france telecom

Innovating for you

éclairer l'avenir

r&d

Summer 2005

IPv6: the new Internet age

FT Group Restricted

contents

Summer 2005

éclairer l'avenir r&d

Internal magazine published by France Telecom, R&D Division (ex-Cnet)
38-40, rue du Général-Leclerc
92794 Issy Moulineaux Cedex 9
Publication Director: *Pascal Viginier*
Executive Director: *S. Brémond*
Editor: *P. Gailhardis*
Translator: *Wordshop*
Special thanks to *Tayeb Ben Meriem, Caroline Philips and all the people who contributed to this issue*
Layout, production, graphics: *Idé*
Artistic Director: *D. Foissey*
Layout: *M. Trubert*
Printing: *Gilbert Clarey*
Print run: *1,500 copies*
Photos : *Axa, P.-F. Grosjean, O. Devillers, P. Desruelles, M. Féral, France Télécom, P.-E. Rastouin, J. Valat, J. Wallace/INRIA, DR.*

France Telecom – a joint stock company with capital of € 9,869,333,704 (as of 13/05/05) – 380 129 866 RCS Paris

Subscribe free of charge to R&D by sending your address to the editor

philippe.gailhardis@francetelecom.com

Read the magazine and R&D news on France Telecom intranet

http://forward.rd.francetelecom.fr/

A Music festival for our telephone lines

On the heels of Orange France on June 9, MaLigne brought out the Fun tones service on 21 June, the date of the Fête de la Musique (Music Festival) in France. It enables users to enliven their call tones with a choice of music clips, funny stories or sound effects. A service developed in less than six months thanks to "Time to Market"-mode steering …

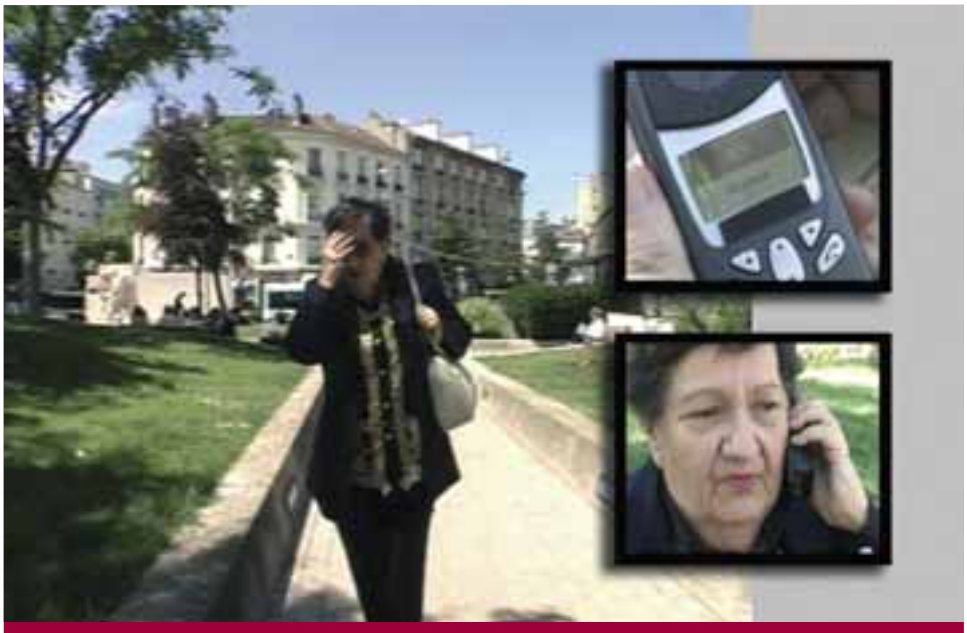
www.agence.francetelecom.com/vf/tel_maison/index.htm

France Telecom / Microsoft: Convergence at the summit

Following the partnership for convergent multimedia products signed on June 29, Didier Lombard and Steve Ballmer presented on July 6, two projects stemming from this agreement: a services platform and an IP telephony suite – LivePhone telephone range (connected to the LiveBox) and Homezone (GSM / WiFi smartphone). To be continued -

AXA + ISSY + FRANCE TÉLÉCOM = INNOVATION TO HELP FELLOW

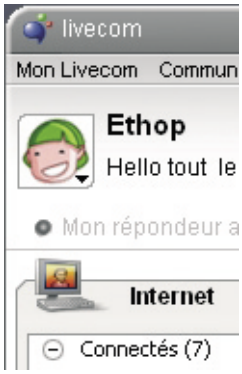
Issy-les-Moulineaux, an "intelligent town", did not wait for the signature of the partnership agreement on 9 June to serve as a test lab for R&D innovations.
Since March, an experiment has been conducted in the town with around a hundred people over the age of 60. Developed in partnership with Axa Assistance, it uses GSM / GPS mobiles to locate people in difficulty. They simply need to press an emergency button to contact the AXA Assistance telephone platform, which, at the same time triggers a text message indicating their location.
Since 27 June, Axa Assistance has also been testing the latest upgrade to Pastel'Form: the basic version of the service has been in the pre-commercialisation phase since the end of 2004. Pastel'Form enables information to be transmitted using a digital pen: the boxes ticked on a paper form can be identified on a remote level. The new version of the service has the added advantage of being able to recognise handwriting.



Axa Assistance Service at Issy-les-Moulineaux: in an emergency, press the button...

LIVECOM: THE FREE PC COMMUNICATION SOFTWARE

On 21 June, France Telecom launched Livecom – a downloadable software integrating videophony, telephony and instant messaging. A forerunner of what may well be a global communication promise, Livecom is an example of the integration of numerous free or paid services proposed by Wanadoo.
Over and above its principal functions, it also enables the user to send e-mails or text messages. R&D piloted Livecom or handled development work for the project on behalf of the Home Division (HDI/SUN).



SIMWIFE: THE SIM CARD, A SUPPORT MEDIUM FOR SECURE SERVICES

From March to June, 65 France Telecom R&D Division employees tested the "SIMWife" package of services: remote access to the FT site, signature and coding of e-mails, storing of Web identifiers / passwords on the SIM card. The SIM card in a mobile phone plays the role normally allocated to a PKI dongle or SecurID.
To take advantage of SIMWife, the user requires a telephone, Bluetooth PC, SIM card with PKI certificates and the SIMWife software on his PC. Considered more ergonomic, the SIMWife solution was found preferable to a dongle, despite the risk of non-availability if the battery goes flat. Moreover, testers consider that SIMWife is a more secure solution. In fact, the mobile has material value and, since it offers a host of services, the user systematically takes it with him when he moves around – unlike the dongle that he admits leaving lying around most of the time.
After this conclusive test, SIMWife software could become a security tool associated with other terminals apart from mobiles: PDAs, intelligent telephones or the livebox (France Telecom's homegateway).

100 Mbit/s on copper

This downlink rate was achieved in Lannion using pre-VDSL2 technology. Two high-definition TV flows encoded in MPEG-4 and three standard TV flows encoded in MPEG-2 were transmitted at the same time as broadband videotelephony and an FTP file transfer service at 40 Mbit/s. The uplink offers a rate of 50 Mbit/s.

France Telecom host to IETF

IETF, the main Internet standardisation body, has chosen France Telecom to organise its next meeting in Paris at the Palais des Congrès, from 31 July to 5 August. Around 1,500 participants are expected. It is only the 2nd time that a telecoms operator is hosting an IETF event …
www.iandf.org/meandings/IAndF-63.html

From Liberty to Fidelity

Navigating securely from one supplier to another on a fixed or mobile network or on the Internet, whilst only putting in your ID once - this is the objective of the Liberty Alliance. The aim of the Eureka "Fidelity" project, inaugurated on April 20 in Issy, is to establish a Pan-European demonstrator. It consists of 10 partners.
www.projectliberty.org/

Eleven operators for one gateway

A full-session meeting of the Home Gateway Initiative took place on July 6-7 in Sophia Antipolis. Currently consisting of 49 members, including the main operators in Europe, Japan and Australia, this forum set up on March 1st is chaired by Michel Dupire (France Telecom/R&D).
www.homegatewayinitiative.org

Dark Age of Camelot on a mobile

"Great, when I nip out to fetch the bread, I can follow what's going on!" One of the reactions of a gaming fan, who is now able to keep in touch with his favourite virtual universe. A joint effort by R&D and Goa, this Wap site is aimed at tens of thousands of players speaking five different languages.

France Telecom sponsors Mobile Web

To make access to the Web as simple from a mobile phone as from a PC - this is the objective of the Mobile Web project launched on 11 May by W3C. As founder sponsor, France Telecom started work on this at the end of June via a contribution from its Boston laboratories.
www.w3.org

QUICKFORMS: OUR SALES STAFF SAYS THANK-YOU…

During the "Noël en agence" (Christmas at the branch) operation, Caen laboratory engineers were invited to share the life of sales teams. They were surprised to see the time lost on Information System input, notably entering the same data several times. Back in their lab, they analysed the problem and proposed solutions. This gave rise to the QuickForms service…

Thanks to QuickForms, browsing is optimised, taking the user directly to the appropriate pages. Moreover, with QuickForms, certain fields on the forms are already completed with input based on previously memorised information. The operator only has to verify and validate.

Technically-speaking, QuickForms is a simple utility positioned between the Web browser and application servers. It therefore has the immense advantage of being non-structuring for the IS and quick and easy to implement.

Currently (end June 2005), QuickForms is already in use on two professional sector portals: Music (for retail branch sales staff) and RPOM (for remote sales staff). Already thousands of hours have been saved on re-entering information and many mistakes avoided …

Thousands of hours of data re-entry already avoided...

IPv6: the new Internet age

A vast range of simpler and more secure Internet services will soon be available anywhere, carried by all fixed and mobile networks. A horde of communicating machines will work for us at home, at the office, in our cars… Only the IPv6 protocol can fulfil this promise. France Telecom is getting ready for it…

CHALLENGES

Recognised as a national issue in the Far East, IPv6 allows the Internet to do what it was originally intended to do: providing an unlimited number of machines with two-way connectivity just like the telephone network. Internet usage will be transformed. A pioneer in Europe, France Telecom intends to establish a presence throughout the IPv6 chain, from the core network to its customers' terminals.

A major issue for the Group

Interview with **Jean-Philippe Vanot**
Executive Director in charge of the Network, Carriers and IT Division

R&D: Is France Telecom in general and the NC&IT Division in particular interested in IPv6? Is it an important issue for the Group?
Jean-Philippe Vanot: France Telecom has been interested in IPv6 for a long time now: we started to install equipment in our network compatible with both the IPv4 and IPv6 standards several years ago. Our initial motive was that we were concerned that we would be short of addresses. Due to the limited number of addresses offered by IPv4, we anticipated a shortage by 2007/2008. This prospect has currently been slightly attenuated. However, the issue at stake goes beyond this.
It is not a simple problem of quantity. In reality, IPv6 is a means for us to offer new services.

R&D: Why?
J-P. V.: First of all, because all our customers will be able to be assigned as many addresses as there are machines to be connected. Secondly, because these addresses will be permanent and not temporary, which is generally the case in the current IPv4 world. It is the gateway to an infinite number of new services based on interaction between machines or between man and machine.

R&D: Considering that the switch to IPv6 is ultimately inevitable with the "natural" renewal of network equipment: can we not simply

"go with the tide" instead of anticipating it?
J-P. V.: No, it is not enough to go with the tide.
If we want to launch new services and bring innovation to the market, we must head the movement and even take part in its definition in association with other carriers. As a result, we must be present on the entire IPv6 chain. Not only with regard to core network equipment, but also customer with regard to terminal equipment. Up to now, we have started by deploying IPv6 for transport in order to satisfy the requirements of certain companies. However, if we leave it there, the risk would be to lose part of the direct contact we have with general public customers, which is of inestimable value to us. Customers would bypass our services to use IPv6 on their terminals and our contribution would only be required, at best, to carry IPv6 packets by possibly encapsulating them within IPv4 flows.

R&D: How will the Group go about "being present on the entire IPv6 chain"?
J-P. V.: To switch all our technical equipment over to IPv6, not to mention the information system, will require co-ordination and take a little time. We are going to hold a meeting with all France Telecom players to amalgamate their action in order to achieve gradual migration. IPv4 and IPv6 are going to have to co-exist for a while. We will continue to implement "dual-stack*" equipment, that is to say equipment that can manage both protocols, and set up various mechanisms for the encapsulation of one protocol in another. These mechanisms call for a certain level of sophistication in our processes.

R&D: Isn't there a financial risk involved in transition to IPv6?
J-P. V.: It is all a question of timing. If we act too fast, we will waste our money. However, we must be ready when the new services that need IPv6 are brought out. This means that risks have to be taken. As a matter of fact, when Marketing asks R&D to develop a service for the Department in three months, we have to have a network ready to support it. However, more than three months are needed to introduce IPv6 into the network! This is why we are in the process of reviewing all the modifications to be made to the network, platforms and information system – domain by domain – with the aim of implementing these modifications at just the right time. Moreover, having a forward-looking vision will enable us to minimise our transformation investments. We are taking advantage of the natural need to renew equipment by replacing it with machines that are IPv6-compatible.
As a result, we are certain that our investments in IPv6 will continue to be compatible with the profitability of the products that they allow us to propose.

R&D: Is there a real general public market for these IPv6 products or are they mainly intended for the most enlightened technophiles?
J-P. V.: They will mainly be aimed at customers with a large number of machines to be connected and a number of uses, which does not necessarily mean that they are enlightened technophiles. An average user will function with IPv6 without being aware of it. IPv6 will be an advantage for household services, personal and business services alike. Having a large quantity of addresses available will allow a wide variety of equipment to be connected via a household gateway. The provision of permanent addresses will facilitate the expansion of mobile data. As far as companies are concerned, they will increasingly equip themselves with IPv6 and will look for end-to-end connectivity. These three market trends will converge around IPv6.

"As many addresses as machines to connect"

R&D: To sum up, is IPv6 therefore a major issue for the Group as a whole?
J-P. V.: It is fundamentally an integrated operator issue. This calls for transversal co-operation by R&D, Marketing and technicians, for the fixed network, for mobiles and corporate networks. The movement is under way.
In two years'time, when the services are required, we will be ready and waiting. ■

**See glossary*

Almost infinite application possibilities

Interview with Latif Ladid
Chairman of the IPv6 Forum, Chairman of the European IPv6 Task Force

R&D: In very general terms, what is at stake for society with IPv6 compared with IPv4?

Latif Ladid: IPv4 has enabled us to connect some 240 million computers to one another. Some 800 million clients connect sporadically to the services offered on these computers. But this is a one-way Internet. Indeed, with IPv4, and especially with the NAT* system, the same IP address is shared among several users. The service can only be started when the customer connects to it. There is no way of knowing in advance which addresses will have to be served, so "push" services are impossible. This is a very archaic service model for the 21st century! It's like when you call from a phone booth on the street: people can only call you back if you tell them the number of the phone booth in question. Having such a large installed base with such a large customer base and doing it with just a one-way service is absolutely not exploiting to the fullest the investment made so far in the Internet.

On the contrary, with its nearly unlimited address space, IPv6 will enable us to connect everyone and everything to the Internet, allowing two-way Internet connectivity, as offered today by the phone system. This will allow us to move from scarcity to abundance and it's then that the much-needed Internet innovations will be ignited for the decades to come: Broadband, VoIP, 3G mobiles, P2P, Grid Computing, Home Networks, Car-2-Car, IP Mobility, ad hoc networks, etc. All these applications require a symmetric/ interactive Internet, secure end2end connection, end2end security, optimised mobility which is transparent for the access technologies, a multicast functioning, and ease of use with an on the fly configuration. The Internet user experience will be totally transformed. It will be possible to plan push services. The best service the phone system gives is that someone can reach me, but reachability on the Internet is not yet part of our Internet culture. This function will be more visible when 3G is widely deployed. Then a 3G device will need not only a single permanent IP address but also multiple ones so that the device can roam from network to network and still keep the connection working. This IP roaming is not possible with IPv4, not only because of lack of addresses, but also because of lack of plug & play and return routability. For large-scale deployment of IP mobility, it's abundantly clear that IPv6 is the only protocol that can offer such a distinct feature. IPv6 will take the Internet where it has not gone before, enabling a myriad of new business models beyond the current web model. IPv6 is a vital plumbing upgrade for building the New Internet. If we finally give designers stable networks upon which to build applications, the possibilities for the New Internet are almost endless. It's the investment of the 21st century for innovation.

*See glossary

R&D: Will IPv6 allow a better response to the Internet's problems in terms of security and quality of service?

L. L.: Security and quality of service involve more than a single protocol. They both require protocols, infrastructure, service level agreements and policies. IPv6 has built-in security and new QoS "flow label" bits. It also restores the end-2-end model so that end-2-end IP identification

is a given, rather than the missing critical piece of a robust protocol. If IPv4 had had these three prerequisites, by now we would probably have developed very interesting security and QoS models far superior to those of today where NAT has been introduced, destroying the very essential piece of IP. NAT is essentially a radical architectural change to the Internet, whereas IPv6 is a conservative approach to the Internet. NAT has been falsely sold as a security box. In fact, NAT only becomes secure when firewalls are added. With IPv6, security should become a business enabler again, rather than a showstopper. IPv6 will enable design of new distributed security firewalls and VPNs that would enable always-on secure connections and facilitate easier deployment of secure applications for mobiles and wireless devices. Deploying QoS could benefit from the flow bits foreseen in the protocol, and new QoS models have been proposed by Dr. Lawrence Roberts (father of the Arpanet) from his new start-up Anagan and from his previous company, Caspian Networks. This space needs to be watched and pioneers in these two fields could take strong leadership in the New Internet.

R&D: What are the main current obstacles to rapid deployment of IPv6?

L. L.: The Internet was introduced back in January 1, 1983. It took Dr. Vint Cerf and Dr. Robert Khan 10 years, beginning in 1974, to convince everyone to move from NCP (Network Control Protocol) to IPv4. It took another 10 years until the so-called "killer app" surfaced from an unexpected place called CERN with the web implementation by Tim Berners-Lee. So the first lesson is "come armed with passion and patience".
IPv6 as a protocol is ready for implementation. However, as always when people are seeking to introduce new technologies, some pieces are missing. The IPv6 Ready Logo[1] programme has been designed to overcome this obstacle.
The technical bit missing is the management side of IPv6. This needs immediate addressing by the IETF and the vendors offering management systems.
Work is in progress on other technical items in the IETF and IPv6 Forum. The one caution here is not to rush to over-specification and over-intellectualisation of the protocol. We need interoperability testing and larger*-scale deployment, to gain experience from networks and feed results back to the IETF for validation of the standards.
The biggest challenges are always the 8th and 9th layer of the OSI model: the business drivers and the political goodwill. I have to say that the 9th layer has been very good to IPv6. Governments around the world have supported IPv6 in a formidable way as they start to have Internet promotion policies especially in the promotion of Broadband. The Taiwan 6 Million IPv6 Broadband policy is exemplary. The private sector, however, has been particularly divided. The European and US private sectors have been going through difficult years of restructuring and cost containment. New technologies have to show immediate return

"Enjoy two-way connectivity, just like the telephone network"

IPv6 ready logo program

Objectives (IPv6 Forum):

- To assist with IPv6 deployment by supplying tests

Resources:

- Implementation of a "light" certification programme in Phase 1, an optimum programme in Phase 2

Mission of the "Logo Programme":

- To establish specifications for conformity and interoperability tests for IPv6 and produce test tools
- To define a procedure for assignment of the logo and ensure its distribution

1. www.ipv6ready.org

on investment to attract everyone's attention. IPv6 is primarily Internet plumbing, not directly an application that an end-user can pay for. But that's a false problem. IPv6 is an infrastructure protocol that leading ISPs should use to differentiate themselves from vanilla ISPs and attract apps vendors to design 2-way apps and get customers excited using these new P2P or any-2-any apps.

R&D: Who are the leading countries?

