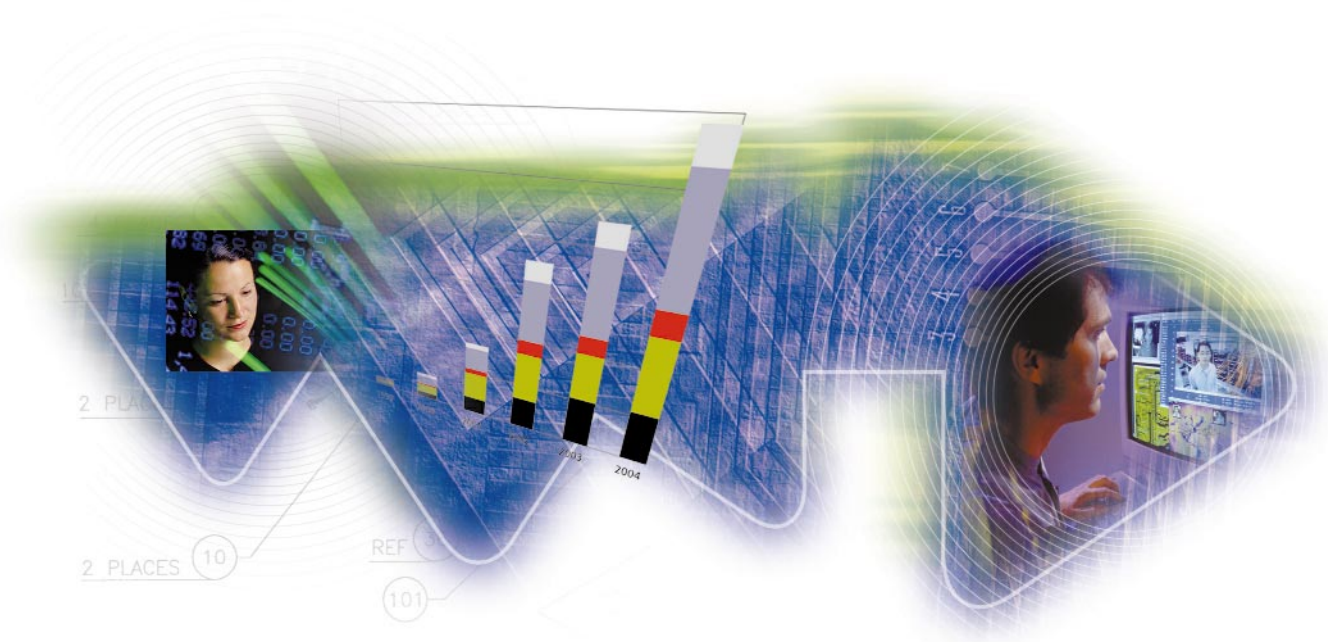


The Move to IPv6

TECHNICAL PAPER



ARCHITECTS OF AN INTERNET WORLD

The Move to IPv6

Introduction	1
The Limitations of IPv4	1
The Need for a New Protocol	1
IPv6 versus IPv4	2
The Benefits of IPv6	3
Standardizing IPv6	3
The Transition to IPv6	3
Dual-Stack Hosts and Routers	4
Tunneling	4
Translators	7
General Transition Considerations	8
IPv6 and the Mobile Industry	9
Mobile IP	9
IPv6 and UMTS	9
VoIP	12
Support for IPv6	13
Alcatel and IPv6	13
Alcatel's Automatic Tunneling Mechanisms	14
Conclusion	15
Glossary	16
References	17

Introduction

Despite the phenomenal success of IPv4 — the standard Internet communications protocol underlying the majority of today's corporate, academic and commercial networks — it does have certain limitations for wireless and wireline networks. These limitations, which include inefficient routing aggregation and the inability to support large numbers of Internet protocol (IP) addresses, can restrict network growth.

From the wireless perspective, the commercial introduction of the Universal Mobile Telecommunications System (UMTS), a third generation (3G) communications system, is creating demand for new mobile devices with “always-on” capabilities and permanent IP addresses. In addition, innovative peer-to-peer communications applications, such as videoconferencing, streaming, gaming, location-based services and home networking will require an IP address for each terminal. These factors are creating the need for large numbers of IP addresses, far beyond the capabilities of IPv4.

The IP address shortage is also expected to become a major issue for wireline networks, particularly in Asia, as countries such as China and Japan jump aboard the Internet bandwagon and service providers need to provision more users than ever before.

This growth trend is dictating the need for a new IP standard — IP version 6 (IPv6). The IPv6 specifications were developed in 1995 by the Internet Engineering Task Force (IETF) and have reached a level and quality suitable for commercial deployment. IPv6 will provide a simple, robust, secure managed infrastructure, offering an extended address space that enables unique addressing for always-on Internet devices, as well as automatic configuration for host IP addresses.

This paper compares IPv4 and IPv6, addressing the many benefits of the latter protocol. It also discusses mechanisms that will ensure a seamless migration from IPv4 to IPv6, ongoing support for IPv6, current plans for the worldwide deployment of IPv6 and, finally, Alcatel's strategy for incorporating IPv6 into the Company's networking products and solutions.

The Limitations of IPv4

The address shortage is one of the most difficult issues associated with the use of IPv4. While network address translation (NAT) and Classless InterDomain Routing (CIDR) have provided a temporary “fix” for the challenges of IPv4, they too have limitations, given that demand — for peer-to-peer applications (such as Kazaa), online gaming (for games such as Quake), home networks, real-time applications and push technologies — continues to explode.

The functionality of NAT, in particular, tends to defy the end-to-end, open Internet model, as NAT “boxes” placed at the edges of the Internet are needed to translate the private addresses used in both private and corporate networks. The resulting model essentially restricts the evolution of the Internet, creating what the Internet community often refers to as a “walled garden.”

The Need for a New Protocol

The need to extend the addressing capabilities of IPv4, providing “have not” countries with more address space, is the key driver for adopting a new IP protocol. Other reasons for designing a new protocol include the need to provide such functions as:

- ▼ Better routing aggregation capabilities, which reduce routing table sizes and result in faster packet processing
- ▼ Security and mobility for end users
- ▼ Auto configuration, whereby a new host can obtain network connectivity by simply plugging into a network (e.g., “plug and play” and “plug and ping”)

IPv6 versus IPv4

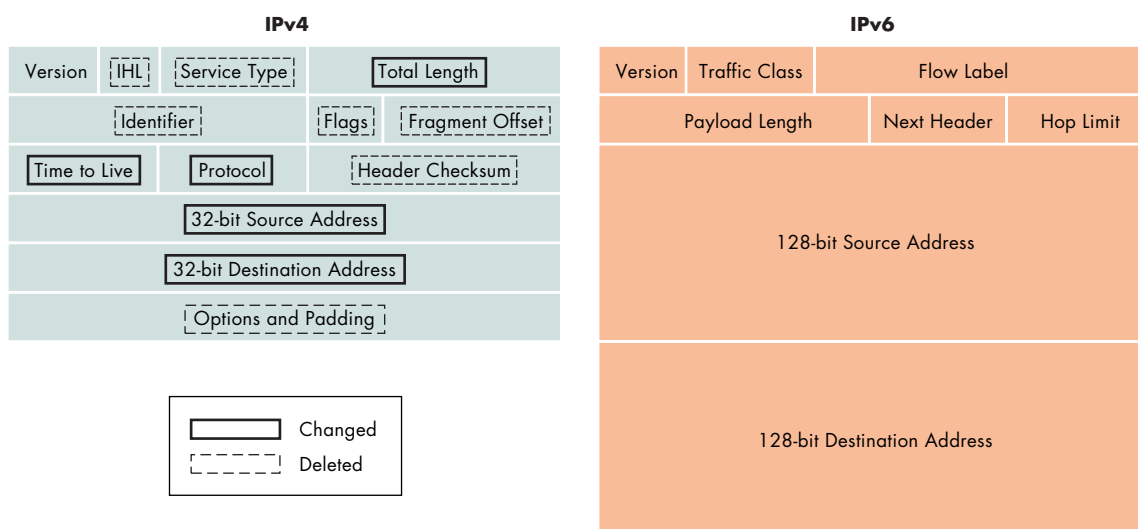
IPv6 exceeds the functionality of IPv4 in several ways. Specifically, IPv6 offers the following feature enhancements:

- ▼ Expanded addressing capabilities, supporting 128 bits of information (much more than the 32 bits supported by IPv4) and address privacy, allowing a new address to be obtained for each outgoing session when privacy is required
- ▼ IP header format simplification (see Figure 1), whereby unnecessary IPv4 protocol fields are removed, which reduces the processing penalty incurred for larger addresses and minimizes bandwidth overhead
- ▼ Support for extensions, when required, providing greater processing efficiency; less stringent size limitations than those of IPv4; and an easier method for intermediate nodes to retrieve relevant extensions
- ▼ Integrated/enhanced authentication and privacy capabilities for end users
- ▼ A flow-labeling capability, currently being refined, that enables packets to be labeled according to a particular flow, allowing senders to request non-default handling of each flow and simplifying network packet processing
- ▼ Integrated support for multicasting, replacing bandwidth-costly broadcast, which is the only option available with IPv4

The quality of service (QoS) that IPv6 networks provide for various Internet communications is equivalent to that offered by IPv4. For the purpose of QoS, IPv4 mainly uses IntServ and/or DiffServ protocols and/or extensions to IPv4. IPv6 also provides a flow identifier field, or flow label, in the IPv6 header that can be used to simplify packet processing. This enables a source to associate a particular flow label with a specific set of parameters, which can be used for network filtering and classification. In the case of DiffServ, these parameters would include destination addresses and ports, source addresses and ports, and protocol fields. This process is simpler in that routers associate the flow label with the set of parameters. They subsequently use the flow label as an access key for the set, rather than looking for the parameters in each packet beyond the IPv6 header.

Security capabilities are embedded in, and needed for, any IPv6 implementation. These capabilities are identical to those provided by IPv4, except that IPv4 security may require protocol add-ons, which may not be available on real platforms. In fact, the public key infrastructure (PKI) issue — namely, the fact that the PKI elements necessary for the use of Internet protocol security (IPSec) (e.g., keys, certificates) cannot be deployed currently on a global basis — affects both IPv4 and IPv6. However, once this issue has been resolved, IPv6 will offer greater ease of use and simplicity than IPv4, as add-ons will not be required for IPv6 hosts and routers.

▼ Figure 1: IP Header Format Simplification



The Benefits of IPv6

IPv6 enables a more consistent network infrastructure than IPv4, offering greater simplicity, robustness, security readiness and the ability to break the “have” and “have not” digital divide, extending Internet-enabled applications and services to many more users worldwide.

IPv6 offers end users, from corporations to residential consumers, the following capabilities:

- ▼ Automatic configuration and management of IP addresses, providing a simpler, less error-free process
- ▼ Embedded encryption and authentication
- ▼ Mobility support, which allows a mobile host who is away from home to communicate directly with a corresponding node, without the traffic having to traverse the home network
- ▼ Multicasting support with embedded scoping, which provides greater network efficiency by restricting traffic to specific areas, according to the scope (local, regional or global)
- ▼ The capability to more easily select or change Internet service providers (ISPs), by assisting with the resulting renumbering of addresses and prefixes
- ▼ More efficient router packet processing, which results in better network performance
- ▼ Freedom to use person-to-person services, such as messaging

IPv6 also enables ISPs and network operators to benefit from:

- ▼ High network scalability due to more efficient route aggregation
- ▼ High scalability in terms of the number of users that can be addressed
- ▼ True end-to-end service delivery so that the Internet is ubiquitous
- ▼ End-to-end transparency, eliminating the need to deploy costly boxes, or NATs, that manipulate packets and limit performance
- ▼ Plug-and-ping and plug-and-manage capabilities, which can reduce/eliminate administrative tasks, making IPv6 suitable for the general public, including home network owners
- ▼ The capability to support next generation applications, such as UMTS or gaming

- ▼ A more efficient data path than that provided by IPv4 for mobile users
- ▼ Improved site renumbering support, allowing subscribers to be automatically renumbered after moving to a new ISP and reducing administrative effort and traffic errors

Standardizing IPv6

The IETF working groups, such as IPv6 (IP Next Generation [IPNG]) and Next Generation Transition (NGTRANS), have made tremendous progress in standardizing IPv6, as well as the mechanisms required for the transition to IPv6 from IPv4. As of the fall of 2001, the core IPv6 specifications have achieved IETF Draft Standard status. These specifications include the IPv6 base protocol, Internet control message protocol (ICMPv6), Neighbor Discovery, Path MTU (PMTU) Discovery, and IPv6-over-any media, such as Ethernet and point-to-point protocol (PPP) link. Related specifications, such as new records for the domain naming system (DNS), and dynamic host configuration protocol (DHCP), are also being standardized by the IPv6 Working Group. Other IETF groups are working on additional specifications, such as mobile IPv6 and header compression, many of which are well advanced. An IETF working group has also been established to standardize multihoming support, a problem that is contributing to the recent surge in the growth of the IPv4 routing table. Such continued development activity is a reflection of the mature status of, and continued interest in, IPv6.

The Transition to IPv6

The transition to IPv6 from IPv4 will be a gradual process, during which the two protocols are expected to coexist for several years. This evolution requires transition mechanisms for IPv6 hosts and routers to enable IPv6-IPv4 communications. It also requires communication between IPv6 nodes across IPv4 zones, which is being addressed by the IETF NGTRANS Working Group. These generic mechanisms may be classified as:

- ▼ Dual-stack hosts and routers
- ▼ Tunneling
- ▼ Translators

While tunneling is useful to enable IPv6 islands to communicate over IPv4, translators are paramount for IPv4-to-IPv6 communication. Combining all three mechanisms — tunnels, translators and dual-stack hosts and routers — will give network administrators the flexibility and interoperability they need to deploy IPv6. Transition mechanisms will also allow organizations that currently depend on IPv4 networks to enjoy the many advanced features enabled by IPv6.

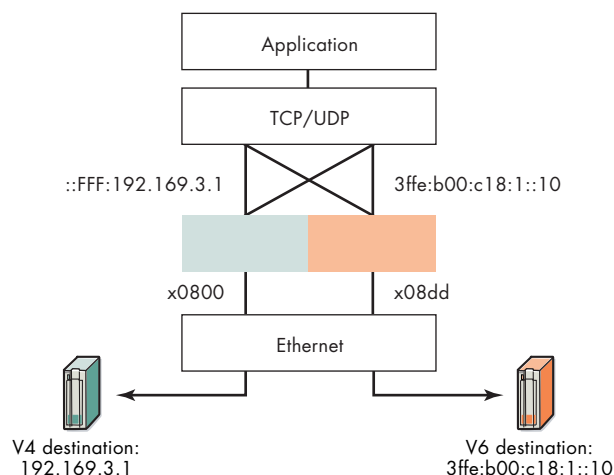
Dual-Stack Hosts and Routers

Initially, IPv6 users will require ongoing interaction with existing IPv4 nodes. This can be achieved by using a dual-stack IPv4–IPv6 approach. Figure 2 illustrates a dual-stack host.

When using the dual-stack IPv4–IPv6 approach, a host has access to both IPv4 and IPv6 resources. Routers running either of the two protocols can forward traffic for both IPv4 and IPv6 end nodes. Dual-stack machines can use either IPv4 (when communicating with native IPv4 hosts) or IPv6 (when communicating with IPv6 hosts). They may also use independent IPv4 and IPv6 addresses, or they may be configured with an IPv6 address that is IPv4-compatible.

Dual-stack nodes may use conventional IPv4 auto-configuration services, such as DHCP, to obtain their IPv4 addresses. IPv6 addresses can be manually configured in local host tables or obtained via IPv6 auto-configuration mechanisms — the preferred approach, because it relieves users from complex configuration tasks. Major servers will continue to run in dual-stack mode until all active nodes have migrated to IPv6.

