Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

ESTUDIO DE SISTEMA DE GESTIÓN PARA RED WIMAX

Eddy Manuel Velásquez Bonilla

Asesorado por Ing. Enrique Edmundo Ruiz Carballo

Guatemala, noviembre de 2010

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

ESTUDIO DE SISTEMA DE GESTIÓN PARA RED WIMAX

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

EDDY MANUEL VELÁSQUEZ BONILLA

ASESORADO POR ING. ENRIQUE EDMUNDO RUIZ CARBALLO

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO ELECTRÓNICO

GUATEMALA, NOVIEMBRE DE 2010

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Inga. Glenda Patricia García Soria
VOCAL II	Inga. Alba Maritza Guerrero Spínola de López
VOCAL III	Ing. Miguel Ángel Dávila Calderón
VOCAL IV	Br. Luis Pedro Ortiz de León
VOCAL V	P.A. José Alfredo Ortiz Herincx
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Ing. José Anibal Silva de los Angeles
EXAMINADOR	Ing. Luis Eduardo Durán Córdova
EXAMINADOR	Ing. Julio Rolando Barrios Archila
SECRETARIA	Inga. Marcia Ivonne Véliz Vargas

HONORABLE TRIBUNAL EXAMINADOR

Cumpliendo con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

ESTUDIO DE SISTEMA DE GESTIÓN PARA RED WIMAX,

tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Eléctrica, en fecha noviembre de 2009.

Eddy Manuel Velásquez Bonilla

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERIA

Guatemala, 28 de JULIO 2010.

Ingeniero
Carlos Eduardo Guzmán Salazar
Coordinador Area de Electrònica
Escuela de Ingenierìa Mecànica Elèctrica
Facultad de Ingenierìa, USAC.

Estimado Ingeniero:

Por este medio le informo que he revisado el trabajo de graduación titulado: "ESTUDIO DE SISTEMA DE GESTIÓN PARA RED WIMAX", elaborado por el estudiante Eddy Manuel Velásquez Bonilla.

El mencionado trabajo llena los requisitos para dar mi aprobación, e indicarle que el autor y mi persona somos responsables por el contenido y conclusiones de la misma.

Atentamente,

Ing Enrique Edmundo Ruiz Carballo
ASESOR

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERIA

Ref. EIME 26. 2010
Guatemala, 28 de julio 2010.

Señor Director
Ing. Guillermo Antonio Puente Romero
Escuela de Ingenierìa Mecànica Elèctrica
Facultad de Ingenierìa, USAC.

Señor Director:

Me permito dar aprobación al trabajo de Graduación titulado: "ESTUDIO DE SISTEMA DE GESTION PARA RED WIMAX", del estudiante, Eddy Manuel Velásquez Bonilla, que cumple con los requisitos establecidos para tal fin.

Sin otro particular, aprovecho la oportunidad para saludarle.

Atentamente,
ID Y ENSEÑAD A TODOS

Ing. Carlos Eduardo Guzmán Salazar
Coordinador de Electrónica

CEGS/sro

UNIVERSIDAD DE SAN CARLOS
FACULTAD DE INGENIERIA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
GUATEMALA

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

REF. EIME 32. 2010.

El Director de la Escuela de Ingeniería Mecánica Eléctrica, después de conocer el dictamen del Asesor, con el Visto Bueno del Coordinador de Área, al trabajo de Graduación del estudiante; EDDY MANUEL VELÁSQUEZ BONILLA titulado: "ESTUDIO DE SISTEMA DE GESTIÓN PARA RED WIMAX", procede a la autorización del mismo.

Ing. Guillermo Antonio Puente Romero

UNIVERSIDAD DE SAN CARLOS
FACULTAD DE INGENIERIA
DIRECCION ESCUELA DE INGENIERIA
MECANICA ELECTRICA
GUATEMALA

GUATEMALA, 19 DE OCTUBRE 2,010.

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

DTG. 399.2010

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica, al trabajo de graduación titulado: **ESTUDIO DE SISTEMA DE GESTIÓN PARA RED WIMAX,** presentado por el estudiante universitario **Eddy Manuel Velásquez Bonilla,** autoriza la impresión del mismo.

IMPRÍMASE:

Ing. Murphy Olympo Paiz Recinos
Decano

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

Guatemala, 24 de noviembre de 2010.

/gdech

ACTO QUE DEDICO A:

Dios	Por guiarme y darme la sabiduría en este largo camino, ya que sin su voluntad y misericordia nada de esto hubiese sido posible
Mis padres	Víctor Manuel y Reyna Isabel, por su amor incondicional y apoyo que me han brindado, ya que los valores que me inculcaron desde pequeño me permitieron cumplir esta meta en mi vida
Mi abuela	María Adela Díaz, que siempre estuvo al pendiente de mí y me brindó su apoyo y consejos.
Mis abuelos	Que ya no se encuentran acá entre nosotros, pero se que en algún lugar ellos también están gozando de este éxito
Mi hermana	Rocío Isabel, que este triunfo le sirva de ejemplo a ella para que también pueda alcanzar en un futuro las suyas.
Mi novia	Rita María, por todo este tiempo en que me ha sabido brindar su amor, apoyo y comprensión
Mis tíos y tías	Que en su momento han compartido conmigo las alegrías a lo largo de este camino y de alguna u otra manera me han aconsejado y apoyado
Mis amigos	Por todas las experiencias vividas a lo largo de la carrera y porque estuvieron ahí cuando los necesite para compartir y apoyarme en los retos que se me presentaron, en especial a Karen, Evelyn, Walter, Axel, Josué, Carlos y Saúl.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

Ancho de Banda (BW) Es la cantidad de información o de datos que se puede enviar a través de una conexión de red en un período de tiempo dado. El ancho de banda se indica generalmente en bits por segundo (bps), kilobits por segundo (Kbps), o megabits por segundo (Mbps).

Broadcast Es un modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

CPE (Equipo Local del Cliente) Es un equipo de telecomunicaciones usado, tanto en interiores como en exteriores para originar, encaminar o terminar una comunicación. El equipo puede proveer una combinación de servicios, incluyendo; datos, voz, video y un host de aplicaciones multimedia interactivos.

DHCP Protocolo de configuración dinámica de host, es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente.

FHSS Es una técnica de modulación en espectro ensanchado, en el que la señal se emite sobre una serie de radiofrecuencias aparentemente aleatorias, saltando de frecuencia en frecuencia sincrónicamente con el transmisor.

Firewall Es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

HiperLAN2 Es una solución estándar, para un rango de comunicación corto que permite una alta transferencia de datos y calidad de servicio del tráfico, entre estaciones base WLAN y terminales de usuarios. La seguridad está provista por lo último en técnicas de cifrado y protocolos de autenticación.

Host Son computadores mono o multiusuario que ofrecen servicios de transferencia de archivos, conexión remota, servidores de base de datos, servidores WWW, etc. Los usuarios que hacen uso de los hosts pueden a su vez pedir los mismos servicios a otras máquinas conectadas a la red.

ICMP Es el sub protocolo de control y notificación de errores del protocolo de Internet (IP). Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado.

IP Es un protocolo no orientado a conexión, usado tanto por el origen como por el destino para la comunicación de datos, a través de una red de paquetes conmutados. Los datos en una red basada en IP son enviados en bloques conocidos como paquetes o datagramas (en el protocolo IP estos términos se suelen usar indistintamente).

IPv4 IPv4 usa direcciones de 32 bits, limitándola a 2^{32} = 4 294 967 296 direcciones únicas, muchas de las cuales están dedicadas a redes locales (LANs).

IPv6 Es una nueva versión de IP (Internet Protocol) diseñada para reemplazar a la versión 4 (IPv4), que actualmente esta implementado en la gran mayoría de dispositivos que acceden a Internet. IPv6 admite 2^{128} o 340 sextillones de direcciones.

MIB Es un tipo de base de datos que contiene información jerárquica, estructurada en forma de árbol, de todos los dispositivos gestionados en una red de comunicaciones. Es parte de la gestión de red definida en el modelo OSI.

NAT Es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles. Consiste en convertir en tiempo real las direcciones utilizadas en los paquetes transportados.

OFDM Es una multiplexación, que consiste en enviar un conjunto de ondas portadoras de diferentes frecuencias, donde cada una transporta información, la cual es modulada en QAM o en PSK.

QoS	Son las tecnologías, que garantizan la transmisión de cierta cantidad de información en un tiempo dado (throughput). Calidad de servicio es la capacidad de dar un buen servicio. Es especialmente importante para ciertas aplicaciones tales como, la transmisión de vídeo o voz.
SNMP	Es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.
Telnet	Es el nombre de un protocolo de red que sirve para acceder mediante una red a otra máquina, para manejarla remotamente como si se estuviera sentados delante de ella.
TCP	Es uno de los protocolos fundamentales en Internet. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir diferentes aplicaciones dentro de una misma máquina, a través del concepto de puerto.
UDP	Es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red, sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera

WiMAX Es una norma de transmisión de datos, que utiliza las ondas de radio en las frecuencias de 2,5 a 3,5 Ghz. Es una tecnología dentro de las conocidas como tecnologías de última milla, también conocidas como; bucle local que permite la recepción de datos por microondas y retransmisión por ondas de radio. El protocolo que caracteriza esta tecnología es el IEEE 802.16.

Wireless La comunicación inalámbrica (inglés wireless, sin cables), es aquella en la que extremos de la comunicación (emisor/receptor), no se encuentran unidos por un medio de propagación físico, sino que se utiliza la modulación de ondas electromagnéticas a través del espacio.

RESUMEN

El rápido crecimiento de las telecomunicaciones, así como la cantidad datos que se transmiten, hacen necesario contar con una red confiable y administrada de manera eficiente, que permita monitorear constantemente cada servicio que se tenga, y responder rápidamente a cualquier alarma que se presente y en lo posible solucionar el problema remotamente.

Este estudio consiste en conocer todos los elementos y conceptos, que están involucrados en una red, en este caso wireless de tecnología wimax, gestionada por medio del protocolo snmp. Esto permite una facilidad en el intercambio de información, entre el administrador y los dispositivos de red.

De esta forma se logra supervisar el buen funcionamiento de la red, buscar y resolver problemas. Esto sumado a las ventajas propias del sistema wimax como es un ancho de banda configurable, velocidades de hasta 70 Mbps, así como una distancia máxima de 50 kilómetros, logrando disponer de una red muy confiable, segura y eficiente.

OBJETIVOS

GENERAL

Realizar un estudio básico e introductivo sobre el gestionamiento de una red, enfocado en un sistema inalámbrico Wimax.

ESPECÍFICOS

- Dar a conocer los diferentes elementos involucrados en una red monitoreada Wimax y las aplicaciones de la plataforma de gestión

- Comprender la importancia del monitoreo de enlaces de telecomunicación y la detección de los problemas que puedan presentarse

- Evaluar los beneficios que tiene este sistema comparado con los costos y su debida recuperación a largo o mediano plazo

INTRODUCCIÓN

El avance de la tecnología ha traído consigo la necesidad de tener en comunicación a tantas personas como equipos por medio de redes de datos, por lo que es importante que todos estos enlaces se mantengan activos en un 99,95% del tiempo, siendo este un valor de referencia para garantizar al usuario la menor afectación posible en su enlace, el cual puede variar según las condiciones de operación del administrador. Para ello es indispensable contar con una herramienta que permita al administrador de red, estar monitoreando todos los eventos que se presenten en cada uno de los servicios, así como en los equipos que están involucrados a lo largo de toda la ruta hacia el cliente.

El detectar una falla y darle su respectiva solución en un tiempo mínimo, es algo primordial para el administrador, con ello logrará un enlace confiable y eficiente que no detenga la productividad de los abonados a su red. En un sistema Wimax que está gestionado, tiene valor agregado, ya que se tendrá una amplia cobertura de la red y al mismo tiempo se logrará solucionar problemas de conectividad, sin necesidad de trasladarse al punto remoto del cliente y esto se traduce a reducir los costos de operación del administrador de red.

1. CONCEPTOS FUNDAMENTALES

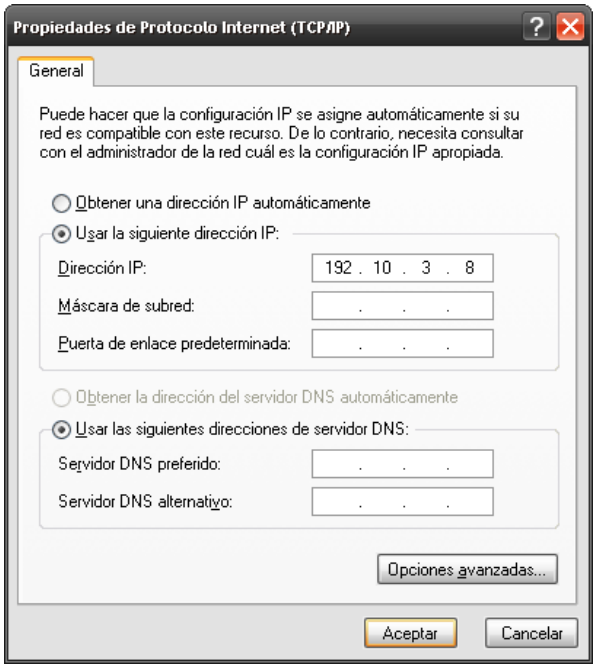
1.1 Direccionamiento IP

En esta sección se estudiará todo lo relacionado a dirección IP, el cual es un concepto fundamental en las telecomunicaciones, y en este caso no es la excepción.

Se parte de todos los elementos básicos que permitan entender como tener gestión de equipos remotos. El direccionamiento es una función clave de los protocolos de capa de Red que permite la transmisión de datos entre hosts de la misma red o en redes diferentes.

El protocolo de internet versión 4 (IPv4) ofrece direccionamiento jerárquico para paquetes que transportan datos. Se examinará detalladamente la estructura de las direcciones IPv4 y su aplicación en la construcción y prueba de redes y subredes IP.

Figura 1. **Cuadro de diálogo para asignación de IP**



1.1.1 Estructura de una dirección IPv4

Cada dispositivo de una red, debe ser definido en forma exclusiva. En la capa de red es necesario identificar los paquetes de la transmisión, con las direcciones de origen y de destino de los dos sistemas finales. Con IPv4, esto significa que cada paquete posee una dirección de origen de 32 bits y una dirección de destino de 32 bits en el encabezado de Capa 3.

Estas direcciones se usan en la red de datos como patrones binarios. Dentro de los dispositivos, la lógica digital es aplicada para su interpretación. Para quienes formamos parte de la red humana, una serie de 32 bits es difícil de interpretar e incluso más difícil de recordar. Por lo tanto, representamos direcciones IPv4 utilizando el formato decimal punteada. Los patrones binarios que representan direcciones IPv4 son expresados con puntos decimales separando cada byte del patrón binario, llamado octeto, con un punto. Se le llama octeto debido a que cada número decimal representa un byte ú 8 bits.

Por ejemplo, la dirección

10101100000100000000010000010100

es expresada en puntos decimales como

172.16.4.20

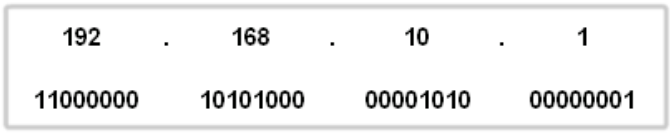
Tenga en cuenta que los dispositivos usan la lógica binaria. El formato decimal punteado se usa para que a las personas les resulte más fácil utilizar y recordar direcciones.

1.1.2 Porciones de red y de host

En cada dirección Ipv4, alguna porción de los bits de orden superior representa la dirección de red. En la Capa 3, se define una red como un grupo de hosts con patrones de bits idénticos en la porción de dirección de red, de sus direcciones.

A pesar que los 32 bits definen la dirección host Ipv4, existe una cantidad variable de bits, que conforman la porción de host de la dirección. El número de bits usado en esta porción del host determina el número de hosts que podemos tener dentro de la red.

Figura 2. **Esta dirección IP pertenece a la red 192.168.10.0**



Por ejemplo, si se necesita tener al menos 200 hosts en una red determinada, necesitaríamos utilizar suficientes bits en la porción del host para poder representar al menos 200 patrones diferentes de bits.

Para asignar una dirección exclusiva a 200 hosts, se utilizará el último octeto entero. Con 8 bits se puede lograr un total de 256 patrones de bits diferentes. Esto significa que los bits para los tres octetos superiores representarían la porción de red.

1.1.3 Tipos de direcciones en una red IPv4

Dentro del rango de direcciones de cada red IPv4, existen tres tipos de direcciones:

1. *Dirección de red:* la dirección en la que se hace referencia a la red.

2. *Dirección de broadcast:* una dirección especial utilizada para enviar datos a todos los hosts de la red.

3. *Direcciones host:* las direcciones asignadas a los dispositivos finales de la red.

1.1.3.1 Dirección de red

La dirección de red es una manera estándar de hacer referencia a una red. Por ejemplo, se podría hacer referencia a la red de la figura 3 como “red 10.0.0.0”. Ésta es una manera mucho más conveniente y descriptiva de referirse a la red que utilizando un término como "la primera red". Todos los hosts de la red 10.0.0.0 tendrán los mismos bits de red.

Dentro del rango de dirección IPv4 de una red, la dirección más baja se reserva para la dirección de red. Esta dirección tiene un cero para cada bit de host en la porción de host de la dirección.

1.1.3.2 Dirección de broadcast

La dirección de broadcast IPv4 es una dirección especial para cada red que permite la comunicación a todos los host en esa red. Para enviar datos a

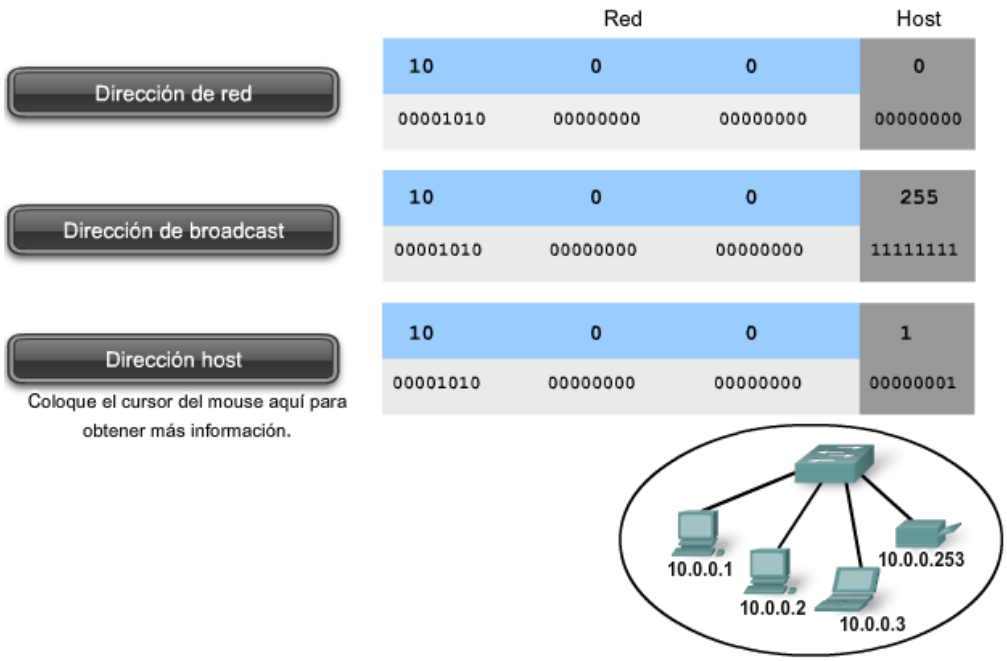
todos los hosts de una red, un host, puede enviar un solo paquete dirigido a la dirección de broadcast de la red.

La dirección de broadcast utiliza la dirección más alta en el rango de la red. Ésta es la dirección en la cual los bits de la porción de host son todos 1. Para la red 10.0.0.0 con 24 bits de red, la dirección de broadcast sería 10.0.0.255. A esta dirección se conoce como *broadcast dirigido*.

1.1.3.3 Direcciones host

Como se describe anteriormente, cada dispositivo final requiere una dirección única para enviar un paquete a dicho host. En las direcciones IPv4, se asignan los valores entre la dirección de red y la dirección de broadcast a los dispositivos en dicha red.

Figura 3. **Tipos de direcciones**



1.1.4 Prefijos de red

Una pregunta importante es: ¿Cómo es posible saber cuántos bits representan la porción de red y cuántos bits representan la porción de host? Al expresar una dirección de red IPv4, se agrega una longitud de prefijo a la dirección de red. La longitud de prefijo es la cantidad de bits en la dirección que conforma la porción de red. Por ejemplo, en 172.16.4.0 /24, /24 es la longitud de prefijo e indica que los primeros 24 bits son la dirección de red. Esto deja a los 8 bits restantes, el último octeto, como la porción de host.

Más adelante en este capítulo, el usuario aprenderá más acerca de otra entidad que se utiliza para especificar la porción de red de una dirección IPv4 en los dispositivos de red. Se llama máscara de subred. La máscara de subred consta de 32 bits, al igual que la dirección, y utiliza números uno y cero para indicar cuáles bits de la dirección son bits de red y cuáles bits son bits de host.

No siempre a las redes se le asigna un prefijo /24. El prefijo asignado puede variar de acuerdo con la cantidad de hosts de la red. Tener un número de prefijo diferente cambia el rango de host y la dirección de broadcast para cada red.

Observe que la dirección de red puede permanecer igual, pero el rango de host y la dirección de broadcast son diferentes, para las diferentes longitudes de prefijos. En esta figura se puede ver también que el número de hosts que puede ser direccionado a la red también cambia.

Figura 4. **Utilización de diferentes prefijos para la red 172.16.4.0**

1.1.5 Unicast, broadcast, multicast: tipos de comunicación

En una red IPv4, los hosts pueden comunicarse de tres maneras diferentes:

1. ***Unicast:*** el proceso por el cual se envía un paquete de un host, a un host individual.

2. ***Broadcast:*** el proceso por el cual se envía un paquete de un host, a todos los hosts de la red.

3. ***Multicast:*** el proceso por el cual se envía un paquete de un host, a un grupo seleccionado de hosts.

Estos tres tipos de comunicación se usan con diferentes objetivos en las redes de datos. En los tres casos, se coloca la dirección IPv4 del host de origen en el encabezado del paquete como la dirección de origen.

1.1.5.1 Tráfico unicast

La comunicación unicast se usa para una comunicación normal de host, a host, tanto en una red de cliente/servidor como en una red punto a punto. Los paquetes unicast utilizan la dirección host del dispositivo de destino como la dirección de destino y pueden enrutarse a través de una internetwork. Sin embargo, los paquetes broadcast y multicast usan direcciones especiales como la dirección de destino.

Al utilizar estas direcciones especiales, los broadcasts están generalmente restringidos a la red local. El ámbito del tráfico multicast también puede estar limitado a la red local o enrutado a través de una internetwork.

En una red IPv4, a la dirección unicast aplicada a un dispositivo final se le denomina dirección de host. En la comunicación unicast, las direcciones host asignadas a dos dispositivos finales, se usan como direcciones IPv4 de origen y de destino. Durante el proceso de encapsulación, el host de origen coloca su dirección IPv4 en el encabezado del paquete unicast como la dirección host de origen y la dirección IPv4 del host de destino en el encabezado del paquete, como la dirección de destino. Es posible enviar la comunicación utilizando un paquete unicast por medio de una internetwork con las mismas direcciones.

1.1.5.2 Transmisión de broadcast

Dado que el tráfico de broadcast se usa para enviar paquetes a todos los hosts de la red, un paquete usa una dirección de broadcast especial. Cuando un host recibe un paquete con la dirección de broadcast como destino, éste procesa el paquete como lo haría con un paquete con dirección unicast.

La transmisión de broadcast se usa para ubicar servicios/dispositivos especiales para los cuales no se conoce la dirección o cuando un host debe brindar información a todos los hosts de la red.

Algunos ejemplos para utilizar una transmisión de broadcast son:

- Asignar direcciones de capa superior a direcciones de capa inferior.

- Solicitar una dirección.

- Intercambiar información de enrutamiento por medio de protocolos de enrutamiento.

Cuando un host necesita información envía una solicitud, llamada consulta, a la dirección de broadcast. Todos los hosts de la red reciben y procesan esta consulta.

Uno o más hosts que poseen la información solicitada responderán, típicamente mediante unicast, de forma similar, cuando un host necesita enviar información a los hosts de una red, éste crea y envía un paquete de broadcast con la información.

A diferencia de unicast, donde los paquetes pueden ser enrutados por toda la internetwork, los paquetes de broadcast normalmente están restringidos a la red local. Esta restricción depende de la configuración del router que bordea la red y del tipo de broadcast, existen dos tipos de broadcasts: broadcast dirigido y broadcast limitado.

1. Broadcast dirigido

Se envía un broadcast dirigido a todos los hosts en una red específica, este tipo de broadcast es útil para enviar un broadcast a todos los hosts de una red local.

Por ejemplo, para que un host fuera de la red, se comunique con los hosts dentro de la red 172.16.4.0 /24, la dirección de destino del paquete será 172.16.4.255. Esto se muestra en la figura 4. Aunque los routers no envían broadcasts dirigidos por defecto, se los puede configurar para que lo hagan.

2. Broadcast limitado

El broadcast limitado se usa para la comunicación que está limitada a los hosts en la red local. Estos paquetes usan una dirección IPv4 de destino 255.255.255.255. Los routers no envían estos broadcasts.

Los paquetes dirigidos a la dirección de broadcast limitada, sólo aparecerán en la red local. Por esta razón, también se hace referencia a una red IPv4 como un dominio de broadcast. Los routers son dispositivos fronterizos para un dominio de broadcast.

A modo de ejemplo, un host dentro de la red 172.16.4.0 /24 transmitirá a todos los hosts en su red utilizando un paquete con una dirección de destino 255.255.255.255.

1.1.5.3 Transmisión de multicast

La transmisión de multicast está diseñada para conservar el ancho de banda de la red IPv4. Ésta reduce el tráfico al permitir que un host envíe un único paquete a un conjunto seleccionado de hosts. Para alcanzar hosts de destino múltiples, mediante la comunicación unicast, será necesario que el host de origen envíe un paquete individual dirigido a cada host. Con multicast, el host de origen puede enviar un único paquete que llegue a miles de hosts de destino.

Algunos ejemplos de transmisión de multicast son:

-Distribución de audio y video.
-Intercambio de información de enrutamiento por medio de protocolos de enrutamiento.
-Distribución de software.
-Suministro de noticias.

Clientes Multicast

Los hosts que desean recibir datos multicast específicos se denominan clientes multicast. Los clientes multicast usan servicios iniciados por un programa cliente para subscribirse al grupo multicast.

Cada grupo multicast está representado por una sola dirección IPv4 de destino multicast. Cuando un host IPv4 se suscribe a un grupo multicast, el host procesa paquetes dirigidos a esta dirección multicast y paquetes dirigidos a su dirección unicast exclusivamente asignada. Como se puede ver, IPv4 ha

apartado un bloque especial de direcciones desde 224.0.0.0 a 239.255.255.255 para direccionamiento de grupos multicast.

1.1.6 Direcciones públicas y privadas

Aunque la mayoría de las direcciones IPv4 de host son direcciones públicas designadas para uso en redes a las que se accede desde Internet, existen bloques de direcciones que se utilizan en redes que requieren o no acceso limitado a Internet. A estas direcciones se las denomina direcciones privadas.

1.1.6.1 Direcciones privadas

Los bloques de direcciones privadas son:

10.0.0.0 a 10.255.255.255 (10.0.0.0 /8)
172.16.0.0 a 172.31.255.255 (172.16.0.0 /12)
192.168.0.0 a 192.168.255.255 (192.168.0.0 /16)

Los bloques de direcciones de espacio privadas, como se muestra en la figura 5, se separa para utilizar en redes privadas. No necesariamente el uso de estas direcciones debe ser exclusivo entre redes externas, por lo general, los hosts que no requieren acceso a Internet pueden utilizar las direcciones privadas sin restricciones. Sin embargo, las redes internas aún deben diseñar esquemas de direcciones de red para garantizar que los hosts de las redes privadas utilicen direcciones IP que sean únicas dentro de su entorno de networking.

Muchos hosts en diferentes redes pueden utilizar las mismas direcciones de espacio privado. Los paquetes que utilizan estas direcciones como la dirección de origen o de destino no deberían aparecer en la Internet pública.

El router o el dispositivo de firewall del perímetro de estas redes privadas deben bloquear o convertir estas direcciones, incluso si estos paquetes fueran a hacerse camino hacia Internet, los routers no tendrían rutas para enviarlos a la red privada correcta.

1.1.6.2 Traducción de direcciones de red (NAT)

Con servicios para traducir las direcciones privadas a direcciones públicas, los hosts en una red direccionada en forma privada pueden tener acceso a recursos a través de Internet. Estos servicios, llamados traducción de dirección de red (NAT), pueden ser implementados en un dispositivo en un extremo de la red privada.

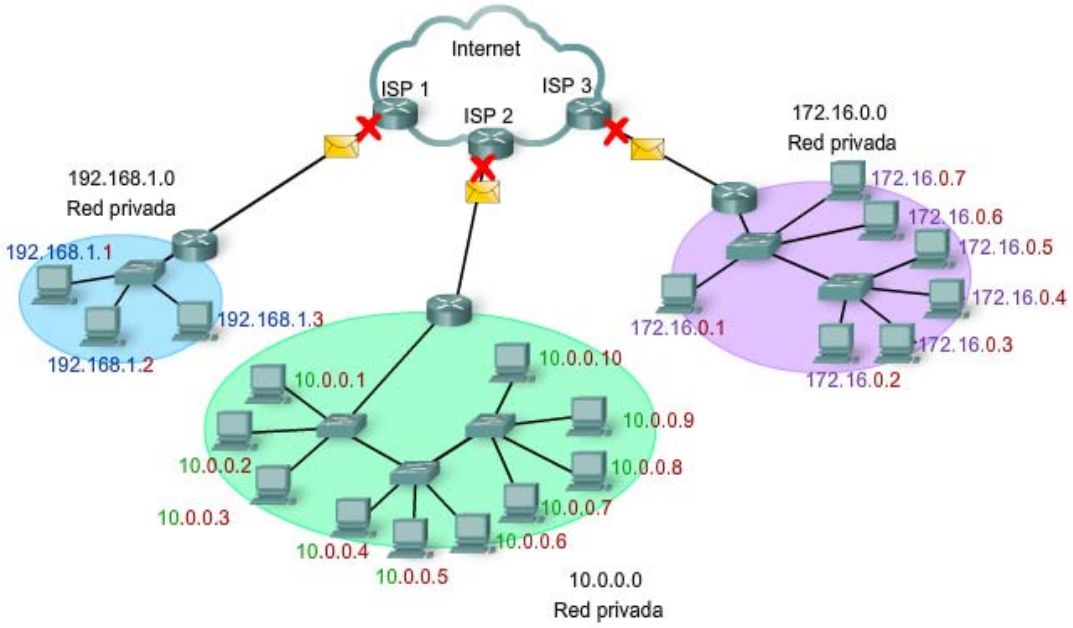
NAT permite a los hosts de la red pedir prestada una dirección pública para comunicarse con redes externas. A pesar que existe algunas limitaciones y problemas de rendimiento con NAT, los clientes de la mayoría de las aplicaciones pueden acceder a los servicios de Internet sin problemas evidentes.

1.1.6.3 Direcciones públicas

La amplia mayoría de las direcciones en el rango de host unicast IPv4 son direcciones públicas. Estas direcciones están diseñadas para ser utilizadas en los hosts de acceso público desde Internet. Aun dentro de estos bloques de

direcciones, existen muchas direcciones designadas para otros fines específicos.

Figura 5. **Direcciones privadas utilizadas en redes sin NAT**



1.1.7 Direccionamiento estático o dinámico para dispositivos de usuario final

1.1.7.1 Direcciones para dispositivos de usuario

En la mayoría de las redes de datos, la mayor población de hosts incluye dispositivos finales como PC, teléfonos IP, impresoras y asistentes digitales personales (PDA). Debido a que esta población representa la mayor cantidad de dispositivos en una red, debe asignarse la mayor cantidad de direcciones a

estos hosts. Las direcciones IP pueden asignarse de manera estática o dinámica.

1.1.7.2 Asignación estática de direcciones

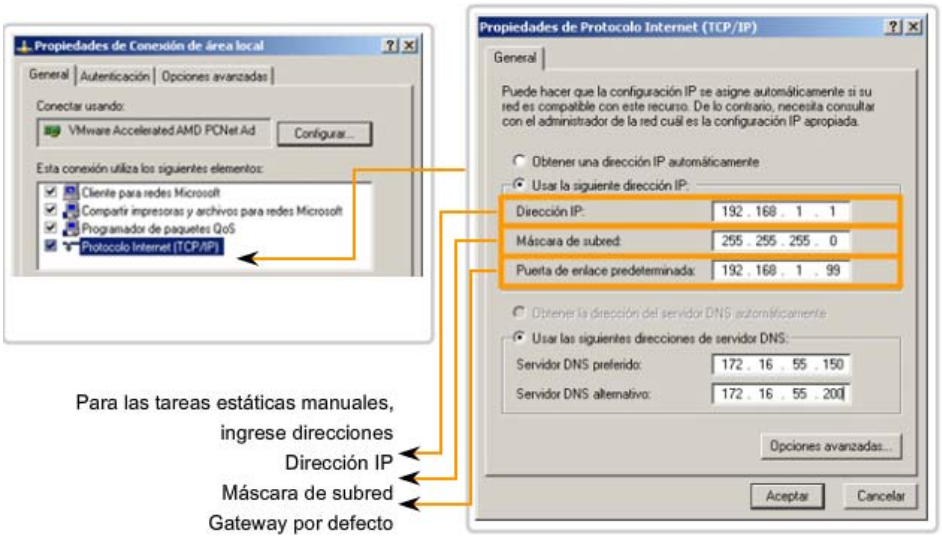
Con una asignación estática, el administrador de red debe configurar manualmente la información de red para un host, como se muestra en la figura. Como mínimo, esto implica ingresar la dirección IP del host, la máscara de subred y el gateway por defecto.

Las direcciones estáticas tienen algunas ventajas en comparación con las direcciones dinámicas. Por ejemplo, resultan útiles para impresoras, servidores y otros dispositivos de red que deben ser accesibles a los clientes de la red.

Si los hosts normalmente acceden a un servidor en una dirección IP en particular, esto provocará problemas si se cambia esa dirección. Además, la asignación estática de información de direccionamiento puede proporcionar un mayor control de los recursos de red.

Sin embargo, puede llevar mucho tiempo ingresar la información en cada host, al utilizar direccionamiento IP estático, es necesario mantener una lista precisa de las direcciones IP asignadas a cada dispositivo. Éstas son direcciones permanentes y normalmente no vuelven a utilizarse.

Figura 6. **Direccionamiento de dispositivos finales**



1.1.7.3 Asignación dinámica de direcciones

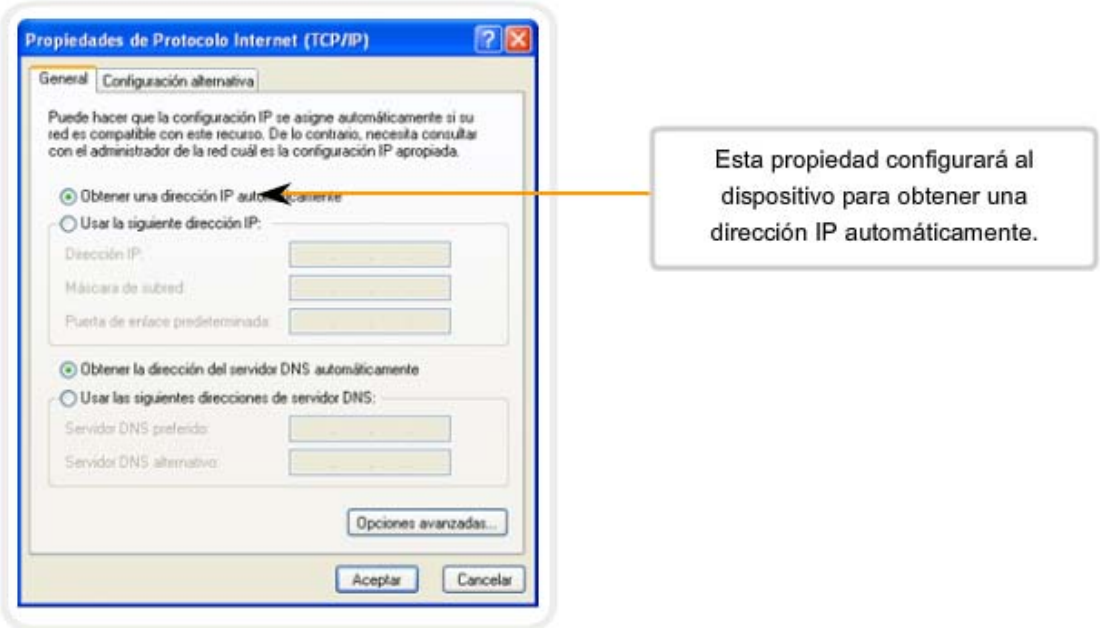
Debido a los desafíos asociados con la administración de direcciones estáticas, los dispositivos de usuarios finales a menudo poseen direcciones dinámicamente asignadas, utilizando el protocolo de configuración dinámica de host (DHCP), como se muestra en la figura.