L. L.: The IPv6 show is definitely happening in Asia. Japan has invented everything except the Internet. So, IPv6 is cherished as their revenge and we will be taking deployment lessons from them on how to be very granular when designing new two-way Internet applications. The Japanese government has been aware of the potential and the geopolitical significance. Japan moved swiftly in rallying industry and the public sector to work together to push forward the IPv6 agenda through various promotion programmes, including tax incentives. South Korea followed suit in February 2001 with similar measures. The current minister of communications is the former Samsung CEO who converted Samsung from an entertainment company to a computer company. As minister, he is rallying the same strategy with a strong focus on industry promotion by devising a new platform called IT839, selecting eight applications, three infrastructures and nine services.
The South Korean model is an interesting benchmarking case for Europe as it shows how a follower can become a leader. Boosted by government support and early adoption by communication carriers, domestic equipment makers, large and small, and research organizations are accelerating development of equipment needed for deployment of the next-generation Internet address system, IPv6. China has instituted a full IPv6 adoption policy by creating the China Next Generation Internet (CNGI) and budgeting over $170 million for completion by 2006. The group which started the first IPv6 initiative, called 6TNET, was formed by Patrick Coquet, Tayeb Ben Meriem and myself, alongside representatives from the Japanese and Chinese

"France Telecom is the only major European IAP to have completed major IPv6 projects."

The communicating car, one of the future applications with a big "appetite" for IP addresses (Orange Sequana, broadband multimedia auto concept car).

governments and industry. This group convinced the Chinese government to launch CNGI, which will be by far the largest commercial backbone ever built from scratch for a single technology, becoming the glue for all services in China for fixed, mobile, GRID* and research. This proves once again that a latecomer can become a leader and leapfrog over other nations if it implements the right policies. As the hub of low cost networking devices, Taiwan joined after a strategy discussion with the minister of communication and a consortium of 10 vendors leading to the creation of the IPv6 Steering Committee which then set up the IPv6 Forum Taiwan.

R&D: What about the rest of the world?

L. L.: The US Department of Defence demonstrated leadership by announcing that all equipment purchased as of June 2003 must be compatible with IPv6, as well as publishing a road map (2003 – 2007) for migrating their networks onto IPv6. This immediately drew support from the German and French Ministries of Defence who did their homework independently and are now cooperating together. The European Commission showed strong leadership and was exemplary in this respect. The number of excellent projects funded and awareness efforts deployed exceeded all expectations. The European model greatly inspired many European countries. The French Government showed us the first light in the tunnel through Senator Trégouet and then, later on, the Minister of Research Mrs. Haigneré. The French IPv6 Task Force has performed an extraordinary job without any funding, drawing exclusively on voluntary work under the leadership of Patrick Cocquet supported by a large group of IPv6 advocates. Recent achievements include the creation of an IPv6 (Poin6) Competence Centre in Brittany and a regional IPv6 Task Force. France Telecom has played a key role due to its position as an IPv6 pioneer and as an integrated operator.

R&D: Europe is still lagging behind, however, Why?

L. L.: There is no lack of political goodwill in Europe. Instead, unlike in Asia, it's industry goodwill that is lacking. This is reflected in the number of products tested using IPv6: just 4 of the 120 products which speak IPv6 properly are European. A genuine technological chasm! European Research & Development has done an excellent job supported by the European Commission, but moving to production appears more difficult. 52% of the IPv6 addresses delegated have been given to European ISPs, but just a handful of ISPs publish their service to real customers. Only a few players have realised the geopolitical impact of this new play. France Telecom is the only large European ISP that has offered and won large projects for IPv6. Japan counts 17 large ISPs and 3 dozen small and medium ISPs. Korean has 4 large ones and 70 small and medium ISPs. Europe is not reaping the benefits of its research investments.

Mobile 3G in Japan: one of the flagship applications of IPv6.

R&D: How is the IPv6 Forum contributing to the spread of IPv6 ?

L. L.: The IPv6 Forum is a world-wide consortium of over 180 leading Internet service vendors, National Research & Education Networks (NRENs) and international ISP. Its mission is to promote IPv6 by improving market and user awareness, creating a high-quality, secure Next Generation Internet and allowing world-wide equitable access to knowledge and technology. 12 IPv6 Summits are organized yearly by the IPv6 Forum and staged in various locations around the world to provide industry and market with the best available information on this rapidly advancing technology[2]. The IPv6 Forum advises governments, Corporations and NGOs on the deployment of IPv6 in all areas. The two biggest achievements are winning some of the best people on the planet to work on IPv6 and training about 24,000 engineers on a yearly basis. The IPv6 Forum is by far the largest IPv6 University in the world. The biggest challenge is to make IPv6 the predominant protocol used on the Internet. ■

2. http://www.ipv6forum.com

APPLICATIONS

"Home" gateways, acting as electronic housekeepers with a whole battery of sensors, webcams, videophones and audiovisual appliances... 3G mobiles providing a broad range of multimedia and interactive applications... Wireless broadband access everywhere in rural areas... Communicating vehicles that skip from one network to the next without losing contact... In each case, IPv6 makes things easier.

Home Networks: Terminals Galore

The increase in broadband access and public access terminals has created a strong need for IP addresses that only IPv6 can fulfil, while keeping things simple for the customer.

Source: Laurent Ruckenbusch

By the end of 2005, over five million households in France will have ADSL. In addition to the Internet, these connections will increasingly provide access to other services such as Voice over IP, videoconferencing, reception of TV programmes and Video-on-Demand. People with access to "triple play" services, such as the eXtense contract linked to the "livebox" (France Telecom's homegateway), will have at least three terminals connected to ADSL via their homegateway: a PC, a telephone and a TV set-top box. More terminals means more IP addresses! In the future, as so many demonstrations have proven, especially in Japan, not just electronic equipment will communicate but the household appliances themselves, from the fridge to the microwave.

As soon as you get home, the mobile or PDA in your pocket will connect to the local homenetwork. This profusion of communicating machines will require a huge amount of IP addresses. Of course, to reduce the consumption of public addresses, it is always possible to give these machines a private address, which can only be used locally. When they need to connect to the public Internet, the homegateway links their private address to a temporary public address. But this address translation system (NAT*) is difficult to manage for the homegateway and causes delays that hinder some end-to-end applications in real time. Only IPv6, with its practically inexhaustible supply of public addresses, can adequately meet home needs by doing away with NATs.

** See glossary*

Communicating home
By enabling the allocation of a public Internet address for each domestic appliance, IPv6 will help to achieve the communicating home.

65,000 subnetworks for one customer

An IPv6 address is composed of 128 bits instead of IPv4's 34 (see p. 24). The first 64 bits identify the network while the latter 64 bits identify an interface of a terminal connected to this network – one interface can have several addresses.
The standard indicates several ways of allocating addresses to a carrier's customers. In the basic offering, the carrier directly allocates a 128-bit sequence: a unique address corresponding to a specific terminal.
For more sizeable needs, the carrier can allocate the customer a 64-bit (/64) network prefix, leaving the customer the freedom to use the remaining 64 bits as he wishes.
Finally, the IPv6 standard will make it possible to allocate a network prefix between a "/48" (48-bit prefix), indicating a customer's entry point to the local network, and the remaining 16 bits, which will enable the customer to define 216 subnetworks (65,536). By using an autoconfiguration mechanism, each terminal can acquire an IPv6 address without any human intervention at all.
Thus, in a consumer context, subnetworks could be dedicated to intrusion detection or the broadcasting of audiovisual programmes within the home.

Automatic configuration

It is true that the allocation of a /48 to private individuals may seem disproportionate to their needs. Allocating a /64 would seem more reasonable while remaining generous. The IPv6 standard is evolving in this direction. Current IPv6 service providers are targeting experienced Internet users and simply e-mail them the addresses they subsequently have to input into their machines. But, when it comes to the general public, France Telecom cannot ask non-specialists to configure their homegateway themselves. Eager for simplicity, our customers want equipment that is ready to use as soon as it is plugged in.
For wide scale distribution, /48 prefixes should be allocated to customers in an automatic and transparent fashion. Equipped with this prefix, the homegateway will then spread the household equipment between as many subnetworks as necessary, up to a maximum of 65,536! In turn, the terminals will connect to the related subnetworks thanks to the autoconfiguration system provided by the DHCPv6 protocol*.
Working in partnership with Asian and American manufacturers, France Telecom R&D has shown that automatically supplying the customer's modem/router (CPE*) with /48 is technically possible.
Focusing on simplicity, France Telecom's future offering could allow the customer to choose from a wide range of solutions: /64 or /48 prefix, manual or automatic configuration and allocation of static address (for a Web server, for example, which must always be reachable at the same address) or dynamic address (for a single terminal). Internet access of the "heroic age", with its single PC connected without a static address, may soon seems just as outdated as the grey S 63 telephone of the last century!

Mobiles: an IP Services Explosion

Non-voice mobile applications are IP address hungry. With the increase in services brought about by broadband and the new IMS architecture, the transition to IPv6 may prove to be a necessity.

Sources: Yohann Gbahoué and Nicolas Martiquet

Current mobiles do not need IPv6: despite Orange France's twenty million or so customers, its data services only "consume" low volumes of temporary IPv4 addresses at peak times But things are changing. The increased speed provided by EDGE and especially UMTS, not to mention Beyond 3G systems, has opened up the way to a wide range of multimedia services carried by IP. Above all, the IMS* architecture will facilitate and stimulate the creation of such services (see text box).

Like in the fixed network, private addressing plans linked to NAT* are partly making up for this shortfall. They allow the same addresses to be reused from one subnetwork to another. But although this "trick" works for "machine-to-machine" type applications within an enterprise network, it is difficult to apply in other cases. This is particularly true of real-time services, the impact of which is not fully identified (particularly at peak times), due to the processing time required by these address translation mechanisms.

*See glossary

The Orange SPV, one of the rare mobile terminals already IPv6 compatible.

IMS and IPv6?

If IMS lives up to its word, IPv6 will quickly become indispensable for overcoming the hurdle of address shortage. The introduction of IPv6, with its practically inexhaustible supply of addresses spaces could also open up a new market, more particularly "push" services. Once the handsets have permanent addresses, the network can distribute information such as stock alerts or videos of football goals in real time, according to the customer's subscriptions. However, this relies on each handset having a constantly activated session – involving other resource constraints in the network. Each handset could even have several different permanent addresses allocated to it, for different uses.

IMS and IPv6 seem therefore to go hand-in-hand, especially since initial standards defined IPv6 as the only version authorised by the IMS. But time to market issues put paid to that idea. The fact that IPv6 solutions are long in coming (2006 at the earliest), and the first IMS solutions with IPv6 still lack maturity,has led that suppliers, who wish to present and market a product as soon as possible, to develop IMS systems on IPv4. This means it is the standards that have had to adapt! Noting this progress (or backwards movement?) the GSM Association has included IPv4 and IPv6 system interconnection in its rigorous testing campaign for 2006.

IMS: A Service Facilitator

Peter wishes to take Clara to see the latest Miyazaki film. After checking that she is available, he contacts her via instant messaging on his mobile phone. Together, they watch the film trailer. Captivated, she agrees to go and all they have to do now is find the nearest cinema, with the help of Mappy…

This scenario is typical of what IMS can provide in terms of service combinations. Today, mobile network cores are built on the client-server model: all requests pass via a network platform. In the future, with IMS*, multimedia sessions will be possible directly from end-to-end, from client-to-client. SIP* will be used to establish these sessions.

With this new architecture, service providers will benefit from the simplicity of SIP to develop new offers. Operators will be able to differentiate tariffs according to the type of service conveyed instead of limiting themselves to the role of bulk conveyor paid according to the quantity of bytes. Above all, SIP signalling will enable service platforms to cooperate with each other and thus build service combinations that enrich one another – including within the framework of cooperation between competitors.

But the appeal of IMS is not limited to mobile networks. With a few adjustments, this architecture can apply to any network, including the good old RTC* which is out of date now – not to mention the Internet, which will probably make massive use of SIP. The adoption of the latter by the mobile market via IMS is therefore a good opportunity to ensure interconnection with players who, on the Internet, would have chosen SIP.

The migration of fixed networks to IMS will be an indispensable way of ensuring fixed-mobile convergence. That is indeed the aim of standardisation with ETSI's* TISPAN project, which is trying to define a way of using IMS in the fixed environment.

UMTS specifications are not to be outdone. The 3GPP* published a technical report in June 2004 stipulating the conditions for IMS deployment using IPv4, accompanied by a solution for interoperation with IPv6. This report became a standard at the end of 2004.
Deployment of IMS using IPv4 by carriers has thus become an option worth considering. According to choices and IMS launch strategies (particularly the year of deployment), the adaptation to an imperfect transitory solution, generating complexity, and requiring a changeover to IPv6 before the end of the decade, may seem attractive to some.

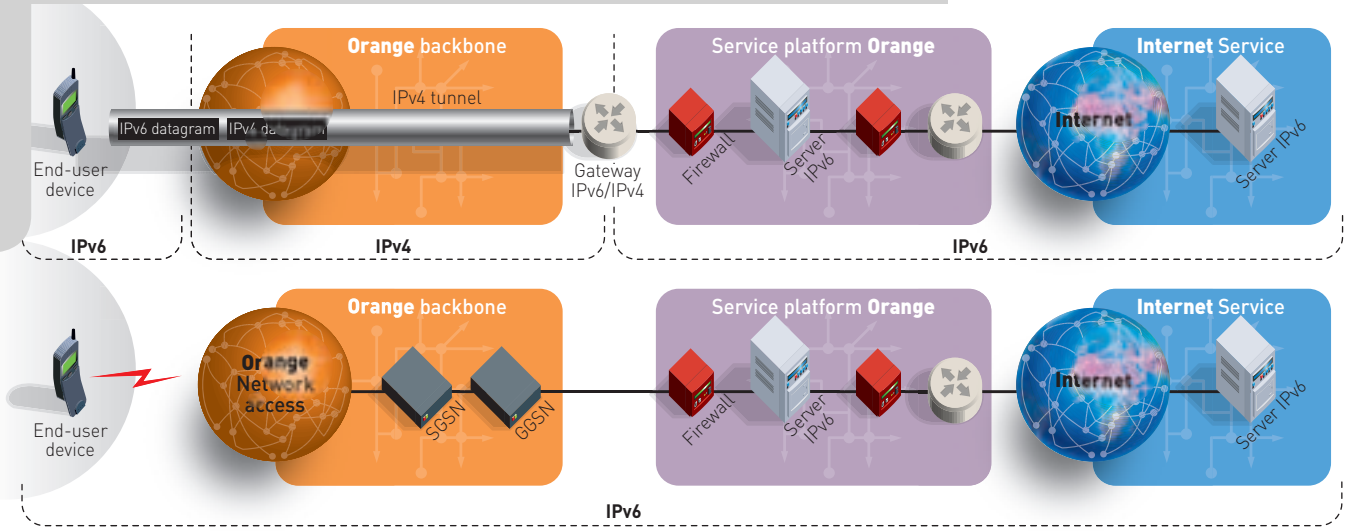
When will the changeover take place?

When will be the best time for this changeover? It is difficult to say as many questions remain unanswered. More generally speaking, the complexity and the cost of the IMS cannot be boiled down to just the IPv4/IPv6 issue.
Another issue to consider is the scale of the mobile IP services market. This largely depends on how quickly customers wish to equip themselves with handsets that are compatible with both IMS and IPv6!

Only a few models (including Orange SPV) currently offer mobiles operating on IPv4 and IPv6. Finally, operating costs need to be taken into account. For a mobile operator, most of these costs are linked to the radio segment, i.e. antennas and their connections. With its 40-byte header (compared with 20 in IPv4), IPv6 loses efficiency in this area compared with IPv4. This has two consequences: the service for the end user is degraded (less effective bandwidth) and each effective quantity of information generates more volume, thus resulting in additional costs for the transmission of the same service. To escape from this trap, operators asked the IPv6 work group at the IETF* to design header compression protocols. But this is not necessarily seen as a priority…

Two transition scenarios

A large amount of equipment is affected by the transition to IPv6. Handsets and service platforms are directly concerned as IPv6 services are provided by a server to the mobile handset itself. But the transition also affects the core of the mobile network, i.e. the part between SGSN and GGSN (see diagram). It is the core of the network that must be capable of routing IP packets, the radio end being content to transmit these packets



Transition scenarios
Above, the core network handles the IPv6 transmission.
Below, the task of IPv4 / IPv6 conversion is given to the terminals...as long as they are capable of this.

without "understanding" them, like any other information. Two very different scenarios are conceivable. The first scenario seems beneficial for the carrier as it does not require any change in the core of the network but increases the overall complexity of the solution. The handsets establish IPv6 "tunnels" through this core by encapsulating IPv6 packets, i.e. preceding them with IPv4 headers (see p. 30). The handsets need to be capable of doing this. The Orange SPV PDA phone has this functionality but as mentioned above, few products are currently available. On the other hand, this encapsulation further exacerbates the problem of header size on the radio interface.
According to the second scenario, it is the equipment in the core network that must forward IPv6 packets.
A function that the main manufacturers (Nokia, Ericsson, etc.) have announced will be available in 2006.

Broadband Access in Rural Areas: An "ad hoc" Solution

Combining satellite point of presence and the ad hoc WiFi network for the local loop seems a good way of providing broadband to rural areas. IPv6 adds its own advantages.

Sources: Philippe Bertin, Jean-François Bresse and Benoît le Sage

Responding to the demand for high-speed Internet for everyone, France Telecom launched experiments at the end of 2003 combining WiFi and satellite to cover "white areas" which are too far from a telephone exchange to have ADSL coverage. This solution was offered to local governments and end users under the name "Pack Surf WiFi" in 2004. Typically, a remote village is connected to France Telecom's backbone network

via a satellite antenna. WiFi terminals enable everyone to access a service comparable to ADSL access. But how can the distribution of these terminals, in other words the radio coverage of the village, be optimised?
Each WiFi terminal is currently connected to the satellite antenna by an Ethernet cable, a relatively costly solution that takes a long time to set up. For these two reasons, France Telecom is interested in an entirely wireless technology: "multi-hop" WiFi (standard 802.11abg).
In other words, access can be provided to buildings far from the satellite antenna by using several WiFi terminals in succession, acting as a relay. These multi-hop links are established directly between WiFi terminals without using machines dedicated to communication forwarding, according to the ad hoc networks principle.
All the terminals form a mesh network of nodes, each having the dual function of access point for customers and router able to forward communications both towards other nodes and the gateway (the satellite antenna) that links the mesh network to the wired network core.

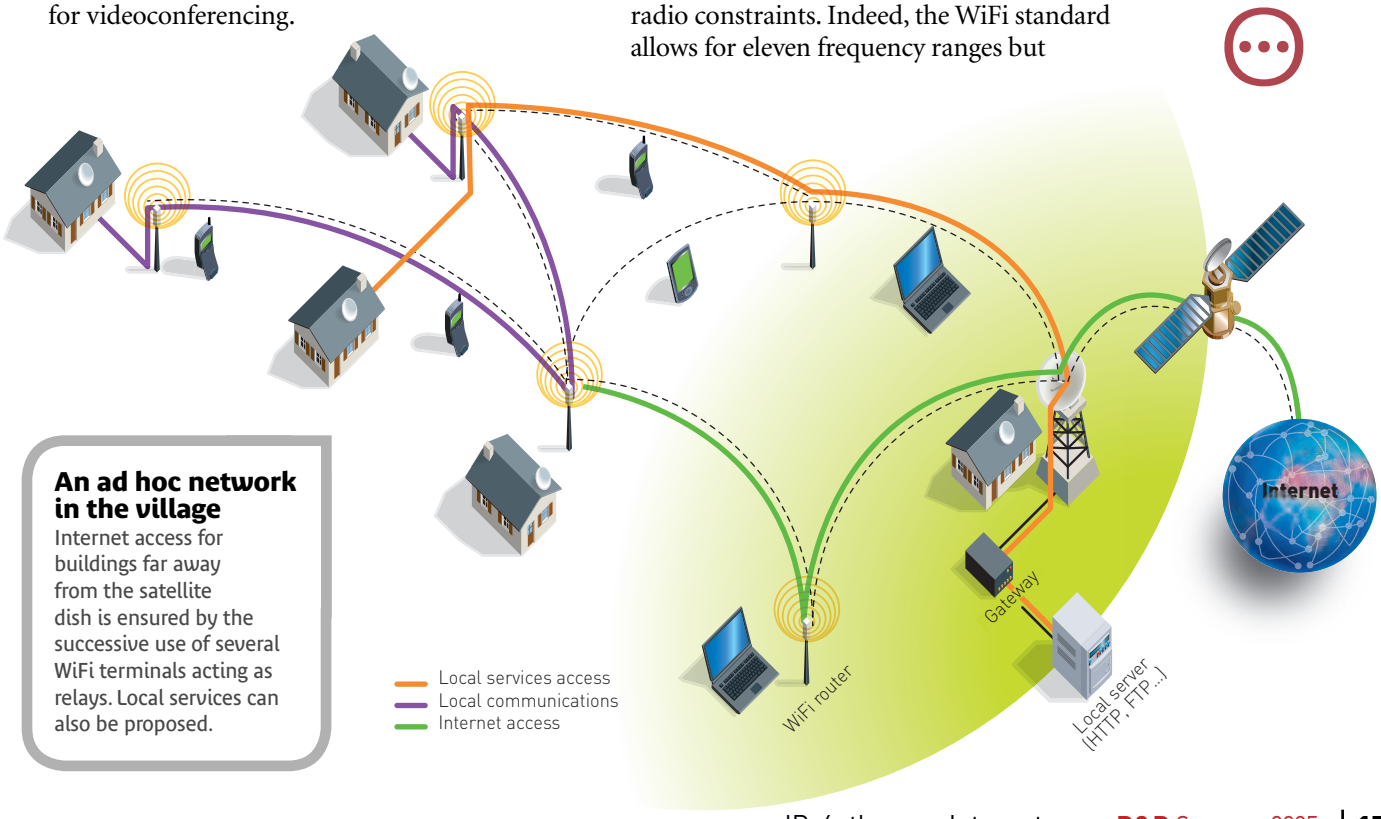
Miniature WiFi nodes

Of the numerous routing protocols available for such networks, France Telecom adopted the INRIA* OLSR*. With this protocol, paths are constantly determined without waiting for a traffic request – proactiveness is crucial for videoconferencing.

