IPv6 Consultation Paper

June 2005

Ministry for
Investment, Industry and Information Technology

Malta Communications Authority

1. INTRODUCTION 3
2. BACKGROUND 4
2.1 IPv4 4
2.2 IPv6 6
3. CURRENT SITUATION 10
3.1 IPv6 Ready Tools 10
3.2 IPv6 and the EU 10
3.3 IPv6 Implementations throughout the World 12
3.4 IPv6 in Malta 13
4. RECOMMENDATIONS 14
4.1 Position of MIIIT and MCA 14
4.2 Possible Issues during Transition 14
4.3 IPv6 Task Force 15
4.3.1 Test Bed Proposal 15
4.3.2 Possible Test Schedule 17
4.3.3 IPv6 Roadmap for Malta 18
5. CONCLUSION 19
6. CONSULTATION FRAMEWORK 20
7. GLOSSARY 21

1. INTRODUCTION

Internet Protocol version 4 (IPv4) is the mechanism through which most computers communicate and interchange data between each other today. This protocol has proven to be robust, easy to implement and interoperable. It has stood the test of scaling a network to a global utility the size of the Internet today.

The current version of IP has not changed substantially since the corresponding Request For Comments (RFC), RFC791, was first launched in 1981. Since then, the Internet infrastructure has expanded and changed drastically. Unfortunately, the initial design had not anticipated and catered for a similar expansion. As a consequence, the current IP space is unable to satisfy the potential huge increase in the number of users (or the geographical needs of the Internet explosion), let alone the requirements of emerging applications such as home area-networks, internet connected transportation (automobiles for example), IP wireless services and distributed games. Consequently, the need was felt of migrating to an improved version of the protocol that can tackle such an expansion. IPv6 is designed to meet these requirements and allow a return to a global environment where the addressing rules of the network are again transparent to the applications. It fixes a number of problems in IPv4. Indeed, technologists note that the greatest demand for IPv6 is heaviest in Asia. Asian countries have, for long, struggled with a minimal number of allocated IPv4 addresses. Thus, the idea of a larger address space is very attractive to these countries.

Due to the pitfalls with IPv4, firms are starting to adopt IPv6 as their new standard. In the near future, as the Internet continues to grow and new applications are employed, IPv6 will definitely become a major focus of ICT activity worldwide. It is expected to replace IPv4 gradually, with the two protocols co-existing for a number of years during the transition period. It is for this reason that Malta needs to start looking ahead by initiating a Research & Development programme geared towards the eventual roll-out of IPv6 on a National basis. Malta should commence experimenting with and planning for this new version of IP. In this way, it will not be caught on the wrong foot when, eventually, the networking world decides to finalise the migration to IPv6 Thus, in line with the National ICT Strategy, Malta needs to be at the forefront in adopting IPv6 – the employment of this protocol will also act as an extra impetus for the country's drive to become a main hub of e-commerce and e-services in the European Union.

2. BACKGROUND

2.1 IPv4

Created to connect hosts through what was known at the time as the ARPANET, IPv4 was not designed to cope with the massive expansion, in terms of use and scope, seen during the last fifteen years. Some of the problems that stem from the IPv4 design include:

- **Insufficient address space**: The 32-bit address space of IPv4 supports about 4 billion IP addresses. In spite of this, the supply of available IP Addresses is declining rapidly. The uneven distribution of addresses during the very early days of the IPv4 deployment implies that some countries, like the United States for example, still enjoy a relative abundance of addresses. Conversely, most Asian countries have either seen their supply dwindling or have run out of addresses. China, for example, has a serious concern over the limited addresses available under the current IPv4 scheme. The lifetime of IPv4 has been extended using techniques such as Network Address Translation (NAT). However, although such techniques appear to increase the address space, they fail to meet the requirements of peer-to-peer and client-server applications.

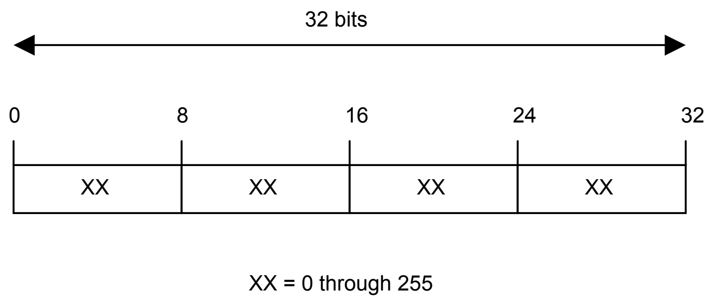


Figure 1. IPv4 Address Format

- **Security:** The age of IPv4 means that most of the security flaws inherent in the protocol have been found and patched. However, IPv4 does not come with a native encryption method. This has resulted in a plethora of proprietary encryption schemes, most of which are not interoperable.
- **Quality of service:** As with encryption methods, there are different interpretations of QoS standards, resulting in incompatibilities between systems.
- **Mobile IPv4:** This is the Internet Engineering Task Force (IETF) standard protocol for handling the mobility of an IPv4 node across the Internet. This protocol allows the use of a single fixed IP address regardless of the IP subnet changes, and hence enables continuous reachability for mobile nodes.
- **Inefficient routing:** In IPv4, a routing device devotes most of its computing power to the maintenance of routing tables. Routing tables

