albentia Systems

ALB-W-000007en

WHITE PAPER

White Paper

Bridging vs Routing in wireless PtmP networks

May 2010
Rev A1

Most of the broadband wireless equipment's manufacturers provide the Bridging mode as the only networking possibility, due to its simplicity. Nevertheless, in Point to Multipoint (PtmP) Access scenarios with a large number of connected users, this mode may not be optimum at all, since all broadcast messages will be transmitted to the whole network through the Bridge (broadcast traffic generated by every users and generated by the Bridge itself when learning the network architecture). This point is essential in such a limited resource as the radio spectrum.

This document is intended to clarify the important implications about configuring in Bridge Mode any broadband wireless system which must handle a big number of users. It also introduces the multiple networking possibilities available in Albentia Systems' equipment, such as Routing or Local Network. First, some general networking issues are going to be explained. Later, these issues will be extrapolated to wireless networks and in particular to those based on the IEEE 802.16-2009 standard (WiMAX).

INTRODUCTION: BASIC NETWORKING CONCEPTS

Bridging Definition

When Ethernet networks began to be used massively, increasing the connected hosts and transmitting more an more data, it became necessary to add some network devices which could solve the collision problems of the hubs: *Bridges and Switches* appeared.

A **bridge** is a device that connects two or more network segments at the Link-Layer (Layer 2) in the OSI model, according to *IEEE 802.1D* standard. It sends the frames according to the destination MAC address in the datagrams, regardless the higher lever protocols used.

⇒ **Self-learning**

Bridges perform a self-learning process of MAC addresses on each network segment, storing them in an internal table (**Forwarding table**), and following the next sequence (see Figure 1):

*(1) **PC_A** (00:1F:4A:00:00:51) sends a frame to **PC_C** (00:1F:4A:00:00:52).*
(2) The Bridge receives the frame and examines the MAC source address (SA). As it is not registered in the Forwarding table, it stores the address/port (ETH1) in the table.
*(3) The destination address (DA) does not appear in the table, so the Bridge does not know to which interface must be sent the frame, so it floods the datagram through every port to also reach **PC_C**.*
*(4) **PC_C** receives the frame and responses with another frame to **PC_A.***
(5) The SA of this frame is not registered in the forwarding table either, so the bridge stores it with the associated source port (ETH3).
*(6) The DS (**PC_A**) is registered in the table since (2), so the bridge sends the packet just through ETH1.*

For transmitting a frame, the *Bridge* searches the destination MAC on its Forwarding table so it forwards the frame only to the correct port (opposite to *hubs)*.

Therefore, we can affirm that Bridges generate a "learning" multicast and broadcast traffic that is sent to every port. Learning is automatic, so Bridges are very easily configured.

Bridges perform an intelligent network connection, with a big advantage: segmentation of *Collision Domains*, creating one domain for each interface. Simplifying, it can be said that in comparison to Hubs, Bridges provide traffic improvements and best isolation between segments in the LAN, and in comparison to routers, configuration and management is easier, but bridges do not provide such a high level of traffic isolation in the LAN.

