Support for the
1st Multi-sites Remote IPv6 Interoperability event,
during Madrid Global IPv6 Submit 2003

12-14 May 2003

Version 3.0

Revision History

Revision	Date	Description	Author (Organization)
v1.1	15/01/2003	Document creation	César Olvera (Consulintel)
v1.2	23/01/2003	Added issues brought by Philippe Cousin (ETSI)	César Olvera (Consulintel)
v1.3	27/01/2003	ToC updated	César Olvera (Consulintel)
v1.4	11/02/2003	Document updated	César Olvera (Consulintel)
v1.5	26/02/2003	Added contribution of Jordi Palet (Consulintel) Added Isabel information	César Olvera (Consulintel)
v1.6	03/03/2003	Document updated	César Olvera (Consulintel)
v1.7		Input from IRISA	Cesar Viho (IRISA) Frederic Roudaut (IRISA)
v2.0	14/03/2003	Document revision	Sébastien Flaux (ETSI)
v2.1	27/03/2003	Document updated	César Olvera (Consulintel)
V2.2		Document updated	Sébastien Flaux (ETSI)
V3.0	29/04/2003	Document updated	Sébastien Flaux (ETSI)

Table of content

Summary

Simultaneously with the Madrid Global IPv6 Summit 2003 from 12th to 14th May, the ETSI Plugtests Interoperability Service will hold a “Multi-sites remote IPv6 interoperability event”.

This document provides a starting point for discussion on the definition of an organizational and technical program of the “1st Remote IPv6 Plugtests”.

It gives first steps on IPv6 related protocols and mechanisms that can be tested in a remote test session. Moreover, it is planned to have a possibly videoconference between participants during the event in order to coordinate more easily remote test sessions.

1. Introduction

ETSI organize the IPv6 Plugtests events where engineers get together to test the interoperability of their implementations against each other. The 1st Multi-site Remote IPv6 Plugtests will 'bring together' companies and laboratories to test interoperability of their IPv6 implementations in their products.

For the first time in such event, a real IPv6 environment will be available, and a permanent IPv6 link from a pan-European Euro6IX network will be used in order to offering remote testing and the opportunity for companies to participate from a distance in the 1st Remote IPv6 Interoperability event.

The aim is to test in site and/or remote way issues as:

- IPv6 Core
- Mobile IPv6
- Transitions mechanisms (6to4, SIIT /NAT-PT)
- Routing
- QOS
- Multicast

It seems particularly difficult to perform remote testing when the links are not totally dedicated to this. For example, tests concerning routing protocols would modify routing table in routers and by this way all the network traffic. Moreover there are so many interactions between the different Autonomous Systems involved or not in the remote testing session that it is not possible to understand all the test traffic path. Furthermore, it is not possible to have probes in all the Autonomous Systems involved in the traffic path.

Hereafter, you will find a part of the IPv6 protocol stack. It will be helpful for understanding at which layer, tests have to be done for a given IPv6 associated protocol.

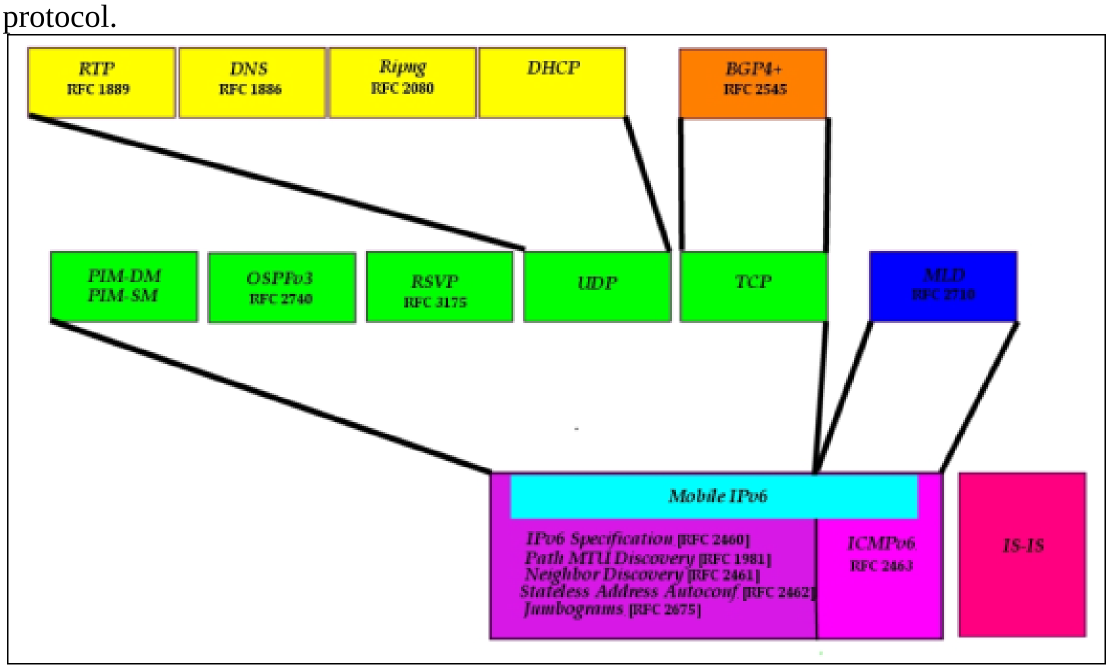


Figure 1-1: IPv6 Protocols Stack

2. Organizational Aspects

2.1 Sites connected and technical contacts

The following table contains the planned sites and technical contacts of each partner that will participate on the event.

