Telefonía básica con voz sobre IP en una plataforma inalámbrica Wi-Fi

Práctica Profesional (Cód. 0047)

Alumno: Gustavo Mario Salvucci

Tutores: Héctor Magnago, Leonardo Torrella

Lugar de trabajo: InterWave Global S.A

Marzo de 2004
Facultad de Ingeniería
Universidad Nacional de Río Cuarto

Resumen

Este proyecto consiste en el diseño de una red que permita la provisión de servicios telefónicos básicos e Internet de banda ancha en la zona céntrica y algunos barrios de la ciudad de Córdoba aplicando conjuntamente las tecnologías de Voz sobre IP y WLAN.
Mi participación en este trabajo se limita a la colaboración en el diseño de la cobertura del sistema, la configuración de los distintos dispositivos que integran el mismo y la instalación de los puntos de acceso como así también de algunos puntos terminales.

La arquitectura de la red esta compuesta por 2 puntos de acceso primarios, denominados ***MAP*** (Master Access Point), que cumplen la función de realizar la acometida a los usuarios mediante la tecnología WLAN y conectar la red de distribución inalámbrica a Internet.

Otro componente de la red que permite extender la cobertura del sistema es el ***Repeater***. Este termino se refiere al dispositivo que se utiliza para realizar la acometida a los usuarios, pero a diferencia del MAP no se conecta directamente a Internet. El Repeater enruta su trafico hacia Internet a través del MAP. Estos dos componentes son utilizados para brindar el servicio de acceso a los usuarios.

Los componentes de la red que se instalan en la ubicación del usuario son dos; el primero de ellos se denomina ***nodo semifijo*** y como su nombre lo indica, permite que el usuario acceda a los servicios del sistema desde distintas ubicaciones.
El segundo dispositivo se denomina ***nodo fijo*.** El mismo, cumple la misma función que el nodo semifijo, pero a diferencia de este no puede ser trasladado de su lugar de fijación.
El trafico, autenticación y tarifación de las llamadas telefónicas a través de Internet esta a cargo de la empresa VoIP Group Inc.

En cuanto al servicio de Internet de banda ancha, se debe mencionar que esta pensado para que accedan al mismo los usuarios a través de los nodos fijos y semifijos como así también cualquier persona que posea una computadora o notebook con un adaptador de red inalámbrico. Es decir, que el servicio de Internet no posee ningún tipo de encriptación, con lo cual cualquier usuario puede acceder al mismo. Una vez que el cliente accedió al sistema y quiere ingresar a cualquier sitio Web, es dirigido hacia un **portal captivo,** donde debe ingresar un nombre de usuario y una contraseña para poder acceder a todos los servicios de Internet (excepto telefonía IP).

En un futuro esta pensado ampliar la cobertura del sistema a la mayor parte de la ciudad de Córdoba.

Este proyecto contribuye al crecimiento de las redes WLAN, las cuales en un futuro podrían ser una alternativa real a la tercera generación de telefonía móvil, debido a que estas tecnologías son de unas posibilidades mayores que el propio UMTS.

Descripción del lugar de trabajo

Este proyecto fue desarrollado en su mayor parte en la empresa InterWave Global, la cual esta ubicada en la Avenida Colon 778, piso 7 de la ciudad de Córdoba. Sin embargo, la propietaria del sistema es la empresa DSC (Diagonal Sur Comunicaciones).

InterWave se dedica principalmente a los e-services y la mensajeria electrónica.

Esta empresa posee una experiencia probada en el área de la informática aplicada y las telecomunicaciones.

En su cartera de clientes figuran empresas de la talla de Cadena 3, Shoping Patio Olmos, UES 21, Viano Sociedad de Bolsa y Metrovias. también proyectó soluciones integrales en grandes proyectos para Arcor y AGD.

En las instalaciones de esta empresa se realizaron las distintas pruebas de configuración de los equipos, como así también el ensamblaje de los dispositivos que fueron colocados en los distintos MAP, Repeaters y usuarios finales.

Indice

1 Introducción

Debido al crecimiento de las redes de IP, cuya presencia es universal en todos los host, el desarrollo de tecnologías avanzadas para la digitalización, compresión y codificación de la voz, mecanismos de control y priorización de tráfico en las redes, protocolos de transmisión en tiempo real, así como la aparición de nuevos estándares, han creado un entorno donde es posible transmitir telefonía sobre redes de paquetes.

Basándose en este concepto es posible la transmisión de señales de voz con una calidad ligeramente inferior a la de la red telefónica publica, pero con la ventaja de que el costo de la llamada es bastante inferior a la de esta ultima, especialmente en lo que se refiere a llamadas de larga distancia.

Otra tecnología que esta evolucionando rápidamente es Wi-Fi (Wireless Fidelity). La misma permite la comunicación de los distintos hosts de una red con una velocidad de hasta 108 Mbps en un medio inalámbrico. La comunicación entre los distintos hosts se realiza mediante ondas de RF a una frecuencia de 2,4 GHz o 5 GHz. Estas dos bandas de frecuencia son no licenciadas, lo que significa que no se debe pagar ningún canon por utilizar la misma. Sin embargo el usuario de esta frecuencia no esta protegido por ninguna normativa.

La intención de este proyecto es brindar telefonía IP a los usuarios realizando el enlace entre los puntos de acceso a la red y el usuario final utilizando la tecnología Wi-Fi en la banda de 2,4 GHz.

Este sistema hace uso de la especificación H.323 para la transmisión de las señales de Voz sobre IP. La topología de H.323 consta de terminales, gateways, gatekeepers y unidades de control multipunto (MCU). Los terminales, a los que se denomina puntos finales, proporcionan conferencias punto a punto y multipunto para audio y de manera opcional, video y datos. Los gateways son los encargados de interconectar la Red Publica de telefonía Conmutada (PSTN) a la red de datos. Los gatekeepers proporcionan el control de admisión y servicios de traducción de direcciones para terminales o gateways. Por ultimo, las MCU son dispositivos que permiten que dos o mas terminales o gateways realicen conferencias con sesiones de audio y/o video.

Hasta el momento la arquitectura del sistema esta compuesta por

- Un Gatekeeper y dos gateways.
- 2 puntos de acceso primario (MAP)
- 1 Repeater
- 10 nodos semifijos.
- Dos servidores de acceso.

Como se menciono anteriormente, el Gatekeeper es el cerebro de la red de telefonía IP y el Gateway es el dispositivo que interconecta Internet con la PSTN. La provisión y configuración de estos artefactos esta a cargo de la empresa VoIP Group INC. Cuya casa central esta ubicada en la Avenida Hipólito Irigoyen 146 piso 2, de la ciudad de Córdoba.

Los MAP cumplen la función de realizar la acometida a los usuarios mediante la tecnología WLAN y conectar la red de distribución inalámbrica a Internet. Esta conexión se realiza a través de los servidores de acceso.

Los repeaters cumplen la función de extender el rango de cobertura del sistema. Estos son idénticos a los MAPs, con la única diferencia de que no poseen servidores de acceso con una conexión a Internet. El Repeater dirige todo su trafico a Internet a través del MAP. Conectándose con este ultimo a una velocidad de 11 Mbps.

Los servidores de acceso se utilizan para realizar la autenticación y el accounting de los usuarios de los servicios de Internet (exceptuando H.323) a través de un portal captivo. Además, los mismos cumplen la función de NAT (Network Address Translator).
Se coloca un servidor de acceso por cada MAP que existe en el sistema, de manera que cada servidor maneje una cantidad de usuarios adecuada y no se sature por tener que procesar los parámetros de demasiados usuarios.

Los puntos finales de la red son los Nodos fijos, semifijos. El primero de ellos permite que el usuario acceda a los servicios del sistema desde distintas ubicaciones. El segundo cumple la misma función que el primero, pero a diferencia de este no puede ser trasladado de su lugar de fijación. Estos nodos se encargan de brindar telefonía e Internet de banda ancha a los usuarios.

En un primer momento se pensó implementar un teléfono IP móvil. Para ello se adquirieron dos teléfonos marca Móvil Netvision que se evaluaron en distintas situaciones. El resultado de las pruebas no fue satisfactorio, ya que este teléfono funciona solo si se tiene una línea de visión directa con la antena transmisora.
Como consecuencia de estas pruebas se decidió no implementar los mismos, debido a que no se acercan a la prestación de un teléfono celular.

Todo el sistema es monitoreado en un centro de cómputos (NOC), donde además se realiza la actualización del firmware de los equipos y en un futuro se realizara la tarifación correspondiente a Internet.

2 Descripción del Standard H.323

H.323 es una especificación de la ITU-T para transmitir audio, video y datos a través de una red IP. El estándar H.323 dirige la señalización y control de llamadas, transporte y control multimedia y control de ancho de banda para conferencias punto a punto y punto multipunto.

2.1 Componentes de un sistema H.323

Los componentes de un sistema H.323 son 4:

- Terminales.
- Gateways.
- Gatekeepers
- Unidades de control punto multipunto.

Terminales

Un *terminal* H.323 es un extremo de la red que proporciona comunicaciones bidireccionales en tiempo real con otro terminal H.323, gateway o unidad de control multipunto (MCU). Esta comunicación consta de señales de control, indicaciones, audio, imagen en color en movimiento y /o datos entre los dos terminales. Conforme a la especificación, un terminal H.323 puede proporcionar sólo voz, voz y datos, voz y vídeo, o voz, datos y vídeo.

El funcionamiento de todo terminal debe incluir el tratamiento necesario de la señal para su envío por la red de datos. Deben realizar la captación, digitalización, y compresión de la señal de forma que la carga a soportar por toda comunicación este repartida entre los diversos terminales.

Existen principalmente dos tendencias en este tipo de elementos, terminales hardware y terminales software.

Tanto la apariencia, como la funcionalidad de cara al usuario de los terminales hardware es igual a los teléfonos actuales. Esto permite eliminar la desconfianza inicial que puede producir el cambio. Ya existen en el mercado terminales que se conectan directamente a la red local. Por otro lado los terminales software ejecutándose en un host pueden producir un mayor rechazo inicial en el usuario, pero las capacidades del software pueden ser muy superiores.

Las funciones de digitalización y compresión de voz la realizan los *codecs.* Básicamente, un codec, realiza la conversión de la señal de voz analógica a una señal digital PCM (Pulse Code Modulation) de 64 Kbps y luego la compresión de esta señal digital en otra con un bit rate mas bajo.

Los codecs son clasificados en tres tipos:

- Codificadores de forma de onda.

- Vocoders.
- Codificadores híbridos.

Los codificadores de forma de onda reproducen la onda analógica tan parecida como sea posible, incluyendo el ruido de fondo. Estos codecs son de alta calidad, pero tienen el inconveniente de tener un alto bit rate.

Los vocoders no reproducen la señal original. En lugar de esto, el codificador construye un set de parámetros, el cual es enviado al receptor, que lo usa para construir la señal de voz.

Por ultimo, los codificadores híbridos combinan la calidad de los codificadores de forma de onda con el bajo bit rate de los vocoders.

La siguiente tabla muestra los codecs aceptados en el estándar H.323.

Codec	Tipo	Bit Rate
G.711	Codificador de forma de onda	64 Kbps
G.729A	Hibrido	8 Kbps
G.723.1	Hibrido	6,4 kbps
G.723.1	Hibrido	5,3 Kbps

Gateways

Un gateway H.323 es un extremo que proporciona comunicaciones bidireccionales en tiempo real entre terminales H.323 en la red IP y otros terminales o gateways en una red conmutada. En general, el propósito del gateway es reflejar transparentemente las características de un extremo en la red IP a otro en una red conmutada y viceversa. En otras palabras, nos servirá de pasarela entre el entorno de vídeo sobre IP H.323 y el entorno vídeo sobre RDSI H.320.

Los Gateways no son necesarios a menos que se requiera la interconexión con la Red de telefonía publica conmutada. Por lo tanto, los terminales H.323 pueden comunicarse directamente sobre la red de paquetes sin conectarse con un Gateway. El Gateway actúa como un terminal H.323 o MCU en la red IP y un terminal telefónico en la red de telefonía publica.

Gatekeepers

Dentro del esquema de Voz sobre IP, la funcionalidad principal que debe ofrecer todo gatekeeper se basa en el control de llamadas y gestión del sistema de direccionamiento, pero el conjunto de tareas puede ser el más importante de todo el sistema.

Aunque los terminales pueden conectarse directamente sin intervención del gatekeeper, este tipo de funcionamiento es muy limitado y difícil para el usuario. La potencia real del sistema se pone de manifiesto cuando dentro de cada zona H.323 existe el correspondiente gatekeeper. Todo terminal antes de realizar una llamada, debe consultar con el gatekeeper si esta es posible. Una vez obtenido permiso, el gatekeeper es quien realiza la traslación entre el identificador de usuario destino y la dirección IP equivalente.

Establecida la comunicación entre los terminales, el gatekeeper no necesita intervenir, con lo que la carga del sistema se reparte entre los terminales.

Todo este proceso se inicia con el registro de los diversos terminales durante la iniciación de estos. De esta forma no tenemos ningún problema de movilidad de los diversos puestos y usuarios. Incluso los distintos terminales pueden obtener direcciones dinámicas mediante DHCP. Este registro permite realizar la traslación antes señalada entre los identificadores de usuario y su localización física de forma automática.

Es la responsabilidad principal del gatekeeper mantener un control de todo el tráfico generado por las diversas comunicaciones, a efectos de mantener un nivel aceptable de saturación de la red. El control de ancho de banda permite al administrador fijar un límite de utilización, por encima del cual se rechazan las llamadas bien sean internas o externas.

Otro aspecto importante que debe manejar el gatekeeper es el enrutamiento de las llamadas. De esta forma, el propio gatekeeper puede redireccionar las llamadas al gateway mas indicado o elegir un nuevo destino sí el original no esta disponible. En este punto es donde una solución software puede dotar al administrador del sistema de herramientas potentes de control y definición de reglas.

En cuanto a otras capacidades añadidas, podemos pensar en el control de costos de llamadas, control de centros de atención al cliente, etc.

Unidad de control multipunto (MCU)

La unidad de control multipunto soporta multiconferencia entre tres o mas terminales y gateways. El MCU consiste de un controlador multipunto (MC) y un procesador multipunto opcional (MP).

El MC soporta la negociación de capacidades con todos los terminales para asegurar un nivel de comunicación común y también puede controlar los recursos en una operación multicast. El MC no es capaz de mezclar trafico de voz, video y datos. Sin embargo, el MP puede realizar estos servicios.

El MP es el procesador central de los flujos de voz, video y datos en una conferencia multipunto.

La siguiente figura muestra como interactúan los componentes de un sistema H.323.

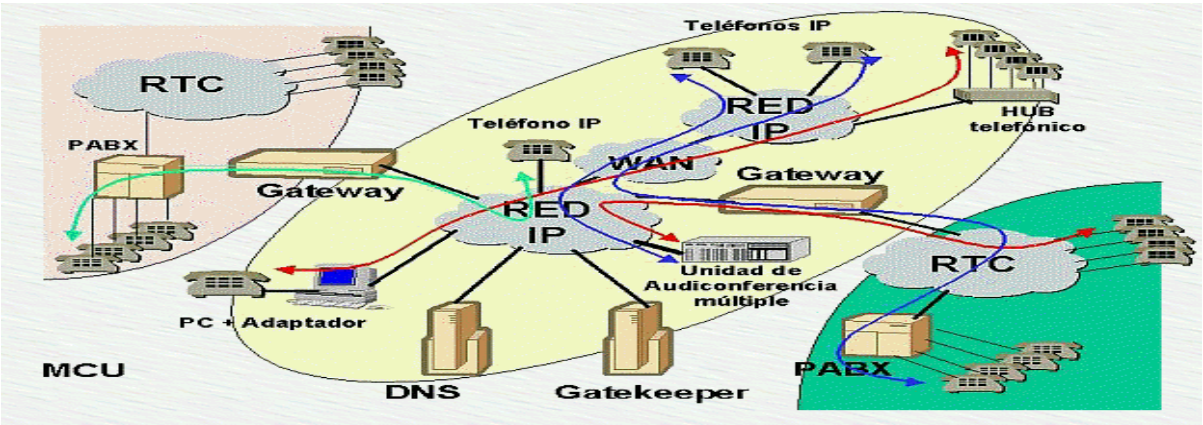


Figura 2.1 Componentes de un sistema H.323

El protocolo H.323 esta dividido en tres áreas de control principales:

- Señalización de registro, admisión y estado (RAS). Proporciona un control de prellamadas en las redes basadas en un gatekeeper H.323.
- Señalización de control de llamadas. Se utiliza para conectar, mantener y desconectar llamadas entre puntos finales.
- Control y transporte de medios. Proporciona el canal H.245 seguro que transporta los mensajes de control de los medios. El transporte ocurre con un flujo UDP no seguro.

La siguiente figura muestra el stack de protocolos H.323

Figura 2.2 Stack de protocolos H.323

2.2 Señalización RAS

La señalización RAS proporciona un control de prellamadas en las redes H.323 donde existen gatekeepers y una zona. El canal RAS se establece entre puntos finales y gatekeepers a través de una red IP. El canal RAS esta abierto antes de que ningún otro canal sea establecido, y es independiente de la señalización de control de llamadas y de los canales de transporte de medios. Esta conexión UDP no segura transporta los mensajes RAS que realizan el registro, las admisiones, los cambios del ancho de banda, el estado y los procedimientos de finalización.

Descubrimiento del gatekeeper

El descubrimiento del gatekeeper es un proceso manual o automático que los puntos finales utilizan para identificar con que gatekeeper registrarse. En el método manual, los puntos finales están configurados con la dirección IP del gatekeeper, por lo tanto puede intentar el registro inmediatamente, pero únicamente con el gatekeeper predefinido. El

método automático permite que la relación entre puntos finales y gatekeepers cambie a lo largo del tiempo y requiere un mecanismo conocido como autodescubrimiento.

El autodescubrimiento permite que un punto final, que tal vez no conozca a su gatekeeper, pueda descubrirlo a través de un mensaje de multidifusion.