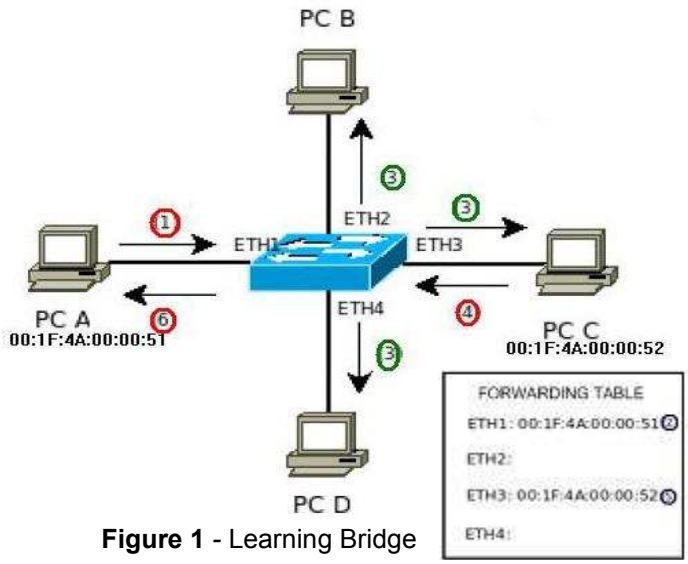

Figure 1 - Learning Bridge

⇒ **Differences between Bridge and Switch**

Both are layer-2 devices with similar functionalities, although Bridges are commonly used for connecting remote segments in a LAN (both wired or wireless), and Switches are normally used for connecting multiple host within a LAN or several adjacent LANs. Besides, the packet switching in Switches is performed via Hardware, while in Bridges is performed via Software. Anyway, in many contexts these two concepts are exchanged or used without distinction.

Routing Definition

Routers are networking devices that operate at Network Layer (Layer 3 in OSI) The main purpose of a router is to connect multiple networks, forwarding packets between them. Its primary forwarding decision is based on the information located in the Layer-3 packet header, specifically the destination IP address. This process is known as "routing". Routers allow IP datagrams to reach any destination address from any part of the network.

To carry out its function, routers have a **Routing table** to store routes to every node in the network, as well al any other information that may be useful for routing. These tables may be configured statically or may be maintained automatically by routing protocols (i.e. RIP, OSPF,...), which enable routers to exchange information with other nodes of the network to decide the best routes.

When a router receives a packet, it reads the IP packet header and determines, by means of the destination IP address, if that packet must be forwarded to a network that is locally accessible by the router. In this case, it sends the packet to the corresponding MAC address. Otherwise, it searches in the Routing table an entry with the destination network specified in that packet, and forwards the packet to the appropriate interface. If no entry with the destination network is found in the table, the router uses a special entry in the routing table: the Default Gateway.

Besides the routing function itself, routers are generally speaking "more intelligent" devices comparing to bridges or switches, and they are able to perform other operations such as packet filtering, fragmentation, IP address allocation (NAT, DHCP, ...), etc...

Like bridges, routers are capable of performing the segmentation of collision domains. However, there is a difference between them: routers, by default, do not forward **broadcast** packets because they also separate the broadcast domains. This is important because it prevents that every devices in the network receive the broadcast messages from the rest, reducing the overall traffic in the network.