El DHCP permite la asignación automática de información de direccionamiento como la dirección IP, la máscara de subred, el gateway por defecto y otra información de configuración. La configuración del sevidor DHCP requiere que un bloque de direcciones, llamado conjunto de direcciones, sea definido para ser asignado a los clientes DHCP en una red. Las direcciones asignadas a este pool deben ser planificadas de manera que se excluyan las direcciones utilizadas para otros tipos de dispositivos.

DHCP es generalmente el método preferido para asignar direcciones IP a los hosts de grandes redes, dado que reduce la carga para el personal de soporte de la red y prácticamente elimina los errores de entrada.

Otro beneficio de DHCP es que no se asigna de manera permanente, una dirección a un host, sino que sólo se le alquila durante un tiempo. Si el host se apaga o se desconecta de la red, la dirección regresa al pool para volver a utilizarse. Esta función es muy útil para los usuarios móviles que entran y salen de la red.

Figura 7. **Asignación de direcciones dinámicas**



1.1.8 Asignación de direcciones a otros dispositivos

1.1.8.1 Direcciones para servidores y periféricos

Cualquier recurso de red como un servidor o una impresora, debe tener una dirección IPv4 estática, como se muestra en la figura. Los hosts clientes acceden a estos recursos, utilizando las direcciones IPv4 de estos dispositivos. Por lo tanto, son necesarias direcciones predecibles para cada uno de estos servidores y periféricos.

Los servidores y periféricos son un punto de concentración para el tráfico de red. Se envían muchos paquetes desde las direcciones IPv4 de estos dispositivos y hacia éstas. Al monitorear el tráfico de red con una herramienta como Wireshark, un administrador de red, debe poder identificar rápidamente estos dispositivos. Utilizar un sistema de numeración consistente para estos dispositivos, facilita la identificación.

1.1.8.2 Direcciones para hosts accesibles desde Internet

En la mayoría de las internetworks, los hosts fuera de la empresa pueden acceder, sólo a unos poco dispositivos. En la mayoría de los casos, estos dispositivos son normalmente algún tipo de servidor, al igual que todos los dispositivos en una red, que proporciona recursos de red, las direcciones IPv4 para estos dispositivos deben ser estáticas.

En el caso de los servidores a los que se puede acceder desde Internet, cada uno debe tener una dirección de espacio público asociada. Además, las variaciones en la dirección de uno de estos dispositivos harán que no se pueda acceder a éste desde Internet. En muchos casos, estos dispositivos se

encuentran en una red numerada mediante direcciones privadas. Esto significa que el router o el firewall del perímetro de la red debe estar configurado para traducir la dirección interna del servidor en una dirección pública. Debido a esta configuración adicional del dispositivo que actúa como intermediario del perímetro, resulta aun más importante que estos dispositivos tengan una dirección predecible.

1.1.8.3 Direcciones para dispositivos intermediarios

Los dispositivos intermediarios también son un punto de concentración para el tráfico de red. Casi todo el tráfico dentro de redes o entre ellas pasa por alguna forma de dispositivo intermediario; por lo tanto, estos dispositivos de red ofrecen una ubicación oportuna para la administración, el monitoreo y la seguridad de red.

A la mayoría de los dispositivos intermediarios se le asigna direcciones de Capa 3, ya sea para la administración del dispositivo o para su operación. Los dispositivos como hubs, switches y puntos de acceso inalámbricos no requieren direcciones IPv4 para funcionar como dispositivos intermediarios. Sin embargo, si es necesario acceder a estos dispositivos como hosts para configurar, monitorear o resolver problemas de funcionamiento de la red, éstos deben tener direcciones asignadas.

Debido a que es necesario saber, cómo comunicarse con dispositivos intermedios, éstos deben tener direcciones predecibles. Por lo tanto, típicamente, las direcciones se asignan manualmente; además, las direcciones de estos dispositivos deben estar en un rango diferente dentro del bloque de red, que las direcciones de dispositivos de usuario.

1.1.8.4 Routers y firewalls

A diferencia de otros dispositivos intermediarios mencionados, se asigna a los dispositivos de router y firewall una dirección IPv4 para cada interfaz, cada interfaz se encuentra en una red diferente y funciona como gateway para los hosts de esa red.

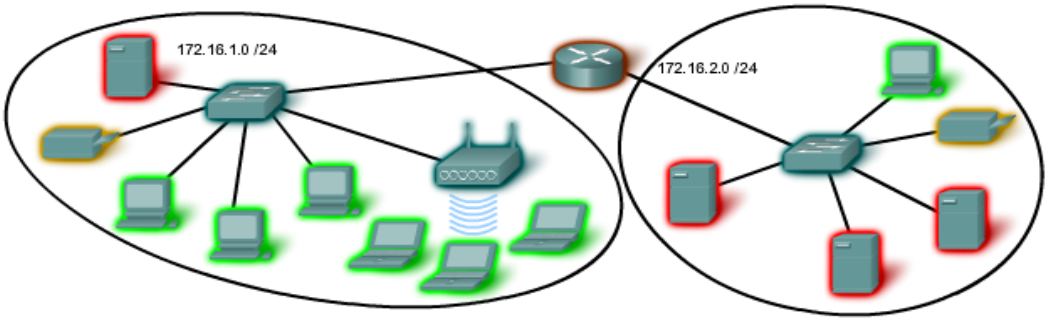
Normalmente, la interfaz del router utiliza la dirección más baja o más alta de la red, esta asignación debe ser uniforme en todas las redes de la empresa, de manera que el personal de red siempre conozca la gateway de la red, independientemente de cuál sea la red en la que están trabajando.

Las interfaces de router y firewall, son el punto de concentración del tráfico que entra y sale de la red. Debido a que los hosts de cada red usan una interfaz de dispositivo router o firewall como gateway para salir de la red, existe un flujo abundante de paquetes en estas interfaces. Por lo tanto, estos dispositivos pueden cumplir una función importante en la seguridad de red al filtrar los paquetes según las direcciones IPv4 de origen y destino.

Agrupar los diferentes tipos de dispositivos en grupos de direccionamiento lógicos, hace que la asignación y el funcionamiento del filtrado de paquetes sean más eficientes.

Figura 8. **Rangos de direcciones IP de los dispositivos**

Uso	Primera dirección	Última dirección	Dirección de resumen
Dirección de red	172.16.x.0	.....	172.16.x.0 /25
Hosts de usuarios (pool de DHCP)	172.16.x.1	172.16.x.127	
Servidores	172.16.x.128	172.16.x.191	172.16.x.128 /26
Periféricos	172.16.x.192	172.16.x.223	172.16.x.192 /27
Dispositivos de red	172.16.x.224	172.16.x.253	172.16.x.224 /27
Router (gateway)	172.16.x.254	.....	
Broadcast	172.16.x.255	.....	



1.1.9 Descripción de IPv6

A principios de los años noventa, el grupo de trabajo de ingeniería de Internet (IETF), centró su interés en el agotamiento de direcciones de red IPv4 y comenzó a buscar un reemplazo para este protocolo, esta actividad produjo el desarrollo de lo que hoy se conoce como IPv6.

Crear mayores capacidades de direccionamiento, fue la motivación inicial para el desarrollo de este nuevo protocolo. También se consideró otros temas durante el desarrollo de IPv6, como:

- Manejo mejorado de paquetes.
- Escalabilidad y longevidad mejoradas.
- Mecanismos QoS (Calidad del servicio).

- Seguridad integrada.

Para proveer estas características, IPv6 ofrece:

- Direccionamiento jerárquico de 128 bits; para expandir las capacidades de direccionamiento.

- Simplificación del formato de encabezado; para mejorar el manejo de paquetes.

- Soporte mejorado para extensiones y opciones; para escabilidad/longevidad mejoradas y manejo mejorado de paquetes.

- Capacidad de rotulado de flujo; como mecanismos QoS

- Capacidades de autenticación y privacidad; para integrar la seguridad

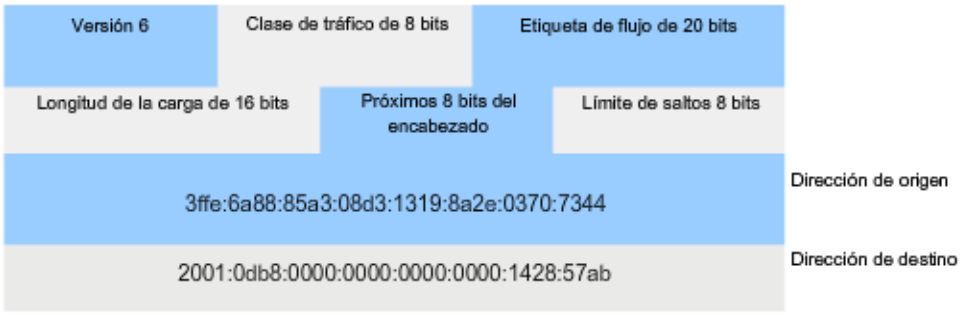
IPv6 no es meramente un nuevo protocolo de capa 3: es un nuevo conjunto de aplicaciones de protocolo, se han desarrollado nuevos protocolos en varias capas del stack, para admitir este nuevo protocolo. Hay un nuevo protocolo de mensajería (ICMPv6) y nuevos protocolos de enrutamiento. Debido al mayor tamaño del encabezado de IPv6, también repercute en la infraestructura de red subyacente.

1.1.9.1 Transición a IPv6

Como se puede ver en esta breve introducción, IPv6 ha sido diseñado con escala para permitir años de crecimiento de la internetwork. Sin embargo, IPv6 se está implementando lentamente y en redes selectas. Debido a las

mejores herramientas, tecnologías y administración de direcciones en los últimos años, IPv4 todavía se utiliza ampliamente y probablemente permanezca durante algún tiempo en el futuro, sin embargo, IPv6 podrá eventualmente reemplazar a IPv4 como protocolo de Internet dominante.

Figura 9. **Encabezado IPv6**



1.1.10 Máscara de subred; definición de las porciones de red y host

Una dirección IPv4 tiene una porción de red y una porción de host, se hizo referencia a la duración del prefijo, como la cantidad de bits en la dirección que conforma la porción de red. El prefijo es una forma de definir la porción de red para que los humanos la puedan leer. La red de datos también debe tener esta porción de red de las direcciones definidas.

Para definir las porciones de red y de host de una dirección, los dispositivos usan un patrón separado de 32 bits, llamado máscara de subred, como se muestra en la figura. La máscara de subred se expresa con el mismo formato decimal punteado, que la dirección IPv4. La máscara de subred se crea

al colocar un 1 binario en cada posición de bit que representa la porción de red y un cero binario en cada posición de bit que representa la porción de host.

El prefijo y la máscara de subred son diferentes formas de representar lo mismo, la porción de red de una dirección. Como se muestra en la figura 10, un prefijo /24 se expresa como máscara de subred de esta forma 255.255.255.0 (11111111.11111111.11111111.00000000). Los bits restantes (orden inferior) de la máscara de subred son números cero, que indican la dirección host dentro de la red.

La máscara de subred se configura en un host junto con la dirección IPv4 para definir la porción de red de esa dirección.

Por ejemplo; viendo el host 172.16.4.35/27:

Dirección:

172.16.20.35

10101100.00010000.00010100.00100011

Máscara de subred

255.255.255.224

11111111.11111111.11111111.11100000

Dirección de red

172.16.20.32

10101100.00010000.00010100.00100000

Como los bits de orden superior de las máscaras de subred son contiguos números 1, existe solamente un número limitado de valores de subred dentro de un octeto. Sólo es necesario ampliar un octeto si la división de red y host entra en dicho octeto; por lo tanto, se usan patrones de 8 bits limitados en las máscaras de subred.

Estos patrones son:

00000000 = 0

10000000 = 128

11000000 = 192

11100000 = 224

11110000 = 240

11111000 = 248

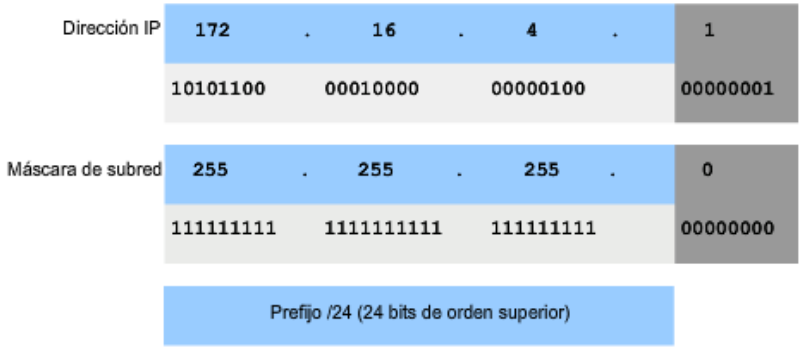
11111100 = 252

11111110 = 254

11111111 = 255

Si la máscara de subred de un octeto está representada por 255, entonces todos los bits equivalentes de ese octeto, de la dirección son bits de red. De igual manera, si la máscara de subred de un octeto está representada por cero, entonces todos los bits equivalentes de ese octeto de la dirección son bits de host. En cada uno de estos casos, no es necesario ampliar este octeto a binario para determinar las porciones de red y host.

Figura 10. **Porciones de red y de host de una dirección IP**



1.1.11 Estructura de Clases

En su organización original las direcciones IP se clasifican; según clases que permiten identificar redes de diferentes dimensiones: pequeñas, medianas y grandes.

La pertenencia de una dirección de red a una determinada clase, es definida por la posición del primer cero binario del primer octeto contando desde la izquierda.

Esto se denomina direccionamiento classful, a partir de la clase, se define cuántos bits u octetos se utilizan para definir o identificar la red, y cuántos quedan para identificar cada nodo individual. IPv4 define 5 clases: A, B, C, D y E.

Las 3 primeras clases están destinadas a uso público, la cuarta se utiliza para identificar el tráfico de multicast, la última, reservada.

Direcciones Clase A

Primer octeto: **0**0000001 a **0**1111111

Rango de direcciones clase A: 0.0.0.0 a 127.255.255.255

Esquema: Red . Nodo . Nodo . Nodo

Representan el 50% del número total de direcciones IP posibles.

Direcciones Clase B

Primer octeto: **10**000000 a **10**111111

Rango de direcciones clase B: 128.0.0.0 a 191.255.255.255

Esquema: Red . Red . Nodo. Nodo

Representan el 25% del número total de direcciones IP posible.

Direcciones Clase C

Primer octeto: **110**00000 a **110**11111

Rango de direcciones clase C: 192.0.0.0 a 223.255.255.255

Esquema: Red . Red . Red . Nodo

Representan el 12,5% del número total de direcciones IP posible.

Direcciones Clase D

Direcciones de Multicast o Multidifusión.

Primer octeto: **1110**0000 a **1110**1111

Rango de direcciones clase D: 224.0.0.0 a 239.255.255.255

Direcciones Clase E

Direcciones de Investigación.

Primer octeto: **11110**000 a 11111111

Rango de direcciones clase E: 240.0.0.0 a 255.255.255.255

1.1.12 Principios de división de subredes

La división en subredes permite crear múltiples redes lógicas de un solo bloque de direcciones. Como se usa un router para conectar estas redes, cada interfaz en un router debe tener un ID único de red. Cada nodo en ese enlace está en la misma red.

Se crean las subredes utilizando uno o más de los bits del host como bits de la red, esto se hace ampliando la máscara para tomar prestado algunos de los bits de la porción de host de la dirección, a fin de crear bits de red adicionales.

Cuantos más bits de host se usen, mayor será la cantidad de subredes que puedan definirse. Para cada bit que se tomó prestado, se duplica la cantidad de subredes disponibles. Por ejemplo, si se toma prestado 1 bit, es posible definir 2 subredes; si se toman prestados 2 bits, es posible tener 4 subredes, sin embargo, con cada bit que se toma prestado, se dispone de menos direcciones host por subred.

Fórmula para calcular subredes

Se usa esta fórmula para calcular la cantidad de subredes:

2^n donde n = la cantidad de bits que se tomaron prestados

En este ejemplo, el cálculo es así:

2^1 = 2 subredes

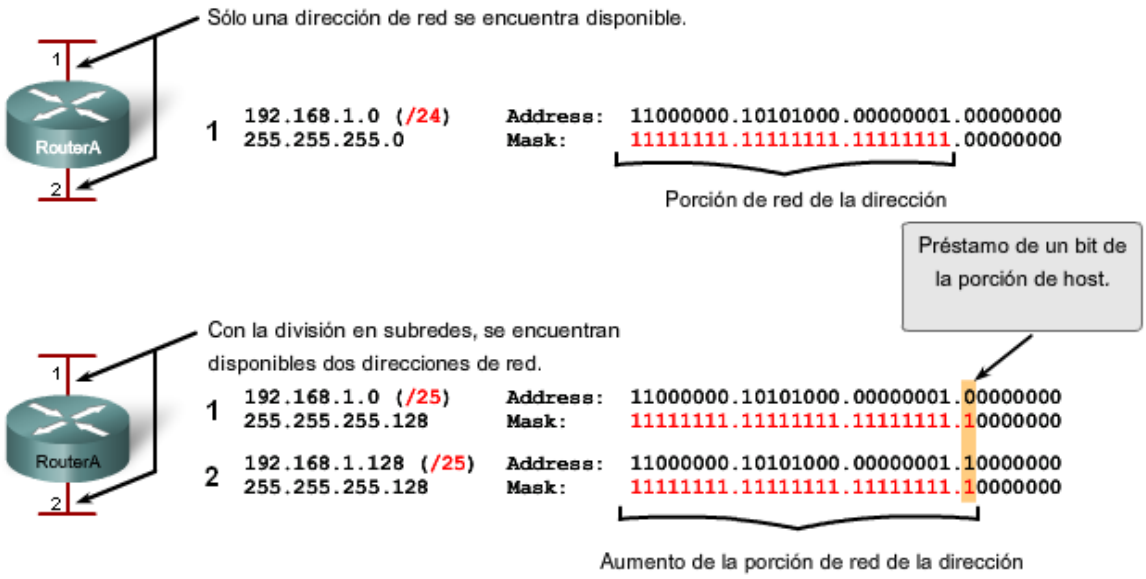
La cantidad de hosts

Para calcular la cantidad de hosts por red, se usa la fórmula 2^n - 2 donde n = la cantidad de bits para hosts. La aplicación de esta fórmula, (2^7 - 2 = 126) muestra que cada una de estas subredes puede tener 126 hosts. En cada subred, se examina el último octeto binario. Los valores de estos octetos para las dos redes son:

Subred 1: **0**0000000 = 0

Subred 2: **1**0000000 = 128

Figura 11. **Préstamo de bits para las subredes**



Subred	Dirección de red	Rango de host	Dirección de broadcast
0	192.168.1.0/25	192.168.1.1 - 192.168.1.126	192.168.1.127
1	192.168.1.128/25	192.168.1.129 - 192.168.1.254	192.168.1.255

1.1.12.1 Ejemplo con 3 subredes

A continuación, piense en una internetwork que requiere tres subredes.

Nuevamente, se comienza con el mismo bloque de direcciones 192.168.1.0 /24, tomar prestado un solo bit, proporcionará únicamente dos subredes; para proveer más redes, se cambia la máscara de subred a 255.255.255.192 y se toman prestados dos bits, esto proveerá cuatro subredes.

Calcule la subred con esta fórmula:

2^2 = 4 subredes

Cantidad de hosts

Para calcular la cantidad de hosts, se comienza por examinar el último octeto. Observe estas subredes.

Subred 0: 0 = 00000000

Subred 1: 64 = 01000000

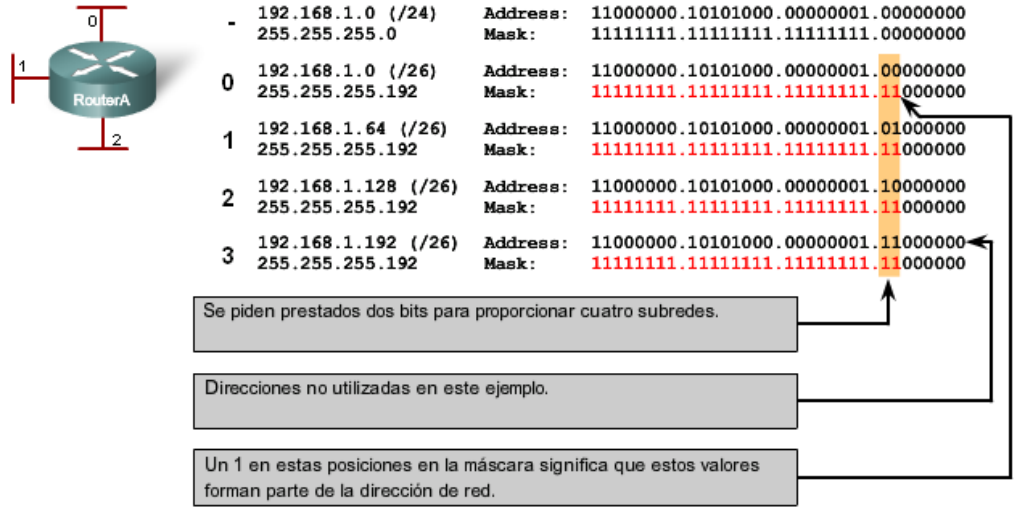
Subred 2: 128 = 10000000

Subred 3: 192 = 11000000

Aplique la fórmula de cálculo de host.

2^6 - 2 = 62 hosts por subred

Figura 12. **Préstamo de bits para subredes (con 4 subredes)**



Se encuentran disponibles más subredes, pero menos direcciones se encuentran disponibles por subred.

Subred	Dirección de red	Rango de host	Dirección de broadcast
0	192.168.1.0/26	192.168.1.1 - 192.168.1.62	192.168.1.63
1	192.168.1.64/26	192.168.1.65 - 192.168.1.126	192.168.1.127
2	192.168.1.128/26	192.168.1.129 - 192.168.1.190	192.168.1.191
3	192.168.1.192/26	192.168.1.193 - 192.168.1.254	192.168.1.255

1.2 Estándares Wireless

1.2.1 Redes de área local IEEE 802

IEEE 802 es un conjunto de estándares para redes de área local (LAN), definidos por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE). Este organismo define los estándares de obligado cumplimento, en este caso en el desarrollo de productos de red, uno de estos estándares es el 802. Existen

muchos estándares individuales dentro del paraguas del 802, incluyendo los 802.3 (redes basadas en cable) y los 802.11 (redes inalámbricas) que se veran en detalle a continuación.

1.2.2 Redes Ethernet por cable IEEE 802.3

Este estándar para redes basadas en cable se originó a finales de los años setenta y es mundialmente conocido como el estándar Ethernet. Inicialmente definió redes a velocidad de 10 Mbps (Megabits por segundo) sobre cable de tipo coaxial o también de par trenzado. La mayoría de las redes de área local operan bajo este estándar o uno derivado del original Ethernet, actualmente Fast Ethernet (100 Mbps) o Gigabit Ethernet (1000 Mbps). Actualmente IEEE está trabajando (y casi terminando) el nuevo estándar de 10 Gbps (Gigabits por segundo).

1.2.3 Redes Ethernet Inalámbricas IEEE 802.11

Este estándar define y gobierna las redes de área local inalámbricas (WLAN) que operan en el espectro de los 2,4 GHz (Giga Hercios) y fue definida en 1997. El estándar orignial especificaba la operación a 1 y 2 Mbps usando tres tecnologías diferentes:

- Frecuency Hopping Spread Spectrum (FHSS)
- Direct Secuence Spread Spectrum (DSSS)
- Infrarojos (IR)

El estándar original aseguraba la interoperabilidad entre equipos de comunicación dentro de cada una de estas tecnologías inalámbricas, pero no entre las tres tecnologías. Desde entonces, muchos estándares han sido definidos dentro de la especificación IEEE 802.11 que permiten diferentes velocidades de operación. El estándar IEEE 802.11b permite operar hasta 11 Mbps y el 802.11a, que opera a una frecuencia mucho mayor (5 GHz), permite hasta 54 Mbps. Además de estos hay otros estándares que se describe a continuación

1.2.4 Ethernet Inalámbrico de alta velocidad IEEE 802.11b

Esta extensión del estándar 802.11, definido en 1999, permite velocidades de 5,5 y 11Mbps en el espectro de los 2,4 GHz. Esta extensión es totalmente compatible con el estándar original de 1 y 2 Mbps (sólo con los sistemas DSSS, no con los FHSS o sistemas infrarojos) pero incluye una nueva técnica de modulación llamada Complementary Code Keying (CCK), que permite el incremento de velocidad. El estándar 802.11b define una única técnica de modulación para las velocidades superiores - CCK - al contrario que el estándar original 802.11 que permitía tres técnicas diferentes (DSSS, FHSS e infrarojos).

De este modo, al existir una única técnica de modulación, cualquier equipo de cualquier fabricante podrá conectar con cualquier otro equipo si ambos cumplen con la especificación 802.11b. Esta ventaja se ve reforzada por la creación de la organización llamada WECA (Wireless Ethernet Compatibility Alliance), una organización que dispone de un laboratorio de pruebas para comprobar equipos 802.11b. Cada equipo certificado por la WECA recibe el

logo de compatibilidad WI-FI que asegura su compatibilidad con el resto de equipos certificados.

Tabla I. **Resumen de estándar IEEE 802.11b**

Resumen 802.11b	
Rango de frecuencias:	De 2.4 a 2.4835 GHz
Acceso:	Direct Sequence Spread Spectrum (DSSS) usando Complementary Code Keying (CCK)
Velocidad:	Hasta 11 Mbps
Compatibilidad:	Compatible con sistemas 802.11 DSSS de 1 y 2 Mbps. No compatible con los sistemas 802.11 FHSS, Infrarrojos (IR) ni con HomeRF
Distancia:	Depende de la instalación y de los obstáculos, 300m típicos
Aplicación	Todo tipo de red de datos Ethernet

1.2.5 Pseudo estándar de 22Mbps IEEE 802.11b+

Es una variación del IEEE 802.11b pero que puede operar a 22Mbps contra los 11Mbps de la versión 11b. Su mayor problema es que no es un estándar; aunque aparece en la mayoría de las documentaciones como IEEE 802.11b+, IEEE nunca lo ha certificado como estándar.

Es un sistema propietario, diseñado por Texas Instruments y adoptado por algunos fabricantes de dispositivos inalámbricos como D-Link y Global Sun que utilizan estos chipsets. Técnicamente utiliza técnicas que forman parte del estándar 11g, comparativamente con el resto de estándares no ofrece grandes diferencias, ya que aunque anuncia velocidades de 22Mbps en prestaciones reales se obtiene una discreta mejora.

Tabla II. **Comparativa de estándares inalámbricos**

	802.11b	802.11a	802.11g	802.11b+
Fecha de definición	Septiembre 1999	Septiembre 1999	Noviembre 2001 (Borrador)	No estándar
Velocidad anunciada	11Mbps	54Mbps	54Mbps	22Mbps
Velocidad media obtenida	4-5Mbps	27Mbps	25Mbps	6Mbps
Frecuencia	2,4GHz	5GHz	2,4GHz	2,4GHz
Modulación	DSSS/CCK	OFDM	DSSS/PBCC	PBCC
Canales	11	12	11	11

1.2.6 Velocidades de 54Mbps en la banda de 2,4GHz IEEE 802.11g

El estándar IEEE 802.11g ofrece 54Mbps en la banda de 2,4GHz, dicho con otras palabras, asegura la compatibilidad con los equipos Wi-Fi preexistentes.

Para aquellas personas que dispongan de dispositivos inalámbricos de tipo Wi-Fi, 802.11g, proporciona una forma sencilla de migración a alta velocidad, extendiendo el período de vida de los dispositivos de 11Mbps. El estándar 802.11g se publicó como borrador en noviembre de 2001 con los siguientes elementos obligatorios y opcionales:

1. El método OFDM (Orthogonal Frecuancy Division Multiplexing) es obligatorio y es lo que permite velocidades superiores en la banda de los 2,4GHz.

2. Los sistemas deben ser totalmente compatibles con las tecnologías anteriores de 2,4GHz Wi-Fi (802.11b). Por lo que el uso del método CCK (Complementary Code Keying) también será obligatorio para asegurar dicha compatibilidad.

3. El borrador del estándar marca como opcional el uso del método PBCC (Packet Binary Convolution Coding) y el OFDM/CCK simultáneo.

Tabla III. **Resumen 802.11g**

Rango de frecuencias:	De 2.4 a 2.4835 GHz
Acceso:	Obligatoriamente Complementary Code Keying (CCK) y Orthogonal Frecuency Division Multiplexing (OFDM), opcionalmente puede incluir Packet Binary Convolution Coding (PBCC) y CCK/OFDM
Velocidad:	Hasta 54 Mbps
Compatibilidad:	Compatible con sistemas 802.11b de 11Mbps y 5,5Mbps. Compatible con sistemas 802.11 DSSS de 1 y 2 Mbps. No compatible con los sistemas 802.11 FHSS, Infrarrojos (IR) ni con HomeRF
Distancia:	Depende de la instalación y de los obstáculos, 300m típicos
Aplicación	Todo tipo de red de datos Ethernet

1.2.7 Redes inalámbricas en la banda de los 5 GHz IEEE 802.11a

El estándar IEEE 802.11a se aplica a la banda de UNII (Unlicensed National Information Infrastructure) de los 5GHz. El estándar usa el método OFDM para la transmisión de datos hasta 54Mbps. Su mayor inconveniente es la no compatibilidad con los estándares de 2,4GHz. Por lo demás su operación es muy parecida al estándar 802.11g. Existe también un estándar desarrollado en Europa, que es muy similar al 802.11a y que se llama HiperLAN2 (descrito una sección posterior).

Tabla IV. **Resumen 802.11a**

Rango de frecuencias:	De 5,15 a 5,25 GHz (50mW) De 5,25 a 5,35 GHz (250mW) De 5,725 a 5,825 GHz (1W)
Acceso:	Orthogonal Frecuency Division Multiplexing (OFDM)
Velocidad:	Hasta 54 Mbps
Compatibilidad:	No compatible con los sistemas 802.11b, 802.11, HiperLAN2, Infrarrojos (IR) ni con HomeRF
Distancia:	Depende de la instalación y de los obstáculos
Aplicación	Todo tipo de red de datos Ethernet

1.2.8 Red de área personal inalámbrica IEEE 802.15

El estándar 802.15 define las redes de área personal (WPAN). Estas redes también se conocen como redes inalámbricas de corta distancia, y se usan principalmente en PDAs, periféricos, teléfonos móviles y electrónica de consumo. El objetivo de este grupo de trabajo es publicar estándares WPAN para el mercado doméstico y de consumo que además sean compatibles con otras soluciones inalámbricas (BlueTooth) y basadas en cable, aún no tienen estándares operativos definidos

1.2.9 Acceso inalámbrico a banda ancha Wireless LAN IEEE 802.16

La misión del grupo de trabajo 802.16 es desarrollar sistemas inalámbricos del Área Metropolitana. En enero de 2003 ha publicado nuevos estándares.

1.2.9.1 54Mbps en la banda de 5GHz (Definición Europea) HiperLAN2

HiperLAN2 ha sido desarrollada bajo el proyecto BRAN (Broadband Radio Access Networks), del Instituto Europeo de Estandarización de las Telecomunicaciones (ETSI); es muy similar al estándar IEEE 802.11a ya que ambas usan la banda de los 5GHz y también el método OFDM para obtener velocidades de hasta 54Mbps.

Las diferencias entre ambas, residen en el control de acceso a medio (MAC), ya que en el caso de la HiperLAN2 está orientada a la conexión. Las conexiones divisiones de tiempo multiplexadas (TDM). A cada canal, o conexión, puede ser asignado a una calidad de servicio (QoS) apropiada, según

necesidades. Debido a estas características, HiperLAN2 será usado inicialmente pasa interconexiones WAN entre nodos.

Actualmente IEEE 802.11ª no ofrece diversidad de canales con QoS variables, por lo que se le compara con Wireless Ethernet, mientras que a HiperLAN2 es más parecida a un ATM inalámbrico.

Tabla V. **Resumen HiperLAN2**

Rango de frecuencias:	De 5,15 a 5,25 GHz (50mW) De 5,25 a 5,35 GHz (250mW) De 5,725 a 5,825 GHz (1W)
Acceso:	Orthogonal Frecuency Division Multiplexing (OFDM)
Velocidad:	Hasta 54 Mbps
Compatibilidad:	No compatible con los sistemas 802.11g, 802.11b, 802.11, ni con HomeRF
Distancia:	Depende de la instalación y de los obstáculos, máximo 150m
Aplicación	WAN/LAN, voz encapsulada, vídeo, datos

1.2.9.2 Interconectividad de dispositivos a corta distancia Bluetooth

Bluetooth (BT) es un estándar de facto, establecido por un grupo de fabricantes. Su nombre proviene del Rey Vikingo Harald Bluetooth (910-940 dc), que no tenía ningún diente azul como sugiere la traducción literal desde el inglés. Su nombre significaba pelo oscuro, característica muy rara entre los Vikingos.

Entre sus hazañas se cuenta la unión de los reinos de Dinamarca y Noruega. En febrero de 1998 se formó el grupo de desarrollo de Bluetooth (BT-SIG). Este estándar se definió para complementar (no competir) con IEEE 802.11b ya que BT está diseñado para redes de área personal (PAN) como

PDA, teléfonos móviles y otros pequeños dispositivos que quieran transmitir información en un rango muy corto (máximo 10 m).

El tipo de red que establece es siempre AD-Hoc. BT usa un salto rápido de frecuencias (1 600 saltos por segundo) en la banda de los 2,4GHz proporcionando una velocidad de 721Kbps.

La potencia de transmisión está limitada a 1 mW, Bluetooth se diseñó específicamente para reemplazar puertos infrarrojos y cables de conexión de periféricos; Bluetooth y 802.11b operan en la misma banda de 2,4GHz. Esto puede provocar interferencias entre ambos sistemas si operan simultáneamente y están muy próximos. Típicamente lo que ocurre es que ambos sistemas se ralentizan considerablemente, algunos fabricantes usan un multiplexador para evitar interferencias.

Tabla VI **Resumen Bluetooth**

Rango de frecuencias:	De 2.4 a 2.4835 GHz
Acceso:	Frecuency Hopping Spread Spectrum (FHSS)
Velocidad:	Versión 1.1 – 721Kbps Versión 1.2 – 10Mbps
Compatibilidad:	No compatible con ningún otro estándar inalámbrico
Distancia:	10 metro máximo
Aplicación	Kits de manos libres para teléfonos, PDA, conexión de periféricos, cámaras de fotos, etc…

1.2.9.3 Redes Inalámbricas de ámbito doméstico HomeRF

HomeRF es el nombre de un grupo de fabricantes formado en 1998 para desarrollar estándares de interconexión entre ordenadores personales domésticos y dispositivos electrónicos.

La especificación resultante se llamó Shared Wireless Access Protocol (SWAP). HomeRF se formó inicialmente porque las empresas involucradas pensaron que los dispositivos basados en 802.11 serían demasiado caros para el mercado del gran consumo. Curiosamente la rápida adopción de los dispositivos 802.11 y la continua bajada de precios, ha provocado todo lo contrario, el problema de la filosofía del HomeRF es que se pensó que no había necesidad de compatibilizar los sistemas inalámbricos domésticos con los usados en las empresas. Esta incompatibilidad hace tremendamente difícil su comercialización, con una velocidad de 1,6Mbps estos sistemas han pasado a ser sustituidos por los dispositivos basados en 802.11b. Aún así en algunos países se hicieron muy famosos e incluso hay una versión 2,0 que soporta hasta 20Mbps.

1.3 Sistema Wimax

1.3.1 Datos antecedentes de Wimax

Evolución de Wimax: Se debe entender el concepto de banda ancha inalámbrica y su evolución antes de introducirnos al área de WiMAX. El término banda ancha inalámbrica representa la combinación de la tecnología inalámbrica y de acceso de banda ancha.

Hay dos tipos de banda ancha inalámbrica, el primer tipo se denomina banda ancha inalámbrica fija, en lugar de usar la solución tradicional por medio de una línea de transmisión, se utilizan los medios de transmisión inalámbrica para la prestación de servicios de banda ancha hacia una estación fija. El segundo tipo se denomina de banda ancha móvil, ofrece una función adicional con la portabilidad, nomadicidad y la movilidad.

En las últimas dos décadas, la industria de las telecomunicaciones se han desarrollado rápidamente, tanto en el área de tecnología y de negocios. Los servicios inalámbricos móviles crecieron de 11 millones de suscriptores en todo el mundo en 1990 a más de 2 mil millones en 2005, al mismo tiempo, Internet se ha extendido por todo el mundo. El requisito de Internet de alta velocidad impulsa el desarrollo de banda ancha de acceso a Internet.

Para sustituir la tradicional tecnología de acceso de línea fija, empresas de telecomunicaciones busca una solución inalámbrica para la prestación del servicio de banda ancha. Muchas empresas desarrollaron sistemas de acceso inalámbrico, estos sistemas son variados en el protocolo, en el espectro de frecuencias, en la aplicación de apoyo, en las capacidades de rendimiento y otros parámetros. Sin embargo, el sistema inalámbrico de banda ancha, no se había desarrollado enormemente debido a la falta de una norma común, WiMAX fue desarrollado para cambiar la situación.

Worldwide Interoperability for Microwave Access (WiMAX), es un estándar basado en solución interoperable para banda ancha inalámbrica. El WiMAX Forum ha sido creado para certificar los productos de banda ancha inalámbrica, para la interoperabilidad y el cumplimiento de una norma.

WiMAX se basa en la creación de redes inalámbricas de área metropolitana, (WMAN) las normas elaboradas por el grupo IEEE 802.16 y adoptadas tanto por el grupo IEEE y ETSI HiperMAN.

