



Benemérita Universidad Autónoma de Puebla

Facultad de Ciencias de la Computación

“RED INALÁMBRICA MIXTA 10/100 Mb”

PRESENTA:

MIRIAM MÓNICA DUARTE VILLASEÑOR

TESIS PROFESIONAL SOMETIDA COMO REQUISITO
PARCIAL PARA OBTENER EL GRADO DE:

LICENCIADO EN CIENCIAS DE LA COMPUTACIÓN

ASESOR:

DRA: BARBARA EMMA SANCHEZ RINZA

PUEBLA, PUE

Primavera 2009

RED INALAMBRICA MIXTA 10/100 Mbps

Miriam Mónica Duarte Villaseñor

SUMARIO

En esta tesis se muestran los avances tecnológicos en redes inalámbricas, protocolos y estándares actualmente inscritos en IEEE, mejoras en la administración y gestión del manejo en redes inalámbricas que se enfoca en el interés de implementar una red inalámbrica eficiente.

En la Secretaría de Desarrollo Social (SDS) de la ciudad de Puebla se requiere de la administración de su red inalámbrica, las especificaciones son:

- Separar la red interna de una red para invitados.
- Reubicar las antenas que proporcionan el servicio inalámbrico para una optima cobertura.
- Implementar seguridad en la red inalámbrica, crear contraseñas WPA.
- Facilitar el acceso de Internet con un ancho de banda de 10 Mbps para usuarios invitados, y 100 Mbps para usuarios privilegiados, (gente que labora en la dependencia).
- Asignación mediante DHCP (asignamiento automático de direcciones IP).

En resumen, se realizó la reingeniería de la red inalámbrica para reubicar las antenas con una mejor cobertura, se reasignaron algunas direcciones IP y se obtuvo satisfactoriamente la pila de direcciones para implementar DHCP, se separó la red de invitados y la red privilegiada, se implementó seguridad WPA2. No se realizó la separación del ancho de banda por falta de recursos pero se pudo realizar una distribución con el número de paquetes que recibe la red de invitados para cubrir con las especificaciones, y en cualquier momento esta puede ser modificada para recibir más o menos paquetes, esto es de mayor o menor rapidez.

Dedicatorias

A la memoria de mi Abue Eva María Teresa Victoria

que me supo inspirar y guiar.

A mi mama MAGDALENA por todas sus enseñanzas,

educación, y apoyo que siempre me acompaña.

A mi tío BETO por el apoyo y el cariño

que toda la vida me da.

AGRADECIMIENTOS

Mi sincero agradecimiento a la Doctora Barbará Sánchez Rinza por todo el apoyo brindado durante el desarrollo de esta tesis; gracias por sus consejos y sobre todo por la paciencia que me tuvo.

A mi familia y amigos por su apoyo moral en la culminación de esta tesis y por estar conmigo.

Este trabajo fue financiado por un programa de la VIEP llamado “Jóvenes Investigadores IV”.

CONTENIDO

	Pagina
Sumario	i
Dedicatorias	ii
Agradecimientos	iii
Contenido	iv
<u>Capítulo 1 Redes Mixtas</u>	<u>1</u>
1.1 Introducción	1
1.2 Fundamentos de Redes	3
1.3 Tipos de Redes	3
1.3.1 Lan inalámbricas	6
1.4 Establecimiento de las Prioridades	6
1.4.1 Topologías de Red inalámbrica	8
1.5 Los Parámetros de Tcp/Ip A Configurar	11
1.5.1 Direcciones IP	11
1.6 El Accesos de Banda Ancha	11
1.6.1 Las ventajas de la banda ancha	12
1.7 La conexión de Wi-Fi con Internet	13
1.8 Medio físico dinámico	14
1.9 Estándares 802	16
1.10 Modelo OSI	20
<u>Capítulo 2 Análisis y Diseño</u>	<u>24</u>
2.1 Selección de velocidad y degrado	24

2.2 Procesamiento de tramas y creación de puentes	25
2.2.1 Del medio inalámbrico al medio con cables	25
2.2.2 Del medio con cables al medio inalámbrico	27
2.3 Acceso múltiple por división de código CDMA	29
2.4 Ubicación de los puntos de acceso	31
2.5 Puntos de acceso virtuales	33
2.6 Conmutación Wi-Fi	36
2.7 Radios definidos por el software	36
2.8 Seguridad	37
2.8.1 Cifrado	38
2.8.2 Autenticación	39
2.8.3 Extensiones del estándar	40
2.8.4 Ventajas del sistema 802.11/EAP	43
2.9 Cambio en el ancho de banda	47
 <u>Capítulo 3 Implementación</u>	 <u>50</u>
3.1 Requerimientos previos	50
3.2 Interfaz de línea de comandos CLI	54
3.3 Recuperación de la interfaz WMI	56
3.4 Creación de SSID invitado	62
3.5 Configuración de la red inalámbrica para invitados	69
 <u>Capítulo 4 Pruebas</u>	 <u>75</u>
4.1 Especificaciones	75
4.2 Separación de la red interna con la red para invitados	75
4.2.1 Las VPN	75
4.2.2 Justificación de las VLAN	76

4.3 DHCP	77
4.4 Seguridad de la red para invitados	78
4.5 Privilegios del ancho de banda	79
4.6. Acceso a la red de invitados	81
Capítulo 5 Conclusiones	84
Bibliografía	86

Capítulo 1

REDES MIXTAS

1.1 Introducción.

La Secretaria de Desarrollo Social ubicada en la 20 Norte 2036 solicita que sea implementada una red inalámbrica que pueda brindar el servicio de internet a los licenciados, secretarias, y demás personal que soliciten el servicio, para ello requieren una mejor distribución del servicio ya que trabajan a una velocidad de 100 Mbps.

Esta secretaria cuenta con equipo Xirrus así como computadoras fijas con tarjetas de red inalámbrica, también cuentan con equipos portátiles como Notebooks y palm.

El servicio de internet con que cuentan lo da la compañía Avantel, mediante un enlace directo a finanzas se restringen ciertas páginas y aplicaciones como el Messenger, youtube, descargas de archivos, con el fin de que no obstruyan el tráfico en el ancho de banda.

La Unidad de Desarrollo Administrativo e Informática (UDAI) es quien se encarga de instalar, y dar mantenimiento al hardware y software de la Secretaria de Desarrollo Social. En Abril de 2008 la secretaria cambia de instalaciones y debido a la conservación de edificios históricos no fue posible hacer perforaciones para facilitar la conexión de la red alámbrica, por esta razón deciden comprar antenas inalámbricas.

La empresa Telsanet que es quien instalo la red en tal secretaria, y les vende unas antenas inalámbricas de la compañía Xirrus, el inconveniente fue que no poseen la información ni cuentan con el personal apropiado para realizar una configuración que le convenga al departamento, es por eso que necesitaron comprar 3 antenas Wi-fi Array XS4- 3500 y la instalación fue la siguiente:

Una antena ubicada dentro de una oficina que cubre alrededor de 20 computadoras. Otra antena fue instalada en el interior de un edificio que cubre aproximadamente 30 computadoras, pero el inconveniente que tuvo esta es que debido al acceso del edificio no

alcanzo a cubrir todas las oficinas y una antena mas se coloco dentro de una oficina cubriendo solo 3 computadoras.

El equipo Xirrus Wi-fi Array XS4-3500 cuenta con dos interfaces para su manejo, una es mediante una página web, para acceder a esta es necesario que el equipo tenga asignada una dirección IP, y la otra es en modo consola para accesar es necesario un cable que del lado de la antena sea RJ45 y del otro lado sea por el puerto serial, la interfaz es con el programa HyperTerminal. En la figura 1.1.1 se muestra la antena Xirrus.



Figura 1.1.1 Xirrus Wi-Fi Array 3500.

Una Red Mixta consiste en una combinación de redes ya sea por alcance, por método de la conexión, por relación funcional o por topología de red, en este caso se trata del tamaño del ancho de banda en un medio no guiado que es la red inalámbrica.

La red inalámbrica trabaja con un ancho de banda de 100 Mbps, y requieren que se dé el servicio a cualquier persona ajena a los trabajadores fijos, estos invitados pueden ser: presidentes municipales o visitantes de otras delegaciones, que traen sus computadoras portátiles y necesiten el servicio de internet, para todos ellos se les quiere otorgar un ancho de banda de 10 Mbps. Y que no puedan ver la red interna para garantizar la seguridad.

1.2 Fundamentos De Redes

Una red de computadoras es un conjunto de equipos conectados por medio de cables, señales, ondas o cualquier otro método de transmisión de datos, que comparten información, recursos y servicios.

Para comunicarse entre sí en una red el sistema de red utiliza protocolos de red. De acuerdo a su extensión las redes pueden ser:

- Área de red local (LAN)
- Área de red metropolitana (MAN)
- Área de red amplia (WAN)
- Área de red personal (PAN) [1]

1.3 Tipos De Redes

Cada computadora o usuario de una red se denomina nodo y la interconexión entre los nodos se llama enlace de comunicaciones. En la mayoría de las redes de computadoras, cada nodo es una computadora personal, pero en algunos casos un dispositivo periférico como una impresora láser puede ser un nodo. Hay tres tipos básicos de redes electrónicas de uso común: LAN, redes de área amplia (WAN, wide-area network) y redes de área metropolitana (MAN, metropolitan-area network).

Redes de área local (LAN). Consiste principalmente en computadoras personales interconectadas dentro de una oficina o edificio. Las LAN pueden tener un mínimo de 3 a 5 usuarios; sin embargo, la mayoría de los sistemas conectan de 10 a 1 000 usuarios.

Una compañía puede usar una LAN pequeña para interconectar varias oficinas en un mismo edificio, caso en que el cableado puede correr entre diferentes pisos del edificio para hacer las conexiones. Las LAN muy grandes pueden interconectarse varios edificios dentro de un complejo.

Algunas LAN enlazan computadoras principales o minicomputadoras a terminales compuestas de un teclado y monitor de video que les permite comunicarse con la computadora. Las terminales por sí mismas, no son PC, sino simples dispositivos de entrada y salida. La generalidad de las minicomputadoras grandes o principales puede

manejar múltiples usuarios con muchas terminales. En resumen, las PC pueden habilitarse para emular una terminal. Con tarjetas de interface interconstruidas o tableros emuladores, más un software especializado, una PC se puede usar como terminal LAN estándar, además de trabajar como computadora.

Otras LAN consisten en múltiples PC enlazadas entre sí y a una minicomputadora o computadora, y continuar operando en forma independiente.

- a) Topologías LAN. La topología de una red describe las trayectorias básicas de comunicaciones y los métodos para conectar los nodos en una red. Las tres topologías más comunes utilizadas en LAN son estrella, anillo y bus. De éstas, las configuraciones bus y anillo son las más comunes. La red Ethernet emplea una topología bus y la popular red Token-Ring usa topología en anillo. La figura 1.3.1 muestra las diferentes topologías.

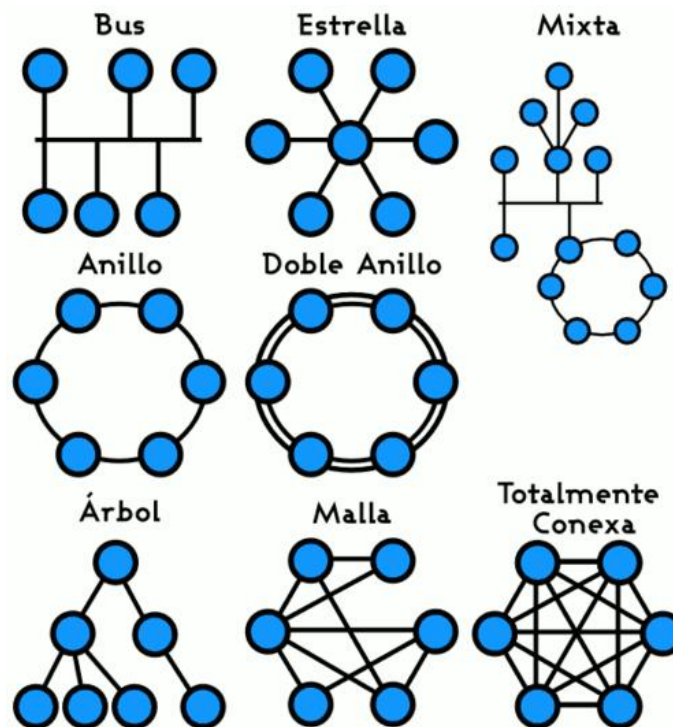


Figura 1.3.1 Diferentes tipos de topologías LAN.

- b) LAN inalámbricas. Una de las partes más complicadas y costosas de cualquier LAN es el cableado. Los cables, así como su instalación y mantenimiento, son caros, en especial si la LAN tiene que instalarse en un edificio ya existente. Además, en

organizaciones grandes y crecientes, la LAN requiere cambios con regularidad. Deben añadirse nuevos usuarios y la red debe reconfigurarse durante la expansión, reorganizaciones y cambios. Para evitar el costo y dolor de cabeza de tender y mantener el cableado de la LAN se pueden usar LAN inalámbricas. Que se comunican a través de técnicas de radio e infrarrojo. Cada PC en una LAN inalámbrica debe tener un módem inalámbrico o transceptor. Este dispositivo puede ser una NIC que se conecta en la computadora o un dispositivo externo que se comunica a través de los puertos I/O estándar en una computadora. En cualquier caso, el transceptor módem convierte a los datos binarios seriales de la computadora en señales infrarrojas o de radio para su transmisión, y transforma las señales infrarrojas o de radio otra vez en datos binarios. Las LAN inalámbricas operan como LAN conectadas por cable, para que cualquier nodo pueda comunicarse con cualquier otro nodo. Tienen limitaciones significativas en cuanto a velocidad; hoy día, la mayoría de las LAN inalámbricas tienen una velocidad tope de 10 Mbps. Sin embargo, esto es suficiente para muchas aplicaciones, entre ellas el correo electrónico, compartimiento de medios de impresión e intercambio de archivos y bases de datos.

- c) RADIO. Las LAN inalámbricas por radio son muchos más versátiles que las LAN inalámbricas infrarrojas. Debido a que las ondas de radio pueden atravesar las paredes y los pisos de edificios, hay mayor flexibilidad en la colocación e interconexión de varias computadoras. Las LAN inalámbricas utilizan transmisores y receptores de microondas para comunicarse. Como se usan frecuencias altas, las antenas son pequeñas y prácticamente pasan inadvertidas. La mayoría de las nuevas LAN inalámbricas operan en bandas de frecuencia de microondas especiales que se han puesto a un lado por la FCC, en particular para las LAN, y no requieren licencia especial para operar. Sin embargo, la potencia de salida de los transceptores está limitada con precisión para prevenir comunicaciones a larga distancia. No obstante que pueden mantenerse comunicaciones inalámbricas dentro de grandes edificios, no son posibles distancias mayores a algunos cientos

de pies. Las señales de microondas reciben una atenuación significativa cuando intentan atravesar paredes o pisos, en particular en estructuras grandes que usan concretos reforzados con acero.

Un transceptor de LAN por radio tiene un módem que convierte los datos binarios de la computadora en señales que modulan a la portadora de microondas. Se usan técnicas de espectro esparcido en la generalidad de los transceptores inalámbricos. Los sistemas de espectro esparcido transfieren los datos digitales a señales que modulan a la portadora de manera que la señal transmitida ocupa una banda entera de frecuencias en vez de un canal de una sola frecuencia. Con estos métodos, la transmisión es segura y permiten a docenas o a cientos de usuarios transmitir en una misma banda al mismo tiempo.

- d) LAN Ethernet. En 1980, Xerox se unió con Digital Equipment Corporation y con Intel para patrocinar un estándar conjunto para Ethernet. La colaboración produjo una definición que se transformó en un estándar conjunto para Ethernet. La colaboración produjo una definición que se transformó en la base para el estándar de IEEE 802.3 (El instituto de ingenieros electricistas y electrónicos establece y mantiene una amplia gama de estándares en los campos eléctrico, electrónico y de computación. La serie 802.X se relaciona con LAN.)[2]

1.3.1 LAN inalámbricas

Las redes inalámbricas tienen un medio de red abierto. Por definición, el medio de red en la red inalámbrica no es una ruta bien definida compuesta por un cable físico, sino un enlace de radio con una codificación y modulación determinadas.

1.4 Establecimiento De Las Prioridades

Una de las diferencias claves entre los estándares 802.3 y 802.12 es también una de las ventajas fundamentales de este último: su capacidad de reconocer dos niveles de prioridad en las solicitudes de transmisión. El protocolo de 100VG-AnyLAN 802.12 reconoce solicitudes de prioridad normal y de prioridad alta. El nivel de prioridad lo puede establecer la estación de trabajo o la aplicación. Si una solicitud de prioridad normal está pendiente durante más de 300 ms, se traslada a la cola de servicio de prioridad alta.

El DPA hace algo más que permitir que se establezca la prioridad de transmisión. También mejora el rendimiento eliminando los datos no útiles de la red asociada con el método de acceso CSMA/CD. En CSMA/CD, todas las estaciones de trabajo luchan por el acceso al canal. Las colisiones, que son bastante frecuentes, requieren su detección y la retransmisión del paquete. Además el esquema DPA tiene una ventaja de rendimiento sobre CSMA/CD: a medida que las colisiones se hacen más frecuentes al aumentar el tráfico en las redes con CSMA/CD, las retransmisiones de paquetes resultantes disminuyen el rendimiento. La red con DPA, que no tiene contenida para la transmisión y que por ello no hay colisiones de paquete, es capaz de manejar más tráfico 100VG-AnyLAN también tiene algo de ventaja en cuanto a seguridad frente al estándar 802.3. El concentrador de 100 VG-AnyLAN sólo transmite paquetes a través de puertos conectados a la dirección de destino del paquete. Esto reduce la posibilidad de una supervisión no autorizada de las transmisiones. En la figura 1.4.1 se muestra el algoritmo CSMA/CD. [3]

Algoritmo CSMA/CD

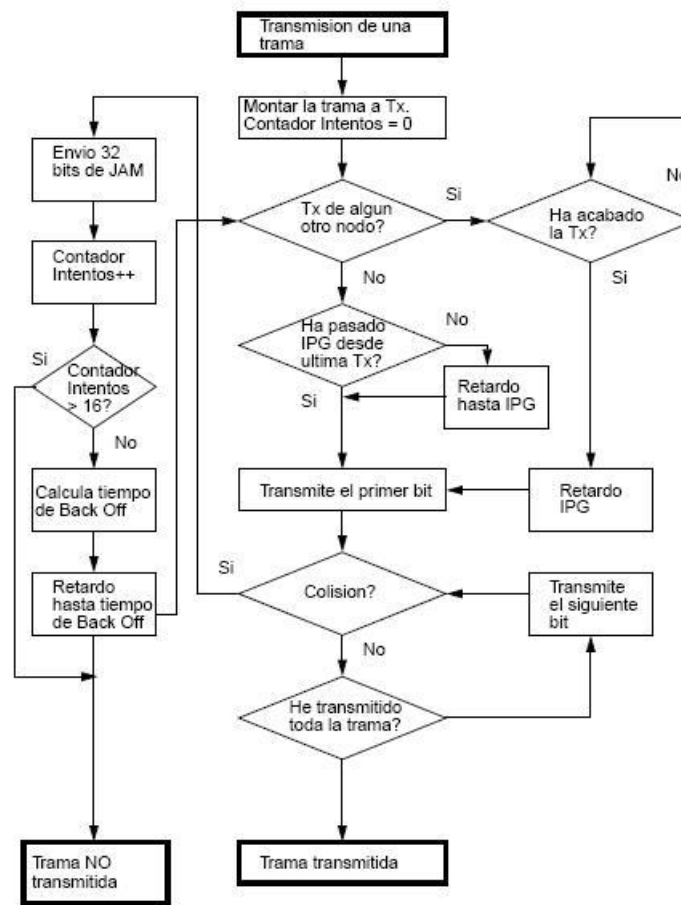


Figura 1.4.1 Algoritmo CSMA/CD.

Mientras se transmite un paquete, se puede recibir señal, entonces se puede detectar que ha habido colisiones antes de que se termine de transmitir la trama.

1.4.1 Topologías de Red inalámbrica

- **Modo ad hoc o IBSS.** Es una configuración en la cual sólo se necesita disponer de tarjetas o dispositivos inalámbricos Wi-Fi en cada ordenador. Los ordenadores se comunican unos con otros directamente, sin necesidad de que existan puntos de acceso intermedios. En la figura 1.4.1.1 se muestra esta topología.

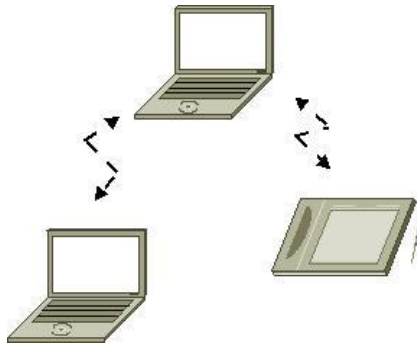


Figura 1.4.1.1 Topología Ad hoc o IBSS.

- **Modo infraestructura o BSS.** En esta configuración, además de las tarjetas Wi-Fi en los ordenadores, se necesita disponer de un equipo conocido como punto de acceso. El punto de acceso lleva a cabo una coordinación centralizada de la comunicación entre los distintos terminales de la red. Las estaciones en un IBSS se comunican directamente entre sí y, por tanto, deben encontrarse dentro del alcance directo de la comunicación. En la 1.4.1.2 se encuentra un BSS de infraestructura; estas redes se distinguen porque utilizan un punto de acceso se utilizan para todas las comunicaciones y las redes de infraestructura, incluyendo la comunicación entre nodos móviles en la misma área de servicio. Si una estación móvil en un BSS de infraestructura necesita comunicarse con una segunda estación móvil, la comunicación debe tener dos saltos. Primero, la estación de origen transfiere la trama al punto de acceso. Segundo, el punto de acceso transfiere la trama a la estación de destino. Esto tiene dos ventajas principales:
 - Un BSS se define por la distancia a la que se encuentra desde el punto de acceso. Todas las estaciones móviles necesitan estar dentro del alcance del punto de acceso, pero no existe ninguna restricción en cuanto a la distancia entre las propias estaciones móviles. Permitir una comunicación directa entre estaciones móviles puede ahorrar potencia de transmisión pero a costa de incrementar la complejidad de la capa física debido a que las estaciones móviles pueden necesitar mantener relaciones de vecindad con el resto de estaciones móviles dentro del área de servicio.

- Los puntos de acceso en redes de infraestructura se encuentran en situación de asistir a las estaciones que intentan ahorrar potencia. Los puntos de acceso pueden advertir cuándo entra una estación en un modo de ahorro de potencia y copiar en el búfer las tramas. Las estaciones que funcionan con baterías pueden desactivar el transceptor y activar sólo para transferir y recuperar las tramas en el búfer desde el punto de acceso.

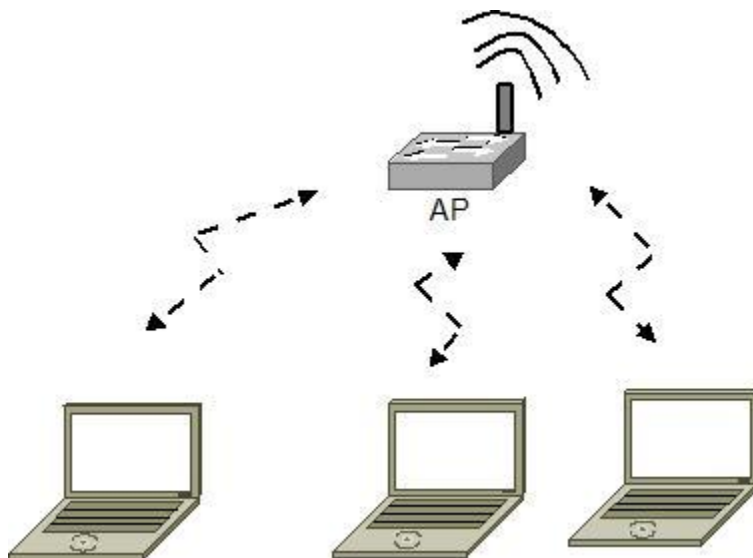


Figura1.4.1.2 Topología BSS.