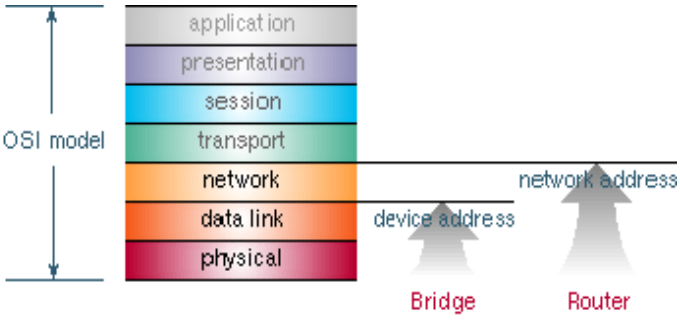

Figure 2 - Bridges and Routers operation levels

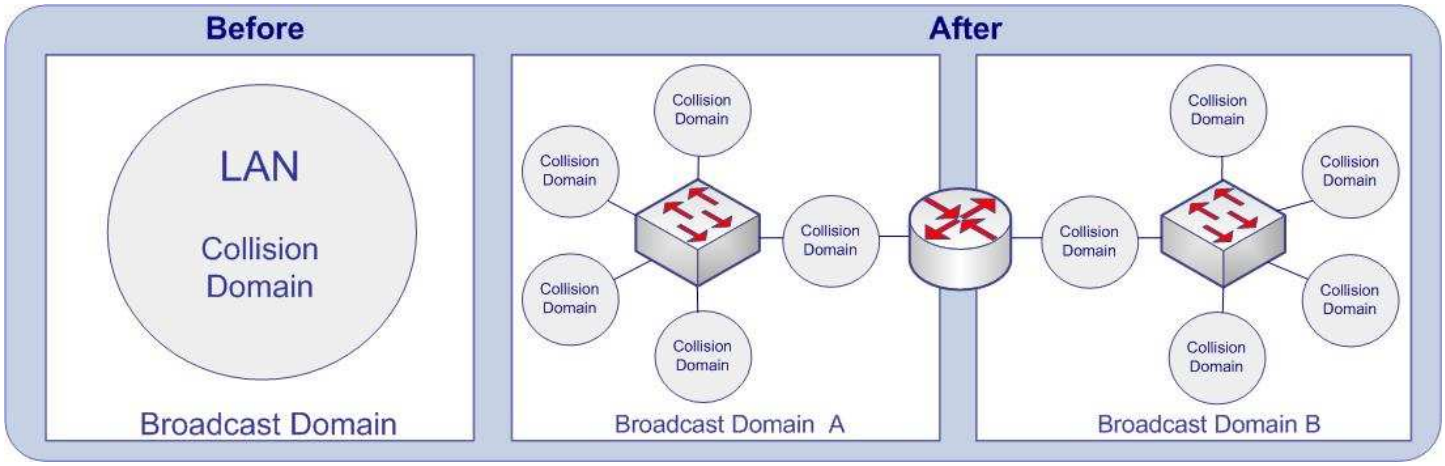

Figure 3 - Collision and Broadcast Domains with Bridges and Routers

Bridge

- Operates at Data Link Layer (Layer 2)
- Connects segments in a local network
- Forwards datagrams according to MAC addresses
- Forwarding Table: MAC/interface
- MAC self-learning in every segment (by means of broadcast traffic)
- Very easy and simple configuration
- Collision Domain segmentation

Router

- Operates at Network Layer (Layer 3)
- Connects different networks
- Routes packets according to IP addresses
- Routing Table (static or dynamic)
- Collision & Broadcast Domains segmentation
- Isolates the traffic in the network, separating the broadcast, multicast and "learning" traffic

BROADCAST/MULTICAST TRAFFIC

Definition

The broadcast traffic is a natural component in a TCP / IP network, and consists on the communication between a source terminal to ALL terminals of a broadcast domain (network, subnet or VLAN).

A Layer 3 (network layer) **broadcast packet** forwarded to every host is a packet whose destination IP address is **255.255.255.255.** A broadcast packet to a specific network (direct broadcast) is a packet whose destination IP address is the broadcast address of that subnet (i.e. **X.X.X.255**).

IP broadcast packets are encapsulated in **broadcast frames** at Link-Laver, those with destination MAC address **FF:FF:FF:FF:FF:FF**. When a bridge or a switch receives a frame with a broadcast destination address, it transmits that frame to all ports, except the port from which it was received.

On the other hand, Multicast traffic is a particular case of broadcast traffic, which uses a special range of multicast addresses (class D, from 224.0.0.0 to 239.255.255.255) that do not identify nodes but a group of nodes (multicast group).

Origin of broadcast/multicast

The three typical sources of broadcast and multicast in IP networks are network devices, multicast applications and hosts:

- **Network devices**: as already explained, network devices like switches or bridges use broadcast and multicast frames at Layer 2 to communicate with other collision domains when they have a packet for an unknown host. Besides, they send to its broadcast domain all the broadcast traffic they receive.
- **Multicast applications**: the IP multicast is an efficient way to send a stream of data to many users, although a big amount of bandwidth is consumed. For instance, a real-time video streaming in multicast mode may generate a data stream greater than 2 Mbps, that in a switched network would be sent to every segment and might cause network congestion.
- **Network hosts**: the network hosts themselves may generate broadcast traffic. There are multiple protocols running over this equipment that need broadcast traffic for its internal process. Some examples of this kind of protocols will be explained below:

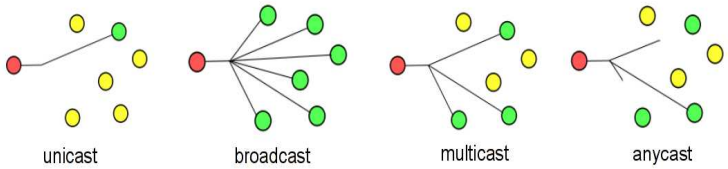

Figure 4 - Routing scheme

⇒ **ARP** (*Address Resolution Protocol*)
This network layer protocol is used by hosts to learn the MAC address of those hosts whose IP address is already known. This information is stored in the internal cache of each host (ARP table). This table may include Dynamic entries (those that are added and deleted automatically, with a maximum lifetime) and Static entries (that remain in the cache until the unit is restarted).