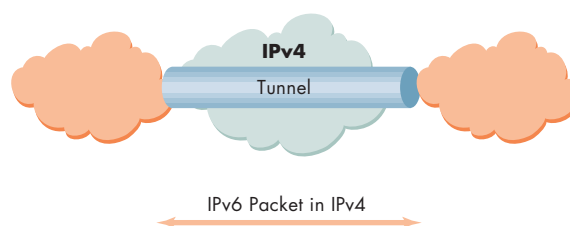
▼ Figure 2: IP Dual-Stack Host



Tunneling

Transition mechanisms that allow IPv6 hosts to communicate via intervening IPv4 networks are based on a technique known as tunneling, which ensures there is no disruption to the end-to-end IP communications model. With IPv6-over-IPv4 tunneling, IPv6 packets are carried within IPv4 packets. This technique, which has been thoroughly tested in IPv6 backbone (6bone) and other network test beds, enables early IPv6 implementations to take advantage of the existing IPv4 infrastructure without the need to change any of the IPv4 infrastructure components (see Figure 3).

▼ Figure 3: IPv6-over-IPv4 Tunneling



A dual-stack router (or a dual-stack host, in the degenerative case where the IPv6 network is a single host) at the edge of the IPv6 topology simply inserts an IPv4 header in front of each IPv6 packet being sent across the IPv4 network. This process, known as “encapsulation,” sends the information as native IPv4 traffic through existing links to the IPv4 infrastructure. IPv4 routers then forward this traffic, without the knowledge that IPv6 is involved. On the other side of the tunnel, another dual-stack router or host “decapsulates”, or removes, the extra IP header and routes the IPv6 packet to its ultimate destination. This is achieved by using standard IPv6 in the destination IPv6 network.

To accommodate different administrative needs, IPv6 transition mechanisms offer two types of tunneling: configured (explicit or static) and automatic (dynamic or implicit). Configured tunneling is typically used when sites or hosts exchange traffic regularly. It is also used when few sites need to be connected, in which case manual configuration of the tunnel ends is not a significant administrative burden for network managers. Configured tunneling offers the advantage of enabling hosts in IPv6 sites to use native IPv6 addresses, rather than IPv4-IPv6 address constructs. In the latter case, the IPv4 address of the tunnel endpoint (TEP) is embedded inside the IPv6 TEP.

Some transition mechanisms, such as tunnel brokers (TBs), relieve some of the burden associated with setting up tunnels manually. A TB is a dual-stack server, which for small, isolated IPv6 sites facilitates tunneling through an IPv4 network to which the server client must be connected. For example, a client may request tunneling through a web server. As such, the client would receive the configuration information needed for its machine to establish a pseudo-automatic tunnel whenever the client triggers tunnel set-up. At the same time, the TB would automatically set up the side of the tunnel bordering the IPv6 network.

Automatic tunneling is a transition scheme that requires an IPv4 address for each host. This enables a node to establish a tunnel without configuration. Automatic tunnels are created when required and eliminated when no longer needed. The IETF has specified various automatic tunneling solutions. These include IPv4-compatible IPv6 addresses, the “6to4” transition mechanism (6to4), and intrasite automatic tunnel addressing protocol (ISATAP). Proposed Alcatel automatic tunneling mechanisms are described in the Alcatel and IPv6 section of this paper.

IPv4-compatible IPv6 addresses

Automatic tunneling with IPv4-compatible IPv6 addresses can be used if the destination is an IPv4 address. With this addressing format, the IPv4 address is embedded at the end portion of the IPv6 address and can be retrieved automatically. The destination host identified by such an address acts as the remote TEP and must be dual-stack. A source host will use this type of address in the IPv6 packets being sent to a destination host. The border node, between the IPv6 and the IPv4 domains near the originator, acts as the local TEP.

That is, the border node encapsulates the IPv6 packets received from the originator host in IPv4. The border node then forwards the packets to the IPv4 destination that it extracted from the destination address of the IPv6 packet.

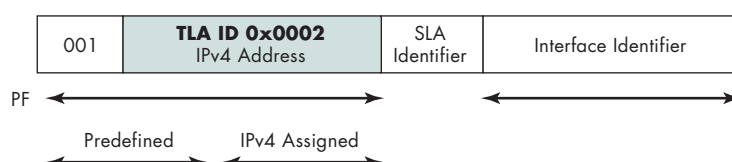
6to4

The goal of the 6to4 transition mechanism is to connect IPv6 domains across IPv4 domains, without using explicit tunnels. An IPv6 domain that uses this technique is called a 6to4 domain. The interface between a 6to4 domain and an adjacent IPv4 domain is assigned an IPv4 address, which represents the TEP between the two domains. The 6to4 transition mechanism defines a specific way to use this IPv4 address to construct IPv6 addresses for the 6to4 domain.

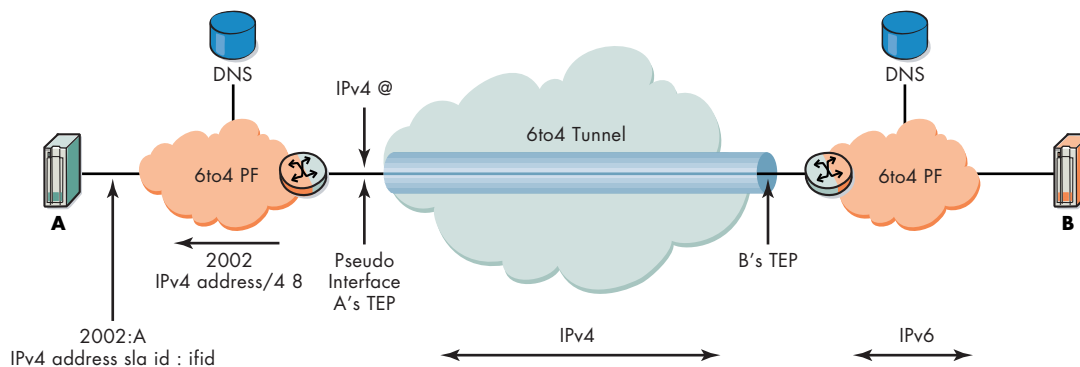
An IPv6 address comprises two components: a prefix and an interface identifier. The prefix represents the provider of the IP service, while the interface identifier represents the node. The addressing format defined by IETF for use in the 6to4 domain is illustrated in Figure 4. This figure shows how a prefix is constructed by embedding the IPv4 address of the border interface (the 6to4 domain TEP) into a predefined bit scheme.

The prefix is used to configure the IPv6 host addresses in the 6to4 domain in the usual IPv6 manner. As a result, each host in a 6to4 domain obtains a minimum of one 6to4 address, enabling automatic retrieval of the TEP at the border of the 6to4 domain. In order to make these hosts visible externally, the DNS is updated with the addresses of the 6to4 domain host names. Following a simple DNS query about a 6to4 host, the source host retrieves the 6to4 address. As a result, the source will know which remote TEP to use.

▼ Figure 4: 6to4 Address Format Used in a 6to4 Domain



▼ Figure 5: 6to4 Architecture



For example, when a source (Host A) retrieves the 6to4 address of a destination (Host B) from the DNS, it sends IPv6 packets to Host B's address. In Host A's domain, the packets are routed to the border node, from which Host A obtained the 6to4 prefix. The border router encapsulates any IPv6 packet addressed to Host B into IPv4, and tunnels the IPv6 packet to Host B's border node (the TEP addressed by the IPv4 address inside Host B's IPv6 address). The remote border node then decapsulates the received packet to retrieve the IPv6 packet from Host A, and forwards it to Host B via classic IPv6 routing. Host B, in turn, sends packets to Host A (see Figure 5), which are handled in a similar way at the TEPs.