- **Modo ESS.** Esta configuración permite unir distintos puntos de acceso para crear una red inalámbrica con una amplia cobertura. Una red ESS está formada por múltiples redes BSS. Las distintas redes BSS se pueden poner pegadas unas a otras para conseguir tener una continuidad de servicio en toda la red ESS. En la figura 1.4.1.3 se muestra esta topología.

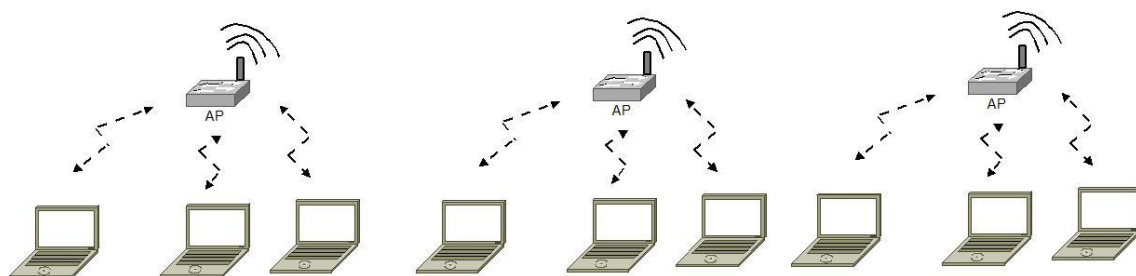


Figura 1.4.1.3 Topología ESS.

- **Áreas de servicio extendidas.** La tabla 1.4.1 muestra la Relación entre distancia y velocidad con las tarjetas Wi-Fi.

Velocidad	Distancia en interior	Distancia en exterior
11 Mbps	50 metros	270 metros
5,5 Mbps	80 metros	380 metros
2 Mbps	130 metros	430 metros
1 Mbps	160 metros	540 metros

Tabla 1.4.1 Relación entre distancia y velocidad con las tarjetas Wi-Fi en ambientes ideales [4].

1.5 Los Parámetros De Tcp/Ip A Configurar

Los parámetros Wi-Fi sirven para configurar los adaptadores de red (las tarjetas Wi-Fi), pero, para que los ordenadores puedan comunicarse, hace falta configurar también el protocolo de comunicación que van a emplear, el protocolo TCP/IP.

Para que funcione el protocolo TCP/IP, solo hace falta que el usuario le configure dos valores: el número IP de cada terminal y la máscara de la red.

1.5.1 Direcciones IP

Las direcciones IP constan de cuatro cifras separadas por puntos. Por ejemplo, 128.54.16.1. Cada cifra está representada por 8 bits lo que quiere decir que el mayor valor puede tener cualquiera de estas cifras es 255. Por lo tanto, los números IP van desde el 0.0.0.0 hasta el 255.255.255.255.

Las direcciones IP se utilizan tanto para redes públicas (como Internet), como para redes privadas (como Wi-Fi). Aunque las redes privadas no son visibles directamente desde Internet, Internet sí podría ser visible desde una red privada no debe tener un mismo número IP que una terminal de Internet. Por tanto, existen direcciones IP reservadas para ser utilizadas exclusivamente por las redes privadas. Ningún terminal de Internet puede disponer de una de estas direcciones. Incluso, por Internet no progresará

ningún paquete dirigido a estas direcciones. Las direcciones reservadas a las redes privadas con las siguientes:

De la 10.0.0.0 a la 10.255.255.255

De la 172.16.0.0 a la 172.31.255.255

De la 192.168.0.0 a la 192.168.255.255

1.6 El Accesos De Banda Ancha

El estar conectado a Internet con banda ancha quiere decir que se dispone de un gran ancho de banda, o lo que es lo mismo, que se está conectado a internet a alta velocidad. En la práctica, esto significa disponer de una conexión igual o superior a 128 Kbps.

El acceso a Internet mediante banda ancha y a bajo costo es un servicio relativamente reciente. De hecho, aunque las redes de televisión por cable ofrecían esta posibilidad desde hace tiempo. La introducción masiva de este tipo de accesos ha venido de la mano del servicio ADSL.

Los servicios de acceso a Internet en banda ancha más comunes son los siguientes:

- Acceso mediante ADSL
- Acceso mediante módem cable
- Acceso vía satélite
- Acceso vía radio LMDS
- Acceso vía circuito dedicado de datos

1.6.1 Las ventajas de la banda ancha

La posibilidad de acceder a Internet con banda ancha está haciendo que surjan servicios que se aprovechen de la alta velocidad. Por ejemplo, la posibilidad de incorporar vídeo está dando paso a popularizar aplicaciones como televigilancia, teleformación o video conferencia. Las ventajas principales de los servicios de acceso a Internet con banda ancha son las siguientes:

- **Alta velocidad.** Ofrece una velocidad de acceso a Internet de hasta 2 Mbps.
- **Siempre conectado.** No hace falta perder tiempo estableciendo la conexión. La conexión de banda ancha está siempre activa y funcionando.
- **Voz y datos simultáneamente.** Funciona de forma completamente independiente al servicio telefónico.
- **Tarifa plana.** Ofrece la posibilidad de disponer del servicio de acceso a Internet las 24 horas del día por un bajo predio fijo mensual.[4]

1.7 La conexión de Wi-Fi con Internet

La conexión de una red inalámbrica Wi-Fi con Internet se lleva a cabo a través del punto de acceso. En el mercado existen distintos modelos de puntos de acceso con distintas características. No obstante, las facilidades que puede presentar un punto de acceso para su conexión a Internet son las siguientes:

- Disponer de un puerto 10/100Base-T (RJ-45 o Ethernet, también conocido como *unlink port*) por donde poder conectarse al módem ADSL, al modem cable o al hub o switch de la red local cableada que ya está conectada a Internet.
- Disponer internamente de la funcionalidad hub. Esto facilitaría de dos a cuatro puertos exteriores de 10/100Base-T (RJ-45 o Ethernet) por donde poder conectarse a la red local cableada con conexión a Internet, o al modem ADSL/cable. Adicionalmente, esta funcionalidad de hub permitiría crear una pequeña red local cableada de dos a cuatro ordenadores. Si se necesitase de más de cuatro puertos, siempre se puede utilizar otro hub o switch y conectarlo al punto de acceso para extender la red cableada.
- Un puerto serie RS-232 a donde se le puede conectar un módem tradicional de red telefónica (V90 a 56 Kbps). Esta conexión a Internet a baja velocidad podría ser utilizada como acceso principal a Internet o como acceso secundario de seguridad en el caso de que falle la conexión principal de banda ancha (ADSL o módem cable).

- Disponer internamente de un módem V90 (56 Kbps) de línea telefónica. En este caso, el punto de acceso muestra al exterior un conector RJ11 (el conector telefónico al que se enchufan los teléfonos normales) que hay que conectar a la línea telefónica. Esta conexión a Internet de baja velocidad podría ser utilizada como acceso secundario a Internet.

Esto quiere decir que la conexión de una red Wi-Fi a Internet pasa, generalmente por conectar e punto de acceso a una red cableada que ya dispone de acceso a Internet, o por conectarlo a un módem ADSL o módem cable.

Aparte de llevar a cabo esta conexión, y configurarla adecuadamente, existen puntos de acceso que incluyen la funcionalidad de router. Esto quiere decir que el punto de acceso podría ser configurado, por ejemplo con una mejores medidas de seguridad (configuración de filtros), para compartir más de una dirección IP pública entre sus usuarios, para permitir que uno de sus ordenadores sea un servidor web, para resolver el problema de acceso a determinadas aplicaciones de Internet, etc.

1.8 Medio físico dinámico

Las ondas de radio rebotan en los objetos, penetran por las paredes y a menudo se comportan de un modo poco predecible. Las ondas de radio pueden sufrir diversos problemas de propagación que pueden interrumpir el enlace de radio, como una interferencia y sombras de múltiples rutas. Sin un medio de red fiable. Las redes inalámbricas deben validar cuidadosamente las tramas recibidas para evitar la pérdida de tramas.

Los enlaces de radio están sujetos a diversas limitaciones adicionales a las que no están sujetas las redes fijas. Como el espectro de radio es un recurso relativamente escaso, se regula meticulosamente. Existen dos métodos para que las redes de radio sean más rápidas. Se puede asignar más espectro o se puede hacer que la codificación en el enlace sea más sensible para que empaquete más datos por unidad e tiempo. Las asignaciones de espectro adicionales son relativamente raras, especialmente en redes con licencia gratuita. Las redes 802.11 han mantenido el ancho de banda de un canal de radio de

estaciones en aproximadamente 30 MHz, mientras que el desarrollo ha mejorado mucho en la codificación para aumentar la velocidad.

Los métodos de codificación más rápidos pueden aumentar la velocidad pero tienen un inconveniente potencial. Como el método de codificación más rápido depende del receptor para recoger diferencias sutiles en las señales, se requieren radios superiores de señal a ruido. Por consiguiente, las velocidades de datos mayores requieren que la estación se encuentre más cerca de su punto de acceso. La tabla 1.8.1 recoge las capas físicas estandarizadas en 802.11 y sus respectivas velocidades.

Estándar IEEE	Velocidad	Banda de Frecuencia	Notas
802.11	1Mbps 2Mbps	2,4 GHz	Primera PHY estándar (1997). Presenta tanto técnicas de salto de frecuencia como de modulación de secuencia directa.
802.11a	Hasta 54 Mbps	5 GHz	Alcance de 50m. Segunda PHY estándar (1999), finales de 2000.
802.11b	5,5 Mbps 11 Mbps	2,4 GHz	Alcance de 100m. Tercera PHY estándar, pero segunda fase de productos.
802.11g	Hasta 54 Mbps	2,4 GHz	Cuarta PHY estándar (2003). Se aplica a las técnicas de codificación de 802.11a para una velocidad superior en la banda de los 2,4 GHz, mientras que conserva la compatibilidad hacia atrás con las redes 802.11b existentes. La tecnología más común se incluyó en portátiles en 2005.

Tabla 1.8.1. Comparación entre capas físicas 802.11 (PHY).

La radio es esencialmente un medio de difusión. Cuando una estación transmite, el resto de estaciones tienen que escuchar. Los puntos de acceso actúan de una forma muy

parecida a los concentradores de red (hub) en lo que respecta a que existe una cantidad fija de capacidad de transmisión por punto de acceso y tiene que compartirse entre todos los usuarios añadidos. La adición de capacidad requiere que un administrador de red añada puntos de acceso mientras reduce simultáneamente el área de cobertura de los puntos de acceso existentes.

1.9 Estándares 802

En los esfuerzos de estandarización relacionados con 802.11 se encuentran implicados diversos grupos de estándares ya que 802.11 reduce muchos de los primeros límites de los sistemas de red. Gran parte de los esfuerzos siguen concentrados en el IEEE, pero se han recibido importantes contribuciones para los estándares de las LAN inalámbricas de diversas ubicaciones importantes.

El primer grupo es el Institute of Electronics and Electrical Engineers (IEEE). Además de sus actividades como sociedad profesional, el IEEE trabaja en la estandarización del equipamiento eléctrico, incluyendo diversos tipos de tecnologías de la comunicación. Los esfuerzos de estandarización de IEEE se organizan en proyectos, a cada uno de los cuales se les asigna un número. El proyecto de IEEE más famoso es el proyecto IEEE 802 para desarrollar estándares LAN. Dentro de un proyecto, grupos de trabajo individuales desarrollan estándares para dirigir una faceta determinada del problema. Los grupos de trabajo también tienen un número, que se escribe tras el punto del proyecto correspondiente. Ethernet, la tecnología LAN de IEEE más utilizada, fue estandarizada por el tercer grupo de trabajo, el grupo 802.3. Las LAN inalámbricas fueron formadas por el undécimo grupo de trabajo, de ahí su nombre: 802.11.

Dentro de un grupo de trabajo, se forman grupos de tarea para revisar aspectos determinados del estándar o para añadir algo al área general de la funcionalidad. A los grupos de tarea se les asigna una letra. El grupo de trabajo y el documento producido por un grupo de tarea combina el proyecto y el número de grupo de trabajo con la letra del grupo de tarea. (Algunas letras que están sujetas a una fácil confusión, como la “l” minúscula, no se utilizan.) En los sistemas de redes inalámbricas, el primer grupo de tarea

en obtener un amplio reconocimiento fue el Grupo de tarea B (TGb), que produjo la especificación 802.11b.

A intervalos periódicos, las adiciones de los grupos de tarea independientes se incluyen en “pliegos” dentro de la especificación principal. La revisión inicial de 802.11 se produjo en 1997. En 1999 se lanzaron cambios poco importantes al texto, como 802.11-1999, que fue el estándar básico durante algún tiempo. En la tabla 1.9.1 se muestran un listado básico de los diferentes estándares de 802.11.

Estándar IEEE	Notas
802.11	Primer estándar (1997). Especificaba el MAC y las técnicas de salto de frecuencia y modulación de secuencia directa originales más lentas.
802.11a	Segundo estándar de capa física (1999), pero los productos no se lanzaron hasta finales de 2000.
802.11b	Tercer estándar de capa física (1999) pero segunda fase de productos.
TGc	Grupo de tarea que realizó una corrección al ejemplo de codificación en 802.11a. Como el único producto era una corrección no existe un 802.11c
802.11d	Amplía el salto de frecuencia en PHY para su uso en múltiples dominios de regulación.
TGe (futuro 802.11c)	Grupo de tarea que produce extensiones de calidad de servicio (QoS) para el MAC. Que información es necesaria para conectar dos redes entre sí. Es muy probable que se implante una instantánea temporal denominada Wi-Fi Multi-Media (WMM) antes de completarse el estándar.
802.11e	Las redes WLAN necesitan de mecanismos de calidad de servicio que permitan priorizar diferentes tipos de tráfico, distintas ubicaciones geográficas a usuarios o departamentos

	concretos.
802.11F	Protocolo de punto de inter acceso para mejorar el tránsito entre puntos de acceso unidos directamente. Permite efectuar el <i>roaming</i> entre puntos de acceso de diferentes vendedores.
802.11g	PHY más recientemente estandarizada (2003) para redes de la banda ISM. Alcanza velocidades de 22 Mbps en la banda de los 2.4 GHz. Una de sus ventajas es que puede coexistir con todos los equipos 802.11b ya instalados aunque disminuye la velocidad a 11 Mbps.
802.11h	Estándar para hacer compatible 802.11a con las regulaciones de emisiones de radio europeas. Otros reguladores han adoptado estos mecanismos por distintos motivos.
802.11i	Mejoras para la seguridad en la capa de enlace. Los mecanismos de seguridad definidos en el estándar original (WEP) no son suficientes y, por esta razón, se ha ampliado para garantizar la autenticación de usuarios y el cifrado de la información.
802.11j	Mejoras a 802.11a para ajustarse a las regulaciones de emisión de radio japonesas.
TGk (futuro 802.11k)	Grupo de tarea para mejorar la comunicación entre clientes y la red para mejorar la administración del uso escaso de la radio.
802.11m	Grupo de tarea para incorporar cambios realizados por 802.11a, 802.11b y 802.11d así como cambios realizados por TCc en la especificación 802.11 principal. 802.11m consiste en un conjunto de normas de mantenimiento relacionados con 802.11 como un todo.
802.11n	Los estándares anteriores ofrecen velocidades teóricas de 11

	Mbps (802.11b) y 54Mbps (802.11a/g). Sin embargo, en la practica el usuario ve reducida esta velocidad drásticamente (5 Mbps y 20 Mbps, respectivamente). Estos anchos de banda resultan mínimos si se compararan con los 100 Mbps que soportan las redes locales convencionales. La solución que pone 802.11n a disposición del usuario tasas binarias reales cercanas a los 100 Mbps. Todos los dispositivos 802.11n son compatibles con las normas anteriores y capaces de interactuar con equipos 802.11a, 802.11b y 802.11g.
TGp (futuro 802.11p)	Grupo de tarea que adopta 802.11 para su uso en automóviles.
802.11R	Mejoras para el rendimiento de tránsito. Variante en la banda infrarroja. Este tipo de redes (LAN ópticas) suelen ser propietario y aporta escaso valor respecto al de las redes WLAN.
TGs (futuro 802.11s)	Grupo de tarea que mejora 802.11 para su uso como tecnología de red de malla.
TGT (futuro 802.11T)	Grupo de tarea que diseña la especificación de prueba y medida para 802.11. Resultados serán independientes; de allí su letra en mayúscula.
TGu (futuro 802.11u)	Grupo de tarea que modifica 802.11 para ayudar en el trabajo con otras tecnologías de red.

Tabla 1.9.1. Estándares IEEE para la comunicación inalámbrica 802.11.

Cuando se hizo evidente que la autenticación en redes inalámbricas se había roto fundamentalmente, la IEEE adoptó diversos estándares de autenticación desarrollados originalmente por el Internet Engineering Task Force (IETF). La autenticación de LAN inalámbrica depende mucho de los protocolos definidos por el IETF.

La Wi-Fi Alliance es una combinación de asociaciones comercial. Organización de pruebas y organización de estandarización. Gran parte del énfasis de Wi-Fi Alliance es actuar como una asociación comercial para sus miembros, aunque también se conoce por su programa de certificación Wi-Fi. Se prueba la interoperatividad de los productos con un banco de pruebas compuesto por productos de suministradores principales y los productos que pasan las pruebas tienen el derecho de utilizar la marca Wi-Fi.

Los esfuerzos de estandarización que Wi-Fi Alliance se llevan a cabo con ayuda de IEEE. En cuanto a la seguridad de las redes inalámbricas. Wi-Fi Alliance ha producido una especificación de seguridad temporal denominada Acceso protegido de Wi-Fi (WPA, Wi-Fi Protected Access). Básicamente, WPA es una instantánea de trabajo realizado por el grupo de tarea de seguridad IEEE. Es un estándar más comercial que técnico ya que la tecnología ha sido desarrollada por el IEEE. Sin embargo, sirve como función para acelerar el desarrollo de soluciones. LAN inalámbricas seguras. [5]

1.10 Modelo OSI

La Organización Internacional de Estándares (ISO) diseño el modelo de interconexión de sistemas abiertos (OSI) como guía para la elaboración de estándares de dispositivos de conexión en red y a su integración para que operen adecuadamente, el modelo OSI incluye siete capas diferentes, que van de la capa física, la cual incluye los cables de red, a la capa de aplicación, que es la interfaz con el software de aplicación que se está ejecutando ver figura 1.10.1.

Capa 7	APLICACIÓN
Capa 6	PRESENTACIÓN
Capa 5	SESION
Capa 4	TRANSPORTE
Capa 3	RED
Capa 2	ENLACE DE DATOS
Capa 1	FISICO

Figura 1.10.1 Modelo OSI.

El modelo OSI establece los lineamientos para que el software y los dispositivos de diferentes fabricantes funcionen juntos. Aunque los fabricantes de hardware y los de software para red son los usuarios principales del modelo OSI, una comprensión general del modelo llega a resultar muy benéfica para el momento en que se expande la red o se conectan redes para formar redes de área amplia (WAN).

Las siete capas del modelo OSI son la física, la de enlace de datos, la de red, la de transporte, la de sesión, la de presentación y la de aplicación. Las primeras dos capas son el hardware que la LAN comprende, como los cables Ethernet y los adaptadores de red. Las capas 3, 4 y 5 son protocolos de comunicación, como el sistema básico de entrada/salida de red (NetBIOS), TCP/IP, y el protocolo medular NetWare (NCP) de Novell. Las capas 6 y 7 son el NOS que proporciona servicios y funciones de red al software de aplicación.

- La capa física se define de la interfaz con el medio físico, incluyendo el cable de red. La capa física maneja temas elementos como la intensidad de la señal de red, los voltajes indicados para la señal y la distancia de los cables. La capa física también maneja los tipos y las especificaciones de cables, incluyendo los cables

Ethernet 802.3, el estándar de interfaz de datos distribuidos por fibra óptica para el cable de fibra óptica y muchos otros.

- La capa de enlace de datos define el protocolo que detecta y corrige errores cometidos al transmitir datos por el cable de red, el que se divide en paquetes o cuadros de información. Cuando un paquete de información es recibido incorrectamente, la capa de enlace de datos hace que se reenvíe. La capa de enlace de datos está dividida en dos subcapas: el control de acceso al medio (MAC) y el control de enlace lógico (LLC).

Los estándares basados en la capa de enlace de datos incluyen el estándar de enlace lógico 802.2 de IEEE, punto a punto (PPP), los estándares de la IEEE para el acceso múltiple con detección de portadora y detección de colisión (CSMA/CD), el estándar Token Ring y el estándar ANSI FDDI.

- La capa de red define la manera en que se dirigen los datos de un nodo de red al siguiente.

Los estándares que se refieren a la capa de red incluyen el protocolo de intercambio de paquetes entre redes (IPX) de Novell, el protocolo de Internet (IP) y el protocolo de entrega de datagramas (DDP) de Apple. El IP es parte del estándar de protocolo TCP/IP.

- La capa de transporte proporciona y mantiene el enlace de comunicaciones. La capa de transporte es la encargada de responder adecuadamente si el enlace falla o se dificulta su establecimiento.

Los estándares que pertenecen a la capa de transporte incluyen el protocolo de transporte (TP) de la Organización Internacional de Estándares (ISO) y el protocolo de intercambio de paquetes en secuencia (SPX) de Novell.

- La capa de sesión controla las conexiones de red entre nodos. La capa de sesión es responsable de la creación, mantenimiento y terminación de las sesiones de red.
- La capa de presentación es la encargada del formato de los datos la capa de presentación traduce los datos entre formatos específicos para asegurarse de que

los datos sean recibidos en un formato legible para el dispositivo al que se presenta.

- La capa de aplicación es la más alta definida en el modelo OSI. La capa de aplicación es la encargada de proporcionar funciones a las aplicaciones de usuario y al administrador de red, así como de proporcionar al sistema operativo servicios como la transferencia de archivos.

Capítulo 2

Análisis y Diseño

2.1 Selección de velocidad y degradado

Todas las interfaces 802.11 del mercado admiten algún tipo de mecanismo de degradado de velocidad, que reduce la velocidad de los datos en respuesta a condiciones adversas en la red. El comportamiento de selección de velocidad también determina cuándo debe actualizar una tarjeta su velocidad de datos debido a una calidad de enlace mejorada. No está especificado exactamente cómo determina una estación 802.11 que debe reducir la velocidad (o aumentarla), por lo que los suministradores de los conjuntos de chips tienen plena libertad para la implantación de la selección de velocidad. Casi todos los conjuntos de chips tienen su propio mecanismo de selección de velocidad y, como resultado, la mayoría de las interfaces 802.11 se comportan en forma diferente. El comportamiento de la selección de velocidad se puede programar y se controla a través del código que ejecuta la interfaz. Este comportamiento se puede ver alterado por los cambios de versión de la unidad con los cambios de firmware para una interfaz.

Los algoritmos más comunes utilizados para determinar cuándo se debe cambiar la velocidad de los datos dependen de algunas medidas de pérdida en la calidad de la señal. La calidad de la señal se puede medir directamente mediante la proporción de señal a ruido o indirectamente observando la cantidad de tramas que tienen que volver a transmitirse. Las medidas directas de las proporciones de señal a ruido pueden ser una medida instantánea de la última trama o pueden ser una media sobre un periodo reciente o cantidad de tramas recibidas recientemente. Algunos conjuntos de chip utilizan una medida directa de la proporción a señal a ruido, pero la convertirán primero en una medida de “calidad de señal”. A medida que disminuye la calidad de la señal, el chip reduce la velocidad de datos para compensar.

