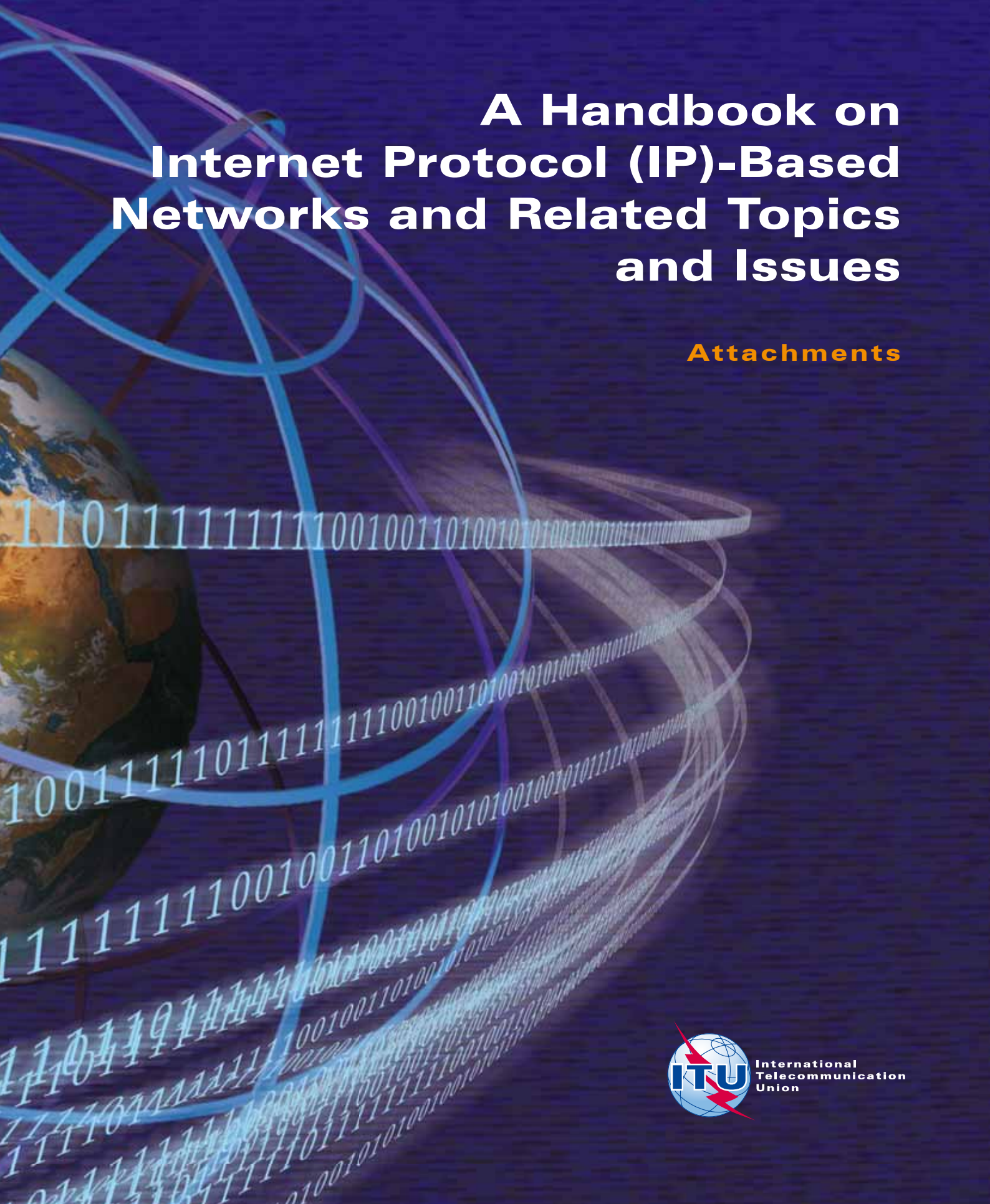
International Telecommunication Union

A Handbook on Internet Protocol (IP)-Based Networks and Related Topics and Issues

Attachments



International Telecommunication Union

International Telecommunication Union

A Handbook on Internet Protocol (IP)-Based Networks and Related Topics and Issues

A Handbook on Internet Protocol (IP)-Based Networks and Related Topics and Issues

Attachments

Table of contents

Attachment 1

Contribution by Mauritius

Table of contents

Contribution by Mauritius

The main issues surrounding the Internet

If the Internet is not like any other established communication technology, what then is it? On one level, the Internet is whatever anyone wants it to be. It is a plastic, decentralized, and constantly evolving network.

It is valuable to understand the Internet as a feedback loop. A feedback loop occurs when the output of a system is directed back into the system as an input. Because the system constantly produces fuel for its own further expansion, a feedback loop can generate explosive growth. As the system expands, it produces more of the conditions that allow it to expand further. All networks are feedback loops, because they increase in value as more people are connected. The Internet, however, is driven by a particularly powerful set of self-reinforcing conditions.

Some "supply" factors (such as the availability of higher-capacity networks) permit an expansion of demand (for example, by allowing bandwidth-intensive services such as high-resolution video transmission).

The Internet feedback loop is a fundamentally positive force, because it means that more and more services will be available at lower and lower prices. So long as effective self-correcting mechanisms exist, the Internet will overcome obstacles to its future growth.

Understanding the underpinnings of the Internet feedback loop is necessary in order to craft policies that facilitate, and do not hinder, its continuation. Four primary factors that support the growth of the Internet are addressed below.

1 Digitization and "deep convergence"

As described above, the Internet exhibits the characteristics of several media that had previously been distinct. Networks carry three types of information – voice, video, and data – and those categories are further subdivided into areas such as pre-recorded vs. live or real-time presentation, and still vs. moving images. Historically, these different forms of information have used different delivery vehicles. The telephone network delivered voice, private corporate networks delivered data, and broadcast networks delivered video. Each service was tightly coupled to a specific form of infrastructure – the telephone network used copper wires to reach subscribers, broadcast television used the airwaves, cable television used coaxial cable, and so forth.

"Convergence" means that those lines are blurring. However, convergence is often understood in a shallow manner, as simply the opportunity for owners of one type of delivery system to compete with another type of delivery system, or as the opportunity for content owners to deliver their content using different technologies. In reality, convergence is something far more fundamental. "Deep convergence" is driven by a powerful technological trend – digitization. Digitization means that all of the formerly distinct content types are reduced to a stream of binary ones and zeroes, which can be carried by any delivery platform. In practical terms, this means not only that specific boundaries – between a telephone network and a cable system, for example – are blurred, but also that the very exercise of drawing any such boundaries must be fundamentally reconsidered or abandoned.

Digitization has been occurring for decades. The long-distance telephone network in the United States is now almost entirely comprised of digital switches and fibre-optic transmission links. These digital facilities, however, have been optimized to transport a single service – voice. The Internet, by contrast, can transmit any form of data. Internet protocols are sufficiently flexible to overcome the boundaries between voice and other services. Innovators can develop new services and immediately load them on to the existing Internet infrastructure. Convergence creates new markets, and new efficiencies, because particular services are no longer locked into specific forms of infrastructure.

2 Moore's Law and Metcalfe's Law

The two technological "laws" that most impact the growth of the Internet are Moore's Law and Metcalfe's Law. Moore's Law holds that the maximum processing power of a microchip, at a given price, doubles roughly every eighteen months. In other words, computers become faster at an explosive rate, or conversely, the price of a given level of computing power decreases at that same dramatic rate. Metcalfe's Law says that the value of a network is equivalent to the square of the number of nodes. In other words, as networks grow, the utility of being connected to the network not only grows, but does so exponentially.

Moore's Law and Metcalfe's Law intersect on the Internet. Both the computers through which users access the Internet, and the routers that transmit data within the Internet, are subject to the price/performance curve described by Moore's Law. At the same time, advances in data transmission technology have expanded the capacity of the Internet's backbone networks. As the bandwidth available through the network continues to grow, Moore's Law states that the price of obtaining a given level of bandwidth continues to drop, while Metcalfe's Law dictates that the value of a connection increases exponentially. The ratio of the cost of Internet access to the value it provides plummets over time. And as it plummets, connectivity and higher-bandwidth connections become that much more important, generating more usage and more capital to upgrade the network.

3 Investment

Moore's Law and Metcalfe's Law describe the technological forces that push the growth of the Internet, but there are also business forces that exert a powerful influence. In a capitalist economy, the "invisible hand" of the market dynamically redirects capital where it is most highly valued, without any direct outside intervention. Companies that demonstrate superior potential for generating future revenues more easily attract investment, and, in the case of public companies, see their stock prices rise. Other companies in the same industry sector often see increases in their stock prices as well, as investors seek to repeat the pattern of the first company and to capitalize on economic trends.

As money flows into a "hot" sector, so do talented people seeking to obtain some of that money by founding or working at a company in that sector. The presence of so many top minds further attracts capital, reflecting a synergistic process. This trend promotes the availability of financing to spur the future growth of the Internet.

4 Competition

Competition enables both the dynamic allocation of capital and talent, as well as the constant innovation in technology that leads to deep convergence and falling prices. In a competitive market, companies must constantly invest and innovate, or risk losing out to competitors. Intel CEO Andy

Grove has observed that in the computer industry there are only two kinds of companies: the quick and the dead. Even those companies with strong positions must always look over their shoulder, because customer loyalty vanishes in the face of superior alternatives.

The benefits of competition are evident in the computer industry, where companies must constantly improve their products to remain successful. Competition in the Internet context means that many different providers of hardware, software and services vie for customers. In a competitive market, providers that can offer superior service or prices are more likely to succeed. Technological innovations that lower costs or allow new service options will be valuable to providers and consumers alike.

5 Threats to the continued spiral

If the Internet truly operates like a feedback loop, why is government intervention necessary?

