Project Number:	**IST-2001-32603**
Project Title:	**6NET**
CEC Deliverable Number:	**32603/SURFnet/DS/3.4.1/A1**
Contractual Date of Delivery to the CEC:	**December 31st, 2002**
Actual Date of Delivery to the CEC:	
Title of Deliverable:	**IPv6 Intra-domain multicast service**
Work package contributing to Deliverable:	**WP3**
Type of Deliverable*:	**P**
Deliverable Security Class**:	**PU**
Editor(s):	**Wim Biemolt**
Contributor(s):	**Kurt Bauer, Wim Biemolt, Tim Chown, Jerome Durand, Piers O'Hanlon, Jean-Jacques Pansiot, Antonio Pinizzotto, Lorenzo Rossi, Tomasz Szewczyk, Stig Venaas**

* Type: P - Prototype, R - Report, D - Demonstrator, O - Other

** Security Class: PU- Public, PP – Restricted to other programme participants (including the Commission), RE – Restricted to a group defined by the consortium (including the Commission), CO – Confidential, only for members of the consortium (including the Commission)

Abstract:

This document describes the IPv6 Intradomain multicast service used with 6NET. At this moment IPv6 Interdomain multicast, involving multiple Protocol-Independent Multicast (PIM) domains and thus multiple PIM Rendezvous Points (RPs) is not possible. Except when using Source Specific Multicast (SSM) since SSM does not require RPs. The French initiative M6Bone was used to deploy and gain experience with IPv6 Intradomain multicast.

Keywords:

6NET, IPv6, multicast

Executive Summary

This document describes the IPv6 Intradomain multicast service used within 6NET. Differences between IPv4 and IPv6 multicasting require several original approaches for the implementation. This deliverable describes the first implementation and deployment experience.

At this moment IPv6 Interdomain multicast, involving multiple Protocol-Independent Multicast (PIM) domains and thus multiple PIM Rendezvous Points (RPs) is not possible. IPv6 Intradomain multicast, involving only one RP, is also a challenge. For a large part of the equipment used within 6NET there exists no software with IPv6 multicast support yet. A separate test bed from 6NET had thus to be used. This test bed was the M6Bone.

The M6Bone, based on Renater3 (French IPv6 enable network), is a test service aimed to offer an IPv6 multicast service to interested sites. The M6Bone is connecting lots of sites from all over the world, and it proved to be valuable test bed to deploy IPv6 multicast and gain experience with this kind of service.

The 6NET participants involved in building an IPv6 multicast service for 6NET (WP3) all connected, using IPv6-in-IPv4 or IPv6-in-IPv6 tunnels together with RIPng, to the M6Bone and could use at least some of the services available. Like the MBone tools (e.g. VIC and RAT) for conferencing, for which versions are available with IPv6 multicast support.

The experience gained will be very useful to deploy IPv6 multicast within 6NET itself as the software with IPv6 multicast support will become available. And to further extend the service to IPv6 Interdomain multicast.

Table of Contents

2. Introduction

2.1 Basics

There are three methods of data delivery, unicast, broadcast and multicast. Unicast is the most common and provides a one-to-one delivery (shown on the left). Broadcast provides one-to-all delivery (shown in the middle) and multicast one-to-many (shown on the right) or many-to-many. The difference between broadcasting and multicasting is that in the case of broadcasting datagrams are delivered to all hosts on a given network, while in the case of multicasting datagrams are delivered only to a specified group of hosts. Datagrams which are not interesting for all the hosts on a network are not sent to these hosts, thus reducing the amount of unnecessary traffic. In the case of multicasting, the datagrams are delivered to all members of a specified group.

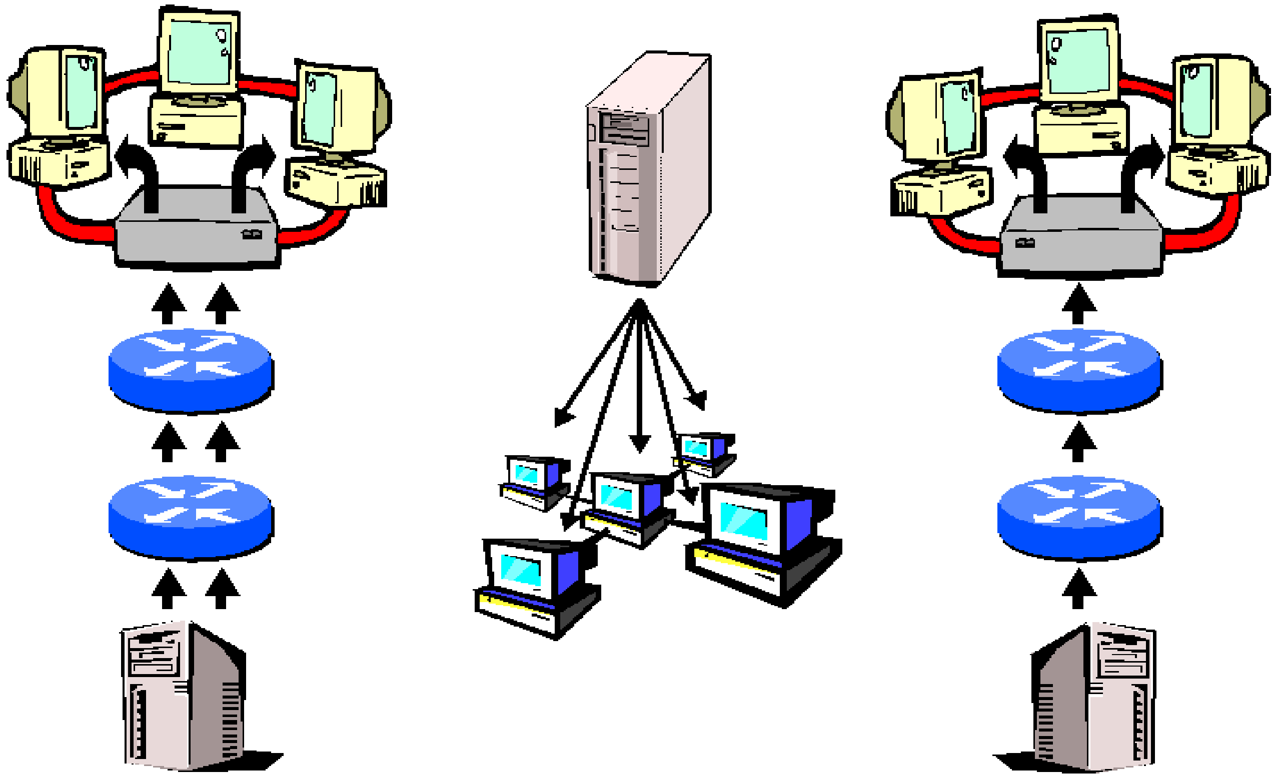


Figure 2.1: unicast, broadcast and multicast.

In IPv6 broadcast does not exist. Broadcast methods included in IPv6 are based on unicast, multicast and anycast. Anycast is a network service that delivers a datagram to any one server out of a group of servers distributed throughout the network. As originally introduced in RFC 1546, anycast is a way to reach the mirror that is the closest (measuring network hops).

Using unicast could result in sending the same message as many times to as many recipients there are. While using multicast, the message would be sent only once from the sender to the multicast group, the interested listeners. To achieve this routers in a network build a distribution tree. The advantages of multicasting are bandwidth demand reduction, server load decrease and less hardware requirements. However, multicasting has some disadvantages as well. Like unreliable packet delivery (as UDP packets are used) and network congestion, as there is no built-in congestion avoidance algorithm used like in TCP.

This deliverable will focus on multicast. For IPv4 multicast was originally defined in RFC 1112 by Steve Deering and has been available since 1988. The deployment of multicast started in 1992 within the MBone project, a virtual network layered on top of portions of the physical Internet to support IP multicast routing. The IPv4 Class D address space was assigned for IP multicast. Therefore, all IP multicast group addresses fall in the range from 224.0.0.0 through 239.255.255.255. Table 2.1 shows the multicast address ranges. Multicast addresses do not have a mask length associated with them and are always assumed to be /32.

Table 2.1: IPv4 multicast address assignments.

Description	Range
Reserved Link Local Addresses	224.0.0.0/24
Globally Scoped Addresses	224.0.1.0 to 238.255.255.255
Source Specific Multicast	232.0.0.0/8
GLOP Addresses	233.0.0.0/8
Limited Scope Addresses	239.0.0.0/8

In IPv6, multicast is an integral part of the protocol and available on all IPv6 nodes. Although multicast routing is not available everywhere and will probably never be in some places. An IPv6 multicast address is an identifier for a group of nodes. A node may belong to any number of multicast groups. Multicast addresses have the format as shown in figure 2.2.

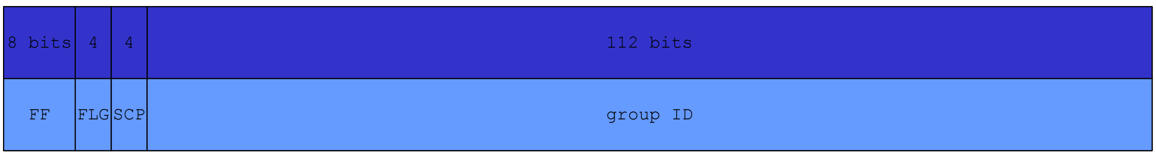


Figure 2.2: IPv6 multicast address format.

When the first eight bits of an IPv6 address are set to 11111111 or FF hexadecimal this identifies the address as being a multicast address. Multicast addresses must not be used as source addresses in IPv6 packets or appear in any routing header.

FLG is a set of four flags. The high-order two flags are reserved, and must be initialised to 0. If the lowest order flag equals 0 this indicates a permanently assigned ("well-known") multicast address, assigned by the global Internet numbering authority. If the lowest order flag equals 1 this indicates a non-permanently-assigned ("transient") multicast address. Concerning the IPv6 multicast prefix, there is now a proposed flag (RFC 3306) (third flag). When set it indicates that the multicast address is constructed from a unicast prefix.

SCP is a 4-bit multicast scope value used to limit the scope of the multicast group. The possible values are shown in table 2.2. The group ID identifies the multicast group, either permanent or transient, within the given scope.

Table 2.2: IPv6 multicast scopes.

Scope		Scope	
0	reserved	8	organization-local scope
1	interface-local scope	9	(unassigned)
2	link-local scope	A	(unassigned)
3	subnet-local scope	B	(unassigned)
4	admin-local scope	C	(unassigned)
5	site-local scope	D	(unassigned)
6	(unassigned)	E	global scope
7	(unassigned)	F	Reserved

2.2 Intradomain Multicast Protocols

There are some protocols needed that are used inside of a multicast domain to support multicasting.

2.2.1 Internet Group Management Protocol (IGMP)

For multicast to be more useful than broadcast it needs to be contained and distributed to the users that desire to receive the multicast stream. For IPv4 multicast the Internet Group Membership Protocol (IGMP) was created for this purpose. IGMP allows hosts to signal routers that they would like to receive a data stream. Routers in turn use IGMP to determine which interfaces to flood multicast packets to and which multicast groups are on which interfaces. At present there are three versions of this protocol, version 1 (RFC 1112), version 2 (RFC 2236) and version 3 (RFC 3376).

2.2.2 Multicast Listener Discovery (MLD)

IGMP cannot be used for IPv6 multicast. The protocol used within IPv6 to discover the presence of multicast listeners is Multicast Listener Discovery (MLD). MLD is derived from IGMPv2. MLD messages are ICMPv6 messages (protocol 58) defined by types 130, 131 and 132. All MLD messages are sent with a link-local IPv6 source address, an IPv6 hop limit of 1, and an IPv6 router alert option in a hop-by-hop options header.

The purpose of MLD is to enable each IPv6 router to discover the presence of multicast listeners on its directly attached links, and to discover specifically which multicast addresses are of interest to those neighbouring nodes. This information is then provided to whichever multicast routing protocol is being used by the router, in order to ensure that multicast packets are delivered to all links where there are interested receivers.