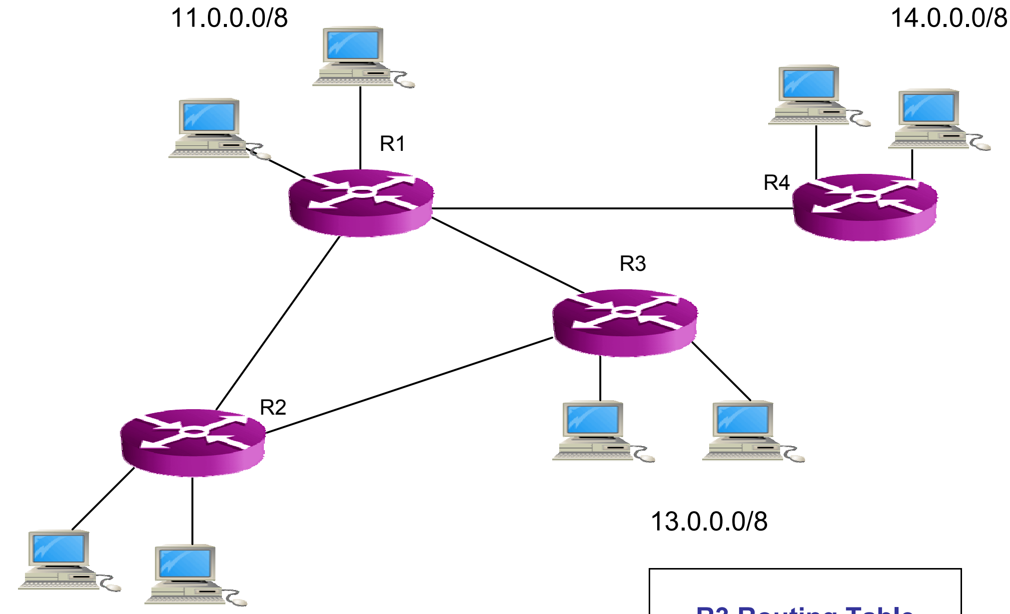
may contain more than 85,000 different routes. In an attempt to minimise these tables, Classless Interdomain Routing (CIDR) was introduced. CIDR is based on the concept of route aggregation. However, although CIDR reduces the routing problem, it is still not scalable, and certainly not efficient.

R1 Routing Table

Network	Route
11.0.0.0/8	Direct
12.0.0.0/8	R2
13.0.0.0/8	R3
14.0.0.0/8	R4

R4 Routing Table

Network	Route
14.0.0.0/8	Direct
11.0.0.0/8	R1
12.0.0.0/8	R1
13.0.0.0/8	R1



R3 Routing Table

Network	Route
13.0.0.0/8	Direct
11.0.0.0/8	R1
12.0.0.0/8	R2
14.0.0.0/8	R1

R2 Routing Table

Network	Route
12.0.0.0/8	Direct
11.0.0.0/8	R1
13.0.0.0/8	R3
14.0.0.0/8	R1

Figure 2. IP Routing and Routing Tables in IPv4

IPv4 has been remarkably resilient in spite of its age. However, the continuous demand for IP addresses – as more machines are introduced onto the internet – together with the various prerequisites imposed by new internet applications, are forcing the internet to put aside IPv4 and begin the transition towards IPv6.

2.2 IPv6

The Internet Engineering Task Force (IETF) developed IPv6, using its own experience gained from the work on IPv4. Though approved as a standard many years ago, the high cost of rolling it out was too severe. At the time, the required networking technologies associated with rolling out the protocol en masse required replacing routers and other equipment geared to IPv4. However, the scenario is nowadays different, since both software and hardware developers are offering technologies based on IPv6.

IPv6 is designed to address the problems related with IPv4. IPv4 and IPv6 operate independently of each other (the two are completely different protocols). This inherent lack of dependencies between IPv4 and IPv6 hosts and routing infrastructure requires a number of mechanisms that allow seamless coexistence. Any migration will have to take into account an interim period where both technologies will coexist in the same network. This should not present any problems since most networking devices are already capable of supporting both technologies simultaneously (Dual IP layer, IPv6 over IPv4 tunnelling and DNS infrastructure are the three mechanisms utilised to permit the coexistence of IPv6 and IPv4 infrastructures). As a consequence, the previously encountered disadvantages related with IPv6 are being counterbalanced, and even superseded, by the advantages of its adoption. IPv6 offers the following benefits:

- **Efficiency/performance:** The IPv6 header is different from the IPv4 header. The former header size is larger yet simpler than the IPv4 header. In the IPv6 header, some IPv4 header fields have been dropped or made optional to reduce the necessary amount of packet processing and to limit the bandwidth cost of the IPv6 header[1]. This has resulted in a header that is only twice the size of a standard IPv4 header, even though the number of available IPv6 addresses is four times larger than the number of IPv4 addresses (128bits as opposed to 32bits used)

[1] http://www.garykessler.net/library/ipv6_exp.html

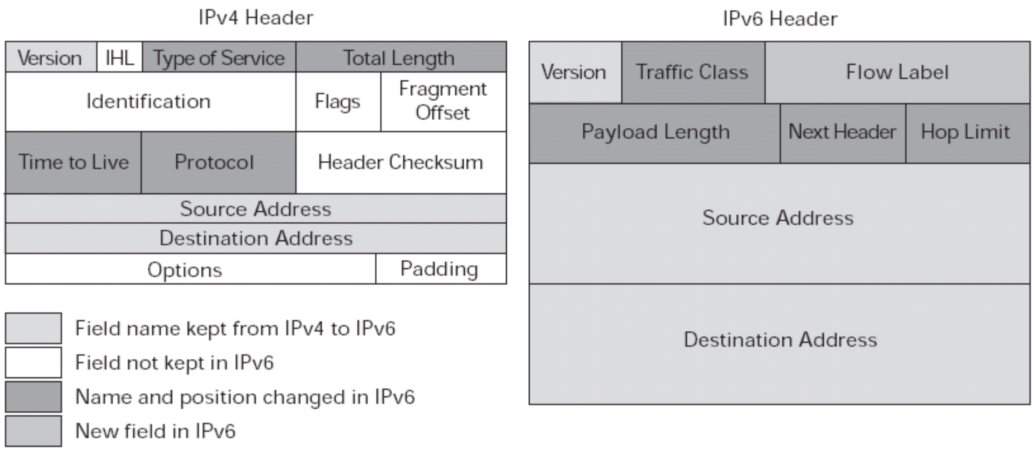


Figure 3. Comparison of the IPv4 and IPv6 header

- **Larger Address Space:** As previously stated, IPv6 addresses are 128 bits long. These 128 bits in IPv6 support approximately 3.4×10^{38} addresses, implying approximately 1030 addresses per person on this planet. It is a matter of speculation whether such a huge address base will spell the end of Network Address Translation (NAT) technologies, once use of IPv6 becomes widespread.