There are many ways in which the Internet spiral could be derailed. Any of the underlying drivers of Internet growth could be undermined. Moving toward proprietary standards or closed networks would reduce the degree to which new services could leverage the existing infrastructure. The absence of competition in the Internet service provider market, or the telecommunications infrastructure market, could reduce incentives for innovation. Excessive or misguided government intervention could distort the operation of the marketplace, and lead companies to expend valuable resources manipulating the regulatory process.

Insufficient government involvement may also, however, have negative consequences.

Some issues may require a degree of central coordination, even if only to establish the initial terms of a distributed, locally-controlled system. A situation may arise when all players find it in their own self-interest to consume limited common resources. The end result, in the absence of collective action, may be an outcome that no one favours. In addition, the failure of the government to identify Internet-related areas that should not be subject to regulation leaves open opportunities for State, local, or international bodies to regulate excessively and/or inconsistently.

6 How government should act

The novel aspects of the Internet require government policies that are sensitive to both the challenges and the opportunities of cyberspace. Three principles should guide such government decision-making:

7 Scalability, not just stability

Rather than seeking to restrain the growth of the Internet, government should encourage it. As long as the underpinnings of the network support further expansion, and self-correcting mechanisms can operate freely, the Internet should be able to overcome obstacles to further development. Additional capital and innovation will be drawn to any challenge due to the prospect of high returns. In addition, a focus on scalability directs the attention of policy makers to the future of the network, rather than its current configuration. Given the rapid rate at which the Internet is changing, such a forward-looking perspective is essential. The "growth" of the Internet means more than an increase in the number of users. It also means that the network will evolve and change, becoming an ever more ubiquitous part of society.

Nevertheless, stability remains important. The Internet must achieve a sufficient level of reliability to gain the trust of consumers and businesses. However, even such stability requires an architecture that is built to scale upward. Otherwise, periods of calm will inevitably be followed by crashes as the Internet continues to grow.

8 Swim with the current

The economic and technological pressures that drive the growth of the Internet should not be obstacles for government. Rather, government should identify ways to use those pressures to support the goals that government hopes to achieve. In telecommunications, this means using the pricing signals of the market to create incentives for efficiency. In a competitive market, prices are based on costs, and the firm that can provide a service for the lowest cost is likely to succeed. Such competitive pressures operate far more effectively with lower administrative costs than direct government mandates.

Similarly, government should look for mechanisms that use the Internet itself to rectify problems and create opportunities for future growth. For example, new access technologies may reduce network congestion, as long as companies have proper incentives to deploy those technologies. Filtering systems may address concerns about inappropriate content.

Competition from Internet services may pressure monopolies or outdated regulatory structures. Government agencies should also use the Internet themselves to receive and disseminate information to the public.

9 The Network, not networks

The Internet is a network. The government's goal should not be to foster the development of any particular network individually, but to maximize the public benefits that flow from the Network that encompasses all of those networks and many more. With the growth of competition and the elimination of traditional regulatory, technological and economic boundaries, networks are more likely than ever to be interdependent, and a policy that benefits one network may have a detrimental effect on others. For example, a mandate that Internet service providers be entitled to connect to the telephone network free of charge might stimulate Internet use, but telephone companies might be forced to increase their rates or offer lower quality service to recover the increased cost of supporting such connections.

Although government should support the growth of the Internet, this support need not involve explicit subsidies that are not independently justified as a matter of public policy and economics. Instead, government should create a truly level playing field, where competition is maximized and regulation minimized.

Attachment 2

Contribution by France

Table of contents

Contribution by France

Response to questionnaire on national Internet policies

Please note that the sections in this contribution follow the numbering of the original questionnaire. No reply is given to some sections of the original questionnaire.

Contacts:

– **ITU-T interface:** Marie-Thérèse Alajouanine
Tel: 01 40 47 71 24
Fax: 01 40 47 71 92
E-mail: marie-therese.alajouanine@art-telecom.fr

– **Content of the contribution:** Hélène Lebedeff
Tel: 01 53 44 90 48
Fax: 01 53 44 90 02
E-mail: helene.lebedeff@industrie.gouv.fr

I General policy factors

1 For IP-based networks, what is your current policy regime?

The regulations relating to network infrastructure are technologically neutral about the kind of traffic circulating on the networks. The establishment and operation of public networks is open to competition and was governed by a system of individual licences until 25 July 2003. The technology used on the networks (whether IP or non-IP) therefore does not affect the regulatory status under which the networks are established or operated. A new regulatory framework, the result of the incorporation of the directives on electronic communications, should be adopted in 2004, replacing the system of individual licences with a system of prior declaration. Among the transitional measures adopted within the spirit of the new framework is an arrangement for prior declarations that was established on 25 July 2003.

2 Are you planning any changes in your policy regime?

No. The only change will consist in the confirmation of the new system of prior declaration for the establishment and operation of networks, replacing the system of individual licences, following the adoption of the new regulatory framework by Parliament in 2004. The new framework also reinforces the concept of technological neutrality. There is, therefore, no specific policy for the establishment or operation of IP networks in particular.

3 For IP-based applications and services, what is your current policy regime?

IP services are provided on a competitive basis. The regulatory description disregards whether the technology used to provide these service is IP or non-IP. The provision of public telephone services is subject to prior declaration (it was subject to individual licensing before 25 July 2003). The other kinds of service are freely provided.

In practice, IP telephony, which is similar to a public telephone service (but different from Internet telephony) is subject to prior declaration. IP services other than telephony are freely provided.

The tariffs of an incumbent operator in respect of services for which it still has a monopoly must be approved by the minister in charge of telecommunications acting on the advice of the regulatory authority.

4 Are you planning any changes in your policy regime?

No. The new regulatory framework drawn up pursuant to the directives on electronic communications does not change the policy on the regulation of IP services. The procedure for approving the tariffs for the services of an incumbent operator in respect of which it still has a monopoly will be simplified in the new regulatory framework.

5 Regarding IP-based networks, do you have policies with respect to:

– Infrastructure for Internet access

To start, when **the telecommunication sector was opened to competition** on 1 January 1998, several networks were established that provided alternatives to the incumbent operator for the provision of services such as Internet access.

Since then, the aim of government policy has been to improve conditions of access to the Internet in order to enable as many people as possible to have such access in the best possible conditions.

The first step taken was to allow effective competition on the access segment, namely the local loop, since competition is the best spur for diversification, a wider range of offers and lower prices.

The diversification of access modes (radio local loop, cable networks) was thus promoted, while at the same time a strong incentive was furnished for opening up to competition the privileged access route that France Telecom's network represents (interconnection for low bit-rate access, unbundling and France Telecom's various options for DSL).

In addition to introducing competition, government policy helped define the conditions for the deployment of infrastructure for new uses (mobile Internet).

This was supplemented by government measures aimed at the broadest possible deployment of high-speed systems; in particular, local communities were advised on how to facilitate the deployment of operators' networks and services, usually by making infrastructure available.

Public policy first considered the **deployment and provision of telecommunication services**, including Internet access, on infrastructure that provided an alternative to that of the incumbent operator:

a) **Cable network infrastructure**: Internet access via cable networks became possible in 1997. Cable Internet access plays a crucial role in allowing competition in high-speed systems for the home. Although it is available in France in only a limited number of areas, it is for the time being the only infrastructure competing with ADSL for the attention of the general public.

The new regulatory framework will introduce a great deal of flexibility in respect of cable networks, and this should make it easier for the operators of those networks to provide Internet access.

b) The **radio local loop (RLL)**, which benefited from public policies in 2000, constitutes an attractive form of Internet access for businesses. It also complements wireline technologies, which are not always suitable for reaching certain areas. Operators holding RLL licences were selected in 2000 on the basis of coverage and land-use planning, and of a series of pledges concerning above all the coverage of people and urban areas. While certain operators appear to be facing difficulties owing to changes in the overall financial context, RLL technology remains a key to infrastructure-based competition.

c) **Interconnection and unbundling** allow other/third operators to receive traffic from telephone subscribers (interconnection), and even to secure complete control of the line connecting the subscriber (unbundling of the copper pair).

Public policy on the infrastructure for low bit-rate Internet access aims to allow the emergence of competition both between transport (or collection) operators and between Internet access providers.

Competition between transport operators is especially important in that it enables competing access providers to develop without having necessarily to rely on one single transport operator (the incumbent operator). This approach is in keeping with the direction thus far taken in opening the telecommunication sector to competition in France: infrastructure-based competition in order to ensure competition between service providers in the long term.

Interconnection

The emergence of competition in respect of switched **Internet traffic collection** was characterized and promoted by several decisions:

– In late 1997, in order to meet a market need to differentiate traffic towards the servers of Internet access providers (IAPs) and thus enable the introduction of specific tariff options for Internet communications and differentiated routing in the telecommunication networks, number series that took the form 0860 PQ MCDU and that had been allocated to Internet access services were set aside for switched Internet access.

At the same time, the introduction of an indirect interconnection model between France Telecom and the alternative operators, enabling the latter to propose collection offers to the IAP, was encouraged.

Pursuant to these decisions, flat rates for Internet access including a number of hours of communication became increasingly common in 2000 and 2001, at ever lower rates.