1.3.2 Antecedentes de la IEEE 802.16 y WiMAX

El grupo de IEEE 802.16 fue creado en 1998 para desarrollar un estándar de interfaz de aire para la banda ancha inalámbrica. 802.16 original, se terminó en diciembre de 2001, que se basa en un único soporte de capa física (PHY) con una ráfaga de multiplexación por división de tiempo (TDM) de capa MAC.

Muchos de los conceptos relacionados con el MAC se han adaptado para la telefonía celular del módem de cable DOCSIS (Datos por Cable Service Interface Specification). Después de esto, una enmienda ha sido la de incluir NLOS (Non-Line-of-Sight) la aplicación en la banda de 2 GHz-11Ghz utilizando multiplexación por división de frecuencia ortogonal (OFDM), en base de la capa física. Para la capa MAC, por división de frecuencia ortogonal de acceso múltiple (OFDMA) fue añadido en esta revisión.

En 2004, el grupo IEEE802.16 produjo un nuevo estándar que se denomina IEEE 802.16-2004, sustituyó a todas las versiones anteriores y ha creado la primera solución WiMAX, estas soluciones WiMAX basadas en el estándar IEEE 802.16-2004 dirigidas a aplicaciones fijas y que fueron llamados como WiMAX fijo. En 2005, el grupo hizo una enmienda al estándar IEEE 802.16-2004. Esta enmienda añade el apoyo a la movilidad en la norma, esta revisión se denomina IEEE 802.16e-2005. Ofrece la base de la solución para la aplicación de nómadas y móviles. Por lo tanto, esta revisión se conoce como WiMAX móvil. A continuación se muestra los datos básicos de las normas antes mencionadas.

Tabla VII. **Datos básicos de los estándares IEEE 802.16**

Datos básicos de IEEE 802.16 Standards			
	802.16	**802.16-2004**	**802.16e-2005**
Status	Completado Diciembre 2001	Completado Junio 2004	Completado Diciembre 2005
Frequency band	10GHz–66GHz	2GHz–11GHz	2GHz–11GHz for fixed; 2GHz–6GHz for mobile applications
Application	Fixed LOS	Fixed NLOS	Fixed and mobile NLOS
MAC architecture	Point-to-multipoint, mesh	Point-to-multipoint, mesh	Point-to-multipoint, mesh
Transmission scheme	Single carrier only	Single carrier, 256 OFDM or 2,048 OFDM	Single carrier, 256 OFDM or scalable OFDM with 128, 512, 1,024, or 2,048 subcarriers
Modulation	QPSK, 16 QAM, 64 QAM	QPSK, 16 QAM, 64 QAM	QPSK, 16 QAM, 64 QAM
Gross data rate	32Mbps–134.4Mbps	1Mbps–75Mbps	1Mbps–75Mbps
Multiplexing	Burst TDM/TDMA	Burst TDM/TDMA/ OFDMA	Burst TDM/TDMA/ OFDMA
Duplexing	TDD and FDD	TDD and FDD	TDD and FDD
Channel band-widths	20MHz, 25MHz, 28MHz	1.75MHz, 3.5MHz, 7MHz, 14MHz, 1.25MHz, 5MHz, 10MHz, 15MHz, 8.75MHz	1.75MHz, 3.5MHz, 7MHz, 14MHz, 1.25MHz, 5MHz, 10MHz, 15MHz, 8.75MHz
Air-interface designation	Wireless MAN-SC	Wireless MAN-SCa Wireless MAN-OFDM Wireless MAN-OFDMA Wireless HUMANa	Wireless MAN-SCa Wireless MAN-OFDM Wireless MAN-OFDMA Wireless HUMANa
WiMAX implementation	None	256 - OFDM as Fixed WiMAX	Scalable OFDMA

Después se completaron las normas, el foro WiMAX diseñó los perfiles de certificación para WiMAX fijo y WiMAX móvil. Estos se muestran en la siguiente tabla. Los perfiles especificados, la banda de frecuencias, ancho de banda del canal y el modo duplex

Tabla VIII. **Perfiles para Wimax fijo y móvil**

Band Index	Frequency Band	Channel Bandwidth	OFDM FFT Size	Duplexing	Notes
Fixed WiMAX Profiles					
1	3.5 GHz	3.5MHz	256	FDD	Products already certified
		3.5MHz	256	TDD	
		7MHz	256	FDD	
		7MHz	256	TDD	
2	5.8GHz	10MHz	256	TDD	
Mobile WiMAX Profiles					
1	2.3GHz–2.4GHz	5MHz	512	TDD	Both bandwidths must be supported by mobile station (MS)
		10MHz	1,024	TDD	
		8.75MHz	1,024	TDD	
2	2.305GHz– 2.320GHz, 2.345GHz– 2.360GHz	3.5MHz	512	TDD	
		5MHz	512	TDD	
		10MHz	1,024	TDD	
3	2.496GHz– 2.69GHz	5MHz	512	TDD	Both bandwidths must be sup-ported by mobile station (MS)
		10MHz	1,024	TDD	
4	3.3GHz–3.4GHz	5MHz	512	TDD	
		7MHz	1,024	TDD	
		10MHz	1,024	TDD	
5	3.4GHz–3.8GHz, 3.4GHz–3.6GHz, 3.6GHz–3.8GHz	5MHz	512	TDD	
		7MHz	1,024	TDD	
		10MHz	1,024	TDD	

1.3.3 Cuadro técnico de Wimax

Principal característica de la tecnología WiMAX: WiMAX tiene una cantidad de buenas características en cuanto a las opciones de implementación y las ofertas potenciales de servicios. Algunas de las características principales son las siguientes:

- **Capa física basada en OFDM**: la capa física de WiMAX se basa en OFDM (multiplexación por división ortogonal de frecuencia). Se reduce la interferencia multicamino y hace que WiMAX puede operar en condiciones NLOS (sin línea vista).

- **Alta velocidades pico de datos**: WiMAX puede ofrecer muy altas velocidades pico de transmisión de datos. Cuando se utiliza espectro amplio de 20MHz, la velocidad de datos PHY (capa física), puede llegar a 70Mbps; cuando se usa espectro amplio de 10MHz y opera en TDD con una relación de 3:1 de bajada y subida, puede lograrse la velocidad máxima de unos 25 Mbps de descarga y 6.7Mbps de carga de datos. Estos picos PHY de velocidad de datos se puede lograr mediante el uso de modulaciones QAM 64 con una tasa de codificación de 5 / 6 de corrección de errores.

- **Ancho de banda escalable y soporte en la velocidad de datos:** WiMAX puede hacerse a escala en varios anchos de banda disponibles. La escala de la tecnología WiMAX, también ofrece la posibilidad de asistencia de los usuarios de roaming a través de redes diferentes que pueden tener diferentes asignaciones de ancho de banda.

- **Modulación y codificación adaptativa (AMC):** WiMAX puede adaptarse entre diferentes tipos de modulación y sistemas de codificación, basado en las condiciones del canal. El algoritmo de adaptación general requiere el uso de la más adecuada modulación y el sistema de codificación que puede ser soportado por la señal-ruido y la relación de interferencia en el receptor, de manera que cada usuario se beneficia de la más alta velocidad de datos posibles que puede ser soportado en sus respectivos enlaces.

- **Retransmisión en la Capa de Enlace**: WiMAX, soporta solicitudes automáticas retransmisión (ARQ) en la capa de enlace. Todos los paquetes transmitidos deben ser reconocidos por el receptor; los paquetes no reconocidos se supone que están perdidos y necesitan ser retransmitido, esta característica aumenta la fiabilidad de las conexiones.

- **Soporte de TDD y FDD:** WiMAX, también soporta tanto por división de tiempo dúplex (TDD) y división de frecuencia dúplex. Tomando nota de, que de momento hay perfiles FDD sólo para WiMAX fijo.

- **Acceso múltiple por división de frecuencia ortogonal (OFDMA):** OFDMA se utiliza como técnica de acceso múltiple por Mobile WiMAX. En OFDMA, la diversidad de frecuencia y la diversidad multi-usuario se utilizan para mejorar la capacidad del sistema.

- **Flexible y dinámica asignación de los recursos por usuario:** WiMAX, puede asignar dinámicamente los recursos basados en las demandas de los usuarios.

- **Soporte de Técnicas de antenas avanzadas:** WiMAX, soporta el uso de múltiples técnicas de la antena, como la formación de haz, el espacio-tiempo de codificación y multiplexación espacial. Mediante el despliegue de múltiples antenas en el transmisor y el receptor, la capacidad del sistema y la eficiencia espectral se puede mejorar.

- **Soporte de Calidad de Servicio (QoS):** WiMAX, puede soportar diferentes servicios, tales como la tasa de bits constante, velocidad de bits variable, en tiempo real, los flujos de tráfico no en tiempo real y así sucesivamente.

- **Seguridad Robusta:** WiMAX, soporta la fuerte encriptación, utilizando Advanced Encryption Standard (AES), tiene una sólida privacidad y el protocolo de gestión de claves. El sistema también ofrece una arquitectura muy flexible de autenticación basado en Protocolo de Autenticación Extensible (EAP). Además, permite una variedad de credenciales de usuario, como nombre de usuario / contraseña, certificados digitales, y así sucesivamente.

- **Soporte para la movilidad**: WiMAX Mobile, permite la movilidad mediante la mejora de rendimiento del control de potencia, subcanalizando la subida del enlace y realizando estimación de canal frecuente.

- **Arquitectura basada en IP**: La tecnología WiMAX, define la red basada en la arquitectura IP.

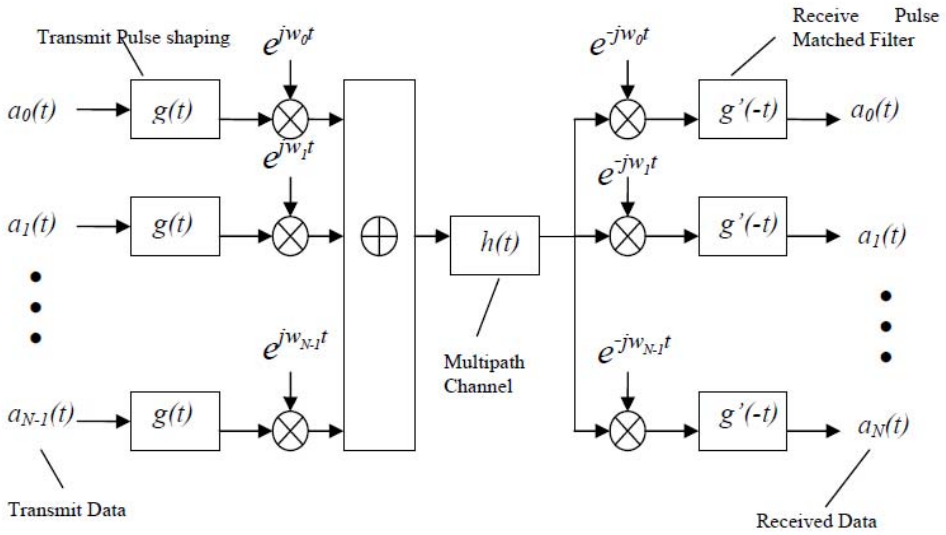
1.3.4 Capa física WiMAX

1.3.4.1 OFDM Básico

WiMAX se basa en la Orthogonal Frequency Division Multiplexing (OFDM), ésta una técnica de multiplexación que divide el ancho de banda en portadoras de múltiples frecuencias. La idea básica de OFDM puede ser mostrado como en la figura posterior. En OFDM, una secuencia (stream) de alta velocidad de bits de datos se divide en, N secuencias paralelas de menor tasa de flujos de bits.

A continuación, los streams se modulan y transmiten en subportadoras separadas. La duración de cada símbolo en subportadora aumenta a T = NT. Si N es suficientemente grande para garantizar que el tiempo de duración es superior a la propagación, el símbolo de retardo de canal, T>> τ, entonces se reduce la interferencia entre símbolos (ISI).

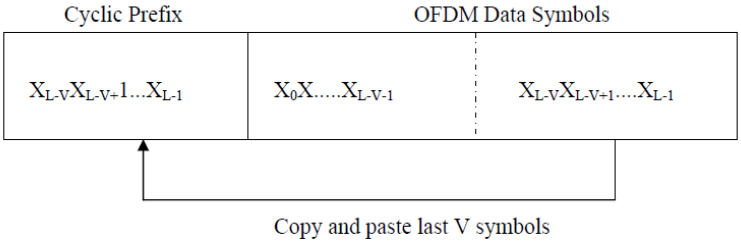
Figura 13. **Arquitectura básica de un sistema OFDM**



Es decir para conseguir una mayor eficiencia, el sistema se realimenta con las condiciones del canal, adaptando continuamente el número de subportadoras asignadas al usuario en función de la velocidad que éste necesita, y de las condiciones del canal. Si la asignación se hace rápidamente, se consigue cancelar de forma eficiente las interferencias co-canal y los desvanecimientos rápidos, proporcionando una mayor eficiencia espectral que OFDM.

Sin embargo, con el fin de eliminar por completo la ISI, prefijo cíclico (CP) se utiliza como un intervalo de guarda entre símbolos OFDM, mientras la duración del CP es más larga que la demora de la propagación multitrayecto, el canal libre de ISI se puede lograr. El CP es una copia de los símbolos por última vez y se coloca en el comienzo del símbolo de datos como se muestra en la figura siguiente. Sin embargo, si el CP es superpuesto esto causa desperdicio de energía y una disminución en la eficiencia de ancho de banda.

Figura 14. **Prefijo cíclico inserto**



Demasiados recursos se utilizan, si las portadoras se transmiten por separado en N, bandas independientes de radiofrecuencias, para resolver este problema, OFDM utiliza una técnica eficaz de cómputo, transformadas de Fourier discreta (DFT), y su aplicación eficaz que se conoce comúnmente como la transformada rápida de Fourier (FFT). La FFT y FFT inversa (IFFT) se utilizan

para crear una multitud de subportadoras ortogonales con una frecuencia de radio única.

WiMAX fijo y móvil se basan en una capa física diferente; WiMAX fijo es basada en IEEE 802.16-2004 y utiliza un 256 FFT basada en la capa física OFDM, WiMAX Mobile basada en IEEE 802.16e-2005 utiliza una capa física escalable basada en OFDMA. En el sector móvil WiMAX, los tamaños varían FFT 128-2048. Parámetros para OFDM y OFDMA PHY-PHY-se muestran en la Tabla siguiente:

Tabla IX. **Parámetros OFDM usados en WiMAX**

Parameter	**Fixed WiMAX OFDM-PHY**	**Mobile WiMAX Scalable OFDMA-PHY**[a]			
FFT size	256	128	512	1,024	2,048
Number of used data subcarriers[b]	192	72	360	720	1,440
Number of pilot subcarriers	8	12	60	120	240
Number of null/guardband subcarriers	56	44	92	184	368
Cyclic prefix or guard time (Tg/Tb)	1/32, 1/16, 1/8, 1/4				
Oversampling rate (Fs/BW)	Depends on bandwidth: 7/6 for 256 OFDM, 8/7 for multiples of 1.75MHz, and 28/25 for multiples of 1.25MHz, 1.5MHz, 2MHz, or 2.75MHz.				
Channel bandwidth (MHz)	3.5	1.25	5	10	20
Subcarrier frequency spacing (kHz)	15.625	10.94			
Useful symbol time (μs)	64	91.4			
Guard time assuming 12.5% (μs)	8	11.4			
OFDM symbol duration (μs)	72	102.9			
Number of OFDM symbols in 5 ms frame	69	48.0			

1.3.5 WiMAX MAC-Layer

La capa MAC (DataLink Layer) es la segunda capa en el modelo de interconexión de sistemas abiertos (OSI); es la interfaz entre las capas de transporte y la capa física (PHY). La capa PHY entrega bits de información desde el transmisor al receptor mediante el uso de un soporte físico. La capa MAC es responsable de controlar los vínculos creados para diferentes aplicaciones al mismo tiempo los diferentes tipos de aplicaciones que no son considerados por la capa PHY. La capa MAC recibe datos de Unidades de Servicio (SDU) de la capa superior y los organiza en unidades de datos de protocolo MAC (MPDU), para su transmisión por el aire; lo hace a la inversa con los datos recibidos de PHY.

1.3.6 Quality of service

WiMAX capa MAC proporciona el soporte QoS, el concepto se basa en el diseño de QoS de la especificación de Interfaz para servicios de datos sobre cable (DOCSIS) estándar.

La arquitectura orientada a conexión MAC se utiliza para construir la función de control de QoS. Todas las conexiones de enlace de carga y descarga son controladas por el servicio de BS (Base Station). Antes de la transmisión se inicia, una relación unidireccional, se crea entre la capa MAC de BS y MS (Mobile Station).

La conexión se identifica mediante un identificador de conexión que es una dirección temporal para la transmisión de datos por el enlace.

Un flujo de servicios se define por WiMAX como un flujo unidireccional de paquetes con un determinado conjunto de parámetros de QoS, se identifica

mediante un identificador de servicio de flujo (SFID). La calidad de servicio puede ser evaluada en diferentes parámetros como la prioridad de tráfico, velocidad máxima sostenida de tráfico, velocidad de ráfaga máxima, la tasa mínima aceptable, la programación de tipo, escriba QRQ, plazo máximo, la fluctuación tolerado, tipo de unidad de servicios de datos y el tamaño, el mecanismo de solicitud de ancho de banda que se utilizará y así sucesivamente.

Cinco diferentes categorías se definen por WiMAX, como seguidores para soportar aplicaciones variables.

Servicios de concesión no solicitados (UGS): este está diseñado para soportar flujos de servicio de tiempo real que generan paquetes de tamaño fijo, de datos en forma periódica, como T1/E1 y VoIP.

Servicio de poleo en tiempo real (RTPS): este está diseñado para soportar servicios en tiempo real, tales como streaming de audio o vídeo que generan los paquetes de datos variables en forma periódica.

Servicio de poleo en tiempo no real (NRTPS): este está diseñado para soportar los servicios que pueden retrasar tolerantes, tales como, transferencia de archivos FTP Protocolo.

Servicio mejor esfuerzo (BE): este está diseñado para apoyar los servicios que no tienen requisitos de QoS estricto, como la navegación Web del servicio. Los datos se envían cuando los recursos están disponibles.

Servicio de poleo en tiempo real Extendido (ErtPS): Este está diseñado para soportar aplicaciones en tiempo real que tienen las tasas de datos variables y

requieren garantizar la velocidad de transferencia en los datos y el retraso, como VoIP con supresión de silencio.

La siguiente tabla muestra los parámetros de calidad de servicio definidos para cada tipo de servicio y los ejemplos de aplicación.

Tabla X. **Servicios soportados en WiMAX**

Service Flow Designation	Defining QoS Parameters	Application Examples
Unsolicited grant services (UGS)	Maximum sustained rate Maximum latency tolerance Jitter tolerance	Voice over IP (VoIP) without silence suppression
Real-time Polling service (rtPS)	Minimum reserved rate Maximum sustained rate Maximum latency tolerance Traffic priority	Streaming audio and video, MPEG (Motion Picture Experts Group) encoded
Non-real-time Polling service (nrtPS)	Minimum reserved rate Maximum sustained rate Traffic priority	File Transfer Protocol (FTP)
Best-effort service (BE)	Maximum sustained rate Traffic priority	Web browsing, data transfer
Extended real-time Polling service (ErtPS)	Minimum reserved rate Maximum sustained rate Maximum latency tolerance Jitter tolerance Traffic priority	VoIP with silence suppression

1.3.7 Gestión de móvil

Hay tres métodos de traspaso (Handoff) soportados en el estándar IEEE 802.16e-2005, estos son el Hard Handover (HHO), la estación base de

conmutación rápida (SPL) y el Handover de macro diversidad (MDHO). HHO es obligatorio, pero los SPL y MDHO son opcionales.

En HHO, la MS (Mobile Station) hace un análisis de frecuencia de radio para medir la calidad de la señal de las estaciones base vecinas. Esta exploración se realiza en los intervalos de la exploración que se asignan por la MS, al mismo tiempo, la MS puede iniciar la conexión con otras estaciones base vecinas, cada vez que una decisión de traspaso se realiza con base en la medición, la MS se sincroniza con la transmisión de enlace que tienen las BS (Base Station) vecinas y lleva a cabo un rango si no se hizo en la exploración, y entonces termina la conexión con la BS anterior.

En FBSS, la MSI mantiene una lista de BSS, que se llama conjunto activo. La MS controla continuamente el conjunto de activos, mantiene las conexiones de identificación de cada uno de ellos. Entre las normas básicas en el conjunto de activos, la MS sólo se comunica con un BS, que se define como ancla BS. Cuando el traspaso es necesario, la conexión se cambia de un BS a otra BS sin explícitamente realizar la señalización de traspaso (Handoff). La MS reporta la BS ancla seleccionada a través del canal CQI. MDHO es similar con FBSS, sin embargo, la MS se comunica con todos los BSS en el conjunto activo. En el enlace descendente, los datos de múltiples enlaces descendentes recibidos por la MS son combinados. En el enlace ascendente, la MS envía los datos a todas las normas básicas y la diversidad de selección se realiza para elegir el mejor enlace.

Ambos FBSS y MDHO tienen mejor rendimiento que el HHO, pero requieren que las estaciones base en el activo o conjunto de diversidad se sincronicen, usen la misma frecuencia portadora, y compartan información relacionada con la entrada de la red.

1.3.8 Gestión de energía

En WiMAX móvil, se definen dos características para ahorrar la energía a los dispositivos portátiles; es el modo de reposo un modo de inactividad, en modo de espera, la MS se apagará por cierto período de tiempo para ahorrar energía. Esta vez es decidido por el MS y el BS, además del ahorro de energía, el modo de suspensión también ahorrará los recursos de radio BS.

Para realizar el handover mientras está en modo de espera, la MS exploración, otros BSs para recoger información, tres clases de ahorro de energía se definen en WiMAX como los siguientes:

- **En la clase 1**, la ventana del sueño es exponencialmente mayor del mínimo al máximo. Esto se utiliza cuando el MS está haciendo más esfuerzo y no en tiempo real del tráfico.

- **En la clase 2**, la ventana del sueño es de longitud fija. Esto se utiliza para el servicio de UGS.

- **En la clase 3**, hay sólo una ventana de un tiempo de suspensión. Esto se utiliza para el tráfico de multicast o de gestión del tráfico en donde el tiempo de tráfico es conocido.

En el modo de reposo, la MS puede estar completamente apagada, recibe los datos de difusión descendente periódicamente, sin registro en cualquier BS. Cuando el tráfico llega descendente, la MS es buscado por la BS, la MS es asignada a un grupo de paginación por BS antes de entrar en modo reposo y se despierta para actualizar el grupo de paginación de forma periódica. El modo de

espera, ahorra más energía, que el modo de suspensión; además, se elimina el tráfico de Handover desde el MS inactivo.

1.3.9 Seguridad

La seguridad ha puesto de relieve a WiMAX desde el principio; la mejor tecnología de seguridad se ha utilizado para garantizar la seguridad de las comunicaciones en el sistema, los aspectos clave de las características de seguridad son los siguientes:

- **Dispositivo / autenticación de usuarios:** para evitar el uso no autorizado, un método de autenticación flexible es utilizada por WiMAX, el marco de autenticación se basa en la Internet Engineering Task Force (IETF) EAP, es compatible con muchas credenciales, como tarjetas inteligentes, certificados digitales y nombre de usuario / contraseña, los dispositivos móviles han incorporado en los certificados digitales X.509 que contienen su clave pública y la dirección MAC. Los operadores hemos utilizado para identificar los dispositivos y luego usar nombre de usuario / contraseña o tarjeta inteligente para la autenticación.

- **Protocolo de Gestión de Claves:** la privacidad y gestión de claves Protocol Versión 2 (PKMPV2) se utiliza para asegurar el intercambio de datos entre BS y MS. PKM utiliza certificados digitales X.509 y RSA (Rivest-Shamer-Adleman), algoritmos de cifrado de clave pública para llevar a cabo de forma segura intercambio de claves entre el BS y MS.

- **La protección de mensajes de control:** los mensajes de control están protegidos mediante el uso de sistemas de síntesis de mensaje tales como; AES basada en CMAC (código de autenticación de mensajes

basado en cifrado) o MD5 (algoritmo de resumen del mensaje 5)-basada HMAC (códigos hash mensaje en función de autenticación).

- **Soporte para la entrega rápida:** Una pre-autenticación se realiza entre la MS y sus BSs dirigida a reducir el tiempo de entrega. Un esquema, de acuerdo de tres vías se utiliza para optimizar los mecanismos de soporte a la reautenticación de entrega rápida, impide ataques del hombre en el medio.

1.3.10 Arquitectura de red WiMAX

Se ha estado discutiendo de las capas PHY y MAC en las dos últimas secciones. Sin embargo, para construir una red interoperable de banda ancha móvil, y una arquitectura de red compatible, es necesario para hacer frente a los problemas de servicio de punto a punto como la conectividad IP, gestión de sesiones, QoS, seguridad y gestión de la movilidad. Network Working Group (NWG) en WiMAX Forum, fue establecido para desarrollar una arquitectura de red.

Un proceso de tres etapas de desarrollo de normas ha sido utilizado por WiMAX Forum; en la etapa 1, se especifican los requisitos de servicio para la red, estos se desarrollan dentro del proveedor de servicios WiMAX Grupo de Trabajo (SPWG), la arquitectura que cumple con los requisitos de servicio se desarrolla en la etapa 2, etapa 3 da todos los detalles del protocolo usado en la arquitectura.

La cuarta versión de la versión 1 se acaba de publicar, al mismo tiempo, la versión 1,5 está en desarrollo. En esta sección, nos centraremos en la arquitectura de red que se mostró en la etapa 2.

1.3.11 Modelo de la red de referencia

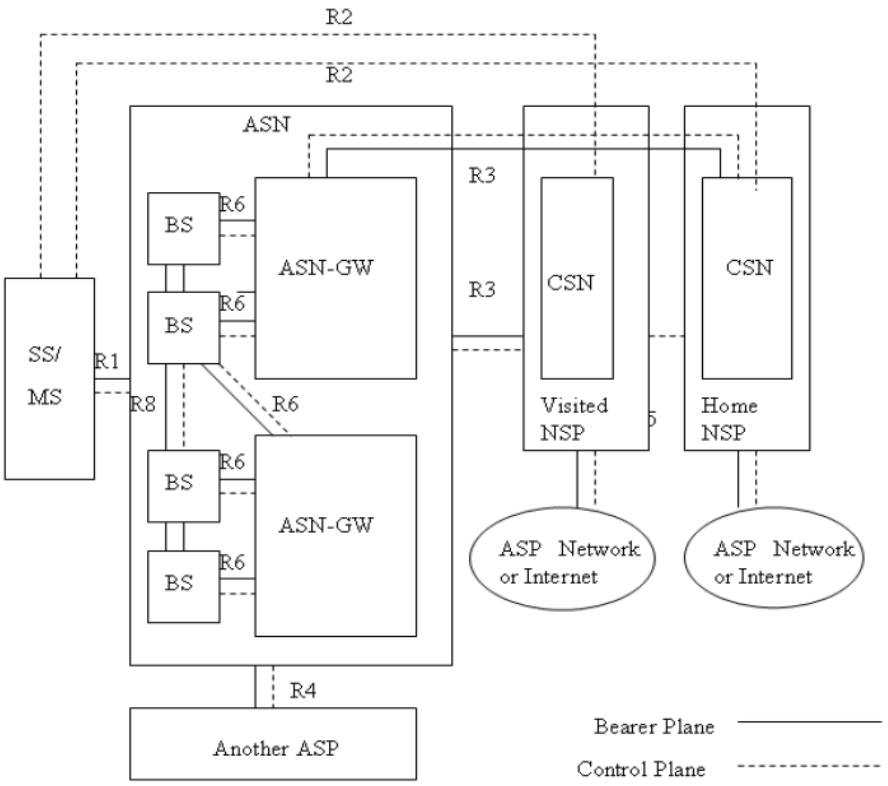
Principios se han establecido para el desarrollo de la arquitectura de red WiMAX, se definen desde diferentes aspectos, tales como: servicios y aplicaciones, la seguridad, la movilidad y la entrega, calidad de servicio, capacidad de gestión, rendimiento y así sucesivamente.

El desarrollo de la arquitectura de red WiMAX debe seguir los principios y los resultados cumpliendo con el requisito de todos los aspectos.

Sobre la base de los principios, el modelo de red de referencia (NRM), fue desarrollado, NRM es una representación lógica de la arquitectura de red, en él se identifican los elementos funcionales y puntos de referencia sobre el que se consiga la interoperabilidad entre entidades funcionales.

La intención de la NRM es lograr la interoperabilidad y permiten múltiples opciones de aplicación de una determinada entidad funcional. NRM consta de tres partes principales que son: MS / SS, acceso a la red de servicios y red de servicios de conectividad como se muestra en la figura 15. El Mobile Station o la Estación suscriptor es el móvil o aparatos fijos que se utiliza para conectar el equipo de abonado y una estación base (BS) podría ser un host o varios hosts.

Figura 15. **Modelo de referencia de red**



1.3.12 Servicio de acceso a red (ASN)

Funciones: ASN es un conjunto completo de funciones de red, necesarios para proveer de acceso de radio a un abonado WiMAX; es propiedad de un proveedor de acceso a red (NAP). A continuación se mencionan algunas funciones:

- WiMAX conectividad de capa 2 con WiMAX MS

- Transferencia de Mensajes de AAA a la portada de abonado WiMAX de proveedores de servicio de red (H-NSP) para la autenticación, autorización y sesión.

- Red de descubrimiento y selección de NSP (proveedor de servicios de red) preferido del abonado WiMAX.

- Funcionalidad para el establecimiento de la conectividad con un MS WiMAX en capa 3 (es decir, la asignación de dirección IP).

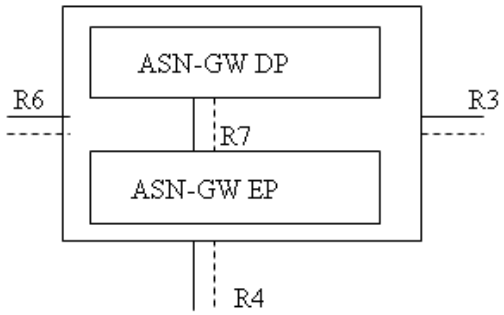
- Gestion de Recursos de Radio.

- Para un entorno portátil y móvil, el servicio de acceso de red (ASN), también necesita un soporte anclado a la movilidad ASN, servicio de conectividad de red (CSN) anclado a la movilidad, paging (datos móviles) y ASN-CSN tunneling.

La figura 16 también muestra la descomposición de ASN. EL ASN se compone de una o más BS (Base Station) y de uno o más Gateways ASN (ASN-GW). BS es una entidad lógica que representa un ejemplo completo de las capas MAC y PHY de WiMAX en cumplimiento con el estándar IEEE 802.16

El ASN-GW se define como una entidad lógica que representa una agregación de entidades de control plano funcional que son vinculados con una función correspondiente de la ASN, una función que reside en el CSN o una función en otro ASN. El ASN-GW puede ser opcionalmente descompuesto en dos grupos de funciones que son punto de decisión (DP) funciones y punto de ejecuciòn (EP) como se muestra.

Figura 16. **Descomposición de ASN**



EP incluye funciones portador plano (bearer plane) y la DP incluye funciones de no portador plano. NRM (Network Reference Model) define tres perfiles diferentes para ASN; perfil de las funciones ASN en BS y ASN-GW. El cuadro siguiente, se muestra la comparación entre los tres perfiles.

Tabla XI. **Descomposición funcional de ASN**

Functional Category	**Function**	**ASN Entity Name**		
		Profile A	**Profile B**	**Profile C**
Security	Authenticator	ASN-GW	ASN	ASN-GW
	Authentication relay	BS	ASN	BS
	Key distributor	ASN-GW	ASN	ASN-GW
	Key receiver	BS	ASN	BS
IntraASN Mobility	Data Path function	ASN-GW & BS	ASN	ASN-GW and BS
	Handover function	ASN-GW & BS	ASN	BS
	Context server & Client	ASN-GW & BS	ASN	ASN-GW and BS
L3 Mobility	MIP Authentication Relay	ASN-GW	ASN	ASN-GW
	MIP foreign agent	ASN-GW	ASN	ASN-GW
Radio resource management	Radio resource controller	ASN-GW	ASN	BS
	Radio resource agent	BS	ASN	BS
Paging	Paging agent	BS	ASN	BS
	Paging controller	ASN-GW	ASN	ASN-GW
QoS	Service flow authorization	ASN-GW	ASN	ASN-GW
	Service flow manager	BS	ASN	BS

2. SISTEMA DE MONITOREO

2.1 PROTOCOLO SNMP

2.1.1 Antecedentes y descripción

En un inicio, cuando había problemas con la red, la única forma de identificar el problema era, ejecutando comandos muy simples como el ping, el cual no brinda suficiente información para resolver rápidamente dichos problemas. En el año de 1990 surge un nuevo estándar llamado: SNMP (Simple Network Managenement Protocol, Protocolo Simple de Administración de Redes), definido en el RFC 1157, este protocolo muestra una manera de administrar y supervisar las redes de cómputo para identificar y resolver problemas, así como para planear su crecimiento, se encuentra implementado en la capa de aplicación y pertenece al grupo de protocolos de TCP/IP.

Simple Network Management Protocol (SNMP), es un protocolo de gestión de red muy utilizado, que permite obtener información de dispositivos de red, memoria libre, uso de la CPU, detección de errores, establecer alarmas, estado de funcionamiento, etc. Por ejemplo, en la gestión de un hub, SNMP podría desconectar automáticamente los nodos que estén corrompiendo la red, o se podrían establecer alarmas para alertar al administrador de la red cuando en un dispositivo el tráfico de datos supere el umbral establecido, o se podrían buscar IPs duplicadas, etc.

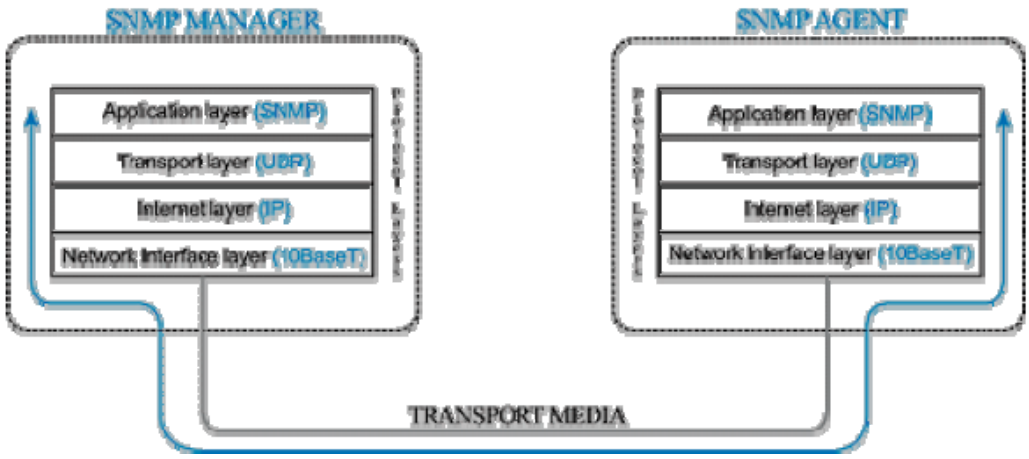
La mayoría de los fabricantes de dispositivos de red soportan SNMP, para ello unos agentes localizados en el dispositivo recogen la información, y la registran en una base de datos en forma de arbol, llamada MIB (Management

Information Base). Los MIB tienen un formato estándar, de forma que aún siendo de fabricantes distintos, las herramientas SNMP puedan obtener información del dispositivo, los MIB se estudiarán a profundidad en una sección posterior. El protocolo SNMP está formado por un agente que se instala en los nodos que se desean monitorear y un gestor que se instala en el ordenador encargado de monitorear la red. El gestor es el que obtiene la información de los agentes, el gestor solicita a los agentes información sobre los dispositivos gestionados, y los agentes responden a dicha solicitud, esto último tiene una excepción, mediante el comando SNMP trap, los agentes pueden enviar datos no solicitados al gestor, por ejemplo cuando hay un fallo eléctrico.
SNMP funciona bajo TCP/IP, lo cual significa que desde un sistema central se puede gestionar, cualquier ordenador de la LAN, WAN o internet.

Hasta el momento existen tres versiones del protocolo: SNMPv1 (versión 1), SNMPv2 (versión 2) y SNMPv3 (versión 3). Las tres son muy parecidas, solo que SNMPv2 tiene algunas mejoras sobre la primera versión, y de la misma forma SNMPv3 tiene ciertas ventajas sobre la segunda versión.

El protocolo SNMP, siendo un protocolo de la capa de aplicación, está diseñado para facilitar el intercambio de gestión de información entre los dispositivos de redes.

Figura 17. **Protocolo SNMP**



2.1.2 Arquitectura de Administración de Redes

El modelo de gestión de redes, que es usado para gestión de redes TCP/IP incluye los siguientes elementos:

-Estación de Gestión (Manager).
-Agente Administrador (Agente).
-Base de Información de Administrada (MIB).
- Protocolo de Administración de Redes.

La **estación de gestión (manager),** es típicamente un dispositivo independiente, que sirve como la interfaz entre la persona administradora de la red y el sistema de gestión, como mínimo la estación administradora (manager) tendrá:

-Un conjunto de aplicaciones de administración, para análisis de datos**,** aplicaciones para recuperación de alguna falla, y demás.