Site	Country	Technical contact	Contact information	Participation	IPv6 connection	Videoconferencing system	Time Zone http://www.jeico.com/timetble.html
Madrid GIS 2003	Madrid, Spain	Cesar Olvera Jordi Palet	cesar.olvera@consulintel.es jordi.palet@consulintel.es	In site	Native to Euro6IX	Isabel	GMT+1
ETSI	Nice, France	Patrick Guillemin Philippe Cousin	patrick.guillemin@etsi.org philippe.cousin@etsi.org sebastien.flaux@etsi.org	In site	Native to Renater	Isabel	GMT+1
IRISA	Rennes, France	Cesar Viho Frederic Roudaut	Cesar.Viho@irisa.fr Frederic.roudaut@irisa.fr	At ETSI			GMT+1
UNH	US	Ben Schultz Fanny Xu	Schultz@io.iol.unh.edu fx@iol.unh.edu	In site	Via 6Bone		GMT -5
TTA	Korea	Dong-Hyun Seok Jongjin Sung	fall@tta.or.kr jsung@tta.or.kr	In site	Native to Eutope through Transeurasia	Isabel	GMT+9
TAHI	Japan	Hiroshi Miyata	H.Miyata@jp.yokogawa.com	In site		Isabel	GMT+9
Chung Hwa Telecom Labs/NICI Ipv6 Testing Lab	Tapei Taiwan	Chin-Chou Chen Chih-Cheng Tsao	chinchou@cht.com.tw atsao@cht.com.tw	In site	Via 6Bone	Isabel	GMT+8
Univerity Libre of brussels	Belgium	Antal Bulanza Paul Van Binst	antal.bulanza@helios.iihe.ac.be paul.vanbinst@helios.iihe.ac.be	In site	Via 6Bone	Isabel	GMT +1
6WIND	France	Cyril Corre	cyril.corre@6WIND.COM	In site	2Mbps via Renater	Isabel	GMT+1

Figure 2-1: Table of sites connected and technical contacts

If you are willing to participate, send your information to document editor: sebastien.flaux@etsi.org

Please include information about:

- what you would bring to the event (devices, test suites, etc)
- your readiness to contribute to the test plan for the event

2.2 Scheduled planning

Activity	Day	Comments
Preparatory tests	March	Tests Isabel Terminal
Preparatory tests	8 April	Get practice using Isabel, test IPv6 connection links (bandwidth, response times), and carry out some IPv6 core tests.
Preparatory tests	April 30	First testing day, final sites selection
Preparatory tests	May 5	Tests with all involved sites
Preparatory tests	May 7	Final tests session
Day 1	12 May	9-17 h
Day 2	13 May	9-17 h
Day 3	14 May	9-17 h

3 Technical aspects

3.1 Network Infrastructure

Regional and International IPv6 networks as Euro6IX, 6NET, Abilene and 6Bone will be the base of a remote multi partner connectivity giving the opportunity for companies and test services to participate from a distance in this Interoperability Plugtests.