MLD is an asymmetric protocol, specifying different behaviour for multicast listeners and for routers. For those multicast addresses to which a router itself is listening, the router performs both parts of the protocol, including responding to its own messages. If a router has more than one interface to the same link, it needs to perform the router part of MLD over only one of those interfaces. Listeners, on the other hand, must perform the listener part of MLD on all interfaces from which an application or upper-layer protocol has requested reception of multicast packets. The MLD messages format is shown in figure 2.3.

8 bits	8 bits	16 bits	16 bits	16 bits
Type	Code	Checksum	Maximum Response Delay	Reserved
IPv6 multicast address				

Figure 2.3: MLD message format.

There are three types of MLD messages usually referred to as "Query", "Report", and "Done"

- Multicast Listener Query (Type = decimal 130)
- Multicast Listener Report (Type = decimal 131)
- Multicast Listener Done (Type = decimal 132)

The Code field is initialised to zero by the sender; ignored by receivers. The Checksum field is the standard ICMPv6 checksum, covering the entire MLD message plus a "pseudo-header" of IPv6 header fields. The Maximum Response Delay field is meaningful only in Query messages, and specifies the maximum allowed delay before sending a responding Report, in units of milliseconds. In all other messages, it is set to zero by the sender and ignored by receivers. The reserved field is initialised to zero by the sender; ignored by receivers.

The IPv6 Multicast Address in a Query message is set to zero when sending a General Query, and set to a specific IPv6 multicast address when sending a Multicast-Address-Specific Query. In a Report or Done message, this field holds a specific IPv6 multicast address to which the message sender is listening or is ceasing to listen, respectively. The length of a received MLD message is computed by taking the IPv6 Payload Length value and subtracting the length of any IPv6 extension headers present between the IPv6 header and the MLD message. If that length is greater than 24 octets, that indicates that there are other fields present beyond the fields described above, perhaps belonging to a future backwards-compatible version of MLD.

2.2.3 Multicast Listener Discovery Version 2 (MLDv2)

MLD Version 2 (MLDv2) is a translation of the IGMPv3 protocol [RFC 3376] for IPv6 semantics of the MLD protocol, when compared to the previous version, adds support for "source filtering", that is, the ability for a node to report interest in listening to packets only from specific source addresses, as required to support Source Specific Multicast (SSM), or from all but specific source addresses, sent to a particular multicast address. MLDv2 is designed to be interoperable with the previous version.

Multicast Listener Queries are sent by multicast routers to query the multicast listening state of neighbouring interfaces. Queries have the format shown in figure 2.4.

8 bits	8 bits	16 bits	16 bits	16 bits
Type	Code	Checksum	Maximum Response Delay	Reserved
IPv6 Multicast Address				
Resv | S | QRV	QQIC	Number of Sources	.. Source Addresses ..	

Figure 2.4: MLDv2 Queries message format.

Version 2 Multicast Listener Reports are sent by IP nodes to report (to neighbouring routers) the current multicast listening state, or changes in the multicast listening state, of their interfaces. Reports have the format shown in figure 2.5.

8 bits	8 bits	16 bits	16 bits	16 bits
Type	Reserved	Checksum	Reserved	Number of Multicast Address Records
Multicast Address Records				

Figure 2.5: MLDv2 Reports message format.

2.2.4 Protocol Independent Multicast

To setup multicast within a domain multicast routing needs to be setup. The most commonly used protocol for this is Protocol Independent Multicast (PIM). In general multicast routing protocols can be classified in dense or sparse protocols. Dense protocols use a broadcast mechanism to inform other routers of multicast sources. This simple approach is very efficient in environments with only a few active groups and most of the subnets contain interested listeners (densely populated domains). In situations when only few subnets contain interested listeners sparse protocols should be used. Sparse protocols forward multicast data only to routers that explicitly request it. Since sparsely distributed receivers are what is commonly seen on the Internet PIM-SM is the predominant multicast routing protocol.

There are two versions of PIM-SM, version 1 and version 2. PIM version 1 messages are IGMP messages (IP protocol 2) with IGMP version set to 1 and IGMP type set to 4. The IGMP Code field distinguishes the type of PIM messages. PIM version 2 messages use IP protocol 103. All routers on a subnet must use the same PIM version, but routers can have a mix of version 1 and version 2 interfaces. At this moment the most recent specification of the PIM-SM protocol is the Internet-Draft draft-ietf-pim-sm-v2-new-07.txt.

There are still a number of issues with PIM-SM, such as the open service model and the complex multicast address allocation. PIM-Source Specific Multicast (PIM-SSM) is a possible solution for some issues. In PIM-SSM multicast channels replace multicast groups. Only the source is able to transmit data on the channel. PIM-SSM doesn’t require a rendezvous point anymore. However, this model implies some important changes.

3. IPv6 multicast enabled networks.

There are at this moment at least two networks, which support IPv6 multicast. The WIDE 6bone and the M6Bone.

3.1 The WIDE 6bone

Probably one of the first implementations of IPv6 multicasting was done by KAME within the WIDE 6bone. PIM-SM was used as multicast routing protocol with two routers as RPs configured according to the geographical distribution of senders and receivers. Multicast applications that were used in the WIDE 6bone included multicast chatting, feeding audio and video streams, and remote lectures using multicasted Digital Video (DV) streams.

3.2 The M6Bone

The M6Bone is an experimental IPv6 Multicast network. The aim of this project is to offer an IPv6 multicast service to interested sites. This service is based on Renater3 (IPv6 enabled network), and benefits from the logistic support of the Aristote association, which is involved in the broadcasting of the ultra-modern technologies and of G6, a French group of IPv6 testers. The first goal is to develop an advanced service on IPv6, in order to participate in the promotion of the protocol. It enables the use of multicast videoconference tools on the network in order to broadcast events. Moreover, the M6Bone allows people who are connected to learn a lot about IPv6 multicast. IPv6 multicast is still an advanced function, and it is interesting that people could learn about it on a test network before using it on a production network.

3.2.1 6NET and the M6Bone

IPv6 multicast is one of the activities of the 6NET project. Many partners are involved in this activity and needed to perform tests using IPv6 multicast. As the 6NET core was not ready to support IPv6 multicast, all the partners involved agreed to join the M6Bone network to start the first IPv6 multicast experiments. Renater, leader of the M6Bone was in charge of connecting the different sites, creating a non-star IPv6 multicast backbone across Europe.

3.2.1.1 Global network topology (the IPv6 multicast paradox)

When the M6Bone started, it was necessary to face two constraints.

Very few routers implemented IPv6 multicast protocols. For this reason, it was needed to use a different topology for IPv6 multicast and IPv6 unicast.

Separate IPv6 multicast routing tables were not implemented. When an IPv6 multicast router receives a packet, it performs the Reverse Path Forwarding (RPF) check. The router checks whether or not the packet came from the interface where the source of the packet is seen in the routing table. If the IPv6 unicast and multicast topologies are not the same, the IPv6 multicast routing protocol performs the RPF check using the multicast routing table. As this is not yet implemented, the RPF checks are performed using the IPv6 unicast routing table. For this reason, it was needed to have the same topology for IPv6 multicast and IPv6 unicast.

The solution to these constraints is to use dedicated equipment for IPv6 multicast. The equipment is linked using IPv6 multicast over IPv6-in-IPv6 unicast tunnels or IPv6 multicast over IPv6-in-IPv4 unicast tunnels. This equipment is never used to route any unicast traffic.

3.2.1.2 The Multicast topology

The M6Bone network is a unique Protocol-Independent Multicast (PIM) domain, all the routers running PIM Sparse Mode protocol. Renater manages the RP with the highest priority. It also acts as the Bootstrap Router (BSR) for the domain.

Most of the M6Bone routers are PCs with BSD OS and the IPv6 KAME stack. This stack includes the pim6dd and pim6sd daemons, corresponding to PIM Dense Mode and PIM Sparse Mode protocols. The latest versions make it possible to have IPv6 multicast routers running PIM SM and PIM SSM at the same time (managing the MLDv2 and MLDv1 compatibility). The deployment of PIM SSM in the M6Bone is foreseen.

Also, the scope field in the IPv6 multicast address can be used to have different RPs for different administrative scopes. A deployment of different RPs in different parts of the M6Bone is also studied.

At this moment there is work going on regarding the PIM-SM daemon (for FreeBSD) to provide

- Compatibility between MLDv1 and MLDv2 (and what to do in presence of MLDv1-only hosts for example).
- Full processing of MLDv2 (include and exclude modes) and interaction with PIM-SM (with ASM addresses, the case of SSM is simple in that case)

This should show up in KAME stack really soon now.

3.2.1.3 The Unicast topology

3.2.1.3.1 IPv6 tunnels and routing

PIM is a protocol that uses the unicast routing table for the RPF check. It implies that unicast and multicast topologies must be the same. This is not the case since the M6Bone is an overlay network. A solution to this problem is to use a multicast routing table but this is not yet implemented on most IPv6 multicast routing equipment. Then a hack is used to overcome this problem. All the sites have to use separate routers for unicast and multicast. The IPv6 multicast tunnels are set up between IPv6 multicast routers. Those routers exchange their unicast routing table that will be used for the RPF check using the RIPng protocol. With RIPng, each site advertises its prefix corresponding to the subnet where IPv6 multicast is enabled through the tunnels.

3.2.1.3.2 IPv6 in IPv6 tunnel issue

A problem can occur when setting up an IPv6-in-IPv6 tunnel. In order to set up the tunnel, it is needed to reach the destination of the tunnel via the unicast network. It is needed to be sure that the address of the tunnel end point is not included in a prefix advertised on the M6Bone. If this is the case (topology choice) it is needed to specify a static route to the tunnel end-point through the unicast network. Note that it is not possible with this solution to run multicast applications on the multicast routers.

3.2.1.3.3 Routing policy

The routing policy makes it possible to advertise in the M6Bone only the prefixes used in the M6Bone. So, each site has to decide which prefix(es) (usually /64) will be used in the M6Bone. All the unknown prefixes are filtered on the RP. This is done to avoid having less experienced sites advertising their entire IPv6 unicast routing table in the M6Bone.

3.2.2 Connected sites

It is important to note that not all the sites of the M6Bone are part of the 6NET project (around half of these sites are 6NET partners). As there is no interdomain multicast routing protocol available, the deployment of IPv6 multicast in 6NET core will divide the IPv6 multicast network into two Parts. Maybe this situation is necessary to show that there is a real need for an IPv6 multicast interdomain protocol.

Another solution that could permit to have two networks is to use a hierarchy of RPs and BSR filtering. This solution would make it possible to segment the network and have parts with different RPs. The 6NET RP would be the RP for the scope eight (organisation scope) and the M6Bone RP would remain the RP for scope E (global scope). The deployment of such a solution is actually foreseen by Renater (managing the M6Bone RP).

Table 3.1: Connected 6NET Partners to the M6Bone.

6NET Site	Location
CNR-IIT	Italy
CSC/FUNET	Finland
Dante, Cambridge	UK
ETRI	Korea
Oulu Polytechnic	Finland
Poznan Supercomputing and Networking Center	Poland
RENATER	France
SURFnet	The Netherlands
UNINETT	Norway
University College of London	UK
Université Libre de Bruxelles	Belgium
Université Louis Pasteur, Strasbourg	France
University of Southampton	UK
Vienna university	Austria

Table 3.2: Other sites connected to the M6Bone.

Non 6NET Site	Location
Association Aristote	Paris (France)
ASTO	Philippines
CINES	Montpellier (France)
Consulintel	Madrid (Spain)
DESS ART	Paris (France)
ESMT/UCAD	Dakar (Senegal)
INRETS	Paris (France)
IRISA/INRIA	Rennes (France)
LIP6	Paris (France)
NCKU	Taiwan
PT inovacao	Portugal
Showroom ENST	Paris (France)
Universidad Carlos III	Madrid (Spain)
Universidad de Guadalajara	Mexico
Universidad de Murcia	Spain
Université de Bretagne sud	Vannes (France)

Figures 3.1 (world), 3.2 (Europe) and 3.3 (France) show maps of the M6Bone network.