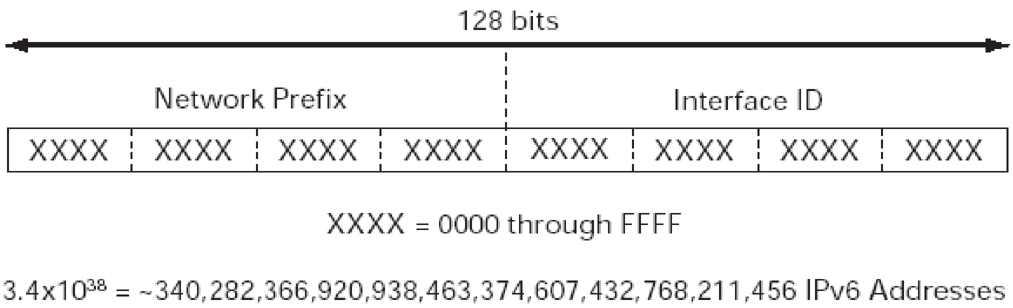


Figure 4. IPv6 Address Format

- **More efficient routing:** The Internet is hierarchical in nature, and the IPv6 protocol is designed with this in mind. The IPv6 protocol is designed so that Internet backbone routers will have much smaller routing tables than they have now. Instead of knowing every possible route, the routing tables will only contain information related to those routers connected directly to them. The IPv6 protocol will contain the rest of the information necessary for a packet to reach its destination. The availability of a very large addressing space and the use of network prefixes, results in more flexible network architectures. This flexibility allows an organisation to use only one prefix for the entire network of the organisation. The larger IPv6 address space enables the use of multiple levels of hierarchy inside the address space. Every level aggregates the traffic at that level. Thus, the allocation of addresses is enhanced in a hierarchical format. This hierarchical addressing structure reduces the size of the Internet routing tables.

- **New configuration options:** The address auto-configuration feature is built into the IPv6 protocol. This facilitates intranet-wide address management and enables a large number of IP hosts to easily discover the network. A new and globally unique IPv6 address, associated with the location, is obtained in the process. This auto-configuration feature enables ‘plug-and-play’ Internet deployment of new consumer devices such as cell phones, wireless devices and home appliances. Consequently, network devices can connect to the network without manual configuration and without any servers, like DHCP servers.
- **Integrated security:** IPSec is optional in IPv4. However, it is mandatory in IPv6 since it is part of the protocol suite. IPv6 provides security extension headers, like the Authentication header, and supports security protocols like the Encapsulating Security Payload (ESP). This makes it easier to implement encryption, authentication and virtual private networks (VPNs). It can provide end-to-end security services.

16	24	32bits
Security association identifier (SPI)		
Sequence Number		
Payload data (variable length)		
Padding (0-255 bytes)		
	Pad Length	Next Header
Authentication Data (variable)		

Figure 5. The ESP header

- **Standardized QoS support:** IPv6 handles QOS in exactly the same way it is currently being handled in IPv4. However, the iPv6 header has a new field named Flow Label that can contain a label identifying a specific flow of information such as video stream or videoconference. The flow label itself is not a feature of QOS. However, it enables QOS devices in the path to take appropriate actions based on this label.[2] Since the QOS instructions are included in the header, the packet’s body can be encrypted without affecting the QOS. QOS will still

[2] http://www.cisco.com/application/pdf/en/us/guest/products/iosswrel/c1127/cdccont_0900aecd8018e369.pdf

function since the header portion containing the instructions is not encrypted.[3] .

- **Mobile IPv6:** Mobility is a built-in feature in IPv6. Any IPv6 node can use mobility as required. IPv6 packets addressed to the home address of a mobile node are transparently routed to its 'care-of' address. This is achieved by caching the bound home address of the mobile's node with its 'care-of' address. This binding allows any packets destined for the mobile node to be directed to it at this 'care-of' address. One useful by-product of this feature is location-based services. The geographic location of a mobile node can be inferred. Hence, customised service or content can be provided using Mobile IPv6 location update signalling. This optional protocol signalling can be turned off if the mobile node's location privacy is an issue.
- **Increased number of Multicast addresses:** IPv6 does not use broadcasts at all. Previously supported IPv4 broadcasts functions are being handled by the IPv6 multicast. Multicast permits IP packets such as video stream to be sent to multiple destinations at the same time. This saves on network bandwidth. Multicast improves the efficiency of the network by limiting the broadcast requests to a smaller number of only interested nodes. As a consequence, IPv6 prevents the problems caused by broadcast storms in IPv4 systems.

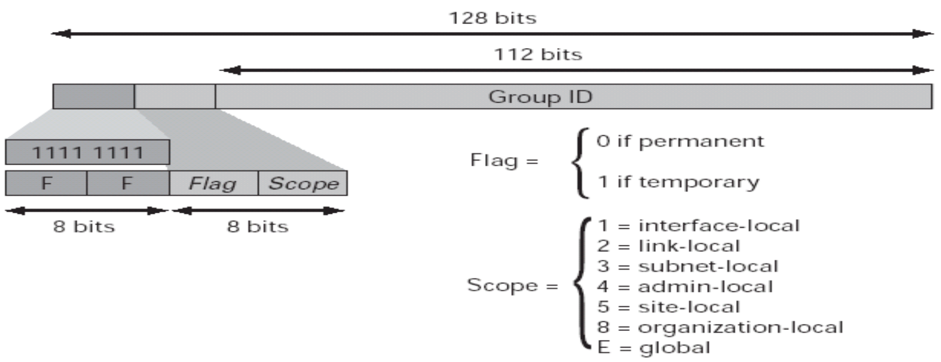


Figure 6. IPv6 Multicast Address Format

[3] http://techrepublic.com.com/5100-6329-5030146.html?tag=e044

3. CURRENT SITUATION

3.1 IPv6 Ready Tools

The drive for IPv6 started a number of years ago. In fact, anticipating the future direction of the Internet, most hardware (Sun, Checkpoint and Cisco for example) and software vendors are already shipping IPv6 capable products. Windows XP Service Pack 2 and most UNIX variants support both IPv4 and IPv6. IPv6 is still not common in consumer devices based on embedded OS. Although various mechanisms were designed to enable communication between IPv6 and IPv4 (embedded IPv4 addresses, pseudo checksum rules were built into IPv6 to support transition and co-existence with IPv4), this interoperability had to be tested. The interoperability among the various IPv6 products themselves had to be tested as well. Thus, various initiatives were set up with the main objective of experimenting with, and enhancing the adoption of IPv6, and supporting the organisations that wished to deploy it. The aim was also to educate people, widening their knowledge base on IPv6 and giving them sufficient information on the equipment and the services available.