Soon, villages with broadband thanks to WiFi and satellite.

This technology was originally developed for mobile nodes, typically laptop computers belonging to mobile users. Here the use context is clearly different as the village's WiFi nodes are fixed and not in the hands of the end user. Indeed, an ad hoc network can only achieve optimal functioning if its nodes remain on constant watch, and if the owners of these nodes agree to share their computing resource for the good of the community! As France Telecom cannot oblige its customers to do this, the nodes on its network needed to remain managed directly by the operator. But this changes nothing as far as the technical fundamentals of the solution are concerned. Each node will enable around ten customers to connect.
This limitation to ten customers is due to radio constraints. Indeed, the WiFi standard allows for eleven frequency ranges but

*See glossary



An ad hoc network in the village
Internet access for buildings far away from the satellite dish is ensured by the successive use of several WiFi terminals acting as relays. Local services can also be proposed.

the risk of interference between neighbouring frequencies limits the number of frequencies that are actually useable on one node to three or four (a total speed of 11 Mbit/s at most). A large consumer of bandwidth due to its headers (see p. 26), the IP only leaves a maximum of 5 Mbit/s of these 11 Mbit/s for payload, which in turns provides the ten customers with 500 kbit/s access.
Following the success of an initial WiFi mesh network model, France Telecom decided to push forward and carry out a comparative test of industry offerings. In September 2005, an experiment will be launched with Supélec engineering institute based on a proprietary solution from Strix Systems: around fifty nodes distributed over the campus will provide access to the institute's intranet and the Internet.

IPv6 contribution

At the same time as these IPv4 developments, France Telecom laboratories have been developing a wireless mesh network using the IPv6 standard since 2004 in order to check the contribution of IPv6 "on actual evidence" in the case in point.
The contribution is threefold: simplification of routing tables, autoconfiguration (p. 25) and facilitated functioning for applications, particularly videoconferencing.

We will not deal with routing here (see p. 24). Customers' machines are autoconfigured via the WiFi node, or access point. This node transmits the prefix to the machines they need to connect to the Internet. The node and the machines communicate in "infrastructure" mode, a WiFi term to describe the master-slave relationship linking the customer's passive terminal with the network's active node. Each node must therefore have two WiFi cards, one for the infrastructure mode with customers, and the other for the ad hoc mode with the other nodes.
Where applications are concerned, France Telecom's R&D tested IP videoconferencing between its French and Japanese sites. The e-Conf software and an IPv6 unicast link were used in this test. It is important to note that the development of this type of application in the company is hindered by the massive use of access routers with IP address translation (NAT*), as this translation is incompatible with IP videoconferencing. IPv6 should overcome this obstacle.
A multicast* interactive videoconferencing experiment involving a large number of correspondents was also carried out via the M6Bone network coordinated by Renater*. This application was developed by the University of London (UCL).
Let us also note that OLSR routing aims to determine the shortest possible path. However, for real-time applications, multicast IPv6 versions minimise the end-to-end transfer time.
Without anticipating the results of the September 2005 experiment, it seems that in IPv4, and all the more so in IPv6, ad hoc WiFi networks could be a simple and cost-effective solution to connect rural areas. On an industrial scale, an IPv6 solution, AirSpace (from Cisco Systems) is already available. In relation to a strictly ad hoc network, spontaneously established between end users, France Telecom's networks should provide genuine added value in terms of quality of service, security and related services, combining, for example, presence management and position determination technology. It is in this way that the France Telecom Group can fully meet the "citizen" requirements of high-speed Internet for everyone.

Videoconference via IPv6

Among the flagship applications of the WiFi/satellite association likely to interest rural areas, France Telecom R&D has notably tested the IP videoconference. It is important to note that the development of this type of application in the company is hindered by the massive use of access routers with IP address translation (NAT*), as this translation is incompatible with IP videoconferencing. IPv6 should overcome this obstacle.
The e-Conf programme and a unicast IPv6 link were used to help conduct this test between R&D's French and Japanese sites.

A multicast interactive videoconferencing experiment involving a large number of correspondents was also carried out via the M6Bone network coordinated by Renater. This application was developed by the University College London.

France Telecom Tokyo laboratory site.

Nomadism moves into networks

In the near future, certain "mobile" networks will be just that, in the true sense of the term. Embedded into vehicles – or people's clothing or equipment – they will be an itinerant version of the local homenetwork. Thanks to IPv6…

Source: David Binet

Better than Robocop? Clad with detectors and communication resources, the future soldier, Pentagon version, will wear his own "personal network" on his travels.
On a more peaceable level, the super firefighter will have an arsenal of heat sensors, cameras and mobile phone integrated into his fireproof uniform – all this linked by WiFi to his control centre. If the WiFi relay is overcome by flames, the link will automatically switch over to a GPRS link.
This firefighter is not a character in the latest Hollywood production but a very real experiment. As part of the international Mesa[1] project, it has been presented to the IETF* Nemo (Network Mobility) working group.
The ulterior motive behind this working group was to make itinerant networks the flagship application of IPv6.
While IP mobility of handsets is now possible, the new technical challenge is to actually enable local onboard networks to keep in contact with the rest of the world even when a vehicle is travelling around. This seems much more difficult to achieve using IPv4 (see inset).
If we take this one step further - imagine our firefighter of the future on a high-speed train connected to the Internet. This interweaving of nomad networks is one of the tricky subjects that operators are trying to resolve with manufacturers and university researchers within the IETF.

Communicating cars and wheelchairs

A number of players are now showing interest in network mobility.

WIDE programmes

KAME Project

Two WIDE research and development programmes relative to implementation of the IPv6 and IPsec protocols.

TAHI Project

Nautilus6

WIDE programme covering the practical application of IPv6 in mobile communications.

1. www.projectmesa.org

*See glossary

Japan is obviously at the leading edge. Headed by Professor Jun Murai, WIDE is a consortium of hundreds of Japanese firms and universities aimed at promoting the Internet of the future. In 2003, France Telecom R&D signed an agreement with this consortium with the objective of collaborating on IPv6 in the areas of security, autoconfiguration and network mobility.
One of the concrete applications studied by WIDE involves transport. In fact, some 1,600 taxis have been equipped with a system that transforms vehicles into mobile probes, collecting data on weather conditions and traffic. In addition, there are multimedia services for passengers. The connection is either via IPv4, for a classic Internet connection, or via MIPv6* to offer a mobile service in addition.
The Nautilus6 working group is another facet of WIDE in which France Telecom is involved. It is specifically devoted to improving mobility functions under Linux

Internet access, video, onboard maintenance and security systems will bring an explosion in the requirements for IP addresses in vehicles.

and the creation of MIPv6 applications. French partners (the INT and ENST engineering schools and the University of Strasbourg, France Telecom / R&D, etc.), together with the group, are experimenting with a wheelchair with an integrated IP network and mobile router. Equipment such as a PDA, telephone and heartbeat sensor could be included in this array. The aim is to give a handicapped person greater independence with assured safety. Since the "customers" are paraplegic, ease of implementation is being studied with particular attention and this work is expected to contribute to the development of autoconfiguration standards.

"All the major automotive manufacturers are concerned by the mobility of networks"

Given the cost of this type of equipment, the business model, linked to the categories of the players involved (hospitals, national health insurance, etc.) is another aspect to be very closely examined.
On another level, all the large automotive manufacturers (not only the Japanese) are concerned by network mobility.
Within the framework of the European OverDRIVE project (started in 2002), Daimler-Chrysler has equipped a car with a mobile router developed by Motorola. Renault, in partnership with Cisco, has integrated a 3200 router into a Laguna. The idea is to equip cars with specific networks for maintenance, communication and video. BMW has studied a road safety system involving machine-to-machine interaction between the vehicle and road signs, traffic lights or other vehicles.
Apart from its involvement in OverDRIVE,

Daimler Chrysler is working on the basis of a "dissident" Nemo type of technology, within the framework of the German FleetNet project. One of the scenarios of FleetNet is based on vehicles rolling together being able to form an ad hoc co-operative network to ensure their connection to the Internet.

Links at 300 kph

Trains are also concerned. Here again, the objective is to enable itinerant executives to maintain a broadband connection with their Intranet. The provision of this kind of service is already a success in Sweden and Great Britain in particular. The SNCF (French Railways) is ready to move into a higher gear with its high-speed trains and is working with France Telecom in this area. The external connection will be via satellite or WiFi while the internal network in carriages will use WiFi. In order to propose a continuous service to users, the implementation of a "Home Agent" (see p. 26) will be necessary. However, initial technical exploration will be to determine if a WiFi link will continue to function when a mobile is moving at 300 kph, not to mention handover problems between cells and networks (WiFi – GPRS for example). Experiments to be carried out in the near future are expected to provide an answer.

Even Boeing passengers should soon have the advantage of an inflight IP connection as the Seattle firm has recently brought out a commercial service offered by an increasing number of airlines. Airbus has not been left out since it has set up a company called "OnAir" in collaboration with SITA in order to offer inflight Telecommunications services. With the growing priority given to public transport, healthcare services and road safety, there is an extremely vast potential network mobility market. France Telecom is aware of the issue at stake. At R&D, a team has been assigned to the study of network mobility and issues regarding security, handover, nested mobility and the resulting multiple attachment (see inset). The various solutions, whether proposed by manufacturers or based on free operating systems , will be tested for efficiency and interoperability. Partnerships will be set up. Intellectual property rights have not been neglected – a network addressing patent has already been filed.

The advantages of IPv6 for network mobility

It is not impossible to provide network mobility using IPv4: Cisco has proved it. However, it does raise a number of problems.

The main problem stems from the fact that a terminal's IP address, apart from the machine identity, also includes its location in the network topology. In a moving vehicle, the location is often modified, which involves the implementation of a mobile protocol, based on the Mobile IP protocol to manage network mobility. However, this has unfortunate consequences.

Firstly, it makes private addressing systems (NAT*) inoperative, a response to the shortage of addresses in IPv4: the NAT server tables have to be modified (which establish a correspondence between private and public addresses) every time the mobile changes the type of access network – in particular if temporary addresses allocated to the mobile router are of a private type. However, with IPv6, every terminal has its own public address without going through a NAT.

Next, network mobility is based on a unique attachment (for example, WiFi or UMTS). With IPv6, on the contrary, due in particular to work on "multihoming", multiple attachments can be envisioned, which enables greater reliability and higher quality of service to be offered.

Another advantage: the automatic configuration enabled by IPv6. When an executive hops into a taxi and then into a high-speed train, it is out of the question to ask him to reconfigure his PDA each time!

Finally, advantage can be taken of IPv6's hierarchical routing approach, which alleviates the task of routers, to optimise routing, which is particularly useful for example when establishing a direct link between nearby vehicles.

Furthermore, security is a very sensitive point when itinerant executives are to be allowed to connect to their Intranets when using public transport. In IPv6, however, security is "native" – even though this is not enough and a security architecture and policy must be implemented.

2. Of these, InternetCAR, OverDRIVE and KAME are already available. Cisco is the first manufacturer to propose an embedded mobile router.

With its incredibly large addressing capacity, IPv6 is the answer to the coming shortage of Internet addresses. It also means more efficient routing, terminals which configure themselves automatically, seamless mobility and a "built-in" security mechanism... The transition from IPv4 to IPv6 will be smooth, using standardised mechanisms which are already available.

Protocol IPv6: The Art of Improving **the Internet**

Providing a sustainable remedy to the address shortage (and solving other problems at the same time), IPv6 is opening the way for a new age in communications: the new-generation Internet.

Source: Mohamed Kassi-Lahlou

IPv4 was designed at a time when the Internet was only a means of communication between research laboratories, but it is now approaching its limits. In 2002, the number of communicating objects was already equal to the population of the planet: some 6 billion. And that was only the beginning. From microwaves operated remotely by mobile phone to forests being monitored by temperature sensors, objects with Internet addresses are proliferating. Equipped with sensors and multimedia equipment, the car of the future will itself be a moving local network connected to the Internet (see p 19) – and there are already more than 800 million vehicles in the world. PCs, which represent the largest usage of the IP protocol, are not to be outdone. Already 10% of the world's population are Internet users; however, in China, they are only about 6%. Yet China is catching up faster and faster…

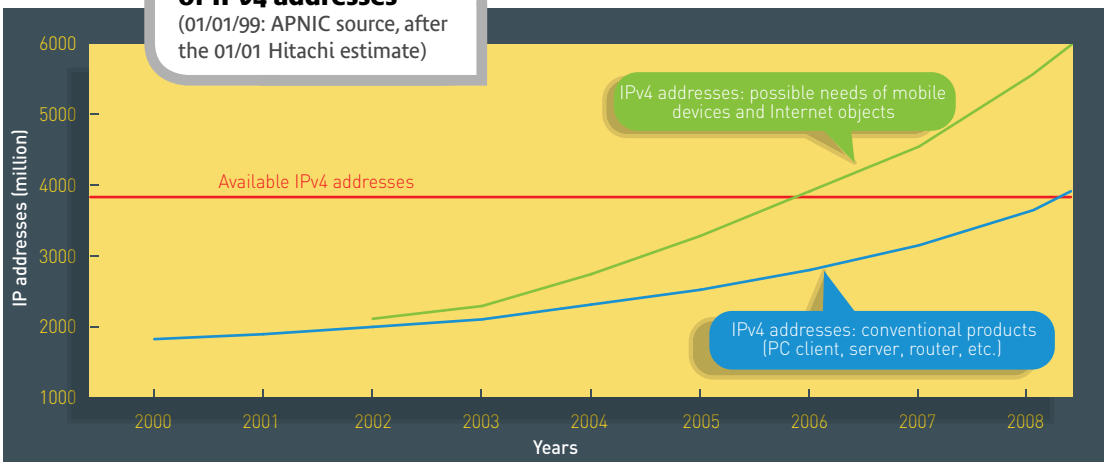
Result: of the 4.3 billion addresses (232) able to be formed using the 32 bits provided by IPv4[1], two thirds are already being used. Simply allocating the space necessary to provide IP addresses for some 1.3 billion Chinese citizens (including 320 million students!) will suffice to exhaust the remaining capacity.

A predicted shortage

This concern is not new. At the dawn of the 90s, studies predicted that at the rate at

1. *IPv4 is the current version of the Internet protocol. IPv0 dates back to 1977, the following three versions to 1978. Version 5 was allocated to an experimental protocol.*

Estimated service life of IPv4 addresses
(01/01/99: APNIC source, after the 01/01 Hitachi estimate)



which the Internet was developing, a shortage of addresses would be felt by the beginning of the current decade.
It must be said that the structure of the addressing space in those days generated great wastage. IPv4 addresses were divided into several classes: Class A enabled the hosting of 16,000,000 machines, Class B 65,000 and Class C 254 machines[2]. A company wishing to connect 30,000 PCs, for example, was allocated Class B, which could also have been used for 65,000 machines. Moreover, Class C, overly-restrictive, remained in low demand. Thus, most of the time only Class Cs are available and one needs to show one "belongs" to obtain them from the regional registers (bodies) in charge of allocating IP addresses. Apart from the wastage, this system of classes had another inconvenient feature: it led to a multiplication of routes to be handled in the routing tables because they were not aggregated: over 100,000 per router! Nowadays, router handling capacities have greatly improved, which means that this difficulty is becoming less of a handicap. Even so, handling capacity should not be squandered as it can be used for other purposes…

Postponing the inevitable

Faced with this situation, the IETF* initially reacted by remedying the most glaring faults in the addressing policy. The "classes" were done away with. Contiguous addresses will henceforth be merged in the routing tables. Addresses allocated by the ICANN* are strictly in proportion to the needs demonstrated by the bodies requesting them. Other answers have been found. ISPs*, for example, do not give a permanent IP address to each Internet user. Each time a user connects to the Internet, the ISP "lends" them a provisional IP address that can be reused by another customer when that user has finished. This "dynamic address allocation" also applies to businesspeople connecting to the Internet via a proxy* server from their company network.
Furthermore, private spaces have their own addressing scheme: the same IP address can be used locally by Peter and James on their respective intranets. Moving from a private domain to the public Internet requires a Network Address Translation (NAT*) that considerably complicates the applications obliged to "juggle" with it. The paradox is that NAT has often been presented as an asset to security, whereas this security is in fact provided by proxies*, for whom address translation is just one function among many. Companies currently equipped with NAT, however, are afraid to remove it because of security, the more so because they have not always finished depreciating it…
Whatever the reason, these empirical measures (supplied by the IETF or manufacturers) have made it possible to postpone the inevitable. They will not remedy the inescapable shortage of addresses looming before the end of this decade.

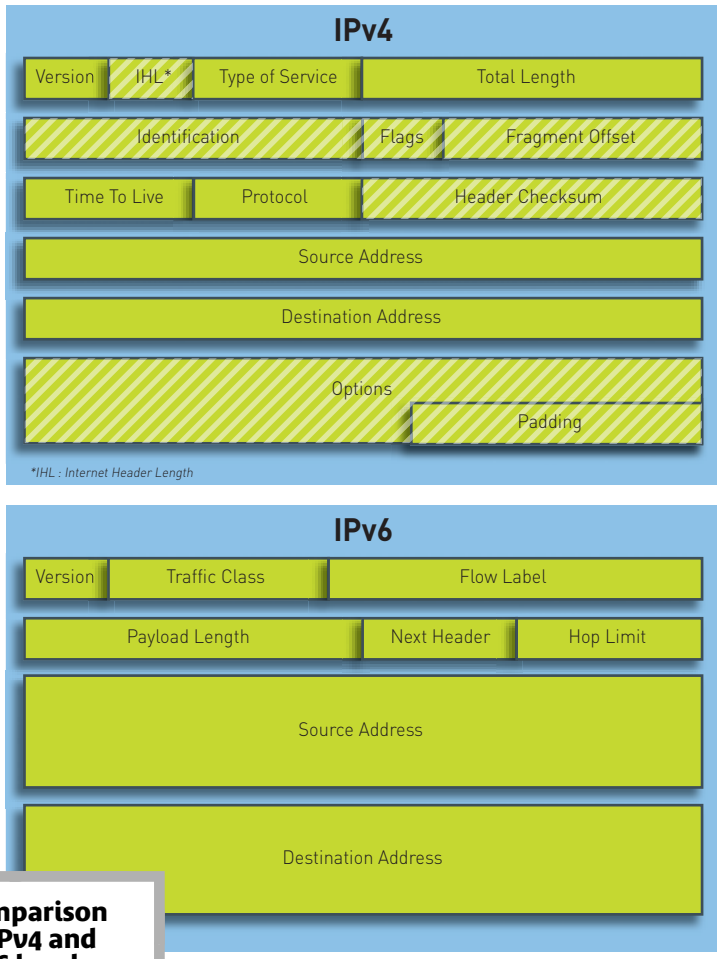
"Of the 4.3 billion addresses which can be formed with the 32 bits prescribed for IPv4, two thirds are already used."