La dirección de difusión del descubrimiento de gatekeeper es 224.0.1.141, el puerto de descubrimiento UDP del gatekeeper es 1718, y el puerto de estado y registro UDP del gatekeeper es 1719. Se utilizan tres mensajes RAS para el autodescubrimiento del gatekeeper:

- Gatekeeper Request (GRQ): Mensaje de multidifusion enviado por un punto que esta buscando al gatekeeper.
- Gatekeeper Confirm (GCF): Respuesta a un GRQ de punto final que indica la dirección de transporte del canal RAS del gatekeeper.
- Gatekeeper Reject (GRJ): Avisa al punto final de que el gatekeeper no quiere aceptar su registro. Normalmente se debe a una configuración en el gateway o gatekeeper.

Registración

El registro es el proceso que permite que los gateways, terminales y MCU alcancen una zona e informen al gatekeeper de sus direcciones IP y alias. El registro, que es un proceso necesario, ocurre después del proceso de descubrimiento, pero antes de que se intente realizar ninguna llamada. Se pueden utilizar los seis mensajes siguientes para permitir que un punto final registre y cancele registros.

- Registration Request (RRQ): Enviado desde un terminal a la dirección del cana RAS del gatekeeper.
- Registration Confirm (RCF): Enviado por el gatekeeper, confirma un registro de punto final.
- Registration Reject (RRJ): Enviado por el gatekeeper, rechaza un registro de punto final.
- Unregister Request (URQ): Enviado desde un punto final o gatekeeper para cancelar un registro.
- Unregister Confirm (UCF): Enviado desde un punto final o gatekeeper para confirmar la cancelación de un registro.
- Unregister Reject (UR): Indica que el punto final no estaba prerregistrado con el gatekeeper.

Localización de punto final

Los puntos finales y gatekeepers utilizan la localización de punto final para obtener información de contacto cuando solo esta disponible la información de alias. Los mesajes locates son enviados a la dirección de difusión de descubrimieno del gatekeeper. El gatekeeper responsable del punto final solicitado responde indicando su propia información de control o la del punto final.

El punto final o gatekeeper puede incluir una o mas direcciones E.164 fuera de la zona en la petición. Se pueden utilizar los siguientes tres mensajes para localizar puntos finales:

- LRQ: Se envia para solicitar información de contacto del punto final o gatekeeper para una o mas direcciones E.164.
- LCF: Se envía por el gatekeeper y contiene el canal de señalización de llamadas o dirección del canal RAS de si mismo o del punto final solicitado. Utiliza su propia dirección cuando se utiliza GKRCS y la dirección del punto final solicitado cuando se utiliza la Señalización de llamada directa de punto final (Direct Endpoint Call Signaling).
- Location Request (LRJ): Se envia por los gatekeepers que reciben un LRQ para el que no esta registrado el punto final solicitado o tiene recursos no disponibles.

Admisión

Los mensajes de admisión entre puntos finales y gatekeepers proporcionan las bases para la admisión de llamadas y control de ancho de banda. Los gatekeepers autorizan el acceso a redes H.323 confirmando o rechazando una petición de admisión. Una petición de admisión incluye el ancho de banda solicitado, que puede ser reducido por el gatekeeper en la confirmación. Los siguientes mensajes proporcionan control de admisión en las redes H.323:

- ARQ: Un intento realizado por un punto final para iniciar una llamada.
- ACF: Una autorización dada por el gatekeeper para admitir la llamada.
- ARJ: Deniega la petición del punto final de tener acceso a la red para esta llamada determinada.

El mensaje ACF contiene la dirección IP del gateway o gatekeeper de terminación y permite que el gateway de origen inicie inmediatamente los procedimientos de señalización de control de llamadas.

Información de estado

El gatekeeper puede utilizar el canal RAS para obtener información de estado desde un punto final. Podemos utilizar este mensaje para monitorizar si el punto final esta en línea o no debido a una condición de fallo. El periodo típico de sondeo para los mensajes de estado es de 10 segundos. Durante la ACF, el gatekeeper puede también solicitar que el punto final envié mensajes de estado periódicos durante una llamada. Podemos utilizar los tres mensajes siguientes para proporcionar el estado en el canal RAS:

- Information Request (IRQ): Se envia desde el gatekeeper al punto final que solicita el estado.

- Information Request Response (IRR): Se envia desde el punto final al gatekeeper en respuesta a una petición de información IRQ. Este mensaje es también enviado desde un punto final si el gatekeeper solicita actualizaciones periódicas de estado.
- Status Enquiry: Se envia fuera del canal RAS en el canal de señalización de llamadas. Un punto final o gatekeeper puede enviar mensajes Status Enquiry a otro punto final para verificar el estado de la llamada. Los gatekeepers suelen utilizar estos mensajes para verificar si las llamadas siguen activas.

Control de ancho de banda

El control de ancho de banda se administra inicialmente a través del intercambio de admisiones entre un punto final y el gatekeeper en una secuencia ARQ/ ACF/ ARJ. Sin embargo, el ancho de banda puede cambiar durante una llamada. Podemos utilizar los siguientes mensajes para cambiar el ancho de banda:

- BRQ: Es enviado por un punto final al gatekeeper pidiendo un incremento o disminución en el ancho de banda de la llamada.
- BCF: Es enviado por el gatekeeper para confirmar la aceptación de la petición de cambio de ancho de banda.
- BRJ: Es enviado por el gatekeeper para rechazar la petición de cambio de ancho de banda (enviada si el ancho de banda solicitado no esta disponible).

Señalización de control de llamadas (H.225)

En las redes H.323, los procedimientos de control de llamadas en la recomendación H.225 de la ITU-T, que especifica la utilización y soporte de los mensajes de señalización Q.931. Un canal de control de llamadas seguro se crea en una red IP en el puerto 1720 del TCP. Este puerto inicializa los mensajes de control de llamadas Q.931 entre dos puntos finales para el propósito de conectar, mantener y desconectar las llamadas.

El control de llamadas real y los mensajes de actividad se mueven a puertos efímeros después de configurar la llamada inicial. Pero 1720 es el puerto que se conoce para las llamadas H.323. H.225 también especifica la utilización de los mensajes Q.932 para los servicios suplementarios. Los siguientes mensajes Q.931 y Q.932 son los mensajes de señalización mas utilizados en las redes H.323:

- Setup: Un mensaje hacia delante enviado por la entidad H.323 que llama en un intento de establecer conexión con la entidad H.323 llamada. Este mensaje se envia en el puerto TCP 1720 de H.225.
- Call Proceeding: Un mensaje hacia atrás enviado desde la entidad llamada a la entidad que llama para avisar que los procedimientos de establecimiento de llamado se han iniciado.
- Alerting: Un mensaje hacia atrás enviada desde la entidad llamada para avisar a la parte llamada que el sonido de llamada se ha iniciado.
- Connect: Un mensaje hacia atrás enviado desde la entidad llamada a la entidad llamante indicando que la parte llamada ha respondido a la llamada. El mensaje de

conexión puede contener la dirección de transporte UDP/ IP para la señalización de control H.245.

- Release complete: : Enviado por el punto final que inicia la desconexión, que indica que la llamada ha sido liberada. Se puede enviar este mensaje únicamente si el canal de señalización de la llamada esta abierto o activo.
- Facility: Un mensaje Q.932 utilizado para solicitar o confirmar servicios suplementarios. también se utiliza si una llamada debe ser dirigida o debe ir a través de un gatekeeper.

Se puede enrutar el canal de señalización de la llamada en una red H.323 de dos maneras: a través de señalización de la llamada directa de punto final (Direct Endpoint Call Signaling) y de Señalización de llamada de gatekeeper enrutado (GKRCS). En el método de Señalización de llamada directa de punto final, los mensajes de señalización se envían directamente entre los dos puntos finales.

En el método GKRCS, los mensajes de señalización de las llamadas entre los puntos finales son enrutados a través del gatekeeper.

Se pueden ofrecer servicios suplementarios a través del método GKRCS si el canal de señalización de la llamada permanece abierto durante la misma. Los gatekeepers también pueden cerrar el canal de señalización de la llamada después de que se haya completado su configuración.

2.3 H.245 y RTP/ RTCP

H.245 maneja mensajes de control de extremo a extremo entre entidades H.323. Los procedimientos H.245 establecen canales lógicos para la transmisión de información de audio, video, datos y canal de control. Un punto final establece un canal H.245 para cada llamada con el punto final que esta participando. El canal de control seguro se crea sobre IP utilizando el puerto TCP dinámicamente asignando en el ultimo mensaje de señalización de llamada.

El intercambio de capacidades, la apertura y cierre de canales lógicos, los modos de preferencia y el control de los mensajes ocurren sobre este canal de control. H.245 también permite el intercambio de capacidades separadas para la transmisión y recepción, así como la negociación de las funciones, como determinar que codec se debe usar.

Si utilizamos la señalización de llamadas de gatekeeper enrutado, podemos controlar el enrutamiento del canal de dos maneras: utilizar Direct H.245 Control, que tiene lugar directamente entre dos puntos finales participantes , o bien utilizar Gatekeeper Routed H.245 Control, que tiene lugar entre cada punto final y su gatekeeper.

Podemos hacer uso de los siguientes procedimientos y mensajes para permitir la operación de control H.245:

- Capability Exchange: Consiste en mensajes que intercambian de manera segura las capacidades entre dos puntos finales. Estos mensajes indican capacidades del terminal para transmitir y recibir audio, video y datos al terminal que esta participando. Para audio, el intercambio de capacidades incluye codecs de transcodificacion de voz de la serie G. también incluye las velocidades de muestreo de las series de la ISO IS.111723 con 32; 44,1 y 48 KHz, e IS.13818-3 con 16;

22,05; 24; 32; 44,1 y 48 KHz; así como los codecs de audio de voz de tasa completa, tasa media y tasa mejorada de GSM.

- Master- Slave Termination: Son procedimientos utilizados para determinar que punto final es el principal (master) y que punto final es el secundario (slave) para una llamada determinada. La relación se mantiene durante la duración de la llamada y se utiliza para resolver conflictos entre puntos finales. Las reglas master-slave se utilizan cuando ambos puntos finales solicitan acciones similares a la vez.
- Round-Trip Delay: Son procedimientos utilizados para determinar el retraso entre los puntos finales de origen y de terminación. El mensaje Round-Trip Delay Request mide el retraso y verifica si la entidad remota del protocolo H.245 esta activa.
- Logical Channel Signaling: Abre y cierra el canal lógico que transporta la información de audio, video y datos. El canal se prepara antes de la transmisión real para asegurar que los terminales están preparados y son capaces de recibir y decodificar información. Los mismos mensajes de señalización establecen los canales unidireccionales y bidireccionales. Cuando se ha establecido la señalización de canal lógico con éxito, el puerto UDP para el canal de medios RTP es pasado desde el punto final de terminación hasta el punto final de origen. Asimismo, cuando se utiliza el modelo Gatekeeper Call Routed, es en este punto donde el gatekeeper puede desviar los flujos RTP proporcionando la dirección UDP/ IP real del punto final de terminación.

Tunneling H.245

Se pueden encapsular mensajes H.245 dentro del canal de señalización de llamadas H.225 en lugar de crear un canal de control H.245 separado. Este método mejora el tiempo de conexión de llamada y la asignación de recursos, y proporciona una sincronización entre la señalización y el control de llamadas. Se pueden encapsular múltiples mensajes H.245 en un mensaje H.225. Asimismo, en cualquier momento un punto final puede conmutar con una conexión H.245 separada.

Terminación de llamada

Cualquier punto final que participe en una llamada puede iniciar el procedimiento de terminación de llamada. En primer lugar, deben cesar las transmisiones de medios (como audio, video o datos) y cerrarse todos los canales lógicos. A continuación, debe finalizar la sesión H.245 y enviarse un mensaje de liberación completa en el canal de señalización de llamada, si sigue estando abierto o activo. En ese momento, si ningún gatekeeper esta presente, se termina la llamada. Cuando un gatekeeper esta presente, se utilizan los siguientes mensajes en el cana RAS para completar la terminación de llamada:

- Disange Request (DRQ): Se envia por un punto final o gatekeeper para terminar una llamada.
- Disengage Confirm (DCF): Se envia por un punto final o gatekeeper para confirmar la desconexión de la llamada.

- Disengaje Reject (DRJ): Se envia por el punto final o gatekeeper para rechazar la desconexión de la llamada.

Transporte de medios (RTP/ RTCP)

RTP proporciona transporte de medios en H.323. De manera mas especifica, RTP permite la entrega de extremo a extremo en tiempo real de audio, video y datos interactivos sobre redes de unidifusion o multidifusion. Los servicios de empaquetamiento y transmisión incluyen la identificación de carga útil, la secuenciación, la marca de temporizacion y la monitorización.
RTP depende de otros mecanismos y de las capas bajas para asegurar la entrega a tiempo, la reserva de recursos, la fiabilidad y la QoS. RTCP monitoriza la entrega de datos y controla e identifica los servicios. El canal de medios se crea utilizando UDP, donde los flujos RTP actúan en un numero de puerto par y el flujo RTCP correspondiente actúan en el siguiente numero de puerto mas alto (impar).

3 Descripción de la tecnología WLAN (Protocolo IEEE 802.11)

El protocolo IEEE 802.11 es conocido como WLAN (Wireless LAN) y Wi-Fi (Wireless Fidelity). Cuando me refiero a este protocolo estoy también involucrando a todos sus estándares , IEEE 802.11b, g, y a. Los dos primeros operan en la banda de 2,4 GHz y el ultimo en la banda de 5,8 GHz.

Una red WLAN es una red inalámbrica en la que una serie de dispositivos (PCs, Workstation, servidores, impresoras, etc.) se comunican entre si en zonas geográficas limitadas sin necesidad de tendido de cables entre ellos.

Una WLAN esta basada en una arquitectura de celular, donde le sistema esta subdividido en celdas, llamadas set de servicios básicos o BBS, y cada celda es controlada por un Access Point (AP).

Aunque una WLAN podría estar formada por una celda con un solo AP, la mayoría de las WLAN están formadas por muchas celdas, donde los AP se conectan entre si a través de un backbone (Ethernet o incluso inalámbrico), llamado sistema distribuido (DS).

Las diferentes celdas interconectadas, sus AP y el sistema distribuido, son vistos por las capas superiores del modelo OSI como una simple red 802. Esta red es llamada Set de Servicios Extendidos (ESS).

La siguiente figura ilustra lo mencionado anteriormente

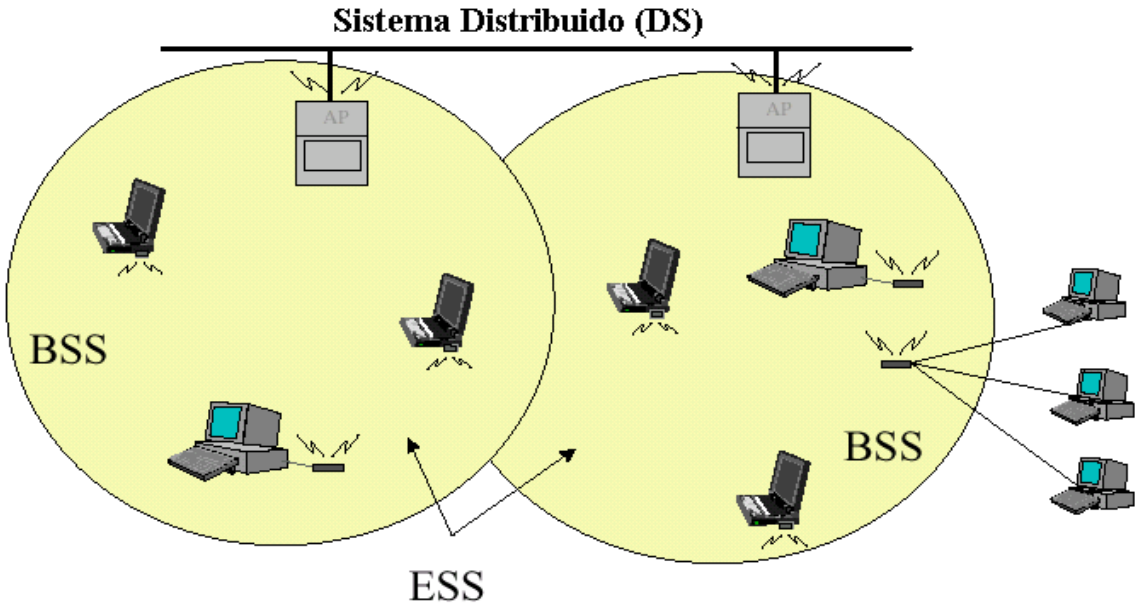


Figura 3.1 Arquitectura de una red WLAN en modo infraestructura

Modos de operación

Ad-Hoc: En este modo de operación, las computadores se conectan entre si de forma Inalambrica, sin la intervención de ningún access point. Este método es una conexión punto a punto entre dos computadoras.

Infraestructura: En este modo de operación, una computadora se conecta con otra a través de un access point que cumple la función de concentrador. Un access point cumple una función similar a la que cumple un hub.

Descripción de las capas del protocolo IEEE 802.11

El protocolo 802.11 define la capa MAC y la capa física. El Standard define una capa MAC que interactúa con tres capas físicas.

- Frecuency Hopping Spread Spectrum (FH-SS).
- Direct Secuence Spread Spectrum (DS-SS).
- Multiplexado por División de Frecuencia Ortogonal (OFDM).

La capa MAC define dos métodos de acceso diferentes. La función de coordinación distribuida y la función de coordinación puntual.

Función de coordinación distribuida

Este método de acceso es básicamente un mecanismo de múltiple acceso de detección de portadora con evitacion de colisión (CSMA/ CA). CSMA funciona de la siguiente manera:

Una estación que desea transmitir sensa el medio, si el mismo esta ocupado, la estación posterga su transmisión, si el medio esta libre, la estación realiza su transmisión.

Este protocolo es muy efectivo cuando el medio no esta muy cargado, debido a que permite a las estaciones transmitir con un retardo mínimo. Sin embargo siempre hay una chance de que dos o mas estaciones transmitan al mismo tiempo producida por el hecho de que las estaciones sensaron el medio libre al mismo tiempo y decidieron transmitir.

