireless Connections”**, además es necesario especificar un nombre para la política el mismo se lo dejo por defecto por motivos de configuración y pruebas véase la figura 4.44.

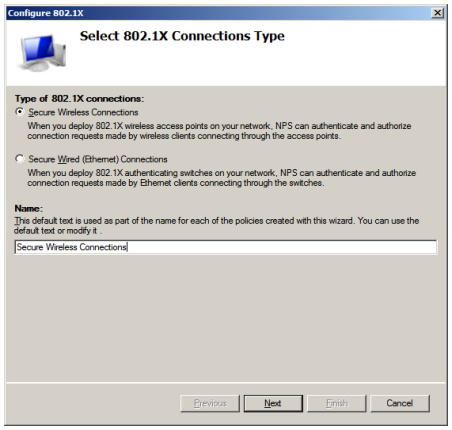


Figura 4.44: Configuración 802.1X (Tipo de Conexión 802.1X)
Creada por: Francisco Palacios.

A continuación se selecciona el cliente "Radius" que se va a utilizar para estas pruebas para mostrar esta ejecución se creó APGerencia luego de escoger esta opción se presiona el botón "Next", para continuar con la instalación, véase figura 4.45.

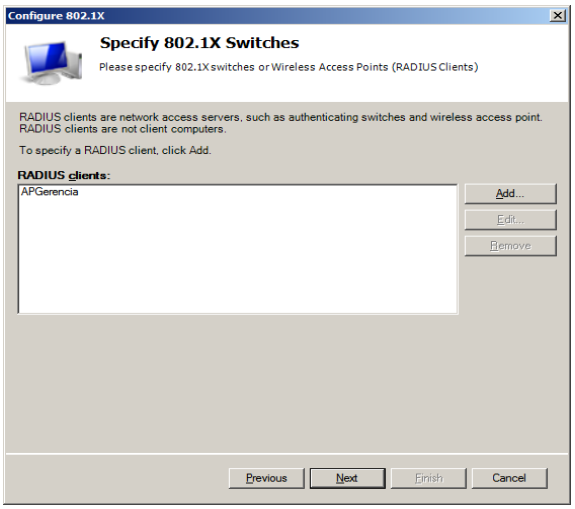


Figura 4.45: Specify 802.1X APGerencia
Creada por: Francisco Palacios.

Luego de esto tal como nos muestra la figura 4.46 se selecciona el tipo de método EAP (Protocolo de autenticación extensible) que se va a utilizar en esta política el cual es "Microsoft: Protected EAP (PEAP)" para configurar el método de autenticación.

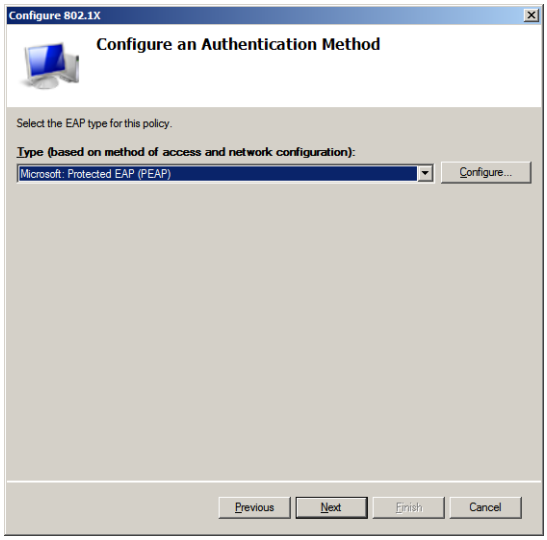


Figura 4.46 Configuración de Método de Autenticación
Creada por: Francisco Palacios.

En el siguiente paso se especifica el grupo de usuarios al cual se aplicará esta política "Usuarios Wireless" en esta etapa se asigna todos los usuarios que van a utilizar la red inalámbrica de forma segura y que se autenticaran con el dominio mediante el "active directory" véase la figura 4.47 y 4.48.

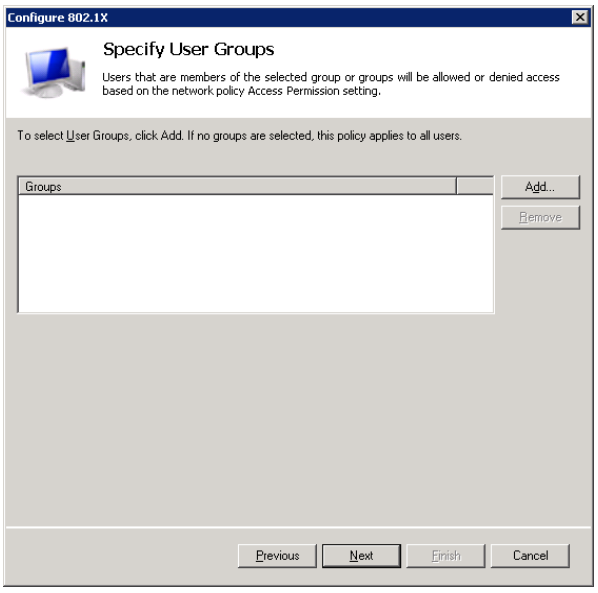


Figura 4.47: Especificación de grupo de usuarios
Creada por: Francisco Palacios.