-Una interfaz, por la cual el administrador de la red pueda supervisar y controlar la red.

-La capacidad de traducir los requerimientos de administración de la red dentro de la supervisión actual y control de elementos remotos en la red.

-Una base de información extraída de la MIBs de todas las entidades en la red.

El otro elemento activo, en el sistema de administración de redes es el **Agente Administrador (agente),** son elementos como: hosts, puentes, ruteadores y hubs, pueden ser equipados con agentes SNMP tal que puedan ser administrados desde una estación administradora (manager). El agente administrador (agente) responde a peticiones, para información y acciones desde la estación de gestión (manager).

Los recursos en la red pueden ser administradas, representándolos como *objetos*. Cada objeto es, esencialmente, un *dato variable* pero representa un aspecto del agente administrador. La colección de objetos se refiere a una **base de información administrada** (MIB Management Information Base).

La MIB funciona como una colección de puntos de accesos en el agente, para la estación de gestión (manager), el cual es un *estándar*. Una estación de gestión (manager) realiza la función de supervisión tomando, el valor de los objetos MIB. Una estación de gestión (manager) puede hacer una *acción* al recurrir en un agente o puede *cambiar* la configuración en un agente modificando el valor de variables específicas.

La estación de gestión (manager), y el agente administrador (agente) están ligados por un ***protocolo de gestión de redes***. El protocolo usado para

la administración de redes TCP/IP es el Simple Network Management Protocol (SNMP), la cual incluye las siguientes capacidades dominantes:

-**Get:** Permite a la estación de gestión (manager), recuperar el valor de los objetos en el agente.

-**Set:** Permite a la estación de gestión (manager), alterar el valor de los objetos en el agente.

-**Trap:** Permite a un agente notificar a la estación de gestión (manager), de eventos significativos.

Los estándares no especifican el número de estaciones de gestión (managers), o el radio de estaciones de gestión (managers) hacia los agentes. En general, es prudente tener por lo menos; dos sistemas capaces de realizar la función de estación de gestión (manager), para proveer redundancia en caso de falla. Otra es una forma práctica de cuantos agentes puede manejar una simple estación de gestión (manager).

2.1.3 Arquitectura del Protocolo Administración de Redes

SNMP fue diseñado para ser un protocolo de la capa de aplicación que es parte de la suite del protocolo TCP/IP. Se piensa operar sobre mensajes UDP.

Figura 18. **Configuración SNMP**

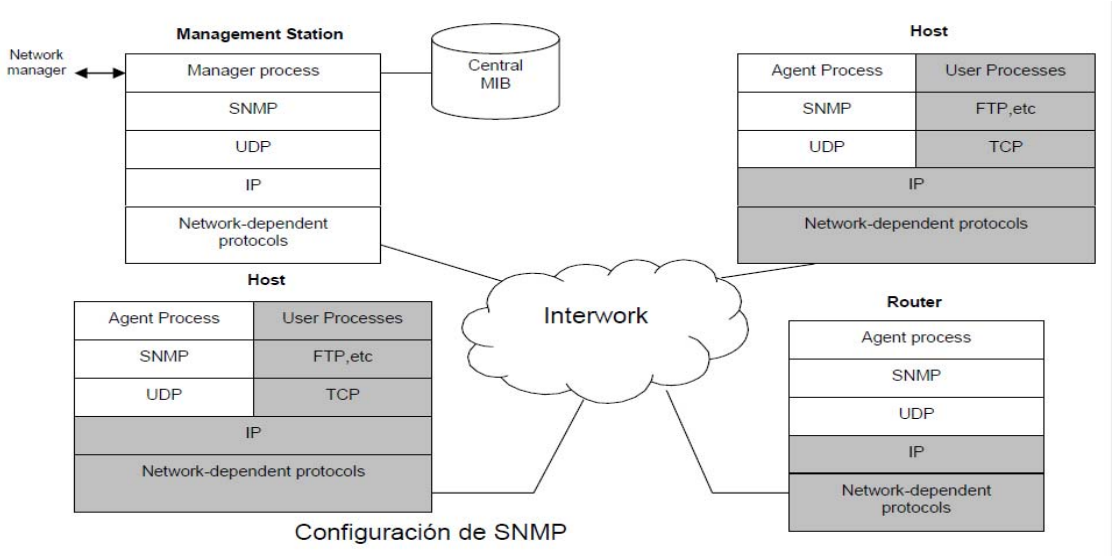
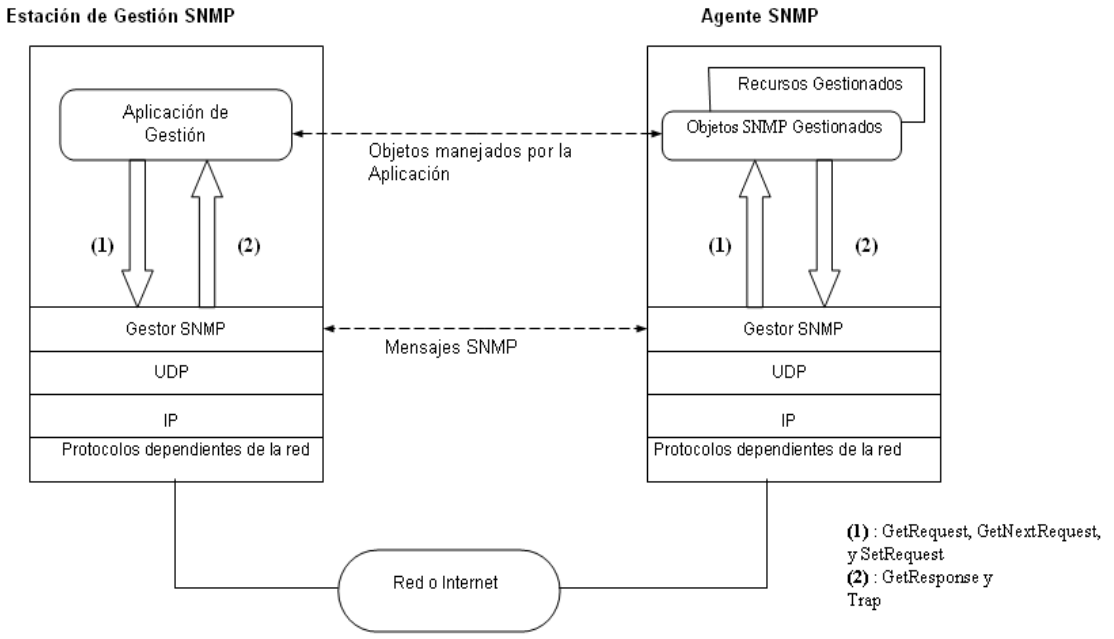


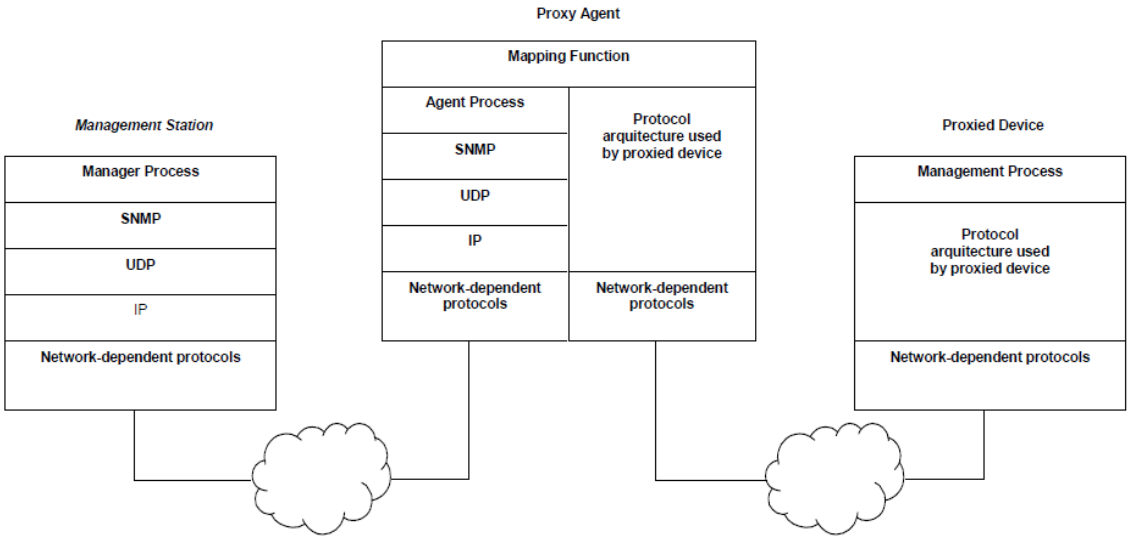
Figura 19. **Función del SNMP**



2.1.4 Proxies

El uso de SNMP requiere que todos los agentes, así como los managers, deben soportar una suite de protocolo, tal como UDP e IP, esto limita la administración directa y excluye otros dispositivos, tales como puentes y módems, que no soportan cualquier parte de la suite del protocolo TCP/IP. Para acomodar dispositivos que no implementan SNMP, el concepto de proxy fue desarrollado. En este esquema un agente SNMP actúa como un proxy para uno o más dispositivos; esto es, el agente SNMP actúa en nombre de los dispositivos que se encuentran en el proxy.

Figura 20. **Agente SNMP como Proxy**

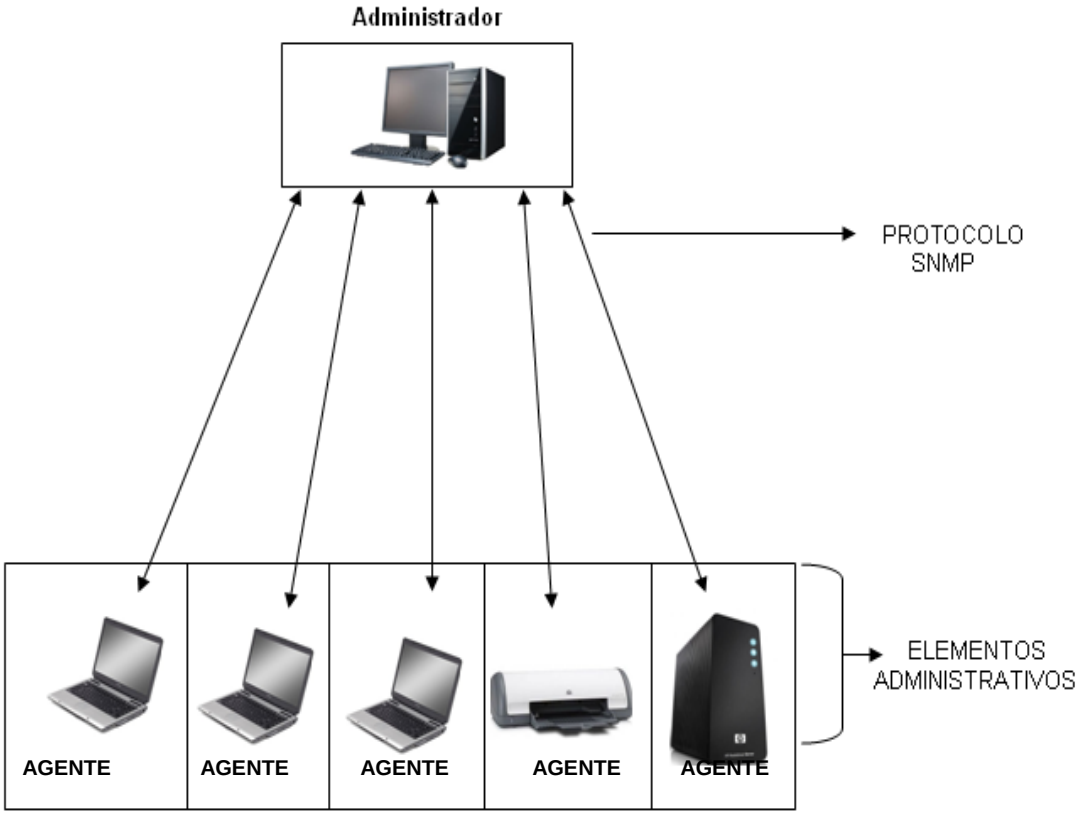


2.2 Comunidades SNMP

2.2.1 Nombramiento de comunidad y comunidades

La administración de la red puede ser vista como una aplicación distribuida, la red de administración SNMP tiene muchas características no típicas de las aplicaciones distribuidas. La aplicación involucra una relación de uno a varios entre el manager y un conjunto de agentes: el manager está disponible a tener y alterar objetos en el agente, y está disponible para la recepción de *traps* de los dispositivos administrados, entonces desde un punto de vista de control y operacional, el manager administra un número de dispositivos administrados.

Figura 21. **Diagrama SNMP**



Se denomina comunidad, a un conjunto de managers y a los dispositivos administrados, a las comunidades se les asignan nombres, de tal forma que este nombre junto con cierta información adicional sirva para validar un mensaje SNMP y al emisor del mismo.

SNMP define una comunidad como una relación entre entidades SNMP, una comunidad SNMP se escribe como una cadena de octetos sin interpretación. Esta cadena se llama nombre de comunidad, cada octeto toma un valor entre 0 y 255, cuando se intercambian mensajes SNMP, contienen dos partes:

- Una cadena de comunidad, mandada en texto sencillo; y

-Datos, conteniendo una operación SNMP y los operandos asociados.

La cadena de comunidad es un simple manejador para las relaciones de gestión, ahora se realizará una valoración de las propiedades de gestión de SNMP:

Identificación origen: como las cadenas de comunidad son enviadas sin protección, cualquier tercera parte capaz de interceptar un mensaje SNMP puede usar el mismo nombre de comunidad y de esa forma demandar, ser un miembro de la comunidad de mensajes.

Integridad del mensaje: cualquier tercera parte puede modificar un mensaje SNMP que intercepte. Protección limitada de reenvíos: cualquier tercera parte puede retrasar un mensaje SNMP que haya interceptado.

Privacidad: cualquier tercera parte puede leer el mensaje SNMP que haya interceptado.

Autorización: los agentes son responsables de mantener información local, así como los MIB que contiene, o las relaciones de proxy válidas; será sencillo para una tercera parte obtener los accesos correctos de una entidad autorizada para monitorear o controlar esos objetos.

Existen tres aspectos a controlar:

-Servicio de autenticación: el agente podría desear limitar el acceso a las MIB a los managers autorizados.

-Políticas de acceso: el agente podría desear privilegios de acceso diferentes a diferentes managers.

-Servicios proxy: un agente podría actuar como un proxy hacia otro agente.

2.2.2 Nombres de comunidad SNMP por omisión como 'public' y 'private'

El protocolo simple de gestión de red (SNMP), es habitualmente utilizado por los administradores de red; para la monitorización y administración de todo tipo de dispositivos conectados a la red, desde routers hasta impresoras pasando por ordenadores. SNMP utiliza, como único mecanismo de autenticación, un nombre de comunidad que se envía sin encriptar. Si la falta de encriptación ya de por si es mala, peor aun es que la mayor parte de los dispositivos SNMP utilizan como comunidad por omisión la palabra public; algunos fabricantes inteligentes de dispositivos de red han cambiado el nombre y utilizan la palabra private.

Los atacantes pueden utilizar esta vulnerabilidad del SNMP para reconfigurar o detener, de forma remota los dispositivos. La captura del tráfico SNMP, por otra parte, puede revelar una gran cantidad de información sobre la estructura de la red, así como de los dispositivos y sistemas conectados a la misma. Esta información es muy útil para los atacantes, en vistas a la selección de blancos para sus ataques.

Sistemas afectados
Todos los sistemas y dispositivos de red.

Registro CVE (Common Vulnerability Exposure):
(estándar de nomenclatura de vulnerabilidades)
Nombre de comunidad (public) SNMP en blanco o por omisión - CAN-1999-0517

Nombre de comunidad SNMP fácilmente identificable - CAN-1999-0516

Nombres de comunidad SNMP ocultos - CAN-1999-0254, CAN-1999-0186

Estos registros candidatos serán, con toda probabilidad, ampliamente modificados antes de ser aceptados como registros CVE.

Consejos para la resolución del problema:

- Si no se utiliza SNMP, deshabilitarlo.
- Si se utiliza SNMP, utilizar la misma política utilizada para las contraseñas y para los nombres de comunidad.

- Validar y verificar los nombres de comunidad mediante snmpwalk.

- Siempre que sea posible, configurar los MIBs en modalidad de solo lectura.

2.3 MIB (Management Information Base)

Para SNMP, la MIB es, en esencia, una estructura de base de datos en forma de árbol. Cada sistema (computadoras, ruteadores, puentes, etc.)en una red o intrared mantiene una MIB que refleja el status de los recursos administrados en ese sistema.

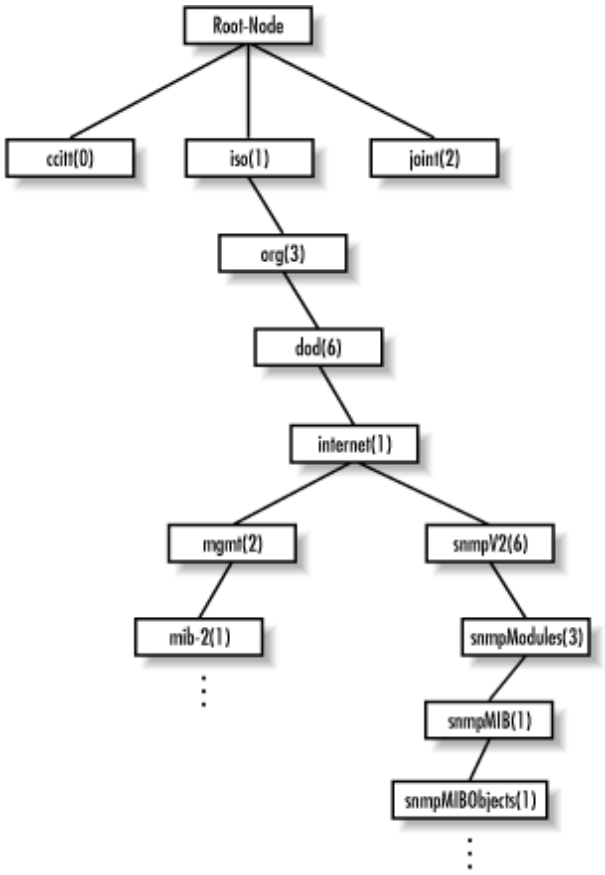
Un manager puede supervisar los recursos en ese sistema leyendo los valores de los objetos en la MIB, y puede controlar el recurso en ese sistema modificando esos valores. A través del **MIB** se tiene acceso a la información para la gestión, contenida en la memoria interna del dispositivo en cuestión.

MIB es una base de datos completa y bien definida, con una estructura en árbol, adecuada para manejar diversos grupos de objetos (información sobre variables/valores que se pueden adoptar), con identificadores exclusivos para cada objeto. Para que la MIB sirva a las necesidades de un sistema de administración de red, este debería conocer ciertos objetivos:

- El objeto u objetos utilizados para representar un recurso particular debería ser el mismo en cada sistema: este punto se refiere a la definición de objetos y la estructura de estos objetos en la MIB.

- Un esquema común para la representación debería ser utilizado para soporte de interoperabilidad: se refiere a la definición de una estructura de información administrada (SMI).

Figura 22. **Esquema de representación MIB**



La arquitectura SNMP opera con un reducido grupo de objetos que se encuentran definido con detalle en la RFC 1066 "Base de información de gestión para la gestión de redes sobre TCP/IP".

Los 8 grupos de objetos habitualmente manejados por MIB (MIB-I), que definen un total de 114 objetos (recientemente, con la introducción de MIB-II se definen hasta un total de 185 objetos), son:

- **Sistema:** Incluye la identidad del vendedor y el tiempo desde la última reinicialización del sistema de gestión.

- Interfaces: Un único o múltiples interfaces, local o remoto, etc.

- **ATT (Address Translation Table)**: Contiene la dirección de la red y las equivalencias con las direcciones físicas.

- IP (Internet Protocol): Proporciona las tablas de rutas, y mantiene estadísticas sobre los datagramas IP recibidos.

- ICMP (Internet Communication Management Protocol): Cuenta el número de mensajes ICMP recibidos y los errores.

- TCP (Transmission Control Protocol): Facilita información acerca de las conexiones TCP, retransmisiones, etc.

- UDP (User Datagram Protocol): Cuenta el número de datagramas UDP, enviados, recibidos y entregados.

- EGP (Exterior Gateway Protocol): Recoge información sobre el número de mensajes EGP recibidos, generados, etc.

Cada objeto dentro de una MIB SNMP está definido de una manera formal; la definición especifica el tipo de dato del objeto, este permite rangos de formas y valores, y su relación hacia otros objetos dentro de la MIB. La notación ASN.1 es utilizada para definir cada objeto individual y también definir el entorno de la estructura MIB

Ejemplos de objetos de algunos grupos. La lista completa está definida en el RFC 1213.

•*Grupo de sistema*

– sysDescr - Descripción completa del sistema(version, HW, OS).
– sysObjectID - Identificación que da el distribuidor al objeto.
– sysUpTime - Tiempo desde la última reinicialización.
– sysContact - Nombre de la persona que hace de contacto.
– sysServices - Servicios que ofrece el dispositivo.

•*Grupo de interfaces*

– ifIndex - Número de interfaz.
– ifDescr - Descripción de la interfaz.
– ifType - Tipo de la interfaz.
– ifMtu - Tamaño máximo del datagrama IP.
– ifAdminisStatus - Status de la interfaz.
– ifLastChange - Tiempo que lleva la interfaz en el estado actual.
– ifINErrors - Número de paquetes recibidos que contenían errores.
– ifOutDiscards - Número de paquetes enviados y desechados.

•*Grupo de traducción de direcciones*

– atTable - Tabla de traducción de direcciones.
– atEntry - Cada entrada que contiene una correspondencia de dirección de red a dirección física.
– atPhysAddress - La dirección física dependiente del medio.
– atNetAddress - La dirección de red correspondiente a la dirección física.

2.4 Trap

Los Traps permiten a los agentes comunicar de manera asíncrona a los gestores de cualquier evento que haya sucedido al objeto gestionado y en el cual, el gestor tiene interés de ser informado.

Los agentes snmp en dispositivos como routers, switches, printers, servidores, etc. pueden enviar alarmas (*traps)* cuando ocurren ciertos eventos: se cae una interfaz, se estropea el ventilador de un router, la carga de procesos excede un límite, se llena una partición de disco, un UPS cambia de estado etc.

Es necesario un mecanismo inteligente para notificar al administrador, sólo cuando interesa. En el agent se pueden definir niveles de threshold para decidir si un evento debe o no generar un trap.

Tabla XII. **Resumen de Traps Genéricos**

EVENTO	SIGNIFICADO
ColdStart	El dispositivo se ha reiniciado, por lo que la configuración del agente podría cambiar.
WarmStart	El dispositivo se ha reiniciado, pero el agente sigue intacto.
LinkDown	El dispositivo ha detectado un fallo en uno de sus enlaces a la red. El enlace que falla es especificado en el campo variable-bindings
LinkUp	El dispositivo ha detectado que uno de sus enlaces con la red se ha activado. El nombre del enlace y el valor de la variable ifIndex aparecen en el campo variable-bindings.
AuthenticationFailure	El agente ha detectado un fallo en la autentificación de un mensaje.
EgpNeighborLoss	Uno de los nodos colaboradores EGP se ha caido. El primer elemento del campo variable-bindings es el nombre y valor de la variable egpNeigAddr del nodo afectado.
EnterpriseSpecific	Evento de un fabricante particular. El evento se identifica con el campo specific-trap.

3. APLICACIÓN SNMPc

3.1 Plataforma SNMPc

3.1.1 Descripción

Para las redes y los gestores del sistema, el secreto del éxito es descubrir un problema antes que nadie y resolverlo antes de que sea notado, para ello, se necesita toda la información de la red, algunos de los mayores retos y desventajas que se ven hoy en día con marco de gestión de red son el costo, la complejidad excesiva y bajo rendimiento de la inversión. Por el contrario, Castle Rock SNMPc es un económico y seguro sistema de gestión de red distribuida que permite supervisar la infraestructura de la red.

3.1.2 Versiones del SNMPc

La aplicación SNMPc se encuentra disponible en los formatos Enterprise y Workgroup.

3.1.2.1 SNMPc Workgroup

Es un sistema que se instala en un solo servidor, enfocado a administrar empresas de pequeñas a medianas. Todos los componentes se ejecutan en un único sistema y soporta solo un usuario, el tamaño de base de datos del mapa se limita a 1 000 objetos. La versión Workgroup no incluye funciones avanzadas de presentación de informes.

3.1.2.2 SNMPc Enterprise

Es un sistema de administración enfocado a administrar decenas de miles de elementos. Cuenta con una arquitectura distribuida con la que se puede acceder de manera remota a los servidores y a los agentes de poleo, tiene capacidades avanzadas de reporteo y publicación de estos vía Web.

Basic System (Sistema Base): es el servidor de SNMPc con una consola de acceso remoto y un agente de poleo remoto.

Remote Access Extension: da la capacidad de instalar y recopilar información de agentes de poleo remoto. Permite el acceso de múltiples consolas remotas para visualizar y configurar los servidores y mapas, así como el acceso a través de cualquier PC con un web browser

Tabla XIII. **Diferencias entre versiones**

ELEMENTOS	VERSIÓN ENTERPRISE	VERSIÓN WORKGROUP
Capacidad	Prácticamente ilimitado (25,000 objetos por servidor y un número ilimitado de servidores)	Permite el moitoreo de hasta 1,000 objetos
Escalabilidad en servidores	Permite la integración e interacción de mas de un servidor	Solamente soporta un solo servidor
Acceso Remoto *	Se puede acceder, configurar y administrar desde una o múltiples consolas remotas	No lo soporta
Visualización del estado de los equipos y reportes a través de un web browser *	Se puede acceder al mapa de la red, conocer las alarmas e incluso recopilar variables MIB desde ualquier estaciónde la red que cuente con un web browser instalado	No lo soporta
Recopilación de información a traves de "pollers" distribuidos *	Se pueden instalar "pollers" (agentes de recopilaciónde información SNMP) en sitios remotos con el fin de minimizar el tráfico y simplificar la administración	No lo soporta
Usuarios soportados	Usuarios ilimitados	Un usuario
Creación de reportes	Tiene la capacidad de crear reportes de "comportamiento de variables", es decir, puede graficar e incluso publicar vía un web server, el comportamiento de la demanda de ancho de banda de los enlaces, el comportamiento de porcentaje de uso del CPU, etc	No lo soporta
Exportación de información "histórica" vía ODBC	La información recopilada para generar reportes en Web se puede exportar a unabase de datos de manera automática y periodica lo que da al usuario una capacidad mucho mayor para generar reportes mucho mas específicos y personalizados	No lo soporta
Sistema Operativo que lo soporta	XP, 2000, NT **	XP, 2000, NT, ME, 98

3.1.3 Descripción de la arquitectura

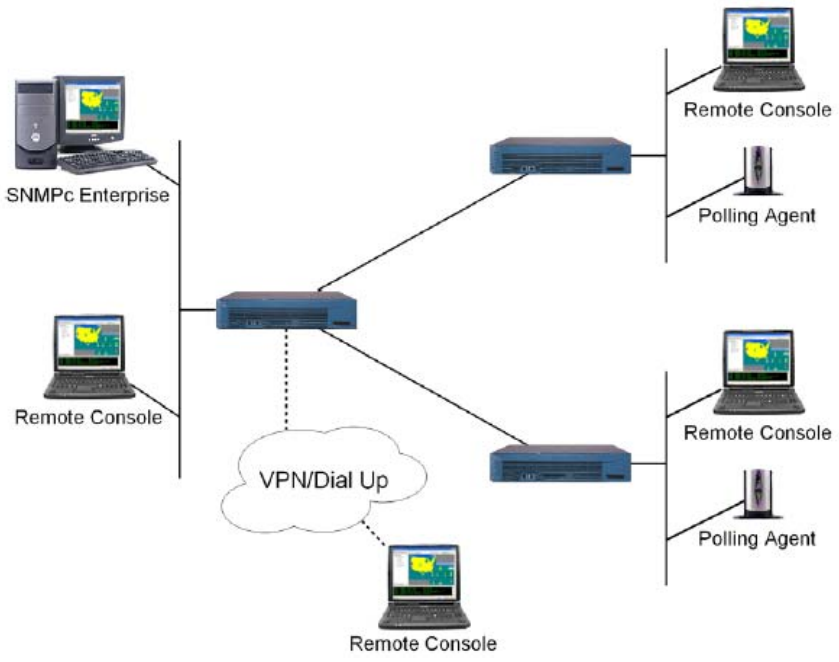
SNMPc es un administrador de red distribuida, de propósito general que ofrece las siguientes ventajas sobre un producto independiente:

- Mediante el uso de poleo y de los componentes de servidor que se ejecutan en varios equipos, SNMPc se puede escalar para gestionar redes muy grandes.

- Al utilizar múltiples consolas remotas, SNMPc fortalece el intercambio de información sobre la gestión de muchas personas.

- SNMPc es rentable debido a una colección de componentes, cuesta menos que un número equivalente de directores independientes.

Figura 23. **Arquitectura distribuida**



SNMPc Enterprise utiliza una arquitectura modular que es escalable desde pequeñas a redes muy grandes, mantener bases de datos de configuración de servidores, realizar acciones de eventos, y generar informes programados, los agentes de Poleo hacen un descubrimiento automático de la red, poleando el estado del dispositivo, guardando las estadísticas históricas, y generando alarmas. La consola proporciona la interfaz de usuario para los servidores y agentes de poleo.

Gracias a la tecnología base de datos distribuida, proporciona una plataforma de alto rendimiento que permite a los componentes SNMPc que se desplegarán en una variedad de escenarios, incluyendo grupos de trabajo, el dominio y configuración de un gestor de gestores.

SNMPc utiliza el popular protocolo de administración SNMP para polear y configurar los dispositivos, estaciones de trabajo y servidores a través de redes IP, junto con todas las características esperadas en cualquier estación de gestión SNMP, SNMPc también incluye las siguientes funciones avanzadas:

- Puede tener hasta 25 000 dispositivos administrados.
- Soporta un gestor de gestores en la arquitectura.
- Escalable, arquitectura distribuida con redundancia opcional.
- Acceso por consolas remotas y por medio de JAVA Web.
- Admite SNMPv1, v2, v3 y RMON.
- Sistema base con alarmas automáticas y notificación de eventos por medio de correo electrónico / buscapersonas .
- Auditoria de eventos para las acciones del usuario (login / edit).
- Servicios de aplicaciones (TCP) de poleo.
- Programación basada en WEB / Informes impresos.
- Expresiones de MIB.

• RMON-I en interfaz de usuario para la aplicación.
• Muestra estadísticas de la red en tiempo real.
• Aplicación de programación de interfaces con ejemplos.

3.1.3.1 Modos de acceso a dispositivo

SNMPc admite varios modos de acceso de dispositivos que incluyen: NONE (solamente TCP), ICMP (ping), SNMP v1, v2c y SNMP V3 SNMP, cada modo se describe brevemente a continuación.

3.1.3.2 NONE (solamente TCP)

Null Access se utiliza para los servicios de poleo solamente en TCP, donde se restringe el acceso ICMP / SNMP por un servidor de seguridad (firewall).

3.1.3.3 ICMP (Ping)

El modo ICMP (ping) se utiliza para dispositivos que no soportan SNMP, pero todavía se puede hacer ping para ver si ellos están respondiendo, esto puede incluir servidores y estaciones de trabajo.

3.1.3.4 SNMP V1 y V2c

SNMP v1 y SNMP V2c son muy similares en protocolo SNMP Agent que es utilizado por la mayoría de los dispositivos de red actualmente empleados, cualquier dispositivo que admita V2c general, también soporta V1.

SNMPc utiliza inteligencia autónoma para cambiar de un modo a otro, según sea necesario, así que en la mayoría de los casos siempre seleccionará SNMP V1 como el modo de acceso para cualquier dispositivo SNMP.

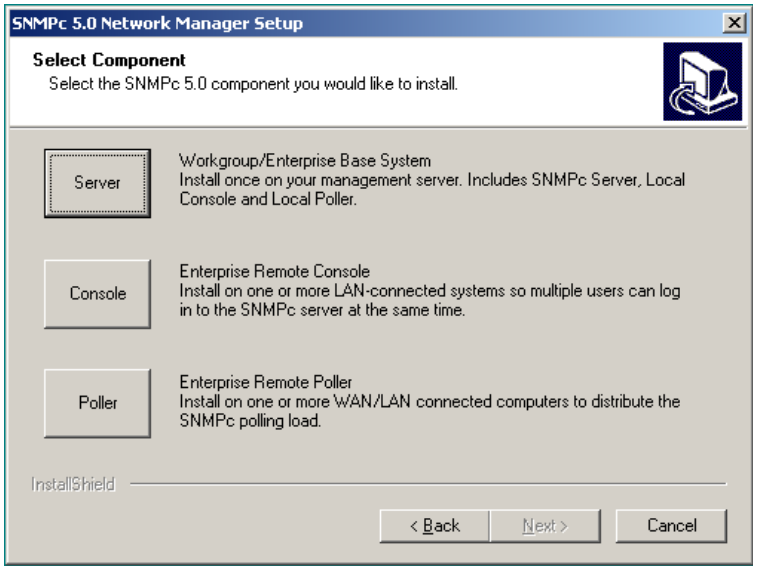
3.1.3.5 SNMP V3

SNMP V3 es un protocolo seguro de SNMP Agent que admite la autenticación y privacidad (encriptación). El uso de SNMP V3 se considera un tema avanzado, el cual no se profundizará en este caso.

3.1.4 Instalación del SNMPc y consola local

El programa de instalación mostrará un diálogo con tres botones de las opciones instalables SNMPc, en el sistema SNMPc principal, sólo tendrá que instalar el componente de servidor, ya que incluye una consola local y agente de poleo.

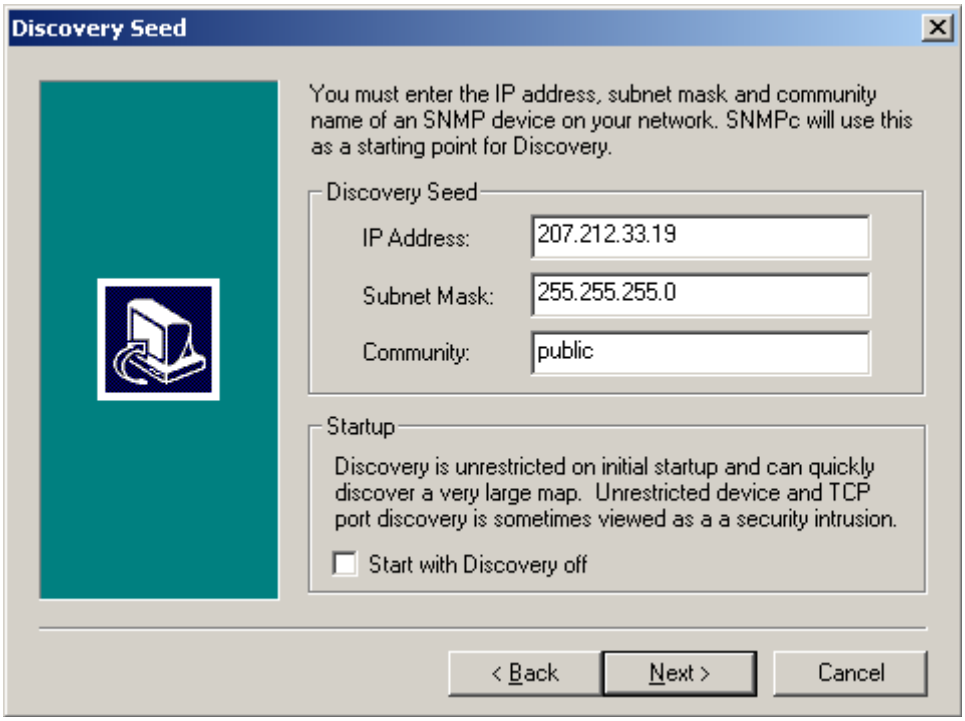
Figura 24. **Cuadro de diálogo al iniciar instalación**



Se pulsa el botón Servidor, y luego preguntará por el directorio donde se hará la instalación, y luego aparecerá el cuadro de diálogo de Discovery Seed, se procede a configurar el Network Auto-Discovery, el Discovery Seed es el punto de partida para en Network Discovery, el Seed idealmente debe ser la dirección IP del Router SNMP local habilitado.

Después de ingresar la dirección IP y la mascara de subred deberá ingresar la lectura de comunidad del Router. Por defecto, la comunidad de lectura para la mayoría de los dispositivos es *Public*, la comunidad de lectura es sensible a caracteres (MAYUSCULAS / minúsculas).