Routers overburdened in IPv4

Besides its limited addressing space, IPv4 has another failing: its headers contain information which is used little or not at all,

2. *There is also Class D which allowed (and still does) group addressing…*

** See glossary*



Comparison of IPv4 and IPv6 headers

but which increases the workload of the routers to no avail.
To recap: a packet is made up of a useful load (the data to be transported) preceded by a header used to forward this data. The header includes information about the packet, the manner in which it must be managed, and the addresses of the sender and addressee (see figure 1).
Some fields of the IPv4 header have aged. They are indicated in the diagram by hatching and have completely disappeared from the new protocol. The same applies to "Checksum". This is supposed to show up transmission errors, but has become doubly useless because networks are now reliable and other layers of protocol perform the same function.
Other fields do not concern core network routers. The latter must, however, lose precious fractions of seconds in deciphering them before establishing that they are not relevant.
Lastly, as IPv4 headers need to contain all sorts of information, their length is not constant. They must be identified for the router so that it does not confuse a header with useful data. Handling headers of variable lengths also helps slow down the transmission of packets.

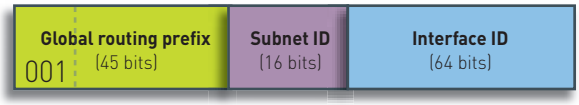
From scarcity to abundance

With IPv6, everything will change – beginning with the shortage of addresses. An IPv6 address (figure 2) comprises 128 bits as against 32 bits in IPv4, and this quadrupling produces an inconceivable plethora: the number of IPv6 addresses is approximately 3.4… followed by 38 zeros. Because of this profusion, one terminal can have several addresses. In fact, IPv6 addresses are allocated not to devices but to the interfaces that connect them to the networks. And one device can have several interfaces, connected to different networks. Moreover, an interface can itself have several addresses, local and/or public, corresponding to different uses.
Lastly, the profusion of addresses makes NAT useless and makes it possible to return to the original design of the Internet: the possibility of each device's being directly contactable via a global address.

Facility routing with IPv6

Not content with putting an end to the address shortage, the designers of IPv6 have taken the opportunity to remedy the failings in the IPv4 headers mentioned above.
Headers now have a fixed length: 40 bytes. "Checksum" has been deleted from the IPv6 header.
Fields relating only to certain equipment have become "options", grouped elsewhere in extensions. From an indicator in the header, the device can tell by which extensions it is concerned and can ignore the others.
Another simplification relates to packet fragmentation. In IPv4, when the size of a packet exceeds the maximum authorized size (MTU), the router divides this packet up

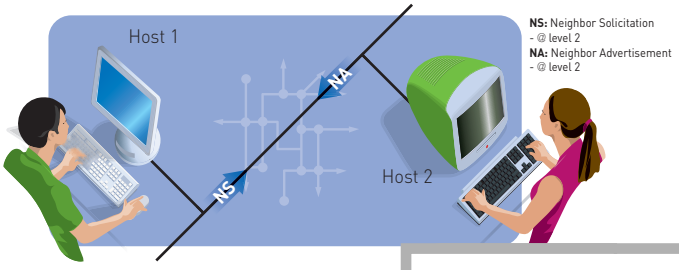
Adresse Unicast Globale
The large IPv6 addressing space makes it possible to express addresses as global unicast addresses, local addresses, multicast addresses etc



into several fragments. There can be several successive fragmentations if the packet is passing through increasingly restrictive routes. The fragments are transmitted separately via the Internet and reassembled by the addressee's device.
Fragmentation and reassembly are now only carried out in the source and destination devices of the packets.

Autoconfiguration and anonymity

Lastly, IPv6 addresses have a key advantage for applications for the general public: the manner in which they are constructed enables devices to automatically configure addresses in the network to which they are attached.
It should be noted that, of the 128 bits of an IPv6 global unicast address, the first 64 correspond to the prefix of the local network, while the following 64 identify a precise interface attached to this local network.
The device makes its own identifier. It can form it directly from the MAC* address of its network interface card. However, to retain anonymity, many will prefer this identifier to be determined in a pseudo-random fashion and recalculated at each connection.
To connect to the Internet, the device must begin by constructing a local address (LLA*) usable only on its local network. The LLA is formed of a 64-bit prefix defined once and for all, to which the device adds the 64 bits of its identifier. Given this LLA, the device will be able to send a neighbour solicitation in order to check if other devices are connected to the local network – devices with which it would be possible to exchange information (figure 3).
When the device discovers a router amongst its neighbours, the device sends the router a network prefix which, added to the device identifier, will enable the router to obtain a global address to connect to the public Internet. Note that one local network can have several prefixes, for example to enable a company to differentiate its accounting services intranet from that of the sales department etc.
Despite all these improvements, IPv6 is not a radical break with the current Internet. The basic principle of IP, i.e. the routing of packets in non-connected mode, remains unchanged, with all its advantages and disadvantages. The former definitely seem to outweigh the latter…



Discovering neighbours

"Neighbour discovery" is carried out by the ND (Neighbour Discovery) protocol through two primitives: NA (Neighbour Advertisement) and NS (Neighbour Solicitation). If, for example, there are two devices (Host 1 and Host 2) on the same local network, Host 1 signals its presence by sending out NAs spontaneously and regularly ("Hello, here I am"), while Host 2 requests a signal of presence ("Is anyone there?") if no NA is emitted after a certain waiting period.

IPv6 Mobility

In the age of "mobility", IPv6 should allow users to stay permanently connected and reachable when moving from one subnetwork to another.


Sources: Mohamed Kassi-Lahlou and Pierre Levis

Connecting to the Internet from your laptop via a WiFi or UMTS hotspot, what could be more ordinary? IP mobility is aiming for something more ambitious: to stay connected while moving from the office to the taxi and then from the taxi to the station and onto the train, despite changes of IP subnetwork likely to interrupt the established sessions. It should

be possible for everyone to be contacted in a transparent fashion everywhere, on the terminal of their choice, via any network. The most difficult issues raised by this goal are not technical but competition- and regulation-related. But let us just talk about the technical side…

The IETF's* MobileIP group has developed a mobility needs solution for IPv4. Its improvement with IPv6 is now a standard and it's a source of simplification and improvement.

Autocars SA salesman Alan goes to visit a customer. He wants to contact Bernard, a Bus employee. The IPv6 mobility of his handset (a PDA phone for example) involves three players: the home agent, the corresponding node and the mobile node (i.e. Alan's PDA).

The home agent performs the role of a dedicated secretary, forwarding all of Alan's communications. It is located in the router to which Autocars' local network is connected.

While putting his jacket on, Alan grabs his PDA and establishes communication with Bernard via the Autocars local wireless network. As soon as Alan leaves the building, the PDA switches over to the local network on a public mobile network that allocates him a temporary address. The PDA immediately informs its home agent and "corresponding node".

From that moment on, the packets exchanged between Alan and Bernard will be routed directly. This is a major advantage over IPv4 mobility, which requires all packets to be transmitted by the home agent and a tunnel to be created between the home agent and the correspondent.

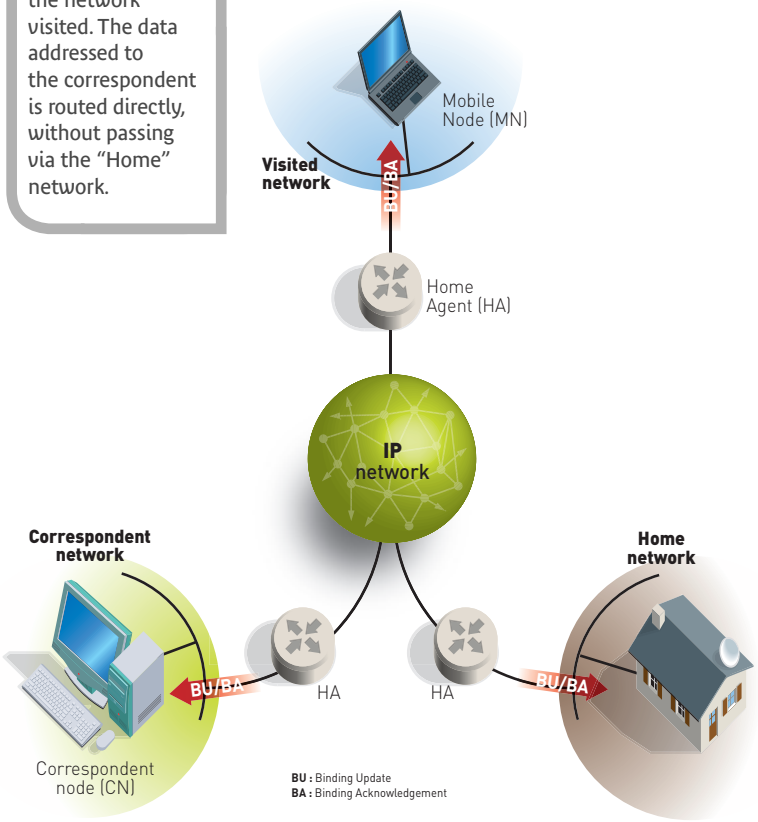
During this time, the home agent continues to act as Alan's secretary by collecting all the packets sent to Alan by other correspondents and forwarding them to him after encapsulation.

The main technical challenge of mobility remains security. In addition to the confidentiality problems raised by connecting to a competitor's intranet, one of the possible weaknesses could stem from "BU" (Binding Update) messages which inform the home agent of the mobile's movements. The particularity of the IP being that it does not separate signalling from payload, it is always possible that a hacker could interfere with the signalling: diverting packets to himself to secretly read or modify them. Solutions, called RR (return routability) or IPsec, are being studied.

** See glossary*

Smart telephone-mobile office with video terminal: the generalisation of this type of equipment will make IP mobility indispensable.

IPv6 mobility
The Home Agent forwards Alain's calls to the network visited. The data addressed to the correspondent is routed directly, without passing via the "Home" network.



Security: where do we stand?

IPv6 was developed to provide a level of security at least equal to IPv4, at a lower cost. It provides new solutions and raises some new problems… which are on their way to being resolved.


Sources: Jean-Michel Combes and Ronan Kervinio

In terms of security, the reality is not always in line with what is generally believed.
Let us take the case of NATs*. This address translation system economises public IP addresses by adopting addressing plans for purely local usage. Often presented as a security factor as it establishes a barrier between IP addresses of machines and the public Internet, it actually makes things more difficult and expensive. More difficult because, as the packets are modified by NATs, it is difficult to apply an end-to-end security policy to them: encapsulation systems must be implemented to overcome this problem. More expensive because encapsulation enlarges packets, therefore a larger bandwidth is required for the same payload. It is also more expensive in terms of development, since the softwares need to integrate the NATs into their code.

NAT vs. ULA

The main "security" argument in favour of NATs states that public addresses that are different from private addresses and only temporarily allocated, prevent an Internet user from the outside to guess the identity of the user or the topology of the local network to which the user is connected. It therefore becomes impossible to target these attacks or the sending of spam(1). Even an Internet user with a permanent ADSL connection changes public address every 24 hours, which makes it impossible to use this information to memorise sites the user normally accesses.
This argument was highlighted to defend the idea that NATs should be maintained in IPv6, although one of IPv6's main advantages is its ability to do without them. Removing NATs does not mean that it is necessary to give up the advantages of anonymity and topology masking. Indeed, IPv6 has a mechanism that allows machines to create pseudo random

** See glossary*

1. This assumes that the NAT is linked to a proxy (cache server), as is generally the case.*

Security Partners

France Telecom participates in numerous collaborative projects based on IPv6 security.

On a national level, within the scope of RNRT*, a project such as MobiSec v6 has allowed a demonstration platform to be built in conjunction with Bull, the ENST Bretagne and the INRIA. This work led to IETF* standardisation. Another RNRT project, Idsa (DNS* Infrastructure and Applications), concerned the securing of DNS transactions and data, with the main aim of using DNS servers to store the security hardware required by IPv6 mobility. France Telecom was the leader of this federating project managed in conjunction with the association of IPv6 users involving the ENST Bretagne, the IRISA and the AFNIC (".fr" domain manager).

At European level, in addition to the work of Eurescom on IPv6 mobility, projects developed within European R&D framework programmes (FP) should be mentioned. With the sixth of these programmes (FP6), the European Commission really embraced the theme of IPv6, considered as a key subject. Thus, the FP6 Daidalos project involves around forty partners with a view to developing an integrated network architecture. Above all, the large "SEINIT" (Security Expert Initiative) project was launched in 2003 as part of FP6. Part of the e-Europe 2005 initiative, it should supply the ENISA, the European Network and the Information Security Agency.

The Key Holders

In IPv6 like in IPv4, one of the challenges of the IPsec protocol involves implementing secure key management. This can be done in three different ways:

- By deploying a public key infrastructure (PKI*). But such an organisation is better in a centralised system rather than between customers of competing carriers.
- By using DNS* servers. As they cover the whole Internet, it would seem a good idea to store the security hardware needed to establish correspondence between the PKIs of the different carriers on them. DNSs must themselves be secure, which should enable the DNSSEC protocol. For the time being, DNSSEC has only been deployed, for a limited period and in an experimental capacity, in the Netherlands, where websites now have a choice between the simple ".nl" domain and the secure domain "sec.nl". In the United States, the powerful Department of Defence is pushing for the adoption of DNSSEC.
- By using the AAA* protocol, which controls access to a paying network. But this protocol is only implemented where Internet access is billed.

Mobiles are a special case. For them, the IEFT* has defined an access control protocol allowing AAA information to be exchanged from any wireless network.

identifiers that are frequently replaced. This non-traceability can only be removed by the ISP at the request of the judiciary authority.
The huge quantity of IPv6 addresses is a security factor in itself. In IPv4, a hacker can infiltrate a local network and successively transmit to all the possible addresses until he reaches an open door, that of a PC in use. All he has to do then is let his Trojan Horse in through the gap. In IPv6, there are so many addresses that, apart from an extraordinary coincidence, a blind scan would take several years.

Who can manage keys and certificates?

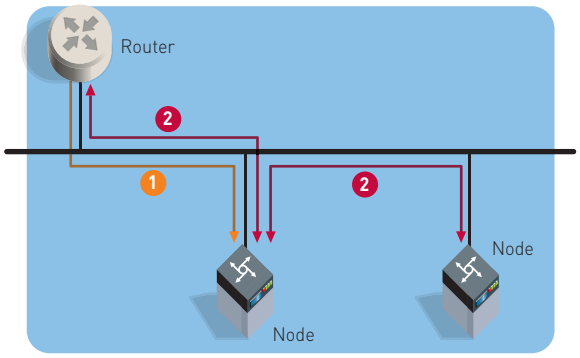
The security role of NATs therefore seems largely mythical in IPv4. On the other hand, couldn't we say as much about the supposedly native security in IPv6?
This idea of native security is based on the fact that the integration of the IPsec* protocol is mandatory in IPv6. The need to create dedicated security mechanisms no longer exists, which means additional expense for the customer and new opportunities for hackers to find weaknesses.
But mandatory implementation does not mean mandatory use. And there's no point having a car if there's no engine under the bonnet! IPsec involves data encryption, thus an exchange of keys between correspondents for which there are different secure protocols. However, how these keys are managed and stored is not provided for by IPsec (text box).
In the end, the implementation of a whole security arsenal along with IPsec does not seem much more simple with IPv6 than with IPv4 and it is feared that its usage will remain limited to the same types of application. Fundamentally, it is a key infrastructure deployment problem, an operation that requires significant investment.

The challenge of mobility

In addition to the abundance of addresses, two major advantages of IPv6 are frequently put forward: simplicity provided by autoconfiguration mechanisms and the ability to communicate without interruption when moving from one network to the other. Each of these functions raises security issues… for which solutions exist.
Autoconfiguration is carried out by a "neighbour discovery" mechanism (see p. 25). Unlike IPv4, IPv6 allows this neighbour discovery to be secured, during which IP addresses (sensitive information) are exchanged. Developed hot on the heels of IPv6, the Send* protocol secures the autoconfiguration procedure at two essential stages. Firstly, when the machine ("mobile node" in IETF language) monitors routers on the local link to configure its address: Send ensures that the information exchanged at this time is not hacked and the address therefore remains confidential.
Next, when links are directly established from node to node on the local link, Send ensures that the recipient's address and the machine have not been masqueraded.

How SEND makes self-configuration secure

(1) Thanks to Send, the node knows that the router is legitimate and configuration information can be sent. The transmission of this information by the router is secure.
(2) Each node (including the router) sends its Mac* address to its neighbours. Send guarantees that the recipient's address has not been usurped.



A hacker, for example, cannot pass off his PC as a printer on the network and store confidential documents sent for printing in the memory. Frequent changes of address resulting from IP mobility make this securing by Send particularly important.
Mobility is indeed one of the main applications and challenges of Internet security (see p. 25). A terminal that changes access network when on the move changes IP address at the same time. Security management rests largely on the knowledge of IP address of terminals authorised to access a certain resource. Furthermore, the mobile executive, user par excellence of mobility services, may connect via networks that are not trusted. The non-disclosure of private information (privacy) is therefore a particularly thorny issue in a mobility context and the IETF is just starting to take an interest in it.
Let us take the case of John, a salesperson at France Telecom. On a visit to Badguy Ltd he needs to be able to access his intranet from Badguy's intranet. In order to do this, the information he exchanges with France Telecom must remain indecipherable to Badguy. Furthermore, he should not be able to access data circulating on the Badguy intranet. Finally, Badguy's firewall should distinguish John from a hacker. This added complexity required of firewalls is compensated by the fact that, in the absence of NAT, their task is considerably simplified.

And if there is no trusted third party?

Security problems inherent to mobility are easily rectified when there is a trusted third party. This role can be fulfilled by an Orange carrier for communications between its customers. If there is no trusted third party, the user is reduced to operating a "low security" policy, hoping that Badguy Ltd does not live up to its name…
Finally, the transition from IPv4 to IPv6 (see p. 30) raises its own security issues. Thus, firewalls are still unable to detect attacks hidden within protocols encapsulated in IPv4 packets. Due to the insufficient market, manufacturers show little willingness to tackle these problems. However, firewall manufacturers have now integrated the IPv6 issue and IPv6-safe firewalls are arriving on the market.
Open transition systems such as Teredo and other 6to4s are not without their problems and old attacks, which have long been countered in IPv4, have come back like Freddy in IPv6. Closed tunnel-based mechanisms provided by a carrier are by far the safest.
To sum up, if IPv6 does not provide a miracle solution to the eternal fight, it at least has the advantage of being as safe as IPv4 in all areas. It makes IPsec implantation easier as machines and gateways will be compatible. Above all, it cuts costs, bearing in mind that from the customer's point of view, security is the least they can expect from France Telecom and it would not acceptable to make it a separately-billed option. Basically, it brings the Internet into the age of everyday security.

"With IPv6, there is such a huge number of addresses that a blind scan would take several years (for a hacker)."