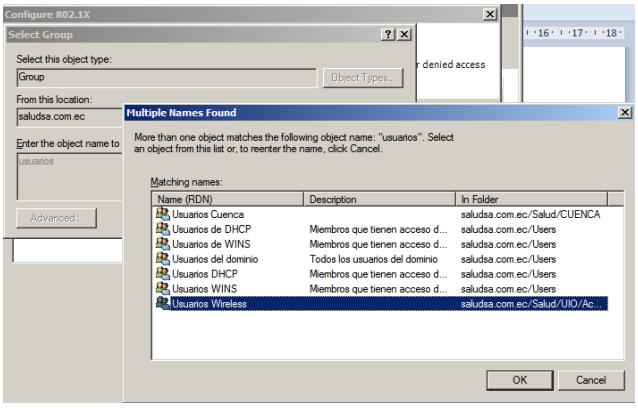


Figura 4.48: Especificación Usuarios Wireless
Creada por: Francisco Palacios.

En la siguiente ventana no se configurará nada, y solo se selecciona el botón "Next". Véase figura 4.49.

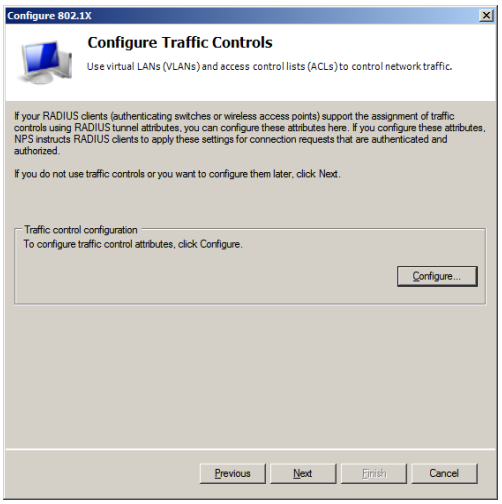


Figura 4.49: Configure Traffic Controls
Creada por: Francisco Palacios.

Por último se muestra una ventana de confirmación y luego se selecciona "Finish" véase la figura 4.50.

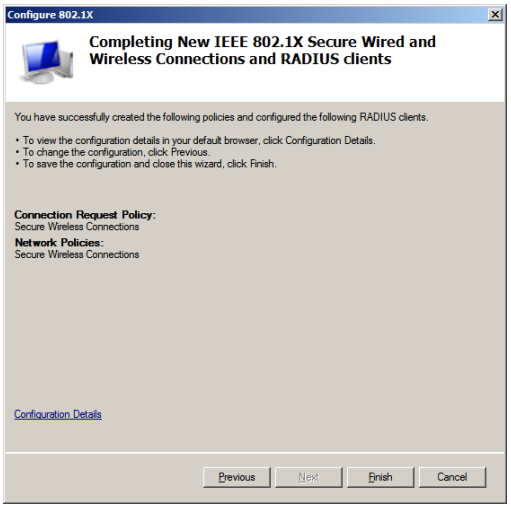


Figura 4.50: Confirmación de Configure 802.1X
Creada por: Francisco Palacios.

Configuración de Access Point AP-GERENCIA

Para esta etapa de la configuración y diseño de nuestra red inalámbrica de la corporación Adsamed se procederá a utilizar un AP Cisco modelo Aironet 1140, el cual es un equipo de última tecnología utilizado para conectar redes corporativas de manera inalámbrica, este equipo tiene una característica adicional dentro de la gama de tecnologías que posee este fabricante, una de ellas radica en que la configuración se la puede realizar mediante una interfaz web y no solamente vía comando como normalmente se la realiza.

Cabe mencionar que en esta parte del proyecto se citara siete puntos importantes de la configuración de uno de los AP, ya que básicamente la configuración del resto de AP que se encuentren en el edificio serán parecidos al AP que se mencionara aquí.

Configuración Previa del AP

Antes de comenzar a configurar el AP es necesario conectarlo en un punto de VLAN especifica, esto dependerá de los administradores de red de la empresa y la asignación de una IP que ellos proporcionen, cabe recalcar que esta asignación se la puede realizar de forma estática manualmente o de forma dinámica por medio del servidor DHCP. Esta VLAN debe ser una en la que no existan equipos para

poder verificar en el servidor DHCP cuantas están ocupadas y monitorear las mismas.

El puerto del conmutador en donde se conecte el AP debe ser del tipo "TRUNK", esto se lo realiza con la finalidad de permitir que todas las "VLAN" se propaguen en todos los conmutadores y no exista errores de configuración ni de conexión en la red inalámbrica.

Configuración Básica del AP

En la siguiente ventana en donde se muestra la figura 4.51 "EXPRESS SETUP" se procede a configurar el nombre del AP y la dirección IP que se colocara al dispositivo "10.X.X.X", existen otras opciones que se pueden configurar pero para efectos de este proyecto no será necesario realizarlas.