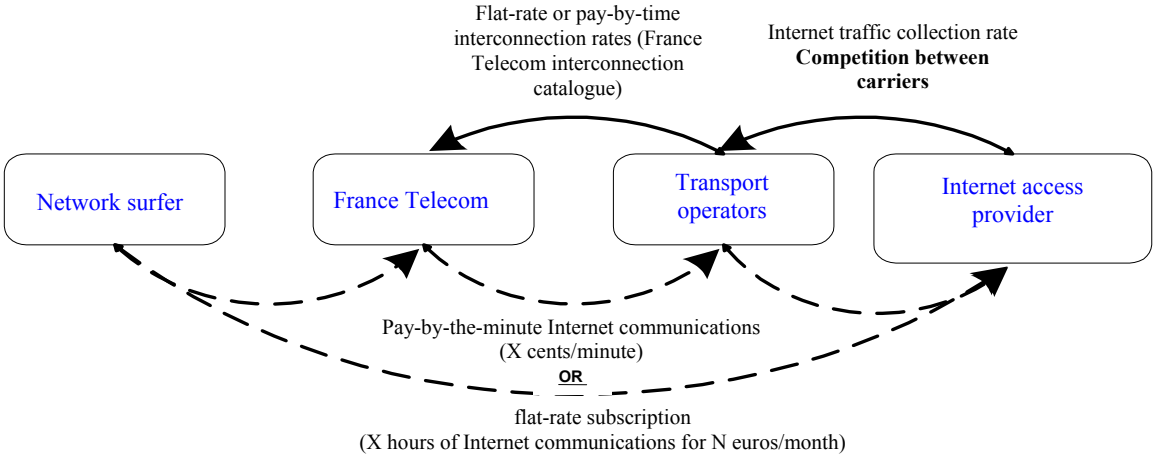
– Following a discussion moderated by the regulatory authority in late 2000/early 2001, France Telecom launched a flat-rate interconnection offer that took effect in September 2001 and was listed in France Telecom's 2002 interconnection catalogue.

The classic "pay-by-time" interconnection can be broken down into fixed fees for the use of a number of interconnection circuits,[1] connection establishment fees and per-minute fees. The flat-rate Internet interconnection (FRII) consists in having the interconnection paid for by a flat rate: a set sum for a specific number of interconnection circuits, no matter how the operators fill those circuits.

As of 2001, the FRII led to a fall of up to 30% in the price charged by access providers for the collection of switched Internet traffic. Several IAPs marketed long-term flat rates at low prices (50 hours per month for 15 euros), and the first so-called "unlimited" flat rates were launched during the summer of 2002.

[1] Per 30-circuit segment: 1 digital primary block: 2 Mbit/s or 30 64-kbit/s circuits.

Diagram of indirect interconnection used to put together flat-rate (X hours of Internet communication for N euros per month) or subscription-free (pay-by-the-minute Internet communications) offers for Internet access



"Indirect" interconnection

This type of relationship between the transport operators and France Telecom is based on the principle whereby the transport operator buys an interconnection service from France Telecom: the collection of Internet traffic on its local loop. This method is said to be one of "indirect" interconnection, as opposed to "direct" interconnection, in which France Telecom purchases an interconnection service from the collection operator: the service consists in terminating calls to the Internet access provider's point of presence. In indirect interconnection:

– the IAP pays the operator a fee for the collection and delivery to a national point of its subscribers' Internet traffic;

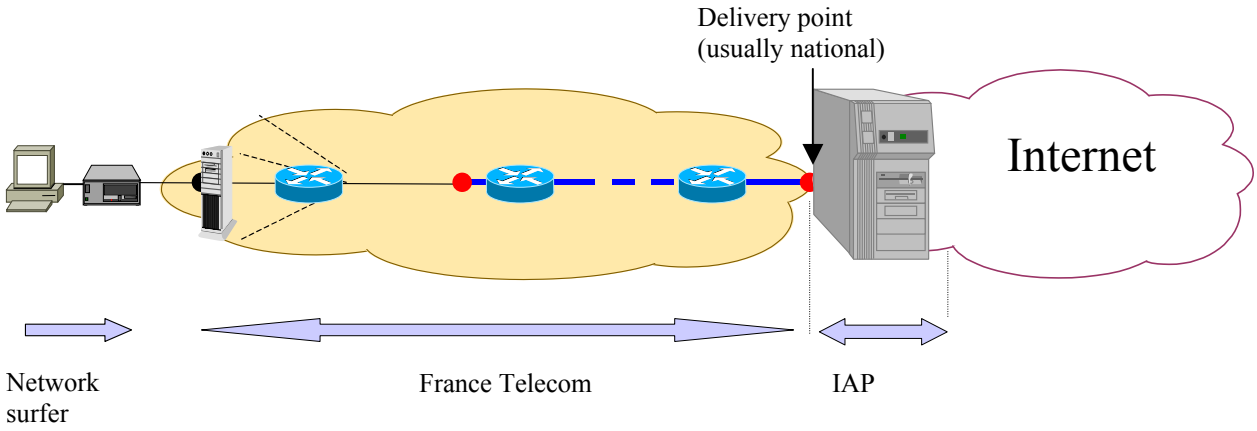
– the operator pays France Telecom an interconnection fee for the collection on France Telecom's local loop of the IAP subscribers' Internet traffic;

– the subscriber pays either a flat rate (X euros for N hours of connection per month) direct to the IAP, or makes payment for his or her Internet communications to France Telecom, which in turn pays the corresponding amounts to the IAP via the operator.

As regards high bit-rate ADSL access, IAPs have three options when it comes to putting together offers for ADSL Internet access:

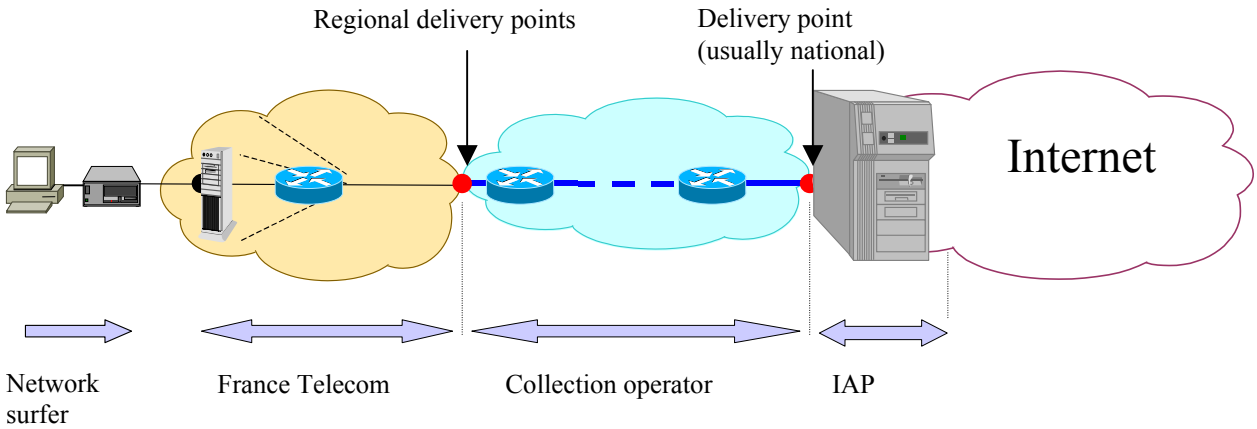
(Option 5) The ADSL subscriber's traffic is delivered direct to the IAP at its server centre by France Telecom. In this case, the IAP is totally dependent on France Telecom for access and all collection.

Access and collection of DSL traffic by France Telecom (option 5)



(Option 3) The operators purchase a service from France Telecom whereby France Telecom collects DSL traffic on its local loop and sells to the IAP a global ADSL access and collection service. The ADSL subscriber's traffic is delivered by France Telecom at the regional level (40 delivery points) to a transport operator. The transport operator then extends the collection to the server centres of its IAP customers. In this case, the IAP is independent of France Telecom for part of the collection, enabling it to afford the customer a wider range of tariffs and service quality (subscriber bandwidth).

Carriage of DSL traffic by a third operator (option 3)

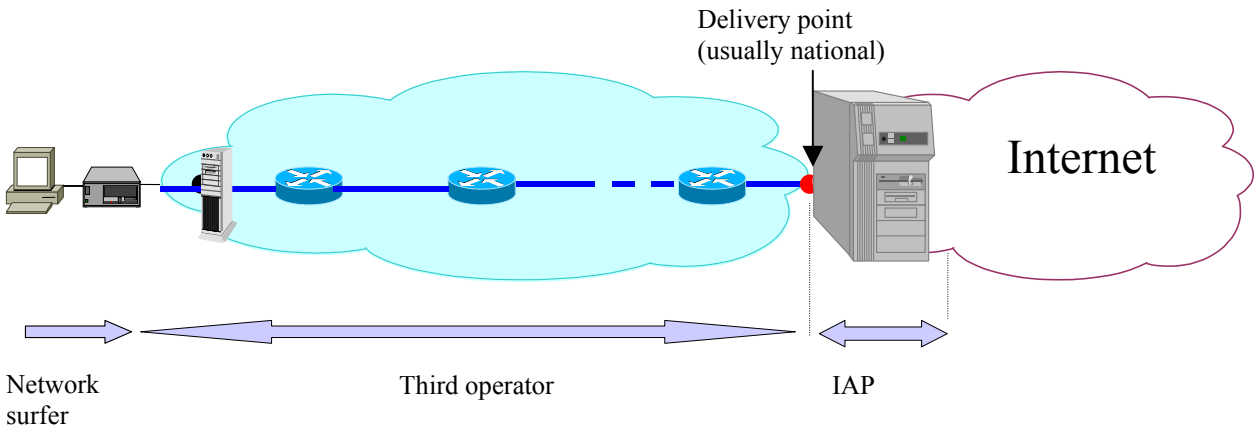


(Option 1) France Telecom makes available to operators its network's local loop, using one of two modes: totally unbundled access, which consists in making available the naked copper pair and enables operators to provide all types of service; and partially unbundled access, which consists in making available copper pair high frequencies with a view to providing Internet services.

For the competing operators, unbundling means that they deploy their infrastructure and install their technical equipment within France Telecom's distribution frames. Given the number of sites required to cover the territory of France (12 000 frames in all), unbundling will concern, at least in the short term, the most densely-populated areas, it being possible to cover the rest of the territory by means of the preceding approach (option 3).