The protocol works as follows:

- ***A** wants to send an IP datagram to **B**.*
- ***A** checks its routing table. It knows B's IP address but it also needs the MAC address.*
- ***A** sends an ARP Request to the broadcast MAC address. When it arrives to **B**, it learns the MAC/IP of **A**, and sends to it an ARP Reply with its MAC address. When **A** receives this reply, it write the information in its table.*
- ***A** is already able to send an Ethernet frame to **B**.*

Therefore, all hosts send a broadcast ARP request every time they need to identify a MAC address that is not in their ARP table (usually because the entry was dynamic and has expired).

As the number of hosts in a subnet increases, ARP tables become larger and have more entries. Thus, the broadcast ARP traffic in the network increases **exponentially** according to the number of hosts.

⇒ **NetBIOS** (Network Basic Input/Output System)
It is a protocol that operates at the application layer and it is exclusive to *Windows* networks. It assigns names and workgroups to workstations and it is mainly used for sharing files and printers and for checking the available resources in *Windows* networks.

⇒ **Routing protocols** (RIP, OSPF, IGRP,…)
Hosts and routers in a network may use these protocols as a mechanism of redundancy and knowledge of the net, but this may increase broadcast traffic significantly. Every 30 seconds, RIPv1 broadcasts the entire routing table to other RIP routers. If 200 computers are configured to run RIP and let's suppose that on average 50 packets are required for transmitting the routing table, workstations would generate 333 broadcast packets per second. Because of this, most of the network administrators configure RIP only in a low number of routers.

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

It is a network-level protocol that hosts use for automatically configuring parameters such as IP address, gateway, netmask, DNS server,... A DHCP server has a dynamic IP-address list and, when receiving a request, it assigns them to Clients.

The process starts when a Client sends a DHCPDISCOVER packet to find any active DHCP server. Afterwards, the server responds with a DHCPOFFER, offering configuration parameters, and the client may accept or reject the offer with a DHCPREQUEST. Finally there is a confirmation and closing DHCPACK message from the server to the Client which ends the transaction. All these messages are sent to the broadcast destination address. The host to whom the DHCPOFFER is directed collects all the information, and the rest of the hosts will receive the packets and discard them.

⇒ **DNS** (Domain Name System)

This protocol is responsible of the name resolution (translation of names to IP addresses). The resolution method used in a network is broadcasting unless another one is specified This method resolves the names correctly, but generates a large amount of traffic on the network. There is also the MDNS (multicast DNS) protocol, an implementation of the protocol name resolution for those local area networks with no real DNS server, and as its name suggests, generates multicast traffic.

⇒ **Others**

Innumerable protocols use at least occasionally broadcast packets . LLC (Logical Link Control), IGMP (Internet Group Management Protocol), etc. Even higher-level applications may use them. For example, a well known antivirus program sends every 30 seconds broadcast packets on UDP 6646 port to check whether there are other computers on the network with this program installed (fort statistic sharing).

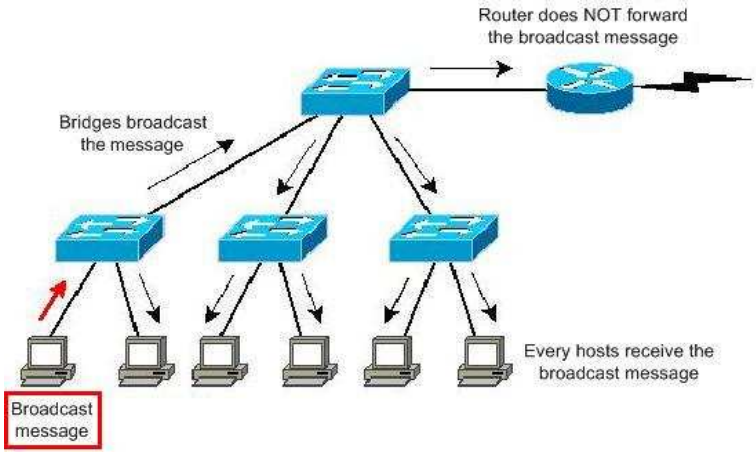

Figure 5 - Bridges' and Routers' performance

The problem

The broadcast traffic is a key element for many protocols. It may be insignificant or it may even collapse the medium, so controlling it is highly recommended. The generation of broadcast and multicast traffic for each host of the network is called broadcast radiation. The main consequences of this radiation are:

- **It floods the network with unnecessary traffic**, reducing the useful capacity of the medium with a kind of "background traffic". The most extreme case in which this radiation comes to saturate the medium and affects the entire network is called broadcast storm.
- **It affects the performance of each host**, consuming hosts' and servers' resources (CPU and NIC), since they must process the received broadcast traffic even though it is often discarded (because it is not destined to them).
- **Vulnerabilities**: broadcast traffic may be used to perform denial of service and traffic flooding attacks to the network: DOS (Denial of Service), *Fraggle*, *Smurf*, IP Flooding, ...

Additionally, configuration problems (such as loops) or failing devices may cause the presence of important amounts of broadcast that limit the regular operation of the network, decreasing their performance significantly.

Broadcast traffic **exponentially** increases as the network's size does, and it is especially critical in environments where the maximum potential capacity is limited, which is the case of any wireless technology.

Solutions

The most direct solution to reduce the negative impact of the broadcast traffic consists on limiting the broadcast domains' size (the amount of hosts that receive a broadcast message). To achieve this, the traditional tools are:

- Splitting the network in subnetworks
- When implementing Level 2-switching, limiting the broadcast by means on VLAN segmentation
- Using Level 3 devices like Routers in order to split the broadcast domains. This may also be done with some switches that incorporate additional intelligence, colloquially named "*brouters*".
- Using STP (Spanning Tree Protocol) switches, to avoid broadcast storming caused by loops
- There are routers, firewalls,... that may detect and prevent accidental or "malicious" broadcast storming
- Some *switches* implement a "Broadcast Storm Control" mechanism by which a certain threshold of broadcast traffic is not exceeded. This does not solve the problem (because it is not focused on the source) but limits the overall traffic in the medium

NETWORKING IMPLEMENTATION IN WiMAX SYSTEMS

Networking in WiMAX Systems

The *IEEE 802.16-2009* standard defines a highly efficient Layer 2 that differs enormously from the common layers in others IP networks (like Ethernet). It is designed to obtain the best performance of the radio channel. The standard defines a reference model that is shown in Figure 6. For implementing all the features, the standard defines an intermediate layer that allows the encapsulation of Ethernet or IP traffic over the WiMAX Protocol stack itself, similar to ATM AAL layers. The top of the MAC layer is the **Convergence Sublayer**, and is the entry of the data packets to the 802.16 MAC and the point where packets are classified into different queues.

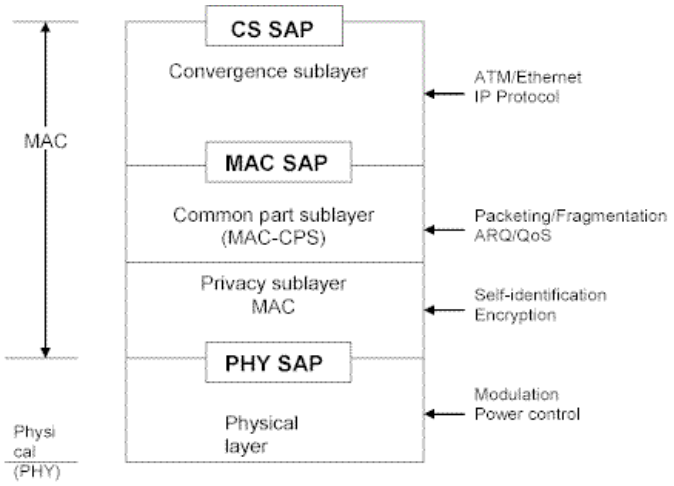

Figure 6 - *IEEE 802.16-2009* Reference model

Albentia Systems' Implementation

The standard defines the main bases of the reference model, but allows the manufacturers to make their own implementation. The carrier-class Albentia Systems' networking implementation supports a CS that allows packet processing carrying IEEE 802.3, IPv4 over 802.3, VLAN and IPv4 over VLAN. These protocols are the most commonly used today for interconnecting networks in Access scenarios.