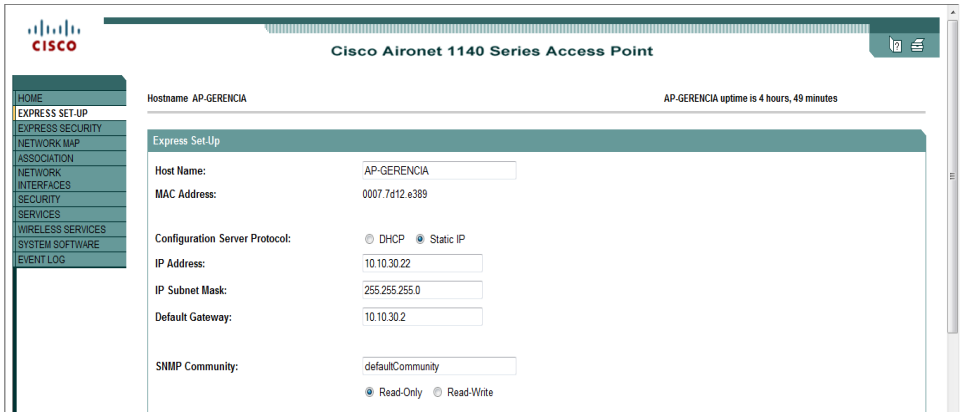


Figura 4.51: Express Setup Aironet 1140
Creada por: Francisco Palacios.

Creación de las "VLAN" para la red inalámbrica de Adsamed

En la pestaña "SERVICES" del menú que se encuentra del lado izquierdo se selecciona la opción "VLAN", en donde se pueden crear las "VLAN" que sean necesarias para esta conexión, en este caso se creó la VLAN XX para la red de "Invitados" y la VLAN XX para "Wireless Salud", véase figura 4.52.

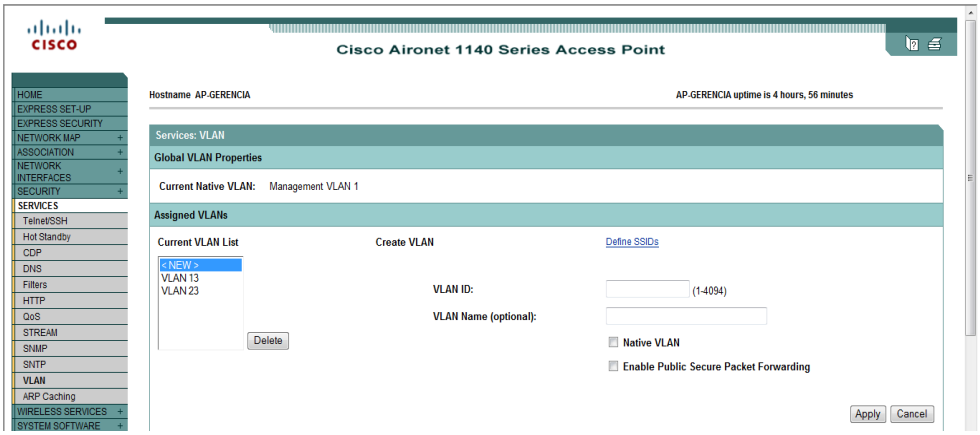


Figura 4.52: Creación de las VLAN de Adsamed
Creada por: Francisco Palacios.

Configuración Encriptación de VLAN.

En la figura 4.53 en la pestaña "SECURITY" se selecciona "Encryption Manager", en donde se escogerá el tipo de inscripción que se tendrán en las VLAN. En la VLAN XX se configura un cifrado TKIP.

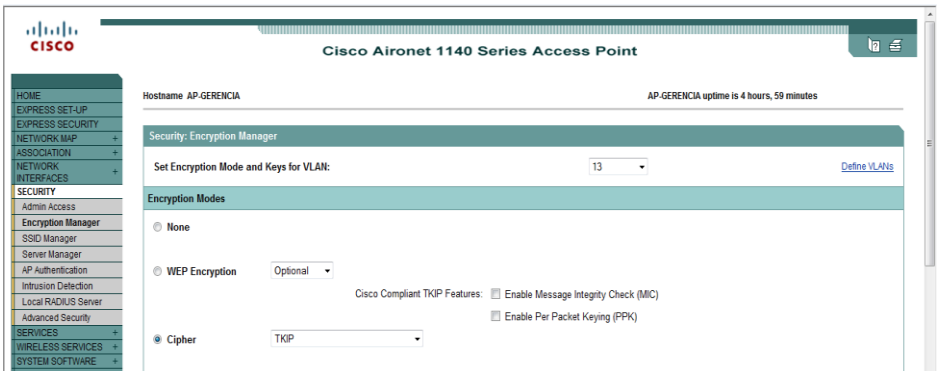


Figura 4.53 Encriptación de VLAN Adsamed
Creada por: Francisco Palacios.

Mientras que para la VLAN XX se configuro una inscripción WEP, la misma que debe ser "Mandatory" véase figura 4.54

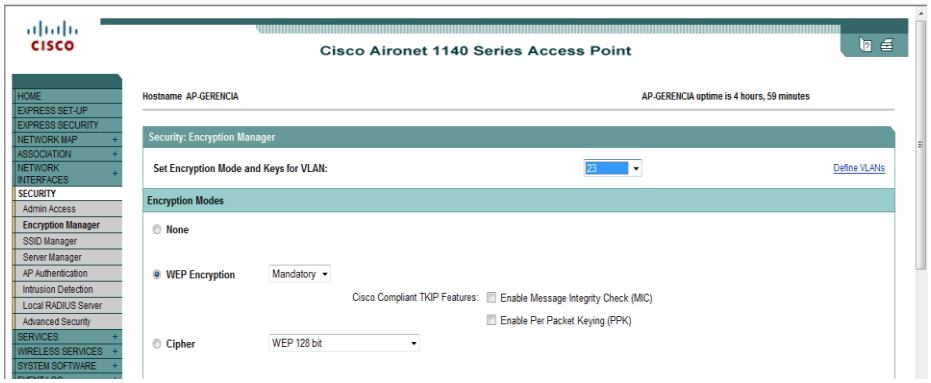


Figura 4.54: Inscripción Web de Tipo Mandatory
Creada por: Francisco Palacios.