The financial and operational conditions for unbundling that prevailed in 2001 did not really allow the method to take off. In addition, the changes in the tariff offer imposed by decision of the regulatory authority in April 2002 are too recent to have had an impact on the number of unbundled lines, which stood at 756 in July 2002.

Access and collection of DSL traffic by a third operator
(option 1 - unbundling of the local loop)



Unbundling

For unbundling, a decree adopted in September 2000 served to specify the conditions of access for alternative operators to the local loop. The incumbent operator must provide an objective and non-discriminatory response to reasonable requests for access to the local loop, insofar as the metallic part of its network between the main distribution frame and the termination point situated at the subscriber's premises is concerned. Several alternative operators have thus been able to set up alternative DSL networks affording high-speed Internet access.

State policy has enabled France Telecom to publish a benchmark offer that is satisfactory from the tariff and operational points of view.

The State's policies have sought to give genuine impetus to the unbundling process over large swathes of the country, and have paved the way for its expansion to residential customers.

In addition, those policies have sought to establish a general competitive balance between the players, in particular vis-à-vis France Telecom on the ADSL market for the general public. That balance must be struck between the IAPs and among operators.

- IAPs must be able to propose ADSL subscriptions that compete with Wanadoo in economically viable conditions of fair competition.
- Operators must be able to propose to IAPs, either via option 1 (unbundling) or via option 3 (France Telecom collection of DSL traffic on its local loop), offers to collect ADSL traffic to the IAPs that are competitive with those proposed by France Telecom (option 5).

These measures have led the incumbent operator to make offers that significantly improve the situation of IAPs on the ADSL market, as well as that of operators wishing to take part in that market by putting forward alternative offers to those of France Telecom.

As regards the infrastructure for Internet access via radio networks, the conditions for using the frequency bands in which those networks operate have been completely liberalized for the use of terminals on existing networks. In the new regulatory framework, the establishment of public networks using this kind of technology is subject to prior declaration.

- **Competitive environment for telecommunication networks**

The priority policy objective when it comes to the competitive environment for the provision of IP services is to create a situation of normal, full and complete competition on the retail market, i.e. fair and healthy competition between high-speed Internet access providers, for the benefit of consumers.

If the incumbent operator's competitors are to win and hold on to shares of the market, they must have access to a competitive wholesale market, which means that the operators competing with France Telecom must be able to provide high-speed access services that are increasingly based on unbundling, with a competitive wholesale offer.

Policies in this area are based on an approach that aims to secure competition on the retail market using competition on the wholesale market as a springboard. This approach is in line with that set forth in new European Union texts, which stipulate that efforts to influence retail markets are necessary, use must first and foremost be made of levers affecting wholesale markets.

See also the previous paragraph.

- **Portability issues**

Portability concerns only fixed or mobile public telephony and is not specific to IP services.

- **Interconnection for telecommunication networks**

When it comes to interconnection for telecommunication networks, the goal of State policy is to allow the emergence both of competition between transport operators (or collection operators) and of competition between Internet access providers.

An interconnection model for Internet access was encouraged by State policies, giving added momentum to competition between transport operators for the collection of low-speed Internet traffic. The policies also encouraged the implementation of a flat-rate interconnection offer for the Internet that considerably reduced the cost of collecting switched Internet traffic, to the benefit of the end customer.

See the paragraph on Internet access infrastructure.

- **Universal access to telecommunication networks**

Switched Internet communications now help to finance the universal telecommunication service in the form of a fee paid by the collection operator for each Internet minute carried. A change in the legislation will make the amount of the contribution to the universal service proportional to the turnover of access providers, on the grounds that a fee that is paid per minute collected considerably increases the collection costs for Internet traffic.

- **Privacy**

On an open network, privacy is essential. This holds true both for individuals, who are concerned to protect their private lives and keep their correspondence secret, and for businesses, a growing number of which are using virtual private networks - intranets linked via the Internet - to enhance their effectiveness and competitiveness.

Under the State's policy, a major endeavour has been launched to liberalize the use of cryptology, so as to enable everyone to communicate confidentially over the networks. However, that liberalization goes hand-in-hand with the introduction of measures aimed at fighting the use of cryptology for criminal purposes. Such measures are required to make sure that illicit practices do not undermine confidence, which would hamper the growth and development of the digital economy.

Thus it is that the provisions of the draft law on confidence in the digital economy introduce complete freedom to use the means and services of cryptology. They establish a new system for the import, provision and export of means of cryptology. They limit the obligations to be met by the providers of such products, while at the same time rendering them responsible. Lastly, they strengthen the means available to the public authorities to fight against the use of cryptology for unlawful purposes.

- **Security**

Generally speaking, State policy seeks to promote the use of all security services. For example, it has recognized the legal validity of electronic signatures, which should serve to accelerate the development of commercial transactions. The incorporation into French law of the European Directive on electronic signature is now complete, particularly with the adoption of Act 2000-230 of 13 March 2000 on the adaptation of the law of evidence to information technologies and Decree 2001-272 of 30 March 2001 establishing reliability criteria for electronic signatures.

These legislative measures are accompanied by monitoring activities and by measures to heighten the awareness of businesses and administrations regarding the security of information systems, such as the security of WiFI.

The establishment of CERTs (for example, CERT-A, for the exclusive use of the Administration) also stems from the concern for protection. The CERTs (Computer Emergency Response Teams) are units that detect and react to disturbances or attacks on computer network systems. Their role is to provide technical and organizational elements that will allow for the prevention of and response to network disturbances or attacks. The first CERT was set up after the first large-scale incident on the Arpanet network, the precursor to the present Internet, in 1998.

There are at present several CERTs in France:

– CERT-A, for the exclusive use of the Administration, to strengthen and coordinate activities designed to protect the State's networks from attack;

– CERT-IST is dedicated to industry, services and tertiary activities. It was set up in January 1999 in partnership with Alcatel, CNES, France Telecom and Total, and serves to coordinate protection and the resolution of incidents in the sector. Services are provided by Alcatel CIT's security department. CERT-IST will become an association under Act 1901 in 2002;

– CERT-Rénater provides services similar to those of the above CERTs for the academic and research community.

Lastly, it must be recalled that the Internet is made up of an interconnection of networks operated for the most part by private operators. The latter are therefore directly concerned by network security problems.

Operators' licences contain provisions relating to public security

In France, a standard clause in the specifications appended to licences granted to operators refers to defence and public security requirements.

Article D.98-1 of the Code of Posts and Telecommunications stipulates that L33.1 and L34.1 operators have a number of obligations in respect of secure communications:

– the operators must take all requisite measures to ensure that communications over their networks are secure;

– the regulatory authority can require information to be provided to it on the measures taken to render the network secure and can, as necessary, issue technical instructions pertaining to security.

Data preservation: identification and technical characteristics of connections

The law contains provisions relating to the preservation of data on communications by operators. Those provisions stipulate that operators shall erase all data relating to communications except certain data that they keep for a maximum period of one year.

7 Regarding IP-based services and applications, do you have policies with respect to:

– Competitive environment for telecommunication services

See § 5.

– Portability issues

Policies on portability are not related to IP services.

– Universal access for telecommunication networks

See § 5.

– Privacy

See § 5.

– **Security**

See § 5.

– **Content restrictions**

– **Online dispute resolution**

9 Would you describe your present policies as new tools with respect to technology?

Yes. First, the new regulatory framework notes that networks can now carry all manner of content and services; it therefore harmonizes the legal regimes governing telecommunication networks and the audiovisual sector, grouping them under the heading "electronic communication networks". In addition, the new framework reinforces the concept of technological neutrality, which was already present in the previous framework. Thus, electronic services and communication networks will be subject to the same regulatory framework and the same economic rules, no matter what technology is used to operate or provide them.

10 Please indicate which of the following you use to encourage deployment of new technologies:

– **subsidies**

– **tax incentives**

– **training**

– **funding for research and development**

II Use of Internet applications and services

11 Please indicate in which area the Internet is being used

– **e-learning**

– **e-government**

– **e-health**

– **e-commerce**

– **personal and business communication**

– **messages (authenticated and unauthenticated e-mail)**

– **inter- and intra-business management (ERP, etc.)**

– **technical inter-and intra-business management (external hosting, telemaintenance, telesurveillance, telemanagement, etc.)**

– **e-agriculture**

– **IP telephony**

– **other**

III Specific policy areas

12 Do you have policies with respect to:

– e-commerce

The certification and authentication policy is being developed (aim: to set up a viable economic model with "reliable" solutions). Promote the development of micro-payments by grouping credit cards (a simplified authentication system for the payment of modest sums without exposing the credit card to security risks).

– IP telephony

The regulations do not differentiate between IP telephony and traditional telephony using switched circuits. There is no specific national policy in this field.

– ENUM

A public consultation was held in the summer of 2001 on the significance of this protocol, in particular as concerns management of the numbering plan and implementation of the domain name system corresponding to the French plan. A multilateral working group meeting under the auspices of the Ministry of Industry and the telecommunication regulatory authority pursued the debate and contributed to the deliberations of standardization bodies on ENUM (ITU-T and ETSI in particular). A pilot project entitled "NUMEROBIS" was accredited by the Ministry of Industry in 2002 and was launched in the spring of 2003 using funds for the financing of telecommunication research projects. The project will run for 19 months and will result in an organization to conduct experiments in conditions approximating reality as closely as possible. It aims to enhance skills relating to the protocol, test the delegated model being considered for implementation in France and deploy a platform among several actors. By helping to identify and resolve problems pertaining to the functioning of such a platform, the project should promote the emergence of ENUM-based services.

– Backbone traffic topology and Internet traffic exchange

No. There is no specific national policy concerning Internet traffic exchange. Such exchanges are carried out freely on public or private exchange nodes. There does not seem to be a need for regulation in this sector, which is self-regulating without any particular problems arising.