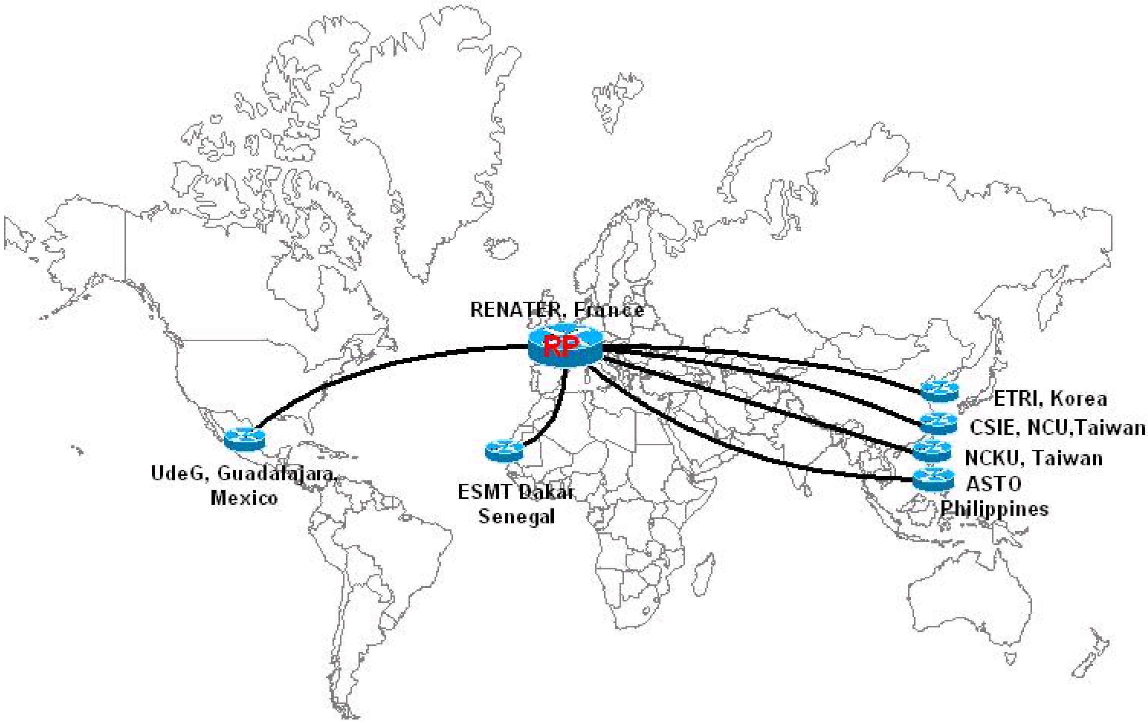


Figure 3.1: World map of the M6Bone.

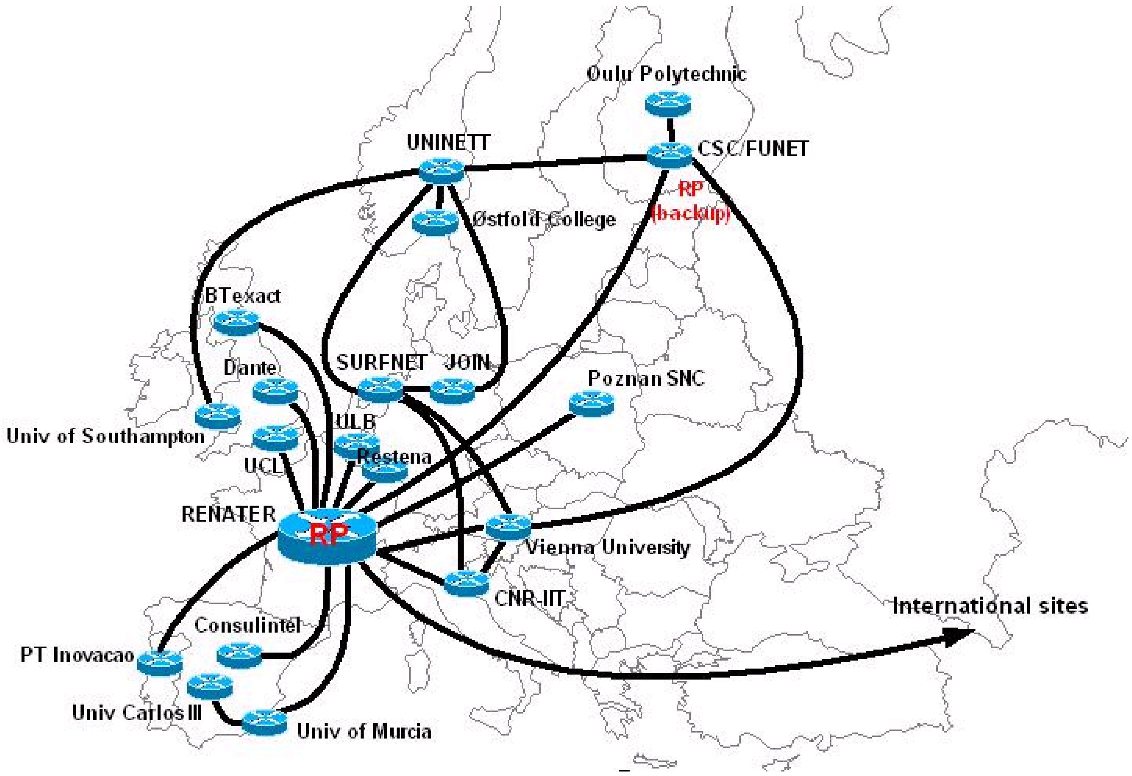


Figure 3.2 European map of the M6Bone.

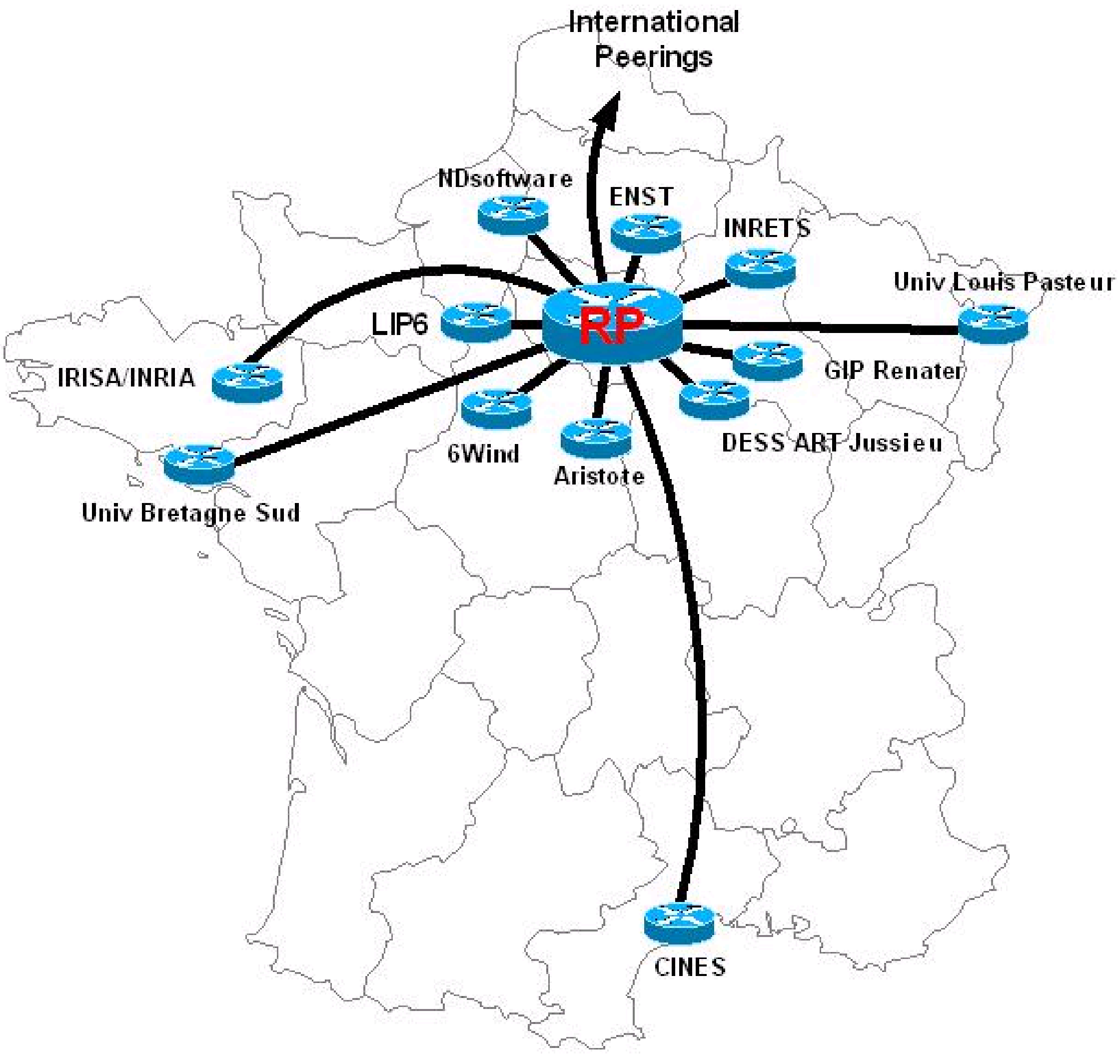


Figure 3.3: French map of the M6Bone.

3.2.3 Services deployed

A number of services such as a looking glass and reflectors are deployed within the M6Bone. This section describes some of the tests (large scale deployment of the MBone tools) and services over the M6Bone.

3.2.3.1 Videoconferencing tools

Table 3.3 is summary compiled at the beginning of November of people visiting "6NET People" session using the MBone tools such as VIC and RAT.

Table 3.3: Participants "6NET People" session.

Name	Site	VIC	RAT	NTE
Wim Biemolt	SURFnet	S*	+*	
Stig Venaas	UNINETT	S#	+#	+
Njål Borch	Invenia, Tromsø	S*	+*	
Pekka Savola	CSC/FUNET	R	+*	
Konstantin Kabassanov	LIP6	S	+	+
Trond Skjesol	UNINETT	X	+	+
Jukka Orajarvi	Oulu Poly	S	+	+
Roland Staring	SURFnet	X*		
Hans Zandbelt	TELIN	S*	+	
Jac Kloots	SURFnet	S*		
Niels den Otter	SURFnet	S*		
Tomasz Szewcsyk	PSNC	S*	+	+
Tim Chown	IST2002	S*		
Jerome Durand	Renater	S	+	
Guido Wessendorf	UniMünster	R*		
CoffeeRoom	ULP/LSIIT	S	+	+
Tina Strauf	UniMünster/JOIN	#		
Cristian Schild	UniMünster/JOIN	S#		
Alexander Gall	SWITCH	S*		
Roger Clot	CICG	+		
Kurt Bauer	ACOnet	R*		
Julien Ridoux	LIP6	#		
Andre Vink		#		
Andre Stolze	UniMünster/JOIN	*		
Ahmed Sahnoun	Renater	S		
Gabi		X		
Pawel Wiatr	KTH/SE	S*		
Lorenzo Rossi	iit.cnr.it	S		
Antonio Pinizzotto	iit.cnr.it	R		
Otto Kreiter	RoEDUNet	+*	+	

*=Via reflector, #=Via 4/6 reflector, R=Receive only, S=Send-camera/receive, X=Send-x11/receive

3.2.3.2 Pseudo looking glass

It is possible to see some useful data on the RP for debugging purposes. Everything is available through a web interface (the RP sends data to the web server periodically) The web page is located at http://supervision.m6bone.net. On this web page, the user can see

- The states of the links directly connected to the RP
- The unicast routing table
- The virtual multicast routing table
- A link to the beacon server web page

This is a first set of facilities that has been deployed. More will come during the project.

3.2.3.3 Reflectors

In the IPv4 multicast world, reflectors have been around for a long time. The idea is generally to receive multicast and send it out again as multiple unicast streams, so that people without multicast connectivity can receive the data. Reflectors are often bidirectional, which means that one can also send unicast to the reflector, and have it forwarded to the multicast group as well as all other unicast participants. In this way one can have say a video conference where people can take part using either multicast or unicast on equal terms.