Estas colisiones deben ser identificadas para que la retransmisión sea realizada por la capa MAC y no por las capas superiores, lo que causaría mucho retardo. En una red Ethernet esta colisión es detectada por las estaciones transmisoras, las cuales realizan la retransmisión basadas en un algoritmo de retransmisión exponencial aleatorio.

Este mecanismo funciona correctamente en una red con cables, pero no sirve para una red inalámbrica por las siguientes razones:

- La implementación de un mecanismo de detección de colisión requeriría un canal de radio Full-Duplex, lo que incrementaría el costo económico.
- En una red inalámbrica no se puede asumir que todas las estaciones se escuchan entre si (la cual es una asuncion básica del esquema de detección de colisión). Además, el hecho de que una estación transmisora sense el medio libre no significa que el mismo esta libre alrededor del área receptora.

Para evitar estos problemas, 802.11 usa un mecanismo de evitacion de colisión junto con un esquema de reconocimiento positivo.
El funcionamiento de este mecanismo es el siguiente:

Una estación que quiere transmitir sensa el medio, si el mismo esta ocupado no realiza la transmisión, si esta libre durante un tiempo especifico (llamado DIFS, Espacio Inter. Trama Distribuido), se le permite transmitir. La estación receptora chequeara el CRC de el paquete de datos recibido y transmitirá un acknowledgment (ACK). Si el transmisor recibe el ACK sabra que no hubo colisión, si no recibe el ACK, retransmitirá el paquete hasta obtener un ACK. Si no recibe un ACK después de un determinado numero de retransmisiones, cesara la transmisión.

Sensado virtual de portadora

Para evitar el echo de que dos estaciones colisionen debido a que no pueden oírse una a otra se usa el censado de portadora virtual:

Una estación que esta esperando para transmitir primero transmitirá un corto paquete de control llamado RTS (Request To Send), el cual incluirá la fuente, el destino y la duración de la siguiente transacción, la estación de destino responderá con un paquete de control llamado CTS (Clear To Send), el cual incluirá la misma información de duración.

Todas las estaciones que reciban el RTS y/ o el CTS setearan su indicador *Sensado de portadora virtual* , llamado NAV (Vector de Asignación de Red) con la duración dada y usaran esta información junto con el sensor de capa física para sensar el medio.

Este mecanismo reduce la probabilidad de colisión en el área del receptor con una estación que esta oculta para el transmisor a la duración del paquete RTS, debido a que las estaciones escucharan el CTS y reservaran el medio como ocupado hasta el final de la transacción.

El siguiente diagrama muestra una transacción entre dos estaciones A y B y el seteo del NAV de las estaciones vecinas.

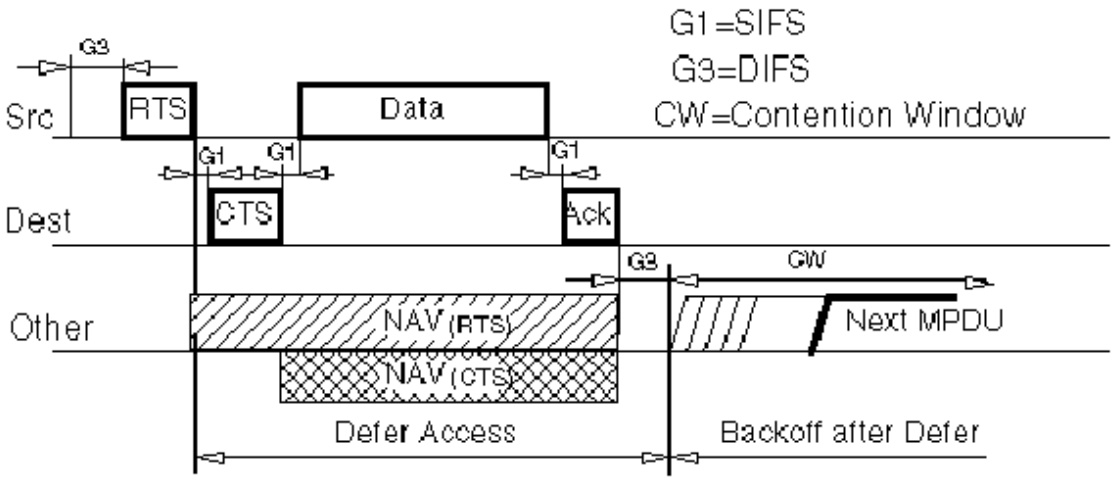


figura 3.2 Transaccion entre 2 estaciones

El estado del NAV es combinado con el sensor de capa física para indicar el estado ocupado del medio.

Acknowledgments a nivel MAC

La capa MAC realiza la detección de colisión esperando la recepción de un ACK para cualquier paquete transmitido (excepto aquellos paquetes que tienen mas de un destino, como lo es Multicast).

Fragmentación y reensamblado

Los protocolos LAN usan paquetes de unos cientos de bytes. Sin embargo, en un ambiente Wireless LAN hay algunas razones para usar paquetes de pocos bytes:

- Debido a que un canal de radio tiene una tasa de error de bit (BER) mas alto que un cable, la probabilidad de que un paquete sea erróneo aumenta con el tamaño del mismo.
- En un sistema Frequency Hopping, el medio es interrumpido periódicamente por saltos de frecuencia, por lo tanto, mientras mas chico sea el paquete, mas pequeña será la chance de que el paquete sea pospuesto para después del tiempo de interrupción.

Por otro lado, no se puede utilizar un protocolo que no puede tratar con paquetes de 1518 Bytes que son usados en una red Ethernet. Por lo tanto se utiliza un mecanismo de fragmentación/ reensamblado en la capa MAC.
Este mecanismo es un simple algoritmo de transmisión y espera, donde no se le permite transmitir a la estación transmisora hasta que suceda uno de los siguientes eventos:

- Reciba un ACK.
- Decida que el fragmento fue retransmitido demasiadas veces y desista de la transmisión.

Espaciado Inter tramas

El tiempo de intervalo entre tramas se llama IFS. Durante este periodo mínimo, una estación estará escuchando el medio antes de transmitir. Se definen cuatro espaciados para dar prioridad de acceso al medio inalámbrico.

- *SIFS (Short IFS).* Este es el periodo más corto. Se utiliza fundamentalmente para transmitir los reconocimientos. También es utilizado para transmitir cada uno de los fragmentos de una trama. Por último, es usado por una estación o Acces Point para enviar testigo a estaciones que quieran transmitir datos síncronos.
- *PIFS (PCF).* Es utilizado por la estaciones para ganar prioridad de acceso en los periodos libres de trafico.

- *DIFS (Distributed IFS)*. Es el espacio intertrama utilizado por una estación que esta esperando para transmitir.
- *EIFS (Extended IFS)*. Controla la espera en los casos en los que se detecta la llegada de una trama errónea. Espera un tiempo suficiente para que le vuelvan a enviar la trama u otra solución.

Roaming

Roaming es el proceso de moverse desde una celda o (BSS) a otra sin perder conexión. IEEE 802.11 no define como se debe realizar el proceso de Roaming, pero define algunas herramientas básicas para lograrlo, como lo son, la búsqueda activa y pasiva y el proceso de reasociación, donde una estación que se mueve de un access point a otro se asocia a este ultimo.

Sincronización

Las estaciones necesitan estar sincronizadas para enviar y recibir datos. En una infraestructura BSS esta sincronización se logra mediante la actualización del clock de las estaciones de acuerdo al clock del access point usando el siguiente mecanismo:

El access point transmite tramas periódicas llamadas Beacon Frames, estas tramas contienen el valor del clock del access point en el momento de la transmisión.

Las estaciones receptoras chequean el valor de sus clocks en el momento de la recepción y lo corrigen para mantener la sincronización con el clock del access point. Esto evita la perdida de la tendencia del clock, lo cual podría causar la perdida de sincronismo después de un par de horas de operación.

Gestión de Potencia

Las estaciones en la red pueden adoptar un modo limitado de potencia. Este modo de funcionamiento implicará que la estación se activara sólo en determinados momentos para conectarse a la red.

Estas estaciones se denominan PS-STAs (Power Save Station) y estarán a la escucha de determinadas tramas como la de portadora y poco más. El control de este tipo de estaciones lo llevará a cabo el access point, que tendrá conocimiento de qué estación se ha asociado en este modo.

El access point mantendrá almacenados los paquetes que le lleguen con destino a los nodos limitados de potencia. Por tanto, el access point mantendrá un mapa de paquetes almacenados y los destinos a quienes tendrá que repartirlos o enviarlos.

Cuando el access point decida enviarle el paquete lo hará enviándole una trama TIM o Traffic Indication Map a la estación para que se active en el próximo intervalo de portadora. De esta manera, estas estaciones recibirán la información con un consumo mínimo de potencia.

3.1 Seguridad en un ambiente WLAN

IEEE 802.11 garantiza la seguridad básica mediante dos métodos: autentificación y encriptación.

La autentificación es el proceso por el cual una estación es verificada para ser autorizada a comunicarse con una segunda estación en un área de cobertura dada. En el modo infraestructura, la autentificación es establecida entre un access point y cada estación.

La autentificación puede ser *Open System* o *Shared Key*.

Autentificación Open System

Autentificación Open System es una forma muy básica de autentificación que consiste de una simple solicitud de autentificación que contiene la ID de la estación y una respuesta de autentificación (ambas en texto plano) que contiene el éxito o fracaso. En caso de éxito, se considera que ambas estaciones están mutuamente autentificadas.

En realidad, este método es un proceso de autenticación nulo ya que se autentica a cualquier cliente que pide ser autenticado.

Autentificación Shared Key

Autentificación Shared key está basada en el hecho de que ambas estaciones tomando parte en el proceso de autentificación tiene la misma clave *compartida*. Se asume que esta clave ha sido trasmitida a ambas estaciones a través de un canal seguro que no es WM. En implementaciones típicas, esto podría ser configurado manualmente en la estación cliente y en el AP. El proceso de autenticación Shared Key es el siguiente:

1. La estación que quiere autenticarse (cliente), envía una trama *AUTHENTICATION REQUEST* indicando que quiere utilizar una *clave compartida.*
2. El destinatario (AP) contesta enviando una trama que contiene 128 octetos de texto (desafío) al cliente. El desafío se genera con la clave compartida y un vector de inicialización (IV) aleatorio.
3. Una vez el cliente recibe la trama, copia el contenido del texto de desafío en el payload de una nueva trama que *encripta con WEP* utilizando la *passphrase* y añade un nuevo IV (elegido por el cliente). Una vez construida esta nueva *trama encriptada*, el cliente la envía al AP.
4. El AP desencripta la trama recibida y comprueba que:
   – El ICV (Integrity Check Value) sea valido.
   – El texto de desafío concuerde con el enviado en el primer mensaje.
5. Si la comprobación es correcta se produce la autenticación del cliente con el AP.
6. Se vuelve a repetir el proceso pero esta vez el primero que manda la trama con el *AUTHENTICATION REQUEST* es el AP, de esta manera se asegura una autenticación mutua.

La encriptación se usa para proveer un nivel de seguridad comparable al de una red LAN cableada. Hay dos formas de encriptación usadas en IEEE 802.11 , las cuales se detallan a continuación.

WEP

WEP (Wireless equivalente privacy) está diseñado para encriptar la información, de manera que la misma solo puede ser desencriptada por los usuarios autorizados.
Su intención era tener las siguientes propiedades:

- **Encriptación razonablemente fuerte.** Depende de la dificultad de recuperar la clave secreta a través de un ataque de fuerza bruta. La dificultad crece con el tamaño de la clave.
- **Auto-sincronización**. No hay necesidad de lidiar con los paquetes perdidos. Cada paquete contiene la información requerida para desencriptarlo.
- **Eficiente.** Puede ser implementado en software de forma razonable.
- **Exportable**. Limitar el largo de la clave conlleva a una mayor posibilidad de exportar más allá de las fronteras de los Estados Unidos.

El algoritmo WEP, esencialmente el algoritmo criptográfico RC4 de Data Security Inc. es considerado un algoritmo simétrico por qué utiliza la misma clave para cifrar y para descifrar la Unidad de Información de Protocolo (PDU) de texto plano. Las características de Wep son las siguientes:

- Utiliza claves de 64 o 128 bits.
- Cada paquete cifrado contiene un vector de iniciación (IV) sin cifrar y el bloque de datos cifrado, el cual a su vez contiene un CRC32 (cifrado) para comprobar integridad.

A continuación se detalla el funcionamiento de WEP.

- A partir de una clave se inicializa una tabla de estados.
- Esta tabla se utiliza para generar una lista de bytes pseudo-aleatorios.
- Estos bytes se combinan mediante la función XOR con los datos sin cifrar.
- El resultado son los datos cifrados.

WEP es un sistema de encriptación con vulnerabilidades. Estas se deben principalmente al sistema de claves y surgen por las siguientes razones.

- Las claves se introducen de forma manual. No hay un sistema automático seguro de distribución de claves.
- Todas las estaciones cercanas a un AP usan la misma clave.
- El cambio de clave es un proceso manual.

WPA

WPA (Wi-Fi Protected Access) es un stándar propuesto para el cifrado de las comunicaciones inalámbricas. Se trata de un sistema que ofrece mejores mecanismos que WEP para el cifrado de los datos y la autenticación de los usuarios, especialmente pensado para su integración en grandes redes.

WPA utiliza el protocolo TKIP (Temporal Key Integrity Protocol). Este protocolo cambia las claves de encriptación para cada paquete a través del mezclado de claves. WPA también incrementa el espacio de claves y permite rechazar los paquetes insertados por un intruso. Por otro lado, permite usar autentificación basada en un servidor (802.1x).

IEEE 802.1x

IEEE 802.1x es un protocolo utilizado para realizar la autentificación de los usuarios y de ese modo reforzar la seguridad de la red. La función de este estándar es transportar EAP (Extensible Authentication Protocol) sobre redes LAN inalambricas o cableadas.

802.1x define tres términos. El usuario que quiere autenticarse es llamado supplicant. El servidor que realiza la autentificación (normalmente un servidor RADIUS *Remote Authentication Dial In User Service*) se llama servidor de autentificación y por ultimo, el dispositivo entre medio de estos dos (generalmente un access point) es llamado autenticador.

El funcionamiento de este protocolo es el siguiente:

Un supplicant (usuario) intenta conectarse con el autenticador (Ej: un access point). Este responde habilitando un puerto para pasar paquetes EAP desde el usuario al servidor de autentificación. El access point bloquea todo el otro trafico (Ej http, POP3, DHCP, etc.) hasta que pueda verificar la identidad del cliente usando un servidor de autenticación (RADIUS). Una vez autenticado, el access point abre los demás puertos para que el cliente pase todo el trafico que requiera.

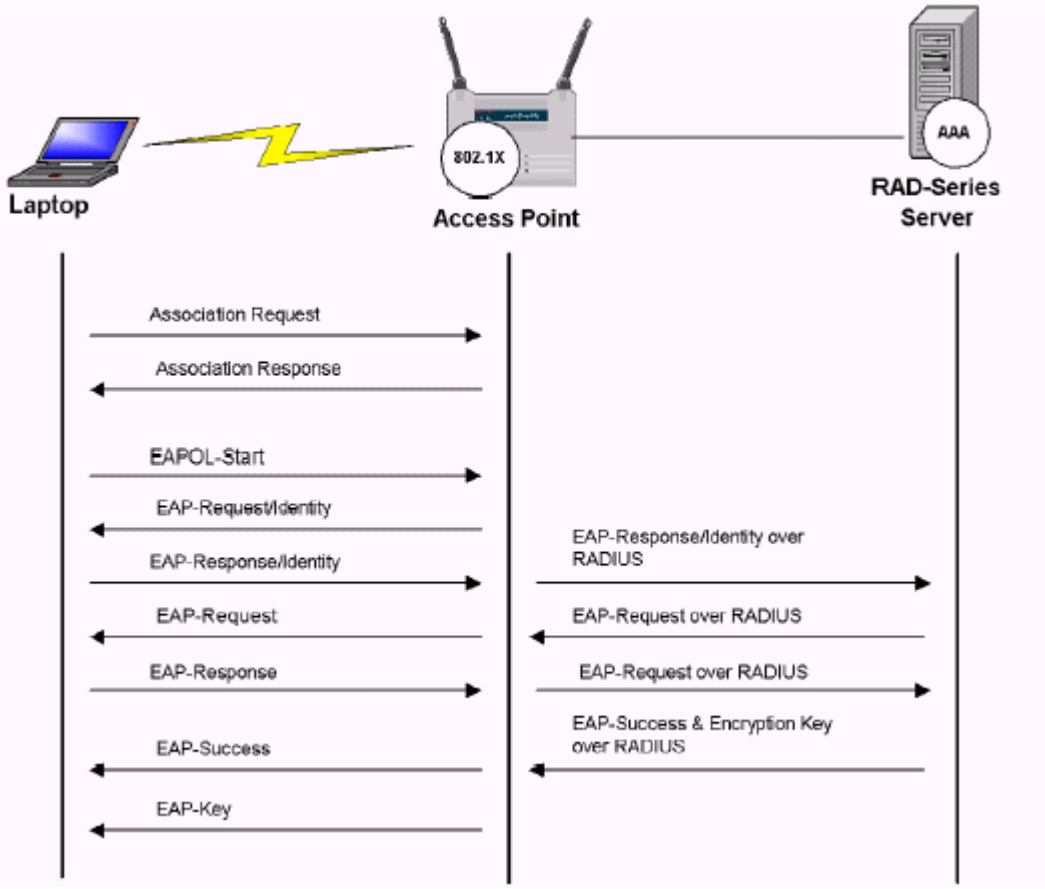
EAP (Extensible Authentication Protocol) es un método utilizado para manejar un intercambio de autenticación entre un usuario y un servidor de autenticación. Los dispositivos intermedios, tales como access points y servidores proxy no intervienen en este intercambio; su unico rol es retransmitir los mensajes EAP entre el usuario y el servidor de autenticación.

Extensible Authentication Protocol Over LAN (EAPOL): 802.1X define un standard para encapsular las tramas EAP, de manera que puedan ser manejadas directamente por la capa MAC de la red LAN.