– IP address allocation

No. There is no specific national policy concerning IP address allocation. On the other hand, the work of the regional bodies managing IP addresses is regularly monitored. In addition, the Government encourages initiatives to develop and use IPv6 addressing, in particular by providing support to the national working group established to work on the matter.

– Country code top-level domain names (ccTLDs)

In France, the terms and conditions under which ".fr" is managed were defined in accordance with certain principles:

– the domain name system (DNS) is a public resource which must be managed in the general interest;

– the manager of a ccTLD must have the backing of the local Internet community and the Government or the competent public authorities;

– the Internet users must have confidence in the name space.

The management rules in respect of ".fr" have been defined by the French Association for Cooperative Internet Naming (AFNIC) and incorporated into the statutes and name charter of AFNIC, whose decisions are binding on all ".fr" users. The management of ".fr" fosters confidence among Internet users, by ensuring that the holders of domain names are properly identified and by making it a general obligation to prove a right of intellectual property over the names registered.

– **Internationalized domain names (IDNs)**

AFNIC is in charge of defining the conditions for the application in France of the framework established by ICANN for internationalized domain names. The corresponding studies have not yet been completed.

The provisions governing IDNs appear complicated at first glance. However, they do not respond to the problems posed by writing or distinguishing domain names in standard writing (use of accents and diacritic characters) that are regularly mentioned by certain users.

– **Other**

13 If you do not have policies in the above areas, are you planning to create any policies?

– **IP addresses**

The draft law on confidence in the digital economy that was adopted by the Senate in June 2003, and which will be examined in second reading when the National Assembly reconvenes, establishes a legal framework for the management of France's top level country codes. It consolidates the legal framework for the management of national domains corresponding to the territory of metropolitan France, the overseas departments and certain overseas territories. The aim is to give the minister in charge of telecommunications authority to designate, following consultation with the users and professionals concerned, the entity or entities to be in charge of managing those top level domains and of guaranteeing that they are managed in the general interest; transparent management rules, respect for intellectual property rights and the possibility of a change in service provider should the register fail (bankruptcy or failure to meet obligations) are among the points explicitly taken into account by the draft law.

Attachment 3

Contribution by Estonia

Table of contents

Contribution by Estonia

Information technology outlook 2003

ESTONIA

Prepared for the OECD Committee for Information Computer and Communication Policy (ICCP), June 2003

This material describes policies, overall strategies and main results related to information technology/information infrastructure/the information or Internet economy/information society and the like, undertaken by different public actors and co-ordination mechanisms in Estonia.

It aims to provide information on:

- the main focus of ICT policies
- shifts in country policies and priorities
- developments in selected areas

leading to the results described below.

PART 1: POLICY ENVIRONMENT

1.1 Cornerstones of Estonian information policy

1.1.1 The main policy focus areas

A common integral ICT environment enabling mutual information exchange has been developed in the Estonian public administration and public sector thanks to numerous measures and activities that have been applied for the coordination of IT developments through the years. The elaboration of State information policy principles that were approved by *Riigikogu* (Parliament) in May 1998 became one such cornerstone paving the way for establishing a framework for building the information society and defining national priorities for realizing this framework.

Similar to the concept of establishing an information society as approved by the European Union, the preparation of the Estonian information policy framework focused on the following four fields:

- modernization of legislation
- assistance in developing the private sector
- development of communication between the State and the citizen
- acknowledgement of problems related to the information society

The general goal of the information policy actions of the Government of Estonia is to help to create a society and State that serves citizens, promotes their participation and cares for their well-being. For that purpose the Government proposes the development of information policy that:

- promotes and ensures democracy in the Republic of Estonia;
- supports the development of the information infrastructure;

- supports the creation of a competitive economy, especially through demonopolization, speeding up the restitution of property, the development of electronic commerce and electronic banking;
- supports the development of Estonian culture and language, considering also the values deriving from cultural diversity;
- supports the modernization and improvement of State defence as a result of the developments in information technology.

The Government develops the information policy based on the needs of the Estonian nation and experience of other countries. One of its goals is to even up the development in Estonia with that of other States, supporting thus the integration of Estonia into the family of developed nations.

The implementation of the information policy supports the creation of a stable economic environment that, in turn, supports the creation of new forms of enterprises, and diminishes bureaucratic barriers and separation lines. The ultimate goal of the information policy is to raise the overall welfare of society.

1.1.2 New policy directions and developments

Every year the information policy framework has been developed further and the Government has defined general priorities for implementing the information policy. In 2002/2003 those priorities are:

- development of services for citizens, the business sector and public administration, especially the elaboration of ID-card applications for the list of e-government services defined in the eEurope+ Action Plan;
- improvement of skills and access of social groups in an unequal position regarding use of electronically provided services;
- elaboration and introduction of systems for digital record management and archival processing;
- development of the system and infrastructure of national and State registers, including the development of systems that ensure the maintenance of databases and the introduction of the data exchange layer (project "X-Road") of information systems;
- better provision of schools with computers to achieve the ultimate goal – one computer per 20 students;
- launching of Tiger University programme to support the development of ICT infrastructure and academic ICT staff, and the infrastructure for post-graduate training.

An important process started in 2002 was the elaboration of a new version of information policy principles. There are several reasons for elaborating a new version – mainly changes resulting from fast IT developments. These changes need to be reflected in the policy source documents passed by the Government and Parliament, and the general public also needs to be informed about tendencies in the purposeful development of Estonian information society.

Debates between different groups have proceeded for almost a year already, while the content of the document and the focuses have been specified and compromises have been reached when needed. The draft of the new version of information policy principles was completed at the end of 2002 and after approval by different parties the draft will be sent to the Government to be reviewed and approved, followed by final approval by Parliament.

The new version of information policy principles includes supplements to previous principles, according to which:

- development of the information society proceeds from the coordinated activities and cooperation of the public authorities, private sector and tertiary sector;
- the information society is created for all Estonian citizens and supports regional development and local initiatives;
- development of the information society provides the opportunity for equal access to information for all citizens;
- development of the information society ensures continuity of the Estonian language and culture;
- development of the information society must not decrease the security of citizens;
- development of the information society is related to national research and development activities;
- activities of information society development are brought out as separate elements in the State's education, culture and social policies;
- development of the information society takes into account the information society building programmes of the European Union;
- the public authority has the same attitude towards different hardware and software platforms and solves the issue of compatibility by establishing general standards.

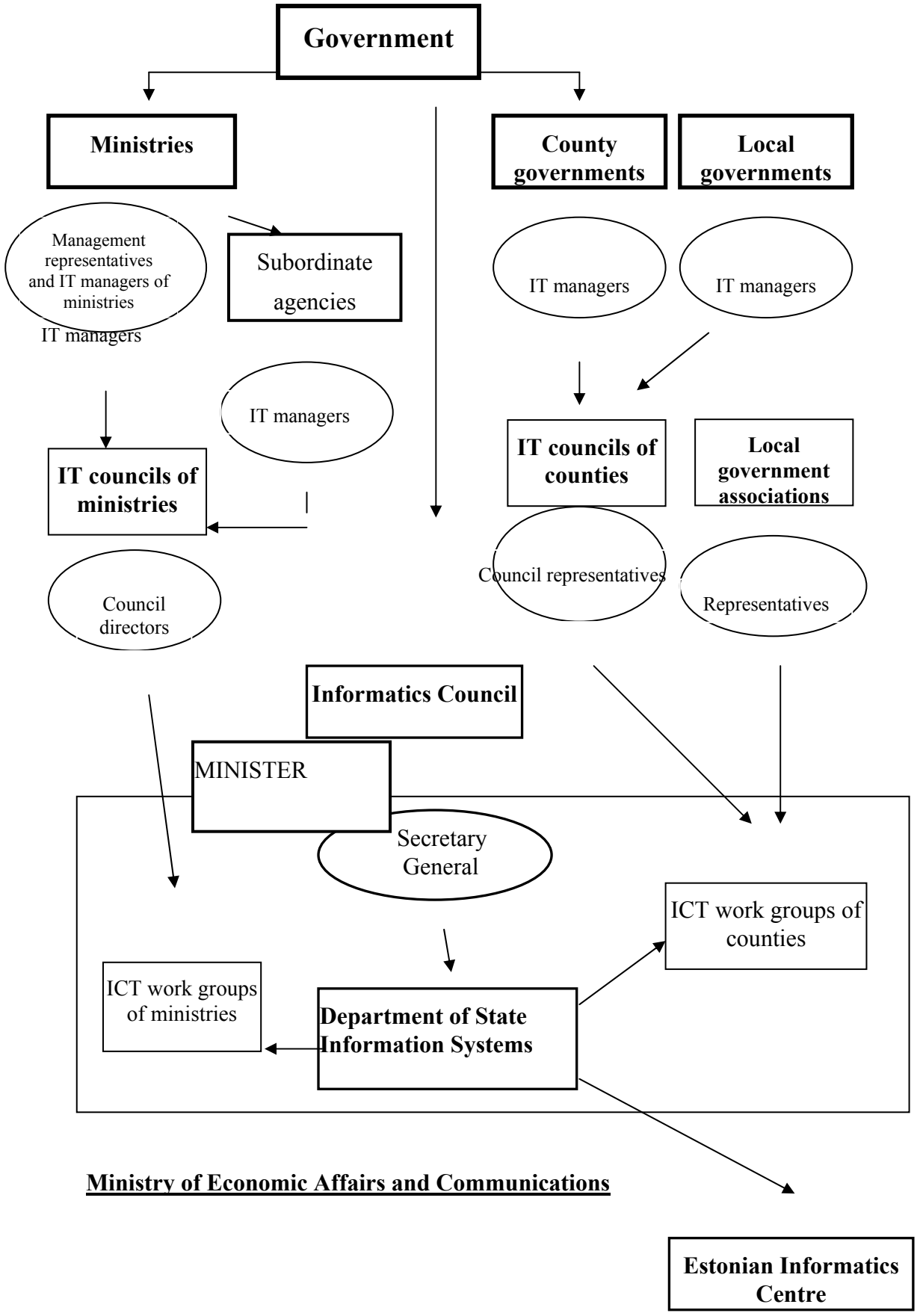
The overall goal of these tasks lies in the development and integration of the ICT infrastructures of the State and local governments into a common, citizen-friendly service environment that observes the principles and requirements of the development of democracy.