Las medidas indirectas pueden supervisar la pérdida de tramas media o instantánea, compensarla correctamente. Un simple algoritmo que utiliza una medida indirecta es “si se pierde la trama y se a gota el contador de intentos de trama, baje hasta la siguiente velocidad de datos y pruebe de nuevo; repita hasta que se entregue la trama a la velocidad de datos más lenta no pueda realizar la entrega”. Los conjuntos de chips que ejecutan medidas de calidad de señal indirectas pueden realizar algunas modificaciones para evitar una reducción que consuma mucho tiempo a través de todas las velocidades admitidas por la PHY, especialmente desde que los conjuntos de chips recientes admiten una gran cantidad de velocidades y el tiempo para el reintento a velocidades más lentas consume mucho tiempo.

2.2 Procesamiento de tramas y creación de puentes

En el fondo, un punto de acceso inalámbrico es un puente que traduce las tramas entre un medio inalámbrico y un medio con cables. La mayoría de los puntos de acceso se diseñan como puentes del estándar 802.11 a Ethernet, por lo que es importante saber cómo se transfieren las tramas entre dos medios.

2.2.1 Del medio inalámbrico al medio con cables

Cuando se recibe una trama en la interfaz inalámbrica de un punto de acceso con destino a la red con cables, hay que crear un puente entre los dos medios para la trama. De modo informal, está es la serie de tareas ejecutadas por el punto de acceso:

1. Cuando se recibe una trama en el punto de acceso primero se comprueba la integridad básica. Se comprueban los encabezados de la capa física y se valida el FCS en la trama 802.11.
2. Tras verificar que la trama es muy probable que se reciba sin errores, el punto de acceso comprueba si se debe procesar más la trama.
 - a. Las tramas enviadas a un punto de acceso tienen la dirección MAC del AP (el BSSID) en el campo Dirección 1 del encabezado MAC 802.11. Las tramas que no coincidan con el BSSID del AP se deben descartar.
 - b. El MAC 802.11 detecta y elimina las tramas duplicadas. Las tramas pueden duplicarse por diversas razones, pero una de las más comunes es que se pierda

o se dañe el acuse de recibo 802.11 durante el tránsito. MAC 802.11 es el responsable de filtrar las tramas duplicadas.

3. Cuando el punto de acceso determina que la trama necesita más procesamiento, tiene que descifrar las tramas protegidas por un algoritmo de seguridad de la capa de enlace.
4. Tras el cifrado correcto de la trama, se comprueba si se trata de un fragmento componente de una trama más larga que requiere una reagrupación. Las tramas reagrupadas están sujetas a una protección de integridad sobre toda la unidad reagrupada, no sobre los componentes individuales.
5. Si el AP tiene que crear un puente para la trama, tal como determina la comprobación del BSSID en el paso 2a, el encabezado MAC inalámbrico relativamente complejo se traduce en el encabezado MAC Ethernet simple
 - a. La dirección de destino, que se encuentra en el campo Dirección 3 del encabezado MAC, se copia en la dirección de destino Ethernet.
 - b. La dirección de origen, que se encuentra en el campo Dirección 2 del encabezado MAC, se copia en la dirección de origen de Ethernet.
 - c. El código de tipo Ethernet se copia desde el encabezado SNAP en el campo Datos al código Tipo en la trama Ethernet. Si la trama Ethernet utiliza también SNAP, se copia todo el encabezado SNAP.
 - d. La información de secuencia se utiliza en la reagrupación de la fragmentación pero se descarta cuando la trama cruza el puente.
 - e. Cuando el procesamiento de calidad de servicio esté estandarizado, la asignación QoS de la interfaz inalámbrica a la interfaz con cables se producirá aquí.
6. Se vuelve a calcular el FCS. Tanto Ethernet como 802.11 utilizan el mismo algoritmo para calcular el FCS pero la trama 802.11 tiene diversos campos adicionales que están protegidos por el FCS.
7. Se transmite la nueva trama a la interfaz Ethernet.

En la figura 2.2.1 se muestra el Filtrado por cable y por medio inalámbrico.

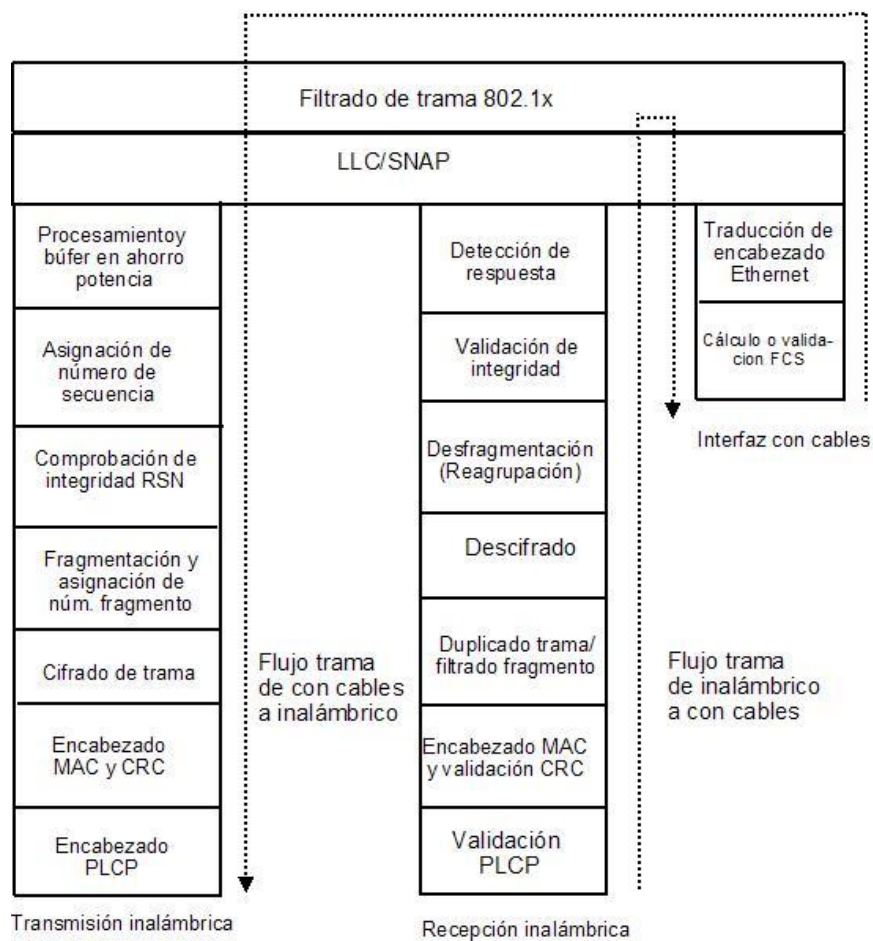


Figura 2.2.1 Traducción de tramas entre un medio inalámbrico y un medio con cables.

2.2.2 Del medio con cables al medio inalámbrico.

La creación de puentes para las tramas de la parte con cables de un punto de acceso al medio inalámbrico es bastante similar al proceso inverso:

- 1 Tras validar el FCS Ethernet, el punto de acceso primero comprueba si una trama recibida necesita más procesamiento mediante la verificación de que la dirección de destino pertenece a una estación asociada actualmente con el punto de acceso.
- 2 Se añade al principio el encabezado SNAP para los datos de la trama Ethernet. El paquete de nivel superior se encapsula dentro de un encabezado SNAP cuyo código Tipo se copia desde el código Tipo de Ethernet. Si la trama Ethernet utiliza también SNAP, se puede copiar todo el encabezado SNAP.

- 3 Se programa la transmisión de la trama. 802.11 incluye operaciones de ahorro de potencia complejas que pueden producir que un punto de acceso guarde la trama en un búfer antes de colocarla en la cola de transmisión.
- 4 Cuando la trama se encuentra en la cola de transmisión, se le asigna un número de secuencia. Los datos resultantes se protegen mediante una comprobación de integridad, si es necesario. Si se requiere una fragmentación, la trama se dividirá según el umbral de fragmentación configurado. Si la trama se fragmenta, también se asignarán números de fragmento en el campo Control de secuencia.
- 5 Si la trama requiere protección, se cifra el Cuerpo de la trama (o cada fragmento).
- 6 El encabezado MAC 802.11 se construye a partir del encabezado Ethernet MAC.
 - a. La dirección de destino Ethernet se copia en el campo Dirección 1 del encabezado MAC 802.11.
 - b. El BSSID se coloca en el campo Dirección 2 del encabezado MAC, como remitente de la trama en el medio inalámbrico.
 - c. La dirección de origen de la trama se copia en el campo Dirección 3 del encabezado MAC.
 - d. Se rellenan otros campos en el encabezado MAC. Se colocan en el campo Duración el tiempo esperado y se rellenan los indicadores apropiados en el campo Control de trama.
- 7 Se vuelve a calcular el FCS. Tanto Ethernet como 802.11 utilizan el mismo algoritmo para calcular el FCS pero la trama 802.11 tiene diversos campos adicionales que están protegidos por el FCS.
- 8 Se transmite la nueva trama de la interfaz 802.11.

Las extensiones de la calidad de servicio pueden afectar al orden de transmisión de las tramas, pero no alterar la ruta básica que sigue una trama a través de MAC 802.11. En lugar de utilizar una sola cola de transmisión. Las extensiones de calidad de servicio

802.11e tendrán múltiples colas de transmisión funcionando en los pasos 4, 5 y 7 del procedimiento de creación de puentes de la red con cables a la red sin cables. En cada uno de estos pasos, se procesan las tramas con un orden de prioridad que se puede ver afectado por el contenido de la trama y las reglas de prioridad configuradas localmente. [5]

2.3 Acceso múltiple por división de código CDMA.

La multiplexación por división de código, acceso múltiple por división de código o CDMA (por sus siglas en inglés) es un término genérico para varios métodos de multiplexación o control de acceso al medio, basados en la tecnología de espectro expandido.

Habitualmente se emplea en comunicaciones inalámbricas por radiofrecuencia, aunque también puede usarse en sistemas de fibra óptica o de cable coaxial o utp. Uno de los problemas a resolver en comunicaciones de datos es cómo repartir entre varios usuarios el uso de un único canal de comunicación o medio de transmisión, para que puedan gestionarse varias comunicaciones al mismo tiempo. Sin un método de organización, aparecerían interferencias que podrían bien resultar molestas, o bien directamente impedir la comunicación. Este concepto se denomina control de acceso al medio.

Para resolverlo, CDMA emplea una tecnología de espectro expandido y un esquema especial de codificación, por el que a cada transmisor se le asigna un código único, escogido de forma que sea ortogonal respecto al del resto; el receptor capta las señales emitidas por todos los transmisores al mismo tiempo, pero gracias al esquema de codificación (que emplea códigos ortogonales entre sí) puede seleccionar la señal de interés si conoce el código empleado.

Otros esquemas de multiplexación emplean la división en frecuencia (FDMA), en tiempo (TDMA) o en el espacio (SDMA) para alcanzar el mismo objetivo: la separación de las distintas comunicaciones que se estén produciendo en cada momento, y evitar o suprimir las interferencias entre ellas. Los sistemas en uso real (como IS-95 o UMTS) suelen emplear varias de estas estrategias al mismo tiempo para asegurar una mejor comunicación.

Una analogía posible para el problema del acceso múltiple sería una habitación (que representaría el canal) en la que varias personas desean hablar al mismo tiempo. Si varias personas hablan a la vez, se producirán interferencias y se hará difícil la comprensión. Para evitar o reducir el problema, podrían hablar por turnos (estrategia de división por tiempo), hablar unos en tonos más agudos y otros más graves de forma que sus voces se distinguieran (división por frecuencia), dirigir sus voces en distintas direcciones de la habitación (división espacial) o hablar en idiomas distintos (división por código) como en CDMA, sólo las personas que conocen el código (es decir, el "idioma") pueden entenderlo.

La división por código se emplea en múltiples sistemas de comunicación por radiofrecuencia, tanto de telefonía móvil (como IS-95, CDMA2000, FOMA o UMTS), transmisión de datos (Wi-Fi) o navegación por satélite (GPS).

En CDMA, la señal se emite con un ancho de banda mucho mayor que el precisado por los datos a transmitir; por este motivo, la división por código es una técnica de acceso múltiple de espectro expandido. A los datos a transmitir simplemente se les aplica la función lógica XOR con el código de transmisión, que es único para ese usuario y se emite con un ancho de banda significativamente mayor que los datos.

Cada usuario de un sistema CDMA emplea un código de transmisión distinto y único para modular su señal. La selección del código a emplear para la modulación es vital para el buen desempeño de los sistemas CDMA, porque de él depende la selección de la señal de interés, que se hace por correlación cruzada de la señal captada con el código del usuario de interés, así como el rechazo del resto de señales y de las interferencias multi-path (producidas por los distintos rebotes de señal).

El mejor caso se presenta cuando existe una buena separación entre la señal del usuario deseado (la señal de interés) y las del resto; si la señal captada es la buscada, el resultado de la correlación será muy alto, y el sistema podrá extraer la señal. En cambio, si la señal recibida no es la de interés, como el código empleado por cada usuario es distinto, la correlación debería ser muy pequeña, idealmente tendiendo a cero (y por tanto eliminando el resto de señales). Y además, si la correlación se produce con cualquier

retardo temporal distinto de cero, la correlación también debería tender a cero. A esto se le denomina autocorrelación y se emplea para rechazar las interferencias multi-path. [6]

2.4 Ubicación de los puntos de acceso

Cuando se selecciona un punto de acceso se deben tener en cuenta diversos factores. Un administrador de red tiene que prometer una compatibilidad con todos los estándares existentes y normalmente necesitaría prometerse para admitir estándares importantes futuros. Diversas organizaciones han lanzado programas de prueba para certificar la interoperatividad. El programa más conocido es la certificación Wi-Fi de Wi-Fi Alliance. El programa de pruebas más riguroso del sector lo lleva a cabo el Inter-Operability Lab (OIL) de la universidad de New Hampshire. El programa de pruebas IOL no se conoce tanto como los programas comerciales ya que está diseñado para ayudar a crear mejores productos.

Para cubrir un área con la cobertura requerida para una implantación grande, normalmente los puntos de acceso tienen que estar ubicados en una zona donde pueda acceder fácilmente a la potencia. Un largo recorrido de antena puede llegar a la calidad de la señal hasta formas inaceptables, por lo que es mucho mejor llevar potencia a la ubicación.

Puede que algunos entornos requieran cobertura tanto en un área interna como externa. Las antenas externas normalmente son útiles para crear una densa cobertura sobre un área o para emitir a señal en una determinada dirección sobre un patio. Las instalaciones externas suelen requerir puntos de acceso fortalecidos para el medio ambiente o incluso encerrados.

La mejor forma de asegurar la interoperatividad entre suministradores es seleccionar un sistema que base la intinerancia y el establecimiento de la conexión en una asignación VLAN dinámica. Cuando se autenticuen las estaciones, conservarán el mismo punto lógico de unión a la red.

En la figura 2.4.1 se muestra la posición en que se encuentran los puntos de acceso de la SDS. Se puede apreciar que solo una antena tiene una buena posición ya que se encuentra en el centro de un edificio y tiene buena cobertura, pero las otras dos antenas

están muy cerca, lo que puede ocasionar interferencias en canales, mala recepción y desperdicio de hardware.

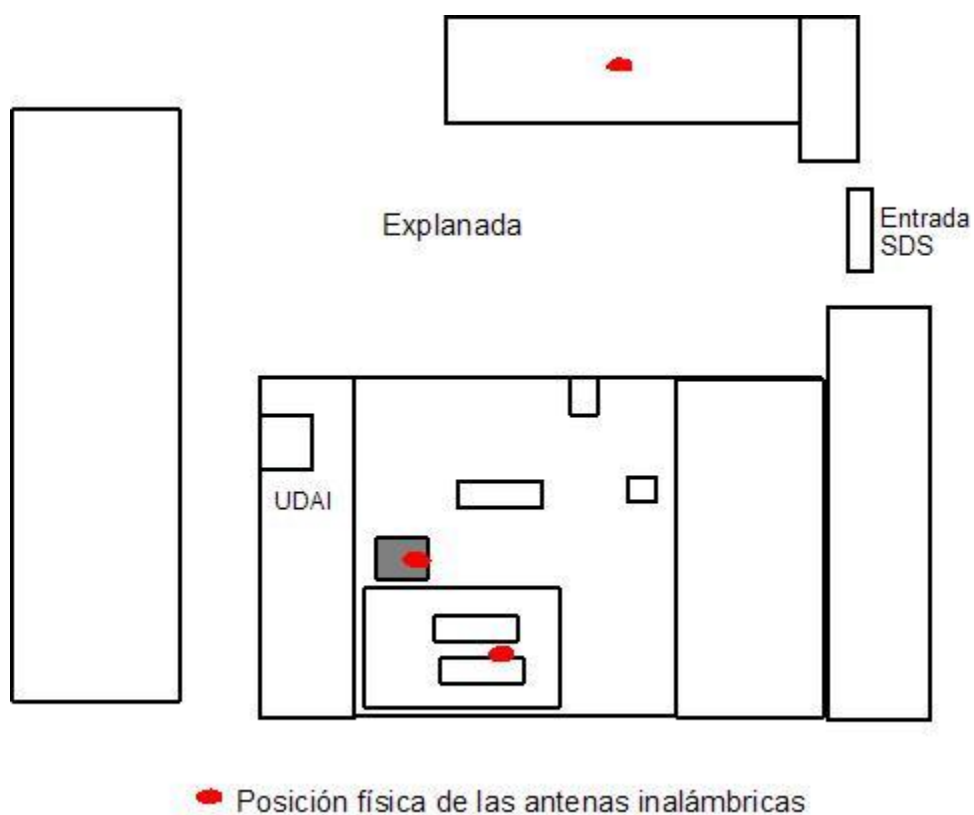


Figura 2.4.1 posición de los puntos de acceso.

Las antenas se encuentran colocadas de esta manera debido a que el edificio no tiene un fácil acceso es la oficina que brinda el servicio a 3 computadora (cuadro sombreado en la figura 2.4.1). El último punto de acceso se encuentra en la parte superior de unos anaqueles en donde se encuentran las computadoras a las que les brinda cobertura. En la figura 2.4.2 se muestra el diseño de la colocación de las antenas.

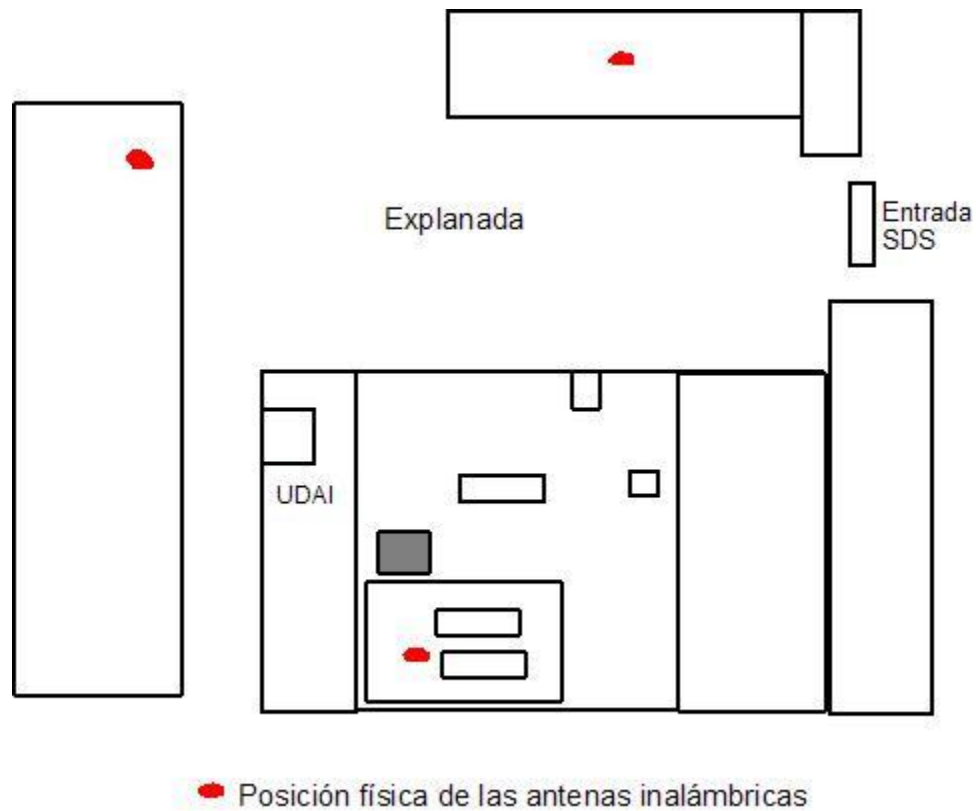


Figura 2.4.2 Posición óptima para brindar una cobertura eficiente.

2.5 Puntos de acceso virtuales

Diferentes redes lógicas tienen que ejecutarse en paralelo, con modelos de seguridad bastante diferentes. Un método de montar múltiples redes lógicas es crear múltiples redes físicas y administrarlas de forma independiente. La competencia del tiempo del administrador de la red, las ubicaciones de los puntos de acceso, la potencia y las conexiones de la red y los recursos de radio hacen que el montaje de múltiples redes físicas sea poco productivo. En su lugar, los arquitectos empiezan a utilizar los puntos de acceso virtuales, que permiten montar múltiples redes lógicas en una sola infraestructura física. El propietario de la red física es el responsable de mantener la infraestructura como una portadora común y de servir como una red de tránsito para otras redes existentes.

Los AP virtuales también tienen mucho sentido para los usuarios de red. Con una organización controlando la instalación física, no hay un esfuerzo de instalación superpuesto y reduce las ofensivas sobre el espectro de radio. Un AP virtual puede ofrecer

los mismos servicios que un AP dedicado, pero un AP normalmente es más barato de instalar gracias a la infraestructura compartida. Los AP más avanzados son exactamente iguales que múltiples AP independientes. Espero que la administración de sistemas AP virtuales ofrezcan la capacidad de extender la infraestructura de administración a los usuarios de forma que exista una interfaz de administración de bajo nivel más la capacidad de configurar redes virtuales para cada cliente que se suscriba a un servicio de red de múltiples inquilinos.

La figura 2.5.1 muestra la apariencia de una red montada sobre puntos de acceso virtuales. Básicamente, permite al administrador de red crear diversas topologías VLAN dinámicas en un conjunto de infraestructura física, estando administrada cada red virtual. En la figura 2.5.1 existen tres redes diferentes a extenderse a través de la LAN inalámbrica. La red A es la típica red corporativa. Los usuarios que deseen obtener acceso a esta red tienen que tener una cuenta en el servidor RADIUS para poder acceder. La red B es un proveedor de servicios de punto interactivo. Para obtener una independencia de los dispositivos, cualquier proveedor de servicios utiliza sistemas de autenticación basados en Web que atrapan las peticiones de los usuarios hasta que los usuarios se hayan identificado a sí mismos y hayan realizado el pago apropiado para acceder a la red. Por último la red C está diseñada para admitir voz sobre IP y tiene un sistema IP PBX. Se despliega un conjunto de puntos de acceso para admitir las tres redes. Un SSID identifica la red A. Dicho SSID es una configuración de seguridad que requiere una autenticación 802.1X frente al servidor RADIUS en la red A y puede que los sistemas que se unan a la red tengan instalado el software de cliente apropiado. Como una protección antivirus. SSID A puede admitir diferentes VLAN en la red A, dependiendo de cómo se configure el servidor RADIUS. La red A también está configurada para admitir un cifrado fuerte. La red B está apoyada por un segundo SSID que se configura para la autenticación basada en Web. Cuando los usuarios se autentican a través del sistema Web, pueden acceder a Internet, la red B no está cifrada porque el proveedor no desea restringir las plataformas informáticas del suscriptor ni requiere un software de cliente especial aparte de explorador Web. SSID C se despliega para admitir voz sobre IP. El tráfico en SSID C seguramente tenga prioridad

sobre los otros dos debido a los requerimientos de calidad servicio para el tráfico de voz. La forma de que se autentican los dispositivos frente a SSID C depende del teléfono utilizado. Muchos teléfonos VoIP no admiten todavía 802.1X, dejando que los administradores de red confíen en el filtrado MAC y en WEP para la seguridad.

