albentia Systems

WHITE PAPER

White Paper

Bridging vs Routing en redes inalámbricas PtmP

Mayo 2010
Rev A1

La mayoría de fabricantes de equipamiento inalámbrico de banda ancha únicamente incorporan la posibilidad de configurar sus equipos en modo de "Bridge transparente", debido a las ventajas y facilidades que ofrece este modo en cuanto a configuración. Sin embargo, en entornos de acceso Punto a Multipunto (PtmP) con un gran número de usuarios conectados, esta práctica puede no ser la más óptima debido a que un Bridge de nivel 2 retransmite a toda la red el tráfico broadcast generado por todos los usuarios así como el tráfico que el propio Bridge genera para aprender la topología de la red. Esto es algo a tener muy en cuenta en un medio tan escaso como el radio.

Este documento pretende aclarar las implicaciones que tiene configurar en Modo Bridging cualquier sistema inalámbrico de banda ancha en escenarios de muchos usuarios, y presenta las alternativas de networking que ofrecen los equipos de Albentia Systems, como el Routing o el modo Local-Network. Se comenzará repasando algunos conceptos de red básicos para luego extrapolarlos a las redes inalámbricas y en concreto a aquellas basadas en el estándar IEEE 802.16-2009 (WiMAX).

INTRODUCCIÓN: CONCEPTOS BÁSICOS DE NETWORKING

Definición de *Bridging*

Cuando las redes Ethernet empezaron a utilizarse de forma masiva, añadiendo cada vez más *hosts* y transmitiendo mayor cantidad de datos, surgió la necesidad de incorporar dispositivos de red que solucionasen los problemas de colisiones que presentaban los *hubs*: aparecieron los *bridges/switches.*

Un ***bridge*** es un dispositivo que conecta dos o más segmentos de red a nivel Ethernet (capa 2 OSI, nivel de enlace) conforme al estándar *IEEE 802.1D*. Encamina las tramas en función de la dirección MAC destino, independientemente de los protocolos de nivel superior utilizados.

⇒ **Autoaprendizaje**

Los bridges realizan un proceso de autoaprendizaje de las direcciones MAC en cada segmento de la red y las almacenan en una tabla interna (**tabla de reenvío**), siguiendo la siguiente secuencia (ver Figura 1):

*(1) **PC_A** (00:1F:4A:00:00:51) manda una trama con destino **PC_C** (00:1F:4A:00:00:52).*
(2) El Bridge recibe la trama y lee la MAC origen. Como no está registrada en su tabla de reenvío, la añade junto con la interfaz correspondiente (ETH1).
*(3) LA MAC destino tampoco aparece en la tabla, con lo que el Bridge no sabe hacia qué interfaz encaminar la trama, y reenvía el paquete por todos los puertos para que llegue también a **PC_C**.*
*(4) **PC_C** la recibe, y responde con otra trama a **PC_A***
(5) La MAC origen de esta trama tampoco está registrada en la tabla del Bridge, así que la añade junto con la interfaz de donde viene (ETH3).
*(6) LA MAC destino (**PC_A**) está en la tabla desde (2), así que el bridge sólo manda el paquete por ETH1.*

Para retransmitir una trama un *bridge* busca en su tabla de reenvío la MAC destino y así puede sacarla sólo por la interfaz correcta (a diferencia de los *hubs*). Se puede afirmar por tanto que el *Bridge* genera un tráfico multicast "·de aprendizaje", además de retransmitir por todas sus interfaces el tráfico *broadcast y multicast*.

El aprendizaje es automático, con lo que los Bridges son muy sencillos de configurar.

Los *Bridges* realizan una interconexión de redes de forma inteligente, con una gran ventaja: segmentan los Dominios de Colisión, provocando la existencia de un dominio por cada interfaz. Simplificando, se podría decir que los *Bridges* proporcionan mejoras de tráfico y mayor aislamiento entre segmentos de LAN que los *hubs* y son más fáciles de configurar y manejar que los *routers*, pero no dan el alto grado de aislamiento de tráfico entre LAN de estos últimos.