1.1.3 The institutional setting relating to ICT policy and coordination mechanisms

Organizational structures for directing ICT development in Estonia and, primarily, in public administration have developed along with the general development of ICT infrastructure and solvable problems. In 2000, the Government decided to transfer the organizational units coordinating IT development in public administration to the area of government of the Ministry of Transport and Communications. The tasks of the latter had until then been mainly confined to the management of media and telecommunication market regulation. This brought along several changes and new initiatives in 2001. The Department of State Information Systems (RISO) of the Ministry of Transport and Communications took on new staff, while several large and significant ICT development projects, described below, were transferred and placed under the organization and responsibility of this department.

The Estonian Informatics Centre was also transferred to the Ministry of Transport and Communications and the Estonian Informatics Council, a government committee of experts, was reorganized as well. The private sector has been more involved in the work of the latter as well as in the activities of several work groups.

In autumn 2002 the Ministry of Transport and Communications and the Ministry of Economic Affairs merged to become the Ministry of Economic Affairs and Communications. This merger entailed transition processes in the organization of State information systems coordination. By the end of 2002 a new organizational structure of ICT development was created – see flow chart below.


Government
Ministries
County governments
Local governments
Management representatives and IT managers of ministries
IT managers
Subordinate agencies
IT managers
IT managers
IT managers
IT councils of ministries
IT councils of counties
Local government associations
Council directors
Council representatives
Representatives
Informatics Council
MINISTER
Secretary General
ICT work groups of counties
ICT work groups of ministries
Department of State Information Systems
Ministry of Economic Affairs and Communications
Estonian Informatics Centre

Organizational structure of ICT management in Estonia

The year 2003 will probably also witness several substantive changes in the organization of ICT development – for technological, organizational and political reasons.

The influences of technological development are primarily related to the fast development of web technology, which has provided new opportunities for the integration and globalization of information systems and entailed a greater need for centralization of the development of applications. This has also created a new situation for the organization of the information systems of State agencies and for the legal framework.

There are manifestations of the integration and consolidation of ICT development and service units of State agencies. For example, on 1 November 2002 the joint IT department of the Tax Board and Customs Board was launched.

In 2002, cooperation also was enlarged between public and private sector organizations in order to implement the joint elaboration and further development of ICT infrastructure and the information society. This is manifest, for example, in the provision of opportunities for using identification systems for clients of commercial banks when entering integrated public sector databases, as well as in agreements concluded between public and private sector organizations for the joint elaboration of systems developing the information society (e.g. Look@World – a major project of public and private companies).

1.2 ICT financing – the key means of coordinating ICT development in public administration

Although at present it is very difficult to draw a clear line between expenditures on the management and functioning of State agencies and expenditures on the use and development of the ICT environment, two kinds of costs related to the application and development of information technology can be distinguished among the latter.

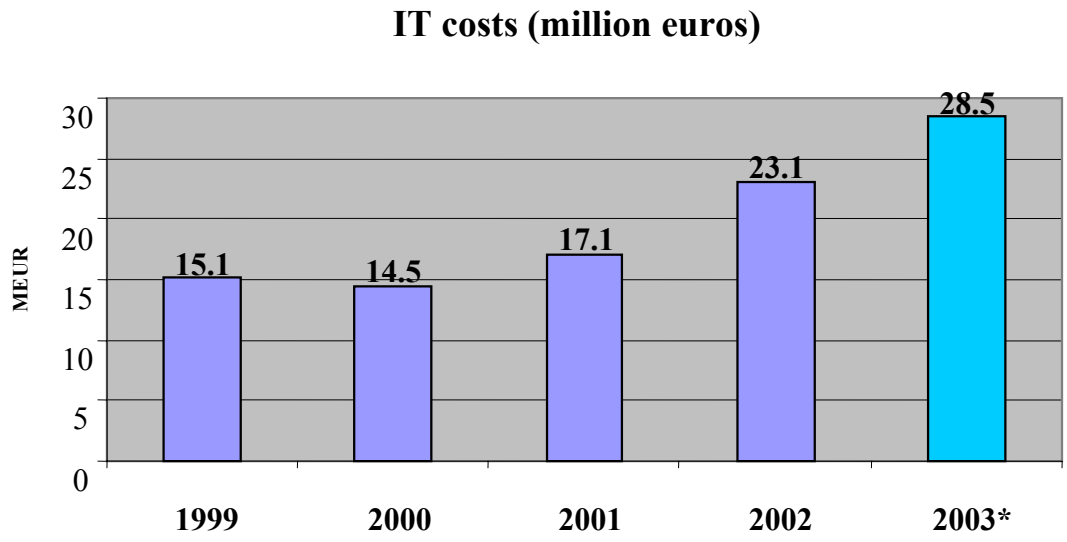
From 1994 to 2002 the Estonian State budget included a separate expenditure item "Information technology" to cover most of the investments in the purchase of hardware and software, the costs of maintenance and preservation of ICT infrastructure, and the contracting of development projects for information systems outside the public sector, i.e. the outsourcing of projects to ICT companies. Applications for financing were dealt with slightly differently compared with other expenditure items, as State agencies and State boards within their administration had to submit so-called "application projects" in order to justify IT costs. These application projects were reviewed by an expert committee. The committee, which was formed by the ministry responsible for the coordination of IT development in public administration, also had at its disposal, in addition to the applications, data on available IT tools and their use in the agencies that had submitted the applications.

This enabled the committee to evaluate the applications submitted and expected financing quite objectively, also taking into account the conformity of applications to the ICT development priorities of the information policy. The applications together with the committee's proposals were then submitted to the Ministry of Finance, where elaboration of the draft State budget was finalized prior to its submission to the Government.

Such a procedure for reviewing financing applications was especially effective during the first period of the elaboration of information technology infrastructure in public administration (1994-1999), enabling a reduction in disparities in the use of ICT in the management of different economic fields and in the development of ICT infrastructure in public administration. Since 2000 the list of expense items covered by "Information technology" in the State budget has grown.

Besides development, the main focus was also on ICT fixed costs, such as those of replacing hardware and software, maintenance of ICT infrastructure, annual software licence fees, data communication, and fixed ICT services.

The share of information technology costs has throughout years formed about 1% of overall costs in the State budget and it has increased in absolute value together with the increase in the overall figure of the State budget (see diagram below). The actual expenditures on information technology in public administration are, without doubt, larger, as the expenditure item does not include the salary costs of ICT staff, expenditures on information technology of public sector agencies which only receive grants from the State budget for developing their activities, ICT training costs, and expenditures on ICT development and use in local government budgets. As compared to many other countries, where expenditure on information technology is estimated to be 2.5-4% of the State budget, Estonia's expenditures have been quite modest.



In connection with the amendment of the State Budget Act, the expenditure item for IT costs was removed from the State budget for 2003 and 2004. Instead, these costs have now been included under "economic costs" and "obtainment and renovation of material and immaterial assets".

Because of this change it is impossible now to monitor ICT expenditures in the State budget and centrally coordinate the activities required for realization of the government policies on ICT.

PART 2: SPECIFIC POLICIES AND PROGRAMMES

2.1 Fostering ICT innovation

2.1.1 Research and development programmes

The national structure for research and development (R&D) has undergone several changes during the last decade. During the process of R&D and higher education reform, which started at the beginning of the 1990s, a mechanism for decision-making has been developed, institutional reform has been carried out, a financing system has been created, and corresponding legislation to support the functioning of the system has been drafted.

The activity of research institutions has been reorganized and internal and international evaluation of research areas has been carried out. Post-graduate education has essentially been brought into line with international criteria.

In 1994, the Organization of Research Act was adopted by the *Riigikogu* (Parliament) and in 1997, the Organization of Research and Development Act was adopted as an updated version. This law provides the bases for the new structure, organization and financing of the R&D system, as well as for state surveillance. At the beginning of 2001, the *Riigikogu* approved the Amendment Act for the aforementioned Act.

During the period 1996–1998, the majority of the former Academy of Sciences research institutes were merged with the universities. In 1990 the Estonian Research and Development Council (TAN) – the strategic advisory body to the Government in research and development issues – was founded, as well as two special-purpose foundations: the Estonian Science Foundation (ETF) and the Estonian Innovation Foundation (EIF). The Estonian Innovation Foundation has since been restructured into the Estonian Technology Agency (ESTAG), as a sub-unit of the Enterprise Development Foundation (EAS) which is under the jurisdiction of the Ministry of Economic Affairs. In 1997, the Research Competency Council (TKN) was established, and in the same year the Archimedes Foundation was founded by the Ministry of Education.

The current emphasis is on raising the effectiveness of the R&D and innovation (RD&I) system by a clearer delineation of functions between the various parts of the system, and by improving mutual cooperation. One of the most significant of such changes is the reform of TAN, initiated in 2000 and completed by autumn 2001, as well as the launching of ESTAG under the competence of the Ministry of Economic Affairs. An effective organizing structure for RD&I is a precondition for an increase in State budget allocations, and their efficient use by the Estonian RD&I system.

The lack of public consensus regarding long-term RD&I development, and the general low financing of this field from the State budget, have emphasized the need for an R&D (including financing) strategy. A diversification of the currently insufficient supporting instruments for technological development and innovation is necessary, in order to be able to cover the entire process – from initial concept to finished product.