For IPv6 it is very useful to have something similar since IPv6 multicast deployment is still in its infancy. One would also like to have some interaction with IPv4, a reflector for IPv4 or IPv6 multicast could support both IPv4 and IPv6 unicast streams at the same time independent of which IP protocol the multicast uses. One might also reflect between IPv4 multicast and IPv6 multicast.

In the 6NET project we have experimented with reflectors that are bidirectional and also support most combinations of IPv4 and IPv6, and unicast and multicast. They can all be found at http://www.kabassanov.com/reflectors/. Many reflectors require static configuration or out of band signalling to initiate or stop streaming for each unicast address (participant). This can be problematic since it places an extra burden on users; they need to either do some manual tasks to control the stream, or may need to install special software to handle e.g. RTSP. The reflectors from Kabassanov however rely on the unicast participants to regularly send data. This means that they can only work with some applications, they do however work with popular MBone tools like VIC, RAT and NTE since they regularly send RTCP reports or other membership information. This means that a user can start e.g. VIC with just unicast IP address of the reflector and a specific port number (the address and port number are the same for all participants), VIC will like other RTP/RTCP applications use two ports, one for RTP and the port right above for RTCP. When VIC is started, it will send to the RTCP port. The reflector monitors both the ports, and when it receives a packet on one of them, it knows that a new unicast receiver is present and will start forwarding packets on both ports. Every five minutes it checks whether any unicast packets are received; if nothing is received, unicast forwarding will stop. RTCP applications like VIC send reports much more frequently, so in effect the reflector will send until a few minutes after VIC is stopped or there is a network failure.

3.2.3.4 IPv6 multicast - IPv6 unicast reflector

This is the reflector we have used most of the time. For each group and port number to reflect one runs one reflector process, specifying group, multicast port number and unicast port number. Note that for RTP/RTCP applications one only specifies the RTP port. Anyone that wants to take part, both sending and receiving, can start VIC, RAT and other applications supplying the unicast address and port as parameters. The main use for this is for people without multicast to take part in conferences together with those that have multicast, or simply to receive video and audio transmissions from some happening that is being broadcast by multicast. It has also been very useful for sending transmissions from e.g. conferencing venues where no IPv6 multicast is available. One can then send unicast to the reflector and the reflector resends it as multicast. Note that in all these cases one uses the same software. The reflector basically has a number of "links", one multicast link and a varying number of unicast links; any time data is received on one link, it is resent on all the others.

The reflectors have also turned out to be useful for debugging. They are a bit like a looking glass, by connecting to a reflector using unicast; you can see what is received by multicast at the site where the reflector is located. By comparing what oneself receives with what is received at another site one can determine whether multicast reception problems are local or not. One could possibly have multiple sites running reflectors for some specific sessions simply to do debugging. It might be better to use multicast beacons for debugging though.

3.2.3.5 IPv6 multicast to IPv4 multicast reflector

We have also used a reflector for this. One could also call this a gateway perhaps. One specifies an IPv4 multicast group and a port number, and also an IPv6 multicast group and port number. For RTP/RTCP one only specifies the RTP port. The reflector joins both groups and listens on the respective ports. Any data received from one group is resent to the other. This is useful for injecting existing IPv4 multicast sessions into the IPv6 world, but also for IPv6 multicast sessions to be injected into IPv4. This might also be useful in transition where IPv4 and IPv6 will coexist for a long time but some networks, hosts or applications might only support one of the protocols. It is also currently used for one of the 6NET applications in WP5 (Trondheim Underground Radio) to send IPv6 multicast, because one could not find a satisfactory tool for streaming both IPv4 and IPv6 multicast directly. So the solution was to stream IPv4 multicast as before and use this reflector to send IPv6 multicast.

3.2.3.6 Monitoring of the multicast transmission parameters - Beacon

At the beginning of the multicast traffic tests it must be decided what parameters are the most relevant to monitor. It is crucial to know the state of the multicast enabled network and subsequently react to particular situations (special transmissions, faults, hacker attacks).

The basic parameters with definitions are listed below.

- Delay

Delay in sense of „one-way-delay" is intuitively defined as the time between a node sending a message and receipt of the message by another node. It is the sum of two parts:

- The time needed by the first bit of the packet to travel from the source to the destination. It is a function of the physical distance, of the number of network devices along the path and instantaneous network load. It is defined in RFC 2330 as „propagation time of a link"
- The time needed to transmit all the bits of the frame, which is a function of the transmission speed of a line.

With software we can directly measure the time between when the source host grabs a time stamp just prior to sending the test packet and when the destination host grabs a time stamp just after having received the test packet.

- Jitter

Jitter is an aberration that occurs when video or voice is transmitted over a network, and packets do not reach its destination in the consecutive order or on a timely basis, i.e. they vary in latency. The distortion of a signal as it is propagated through the network, where the signal varies from its original reference timing is a distortion of the interpacket arrival times compared to the times of the original transmission, and is particularly damaging to the multimedia traffic.[1]

- Packet loss

The packet loss is the number of packets sent but not received at the destination or received with errors. It is a function of instantaneous network load, equipment configuration, its transmission error rate and failure. Measurement of it is detailed in RFC 2680.

- Packet duplication

IP networks tend to have complex topologies with alternate paths built in for redundancy. The packet duplication occurs when there are alternative paths in a network or routing loops. Because many multicast applications are data intense, the packet duplication is a significant disadvantage of the subnet broadcast.[2]

---

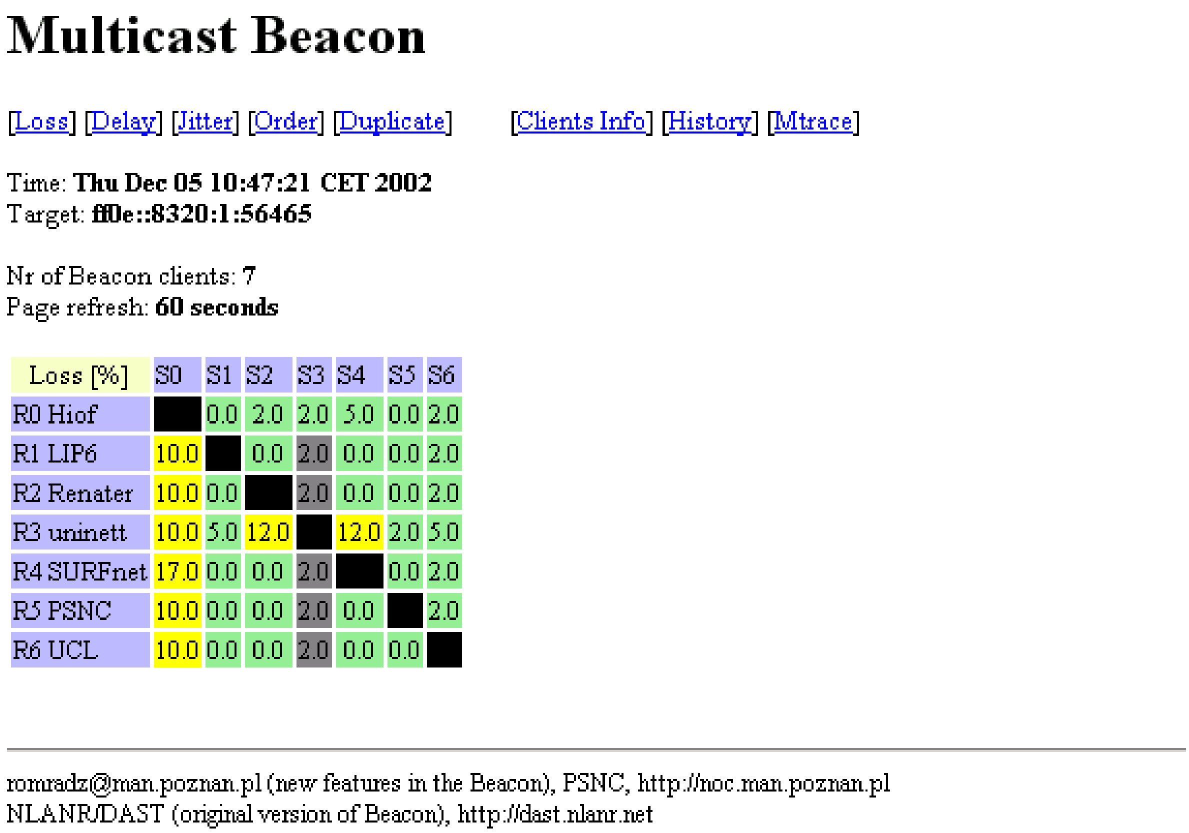
[1] IP QoS FAQ (draft version 0.7) http://www.qosforum.com/docs/faq

[2] Troubleshooting TCP/IP.http://www.cisco.com/univercd/cc/td/doc/cisntwk/itg_v1/tr1907.htm

A Multicast Beacon is the application for monitoring the parameters of multicast traffic. These parameters (discussed earlier) are:

- Loss
- Delay
- Jitter
- Duplicate
- Order

The application consists of two parts: a server and clients. The role of the server is collecting information received from clients and presenting them by means of a stand-alone GUI tool or HTTP interface. The second approach is very usable for a large number of users interested in the collected results. They can observe the parameters via a web browser, like Internet Explorer or Netscape Navigator.



Multicast Beacon

[Loss] [Delay] [Jitter] [Order] [Duplicate]   [Clients Info] [History] [Mtrace]

Time: **Thu Dec 05 10:47:21 CET 2002**
Target: **ff0e::8320:1:56465**

Nr of Beacon clients: **7**
Page refresh: **60 seconds**

Loss [%]	S0	S1	S2	S3	S4	S5	S6
R0 Hiof		0.0	2.0	2.0	5.0	0.0	2.0
R1 LIP6	10.0		0.0	2.0	0.0	0.0	2.0
R2 Renater	10.0	0.0		2.0	0.0	0.0	2.0
R3 uninett	10.0	5.0	12.0		12.0	2.0	5.0
R4 SURFnet	17.0	0.0	0.0	2.0		0.0	2.0
R5 PSNC	10.0	0.0	0.0	2.0	0.0		2.0
R6 UCL	10.0	0.0	0.0	2.0	0.0	0.0	

romradz@man.poznan.pl (new features in the Beacon), PSNC, http://noc.man.poznan.pl
NLANR/DAST (original version of Beacon), http://dast.nlanr.net

Figure 3.4: Multicast Beacon main page

The clients exchange packets using the multicast technology and this way they can easily determine values of traffic. The clients send such information to the server. To have a matrix of states of multicast traffic between some locations, the beacon administrator can locate the clients there and in the central place deploy the server, which would be the interface for a user. The original version of the Multicast Beacon was developed in the National Laboratory for Applied Network Research

(NLANR) in the USA.[3] Some new additional features (like storing statistics, a message module and the mtrace module) were introduced by the Poznan Supercomputing & Networking Center (PSNC) in Poland. The application is the open source initiative, developed in Java language, an operating system independent language that is IPv6 enabled (using jsdk version 1.4).