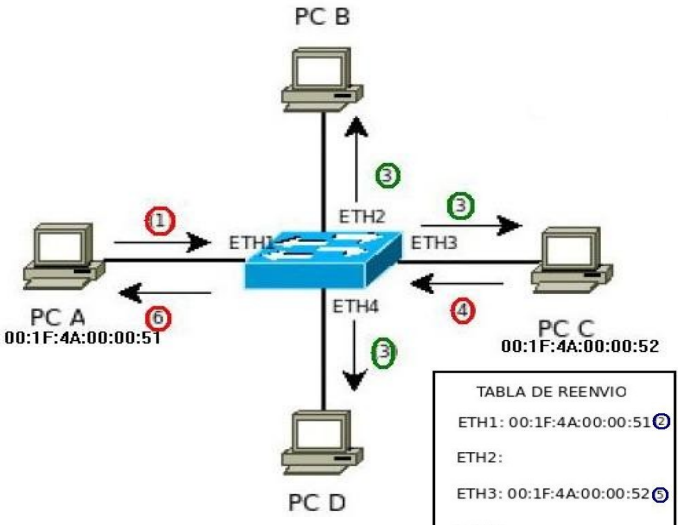

Figura 1 - *Learning Bridge*

⇒ **Diferencias entre *Bridge* y *Switch***

Ambos son dispositivos de nivel 2 con funcionalidades similares, aunque se diferencian comúnmente en que los *bridges* interconectan segmentos remotos de redes LAN (de forma cableada o inalámbrica), mientras que el *switch* es normalmente usado para conectar varios hosts dentro de una LAN, o redes LAN adyacentes. Así mismo la conmutación de paquetes en *switches* se realiza por HW, mientras que en *bridges* suele ser por SW. De todas formas en muchos contextos estos dos conceptos se intercambian o se usan indistintamente.

Definición de *Routing*

Los ***routers*** son dispositivos de interconexión de redes que operan en la capa 3 OSI (nivel de red). Su función principal es encaminar paquetes entre distintas redes. Los *routers* son los equipos que conforman la red a nivel general, interconectando a nivel lógico las diferentes redes físicas, y gracias a ellos los datagramas IP pueden fluir desde cualquier parte de la red hasta cualquier otro lugar.

Para llevar a cabo su función, los *routers* disponen de una **tabla de rutado** en la que almacenan las rutas para llegar al resto de nodos de la red, junto con otra información útil para el encaminamiento. Estas tablas pueden estar configuradas de forma estática o pueden ser mantenidas de forma automática mediante protocolos de encaminamiento (i.e. RIP, OSPF,...), que permiten a los *routers* intercambiar información con otros nodos de la red para decidir las rutas.

Al recibir un paquete, el *router* lee la cabecera del paquete IP y determina, mediante la dirección IP destino, si está dirigido a una red a la que el *router* tiene acceso de forma local. En este caso, envía el paquete a la dirección MAC correspondiente. En caso contrario, busca en su tabla de rutado una entrada con la red de destino del datagrama, y reenvía el paquete por la interfaz apropiada. Si no existe ninguna entrada con la red de destino indicada en el paquete, utiliza una entrada especial de la tabla de rutas, en donde se guarda la ruta por defecto (*Default Gateway*).

Además de su función de encaminar, los *routers* son en general dispositivos más "inteligentes" que *bridges* o *switches* y pueden llevar a cabo otras operaciones, como el filtrado de paquetes, la fragmentación, la asignación de direcciones IP (NAT, DHCP,…), etc...

Al igual que los *bridges*, los *routers* segmentan los dominios de Colisión. Sin embargo, existe una diferencia con respecto a estos, y es que los *routers*, por defecto, no reenvían los paquetes de ***broadcast***, o lo que es lo mismo, segmentan también los dominios de Difusión. Esto es importante, pues impide que todos los dispositivos de la red escuchen los mensajes de difusión del resto, reduciendo el tráfico total en la red.