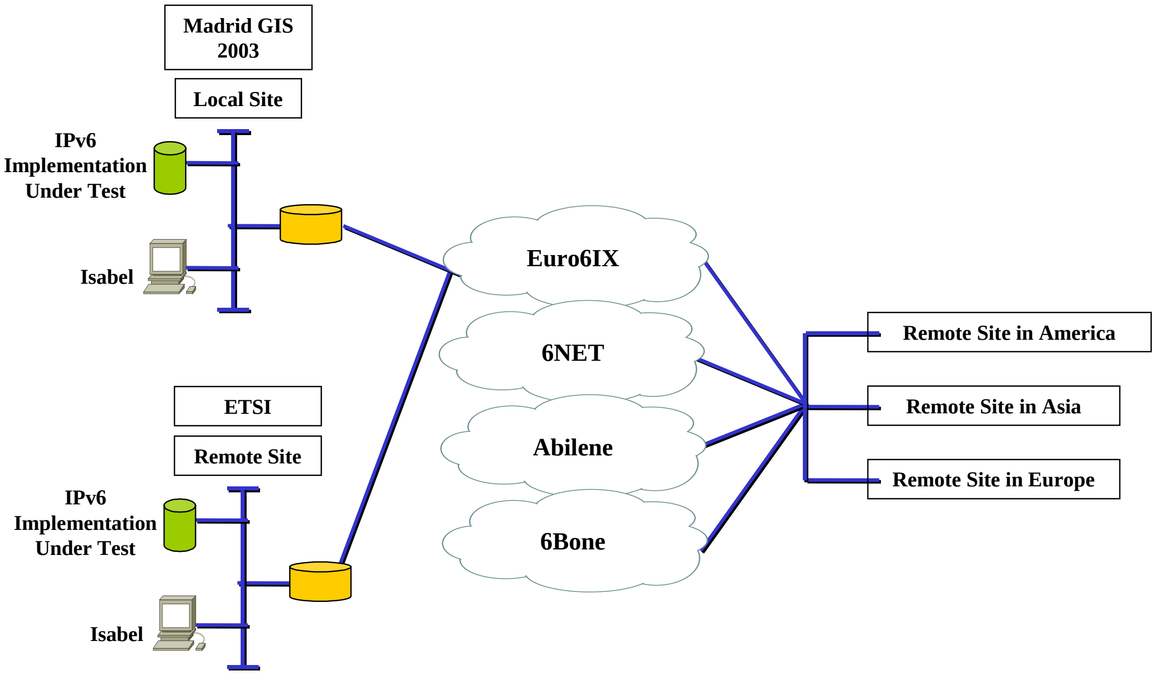


Figure 3-1: Basic network connection

3.2 Protocols under tests

3.2.1 Basic Protocols

IPv6 Basic protocols include Core IPv6 Support specification, Jumbo Payload option, Internet Control Message Protocol, Neighbor Discovery, Stateless Address Auto-configuration, Redirect and Path-MTU Discovery.

The main part of tests concerning IPv6 core protocols could not be done in remote testing because main aspects of core protocols concern a local network. Furthermore in remote testing we have to deal with ingress filtering which is one of the mechanisms suggested to prevent attacks that are staged using spoofed source addresses. This involves configuring the routers to drop packets that have illegitimate source IP addresses.

The Jumbo Payload option is relevant only for IPv6 nodes that may be attached to links with a link MTU greater than 65,575 octets (that is, 65,535 + 40, where 40 octets is the size of the IPv6 header). Nevertheless, for IPv6, only the Loose Source Routing is available. As a consequence we cannot know the path that the different packets will follow. So, it is not possible to test it in a remote testing.

Nevertheless, it is possible to test some basic aspects of IPv6 like:

- Path MTU Discovery
- ICMPv6 error messages or ICMPv6 informational messages which are mainly used by some well-known Network tools like *ping* or *traceroute*

References:

- RFC 2460, Internet Protocol Version 6 (IPv6) Specification. S. Deering, R. Hinden. December 1998. PROPOSED STANDARD.
- RFC 2463, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6). A. Conta, S. Deering. December 1998. PROPOSED STANDARD.
- RFC 1981, Path MTU Discovery for IP version 6. J. McCann, S. Deering, J. Mogul. August 1996. PROPOSED STANDARD.
- RFC 2461, Neighbor Discovery for IP Version 6 (IPv6). T. Narten, E. Nordmark, W. Simpson. December 1998. PROPOSED STANDARD.
- RFC 2462, IPv6 Stateless Address Autoconfiguration. S. Thomson, T. Narten. December 1998. PROPOSED STANDARD.
- RFC 2675, IPv6 Jumbograms. D. Borman, S. Deering, R. Hinden. August 1999. PROPOSED STANDARD

3.2.2 Routing

Routing protocols can be divided in two groups. The interior gateway protocols (IGP) are in charge of routing packets within an autonomous IPv6 domain, whereas the exterior gateway protocols (EGP) allow the connectivity between domains.

- IGPs:

    - RIPng is the Routing Internet Protocol version 2 adapted for IPv6. This protocol is based on distance vectors. It was the first routing protocol to be implemented because of its simplicity and its stability in previous IP version (IPv4).
    - OSPFv3 (as Open Shortest Path First for IPv6) is, as for IPv4, designated to be the reference routing protocol. This protocol is based on the maintenance of link states, and the IPv6 version is younger than RIPng.
    - IS-IS is a routing protocol based on the maintenance of link states developed by the OSI. At the beginning of the Internet, two network protocols emerged: IP and CLNP (Connectionless Network Protocol) developed by the OSI. The OSI chose IS-IS as their main IGP and the IETF community chose OSPF. Later, an adaptation of IS-IS called Dual IS-IS permitted it the routing of IP and CLNP. Nevertheless, the development of IS-IS and CLNP was longer than the development of IP and OSPF; as a consequence IP was chosen for the transport Layer of the Internet.