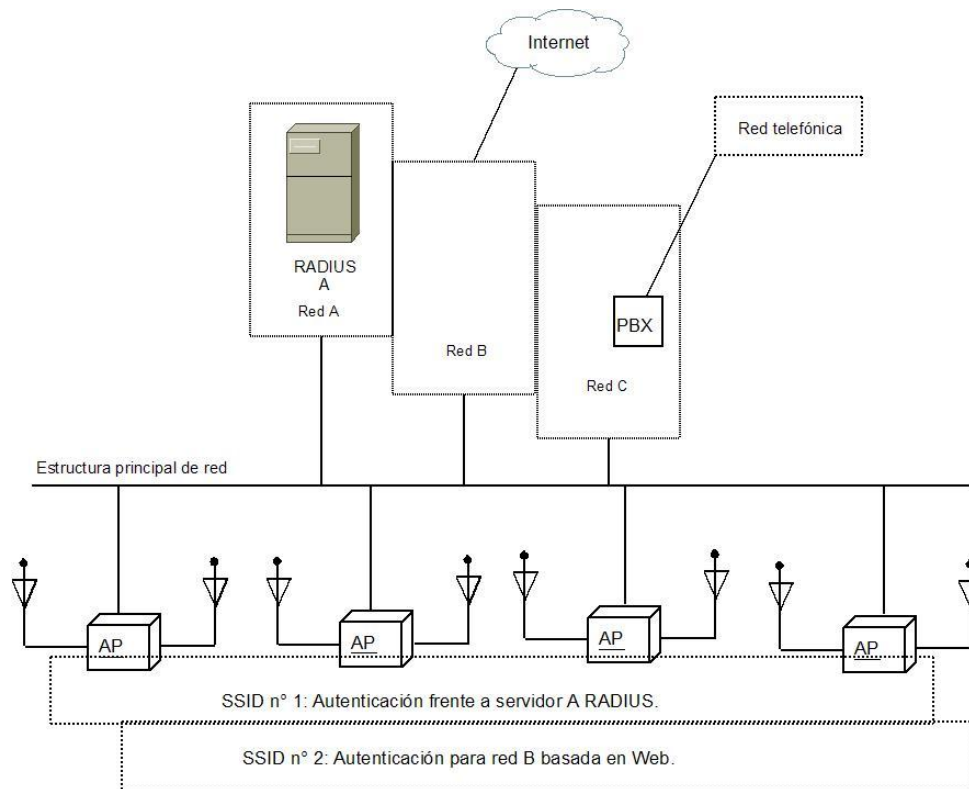


Figura 2.5.1 Puntos de acceso virtuales

Igual que cualquier otro AP, un AP virtual conecta una red de radio a una red con cables. En el caso de un AP virtual, tanto la red de radio como las redes fijas se pueden crear sobre una infraestructura física compartida. En el lugar de una red con cables o un conjunto de redes propiedad de una organización, puede existir la necesidad de conectarse a diversas redes de clientes en segundo plano. Con todas las redes que pertenecen a una organización, probablemente tengan requerimientos de subidas similares y se puedan conectar fácilmente a las redes inalámbricas.

2.6 Conmutación Wi-Fi

Los conmutadores Wi-Fi mueven las funciones de red desde los puntos de acceso (AP) a un dispositivo de agregación que proporciona funciones de control y administración.

Las funciones de control y administración son bastante importantes para una red inalámbrica. Las redes inalámbricas normalmente requieren mucha administración de red ya que están compuestas por una variedad de pequeños dispositivos. Los conmutadores Wi-Fi pueden ayudar a los administradores a montar redes más grandes proporcionando ayuda para la administración. En lugar de administrar muchos puntos de acceso autónomos, los administradores de red pueden trabajar con dispositivos de conmutación que controlan los puntos de acceso.

Al reducir el tiempo y esfuerzo requerido para controlar un AP, los conmutadores Wi-Fi pueden hacer que existan más puntos de acceso en una red inalámbrica. Normalmente tener más puntos de acceso significa tener una cobertura más tensa con áreas de cobertura más pequeñas para cada punto de acceso y menos atención de ancho de banda.

2.7 Radios definidos por el software

Dos problemas importantes con 802.11 son la ineficiencia del MAC, que limita el rendimiento, y el rápido cambio en la tecnología de la capa física, que hace que los dispositivos se queden obsoletos enseguida. Una reacción natural a la ineficiencia, especialmente de los ingenieros técnicamente adeptos, es desear implantar organizaciones específicas o nuevas opciones de protocolo en el hardware que ya poseen.

Con las LAN inalámbricas, personalizar el comportamiento de la interfaz generalmente no es posible. El procesador de la banda base, o las funciones del procesador de la banda base, se implantan directamente en el circuito integrado para las velocidad y no se pueden cambiar. Los denominados circuitos de aplicación integrados específicamente tienen un diseño lógico particular en su propio sistema de circuitos y no se pueden utilizar para nada para lo que no haya sido diseñado. Asimismo, las interfaces de LAN inalámbricas utilizan componentes de radio optimizados para su ejecución con las frecuencias asignadas a utilización de las LAN inalámbricas por los legisladores.

Sin embargo, las futuras radios se podrán volver a programar. En lugar de utilizar un hardware dedicado para el procesador de la banda base. Los diseñadores pueden utilizar dispositivos “lógicos programables” como las Matrices de campo de portal programable (FPGA). Las ondas de radio son ondas analógicas que transportan datos digitales. En muchas ocasiones, las radios sólo necesitan un procesamiento de señal programable y pueden utilizar chips de Procesador de señal digital. Independientemente del tipo de lógica programable utilizado, el objeto final es el mismo. En lugar de tener una modulación fija en la fase de diseño, las radios basadas en la lógica programable pueden cambiar la modulación la codificación y la velocidad de bits en el momento con un nuevo software. El precio de esta flexibilidad es que los dispositivos de lógica programable son mayores, se ejecutan más lentamente y consumen potencia que los dispositivos no programables. Los dispositivos de lógica programable normalmente se utilizan en el diseño de dispositivos específicos de la aplicación., una vez diseñada y probada la lógica, el FPGA se volverá a diseñar como un dispositivo específico de la aplicación. El dispositivo de lógica fija resultante a veces se denomina “copia” de su predecesor programable. Al utilizar dispositivos programables, se puede cambiar el comportamiento de la radio a voluntad, simplemente cargando un nuevo software. Se pueden implantar nuevos tipos de modulación, velocidades de bits o incluso nuevas bandas de frecuencia sin cambiar el hardware.

Las interfaces de radio controladas completamente por el software se denominan radios definidas por software o radios universales. En entornos donde la modulación y la codificación cambian rápida o frecuentemente, son muy útiles.

2.8 Seguridad

El primer paso para diseñar una política de acceso seguro es identificar las potenciales amenazas. Por las características inherentes a una red inalámbrica, cualquier usuario podría conectar su propio punto de acceso y acceder de este modo a la red. Una posibilidad es instalar un punto de acceso aislado que conecte, por ejemplo los dispositivos de casa de un usuario que construye una posible fuente de interferencias para puntos de acceso “registrados”, disminuyendo las prestaciones de la red y, además,

abriendo la puerta a posibles ataques. Otro aspecto a tener en cuenta son los dispositivos inhibidores que introducen un ruido interferente que impide que la transmisión sea posible. Finalmente un usuario no autorizado puede intentar acceder a la red para propósitos poco honrosos.

Cualquier red inalámbrica se caracteriza porque emplea como medio de transmisión el aire. Esto quiere decir que, al menos en principio, cualquier persona equipada con los dispositivos adecuados puede acceder a la información que transita por la red. Por esta razón, es necesario tomar medidas que eviten, por un lado, que usuarios no autorizados se conecten a la red y, por otro, la confidencialidad de las comunicaciones entre dos usuarios.

Los mecanismos de seguridad que define el estándar 802.11 se puede clasificar en dos grupos; cifrado y autenticación. Aunque estas herramientas de seguridad son suficientes en los casos de pequeñas empresas o en situaciones en las que los datos que se transmiten no son críticos, es necesario definir soluciones de seguridad más robustas. Por este motivo, se ha definido el estándar 802.11i, que especifica las acciones a tener en cuenta para disponer de una red WLAN segura.

2.8.1 Cifrado

El mecanismo de encriptación de tramas definido por 802.11, que emplea un cifrador de flujo RC4, recibe el nombre de WEP (Wireless Equivalent Privacy). Se trata de un cifrador de flujo simétrico que trabaja con una clave de longitud variable (hasta 256 bytes). Al ser simétrico, la clave es compartida por los dos extremos de la comunicación. Con el fin de evitar que el mismo texto en claro no genere el mismo texto cifrado, el estándar especifica un vector de inicialización que se adjunta a la clave simétrica antes de generar los datos cifrados. En la figura 2.8.1.1 se muestra el cifrado WEP

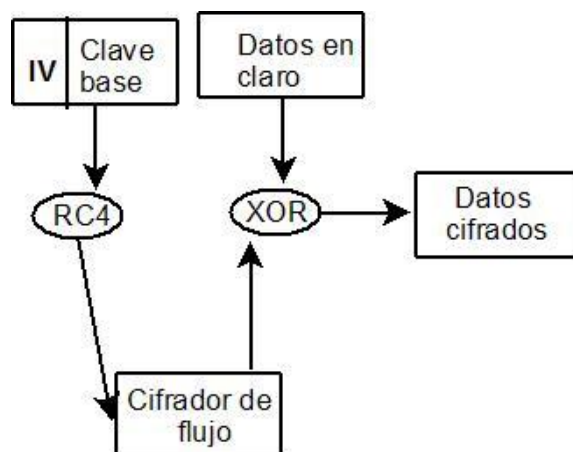


Figura 2.8.1.1 Cifrado WEP.

El vector de inicialización (IV) está formado por 24 bits cuyo valor se aconseja cambiar en cada trama. Dado que el origen genera el IV sin ningún patrón fijo, se debe enviar al receptor sin encriptar en la cabecera de la trama 802.11. De este modo, el receptor lo añadirá a la clave WEP que tiene seguridad guardada localmente y así podrá descryptar las tramas de información.

WEP exige que los dos extremos de la comunicación compartan la misma clave secreta, pero el estándar no indica nada sobre el modo en que las claves deben distribuirse. Sin un mecanismo automático de distribución de claves, cualquier protocolo de encriptación es susceptible a los errores humanos.

2.8.2 Autenticación

El estándar 802.11 especifica dos mecanismos de autenticación. El primero es la autenticación abierta que le permite el acceso a cualquier nodo que se identifique y que proporcione el SSID (Service Set ID) correcto. En un esquema de este tipo, el cliente inalámbrico no podrá enviar o recibir datos del punto de acceso a menos que disponga de la clave WEP correspondiente. La segunda forma de autenticación recibe el nombre de autenticación de clave compartida. En este caso, el cliente que desea acceder a la red envía una solicitud de autenticación al punto de acceso y éste, a su vez, le devuelve una trama de prueba sin cifrar (en claro). El cliente debe, encriptar esa trama utilizando su clave WEP y enviar el resultado al punto de acceso. Si el cliente no dispone de la clave

WEP correcta, la autenticación fallará y el cliente no podrá asociarse al punto de acceso en cuestión. Este procedimiento no es considerado seguro puesto que cualquiera que capture la trama prueba en claro y la trama de prueba cifrada puede obtener la clave WEP.

2.8.3 Extensiones del estándar

WEP presenta vulnerabilidades que tienen como consecuencia que la seguridad de una red 802.11 sea débil como se muestra en la tabla 2.8.3.1.

Vulnerabilidad	Descripción
Fragilidad del algoritmo de cifrado	El algoritmo RC4 se basa en la utilización de una clave compartida y estática.
Control de seguridad no fiable	Con un CRC-32 para comprobar la integridad de los datos, resulta muy sencillo que un atacante modifique la información y pase desapercibido.

Tabla 2.8.3.1 Vulnerabilidades WEP.

Los ataques a la seguridad de la red se agrupan en dos grandes categorías: pasivos y activos. Los ataques pasivos son aquellos en los que el único propósito del intruso es acceder a la información intercambiada entre los extremos de la comunicación. Por el contrario, el intruso activo tiene como fin alterar y modificar la información y son los más peligrosos. Entre los que se destaca:

- Escucha (eavesdropping): las comunicaciones inalámbricas viajan libremente por el aire y esto hace susceptible de ser captada por cualquiera que esté equipado con un transceptor que opere en el rango de frecuencias adecuado y dentro del área de cobertura de la red. Una variante de la escucha es la intrusión, en la que el usuario capta la señal conscientemente. En ambos casos, se trata de un ataque pasivo.

- Captura de canales (hijacking): un intruso puede hacerse con un canal, que desde ese momento ya no estará disponible para usuarios autorizados disminuyendo así las prestaciones de la red. Otra posibilidad es que un punto de acceso intruso logra conectarse a la red para que estaciones le envíen información reservada, como nombres de usuario, contraseñas, etc. este es un ataque activo.
- Ataques DoS (Denial of Service): son aquellos en los que el intruso consigue que los usuarios autorizados no puedan conectarse a la red. Un ejemplo es crear un nivel muy elevado de interferencias en una zona cercana al punto de acceso.

Las soluciones a estos ataques son muy variadas, cada una con sus puntos fuertes y sus puntos débiles. En cualquier caso, el primer punto que debe plantear a la hora de implementar una estrategia de seguridad es la necesidad de la misma, para partir de ese análisis, identificar los peligros y evaluar el coste de estar protegidos frente a ellos.

Los problemas de seguridad que presenta 802.11 derivan de la utilización de claves, WEP estáticas. Una clave estática es una clave de longitud fija definida por el administrador del sistema en el punto de acceso y en todos los clientes que se conectan a él. Si un dispositivo que utilice la clave WEP estática se pierde o es robado, su poseedor podrá acceder a la red WLAN sin que el administrador tenga la posibilidad de detectarlo, a menos que el robo sea notificado. En ese caso, el único modo de volver a disponer de comunicaciones seguras es que el administrador cambie manualmente la clave WEP de todos los clientes y puntos de acceso que utilicen la misma clave que el dispositivo perdido. Finalmente puesto que el vector de inicialización se transmite en claro en la cabecera de la trama 802.11, cualquier sniffer podrá leerlo. El mismo vector de inicialización, aplicado con la misma clave en un puente encriptado, permite a un hacker capturar las tramas de datos y obtener información tanto de dichos datos como de la propia red.

Una solución pasa por proporcionar un entorno de autenticación centralizada y distribución automática de claves. Esta aproximación está basada en el estándar 802.11i y

emplea 802.1X y EAP (Extensible Authentication Protocol). En un sistema de ese tipo, cuando un cliente sea asociado a un punto de acceso no podrá acceder a la red hasta que ésta no lo identifique. Tras la asociación, el cliente y la red (el punto de acceso o el servidor de autenticación) intercambia mensajes EAP para autenticarse mutuamente examinando sus credenciales. Hecho esto, el cliente y el servidor de autenticación acuerda una clave WEP específica para ese cliente y que se empleará únicamente durante la sesión activa. Las contraseñas y las claves de sesión nunca se envían en claro por el enlace radio. Este proceso queda recogido en la tabla 2.8.3.2.

	Fortalezas	Debilidades	Implantación
WEP Estática		IV débil. Integridad de los datos basada en CRC.	No se recomienda
WEP Dinámica	Resuelve el problema del carácter estático de la clave WEP. Emplea diferentes claves para unicast y munticast/broadcast.	Verifica la integridad de los datos con mecanismos CRC	Implantación sencilla puesto que no exige ningún cambio en los AP.
WPA con TKIP	Cifra la clave WEP y el IV eliminando la vulnerabilidad de la clave. Utiliza una función hash para verificar la integridad de la información. Claves diferentes	Vulnerable a los ataques por DoS. Si TKIP detecta dos errores de integridad en el mismo minuto, el AP desconecta a	Necesita una actualización del software de algunos AP.

	para cifrado e integridad.	todos los clientes.	
WPA con AES	Algoritmo de encriptado más robusto	Ninguna conocida	Requiere de la instalación de software para los clientes y algunos AP.

Tabla 2.8.3.2 Mecanismos de seguridad en redes 802.11.

2.8.4 Ventajas del sistema 802.11/EAP

Autenticación mutua entre los clientes y el servidor de autenticación (como un servidor RADIUS).

Generación dinámica de claves tras la autenticación.

Control centralizado que garantiza que, una vez expirada la sesión, el cliente debe reautenticarse y se vuelven a generar nuevas claves. En la figura 2.8.4.1 se muestra la autenticación EAP.

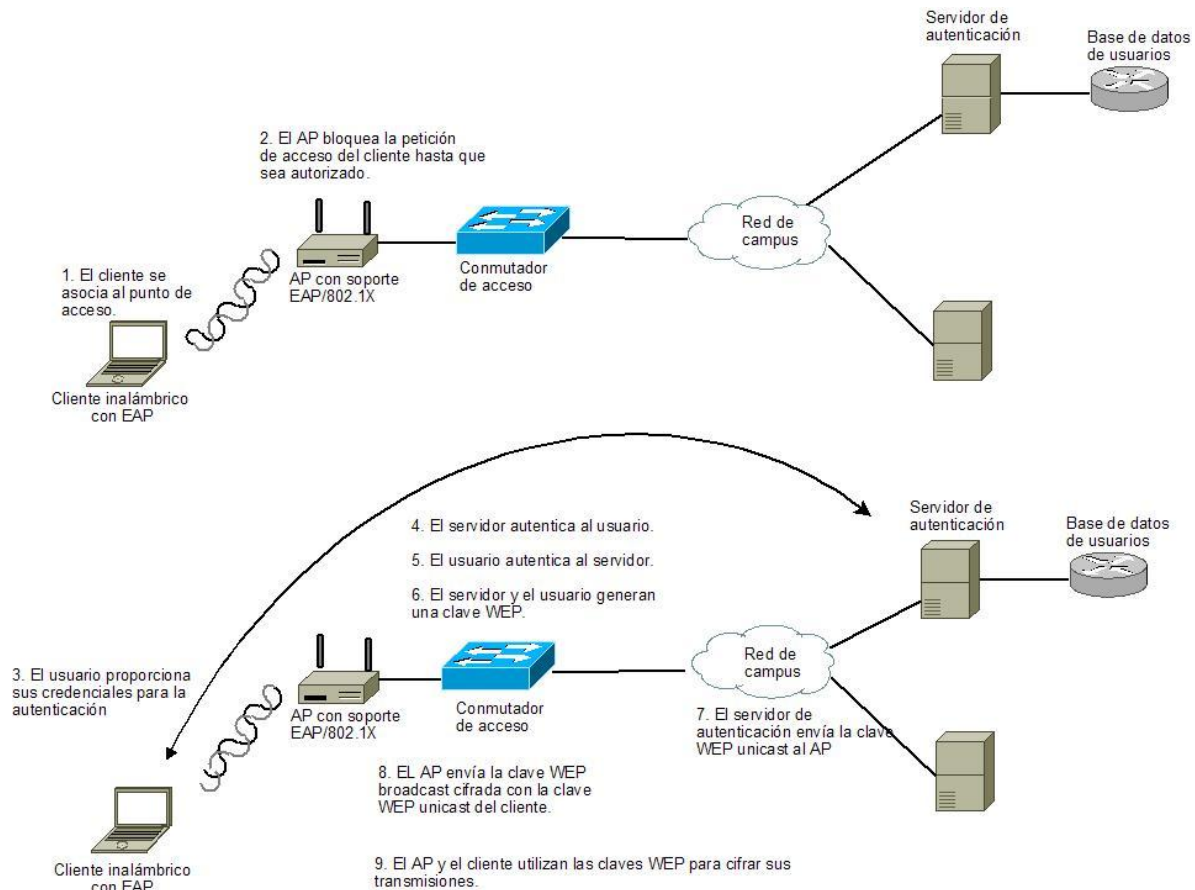


Figura 2.8.4.1 Autenticación EAP.

Existen varios protocolos de autenticación EAP. El primero es EAP-TLS. Se trata de un estándar de IETF recogido por la RFC 2716 y basado en el protocolo TLS (Transport Layer Security) descrito en la RFC 2246. EAP-TLS, utiliza certificados digitales tanto para el cliente como para el servidor de autenticación. Como se muestra en la figura 2.8.4.2, el servidor de autenticación envía su certificado al cliente en lo que se denomina fase 1 de la autenticación (autenticación TLS del servidor). El cliente valida el certificado del servidor verificando su emisor (autoridad de certificación) y sus contenidos. Finalizada esta operación, el cliente envía su certificado al servidor de autenticación, comenzando así la segunda fase (autenticación TLS del cliente). El servidor de autenticación valida el certificado del cliente comprobando su emisor y su contenido y, en caso de éxito, envía un mensaje EAP-Success al cliente y ambos acuerdan una clave WEP.

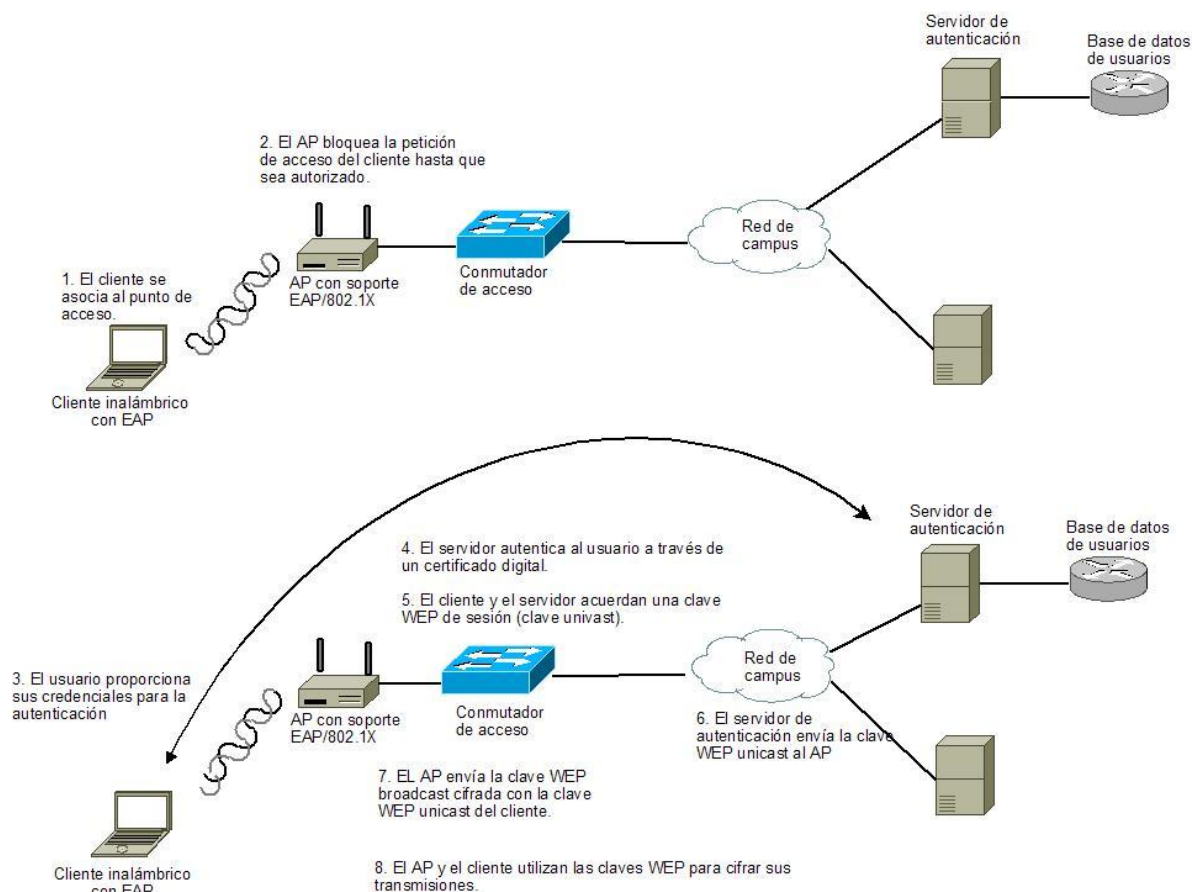


Figura 2.8.4.2 Autenticación EAP – TLS.