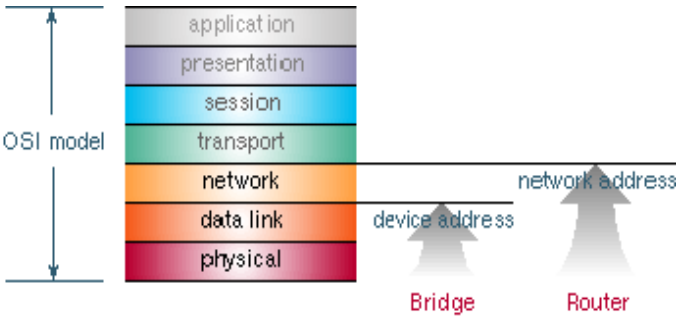

Figura 2 - Ámbito de aplicación de *Bridges* y *Routers*

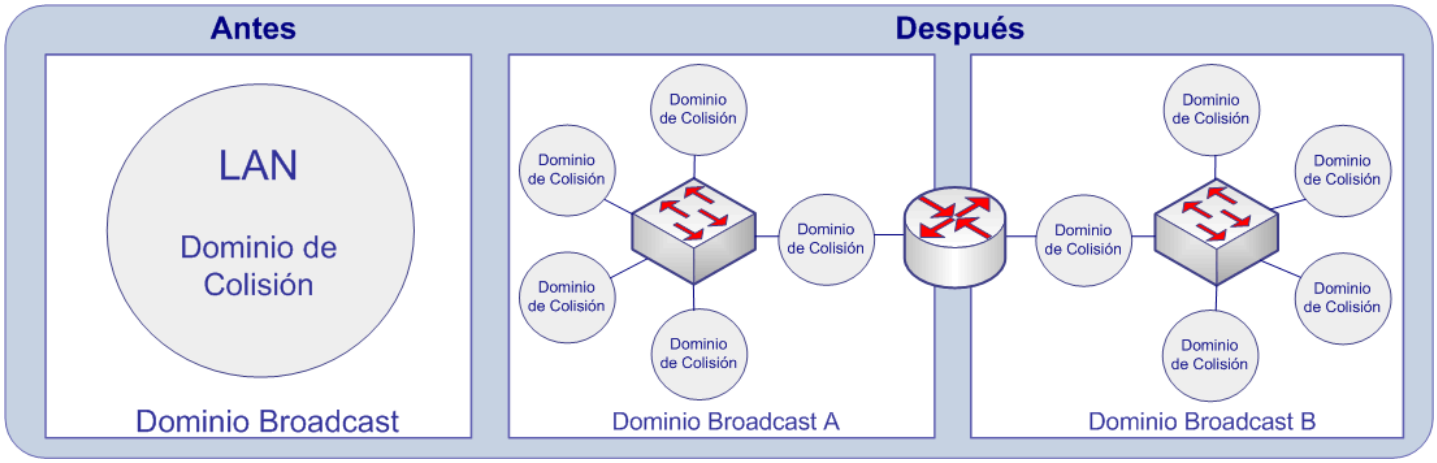

Figura 3 - Dominios de Colisión y Difusión con *Bridges* y *Routers*

Bridge

- Funciona hasta capa 2 (nivel de enlace)
- Conecta segmentos de una red local
- Encamina tramas en base a direcciones MAC
- Tabla de reenvío: MAC/interfaz
- Auto-aprendizaje de MACs por cada segmento (mediante tráfico *broadcast*)
- Muy fácil y simple de configurar
- Segmentan los Dominios de Colisión

Router

- Funciona hasta capa 3 (nivel de red)
- Conecta distintas redes
- Encamina paquetes en base a direcciones IP
- Tabla de rutas (estática ó dinámica)
- Segmenta los Dominios de Colisión y los Dominios de Difusión
- Aísla el tráfico de la red, cortando el tráfico *broadcast, multicast, y "de aprendizaje"*

TRÁFICO BROADCAST/MULTICAST

Definición

El tráfico de *broadcast* es un componente natural de las redes TCP/IP, y consiste en la comunicación de un terminal origen con TODOS los terminales de un dominio de Difusión (red, subred o VLAN).

Un **paquete *broadcast*** de nivel 3 (capa de red) a todos los hosts es un paquete cuya dirección IP de destino es la **255.255.255.255**. Un paquete de *broadcast* a una subred específica (*broadcast* directo) tiene como dirección destino la dirección *broadcast* de esa subred (i.e. **X.X.X.255**).

Los paquetes de *broadcast* se encapsulan a nivel de capa de enlace en **tramas *broadcast***, aquellas con dirección MAC destino **FF:FF:FF:FF:FF:FF**. Cuando un *bridge* o un *switch* recibe una trama con una dirección *broadcast* de destino, transmite esa trama por todos los puertos, salvo por el que recibió la trama.

El ***multicast***, en cambio, es un caso particular de tráfico *broadcast*, en el que multidifusión utiliza un rango especial de direcciones (clase D, desde la 224.0.0.0 a la 239.255.255.255) que no identifican nodos sino un grupo de nodos (grupo *multicast*).

Origen del tráfico

Las tres fuentes típicas de *broadcast* y *multicast* en las redes IP son los dispositivos de red, los propios hosts, y las aplicaciones *multicast*:

- **Dispositivos de red**: como se ha comentado previamente, dispositivos de red como *switches* o *bridges* utilizan tramas de *broadcast* y *multicast* a nivel de Capa 2 para comunicarse con todos los dominios de Colisión cuando tienen que retransmitir un paquete a un host desconocido. Así mismo, retransmiten todo el tráfico de *broadcast* que reciben a todo su dominio de Difusión.
- **Aplicaciones multicast**: el *multicast IP* es una forma eficiente de enviar un flujo de datos a muchos usuarios, aunque consume mucho ancho de banda. Por ejemplo, un *streaming* de vídeo en tiempo real en modo *multicast* puede generar un flujo de datos superior a 2 Mbps que en una red conmutada se enviarían a cada segmento, pudiendo causar congestión.
- **Nodos de la red**: los propios hosts de la red generan tráfico de *broadcast*. Existen múltiples protocolos que corren en estos equipos que necesitan para sus procesos generar tráfico de *broadcast*. A continuación se citan ejemplos de este tipo de protocolos.

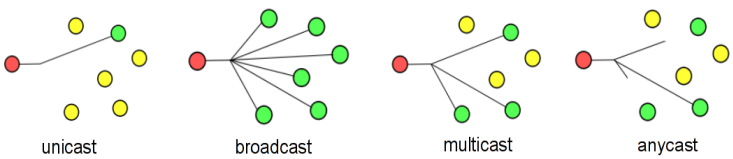

Figura 4 - *Esquemas de rutado*

⇒ **ARP** (*Address Resolution Protocol*)
Es un protocolo de nivel de red empleado por los hosts para conocer las direcciones MAC de equipos con determinada dirección IP. Esta información es almacenada en la caché interna de cada host, dentro de una tabla ARP. Esta tabla puede incluir entradas dinámicas (aquellas que se añaden y se borran automáticamente a lo largo del tiempo, con un tiempo de vida máximo), y entradas estáticas (que permanecen en la caché hasta que se reinicia el equipo).