In Albentia Systems' MAC layer implementation, the entrance to the MAC layer for each wireless device "X" is performed through independent logical interfaces called **wethX**, which may be configured in different networking modes.

Although WiMAX is a Link-level technology (layer 2 in OSI model), it must be able to interconnect other technologies so that a network operator is able to provide an end-to-end connectivity solution. Albentia Systems equipment, and particularly its interoperable Base Station, is designed considering the demanding network requirements of the operators, implementing many different strategies for networking. There are 3 main modes of operation: **Bridging, Routing and Local Network**.

⇒ Bridging

This mode is the simplest working mode and it solves the interconnection issue by doing the WiMAX link transparent at level 2 to the whole network. For that purpose, the WiMAX device works like a multiport bridge that connects the BS's Ethernet interface with each logical wireless interface (wethX), associated to each of the connected wireless devices.

Therefore, a WiMAX BS configured in Bridge mode with 150 connected users, it is like a huge switch with 151 "ports". When a packet with an unknown address is received, the bridge will forward it for every ports except the one from which it arrived, so this message will be transmitted 150 times. The same applies for any type of broadcast traffic, which will be forwarded to all the interfaces and therefore it will be replicated as many times as users in the cell. In such a network, WiMAX devices are completely invisible to the rest of the interconnected networks.

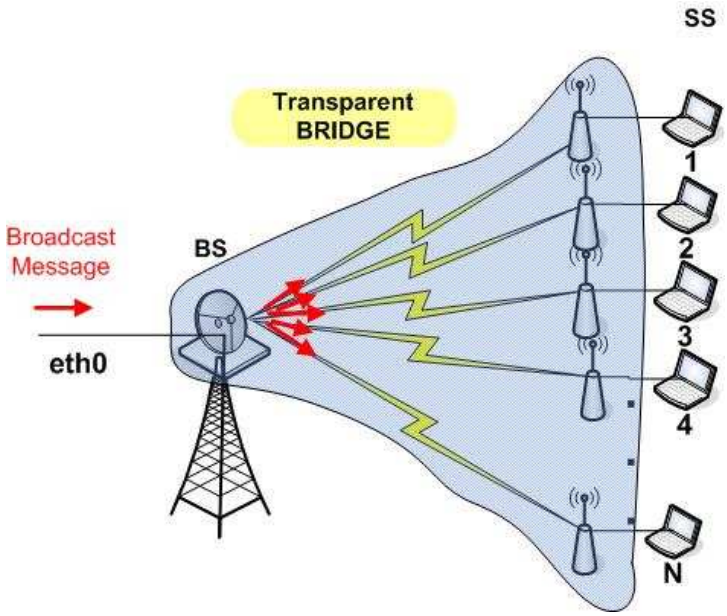

Figure 7 - Bridging Mode

⇒ Routing

Routed mode is the classic paradigm of Layer 3 network connection. Each one of the **wethX** interfaces that represent the wireless connection of the equipment will be configured with an IP address, and the operator should manually add the necessary routes in the BS to access those hosts behind the other side of the net. The BS has a routing table and therefore it filters the broadcast traffic.