Esta forma encapsulada de las tramas EAP es conocida como EAPOL. Además de transportar tramas EAP, EAPOL también provee funciones de control, tales como, inicio, logoff, y distribución de claves

RADIUS (RFC 2865) es un protocolo que fue desarrolladado para permitir la autenticación, autorización y el control de acceso en forma centralizada. El mismo se desarrollo para evitar que cada servidor de acceso de una red tuviera que mantener una lista

los nombres de usuarios y contraseñas habilitadas en el sistema. De esta manera, estos requerimientos se procesan en un solo servidor denominado AAA (autenticación, autorización y accounting). Esto permite manejar todo el sistema con una sola base de datos.
La siguiente figura muestra los pasos del protocolo IEEE 802.1x



4 Ensayos de configuración en un ambiente local

A continuación se detallan las distintas opciones de configuración realizadas con el objetivo de verificar el funcionamiento de los dispositivos wireless. Las pruebas se realizaron con access points Linksys WAP11, bridges Linksys Wet11 y adaptadores USB Netgear MA111. Todos ellos respondiendo al protocolo IEEE 802.11b.

4.1 Escenario Wi-Fi N^{ro} 1

En esta configuración se usa un access point conectado a la red LAN de la empresa InterWave con el fin de brindar señal a los distintos receptores inalámbricos.

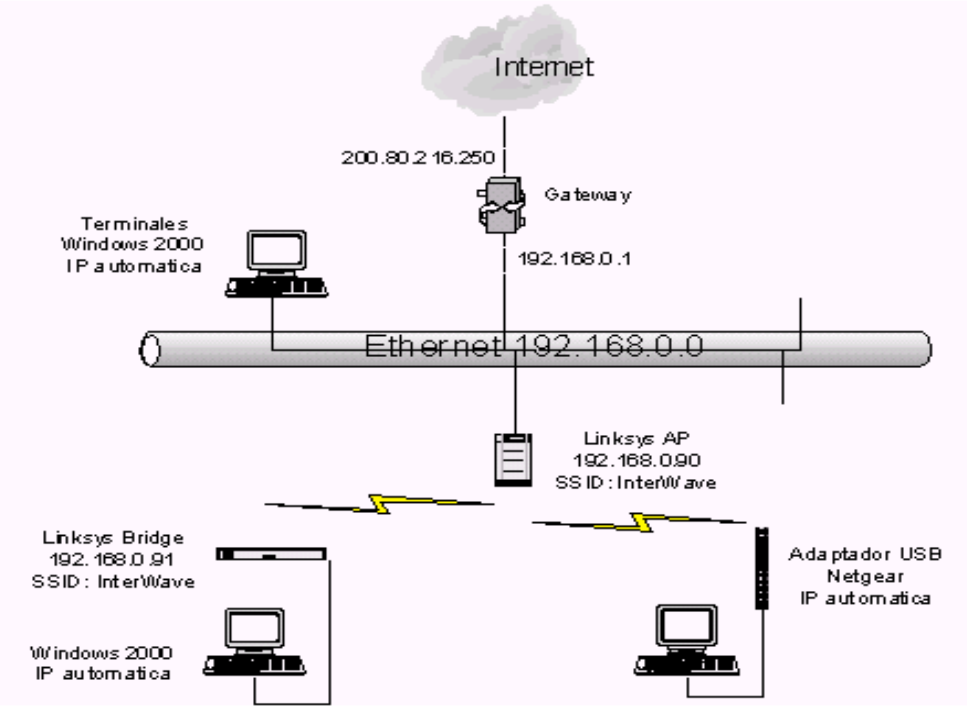


Figura 4.1 Interconexión de los distintos dispositivos

4.1.1 Configuración del Access Point Linksys WAP11

Este access point se configura a través de un web browser (en este caso Internet Explorer). Una vez conectado el access point a la red LAN se debe escribir en la barra de estado la dirección IP 192.168.1.251, la cual es la dirección IP que trae el Access Point por defecto. Después de hacer esto aparece una ventana que nos pide un nombre de usuario y una contraseña; el nombre de usuario se deja en blanco y la contraseña que se ingresa es *admin.* (la que trae por defecto el access point). Finalizado este paso ingresamos al menú de configuración.

En la parte de superior del menú hay seis botones; Setup, Password, Status, Log, Help y Advanced.

Setup

El menú setup se deben configurar las siguientes opciones.

AP name: Indica el nombre del access point. El valor ingresado para este caso es InterWave 0001.

LAN IP Address: Aquí se debe ingresar la dirección IP, la mascara de subred y el gateway correspondientes al Access point. En caso de poseer un servidor DHCP, puede configurar el access point para obtener todos estos parámetros automáticamente..
En nuestro caso la configuración es como sigue:

dirección IP	192.168.0.90
Mascara de subred	255.255.255.0
Gateway	192.168.0.1

Se asigno esa dirección IP debido a que el rango de direcciones IP 192.168.0.100 a 192.168.0.255 son asignadas automáticamente por el servidor DHCP de la empresa.
El Gateway en este caso es una PC con dos placas de red que tiene una conexión directa a Internet y cumple la función de NAT (Network Address Translator), el mismo es utilizado para conectar todas las computadoras a Internet usando una sola dirección IP ruteable.

SSID (Service Set Identifier): Como se menciono anteriormente, las diferentes celdas interconectadas, sus AP y el sistema distribuido, son vistos por las capas superiores del modelo OSI como una simple red 802. Esta red es llamada Set de Servicios Extendidos (ESS). El SSID es el identificador de esta red.
Todos los dispositivos wireless en una misma red deben tener el mismo SSID para poder comunicarse entre ellos. también se conoce como ESSID (Extended Service Set Identifier). En este caso el SSID es InterWave.

Channel: IEEE 802.11 especifica 11 canales de transmisión en EE.UU. dentro de la banda de 2,4 GHz. En este caso se utilizo el canal 6.

Wep: Como se menciono anteriormente Wep es un sistema de encriptación que se utiliza para brindarle seguridad a la red. Este Access Point permite setear una clave Wep de 64 o 128 bits en formato Hexadecimal o ASCII, las cuales corresponden a 10 letras de la A a la F y números del 0 al 9 para el caso de 64 bits Hexadecimal o 5 caracteres ASCCI para el caso ASCII de 64 bits. Del mismo modo, se utilizan 26 letras de la A a la F y números del 0 al 9 para el caso Hexadecimal de 128 bits o 13 caracteres ASCII para el mismo caso de 128 bits.
Los dispositivos wireless de la línea Linksys permiten crear la clave wep a partir de una *passphrase* de cualquier longitud.
Si se usa Wep todos los artefactos (access point, bridges, tarjetas inalambricas, etc.) deben usar la misma clave para poder intercomunicarse entre ellos..

La clave Wep usada fue una clave Hexadecimal de 64 bits, cuyo valor fue *64656d6f63*.

AP mode: Este parámetro especifica la función que realizara el access point, la cual puede ser acess point, access point cliente, wireless bridge, wireless bridge punto-multipunto o repeater. En este caso se utilizo la función access point.

Password

Este menú permite cambiar el password que se requiere para ingresar al menú de configuración Web. El password original (admin.) fue cambiado por 22123 por razones de seguridad..

Advanced

En este menú se puede configurar un filtro en base a las direcciones Mac, para permitir que solo las direcciones Mac especificadas entren al sistema o para negar el acceso al sistema a las Mac especificadas. En nuestro caso tenemos el filtro deshabilitado.

Wireless

Este menú permite configurar todo lo relacionado a las dos primeras capas del protocolo IEEE 802.11

Beacon interval: Indica la frecuencia de transmisión de los paquetes beacon. Estos paquetes se usan para la sincronización de la red. Se utiliza el valor de 100 mseg recomendado por defecto.

Basic Rates : Es la mínima velocidad a la cual se le permite conectarse al access point a un cliente.

RTS Threshold (Request To Send): Es una señal enviada desde la estación transmisora a la estación receptora requiriendo permiso para transmitir. Se usa el valor por defecto de 2346.

Fragmentation threshold: Indica el tamaño máximo que puede alcanzar el paquete antes de ser fragmentado. Se recomienda usar un valor de 2346 Bytes.

DTIM Interval: Indica el intervalo del paquete DTIM. Cuando el access point a almacenado mensajes de broadcast o multicast para los clientes asociados, este envia una trama DTIM (Delivery Traffic Indication Message) con un valor de intervalo de trama TIM. En base a este valor, los clientes escuchan las tramas beacons y se activan para recibir los mensajes broadcast y multicast.

Preamble Type: Define la longitud del bloque CRC (Codigo de Redundancia Ciclica) para la comunicación entre el access point y el adaptador de red inalámbrico. Todos los artefactos de la red deben usar el mismo preámbulo. En este caso utilizamos long preambule.

Authentication Type: Como se menciono anteriormente la autentificación puede ser Open System o Shared Key. En este caso se utilizo Shared key debido a que proporciona mayor seguridad.

Antenna Selection: Permite usar una o dos antenas. Cuando se usa una antena se puede elegir entre derecha e izquierda. Cuando se usan dos antenas se debe elegir diversity. En este caso se utilizo diversity. Al seleccionar diversity se implementa un sistema de diversidad espacial, el cual permite mejorar la performance en la recepción.

SSID Broadcast: Si se deshabilita, el access point no emite Beacon Frames o los emite sin el SSID. Por lo tanto permite que solo los usuarios que conozcan el SSID de la red puedan conectarse. En este caso esta opción esta habilitada.

4.1.2 Configuración del bridge Linksys WET11

El bridge inalámbrico es un dispositivo que permite que uno o mas usuarios conectados al mismo se comuniquen de manera inalámbrica con otros dispositivos a través de un access point.

Este bridge inalámbrico se configura de una manera muy parecida al access point Linksys WAP11. El proceso de conexión es idéntico al del AP, solo que la dirección IP a colocar en la barra de direcciones del Internet Explorer es 192.168.1.225. En el menú de configuración aparecen las siguientes opciones: Setup, Password, Status y Help

Setup

Este menú es idéntico al del AP, con la diferencia de que no figuran las opciones Channel y AP mode y se agrega la opción Network Type.

El parámetro Channel no figura debido a que el bridge se asocia al access point del cual recibe el mayor nivel de señal y utiliza el canal de ese access point.

La opción Network Type permite elegir entre infrastuctura (el bridge se conecta a la red a través de una access point) o AD-HOC (se conecta directamente con otro bridge o computadora). En este caso se eligió la opción infraestructura.

Además, el SSID del bridge es idéntico al del AP (InterWave) y utiliza la misma clave Wep. La dirección IP asignada al bridge es 192.168.0.91 .

Password

Este menú es idéntico al del access point.

Advanced Wireless setting

Este menú consta de 2 ítems.

Transmit Rate: Permite elegir la velocidad de transmisión. En este caso se usa automático.

AP density: Selecciona la cantidad de AP que hay en la red. Se puede elegir entre alta,

media y baja. En este caso se eligió baja, ya que solo existe un access point en funcionamiento.

4.1.3 Configuración del adaptador USB Netgear MA111.

Este adaptador debe ser instalado en una PC o notebook. El mismo cumple la función de adaptador de red inalámbrico. Antes de realizar la configuración se deben instalar los drivers correspondientes a este adaptador, los cuales se pueden bajar de www.netgear.com . Una instalados los drivers se debe conectar el dispositivo en el puerto USB de la maquina, con lo cual Windows le mostrara una pantalla de nuevo hardware encontrado , en este paso debe indicar la ruta del driver.

Para realizar la configuración se debe hacer doble clic en el indicador de red de la barra de escritorio de Windows con lo cual se accede al menú de configuración. En el mismo se debe ingresar el SSID (en este caso InterWave) y la clave Wep (ingresamos 64656d6f63, 64 bits en formato Hexadecimal).

Como segundo paso debemos configurar el protocolo TCP / IP de la PC (en este caso utilizamos Windows 2000 profesional) , para lo cual hacemos clik derecho en my computer, luego en conexiones de red, luego click derecho en netgear MA11, luego en propiedades, TCP /IP. En este punto debemos seleccionar si usamos una IP fija o dinámica. En este caso seleccionamos *obtener una dirección IP automáticamente* y *obtener DNS automáticamente,* debido a que contamos con un servidor DHCP que provee estos parámetros.

4.2 Escenario Wi-Fi N^{ro} 2

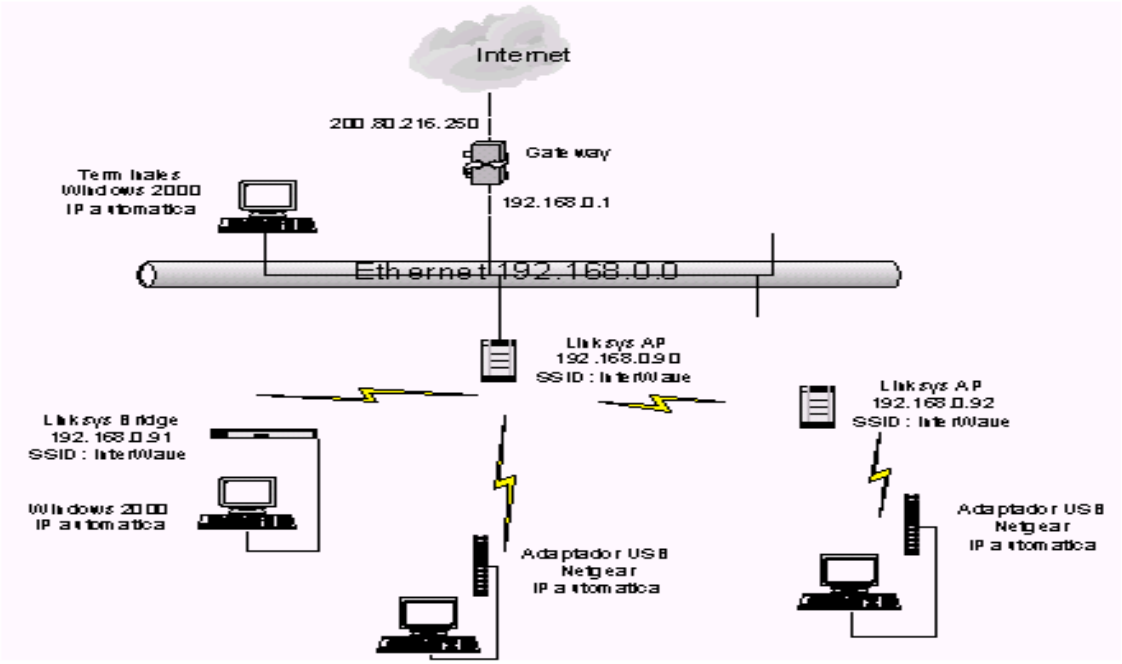


figura 4.2 Interconexión de dispositivos inalámbricos

En este escenario se agrego un segundo access point con una configuración idéntica al primero, con la excepción de que en la opción AP mode del menú setup se configuro al mismo como *Wireless Repeater* de tal forma que este access point se comunica en forma inalámbrica con el primero y a su vez tiene un cliente asociado a el. Al usar esta configuración obtenemos un sistema constituido por dos celdas.

5 telefonía IP sobre una plataforma Wi-Fi

5.1 Escenario H.323 N^{ro} 1

El siguiente objetivo es brindar telefonía IP conectando un Terminal H.323 marca ATA186 a la red LAN a través de un bridge inalámbrico y un access point Linksys como muestra el siguiente esquema

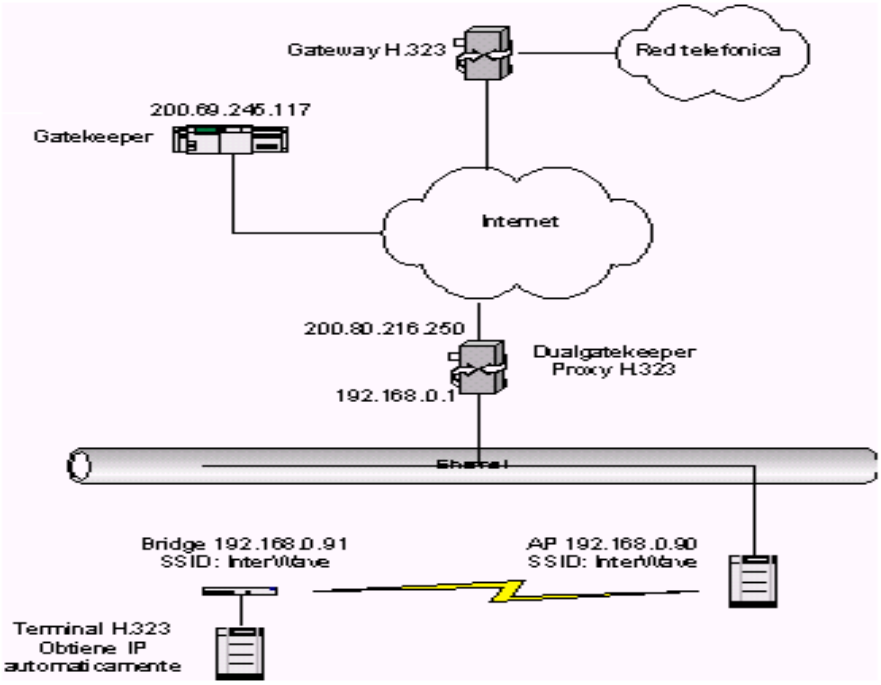


Figura 5.1 telefonía IP dentro de una red LAN

En este esquema se puede observar que el terminal H.323 se conecta al bridge inalámbrico, el cual se conecta al access point para tener acceso a la red LAN. La configuración de los dispositivos wireless es idéntica a la del escenario Wi-Fi n^{ro} 1. El gatekeeper y el gateway son provistos y configurados por la empresa VoIP grup Inc. Como se puede observar en el esquema, los terminales H.323 tienen una dirección IP privada, por lo tanto para poder realizar llamadas afuera de la red LAN es necesario colocar un Proxy H.323, ya que si no lo hiciéramos no podríamos realizar llamadas por que H.323 abre puertos aleatorios que serian bloqueados por el por el gateway de acceso a Internet (Windows 2000 con ISA Server). El Proxy H.323 es el programa Dualgatekeeper, el cual

realiza la traducción de la dirección IP privada del ATA 186 a la dirección publica 200.80.216.250 (en este caso).