El protocolo funciona de la siguiente forma:

- ***A** dispone de un datagrama IP para enviar a **B**.*
- ***A** consulta su tabla de encaminamiento. Conoce la IP de **B** pero necesita también la dirección MAC.*
- ***A** envía una solicitud de ARP "ARP Request" a la dirección MAC de broadcast. Cuando llega a **B**, ésta aprende la asociación entre dirección MAC y dirección IP de **A**, y responde a **A** con su dirección MAC en un mensaje de respuesta ARP "ARP Reply". Cuando recibe este mensaje, **A** lo añade a su tabla.*
- ***A** ya puede enviar la trama Ethernet a **B**.*

Por lo tanto, todo host envía en *broadcast* una petición ARP cada vez que necesita ubicar una dirección MAC que no encuentra en su tabla ARP (generalmente porque la entrada era dinámica y ya ha expirado).

A medida que aumenta el número de hosts en una subred, las tablas ARP de cada uno son más grandes y tienen más entradas, con lo que según crece el número de hosts aumenta exponencialmente el tráfico ARP de *broadcast* que circula por la red.

⇒ **NetBIOS** (*Network Basic Input/Output Sytem*)
Es un protocolo que funciona a nivel de capa de aplicación y es exclusivo de redes *Windows*. Se utiliza para asignar nombres y *workgroups* a las *workstations* y sirve fundamentalmente para compartir archivos e impresoras y para ver los recursos disponibles en redes Windows.

⇒ **Protocolos de enrutamiento** (RIP, OSPF, IGRP,…)
Los hosts y *routers* de una red pueden usar estos protocolos como mecanismos de redundancia y alcance, pero esto puede aumentar el tráfico de *broadcast* de modo significativo. Cada 30 segundos, el RIPv1 utiliza *broadcast* para retransmitir toda la tabla de enrutamiento a otros *routers* RIP. Si 200 equipos se configuraran para ejecutar RIP y, supongamos que como media se requieren 50 paquetes para transmitir la tabla de enrutamiento, las estaciones de trabajo generarían 333 *broadcast* por segundo. Es por esto que la mayoría de los administradores de red sólo configuran RIP en un número pequeño de sus *routers*.

⇒ **DHCP** (*Dynamic Host Configuration Protocol)*

Es un protocolo de nivel de red empleado para que los *hosts* puedan configurar automáticamente parámetros como dirección IP, puerta de enlace, máscara de red, servidor DNS... Un servidor DHCP tendrá una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres.

El proceso comienza con el envío por parte del cliente de un paquete DHCPDISCOVER para encontrar servidores DHCP activos. Posteriormente el servidor responde con un DHCPOFFER ofertando parámetros de configuración, y el cliente acepta o rechaza la oferta con un DHCPREQUEST. Finalmente hay un mensaje DHCPACK de confirmación y cierre desde el servidor hacia el cliente indicando los parámetros definitivos. Todos estos mensajes son enviados a la dirección de destino *broadcast*. El host al que va dirigido el DHCPOFFER recogerá la información, y al resto de hosts los paquetes sí llegarán pero serán descartados.

⇒ **DNS** (*Domain Name System*)

Es el protocolo encargado de la resolución de nombres (traducción de nombres a direcciones IP). El método de resolución empleado en una red es el *broadcasting* salvo que se haya configurado otro. Este método resuelve los nombres de forma correcta pero genera una cantidad de tráfico elevada en la red. Existe también el MDNS (*Multicast DNS*), una implementación del protocolo de resolución de nombres (DNS) para redes de área local, donde no existe un servidor DNS real, y que como su nombre indica, genera tráfico multicast.

⇒ **Otros**

Infinidad de protocolos utilizan al menos ocasionalmente paquetes *broadcast*. LLC (*Logical Link control*), IGMP (*Internet Group Management Protocol*), etc. Incluso aplicaciones de más alto nivel pueden hacerlo. Por ejemplo, un conocido antivirus emite cada 30 segundos paquetes broadcast en el puerto UDP 6646 para ver si existen otros PCs en la red con este programa instalado, y así compartir estadísticas.