Configuración Servidor RADIUS

En la pestaña "SECURITY" del mismo menú del AP se selecciona la opción "Server Manager", aquí se establece la dirección del servidor RADIUS (10.10.40.98), en esta etapa también hay que colocar una contraseña para continuar con la configuración y adicionalmente verificar que estén los puertos Autenticación y "Acounting" 1645 y 1646 respectivamente, luego se procede a presionar el botón "Apply". Véase figura 4.55

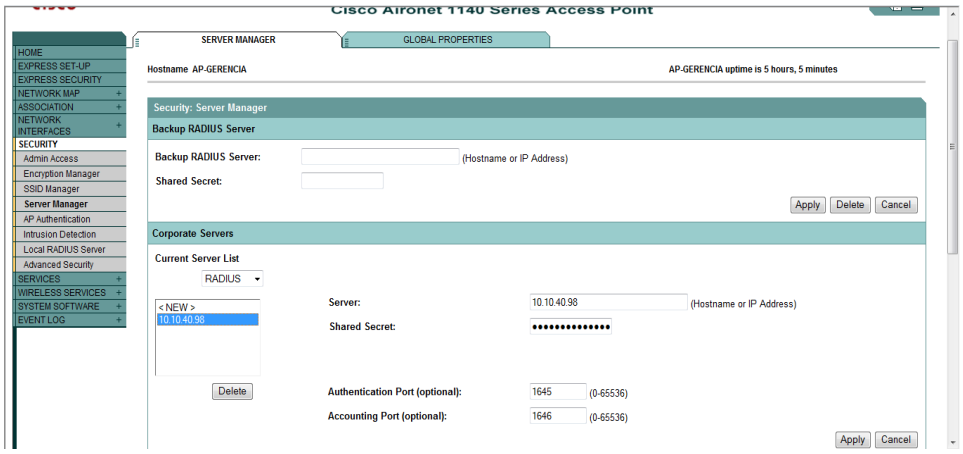


Figura 4.55: Configuración de server radius en AP
Creada por: Francisco Palacios.

En esta misma sección, hay que configurar el orden de prioridad de los servidores para los diferentes tipos de autenticación, en este caso únicamente "EAP

Authentication" en el que se encontrará el servidor RADIUS que se creó anteriormente (10.10.40.98) si existiera otro servidor se lo coloca en esta parte de igual manera según el orden de prioridad, véase la figura 4.56.

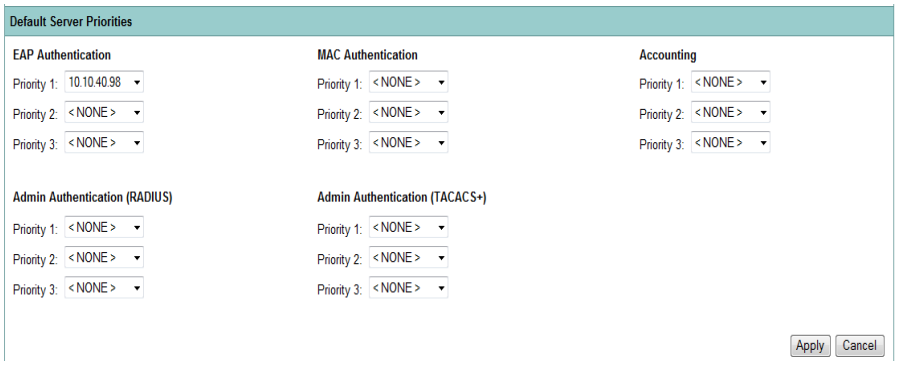


Figura 4.56: Orden de Prioridad de los servidores
Creada por: Francisco Palacios.

Creación SSID "Wireless Salud"

En la pestaña "SECURITY" tal como se muestra en la figura 4.57 se selecciona la opción "SSID Manager", aquí se procederá a crear el SSID "Wireless Salud" y se establecerá la VLAN (en este caso VLAN XX). También hay que asegurar que se encuentre seleccionada la interfaz Radio 0-802.11N$^{2.4GHz}$

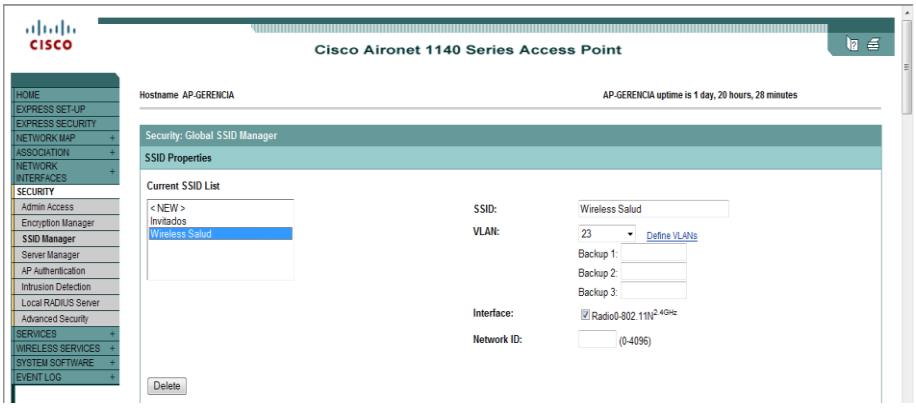


Figura 4.57: Creación del SSID "Wireless Salud"
Creada por: Francisco Palacios.