Multicast Beacon

[Loss] [Delay] [Jitter] [Order] [Duplicate]   [Clients Info] [History] [Mtrace]

Time: **Thu Dec 05 11:06:29 CET 2002**
Target: **ff0e::8320:1:56465**

Table of beacon clients

Beacon	IP	OS	Version	Arch	Java	Refreshed
R0 Hiof	eth0: 2001:700:a00:5:0:0:0:3, fe80:0:0:0:202:b3ff:fe88:b34d, eth1: fe80:0:0:0:202:b3ff:fe4c:5113, 192.168.1.100,	Linux	2.4.18-3	i386	1.4.1_01	Yes
R1 LIP6	eth0: 2001:660:10c:3d:250:fcff:fe0b:9966, fe80:0:0:0:250:fcff:fe0b:9966, 132.227.72.148,	Linux	2.4.18-14	i386	1.4.0_02	Yes
R2 Renater	eth0: 2001:660:10a:4002:260:8ff:fe49:2d8, fe80:0:0:0:260:8ff:fe49:2d8, 193.49.160.200,	Linux	2.4.18-14	i386	1.4.1_01	Yes
R3 uninett	eth0: 2001:700:1:0:290:27ff:fe22:7186, fe80:0:0:0:290:27ff:fe22:7186, 158.38.62.80,	Linux	2.4.18-3	i386	1.4.1_01	Yes
R4 SURFnet	eth0: 3ffe:666:3ffe:666:2c0:4fff:fea4:d53f, fe80:0:0:0:2c0:4fff:fea4:d53f, 192.87.110.163,	Linux	2.4.18-3	i386	1.4.1	Yes
R5 PSNC	eth0: 3ffe:8320:5:101:210:4bff:fe91:9120, fe80:0:0:0:210:4bff:fe91:9120, 150.254.162.225,	Linux	2.4.18-3	i386	1.4.0	Yes
R6 UCL	eth0: fe80:0:0:0:250:daff:fe38:cab5, 3ffe:2101:7:4:250:daff:fe38:cab5, 128.16.64.165,	Linux	2.4.18-14	i386	1.4.1_01	Yes

romradz@man.poznan.pl (new features in the Beacon), PSNC, http://noc.man.poznan.pl
NLANR/DAST (original version of Beacon), http://dast.nlanr.net

Figure 3.5: Beacon client's info

Some new features added to beacon in PSNC are still in development phase. The "History" feature allows now to collect all parameters in *.res files, but the chart generation must be improved. Currently this option is disabled because server goes down during chart generation when too many data is collected from beacon clients.

[3] Multicast Beacon Application http://dast.nlanr.net/projects/beacon/

3.2.4 Experience gained through M6Bone

The first thing we learnt is that to build an IPv6 multicast network can be done but that it is not possible to link two multicast domains because no interdomain protocols are available. We also learnt that it was necessary to use different equipment for unicast and multicast because of the lack of separate IPv6 multicast routing tables.

3.2.5 Future work and Issues

The work foreseen regarding IPv6 multicast for the next months is:

- Deploy PIM SSM on the M6Bone
- Deploy different RPs with BSR filtering and manage some administrative scopes

The big issues with respect to IPv6 multicast at the moment are:

- The lack of any IPv6 multicast interdomain protocol
- The lack of IPv6 multicast routing tables

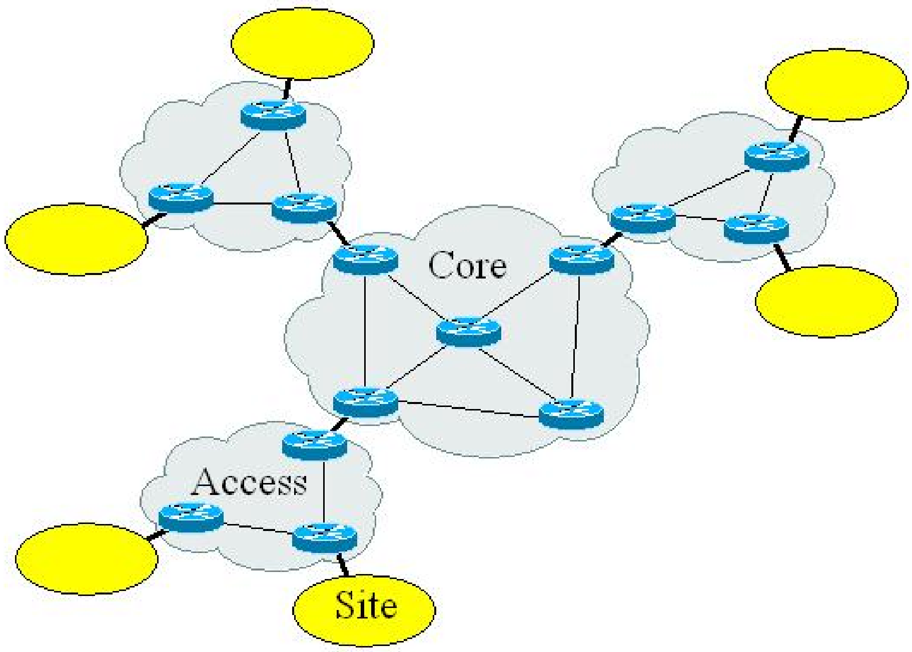


Figure 3.6: Topology of 6NET network (Core, Access and Site)

Figure 3.6 represents in a schematic way the current topology of the 6NET network. It involves basically three components: core, access (NRENs) and sites. The IPv6 multicast clients which are located in the sites use at this moment M6Bone tunnels for their IPv6 multicast connectivity. From this figure it can be seen that IPv6 multicast can be deployed in the core if there are clients directly connected to the core. Or by deploying clients in the sites while bypassing the NRENs, which do not support IPv6 multicast at this moment, using tunnelling techniques such as MPLS or dedicated circuits based on for example ATM. Using manual configured tunnels on the Cisco 12000, series routers which are widely used within 6NET, is probably not a good option to bypass the NREN network[4]. In any case a separate IPv6 multicast routing table is needed because the unicast and multicast topologies are not the same. This constraint is not PIM-SM specific, as all multicast routing protocols must perform the RPF check.

The deployment of IPv6 multicast in the core cannot be done at this moment. It is needed to start validating the latest EFT images for IPv6 multicast provided by Cisco on some sites and to gain experience with these new images. The EFT image should have at least the following features

- IPv6 multicast routing tables (for example MBGP support)
- PIM-SM, PIM SSM
- MLDv1, MLDv2

Also this EFT image would probably make it possible to test some security aspects of IPv6 multicast (e.g. DoS attacks...).

Figure 3.7 represents the next step in IPv6 multicast deployment within 6NET. This figure shows that while building a dedicated IPv6 multicast domain for 6NET (the M6Net) we need to maintain IPv6 connectivity with the M6Bone. The sites will now use the same equipment for unicast and multicast and validate that it is possible to have both functions on the same routing equipment without major impacts on the features, which are currently supported. When the tested images are approved by the partners involved in the IPv6 multicast activity, then the deployment in the core can be done, keeping in mind that this has an interest only if at least one NREN has deployed IPv6 multicast in some part of its network or has at least clients directly connected to the 6NET core.

Some access networks, like NORDUNETT, SURFnet and UNINETT, are volunteer to deploy an image with IPv6 multicast in (parts of) their network as soon as some tests proofed that images with IPv6 multicast support have no impact on the other features used within the network.

[4] Since Cisco IOS Release 12.0(23)S, the Cisco 12000 series should provide enhanced performance for IPv6 manually configured tunnels by processing traffic on the linecard. In previous releases, traffic destined for or received from an IPv6 manually configured tunnel would be given a very low priority by the RP. Therefore, for the releases before 12.0(23)S, the use of IPv6 tunnels should be avoided.

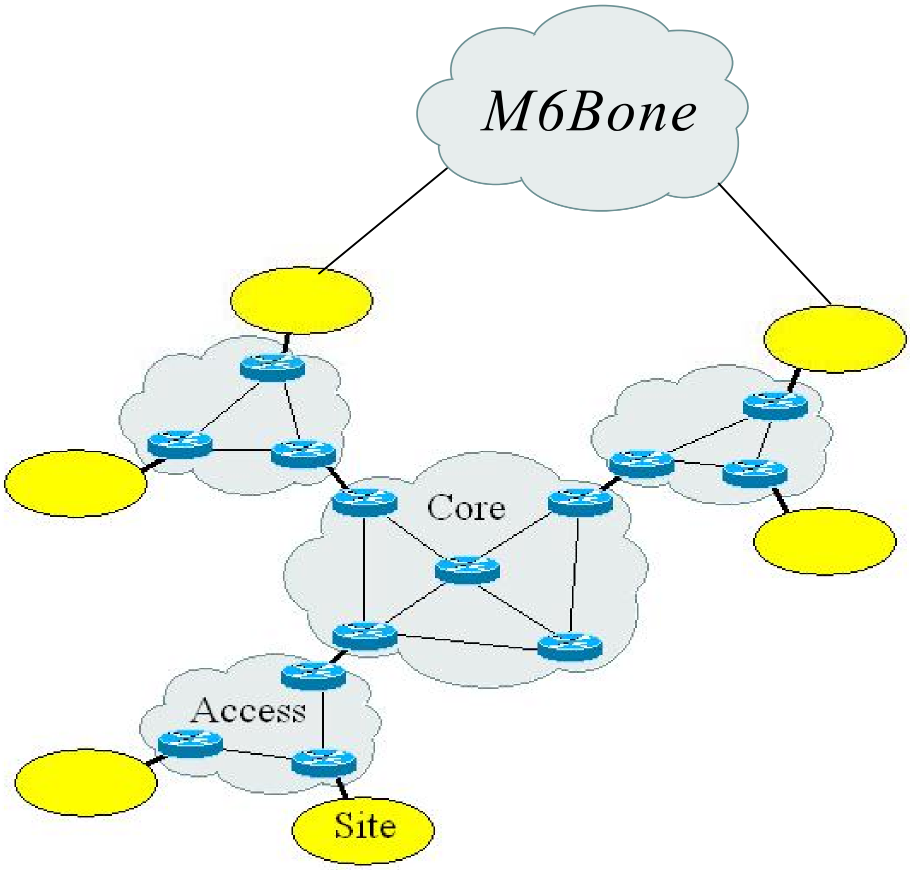


Figure 3.7: Future IPv6 multicast deployment

3.3 IPv6 multicast between 6NET and Euro6IX

This section describes the plans for collaboration between 6NET and Euro6IX for IPv6 multicast; the plans are also reported in Euro6IX Deliverable D4.1A.

The Euro6IX project is seeking to build its own IPv6 multicast infrastructure. However, the lack of availability of PIM-SM or PIM-SSM support across the Euro6IX network at this stage of the project means that IPv6 multicast connectivity, as is often the case with IPv4, has to be provisioned through unicast tunnels, either IPv6 multicast in IPv4 unicast or in IPv6 unicast tunnels.

UoS is jointly a participant in Euro6IX and 6NET. The bulk of its IPv6 multicast work is being carried out in the 6NET project, but it is also relevant to Euro6IX due to UoS' unique participant situation. Joint collaborative activities have been defined in Deliverable 7.9 of Euro6IX, which is also reported as Deliverable D5.3 of the 6NET project. One such joint activity is IPv6 multicast.

It is thus highly desirable to establish IPv6 multicast connectivity between the Euro6IX and 6NET partners. Currently 6NET also has no native IPv6 multicast connectivity on its backbone network because no PIM-SM images are yet available for the Cisco GSR routers (it is on their roadmap for 2003). As a result, the M6Bone network, an IPv6 multicast network that originated in Paris, from Renater3, and that has evolved since 2001 with discussion in the TERENA task force TF-NGN working groups, seems an ideal vehicle for IPv6 multicast experiments until native multicast becomes available in each project.

The M6Bone has over 35 participants, and during 2002 partners have joined the network from both the 6NET and Euro6IX projects. It is described in more detail elsewhere in this deliverable. The 6NET participants include UoS, UCL, DANTE, ULB, JOIN, UNINETT and CSC/FUNET, while Euro6IX partners include Consulintel and the University of Murcia.

There is a single PIM-SM RP in Paris managed by Renater; there is as yet no method in IPv6 for interdomain PIM-SM to operate through multiple RPs (MSDP exists for IPv4, but is a “stop-gap” measure that is not likely to be taken forward to IPv6, while BGMP is still also in its implementation infancy). It is possible that PIM-SSM may become the way forward for multicast services in IPv6.

The M6Bone is used for a variety of multicast applications including:

- VIC and RAT for videoconferencing (Linux, BSD and Windows clients)
- NTE whiteboard sharing
- VideoLAN and other video streaming
- Icecast, CRadio and other MP3 streaming (including Trondheim Underground Radio)

Many of the French Aristote association seminars are transmitted on the M6Bone.

4. Snap shot IPv6 multicast configuration at 6NET partners

This section describes briefly the experience and setup of the various 6NET Partners to connect to the M6Bone and deploy IPv6 multicast connectivity within some parts of their network. It also presents the IPv6 multicast setup used during the IST 2002 conference in Copenhagen in November 2002.