The current[1] situation in R&D is characterized by the following indicators: the volume and structure of R&D, human capital, the number of patent applications, and success in international cooperation. The indicators for R&D volume and structure are the funds invested into the sector and their distribution between basic research, applied research, and development, as well as the distribution of investment between the public and private sectors. The indicator for human capital is the share of researchers and engineers within the labour force.

In Estonia, total expenditure during the period 1995-1998 on R&D remained at 0.6% of GDP. In 1999, this increased to 0.76%. Using international comparisons, it can be seen that this indicator is very low, constituting only 40% of the average for EU member states (1.9% of GDP in 2000), and being at the same level as Portugal (0.6% of GDP, 1998).

---

[1] Knowledge-based Estonia; Estonian Research and Development Strategy 2002-2006, Tallinn, 2002.

The actual increase in total expenditure for Estonian R&D has remained modest, at an average of 4.3% annually (according to 1995 fixed prices). Comparing the sources for financing R&D, the main R&D investor in Estonia for the entire period under observation has been the public sector. In 1999, the share of the public sector in total expenditure on R&D in Estonia was 76%, while the corresponding average for EU member states was 34% (2000).

However, public sector expenditure (0.57% of GDP in 1999) on R&D in Estonia is still lower than the EU member state average (0.65% of GDP in 2000). On average, 90% of State budget R&D funds have been allocated during the period under observation to research only, whereas State support for development and stimulation of innovation has been limited.

One of the indicators for the innovative capacity of enterprises, and the basis for assessing long-term competitiveness, is the expenditure by enterprises on R&D. The development intensity of Estonian enterprises is low – expenditure by enterprises on R&D was only 0.19% of GDP in 1999 (1.25% of GDP in the EU, 2000), and 24% of the total expenditure on R&D.

The motivation for existing highly qualified researchers and engineers to apply their knowledge in business is low, and there is also a lack of State measures to stimulate interest. Cooperation between researchers and enterprises is not sufficiently intensive. In 1998, only 0.66 researchers and engineers per 1000 workers were employed in Estonian enterprises. In 1999, this ratio decreased to 0.54. The corresponding EU indicator is 2.5 (1997).

There is considerable scientific potential in Estonia, witnessed by the numerous publications in the international specialized press, and active international cooperation: 54.6% of the articles published in international journals by Estonian authors are a result of international cooperation.

Estonia has successfully participated in the EU R&D framework programmes. According to the preliminary results (as of 1 July 2001) of the open project competition for the EU R&D 5th Framework Programme in 1999, 425 project applications were made with Estonian participation, and of these, 24.2% were successful. Such a rate of success is comparable to the EU member state average. As to other international RD&I cooperation and information networks, Estonia is a full member of COST, EUREKA and GEANT, and belongs to the Innovation Relay Centre (IRC) network.

State financing of R&D, with its focus on research, has ensured a high level of basic research in some specialities, but the link between the creation of new knowledge and the consequent development of new technologies has remained weak. The transfer of ideas and knowledge created by research into competitive products and services on the market requires more than the current level of attention and effort by the State.

2.1.1.1 Key areas

No small nation can manage to be successful in all areas of RD&I or to solve all RD&I problems simultaneously. The chosen strategy[2], therefore, will define the key areas and foresee an increase in the share of State resources (both human and material) allocated to these areas.

Estonia's key RD&I areas have been defined taking into account specific opportunities for development in Estonia, the existing research potential, the existing economic structure and international orientations in the field of RD&I.

---

[2] Knowledge-based Estonia; Estonian Research and Development Strategy 2002-2006, Tallinn, 2002.

In the implementation of planned objectives and visions for the future, the key areas are the following:

- user-friendly information technologies and development of the information society;
- biomedicine;
- materials technologies.

In parallel with the development of these key areas, the following will also be ensured:

- the continuity and promotion of research related to the Estonian people, language, national culture and history;
- the continuity and promotion of research related to Estonian statehood and the sustainable development of society, as well as ensuring national security;
- the continuity and promotion of research related to the everyday environment and protection of nature, the sustainable use of natural resources, and the development of rural areas.

In order to identify more precisely the best opportunities for Estonia in key areas, studies will be undertaken continuously to analyse existing preconditions and the cost-effectiveness of results.

The Ministry of Economic Affairs and Communications and the Ministry of Science and Education, in cooperation with R&D institutions and business representatives, will compile and launch national programmes for the development of key areas.

Bringing the key areas into line with the European Union's RD&I priorities will encourage active participation by Estonian researchers and enterprises in international RD&I cooperation and will enable us to obtain additional financing for the achievement of national priorities.

In developing high technology industry in key areas, attention will be paid to strengthening the cooperation between traditional industry and the so-called new economy, as well as to the technological updating of traditional industrial branches in Estonia. The application of the innovations created in the information, biomedical and materials technologies sectors will be encouraged in traditional industries.

In order to achieve technological renewal in the economy and the growth of added value, the capacity of traditional industrial branches to apply modern technologies should be increased. As a result of this adaptation, added value will grow, and the knowledge and skills that allow consequent independent development activity will be increased.

In supporting technological transfer, attention should be paid to the involvement of foreign investment, which is the main channel for international technology transfer.

2.1.1.2 eVikings

Concerning R&D programmes fostering ICT innovation, the Estonian *e*Vikings project (IST-2000-26453) should be mentioned. This project aimed to better integrate Estonian leading information society technologies (IST) research and development labs and companies through everyday collaborative research and technological development (RTD) projects with European academia and industry and innovation networks.

The pilot phase of the project, supported by the European Commission, started with the building up of the Virtual Centre of Excellence for IST RTD by strengthening the existing innovation infrastructure. It aimed to open additional synergies and enable the main objective of the project – European integration in IST RTD – to be benefited from in a cost-effective way.

The Estonian *e*Vikings project concentrated during the pilot phase on:

- strengthening the links between the Estonian and European IST R&D communities, starting from the closest neighbours around the Baltic Sea, but with focus maintained on Europe as a whole;
- supporting the efforts of the Estonian R&D labs to become modern by assisting with the introduction of new European cooperative R&D projects (either European framework, bi- or multilateral);
- special attention was paid to updating and giving advice in order to improve the focus of the national research and technology policies.

This project pilot phase included evaluation of the Estonian IT cluster and compilation of a technology foresight review for Estonia. This was followed by consensus-based independent national IT R&D policy recommendations prepared for the national authorities and a research agenda established for the Virtual Centre of Excellence.

The Estonian *e*Vikings project supports the above-mentioned goals on IST by strengthening local, regional and European RTD cooperation on IST by establishing a Virtual Centre of Excellence for IST RTD. While uniformly high quality of research must be the leading criterion, a well-designed virtual centre will lead to excellence in different fields, creating a truly synergistic effect. Therefore, a multidisciplinary research agenda ought to be an essential characteristic of such a centre.

The work plan of the Estonian *e*Vikings project (January 2001 – March 2002) included a major package of awareness, training and policy planning activities for the successful establishment of new RTD projects and exploitation of international markets. All this basically ensures the European dimension throughout the life cycle of national RTD policy and R&D project planning.

*e*Vikings II is a follow-up project to the Estonian *e*Vikings project. eVikings II is an FP5 IST programme accompanying measures project (IST-2001-37592, November 2002 – April 2005). The project aims at:

- strengthening existing IT-related science and technology in Estonia
- energizing Estonia's innovation system by enhancing its ability to anticipate future development and manage the related innovation processes.

The coordinating institution of eVikings II is the Institute of Cybernetics of the Tallinn Technical University.

2.1.2 Government ICT development projects and target programmes

The Estonian Information Policy Framework contains priority projects the outcomes of which create new services focused on citizens and entrepreneurs, as well as projects aimed at integrating IT solutions, which have so far functioned autonomously, into integral information systems functioning over the Internet. The shift towards the client-oriented approach is characterized by the fact that along with the development of e-government there is ever more talk about the e-citizen and e-services provided for the e-citizen.

For implementation of the Public Information Act and the Digital Signatures Act an extensive set of measures was initiated called the **Records Management Programme of government agencies**, aimed at reorganizing and transferring the records management of government agencies to a modern technological basis for the entire lifetime of a document, from its initiation, signing, registration and processing to archiving and preservation. Modernization of records management forms the first pillar of the development plan of the public sector ICT infrastructure.

The second pillar of the ICT infrastructure comprises **modernization of public sector databases** by implementing an integral Internet-based search system, which speeds up and simplifies the use of data in numerous databases by those authorized.

The third pillar comprises ICT infrastructure developments and **services for the citizen to participate in national e-commerce and e-democracy**. This includes several projects, such as the ID-card programme, implementation of digital signature, e-Citizen, TOM (*Täna Otsustan Mina* – in English "Today I Make Decisions"), *e*TaxBoard, internetization of public libraries, and several others, which help to develop and form the Internet-based ICT infrastructure in Estonia.

There are two basic issues in establishing Internet-based services: trust and availability – even though computer and Internet skills and their general distribution should not be underestimated. For interactive services to be usable, the user has to trust these services. One of the technical bases for establishing trust is the public key infrastructure (implemented at the beginning of 2002) together with its basic components, which provided opportunities for practical use of the ID-card – for identification and digital signature.

Development of the availability, feasibility and user skills in respect of Internet services is, however, a more general task, which cannot be limited to the efforts of the State and public sector. These issues will be discussed below in greater detail.

2.1.2.1 The Records Management Programme

The Records Management Programme (RMP) of government agencies is a cooperation programme for transition to inter-agency digital records management. Preparations for the initiation of the programme started in 1999, it was launched in the middle of 2000 and was planned to last for three years. The State Chancellery of the Estonian Republic assumed responsibility for implementation of the programme.