El software Dualgatekeeper prácticamente se autoconfigura, ya que solo se debe ingresar la dirección IP del gatekeeper (o de un gateway en caso de no usar un gatekeeper), siendo la misma 200.69.245.117 .

5.2 Escenario H.323 N^{ro} 2

Este escenario es idéntico al anterior, con la única diferencia de que se agrega otro dispositivo ATA 186. Al realizar esta configuración surge un problema con las llamadas entrantes. Cuando se realiza una llamada hacia un terminal H.323 se produce un problema para establecer la comunicación debido a que H.323 no soporta la función de traducción de direcciones (NAT).

NAT permite conectar a Internet varias PCs de una misma subred que utilizan direcciones IP no ruteables, utilizando únicamente una dirección IP pública para ello. NAT se aprovecha de las características de TCP/IP, que permiten a una PC mantener varias conexiones simultáneas con un mismo servidor remoto. Esto es posible gracias a los campos de las cabeceras que definen unívocamente cada conexión, estos son: dirección origen, puerto origen, dirección destino y puerto destino. Las direcciones identifican los equipos de cada extremo y los puertos cada conexión entre ellos.

Como sólo queremos utilizar una dirección pública, ésta se asigna al equipo que implementa NAT (Ej. router), mientras que los hosts de la subred poseen direcciones privadas estas últimas sólo son válidas para identificar al host en el ámbito de la subred. El router multiplexa el tráfico de la subred y lo presenta a Internet como si hubiera sido generado todo por una misma máquina. Esto se consigue sustituyendo cada dirección origen privada de las cabeceras de los paquetes IP por la dirección pública, por lo tanto todos los paquetes de salida tendrán la misma dirección origen. Para poder identificar entonces cada tráfico de las diferentes computadoras, se utiliza el número de puerto de cada conexión. Como estos deben ser únicos, el router se encarga también de realizar una conversión de puertos (NAPT, Network Address Port Translation). Para hacer todo esto, el router debe mantener una tabla con la dirección y puerto real de la máquina, el número de puerto que se le ha asignado, y dirección y puerto destino. De esta forma el router puede entregar los paquetes de vuelta a los hosts correspondientes

H.323 comprende una serie de estándares y se apoya en una serie de protocolos que cubren los distintos aspectos de la comunicación, tal y como el H.225, H.245, RTP, etc. Es en alguno de estos protocolos donde se da el problema con el uso de NAT, ya que introducen direcciones IP y números de puertos en el campo de datos de los paquetes. Cuando la dirección IP de origen se incluye en el campo de datos del paquete si esta dirección llega sin ninguna modificación al destino, el equipo remoto no sabrá qué hacer con ella, ya que se trata de una dirección privada.

Este problema se puede solucionar en parte con el software Dualgatekeeper, ya que el mismo permite realizar llamadas salientes sin ningún problema, pero cuando recibe una llamada entrante pueden suceder dos cosas:

1. Se puede configurar el soft Dualgatekeeper para que cuando reciba una llamada entrante suenen todos los terminales H.323 conectados al mismo, o.

2. Se puede configurar el soft Dualgatekeeper para que cuando reciba una llamada entrante suene un solo terminal, pero siempre sonara el mismo sin importar a que numero se marque.

Cabe aclarar que las direcciones IP de los dispositivos wireless no son utilizadas por el protocolo IEEE 802.11, pero son configuradas para poder tener acceso al dispositivo inalámbrico mediante su menú de configuración web.

5.3 Configuración del dispositivo ATA 186

El dispositivo ATA 186 es un producto de CISCO. El mismo es un terminal H.323, cuya función principal es convertir la señal de voz analógica en tramas del protocolo H.323. Este dispositivo posee dos puertos FXS RJ11 donde se conectan dos teléfonos analógicos y un puerto Ethernet 10BaseT RJ45 que sirve para conectar el dispositivo a la red IP.

El ATA 186 puede configurarse mediante el Cisco Call Manager TFTP Server, mediante el menú de configuración de voz o mediante el menú web. En nuestro caso, la configuración se realizo con los dos últimos métodos.

Para configurar el ATA 186 se lo conecto a una PC mediante un cable cruzado.

Antes de realizar la configuración se debe instalar el firmware para el protocolo H.323 y SIP, ya que el ATA 186 trae instalado solamente el firmware para MGCP y SCCP.

Para instalar el firmware se deben ejecutar los siguientes pasos:

1. Ejecutar en el Promt de DOS el comando ata186us –any –d1 – ata18x-v2-15-020927a.zup . Donde any significa que permite actualizar cualquier versión de software, d1 es el nivel de debugging.
2. Levantar el tubo del teléfono, presionar el botón del ATA 186 y marcar en el teléfono 100# 192*168*0*125* 8000#. Donde 192.168.0.125 es la dirección IP de la PC y 8000 es el numero de puerto de configuración por defecto.
3. Una vez finalizada la actualización se debe escuchar por el teléfono upgrade successfull

Después de instalado el firmware debemos conectar el ATA 186 a la red LAN y presionar el botón del dispositivo, con lo cual accedemos al menú IVR. Luego marcamos en el teléfono 1# para conocer la dirección IP que el servidor DHCP le asigno al dispositivo.

Si queremos cambiar la dirección IP mediante el menú IVR debemos marcar 20#, luego 0# para deshabilitar DHCP y por ultimo 3# para grabar. Cumplido este paso debemos asignarle una dirección IP al dispositivo, para tal fin marcamos 1# y luego la dirección IP (Ej. 192*168*0*58#), después debemos ingresar la mascara de red marcando 10# y la mascara de red (de la misma forma que se ingreso la dirección IP) y la ruta estática marcando 2# y la ruta estática (de la misma forma que se ingreso la dirección IP).

En nuestro caso la configuración se realizo mediante el menú web, es decir, una vez conocida la dirección IP del dispositivo asignada por el servidor DHCP se ingreso la misma en la barra de direcciones del Internet Explorer con el siguiente formato:

http://direccionIPdelATA186/dev

Ejecutado este comando ingresamos al menú web, donde aparecen varios parámetros a ser configurados. El primer parámetro que se configuro es el UIPassword, el cual se utiliza para setear una contraseña que es solicitada cada vez que se intenta acceder al menú web o al menú IVR. En este caso se seteo este valor a 22123. Si el valor del UIPassword es cero no se solicita ninguna contraseña.

Los otros parámetros que se configuraran son los siguientes:

- *DHCP:* Este valor se setea a 1, de esta manera el dispositivo obtiene automáticamente una dirección IP cada vez que se enciende. Para deshabilitarlo se setea a 0.
- Los parámetros *StaticIP, StaticRoute y StaticNetMask* no se configuran ya que usamos un dirección IP dinámica asignada por el servidor DHCP.
- *NTPIP:* Aquí debe ingresarse la dirección IP del servidor NTP. Este servidor es usado por el ATA 186 para obtener las coordenadas de tiempo universal (UTC) que el mismo usa para setear el Time-Stamp en los paquetes IP. En nuestro caso se seteo el valor 132.163.4.102 el cual es provisto por la empresa VoIP Group.
- *DNS1IP:* En este parámetro debe ingresarse la dirección IP del servidor DNS primario. En este caso es 200.69.139.1
- *DNS2IP:* En este parámetro debe ingresarse la dirección IP del servidor DNS secundario. En este caso es 65.105.249.3 .
- *GkOrProxy:* Aquí se ingresa la dirección IP del gatekeeper, en este caso se ingreso la dirección 192.168.0.1, la cual es la dirección IP donde se encuentra el Proxy H.323 (Dualgatekeeper).
- *UID0:* Este parámetro se usa para configurar el alias E.164 del usuario del puerto 1. En este caso se deja este parámetro en 0, con lo cual se deshabilita el puerto FXS N^{ro} 1.
- *PWD0 y PWD1:* En este campo se debe ingresar el password con el que el usuario del puerto 1 y 2 respectivamente se identifican en el sistema. En este caso estos campos no se usan, por lo tanto se dejan en blanco .
- *UID1:* Este parámetro se usa para configurar el alias E.164 del usuario del puerto 2. En este caso el valor ingresado es 7853433 para el primer ATA y 7858583 para el segundo, el cual es provisto por la empresa VoIP Group.
- *LoguinID0:* En este campo se debe ingresar el usercode y el password del puerto 1. En este caso no se ingresa ningún valor ya que el puerto 1 no se utiliza.
- *LoguinID1:* En este campo se debe ingresar el usercode y el password del puerto 2. Donde el usercode es el numero del usuario. Este campo se configura de la siguiente manera:

{UserCode}={Password} :{CountryCode}:{AreaCode}:{IddPrefix}:{NddPrefix}:{TimeZone}:{UseAreaCode}

Donde:

{CountryCode}: Código de País.
{AreaCode}: Código de Área.
{IddPrefix}: Prefijo para llamadas internacionales.
{NddPrefix}: Prefijo para llamadas nacionales.
{TimeZone}: Zona horaria. Acepta valores negativos. Ejemplo: -3.

{UseAreaCode}: Toma valor 0 (No marca código de área) o 1 (Marca código de área) dependiendo si el plan de numeración del País requiere marcar el código de área para llamadas locales

3433=3433:54:351:00:0:-3:0
8583=8583:54:351:00:0:-3:0

- *UseLoguinID:* Si este parámetro se setea a cero el terminal realiza la autenticación contra el sistema con los parámetros UID0 y UID1, si se setea en 1, la autenticación se realiza con los parámetros LoguinID0 y LoguinID1. En este caso el valor ingresado es 1, ya que es necesario setearlo de este manera cuando se utiliza H.323.
- *Gateway:* En este parámetro se debe ingresar la dirección IP del gateway. Si el sistema posee un gatekeeper este parámetro se setea en 0. Por lo tanto, en este caso el valor ingresado es 0.
- *LBRCodec:* Este parámetro se usa para especificar que codecs están disponibles. Cuando este valor se setea en cero, los dos puertos FXS utilizan el codec G.723.1. Cuando se setea en 3 el puerto N^{ro} 1 utiliza el codec G.711 y el puerto N^{ro} 2 utiliza el codec G.729. Siempre que el parámetro AudioMode conserve su valor por default (0x00150015).En este caso se seteo este valor en 3, ya que se obtiene una calidad de audio superior a la que se obtiene si se usa el codec G.729 y el puerto N^{ro} 2 (G.711) no se utiliza debido a que la calidad de audio es muy mala.
- *RxCodec:* En este campo se especifica la preferencia de los codecs del receptor. Se setea un valor de 3, lo que significa que se utilizara el codec G.729. El mismo posee una tasa de compresión de 8 Kbps.
- *TxCodec:* En este campo se especifica la preferencia de los codecs del transmisor. Se setea un valor de 3, lo que significa que se utilizara el codec G.729.
- *NumTxFrame:* Aquí se debe ingresar el numero de tramas del codec por paquete. Al variar este parámetro se modifica el ancho de banda total utilizado por el dispositivo. Este parámetro esta configurado en 2 por defecto. Si utilizamos el mismo, podemos calcular el ancho de banda ocupado de la siguiente manera:

Tiempo de trama: 10ms
Tasa de compresión: 8 Kbps
Tramas por paquete: 2

Duración de cada paquete = Tramas por paquete x Tiempo de trama = 20 ms
Bit p/paquete antes de la compresión = Durac c/ paquete x 64 Kbps = 1280 bits
Bit p/paquete después de la compresión = Bit Rate antes de la compresión / 8 =160 bits = 20 Bytes
Tasa de paquetes = 1 Kbyte/seg / 20 Bytes/paquete = 50 paquetes/ seg
Longitud de cada paquete= Long Codec+header RTP+header UDP+header IP = 60 bytes
Ancho de banda = Long c/paquete x Tasa de paquetes = 24 Kbps

Al utilizar 2 tramas por paquete, los headers de los demás protocolos producen una relación datos/ header muy baja, es decir que transmitimos muchos bits adicionales por cada bit de datos.

Para mejorar esta relación se seteo el numero de tramas de transmisión a 6 y se realizo el calculo anterior para saber el ancho de banda ocupado. Lo cual arrojo como resultado 13,2 Kbps. Por lo tanto, se utilizara siempre este valor, ya que el ancho de banda ocupado es menor que en caso anterior y además la eficiencia del protocolo es superior.

Todos los demás parámetros no se modifican ya que no tienen una relevancia importante en el proceso del establecimiento, desarrollo y terminación de una llamada.
Una vez configurados todos los dispositivos ya se pueden establecer comunicaciones H.323 ya sea con un teléfono fijo o con otro terminal H.323.

5.4 Solución Definitiva (IP Publico)

Para poder realizar llamadas salientes y entrantes sin ningún problema se elimina el NAT, es decir, los terminales H.323 se conectan directamente a Internet utilizando una dirección IP publica. El esquema de conexión es el siguiente.

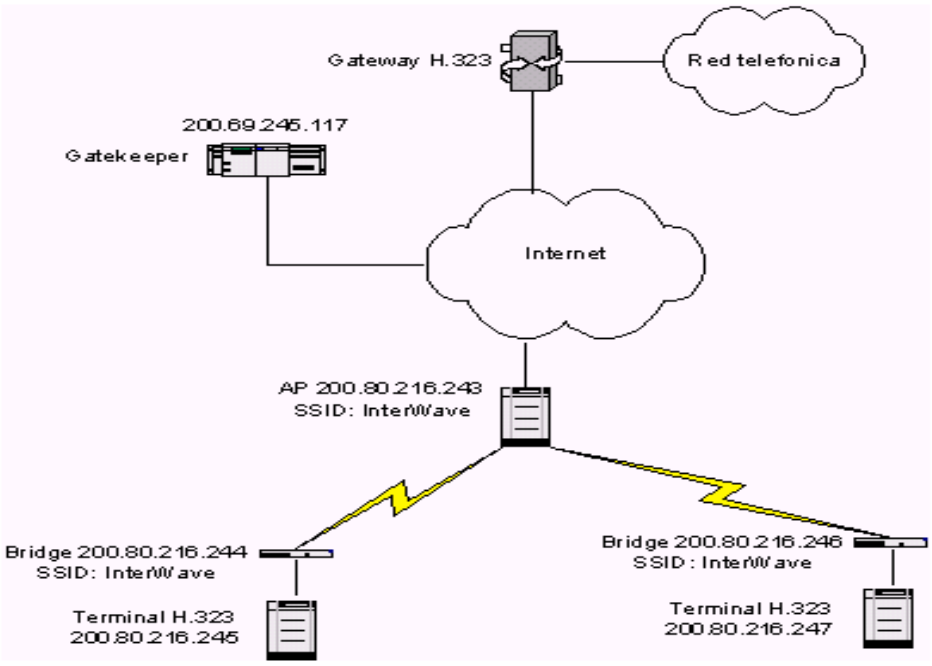


Figura 5.2 Solución de conexión definitiva

Para poder establecer llamadas H.323 se deben cambiar los siguientes parámetros del ATA 186:

- *DHCP:* Como utilizamos una dirección IP fija se deshabilita este parámetro seteandolo a cero.
- *StaticIP:* Se ingresa la dirección IP correspondiente a cada dispositivo, tal como lo muestra el esquema anterior.

- *StaticRoute:* Se ingresa el valor mostrado en el esquema. Esta dirección IP es la que utiliza el ISP (Iplan) para rutear el tráfico hacia Internet.
- *StaticSubnetMask:* Se ingresa el valor mostrado en el esquema.
- *GkOrProxy:* Aquí se ingresa el valor 200.69.245.117, la cual es la dirección IP del gatekeeper de la empresa VoIP Group.

Para realizar una comunicación desde el ATA 186 con un teléfono fijo solo es necesario discar el numero del teléfono fijo, para realizar una llamada hacia el ATA 186 se debe discar su virtual number (5682905 para el ATA Nro 1 y 5682906 para el Nro 2), el cual esta configurado en el gatekeeper de la empresa VoIP Group.

6 Arquitectura del sistema

Como se menciono anteriormente, el objetivo del sistema es brindar telefonía IP e Internet de banda ancha a los usuarios. En el caso de Internet, los usarios no tendrán que configurar ninguna clave de autenticación ni cifrado en sus placas de red inalambricas. El objetivo es que los mismos se conecten al sistema sin ningún inconveniente, pero cuando quieran ingresar a un sitio web, sean trasladados hacia una pagina web donde se le pida un nombre de usuario y una contraseña. En el caso de telefonía IP, el sistema es similar al del esquema que se muestra en la figura anterior. Por lo tanto el diagrama lógico del sistema es el siguiente.

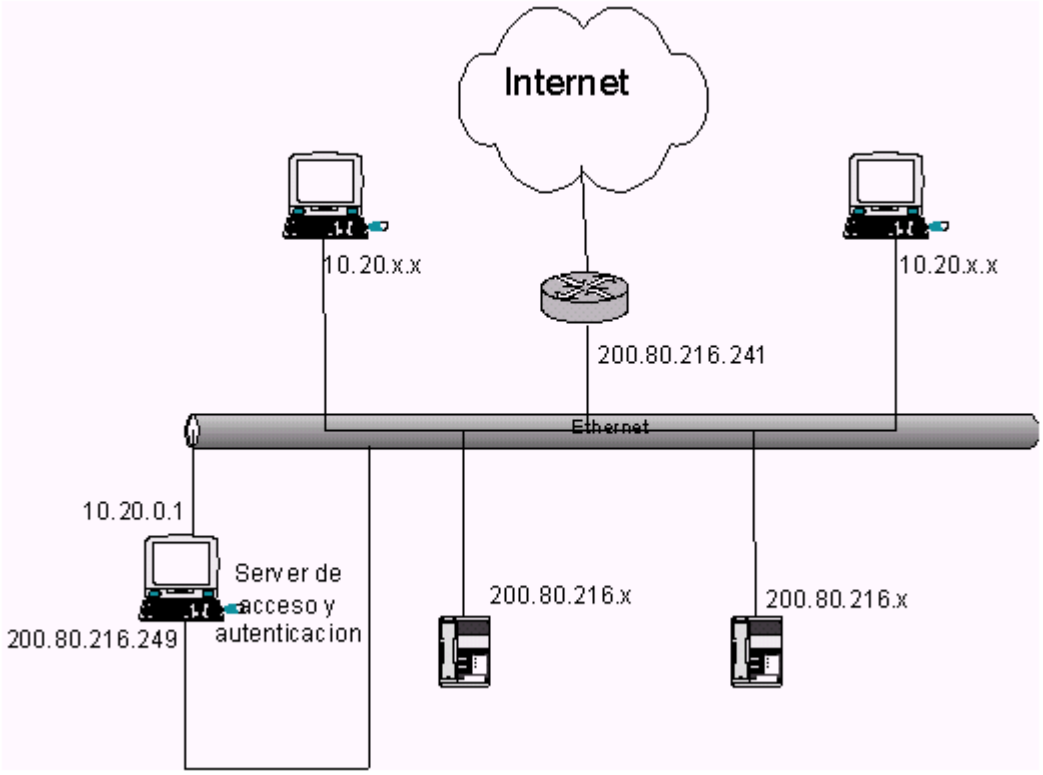


Figura 6.1 Esquema de conexión lógico

Como se puede observar en la figura anterior, se utiliza la dirección de red privada 10.0.0.0 y se configura una mascara de subred 255.255.0.0 para formar la subred 10.20.0.0, obteniendo 65534 direcciones IP utilizables.