4.1 IPv6 Multicast experiments at ACOnet (Austria)

ACOnet uses a FreeBSD box as its multicast router. This box has various tunnelled connections, of which the ones to Renater (France), SURFnet (Netherlands) and CSC/FUNET (Finland) are IPv6-in-IPv6 tunnels; the one to CNR-IIT (Italy) is an IPv6-in-IPv4 tunnel. The router has two Ethernet-connections to our IPv6-world, which is further distributed via VLANs throughout our whole network. As end-systems we mainly use Linux, but also Windows XP, FreeBSD and Solaris were tested.

4.2 IPv6 Multicast experiments at CNR-IIT, Pisa (Italy)

The CNR-IIT activity regarding IPv6 multicast, until now, has focused on the following points:

- Deployment of an IPv6 multicast network using the existing implementations FreeBSD/KAME PIM-SM;
- Testing intradomain IPv6 multicast;
- Running multicast applications.

The most part of the work in progress comes from the involvement of CNR-IIT in Renater M6Bone test network project using FreeBSD based IPv6 multicast routers (m6router).

Concerning the topology, the point-to-point links with the other mrouters are IPv6 in IPv4 tunnels. As shown in the figure 4.1, at the moment there are tunnels to Renater (France), SURFnet (the Netherlands) and Vienna University Computer Center (Austria). These tunnels are still IPv6 in IPv4 because of the bottleneck in the link between the 6NET PoP in Pisa and the GARR 6NET PoP in Milan, a 2 Mbps ATM PVC. Using IPv6 in IPv6 tunnels on 6NET network could be a problem because the multicast data flow through the CNR-IIT m6router is the sum of the traffic triggered by local hosts (transmitted and received streams) and the transit traffic among the other hosts on M6Bone. The overall traffic of IPv6 in IPv4 tunnels can have peaks up to 3-4 Mbps.

The routing protocols used on tunnels and running on FreeBSD are

- Unicast: RIPng (“route6d daemon”);
- Multicast: IPv6 PIM Sparse-Mode (“pim6sd daemon”).

The following MBone tools, compiled for IPv6 by Konstantin Kabassanov, were tested on Windows XP/2k platform: SDR, VIC, RAT and NTE; some of them, SDR and VIC, have been tested on FreeBSD as well. Multicast video streams were delivered up to 1.5 Mbps with a good quality at the receivers.

As a next step Cisco PIM-SM implementation (EFT IOS) will be setup to interoperate with the FreeBSD one, in the same PIM domain. PIM SSM implementation will be tested on FreeBSD m6router as well. Figure 4.1 shows the IPv6 multicast setup of CNR-IIT.

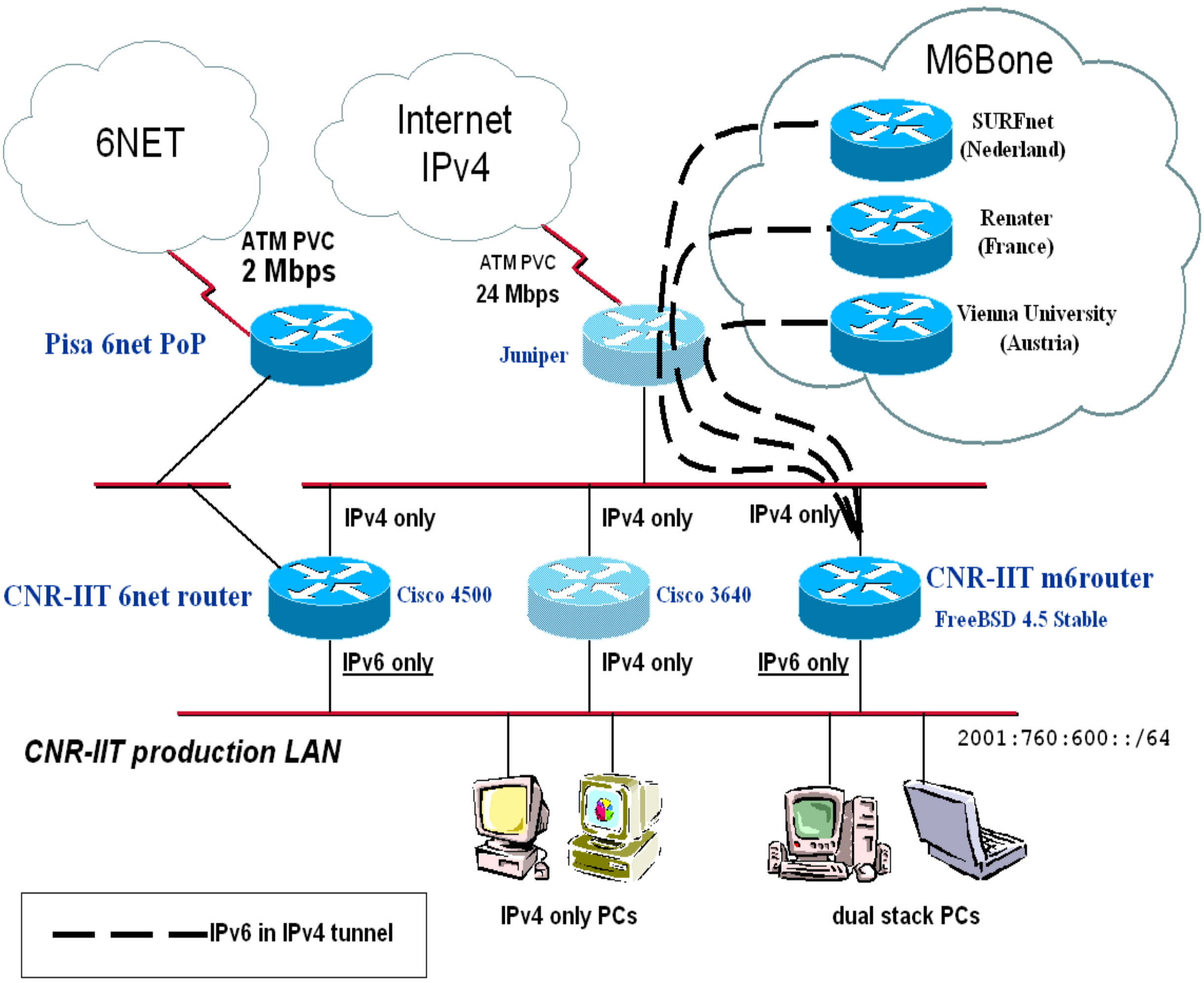


Figure 4.1: IPv6 multicast service at CNR-IIT.

4.3 IPv6 Multicast experiments at Renater (France)

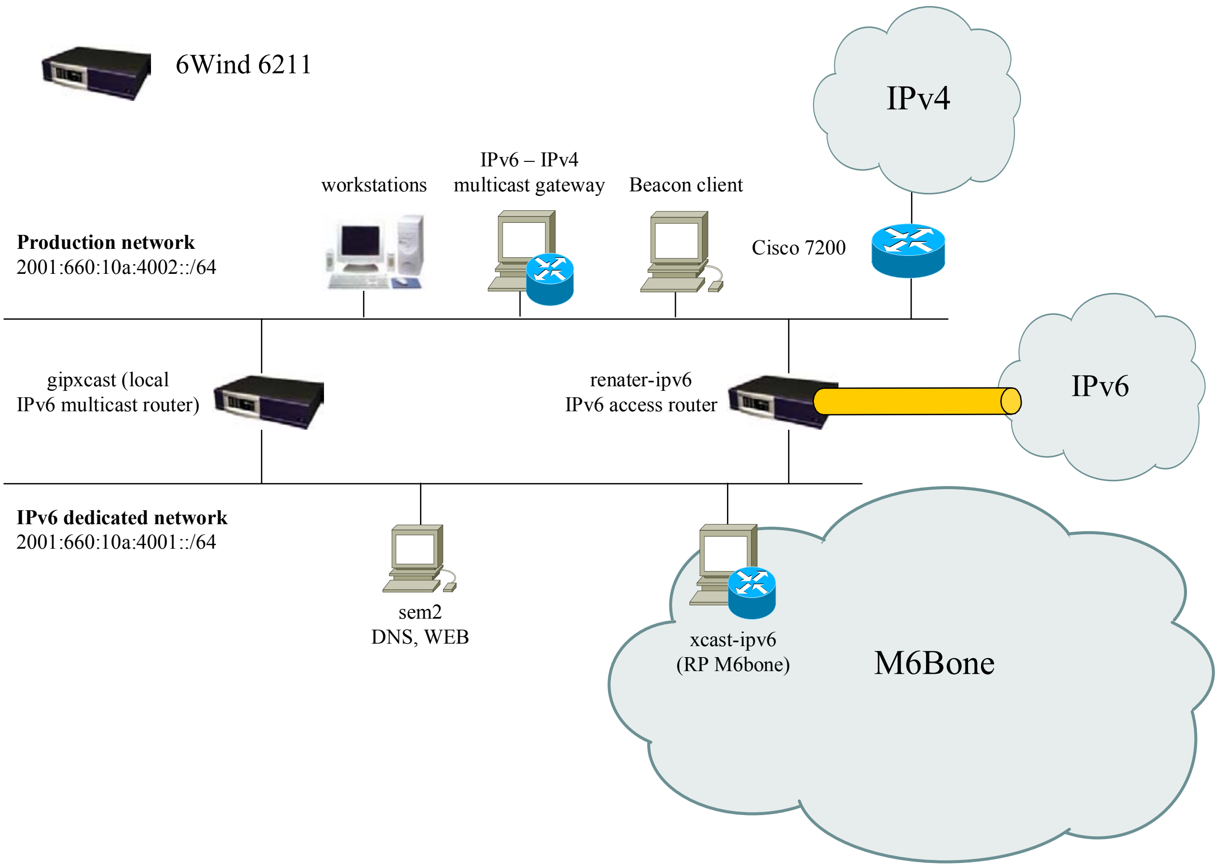


Figure 4.2: IPv6 multicast service at Renater.

Renater's network is basically divided in two networks. All the workstations are on the same Ethernet link. Because no MLD snooping was available at that time, it was not possible to have the M6Bone RP (that generates around 4 Mbps) on the production link. We decided to segment the network and have some IPv6 dedicated equipment (like reverse DNS for Renater's zone, and the M6Bone RP) on another link.

As it is not possible (because of the lack of IPv6 multicast routing tables) to use the IPv6 access router for multicast, we use two different routers for each purpose.

All the workstations on the production network can have IPv6 multicast connectivity, without any impact on IPv6 unicast (being routed via renater-IPv6 router) This makes it possible for any employee to have the MBone tools installed and do IPv6 multicast videoconferences.

An IPv6 - IPv4 multicast gateway was installed. Luc Beurton from the University of South Brittany provided the source code. It has to be on the production link as there is no IPv4 multicast connectivity on the IPv6 dedicated network. This is an issue because the production networks gets loaded every time we use the gateway.

An IPv6 beacon client was deployed, and sends its statistics periodically to the beacon server beaconserver.m6bone.pl. This makes it possible to know the delay, the loss ratio, and other interesting features with all the sites that deployed their own beacon.

GIP Renater has a native connection the RP managed by Renater. The sites shown in table 4.1 are connected using IPv6-in-IPv6 or IPv6-in-IPv4 tunnels.

Table 4.1: Sites connected to Renater.