Figura 25. **Cuadro de diálogo para configurar el Discovery Seed**



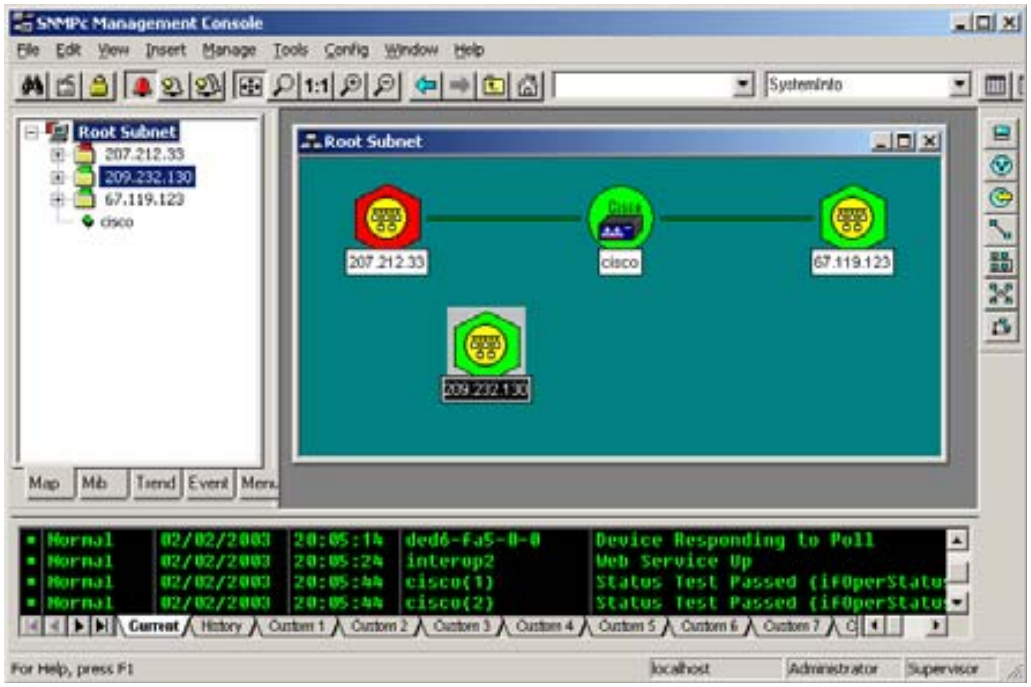
El cuadro de chequeo es proporcionado para deshabilitar el Network Discovery al inicio.

Cuando el SNMPc haya sido instalado, reinicie la maquina y el SNMPc deberá arrancar automáticamente, el SNMPc Enterprise puede ser configurado para correr como un servicio bajo entorno Windows, usted deberá ver el icono amarillo de SNMPc en el área de notificación de Windows.

3.1.5 Iniciando el Servidor de SNMPc y Consola Local

Para controlar las tareas SNMPc, debe iniciar sesión en Windows con permisos de administrador, después de la instalación del componente SNMPc Server, se le pedirá que reinicie el sistema Windows, cuando el sistema se ha reiniciado y de inicio la sesión de Windows, el servidor SNMPc y la Consola de aplicaciones se iniciarán automáticamente y será Logueado.

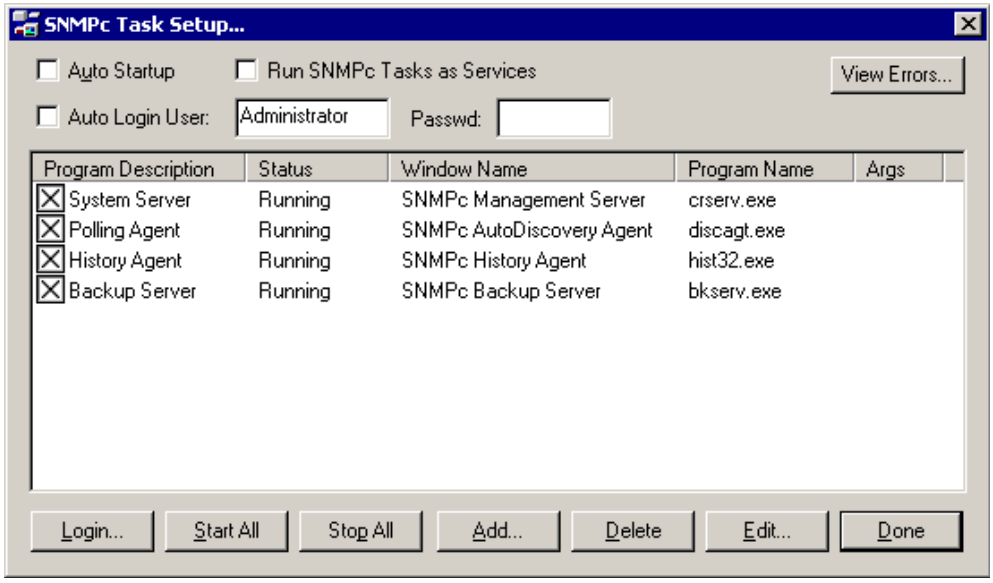
Figura 26. **Consola SNMPc**



3.1.5.1 Desactivación de la sesión automática de Consola

Para desactivar la consola automática de arranque y Login, se va al menú Inicio de Windows y utilizar la dirección de menú *Programs/ SNMPc Network Manager / Configure Task.* Desactivar la casilla de verificación Auto Login de usuario y pulse el botón Done.

Figura 27. **Ventana de configuración de arranque inicial**



3.1.6 Inicio de una sesión de consola local

Ir al menú Inicio de Windows y utilizar la dirección de menú *Programs / SNMPc Network Manager / Login Console*, en la entrada del sistema, escriba localhost como dirección del servidor, escriba el nombre de usuario y contraseña y pulse aceptar, al principio sólo hay un usuario llamado administrador sin contraseña.

3.1.7 Detener e iniciar el servidor

Ir al menú Inicio de Windows y utilizar el menú Programs / SNMPc Network Manager / Shutdown System para detener las tareas del SNMPc Server System, utilice el menú Inicio y luego Programs / SNMPc Network Manager / Startup System para reiniciar las tareas del SNMPc Server System.

3.1.8 Usando los elementos de Consola

El siguiente diagrama y la tabla muestran los principales elementos de la Consola de SNMPc.

Figura 28. **Localización de botones de consola**

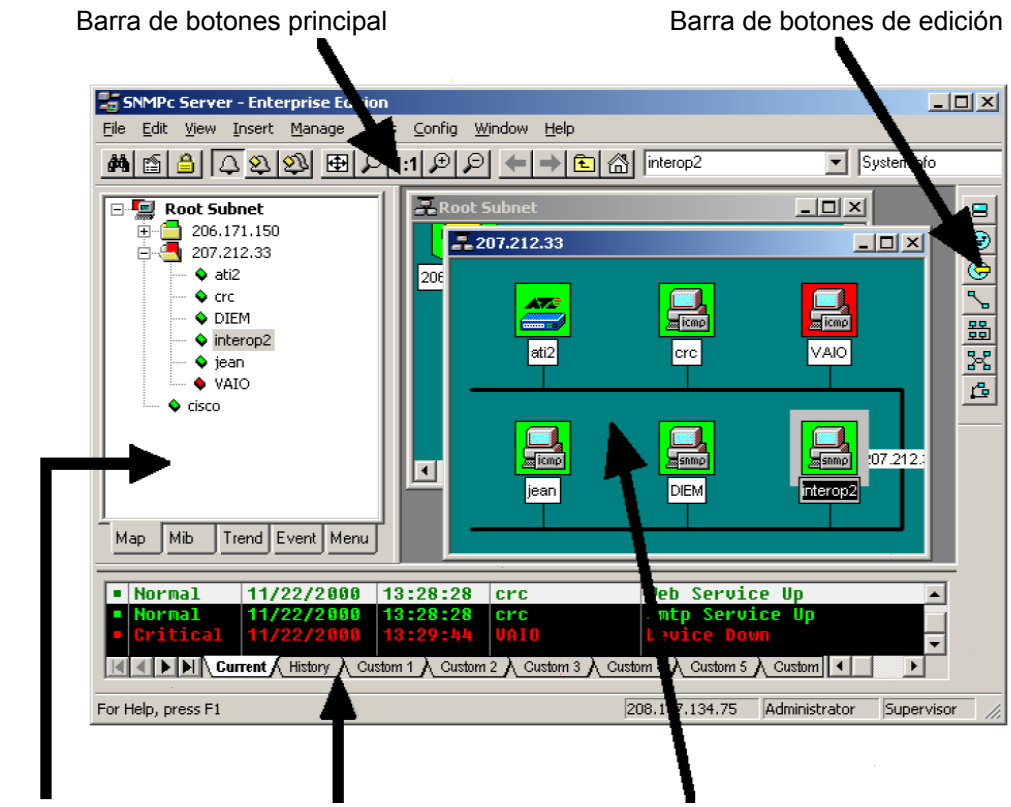


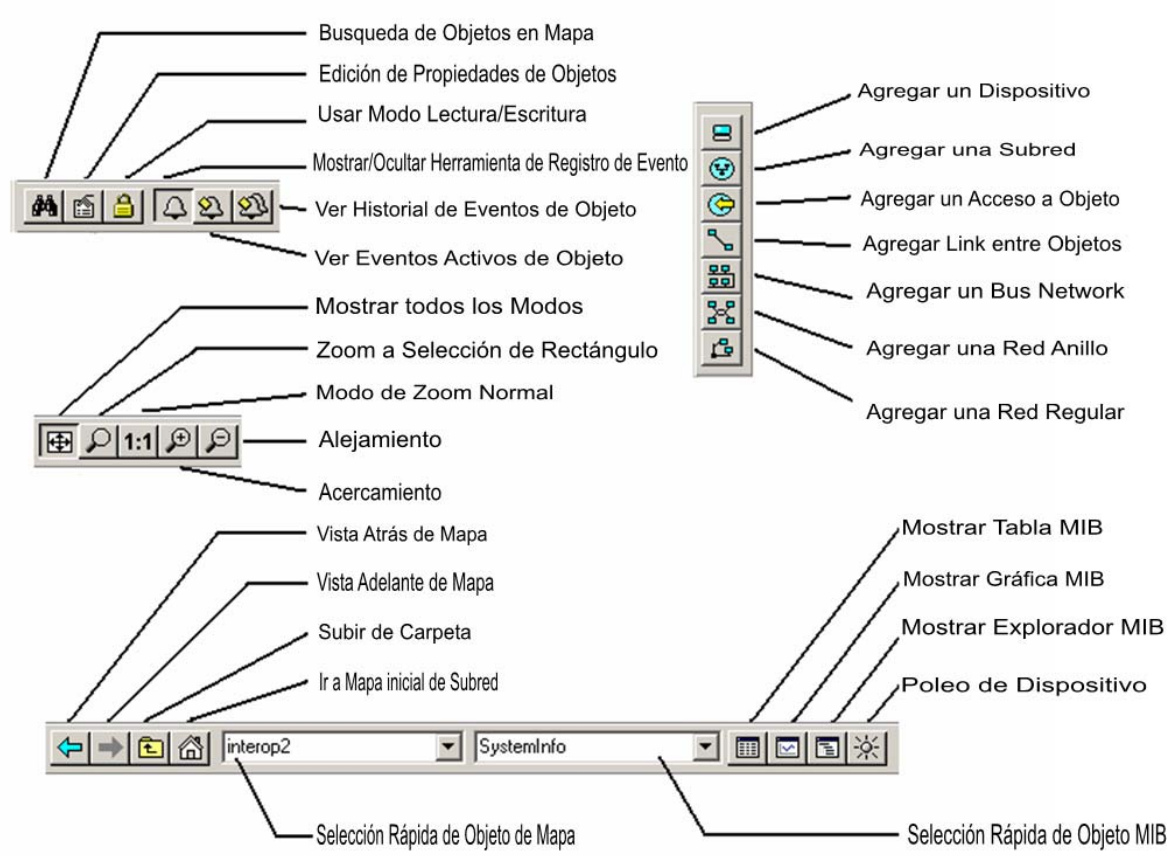
Tabla XIV. **Descripción de los grupos de botones de consola**

ELEMENTO	FUNCION
Barra de Botones Principal	Botones y controles para ejecutar comandos comunes con rapidez
Barra de Botones de edición	Botones para insertar rápidamente elementos en el mapa
Selección de Herramientas	Control de pestañas para la selección de los objetos dentro de los diferentes módulos funcionales SNMPc
Herramienta de Registro de Eventos	Control de pestañas para la visualización de las entradas del registro de eventos filtrados
Area de Vista de Ventana	Vista de mapa, de las Tablas Mib, y las ventanas de Mib gráfico se muestran aquí

3.1.9 Botones de Comandos de Consola

El siguiente diagrama muestra la función de cada botón en la barra principal, y en el de editar, cada uno de estos botones tiene un elemento correspondiente del menú principal.

Figura 29. **Descripción de botones de consola**



3.1.10 Herramienta de selección

Si usted no puede ver la herramienta de selección, utilice en el menú View / Selection Tools para mostrarlo, usar la herramienta de selección para manipular objetos de una de varias bases de datos, utilice el control de arrastre a la derecha de la herramienta de selección, para cambiar su tamaño, seleccione una de las pestañas de selección de herramientas, para mostrar un control de árbol de la base de datos, utilice el menú del botón derecho dentro del árbol de selección de los comandos específicos de bases de datos.

Tabla XV. **Descripción de pestañas de consola**

SELECCIÓN DE PESTAÑAS	DESCRIPCIÓN
Mapa	Mapa de objetos de base de datos, incluidos los dispositivos y subredes.
Mib	Compila MIB de SNMP, tablas personalizadas y las expresiones personalizado Mib.
Trend	Reporta perfiles que definen los procedimientos de poleo a largo plazo y progración de reportes
Event	Filtros de Eventos utilizados para determinar lo que sucede cuando se recibe un evento.
Menu	Personaliza menús que aparecen en la Gestión, Herramientas, menús y la Ayuda SNMPc.

3.1.11 Herramienta de Registro de Eventos

La herramienta de registro de sucesos, muestra diferentes vistas filtradas del registro de eventos SNMPc, si no puede ver el registro de sucesos de la herramienta, utilice en el menú View / Event Log Tool para mostrarlo.

• Seleccione la pestaña *Current* para mostrar los eventos (actuales) no reconocidos, estos eventos tienen un cuadro de color de la parte izquierda de la entrada del registro, el color de los objetos del mapa está determinado por la prioridad más alta de eventos, no reconocidos para ese objeto.

• Seleccione la pestaña *History* para mostrar todos los eventos, incluyendo eventos reconocidos como no reconocidos.

• Seleccione una de las pestañas *Custom* y utilice el botón derecho del ratón para el menú *Filter View* para especificar qué eventos se debe mostrar en esa pestaña.

• Haga doble clic en una entrada de evento, para mostrar una ventana Map View con el icono del dispositivo visible correspondiente.

• Para ver rápidamente los eventos, para un determinado dispositivo, primero seleccione el dispositivo y luego utilice uno de los botones de View Event (o en el menú View / Active Events y View / History Events). Esto mostrará los eventos dispositivo en una ventana independiente en la zona de Vista de Windows.

• Para borrar uno o más eventos, seleccione los eventos y pulse la tecla suprimir.

• Reconocer (quitar el estado actual de) un evento, seleccione el evento y utilice el menú del botón derecho *Acknowledge.*

• Para borrar el registro completo de eventos, utilice en el menú File / Clear Events.

3.1.12 Área de Vista de Ventana

El área de Vista de Ventana es la principal interfaz para visualizar el mapa SNMPc, y los resultados de comandos. Esta área utiliza la especificación Multi-Document-Interface (MDI) para mostrar varias ventanas al mismo tiempo, use el Menú Window/Cascade and Window/Tile para reordenar las ventanas del área de Vista de una manera que hace que sean visibles.

Las ventanas en esta área pueden estar en una de varias formas:

• Una ventana *maximizada* utiliza toda la zona y cualquier otra ventana se oculta detrás de ella, si cierra una ventana maximizada, la siguiente ventana se mostrará en nivel superior en el estado maximizado, se necesita tener cuidado al usar ventanas maximizadas, porque es fácil perder la pista de cuántas ventanas se haya abierto y hay un límite superior, use el menú Windows para ver una lista de las ventanas, use el menú Windows/Cascade para ver todas las ventanas al mismo tiempo.

• Una ventana *superpuesta* no ocupa toda la zona, una ventana será completamente visible y otras ventanas están parcialmente ocultas detrás de ella, esta es la situación más común para el área de Vista de Ventana ya que permite consultar mapas, tablas y gráficos al mismo tiempo y rápidamente se mueve entre ellas.

• Una ventana *minimizada* se muestra como una barra de título pequeña con botones para abrir/cerrar la ventana, las ventanas no son comumente cerradas dentro del área de Vista de Ventana porque, a diferencia del caso de maximizado, estas se pueden perder fácilmente detrás de otras ventanas.

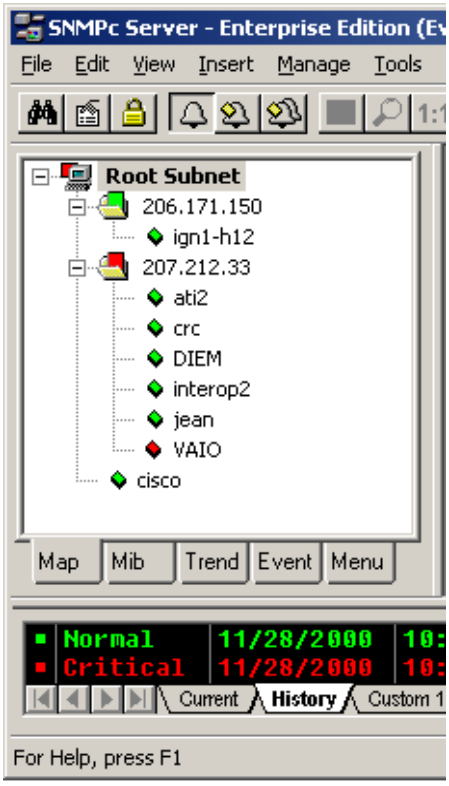
3.2 Mapas

3.2.1 Trabajando con la base de datos de mapa

3.2.1.1 Usando el árbol de selección mapa

Se localiza el Selection Tool en el lado derecho de la consola, si no se puede ver el Selection Tool, se debe usar el menú View/Selection Tool para mostrarlo. Se selecciona la primera pestaña marcada ***Map***, *a*parecerá el árbol de selección de Mapa, este muestra todos los iconos de los objetos en el Mapa, incluyendo subredes (que contienen niveles inferiores del mapa), dispositivos, e iconos de acceso. Las Redes y Links no se muestran en el árbol de selección de mapa.

Figura 30. **Diagrama de árbol de mapas**



• Un solo clic sobre el pequeño cuadro a la izquierda del icono, de una subred (icono de carpeta) para abrir o cerrar ese subnivel en el árbol de selección.

• Un doble clic en el nombre de subred (a la derecha del icono de la carpeta) para abrir ese nivel de subred como una ventana en la vista de Mapa (ver más abajo).

• Un clic izquierdo en cualquier nombre de objeto para seleccionar dicho Objeto, se utilizan las teclas Shift y Ctrl para seleccionar varios objetos.

• Con la Tecla *Suprimir* se remueven los objetos seleccionados.

• Después de abrir dos niveles de subred, se selecciona los nombres de múltiples dispositivos y se puede arrastrar con el ratón para pasar de una subred a otra, se debe tomar en cuenta que ningún Link y Network adjunto se mueven, y los Links serán eliminados durante el movimiento (se puede volver a agregar manualmente más tarde).

• Un clic derecho en el icono de un dispositivo (rectángulo de color) o en el nombre para ver la disposición del menú de clic derecho, se usan esos menús para editar las propiedades del objeto seleccionado, desplegar tablas, y ejecutar los menús personalizados.

• Abrir un árbol de subred y usar el menú Insert/Map Object o los botones de Edit Button Bar para agregar iconos de objetos al árbol de subred.

Cada icono en el árbol de selección de Mapa, es del color según el estado del objeto representado, los iconos de subred (y el nivel superior el icono

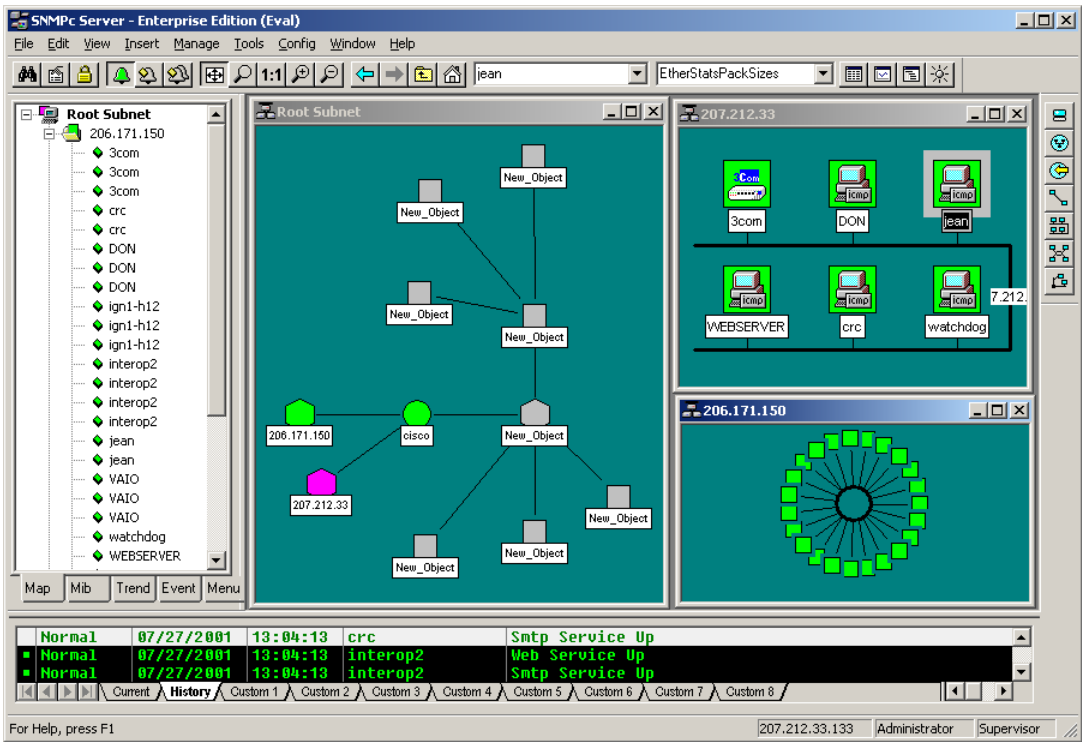
principal de subred) muestran el color de más alta prioridad de todos los objetos subyacentes.

3.2.2 Uso de la ventana de vista de mapas

La ventana de vista de mapas es un solapado de ventadas que se muestran en el área de vista de ventana del SNMPc, esta es el área principal donde se puede ver la topología del mapa, como un diagrama y manipular fácilmente los objetos del mapa (añadir, borrar, mover).

Se debe tomar en cuenta que el área de vista de ventana, muestra varias ventanas y si la ventana superior es maximizada (ocupa toda el área), entonces cualquier otra ventana se ocultará, se usa el menú Windows/Cascade para mostrar todas las ventanas dentro del área de vista de ventana.

Figura 31. **Vista de mapas en consola**



• El menú View/Map View/Root Submap muestra el nivel superior del mapa de SNMPc

• Doble Clic sobre el nombre de una subred en el árbol de selección de mapa, o icono de subred en la vista de mapa muestra una vista del mapa de esa subred.

• Para moverse fácilmente a la vista de mapa, se hace clic derecho en cualquier lugar de la vista y se arrastra el ratón para mover el contenido de la vista, también se puede utilizar la barra de desplazamiento, pero esto no es tan fácil.

• Los botones de Zoom sirven para alejar o acercar la vista del mapa, el Pan/Zoom sirve para hacer Zoom dentro de un rectángulo de selección (clic izquierdo y se arrastra el rectángulo), el botón 1:1 permite volver al modo normal de Zoom (icono y nombre visible).

• Los botones Previous View y Next View sirven para moverse hacia adelante y hacia atrás, entre los diferentes niveles de Zoom que se hayan seleccionado.

3.2.3 Moviendo objetos de mapa

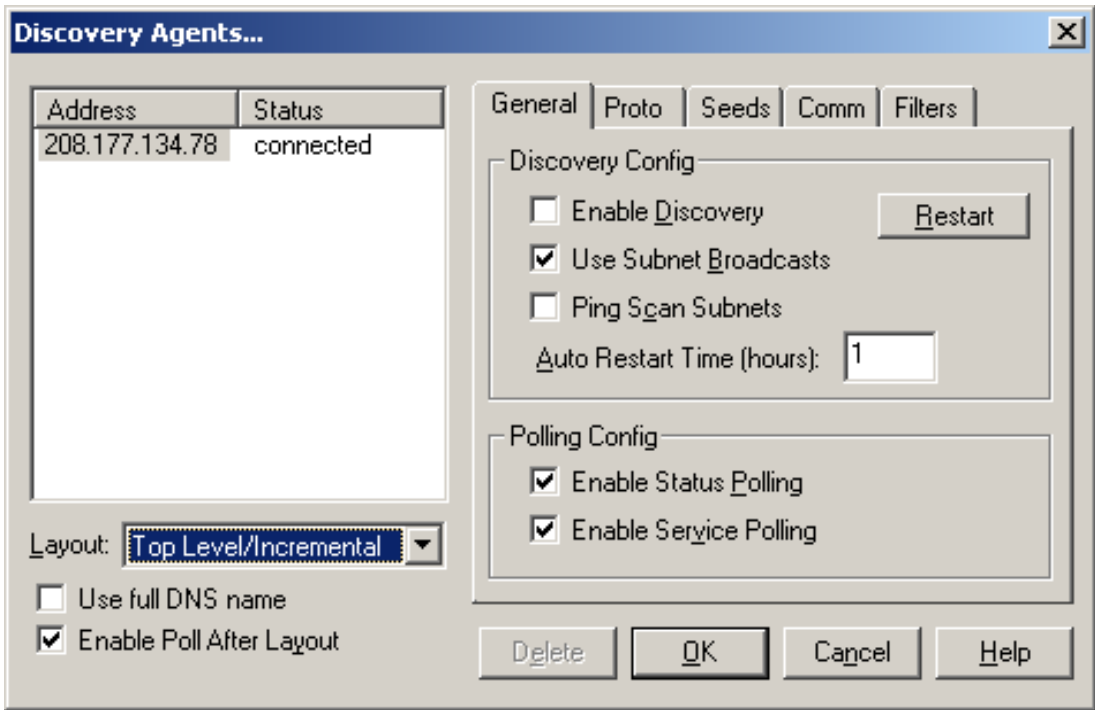
SNMPc, normalmente utiliza un proceso de descubrimiento para agregar subredes, dispositivos, enlaces y redes en una topología lógica, que representa una jerarquía de dos niveles de subred IP, el nivel superior incluye todos los dispositivos de router y los iconos de subred, la segunda capa incluye los dispositivos de un solo puerto relacionados con los buses de Red en los iconos de subred adecuada, el mapa de nivel superior se organiza automáticamente como una red en estrella.

Los objetos de Mapa, son colocados lo más cercano a una organización cuadriculada, cuando estos son movidos, se usa el menú Config/Console Option y se selecciona Show Grid para chequear el cuadriculado del mapa, ajuste el tamaño de la cuadrícula en el Editor de Grid Spacing.

3.2.4 Moviendo objetos al nivel principal

Dado que el agente se encargará de descubrir continuamente el nivel de mapa superior, antes de cambiar manualmente el nivel de superior (Root) es necesario cambiar la manera de descubrimiento.

Figura 32. **Ventana de agente de descubrimiento de red**



1. Se desactiva la casilla de verificación *Habilitar Descubrimiento* con esto el descubrimiento queda totalmente desabilitado

2. Seleccionar los objetos descubiertos del Layout desplegado a fin de que los objetos recientemente descubiertos, se añadan a un icono de subred separado, nombrado objetos descubiertos (Discovered Objects).

3. Seleccionar Top Level / Incremental del Layout de modo que los objetos recientemente descubiertos se agregan utilizando un algoritmo de disposición gradual que no altere el trazado existente.

Para mover los objetos en el nivel superior, sólo se tiene que seleccionar uno o más objetos en una vista de mapa, y arrastrar el ratón, los objetos seleccionados se mueven a la ubicación nueva del ratón, las siguientes dos vistas de mapa muestran una forma automática (figura 33) y una forma manual (figura 34) de un submapa ordenado (Root):

Figura 33. **Objetos ordenados automáticamente en una subnet**

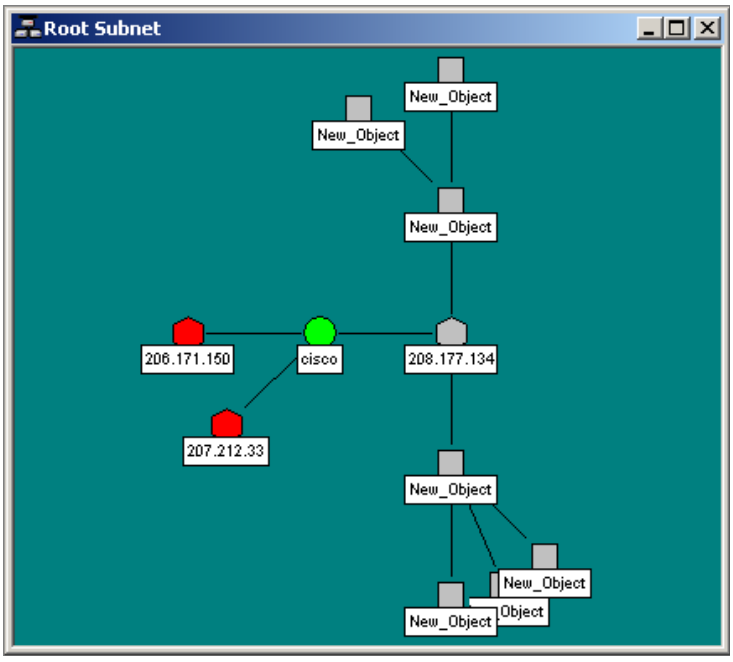
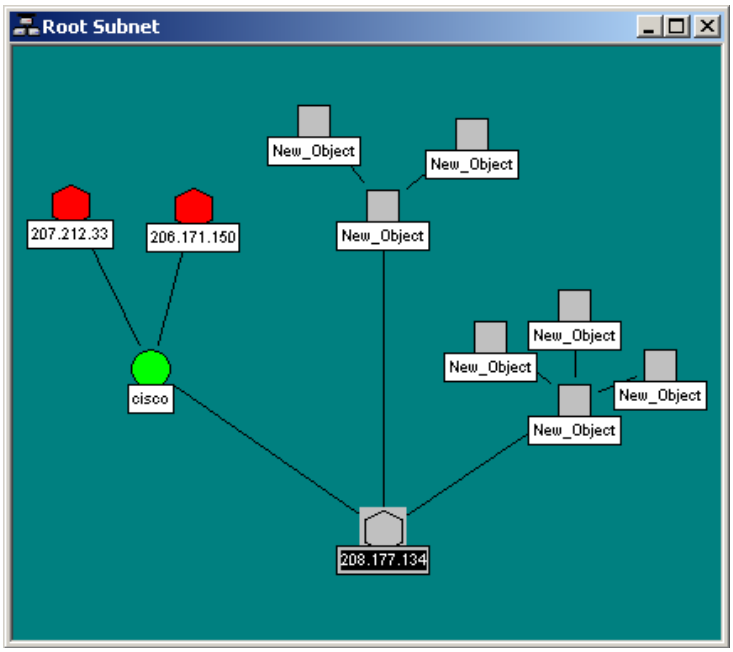


Figura 34. **Objetos ordenados manualmente en una subnet**



3.2.5 Moviendo objetos dentro de los niveles de subred

Los dispositivos de un solo puerto son agregados a un mapa secundario, por debajo de los iconos de subred de nivel superior, cada capa de subred también incluirá un Bus Network al que todos los dispositivos son agregados, se puede mover dispositivos de todo el Bus Network seleccionándolos y arrastrándolos a la nueva posición, sin embargo, el Bus Network es ordenado automáticamente y el objeto será únicamente colocado en donde fue arrastrado.

Si se necesita reordenar totalmente los niveles inferiores, entonces lo mejor es cambiar la red de un Bus a una red normal, esta red no se ordena automáticamente y se puede mover iconos en cualquier lugar de la vista, así como cambiar la forma en la red con el uso de los puntos de unión, se puede hacer clic y arrastrar cualquier punto de unión o segmento de red, y añadir o eliminar puntos de unión con un doble clic en la red.

También se puede desconectar los objetos del Bus Network mediante el borrado del Link de agregado, a continuación, el objeto suelto puede ser trasladado a cualquier parte en la vista; las siguientes dos vistas de los mapas muestran un nivel de subred que se ordenan automáticamente (figura 35) y ordenada de forma manual utilizando una red regular (figura 36):

Figura 35. **Subred ordenada automáticamente**

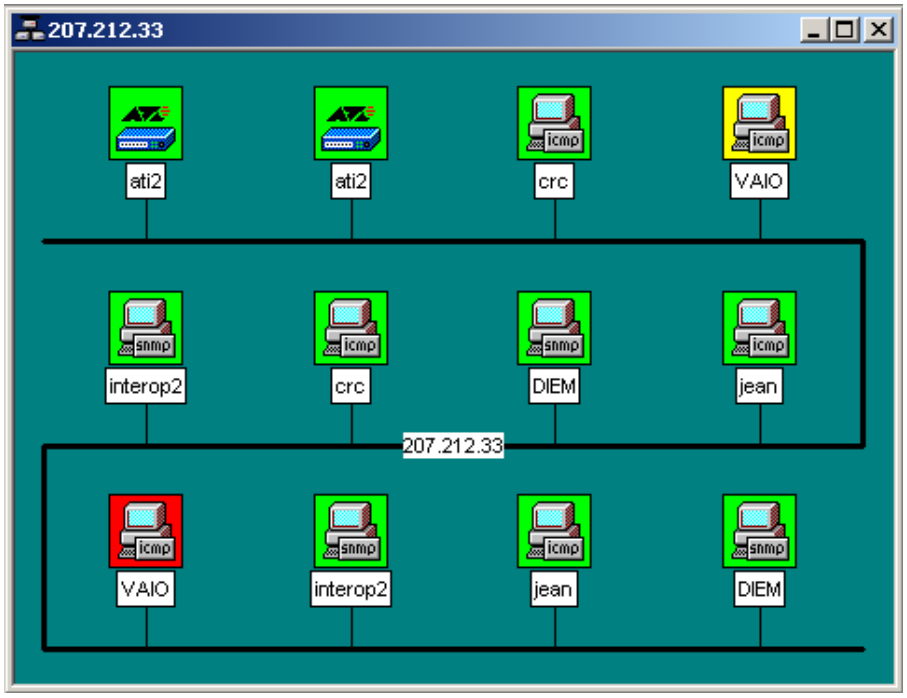
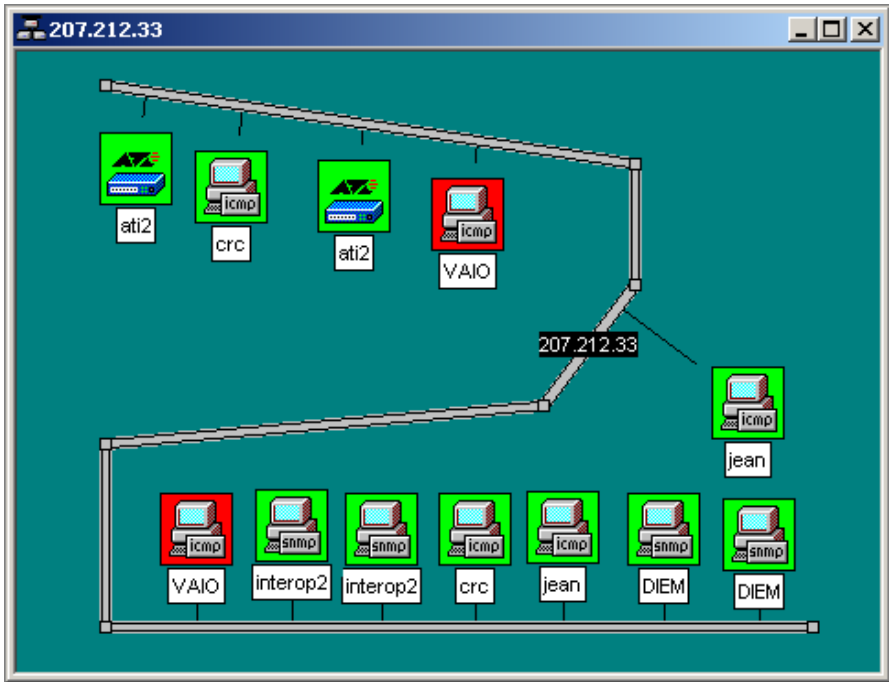


Figura 36. **Subred ordenada manualmente**



3.2.6 Cambiando las propiedades a los objetos

• Se usa el menú Edit/Propierties para cambiar los atributos de uno o más objetos seleccionados, para editar múltiples objetos, todos los objetos seleccionados deben ser del mismo tipo (subred, dispositivo, etc)

• Se define el nombre del objeto en la etiqueta del cuadro de edición.

• Se establece el tipo de objeto en Type, el tipo de objeto sólo puede ser cambiado para los objetos de tipo de red (anillo, bus, Red).