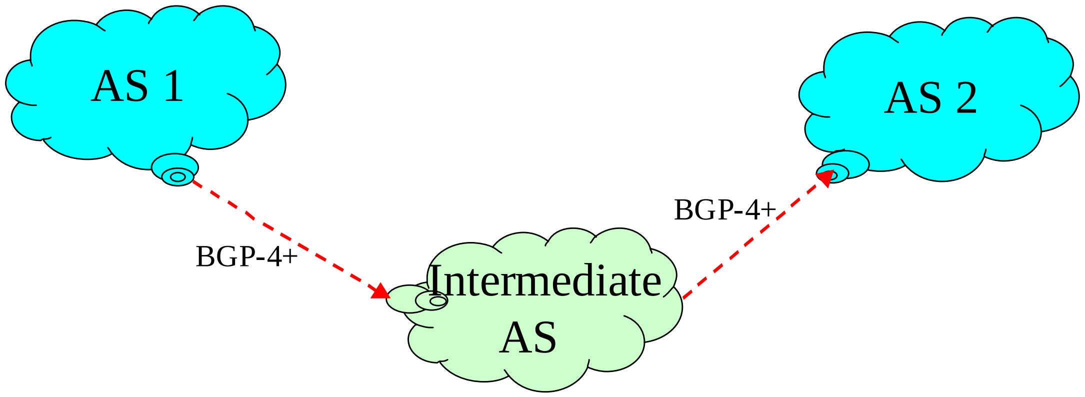
- EGPs:

    - BGP-4 is the main inter-domain routing protocol used. It supports extensions for routing of traffic from IPv6 domains. In this case the protocol is called BGP-4+.

We can consider each remote test site as made of at least one Autonomous System (AS). Each autonomous System has to use an IGP, and the connectivity between each Autonomous System is handle by BGP-4+. So for testing IGPs like OSPFv3, RIPng or IS-IS, we do not have to use our entire multi-site test network. The different tests have to be located in each Autonomous System.

The main difficulty will be to test EGPs. Indeed, let's consider 2 Autonomous Systems, AS 1 and AS 2. AS 1 and AS 2 are not directly connected together. So, the network accessibility of AS 1 will be announced by an intermediate AS (IAS) according to its policy. In this case, we have two main problems for testing the EGPs:

1. We have to deal with the policies of the different Intermediate AS.
2. If we modify announces of networks accessibility of AS 1 to Intermediate AS, the external routing tables of the Intermediate AS will be modified.



However, it will not be possible to have some control and observation points in each Intermediate System. It is possible to have some basic tests between two remote AS although it will be difficult to isolate the reason of the eventual problems. It would be easy to detect the correct network accessibility of AS 1 in AS 2, but if a problem occur, we will have big difficulty to detect the reasons. Is it because of AS 1 or AS 2 edge routers or is it because of the Intermediate AS?

Moreover, we forgot that now Internet is not like the former ARPANET, based upon a backbone connecting each Autonomous System. Internet is more like a giant graph connecting the different AS. It means that our IAS is certainly connected to some more AS. There could be some redundancy in the paths between AS 1 and AS 2. Moreover, in the real Internet the connectivity between our two test sites could be done through more than one Intermediate AS. These possibilities add more complexity to detect the reasons and the place of the failure.

The best way for isolating our test network would be to use IPv6 over IPv6 tunnels to interact between the different sites. BGP-4+ would be used as EGP between our Autonomous Systems. The using scope of the test EGP should be limited to the tunnel part and each edge router of the different AS should be configured to separate routing announces coming from the tunnel part and from the remaining Internet. In this case it would be easier, with a probe on the edge routers to detect errors.

Our opinion is that even if we establish some IPv6 over IPv6 tunnels between the different sites we will have some difficulties to separate correctly routing traffic coming from the tunnel from the others routing announces.

References:

- RFC2080, RIPng for IPv6, G. Malkin, R. Minnear, January 1997, PROPOSED STANDARD.
- RFC2545, Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing P. Marques, F. Dupont, March 1999, PROPOSED STANDARD
- RFC2858, Multiprotocol Extensions for BGP-4 T. Bates, Y. Rekhter, R. Chandra, D. Katz, June 2000, PROPOSED STANDARD
- RFC2740, OSPF for IPv6, R. Coltun, D. Ferguson, J. Moy, 1999, PROPOSED STANDARD.
- draft-ietf-isis-ipv6-05.txt, Routing IPv6 with IS-IS, Christian E. Hopps, January 2003, INTERNET DRAFT.

3.2.3 Transition mechanisms

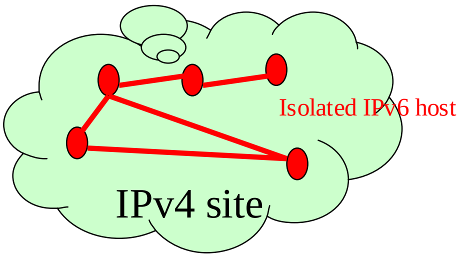
The transition mechanisms are a set of mechanisms for ensuring the integration of IPv6 networks in some existing IPv4 infrastructures, and guaranteeing communications between the two IPv4 and IPv6 worlds.

We can classify the transition mechanisms in four sets:

- *Mechanisms permitting the construction of an IPv6 network over an IPv4 infrastructure*. The set of these mechanisms uses essentially v6 over v4 tunnels. The main mechanisms developed are 6over4 (Transmission of IPv6 over IPv4 Domains without Explicit Tunnels), ISATAP(Intra-Site Automatic Tunnel Addressing Protocol).
- *Mechanisms permitting the accessibility to an already existing IPv6 network*. We can distinguish transition mechanisms like 6to4(Connection of IPv6 Domains via IPv4 Clouds), Tunnel Broker.
- *Cohabitation mechanisms* developed in order to permit communication between IPv4 and IPv6 applications. Main mechanisms are SIIT, NAT-PT where the transition is only done at the edge of the site by a header translation; and DSTM(Dual Stack Transition Mechanism), which use IPv4 over IPv6 tunnel inside the site with the advantage of allowing IPv4 application to communicate over IPv6 infrastructure even if they have not been v6fied (not adapted to be used with IPv6).
- *Mechanisms to generate IPv6 packets from IPv4 applications*. The main mechanisms are Bump in the Stack and Bump in the API.