	IPv6 in IPv6 tunnels		IPv6 in IPv4 tunnels
1	LIP6, Paris, (France)	20	DESS ART Jussieu, Paris
2	Université Libre de Bruxelles	21	INRETS, France
3	ETRI, (Korea)	22	DANTE, Cambridge
4	Université de Bretagne Sud, Vannes, (France)	23	CNR-IIT, Italy
5	Université Louis Pasteur, Strasbourg	24	UG, Guadalajara, Mexico
6	University College of London		
7	ESMT, Dakar, (Senegal)		
8	Vienna University Computer Center, (Austria)		
9	CINES, Montpellier		
10	Poznan Supercomputing and Networking center		
11	CSC/FUNET, (Finland)		
12	Showroom ENST Paris		
13	IRISA/INRIA, Rennes, (France)		
14	NCKU, (Taiwan)		
15	University of Murcia, (Spain)		
16	ASTO, Quezon, (Philippines)		
17	Consulintel, Madrid (Spain)		
18	PT inovacao, Aveiro (Portugal)		

The numbers before the sites are the tunnel numbers (gif interfaces on the BSD)

The prefix 2001:660:10a:6000::/52 is dedicated to M6Bone. The tunnels are numbered in the prefixes

- 2001:660:10a:6400::/56 for IPv6-in-IPv4 tunnels
- 2001:660:10a:6600::/56 for IPv6-in-IPv6 tunnels
- 2001:660:10a:6800::/56 for test tunnels

4.4 IPv6 Multicast experiments at SURFnet (the Netherlands)

Figure 4.3 below shows the set-up for testing IPv6 multicast at SURFnet. SURFnet is using a server with FreeBSD 4.7 as the central IPv6 multicast router with IPv6-in-IPv4 and IPv6-in-IPv6 tunnels to other partners connected to the M6Bone (see also Table 4.2). On the FreeBSD router route6d (RIPng) is used together with pim6sd (20021111a). Since the latest Cisco IOS IPv6 multicast EFT images (from the beginning of august 2002) doesn't handle IPv6-in-IPv6 tunnels properly yet the Cisco 3620 router parallel with the FreeBSD router isn't used for IPv6 multicasting at this moment. It was only used for IPv6 unicast connectivity.

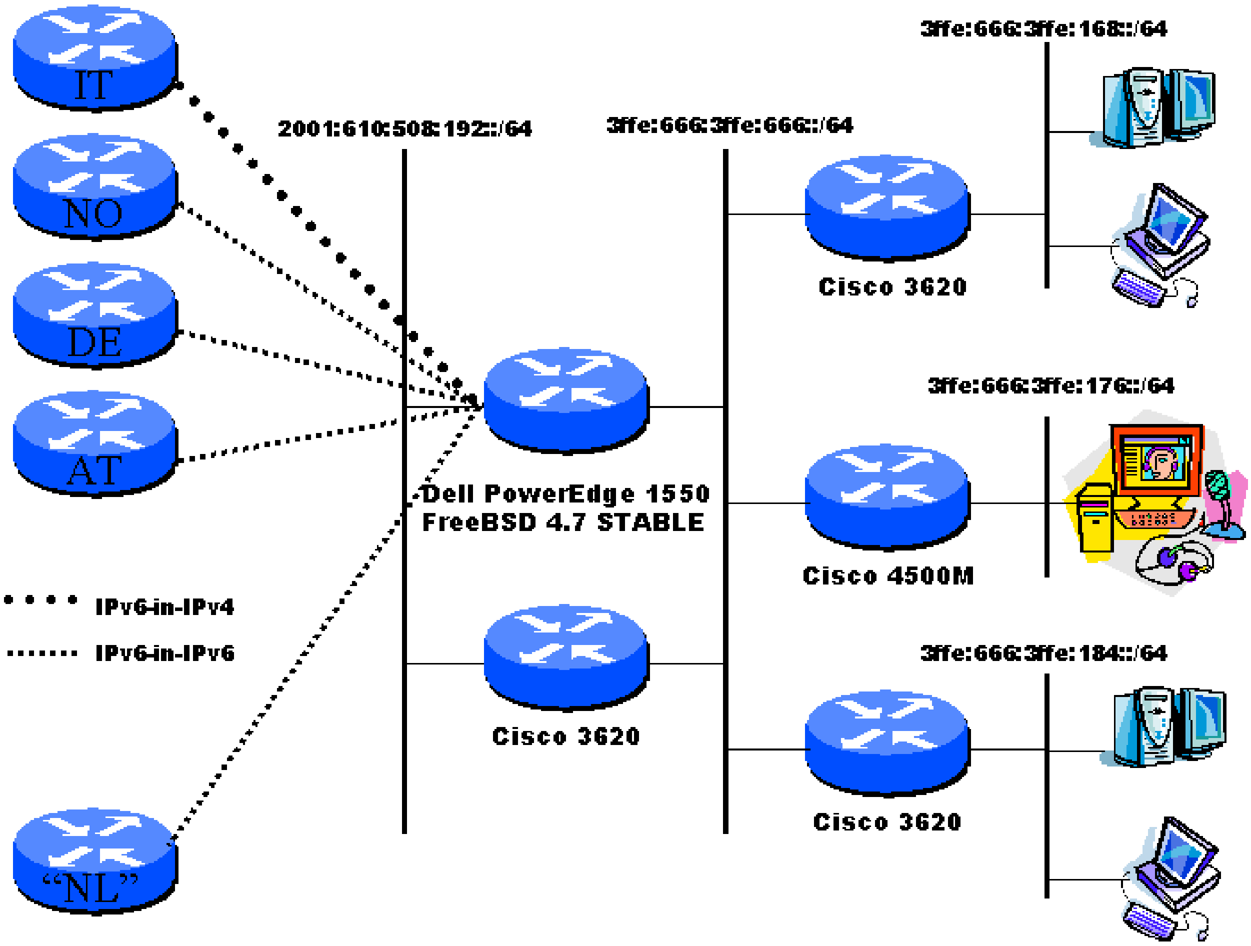


Figure 4.3: IPv6 multicast service at SURFnet.

The other two Cisco 3620 routers and the Cisco 4500 are all running IPv6 multicast EFT images and were used to test IPv6 multicast routing within a LAN environment. Connected are a mix of Linux (RedHat 7.3 and 8.0), Solaris 9 and Windows (XP and a .NET beta server) systems. The routers all had IPv6 unicast as well as IPv6 multicast enabled.

```
!
ipv6 unicast-routing
ipv6 multicast-routing
!
```

The routers used static group-to-RP mapping, they were manually configured with the address of the RP.

```
!
ipv6 pim rp-address 2001:660:10A:6802::1
!
```

Table 4.2 shows the parameters used for tunnels between SURFnet and other partners. We deployed NET-SNMP with MRTG to measure the amount of traffic and IPv6 multicast packets of the tunnels.

Table 4.2: Addresses used for IPv6 multicast tunnels.

Tunnel	Tunnel source	Tunnel destination	Tunnel address	Tunnel address
NO	2001:610:508:192:192:508:610:2001	2001:700:1::3	3ffe:666:3ffe::1	3ffe:666:3ffe::2
IT	192.87.110.201	146.48.127.23	3ffe:666:3ffe::11	3ffe:666:3ffe::12
DE	2001:610:508:192:192:508:610:2001	2001:638:500:200::ff00	3ffe:666:3ffe::21	3ffe:666:3ffe::22
AT	2001:610:508:192:192:508:610:2001	2001:628:402:1:2a0:24ff:fe9d:5094	2001:628:402:0:b000::8	2001:628:402:0:b000::7

4.5 IPv6 Multicast experiments at ULP (France)

The ULP University network (Osiris) is connected to the Renater IPv6 backbone via a 2Mbps ATM VP and a Cisco router. IPv6 is then distributed to all campuses using a specific VLAN (itself transported as an ELAN through an ATM intercampus backbone). Our lab has a FreeBSD PIM-SM IPv6 router connected to this VLAN, and via a tunnel to the Renater part of the M6Bone.

IPv6 multicast is then redistributed to our operational LAN including a VIC/RAT Windows 2000 station, and workstations of most researchers in our team. We have several FreeBSD 4.7 routers for testing our PIM6-SD/MLDv2 implementation: compatibility between MLDv1 and MLDv2 hosts on the same interface, implementation of the full MLDv2 messages (INCLUDE and EXCLUDE mode in the ASM range).

4.6 IPv6 Multicast experiments at UNINETT (Norway)

UNINETT is connected to the M6Bone network using a PC with FreeBSD. This machine works as a PIM-SM router and is a node in the M6Bone network with connections to other participants. This router is also connected to an Ethernet where it gives IPv6 multicast connectivity to several workstations. Note that all unicast traffic from the workstations is routed to another router.

UNINETT has also done some tests with a multicast test image of IOS on a Cisco router. This router was then placed at the edge, so that all workstations used this router instead of the FreeBSD router. The Cisco router was then connected to the FreeBSD router, so one might say that the Cisco was inserted at the edge between the FreeBSD router and the workstations.

UNINETT has also done some tests with reflectors between unicast and multicast, and between IPv4 and IPv6 in different combinations.

4.7 IPv6 Multicast experiments at UCL (UK)

University College London has been connected to M6Bone using a FreeBSD 4.7 machine since 2001. The connection is an IPv6-in-IPv6 tunnel, which runs over our native IPv6 link, via ULCC, to 6NET. We are currently running PIM-SM. The multicast is accessible on our 'MICENET' network, and has also been connected to various internal test networks.

A number of conferences and tests have been conducted over the connection, including the VIC and RAT. Additionally we are now running the modified multicast beacon from PSNC, which is running on an NTPv6 stratum 2 synchronised machine.

4.8 IPv6 Multicast experiments at UoS (UK)

The University of Southampton has an extensive IPv6 network that extends to the majority of its 800 hosts, offering dual-stack networking. The details of how IPv4 and IPv6 are provisioned over VLANs are presented elsewhere in the Transition Cookbook deliverables from Work Package 2 (to be initially published as Deliverable D2.3.2). A parallel IPv6 routed infrastructure is run using a FreeBSD hierarchy, and this has full PIM-SM capability using the raw FreeBSD installation with the KAME snap kit added.

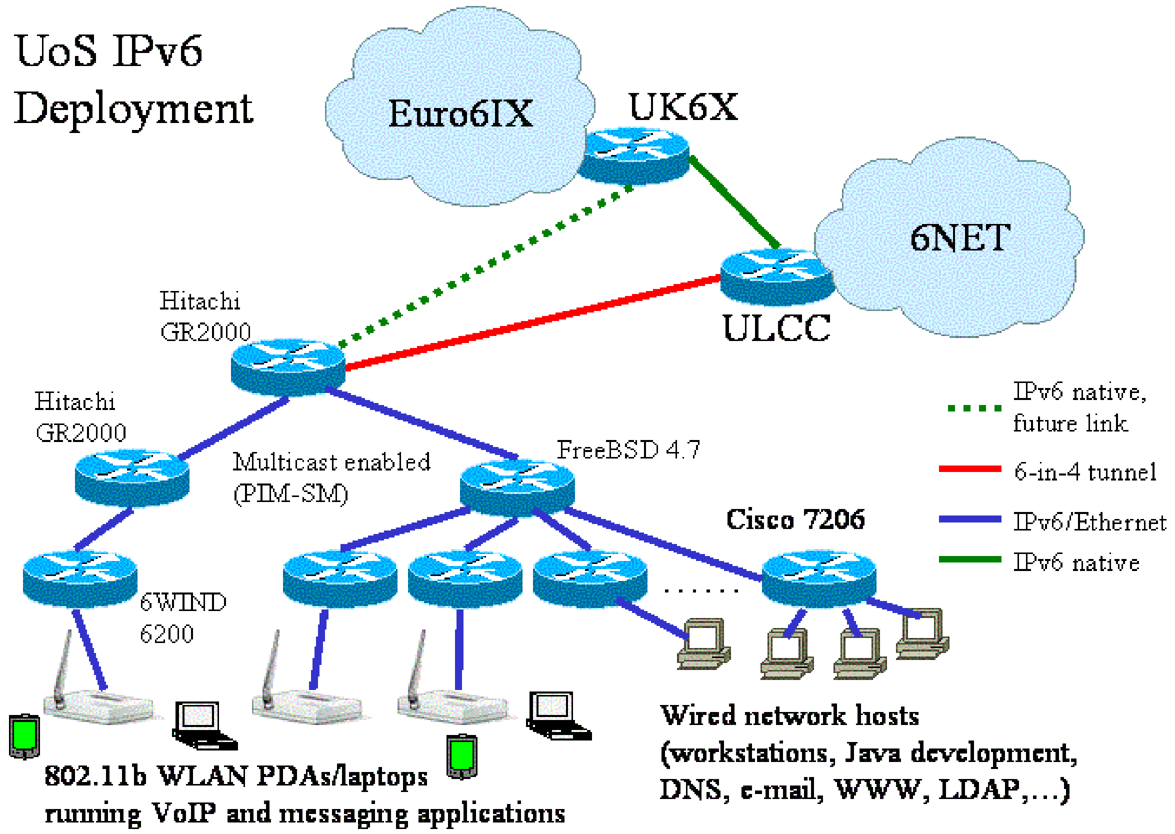


Figure 4.4: UoS IPv6 infrastructure including PIM-SM hierarchy

This topology allows all users in research groups and student workstation clusters to have PIM-SM connectivity between their IPv6 subnets. The RP is situated at the head router of the BSD hierarchy.