3.2 IPv6 and the EU

In January 2000 the 6INIT project was created. The aim of this project was to validate IPv6 and to promote the introduction of IPv6 multimedia and security services in Europe. The project had a running time of 16 months. Since then, the number of initiatives has risen to over forty, with a total expenditure of over €180M by the EU and various business entities. The scope of these initiatives is very wide and far-reaching. Some of them place particular emphasis on IPv6, whereas others include it as a peripheral issue. Addressed technologies include wireless and satellite broadband access, QoS and Broadband through Power Lines.

EURO6IX and 6NET are two very large test-beds that contributed in no small measure to the testing and the spreading of knowledge on IPv6.

The 6NET project is a three-year European project. Its main aim was to demonstrate that the continued growth of the Internet can only be met using IPv6 technology. The project has built a native IPv6-based network connecting 16 countries in order to gain experience of IPv6 deployment and migration from existing IPv4-based networks. Extensive tests were held on a variety of new IPv6 services and applications, as well as the interoperability with legacy applications. 6NET has demonstrated that IPv6 is deployable in a production environment. Not only does IPv6 solve the shortage of addresses, but it also promises a number of enhanced features that are not an integral part of IPv4. The project was a major factor in accelerating the rollout of dual-stack operation on the GÉANT and NORDUnet networks, as well as many National Research and Education Networks (NRENs). The 6NET network itself has been used to provide IPv6 connectivity to a number of worldwide events, including IST 2002 (November 2002), IETF 57 (July 2003), IST 2003

(November 2003) and the Global IPv6 Service Launch (January 2004), showing that it is ready for full deployment.[4]

Euro6IX is a Pan-European initiative aimed at contributing and supporting the rapid introduction of IPv6 in Europe. The Euro6IX testbed can be considered as a complete test-bed for the future IPv6. The testbed includes most of the Internet elements (External Peerings, International Backbone of IPv6 dedicated links, IX's, Leaf Nodes) and actors (Operators/ISPs, R&D Organizations, Network Consultants, Vendors, Beta-tester Users).[5]

During the European Council meeting, in 2002, the European Commission IPv6 Task Force presented its results to the European Commission. The Task Force requested the Commission to compile a set of recommendations, with the prime aim of giving priority to the deployment of IPv6 as part of the e-Europe 2005 initiative. In reply to this request, the Commission issued a communication to the Council and the European Parliament named "Next Generation Internet – priorities for action in migrating to the new Internet Protocol IPv6". The Commission also called for the renewal of the mandate of the IPv6 Task Force as a platform for debate on critical issues concerning IPv6 deployment.[6]

Currently there are more than 25 Task Forces operating at a national level. 12 of the Task Forces are in EU member states. These task forces are all directly supported by the IPv6 Task Force Steering Committee (IPv6 TF-SC). The Committee is still the main player behind the drive for the global deployment of IPv6

Many of the IPv6 projects have either reached their end of life or are approaching their final stage (the 6NET project, for example, terminated in December 2004). The results achieved from these projects were positive and in favour of IPv6. Projects like GÉANT (which links multiple academic institutions at Gigabit speed) have already activated IPv6. ISPs and Telco's who participated in the EURO6IX project have already announced IPv6 services. In the meantime, global coverage has been demonstrated to be feasible at a recent demonstration called "Global IPv6 Service Launch". At the venue, the efforts of 6NET, Euro6IX, GÉANT, the IPv6 Cluster, Eurov6 and the European IPv6 Task Force were jointly combined to make a successful global connection using only a native IPv6 infrastructure. Also on show were some ten demonstrations of IPv6 technology in action from European research projects, including IPv6 over satellite, IPv6 over power lines and Remote home automation and interaction.

The EU is at the forefront of IPv6 development. Indeed, it's ambition to be the most competitive and dynamic knowledge-based economy by 2010 can only be realised if it also plays a leading role in the upgrading of the Internet's capabilities. Maintaining and building on its wireless and mobile communications and providing for an efficient transition to the next generation

---

[4] http://www.6net.org/publications/info/6net-2004.pdf

[5] http://tb.tid.euro6ix.org/enext/EURO6IX.pdf

[6] http://www.usipv6.com/6sense/2004/jun/june002.htm

Internet, based on the new Internet Protocol (IPv6), are crucial factors in this regard.[7]

3.3 IPv6 Implementations throughout the World

The subject of IPv6 is causing interest all around the globe. Several countries are looking at IPv6 as an alternative protocol to its IP predecessor, IPv4. The main drive in most of the cases is the lack of address space. Many firms in Asia are adopting IPv6 technology because they need IP addresses and have no other choice. Japan has a government-imposed deadline to upgrade its IT sectors to run on IPv6 by 2005.[8] Through the setup of a large-scale Next Generation Network with an IPv6 core, China is becoming a powerful engine for the world's IPv6 industry development. Even in the Americas, where there is ample address space available, the interest in IPv6 is growing slowly but steadily. Recent reports suggest that IPv6 will start to take up so rapidly that there is the danger of a divide in Internet users: those with IPv4 and those with IPv6.

The Internet Address Registries have already worked out and adopted a common IPv6 Allocation Policy and a number of companies have already been allocated IPv6 addresses.

Many of the xDSL providers are also the old incumbent Telco's. A large proportion of their revenue stream is obtained from the existing PSTN. The existing PSTN exchanges are in need of replacement/upgrades. However, with lifetimes of 20+ years, the providers are reluctant to invest money in the PSTN when there is a generally accepted view that voice traffic will migrate from the PSTN to IP technology. As a result, some operators are taking the plunge and have announced that all telephone traffic will run over IP in 10 to 15 years time. Among these companies we find Deutsche Telekom and BT.

VoIP is another application that is not being allowed to flourish worldwide due to IPv4. Currently, one of the major difficulties of deploying VoIP service is the wide usage of network address translators and private addresses in the Internet. While it is quite possible to connect out from a NAT network, it is considerably harder, if not impossible, to connect in to a NAT network, especially with multiple services running within it. With the wider deployment of VoIP services, and the introduction of VoIP services in next generation wireless networks (3GPP), the lack of addresses in the IPv4 world will impose even larger barriers on the successful deployment of VoIP solutions. In this context, Internet-Telephony is one field that will profit from the wide range of IPv6 addresses in addition to the general advantages of the IPv6 technology. VoIP is touted to be one of the most promising technologies in the drive to revolutionise the telecommunication market. It will be a major contributor to the movement for the world-wide implementation of IPv6.