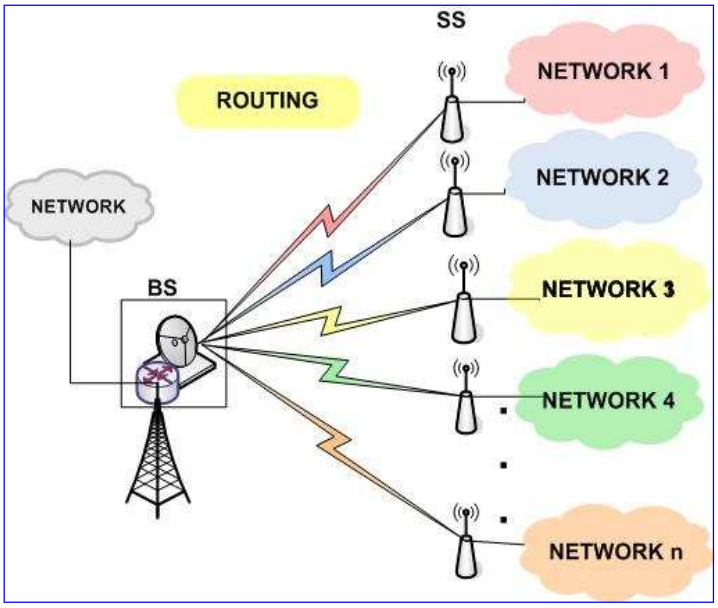

Figure 8 - Routing Mode

⇒ **Local-Network / Double NAT**

This mode was created to make easier the deployment of CPEs in scenarios with a big number of users . If a CPE does not natively support the configuration of its network interface in dynamic mode (DHCP or similar), management of this kind of network in Bridge mode may be complicated, since every CPE should be configured one-by-one. It would be also convenient to avoid configuring CPEs during the installation, or at least the configuration should be as simple as possible. "Local Network" Mode provides the possibility of configuring the users' networking dynamically without configuring anything on each CPE.

In the most common utilization of this mode, every CPE come factory-preconfigured with an IP address, and the necessary address translation for reaching the equipment is done in the BS. Conceptually, it is like if every CPE was connected to a virtual network within the BS. Afterwards, the BS makes the address translation between this *local network* and its "outbound network", so that CPEs will work as if they were virtually bridged.

In this model, firstly the concept of *local network* within the BS is introduced. It consists in providing a virtual Ethernet segment that provides connectivity to the CPEs with other CPEs and with the BS. This local network is actually a logical internal bridge in the BS.

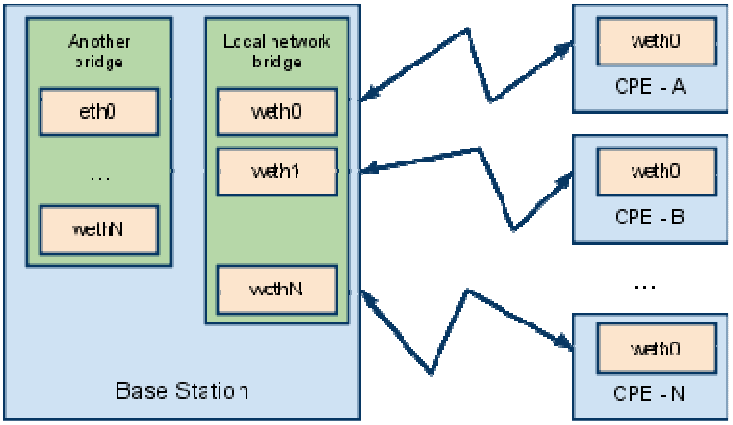

Figure 9 – Logical scheme of "Local Network"

Since all CPEs are configured with the same default IP address, the BS must translate these IPs to the correct addresses in the "Local Network Bridge". For this purpose, it performs a static addresses translation, which means that to all packets going out the interface corresponding to a CPE, their destination address is going to be changed by the factory default address, and to all packages entering, its source address (the factory address by default) is going to be changed by the IP address corresponding to that port of the bridge. This way the virtual network is established.

The local network itself does not have any access to the outbound network. To get the communication, it is required to add the necessary routing rules between the local network bridge and the bridge that can access the outbound network.

On the other side, the BS must carry out the Proxy-DHCP functions, so that it is able to get an IP address for assigning to every CPE. Once the address is obtained, the BS performs the DNAT and SNAT address translations, necessary for making the device externally visible. Besides these translations, it is necessary that the BS works like a ARP-Proxy of the CPE's IP address, so that the BS receives the traffic with destination the CPE, and manages to forward it to the CPE. Figure 8 shows the address translations performed by this mode.