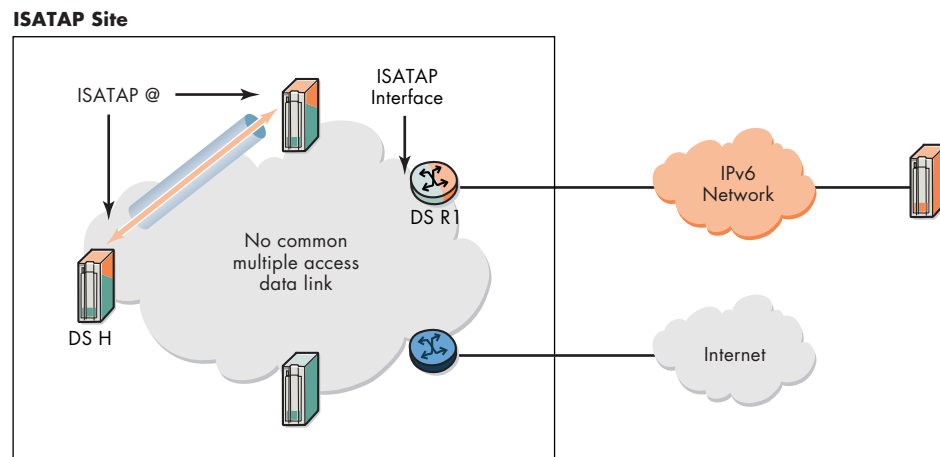
ISATAP

ISATAP is a transition mechanism that enables automatic tunneling to occur between IPv6 hosts located inside a site with an IPv4 network infrastructure. This tunneling occurs without the need for direct access to an IPv6 router at the

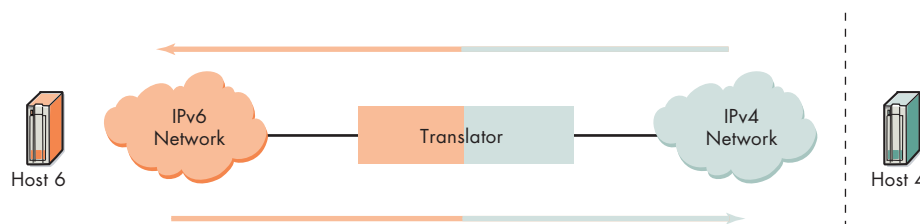
site border. ISATAP also allows IPv6 hosts to access an IPv6 Internet network via a border router. ISATAP specifies a new IPv6 addressing format, in which the IPv4 address of a dual-stack host is embedded in the interface identifier section of its IPv6 address, using proper formatting. The IPv6 address prefix can be any prefix that is valid according to IPv6 addressing rules; however, it is reserved for ISATAP use inside the site. An example of ISATAP address encoding syntax is PF::0200:5EFE:IPv4 @.

ISATAP allows IPv6 hosts and routers that do not have an IPv6 link between them to discover one another; enables addressing in the IPv4 infrastructure; and performs IPv6 automatic configuration, including providing addresses for interfaces and default routes to the IPv6 border router. Once this process has been completed, automatic tunneling over an IPv4 infrastructure supports communication between IPv6 hosts or between IPv6 hosts and border routers (see Figure 6).

▼ Figure 6: Enabling Automatic Tunneling Using ISATAP



▼ Figure 7: Translators — Enabling Communication Between IPv6 and IPv4 Hosts



Translators

To enable communication between IPv4- and IPv6-only domains, a combination of dual-stack nodes and translation techniques at the network, transport and application layers must be applied. Figure 7 illustrates the translation process that enables IPv6 and IPv4 hosts to communicate. In this case, the IPv6 hosts can be either IPv6-only nodes or dual-stack hosts, whereby both IPv6 and IPv4 protocols are supported in the host.

For IPv6-only nodes, NAT-protocol translation (NAT-PT) must be deployed, as these nodes understand and “speak” only IPv6 language. If, on the other hand, dual-stack hosts are deployed but an administrator does not want to configure an IPv4 stack, a dual-stack transition mechanism (DSTM) is an appropriate solution, as it enables IPv4 communication without requiring translation or configuration.

NAT-PT

NAT-PT translates IP addresses and protocol fields between IPv6 and IPv4 domains. The communication application layers above the IP network layer may use addresses that also need translation, requiring a NAT-PT box that contains application-level gateway (ALG) functions.

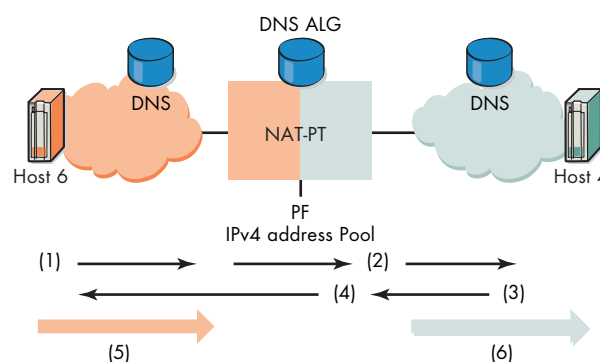
Figure 8 illustrates how the NAT-PT mechanism works when an IPv6 host initiates communication with an IPv4 host through the following steps:

- ▼ Step 1: The initiating Host 6 issues a DNS query, asking for the IPv6 address of the destination Host 4’s designated DNS name. Since the DNS in the IPv6 domain has no record of the IPv4 hosts, this request is forwarded to the DNS in the IPv4 domain, via NAT-PT.
- ▼ Step 2: The ALG translates the query into an IPv4 DNS query, and then sends it over the IPv4 network.
- ▼ Step 3: The IPv4 DNS replies, providing the IPv4 address of Host 4, the queried host.
- ▼ Step 4: The DNS reply is sent through the NAT-PT device,

which transforms it into a DNS IPv6 reply containing an address with a prefix that is assigned to the NAT-PT, and Host 4’s IPv4 address. This prefix is required to enable traffic directed at the IPv4 network to be sent to the NAT-PT device.

- ▼ Step 5: Host 6 then sends an IPv6 packet, for Host 4, to the router that is hosting the NAT-PT function. The packet contains the destination address of Host 4 that is received as a result of the DNS query.
- ▼ Step 6: The NAT-PT device then allocates an IPv4 address from its address pool to the source, Host 6. This device, in turn, translates the IPv6 packet into an IPv4 packet, according to specified rules. The destination address for the IPv4 packet will be the IPv4 address of destination Host 4, and the source address for the IPv4 packet is the one selected for Host 6 by NAT-PT.

▼ Figure 8: NAT-PT Overview



DSTM

DSTM enables communication between IPv6 hosts (with both IPv6 and IPv4 capabilities) and IPv4-only hosts. It combines two mechanisms: one that allows temporary assignment of IPv4 addresses to IPv6 in the DHCP IPv6 server, and one that tunnels (either statically or dynamically) IPv4 packets over the IPv6 network to which the IPv6 node is connected.

The manner in which DSTM enables communication between IPv6 and IPv4-only hosts can be explained using an example whereby an IPv6 host initiates communication with an IPv4 host.

As illustrated in Figure 9, the IPv6 host initiates communication with an IPv4 host in four steps:

- ▼ Step 1: The IPv6 host (Host 6) sends a DNS request, asking for the IPv6 address (e.g., a DNS record type AAAA for the IPv4 host, Host 4)
- ▼ Step 2: The DNS replies with the IPv4 host address of Host 4
- ▼ Step 3: Recognizing that Host 4 is an IPv4-only host, Host 6 requests a temporary IPv4 address for itself from the DHCP
- ▼ Step 4: The IPv6 and IPv4 hosts communicate with each other via IPv4

The path between the IPv6 and the IPv4 hosts can be split into two parts: Host 6 to the edge router, and the IPv4 edge router to Host 4. Currently, transport from Host 6 to the edge of the network is achieved by tunneling IPv4 into IPv6. This allows Host A's domain to be a native IPv6 network, where only the border router is dual-stack.

General Transition Considerations

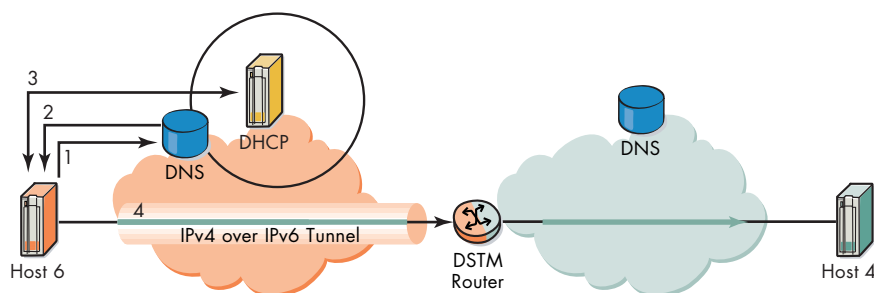
Organizations planning to migrate to IPv6 must understand the interaction between the various transition mechanisms. They also need to carefully consider the various transition costs, which may include new software and/or hardware upgrades, as well as administrative, training and application conversion costs.