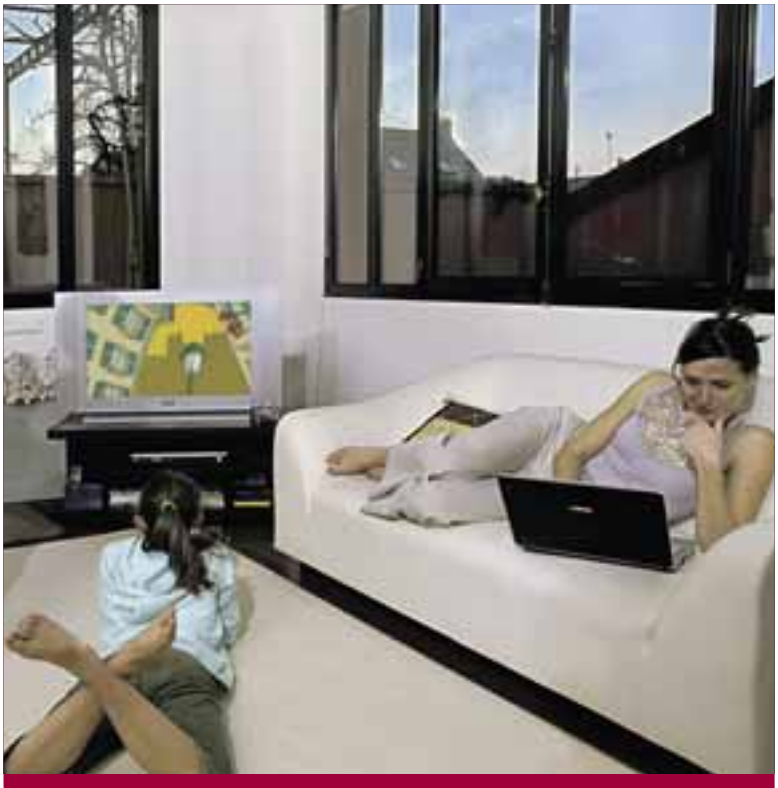
From IPv4 to IPv6: A Smooth Transition

No Millennium-style fuss: IPv4 will operate alongside IPv6 for a long time before being replaced. A range of tools is available to carriers to get this coexistence underway.

Sources: Alain Baudot and Nicolas Maroteaux

In with the new is easier when out with the old is not required! At the IETF*, the desire for a smooth transition is so great that the work group (ngTrans) in charge of preparing for IPv4-IPv6 coexistence was created at the same time as the group dedicated to actually creating IPv6. This group defined a set of mechanisms to allow each player to take the plunge when required. Then, in 2002 it gave way to a new work group (v6ops) which was more focused on practical problems – particularly that of usage scenarios.

*See glossary.



An IPv4 / IPv6 terminal isn't any more expensive than a simple terminal.

Fixed and mobile access network, enterprise network orhome network, there is set of tools for each case, divided into three main groups: translation, tunnelling and dual stack.

Faithful translation?

Translation should enable dialogue between purely IPv4 terminals and applications and their purely IPv6 counterparts. It can be done at the base (at the IP layer level itself) or at a higher level.
Without going into too much detail, translation tools in the first category act directly on the packet headers. They are imperfect inasmuch as certain fields or options of these headers have no equivalent from one version to another (see p. 24).
As the saying goes "translation is betrayal": information is altered, particularly in the case of header extensions, which do not exist in IPv4.
The other translation tools are relays or proxies*. They generally operate at an application level, which implies that they can only be used within the scope of the application for which they were designed. It is the "for lack of something better" solution for terminals or applications that cannot function in dual stack (see below).

A tunnel for every situation

Tunnelling removes the need for translation inasmuch as it travels across foreign soil without any contact with the natives!
The tunnels are created by encapsulating the packets of one protocol in the packets of another protocol. At the other end of the tunnel, a reverse operation returns

packets to their initial state. Tunnels can be established between routers, terminals or between a router and a terminal.
This encapsulation function requires effective coordination between the ends of the tunnel. This task is all the more difficult if the packets need to use several tunnels successively, or if the ends of these tunnels belong to different organisations. That is why automatic configuration mechanisms have been designed.
Manufacturers are marketing a wide variety of tunnelling techniques; each solution being a response to a specific need. France Telecom is particularly interested in Cisco's 6PE system, initially specified by the IETF under the name "BGP tunnel". Their interest stems from the fact that 6PE is based on MPLS* tunnels, which are already deployed in some of the Group's networks (see p. 32). It should be noted that there is an analogue system based on L2TP* tunnels.

Relays and mediators

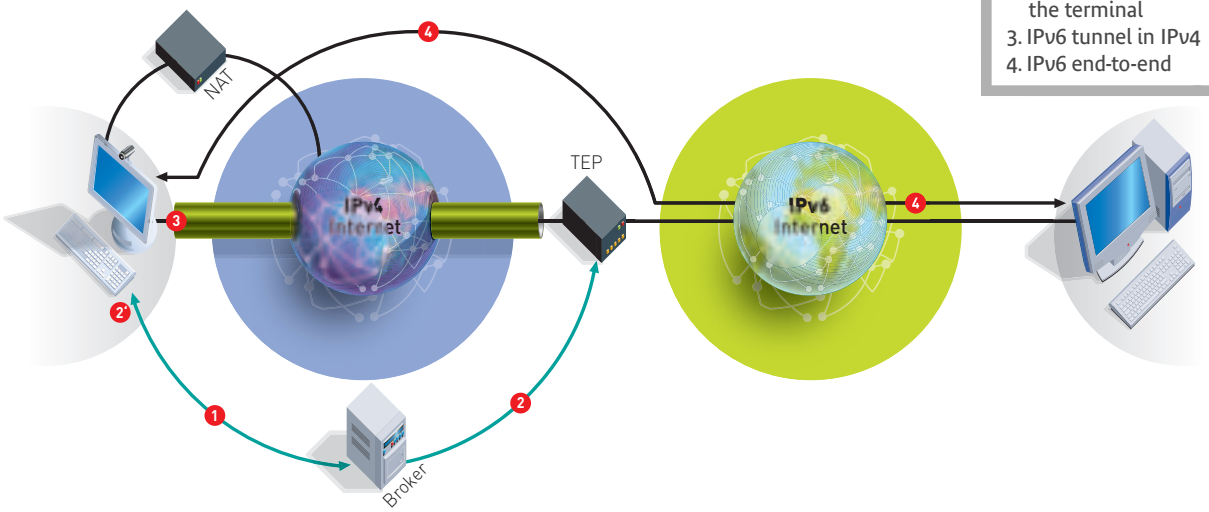
Three other tunnelling methods can be mentioned here: 6to4, Teredo and Tunnel Broker.
The purpose of 6to4 is to allow the interconnection of an IPv6 site isolated via a fully automated mechanism. It is based on a specific prefix format integrating the IPv4 address of the edge router in charge of packet encapsulation. As all the parameters required by this encapsulation are contained in the IPv6 address, no manual configuration is needed.

Microsoft designed Teredo for IPv6 terminals linked to a private addressing plan (intranet for example). Teredo enables IPv6 communication via an IPv4 tunnel that it configures automatically. The tunnel is located at UDP* protocol level, thus above the IP layer where the addresses are located. This is a way of getting over the hurdle of NATs*: translation systems between private and public addresses. Teredo implements a specific 32-bit IPv6 prefix that heads the IPv4 address of the Teredo server. The IPv4 address of the terminal and that of the NAT port through which this terminal can be reached are both indicated in encrypted form in the IPv6 address. A Teredo relay is also used. The whole system appears to be highly complex and should be considered as a last resort…
Tunnel Broker targets Internet users who, connected to an IPv4 network, wish to connect to a remote IPv6 network. The broker in question is an automatic device in charge of automatically configuring tunnels between these Internet users and the IPv6 network. It can also manage user accounts and address allocations. A Tunnel Broker is also capable of creating a tunnel from the whole of a website or network. And even of creating a tunnel via a NAT…

The advantages of bilingualism

The dual stack remains the best solution. It involves equipping

Tunnel Broker
1. Parameter negotiation
2. Configuration of the TEP (Tunnel End Point)
2'. Configuration of the terminal
3. IPv6 tunnel in IPv4
4. IPv6 end-to-end



routers and terminals with one IPv4 stack and one IPv6 stack. Totally bilingual, they can thus communicate with "monolingual" machines and applications in their own version of the protocol. In reality, much of the machine code remains common to both stacks, since IPv6 is not fundamentally different from IPv4.
Due to constant progress in electronics, a dual-stack terminal now costs no more than a single terminal. This solution, which has no particular technical constraints, aims to extend to the core of France Telecom's fixed network within the scope of "normal" updating of the installed base due to wear and obsolescence.
As for the transition to "all IPv6", the extent of what already exists on the Internet means that it could take quite a few more years… The time for IPv4 to become a dead language!

From tunnels to the VPN… or how to smooth out difficulties

There's no point in making a song and dance about switching from IPv4 to IPv6 on the Internet! MPLS "tunnels" can solve the problem…



Sources: Marc Capelle and Bruno Decraene

For any operator, the problem of switching to IPv6 is obvious: how to switch over at the lowest possible cost?
On the periphery of the network, a simple, low-cost update of the software will enable routers to "understand" both protocols.
However, the same does not apply in the core network. Here, packets have to be channelled at very high speed using costly dedicated circuits (ASIC), not easy to programme. The adaptation of core network routers means that ASIC IPv4 cards need to be replaced by "dual stack" cards (IPv4 and IPv6). To limit the expense, the upgrade is being implemented gradually at the "normal" pace of replacement of routers.
In other words, IPv4 and dual-stack routers are going to co-exist for yet another few years within France Telecom core networks.
A communication between IPv6 terminals will not necessarily be channelled by routers that are all IPv6-compatible routers. Hence the idea of using MPLS* tunnels. The advantage is that they permit fast deployment with a low level of capital expenditure and operating costs.

"As the core network is already able to manage MPLS frames, there is no need to change the equipment or its configuration."

The piggyback principle

The aim of the MPLS* protocol is to set up "circuits" ("LSPs*") in a network that is generally without them: the Internet[1].
Let us assume that we want to exchange data between Site A and Site B. With the IP protocol, the packets to be carried move from router to router, without any preconceived plan, until they reach their destination point. With MPLS, the IP packets sent by A to B must take a predetermined path by the first

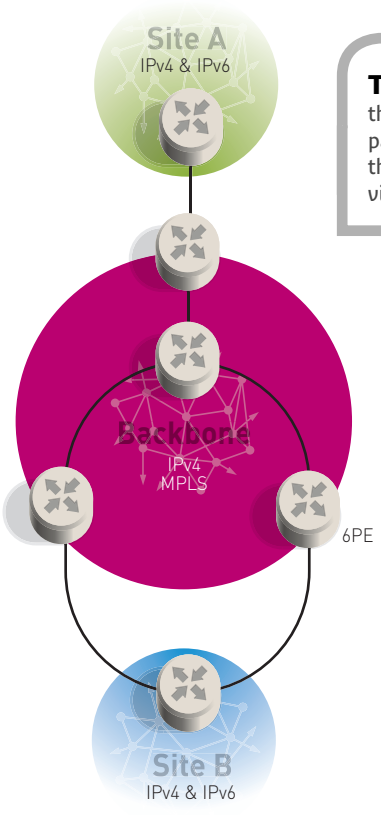
*See glossary.

1. See R&D Winter 2003-2004 p. 13.

router. This path constitutes something like a tunnel hollowed out inside the IP network to link A directly to B.
This works like a piggyback system. When the packets for B enter the core network, the first router they encounter, a so-called LER*, provides them with a label (MPLS label). Thanks to this label, it will be possible to direct the MPLS frame formed into the tunnel to the LER nearest to the recipient site.
Since this MPLS tunnelling technique ensures that flows are leaktight, it has been adopted in most of the Group's backbone networks to produce Virtual Private Networks (VPNs*) for companies on France Telecom IP networks: the RBCI*, the backbone network of Transpac France (RAEI), the Equant Internet Global network (IGN) and part of the Open Transit network (see p. 38) already support MPLS.
However, we have now realised that we are going to be able to reuse the investment in MPLS since it offers another advantage: as the letters "MP" in the name indicate, it is "Multi Protocol". In the same way as a railway truck can carry any make of lorry, MPLS is able to encapsulate any type of packet – including IPv6 packets! This being the case, the IPv4 core network can carry IPv6 concealed in MPLS frames without any problem.

Minimum investment

MPLS applied to IPv6 has two variants: 6PE* and 6VPE*.
The aim of the 6PE solution is to provide very high speed Internet on an existing network. As the core network is already able to manage MPLS, there is no need to change the equipment or its configuration, which thus limits the risk of error. On the periphery, however, the LER that receives the IPv6 packets from the client before encapsulating them must know the IPv6 protocol! A software update or change of card is therefore necessary for the LER.
We can therefore see that 6PE is particularly advantageous if there are a large number of IPv4 routers situated in the network compared with the number of LERs to be modified. Moreover, with 6PE transition can be very gradual, in proportion with requirements: if demand initially only concerns two sites, all that is needed is to modify the two corresponding LERs without



The 6PE principle: the encapsulation of IPv6 packets in MPLS allows these packets to be sent via an IPv4 core network.

touching the rest. On the other hand, there is no point in using 6PE if the core network already contains a high proportion of dual-stack routers or when an operator wants to offer IPv6 throughout its territory.
The 6PE solution, as a "tunnelling" technique, should be classified in the transition mechanism family (see p. 30). In fact, unlike the mechanisms standardised in the IETF 'ngTrans" and "v6OP" working groups, it only applies to MPLS backbones. It enables IPv6 to be deployed until a dual-stack card is installed in all network routers.
As far as 6VPE is concerned, it is simply a combination of the three types of technology already mentioned: VPN, MPLS and IPv6. Unlike 6PE, a transition solution, 6VPE meets the requirement of companies expected to grow in the future: the need to link their sites by private virtual networks using IPv6. This 6VPE solution is necessary inasmuch as it does not require any further investment in the network core, as is the case for 6PE, and investments to be made on the periphery are strictly linked to the requirements of customer companies. The financial risk is therefore limited.
We would like to bet that 6VPE will become as popular with companies as current private virtual networks on MPLS using the IPv4 standard

Having contributed to the development of the protocol right from the beginning, France Telecom has remained at the cutting edge in terms of the experiments, as well as national and international initiatives regarding IPv6. Today, the accumulated know-how is leaving the laboratories and entering the initial operational phase. Others will follow. R&D is already preparing for new challenges…

Truly Very High Speed: IPv6 put to the test

Transition management, network administration, unicast and multicast applications, etc. For IPv6, the experimental VTHD (truly very high speed) network has been a real-size testing ground. An instructive, conclusive test…

Sources: Bruno Fillinger, Philippe Le Norment and Lionel Thual

1999. Launched by the RNRT*, the VTHD (Truly Very High Speed) network is designed to support the French New Generation Internet. The GET*, INRIA* and LSR-IMAG* are the principal partners involved alongside France Telecom, the infrastructure provider. Its name is justified by its 2.5Gbps optical links.

January 2001. As one of the first operators to receive a 35-bit prefix from the RIPE* (the prefix was then transformed into /32), France Telecom immediately decided to deploy IPv6 in the VTHD network and assign it a /42 prefix for this purpose[1] derived from its own prefix. Each VTHD partner obtained a /48 prefix taken from this /42, including France Telecom for its VTHD backbone network addressing and administration platform requirements.

In 2002, the VTHD project moved into its second phase, VTHD++, which was to be completed, as scheduled, at the end of 2004. The objective was to test new services, automate the administration of these services and open up to new partners. The IPv6 protocol was to occupy a prime position in this project.

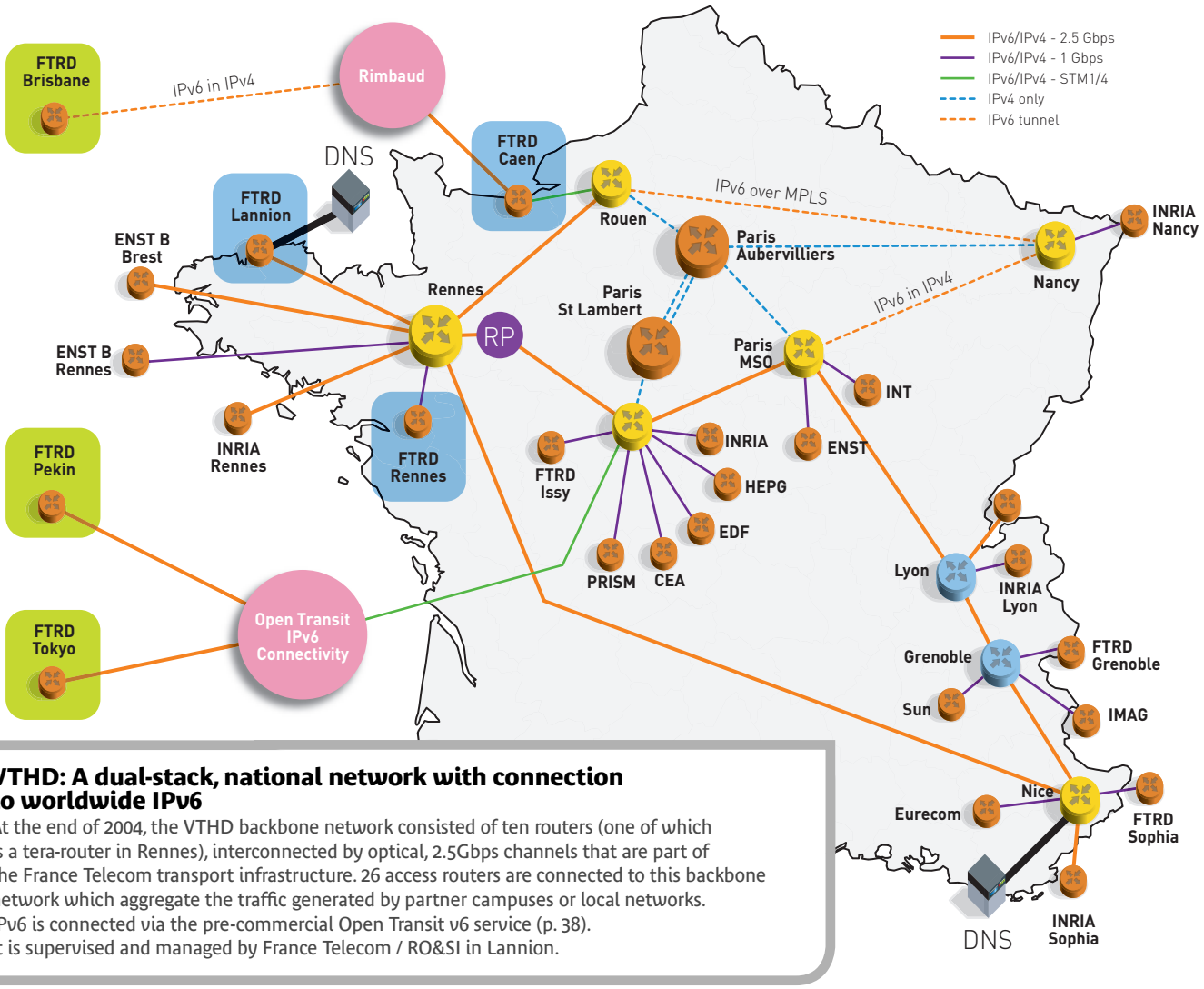
Three-stage transition

The deployment of IPv6 started back in June 2001. This was an opportunity for real-size testing of the principal transition strategies proposed by the IETF and manufacturers (see p 30).

** See glossary.*

1. /42 composed of 64 /48 contiguous prefixes.

While the architecture targeted from the outset was based on a dual-stack* approach (based on routers capable of managing both protocols), deployment phases were to be punctuated by the implementation of IPv6 in VTHD equipment at various intervals.
In the initial phase, IPv6 was implemented in peripheral dual-stack routers (Cisco). At this stage, the core network was still composed of Gigarouters that were incompatible with IPv6 (Cisco, Juniper, Avici). The technique used was VLL* IPv6 virtual link, implemented by proprietary L2 VPN* MPLS* techniques. The IPv6 flows collected by IPv4/IPv6 peripheral routers were carried in a frame* in a transparent and efficient manner since the speed of the physical links was totally maintained.
The second phase of IPv6 deployment started in December 2001 with the implementation of dual-stack IPv6 in Juniper Gigarouters. The core network then switched part of its links to dual-stack mode – without any impact on performance. To get around the problem of routers incompatible with IPv6, the network used the configured tunnels technique, which consisted of encapsulating IPv6 packets within IPv4 packets. These tunnels were implemented in the VTHD core by means of special high-speed cards (around 800 Mbps) performing the encapsulation function.
The third period of deployment started in October 2002. It involved widespread deployment of IPv6 in the VTHD core network in dual-stack mode, still without any impact on performance. To do this, a new generation of cards had to be put into service in Cisco Gigarouters. Nonetheless, there were still two purely IPv4 routers in the core network, that is to say, two Avici Téra routers. The 6PE technique (see P. 33) was then introduced and enabled the purely IPv4 Avici routers to be bypassed, at the same time offering nominal performance (2.5 Gbps) where configured tunnels were limited to 800 Mbps.