Las computadoras de los usuarios están configuradas para obtener automáticamente una dirección IP en el rango de 10.20.0.150 hasta 10.20.255.254. Estas direcciones son provistas por el servidor de acceso, el cual, además les instruye a los usuarios que usen la dirección IP de su placa de red (10.20.0.1) como gateway para acceder a Internet. En la figura anterior se observa que los usuarios están conectados directamente a Internet, pero ellos deben usar el servidor de acceso obligatoriamente ya que sus direcciones IP no son ruteables a través de Internet. De esta manera el servidor de acceso cumple la función de NAT (Network Address Translator).

Esta configuración se repite en cada MAP del sistema, ya que cada uno posee su propia conexión a Internet a través de una interfaz distinta del router.

Los terminales H.323 poseen una dirección IP ruteable, de esta manera no pasan a través del servidor de acceso. De todas formas, la autenticación la realizan en el gatekeeper H.323.

Al utilizar la dirección de red 200.80.216.0 solo es posible contar con 254 usuarios de telefonía. Sin embargo este numero es suficiente para la fase inicial del proyecto. De todas formas, en un futuro la empresa VoIP Group implementara el protocolo SIP, el cual permite usar direcciones IP privadas. Permitiendo entonces incrementar el número de usuarios.

Seguridad

La seguridad del sistema esta actualmente manejada íntegramente por la empresa VoIP Group. Para ello, en la misma se ha implementado un servidor RADIUS para realizar la autenticación de los usuarios.

A cada cliente se le otorga un numero de cuenta y una contraseña para realizar la autenticación, la misma esta configurada en el parámetro LoguinID1 del terminal H.323 ATA 186. Por lo tanto, solo los clientes autorizados pueden acceder al servicio de telefonía.

El tema pendiente a resolver es que alguien configure su PC con una dirección IP publica (perteneciente a la misma red de los terminales H.323) y utilice libremente los servicios de Internet (excepto la telefonía IP). Sin embargo, este problema no es relevante ya que el núcleo del negocio es la telefonía y no la provisión de Internet.

7 Componentes del sistema

En el sistema existen cinco componentes principales:

- *MAP (Master Access Point):* Es el que permite a los usuarios tener acceso a Internet. El mismo esta compuesto de 8 o 6 antenas direccionales (con sus respectivos access points), según sea el caso, que proporcionan una cobertura omnidireccional. El MAP se conecta a Internet a través de los servidores de acceso.
- *Servidores de acceso:* Son dos PCs con dos placas de red c/u que por un lado se conectan al MAP y por el otro a Internet a través de una conexión de 1 Mbps.
- *Repeater:* Cumple la misma función que el MAP, pero no posee una conexión a Internet a través de los servidores de acceso, si no que se conecta a la misma a través de un MAP.
- *Nodo semifijo:* Esta compuesto por una antena omnidireccional, un bridge inalámbrico, un swicht y un terminal H.323 ATA 186. El mismo es utilizado por el usuario para tener acceso a los servicios del sistema. Este nodo semifijo puede trasladarse de un lugar a otro, siempre y cuando se tenga cobertura radioeléctrica.
- *Nodo fijo:* Es idéntico al nodo semifijo, pero este no se puede trasladar de un lugar hacia otro.

La siguiente figura muestra un esquema con la interconexión de los elementos descriptos anteriormente.

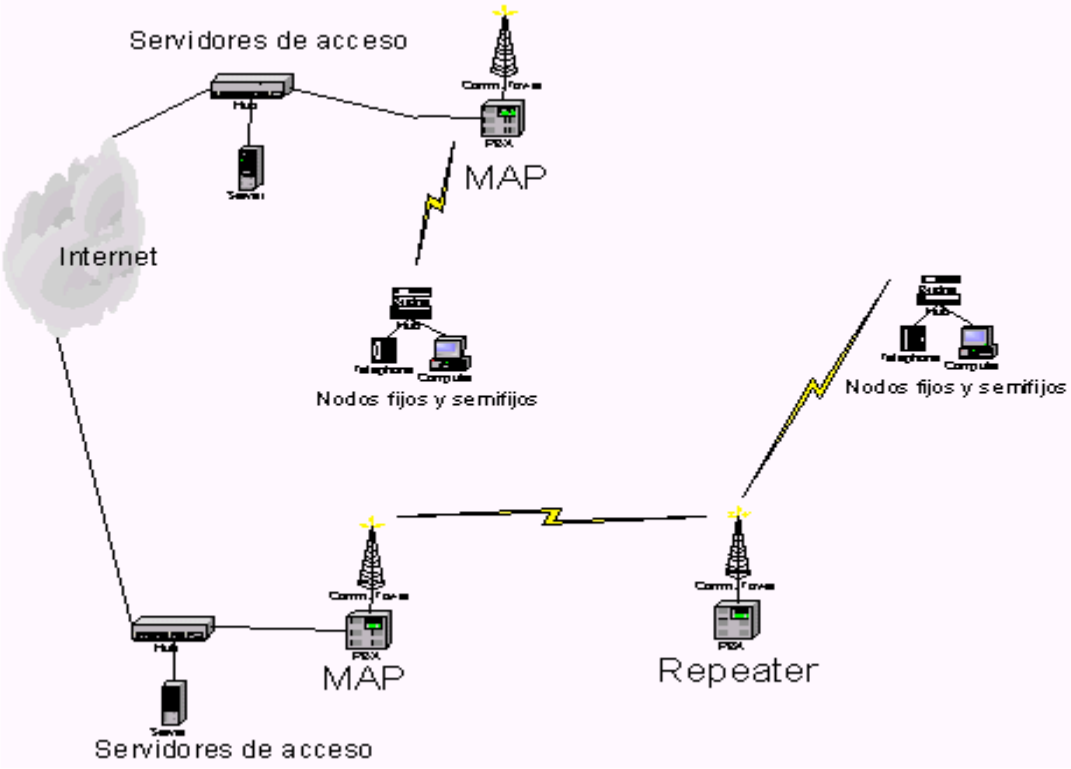


figura 7.1 Interconexión de los componentes del sistema

A continuación se describen en detalle cada uno de los componentes del sistema.

7.1 MAP

Como se dijo anteriormente el MAP es el principal punto de acceso a la red. A través de el se pueden conectar a Internet los usuarios y los Repeaters.
La función del MAP es la de brindarle acceso a Internet a los usuarios. Para lograr esto, el mismo debe proporcionar una cobertura radioeléctrica omnidireccional, la cual es lograda mediante un arreglo de antenas del tipo panel direccionales. Este arreglo de antenas varia según la forma de la terraza donde se encuentre ubicado el MAP; de todas maneras, se utilizan dos tipos diferentes de arreglos:

1. El que se utiliza en terrazas que por ser demasiado grandes o por no tener acceso al centro de la misma no es posible colocar las antenas en el centro de la terraza ya que si se hiciera esto no se lograría la propagación de la mayor parte de la energía. La siguiente figura explica este fenómeno.

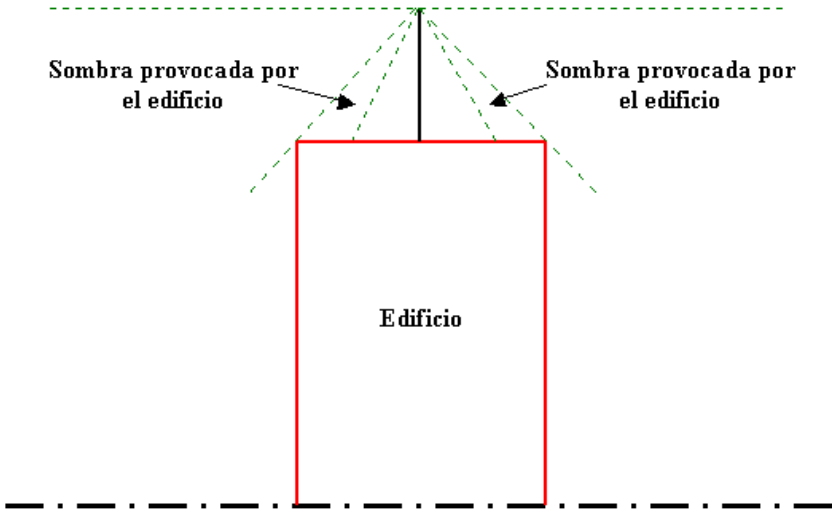


figura 7.2 Efecto de sombra provocado por el edificio

Para evitar este fenómeno, se colocan 8 antenas direccionales distribuidas en cuatro postes colocadas en los extremos de la terraza.

2. El que se utiliza en terrazas de edificios que por ser angostos no presentan el problema anterior. Por lo tanto, aquí se colocan 6 antenas direccionales en un mismo poste.

Hasta el momento se ha colocado un MAP en la terraza del edificio Columbus ubicado en Av. Colon 778 y se ha desarrollado completamente otro que será colocado en el edificio Bussines Tower ubicado en Hipolito Irigoyen 146. El primer MAP será usado como ejemplo para la descripción de todos los demás.

El MAP que se describe utiliza el arreglo de antenas numero 1 (8 antenas direccionales). En cada poste se colocan dos antenas de panel direccionales, las que se conectan, protector gaseoso mediante a sus respectivos access points colocados en el mismo poste como se muestra a continuación.

Los protectores gaseosos cumplen la función de evitar que el access point sea dañado por altos voltajes provenientes de alguna descarga eléctrica inducida por un rayo que caiga en la zona cercana, por estática acumulada en la antena, etc.

figura 7.3 Disposición física de las antenas y los access points

Las antenas utilizadas poseen un ancho del lóbulo principal de 70° tanto en el plano vertical como en el horizontal. Como se observa en la figura, las antenas poseen un tilt de 35°, de esta manera se logra una cobertura casi completa en el plano vertical.

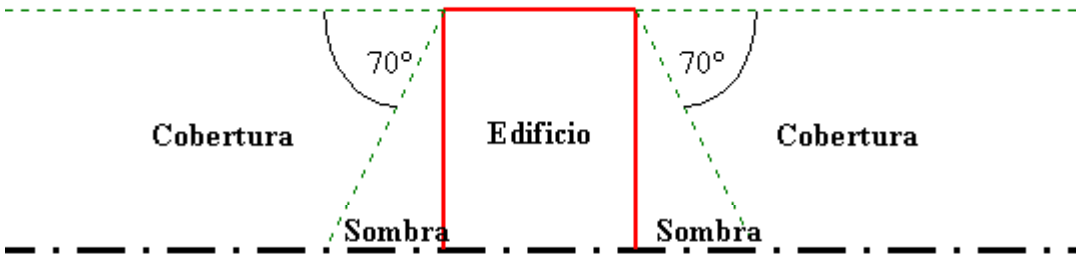


figura 7.4 Cobertura vertical

En el centro de la terraza se encuentran colocados dentro de un gabinete un switch Ethernet de 16 puertos y 10/100 Mbps y una patchera que se utiliza para alimentar a los access points por medio del cable UTP. Además, dentro del mismo gabinete se coloca una UPS de 700 VA que es utilizada en caso de que ocurra un corte de energía, proveyendo una autonomía de 4 horas.

La alimentación de los access points se realiza utilizando los pares azul y marrón, ya que estos no son utilizados para transmitir información.

El cable UTP transportando la alimentación llega hasta el gabinete donde se encuentra el access point, allí se conecta a un jack RJ-45 y del mismo sale un cable UTP sin los pares azul y marrón que se conecta al puerto LAN del access point. Desde el mismo

Jack se conecta el par azul al borne positivo del conector de potencia y el par marrón al borne negativo.

La siguiente figura muestra el montaje del swicht, la UPS y la patchera desde donde sale el cable UTP que se dirige hacia el access point.

figura 7.5 Disposición física del swicht y la UPS

Desde el swicht ubicado en el gabinete bajan 2 cables UTP (uno de backup) que se conectan a los servidores de acceso ubicados en el 7mo piso y un cable de alimentación que le brinda energía al MAP.

Los access points utilizados en el MAP cumplen la norma 802.11g, los mismos son marca D-Link DWL-2000AP y tienen la siguiente configuración:

Parametro	Valor	Descripción
SSID	DSC	Identificador de la red inalámbrica
Channel	1 al 8	Canal de transmisión
Wep	Deshabilitado	Cifrado de la información
Dirección IP	10.20.0.3 al 10.20.0.10	Permite ingresar al menu web
Mascara de subred	255.255.0.0	
Servidor DHCP	Deshabilitado	El AP incorpora un servidor DHCP
Beacon Interval	100 ms	Intervalo de la trama de sincronización
DTIM Interval	3	Intervalo de la trama DTIM
Tx Rates	Auto	Velocidad de transmisión
Wireless mode	Mixto	Funciona como 802.11b y 802.11g
Aautenticacion	Open System	Metodo de autenticación
SSID Broadcast	Habilitado	Permite que los usuarios visualicen el SSID

Los canales utilizados por los access point varían en forma consecutiva desde el 1 hasta el 8 de tal manera que no se superpongan las frecuencias de las señales que se irradian de antenas adyacentes. Los access points poseen una dirección IP privada con el único fin

de ser monitoreados, ya que el protocolo IEEE 802.11 solo abarca hasta la capa 2 del modelo OSI.

7.1.1 Calculo de cobertura

A continuación se hace una estimación de la cobertura radioeléctrica del MAP. Este modelo de cobertura se utilizara en todos los MAP y Repeaters, debido a que utilizan los mismos dispositivos inalámbricos.

El calculo de la cobertura del sistema esta basado en el hecho de que los nodos finales deben tener una línea de visión directa con las antenas del MAP. No obstante, es posible establecer el enlace aun cuando no existe una línea de visión si las distancias entre antenas son cortas.

Se desea obtener un radio de cobertura de 1,5 Km. y también se pretende que exista una velocidad de conexión de 11 Mbps. Sobre la base de estos parámetros se calcula la ganancia que debe poseer la antena utilizada por el usuario.

7.1.2 Potencia recibida en el receptor (usuario)

La frecuencia utilizada para el calculo del enlace es de 2,44 GHz, ya que dependiendo del canal de transmisión utilizado, la frecuencia puede variar desde 2,4 GHz para el canal 1 hasta 2,4835 para el canal 11. Además, se utilizan los cables coaxiales que traen los access points y se inserta un protector gaseoso entre la antena y el access point, tanto en el transmisor como en el receptor.

Datos

Potencia transmisor (PT) = 16 dBm
Ganancia antena transmisora (GA) = 8,5 dBi
Perdida total en cables = 0,6 dB
Perdida por cada protector gaseoso = 0,5 dB
Perdida por cada conector = 0,5 dB
Distancia = 1,5 Km.
Frecuencia = 2,440 GHz
Potencia recibida (PR) = -85 dBm

$$Margen\ de\ Fading = -30\log D - 10\log(6Abf) + 10\log(1-q) + 70$$

Donde
D = Distancia (Km.)
A = Rugosidad del terreno (1 para tierras intermedias)
B= Factor de conversión de probabilidad del peor mes a probabilidad anual (0,25 área mediterránea)
F =frecuencia (GHz)
Q= Objetivo de calidad del enlace (99,999 %)

Margen de Fading (MF) = 9,9 dB

Perdida en el espacio libre (dB) = -20 log (FREC(MHz)) –20 log (distancia) –32,46
Perdida en el espacio libre (dB) = -20 log (2440) –20 log (1,5) –32,46
Perdida en el espacio libre = -103,72 dB

Perdidas varias (dB) = Perd conectores + Perd protector gaseoso + Perd cable
Perdidas varias (dB) = 0,5x8 + 0,5 x 2 + 0,6
Perdidas varias = 5,6 dB

GR = PR – PT –GT + Perdidas varias + Perdida en espacio libre + MF
GR = -85 dBm –16 dBm –8.5 dBi + 5,6 dB + 103,72 dB + 9,9 dB

GR = 9,72 dB

7.1.3 Potencia recibida en el MAP

En base al calculo anterior se elige una antena panel de 14 dBi de ganancia y se comprueba que la potencia recibida en el MAP sea la adecuada.

Potencia transmisor (PT) = 15 dBm
Ganancia antena transmisora (GA) = 14 dBi
Ganancia antena Receptora (GR) =8,5 dBi
Perdida en el espacio libre = -103,72 dB
Perdidas varias = 5,6 dB
Potencia recibida (PR) = -82 dBm – 11 Mbps
MF = 9,9 dB

PR = PT + GR + GT - Perdidas varias - Perdida en espacio libre - MF
PR = 15 dBm +8,5 dBi + 14 dBi –5,6 dB –103,72 dB – 9,9 dB
PR = -81,72 dBm

Se concluye que se puede establecer el enlace en condiciones aceptables, siempre que las antenas estén en una línea de visión directa.