One interesting topic lies in how site-local PIM-SM can be run in conjunction with connectivity to the external M6Bone test-bed. This topic will be investigated.

4.8.1 Router Configurations

An example of the FreeBSD router configuration is as follows:

```
ipv6_enable="YES"
ipv6_gateway_enable="YES"
ipv6_router_enable="YES"

ipv6_ifconfig_dc0="2001:630:d0:111::2 prefixlen 64"
ipv6_ifconfig_dc1="2001:630:d0:132::2 prefixlen 64"

ipv6_static_routes="default"
ipv6_route_default="default fe80::280:c8ff:feb9:a8b9%dc0"
```

An example of the M6Bone-specific configuration is as follows:

```
ipv6_router="/usr/local/v6/sbin/route6d"
ipv6_router_flags="-N dc0,dc1"

gif_interfaces="gif0"
gifconfig_gif0="152.78.65.67 158.38.62.72"
ipv6_ifconfig_gif0="3ffe:2a00:100:7efb::2 prefixlen 64"

mroute6d_enable="YES"
mroute6d_program="/usr/local/v6/sbin/pim6sd"
```

UoS plans to continue to operate its own IPv6 multicast infrastructure, to participate actively in the M6Bone, and to join the Euro6IX and 6NET native multicast infrastructures as they become available during the lifetime of both projects. Specific new technology will also be tested as it becomes available, e.g. PIM-SSM and MLDv2 implementations.

4.8.2 M6Bone at IST2002

At the IST 2002 conference in Copenhagen in November 2002, a Linux RedHat 7.3 (laptop) PC was set up by UoS at the IPv6 Cluster booth. This used Linux kernel 2.4.18, with the freely available VIC and RAT tools, and the ALSA Linux sound drivers. The PC was able to receive the M6Bone “6NET people” multicast group which had over 20 participants. Because no M6Bone router was installed at the conference venue, video and audio was streamed from and received to the booth via an IPv6 unicast to multicast reflector hosted at UNINETT (topologically close to the event, which was connected for IPv6 via NORDUnet). Other reflectors, including an IPv4 to IPv6 multicast gateway, also exist, and are described elsewhere in this report.

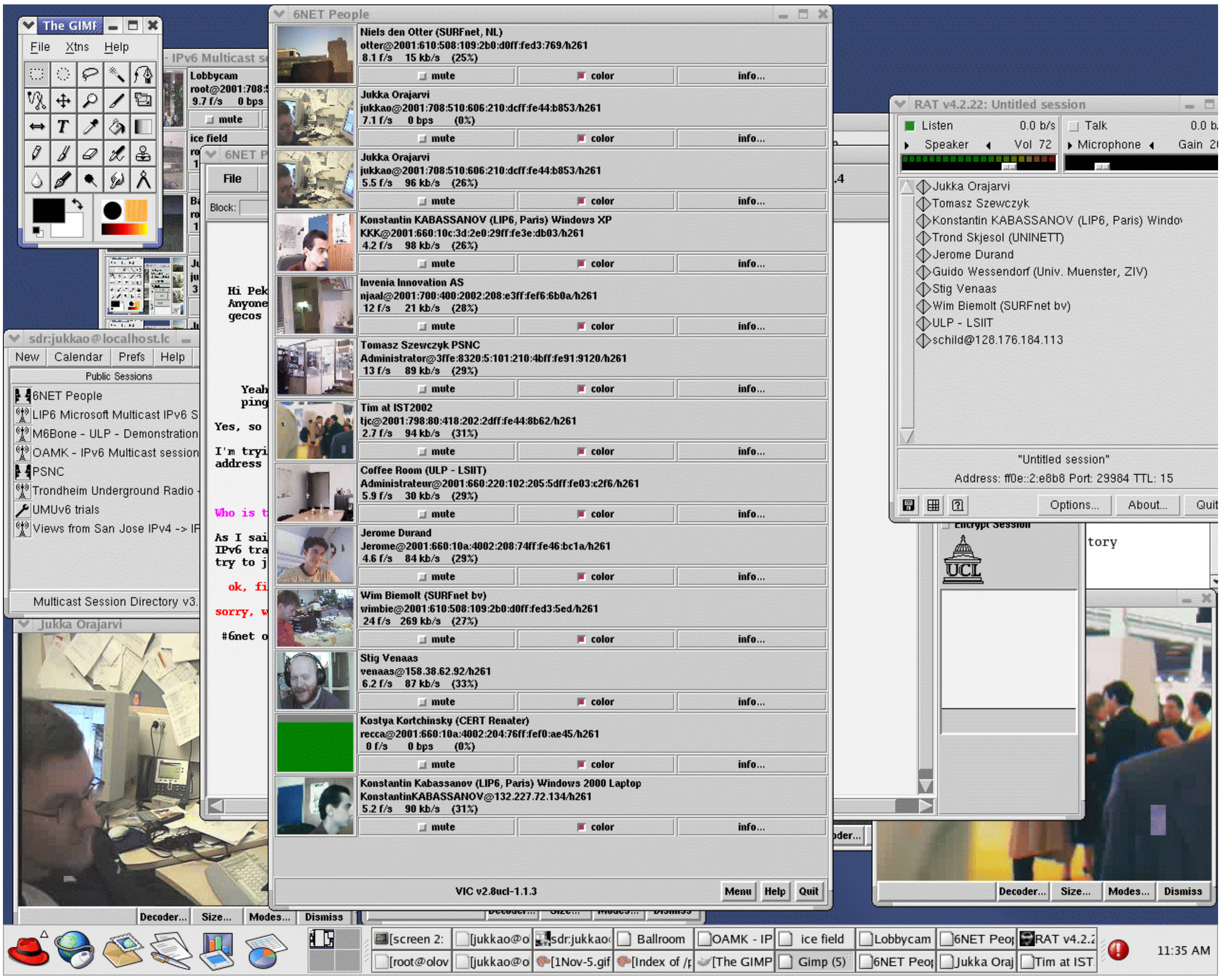


Figure 4.5: The M6Bone in use (VIC, RAT and NTE) at the IPv6 Cluster booth at IST2002.

5. Summary

This document describes the 6NET IPv6 Intradomain multicast service available through the M6Bone. Since for a large part of the equipment used within 6NET there exists no software with IPv6 multicast support yet. A separate tested from 6NET had thus to be used, the M6Bone.

The 6NET participants involved in building an IPv6 multicast service for 6NET (WP3) all connected, using IPv6-in-IPv4 or IPv6-in-IPv6 tunnels, to the M6Bone. They could use at least some of the services available, like the MBone tools for conferencing.

The experience gained will be very useful to deploy IPv6 multicast within 6NET itself as the software will become available and to extend the service to IPv6 Interdomain multicast.

6. Glossary

Anycast	Communication between a single sender and the nearest of several receivers in a group.
ASM	Any Source Multicast. Requires IPv6 support for MBGP, PIM, MLDv2., MSDP and PIM RP support.
Bi-dir PIM	Bi-directional PIM is an extension to the PIM suite of protocols that implements shared sparse trees with bi-directional flow of data. In contrast to PIM-SM, Bidir-PIM avoids keeping source specific state in router and thus allows trees to scale to an arbitrary number of sources.
Broadcast	One-to-all transmission where the source sends one copy of the message to all nodes, whether they wish to receive it or not.
BSR	Bootstrap router. Functionality added to PIM version 2 as a means to provide dynamic group-to-RP mapping.
Distribution Tree	Multicast traffic flows from the source to the multicast group over a distribution tree that connects all of the sources to all of the receivers in the group. This tree may be shared by all sources (a shared-tree), or a separate distribution tree can be built for each source (a source-tree). The shared-tree may be one-way or bi-directional.
DR	Designated Router. The router in a PIM-SM tree that instigates the Join/Prune message cascade upstream to the RP in response to IGMP membership information it receives from IGMP hosts.
IGMP	Internet Group Membership Protocol. Version 2 is used by IPv4 routers and their immediately connected hosts to communicate multicast group membership states. Version 3 is the protocol used by IPv4 systems to report their IP multicast group memberships to neighbouring multicast routers. Version 3 adds support for "source filtering", that is, the ability for a system to report interest in receiving packets only from specific source addresses, or from all but specific source addresses, sent to a particular multicast address. IGMP messages are encapsulated in standard IP datagrams with an IP protocol # of 2 and the IP Router Alert option (RFC2113).
MBGP	Multi-protocol Extensions for Border Gateway Protocol. Also known as BGP+, MBGP represents multicast extensions to the BGP Unicast inter-domain protocol. It adds capabilities to BGP to enable multicast routing policy throughout the Internet and to connect multicast topologies within and between BGP autonomous systems. That is, MBGP is an enhanced BGP that carries IP multicast routes. MBGP carries two sets of routes, one set for unicast routing and one set for multicast routing. The routes associated with multicast routing are used by Protocol Independent Multicast (PIM) to build multicast data distribution trees.
MLD	Multicast Listener Discovery. The protocol used within IPv6 to discover the presence of multicast listeners. MLD version 1 is derived from IGMP version 2 and MLD version 2 is derived from IGMP version 3.

MLD Query — Messages originating from the router(s) to elicit multicast group membership information from its connected hosts.

MLD Report — Messages originating from the hosts that are joining, maintaining or leaving their membership in a multicast group.

MSDP — Multicast Source Discovery Protocol. A mechanism to connect multiple PIM sparse-mode (SM) domains. MSDP allows multicast sources for a group to be known to all rendezvous point(s) (RPs) in different domains. Each PIM-SM domain uses its own RPs and need not depend on RPs in other domains. An RP runs MSDP over TCP to discover multicast sources in other domains. MSDP is also used to announce sources sending to a group. These announcements must originate at the domain's RP. MSDP depends heavily on MBGP for interdomain operation.

Multicast — A routing technique that allows IP traffic to be sent from one source or multiple sources and delivered to multiple destinations. Instead of sending individual packets to each destination, a single packet is sent to a group of destinations known as a multicast group, which is identified by a single IP destination group address. Multicast addressing supports the transmission of a single IP datagram to multiple hosts.

PIM — Protocol Independent Multicast. A multicast routing architecture defined by the IETF that enables IP multicast routing on existing IP networks. Its key point is its independence from any underlying Unicast protocol such as OSPF or BGP.

PIM-DM — PIM dense mode (Internet Draft): Actively attempts to send multicast data to all potential receivers (flooding) and relies upon their self-pruning (removal from group) to achieve desired distribution.

PIM-SM — PIM sparse mode (RFC 2362): Relies upon an explicitly joining method before attempting to send multicast data to receivers of a multicast group.

Prune — Multicast routing terminology indicating that the multicast-enabled router has sent the appropriate multicast messages to remove itself from the multicast tree for a particular multicast group. It will stop receiving the multicast data addressed to that group, and therefore cannot deliver the data to any connected hosts until it rejoins the group.

RP — Rendezvous Point. The multicast router that is the root of the PIM-SM shared multicast distribution tree.

RPF — Reverse Path Forwarding. RPF check. The router checks whether or not the packet came from the interface where the source of the packet is seen in the routing table.

Source Tree — A multicast distribution path that directly connects the DRs (or the RP) of the source and receivers to obtain the shortest path through the network. Results in most efficient routing of data between source and receivers, but may result in unnecessary data duplication throughout network if built by anyone other than the RP.

SSM — Source Specific Multicast. Requires IPv6 support for MBGP, PIM, and MLDv2.

Unicast — Point-to-point transmission requiring the source to send an individual copy of a message to each requester.