Otro protocolo de autenticación es PEAP (Protected EAP). En este caso, se utiliza un certificado digital para la autenticación del servidor y para la del cliente se emplean varios métodos sobre un túnel seguro TLS. La fase 1 es idéntica a EAP-TLS y tiene como resultado la creación de un túnel TLS cifrado entre el cliente y el servidor de autenticación por el que circularán los mensajes EAP. En la fase 2, el servidor autentica al cliente mediante algún otro tipo de EAP.

Sin embargo, la utilización de WEP con distribución dinámica de claves continúa utilizando un mecanismo de CRC para verificar la integridad de los datos, esto hace posible alterar la información y que dicha modificación pase desapercibida.

Para resolver este problema, la Wi-Fi Alliance propone el empleo de WPA 1.0, una autenticación basada en 802.1X junto con un cifrado TKIP. TKIP se basa en tres elementos

principales PPK (Per Packet Keying), MIC (Message Integrity Check) y la extensión del vector de inicialización de 24 a 48 bits. Una de las vulnerabilidades más claras de WEP deriva del hecho de que se utiliza la misma clave para cifrar todas las tramas, puesto que el conjunto de la clave WEP y el vector de inicialización es fijo. La solución más sencilla es cambiar este conjunto en cada paquete. Como muestra la figura 2.8.4.3, al vector de inicialización y la clave WEP se le aplica una función hash de la que se obtiene una clave única (clave temporal) y que será la que, combinada con el vector de inicialización, se utilizará para cifrar las tramas. Para evitar los ataques debidos a las colisiones en la inicialización de IV, el valor de la clave base debe cambiarse antes de que se repita el vector de inicialización.

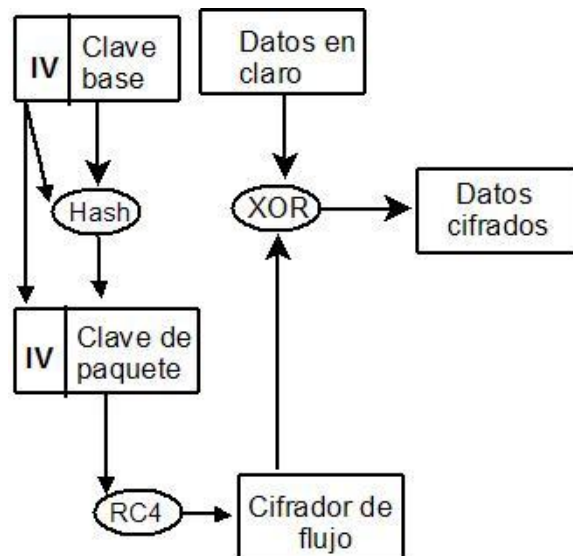


Figura 2.8.4.3 WEP con PPK.

Por otra parte, MIC protege las tramas cifradas con WEP de las alteraciones malintencionadas. MIC utiliza una semilla, las direcciones de MAC origen y destino y la carga útil, a los que aplica una función hash, para obtener un valor que se enviará junto con los datos encriptados como se muestra en la figura 2.8.4.4. De este modo, cualquier alteración en el contenido de los datos dará un valor de MIC erróneo.

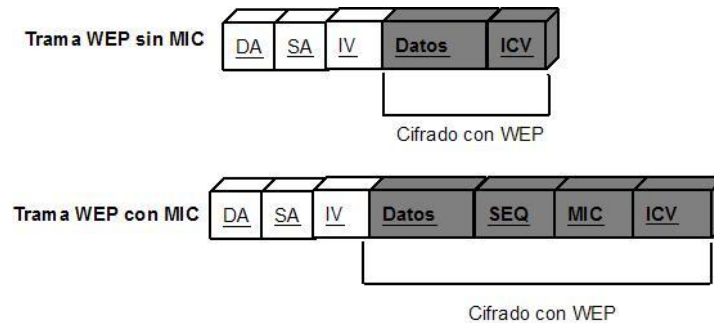


Figura 2.8.4.4 Cifrado WEP con MIC.

Hay una arquitectura de seguridad más robusta, procedente de una evolución de la anterior, WPA 2.0 con AES. Consistente en cambiar el algoritmo de cifrado RC4 por otro mucho más fuerte. [7]

WPA2™ es una certificación de producto que otorga Wi-Fi Alliance y certifica que los equipos inalámbricos son compatibles con el estándar 802.11i. WPA2 admite las características de seguridad obligatorias adicionales del estándar 802.11i que no están incluidos para productos que admitan WPA. Con WPA2, el cifrado se realiza mediante AES (estándar de cifrado avanzado), que también reemplaza WEP por un algoritmo de cifrado más seguro. Al igual que TKIP para WPA, AES proporciona la determinación de una clave de cifrado de unidifusión de inicio exclusiva para cada autenticación y el cambio sincronizado de la clave de cifrado de unidifusión para cada trama. Debido a que las claves AES se determinan automáticamente, no es necesario configurar una clave de cifrado para WPA2. WPA2 es la forma más eficaz de seguridad inalámbrica. [8]

2.9 Cambio en el ancho de banda

La red requerida es tipo BSS que pueda proporcionar servicio a dos redes inalámbricas, una para usuarios privilegiados y la otra para usuarios invitados, con restricciones en el uso del ancho de banda para evitar que los usuarios abusen del ancho de banda, haciendo descargas o bajando información demasiado grande y así evitar el tráfico en la red, utilizar seguridad para ambas redes, para evitar el ataque de intrusos. El diseño de esta red se ve en la figura 2.9.1.

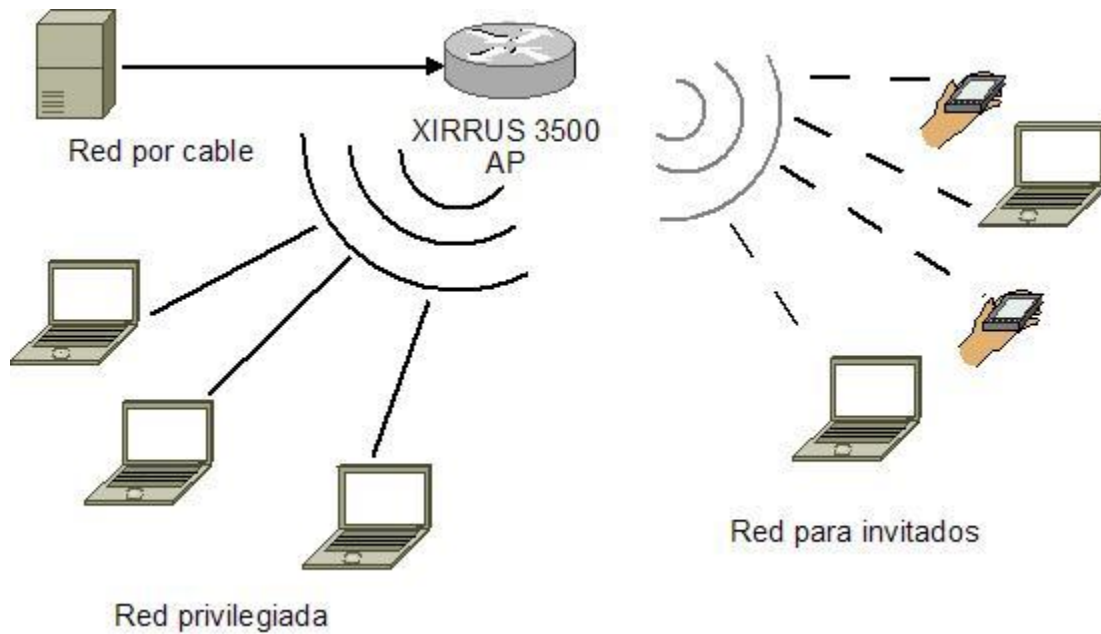


Figura 2.9.1 Diseño de la red inalámbrica para la Secretaría de Desarrollo Social.

En la figura 2.9.2 se muestra el esquema para realizar la conversión del ancho de banda. El ancho de banda es la capacidad de transferencia de datos, en otras palabras, la cantidad de datos que se pueden mover de un punto a otro en cierta cantidad de tiempo.

El tener una comunicación de datos implica dos cosas:

- Un conjunto de conductores eléctricos utilizados para hacer posible la comunicación a bajo nivel.
- Un protocolo para facilitar la comunicación de datos confiable y eficiente.

Hay dos tipos de componentes de sistemas que satisfacen estos requerimientos:

- Buses
- Datapaths [9]

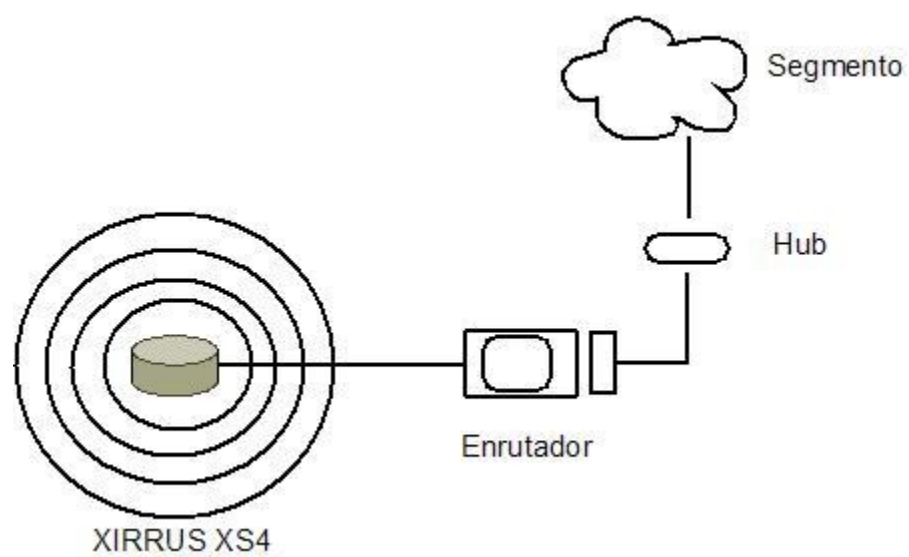


Figura 2.9.2 Esquema para la conversión del ancho de banda en Xirrus XS4 3500.

Capítulo 3

Implementación

3.1 Requerimientos previos

En la Secretaría de Desarrollo Social (SDS) cuentan con 3 matrices marca Xirrus modelo XS4 3500 como se muestra en la figura 3.1.1. Sus características son: Integra 4 puntos de acceso (4 802.11a/b/g) con un conmutador WLAN integrado de 500Mbps. Soporta 802.11i / WPA2 y dispone de capacidades de failover.

	 Modelo XS4
Radios 802.11a/b/g	4
Los puertos de enlace ascendente Ethernet	1 Gigabit
Máximo ancho de banda Wi-Fi	216 Mbps
Wi-Fi integrado	Sí
amenaza del sensor	Sí
Analizador de espectro integrado	Sí
Número máximo de usuarios por radio	64
Número máximo de usuarios por matriz	256
Número de Llamadas de Voz por matriz	36
Número de flujos de vídeo por matriz	9

Figura 3.1.1 Matriz Xirrus XS4 3500 y sus principales características.

La posición dentro de la SDS de las antenas era la que muestra la figura 3.1.2 la imagen del Xirrus 1 y Xirrus 3 están bien colocados en el techo de las oficinas, pero el Xirrus 2 no tiene una buena colocación. En la figura 3.1.3 se muestra la posición física de las matrices

Xirrus en donde es notable que la matriz Xirrus 2 y Xirrus 3 están muy cerca y una sola matriz Xirrus XS4 es suficiente para cubrir esa área, por esta razón hubo que reubicar las matrices para que den un servicio óptimo.



Figura 3.1.2 Antigua posición de las antenas Xirrus

El uso de matrices inalámbricas es por la conservación de edificios históricos ya que no se pueden realizar perforaciones ni daños en la infraestructura .

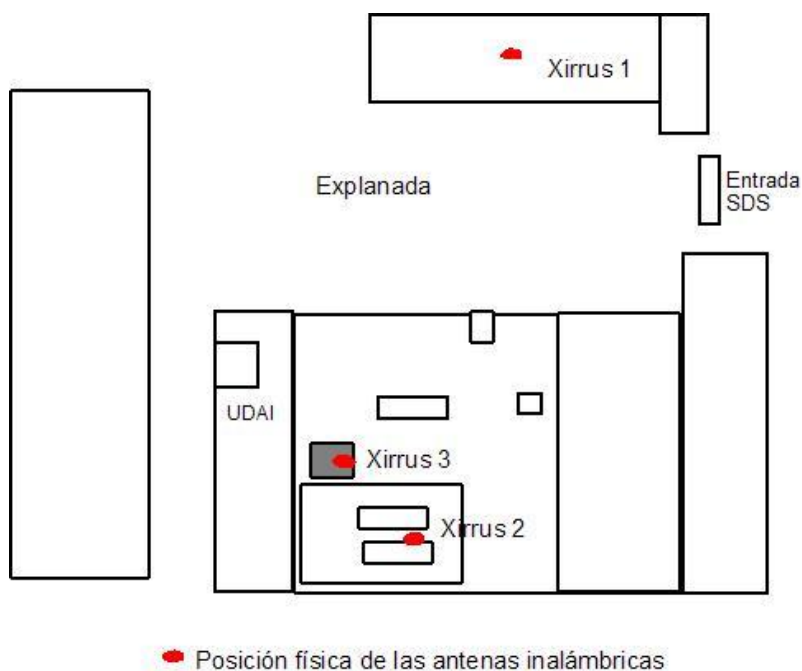


Figura 3.1.3 Mapa representativo de la posición de las antenas inalámbricas Xirrus XS4 3500 dentro de la SDS.

La propuesta para rehubicar las antenas se muestra en la figura 3.1.4. La matriz Xirrus 3 cubre un área muy pequeña con solo 3 estaciones que requieren el servicio y la señal de Xirrus 2 no llega; es así que decidí que Xirrus 2 debe tener una mejor posición para cubrir la oficina en donde se encontraba Xirrus 3.

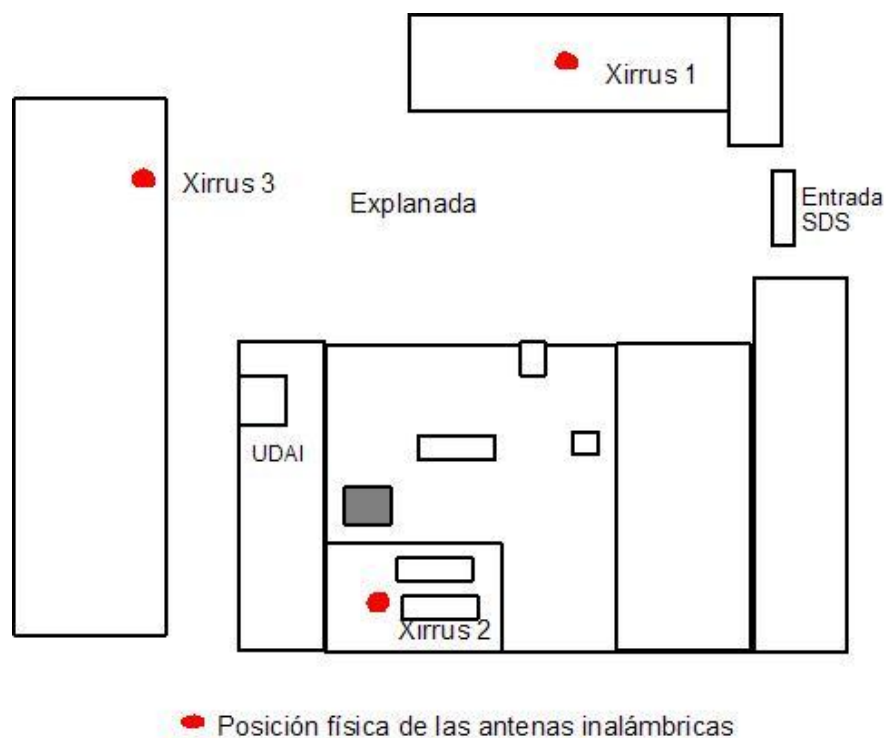


Figura 3.1.4 Propuesta para ubicar las matrices Xirrus XS4 3500 en la SDS.

Antes de realizar los cambios es necesaria la comunicación con las matrices, estas ofrecen dos interfaces para su manipulación, una es interfaz de gestión de ventanas (WMI) su modo de operación es mediante un explorador como Internet Explorer en la barra de dirección se coloca la dirección IP de la matriz a la que se le va a dar servicio, y la otra interfaz es por línea de comandos (CLI) está utiliza un cable que en un extremo tiene entrada rj45 y en el otro extremo una entrada para puerto serial en la figura 3.1.5 se muestra el cable requerido para la comunicación CLI.



Figura 3.1.5 Cable de consola para la matriz Xirrus XS4 3500.

Debido a que algunos usuarios de la SDS cambian la configuración de su dirección IP la dirección que se asignó a las matrices fue duplicada, lo que ocasionó que la interfaz WMI no pueda ser utilizada. Como algunos usuarios han modificado su número IP es necesario restablecerlo ya que no se tiene un buen control, esto mismo servirá para que se solucione el problema que se tiene con la asignación de IP libres y así se tendrá un rango amplio de direcciones IP para la asignación mediante DHCP (asignamiento automático de direcciones IP).

Para realizar esta reasignación se obtuvo sus actuales direcciones mediante una tabla como se muestra en la figura 3.1.6. Luego se capturaron los datos y se re direccionaron algunas direcciones IP, finalmente el departamento cuenta con esta información para que los usuarios eviten el re asignar su dirección. También se libero un número considerable de direcciones IP para la pila de direcciones por DHCP necesaria para el asignamiento automático de la matriz Xirrus 3 para la red de invitados.

  Unidad de Desarrollo Administrativo e Informática (UDAI)					
Depto.	Nombre	Grupo Trabajo	Dir. IP	P. Enlace	Macadrees

Figura 3.1.6 Tabla para obtener dos datos de cada computadora en la SDS.

El cable requerido para la interfaz por línea de comandos no le fue entregado al departamento UDAI cuando se realizó la compra de los arreglos, es por eso que me comunique con el personal de Xirrus, Inc. quienes respondieron claramente a mi solicitud y me enviaron el cable para la comunicación CLI.

3.2 Interfaz de línea de comandos CLI

La matriz Wi-Fi XS4 3500 provee un procedimiento para el establecimiento de una conexión Telnet a la matriz. Se utiliza el procedimiento para inicializar el sistema conectando el cable serial a la computadora y el otro extremo a la matriz. En el símbolo de logging, se ingresa el nombre de usuario y contraseña. La raíz de comandos (**Root Command Prompt**) es el primer símbolo que se verá después de acceder a la CLI. Si se encuentra en un nivel distinto de la raíz de mando se puede volver a ese símbolo en cualquier momento utilizando el comando **exit**. La raíz de comandos que ve en la ventana de CLI está determinada por el nombre del host que se le haya asignado.

El comando **Help** ofrece la ayuda, genera una ventana que ofrece información acerca de los tipos de ayuda que están disponibles con la CLI, solo se encuentra disponible en la raíz.

Comando **?** este comando está disponible en cualquier prompt y provee ayuda completa o parcial, cuando se coloca como argumento de cualquier comando mostrará todos los posibles argumentos permitidos, y si no se coloca ningún comando antes mostrará todos los comando posibles que pueden ser solicitados.

Todos los comandos no son sensibles de mayúsculas y minúsculas. La tabla 3.2.1 muestra el nivel superior de los comandos [11]

COMANDO	DESCRIPCIÓN
configure	Entrar al modo de configuración
exit	Salir de CLI y terminar sesión, si este comando es usado en otro nivel diferente del root prompt entonces regresa a un nivel previo.

help	Muestra una descripción de ayuda interactiva del sistema.
more	Turno de paginación ON u OFF.
quit	Salir de la línea de comandos CLI
save	Guardar la configuración a la memoria FLASH
show	Muestra información de un tema
statictics	Muestra datos estadísticos de la Matriz
uptime	Muestra el lapso de tiempo desde la última vez que inicio.

Tabla 3.2.1 Primer nivel de comandos de la interfaz CLI.

En el segundo nivel de comandos que son válidos una vez que se esté dentro de configure. Ver tabla 3.2.2

COMANDO	DESCRIPCIÓN
acl	Configura la lista de Control de acceso
administrator	Define parámetros de acceso del administrador
clear	Borra o limpia los elementos requeridos
contact-info	Información del contacto para la asistencia de la Matriz
date-time	Configurar la fecha y hora
dhcp-server	Configurar el servidor DHCP
dns	Configurar el DNS
end	Salir del modo configuración
exit	Subir un nivel
filter	Define protocolos de los parámetros
fips	Ejecuta FIPS de seguridad
help	Describe la ayuda interactiva del sistema
hostname	Nombre de la Matriz
https	Habilitar o deshabilitar HTTPS
interface	Seleccionar interface de configuración
quit	Salir de la Interfaz CLI
radius-server	Configurar los parámetros del servidor RADIUS

reboot	Reiniciar la matriz
reset	Borra todas las configuraciones, volver a los valores por default y reiniciar.
run-test	Correr una prueba de test
save	Guardar la configuración
security	Configura los métodos de seguridad de la matriz.
show	Despliega toda la información acerca de un tema seleccionado
snmp	Habilitar, deshabilitar o configurar SNMP
ssh	Habilitar, deshabilitar SSH
ssid	Configurar los parámetros SSID
standby	Configurar los parámetros standby
statistics	Despliega estadísticas
uptime	Despliega el tiempo desde la última vez que inicio
vlan	Configurar los parámetros VLAN

Tabla 3.2.2 Segundo nivel de comandos de CLI.

3.3 Recuperación de la interfaz WMI.

El acceso al Xirrus 2 que se muestra en la figura 3.1.2 es fácil y fue el primero en ser recuperado de la siguiente manera:

Se conecta el cable en la parte posterior de la matriz en la entrada que dice CONSOLE figura 3.3.1, y el otro extremo a una computadora en el puerto serial. Entrar a HyperTerminal para realizar la comunicación: Inicio-> Todos los programas -> Accesorios-> Comunicaciones -> HyperTerminal.



Figura 3.3.1 parte posterior del Xirrus XS4 3500.