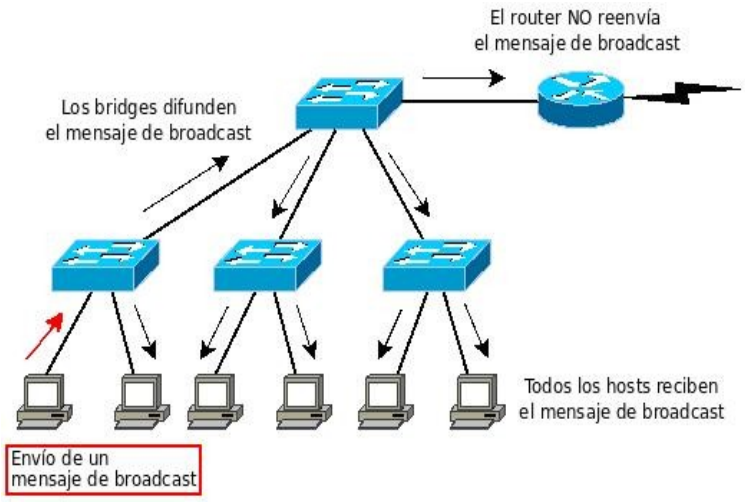

Figura 5 - *Funcionamiento con Bridges y Routers*

El problema

El tráfico de *broadcast* es un elemento fundamental para muchos protocolos. Puede ser despreciable o puede llegar a saturar el medio, con lo que conviene controlarlo. La generación de tráfico de *broadcast* y *multicast* por cada host de la red se denomina radiación de *broadcast*. Los problemas principales que supone esta radiación son:

- **Inunda la red con tráfico innecesario**: se reduce la capacidad utilizable del medio con una especie de "tráfico de fondo". El caso más extremo, en el que esta radiación llega a saturar el medio y afecta a toda la red, se denomina tormenta de *broadcast* o tormenta de difusión.
- **Afecta al rendimiento de cada host**: consume recursos (CPU y NIC) de hosts y servidores, que deben procesar el tráfico *broadcast* que reciben a pesar de que muchas veces lo descarten (por no ser los destinatarios reales).
- **Vulnerabilidades**: el tráfico de *broadcast* puede ser utilizado para realizar ataques de negación de servicio y de inundación de tráfico a la red: DOS (*Denial of Service), Fraggle, Smurf, IP Flooding, ...*

Adicionalmente, problemas de configuración (como bucles) o fallos en los dispositivos pueden provocar la presencia de cantidades muy importantes de *broadcast* que limitan la operación regular de la red, bajando de modo notable su rendimiento.

El tráfico de *broadcast* aumenta proporcionalmente a medida que aumenta el tamaño de la red y el número de hosts, y es especialmente sensible en medios en donde la capacidad total es limitada, como ocurre especialmente en cualquier tecnología inalámbrica.

Soluciones

El recurso más directo para limitar el impacto negativo del tráfico de *broadcast* es limitar el tamaño de los dominios de *broadcast* (el conjunto de nodos que reciben un paquete de *broadcast*). Para esto, las herramientas tradicionales son:

- Dividir la red en subredes.
- Al implementar *switching* a Nivel 2 se puede limitar la difusión de broadcast segmentando la red en VLANs.
- Utilizar dispositivos de Nivel 3 como *routers* para que segmenten los Dominios de Difusión. Esto también lo pueden hacer algunos *switches* con inteligencia adicional, coloquialmente llamados "*brouters*".
- Utilizar *switches* que implementen STP (*Spanning Tree Protocol*) para evitar tormentas de difusión por bucles.
- Existen *routers*, *firewalls*,... que pueden detectar y prevenir tormentas de difusión, involuntarias o malintencionadas.
- Algunos *switches* implementan un "*Broadcast Storm Control*", mecanismo mediante el cual no superan un cierto umbral de tráfico broadcast retransmitido. Esto no resuelve el problema (ya que no se va a la fuente) pero limita el tráfico total en el medio.

IMPLEMENTACIÓN DE NETWORKING EN SISTEMAS WiMAX

Networking en sistemas WiMAX

El estándar *IEEE 802.16-2009* tiene definida una Capa 2 muy eficiente y distinta a otras capas habituales en redes IP (como por ejemplo Ethernet). El estándar define un modelo de referencia para el tratamiento de los datos que se muestra en la Figura 6. Para implementar todas las funcionalidades, el estándar define una capa intermedia que permite el encapsulado de tráfico Ethernet o IP sobre la propia pila WiMAX, de una forma similar a las capas AAL de ATM. La parte más alta de este modelo se denomina **Subcapa de Convergencia** (*CS, Convergence Sublayer*), y es el punto por el cual los paquetes de datos entran dentro de la MAC 802.16 y son clasificados en diferentes colas.

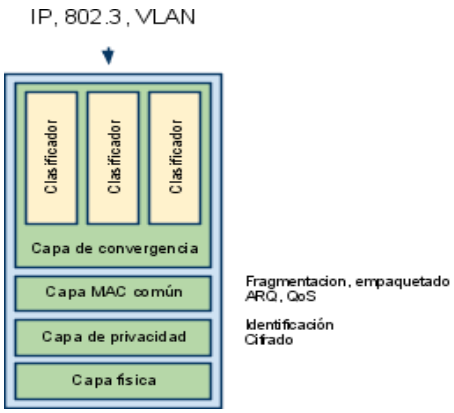

Figura 6 - Modelo de referencia en WiMAX

Implementación de Albentia Systems

El estándar define las bases principales del modelo de referencia, pero deja libertad a los fabricantes que hagan su particular implementación. La implementación de *networking* de *Albentia Systems* es la más completa del mercado, soportando una CS de paquetes que permite el procesado de paquetes que lleven protocolos IEEE 802.3, IPv4 sobre 802.3, VLAN o IPv4 sobre VLAN. Estos protocolos son los más utilizados en la actualidad para la interconexión de redes en escenarios de Acceso.