7.1.4 Mediciones Practicas

Para complementar el calculo teórico se hicieron mediciones de campo a distintas distancias del MAP utilizando una notebook equipada con una adaptador de red inalámbrico. Las mismas se realizaron con el software *Netwok Stumbler*, el cual permite medir la potencia de las distintas señales en la banda de 2.4 GHz discriminándolas a partir del SSID y de la dirección MAC del access point del cual provengan.

Se tomaron 6 mediciones radiales a distancias de aproximadamente 1,5 Km. del MAP. No se tomaron mas mediciones ya que no se pudo tener acceso a las terrazas de los edificios necesarios para realizar las mediciones optimas.

A continuación se muestra una pantalla con una medición efectuada y su equivalente en formato xls.

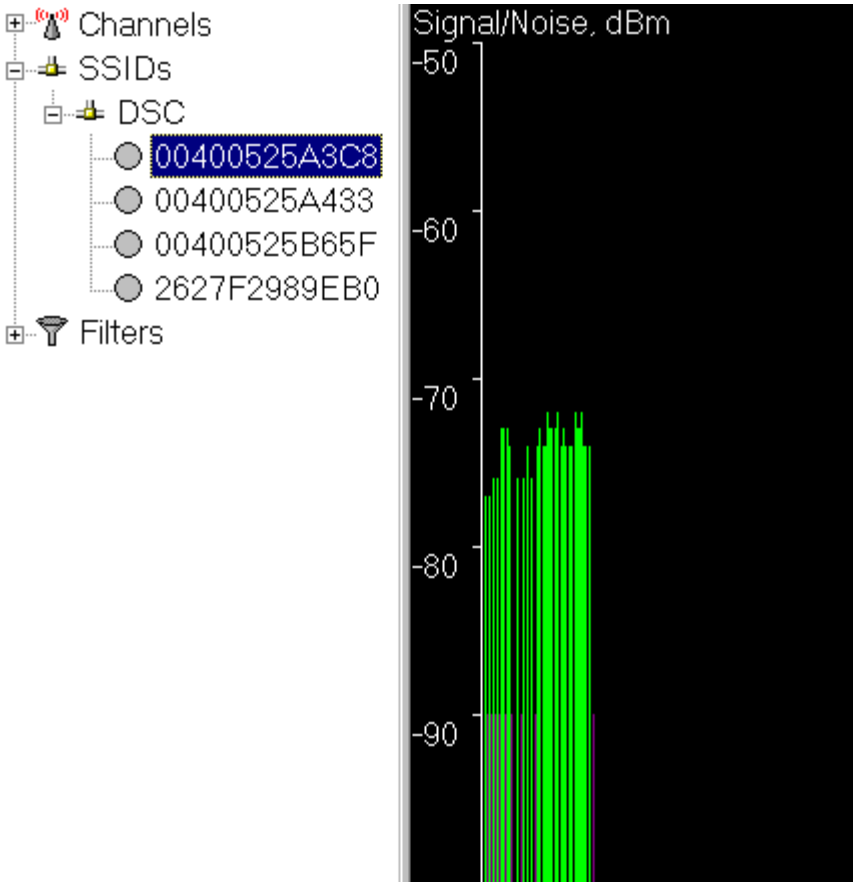


Figura 7.6 Pantalla del software de medición Networt Stumbler

# $Creator: Network Stumbler Version 0.3.30						
# $Format: wi-scan summary with extensions						
# Latitude	Longitude	(SSID)	Type	(BSSID)	Time (GMT)	[SNR Sig Noise]
# $DateGMT: 2004-01-12						
N 0.0000000	E 0.0000000	(DSC)	ad-hoc	(26:27:f2:98:9e:b0)	00:37:49 (GM	[0 49 49]
N 0.0000000	E 0.0000000	(DSC)	BBS	(00:40:05:25:b6:5f)	00:38:14 (GM	[31 80 49]
N 0.0000000	E 0.0000000	(DSC)	BBS	(00:40:05:25:a4:33)	00:38:14 (GM	[30 79 49]
N 0.0000000	E 0.0000000	(DSC)	BBS	(00:40:05:25:a3:c8)	00:38:29 (GM	[28 77 49]

La siguiente tabla muestra las mediciones efectuadas usando este software. Solo se muestran las potencias de las señales con mayor nivel.

Ubicacion	Distancia	Señal (dBm)
Bedoya y Rivera Indarte	1,3 Km	-89 dBm
Hirigoyen 146	1,2 Km	-90 dBm
Sta y Puyrredon	1,4 Km	-86 dBm
Bv Los Andes y Cerrito	1,2 Km	-88 dBm
Shopping Nvo Centro	1,1 Km	-78 dBm
Colon y Haedo	1,2 Km	-90 dBm

Cabe destacar que la medición de potencia se efectuó sin una antena receptora. Debido a este hecho, no coincide el calculo teórico con la medición practica.

7.2 Servidores de acceso

Estos servidores son los que conectan a cada MAP con Internet. Como se observa en la figura 6.1, los mismos se utilizan para la autenticacion y administración de los usuarios que quieran acceder a los servicios de Internet. La autenticación y la tarifación de los usuarios telefónicos la realiza la empresa VoIP utilizando el protocolo RADIUS. Como vemos en la figura, las computadoras de los usuarios poseen una dirección IP "privada" en el rango de 10.20.0.150 a 10.20.255.254, que no son ruteables a través de Internet, además, las mismas poseen como puerta de enlace la dirección IP del servidor de acceso (10.20.0.1); por lo tanto, cuando una maquina intente acceder a Internet será dirigida hacia el servidor de acceso, el cual mediante un *portal captivo* le pedirá un nombre de usuario y contraseña.

Esto es posible ya que todas las maquinas se encuentran en la misma red interna, por lo tanto pueden comunicarse con otras computadoras que estén en su misma red, aunque todas posean una dirección IP no ruteable a través de Internet.

El caso de los teléfonos es totalmente distinto al de las computadoras. Estos poseen una dirección IP "publica" que es ruteable a través de Internet, por lo tanto, se comunican, a través del router de acceso a Internet, directamente con el gatekeeper de la empresa VoIP, donde se realiza la autenticación y facturación.

Cuando una computadora quiere acceder a una pagina Web es redirigida hacia una pagina Web del servidor de acceso, donde se le pide un nombre de usuario y contraseña. Esta pagina, se denomina "portal captivo" y en realidad es un software que corre bajo Windows llamado " Firstspot" que se encarga de la administración de las cuentas de usuarios, autenticación, etc.

Firstspot tiene un servidor de autenticación basado en una base de datos de access. La misma se construye automáticamente al ingresar los parámetros de las cuentas de los usuarios en el menú de configuración del software. Estos parámetros son:

- Nombre de la cuenta del usuario. Es el que debe ingresar el mismo cuando el portal captivo le solicita un nombre de usuario.
- El password de la cuenta del usuario.
- Tiempo de navegación. Este parámetro se utiliza para ingresar los minutos de navegación que posee el usuario. Cada vez que ingresa a Internet se le descuentan los minutos de navegación que posee su cuenta. Este parámetro esta pensado para los usarios que poseen cuentas prepagas.
  Si no se ingresa ningún valor en este parámetro el usuario puede acceder a Internet sin ninguna restricción de tiempo.
- Limitación del ancho de banda. Es posible definir en Kbytes/ seg el ancho de banda de subida y de bajada correspondiente a cada usuario. Este parámetro se utiliza para que siempre exista un ancho de banda disponible para telefonía.

Además de todo esto, en la base de datos se guarda la fecha y hora en que el usuario se logueo y se deslogueo en el servidor. A partir de esta base de datos se tiene pensado construir en el futuro un software que realice la tarifación de los usuarios.

Este software también cumple la función de DNS y servidor DHCP proveyéndoles a los usuarios una dirección IP en el rango de 10.20.0.150 a 10.20.255.254, la mascara de subred, la dirección IP de la puerta de enlace (10.20.0.1) y la dirección IP del servidor DNS (10.20.0.1); por lo tanto las computadoras de los usuarios deben estar configuradas para obtener su dirección IP y la dirección del servidor DNS automáticamente.

Cabe aclarar que a cada MAP se conectan dos servidores de acceso mediante un swicht. El primero es una PC Pentium IV con 256 MB de RAM corriendo el software Firstspot en una plataforma Windows 2000 Server.

El segundo servidor de acceso es una imagen del primero y se utiliza de backup en caso de que ocurra algún problema con el primer servidor.

El conjunto de dos servidores de acceso mas un swicht, una pacthera y una UPS de 700 VA y 230 Volts se montan en un rack dentro de un gabinete.

Los servidores de acceso correspondientes al MAP Columbus están ubicados en la empresa InterWave.

Control del ancho de banda

Como se menciono anteriormente, el software Firstspot realiza el control del ancho de banda. El ancho de banda máximo asignado a cada usuario se calcula tomando como referencia que la conexión desde un *servidor de acceso* a Internet posee un ancho de banda de 1 Mbps y el 80 % del mismo debe ser usado para los servicios telefónicos.

Por lo tanto solo restan 200 Kbps para ser utilizados en los otros servicios de Internet. Además, se estima que en el futuro cada MAP o Repeater podrá alojar 90 usuarios, de esta forma, para la situación de que exista un MAP y un Repeater saliendo ambos por la misma conexión a Internet, existirá un máximo de 180 usuarios, de los cuales se estima que solo el 30 % utilizara el servicio de telefonía simultáneamente. Basándonos en el calculo del ancho de banda por usuario de la sección 5.3 y dejando un margen, obtenemos que cada usuario de telefonía utilizara 20 Kbps.

A cada usuario se le asigna para los servicios de Internet un ancho de banda de bajada de 40 Kbps, teniendo en cuenta que el trafico de Internet es en forma de ráfagas. De esta manera, se le permite al usuario navegar a una velocidad moderada y además no se satura el sistema.

Se debe aclarar que en esta primera fase del proyecto, existirá un máximo de 256 usuarios. Cantidad que se incrementara cuando la empresa VoIP implemente el protocolo SIP.

7.3 Repeater

Como se observa en la figura 7.1 el Repeater tiene la misión de extender la cobertura del sistema. El mismo es idéntico al MAP, con la diferencia de que el Repeater se conecta a Internet de manera inalámbrica a través de un MAP.

Un Repeater esta compuesto de 6 u 8 access point conectados a sus respectivas antenas. Las mismas son idénticas a las del MAP; por lo tanto se logra una cobertura omnidireccional.

Estos access point se conectan mediante cable UTP Cat5 a un switch de 16 puertos. En el mismo swicht se conecta a un bridge que esta configurado para asociarse a algún access point correspondiente a un MAP; cabe aclarar que el bridge siempre se asociara al access point del cual reciba mayor nivel de señal.

El bridge esta conectado a una antena de 14 dBi mediante un cable RG-213 de 60 cm.

A continuación se muestra el esquema de conexión de un Repeater.

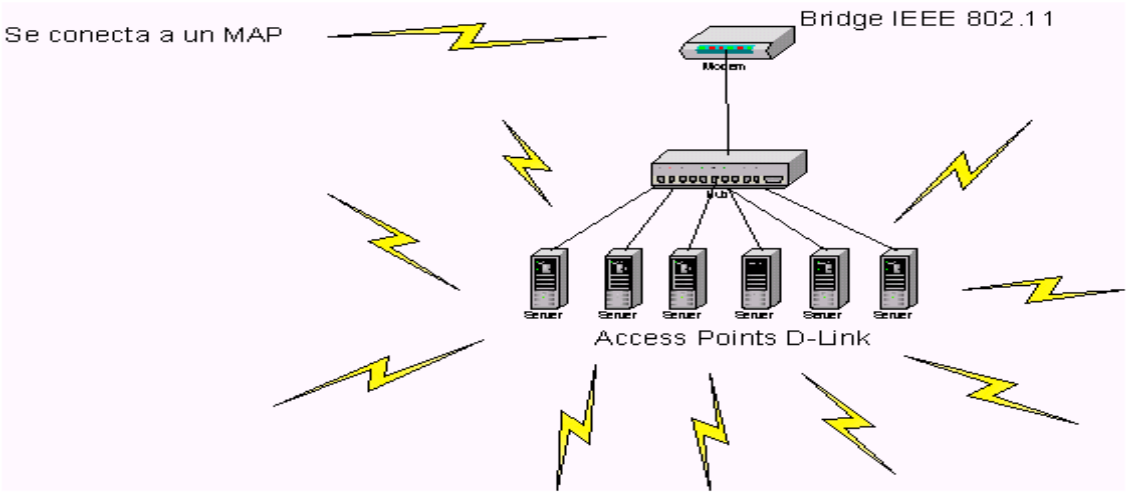


figura 7.7 Esquema del repeater

La configuración física del repeater también es idéntica a la del MAP, es decir, que los access points se agrupan de a par dentro de un gabinete llamado "Slave" y dentro de un gabinete mas grande se coloca una patchera, un swicht de 16 puertos y una UPS de 700 VA. La alimentación de todos los dispositivos wireless se realiza a través del cable UTP.

Hasta el momento se ha instalado un Repeater en la intersección de las calles Sta Cruz y Pueirredon (Barrio Observatorio), el mismo se encuentra a una distancia del MAP Columbus de 1,4 Km. en línea recta.

A continuación se muestra la configuración de los dispositivos que integran el único Repeater instalado hasta el momento. La configuración de los Repeaters que se instalen en el futuro será idéntica a este, siendo la dirección IP de los dispositivos la única variante.

7.3.1 Configuración de los access points

Parametro	Valor	Descripción
SSID	DSC	Identificador de la red inalámbrica
Channel	1 al 8	Canal de transmisión
Wep	Deshabilitado	Cifrado de la información
Dirección IP	10.20.0.11 al 10.20.0.18	Permite ingresar al menu web
Mascara de subred	255.255.0.0	
Servidor DHCP	Deshabilitado	El AP incorpora un servidor DHCP
Beacon Interval	100 ms	Intervalo de la trama de sincronización
DTIM Interval	3	Intervalo de la trama DTIM
Tx Rates	Auto	Velocidad de transmisión
Wireless mode	Mixto	Funciona como 802.11b y 802.11g
Aautenticacion	Open System	Metodo de autenticación
SSID Broadcast	Habilitado	Permite que los usuarios visualicen el SSID

7.3.2 Configuración del Bridge

Parametro	Valor
Device Name	Bridge 0001
Direccion IP	10.20.0.19
Mascara de subred	255.255.0.0
SSID	DSC
Tipo de red	Infraestructura
Wep	Desabilitado
Velocidad de transmision	Automatica
AP density	Media
Filtro de encriptacion	Desabilitado

Como se menciono anteriormente, el bridge se asocia al access point del que recibe mas señal, por lo tanto al estar ubicado físicamente muy cerca de los access point que integran el Repeater siempre recibirá el mayor nivel de señal por parte de estos y se asociara a algún access point del Repeater. Pero si esto ocurre se formara un lazo cerrado y los usuarios no podrán acceder a Internet. además, al estar el bridge conectado a los access points mediante cable UTP se produce un desperfecto del primero que origina un conflicto de direcciones IP con los demás dispositivos de su red.

Este inconveniente se soluciona evitando que el bridge se asocie a algún access point del Repeater. Para lograr esto se habilita en cada access point del mismo el filtro de direcciones MAC. En este filtro se introduce la dirección MAC del bridge y se habilita la opción “no dejar que estas MAC se asocien al access point”.

7.4 Nodo semifijo

Este termino se refiere al artefacto que le permite al usuario tener acceso a Internet y realizar llamadas telefónicas.

Como su nombre lo indica, este dispositivo puede ser trasladado de un lugar a otro siempre que se tenga cobertura. En realidad, esta pensado para ser usados en lugares que tengan una línea de visión con un MAP o Repeater bastante despejada.

El nodo semifijo esta compuesto por una antena omnidireccional de 2 dBi de ganancia, un bridge inalámbrico IEEE 802.11b , un swicht de 4 puertos, un terminal H.323 ATA 186 y una fuente de alimentación de 5 volts.

figura 7.8 Nodo semifijo

Hasta el momento se han desarrollado 8 nodos semifijos, los cuales son utilizados para efectuar pruebas y demostraciones en cercanía del MAP y del Repeater actualmente instalado. Sobre la base de uno de estos 8 nodos se muestra a continuación la configuración de los distintos componentes del mismo.

Bridge inalámbrico IEEE 802.11

Parametro	Valor
Device Name	Bridge 0002
Direccion IP	10.20.0.20 a 10.20.0.27
Mascara de subred	255.255.0.0
SSID	DSC
Tipo de red	Infraestructura
Wep	Desabilitado
Velocidad de transmision	Automatica
AP density	Media
Filtro de encriptacion	Desabilitado

El terminal H.323 que permite realizar llamadas telefónicas tiene una configuración idéntica a la que se explica en la sección 5.4 . Al usar esta configuración se utiliza solamente un puerto FXS del ATA 186 con el codec G.729A. El otro puerto FXS se configura automáticamente con el codec G.711 y no se utiliza.

De esta manera, se sacrifica un puerto FXS en pos de una mejor calidad de audio.

Como se ve en la figura anterior, el nodo semifijo posee dos conectores RJ-45 hembra que son utilizados para conectar una computadora y un conector RJ-11 que se usa para conectar un teléfono analógico al terminal H.323. Este teléfono es el Panasonic Kx-TS500 y forma parte del nodo semifijo.

En un futuro, se tiene planeado incorporar una UPS al nodo semifijo, ya que la Comisión Nacional de Comunicaciones exige que el servicio telefónico sea brindado en forma independiente de la energía eléctrica. Es decir, que el teléfono debe seguir funcionando cuando no exista disponibilidad de energía eléctrica.

7.5 Nodo Fijo

El nodo fijo es utilizado para que los usuarios puedan tener servicio telefónico y acceder a Internet en los lugares donde debido al escaso nivel de señal no sea posible utilizar un nodo semifijo.

Este nodo fijo, como su nombre lo indica posee una antena direccional que permanece siempre en el mismo lugar.

El nodo fijo existe en dos versiones; la de un único usuario y la de múltiples usuarios.