En esta misma sección hay que definir el método de autenticación que se va a tener para este SSID. Hay que asegurarse que se esté apuntando al Servidor Radius

10.10.40.98 tal como se observa en la figura 4.58

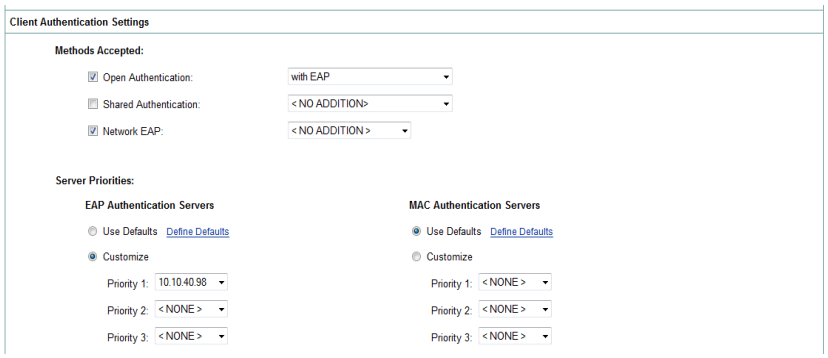


Figura 4.58: Método de Autenticación para el SSID
Creada por: Francisco Palacios.

En la sección "Multiple BSSID Beacon Settings" se habilita la opción "Set SSID as Guest Mode", tal como muestra la figura 4.59

Figura 4.59: "Multiple BSSID"
Creada por: Francisco Palacios.

Para finalizar todas las configuraciones es necesario presionar "Apply" para terminar con la creación de este SSID.

Creación SSID "Invitados" de Adsamed

Tal como se realizó la configuración del SSID "Wireless Salud" se debe crear el SSID "Invitados", pero este tendrá la VLAN XX. También hay que asegurar que se encuentre seleccionada la interfaz Radio0-802.11N$^{2.4GHz}$ Véase la figura 4.60

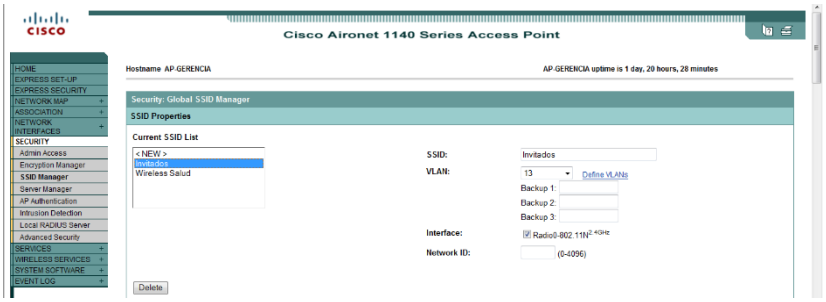


Figura 4.60: Creación SSID "Invitados" de Adsamed
Creada por: Francisco Palacios.

De la misma forma se debe asegurar que exista el método de autenticación donde únicamente se establecerá que sea "Open Authentication" sin ninguna opción adicional, tal como se muestra en la figura 4.61

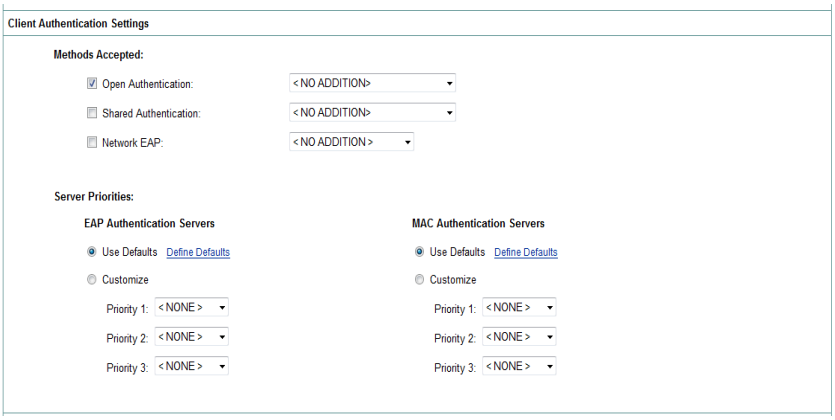


Figura 4.61: Método de Autenticación "Open Authentication"
Creada por: Francisco Palacios.

A continuación en la figura 4.62 se va establecer la contraseña que se va a utilizar para el acceso a este SSID.

Figura 4.62: Definición de Contraseña para el SSID Invitados
Creada por: Francisco Palacios.

En la sección "Multiple BSSID Beacon Settings" se habilita la opción "Set SSID as Guest Mode" véase la figura 4.63.

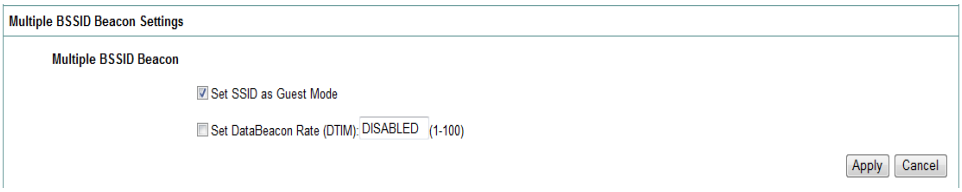


Figura 4.63: "Multiple BSSID Beacon Settings"
Creada por: Francisco Palacios.