En la implementación de la MAC realizada por *Albentia Systems*, la entrada a la capa MAC para cada dispositivo inalámbrico "X" se realiza a través de interfaces lógicas independientes denominadas **wethX**, que a su vez pueden configurarse en diferentes modos de *networking*.

Si bien WiMAX es una tecnología de nivel de enlace (2 en la pila OSI), debe poder interconectar otras tecnologías de modo que un operador de red sea capaz de dar una solución de conectividad extremo a extremo. El equipamiento *Albentia Systems*, y en particular la Estación Base interoperable, está diseñado teniendo en cuenta los exigentes requisitos de *networking* de los operadores, con lo que implementan distintas estrategias de *networking*. Existen 3 grandes modos de operación: **Bridging**, **Routing** y **Local-Network**.

⇒ *Bridging*

Este modo es la forma más sencilla de trabajar, y resuelve el problema de la interconexión haciendo el enlace WiMAX transparente a nivel 2 para el resto de la red. Para ello, el dispositivo WiMAX se comporta como un *bridge multipuerto* que interconecta la interfaz Ethernet de la BS con cada una de las interfaces inalámbricas lógicas (wethX) asociadas a cada uno de los dispositivos inalámbricos conectados.

Por tanto, una BS de Acceso WiMAX con 150 usuarios conectados y configurada en modo Bridge, es un gigantesco *Switch* con 151 "bocas". Cuando se reciba un paquete con dirección desconocida, el bridge lo transmitirá sobre todas sus conexiones excepto por la que llegó, con lo que transmitirá este paquete 150 veces. Lo mismo ocurre con cualquier tipo de tráfico broadcast, que será lanzado por todas las interfaces y por tanto irá replicado por el aire tantas veces como usuarios haya en la celda. En una red de este tipo, los equipos WiMAX son totalmente invisibles para las redes que interconectan.

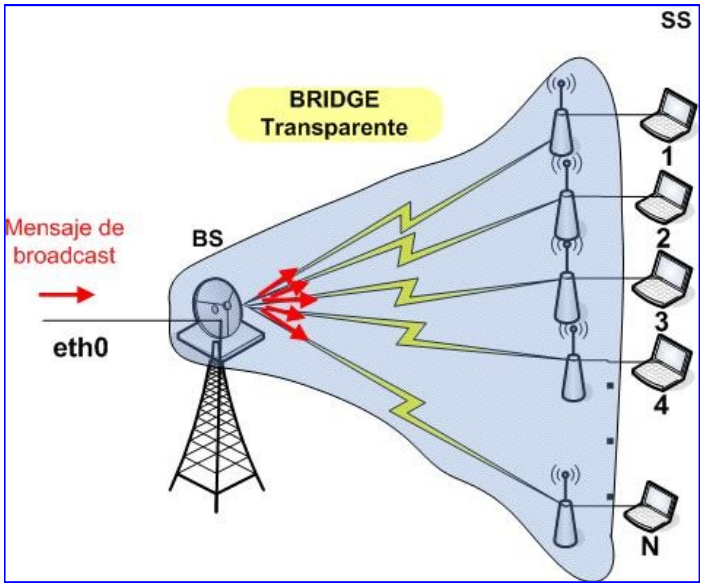

Figura 7 - Modo *Bridging*

⇒ *Routing*

El modo *routed* consiste en el paradigma clásico de interconexión de redes a nivel 3. Cada una de las interfaces **wethX** que representan las conexiones inalámbricas del equipo será configurada con una dirección IP, y el operador deberá añadir manualmente en la BS las rutas necesarias para acceder a los equipos que estén detrás del otro extremo del enlace. La BS tendrá una tabla de rutado y por lo tanto realizará un filtrado del tráfico de *broadcast*.