- Unico usuario: En este caso, el nodo esta compuesto por una antena panel de 14 dBi apuntando a un MAP o Repeater, la que esta fijada en un lugar donde posea una línea de visión directa con el MAP o Repeater de manera que permita obtener un nivel de señal adecuado. Junto a la antena se coloca un gabinete que contiene un bridge IEEE 802.11b conectado a la misma, un swicht de 4 puertos y un terminal H.323 ATA 186. Desde este gabinete se bajan un cable UTP CAT5 y un par telefónico hasta la ubicación del usuario. Además, desde esta se sube un cable de alimentación hasta el gabinete.
- Múltiples usuarios: En este caso se coloca la misma antena direccional que en el caso anterior y junto a la misma se colocan dentro de un gabinete un bridge IEEE 802.11b, un swicht de 16 puertos y una UPS de 700 VA. Desde este swicht se baja con un cable UTP hasta la ubicación de cada usuario. Una vez arribado a esta ubicación, se conecta este cable a un swicht de 4 puertos donde se conecta el terminal H.323 ATA 186 y además se provee una conexión a Internet. Los dispositivos anteriormente mencionados se encuentran dentro de un gabinete similar al del nodo semifijo.

Cabe aclarar que todavía no se ha desarrollado ningún nodo fijo.

8 Equipos utilizados en cada componente de la red

Ubicacion	Descripcion	Marca	Modelo
MAP	Access Point IEEE 802.11g	D-Link	DWL-2000AP
	Antena Pico Cell	D-Link	ANT24-0801
	Patchera de conexion	AMP	Netconnect
	Descargadores gaseosos	D-Link	ANT24-SP
	UPS de 700VA 230 Volts	APC	SU700INET
	Swicht de 16 puertos	D-Link	DES1016D
Repeater	Access Point IEEE 802.11g	D-Link	DWL-2000AP
	Antena Pico Cell	D-Link	ANT24-0801
	Patchera de conexion	AMP	Netconnect
	Descargadores gaseosos	D-Link	ANT24-SP
	UPS de 700VA 230 Volts	APC	SU700INET
	Swicht de 16 puertos	D-Link	DES1016D
	Bridge IEEE 802.11b	Linksys	Wet11
	Antena Panel 14 dBi	D-Link	ANT24-1400
Servidores de acceso	PC Pentiun IV	Generica	
Nodo semifijo	Terminal H.323	Cisco	ATA 186
	Bridge IEEE 802.11b	Linksys	Wet11
	Swicht de 4 puertos	Intellinet	
	Telefono analogico	Panasonic	Kx-Ts500
Nodo Fijo	Terminal H.323	Cisco	ATA 186
	Bridge IEEE 802.11b	Linksys	Wet11
	Swicht de 16 puertos	D-Link	DES1016D
	Telefono analogico	Panasonic	Kx-Ts500
	Swicht de 4 puertos	Intellinet	
	Antena Panel 14 dBi	D-Link	ANT24-1400

9 Referencias

(In)seguridad en redes 802.11b-Pau Oliva. Febrero de 2003.
Teoría de Radio y planeo de link para Wireless LAN.
VHF/UHF/Microwave Radio Propagation: A Primer for Digital Experimenters.
Introduction to 802.1X for Wireless Local Area Networks.
802.1X Offers Authentication and Key Management.- Jim Geier.
SECURITY for WLAN –Henric Johnson-Institute of Technology Sweden.
What is 802.1x?- Joel Snyder, Network World Global Test Alliance- Junio de 2002
RFC 2865 (RADIUS).
Voice over IP Protocols for voice transmission.
RFC 2663 (NAT)
El estándar IEEE 802.11 Wireless LAN- Francisco López Ortiz.
Using RADIUS For WLAN Authentication-Lisa Phifer.
www.H323forum.org
www.wi-fiplanet.com
www.d-link.com
www.cisco.com
www.dualgatekeeper.com
www.patronsoft.com/firstspot
www.netstumbler.com

10 Anexo

10.1 Esquema de costos

MAP					
Componente	***Marca***	***Precio unitario (US$)***	***Cantidad***	***Proovedor***	***Total***
Gabinete	Gabexel		1	Richetta	
UPS + modulo de monitoreo	APC 700 VA	847	1	Compuserv	847
Swicht de 16 puertos	D-Link	112	1	Compuserv	112
Patchera	AMP	71.85	1	Compuserv	71.85
Gabinete Slave	Gabexel	12	4	Richetta	48
Access Point	D-Link	148.41	8	PC-Arts	1187.28
Antena + Descargador y coaxial	D-Link	140	8	PC-Arts	1120
Poste		9	4	Caños Cordoba	36
Otros					16
					3438.13

Servidores de acceso					
Componente	***Marca***	***Precio unitario (US$)***	***Cantidad***	***Proovedor***	***Total***
Rack + accesorios	AMP	800	1	Compuserv	800
PC	Intel Pentiun IV	1000	2	Pentacom	2000
Licencia software	Firstspot	295	1	Patronsoft	295
Swicht de 16 puertos	D-Link	112	1	Compuserv	112
UPS + modulo de monitoreo	APC 700 VA	847	1	Compuserv	847
					4054

Nodo Semifijo					
Componente	***Marca***	***Precio unitario (US$)***	***Cantidad***	***Proovedor***	***Total***
Gabinete	Gabexel	15	1	Richetta	15
Bridge inalambrico	Linksys	110	1	Solution Box	110
Swicht	Intellinet	20	1	PC-Arts	20
Terminal H.323	Cisco ATA 186	176	1	PC-Arts	176
Telefono	Panasonic	27	1	Julia Saul	27
					348

10.2 Hojas de datos técnicos

DWL-2000AP+

Standards

- IEEE 802.11g
- IEEE 802.11
- IEEE 802.11b
- IEEE 802.3
- IEEE 802.3u

Device Management

- Web-Based- Internet Explorer v6 or later; Netscape Navigator v6 or later; or other Java-enabled browsers
- DHCP Server and Client

Wireless Operating Range

- Indoors – up to 328 feet (100 meters)
- Outdoors – up to 1312 feet (400 meters)

Temperature

- Operating: 32ºF to 149ºF (0ºC to 55ºC)
- Storing: 4ºF to 167ºF (-20ºC to 75ºC)

Humidity:

- 95% maximum (non-condensing)

Safety and Emissions:

- FCC
- UL

Wireless Frequency Range:

- 2.4GHz to 2.4835GHz

Wireless Data Rates with Automatic Fallback:

- 54 Mbps
- 48 Mbps
- 36 Mbps
- 24 Mbps
- 22 Mbps
- 18 Mbps
- 12 Mbps
- 11 Mbps
- 9 Mbps
- 6 Mbps
- 5.5 Mbps
- 2 Mbps
- 1 Mbps

Technical Specifications (continued)

Receiver Sensitivity:

- 54Mbps OFDM, 10% PER, -68dBm
- 48Mbps OFDM, 10% PER, -68dBm
- 36Mbps OFDM, 10% PER, -75dBm
- 24Mbps OFDM, 10% PER, -79dBm
- 22Mbps PBCC, 8% PER, -80dBm
- 18Mbps OFDM, 10% PER, -82dBm
- 12Mbps OFDM, 10% PER, -84dBm
- 11Mbps CCK, 8% PER, -82dBm
- 9Mbps OFDM, 10% PER, -87dBm
- 6Mbps OFDM, 10% PER, -88dBm
- 5.5Mbps CCK, 8% PER, -85dBm
- 2Mbps QPSK, 8% PER, -86dBm
- 1Mbps BPSK, 8% PER, -89dBm

Physical Dimensions:

- L = 5.6 inches (142mm)
- W = 4.3 inches (109mm)
- H = 1.2 inches (31mm)

Wireless Transmit Power:

- 11g: 14dBm typical
- 11b: 16dBm typical

Security:

- 802.1x
- WPA*-WiFi Protected Access
  (64-,128-,256-WEP with TKIP, MIC, IV Expansion, Shared Key Authentication)

External Antenna Type:

- 2.0dBm gain with reverse SMA connector

Modulation Technology:

- Orthogonal Frequency Division Multiplexing (OFDM)
- Complementary Code Keying (CCK)
- Complementary Code Keying (PBCC)

**WPA will be available Q4 2003*

Technical Specifications (continued)

Media Access Control:

- CSMA/CA with ACK

Power Input:

- Ext. Power Supply DC 5V, 2.5A

Weight:

- .44 lbs. (200 g)

Wireless Bridge Linksys WET11

Model	WET11
Standards	IEEE 802.11b, IEEE 802.3
Ports	One 10BaseT RJ-45 port, Power port
Buttons	MDI/MDI-X slide switch, Reset button
Cabling Type	Category 5 or better
LEDs	Power, LAN, WLAN, Diag
Peak Gain of Antenna	5 dBi
Transmit Power	15 dBm @ Normal Temperature
Receive Sensitivity	-85 dBm
Security	WEP 64/128-bit
Dimensions	4.72" x 1.22" x 3.70" (120 mm x 31 mm x 94 mm)
Unit Weight	7.04 oz. (0.2 kg)
Power	External, DC 5V
Certifications	FCC, CE, IC-03, Wi-Fi
Operating Temp.	32°F to 104°F (0°C to 40°C)
Storage Temp.	-4°F to 158°F (-20°C to 70°C)

Technical Specifications

Electrical Specifications

Frequency Range
2.3-2.5GHz

Gain
14 dBi

VSWR
1.5:1 Max

Polarization
Linear, vertical

HPBW
- horizontal - 30°
- vertical- 30°

Front to Back Ratio
15 dB

Downtilt
0°

Power Handling
50W (cw)

Impedance
50 Ohms

Connector
N female

Cable
(N-male to RP-SMA plug) - 1.5 feet - 0.83db lost per meter

Environmental & Mechanical Characteristics

Temperature
-40°F to 176°F (-40°C to 80°C)

Humidity
100%@ 77°F (25°C)

Lightning Protection
DC ground

Radome Color
Gray-white

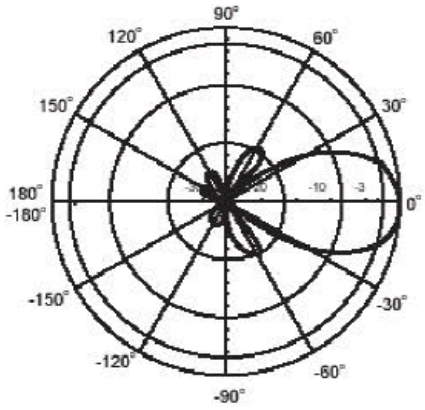
Radome Material
ABS, UV resistant

Weight
1.82 lbs (0.825kg)

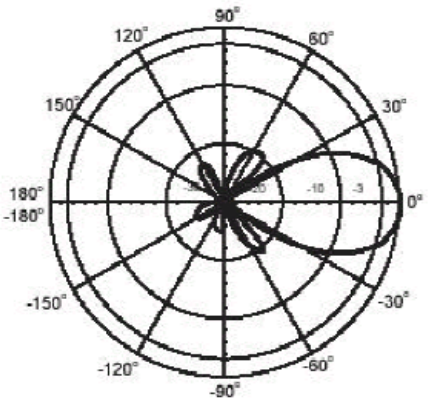
Dimensions
9.45 x 9.45 x 2.74 in. (240 x 240 x 69.5 mm)

Survival Wind Speed
112 miles/hr

Warranty
1 Year



Horizontal



Vertical

www.dlink.com
D-Link Systems, 53 Discovery Drive
Irvine, CA 92618 • 949.788.0805

D-Link ANT24-0801

8.5dBi Pico Cell Patch Antenna

Data Sheet

Technical Specifications

Electrical Specifications

Frequency Range
2300 MHz -2500 MHz

Gain
8.5dBi

VSWR
1.5: 1 Max

Polarization
Linear, vertical

HPBW
- horizontal: 70°
- vertical: 65°

Front to Back Ratio
15 dB

Power Handling
50W (cw)

Impedance
50 Ohms

Connector
N-female

Cable Length
3 Meters

Environmental & Mechanical Characteristics

Survival Wind Speed
200 km/hr

Temperature
-40°C to 80°C

Humidity
100% @ 25°C

Lightning Protection
DC ground

Radome Color
Gray-white

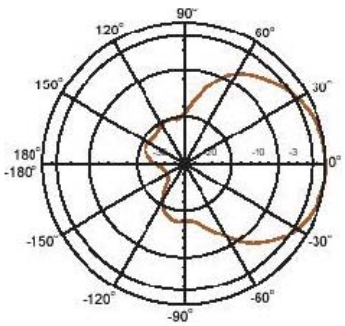
Radome Material
ABS, UV resistant

Housing Material
AL6063

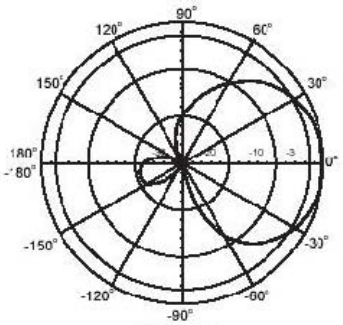
Weight
0.3 kgw

Dimensions
120 x 120 x 43mm

Warranty
1 Year



Horizontal



Vertical

www.dlink.com
D-Link Systems, 53 Discovery Drive
Irvine, CA 92618 • 949.788.0805

Cisco ATA Specifications

This section describes the Cisco ATA specifications:

Note The term *Cisco ATA* is used throughout this manual to refer to both the Cisco ATA 186 and the Cisco ATA 188, unless differences between the Cisco ATA 186 and Cisco ATA 188 are explicitly stated.

Physical Specifications

Table C-1 Physical Specifications

Description	Specification
Dimensions	1.5 x 6.5 x 5.75 in. (3.8 x 16.5 x 14.6 cm) (H x W x D)
Weight	15 oz (425 g)

Electrical Specifications for Cisco ATA

Table C-2 Electrical Specifications

Description	Specification
Power	3.5 to 7.5W (idle to peak)
DC input voltage	+5.0 VDC at 1.5A maximum
Power adaptor	Universal AC/DC ~3.3 x 2.0 x 1.3 in. (~8.5 x 5.0 x 3.2 cm) ~4.8 oz (135 g) for the AC-input external power adaptor ~4 ft (1.2 m) DC cord 6 ft (1.8 m) cord

Environmental Specifications

Table C-3 Environmental Specifications

Description	Specification
Operating temperature	41 to 104° F (5 to 40° C)
Storage temperature	–4 to 140° F (–20 to 65° C)
Relative humidity	10 to 90% noncondensing, operating, and nonoperating/storage

Immunity Specifications

EN50082-1, including the following:

- EN61000-3-2, Electromagnetic Compatibility
- EN61000-3-3, Electromagnetic Compatibility
- EN61000-4-2, ESD
- EN61000-4-3, Radiated Immunity
- EN61000-4-4, Burst Transients
- EN61000-4-5, Surge
- EN61000-4-6, Injected RF
- EN61000-4-11, Dips and Sags

Physical Interfaces

Table C-4 Physical Interfaces

Description	Specification
Ethernet	Two RJ-45, IEEE 802.3 10BASE-T standard
Analog telephone	Two RJ-11 FXS voice ports
Power	5 VDC power connector
Indicators	Function button with integrated status indicator Link and activity LED indicating network activity

Ringing Characteristics

Table C-5 Ringing Characteristics

Description	Specification
Tip/ring interfaces for each RJ-11 FXS port (SLIC)	
Ring voltage	$40V_{RMS}$ (typical, balanced ringing only)
Ring frequency	25 Hz
Ring waveform	Trapezoidal with 1.2 to 1.6 crest factor
Ring load	1400 ohm + 40 microF (per line)
Ringer equivalence number (REN)	Up to 5 REN per RJ-11 FXS port
Loop impedance	Up to 200 ohms (plus 430-ohm maximum telephone DC resistance)
On-hook/off-hook characteristics	
On-hook voltage (tip/ring)	–50V
Off-hook current	25 mA (nominal)
RJ-11 FXS port terminating impedance option	The Cisco ATA186-I1 and Cisco ATA188-I1 provide 600-ohm resistive impedance. The Cisco ATA186-I2 and Cisco ATA188-I2 provide 270 ohm + 750 ohm // 150-nF complex impedance.

Software Specifications

Table C-6 Software Specifications (All Protocols)

Description	Specification
Call progress tones	Configurable for two sets of frequencies and single set of on/off cadence
Dual-tone multifrequency (DTMF)	DTMF tone detection and generation

Table C-6 Software Specifications (All Protocols) (continued)

Description	Specification
Fax	G.711 fax pass-through and G.711 fax mode. Enhanced fax pass-through is supported on the Cisco ATA. Success of fax transmissions up to 14.4 kbps depends on network conditions, and fax modem/fax machine tolerance to those conditions. The network must have reasonably low network jitter, network delay, and packet-loss rate.
Line-echo cancellation	• Echo canceller for each port • 8 ms echo length • Nonlinear echo suppression (ERL > 28 dB for frequency = 300 to 2400 Hz) • Convergence time = 250 ms • ERLE = 10 to 20 dB • Double-talk detection
Out-of-band DTMF	• H.245 out-of-band DTMF for H.323 • RFC 2833 AVT tones for SIP, MGCP, SCCP
Configuration	• DHCP (RFC 2131) • Web configuration via built-in Web server • Touch-tone telephone keypad configuration with voice prompt • Basic boot configuration (RFC 1350 TFTP Profiling) • Dial plan configuration • Cisco Discovery Protocol for SCCP
Quality of Service	• Class-of-service (CoS) bit-tagging (802.1P) • Type-of-service (ToS) bit-tagging
Security	• H.235 for H.323 • RC4 encryption for TFTP configuration files
Voice coder-decoders (codecs)	**Note** In simultaneous dual-port operation, the second port is limited to G.711 when using G.729. • G.723.1 • G.729, G.729A, G.729AB • G.723.1 • G.711A-law • G.711µ-law

Table C-6 Software Specifications (All Protocols) (continued)

Description	Specification
Voice features	• Voice activity detection (VAD) • Comfort noise generation (CNG) • Dynamic jitter buffer (adaptive)
Voice-over-IP (VoIP) protocols	• H.323 v2 • SIP (RFC 2543 bis) • MGCP 1.0 (RFC 2705) • MGCP 1.0/network-based call signalling (NCS) 1.0 profile • MGCP 0.1 • SCCP