HyperTerminal es un programa que permite conectarse con otros equipos, sitios Telnet de Internet, servicios de boletines electrónicos, servicios en línea y equipos host con un módem o un cable de conexión directa.[10]

Una vez que se abre el programa HyperTerminal pedirá un nombre para la conexión para este caso fue Xirrus ver figura 3.3.2 A), después el puerto para comunicarse en este caso el COM1 ver figura 3.3.2 B), entonces aparece la ventana para la configuración del puerto ver figura 3.3.2 C), los parámetros que se necesitan son:

Bits por segundo: 115200

Bits de datos: 8

Paridad: Ninguna

Bits de parada: 1 y

Flujo de control: Ninguno

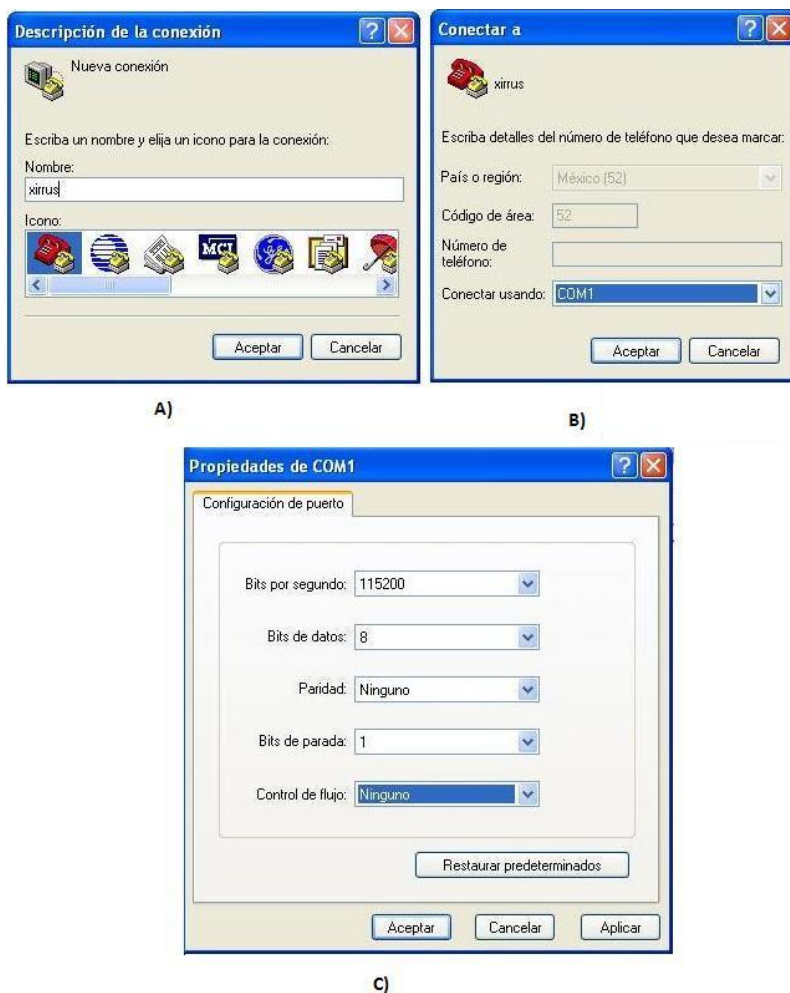


Figura 3.3.2 Conexión de Xirrus 3500 con Hyper Terminal. A) Nombre de la conexión, B) puerto de comunicación, C) configuración del puerto para la comunicación.

Una vez establecida la comunicación Hyper Terminal se solicitará el usuario y la contraseña para poder establecer la comunicación con el equipo Xirrus, por defecto el usuario es admin y la contraseña es admin ver figura 3.3.3. Los comandos en modo consola van por niveles y funcionan según lo que se requiera realizar.



Figura 3.2.3 Login en modo consola del Xirrus XS4.

Para saber que comandos pueden ser ejecutados se puede utilizar el comando signo de interrogación ?. Este comando muestra una lista de las opciones validas que pueden ser configuradas en este momento ver figura 3.3.4.

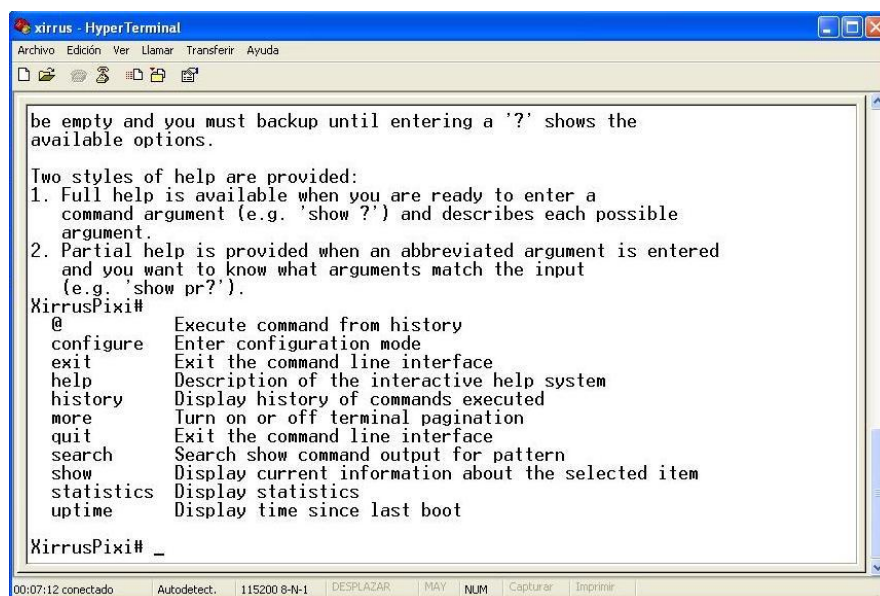
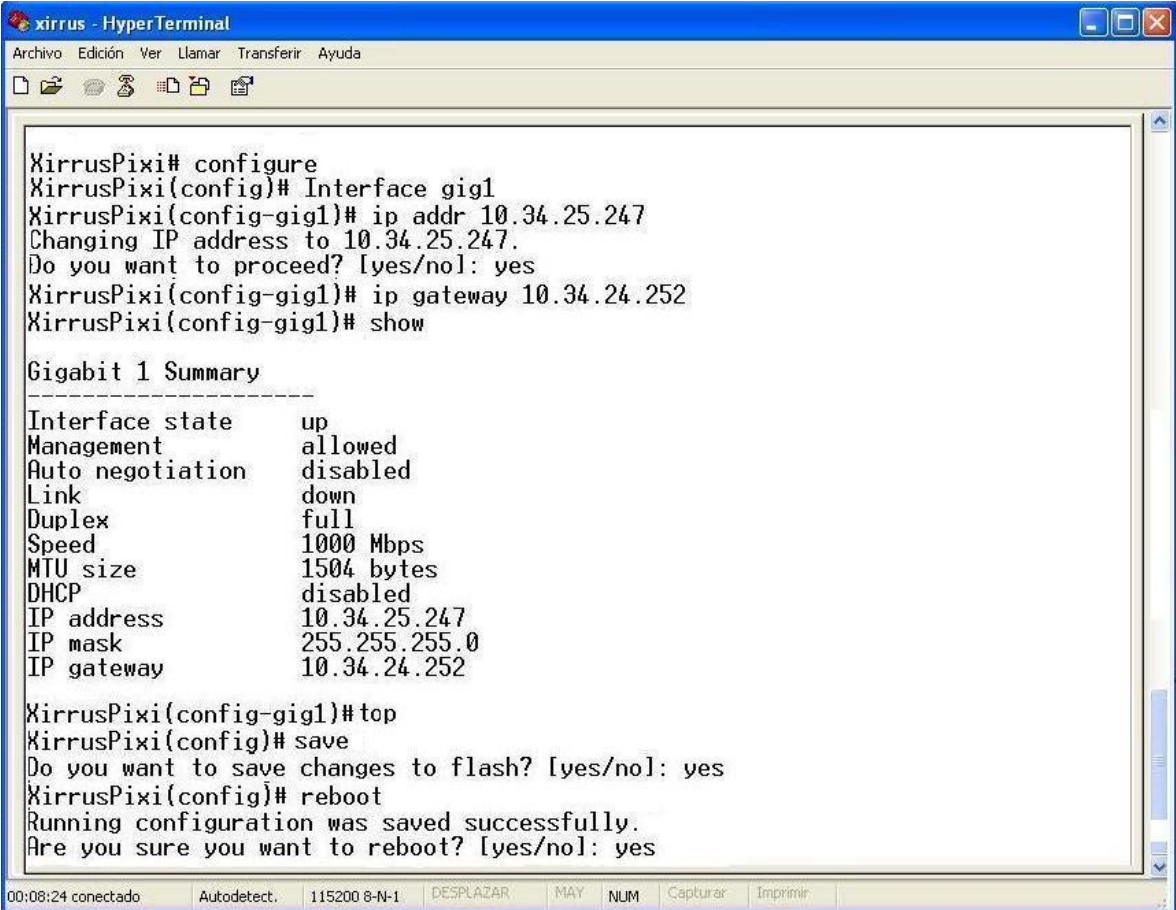


Figura 3.3.4 Comando ? muestra las pociones válidas a realizar en cualquier nivel de consola para las matrices Xirrus XS4 3500.

Los comandos a seguir para la recuperación de IP de la matriz Xirrus es la siguiente:

- Configure. Entrar al modo de configuración.
- Interface gig1. Se establece la ubicación de la matriz; de donde se ofrecen los servicios de red.
- Ip addr 10.34.25.247. Cambio de dirección Ip.
- Yes. Confirmar el cambio de dirección.
- Ip Gateway 10.34.24.252. Puerta de enlace.
- Show. Muestra la configuración.
- Top. Regresa un nivel en este caso a Configure.
- Save. Guardar los cambios realizados yes para confirmar.
- Reboot. Reinicia la matriz para efectuar los cambios realizados.

En la figura 3.3.5 se muestra la inserción de estos comandos.



```

XirrusPixi# configure
XirrusPixi(config)# Interface gig1
XirrusPixi(config-gig1)# ip addr 10.34.25.247
Changing IP address to 10.34.25.247.
Do you want to proceed? [yes/no]: yes
XirrusPixi(config-gig1)# ip gateway 10.34.24.252
XirrusPixi(config-gig1)# show

Gigabit 1 Summary
-----
Interface state      up
Management           allowed
Auto negotiation     disabled
Link                  down
Duplex                full
Speed                1000 Mbps
MTU size              1504 bytes
DHCP                  disabled
IP address            10.34.25.247
IP mask               255.255.255.0
IP gateway            10.34.24.252

XirrusPixi(config-gig1)# top
XirrusPixi(config)# save
Do you want to save changes to flash? [yes/no]: yes
XirrusPixi(config)# reboot
Running configuration was saved successfully.
Are you sure you want to reboot? [yes/no]: yes
  
```

Figura 3.3.5 Comandos para la re asignación de dirección IP del modo consola para recuperar las matrices Xirrus XS4 3500.

El Xirrus 2 fue recuperado satisfactoriamente. Para recuperar la dirección IP del Xirrus 1 que se encuentra en el techo de un edificio ver figura 3.1.2 fue necesaria la ayuda de varios compañeros de la dependencia para alcanzar la matriz, en la figura 3.3.6 se muestran las maniobras para su recuperación.



Figura 3.3.6 Recuperación de la matriz Xirrus 1.

Después de colocar el cable en Xirrus 1 se reasigno su dirección IP la cual fue 10.34.24.248, para así disponer desde ese momento con sus respectivas interfaces gráficas WMI.

El Xirrus 2 lo coloque 1 semana en otra posición dentro de la misma oficina para encontrar el lugar óptimo para cubrir la misma área y también la oficina en donde se encontraba Xirrus3. Ver figura 3.3.7 A). Luego de decidir la altura apropiada se fijo, no en el techo porque otras oficinas no tenían cobertura ver figura 3.3.7 B).



Figura 3.3.7 Reubicación de Xirrus 2. A) Realizando pruebas de cobertura. B) Xirrus 2 fijo.

Para Xirrus 3 no fue necesario realizar su reasignación de dirección IP en ese momento ya que cuando se realizaron las pruebas de Xirrus 2 apagué el equipo para evitar el ruido, que no interfirieran en los canales y para saber hasta dónde llegaba la cobertura de Xirrus 2 para poder quitar Xirrus 3 sin dejar a nadie sin servicio. Después de fijar Xirrus 2, Xirrus 3 fue retirado de la oficina.

3.4 Creación de SSID invitado

Para acceder al modo WMI se escribe la dirección IP de la matriz en la barra de dirección de un explorador, la computadora que realiza la petición debe estar conectada a la red alámbrica ya que por razones de seguridad la matriz no puede ser manejada desde la red inalámbrica. Aparecerá una pantalla como la que se muestra en la figura 3.4.1 en donde se solicita un usuario y su contraseña por default el usuario y la contraseña es admin. Una vez identificados se puede manejar la matriz Xirrus XS4 3500.

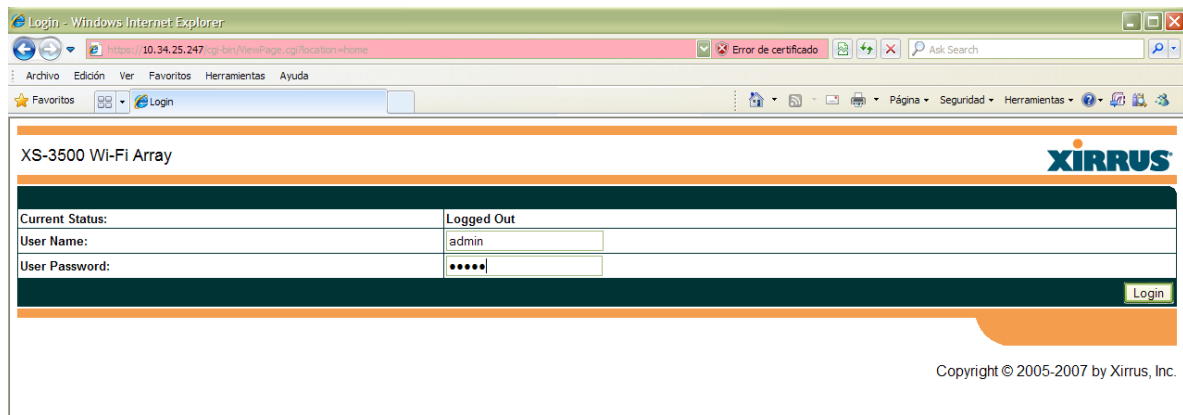


Figura 3.4.1 Logging de la interfaz WMI del Xirrus XS4 3500.

En esta interfaz se muestra un menú del lado izquierdo en la pantalla donde muestra todos los componentes de la matriz que pueden ser manejados, los menús que tienen una flecha de lado izquierdo significa que tienen submenús, una vez que se realizan los cambios que requerimos se aplican y finalmente se guardan, si es necesario se reinicia el equipo para ver los cambios. Ver figura 3.4.2.

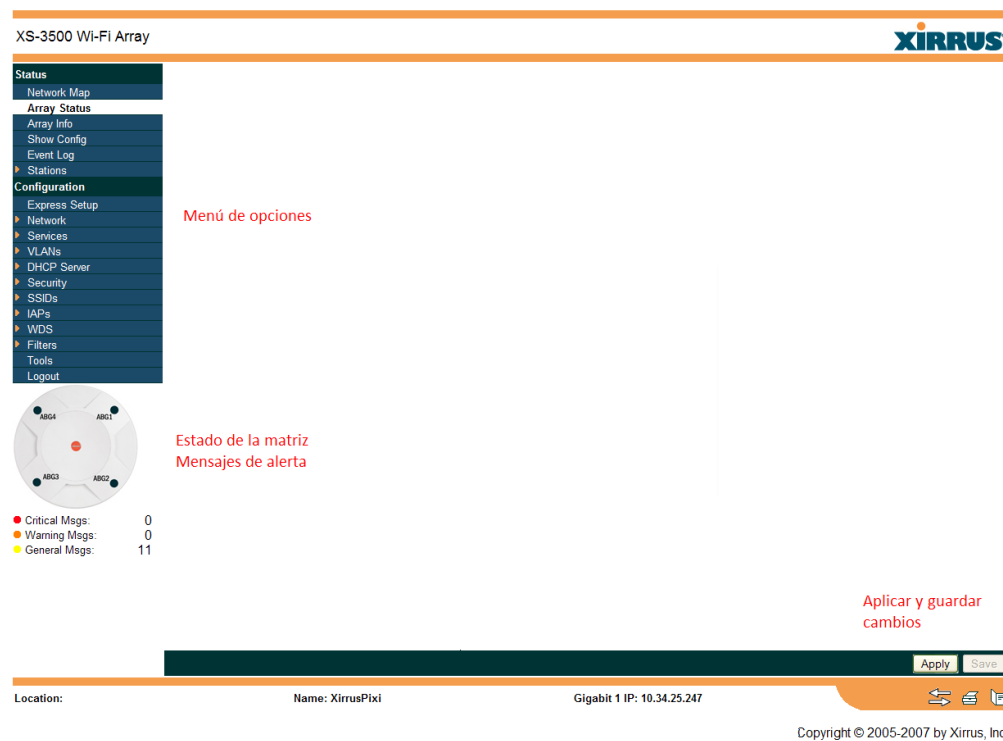


Figura 3.4.2 Opciones configurables de la matriz Xirrus XS4 dentro de la interfaz WMI.

Para crear una red en el menú SSID's tiene el submenú SSID Management que es el manejador de las redes. Primero se crea el nombre de la red y se le da click en el botón create por default la matriz va a crear la red en la matriz de manera deshabilitada ya que hayamos hecho los cambios requeridos se habilita, se da click en el botón Apply y por último en Save. En la figura 3.4.3 se muestran las opciones de la configuración de una red sin seguridad llamada SDS_Humboldt.

The screenshot displays the 'SSID Management' configuration page. On the left is a sidebar with navigation options: Status, Network Map, Array Status, Array Info, Show Config, Event Log, Stations, Configuration, Express Setup, Network, Services, VLANs, DHCP Server, Security, and SSIDs. The 'SSIDs' section is expanded, showing 'SSID Limits Summary' and 'SSID Management'. Below this is a circular diagram of an array with four stations labeled ABG1, ABG2, ABG3, and ABG4. A legend indicates 'Critical Msgs: 0' and 'Warning Msgs: 0'. The main configuration area for 'New SSID Name' is titled 'Up time - 0 days 0 hours 21 minutes'. It includes a 'Create' button and a table of existing SSIDs. The selected SSID is 'SDS_Humboldt (Broadcast)' with a 'Delete' button. Below the table are various configuration options: State (radio buttons for Enable and Disable), Broadcast SSID (radio buttons for Enable and Disable), Band Association (radio buttons for 802.11a, 802.11b/g, and Both), QoS Priority (a dropdown menu set to 2), VLAN ID (a dropdown menu set to (none) and a VLAN Number input field), Internal DHCP Pool Assigned (a dropdown menu set to (none) and a Station Limit input field set to 256), Overall Traffic Limit (radio buttons for Unlimited and Packets/Sec), Traffic Limit per Station (radio buttons for Unlimited and Packets/Sec), Day/Time Limit (radio buttons for Active and Inactive), Time Active (radio buttons for Always, Time On, and Time Off), Days Active (checkboxes for All, Sun, Mon, Tue, Wed, Thu, Fri, and Sat), Web Page Redirect (WPR) (radio buttons for Enable and Disable), Authentication Type (a dropdown menu set to Open), Encryption Type (a dropdown menu set to None), and Security Settings (radio buttons for Use Global Settings and Use Unique Settings). At the bottom right are 'Modify' and 'Save' buttons.

Figura 3.4.3 Configuración de la red SDS_Humboldt.

Esta red está habilitada, las opciones de configuración son:

- New SSID Name: Permite crear el nombre de una nueva SSID.
- SSID: En este campo se proporciona una tabla con todas las SSID asignadas. Si se da click en cualquiera de ellas se podrán cambiar sus opciones.
- State: Cualquier SSID puede estar habilitada o deshabilitado.
- Broadcast SSID: indica si es publicable. Si esta activada esa SSID será visible a todos los clientes de la red y si se encuentra deshabilitada entonces los equipos que conozcan el nombre de la red serán los que podrán conectarse, es decir, esta red se aparecerá oculta.

- Band Association: indica las bandas de los estándares 802.11a, 802.11b/g o ambos. La mayoría de los equipos inalámbricos trabajan mejor con 802.11b/g.
- QoS priority: (Opcional). Se puede filtrar la calidad de los datos y puede ser:
 - 0: Poco, donde hace su mejor esfuerzo en de filtrado y priorización de datos, vídeo y tráfico de voz sin comprometer el rendimiento de la red. Se este ajuste en ambientes donde el tráfico de prioridades no es una preocupación
 - 1: Medio, con el agregado de prioridades QoS a través de todo el tráfico.
 - 2: Alto, donde QoS filtrado normalmente da prioridad al tráfico de vídeo.
 - 3: La mayor fijación de prioridades QoS, donde normalmente filtrado QoS da prioridad a la voz (VoIP) del resto de tráfico.
- VLAN ID: si es que se quiere asociar a una VLAN. La VLAN debe ser definida previamente.
- Internal DHCP Pool Assigned: si las Direcciones IP se asignan dinámicamente se selecciona el rango esté debe ser declarado previamente.
- Station Limit: Permite limitar el número total de estaciones que se permiten para esa SSID, por default es 256 que es el total de estaciones soportadas por Xirrus XS4 3500.
- Overall Traffic Limit: Límite general del tráfico puede ser ilimitado o limitarlo a paquetes por segundo para obligar a una restricción de tráfico de las estaciones asociadas en esta SSID.
- Traffic Limit per Station: Limitar el tráfico por estación puede ser ilimitado o introducir el número de paquetes para cada estación.
- Day/Time Limit: Este campo informa si el día y la hora actual esta activada la SSID.

- Time Active: Puede ser que siempre se encuentra activa o puede introducir las horas en que desee proporcionar el servicio. En la figura 3.4.3 se muestra el horario de 8 de la mañana a 8:59 pm.
- Days Active: Pueden ser todos los días de la semana o puede seleccionar los días que desee proporcionar el servicio. En la figura 3.4.3 se muestra que solo está activo de lunes a sábado.
- Web Page Redirect (WPR): Si se habilita esta opción se puede elegir una página web. La funcionalidad de redireccionar una página puede utilizarse como alternativa para autenticarse o para mostrar una pantalla de bienvenida cuando un usuario se conecta por primera vez a esta SSID.
- Authentication Type: El tipo de autenticación ofrece las siguientes opciones:
 - Open: Esta opción no proporciona autenticación.
 - RADIUS MAC. Autentica las estaciones de la red Wi-Fi de un servidor RADIUS basado en su dirección MAC.
 - 802.1X: 802.1x: autentica en las estaciones de la red Wi-Fi a través de un radio servidor mediante 802.1x con EAP. El servidor RADIUS puede ser interno (proporcionado por la matriz) o externo.
- Encryption Type: Tipo de cifrado. Ofrece una lista desplegable donde se puede elegir entre Ninguno, WEP, WPA, WPA2 o WPA – Both.
- Security Settings: Puede ser Global Settings para utilizar la configuración global que previamente se estableció o puede ser Unique Settings para tener prioridad sobre estos parámetros.

Así como esta red está configurada, las demás redes de Xirrus 1 y Xirrus 2 están su único método de seguridad es la configuración IP ya que se ingresa manualmente, el método para asignar una dirección IP es el siguiente:

Panel de control -> conexiones de red -> dar click con el botón derecho del mouse en conexiones de red inalámbrica -> propiedades -> doble click en Protocolo Internet (TCP/

IP) aparecerá una ventana como la que se muestra en la figura 3.4.4. Donde hay que seleccionar la opción Usar la siguiente dirección IP.

La SDS cuenta con un enlace a Finanzas por lo que tiene habilitado 2 rangos el 10.34.24.xx y el 10.34.25.xx, donde xx va del rango 1 al 255, y se utilizan los últimos del 10.34.24.250 al 10.34.24.255 para uso exclusivo de servidores, y puntos de acceso inalámbrico. Las direcciones 10.34.24.xx son las más utilizadas por casi todos los departamentos, donde comparten archivos y se encuentran sus grupos de trabajo. El rango 10.34.25.xx es utilizado por muy pocas computadoras que raramente comparten archivos o que no quieren que vean sus archivos, es por esta razón que hay más IP libres en el rango 10.34.25.xx.

La máscara de subred es 255.255.255.0. La puerta de enlace es 10.34.24.252, ya que la computadora con IP 10.34.24.252 es el Proxy de la red, esta computadora tiene el sistema operativo Linux Open Suse y el proxy se controla con el programa squid, esté restringe algunas descargas, paginas, Messenger, y actualmente se encuentra en mejoras para brindar un mejor servicio.

El servidor DNS es 200.52.12.131 y el alternativo es 172.21.9.36, estos parámetros fueron dados por finanzas.