VTHD: A dual-stack, national network with connection to worldwide IPv6

At the end of 2004, the VTHD backbone network consisted of ten routers (one of which is a tera-router in Rennes), interconnected by optical, 2.5Gbps channels that are part of the France Telecom transport infrastructure. 26 access routers are connected to this backbone network which aggregate the traffic generated by partner campuses or local networks.
IPv6 is connected via the pre-commercial Open Transit v6 service (p. 38).
It is supervised and managed by France Telecom / RO&SI in Lannion.

Conclusive performance

At the end of 2003, dual-stack link performance tests were conducted within VTHD. New-generation Gigarouters made by different manufacturers were used. The tests were conducted using packets of lengths varying from 64 to 9188 bytes and confirmed that it was possible to activate IPv6 in parallel with IPv4 with nominal levels of performance for both versions of the protocol.

An IPv6 videoconference with Beijing

The partners of the project, the ENST* Bretagne, in Rennes, and the IMAG, made a substantial contribution to the studies on transition techniques, in particular by experiments on the France Telecom Lannion site with a DSTM (Dual-Stack Transition Mechanism) router. The objective of the DSTM is to enable a terminal connected locally via IPv6 to communicate with classic Internet (IPv4). To do this, the terminal must also be dual-stack and encapsulate IPv4 packets within IPv6 packets. When they reach the boundary of the IPv6 and IPv4 networks, these IPv6 packets are disencapsulated by the DSTM router and then re-issued towards the IPv4 environment.
The prototype for the encapsulation / disencapsulation software designed and tested by the ENST Bretagne and the IMAG obtained speeds of around 500 Mbps.
The deployment of IPv6 on VTHD also enabled absolutely new routing engineering problems to be tackled. In fact, the v6 versions of routing protocols, the precursor, RIP* (RIPng) in particular, and ISIS*, compliant with the OSI* model had to be tested. The latter was preferable since it performed better and was already in use in IPv4 for internal routing in the VTHD core network. IS-IS Multi-topology (IPv4/IPv6) was successfully tested and implemented in 2003.
The VTHD network also demonstrated one of the advantages of IPv6 in terms of engineering: The implementation of aggregation allowed routing tables to be considerably reduced. In fact, IP addressing enabled the increase in the number of interfaces on each node to be anticipated and these interfaces could be activated without affecting the routing plan.

Administration along the same lines

Particular attention was devoted to VTHD network administration. A team of four people from France Telecom / RO&SI was assigned to the administration of versions v4 and v6. There were few administration tools available for IPv6. Only one company had a version of its product that was compatible with v6. This tool, derived from the software designed for IPv4, was not yet up to scratch, inasmuch as the large number of addresses available in IPv6 generated excessively long processing times. Moreover, it was impossible to retrieve data relative to IPv6 traffic.
In partnership with the Lorraine INRIA, France Telecom therefore developed a management and supervision tool, inspired by RBCI* supervision software and existing commercial applications.
The solution adopted was not to use probes but directly call upon the MIB* databases associated with routers. The problem was that the standard suitable for IPv6 MIBs was not completely finalised. Each manufacturer had developed a proprietary solution and long-term availability of records from one router to the next was not guaranteed. As a result, a fairly basic method had to be used …
Supervision data was viewed via a Web page by means of a server developed using free software. In the event of a fault, a mirror module enabled VTHD partners to locate the sources of problems themselves on a map.
Moreover, in 2002, using free software (Bind 9), France Telecom developed a DNS* naming service common to IPv4 and IPv6. This DNS service was integrated into the worldwide DNS tree structure. In 2004, an experiment with secure DNS (DNSsec)

took place, taking advantage of the results of the RNRT IDsA project[2].

Grid software

A tool as efficient as VTHD is a tremendous vector for a wide variety of applications, in IPv6 in particular.
Example of a speed-consuming type of use: Grid and network software (Grid computing) that enables complex computations to be shared between a large number of remote computers. This experiment is part of a futuristic vision where a private individual can connect a PC to the Worldwide Internet in order to access phenomenal computation capability.
The capability in question is due to the interconnection (Grid setup) of unused central unit resources on other computers connected to the same Grid. This technique is even more efficient if opened up to an unspecified number of machines communicating with one another on a point-to-point basis. This is where IPv6 offers a veritable plus point, due to its capacity to assign global addresses (see P. 24) to each Internet terminal.
An example of the application of speed-consuming Grid Computing techniques: the display of 3D "interactive and distributive" synthesis images. Here again, this involves distributing computations between clusters of remote terminals. Experiments with this technique were conducted by the Lorraine INRIA on VTHD using IPv6. The application checks the IPv6 performance of the VTHD network since two-directional speeds of up to 2Gbps are observed.

Demonstration of the V-Eye programme; example of an interactive multimedia application on the Internet with a large number of participants.

Applications with excellent media capability

Another advantage of IPv6 is that it lends itself well to multicast*. On the VTHD network, this IPv6/multicast association is used to advantage by V-Eye, the INRIA software that enables a large number of people to participate in the same voice over IP videoconference.
IPv6 multicast also has many video applications, such as VoD (video on demand) or the broadcasting of TV programmes by streaming (in real time, without prior downloading). France Telecom R&D checked it by setting up a unicast* and multicast streaming application on a Windows Media 9 server located in Rennes. A connection was established with the M6Bone network controlled by Renater (French research network) using a technique encapsulating multicast packets within IPv6 unicast packets. Work on IPv6 multicast continues with France Telecom playing an active part.
France Telecom also uses VTHD extensively in-house. The IPv6 interconnection between R&D sites was extended to San Francisco for the demonstration of services such as videoconferencing with the e-Conf videophony software (see R&D Winter 2005, P. 23), which is now IPv6-compatible. A videoconference using IPv6 e-Conf can even take place between Lannion and Beijing (China).
Finally, VTHD++ has above all allowed IPv6 to be put to the test. Inter-operation with IPv4, service quality and protocol implementation mechanisms have been tested in a real-size environment, together with customer management and a wide variety of applications. R&D teams have acquired further skills of benefit to the Group as a whole, both in improving response to RFQs as well as assisting with the training of operators in the field.

2. http://www.idsa.prd.fr/

Open Transit v6: IPv6 connectivity – right, left and centre!

In the autumn of 2005, around fifty hotspots in the world will be interconnected with IPv6 via the Open Transit operator-dedicated backbone network. This is the culmination of three years of preparation and gradual integration of IPv6.

Source: Vincent Gillet

From July 31 to August 5, 2005, the 63rd meeting of the IETF held in Paris is expected to be a showcase for France Telecom's expertise in IPv6. The Group will, in fact, be responsible for the IPv6 connectivity of the meeting with other countries via its long-distance networks. This well-publicised event represents only one stage of a long journey. Since 2002, IPv6 connectivity has been proposed to real customers on a dedicated network linking Paris, London, Brussels, Frankfurt, New York and Tokyo. The links between these cities are handled by the Group's international backbones, notably the EBN* (for Europe) and the NABN* (North America). The points of presence of this dedicated IPv6 network were obtained by upgrading relatively old routers "only" capable of handling bit rates of 155 Mbps. This choice was motivated by the desire to "gain some experience" with a relatively modest sized network that would not require any additional capital expenditure or operating costs.

For operators accustomed to standard Internet, "steering" IPv6 equipment requires a period of adaptation – rather like someone driving an automatic car when used to a manual gear box. Since this dedicated network could tolerate a few hiccups, operating teams were able to get used to it gently, without any apprehension.

In light of this conclusive precedent, France Telecom decided to shift into a higher gear on the Open Transit network by introducing widespread integration of IPv6. Connecting

*See glossary

Open Transit: an IPv6 backbone
Dedicated to operators (including France Telecom), research networks and IAP's, this international backbone network is now entirely "double stack" IPv4 – IPv6.

around fifty sites, Open Transit is the Group's international backbone network for fixed or mobile carriers, research networks and IAPs*. Once manufacturers (Cisco and Juniper) had demonstrated that their dual-stack* routers were fully operational, in June 2005, it became possible for Open Transit to migrate to a 10 Gbps network, able to support both IPv4 and IPv6. The IPv6 traffic currently handled on the dedicated network is expected to switch over to this "Open Transit v4-v6" in the autumn. Since the beginning of the year, IPv6 has been an option proposed free of charge to Open Transit customers when permitted by their sites. Renater (the French research network) and German, French and Belgian IAPs have already taken advantage of the option, as well as Wanadoo and the VTHD* project (very high speed), France Telecom's experimental network. With the extension to around fifty sites, this IPv6 offer will continue to be a free option integrated into the normal Open Transit contract.
Moreover, the Group has started to interconnect Open Transit v6 to the networks of other carriers such as NTT or Tiscali.
And in everyone's best interests, it is encouraging those lagging behind to take the plunge…

Promise kept

In January 2004, at the "Global IPv6 Launch Service", a major milestone for the launch of IPv6 in Europe, France Telecom made a promise: the Group will satisfy IPV6 connectivity requirements by adapting its international IP transport network. This commitment is part of the roadmap (2004 – 2006) recommended by the European Commission IPv6 Task Force. France Telecom is a member of the Steering Committee for this Task Force. With Open Transit v6, this promise has become a reality.

IPv6 by satellite: a conclusive test

With the SATIP6 project, France Telecom and its European partners have demonstrated the feasibility and advantage of using IPv6 for point-to-point links routed via a satellite connection

Source: Alain Debray

On the heels of Télécom 1 and Télécom 2 and its participation in ex-consortiums such as Intelsat and Eutelsat, France Telecom has established itself as a major player in the realm of telecommunications satellites. The role of its subsidiary, Globecast, the world leader on its market, is an additional proof.
Launched in 2000, the "Demons" projects aimed to reproduce the behaviour of a satellite IP multimedia system in real time. Its migration to IPv6 was handled by means of in-house projects. The European SATIP6 project is part of a similar satellite service development perspective.
From 2002 to the end of April 2004, the SATIP6 project included France Telecom, Alcatel Space, AQL, the software house, the CNRS LAAS[1], Sintef, the Norwegian laboratory and the University of La Sapienza, in Rome. For France Telecom R&D Division, this project is part of an innovative approach aimed at defining the IP networks of the future, based on heterogeneous access networks. SATIP6 follows on from the Brahms project that defined IPv4 network interconnection solutions via a transparent satellite. Its principal goal is to conduct experiments with IPv6 transiting via a "regenerative" satellite using DVB-S/DVB-RCS technology*. The architecture of the network studied was a VPN* connected to the IPv6 network via a gateway. In this case, the platform set up to conduct the tests was connected to the experimental RENATER IPv6 network that functioned with public IP addresses.

1. Systems analysis and architecture laboratory

**See glossary*

Did you say regenerative?

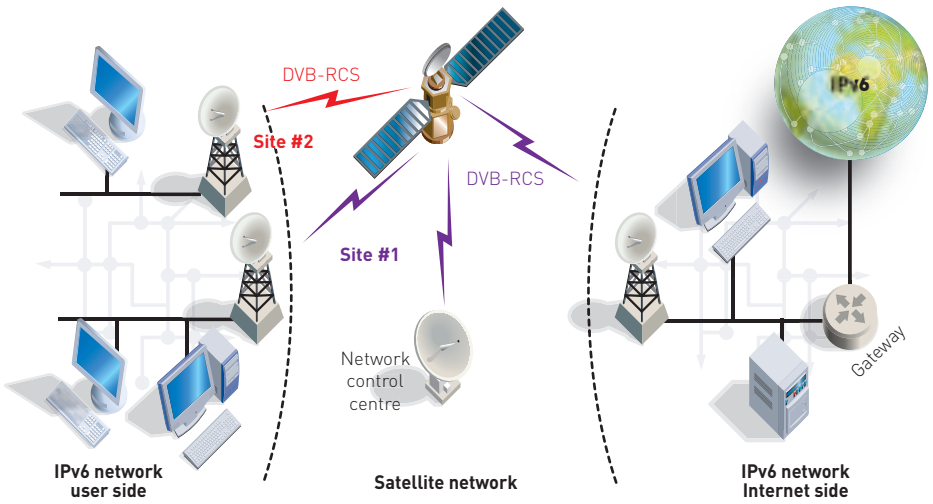
A regenerative (or OBP – onboard processing) satellite is one able to switch flows at the level of the lower layers of the IP protocol: satellite terminals can dialogue directly with one another, which enables cutting transmission latency time in half. At the same time, OBP allows better use of the bandwidth.

The project started with a review of State-of-the-Art technology and market requirements. Partners then established architecture models and scenarios. They drew up the functional needs and specifications. Next, they conducted tests on a simulator before moving on to the development and setup of the actual platform. Simulations enabled the testing of mechanisms to improve service quality and optimise TCP* performance in order to rectify the problem of latency inherent in satellites[2].
Once these mechanisms had been installed on the satellite platform, IPv6 tests showed that end-to-end quality of service could be defined directly by the user by means of a QoS* agent, configurable via a graphic interface. This function was used by European space agency projects within the framework of its research into NGNs[3]. Moreover, the priorities managed from satellite terminals were defined with the DiffServ* protocol.
Experiments were successfully conducted with teleconferencing and videoconferencing, video streaming and mobility assured by a parent agent (see p. 26): automatic reconfiguring of a PC in a mobile situation on a foreign network took under three seconds. Static multicast video streaming tests were also carried out. The home page of the Japanese Kame project, well known to the IPv6 world was also successfully tested: this page shows a little tortoise that can only be animated with IPv6.
From a security standpoint, Alcatel Space developed a protocol to secure the IP layer on the satellite link (SATIPSec). This protocol, based on the exchange of keys (called Flat Key Hierarchy) demonstrated its simplicity and efficiency. Although it also functions with IPv4, it is particularly suitable to IPv6 and multicast.
The IPv6 layer is supported by a link layer protocol also developed by Alcatel Space. This protocol ("IP Dedicated") sets up a virtual satellite LNA* via an IP packet labelling technique. Like SATIPSec, IP Dedicated is optimised for IPv6.
To sum up, the SATIP6 platform has proved to be perfectly reliable, reusable and adaptable since its development work was carried out using a Linux base. As far as IPv6 is concerned, it kept its promises by showing that it worked perfectly in this context and, at the same time, offered new possibilities. This work, which might be of interest for the connection of rural areas (see p. 16), has been successfully presented in various forums and symposiums. The standardisation groups, the ETSI* in particular, have made a start on its translation.
What's next? Following the fourth call for projects within the framework of the 6th PCRD, the European Commission has chosen a project that uses part of the results of SATIP6, at the same time developing upstream solutions and technology. Proof, if it were needed, of the usefulness of EC bodies for IP satellite solutions and, more particularly for IPv6, within the framework of its broadband access everywhere policy. The project, called SATSIX, will start at the end of 2005.

2. The solutions tested were of the PEP (Performance Enhancing Protocol) type, TCP Sack…

3. Next Generation Networks

This tortoise only comes to life in IPv6… (www.kame.net)



SATIP6 : an IPv6 network by satellite
IPv6 virtual private networks (VPN) are established via a gateway.

France Telecom, a key player in IPv6 on the world stage

Interview with Pascal Viginier, Executive Director responsible for the Research & Development Division

Interview by Tayeb Ben Meriem

R&D: How long has France Telecom been interested in IPv6? What know-how has it built up in the field?

Pascal Viginier: France Telecom has been involved in the work on the protocol since the very beginning. From 1994, our laboratories participated in the ETF* working groups which first developed it. They developed conformity tests which enabled the very first IPv6 router to be test-benched in 1996.

We are also contributing to the 3GPP* on questions linked to IPv6, particularly at IMS* level.

Finally, the IPv6 question has also been discussed in the UIT-T*. In this context, France Telecom, in 2002, contributed proposals to Study Group 13 (SG 13) to include IPv6 as an area of study.

In France, we are a founding member of the G6: this association, led by Renater*, was set up in 1995 to group all the French IPv6 experts, and notably publishes the reference book on IPv6[1], regularly updated with contributions from France Telecom R&D Division on developments of the standard and associated protocols. Along with our contribution to the "G6 Book" group, we organise the G6 deployment working group. The G6 has given IPv6 genuine visibility in France, notably by overseeing deployment of the G6bone network.

In 1998, France Telecom set up Rimbaud, its first experimental IPv6 network connecting five R&D centres and interconnecting with the 6bone (the worldwide experimental IPv6 network).

We then determined that our priority should be the dissemination of IPv6 expertise, setting up an IPv6 Skills Centre in 2000 to federate our efforts, launch new initiatives and seek out zones in the world with a highly-innovative attitude to IPv6.

R&D: Where are these zones of innovation?

P. V.: They are mainly in Asia, the United States came on board later.

In July 2000, the Japanese government made a major commitment to IPv6, creating the WIDE consortium. Led by Professor Jun Murai of Keio, it brings together more than 100 companies and 30 Japanese academic institutions, with more than 500 members.

WIDE gave rise to several ambitious projects and France Telecom was immediately determined to join them. A draft agreement (MoU) has been drawn up to combine our skills in network mobility, security and auto configuration. This is the framework for our participation in Nautilus[2], in particular. For France Telecom, this agreement represents a unique opportunity to acquire know-how which contributes directly to projects ranging from preliminary research to operational deployment, in a region aiming to become the world leader in IPv6.

"Our laboratories participated in the IETF working groups which designed IPv6."

We are also involved in other projects in Japan, including direct collaboration with local universities. In this context, our laboratory in Tokyo significantly facilitates initial contact.

**See glossary*

1. "IPv6, théorie et pratique", by Gisèle Cizault, see bibliography p. 52.

2. See p. 19.

R&D: And who comes after Japan?

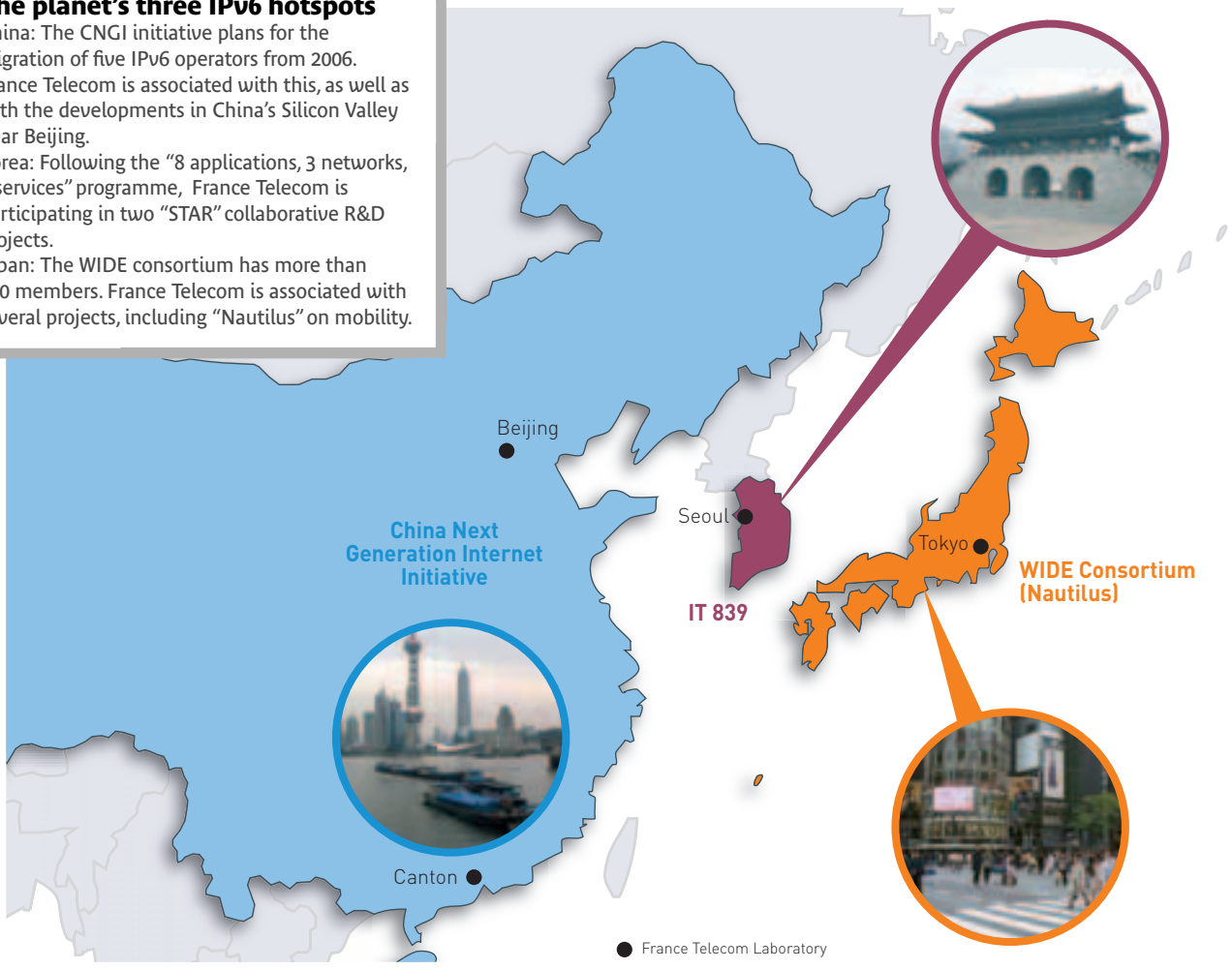
P. V.: Due to the determination shown by its research centres and industrial companies, Korea is ranked second in the world for IPv6 innovation. Indeed, the Korean government chose to follow the example of the Chinese government in February 2001. The Korean Minister of Communication and Information announced a very ambitious action plan involving industrial companies and research institutions, and accompanied all of the above by a clear strategy based on a winning magic formula: 8-3-9 (8 applications – 3 networks – 9 services). Here again, we wanted to be involved in this initiative. Following a French government mission in the September 2003 and a large number of bilateral meetings, we were chosen, along with two Korean companies, as one of the two French partners for the STAR (Science and Technology Amicable Research) project jointly funded by the two embassies. A second, larger STAR project to deal with auto configuration and mobility is being discussed. Here again, the presence of an R&D team in Seoul is a major advantage in terms of contacts.