Finalmente se presiona el botón "Apply" para terminar con la creación de este SSID.

Configuración de difusión de múltiples SSID.

En la pestaña "SECURITY → SSID Manager", se puede observar en la parte final las opciones de "Guest Mode/Infrastructure SSID Settings" tal como se muestra en la figura 4.64 en donde se procede a seleccionar la opción "Multiple BSSID" para que el "Access Point" difunda los SSID previamente creados.

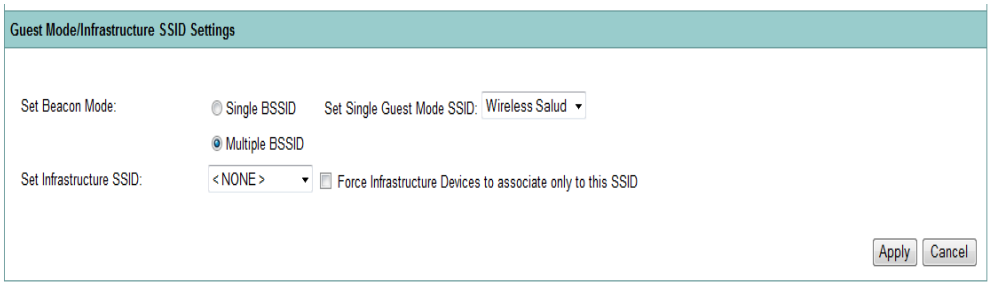


Figura 4.64: Difusión de Múltiples SSID
Creada por: Francisco Palacios.

Configuración y verificación del acceso a la red inalámbrica de ADSAMED

Resolución de problemas de acceso al cliente inalámbrico.

En ocasiones cuando se realiza algún cambio de configuración en el servidor Radius como por ejemplo la dirección IP es necesario bajar el servicio NPS y volverlo a iniciar véase el ejemplo en la figura 4.65. Cuando se configure un nuevo AP es necesario volver a crear la política para todos los AP.

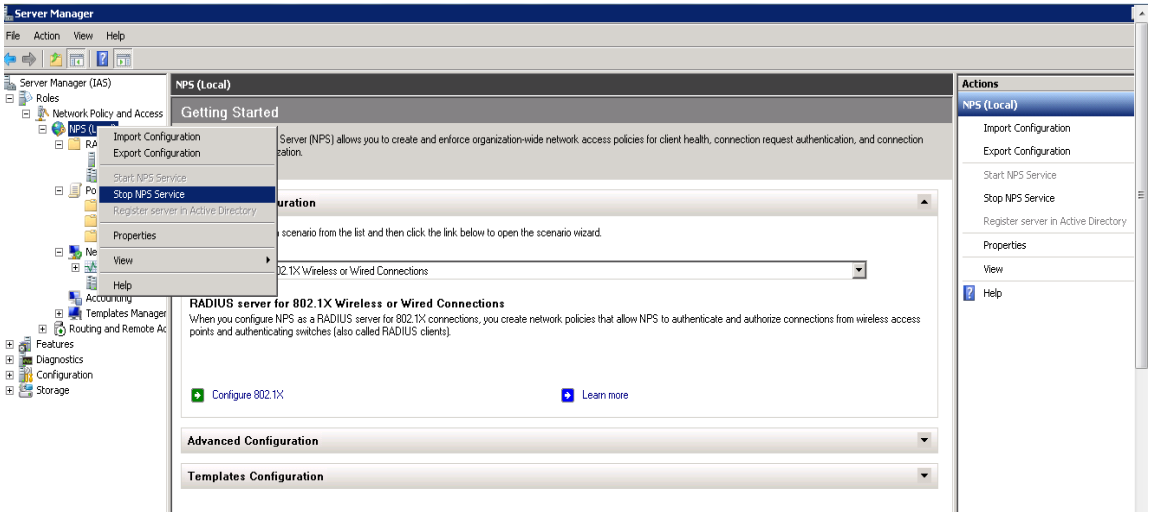


Figura 4.65: Bajar servicios de NPS
Creada por: Francisco Palacios.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Podemos concluir lo siguiente:

- Existen distintas posibilidades de implementar soluciones de redes inalámbricas conociendo e investigando sobre cada una de ellas las mismas que en gran medida serán utilizadas en infraestructuras de red pequeñas, medianas o grandes.

- Se analizaron las distintas tecnologías que existen en el mercado pero se propuso la utilización de un fabricante en especial por considerar la topología actual de la empresa, por cuanto los equipos propuestos para este proyecto son de fabricación de la empresa CISCO, pero dependiendo de la magnitud y alcance que le den los administradores, gerentes y demás directivos pueden variar o no la elección del fabricante de los dispositivos

- El proyecto es realizable en un tiempo determinado y si bien es cierto que el costo total del proyecto inalámbrico para la corporación Adsamed en todas sus etapas puede ser más elevado que una red cableada, la recuperación de la inversión a corto, mediano y largo plazo será más importante después de apreciar la utilidad y beneficios institucionales que nos provee la implementación de esta nueva arquitectura de red para la conexión de nuestros usuarios autenticados y no autenticados.