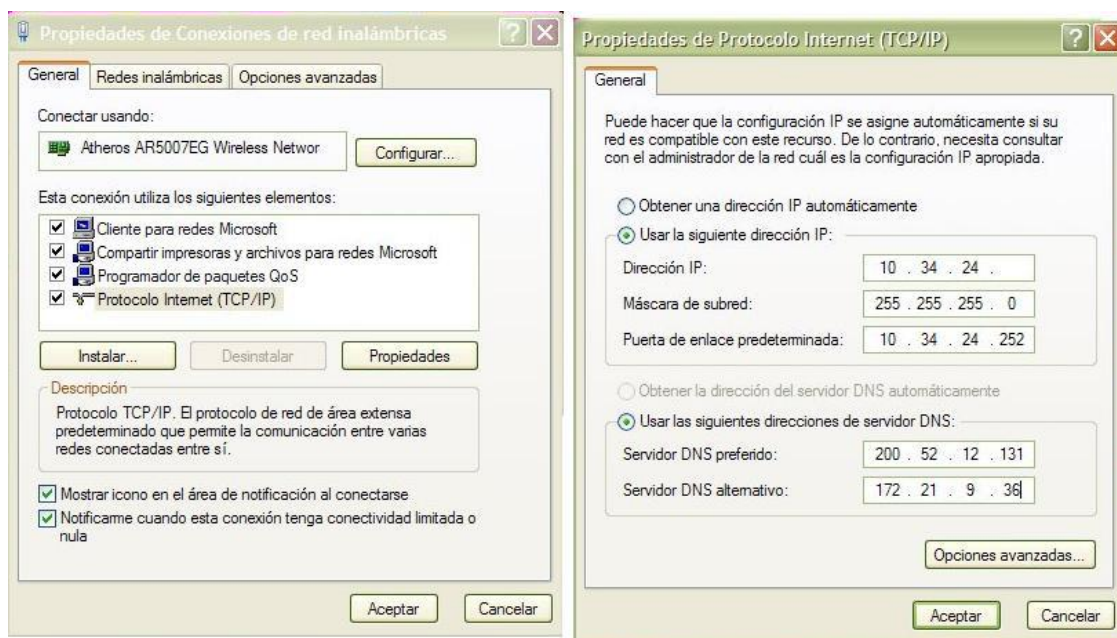


Figura 3.4.4 Propiedades de redes inalámbricas.

Después de ingresar la IP dar click en opciones avanzadas, en la pestaña DNS donde aparece una venta como se muestra en la figura 3.4.5 se habilita la opción Anexar estos sufijos DNS y se agrega sfdspuebla.gob.mx, también en Sufijo DNS para esta conexión.

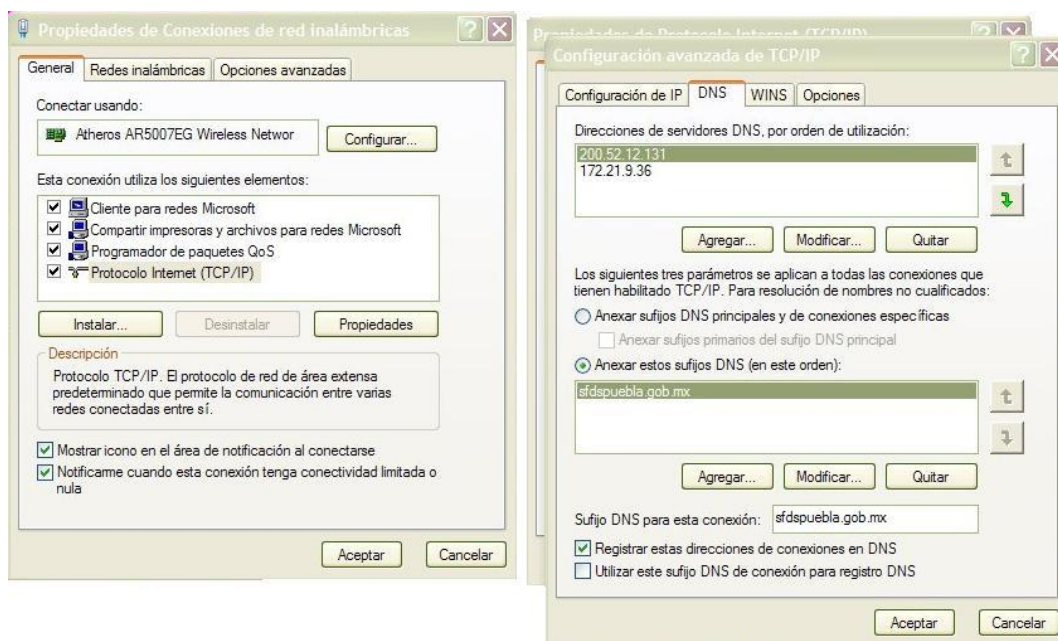


Figura 3.4.5 Configuración avanzada de TCP/IP.

Una vez configurada la dirección IP se debe de quitar el firewall de Windows ya que el servidor proxy se encargara de ser el corta fuegos de internet, para habilitarlo se abre el explorador y en el menú de Herramientas -> opciones de internet se da click en la pestaña Conexiones se abre una ventana como la que se muestra en la figura 3.4.6 A), se da click en la opción Configuración de LAN, se abre una ventana como muestra la figura 3.4.6 B), se escribe la dirección: 10.34.24.252 puerto 8080 y Aceptar.

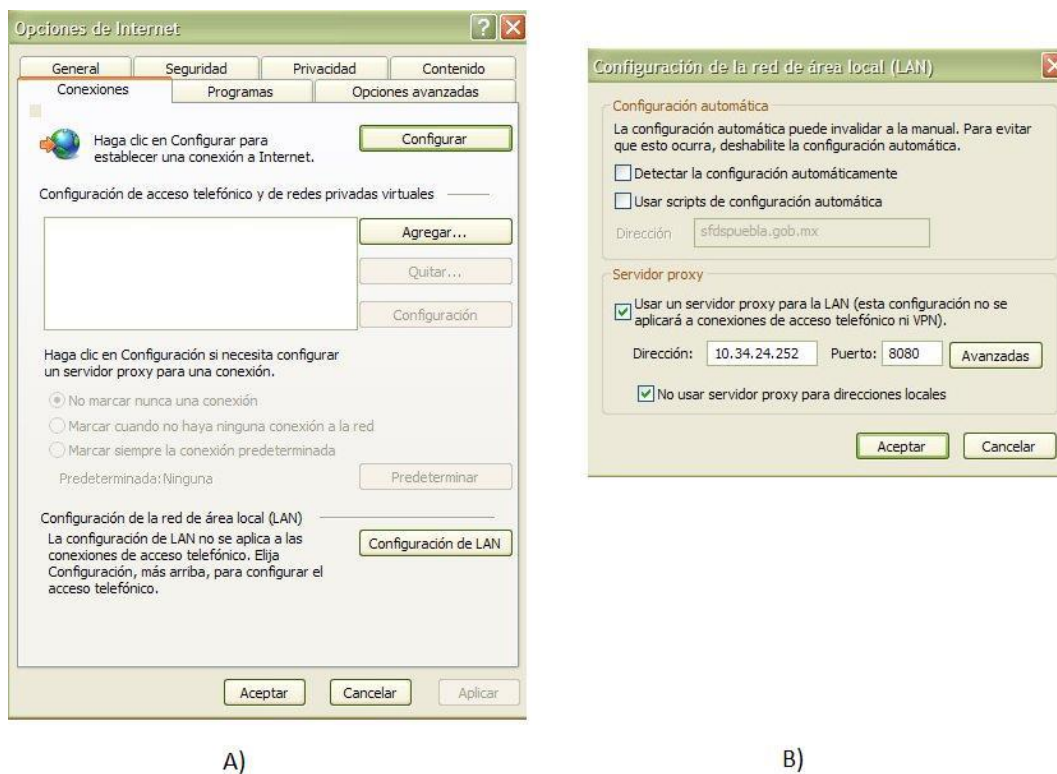


Figura 3.4.6 Opciones de internet A) Configuración de LAN. B) Servidor proxy.

3.5 Configuración de la red inalámbrica para invitados

Para realizar la implementación de la red inalámbrica para invitados se registraron los siguientes parámetros:

- Nombre de la SSID: pixina.
- State: Enable. Su estado es habilitado.
- Broadcast SSID: Enable. Esta SSID está habilitada, esto es que es publicable.

- Band Association: Both indica que es compatible con las bandas de los estándares 802.11a/b/g. Para no dejar a ninguna tarjeta de red inalámbrica fuera del servicio.
- QoS priority: (Opcional). 0: Ya que no interesa la prioridad de los datos para esta SSID.
- VLAN ID: No hay la necesidad de una VLAN para esta SSID.

En la figura 3.5.1 se muestran los parámetros ingresados para el manejo y control de la red inalámbrica para usuarios invitados.

Status		Uptime - 0 days 0 hours 21 minutes	
Network Map	New SSID Name:		Create
Array Status	SSID:	SDS_Humboldt (Broadcast) pixina (Broadcast)	Delete
Array Info	State:	☒ Enable ☐ Disable	
Show Config	Broadcast SSID:	☒ Enable ☐ Disable	
Event Log	Band Association:	☐ 802.11a ☐ 802.11b/g ☒ Both	
Stations	QoS Priority:	0	
Configuration	VLAN ID:	(none)	VLAN Number:
Express Setup	Internal DHCP Pool Assigned:	ip_otras	
Network	Station Limit:	256	
Services	Overall Traffic Limit:	Unlimited: ☒	Packets/Sec:
VLANs	Traffic Limit per Station:	Unlimited: ☐	Packets/Sec: 20
DHCP Server	Day/Time Limit:	Active	
Security	Time Active:	Always: ☐	Time On: 08:00 Time Off: 20:59
SSIDs	Days Active:	All: ☐ Sun: ☐ Mon: ☒ Tue: ☒ Wed: ☒ Thu: ☒ Fri: ☒ Sat: ☒	
SSID Limits Summary	Web Page Redirect (WPR):	☐ Enable ☒ Disable	
SSID Management	Authentication Type:	802.1x	
IAPs	Encryption Type:	WPA2	
WDS	Security Settings:	☐ Use Global Settings ☒ Use Unique Settings	
Filters	WPA		
Tools	PSK Authentication:	☒ Yes ☐ No	
Logout	WPA Preshared Key / Verify Key:	***** *****	
	EAP Authentication:	☐ Yes ☒ No	
	RADIUS		
	RADIUS Server Mode:	☐ Internal ☒ External	
	Primary IP Address:		
	Primary Port Number:	1812	
	Secondary IP Address:		
	Secondary Port Number:	1812	
	Timeout (seconds):	600	
	Primary Shared Secret / Verify Secret:	***** *****	
	Secondary Shared Secret / Verify Secret:	***** *****	
	Accounting	☒ Off ☐ On	
		Modify Save	

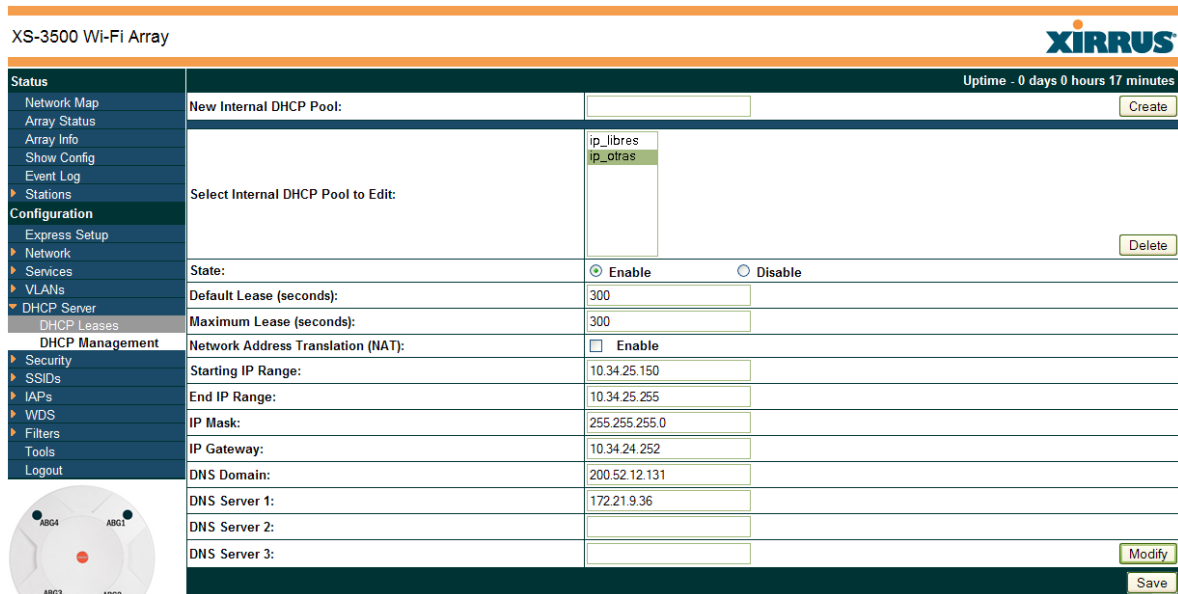


Critical Msgs: 0
 Warning Msgs: 0
 General Msgs: 16

Location: Name: XirusPixi Gigabit 1 IP: 10.34.25.247

Figura 3.5.1 Parámetros registrados de la red inalámbrica para invitados.

- Internal DHCP Pool Assigned: ip_otras, donde ip_otras fueron las ip que se liberaron del rango 25 y su configuración se muestra en la figura 3.5.2; ip_otas comienzan en 10.34.25.150 y terminan en 10.34.25.255 ofreciendo un total de 105 direcciones de ip libres para ser ocupadas en esta asignación dinámica. Como la puerta de enlace es 10.34.24.252, esto es que pasan por el proxy de la SDS entonces se bloquean ciertas aplicaciones y páginas que ocupan demasiado ancho de banda.



The screenshot shows the configuration page for the XS-3500 Wi-Fi Array. The left sidebar contains a navigation menu with options like Status, Network Map, Array Status, Array Info, Show Config, Event Log, Stations, Configuration, Express Setup, Network, Services, VLANs, DHCP Server, DHCP Leases, DHCP Management, Security, SSIDs, IAPs, WDS, Filters, Tools, and Logout. The main content area is titled 'New Internal DHCP Pool:' and shows a list of pools: 'ip_libres' and 'ip_otras'. The 'ip_otras' pool is selected. Below the list, there are fields for 'State' (set to 'Enable'), 'Default Lease (seconds)' (300), 'Maximum Lease (seconds)' (300), 'Network Address Translation (NAT)' (set to 'Enable'), 'Starting IP Range' (10.34.25.150), 'End IP Range' (10.34.25.255), 'IP Mask' (255.255.255.0), 'IP Gateway' (10.34.24.252), 'DNS Domain' (200.52.12.131), 'DNS Server 1' (172.21.9.36), 'DNS Server 2' (empty), and 'DNS Server 3' (empty). There are 'Create', 'Delete', 'Modify', and 'Save' buttons.

Field	Value
State	Enable
Default Lease (seconds)	300
Maximum Lease (seconds)	300
Network Address Translation (NAT)	Enable
Starting IP Range	10.34.25.150
End IP Range	10.34.25.255
IP Mask	255.255.255.0
IP Gateway	10.34.24.252
DNS Domain	200.52.12.131
DNS Server 1	172.21.9.36
DNS Server 2	
DNS Server 3	

Figura 3.5.2 DHCP ip_otras comienza en 10.34.25.150 y termina en 10.34.25.255 mascara de red 255.255.255.0, puerta de enlace 10.34.24.252, servidor DNS preferido: 200.52.12.131 y servidor 1 DNS: 172.21.9.36.

- Station Limit: se dejo este parámetro en 256 porque no es necesario delimitarlo ya que no interfiere en otras SSID.
- Overall Traffic Limit: El límite general de tráfico es ilimitado con el fin de no alentar todavía más la red de invitados.
- Traffic Limit per Station: se limito el tráfico a 20 paquetes por estación, de esta manera se resuelve el problema de que los usuarios descarguen música, videos, o cualquier software que ocupe demasiado ancho de banda. Ya que

como se esperan los datos y tardan en llegar la comunicación lanza una alerta que dice que hay un problema de conexión pero la conexión no se interrumpe en ningún momento.

- Day/Time Limit: Este campo informa si el día y la hora actual esta activada la SSID. En el momento de realizar los cambios si estaba activada la SSID.
- Time Active: El tiempo de activación es de 8 de la mañana hasta las 20:59 Hrs.
- Days Active: Los días de la semana que se encuentra la SSID activa son de lunes a sábado.
- Web Page Redirect (WPR): Esta opción está deshabilitada porque no es necesario crear una página de re direccionamiento.
- Authentication Type: La autenticación es por 802.1X ya que proporciona un candado de seguridad por que se deben de registrar los equipos antes poder conectarse a la red pixina si un equipo no identificado quiere conectarse a esta red no lo podrá hacer porque la matriz XS4 negara el servicio lanzando un letrero que dice que no se puede establecer la conexión. En la parte de mensajes se generan todos los eventos registrados entre los mensajes se mostrará la dirección MAC que quiere conectarse, o bien se consigue la dirección en el símbolo del sistema la ruta es la siguiente:

Inicio-> Ejecutar -> cmd escribir el comando ipconfig -all, este mostrará la dirección MAC que es necesaria agregar en la configuración de Xirrus en Security MAC Access List como se muestra en la figura 3.5.3, la manera de agregarlo es en el apartado New MAC Address: 00:1f:3a:82:06:63 y click en el botón Add y se guardará la configuración.

Si se desea negar el servicio se selecciona la MAC a denegar y click en el botón Delete. Una dirección MAC consta de 12 números hexadecimales separados cada dos números por dos puntos.

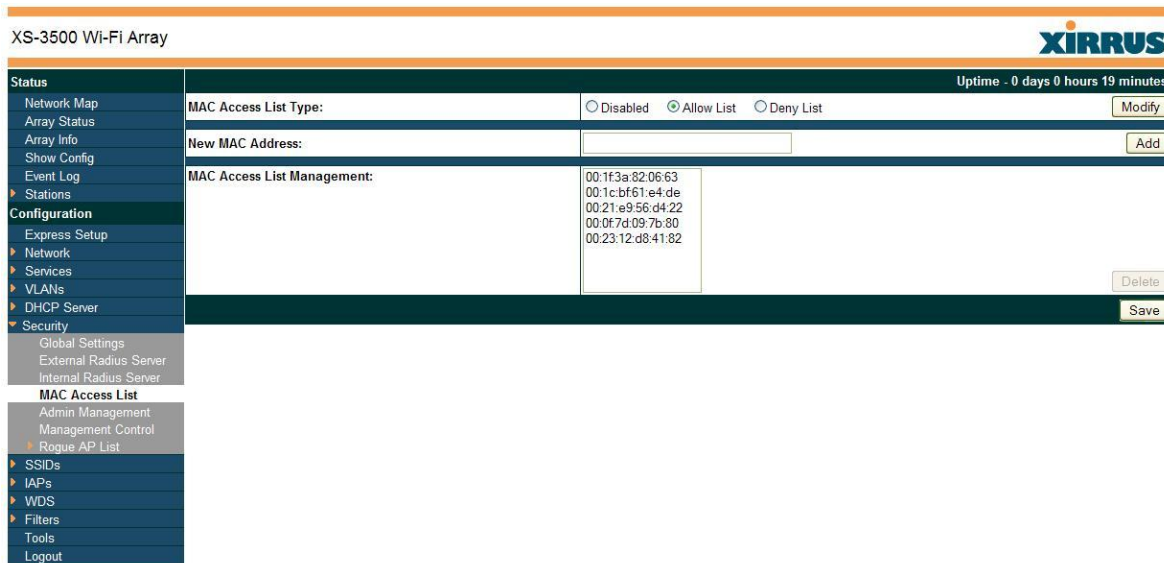


Figura 3.5.3 Lista de direcciones MAC para que un equipo pueda conectarse a esta red.

- Encryption Type: El tipo de encriptación es WPA2 ya que actualmente es el método de encriptación más avanzado la contraseña es **udai2009** esta clave puede ser modificada en cualquier momento cambiando la contraseña en el campo de WPA key.

Los parámetros de la creación de la red pixina pueden ser cambiado en el momento en que se requieran solo el nombre SSID no podrá cambiar.

Para acceder a la red de invitados se deberá de realizar los siguientes pasos:

Identificar la red en la lista de redes inalámbricas, y conectarse a la red pixina. Si se conecta por primera vez acudir al departamento UDAI para que su dirección MAC sea agregada a la lista de MAC Access List.

Se solicitará la clave porque se utiliza WPA2 la clave es udai2009, se confirma y se le da click en el botón conectar.

Como la red está configurada para que la puerta de enlace sea el proxy 10.34.24.252 entonces se deberá activar el proxy en el explorador de windows, para ello se entra en el menú herramientas -> Opciones de Internet -> Conexiones -> Configuración LAN se activa

la casilla de usar un servidor proxy con la dirección: 10.34.24.252 puerto 8080 como se muestra en la figura 3.5.4.



Figura 3.5.4 Activación del Servidor proxy en el explorador de windows.

Cuando termine de ingresar estos datos en su equipo portatil o PDA se podrá realizar el uso del Internet y unicamente le restará la autenticación con el proxy para esto se puede ingresar con el usuario **prueba** y contraseña **prueba**.

Capítulo 4

Pruebas

4.1 Especificaciones

La red Inalámbrica creada para invitados en la Secretaría de Desarrollo Social debe cubrir las siguientes especificaciones:

- Separar la red interna de una red para invitados.
- Asignar direcciones IP automáticamente por DHCP para la red de invitados.
- Implementar seguridad en la red inalámbrica, crear contraseñas WPA.
- Facilitar el acceso de Internet con un ancho de banda de 10 Mbps para usuarios invitados, y 100 Mbps para usuarios privilegiados, (gente que labora en la dependencia).

Para llevar a cabo estas acciones se creó la red “**pixina**” se habilito, es compatible con las bandas de los estándares 802.11a, 802.11b y 802.11g.

4.2 Separación de la red interna con la red para invitados

La separación de la red interna que se ocupa en la dependencia no resulto ser implementada ya que existen 2 rangos que son libres el 10.34.24.00-255 y el 10.34.25.00-255 el más utilizado es 10.34.24 y los equipos que están en el rango 10.34.25 difícilmente pueden acceder a los equipos del otro rango.

La propuesta para la separación de la red es crear una VLAN en la que los equipos de la red para invitados puedan acceder sin problema de que puedan infiltrarse en la red de la dependencia.

4.2.1 Las VPN

Una red privada virtual (Virtual Private Network, VPN) emplea tecnologías de cifrado para crear un canal virtual privado sobre una red de uso público. Las VPN resultan especialmente atractivas para proteger redes inalámbricas, debido a que funcionan sobre cualquier tipo de hardware inalámbrico y superan las limitaciones de WEP. Para configurar

una red inalámbrica utilizando las VPN, debe comenzarse por asumir que la red inalámbrica es insegura. Esto quiere decir que la parte de la red que maneja el acceso inalámbrico debe estar aislada del resto de la red, mediante el uso de una lista de acceso adecuada en un enrutador, o agrupando todos los puertos de acceso inalámbrico en una VLAN si se emplea switching. Dicha lista de acceso y/o VLAN solamente debe permitir el acceso del cliente inalámbrico a los servidores de autorización y autenticación de la VPN.

Deberá permitirse acceso completo al cliente, sólo cuando éste ha sido debidamente autorizado y autenticado.

Los servidores de VPN se encargan de autenticar y autorizar a los clientes inalámbricos, y de cifrar todo el tráfico desde y hacia dichos clientes. Dado que los datos se cifran en un nivel superior del modelo OSI, no es necesario emplear WEP en este esquema. En la figura 4.2.1.1 se muestra la estructura de una VPN para el acceso inalámbrico seguro. [12]

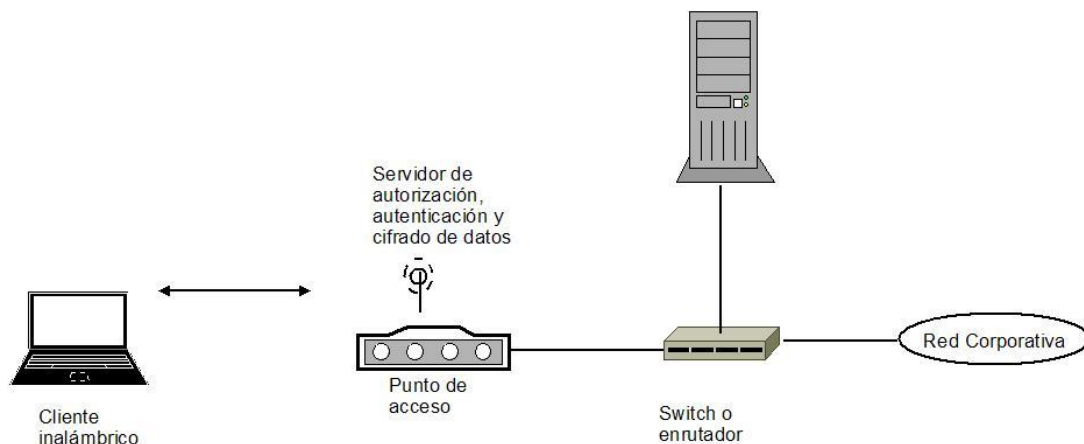


Figura 4.2.1.1 Modelo VPN.