---

[7] http://europa.eu.int/eur-lex/en/com/cnc/2002/com2002_0096en01.pdf

[8] http://www.macnewsworld.com/story/31230.html

3.4 IPv6 in Malta

Malta enjoys one of the highest penetration rates of IT per Capita in Europe. This is reflected in the proportion of households with Internet access and also the number of companies that regularly use a computer and have a network installed.

As previously stated, the EU is at the forefront of IPv6 development. A variety of initiatives have been set up, aimed at pushing the adoption of this technology as early as possible. The advantages of an early adoption are understood to be numerous.

Unlike some of the other countries in the EU, Malta has adopted a rather passive attitude towards IPv6. No activity appears to be going on as regards to the testing and the evaluation of IPv6 among the various organisations. For the moment, this lack of involvement does not have any drastic effects on the country's technological development. However, in the near-future, as applications become more enhanced and more versatile (like e-services for example) in nature, Malta will not be able to benefit to the full from these applications since they will require the presence of IPv6 in order to be completely operational. Many of the organisations concerned with IPv6 already have hardware and software that can cater for both IPv4 and IPv6. From the government's side, most of the infrastructure is up-to-date and can deal with both standards as well. Recently installed Windows, UNIX and LINUX servers have inbuilt support for IPv6. Having said this, the transition from one standard to another requires a lot of planning and preparation. A significant amount of testing has to be performed. In addition, the actual transition to IPv6 will have to be scheduled over a time span of a number of years (Korea, for example, is aiming to have IPv6 fully deployed by 2011). The transition certainly cannot occur overnight. In sum, Malta will definitely benefit if it had to migrate to IPv6. There is a global interest in getting IPv6 implemented as quickly as possible and it is gaining rapid momentum particularly from the advent of Radio Frequency ID tags (RFIDs), which are revolutionizing the logistics, warehousing and distribution services offered, and 3G. Since the migration to IPv6 will take a few years to reach its final stage, now is the right time to commence planning the transition if Malta wants to remain in step with the rest of the Internet community.

4. RECOMMENDATIONS

4.1 Position of MIIIT and MCA

A technology with the far-reaching effects of IPv6 requires a special course of action to be taken. Care must be taken with every step to ensure that no disruption of service occurs through lack of forethought and planning. Nevertheless, it is important to be realistic and appreciate that today IPv6 is still relatively unknown territory for Malta. It is therefore necessary to start by first learning the basics. All stakeholders need to understand that we are in the early stages and, as such, we are a very long way from adoption of IPv6 as a standard; let alone as a technology for everyday use.

In this context, it is necessary to strike a balance between the urge to be amongst the early adopters of this technology, and the need to follow a gradually-paced timetable, avoiding unnecessary and ego-fuelled research projects. It is important to keep in mind the clear objective of giving top priority to the roll-out of IPv6. This will strengthen the competitiveness of the local industry and avoid the risk of inhibiting the attraction of Foreign Direct Investment (FDI) in the logistics, warehousing and distribution sectors.

However, having said all this, the transition to IPv6 is inevitable. If Malta wants to be at the forefront of technology trends, offering services like 3G for example, then IPv6 is the only way forward. IPv6 will bring along a myriad of possible applications. Consequently, the customer will also benefit from this deployment. It is therefore imperative that Malta gives this issue its due importance. Good preparatory work will ensure that Malta has the necessary knowledge and hands-on experience required for such an important task. It is essential that each one of us is reasonably conversant with the advantages that IPv6 has to offer but also with its limitations given it is a relatively new technology.

4.2 Possible Issues during Transition

Protocol transitions are not easy and the transition from IPv4 to IPv6 is no exception. Such transitions are typically deployed by installing and configuring the new protocol on all the nodes within the network. It must then be verified that all node and router operations work successfully. The challenge of accomplishing such a task, in an efficient and timely manner, increases exponentially according to the size of the network involved. Given the scope of the Internet, rapid protocol transition becomes an impossible task.

The designers of IPv6 recognized that the transition from IPv4 to IPv6 will take years. Therefore, while migration is the long-term goal, equal consideration must be given to the interim coexistence of IPv4 and IPv6 nodes. Rightly so, queries and issues will definitely arise during this interim period. People might lack the knowledge required to operate a combined IPv6 and IPv4 network. Organisations might not want to invest in new capital. So, the challenge is to make the best out of the existing hardware (if it can already handle IPv6) while replacing the IPv4-only supporting hardware.

Since the migration to IPv6 will take place over a long period of time, organisations will have ample time to experiment, discuss problems with their peers and learn about the new standard. In this way, operators will have sufficient time to co-operate between themselves the transition. In addition, consumers will also be affected, since they will have to reconfigure their network settings (this might imply an Operating System (OS) upgrade). So, it is of utmost importance that they are educated about the matter as well. This will help to solve any problems and queries that they might encounter.

4.3 IPv6 Task Force

There are some 25 task forces operating in different EU member states and other countries. The initiatives taken by these Task Forces were fundamental to the eventual adoption of IPv6. They fostered a culture of innovation in technology that can take advantage of the new possibilities offered by IPv6.

To start the wheel rolling, it is the aim of MIIIT and MCA to set up a National IPv6 Task Force for the Maltese Islands (IPv6TF-MT). The Task Force will facilitate the transition to IPv6.

The Task Force will be chaired by MCA. The latter will be responsible for the logistical and administrative elements of the task force. Any research activities will be jointly undertaken by the MCA and MIIIT. It is recommended that the Task Force adopts the following Terms of Reference:

- Monitor the status of IPv6 penetration in Malta, Europe and globally;
- Identify key initiatives for the implementation of IPv6 in Malta;
- Identify and advise upon the potential barriers and problems which could obstruct the objective in (2) at the national level;
- Identify actions for the deployment of IPv6 that may be taken at public and private organisational level;
- Facilitate the development and deployment of a national IPv6 Test-bed;
- Increase the level of awareness of the benefits and opportunities offered by IPv6; and
- Associate and coordinate with the European Commission IPv6 Task Force in order to conform to current European working models and practices.