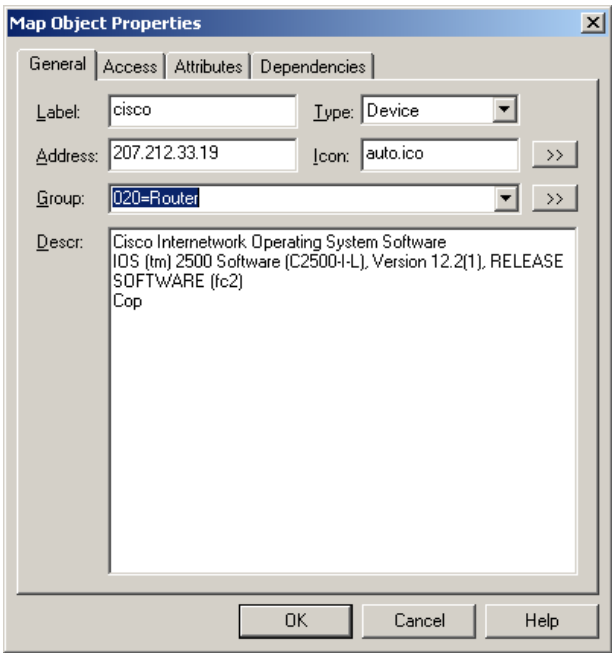
• Para objetos de dispositivos, se define la dirección IP el objeto en el cuadro de edición de direcciones, esto puede ser en formato de punto o un nombre DNS, también se puede añadir un número de puerto UDP a una dirección IP , notación punto (es decir, 198.22.11.22.168).

• Para los objetos de Goto, establecer el nombre de la subred a la que salta ese Goto en el cuadro de edición de dirección.

• Se define un nombre de alias para un grupo de objetos de dispositivo similares, en el Group del cuadro de edición.

• Para iconos de tipos de objetos (de subred, de dispositivos, Goto), se define el icono en Icon del cuadro de edición, esto normalmente se pone en auto.ico de manera que un icono se selecciona automáticamente en función del dispositivo, que indique el identificador de objeto del SNMP.

Figura 37. **Propiedades de un objeto**



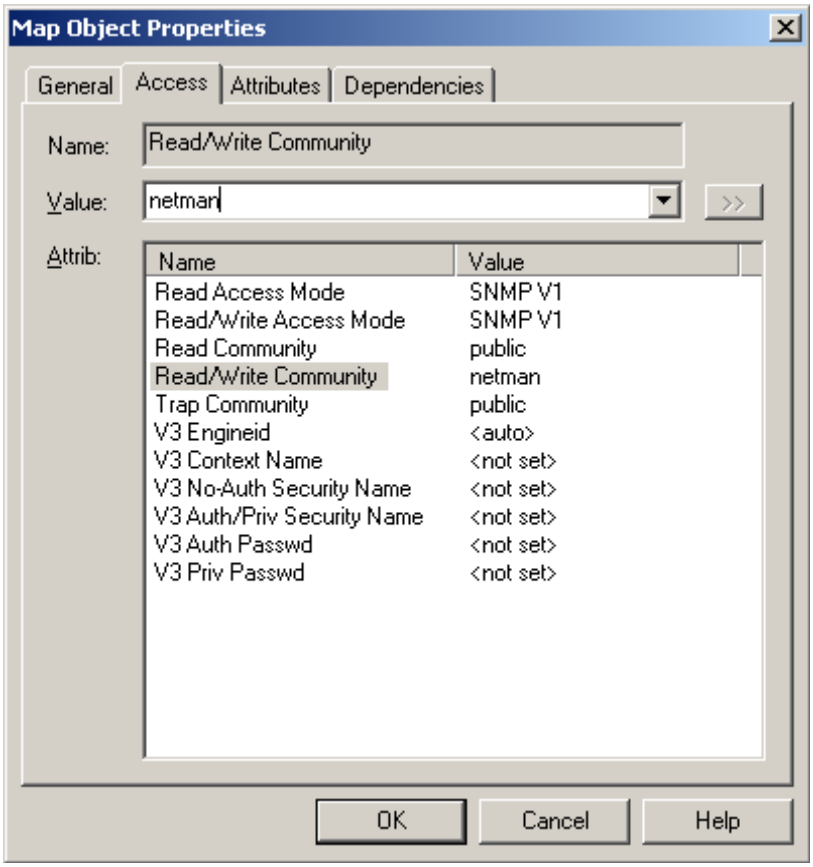
• Seleccione la pestaña Access para establecer los parámetros de acceso de un dispositivo, enlace, o un objeto de red, para obtener una descripción de los parámetros de acceso, se puede verificar la tabla que se muestra en la página siguiente.

• Para cambiar un parámetro de acceso, primero seleccione el nombre del parámetro en la tabla de atributo, el nombre del parámetro seleccionado se muestra en el cuadro Name y el valor actual, en el valor del control desplegable.

• En el valor desplegable, seleccione uno de los valores que se muestran o escriba un nuevo valor, tenga en cuenta que el valor desplegado no necesariamente refleja todos los valores posibles para el atributo.

• Cuando se edita varios objetos, los parámetros de acceso que tiene un valor diferente, para los diferentes objetos se muestra como #####, la modificación de estos atributos se define como el nuevo valor para todos los objetos seleccionados.

Figura 38. **Configuración de comunidad de objeto**



En la tabla XVI se describen los parámetros de acceso disponibles en la pestaña de Access de las propiedades de objetos para dispositivo, link, y Network. Los parámetros de Access no son válidos para los tipos de objetos como subred y Goto.

Tabla XVI. **Descripción de parámetros de objetos**

Nombre de Atributo	Descripcion
Read Access Mode	El modo usado para las operaciones de poleo y lectura SNMP. Selecciona *ICMP (Ping)* para dispositivos no SNMP. Selecciona *SNMP V1* para el estándar de dispositivos SNMP. Selecciona *NONE (TCP Only)* para los dispositivos que sólo tienen servicios de poleo TCP .
Read/Write Access Mode	El modo utilizado para operaciones de escritura SNMP. Seleccione SNMP V1 para el estándar de dispositivos SNMP. También puede forzar este modo para ser utilizado tanto para operaciones de lectura y escritura de la consola (no las operaciones de poleo) mediante el botón Read and Write en la barra de botones SNMPc (3er botón de la izquierda).
Read Community	El nombre de la Comunidad utilizado para las operaciones de SNMP V1/V2c cuando el modo de acceso de lectura se utiliza.
Read/Write Community	El nombre de la Comunidad utilizados para las operaciones de SNMP V1/V2c cuando se utiliza el modo de acceso de lectura / escritura
Trap Community	El nombre de la Comunidad esperado en el receptor de Traps de SNMP V1/V2c. Esto se utiliza para que coincida con un trap entrante un objeto de mapa.
V3 Engineid	SNMP V3 identificador del motor (detectado automáticamente).
V3 Context Name	SNMP V3 Nombre de contexto (normalmente blanco).
V3 No Auth Security Name	Nombre SNMP V3 de Seguridad para su uso con el modo de acceso no auth (no autenticación, no privado).
V3 Auth/Priv Security Name	Nombre SNMP V3 de Seguridad para el uso con los modos de acceso autenticado o privado (encriptado).
V3 Auth Password	SNMP V3 contraseña a utilizar para autenticación
V3 Priv Password	SNMP V3 contraseña a utilizar para la privacidad (encriptación).

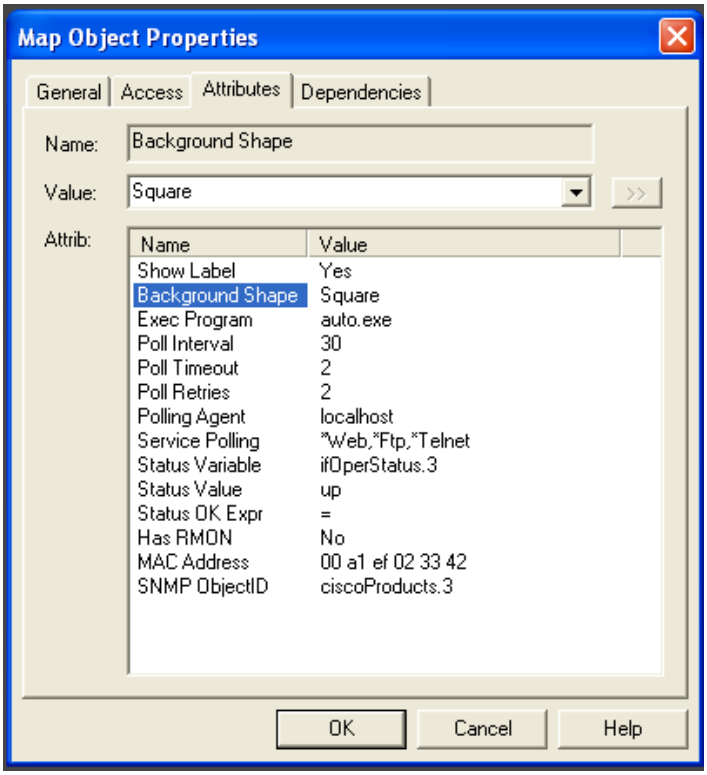
• Seleccione la pestaña de Attribute para establecer los atributos que dependen del tipo, para ver una descripción completa de todos los tipos de atributos dependiente del objeto, se muestra la tabla en la página siguiente.

• Para cambiar un atributo, primero seleccione el nombre del atributo en la pestaña Attrib, el nombre del atributo seleccionado se muestra en el cuadro Name y el valor actual, en el valor del control desplegable.

• En el valor desplegable, seleccione uno de los valores desplegable o escriba un nuevo valor, tenga en cuenta que el valor desplegado no necesariamente refleja todos los valores posibles para el atributo.

• Cuando se edita varios objetos, los parámetros de acceso que tiene un valor diferente para los diferentes objetos se muestra como #####, la modificación de estos atributos se define como el nuevo valor para todos los objetos seleccionados.

Figura 39. **Configuración de atributos de objeto**



La tabla XVII muestra cada atributo disponible en la pestaña de Object Properties Attributes, los tipos de objeto que tienen validez y una descripción del atributo.

Tabla XVII. **Descripción de atributos según el objeto**

OBJECT	ATTRIBUTE NAME	DESCRIPCIÓN
D,L,N,S,G	Show Label	Muestra u oculta el nombre del objeto.
S, G, D	Background Shape	Icono de fondo, como Cuadrado, Círculo, Hexágono, Octágono, o Diamante.
S	Bitmap	Fondo con imagen de mapa de bits
S	Bitmap Scale	Fondo con imagen de mapa de bits escalada (mas grande según el número)
L	Show Link Name	Nombre de Link
D	Exec Program	Hacer doble clic para programa de los dispositivos. Incluye alguno de los argumentos de programa especiales siguientes: $ a - Dirección IP, $ n - »nombre de nodo, $ g - Comunidad de lectura; $ S - Establecer la comunidad, $ w - Número de la consola de la ventana.
D, L, N	Poll Interval	Segundos entre secuencias de poleo
D, L, N	Poll Timeout	Segundos para esperar una respuesta después del poleo
D, L, N	Poll Retries	Numero de intentos fallidos de poleo despues de una secuencia
D, L, N	Polling Agent	Dirección IP del sistema de Polling Agent que genera estadisticas de desempeño según el poleo para un objeto. A menos que se use un Remote Polling Agents, esto se deja como *localhost*.
D, L, N	Service Polling	Lista de servicios de poleo (TCP or servicio personalizado de poleo)
D, L, N	Status Variable	Una variable SNMP con instancia que se polea para determinar el estado del dispositivo (en lugar de sólo la respuesta del dispositivo). Por ejemplo, ifOperStatus.3.
D, L, N	Status Value	El número a ser comparado con el valor devuelto de estado variable.
D, L, N	Status OK Expr	La expresión a utilizar al comparar el valor de estado a la variable de estado resultante para determinar si el estado está bien (<,>, <=,> =, =, =).
D, L, N	HasRMON	Se coloca TRUE para activar la herramienta RMON.
D, L	MAC Address	dispositivo principal de direcciones MAC o un enlace de direcciones MAC, si se conoce.
D, L, N	SNMP ObjectID	De sólo lectura. El sistema de identificador de objeto de un objeto SNMP.

Nota: Dispositivo = D, L = Link, N = Anillo, Bus, Red, S = subred, G = Goto

3.2.7 Agregando objetos al mapa

SNMPc, soporta varios tipos de objetos, incluyendo subredes, dispositivos, links y redes, para agregar objetos, primero se abre una ventana para ver el mapa y luego se usa el menú Insert/Map Object o el botón en la barra de edición, después de agregar el icono del objeto, se necesita moverlo a la posición deseada, si no se puede ver el nuevo objeto, se puede usar el botón View All.

La tabla XVIII describe los diferentes tipos de objetos:

Tabla XVIII. **Descripción de objetos del mapa**

TYPE	DESCRIPTION
Subnet	Un icono de subred contiene otras capas del mapa, incluyendo posiblemente otras subredes. • Se hace doble clic en un icono de subred para abrir una ventana de vista de la capa inmediatamente inferior. • Utiliza el botón de la ventana primaria para subir una capa a la vista de subred primaria. • Utiliza el botón de Root Subnet para abrir la vista de mapa de nivel superior.
Device	Un icono de dispositivo representa un dispositivo que es poleado, incluyendo SNMP y dispositivos poleados por Ping. • Cuando se agrega un objeto de dispositivo, es necesario establecer la dirección del dispositivo, esta aparece en el cuadro de diálogo Propiedades. Se puede añadir un puerto UDP opcional a la dirección como x.x.x.Port. • A continuación, seleccione la pestaña Access y se define el modo de acceso de lectura y lectura / escritura parámetros Modo de acceso. Utilice ICMP (ping) para dispositivos no SNMP (o NONE en el que sólo quiere polear servicios TCP), y el uso de SNMP V1 para los dispositivos SNMP. Para los dispositivos SNMP V1, también se debe establecer la Comunidad de lectura y de lectura / escritura de la Comunidad estos parámetros validarán el nombre de la comunidad. • Por último, seleccione la pestaña Attributes y seleccione los valores adecuados para el intervalo de poleo, el tiempo de espera de poleo, y los reintentos al polear.
Link	Un objeto de Link es una línea entre dos iconos de objetos (subred, dispositivo, goto). Los objetos de Link pueden ser poleados por lo que opcionalmente puede establecer con una dirección IP y el access / attributes de poleo de un dispositivo. Sin embargo, mediante un enlace por defecto el intervalo de poleo para los Link se fija en cero por lo que no se polea. Para agregar uno o más objetos de enlace, primero seleccione los objetos de dos o más dispositivos y, opcionalmente, una subred o un objeto único de la red, a continuación, pulse el botón Agregar Link desde la barra de Editar.
Network	Existen varios tipos de objetos de Network que tienen diferentes estilos de diseño. • Un Bus Network organiza automáticamente la red y los Links/ iconos adjuntos en una configuración de bus. • Un anillo de la red organiza automáticamente los objetos adjuntados en un anillo. • Un objeto regular de red pueden ser en forma manual. Haga doble clic en una red regular de objetos para crear un punto de unión. Haga doble clic en un punto de unión existente para eliminarlo. Haga clic en un objeto de unión o segmento de la red y arrástrelo para moverlo en la vista de mapa. • Los objetos de red también pueden ser poleados, pero el intervalo de poleo se establece en cero (no poleados) de forma predeterminada. Utilice uno de los botones Add Network de la barra de Editar para agregar una red. Si primero seleccionar varios objetos, SNMPc también añadirá links entre los iconos y la nueva red.
Goto	Un objeto Goto es como una subred en que se puede hacer doble clic en ella para abrir una ventana nueva de vista de mapa. Sin embargo, un objeto Goto muestra el mapa de la subred que se nombra en el campo Address. Para hacer un Goto que abra el Submapa principal, se deja el campo de direcciones en blanco.

3.3 Registros, estadísticas y gráficas de SNMPc

3.3.1 Visualización de datos de dispositivo Mib

3.3.1.1 Usando el árbol de selección Mib

• Primero, seleccione una o más objetos de dispositivo SNMP.

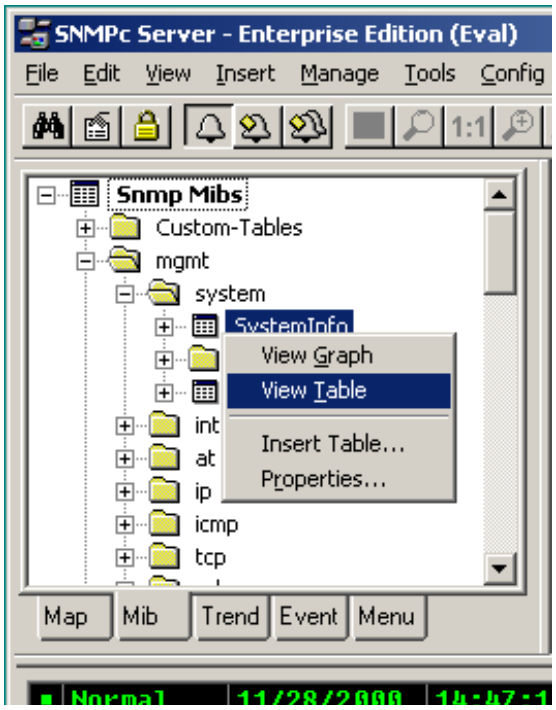
• Localice la herramienta de selección a la izquierda de la ventana de consola, si no puede verlo, se utiliza el menú View/ Selection Tool para mostrarlo, pulse la pestaña Mib para activar el árbol de selección de MIB, este árbol muestra todos los MIBs compilados estándar y privado.

• Abra el subárbol Mgmt para mostrar los elementos Mib, abra el subárbol privado para mostrar los elementos Mib específicos del fabricante, tenga en cuenta que cada dispositivo admite un subconjunto de MIB estándar y privado, depende de uno para determinar si un dispositivo es compatible con una particular tabla MIB.

• Abrir elementos subárbol hasta que aparezca uno o varios iconos de cuadrícula, de la tabla en la lista, estas son las definiciones de tablas Mib que serán en su mayoría trabajadas.

• Haga clic en uno de los nombres de tabla y utilice en el menú View Table o View Graph para mostrar el contenido de la tabla para los dispositivos seleccionados como una figura o un gráfico.

Figura 40. **Árbol de MIB**



3.3.1.2 Usando Menús de Gestión

Seleccionar uno o más dispositivos SNMP objetos y utilizar el botón derecho gestionar o-menús para mostrar tablas MIB SNMP común en varios formatos, tener en cuenta que no todos los dispositivos aplican todas las tablas de estos menús así que en algunos casos, los menús producirán un error para mostrar un resultado, depende de usted para determinar si la tabla que especifica el menú es compatible.

• Utilizar el menú List <tablename> para mostrar una tabla de entrada.

• Utilizar el menú Edit <tablename> para mostrar un diálogo de edición para una tabla de entrada.

• Utilizar el menú Display <tablename> para mostrar una tabla de entrada múltiple.

• Utilizar el menú Graph <tablename> para mostrar un gráfico de todas las instancias de la tabla, también puede iniciar un gráfico después de seleccionar algunos elementos en una tabla de muestra.

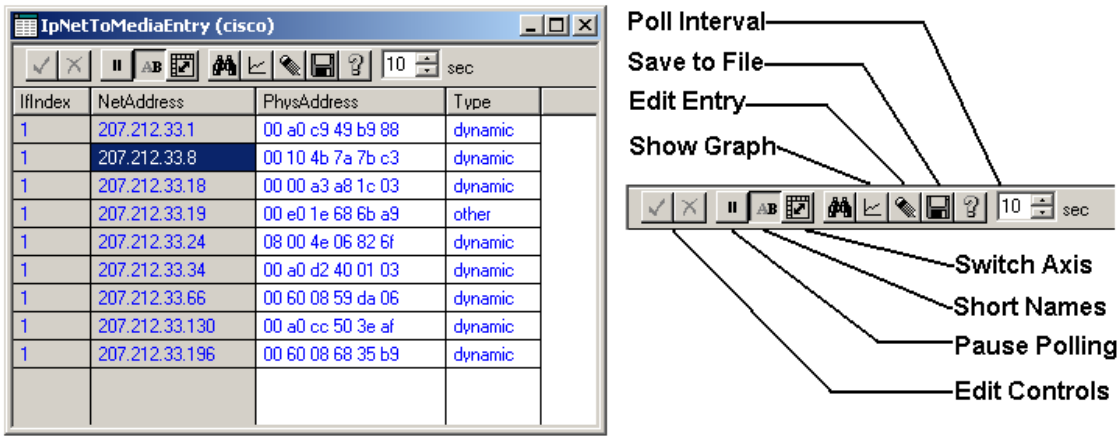
3.3.2 Uso de los menús personalizados

Los menús manager son en realidad los menús integrados personalizados de un archivo de configuración externo, también puede añadir menús personalizados para mostrar tablas en particular, por ejemplo, si usted solamente tiene unos pocos tipos de dispositivos en su red a la que probablemente debería añadir menús personalizados, para mostrar los cuadros de proveedores específicos para dichos dispositivos, a continuación, puede mostrar información Mib utilizar los menús del botón derecho en lugar de buscar tablas Mib en el árbol de selección, para obtener más información sobre los menús personalizados, seleccione la pestaña Menú del Selection Tool y pulse la tecla F1.

3.3.3 Elementos mostrados en la tabla

El siguiente diagrama enseña la tabla desplegada y describe la función de sus controles.

Figura 41. **Botones de tabla**



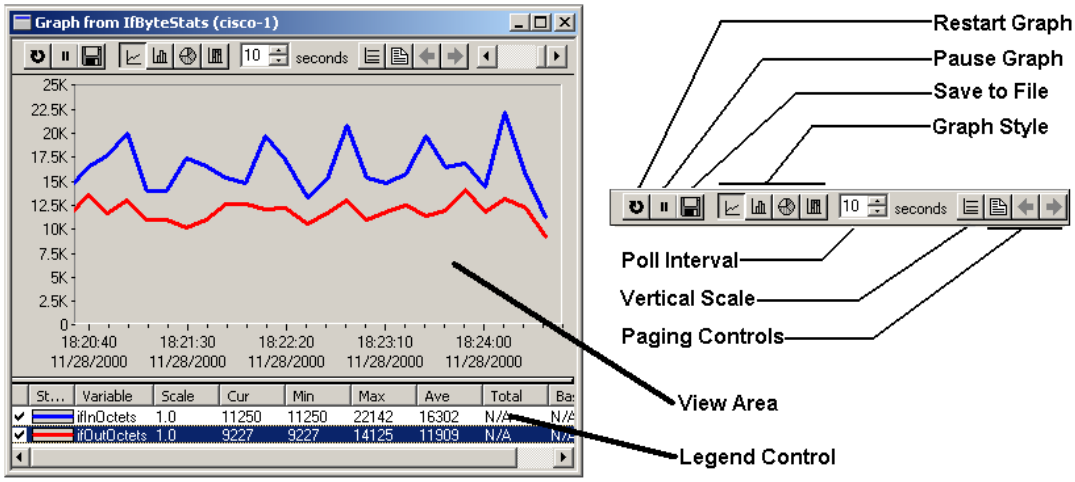
• Para iniciar una visualización de gráfico, primero seleccione una o más celdas (filas, columnas o celdas individuales), a continuación, utilice el botón Show Graph.

• Para cambiar una celda de la tabla y hacer una operación para el dispositivo, en primer lugar se deben localizar las celdas seleccionadas (los que se muestran en azul), haga doble clic en la celda para moverse en el modo Edit, introduzca el nuevo valor directamente en la celda (o seleccione en el desplegable si aparece), a continuación, pulse el botón Check Edit Control, para cancelar una operación de conjunto en curso, pulse el botón Cross Edit Control.

3.3.4 Elementos de la gráfica

El siguiente diagrama muestra una visualización de gráfico y la función de control gráfico.

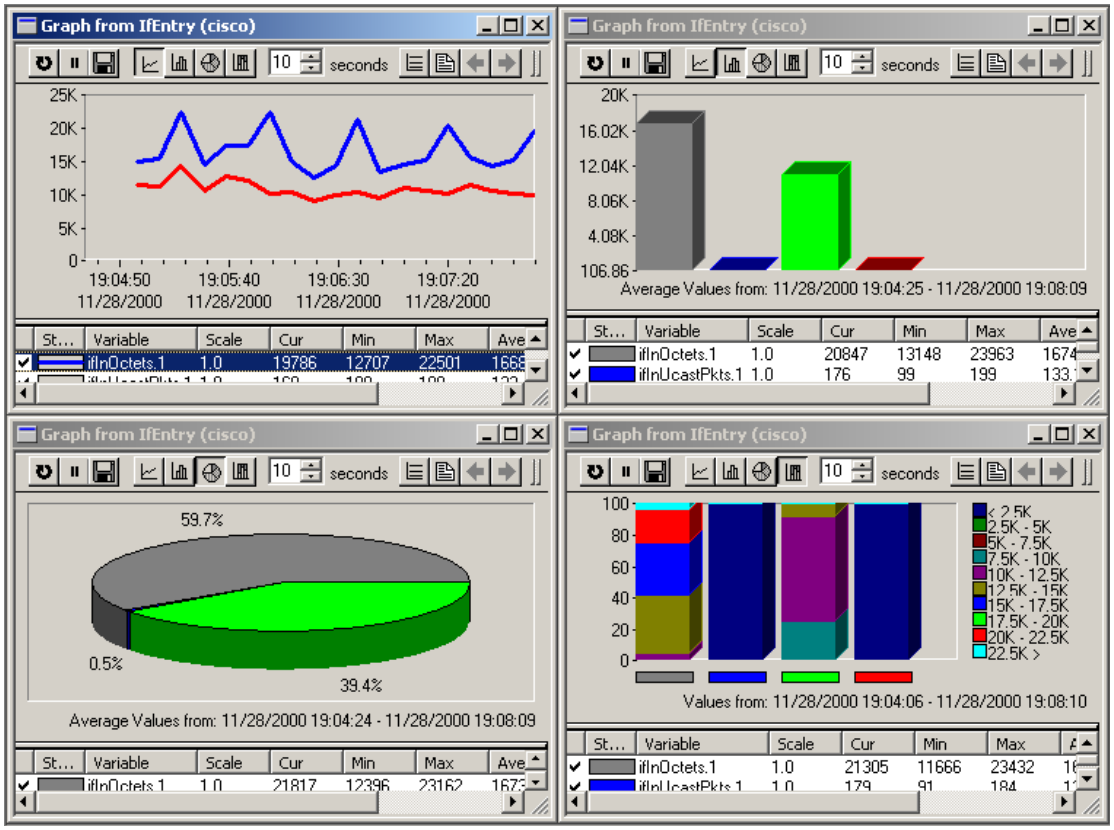
Figura 42. **Botones de gráfica**



3.3.5 Estilo de gráficas

La figura 43 muestra los ejemplos de visualizaciones de los cuatro estilos de gráficos: líneas, barras, distribución y pie, tenga en cuenta que la barra y pie muestran los valores promedio.

Figura 43. **Tipos de gráfica**



3.3.6 Controles de paginación de gráfica

El gráfico dificulta ver con muchas variables al mismo tiempo, se usa Page Controls para habilitar bloques de variable, usa el botón Paginate (iconó de hoja de papel) para habilitar todas las variables o solo la primer página (8 variables), usa los botones Prev Page y Next Page para habilitar la previa o siguiente página de variables.

3.3.7 Gráfico de control de leyenda

El Legend Control muestra todos los nombres de variables y un resumen de datos, incluído el actual, mínimo, máximo, y los valores medios.

• Arrastre la barra en la parte superior de Legend Control, para que el control sea más grande o más pequeño.

• Haga doble clic en el check mark a la izquierda, para activar o desactivar de una variable.

• Utilice el menú del botón derecho en propiedades, para establecer las propiedades de la línea y la ampliación de una variable.

• Haga doble clic en el Graph View para mostrar u ocultar la leyenda de control.

3.3.8 Almacenamiento de estadísticas

SNMPc guarda informes de las estadísticas a largo plazo para cualquier tabla SNMP y también del SNMPc Service Polling pseudo-tables, cada informe guarda los datos de una tabla y hasta diez dispositivos, se puede definir alarmas de umbral manual para cualquier instancia variable para generar un evento cuando una variable alcanza un valor específico, los datos se guardan en una base de datos privada en formato de uno o varios sistemas, de agente de poleo (polling agent system); los datos se pueden descargar y ver en una ventana gráfica regular durante un período de fechas especificado.

Para la versión Enterprise Edition únicamente, SNMPc también exporta datos del informe de forma automática a las impresoras, archivos de texto,

archivos Web HTML, y a una base de datos ODBC, los informes exportados se pueden generar sobre una base cada hora, diaria, semanal y mensualmente.

3.3.9 Para crear un nuevo informe

• Primero se selecciona uno o más dispositivos, usando el Map Selection Tree o una ventana de vista de mapa.

• Localizar el Selection Tool que se encuentra a la izquierda de la consola, si no se puede ver el Selection Tool, usar el menú View/Selection Tool para mostrarlo.

• Seleccionar la pestaña Trend y abrir el nombre de grupo SNMPc Trend Report.

• Usar el menú de Clic Derecho Insert Report para agregar un nuevo reporte.

• Colocar un nombre para el nuevo reporte.

• Seleccionar uno de los nombre de la Mib Table que aparece, se puede también presionar el bontón >> para seleccionar una tabla Mib estándar o privada.

• Para fines de prueba inicial, establecer el intervalo de poleo de 1 minuto, se recomienda utilizar un intervalo de poleo de 10 minutos, si se tiene varios informes.

• Pulsar OK para guardar el informe con la configuración estándar.

Figura 44. **Árbol de selección de reporte**

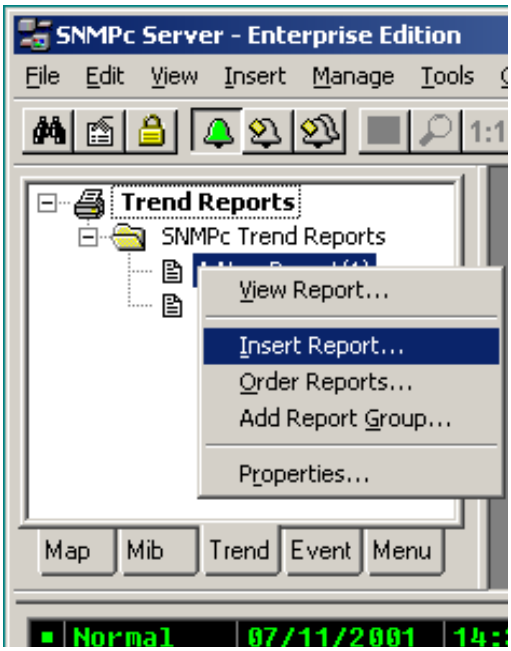
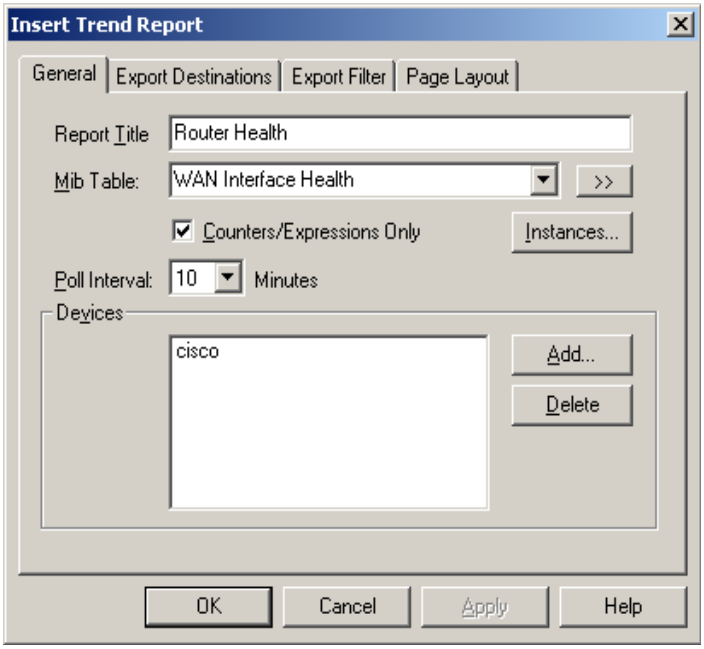


Figura 45. **Cuadro de diálogo para insertar reporte**



3.3.10 Vista de los datos en una ventana gráfica

• Asumiendo que se define un intervalo de poleo de 1 minuto, se espera unos 10 minutos para guardar algunos datos.

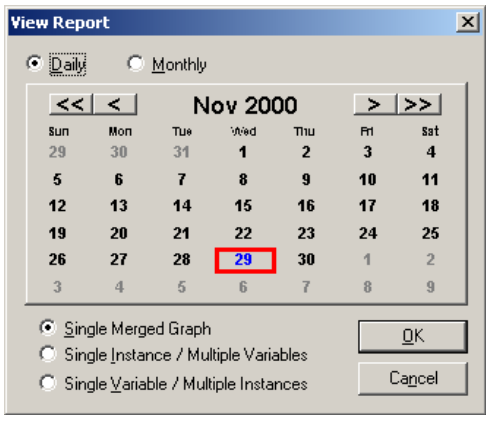
• Con el clic derecho sobre el nombre del nuevo reporte en el Trend Report Selection Tree y usar el menú de propiedades

• Usar el menú View Report

• Seleccionar el día actual y Single Merged Graph para ver todos los datos en un gráfico.

• Pulsar OK, algunos diálogos de progreso se mostrarán a continuación, luego los datos del informe se mostrarán en una ventana normal gráfica SNMPc.

Figura 46. **Selección de reporte**



Independientemente del intervalo de poleo para el informe, todas las variables se muestran en una ventana gráfica donde se normalizan a valores por segundo.

3.3.11 Visualización de datos de tendencias como informes Web

El SNMPc Enterprise Edition, sólo se puede exportar de forma automática, los datos de informe de tendencia a una variedad de objetivos. El objetivo de exportación más común son los archivos de formato HTML que se puede ver de forma remota mediante un navegador WEB.

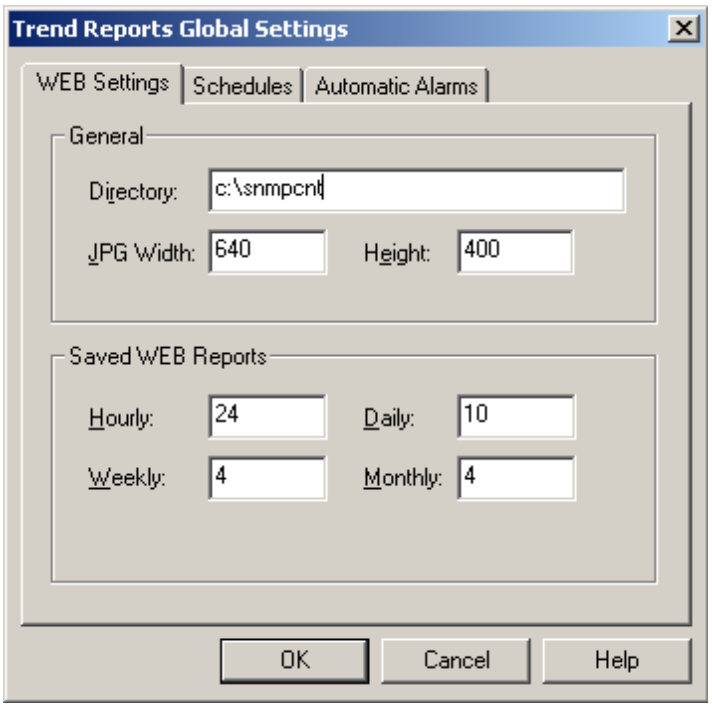
3.3.12 Definiendo el Directorio Web

• Se usa el Menú Config/Trend Reports.

• Seleccionar en el cuadro de edición de Web Directory para colocar el nombre de un directorio al que se podrá acceder tanto por SNMPc y por su servidor Web.

• Los informes SNMPc WEB serán exportados a un subdirectorio denominado TrendReports y el archivo HTML principal, se llama reportGroups.html.

Figura 47. **Selección de directorio Web**



3.3.13 Definiendo la exportación de reporte programado

• Presionar la pestaña Trend en el Selection Tool.

• Con el Clic derecho sobre el nombre y usar el menú de propiedades.

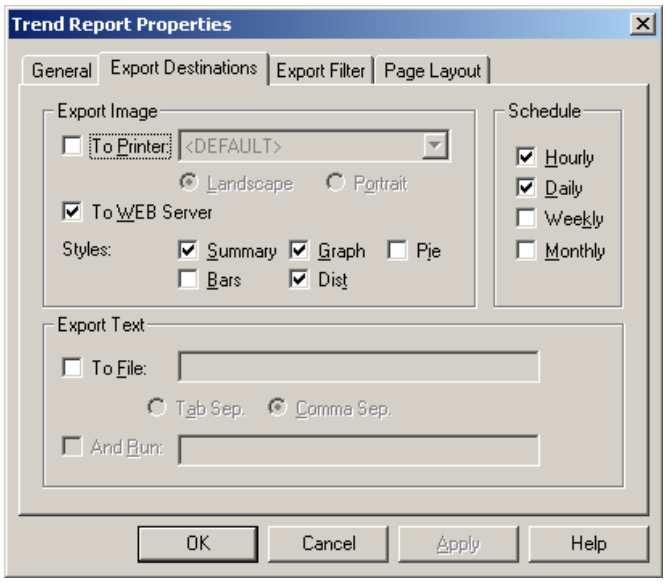
• Seleccionar la pestaña Export Destinations.

• Asegurar tener activa la casilla To Web Server.

• Marcar la casilla programada a cada hora.