R&D: China will certainly not take a back seat...

P. V.: In 2002, we started discussions with a view to join 6TNet, a major government project designed to explore the opportunities of IPv6. The project involved the five Chinese operators, the world academic operator (CERNET), Japanese and Chinese manufacturers and France Telecom, a member of the steering committee. Our Group contributed two crucial elements: the eConf visioconferencing software and a platform of IPv6 quality of service measurement. The 6TNet project led to the CNGI (China Next Generation Internet) initiative, the most important milestone in the world in this domain as it plans to migrate the networks of the five operators to IPv6

The planet's three IPv6 hotspots

China: The CNGI initiative plans for the migration of five IPv6 operators from 2006. France Telecom is associated with this, as well as with the developments in China's Silicon Valley near Beijing.
Korea: Following the "8 applications, 3 networks, 9 services" programme, France Telecom is participating in two "STAR" collaborative R&D projects.
Japan: The WIDE consortium has more than 500 members. France Telecom is associated with several projects, including "Nautilus" on mobility.



in 2006. France Telecom was determined to be involved in this important initiative and particularly in its R&D component. As a member of the IPv6 Forum, we are actively involved in the IPv6 Forum Summit in Beijing and its demonstrations.
Finally, in 2004, the year of France in China, we jointly organised a seminar in Beijing with the Ministry of Research including a workshop on IPv6.
In April 2005 in Beijing, ministerial cooperation led to the signature of a draft agreement (MoU) between the two Ministers of Industry in the presence of France Telecom's CEO.
A working group will be set up at the Ministry of Industry under the responsibility of the national IPv6 Task Force, where France Telecom R&D Division will play a central role.
The aim is to devise an IPv6 action plan to set up projects of mutual interest with Chinese entities involved in this IPv6 technology.
More generally, we have extensive ambitions in this key region. As well as having laboratories in Beijing and Canton, we should also mention France Telecom's role as one of the four non-Chinese members of the international committee of IPv6 consultancy experts for Zhong Guan Cun, along with the IPv6 France Task Force, the IPv6 Forum and NTT.
Located in the north of Beijing, this "Chinese Silicon Valley" has been placed under the responsibility of the Beijing city authorities. This is the best sign of recognition of our know-how and our involvement in IPv6 in China.

The Beijing Olympic Games will be a showcase for IPv6... with the help of France Telecom (visit by the Chinese delegation to the Issy site).

R&D: Is there as much political determination in the United States?

P. V.: Since they had a large quantity of IPv4 addresses, the United States took a back seat until the Pentagon and then the Department of Commerce decided to enter the race in 2003 - mainly for reasons of security, but also mobility and autoconfiguration. A road map established in 2003 plans to migrate the entire Pentagon's terrestrial and satellite networks to IPv6 by 2007.
A North American IPv6 Task Force and a project, Moonv6, to which we have contributed, are the immediate results of this. Moonv6 aimed to deploy an experimental IPv6 structure nationwide and to test IPv6 applications. This contribution to the project was possible due to our position as an active member of the IPv6 Forum and a member of the European IPv6 Task Force steering committee, bodies with which the North American IPv6 Task Force has been closely collaborating for three years. Our laboratory in San Francisco also facilitates contacts.

R&D: What about Europe?

P. V.: Europe's positioning regarding IPv6 was determined in 2001 with the creation of the European IPv6 Task Force with France Telecom R&D Division as one of its founding members. Our road map proposal was accepted, as well as the plan to deploy a WLAN* network based on Mobile IPv6 between European university campuses. More particularly, France Telecom contributed to the WG4 (Trials) working group. We have continued this cooperation as a member of the Steering Committee of the European IPv6 Task Force, set up in 2004 with the purpose of drawing up a strategy and a road map for the deployment of IPv6 across Europe.
The Commission also wanted to give a strong signal by supporting the establishment of two pan-European networks,

6Net for the academic world and Euro6IX, run by operators including France Telecom. Our contribution to this network consisted of two IPv6 links, Paris to Berlin and Paris to London, as well as an IPv6 exchange point in Paris. This was made possible by the NC&IT IPv6 OpenTransitv6 international connectivity offer for Europe. France Telecom also participated in the FP5 and FP6[3] projects including an IPv6 section: 6QM (IPv6 Quality of Service Measurement), SatIP6[4], and Daidalos on cooperation between networks aimed at providing seamless mobility. Lastly, we have participated in various R&D cooperation projects with other European operators via Eurescom, particularly on the transition between IPv4 and IPv6.

3. Community R&D framework programme, see R&D, Spring 2003.

4. See p. 39.

"As early as 2000, France Telecom R&D identified IPv6 as a crucial technology and set up a world IPv6 skill centre."

R&D: Coming back to France...

P. V.: In 2002, the minister responsible for research clearly stated the government's support for IPv6. This led to the creation of a French IPv6 Task Force, inaugurated in September 2002 at the Senate. Its mission is to devise recommendations on IPv6 deployment in France. France Telecom has accompanied the application of two regional Task Forces in Brittany and Normandy. France Telecom is one of the key members of its Steering Committee. Beyond these institutional aspects, we are involved in a variety of RNRT cooperation projects such as DNSsec[4], IDSA (on secure IPv6 mobile signalling) and Cyberté, aimed at providing mobile handsets with simultaneous access or successive access to several wireless technologies. Finally, we are taking part in the IPv6 operations through the competitiveness centres: we supported the establishment of the IPv6 Skills Centre (Point6) in Brittany.

R&D: It is clear that IPv6 has become a worldwide challenge and that France Telecom is closely involved in it. How are we organised to meet this challenge?

P. V.: France Telecom R&D Division identified IPv6 as a major technology in the year 2000 and decided to set up a worldwide IPv6 Skills Centre to federate and promote it. Our laboratories, and particularly those located abroad, have been heavily involved. We also set up an entity responsible for interfacing with all the Group's business units and subsidiaries to transfer skills and provide support for testing and deployment. Among the concrete operations carried out by the Group, we can name the establishment of a multi-service, multi-access IPv6 platform interconnecting our laboratories in London, Beijing, San Francisco, Tokyo and Warsaw with our French sites. It is a facility which helps our business units carry out full-scale tests of IPv6's advantages and the commercial feasibility of the resulting services. It is also a promotional tool for our key accounts which could be invited to participate in these demonstrations. With these initiatives, France Telecom R&D Division has contributed to the establishment of the Group's IPv6 strategy and road map. These will continue to be applied to projects, tests and deployments for which our laboratories will provide their support and expertise, transferring these skills to operating units.

R&D: In other words, IPv6 will become mainly the concern of the operational entities?

P. V.: The Group's Networks, Carriers and IT division has largely taken over the preparation for deployment of IPv6 on our operational IP networks. This does not mean that R&D work on this theme will be halted. We are already committed to a road map up to 2010 and beyond, a decade that will see the launch and mass deployment of communicating objects (M2M, Machine to Machine) such as RFID*labels, nanomachines and sensor networks. These objects will generate very high levels of traffic, requiring autoconfiguration, self-management, naming, mobility and location functions, and very elaborate security for which we will have to design, dimension and deploy new network concepts. Here again, IPv6 should provide interesting solutions...

contact: eileen.lee-lavergne@6wind.com

6WIND

The O.N.E. Software Company for Converging Multimedia Communications

Competition to create innovative bundles of blended voice, video and data services corresponding to user demands and lifestyles is heating up. In parallel, so are IP-based architectures to deliver unified network configuration, management and interoperability across different access technologies. Within this context, the New Internet (IPv6), with its large capacity of address space, in-built security, QoS, auto-configuration and enhanced mobile IP service, is predicted to further boost IP proliferation for true end-to-end multimedia communications. ISPs hoping to gain an edge in the rapid development of new IP multimedia services cannot therefore, afford to ignore or delay IPv6 implementation.

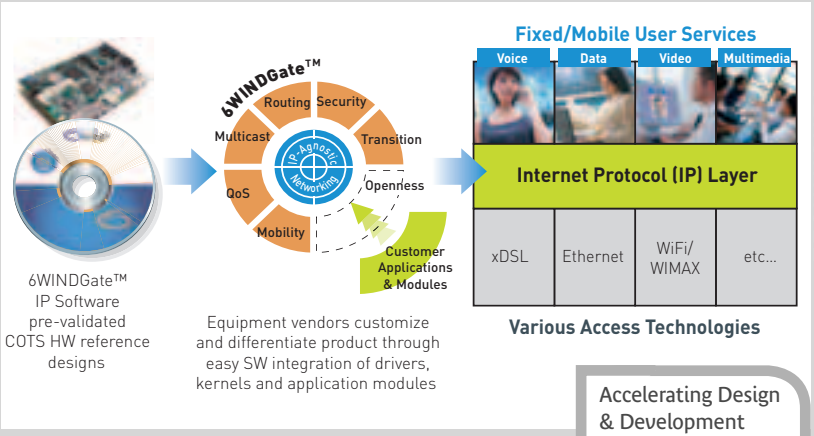
However, since IPv4 and IPv6 will increasingly co-exist, delivery of multimedia content and services must be totally transparent over both, making secure and ubiquitous access a priority for users getting connected.

6WIND's software, 6WINDGate™, has been conceived to master the complexities of dual-IP through a decade of hands-on expertise in defense and electronics networking, including experience in over 80 major dual-IP trials and operational deployments worldwide. Operators like China Telecom, KDDI, and NTT use 6WINDGate™ to deploy pre-commercial services e.g. wireless broadband over IPv6. Equipment vendors, on the other hand, (Alcatel, Arkoon, Mercury and Samsung) license the software for innovative creation of new multi-services business and home gateways.

6WINDGate™ enables fast product customization, differentiation and integration of various access technologies such as xDSL, WiFi/WiMAX, Ethernet, DVB, etc to address innovative services around richer secure triple play, peer-to-peer and mobility applications. This paves the way for ISPs to create whole new service-revenue generation opportunities from professionals and consumers.

6WINDGate™ software is based on an **Open Network Engine (O.N.E.)** strategy, conceived to anticipate, address and manage comprehensively both IP at the data and control plane functions, unlike conventional protocol stack approach.

OPEN refers to 6WINDGate™'s open architecture held together by 6WINDGate™ XMS, an extensible management framework, to speed up easy addition and customization of new interfaces, features and applications. It also incorporates a smart mix of open source codes, debugged and stabilized by 6WIND, with in-house patented technologies developed to offer advanced features on mobile IPv6, multicast and IPv4-IPv6 transition for example. This allows differentiation and integration of various access technologies such as WiFi/WiMAX, Ethernet, DVB, etc.



Accelerating Design & Development to Facilitate Converging Communications

NETWORK refers to 6WINDGate™'s wholesome IP-agnostic features (fully IPv4-IPv6) such as routing, mobility, QoS, security, transition, address and device management at the networking layer. Tested and field-proven, they render 6WINDGate™ future-proof to co-existing network infrastructures and service evolution.

ENGINE refers to empowering accelerated platform or system development with 6WINDGate™'s networking-ready framework that has been pre-validated on COTS hardware and major reference designs. This way, overall total cost of ownership for vendors and ISPs are optimized and IP-agnostic services can be immediately deployed to start generating ROI.

For information on 6WINDGate™-powered product design wins and 6WIND's application deployments, visit www.6wind.com or contact eileen.lee-lavergne@6wind.com.

Lucent Technologies
Bell Labs Innovations

contact: aabbass@lucent.com

VitalQIP® IP Address Management

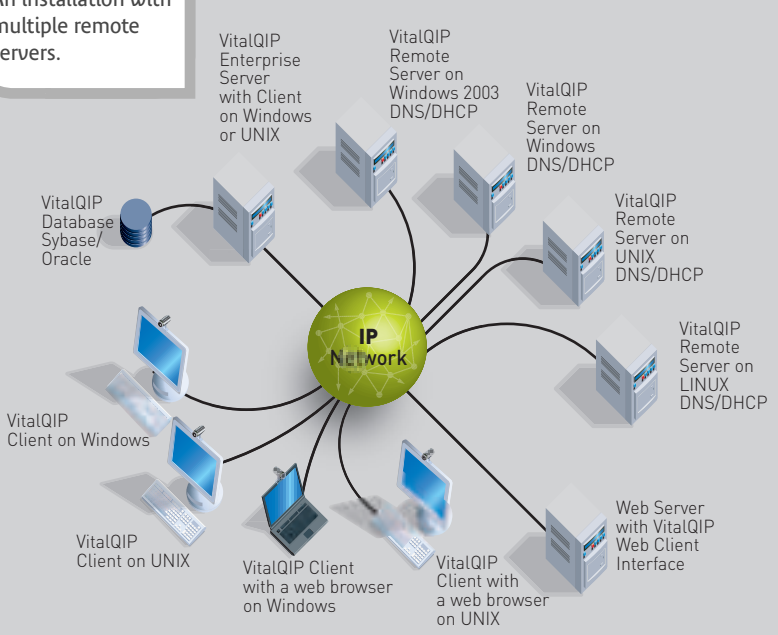
Centralized and Secure Address and Name Service Management for IPv6 and IPv4

IP address exhaustion, advanced services requirements, and security concerns are prompting a move to the next generation of the Internet Protocol, IPv6. Profit potential for innovative mobile, broadband, and IP Multi-media Subsystem (IMS) technology are maddening this rush. In addition to the greatly expanded address space, technical benefits of IPv6 include performance improvements, better security and enhanced support for mobility.
However, complexities associated with the adoption of IPv6 raise significant network planning, operations, and management concerns. The impact of poorly managed IPv6 address space, which includes allocation errors and poor capacity planning, can potentially have severe consequences.

Meeting these challenges with Next Generation IP Address Management Software

Lucent Technologies' market leading VitalQIP® IP Address Management Software is positioned to help operators centrally manage both IPv4 and IPv6 address spaces and name services including transition technologies. Lucent Technologies offer a next generation, multi-platform solution that includes modular, high-performance network servers (DNS, DHCP) to address the ever-growing needs of the next generation network.

VitalQIP® IP Address Management Software
An installation with multiple remote servers.



Facilitate IP Address Acquisition and Allocation

The first step in successfully implementing IPv6 is the acquisition of IPv6 address space from an Internet Registry, such as RIPE Network Coordination Centre (RIPE NCC). Next, the process of further subdividing address space must be carefully performed considering at least one of several popular address allocation methodologies. Software tools such as VitalQIP facilitate orderly address distribution ensuring the greatest amount of flexibility and ultimately efficient address utilization. VitalQIP simplifies the application of many of the standards, rules, and recommendations that reduce allocation waste, address tracking and reporting requirements, and enforce best practices. Equally as important is the ability to determine address utilization in an instant, facilitate address assignment, and maintain accountability. Robust IP address management features like those offered in VitalQIP assist in securing and streamlining the IP address acquisition and allocation process.

Ease IP Address Deployment

IP administrators must consider addressing and node configuration deployment strategies that yield the appropriate levels of automation, flexibility, and control. IPv6 deployments will typically utilize one or more address types including unicast, multicast, and anycast, as defined by RFC 2373. Address assignment and node configuration choices include static, stateful DHCPv6, stateless DHCPv6, and stateless

auto-configuration must also promote error-free, efficient deployments.
Advanced implementation of converged services demand evaluation and dynamic policy setting of IP addresses and configuration options based on provider defined criteria. Flexible policy tools and open APIs simplify deployment through automated rules-based address allocation, renumbering, and other complex operational tasks.

Managing Network Services

Centralized management and monitoring of critical network services (DNS, DHCP, TFTP, ENUM, and others) simplifies administration, masks underlying complexities, and promotes maximum availability. For all but the smallest IPv6 environments, the management of DNS servers, zones (forward and reverse), resource records and other complex configuration parameters must be straightforward. Implementing a high-reliability, redundant DNS solution is even more critical with IPv6, given the complex new format and variety of address types.

To capitalize on the benefits that DHCPv6 offers, centralized management is also essential. DHCPv6 management should provide the ability to configure a server for stateful, stateless, or both modes simultaneously, while preventing the inadvertent use of overlapping address pools and duplicate assignments. A properly managed DHCPv6 implementation can also be used to determine the accurate state of address utilization, as well as manage relationships among DHCPv6 servers. Scaling to millions of addresses and deployed today at the world's largest mobile and fixed providers, VitalQIP® software reliably powers always-on services, while reducing operating costs through centralized management.

Monitoring and Auditing

Security and regulatory requirements compel enterprises and service providers alike to monitor and audit network access for both IPv4 and IPv6. This is most notable in broadband environments. Additionally, being able to determine difference between current and last known state of a network is instrumental in detecting and confronting network irregularities including unauthorized access. Moreover, the stateless auto-configuration feature of IPv6 enables the possibility of undetected and unauthorized network access. VitalSuite software solutions can be employed to discover and audit IP networks, determine network utilization, perform network accounting, and increase security.

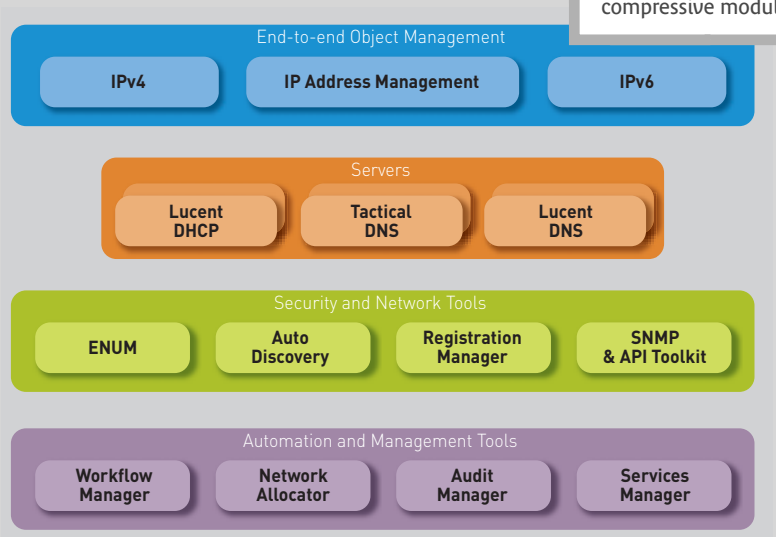
Integrated Management

Finally, network management and operations benefit from a centralized repository of IPv4 and IPv6 network data where all address space and services are managed by one solution. Moreover, the use of transition technologies (dual-stack, tunnels, etc.) will be used to introduce IPv6 into existing network infrastructures facilitating the evolution of IP networks. VitalQIP automates and simplifies the management of co-existing IPv4 and IPv6 networks in an integrated fashion helping to increase reliability and add value to ongoing IP related projects, while reducing costs.