4.3.1 Test Bed Proposal

The idea is to setup a test bed (Figures 7 and 8 depict a sample network topology. Other platforms not illustrated in the diagram, like GPRS, can also be implemented) between voluntary members from the industry. This project should help the industry get an idea what technical issues are involved in such transitions. Fear of the unknown can sometimes hinder a technology from evolving. The project should help provide solutions and act as a catalyst for the transition. It will also be the ideal place to test various technical aspects of the migration to IPv6, for example:

- Co-existence with IPv4
- Performance of ADSL, broadband or other technologies over IPv6
- Interaction between ATM and IPv6

Every member will be able to suggest trials that are more pertinent to the member's line of work. All this will take place in a neutral environment, which will guarantee the integrity of the individual business strategies.

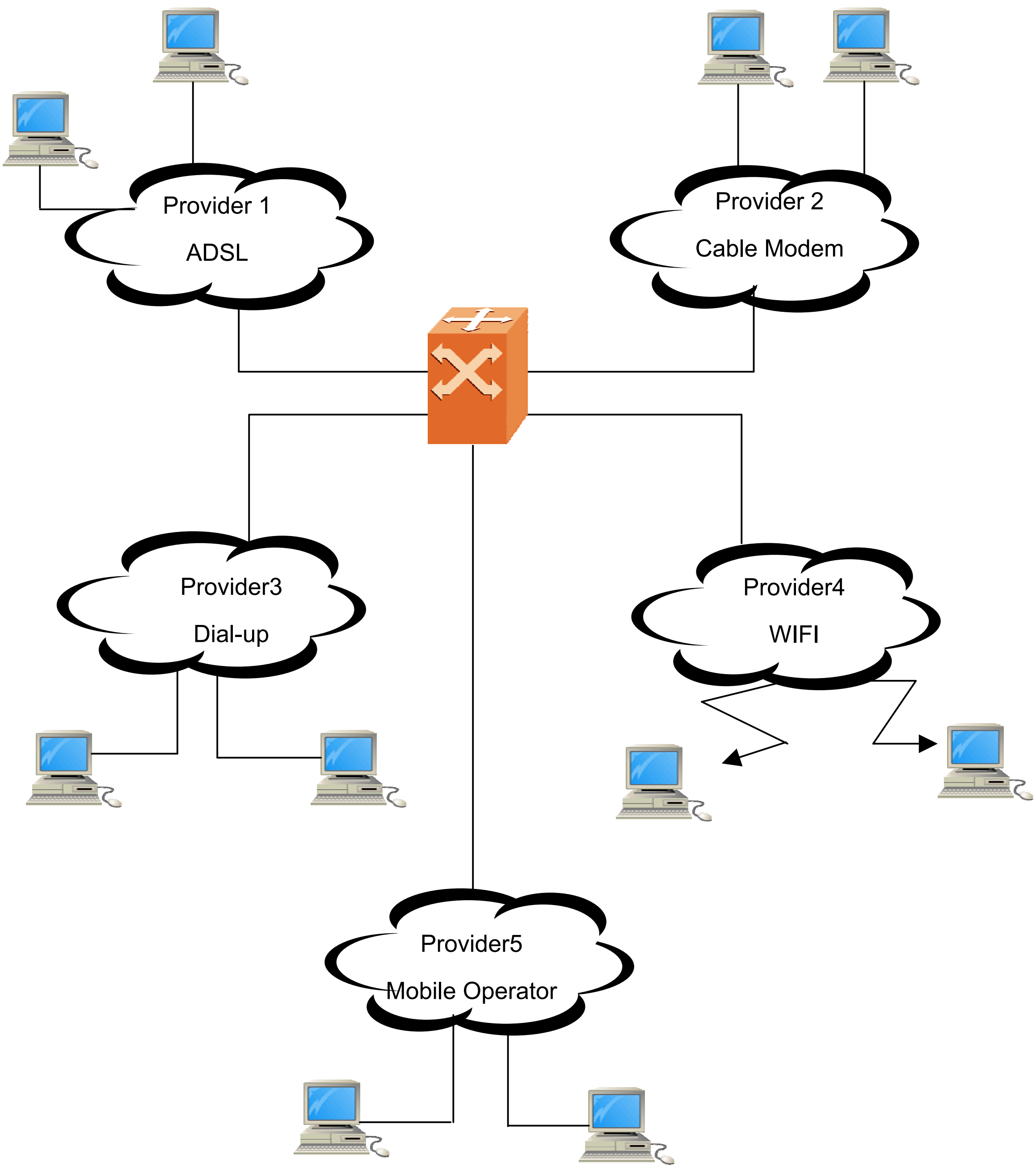


Figure 7: A sample of the network that can be setup as a test-bed

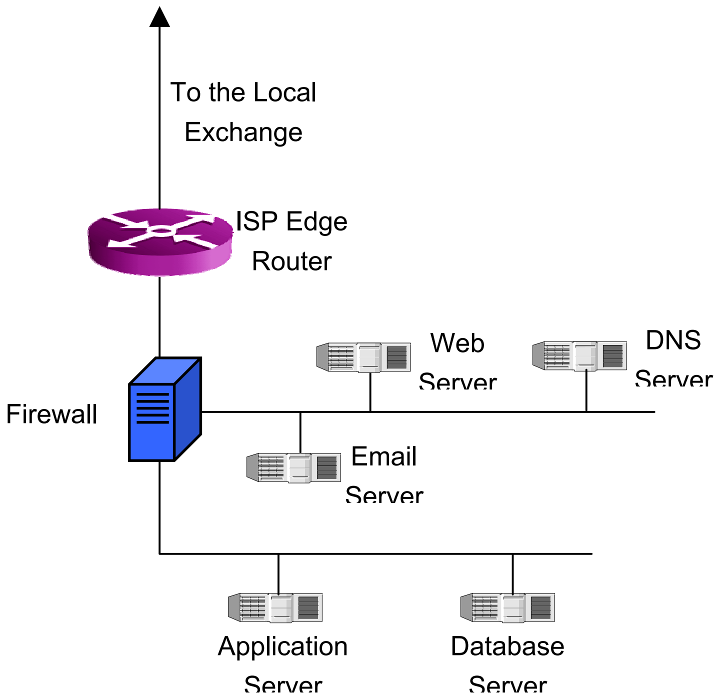


Figure 8: Possible setup at provider's end

4.3.2 Possible Test Schedule

The purpose of the test bed is to gather as much knowledge as possible. It should therefore focus on two different aspects: the migration to IPv6 (including the interoperation between IPv4 and IPv6 during the interim period) and the performance of an IPv6 network.