Conclusión Final: Se cumplieron todos los objetivos inicialmente planificado, es importante mencionar que la inversión varia en el tiempo dependiendo de la magnitud y los alcances que los directivos y gerentes le quieran dar al proyecto ya que en la actualidad este proyecto está siendo implementado en una de las oficinas principales pero sería extraordinario implementarlo en el resto de agencias y sucursales a nivel de todo el país, ya que redundaran en beneficio para los empleados y demás clientes con que cuente la Corporación Adsamed.

Recomendaciones

En la implementación del proyecto se recomienda utilizar dispositivos de fabricación de la empresa CISCO debido a su robustez, calidad y operatividad que se ha presentado en las pruebas que se realizaron y sobre todo para mantener el estándar con que actualmente cuenta la empresa Adsamed, se recoge que todos sus dispositivos de conexión tanto como conmutadores, enrutadores son de este fabricante por lo que utilizar otro fabricante para la implementación de este proyecto de redes WLAN puede ser muy tedioso, sobre todo en la compatibilidad en la ejecución de ciertas configuraciones y controles que varían entre un fabricante y otro.

Por todo lo antes dicho es recomendable implementar esta solución tomando en cuenta los múltiples beneficios que se tendrán en un futuro gracias a esta nueva arquitectura de red inalámbrica.

REFERENCIAS BIBLIOGRÀFICAS

[1] http://www.maestrosdelweb.com/principiantes/evolucion-de-las-redes-inalambricas/
Fecha de consulta: agosto de 2010

[2] http://cecy150.tripod.com/pag2.html
Fecha de consulta: agosto de 2010

[3] http://redesinl.galeon.com/aficiones1342927.html
Fecha de consulta: agosto de 2010

[4] http://www.manual-wifi.com/tipos-de-redes-inalambricas/
Fecha de consulta: agosto de 2010

[5] http://www.maestrosdelweb.com/editorial/redeswlan/
Fecha de consulta: septiembre de 2010

[6] http://www.cgmenor.com/pdf/redesinalambricas.pdf
Fecha de consulta: septiembre de 2010

[7] http://www.monografias.com/trabajos/redesinalam/redesinalam.shtml
Fecha de consulta: septiembre de 2010

[8] http://www.alegsa.com.ar/Dic/ipsec.php
Fecha de consulta: septiembre de 2010

[9] http://www.crice.org/ Comunidad de Redes Inalámbricas Cuenca-Ecuador
Fecha de consulta: septiembre de 2010

[10] http://www.softonic.com/windows/redes-inalambricas-wifi
Fecha de consulta: marzo de 2011

[11] http://www.redsinfronteras.org/pdf/redes_wireless.pdf
Fecha de consulta: marzo de 2011

[12] http://www.superinventos.com/wifi.htm
Fecha de consulta: marzo de 2011

[13] http://es.kioskea.net/contents/wireless/wlintro.php3
Fecha de consulta: marzo de 2011

[14] http://www.wi-fi.org/knowledge_center_overview.php
Fecha de consulta: marzo de 2011

[15] http://technet.microsoft.com/es-ar/library/dd578360.aspx
Fecha de consulta: agosto de 2011

[16] http://multingles.net/docs/alezito/alezito_inalamb.htm
Fecha de consulta: agosto de 2011

[17] http://pdf.rincondelvago.com/redes-inalambricas_1.html
Fecha de consulta: abril de 2011

[18] http://lat.3com.com/lat/technology/technnical.papers/wireless_qa.
Fecha de consulta: abril de 2011

[19] http://www.wirelessethernet.com
Fecha de consulta: abril de 2011

[20] http://www.monografias.com/trabajos12/reina/reina.shtml
Fecha de consulta: mayo de 2011

[21] http://www.microsoft.com/spain/technet/recursos/articulos/wifisoho.mspx
Fecha de consulta: mayo de 2011

[22] http://mundopc.net/redes-inalambricas/
Fecha de consulta: junio de 2011

[23] http://www.uam.es/ss/Satellite/es/1234886352083/1234886530667/
servicioti/ServicioTI/Red_Inalambrica_de_la_UAM.htm
Fecha de consulta: junio de 2011

[24] **Stephen Grossberg.** "Teoría de Resonancia Adaptada". Disponible
http://inf.udec.cl/~yfarran/web-redes/ind-redes.htm
Fecha de consulta: julio de 2011

[25] http://www.airtightnetworks.com/home/products/spectraguard-
planner.html Fecha de consulta: agosto de 2011

[26] http://www.airmagnet.com/products/planner/ Fecha de consulta: agosto de 2011

[27] http://www.trapezenetworks.com/products/ringmaster_software/ Fecha de consulta: agosto de 2011

[28] http://www.connect802.com/suite_spot.htm Fecha de consulta: agosto de 2011

[29] http://www.tobesecurity.com Fecha de consulta: agosto de 2011

[30] Academia de Networking de CISCO SYSTEM, Fundamentos de Redes

Inalámbricas 1era edición.

Lugar y Fecha de publicación: Madrid – España en el 2006.

Editorial: PERSON EDUCACIÓN S.A.

Equipo Editorial: David Fayerman, Técnico Editorial: Ana Isabel García

Traducción: José Manuel Díaz

[31] Windows y Macintosh, Introducción a las redes inalámbricas 802.11a, 802.11b, Airport y Airport Extreme de Apple.