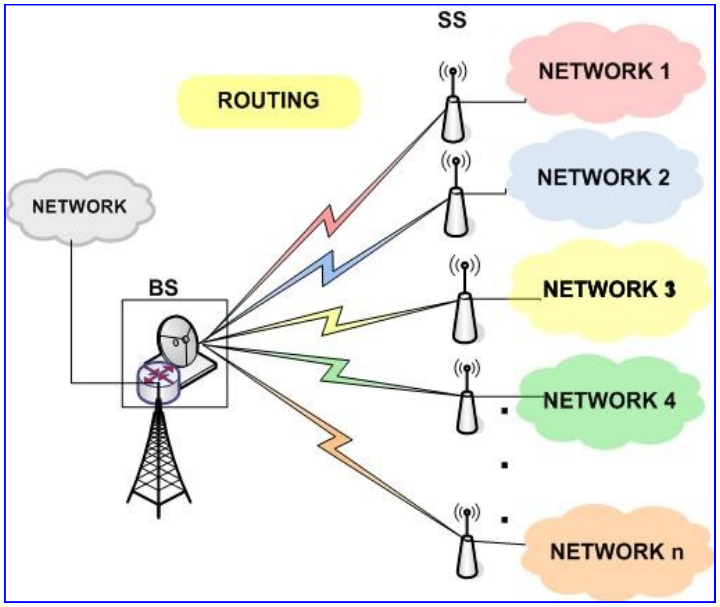

Figura 8 - Modo *Routing*

⇒ ***Local-Network / Doble NAT***

Este modo nace para facilitar a los operadores el despliegue de terminales de usuario (CPEs) en entornos con muchos clientes. Si éstos no soportan nativamente la configuración de su interfaz de red de modo dinámico (DHCP o similar) puede ser realmente engorroso el mantener este tipo de red en modo "*Bridge*", dado que los CPEs deberían ser configurados uno a uno. Asimismo, sería conveniente el no tener que configurar los CPEs en el momento de la instalación, o al menos, que esta fuese lo más simple posible. El modo "*Local Network*" proporciona la capacidad de configurar la parte de red de los usuarios dinámicamente sin tener que configurar nada en cada CPE.

En la utilización más habitual de este modo, todos los CPEs vienen con una dirección IP preconfigurada de fábrica, y en la BS se hacen las traducciones de direcciones necesarias para alcanzar a los equipos. Conceptualmente, es como si todos los CPEs se conectaran a una red virtual dentro de la BS. Posteriormente, la BS hace una traducción de direcciones entre esta *red local* y su red de tránsito, de modo que los terminales de usuario aparecen virtualmente como *bridgeados.*

En este modelo, en primer lugar se introduce el concepto de *red local* dentro de la BS; esto consiste en proporcionar un segmento Ethernet virtual en el que los equipos van a tener conectividad entre ellos y con la BS. Esta red local, es en realidad un *bridge* lógico interno del equipo.

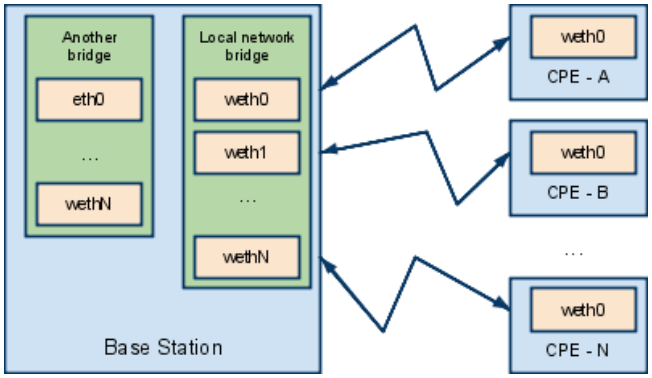

Figura 9- Esquema lógico del "*Local Network*"

Como todos los CPEs están configurados en la misma dirección IP de fábrica, la BS debe traducir estas IPs a las direcciones correctas dentro del "*Bridge Local Network*". Para ello, realiza una traducción de direcciones estática, es decir, a todos los paquetes que *salgan* por la interfaz correspondiente a un CPE se le va a traducir la dirección destino por la dirección por defecto de fábrica y a todos los paquetes que *entren* se cambiará la dirección origen (por defecto de fábrica) por la dirección IP correspondiente a esa boca del *bridge*. De esta manera se consigue la red virtual.

Esta red local, como tal, no tiene acceso a la red de tránsito exterior a la base. Para ello, se deben añadir las reglas de rutado entre el *bridge* correspondiente a la red Local y el *bridge* con conectividad exterior adecuadas.

Por otro lado, la BS debe hacer las funciones de Proxy-DHCP, de modo que sea capaz de pedir hacia el exterior una dirección IP asignable a cada CPE. Una vez obtenida, realiza las traducciones de direcciones DNAT y SNAT necesarias para hacer externamente visible al dispositivo. Además de estas traducciones, es necesario que la BS haga de Proxy-ARP de la dirección IP del CPE, de manera que reciba el tráfico destinado a él y pueda hacérselo llegar. La Figura 8 muestra las traducciones de direcciones involucradas en este modo.

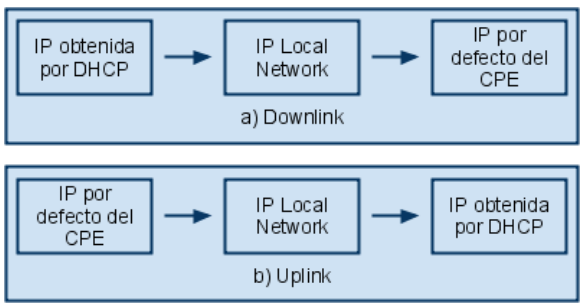

Figura 10– Esquema de traducción de direccio-

La recomendación de *Albentia Systems*

El equipamiento de *Albentia Systems* soporta distintos modos de *networking*, porque es importante que el operador de red pueda tener flexibilidad y elegir el modo más eficiente para cada escenario. Otros fabricante sólo implementan el modo Bridging, que en ciertos escenarios resulta ineficiente.