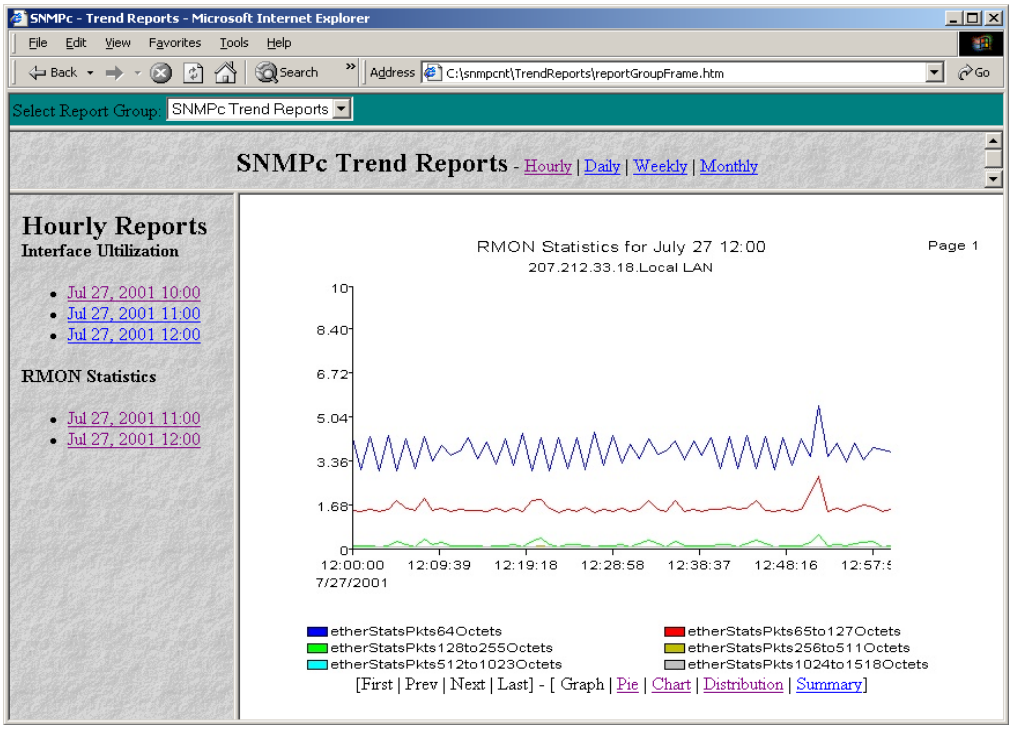
• Presionar OK.

Figura 48. **Configuración de exportación de reporte**



El informe WEB se exportará a la hora con los datos de los valores de la hora anterior, esperamos varias horas y luego utilizamos el menú Tools/Web Reports para ver los informes Web en un navegador WEB, el siguiente es un informe de ejemplo SNMPc WEB de cada hora, se toma en cuenta que las escalas se normalizan a valores por segundo.

Figura 49. **Reporte Web**



3.4 Alarmas

3.4.1 Configuración de las alarmas de umbral

Se puede generar una alarma de umbral cuando el valor de la variable poleada por SNMP alcanza ciertos criterios, SNMPc soporta tres mecanismos distintos para la generación de alarmas de umbral, como se describe en la siguiente tabla.

Tabla XIX. **Descripción de configuraciones de alarma**

TIPO DE ALARMA	DESCRIPCIÓN
Status Variable Polling	Utilice el Object Properties para establecer una única variable SNMP además de instancia que se polee en tiempo real (Poll Interval attribute seconds). Utilizar esto para polear un Estado Critico de un dispositivo. Por ejemplo, poleo para fallo en la batería de UPS, disco completo, o condiciones de Link Down.
Automatic Trend Baseline	SNMPc determina automáticamente un valor de referencia para todas las variables en los informes que se agreguen. La línea de base se fija después de un periodo de monitoreo y es adaptado periódicamente. El agente de poleo generará alarmas si un valor que es poleado excede la línea de base en un porcentaje preestablecido.
Manual Trend Threshold	Use alarmas del umbral manual en los informes de tendencia para especificar una condición particular para poner a prueba. Esto se usa comúnmente para monitorear la utilización de Variables de la línea. En este caso la condición de alarma es bien conocida por el usuario e implica un largo período de poleo (por ejemplo, el 80% más de 10 minutos).

3.4.2 Configuración de estado de poleo variable

• Usando el Map Selection Tree o una Ventana de Vista de Mapa, hacer clic derecho sobre un objeto, dispositivo SNMP, Link o Network y usar el menú de Properties.

• Asegurarse que el campo Address tenga una dirección IP válida. Si se desea, se puede añadir un número de puerto UDP para la dirección como xxxxPort.

• Seleccionar la pestaña Access

• Para un dispositivo SNMP V1, seleccionar SNMP V1 en Read Access Mode y luego seleccionar Read Community para colocar un nombre valido de comunidad.

• Seleccionar la pestaña Attributes.

• Seleccionar en Poll Interval, el número de segundos entre cada poleo.

• Seleccionar Status Variable para colocar el nombre de una variable Integer SNMP incluyendo una instancia (por ejemplo, ifOperStatus.3).

• Seleccionar Status Value para colocar el valor numérico para su comparación. (O seleccionar una de las opciones que se despliegan)

• Seleccionar Status Ok Exp para colocar la expresión que determinará si el estatus pasa la prueba, utilizar los valores que se despliegan (=,<,>, etc)

3.4.3 Configuración de alarmas automáticas

Usar el menú Config/Trend reports y seleccionar la pestaña Automatic Alarms, se puede configurar varios parámetros del algoritmo automático de alarma en este diálogo, generalmente los ajustes por defecto son adecuadas y la principal sería que se desee desactivar alarmas automáticas desmarcando la casilla de verificación Enable Automatic Alarms.

3.4.4 Configuración manual de alarmas de umbral

Primero debe crear un informe de tendencia para un conjunto de dispositivos y una tabla SNMP MIB, esto se vio en una de las secciones anteriores (Almacenamiento de Estadisticas)

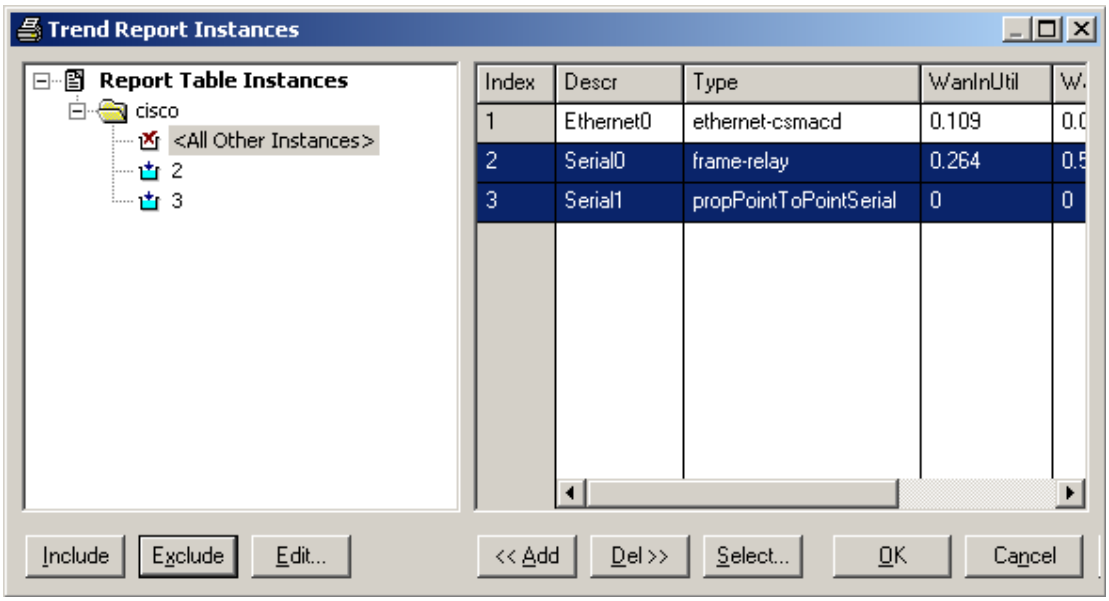
Seleccionar el nombre del reporte en el Trend Selection Tree y usar el menú Properties con clic derecho, entonces usar el botón Instances (Instancias).

• Seleccionar una o más filas de la tabla aparece y pulse el botón Add para agregarlo al Instances Tree a la izquierda.

• En el Instances Tree, seleccionar una o mas etiquetas (incluyendo <All Other Instances>) y presionar el botón Incluye or Exclude.

• Para cada instancia incluída, usar el botón Edit para las alarmas por cada variable.

Figura 50. **Ventana de selección de interfaces para alarma**



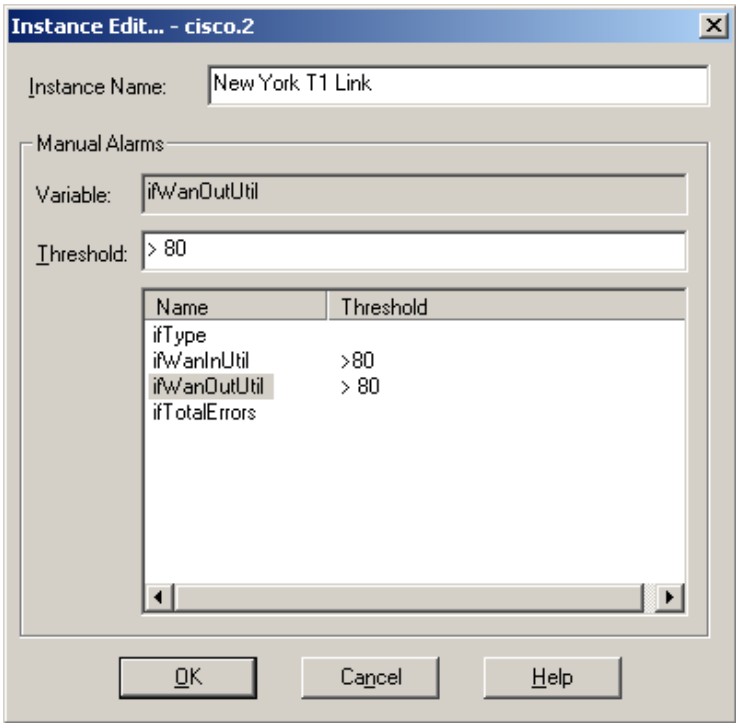
• Seleccionar un nombre de variable de la lista en la parte inferior del cuadro de diálogo Instante Edit.

• Escriba una expresión simple en el cuadro de edición Threshold, este es un operador (>,<,=,>=,<=,!=) y una constante numerica.

• Opcionalmente, también se puede introducir un nombre para esta instancia de variable en el cuadro Instace Name, esto hace que sea más fácil determinar cuál es el umbral de la alarma a que se refiere.

• Pulse Ok, se verá un signo de exclamación de color rojo junto al icono en el Instances Tree, en todas las instancias que tienen alarmas manuales.

Figura 51. **Selección de valor umbral para alarma**

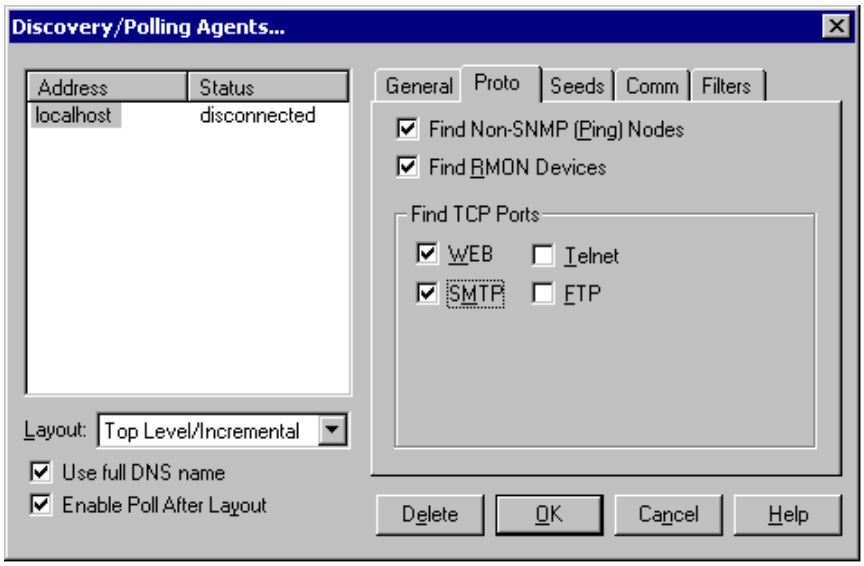


Hay que tener en cuenta que para las variables de Counter, los valores establecidos en el umbral manual se comparan con una muestra de Poll (poleo). La muestra de poleo será mayor o menor dependiendo del intervalo de poleo del informe, por ejemplo, un Link que muestra 100 Kb (Kilobytes) en un minuto puede mostrar 1 000 Kb en 10 minutos, esto es diferente a lo que se ve en el gráfico de tendencia, en el que las muestras están normalizadas a los valores por segundo.

3.4.5 Aplicación de servicios de poleo

SNMPc soporta poleos personalizados de alguna aplicación de servicio TCP, teniendo entre ellos cuatro servicios integrados de aplicación TCP (FTP, SMTP, WEB y TELNET) y un poleador externo de servicios no TCP, en esta sección se describe como polear servicios TCP.

Figura 52. **Configuración de agentes de poleo**

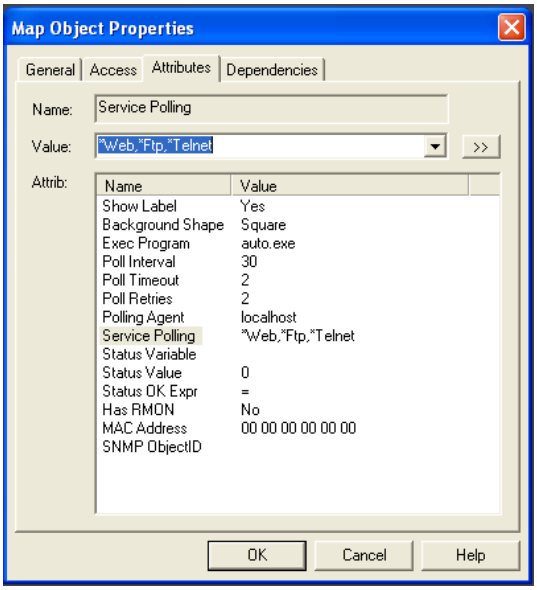


Los agentes de poleo SNMPc pueden automáticamente chequear si existe incorporado un servicio TCP, en los dispositivos descubiertos y configura esos servicios para polear, use la pestaña Proto del cuadro de díalogo Config/Discovery-Polling para habilitar el descubrimiento de los cuatro servicios TCP incorporados.

Para habilitar el servicio de poleo para un dispositivo, haga clic en el dispositivo de objeto en una vista de mapa y se usa el menú Propierties y

después seleccione la pestaña Attributes, seleccionar el atributo para el servicio de poleo.

Figura 53. **Ventana para seleccionar el servicio de poleo**



• Utilice la lista desplegable Value para seleccionar uno de los servicios disponibles (*FTP, *Telnet, * Smtp, * Web y los nombres personalizados).

• Para seleccionar múltiples servicios para el dispositivo, escriba los nombres de servicios en el valor de cuadro de edición, separados por comas. Por ejemplo: * FTP, * Web.

• Como alternativa, haga doble clic en el atributo de Service Polling, o utilizar el botón >>, para seleccionar múltiples servicios.

La definición de servicios personalizados: permite más flexibilidad y potencia de poleo para los servidores de aplicaciones:

• Si se desea, se puede enviar una cadena de texto a un servicio de TCP y comparar la respuesta a un patrón de texto.

• Cada objeto de mapa puede polear hasta 16 diferentes servicios personalizados.

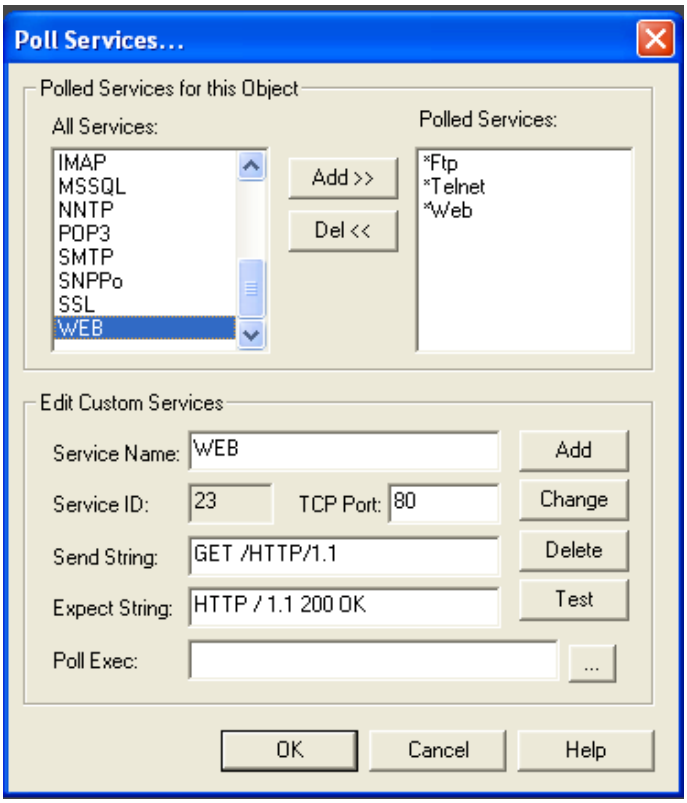
• No hay límite en el número total de definiciones de servicios personalizados que se pueden crear.

• Si se desea, se puede ejecutar una aplicación personalizada externa para el poleo del servicio.

Con doble clic en el atributo de Service Polling, o utilizando el botón >>, se editan las definiciones de servicio.

El cuadro de diálogo de Poll Services se desplegará en la pantalla, use los controles en la parte superior del Polled Services for this Object para gestionar el poleo para el dispositivo seleccionado.

Figura 54. **Ventana para agregar los servicios de poleo**



Para habilitar el poleo de un servicio para el dispositivo:

• Seleccionar el nombre del servicio en la lista All Service.
• Presionar el botón Add>>

Para deshabilitar el poleo de un servicio para el dispositivo:

• Seleccionar el nombre del servicio en la lista Polled Services.
• Presionar el botón Del<<.

Use los controles de la parte inferior Edit Custom Service para agregar, borrar o cambiar las definiciones del servicio personalizado (Custom Service).

Para agregar una nueva definición de servicio personalizado TCP:

• Ingresar un nuevo nombre en el cuadro de edición Service Name.

• Ingresar un número de puerto TCP para un servicio TCP en el cuadro de edición TCP Port.

• Opcionalmente ingrese una cadena corta para transmitir a un servicio TCP en el cuadro de edición Send String.

• Opcionalmente ingrese una cadena patrón para comparar la respuesta del servicio TCP en el cuadro de edición Expect String. Puede usarse texto ASCII y caracteres especiales (‘*’).

• Presionar el botón Add.

Después de agregar una definición de nuevos servicios, se necesita presionar el botón Add>> si se quiere este servicio para ser poleo a el actual dispositivo seleccionado.

Para eliminar una definición de servicio personalizado existente:

• Seleccionar el nombre de servicio en la lista All Services

• Presionar el botón Delete.

Para modificar una definición de servicio personalizado existente:

• Seleccionar el nombre del servicio en la lista All Services

• Hacer cambios en los campos de Service Name, TCP Port, Send String, Expect String, o Poll Exec.

• Presionar el botón Change.

3.4.6 Uso de otros tipos de eventos

Utilizar el evento pollDeviceDown como un ejemplo para esta sección, el mecanismo es el mismo para otros tipos de eventos, incluyendo los generados por Status Variable y Manual Threshold Alarms.

La tabla XX muestra los eventos comunes SNMPc y cuando se producen.

Tabla XX. **Descripción de alarmas de SNMPc**

SUB-ÁRBOL DE EVENTOS	NOMBRE DE TRAP	DESCRIPCIÓN
Snmpc-Status-Polling	pollDeviceDown	El dispositivo no ha respondido a las secuencias de tres poleos consecutivas.
	pollNoResponse	Dispositivo no respondió a una secuencia de poleo
	pollRequestRejected	Dispositivo rechazó la sysObjectId.0 o la variable de poleo de estado establecido por el usuario.
	pollResponse	Dispositivo responde a la secuencia de poleo.
	pollServiceDown	No se pudo conectar al puerto TCP después de tres intentos consecutivos.
	pollServiceNoResponse	No se pudo conectar al puerto TCP después de un intento
	pollServiceResponding	Conexión a puerto TCP establecida
	pollStatusTestFail	Fallo de prueba de variable de estado
	pollStatusTestPass	Prueba de variable de estado exitosa
Snmpc-System-Info	pollAgentConnect	Conexión del Agente de Poleo SNMPc a el servidor establecida
	pollAgentDisconnect	Perdida de Conexión del Agente de Poleo SNMPc a el servidor
Snmpc-Threshold-Alarm	alarmAutoThresholdExpand	Trend auto-baseline elevado
	alarmAutoThresholdReduce	Trend auto-baseline moved dismunuido.
	alarmAutoThresholdSet	Trend auto-baseline inicialmente establecido.
	alarmAutoThresholdTrigger	Trend auto-baseline excedido,
	alarmManualThresholdTrigger	Tendencia de alarma manual pasa el umbral
	alarmManualThresholdReset	Luego de dispararse, la alarma manual no pasa la prueba de umbral
snmp-Traps	authenticationFailure	Trap generado por un dispositivo por medio de un acceso illegal (nombre de comunidad inválido)
	coldStart	Trap generado por un dispositivo luego de reiniciarse
	linkDown	Trap generado por un dispositivo cuando el Link falla
	linkUp	Trap generado por un dispositivo cuando el Link que estaba down se restablece

4. EJEMPLO DE UNA RED WIMAX GESTIONADA

4.1 Topología de Red

4.1.1 Estación base y CPE

La estación base WiMAX es uno de los elementos más críticos para una solución con red WiMAX, hay diferentes tipos de estaciones bases disponibles en el mercado, están diseñados para soportar tanto WiMAX fijo como Wimax móvil, con más funciones avanzadas para mejorar la capacidad y rendimiento tal como soporte del Adaptive Antenna System, diversidad de múltiples canales para Transmisor/Receptor, así también soporte de Space Division Multiple Access, GPS Clock Synchronization, Turbo Coding, etc; diferentes estaciones base están también diseñadas para diferentes aplicaciones de Macro cell, Micro cell y Pico cell.

Por el lado del usuario, muchas CPEs exterior e interior se desarrollan para construir la comunicación con la estación base, además del rendimiento, la comodidad, la fiabilidad y la seguridad son también las cuestiones clave que deben tenerse en cuenta al diseñar el CPE, muchas de las CPEs en el mercado ofrecen tanto WiMAX como WiFi, hay CPEs de modo dual que soportan tanto IEEE802.16-2004 y 2005-IEEE802.16e.

Los CPEs WiMAX para voz son más requeridos por los mercados emergentes, donde el servicio de voz es la mayor demanda, los CPEs WiMAX de datos tiene el principal mercado en el los países desarrollados donde el servicio de banda ancha móvil es la mayor demanda. En las siguientes figuras se muestran dos de las topologías que puede tener una red WiMAX.

Figura 55. **Arquitectura Macro cell**

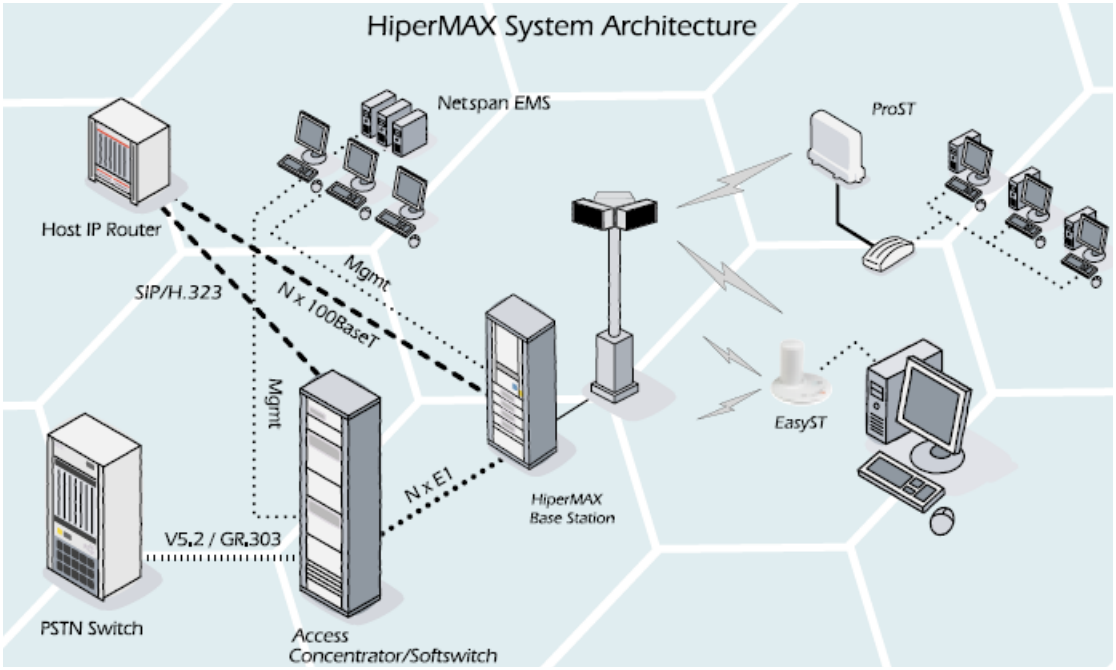
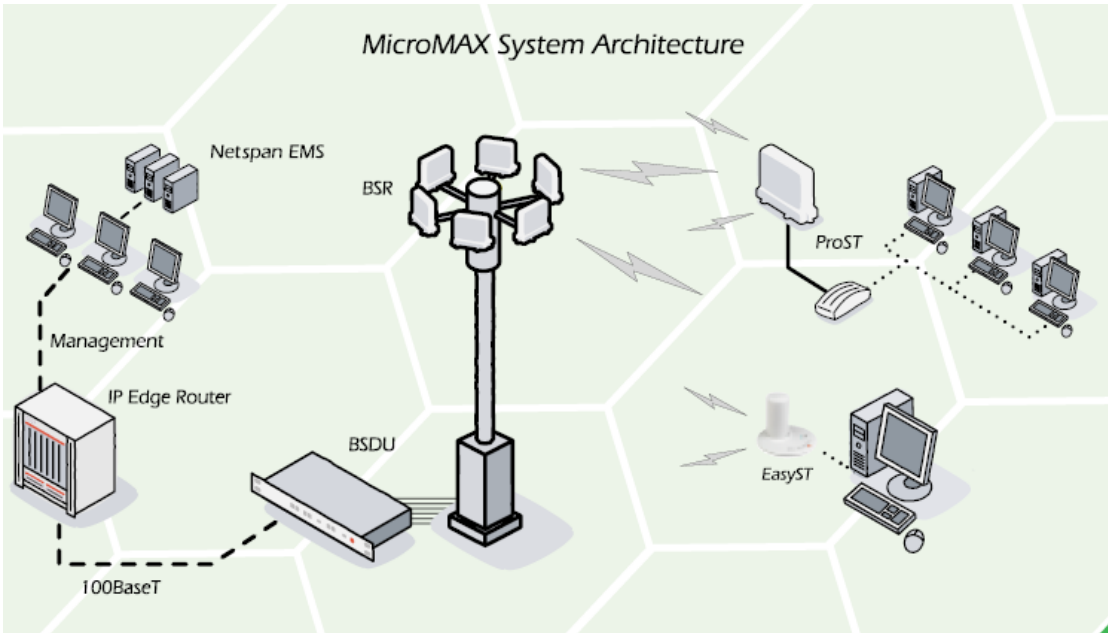


Figura 56. **Arquitectura Micro cell**



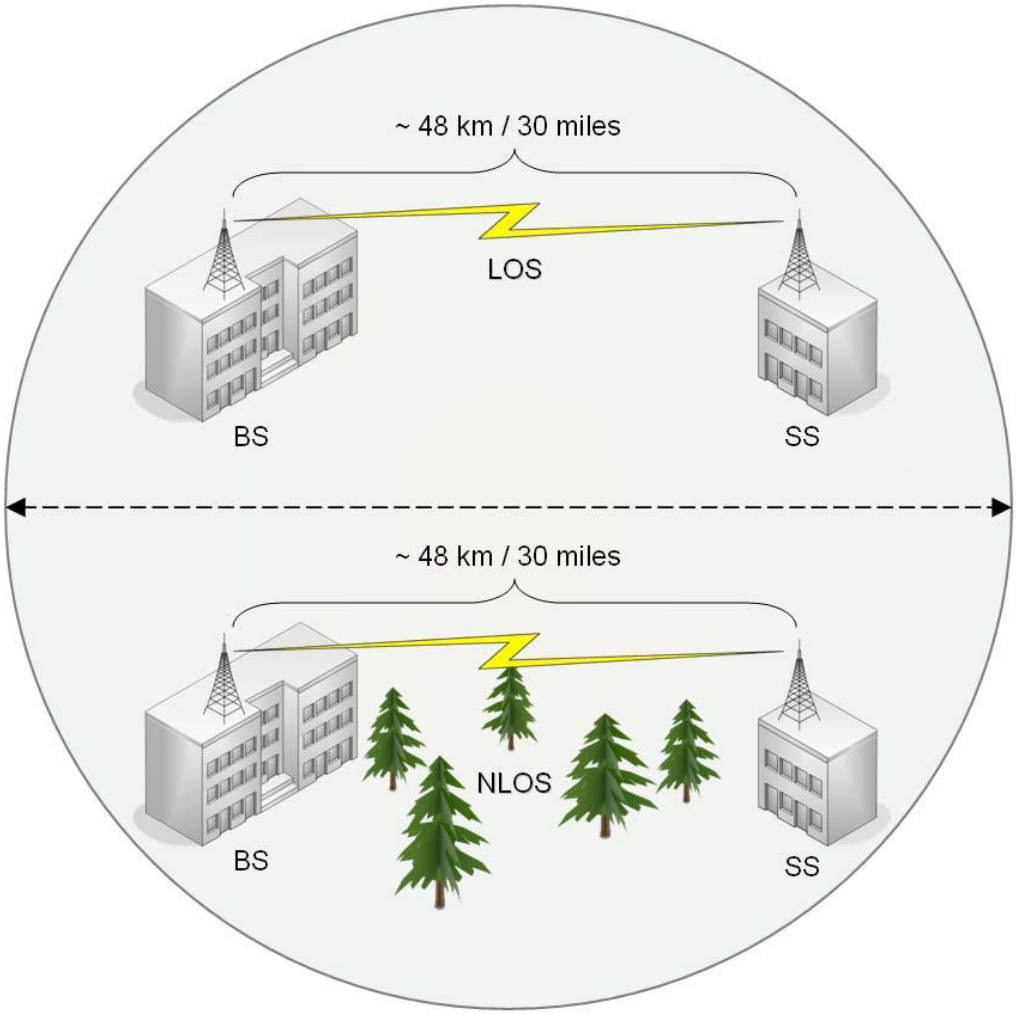
4.1.2 Topologías de operación

Hay cuatro principales topologías de WiMAX: punto a punto, punto a multipunto, multi-hop relay (es decir, la creación de redes de malla), y móviles, cada uno de estos se describen brevemente a continuación.

4.1.2.1 Punto a punto (P2P)

Una topología punto a punto (P2P) se compone de una dedicada conexión wireless a larga distancia y de alta capacidad entre dos sitios, por lo general, el sitio principal o central tiene la BS (Base Station) y el sitio remoto la SS (Suscribe Station) como se muestra en la siguiente figura, la BS controla los parámetros de comunicación y seguridad para establecer el enlace con la SS. La topología P2P es utilizada para un servicio inalámbrico de mayor ancho de banda a una distancia máxima de operación aproximadamente de 48 km utilizando señal de propagación LOS o NLOS (Non-line-of-sight) sin línea vista.

Figura 57. **Topología punto a punto**

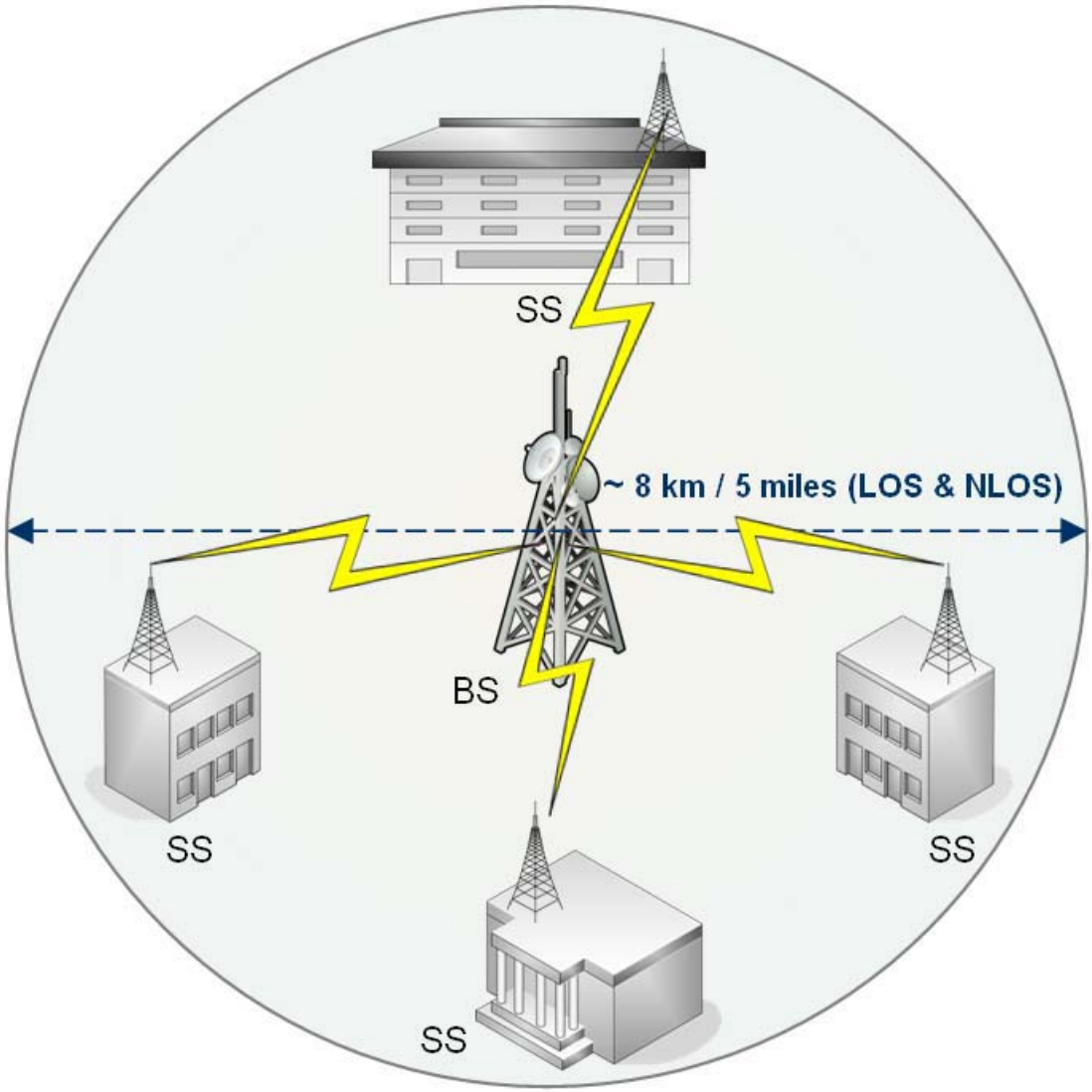


4.1.2.2 Punto a multipunto (PMP)

Una topología punto a multipunto está compuesta de una BS central soportando multiples SSs, proporcionando acceso a la red de un lugar a muchos, es comúnmente usado para el acceso de banda ancha de última milla, conectividad de la empresa privada para oficinas remotas, servicios inalámbricos de largo alcance para varios sitios, las redes PMP pueden operar usando

propagación de señal LOS o NLOS, cada BS tiene un rango de operación típico de 8 km, la siguiente figura muestra la topología PMP.