4.2.2 Justificación de las VLAN

La VLAN no se implementó debido a que personal de la dependencia me solicitó que no se crearan las VLAN, esto es porque las personas del rango 10.34.25 no tienen archivos compartidos, y no hay peligro de que puedan ser alterados sus datos, sin embargo el equipo Xirrus soporta el empleo de VLAN y en el momento en que se requieran se pueden configurar sin que se afecte el desempeño de la red para invitados.

4.3 DHCP

Con anterioridad se creó la lista de las direcciones IP libres para la asignación DHCP, que será utilizada en la red para invitados.

Las direcciones que se ocuparon para la red pixina comienzan en 10.34.25.150 y terminan en 10.34.25.255 ofreciendo un total de 105 direcciones de ip libres para ser ocupadas en esta asignación dinámica.

La puerta de enlace puede ser 10.34.24.1 que es la salida directa a finanzas, esta salida permite el uso del Messenger, niega paginas de televisión, algunas descargas y salas de chat, no es necesario hacer más configuraciones.

Otra puerta de enlace es 10.34.24.252, está salida es por medio del proxy y es necesario configurar el explorador en el menú herramientas -> Opciones de Internet -> Conexiones -> Configuración LAN como se muestra en la figura 4.3.1.



Figura 4.3.1 Configuración del servidor proxy en el explorador de Windows.

La conexión por proxy restringe el Messenger, paginas de descarga de programas, salas de chat, entre otras. Para conectarse se solicitara un usuario y contraseña por convención se podrán autenticar como prueba y contraseña prueba.

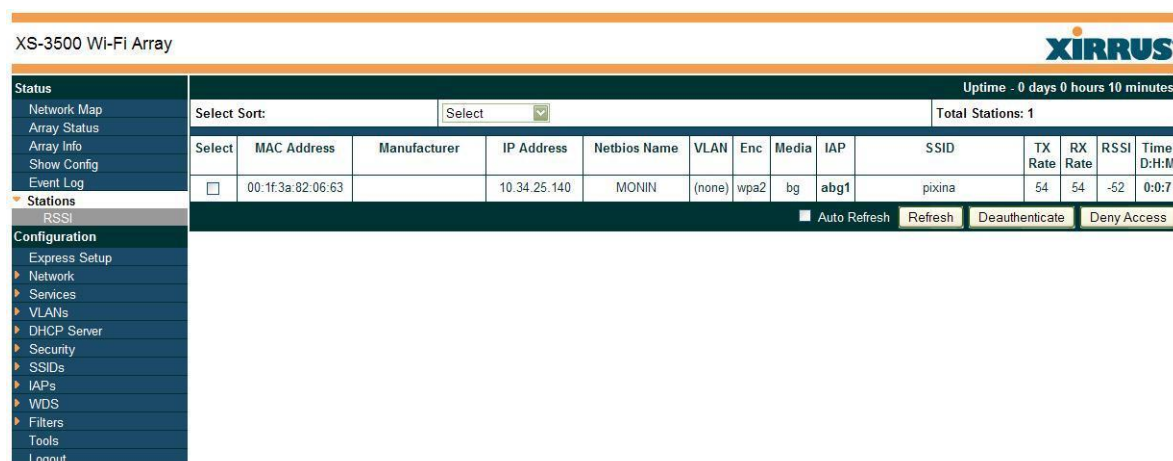
La puerta de enlace para la red de invitados finalmente fue 10.34.24.252 ya que el departamento UDAI así lo especifico para tener un mejor control de los recursos de la red; el inconveniente que encontré es que el usuario que requiera el servicio deberá acudir al

departamento para configurar el proxy y cuando no requiera más del servicio deberá cambiar esta configuración ya que la ninguna otra red pasara por este proxy.

4.4 Seguridad de la red para invitados.

La seguridad en la red inalámbrica pixina se realizó con WPA2, acompañada de la autenticación 802.1X, para que un usuario pueda acceder a la red primero se deberá de registrar su dirección MAC en la interfaz WMI que proporciona Xirrus XS4 3500, ya que si un usuario no autenticado quiere conectarse a la red aunque conozca la contraseña WPA2 no podrá conectarse porque la matriz Xirrus XS4 negara el servicio lanzando un letrero que dice que no se puede establecer la conexión.

Esto es con la finalidad de que se tenga un control de las personas a quienes se les quiere dar el servicio. Para negar el servicio a algún cliente se puede eliminar su dirección MAC o en la parte de Stations se muestran las estaciones conectadas y se pueden Desautenticar seleccionando la casilla correspondiente y después dar click en el botón Deauthenticate, esto negara el servicio temporalmente o si se da click en el botón Deny Access se negará el servicio hasta que se vuelva a admitir su dirección MAC. En la figura 4.4.1 se muestra la pantalla correspondiente para negar el servicio a estaciones del Xirrus XS4 3500.



XS-3500 Wi-Fi Array

Uptime - 0 days 0 hours 10 minutes

Total Stations: 1

Select	MAC Address	Manufacturer	IP Address	Netbios Name	VLAN	Enc	Media	IAP	SSID	Tx Rate	Rx Rate	RSSI	Time D:H:M
☐	00:1f:3a:82:06:63		10.34.25.140	MONIN	(none)	wpa2	bg	abg1	pixina	54	54	-52	0:0:7

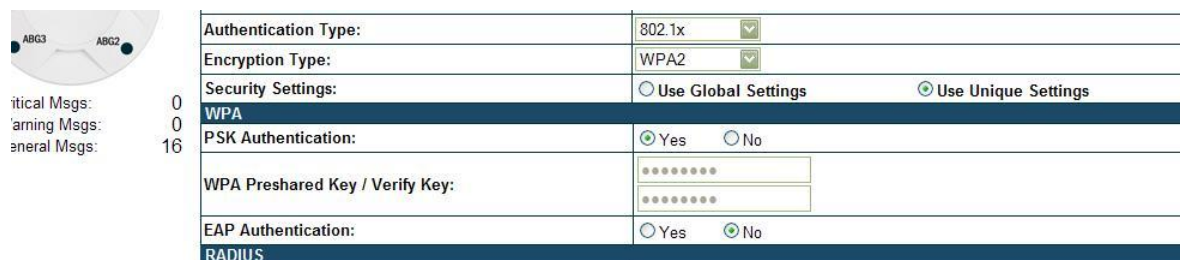
Auto Refresh Refresh Deauthenticate Deny Access

Configuration

- Express Setup
- Network
- Services
- VLANs
- DHCP Server
- Security
- SSIDs
- IAPs
- WDS
- Filters
- Tools
- Logout

Figura 4.4.1 Estaciones conectadas en la matriz Xirrus XS4 3500.

Se estableció la seguridad por medio de WPA2 ya que actualmente es el mejor método de cifrado la contraseña actual es **udai2009** pero esta contraseña puede ser cambiada en cualquier momento dentro de SSID's -> Management se elige la red pixina y en la parte WPA se tiene el campo WPA Preshared Key / Verify Key: donde se ingresa la nueva contraseña y se verifica para comprobar que no se equivoque al ingresar la nueva contraseña se aplican los cambios y se guardan como se muestra en la figura 4.4.2.



Authentication Type:	802.1x
Encryption Type:	WPA2
Security Settings:	☐ Use Global Settings ☒ Use Unique Settings
WPA	
PSK Authentication:	☒ Yes ☐ No
WPA Preshared Key / Verify Key:	
EAP Authentication:	☐ Yes ☒ No
RADIUS	

Figura 4.4.2 Contraseña WPA2 para la red pixina.

4.5 Privilegios del ancho de banda.

Para implementar el cambio del ancho de banda era necesaria la compra de un bus que tendría que ir conectado en la matriz y esta a un enrutador para restringir el ancho de banda. Por falta de recursos no se realizó la compra del equipo requerido pero la limitación del tráfico se pudo implementar gracias a que el equipo Xirrus XS4 3500 puede distribuir el número de paquetes que puede recibir ya sea una SSID o cada estación.

En la opción Traffic Limit per Station: se establecen los paquetes por segundo que recibe una estación. La red pixina se probó con 10 paquetes pero resultó ser un valor demasiado bajo ya que tardaba demasiado tiempo en abrir páginas, luego se probó con 15, con 20, con 25 y con 30 paquetes por segundo.

El valor que mejor se comportó de acuerdo a las peticiones del departamento UDAI fue de 20 paquetes por segundo como se muestra en la figura 4.5.1.

Array Info		SDS_Humboldt (Broadcast)	
Show Config		pixina (Broadcast)	
Event Log			
Stations	SSID:		
Configuration			
Express Setup			
Network			
Services	State:	☒ Enable	☐ Disable
VLANs	Broadcast SSID:	☒ Enable	☐ Disable
DHCP Server	Band Association:	☐ 802.11a	☐ 802.11b/g ☒ Both
Security	QoS Priority:	0	
SSIDs	VLAN ID:	(none)	VLAN Number:
SSID Limits Summary	Internal DHCP Pool Assigned:	ip_otras	
SSID Management	Station Limit:	256	
IAPs	Overall Traffic Limit:	Unlimited: ☒	Packets/Sec:
WDS	Traffic Limit per Station:	Unlimited: ☐	Packets/Sec: 20
Filters			
Tools			
Logout			

Figura 4.5.1 paquetes por segundos que recibe cada estación de la red pixina.

En la figura 4.5.2 se muestra la ventana del estado de la conexión inalámbrica pixina donde se muestra que después de 10 minutos de estar conectado, los paquetes recibidos son aproximadamente el 60% de los paquetes enviados, esto es que no van a la par porque el rendimiento de la red ha descendido.

Estado de Conexiones de red inalámbricas

General Soporte

Conexión:

Estado: Conectado

Red: pixina

Duración: 00:10:25

Velocidad: 54,0 Mbps

Intensidad de señal:

Actividad

Enviados — — Recibidos

Paquetes: 2,626 | 1,591

Propiedades Deshabilitar Ver redes inalámbricas

Cerrar

Figura 4.5.2 Estado de conexiones de red inalámbricas.

El descenso de los paquetes recibidos por estación proporciona la certeza de que un usuario no podrá abusar de los servicios de la red inalámbrica ya que al intentar descargar archivos se muestran leyendas de error como la que se ve en la figura 4.5.3.

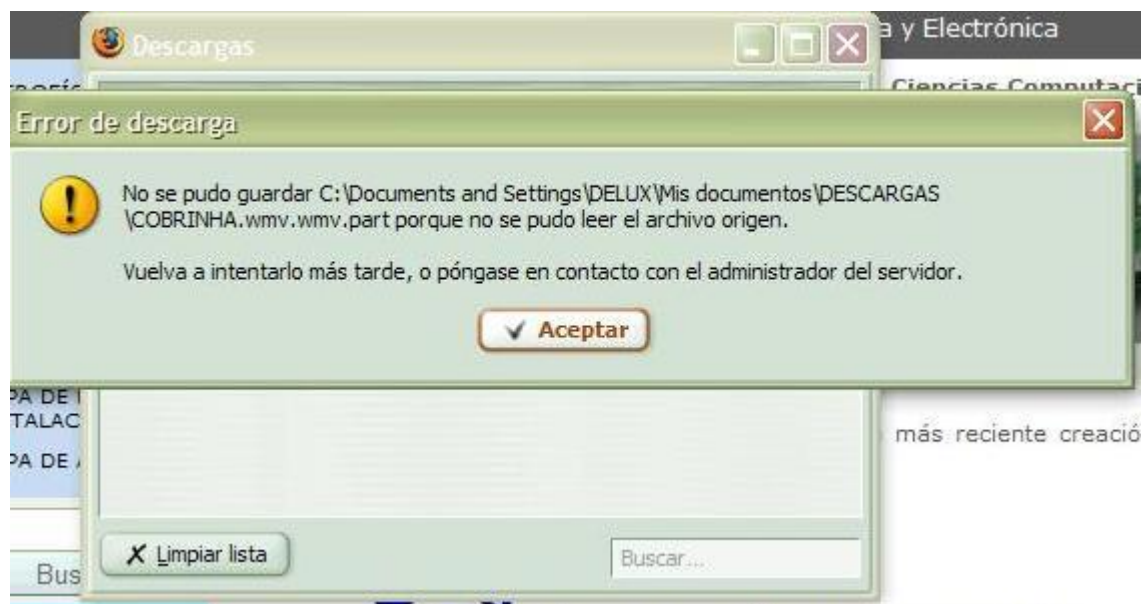


Figura 4.5.3 Error al descargar un archivo dentro de la red pixina.

De esta manera se cumplen todas las especificaciones solicitadas para la implementación de una red inalámbrica para invitados dentro de las instalaciones de la Secretaria de Desarrollo Social.

4.6. Acceso a la red de invitados.

Para poder acceder a la red de invitados "pixina", lo primero es acudir al departamento UDAI para que su dirección MAC sea registrada en la lista de acceso solo para la primera ocasión. UDAI tendrá que activar y desactivar el proxy ya que muchos usuarios no están familiarizados para realizar esta configuración.

Ubicarnos en un lugar que tenga cobertura dentro de las instalaciones de la SDS para identificar la red como se muestra en la figura 4.6.1 y dar click en el botón conectar.

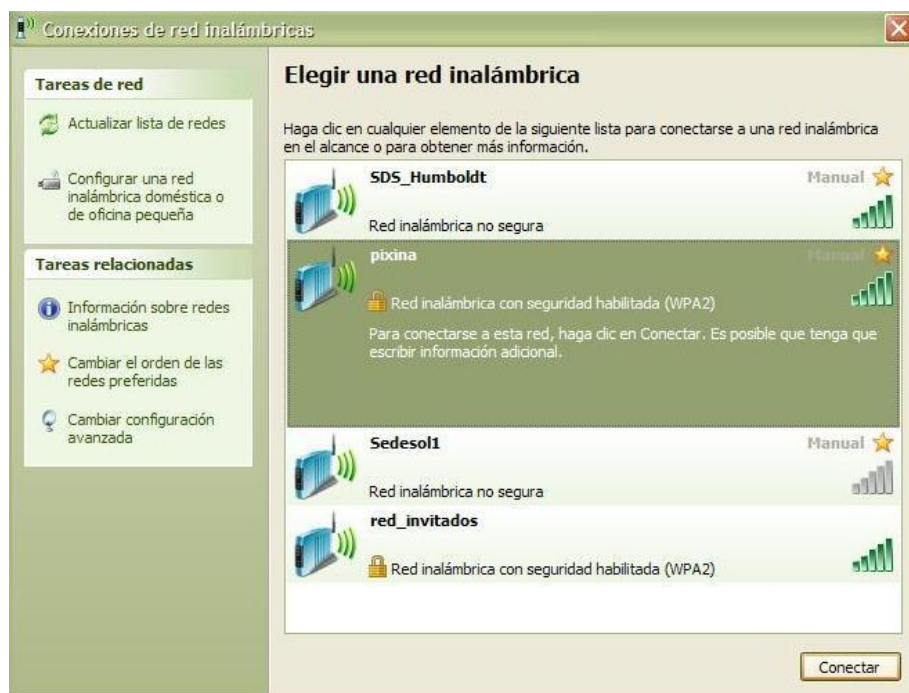


Figura 4.6.1 Lista de redes inalámbricas que están al alcance.

Como la red tiene seguridad WPA2 será necesario ingresar la clave como se muestra en la figura 4.6.2.



Figura 4.6.2 Clave de la red pixina.

En la figura 4.6.3 se muestra la leyenda que muestra que la conexión se ha establecido. Muestra el nombre de la red y la intensidad de la señal.

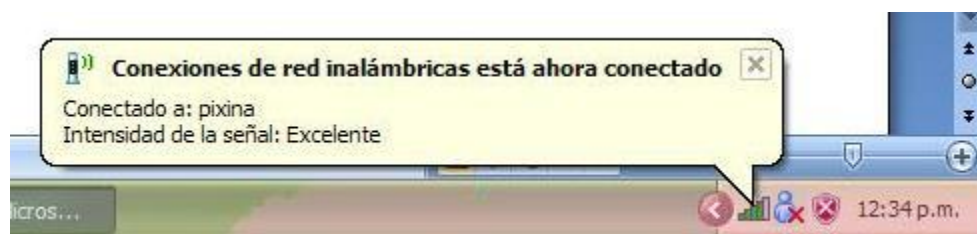


Figura 4.6.3 Icono de la red inalámbrica.

En la figura 4.6.4 se muestra en la parte A) el estado de la conexión donde dice el nombre de la red a la que se está conectado, el tiempo y el número de paquetes enviados y recibidos. En la parte B) se muestra el soporte que le fue dado a la conexión, muestra que la dirección IP fue asignada por DHCP, esta dirección se encuentra en el rango 10.34.25 y la puerta de enlace es por el proxy. En la parte C) se muestran los detalles de la conexión.

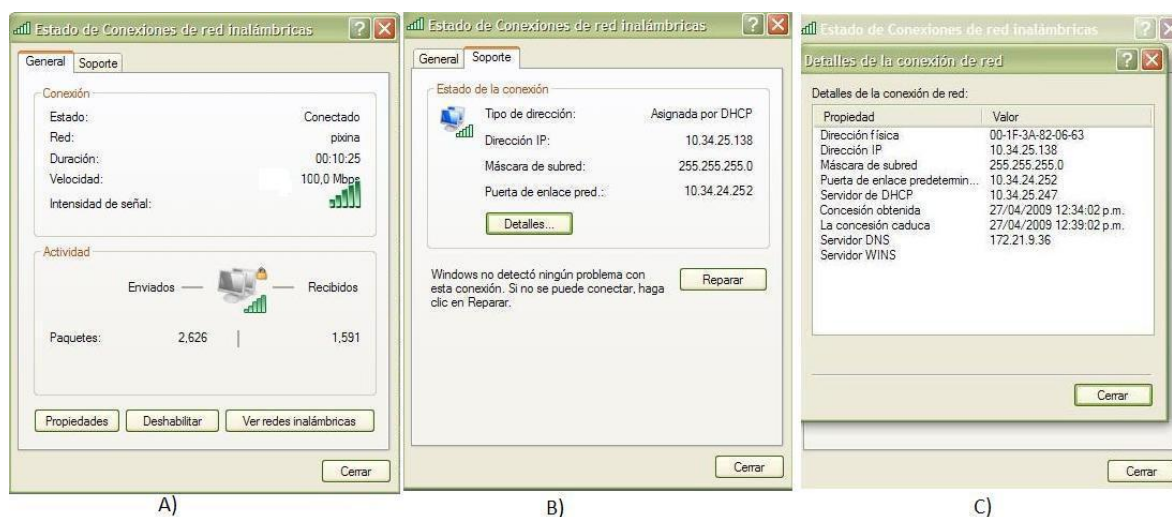


Figura 4.6.4 Detalles de la conexión para usuarios invitados A) estado general, B) soporte de la red pixina, C) Detalles técnicos de la red.

Capítulo 5

Conclusiones

Todas las señales inalámbricas son públicas, para diferenciarlas, interpretarlas y descifrarlas es necesario conocer el método de cifrado que utilizan, los canales y las frecuencias que se emplean. Para que usuarios y proveedores puedan comunicarse son creados los protocolos y los estándares, es decir hablar el mismo idioma.

El separar una red interna de otra involucra la creatividad del administrador de la red inalámbrica, asegurar que una red no pueda ver a la red privilegiada es realmente útil y tiene muchas aplicaciones ya sea en el ámbito laboral, educativo, de gobierno, etc. ya que se tiene la confianza de trabajar en una red interna sin que sea interceptada por usuarios de la red restringida, esto da un ahorro de gastos ya que no será necesario contratar a un segundo proveedor de servicio de Internet para poder brindar una segunda red para usuarios invitados.

La división del ancho de banda en este caso no pudo ser implementada porque implicaba realizar la compra de hubs o datapaths y no había recurso para este gasto. Pero se pudo solucionar esto con la restricción de paquetes en la configuración de la red para invitados, con esto no solo se ahorro en hubs sino que también se tiene la certeza que no se realizarán descargas, ya sea de audio o video; porque como se restringió el servicio a 20 paquetes por segundo la conexión indicará que tuvo fallas de conexión y no descargara la petición que un usuario haya solicitado.

La seguridad es un elemento primordial en el manejo de cualquier red inalámbrica, ya que es nuestro candado de acceso, es por eso que decidí implementar WPA2, que es un método de cifrado bastante bueno y acompañado de la autenticación 802.1X ayuda a identificar a los usuarios para asegurar que solo quienes estén registrados se puedan conectar a la red para invitados y sean las personas a quienes queremos dar el servicio de red.

Un usuario común solo le importa poder conectarse a la red sin dificultades es por eso que la asignación automática de dirección IP es un factor elemental para cualquier red inalámbrica, aunque no fue fácil realizar la tarea implementar una pila de direcciones para DHCP debido a la estructura de la red que se tiene en la SDS es de mucho valor ya que la red para usuarios invitados no tendrá problemas de conexión por falta de direcciones IP.

El único obstáculo que el usuario invitado presentará será el acudir al departamento UDAI para que sea dada de alta su dirección MAC por primera y única vez, y para la activación del servidor proxy.

La ganancia que se obtuvo al mover un arreglo fue de 3 usuarios a 250 usuarios, esto es un avance considerable ya que la dependencia además de brindar un servicio inalámbrico a usuarios invitados también podrá brindar servicio a usuarios que se encuentran en el área de cobertura, la migración de servicio alambicó a inalámbrico no es costosa y por la experiencia de trabajar con el equipo inalámbrico, esté servicio tendrá menos fallas que la red alambrica.

Bibliografía

- [1] Frenzel, Sistemas Electrónicos de Comunicaciones, Editorial Alfaomega, segunda edición, 2003
- [2] Mark Gibbs Todd Brown, Redes para todos, Prentice Hall Hispanoamericana, S.A, segunda edición, 2001
- [3] Tere Parnell Osbone, LAN times guía de redes de alta velocidad, McGraw-Hill, l .
- [4] José A. Carballar, Wi-Fi Cómo construir una red inalámbrica, Alfaomega.
- [5] Matthews S. Gast, Redes Wireless 802.11, editorial ANAYA MULTIMEDIA, 2006.
- [6]http://es.wikipedia.org/wiki/Acceso_m%C3%BAltiple_por_divisi%C3%B3n_de_c%C3%B3digo 12 febrero 2009
- [7] David Roldán Comunicaciones Inalámbricas un enfoque aplicado, Editorial RA - MA, primera edición, 2005
- [8] <http://abadcomputacion.com/redes.html> 1 abril 2009
- [9] <http://igor.tamarapatino.org/escritos/conf/wireless/implantacion.html> 17 marzo 2009
- [10] . <http://technet.microsoft.com/es-es/library/cc736511.aspx> 12 enero 2009
- [11] Manual Xirrus xirrus_array_userguide_3.2-497.pdf,<http://www.xirrus.com/guides/> 4 febrero 2009
- [12]Madrid Molina Juan Manuel,Seguridad en redes inalambricas 802.11,paper de la universidad Icesi,colombia, 2004
http://dspace.icesi.edu.co/dspace/bitstream/item/888/1/sist_telema3.pdf 23 marzo 2009