Network designers recommend deploying IPv6 at the end first and then moving towards the network core. This reduces the cost and the operational impacts of the integration. The key strategies used in deploying IPv6 at the edge of a network involve carrying IPv6 traffic over the IPv4 network, allowing isolated IPv6 domains to communicate with each other before the full transition to a native IPv6 backbone. It is also possible to run IPv4 and IPv6 throughout the network, from all edges through the core, or to translate between IPv4 and IPv6 to allow hosts communicating in one protocol to communicate transparently with hosts running the other protocol. All techniques allow networks to be upgraded, and IPv6 deployed incrementally with little to no disruption of IPv4 services.[9]

The following tests could be performed on the test bed, once the latter is set up:

- A single organisation upgrades to IPv6 (starting from the edge network and moving towards the core as outlined above). This initial step is a

---

9 http://www.cisco.com/application/pdf/en/us/guest/products/iosswrel/c1127/cdccont_0900aecd8018e369.pdf

good test for the interoperability between the two protocols since IPv4 and IPv6 will be functioning concurrently within the same network.

- This upgrade is followed by a detailed analysis of the system's performance. This stage is particularly important since it gives an idea whether certain upgrades are dependent on others.

- Following this, the exchange can be upgraded. Tests can be performed at this stage to check that all the ISPs functionality is unaffected.

- Subsequently, the remaining organisations can be upgraded, one by one. Adequate testing is performed after every individual upgrade.

- On completion of the organisations' upgrades, clients can commence to upgrade their PCs to IPv6. As previously discussed this is certainly not a trivial feat. Customers will have to be appropriately educated, especially since most of them will have to upgrade their PC's OS in order to be able to work with IPv6.

Once the network has been set up, other tests can be performed focusing on performance issues, such as load tests and the length of routing tables. The tests should be performed with various OS so as to verify the correct operation of IPv6 with all platforms.

4.3.3 IPv6 Roadmap for Malta

The first key deliverable of the Task Force will be an IPv6 Roadmap for Malta. A number of recommendations can be set up stating the way forward for the adoption of IPV6 in Malta. The report will also include impact assessments on the local industry, implementation time-table, and the results obtained from the IPv6 test-bed

The task force will work towards the following deliverables:

- Issue ongoing reports on the results obtained through the test bed;

- Promote the increased deployment in Enterprise Intranets, Service Provider Networks and Carriers, and across the Internet;

- Promote the increase in the number of content and application vendors utilising IPv6 solutions;

- Increase the knowledge of IPv6 standards, technologies, products and services;

- Partner with other players to devise models for financial and cost/benefit analysis of transition, with regard to cost and potential revenues;

- Support educational institutions to gain access to IPv6-related knowledge;

5. CONCLUSION

The continuous growth of the global Internet requires that its overall architecture evolve to accommodate the new technologies that support the growing numbers of users, applications, appliances, and services. Internet Protocol Version 6 (IPv6) is designed to meet these requirements and allow a return to a global environment where the addressing rules of the network are again transparent to the applications.

Industry is in the early stages of IPv6 deployment—few IPv6 innovative applications are in the market. First-generation products need to make tradeoffs between available IPv6 services. Although the success of IPv6 will ultimately depend on the new applications that run over IPv6, a key part of the IPv6 design is its ability to integrate into and coexist with existing IPv4 networks. It is expected that IPv4 and IPv6 hosts will need to coexist for a substantial time during the steady migration from IPv4 to IPv6. The development of transition strategies, tools, and mechanisms has been part of the basic IPv6 design from the start.

Many countries in Europe, and in the world, have already started their long journey towards an all-IPv6 network. Organisations in Malta do not appear to be following this trend. As the main problems related with IPv4 start to emerge to the surface, and as applications become more dependable on the IPv6 protocol in order to operate correctly and fully, it is only logical that organisations in Malta go along with the crowd and begin considering seriously the adoption of IPv6.

6. CONSULTATION FRAMEWORK

The MCA and MIIIT wish to invite comments from interested parties in relation to any of the issues raised in this documents. The consultation period will run until **12:00pm on Friday 22nd July 2005**.

Comments in response to this document should be sent (preferably **in electronic format**) to:

Clara Delia	Adrian Scicluna
Technical Specialist	Project Coordinator - ICT Environment Consolidation
Malta Communications Authority	Ministry for Investment, Industry and Information Technology
Suite 43/44, 'Il-Pjazzetta'	Information Society Secretariat
Tower Road	54/2 Zachary Street
Sliema SLM16	Valletta VLT 08
Malta	Malta
Tel: +356 21 336 840	Tel: +356 21 255495
E-Mail: cdelia@mca.org.mt	E-mail: adrian.scicluna@gov.mt

Receipt of comments will be confirmed. Comments will be made publicly available at the MCA and MIIIT unless declared confidential. Respondents are therefore asked to separate out any confidential material into a clearly marked annex. Respondents are also kindly requested to refer their comments to the specific sections of the document.

7. GLOSSARY

Asynchronous Transfer Mode, ATM

ATM is a dedicated-connection switching technology that organizes digital data into 53-byte cell units and transmits them over a physical medium using digital signal technology. Individually, a cell is processed asynchronously relative to other related cells and is queued before being multiplexed over the transmission path.

Authentication

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks (including the Internet), authentication is commonly done through the use of logon passwords. Knowledge of the password is assumed to guarantee that the user is authentic.

Classless Inter-domain Routing, CIDR

CIDR (sometimes known as supernetting) is a way to allocate and specify the Internet addresses used in inter-domain routing more flexibly than with the original system of Internet Protocol (IP) address classes. As a result, the number of available Internet addresses has been greatly increased. CIDR is now the routing system used by virtually all gateway hosts on the Internet's backbone network. The Internet's regulating authorities now expect every Internet service provider (ISP) to use it for routing.

Client-Server Applications

Client/server describes the relationship between two computer programs in which one program, the client, makes a service request from another program, the server, which fulfils the request.