On the software side, if the source code for an application is available, it is easy to modify/port it to work with both IPv6 and IPv4 stacks in the host. This is because IPv6 does not modify the interface (the application programming interface [API]) between an application and the IP stack. Since most software vendors, such as Microsoft, are or will be migrating their software to support IPv6, the acquisition costs would be no different than the costs associated with upgrading traditional software.

On the network equipment side, router manufacturers provide IPv6-ready upgrades. However, early implementations of IPv6 routers may initially lack hardware support, which could result in less than optimal performance — something organizations must factor into their transition plans.

Administrative costs, such as those associated with address and route management, tunnel configuration and security, are also important factors to consider when planning the transition to IPv6. As with IPv4, IPv6 requires robust DNS services, such as name-to-address and address-to-name translations, as well as DHCP IPv6 implementation. This is necessary when administrators want greater configuration control than that provided automatically by IPv6.

▼ Figure 9: Enabling Communication Between IPv6 and IPv4-Only Hosts



1. Host 6 requests Host 4's IPv6 address (e.g., DNS record type AAAA)
2. DNS replies with Host 4's IPv4 address
3. Host 6 requests an IPv4 address from DHCP6 and receives a temporary IPv4 address
4. IPv6 and IPv4 hosts communicate via IPv4

DNS operations for IPv6 will be crucial for large-scale deployments and are also useful for some transition mechanisms. DHCP, used in conjunction with IPv6 auto configuration or DSTM, is another critical component (see Figure 8). The IPv6 Forum supports the move to make DNS source codes freely available to the community in the near future. A similar effort will cover DHCP IPv6 software.

For service providers, a key consideration is when to make the transition to IPv6. The transition will require time, effort, financial resources and training to ensure that they, and their customers, will benefit from the enhanced productivity, reliability, and other features enabled by IPv6.

IPv6 and the Mobile Industry

Mobile IP

There are essentially two types of mobility: discrete mobility, also known as nomadicity, and continuous mobility, which is being examined by the IETF Mobile IP Working Group. With discrete mobility, users log on to a network that is different from their home network and remain there for the duration of an IP session. A typical example is a remote access server (RAS) connection, whereby an employee checks e-mail from home or a hotel, for example.

With continuous mobility, users are able to change networks during an IP session, without interrupting or impacting higher layer functions and/or applications, such as e-mail. The impact of changing networks, or “handovers,” for various applications, can be minimized by ensuring users maintain the same IP address while they roam different networks. These IP addresses can be static, or they can be obtained during the initialization phase, in which case they would either belong to the service provider network or the visited network.

Continuous mobility comprises two levels: micro and macro mobility, both of which are based on handover frequency. Macro mobility enables packets of information to be routed to the current access network of the mobile terminal, resulting in low handover frequency. This solves the problem of moving between different access networks. Mobile IP (MIP) — both for IPv6 (MIP6) and for IPv4 (MIP4) — are examples of macro mobility.

By contrast, micro mobility (for example, cellular IP) supports mobility within a small geographical region, in which case handover frequency may be high. Since all traffic is handled locally within one network, faster handovers can be achieved by loosening security requirements and linking the radio layer to micro mobility protocols.

Micro mobility, as experienced in a mobile radio network, is being considered by the IETF as an enhancement to existing mobile IP solutions. However, the Third Generation Partnership Project (3GPP), the standardization organization for European and Asian UMTS networks, is also developing solutions. Therefore, for the time being, MIP and UMTS solutions can be considered independently. In general, MIP may be viewed as an additional service, which supports seamless movement between different access networks. For example, a corporate employee may have uninterrupted access to his or her company’s database while in a taxi, via UMTS, or at a hotel, via a wireless LAN.

IPv6 and UMTS

UMTS is the next generation Global System for Mobile Communications (GSM). The UMTS network architecture comprises the user equipment (UE) domain and the infrastructure domain (see Figure 10). The Infrastructure domain may be further divided into the radio access network (RAN) and the core network (CN). The UMTS access network is called the UMTS Terrestrial Radio Access Network (UTRAN).

▼ Figure 10: The UMTS Network Architecture

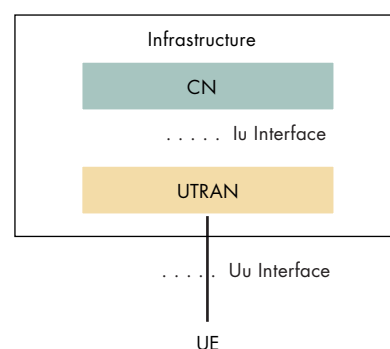


Figure 11 illustrates the scope of IPv6, which is currently optional in the CN. In the access chain between the mobile terminal and the Gateway GPRS Support Node (GGSN), a combination of protocol stacks provides a transport mechanism for carrying information upstream and/or downstream. Above this transport (see GTP below), an IPv6 protocol, referred to as application-level IP, carries the IMS traffic between multimedia components, including terminals, GGSNs and servers. The multimedia servers constitute the IP multimedia domain, beyond the CN.

For multimedia services, UMTS R5 has chosen IPv6 for application level information transport and session initiation protocol (SIP) for multimedia sessions. While the standards have been delayed, this does not affect the essential role UMTS plays in the deployment of IPv6.

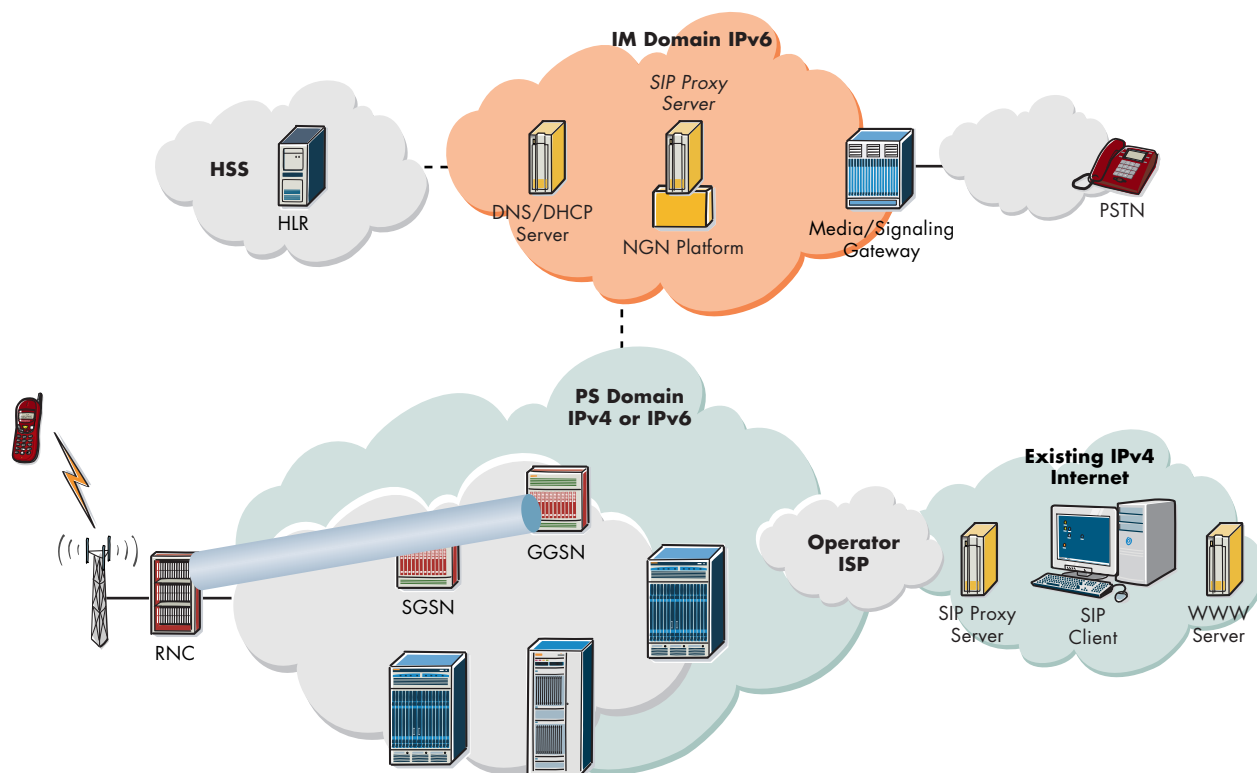
Essentially, IPv6 can be introduced in several independent domains in UMTS architectures, including:

- ▼ The IMS CN subsystem (the user/application layer), incorporating all IMS control entities, such as CSCF, MGCF and HSS
- ▼ The General Packet Radio Service (GPRS) backbone, which comprises the Serving GPRS Support Node (SGSN), the GGSN and an underlying data infrastructure, whereby IP is used for packet access to the Internet/intranets and the IMS subsystem
- ▼ The UTRAN, in which IP-based transport is optional

IP in the IMS CN subsystem

It is important to note the distinction between the IP transport network (the UMTS backbone) and the application-level IPv6 mandated by 3GPP.