Por: Adam Engst and Glenn Fleishman.

Lugar y Fecha de publicación: Madrid – España en el 2003

Editorial: Ediciones Alaya Multimedia.

Equipo Editorial: Víctor Manuel Ruiz Calderón y Susana Krahe Pérez – Rubín.

Traducción: Daniel García

[32] Redes y Servicios de Banda Ancha, 1era edición

Por: José Manuel Huidobro, Ingeniero de Telecomunicación Universidad Politécnica de Madrid (UPM).

David Roldán, Ingeniero de Telecomunicación Universidad Politécnica de Valencia (UPV)

Lugar y Fecha de publicación: Madrid – España en el 2004

Editorial: Mc Graw – Hill Profesional Interamericana de España S. A. U.

Equipo Editorial: Antonio García Brage.

Pagina Web: http://www.mcgraw-hill.es / profesional@mcgraw-hill.es

GLOSARIO DE TÉRMINOS

SMTP	Simple Mail Transfer Protocol
ADSAMED	Administradora de Salud de Medicina Prepagada
ADSL	Asymmetric Digital Subscriber Line
Bluetooth	Especificación industrial para Redes Inalámbricas de Área Personal
BSA	Área de servicios básicos
BSS	Conjunto de Servicios Básicos
BSSID	Dirección MAC del punto de Acceso
CDMA	Código de división de múltiple acceso
DECT	Digital Enhanced Cordless Telecommunication
EAP	Protocolo de autenticación extensible
EHF	Extremely-high frequency
ESA	Área de servicio extendida
ESS	Conjunto de servicios extendidos
HTTP	HyperText Transfer Protocol
IBM	Internacional Bussines Machines
IBSS	Conjunto de Servicios Básicos Independientes
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IMAP	Internet Message Access Protocol
ISM	Industrial, Scientific and Medical
LAN	Local Area Network
MAN	Metropolitan Area Network
OFDM	Orthogonal Frequency Division Multiplexing
PC	Personal Computer
PDA	Personal Digital Assistants
PING	Utilidad diagnóstica en redes
POP	Post Office Protocol
SHF	Super-high frequency
STREAMS	Stream Control Transmission Protocol
TCP/IP	Protocolo de control de transmisión/Protocolo de Internet
UDP	User Datagram Protocol
UHF	Ultra-high frequency
WEP	Wired Equivalent Privacy

Wi-Fi	Fidelidad inalámbrica
Wimax	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Nerwork
WPAN	Wireless Personal Área Networks
GUNN	Diodo usado en la electrónica de alta frecuencia
IMPATT	Tiempo de transito por avalancha y ionización por choque

DATOS DE LOS AUTORES

ING. FRANCISCO PALACIOS ORTIZ. (AUTOR)

Francisco Gerardo Palacios Ortiz, Ingeniero en Sistemas Computacionales graduado en la Universidad de Guayaquil, con estudios de Postgrado obteniendo el título de Magister en Telecomunicaciones realizado en la Universidad Católica Santiago de Guayaquil; Diplomado en Pedagogía Superior realizado en la Universidad Técnica Particular de Loja, Docente Universitario con experiencia de más de 11 años, los cuales ejerció en las Universidad Ecotec Facultad de Redes y Telecomunicaciones, Universidad de Guayaquil Facultad de Ciencias Matemáticas y Físicas, Carrera de Ingeniería en Sistemas Computacionales e Ingeniería en Networking y Telecomunicaciones(actual). Especialista en: Redes, Telecomunicaciones, Seguridad Informática, Infraestructura de Servidores, Data Center, Cloud Computing, con experiencia de más de 12 años en las áreas de Tecnología tanto en la empresa Privada como en la Publica.

ING. DIANA JOSELYN ESPINOZA VILLÓN (AUTOR)

Diana Joselyn Espinoza Villón, Ingeniera en Sistemas Computacionales graduada en la Universidad de Guayaquil, Estudiante del Máster Universitario Análisis y Visualización de Datos Masivos(Big Data) en la Universidad de la Rioja. Docente Universitaria con 3 años de experiencia ejerciendo en el Tecnológico Euroamericano y Universidad de Guayaquil Facultad de Jurisprudencia y Ciencias Sociales; Carrera de Derecho, Sociología y Nivelación (actual). Cursos realizados en informática forense; academia de Cisco-Espol y metodología de la investigación; Universidad de Guayaquil. Conocimientos en Mongodb, Minería de Datos (weka), Encase.

ING. FAUSTO RAÚL OROZCO LARA. (AUTOR)

Fausto Raúl Orozco Lara, Ingeniero en Sistemas Computacionales graduado en la Universidad de Guayaquil, con estudios de Postgrado obteniendo el título de Magister en Telecomunicaciones realizado en la Universidad Católica Santiago de Guayaquil; Docente Universitario con experiencia de 11 años los cuales ejerció en: Universidad Estatal Península Santa Elena extensión Playas, Carrera de Ingeniería en Sistemas, Escuela de Marina Mercante Nacional y Universidad de Guayaquil, Facultad de Ciencias Matemáticas y Físicas, Carrera de Ingeniería en Sistemas Computacionales e Ingeniería en Networking y Telecomunicaciones(actual). Especialista en Servidores de plataforma Unix, Virtualizacion, Redes y Telecomunicaciones. Diplomado de Seguridad Informática Ofensiva.