Digital Subscribers Line, DSL

DSL technologies use sophisticated modulation schemes to pack data onto copper wires. They are sometimes referred to as last-mile technologies because they are used only for connections from a telephone switching station to a home or office, not between switching stations.

e-commerce

E-commerce (electronic commerce or EC) is the buying and selling of goods and services on the Internet, especially the World Wide Web.

e-services

E-services, a business concept developed by Hewlett Packard (HP), is the idea that the World Wide Web is moving beyond e-business and e-commerce (that is, completing sales on the Web) into a new phase where many business services can be provided for a business or consumer using the Web. Some e-services, such as remote bulk printing, may be done at a Web site; other e-services, such as news updates to subscribers, may be sent to the computer. Other e-services will be done in the background without the customer's immediate knowledge.

Foreign Direct Investment, FDI

FDI is defined as a firm based in one country (the 'home country') owning 10 percent or more of the stock of a company located in a foreign country (the 'host country') -- this amount of stock is generally enough to give the home country firm significant control rights over the host country firm. Most FDI is in wholly-owned or nearly wholly-owned subsidiaries.

General Packet Radio Service, GPRS

GPRS is a packet-based wireless communication service that promises data rates from 56 up to 114 Kbps and continuous connection to the Internet for mobile phone and computer users. GPRS is based on Global System for Mobile (GSM) communication and will complement existing services such as circuit-switched cellular phone connections and the Short Message Service (SMS).

Internet Engineering Task Force, IETF

The IETF is charged with developing and promoting Internet standards. It is an open, all-volunteer organization.

Internet Protocol, IP

The IP is used to route messages within an IP network. Every IP packet contains its own header. This provides the information that allows the packet to reach its destination. IP packets can vary in size, providing great flexibility in transporting traffic and maximising use of the available bandwidth.

IP address

An IP address is a 32-bit number (in the case of IPv4) or a 128-bit number (in the case of IPv6) that identifies every sender or receiver of information that is sent in packets across the Internet.

Internet Protocol Security, IPSec

IPSec is a set of protocols, developed by the IETF to support secure exchange of packets at the IP layer.

Internet Service Provider, ISP

An ISP (Internet service provider) is a company that provides individuals and other companies access to the Internet and other related services such as Web site building and virtual hosting. An ISP has the equipment and the telecommunication line access required to have a point-of-presence on the Internet for the geographic area served.

Multicast

Multicast is communication between a single sender and multiple receivers on a network. Typical uses include the updating of mobile personnel from a home office and the periodic issuance of online newsletters. Multicast is one of the packet types in the IPv6.

National Research and Education Network, NREN

The primary purpose of the NREN Program is to establish a gigabit communications infrastructure that will dramatically enhance the ability to collaborate among members of the research and education community. In order to establish such an infrastructure, networking technologies have to be developed and services from common carriers and other communications service providers must be made available in this development effort.

Network Address Translation, NAT

NAT is the translation of an Internet Protocol address used within one network to a different IP address known within another network. One network is designated the *inside* network and the other is the *outside*. Typically, a company maps its local inside network addresses to one or more global outside IP addresses and un-maps the global IP addresses on incoming packets back into local IP addresses. This helps ensure security since each outgoing or incoming request must go through a translation process that also offers the opportunity to qualify or authenticate the request or match it to a previous request. NAT also conserves on the number of global IP addresses that a company needs and it lets the company use a single IP address in its communication with the world.

Peer-to-Peer applications

Peer-to-peer is a communications model in which every party has the same capabilities and either party can initiate a communication session.

Public Switched Telephone Network, PSTN

PSTN is the world's collection of interconnected voice-oriented public telephone networks, both commercial and government-owned. It's also referred to as the Plain Old Telephone Service (POTS). It's the aggregation of circuit-switching telephone networks. Today, it is almost entirely digital in technology except for the final link from the central (local) telephone office to the user.

Quality of Service, QoS

QoS is a networking term that specifies a guaranteed throughput level.

Radio Frequency Identification, RFID

RFID is a technology similar to barcode identification. With RFID, the electromagnetic or electrostatic coupling in the RF portion of the electromagnetic spectrum is used to transmit signals. An RFID system consists of an antenna and a transceiver, which read the radio frequency and transfer the information to a processing device, and a transponder, or tag, which is an integrated circuit containing the RF circuitry and information to be transmitted.

Requests for Comment, RFC

The Requests for Comments (RFC) document series is a set of technical and organizational notes about the Internet (originally the ARPANET), beginning in 1969. Memos in the RFC series discuss many aspects of computer networking, including protocols, procedures, programs, and concepts, as well as meeting notes, opinions.

Router

A router is a device or, in some cases, software in a computer, that determines the next network point to which a packet should be forwarded toward its destination. The router is connected to at least two networks and decides which way to send each information packet based on its current understanding of the state of the networks it is connected to.

Routing Table

A router may create or maintain a table (called a routing table) of the available routes and their conditions and use this information along with distance and cost algorithms to determine the best route for a given packet.

Telco

In the United States and possibly other countries, "telco" is a short form for a telephone company. Sometimes it means a local telephone company, such as a Bell operating company or an independent local telephone company. Sometimes it means any telephone company, including one offering long-distance services.

Third Generation Communications, 3G

3G is the generic term used for the next generation of mobile communications systems. The new systems will enhance the services available today and offer multimedia and internet access and the ability to view video footage.

Third Generation Partnership Project, 3GPP

The 3rd Generation Partnership Project (3GPP) is a collaboration agreement that was established in December 1998. The collaboration agreement brings together a number of telecommunications standards bodies that are known as “Organizational Partners”. The current Organizational Partners are ARIB, CCSA, ETSI, ATIS, TTA, and TTC.

Virtual Private Network, VPN

VPN is a way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.

Voice over IP, VoIP

VoIP (that is, voice delivered using the Internet Protocol) is a term used in IP telephony for a set of facilities for managing the delivery of voice information using the Internet Protocol (IP). In general, this means sending voice information in digital form in discrete packets rather than in the traditional circuit-committed protocols of the public switched telephone network (PSTN). A major advantage of VoIP and Internet telephony is that it avoids the tolls charged by ordinary telephone service.

xDSL

xDSL Refers collectively to all types of **DSL**, the two main categories being ADSL and SDSL. Two other types of xDSL technologies are High-data-rate DSL (HDSL) and Very high DSL (VDSL).