▼ Figure 11: The Scope of IPv6 in UMTS



Legend

CSCF	call session control function
HSS	home subscriber system
HLR	home location register
MGCF	media gateway control function
RNC	radio network controller

In deploying IPv6 in 3G data backbones, mobile operators may choose to implement IPv6 networks from day one. This is because IPv6 provides an extended address space capability and, therefore, offers unique addressing for all mobile Internet devices, including those that are always on. IPv6 also provides automatic configuration of host IP addresses, without the need to use DHCP, and offers support for end-to-end security, as well as QoS. In addition, the Public Land Mobile Network (PLMN) is a “closed” network where interoperability with IPv4 legacy networks can be accomplished at the edge of the network, using a variety of transition mechanisms.

IP in the GPRS backbone

Unlike traditional CS voice, GPRS delivers a packet-based access service. As an added function, UMTS data, such as that used to access the World Wide Web and IMS services, are supported on top of GPRS. GPRS uses two levels of IP — one for applications, the other as a means of transport. The application-level IP is tunneled on top of IP, using the GPRS tunneling protocol (GTP). This lower level of IP is called the transport layer. Tunneling user data solves the mobility problem by hiding the location information from end users. As a result, handovers are only visible at the transport level.

Independent of the application level IP, a network operator has the choice of using IPv6 or IPv4 at the transport level of GPRS. The IPv6 IMS packet can be transported on top of IPv4 between the core network elements.

The GPRS ETSI UMTS 23.060 specification states that for the GPRS transport backbone, IPv4 is mandatory, while IPv6 is optional. There is no need to introduce IPv6 in the

backbone, since it is a private network with private IP addressing and QoS capabilities.

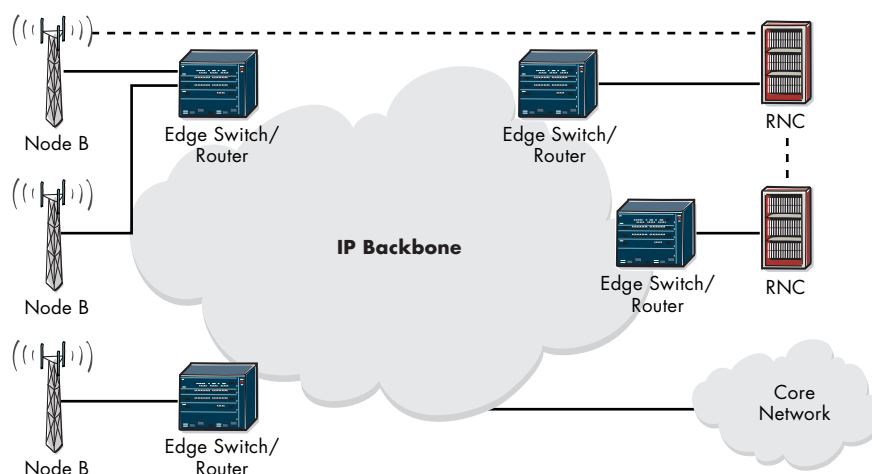
In the CS domain, the classic mobile switching center (MSC) is split into a control portion called the MSC server and a transport portion called the media gateway (MGW). Voice frames originating from the public switched telephone network (PSTN) or the UTRAN, are packetized by the MGW and sent via IP over the CN. The GPRS and CS IP backbone will likely be a shared one.

IP as a transport option in the UTRAN

Currently, asynchronous transfer mode (ATM — ATM adaptation Layer 2 [AAL2]) is used to transport signaling and voice and data traffic across the UTRAN. In UMTS R5, IP in the UTRAN can provide this transport functionality (see Figure 12). Used datagram protocol (UDP) ports and IP addresses define flow streams rather than ATM connections. In terms of providing QoS, flow stream multiplexing and header compression are performed at Layer 2 over the “last mile,” which is where bandwidth must be optimized.

As radio access is independent of the transport network layer, when migrating to IPv6, changes should be made only to the transport layer. 3GPP mandates the use of IPv6 in the UTRAN, whereas IPv4 is optional. However, in order to ease the operation between IPv6 and IPv4 nodes during the transition, 3GPP recommends that dual-stack hosts (shown as RNCs and Node Bs in Figure 12) be used. Dual-stack hosts eliminate the need for translators, which would result in additional delays between RNCs and Node Bs. Delay is critical because of the constraints of radio technology.

▼ Figure 12: The IP Transport Network in the UTRAN



When IP is deployed in both the UTRAN and the CN, the immediate benefit is the resulting unified data infrastructure, which minimizes operation and maintenance costs.

Even when IP is not used in the UTRAN as a transport option, IP is not transparent to the application-level IP, and requires a media-handling function in the UTRAN. In order to efficiently deliver voice over IP (VoIP) IMS services beyond the radio resources, IPv6 media handling is required in the UTRAN. To minimize the use of radio resources for downstream transport toward the mobile terminal user equipment, the real-time protocol (RTP)/UDP/IP headers used for VoIP are compressed or stripped. The most recent RTP/UDP/IP header compression (robust header compression) enables bandwidth to be reduced. Robust header compression requires that the UTRAN be aware of the IPv6 header in order to compress/decompress bandwidth and eliminate/regenerate bandwidth.

The introduction of IPv6 for IMS services and the use of IPv4 for applications, such as VoIP, will result in the need for the UTRAN to support both IPv6 and IPv4 at the application level. This will enable functions, such as header compression/decompression.

VoIP

For multimedia applications, such as VoIP, IPv4 is not the optimal protocol, given its limited addressing capabilities. However, adopting NAT technology may not be the ideal solution, because of its restrictions.

The most appropriate choice for VoIP signaling is SIP, which is generally used in combination with session description protocol (SDP). SIP is a client-server protocol that enables prospective partners to find each other (application address translation) and signal to one another the desire to communicate. SIP manages calls independently of the media descriptions handled by SDP. The latter aims to describe a media session's characteristics (for example, the type of medium and CODEC), as well as the media information transport mechanisms in which IP addresses are included. Therefore, if a user agent (UA), or a user application within a private network using private IP addresses, were to send a message with an IP address in SDP, all of the media packets returned by the receiving party would be misdirected or lost. This could be avoided only if an additional capability, such as an ALG/NAT, were used to translate the packets. SIP messages also comprise SIP headers that may contain either domain names or IP addresses. If IP addresses are used in the SIP request message initiated by the private network, the subsequent responses from the public network

would be misdirected, as those IP addresses could not be routed across the globe.

Given that one of the most problematic issues related to deploying VoIP using IPv4 is the use of NAT, a potential solution is either to make NAT application-aware, using ALGs, or to extend the SIP proxy to allow it to control NAT. However, there are drawbacks to both solutions.