Figura 58. **Topología multipunto**

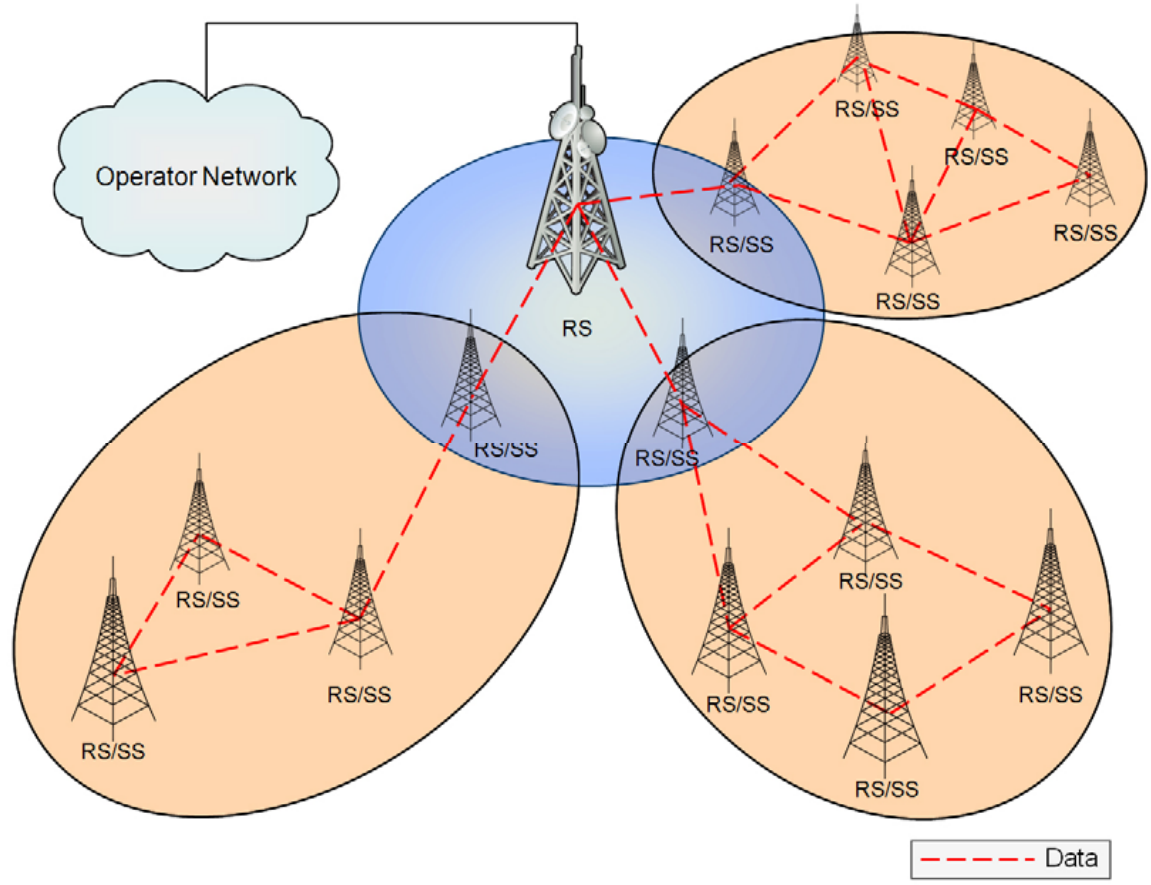


4.1.2.3 Multi-Hop Relay

Una topología multi-hop relay es definida por la IEEE 802.16j-2009 para extender el área de cobertura de las BS's, permitiendo SSs/MSs para transmitir el tráfico, actuando como RSs (Repeater Station), los datos destinados a un SS / MS fuera del rango de la BS se retransmite a través de las RSs adyacentes. Una RS sólo puede reenviar el tráfico a RSs / SSs dentro de su zona de seguridad, una zona de seguridad es un conjunto de relaciones de confianza entre un BS y un grupo de RSS.

Los datos que se originan fuera de un área de cobertura de BS se envían por RSs múltiples, aumentando en la red el área total de cobertura geográfica, como se ve en la figura siguiente. La Topología Multi-hop relay normalmente utiliza la propagación de señal NLOS porque su objetivo es abarcar grandes áreas geográficas que contienen múltiples obstáculos RF, sin embargo, técnicamente puede funcionar con la propagación LOS, el rango de operación máxima para cada nodo en una topología de multi-hop relay es de aproximadamente 8 km (5 millas).

Figura 59. **Topología Multi-Hop Relay**

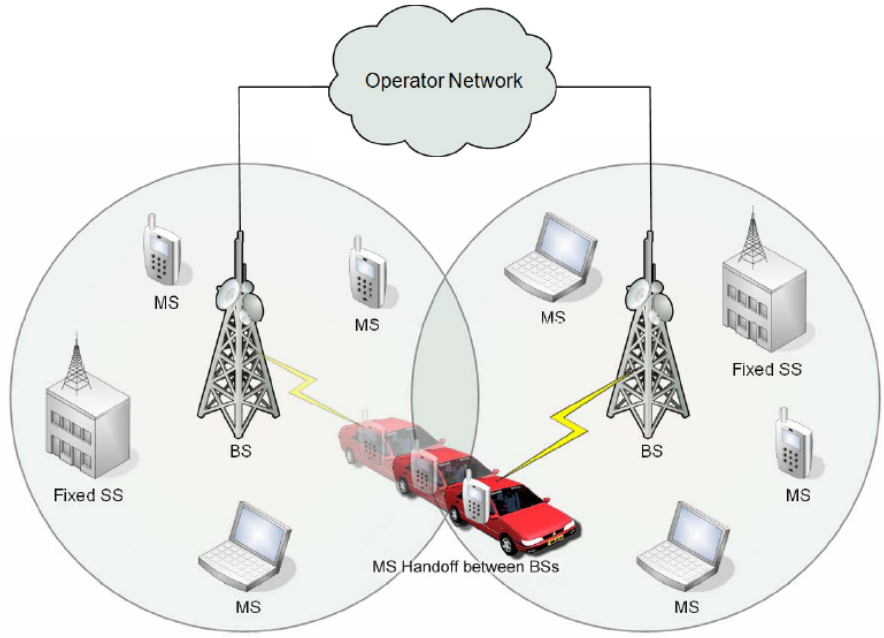


4.1.2.4 Móvil

Una topología móvil es similar a una red celular porque esta formada por múltiples BSs que colaboran para prestar servicios de comunicaciones integradas en una red distribuida tanto a SSs como a MSs. Esta topología combina el área de cobertura de cada miembro de BS e incluye medidas para facilitar transferencias de los MSs (Handoffs) entre áreas de cobertura de cada BS, como es mostrado por el vehículo (MS) en la figura siguiente, se utiliza una avanzada tecnología de señalización de RF para soportar el aumento de la complejidad RF necesario para las operaciones móviles. Cada área de

cobertura BS es de aproximadamente 8 km (5 millas), WiMAX móvil funciona con la propagación de señal NLOS en frecuencias que oscilan entre 2 y 6 GHz.

Figura 60. **Topología móvil**



4.2 Costos de adquisición y recuperación en el tiempo

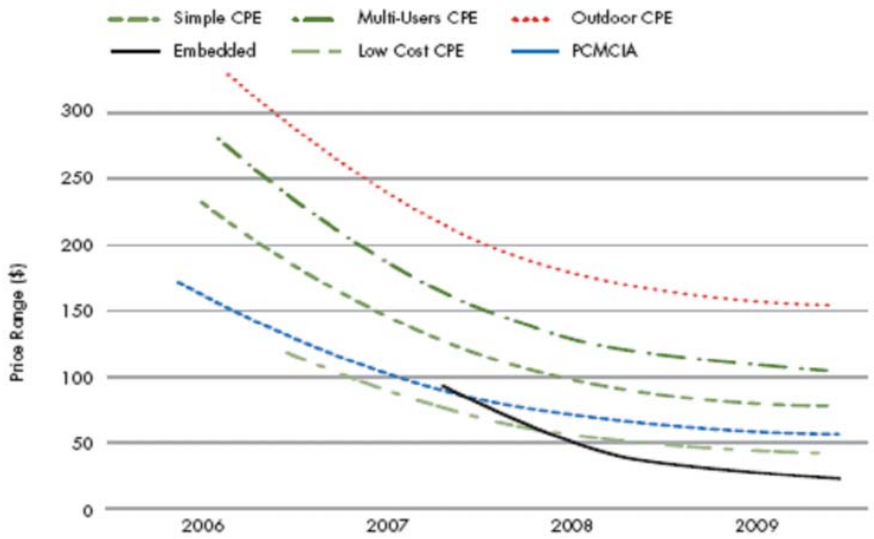
El crecimiento de Internet ha dado lugar a una reducción de los costos de acceso así como una reducción de los costos de transmisión de información sobre la red, tal como sucede con otras tecnologías inalámbricas, hay una ventaja económica al emplear Wi-MAX para ofrecer servicios inalámbricos fijos en localidades donde los despliegues de redes cableadas aún no han tenido lugar o donde hay poca competencia, es atractiva.

Al considerar ciertos aspectos, es probable que Wi-MAX tenga una estructura de menor costo y alto rendimiento respecto de la porción de red que se encuentra detrás de las estaciones base, ya que Wi-MAX utiliza específicamente el protocolo IP, lo que significa que es escalable y por tanto, puede soportar un mayor nivel de tráfico de usuarios para una cantidad dada de recursos de la red, la cual debe ser aprovechada en beneficio de mejorar las condiciones de acceso a los servicios de telecomunicaciones a bajo precio, permitiendo que más personas puedan hacerlo.

Al eliminar la necesidad de utilizar cobre o fibra, un operador puede reducir significativamente sus gastos de capital iniciales mientras que, a la vez, reduce el riesgo de que haya problemas con el servicio. Una vez que los consumidores puedan instalar por sí mismos el CPE, los costos se tornan incluso más convincentes.

El efecto combinado de altos gastos de capital y el costo de CPE representan el mayor desafío para Wi-MAX cuando intente establecerse como otra opción de oferta de datos inalámbricos. Como se puede ver en la Figura 4.1, el costo de los diferentes tipos de CPEs disminuye conforme transcurre el tiempo, es así que después de algunos años estos costos estarán al alcance de un mayor número de clientes.

Figura 61. **Gráfica de precio respecto al año**



4.2.1 Costos de implementación una red wimax con equipos AS.MAX de Airspan

A continuación, la Tabla XXI muestra los costos referenciales que tendría la implementación de los radioenlaces, utilizando equipos AS.MAX de Airspan según los precios proporcionados por los proveedores en US$.

Tabla XXI. **Precios estimados para implementación de WiMAX con Airspan**

COMPONENTE	VALOR UNITARIO ($)	CANTIDAD	VALOR TOTAL ($)
Estación Base			
Estación Base HiperMAX FDD 3.5GHz 3 sectores	62 836,71	1	62 836,71
Equipos de Usuario (CPEs)			
ProST 3.5GHz FDD Outdoor	558,32	9	5 024,88
SDA-1 Tipo 2 – US (Para ProST)	33,00	9	297,00
EasyST 3.5GHz FDD	455,40	58	26 413,20
Sistema de Administración de la Red			
Licencia AS8200 NMS RTU plus para 100 CPE	6 201,25	1	6 201,25
Licencia AS8200 para extensión de red 100 CPE	1 136,25	1	1 136,25
Repuestos	14 864,14	1	14 864,14
Servicios			
Instalación y comisionamiento Radiobase-Gestión	2 043,52	1	2 043,52
Instalación y comisionamiento de CPE Outdoor	88,72	9	798,48
Instalación y comisionamiento de CPE In/Outdoor	52,65	58	3.053,70
Capacitación (2 Semanas) – Equipamiento	18 339,20	1	18 339,20

SUBTOTAL:	141 008,33
12% IVA:	16 920,99
TOTAL:	157 929,32

4.2.2 Costos de implementación una red WiMAX con equipos BreezeMAX DE ALVARION

Para esta línea de productos se pudo obtener mayor información con respecto a los costos de los equipos, ya que existen varios proveedores de Alvarion. A continuación se muestra en la Tabla XXII los costos referenciales.

Tabla XXII. **Precios estimados para la implementación Wimax con Alvarion**

COMPONENTE	VALOR UNITARIO ($)	CANTIDAD	VALOR TOTAL ($)
Estación Base			
Estación Base BreezeMAX FDD 3 sectores	63 348,00	1	63 348,00
Equipos de Usuario (CPEs)			
BreezeMAX PRO 3.5GHz FDD Outdoor	602,14	9	5 419,26
BreezeMAX Si 3.5GHz FDD Indoor/Outdoor	522,53	58	30 306,74
Sistema de Administración de la Red			
Licencia para los elementos de red de 1 Estación Base y 30 CPEs	2 926,00	1	2 926,00
Licencia para los elementos de red de 100 CPEs	4 389,00	1	4 389,00
Repuestos	15 123,52	1	15 123,52
Servicios			
Instalación y comisionamiento Radiobase-Gestión	3 750,00	1	3 750,00
Instalación y comisionamiento de CPE Outdoor	85,00	9	765,00
Instalación y comisionamiento de CPE In/Outdoor	50,00	58	2 900,00
Capacitación (2 Semanas) – Equipamiento	18 500,00	1	18 500,00
SUBTOTAL:			147 427,52
12% IVA:			17 691,30
TOTAL:			165 118,82

En ambos casos, el costo por instalación, mantenimiento y repuestos del sistema de transmisión está incluído dentro del costo total de la implementación de los radioenlaces.

En la Tabla XXIII se realiza una comparación entre las opciones de equipos Wi-MAX, de acuerdo con la estimación de costos realizada.

Tabla XXIII. **Comparación de precios entre las diferentes marcas**

	AIRSPAN ($)	**ALVARION ($)**
Estación Base	62 836,71	63 348,00
Equipos de Usuario (CPEs)	31 735,08	35 726,00
Sistema de Administración de la Red	22 201,64	22 438,52
Servicios	24 234,90	25 915,00
SUBTOTAL:	141 008,33	147 427,52
12% IVA:	16 920,99	17 691,30
TOTAL:	157 929,32	165 118,82

Una vez realizada la estimación de costos de los equipos y considerando las mejores características técnicas, se puede decir que la mejor opción para la implementación del sistema de transmisión Wi-MAX sería utilizando equipos AS.MAX de Airspan, ya que su implementación resulta más económica y se tiene un mejor presupuesto del enlace.

4.2.3 Costos de operación y mantenimiento

Los costos de operación y mantenimiento son muy importantes a considerar, ya que serán los que se pagarán mensualmente durante todo el tiempo de vida del nuevo sistema de transmisión Wi-MAX,

Si se considera que la vida útil de los equipos es de 10 años, entonces se destinará el 10% del valor total, el cual será invertido anualmente en repuestos y mantenimiento como se muestra en la Tabla XXIV.

Tabla XXIV. **Estimación de costo de mantenimiento de red**

Descripción	Valor total $	Valor anual $
Mantenimiento y Repuestos de Equipos Wi-MAX	14 864,14	1 486,41

4.2.4 Costos de ingeniería

Los costos de ingeniería son muy importantes a considerar, ya que corresponden a los honorarios que la empresa tendrá que cancelar a la persona encargada del estudio de campo de la zona y diseño del sistema de transmisión Wi-MAX. En la Tabla XXV se presentan los costos de los servicios de ingeniería en la cual se incluye los siguientes aspectos.

- El estudio de campo y verificación de infraestructura se evalúa de acuerdo a la factibilidad de acceso a la localidad, medición de la situación geográfica y condiciones climáticas de la zona, en este caso, se considera un costo de $50 por población.

- El costo del diseño incluye: estudio de la situación actual, estimación de demanda, mapas y perfiles topográficos, esquemas de la red, selección de equipos y demás aspectos a considerar en el diseño.

Tabla XXV. **Estimación de costos de ingeniería**

DESCRIPCIÓN	VALOR UNITARIO ($)	CANTIDAD	VALOR TOTAL ($)
Estudio de Campo (Por poblaciones)	50,00	16	800,00
Diseño del Sistema de Transmisión Wi-MAX	10 000,00	1	10 000,00
TOTAL:			10 800,00

4.2.5 Recuperación de la inversión

Tarifas y planes de comercialización del sistema de transmisión Wi-MAX

Con respecto a las tarifas que el usuario final deberá pagar para acceder al servicio de Internet banda ancha utilizando tecnología Wi-MAX, se tomarán como referencia las tarifas y planes de comercialización del mercado actual.

4.2.5.1 Plan con Factor de Sobresuscripción 1:1

Este tipo de plan ofrece al usuario final todo el ancho de banda contratado, el cual estará disponible todo el tiempo. La Tabla XXVI muestra las tarifas de acuerdo a la velocidad requerida.

Tabla XXVI. **Estimación de tarifas por servicio con factor 1:1**

PLAN	128 Kbps	256 Kbps	512 Kbps	1 000 Kbps
Precio a la venta ($)	40,00	78,00	151,00	286,00
Derecho de Inscripción ($)	200,00	200,00	200,00	200,00
TOTAL ($):	***240,00***	***278,00***	***351,00***	***486,00***

4.2.5.2 Plan con Factor de Sobresuscripción 8:1

A diferencia del plan anterior, el ancho de banda contratado por el usuario final será compartido, razón por la cual, el derecho de inscripción y de las tarifas considerando las mismas velocidades de transmisión, también disminuyen como se muestra en la tabla XXVII.

Tabla XXVII. **Estimación de tarifas por servicio con factor 8:1**

PLAN	128 Kbps	256 Kbps	512 Kbps	1 000 Kbps
Precio a la venta ($)	26,00	52,00	103,00	199,00
Derecho de Inscripción ($)	100,00	100,00	100,00	100,00
TOTAL ($):	***126,00***	***152,00***	***203,00***	***299,00***

Como se puede ver en las tablas anteriores, las tarifas determinadas para estos tipos de planes, constituyen un referente más atractivo desde el punto de vista económico, al tratarse de una zona en donde la demanda de Internet no es muy alta, se considera un plan con factor de sobresuscripción de 8:1, tomándolos con una velocidad de transmisión promedio de 256 Kbps entre todos los suscriptores podemos tener la siguiente estimación de ingresos. (Estimamos unos 60 clientes en el sector)

Derecho de Inscripción (Instalación):

$$60 \text{ usuarios} * \frac{\$100}{\text{usuario}} = \$\ 6\,000{,}00$$

Internet (Beneficio Anual):

$$60 \text{ usuarios} * \frac{\$52}{\text{mes} * \text{usuario}} * 12 \text{ meses} = \$\ 37\,440{,}00$$

A continuación se muestra una tabla en la cual se detalla el tiempo de recuperación del costo de la implementación de un Sistema Wimax.

Tabla XXVIII. **Tabla de costos y recuperación en tiempo**

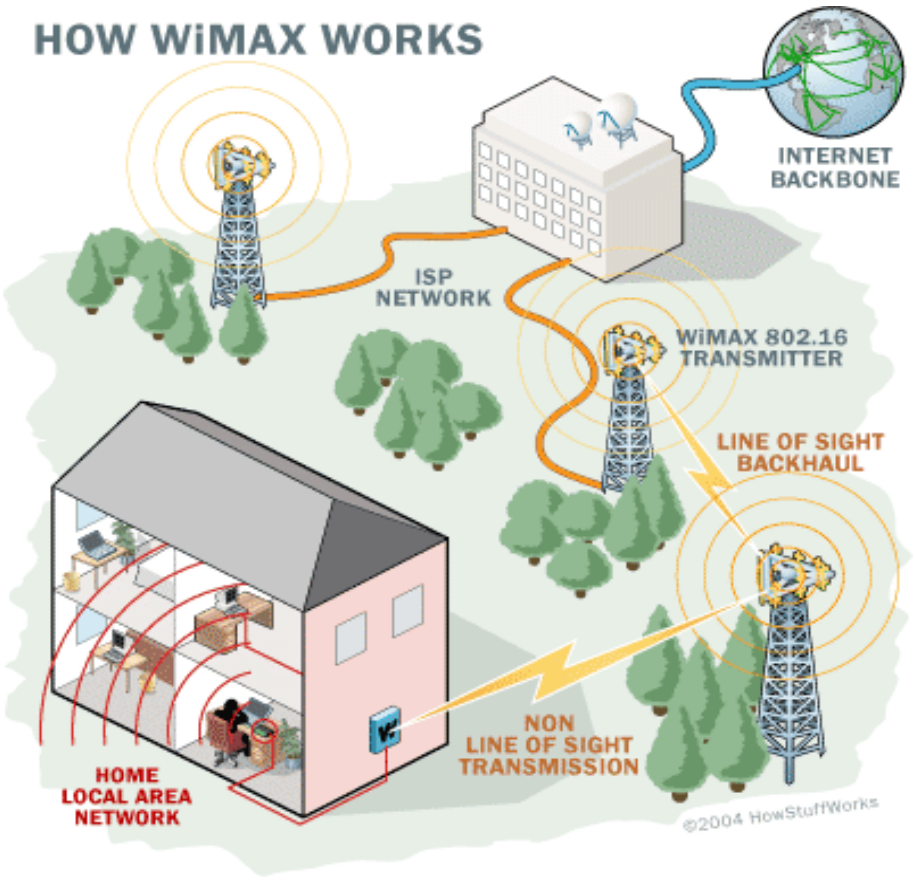
Descripción	Año 0 $	Año 1 $	Año 2 $	Año 3 $	Año 4 $	Año 5 $	Año 6 $	Año 7 $	Año 8 $	Año 9 $	Año 10 $
	BENEFICIOS										
Instalación	6 000,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Internet	0,00	37 440,00	37 440,00	37 440,00	37 440,00	37 440,00	37 440,00	37 440,00	37 440,00	37 440,00	37 440,00
Total	6,000.00	37 440,00	37 440,00	37 440,00	37 440,00	37 440,00	37 440,00	37 440,00	37 440,00	37 440,00	37 440,00
	COSTOS										
Costos Equipos AS.MAX	157 929,32	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Costos de Ingeniería	10 800,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Mantenimiento y Repuestos	1 486,41	1 486,41	1 486,41	1 486,41	1 486,41	1 486,41	1 486,41	1 486,41	1 486,41	1 486,41	1 486,41
Total	170 215,73	1 486,41	1 486,41	1 486,41	1 486,41	1 486,41	1 486,41	1 486,41	1 486,41	1 486,41	1 486,41
Balance de Ingresos	**-164 215,73**	**35 913,59**	**35 913,59**	**35 913,59**	**35 913,59**	**35 913,59**	**35 913,59**	**35 913,59**	**35 913,59**	**35 913,59**	**35 913,59**

Con esta estimación se puede observar que la inversión realizada es recuperable en el transcurso del tiempo a mediano plazo.

4.3 Ventajas de la red

Combinando la tecnología WiMAX con la plataforma de Gestión SNMPc , se podrá crear una red inalámbrica con una eficiencia y fiabilidad mayor, en la cual podremos administrar remotamente cada uno de los dispositivos que la componen a través de una interfaz gráfica, con muchas funcionalidades. Desde un router central, pasando por la BS y la SS, hasta dispositivos de la LAN del cliente final (tales como routers, switches y PCs) podrán ser monitoreados.

Figura 62. **Ejemplo de una red WiMAX gestionada**



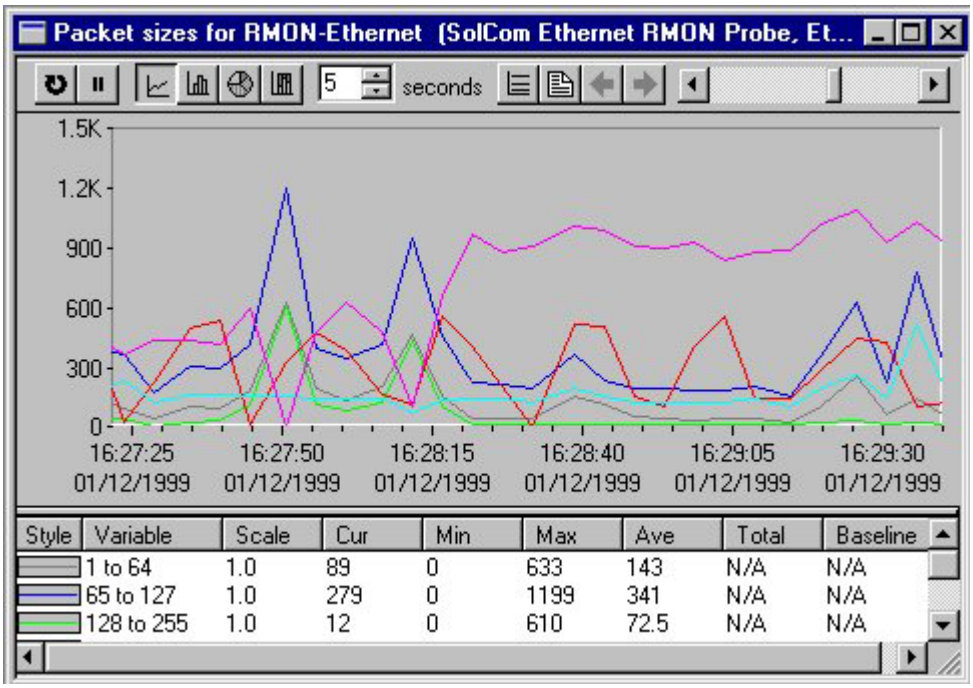
Esto permitirá tener una red extensa en la cual, al momento de surgir alguna falla se pueda localizar en el menor tiempo posible, identificando las razones, y resolviéndolas en el mejor de los casos remotamente. Esto se traducirá en una rápida respuesta de resolución ante un inconveniente y un menor costo de operaciones ya que se determinará el punto del problema, evitando que personal se desplace a diferentes localidades haciendo pruebas para encontrar la falla.

Se podrá tener a la vista todas las SSs (Subscriber Station) que cuelgan de una BS (Base Station) y realizar pruebas de conectividad tales como: pérdidas de paquetes y latencia a través del protocolo telnet.

Figura 63. **Servicio Telnet por medio de la gestión**

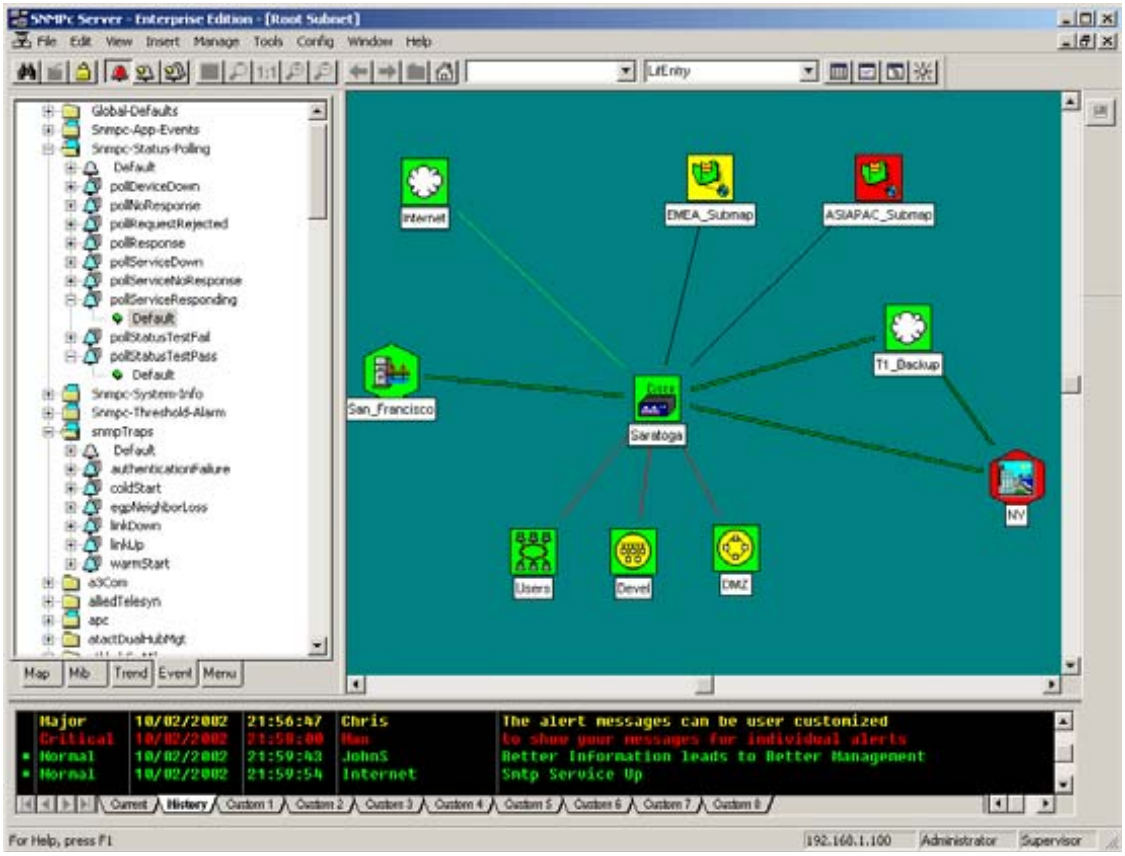
Otra de las ventajas que brinda esta composición de red es que se puede realizar un monitoreo del ancho de banda consumido, por un cliente a través de una interface, este consumo se desplegará en una gráfica. A través de esta función se puede verificar si alguno de los subscriptores esta llegando a límite de ancho de banda que tiene designado.

Figura 64. **Gráfica de consumo de un servicio**



En el mapa del SNMPc se muestra cada uno de los dispositivos, los de color verde son los que tienen una conectividad sin problemas, y los rojos son lo que se encuentran fuera de servicio.

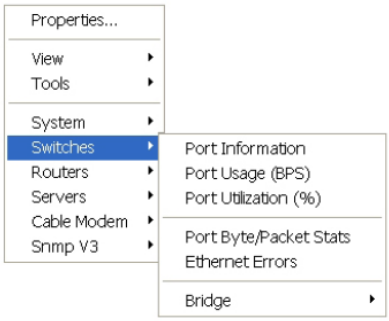
Figura 65. **Red gestionada desde consola de SNMPc**

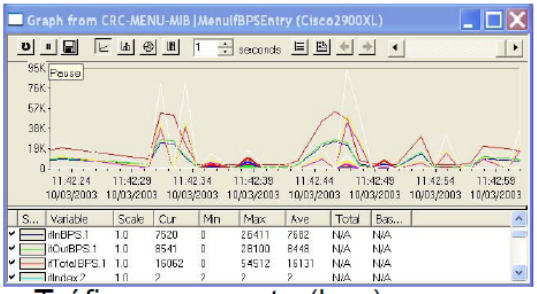


Con esta interfaz se estará recibiendo alarmas visuales y sonoras de todos los eventos que se presenten en nuestra red, con esto se podrá hacer una revisión remota del punto para encontrar la posible falla y proceder a la reparación de la misma.

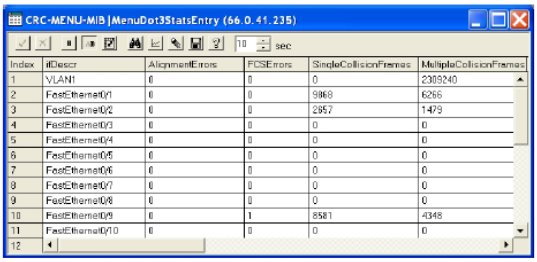
Otra de las ventajas que se tendrá en esta red por medio de la plataforma SNMPc, sería los diferentes menús de dispositivos específicos, como lo son Switches, routers y Server. Las siguientes figuras muestran los diferentes menús:

Figura 66. **Menú para switches**



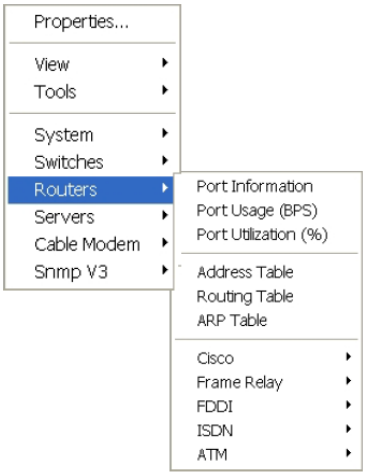


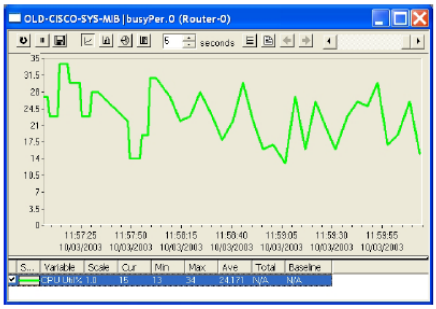
Tráfico por puerto (bps)



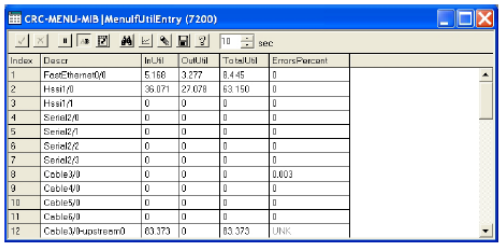
Errores por Puerto

Figura 67. **Menú para routers**



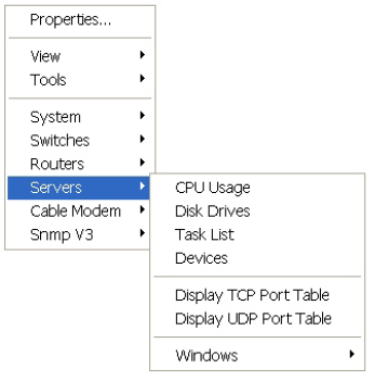


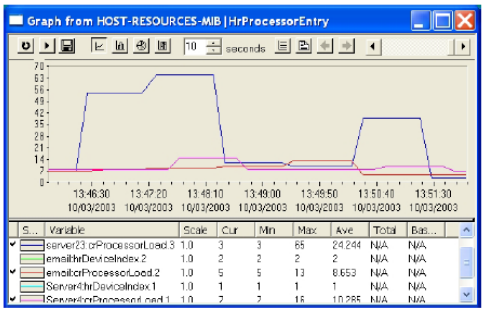
Utilización de CPU de routers Cisco



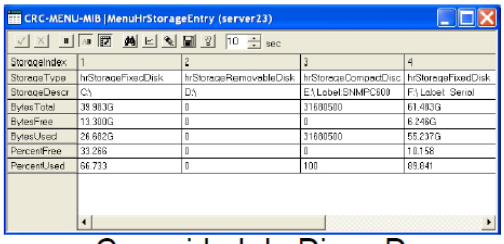
Utilización de puertos (%)

Figura 68. **Menú de server**





Utilización de CPU (Múltiples Servers)



Capacidad de Disco Duro

Esto permitirá un monitoreo integral de la red y de esta forma aprovechar al máximo toda su capacidad, y al mismo tiempo poder responder inmediatamente a cualquier eventualidad que surja en cualquiera de los dispositivos que conforman la red.

CONCLUSIONES

1- Con este estudio se puede concluir que para la implementación de una red inalámbrica confiable y eficiente es necesario contar con las herramientas necesarias que permita una facilidad en el intercambio de información entre el administrador y los dispositivos de red para la supervisión del buen funcionamiento de la red.

2- Las herramientas de gestión proporcionan la información necesaria para que al momento de existir alguna falla en alguno de los componentes de la red, se pueda proceder de manera más rápida a un diagnóstico y resolución del problema. Con ello disminuyen los costos de operación y el tiempo de afectación en los servicios.

3- El uso de la tecnología WiMAX basada en OFDM y OFDMA es la mejor opción en cuanto a ancho de banda, alcance, capacidad de usuarios, optimización del espectro y costos, ya que permite alcanzar hasta 50 km, velocidades de hasta 70Mbps, operación en ambientes con LOS y NLOS, la utilización de diferentes perfiles de transmisión para cada usuario de acuerdo con sus necesidades, QoS diferenciado, privacidad, seguridad y flexibilidad en anchos de canal, además de otras características.

4- La plataforma SNMPc es una herramienta que permite visualizar la topología de la red, unificando todos los elementos de la red en una sola pantalla. Permitiendo con ello monitorear los parámetros de cada uno de estos y accionar proactivamente ante algún evento que pueda afectar la red.

RECOMENDACIONES

1- Tener en cuenta que la tecnología Wimax con la plataforma SNMPc se complementan para tener el desempeño deseado de la red, por lo que se debe verificar desde la topología de red a utilizar según las condiciones de campo que se tengan hasta como configurar los parámetros necesarios del gestor, para que éste utilice óptimamente sus recursos en la red que se estará monitoreando.

2- Se debe tener siempre a la mano los procedimientos a seguir según el evento que se presente en la plataforma de gestión, y de esta forma realizar prontamente las correcciones y reparaciones necesarias para normalizar el funcionamiento de la red o de una parte de ella.

3- Cuando se selecciona equipos para la implementación de una red, se debe prestar atención a lo que realmente ofrecen los fabricantes, ya que algunos equipos no cumplen con el estándar IEEE 802.16-2004 y solamente son soluciones propietarias pre-WiMAX, las mismas que no garantizan interoperabilidad con otros fabricantes.

4- Es importante antes de adquirir equipos, realizar una prueba con éstos para comprobar su alcance y capacidad real, pues las características que los fabricantes ponen a disposición del cliente son para condiciones ideales que no corresponden a la realidad, por lo que en la mayoría de casos el desempeño real de un equipo es significativamente menor al ofrecido.

BIBLIOGRAFÍA

1. Vicente, Carlos. Gestión de Traps SNMP, Servicios de Red, Universidad de Oregon. 2008

2. Castle Rock Computing, Evaluation Guide for SNMPc V7.0. 2009

3. Castle Rock Computing, Getting Started, SNMPc V7.1. 2009

4. Cisco Networking Academy. Aspectos básicos de networking, CCNA Exploration, 2007

5. Smith, Clint y Gervelis, Curt. **Wireless Network Perfomance Handbook**, Estados Unidos: McGraw-Hill, 2003

6. Sosa Sosa, Víctor J. SNMP, 2008

7. Gao, Feng. A Technical and Market study for WiMAX. Thesis of Master of Science in Technology, Faculty of Electronics, Communication and Automation, Helsinki University of Technology, 2009

8. Navarro Lucas, Joaquín. Redes Inalámbricas: Wimax, Ampliación de Redes, Ingeniería Informática, 2005

9. Scarfone, Karen. Tibbs, Cyrus y Sexton, Matthew. **Guide to Security for WiMAX Technologies**, National Institute of Standards and Technology Gaithersburg, United States, 2009

10. Utard, Marcelo y Ronco, Pablo. Redes de Datos, Facultad de Ingeniería, Universidad de Buenos Aires, 2007

11. http://tecnologia-wimax.blogspot.com/ consultado en mayo de 2010

12. http://www.snmptt.org consultado en mayo de 2010

13. http://es.kioskea.net/contents/internet/snmp.php3 consultado en junio de 2010

14. http://www.castlerock.com/products/snmpc/default.php consultado en mayo de 2010

15. http://www.snmpc.ca/ consultado en mayo de 2010

16. http://vdvnetworks.homestead.com/files/SNMPc_v6_PresentACI_N_2.0.pdf consultado en junio de 2010