3.2.3.1 Testing construction mechanisms of an IPv6 network over an IPv4 infrastructure

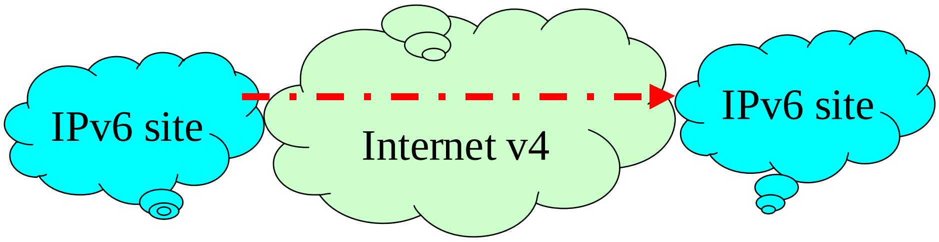
The motivation for this method is to allow isolated IPv6 hosts, located on a physical link which has no directly connected IPv6 router, to become fully functional IPv6 hosts by using an IPv4 multicast domain as their virtual local link.



For testing this kind of transition mechanisms, there is no need for having a remote test session. All tests have to be done on an IPv4 site with a few isolated IPv6 hosts.

3.2.3.2 Testing mechanisms for accessing an existing IPv6 network

The motivation for this method is to allow isolated IPv6 domains or hosts, attached to an IPv4 network which has no native IPv6 support, to communicate with other such IPv6 domains or hosts with minimal manual configuration, before they can obtain native IPv6 connectivity.



Tests for this kind of mechanisms can be done in remote between two IPv6 sites using the IPv4 Internet world.

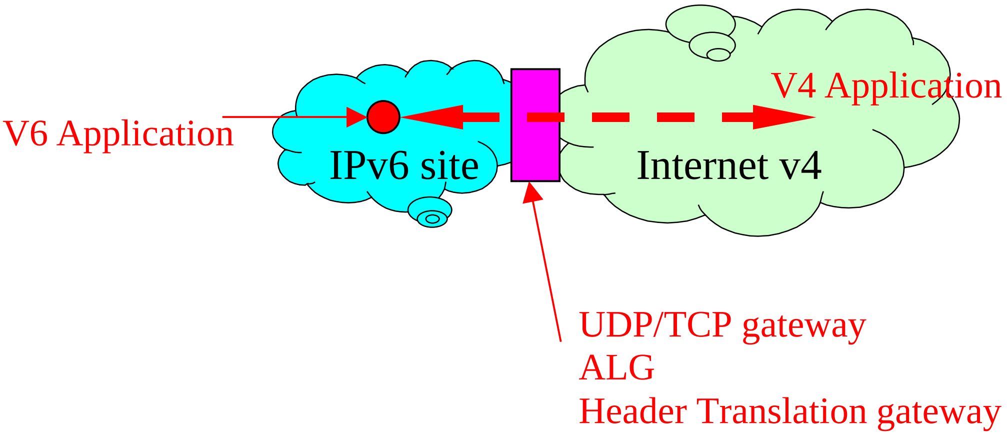
3.2.3.3 Testing Cohabitation Mechanisms

These mechanisms are used for allowing communication between IPv4 and IPv6 applications. This Translation can be done at different layer of the protocol stack:

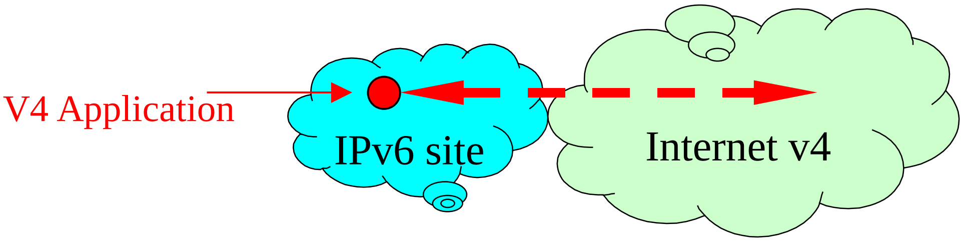
- At the layer 2: by the creation of IPv4 over IPv6 tunnels. This is the operation mode of DSTM.
- At the transport layer : by the use of UDP or TCP Gateways.
- At the application level: by the use of ALG (Application Level Gateway) which integrates the dual stack. It can be the case with printer spoolers, web proxy.
- At the edge of the site: by the use of header translation. SIIT and NAT-PT operate like this.