More specifically, the former solution may burden NAT with an application layer protocol, while the latter solution may require a new control protocol. In addition, both solutions are complex given:

- ▼ The potential number of fields that can transport IP addresses in a SIP message
- ▼ The number of exchanged SIP messages required for call set-up, since SIP may need to be extended with new headers and methods for traditional supplementary services, such as voice — meaning potentially more messages would be exchanged
- ▼ As SDP is not a mandatory media session description protocol, it may be necessary to use new media description protocols in combination with SIP
- ▼ The deployment of bidirectional NATs, with a DNS ALG, may be required, as a telephone application is bidirectional (i.e., calls can be initiated from inside and outside the private network)

However, IPv6's unlimited addressing capacity can resolve many of these NAT-related issues.

IPv6 will also provide other benefits, such as addressing privacy and automatic configuration, which are advantageous for VoIP. With IPv6, the only address that needs to be stable, albeit not permanent, is the address that corresponds to the DNS name of a called user to enable always-on features. For an outgoing VoIP session, a user can adopt a temporary random address to protect his or her identity.

Deploying IPv6 presents several issues and challenges, which the IETF is addressing with various technical solutions. These challenges include:

- ▼ The fact that IPv6 introduces overhead that may impact low-speed links — an issue that can be resolved by using compression mechanisms
- ▼ While the IETF has defined a uniform resource locator (URL) format to manage IPv6 addresses, the representation of IPv6 addresses, such as 1080:0:0:8:800:200C:417A within a URL in SIP, is not “user friendly.” It is expected that, in most cases, individuals would use friendlier DNS names for their correspondence, such as toto@velizy.alcatel.fr
- ▼ The selection of the best possible VoIP transition tool to enable interaction between IPv4 and IPv6, ensuring high quality and minimal delays

Support for IPv6

Some of the world’s largest and most successful service providers and enterprises support the move to IPv6. In fact, many have already upgraded their IP gear to IPv6. Others expect to follow suit sometime between 2002 and 2005. In addition, ISPs across the globe are supporting IPv6 in trials and/or pilot projects, and some have already begun to offer commercial IPv6 services.

One of the European Council’s key objectives is to adopt IPv6 across Europe, with the goal of accelerating Internet and UMTS deployment, IPv6-enabled applications and e-commerce to the level currently enjoyed in North America. The European Union (EU) also recommends that its members migrate networks supporting research and government activities to IPv6 by 2005. As a result, the EU has launched an IPv6 Task Force to create projects that support and build on the use of IPv6 in applications and infrastructures.

Furthermore, both Japan and Korea have decided that every ISP must be IPv6-ready by 2005. Some ISPs, such as NTT Communications and Internet Initiative Japan Inc. (IIJ), already offer several IPv6 commercial services. In addition, the U.S. government supports the next generation of the Internet (Internet2), which deploys both IPv6 and IPv4.

The increasing interest shown by major operators and the maturity of IPv6 technology are sending strong market signals that support the move to IPv6. Despite the perils of predicting

the timeframe for IPv4 address depletion, recent studies suggest a period extending from 2005 to 2011. As a result, Alcatel believes that the migration to IPv6 will occur gradually from 2004 on, and from 2003 to 2004 for mobile devices.

Alcatel and IPv6

Alcatel believes that the introduction of IPv6 must support end-to-end transparent communication and, therefore, IPv6 should be introduced from the edge toward the core of the network.

Given the widespread deployment of IPv4 and the many services and applications it supports, the deployment of IPv6 must seamlessly interoperate with IPv4. As a result, the deployment of IPv6 will be a gradual process, and IPv4 services must continue to be available for an indefinite period of time.

If the deployment of IPv6 is to be a success, several requirements must be met. For example, there must be no adverse impact on the existing IPv4 infrastructure or its overall performance when a network deploys both protocols over the same infrastructure. The solutions used to enable a seamless migration must be highly scalable.

Any migration strategy needs to ensure that all of the incurred planning, procurement, administration and training costs be kept to a minimum.

Service providers will undoubtedly have different approaches to deploying IPv6 than corporate and residential users. Corporate users’ connectivity requirements, for example, will typically focus on access to local e-mail, the World Wide Web, databases and application servers. In this case, it may be best initially to upgrade only isolated groups and/or departments to IPv6 and to implement backbone router upgrades at a slower rate. Independent workgroups can upgrade their clients and servers to dual-stack IPv4–IPv6 hosts or IPv6-only hosts, creating “islands” of IPv6 functionality. After the initial IPv6 routers are in place, it may be preferable to connect the IPv6 islands with router-to-router tunnels, whereby one or more routers in each island would be configured as TEPs. Dual-stack routers running interior gateway protocols (IGPs) can propagate link-state reachability advertisements, such as prefixes for IPv6 destinations (e.g., in the IPv6 islands), through tunnels — just as they would across conventional point-to-point links.

Initially, Internet backbone providers will upgrade their access points to native IPv6 or dual-stack services. IPv6 will be tunneled either throughout the CN into IPv4 datagrams or into multiprotocol label switching (MPLS) tunnels between the network access edges. This allows backbone providers to ensure the IPv4 CN remains untouched. In the future, as traffic increases, providers will convert the core of their network to IPv6 by deploying dual-stack routers.

Alcatel, as a major player in the carrier-grade Internet space, provides the critical network elements and support that will enable its customers to seamlessly deploy IPv6. As a result, Alcatel will begin introducing IPv6 in 2003 in its routing product line, including the Alcatel 7670 Routing Switch Platform (RSP) and the Alcatel 7770 Routing Core Platform (RCP). These routers will support the migration to IPv6, providing network performance that will equal or surpass that supported today by IPv4. The use of network processor technology facilitates the evolution of hardware forwarding. The Alcatel Omni family of corporate switches and routers will also support IPv6 in 2003.

Other Alcatel products that have been made IPv6 ready include:

- ▼ Gateways used between packet and circuit networks
- ▼ The portfolio of access products (ADSL, LMDS), as IP pushes its way into the access architecture
- ▼ Network management nodes, such as the Alcatel 5620 Network Manager
- ▼ UMTS equipment, SGSN and GGSN, which are based on the Alcatel routing platform
- ▼ Multimedia over IP products, for which Alcatel has selected SIP

Alcatel's Automatic Tunneling Mechanisms

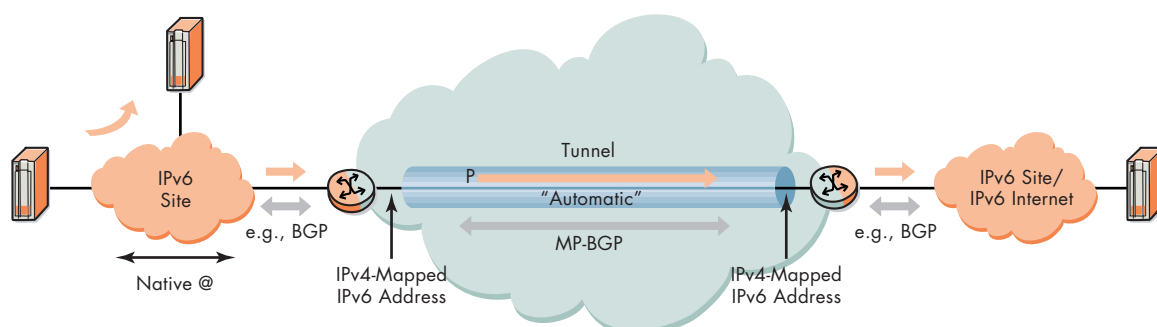
As well as introducing IPv6 in its routing product line, Alcatel has been active in the IETF, particularly with respect to the IPv6-related working groups. In fact, Alcatel has successfully introduced two automatic tunneling mechanisms to the IETF.

The first mechanism leverages existing Layer 3 virtual private network (VPN) solutions, which rely on the multiprotocol border gateway protocol (MP-BGP) and MPLS tunnels, and is aptly named BGP-MPLS v6 VPN. This mechanism does not require IPv6 capability in the routers of the IPv4 network core.

The second transition mechanism, called BGP tunneling, does not require the sites to be part of a VPN and does not restrict the type of tunnels used in the core. Rather, tunneling can be provided by any type of automatic tunneling mechanism. These include IPv4-compatible IPv6 addresses, ISATAP or MPLS. MP-BGP, the BGP protocol version to be used for IPv6, provides the means to distribute routing information and also destination prefixes about a provider's IPv6 customers, across the core of an infrastructure.