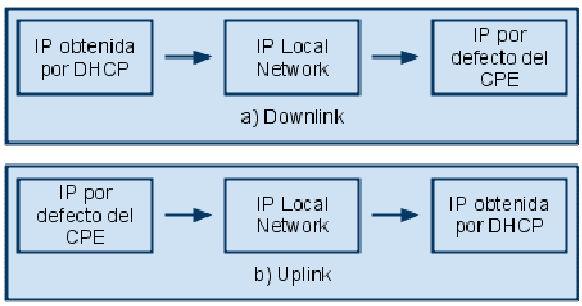

Figure 10 – Address translation scheme

Albentia Systems' recommendation

Albentia Systems' equipment supports different networking modes because it is important that the network operator has flexibility and may choose the most efficient mode for each scenario. Other manufacturers just implement the Bridge mode, which is inefficient in some scenarios.

Albentia Systems' general recommendations are:

A) In PtP and PtmP scenarios with low density of users, any networking mode is perfectly usable. In most of these scenarios, ***Bridging*** will be probably the best choice due to its easy an quick configuration possibilities and to the transparency to the final user.

B) In PtmP scenarios with a medium/high number of users, bridging mode lacks of interest, since this mode forwards all the broadcast traffic to every user, reducing the efficiency as the number of CPEs increases. Thus, ***Routing*** or ***Local Network*** mode are recommended. These modes reduce the broadcast, provide more functionalities, and are designed according to the operators' needs in many users' scenarios.

Recent tests and measurements to Albentia Systems' BSs in scenarios with a large number of users (over 100) have demonstrated that migrating from Bridging to Local Network implies important improvements in the cell performance. Broadcast traffic in the air is incredibly reduced, so overall throughput is increased as that "background" traffic nearly disappears. The overall throughput the BS is able to provide does not change, but when the BS carries broadcast traffic constantly to every CPEs, useful throughput is being wasted. Do not forget that broadcast traffic increases **more than proportionally** as the number of users does. Having **[n]** users generating a broadcast event per second, every CPE will transmit a message to the rest **[n-1]** CPEs every second. Thus, in that slot of time, there would be in the air n packets, (n-1) times. This means that in Bridging mode, having 4 CPEs there would be 12 broadcast packets per second in the air, and having 150 CPEs, 150*149 = 22350 not "useful" broadcast packets per second in the air. It is a **non proportional increase, but exponential**.

Besides, modes like Local Network are very attractive for the operators due to the **extra functionalities:** address translation, CPEs isolating, centralized configuration in the BS, deployment of CPEs with factory parameters, etc.

CONCLUSIONS

1) Bridging and Routing are two different networking models in data networks: while the first one works up to Layer 2 (link layer in OSI), the second one does up to layer 3 (network layer in OSI). A bridge forwards the frames according to a fixed MAC address, while a router makes routing decisions according to IP addresses (that may change automatically). Bridges are simple to configure and transparent, and segment Collision Domains, but they have the disadvantage that they do not segment the Broadcast Domains (like routers do): when receiving a packet with unknown, broadcast or multicast IP address, a multi-port bridge will forward it to all its interfaces, (except to the one that received it).

2) Broadcast and Multicast traffic are two very common types of traffic in today's networks, and they are essential for the correct protocols' and hosts' performance. Nevertheless, it is important to control them because they may reduce the network performance mainly due to the air interface congestion. Obviously, this problem is more critical when increasing the number of users and when capacity is limited, which happens in every wireless system.

3) Albentia Systems' equipment provides the more complete solution in terms of networking in the whole industry. This is due to the permanent contact with network operators, with particular attention to their needs. Any person acquiring WiMAX equipment should be able to choose the networking mode that better fits its needs. In this sense, Albentia Systems' equipment does not only allow operating in Bridging mode like most of the manufacturers do, but it is also perfectly suitable for every scenario.

4) To sum up, a generic recommendation regarding networking would be:

- In PtP or PtmP scenarios, with a **limited number of users**, Bridging mode is a very attractive option, since it makes the communication easy, it is simple to configure and it is transparent to the final user. It is a proper mode for connecting buildings, for Point to Point radiolinks, for collecting video signal from some IP cameras, etc.
- In a Access PtmP scenario with **many users**, Bridging loses efficiency and Albentia Systems recommends shifting to Routing or Local Network mode. "Many users" concept is a criteria that concerns the operator and it is not easy to unify since it depends on each situation, but Albentia Systems would not recommend Bridging mode in a network access with more than 25 or 30 users.