All these transition mechanisms can be tested in a remote testing session although it will be mandatory to use the v4 Internet world.

Hereafter we can see a brief topology of the network to put into place for testing UDP/TCP gateways, ALG or SIIT/NAT-PT. In this case, an IPv6 Application wants to communicate with an IPv4 Application. The translation gateway will be at the edge of the IPv6 site. It would be interesting to have the IPv4 application on an IPv4 site with which we want to communicate. Nevertheless, it is not an obligation to have an IPv4 application on an IPv4 site to test the gateways. It could be efficient enough to have another IPv6 site with another gateway at the site edge.



It will be a bit different to test DSTM. DSTM is intended for IPv6-only networks in which hosts still need to exchange information with other IPv4 hosts or applications. The main benefit of DSTM is that IPv4 applications are run over an IPv6-only network. Hereafter we can see a brief topology of the test network for DSTM.



References:

- RFC2529, Transmission of IPv6 over IPv4 Domains without Explicit Tunnels, B. Carpenter, C Jung, March 1999, PROPOSED STANDARD.
- RFC2765, Stateless IP/ICMP Translation Algorithm (SIIT), E. Nordmark, February 2000, PROPOSED STANDARD
- RFC2766, Network Address Translation - Protocol Translation (NAT-PT) G. Tsirtsis, P. Srisuresh, February 2000, PROPOSED STANDARD
- RFC2767, Dual Stack Hosts using the Bump-In-the-Stack Technique (BIS), K. Tsuchiya, H. Higuchi, Y. Atarashi, February 2000, INFORMATIONAL
- RFC2893, Dual Stack, Configured tunneling of IPv6 over IPv4, IPv4-compatible IPv6 addresses, Automatic tunneling of IPv6 over IPv4, R. Gilligan, E. Nordmark, August 2000, PROPOSED STANDARD
- RFC3053, IPv6 Tunnel Broker, A. Durand, P. Fasano, I. Guardini, D. Lento, January 2001, INFORMATIONAL
- RFC3056, Connection of IPv6 Domains via IPv4 Clouds, B. Carpenter, K. Moore, February 2001, PROPOSED STANDARD
- RFC3089, A SOCKS-based IPv6/IPv4 Gateway Mechanism, H. Kitamura, April 2001, INFORMATIONAL
- RFC3142, An IPv6-to-IPv4 Transport Relay Translator , J. Hagino, K. Yamamoto, June 2001, INFORMATIONAL
- draft-ietf-ngtrans-dstm-08.txt, Dual Stack Transition Mechanism (DSTM), Jim Bound, Laurent Toutain, Octavio Medina, Francis Dupont, Hossam Afifi, Alain Durand

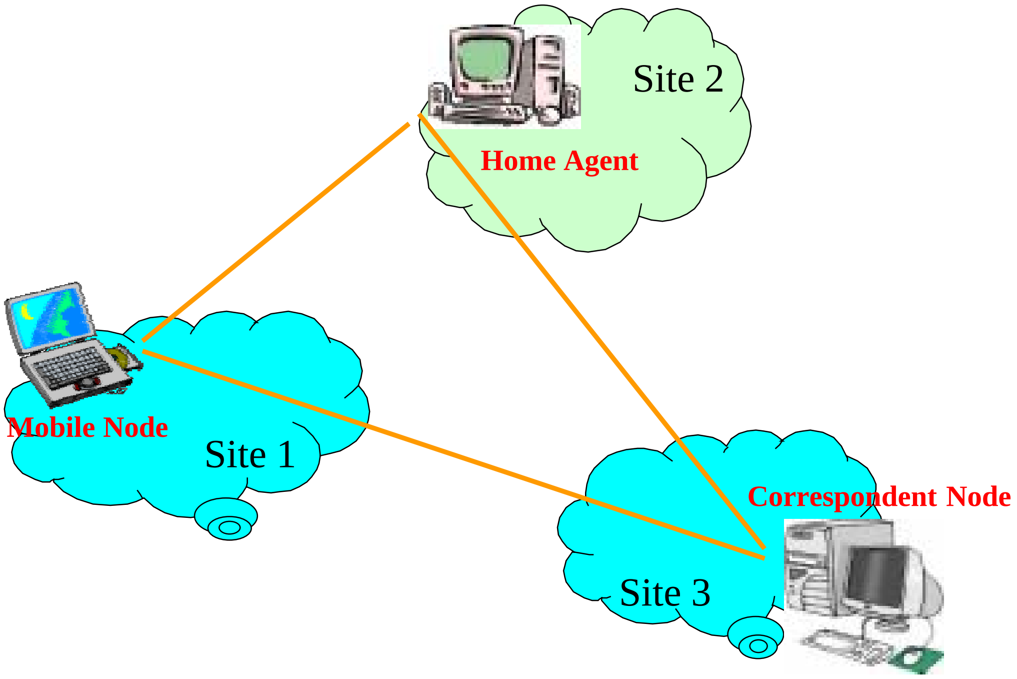
3.2.4 Mobile IPv6

The Mobile IPv6 protocol allows a mobile node to move from one link to another without changing the mobile node's "home address". Packets may be routed to the mobile node using this address regardless of the mobile node's current point of attachment to the Internet. The mobile node may also continue to communicate with other nodes stationary or mobile) after moving to a new link. The movement of a mobile node away from its home link is thus transparent to transport and higher-layer protocols and applications.