As neither of these mechanisms requires infrastructure upgrades or changes to the backbone of the network, they enable ISPs to offer IPv6 connectivity at a low cost and without network disruption. Figure 13 illustrates how BGP tunneling works. In this example, a BGP routing protocol exchanges the destinations or prefixes between the customer's network and the service provider's access point. The MP-BGP router then exchanges this information with its peers in the provider's other access points, and identifies itself as the next hop for these destinations via an IPv4-mapped IPv6 address. As a result, each access point has the necessary information to automatically tunnel traffic between access points. Customers' IPv6 traffic (see yellow arrow in Figure 13) is encapsulated in IPv4, for example, over the BBN (see green and yellow arrows in Figure 13). The TEPs encapsulate and decapsulate the IPv6 traffic into, or from, IPv4.

▼ Figure 13: Alcatel's BGP Tunneling Transition Mechanism



Conclusion

The move to IPv6 is supported by organizations across the globe. The new protocol will offer true end-to-end service delivery and transparency and a robust, highly scalable, built-for-the-future infrastructure. This will enable service providers to support current and next generation applications for many more users worldwide.

The standardization of IPv6 is well on its way, with many of the world's largest and most successful service providers and enterprises taking the necessary steps to upgrade their networks to the new protocol. The migration from IPv4 to IPv6 will be a gradual process that will entail careful planning and the capability to deploy transition mechanisms that help minimize training, procurement, administration and other costs. Committed to enhancing its leadership position in the Internet arena, Alcatel is doing its part to deliver high value solutions that will give customers the flexibility and interoperability they need to enjoy a seamless migration to IPv6. Deploying the new protocol will allow them to enjoy enhanced productivity and reliability and achieve success in tomorrow's dynamic electronic world.

Glossary

3GPP	Third Generation Partnership Project	PKI	public key infrastructure
6bone	IPv6 backbone	PLMN	Public Land Mobile Network
ALG	application-level gateway	PMTU	path MTU
A-MGW	access media gateway	PPP	point-to-point protocol
API	application programming interface	PSTN	public switched telephone network
ATM	asynchronous transfer mode	QoS	quality of service
BGP	border gateway protocol	RAN	radio access network
CIDR	Classless InterDomain Routing	RAS	remote access service
CN	core network	RNC	radio network controller
CS	circuit switched	RTP	real-time protocol
CSCF	call session control function	SDP	session description protocol
DHCP	dynamic host configuration protocol	SGSN	Serving GPRS Support Node
DNS	domain naming system	SIP	session initiation protocol
DSTM	dual-stack transition mechanism	SLA	site level aggregator
ETSI	European Telecommunications Standards Institute	TB	tunnel broker
EU	European Union	TCP	transmission control protocol
GGSN	Gateway GPRS Support Node	TEP	tunnel endpoint
GPRS	General Packet Radio Service	TLA	top level aggregator
GSM	Global System for Mobile Communications	UA	user agent
GTP	GPRS tunneling protocol	UDP	used datagram protocol
HLR	home location register	UE	user equipment
HSS	home subscriber system	UMTS	Universal Mobile Telecommunications System
ICMP	Internet control message protocol	URL	uniform resource locator
IETF	Internet Engineering Task Force	UTRAN	UMTS Terrestrial Radio Access Network
IGP	interior gateway protocol	VoIP	voice over IP
IMS	IP multimedia service	VPN	virtual private network
IP	Internet protocol		
IPNG	IP Next Generation		
IPSec	Internet protocol security		
ISATAP	intrasite automatic tunnel addressing protocol		
ISP	Internet service provider		
MGCF	media gateway control function		
MGW	media gateway		
MIP	mobile Internet protocol		
MP-BGP	multiprotocol border gateway protocol		
MPLS	multiprotocol label switching		
MSC	mobile switching center		
MTU	maximum transmission unit		
NAT	network address translation		
NAT-PT	NAT-protocol translation		
NGTRANS	Next Generation Transition		

References

1. "Internet Protocol, Version 6 (IPv6) Specifications," RFC 2460, December 1998, S. Deering, Cisco Systems, R. Hinden, Nokia.
2. "IP Version 6 Addressing Architecture," <draft-ietf-ipngwg-addr-arch-v3-05.txt>, March 2001, R. Hinden, Nokia, S. Deering, Cisco Systems.
3. "Neighbor Discovery for IP Version 6 (IPv6)," RFC 2461, December 1998, T. Narten, IBM, E. Nordmark, Sun Microsystems, W. Simpson, Daydreamer.
4. "IPv6 Stateless Address Auto Configuration," RFC 2462, December 1998, S. Thomson, Bellcore, T. Narten, IBM.
5. "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification," RFC 2463, December 1998, A. Conta, Lucent Technologies, S. Deering, Cisco Systems.
6. "Transition Mechanisms for IPv6 Hosts and Routers," RFC 2893, August 2000, R. Gilligan, Freigate Corp., E. Nordmark, Sun Microsystems.
7. "Network Address Translation - Protocol Translation (NAT-PT)," RFC 2766, February 2000, G. Tsirtsis, BT, P. Srisuresh, Campio Communications.
8. "Connection of IPv6 Domains via IPv4 Clouds," RFC 3056, February 2001, B. Carpenter, K. Moore.
9. "IPv6 Tunnel Broker," RFC 3053, January 2001, A. Durand, Sun Microsystems, P. Fasano, I. Guardini, CSELT S.P.A., D. Lento, Telecom Italia Mobile.
10. "Dual Stack Transition Mechanism (DSTM)," <draft-ietf-ngtrans-dstm-04.txt>, February 2001, J. Bound, Nokia, L. Toutain, F. Dupont, ENST Bretagne, H. Afifi, Institut National des Télécommunications (INT), A. Durand, Sun Microsystems.
11. "Connecting IPv6 Domains across IPv4 Clouds with BGP," <draft-ietf-ngtrans-bgp-tunnel-02.txt>, June 2001, J. De Clercq, G. Gastaud, T. Nguyen, D. Ooms, Alcatel, S. Prevost, BT, F. Le Faucheur, Cisco Systems.
12. "Transmission of IPv6 Packets over Ethernet Networks," RFC 2464, December 1998, M. Crawford, Fermi National Accelerator Laboratory (Fermilab).
13. "IP Version 6 over PPP," RFC 2472, December 1998, D. Haskin, E. Allen, Bay Networks, Inc.
14. "Generic Packet Tunneling in IPv6 Specification," RFC 2473, December 1998, A. Conta, Lucent Technologies, S. Deering, Cisco Systems.
15. "An Overview of the Introduction of IPv6 in the Internet," <draft-ietf-ngtrans-introduction-to-IPv6-transition-07.txt>, W. Biemolt, SEC, A. Durand, Sun Microsystems, D. Finkerson, University of Nebraska-Lincoln (UNL), A. Hazeltine, ASCI, M. Kaat, SEC, T. Larder, Cisco Systems, H. Steenman, AT&T, R. van der Pol, SURFnet, Y. Sekiya, Keio Univ., G. Tsirtsis, Flarion Technologies.
16. "Dynamic Host Configuration Protocol for IPv6 (DHCP)," <draft-ietf-dhc-dhcpv6-20.txt>, J. Bound, M. Carney, C. Perkins, R. Droms.
17. "DNS Extensions to Support IP Version 6," RFC 1886, December 1995, S. Thomson, Bellcore, C. Huitema, Institut National de Recherche en Informatique et en Automatique (INRIA).
18. "BGP-MPLS VPN Extensions for IPv6 VPNs over an IPv4 Infrastructure," <draft-ietf-nguyen-bgp-IPv6-vpn-02.txt>, June 2001, J. De Clercq, G. Gastaud, T. Nguyen, D. Ooms, Alcatel, M. Caragi, France Telecom.

www.alcatel.com

Alcatel and the Alcatel logo are registered trademarks of Alcatel. All other trademarks are the property of their respective owners. Alcatel assumes no responsibility for the accuracy of the information presented, which is subject to change without notice.

© 04 2002 Alcatel. All rights reserved.

3CL 00469 0234 TQZZA Ed.02 14014



ARCHITECTS OF AN INTERNET WORLD