VitalQIP® IP Address Management Software

VitalQIP IP Address Management software is a key part of the VitalSuite® software, a complete service enablement and assurance portfolio of OSS and IT management software for service providers and enterprises with over 1800 customers worldwide. VitalSuite software is an enabling factor for access independent IMS and converged services and networks.

VitalQIP® IP Address Management Software
A look at the compressive modules.



VitalQIP IP software was the Network World 2005 Clear-Choice award winner. The system supports a range of user interfaces including Windows 95/98/NT/2000, UNIX, and web-based. It operates on a variety of platforms: Windows NT/2000/2003, Solaris, HP-UX, AIX, and Linux. The software supports the management of Lucent Technologies' DNS/DHCP servers as well as IBM and Microsoft NT/2000 DNS/DHCP servers. Optional VitalQIP add-on software modules such as ENUM and Audit Manger extend the system's capabilities to address an even wider of IP network management requirements.

contact: sbaillav@cisco.com

IPv6 – New growth relays for France Telecom

The continued growth of the Internet, and IP-based solutions and the increasing number of ways in which IP can be used has driven protocol development to meet the growing expectations of multiple users, applications and services. IPv4 is no exception to this rule of technological adaptation and IPv6 was designed right from the outset to meet the new technical and commercial challenges.
Cisco Systems plays a particularly proactive role in standardisation systems such as the IETF in defining and implementing IPv6 architecture, which is how Cisco Systems came to be involved as far back as the early 1990s in different Working Groups such as:
- The Next Generation WG Internet Protocol (IPng, which became IPv6) – Co Chairman.
- WGNext Generation Transition (Ngtrans) – since converted into WG v6Ops - Co Chairman.
- Dynamic Host Configuration (DHC), IPv6 Mobile and others.

Cisco Systems is also a founder member of the IPv6 Forum and a committed participant in major experimental ventures such as the recently completed 6Net project (www.6net.org), a European network bringing together 16 countries for the purpose of evaluating IPv6 deployment.

Opportunities for new markets and services

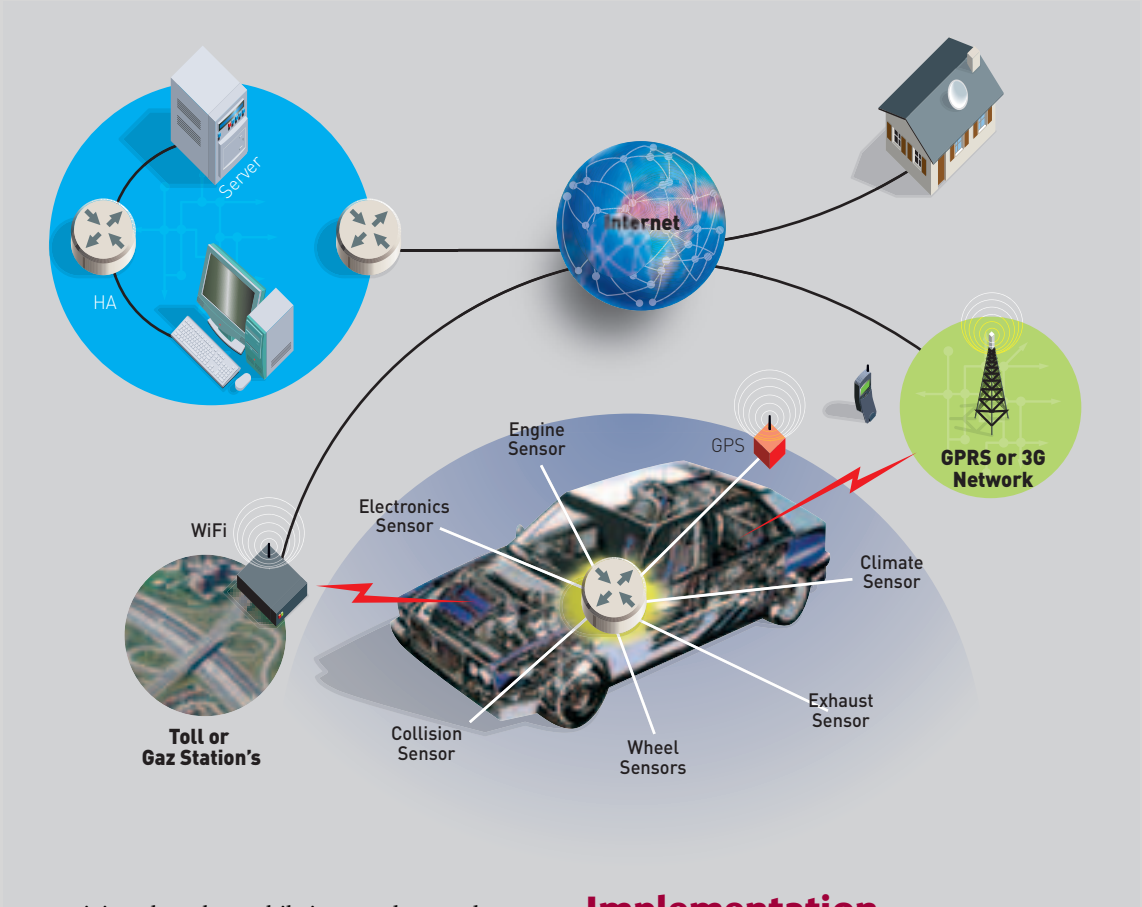
IPv6 incorporates all the improvements made over the last 20 years to IPv4, and goes well beyond merely improving the address possibilities. Although the new address system will be able to offer new service opportunities, IPv6 has also been concerned with IP environment related technologies by improving:

- **Security:** IPV6 incorporates IPsec as native. Development at protocol level allows encryption and native authentication and will facilitate the implementation of VPNs. When implemented these will help give better control of end to end security and protect data integrity, but security should not be limited to IPsec alone. According to analysts, these solutions will help the development of E-commerce.

- **Quality of service:** Not all data, even that carried on the same IP network, has the same characteristics and it needs to be adapted in terms of transport.
IPv6 is identical to the IPv4 models (DiffServ, IntServ) with an added "Flow Label" field encoded in 20 bits, which when its use is defined, will allow applications to manage QoS more carefully.

- **The possibilities of auto-installation:** this is for sure one of the most important features giving new opportunities for the development of mass-market IPv6 technology based deployment, in relation to the expansion of the address field. With these different auto-installation modes, IPv6 will allow any mobile telephone, wireless equipment, home automation equipment, hifi or the like, to be connected to the Internet in a way that is transparent to the user. The networking of these new forms of equipment means that a whole host of new operator services can be contemplated.

- **Mobility:** a rapidly expanding market both in terms of the numbers and types of connection terminals, and in terms of the services expected by users.
IPv6 builds in mobility through the RFCs 3775 and 3376 delivering more flexible solutions than with IPv4, as part of a large-scale implementation. IPv6 mobility endeavours inter alia to reduce localisation-related constraints (Connection to different types of network) and to maintain IP



connectivity when the mobile is moved around, in a way that is transparent to the user and to the applications.

For example, Cisco has developed a "Mobile Router" that supports IPv6 known as Cisco 3200. Cisco 3200 provides WAN connectivity between this on-board vehicle router and information or management centres, through different types of miscellaneous technology wireless networks. These solutions allow carriers to carry IP on their fleets and to install new applications (Fleet management, traffic info, security, maintenance etc.) that will increase their productivity.

Integration and Coexistence

IPv6 implementation is at a more or less advanced stage, depending on the country involved, but it may be considered as being in the early phases of a major sea change. Although the success of IPv6 will depend on the new applications operating on IPv6 and will take some time, it seems obvious that IPv4 and IPv6 will have to coexist for some time and transition strategies, tools and mechanisms have been taken into account in the design of IPv6.
Cisco has always associated itself with this procedure, participating in transition technique developments so that this development is as flexible as possible.

Implementation

Until now, the IPv6 protocol has been supported by the IOS (Cisco Internetworking Operating System) on more than 20 platforms integrating all the advanced IPv6 functionalities, coexistence techniques between IPv4 and v6 (Tunneling, IPv6 Provider Edge router (6PE), Network Address Translation-Protocol Translation etc.), security (authentication, authorization, and accounting, IP Sec, Firewall), QoS and Multicast. IPv6 implementation at Hardware level covers some routers in the range, including the Cisco CRS-1 Carrier Routing System, Cisco 12000 et 7600, Lan switches (Catalyst 6500 and 3750) and firewalls. Cisco is pursuing its development plan by continually extending its offer around IPv6 via new software functionalities or new hardware implementations.

IPv6 has been designed to encourage end users to make even more extensive use of the Internet and in an attempt to get free of the limitations of IPV4. The success of IPv6 is closely bound up with the emergence of applications that relate in a native way to this protocol. These will be the true catalysts for the creation of new services and new revenues for the operator. This is why Cisco Systems has positioned itself as a strategic player in the provision of equipment that supports IPv6 through constant innovation in this technology.

Tools to protect privacy

When it comes to respect for privacy, corporate social responsibility and commercial interest converge: there can be no development of electronic interchange without confidentiality which is completely above suspicion! That's why the R&D Division has launched the Privacy project.

Source: Stéphane Guilloteau

"Personal data consists of any information relating to an individual who is identified or can be identified, directly or indirectly, by reference to an identification number or by one or several elements exclusive to that person." What the new law on French Data Protection Act highlights in this statement is the value represented by personal data – a value that can be exploited by third parties with more or less legitimate aims. And without evoking the hijacking of confidential information, the simple fact of knowing who consults what can also represent a problem. Having good knowledge of the habits of consenting customers in order to achieve better personalisation of offers is certainly not reprehensible…quite the contrary. But the lack of guarantees which often goes with this approach can lead to difficult situations.

Anti-Big Brother software

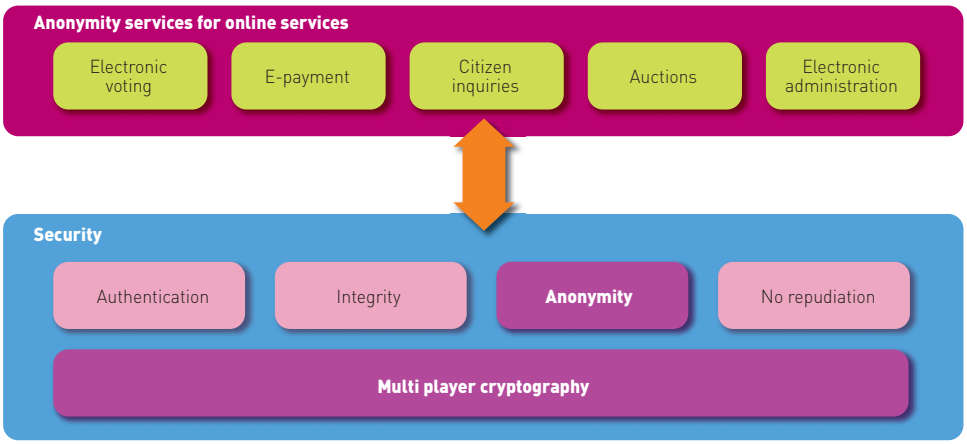
** See glossary*

Examples of "accidents" abound. In 2003, brands as reputable as Gillette or Benneton were the targets of protest from associations because they wanted to give their products electronic labels (RFID*), which their detractors said would make it possible to closely monitor customers. The same year, Microsoft decided to scrap its PassPort, a single identification service called into question because of its potential threat to privacy. Google's Gmail electronic message service, insufficiently protected, the RATP's* ticket pass Navigo, memorising passengers' journeys, or even the project for the French electronic national identity card, decried as an intrusion by Big Brother, are just a few illustrations of the era of suspicion which the new technologies have entered.

There are numerous reasons for distrust. What is the point of collecting all this personal data? Is it transferred and stored in complete security? Isn't there a danger of the data being altered mistakenly or maliciously? Will the data be given or sold to third parties? Don't I run the risk of being inundated with commercial proposals linked with my stated preferences? Is my anonymity guaranteed?

Yet legal and technical tools do exist. In France, the CNIL (national commission for data protection) has been a completely independent watchdog protecting privacy since 1978. And there is certainly no lack of protection technologies. Web anonymisers can hide users' IP addresses. Encryption and signature software

ensure the confidentiality of e-mail. The P3P (Platform for Privacy Preferences) allows users to control data concerning their private lives when visiting websites. PCs can be protected by filtering systems, anti-spam and anti-spy software. There are also systems for securing access to data, the management of this data and RFIDs, as well as mechanisms for anonymous signature or "pseudo-anonymity" (with anonymity only being lifted by an empowered authority)…



Voting, an exemplary application

In this emerging and rapidly-growing market, France Telecom can boast solid know-how – particularly in the field of cryptography, where the Group holds many patents. Launched in 2005, the Privacy project aims to create a whole range of confidentiality tools based on this – confidentiality tools independent of the network, platform or terminal. The purpose of these tools is to enrich the Group's offer and they could be integrated into Certatoo, the range of secure services based on a common platform (see R&D Winter 2003 - 2004, pp. 44 and 50).
From the point of view of technical complexity, the key application remains remote electronic voting: this involves guaranteeing tough authentication, and the anonymity, integrity and verifiability of the results. France Telecom's laboratories have developed a security protocol which satisfies these criteria and their involvement in the European project E-Poll2 allows them to apply this "in the field". The aim of this is to combat abstentions by making it possible to vote, either by Internet or in a polling station away from home[1]. In this way, in 2004, students at Lyons 2 and Nantes were the first to test the E-Poll2 system in the context of the elections for the student representative body. In the referendum of May 29th 2005, some 2,000 voters in Issy-les-Moulineaux were the first (after their counterparts in Nantes, Lyons and Italy) to use a remote voting machine, which dispensed with any signature requirement. This electronic voting solution could be generalised with the support of the Interior Ministry.
And if we can do this, we can also handle less sensitive processes. Mastery of the safeguards demanded by electronic voting demonstrates that France Telecom is able to respond to less technically complex, but just as sensitive requirements. This is particularly the case for medical records, remote administrative procedures, anonymous payment based on pre-paid tickets, anonymous signatures for "super smart cards" in the context of the European InspireD project, etc.
For all these services, as for many others, the inviolable security of data and "ensured discretion" are prerequisites for their acceptability among customers. It is through its mastery of techniques capable of guaranteeing this that France Telecom intends to make the difference, while consolidating its aim of recreating the social relationship…with complete respect for the individual.

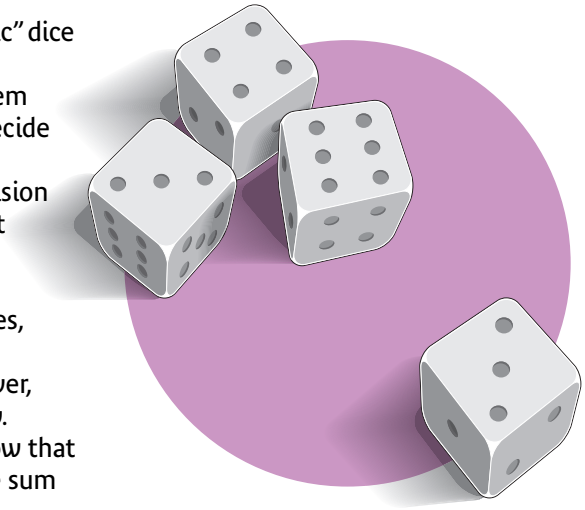
Cryptography
France Telecom expertise forms the basis for a range of services to protect our private life.

1. For political elections where visiting the polling booth is obligatory in France.

Brainteasers

by Gilles Macario-Rat

Power of prediction



Here is magic trick is easy to perform. It only requires a few "magic" dice and a little mental arithmetic on your part.
Roll the dice one by one on a table in view of everyone, taking them from your pocket, for example. Each time you throw a dice, you decide either to carry on and throw another one or to stop, based on a criterion known only to yourself. For this, we assume that the decision to carry on is not limited to the number of dice still in your pocket and depends only on the dice already present.
Then you put on a blindfold and ask someone in the audience to choose as many dice as you indicate, it does not matter which ones, so that everyone except you can identify them.
You then ask this person to take the dice chosen and turn them over, showing the opposite side of the dice to the side currently in view.
You then announce that, due to your power of prediction, you know that the sum of the dots on the sides of the dice chosen is equal to the sum of the dots on the sides of the dice not chosen. Amazing isn't it?

Questions:

For the trick to be successful, what is the criterion that enables you to decide whether or not to continue adding a dice to those already present? If you have satisfied this criterion, how many dice should you ask the person to turn over?

Index: Remember that the sum of the points of two opposite sides is always 7!

Sudoku

			7	1		4		
	2						5	
					5			
	4		9			3		7
9		1					4	
	6			3	2			
3			2			1		9
		5		4	7		6	8
2				8				

Sudoku is apparently a very old game.
The rules are simple. **You fill in a 9x9 grid with the numbers 1 to 9**, so that each of the 9 numbers only appears once and once only on each line, in each column and in each of the 9 3x3 sub-grids. Obviously, some boxes have already been filled in.

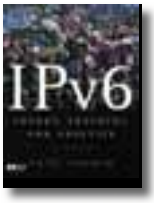
Solutions online shortly on the Comet site of France Telecom intranet (R&D News-stand/Publications section)

For more information …

ABOUT IPV6

IPv6, Théorie et pratique
Gisèle Cizault
3rd edition, Editions O'Reilly, Paris, 2002 – 456 pages. (in French)
www.oreilly.fr

Gisèle Cizault is the pseudonym of a collective of university academics and leading engineers (including France Telecom experts), who participate, particularly through G6, in the development of IPv6 on an international scale. Apart from an overview and a detailed study of the protocol, this work supplies practical details concerning its implementation with the widest range of systems and routers, as well as practical examples of its introduction.



IPv6 – Theory, Protocol and Practice
Peter Loshin
2nd edition, Morgan Kaufmann, 2004 – 536 pages.
(available at www.alapage.com under the title "IPv6 clearly explained")

"This completely rewritten edition guides readers through implementation and deployment of IPv6. The Theory section takes a close, unbiased look at why so much time and effort has been expended on revising IPv4. In the Protocol section is a comprehensive review of the specifics of IPv6 and related protocols. Finally, the Practice section provides hands-on explanations of how to roll out IPv6 support and services."
(extract from the publisher's presentation)

ON USAGES

Réseaux, n°129 – 130 / 2005 "Visibilité / Invisibilité"
Review published by France Telecom / RD, Editions Lavoisier – 360 pages (in French)
http://reseaux.revuesonline.com/

Seeing, being seen, remaining unseen… Here this topic, which has been widely explored by the human and communication sciences, is reviewed in its political and epistemological dimensions by a group of experts brought together by Olivier Voirol, of the EHESS (advanced school of social science studies). An intellectually stimulating work…

Usages, n°21, July 2005
Newsletter published by France Telecom / RD (in French)
http://comet.francetelecom.fr ("kiosque R&D" section)

This edition focuses on the topic of the creativity of users, illustrated by the phenomenon of blogs, and on the innovations emerging from the non-commercial sector, such as Wikipedia, the free encyclopaedia. How do these creations spread and how can the commercial sector fit into this approach?

agenda

France Telecom's R&D is exhibiting…

1 and 2 September
Summer communications conference on sustainable development
84120 - La Bastidonne
http://iltic.org/

28 – 29 September
World i-democracy forum
Issy-les-Moulineaux, Palais des Arts et des Congrès
www.issy.com

3 – 6 October
Broadband World Forum Europe
Madrid, Conference Centre
www.iec.org/events/

4 October
"Participative Democracy" Congress
Paris, Cité des sciences et de l'industrie

4 – 5 October
Symposium on "ICTs, a new plus point for the handicapped"
Paris, Bibliothèque Nationale

7 - 10 October
Fête de la Science
France Telecom / RD, Grenoble site

17 – 21 October
MPEG Meeting
Nice - Acropolis

7 – 8 November
CORESA 2005
France Telecom / RD, Rennes site
coresa.irisa.fr

16 - 18 November
SMSI (World Summit on the Information Society)
Tunis
smsi.internet.gouv.fr/