The Mobile IPv6 protocol is just as suitable for mobility across homogeneous media as for mobility across heterogeneous media. For example, Mobile IPv6 facilitates node movement from one Ethernet segment to another as well as it facilitates node movement from an Ethernet segment to a wireless LAN cell, with the mobile node's IP address remaining unchanged in spite of such movement.

For the moment, there is no standard about mobility support for IPv6. Mobile IPv6 is only described by two drafts. The main draft called “draft-ietf-mobileip-ipv6-XX” where “XX” is the version number describes the whole MIPv6 architecture. The last draft (Version 21) is available since February 2003. The different versions of the drafts are not interoperable with each other.

There is no really problem to test Mobile IPv6 in a remote test session. One site has to be chosen as the home site of the mobile. One host must be available on the Home Link (the Home Agent Link) if necessary to simulate the returning home process. Thus, if the Mobile Node is unplugged in the home Link, the moving process to a foreign link in another site for example, can be handle easily. Our “new” Mobile Node only has to know his home address. All the different aspects of the Mobile node specification can be tested in a remote testing session: return routability process, Dynamic Home Agent Address Discovery, returning home, moving from one care-of address to another care-of address…



References:

- draft-ietf-mobileip-ipv6-21.txt, Mobility Support in IPv6, D. Johnson, C. Perkins, J. Arkko, February 26, 2003, Internet-Draft
- draft-ietf-mobileip-mipv6-ha-ipsec-03.txt, Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents, J. Arkko, V. Devarapalli, F. Dupont, February 18, 2003, Internet-Draft

4 Test plan

This document gives the basic aspects of which protocols or mechanisms can be tested in a remote session. We now have to look more deeply at the different protocols in order to distinguish which tests can be done and are relevant. Moreover this document does not describe the test possibility for multicast (MLD, PIM-SM, PIM-DM …), for security, for QoS.

The following table gives a summary of what can be done in remote way. The different protocols no described here will be analyzed in a next document.

	Testable in remote session ?	**Who can provide the tests ?**
A. IPv6 Basic Protocol:		**TAHI**
a) IPv6 Specification *[RFC 2460]*	**NO**	
b) IPv6 Jumbo Payload Option *[RFC 2675]*	**NO**	
c) ICMPv6 *[RFC 2463]*	**YES**	
d) Neighbor Discovery *[RFC 2461]*	**NO**	
e) Path MTU Discovery *[RFC 1981]*	**YES**	
f) Stateless Address Autoconfiguration *[RFC 2460]*	**NO**	
B. *Mobile IPv6:*	**YES**	**IRISA**
C. Transition:		**IRISA**
a) 6over4 *[RFC 2529]*	**NO**	
b) ISATAP	**NO**	
c) 6to4 *[RFC 3056]*	**YES**	
d) SIIT *[RFC 2765]*	**YES**	
e) NAT-PT *[RFC 2766]*	**YES**	
f) DSTM	**YES**	
D. Routing:		
a) RIPng *[RFC 2080]*	**NO**	
b) *OSPFv3 [RFC 2740]*	**NO**	
c) *IS-IS*	**NO**	
d) *BGP-4+ [RFC 2545, 2858]*	**YES**	
E. Security:		**Not studied**
a)IPSec AH *[RFC 2401, 2402]*	**YES**	
b)IPSec ESP *[RFC 2401, 2406]*	**YES**	
F. Header compression		**Not studied**
a) ROHC *[RFC 3095]*	**YES**	
G. Multicast		**6WIND**
a) PIM-SM	**YES**	
b) PIM-SSM	**YES**	
H. QOS	**YES**	**Consulintel**
I. DHCPv6	**To be studied**	**Not studied**

Figure 4-1: Test Plan

5 Videoconference Systems

It is planned to have videoconference systems during the remote interoperability event among the different partners involved to coordinate more easily the test sessions. Isabel system or M6Bone tools can be use.

5.1 Isabel System

The event will be distributed using the Isabel application. Several institutions will get connected to the event and will follow it in a distributed way. The Isabel CSCW application (http://isabel.dit.upm.es) is a group collaboration tool for the Internet (or VPNs), which uses TCP-UDP/IP protocols (IPv4, IPv6 and dual stack). Isabel supports the realization of distributed meetings, classrooms, congresses, etc, by using an innovative service concept. The commercial version of Isabel can be purchased from Agora Systems S.A. (http://www.agora-2000.com/).

The Isabel Platform infrastructure must be set up to allow each institution to participate in Isabel sessions. The infrastructure includes 3 basic elements: the Isabel terminal, network connectivity and the videoconference room.

5.1.1 Set up of Isabel Terminal

The Isabel terminal is a PC with Linux and Isabel installed. The Isabel version used for this event will be Isabel 4.6.