La recomendación general de *Albentia Systems* es:

A) Para escenarios PtP y escenarios PtmP con baja densidad de usuarios, cualquier modo de *networking* es perfectamente válido. En la mayoría de escenarios de este tipo, es probable que el ***Bridging*** sea la mejor opción debido a su facilidad de configuración, rapidez y transparencia hacia el usuario final.

B) Para escenarios PtMP con un número medio/alto de usuarios, el modo *Bridging* pierde interés, debido en gran parte a que retransmite todo el tráfico de *broadcast* a todos los usuarios, con lo que es más ineficiente a medida que aumenta el número de CPEs. Se recomienda por tanto ***Routing*** o ***Local Network***, modos pensados para operadores y muchos usuarios, que reducen el broadcast y aportan más funcionalidad.

Recientes pruebas y medidas realizadas en BSs de *Albentia Systems* en escenarios con muchos usuarios (más de 100) han demostrado que la migración del modo *Bridging* al modo *Local Network* ha supuesto mejoras llamativas en el funcionamiento de la celda. Se reduce drásticamente el tráfico de *broadcast* en el aire, que es como un "*tráfico de fondo*", con lo que queda más tráfico útil disponible. La BS "*gasta*" menos tráfico, no porque mande menos datos, sino porque elimina tráfico de *broadcast* permanente hacia todos los CPEs. No hay que olvidar que tráfico de broadcast aumenta **más que proporcionalmente** con el número de usuarios. Con **[n]** usuarios generando un evento broadcast por segundo, cada CPE transmitirá cada segundo un paquete a otros **[n-1]** CPEs. En cada segundo, habría en el aire n paquetes, (n-1) veces. Esto significa que en modo *Bridging*, con 4 CPEs tendríamos 12 paquetes broadcast/sg en el aire, pero con 150 CPEs, tendríamos 150*149 = 22350 paquetes/sg de tráfico broadcast no útil en el aire.

Además de esto, modos como el *Local-Network* son muy atractivos para el operador por sus **funcionalidades añadidas**: traducción de direcciones, inaccesibilidad entre CPEs, configuración centralizada en la BS y posibilidad de despliegue de CPEs con valores de fábrica, etc…

CONCLUSIONES

1) El *Bridging* y el *Routing* son dos maneras distintas de trabajar en redes de datos: mientras que el primero se realiza hasta capa 2 (nivel de enlace en OSI), el segundo se realiza hasta capa 3 (nivel de red en OSI). Un *Bridge* encamina tramas según la dirección MAC (fija) mientras que un *router* toma sus decisiones de encaminamiento según direcciones IP (que pueden cambiar). Los Bridges son sencillos de configurar, son transparentes y segmentan los dominios de Colisión, aunque tienen la desventaja de que no segmentan los dominios de Difusión (como sí hacen los routers): cuando reciben un paquete con dirección desconocida, o *broadcast*, o *multicast*, un *bridge multipuerto* lo retransmite por todas sus interfaces (excepto por la que llegó).

2) El tráfico *Broadcast* y *Multicast* es un tipo de tráfico muy presente en las redes actuales, y vital para el correcto funcionamiento de protocolos y *hosts*, aunque hay que controlarlo porque puede llegar a afectar al rendimiento de la red, sobre todo congestionando el medio. Evidentemente, este problema es más crítico a medida que aumenta el número de usuarios y en medios con una capacidad limitada, cosa que sucede en cualquier sistema inalámbrico.

3) Los equipos de *Albentia Systems* ofrecen la solución más completa del mercado en cuanto a modos de *networking*, debido en gran parte a la interacción con operadores de telecomunicaciones y la atención de sus necesidades. Cualquier persona que adquiera equipamiento WiMAX debería ser capaz de poder elegir el modo de networking más adecuado. En ese sentido, el equipamiento de Albentia Systems no sólo permite trabajar en modo Bridging como hacen muchos fabricantes, sino que se adapta a cada escenario.

4) En resumen, una recomendación de *networking* genérica podría ser la siguiente:

- En escenarios PtP o PtmP con un **número limitado de usuarios**, el modo "*Bridging*" es una opción muy atractiva, ya que facilita mucho las conexiones y resulta sencillo de configurar y transparente al usuario final. Es un buen modo de trabajar para interconectar varios edificios, en un enlace Punto a Punto, para recoger señal de vídeo de unas pocas cámaras IP, etc.
- En el escenario de Acceso PtmP con **muchos usuarios**, el modo Bridging empieza a ser menos eficiente y *Albentia Systems* recomienda pasarse a los modos "*Routing*" o "*Local Network*". Qué es "muchos usuarios" es un criterio del operador y depende de cada caso, pero *Albentia Systems* desaconsejaría utilizar modo *Bridging* en una red de Acceso con más de 25 ó 30 usuarios.