An installation CD exists which installs “SuSE 8.1 + Isabel 4.6” in a single and simple installation. This CD should be used for setting and installing the Isabel terminal. The CD can be provided by the session organizers, by Agora Systems (http://www.agoratechnologies.com), or can be downloaded from the Isabel Web page (http://isabel.dit.upm.es) (400 Mbytes approx.). This installation CD will make the set up of the Isabel Terminal very easy. A Linux expert may be able to install Isabel over other Linux distributions, but it requires much more effort and expertise.

For more information about Isabel 4.6, and further instructions on how to install Isabel and Isabel manual visit the Isabel web site http://isabel.dit.upm.es/.

5.1.2 Connection to an Isabel Session

The connection of Isabel terminals to a session is coordinated with Web pages and session definition files accessible with a session URL, which is usually provided by the organizers.

For Plugtests event, you will found an entry in http://isabel.dit.upm.es/events. The pages will contain technical and organizational details.

5.1.3 Isabel On-line support during the event

An IRC (Internet Relay Chat) will be used for communication between Isabel operators during both Isabel test periods and Plugtests event.

- Make sure you have an appropriate IRC Client (e.g. ircII or BitchX (recommended) for Unix or Windows, MIRC for Windows) on your Control Station or a computer near your Control Station. If you only have IPv6 access to the IRC server, make sure that your IRC client provides IPv6 support (compile xchat with IPv6 support, or install a IPv6 enabled IRC client for Windows).
- Please care for a phone in your conference room which will be used for emergency only.

There will be a chat server at UPM site. Public Internet is required to access the chat server. The chat server will also be available using IPv6 through the Euro6IX network.

- External network chat server: malpica.dit.upm.es (138.4.4.145), port: 7000. If you are using IPv6, connect to irc.upm.euro6ix.org (2001:800:40:2b01::a100).
- This will be the channel, during the remote Plugtests, for the chat server: channel: #ipv6plugtests, using your site code as nickname.
- When several persons are connected from the same site, add your name to the site code (e.g. Charles and John from UPM will join as UPMCharles and UPMJohn).

5.2 M6Bone Systems

It should not be very difficult to have a videoconference system based on Multicast tools. The M6Bone network (http://www.m6bone.net) is a test service developed in order to offer an IPv6 multicast service to interested sites. This service is based on the IPv6 pilot of Renater. It enables to use multicast videoconference tools on the network in order to broadcast events. Because multicast routing is not yet available on the routers, the M6Bone is tunnel architecture with edge equipments over IPv6 native networks which support IPv6 multicast.

There are different ways to be connected to M6Bone. It depends if sites already have IPv6 connectivity or only have IPv4 connectivity. In general, IPv6 connectivity is already available for the different partner involved in the Madrid event; thus, the best way to connect to the M6Bone is to create a tunnel between the site and an existing M6Bone router. The tunnel will be an IPv6 (multicast) in IPv6 (Unicast) tunnel.

The routing multicast protocol used on the whole network is PIM Sparse Mode. PIM is a protocol that uses Unicast routing table. The Unicast routing is done with the RIPng protocol. One host on which the tunnel is set up has to be dedicated to the multicast routing. The best if it is not the only way to have multicast routing is to use FreeBSD with the IPv6 stack developed by Kame.

5.2.1 Set up of M6Bone router

A PC running under FreeBSD 4.6 and over seems to be the solution. The experimentation done show that one host has to be dedicated to this task. It could not be the same which do Unicast routing and the different multicast IPv6 enabled applications we have to use for videoconference must not be installed on this host.
For some instructions about this installation see http://www.m6bone.net/routers.html

5.2.2 Multicast applications

The different multicast IPv6 enabled applications we have to use for videoconference are either RAT, VIC and SDR developed by UCL (University College London) either Isabel developed by Agora Systems. We have already done a few experimentation using the UCL tools during the 3rd IPv6 ETSI Plugtests. SDR is a session directory tool based upon MLD (Multicast Listener Discovery) designed to allow the advertisement and joining of multicast conferences on the M6bone. RAT is an open-source audio conferencing and streaming application that allows users to participate in audio conferences over the M6Bone and VIC is a video conferencing application. These tools are available on different platforms: Linux, FreeBSD, Windows 2000.

We must have some special features also: soundcard for RAT, and either a camera with a video capture card or a Webcam for VIC.

You can find in http://www.m6bone.net/sites-map.html the sites already connected to the multicast network and the maps of the French part, the European part and the international part of the M6bone.

6 Conclusion

We saw before, that our whole network will be a set of autonomous system interconnected together. If we want to do test for Inter-domain routing protocol like BGP-4+, it should be mandatory to use IPv6 over IPv6 tunnels and to separate correctly the traffic from our multi-site network from the remaining traffic coming from the Internet. With our tunnels we have to simulate an independent multi-site network, with all the different problematic points we could find in a really deployed network: backdoor link, possible loops.

Furthermore, it seems interesting to have an IPv4 site available in order to realize tests for transition mechanisms. It should be necessary to use the IPv4 Internet also to do test for transition mechanisms.