Typewriting bureaux have been superseded by computers in government agencies and documents have been handled via electronic information systems for years already, but the inter-agency management has not yet been replaced by integral digital management and information exchange, even though it might considerably save time and money and increase the uniformity and quality of records management.

The organization of digital management between agencies as well as all other organizations requires:

- **common methodology:** the State's records management policy, which is a part of the State's administration, information and Internet policy, will be defined with respect to global processes and the particular needs of the State;
- **common standards:** documents must not depend on hardware, software or netware; they are used in data exchange between officials, information systems as well as computer programs;
- **administration reform**: aimed at digitization of the State's records management and its modification according to information society rules;
- **common information technology solutions:** successful solutions to records management reform for government agencies will be turned into national solutions and necessary information technology resources will be drawn together to that end;
- **coordination:** activities concerning the topic and projects of the records management of government agencies will be drawn under common coordination.

Thus, transition to digital records management and its proper functioning require:

- elaboration and enactment of legislation for the regulation of digital records management;
- elaboration of work processes for records management for the entire lifetime of a document (initiation, usage, preservation, destruction);
- elaboration of IT environment and a set of IT tools using common standards in order to secure digital records management processes;
- elaboration and application of communication rules for inter-agency records management, establishing general requirements for the usage of information and communication means;
- skills and knowledge to use information systems and organize the functioning and development of the systems.

In 2001 the activities of RMP were oriented towards:

- development of legal environment for records management;
- preparation of standards for digital management;
- testing and introduction of preliminary RMP results in cooperation with other agencies and projects;
- elaboration of a strategic RMP training programme,

in 2002 these activities reached the application stage.

In order to ensure the "vitality" of management-regulating acts, RMP has focused on the description of management processes in an electronic environment and on the elaboration of necessary standards, which, after testing, would be the basis for the elaboration of legislation.

In order to apply the Digital Signatures Act and Public Information Act, the State Chancellery elaborated a document called the "Common bases for records management procedure", which regulates the processing of the paper and digital records management of State and local government agencies and legal persons in public law, and establishes the principles applicable to the public disclosure of public information. The document was enacted by the Government's regulation for compliance with the State agencies.

Rules for archiving constituted an important implementation provision, as did the consequent obligation for agencies to draw up records schedules. The records schedule is a classification scheme based on the functions of an organization and lists series of records under every function. By the end of 2002 all State agencies had drawn up the records schedules.

The RMP working group in cooperation with the National Archives, county governments and the Association of Estonian Cities has elaborated and made available on the Internet sample records schedules for local and county governments.

The most important results of RMP's standardization activities can be divided into three groups:

- translation of international standards of records management into Estonian,
- standardization of documents,
- adaptation of international standards and records management legislation with respect to the functionality requirements of RMP.

The records management standard ISO 15489 *"Information and documentation – Records management. 1. General, 2. Guidelines"* has been translated into Estonian and the public discussion ended on 1 November 2002. In the beginning of 2003 the version including proposals was

completed. It is hoped that it will be enacted as the official standard in Estonia in 2003. The use of the abovementioned standard will guarantee the integrity of records management in an agency. The standard is also recommended by the European Union as a tool for structuring records management.

Another important document recommended by the European Union is *"MoReq – Model requirements for management of electronic records"*, which was prepared in cooperation with the IDA programme. The document describes EU requirements for the composition of data models and metadata for records management systems, which can be directly applied and used also in Estonian records management systems.

Taking into account the recommendations of international standardization organizations and the specificity of information systems used in Estonia, the XML (*eXtensible Marking Language*) format based on the open systems principle (independent of software producer) and suitable for Internet-based applications was chosen as the digital document format for Estonian records management systems. The first draft standards have been tested; the problem with introduction lies in finding a text redactor which would allow the creation of documents with complicated structure and be expedient for use in State agencies. The use of simpler kinds of documents, primarily forms that can be filled in directly on the Internet, has already been introduced in many agencies.

In order to simplify the work of agencies in the development of records management systems a document called "Requirements to the functionality of electronic records management systems" and a user manual were completed by the end of 2002. This document describes the functions of records management throughout the document's lifetime.

It is worth mentioning two results of RMP's activities related to the testing of elaborated standards and rules on systems actually functioning.

1 According to the cooperation agreement of the State Chancellery and six county governments the sample records list of county governments has been tested and introduced. The cooperation project **eCounty** is one of the most important testers of results developed by RMP.

2 One of the practical aims of RMP is the development of an integrated information system of legislation, which would comprise the coordination of draft legislations, their legislative processing by the Government of the Republic, in the case of draft acts their submission to the Parliament, and the publication of approved documents in the State Gazette. The following stages have been completed:

- Electronic coordination system for draft legislation (**eJustice**) – a project managed by the Ministry of Justice.
- On 1 June 2002 the electronic information system of the State Gazette was launched. In addition to the publication system for legislation, the system includes the functionality of the electronic submission of data.
- As to the Government of Ministers Session Information System, the number of users has increased, and an inquiry system and XML-based input-output documents module have been created.

The people engaged in RMP consider the process of gathering, analysing and distributing necessary know-how to be the most important result of the three-year programme and a guarantee for the development of digital records management. RMP has elaborated and/or gathered know-how and recommendations, an analysis of related regulations and practical experiences, these have all been systematized and an information management system **eCounsellor** has been created. This Counsellor of electronic records management is an Internet-based electronic skills base, to advise State agencies on the transition to digital records management.

In addition, the State Chancellery, in cooperation with the Estonian Public Administration Institute, has elaborated a set of training materials on the transition to electronic records management, consisting of a training programme, a slide show and ancillary materials for the lecturers, learning materials for independent work and distribution principles for the training materials.

On 4 June 2002 the Government of the Republic endorsed the Development Plan for Records Management and Archiving 2002-2005. The development plan aims at developing a common and integrated system for records management and archiving in the public sector, which would be based on similar principles, rules and standards. The development plan includes records management trends in the near future, defines the development priorities for public archives and describes the State Chancellery's activities related to the coordination and organization of records management in Estonia.

2.1.2.2 The X-Road project

The aim of the second project – **the national databases modernization programme (X-Road project)** was to develop software, hardware and organizational methods for the standardized usage of most of the national databases. X-Road enables civil servants and legal and natural persons to search data from national databases over the Internet, provided they are entitled to do so. The system ensures sufficient security for the treatment of inquiries made to databases and responses received.

Preparatory work for the programme started already in 2000 with the realization and successful testing of a technological pilot project between three databases. The development activities of X-Road started at the beginning of 2001.

The basis of the X-Road programme lay in a vanguard and resource-saving idea to use one integral set of user interfaces for organizing communication with databases, suitable for dialogue between the consumer (citizen, civil servant, private entrepreneur) and numerous databases as well as for realizing cooperation between application programs and databases.

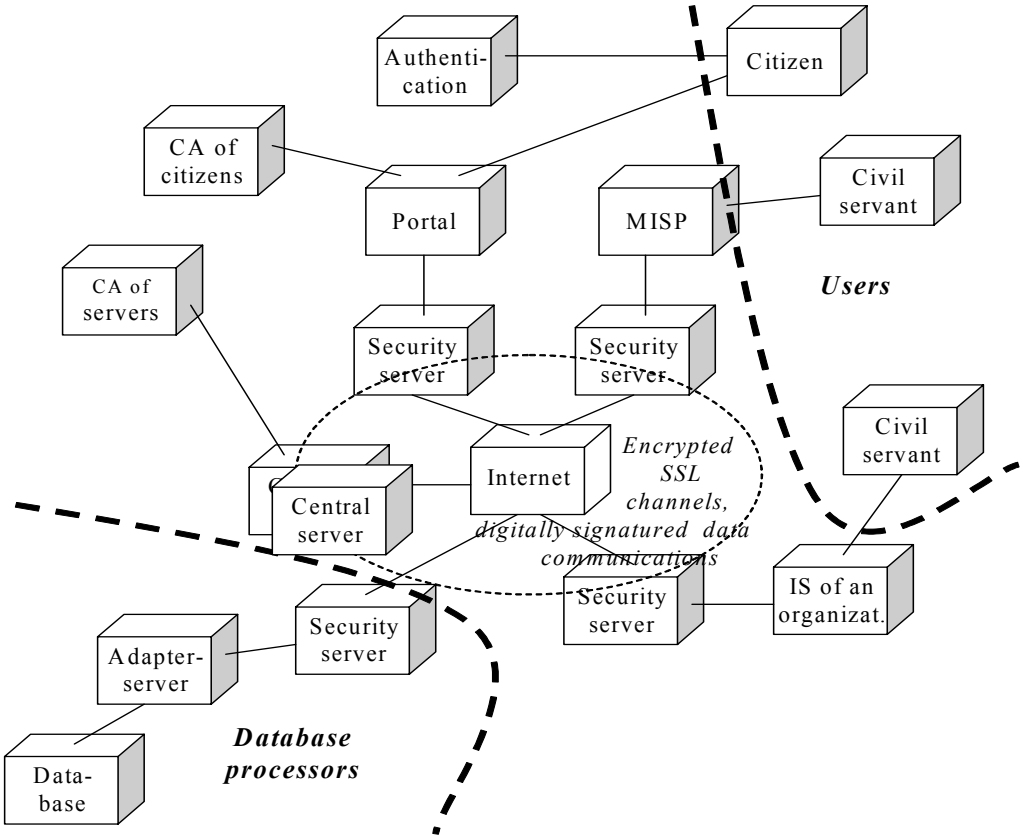
The programme's technical basis does not lie in the transition of all databases to some larger data management system but in the creation of unified user interfaces for different databases. Communication between databases as well as between users and databases takes place via the centre or the so-called central service layer (official name: *data exchange layer of information systems*). The data exchange layer, which constitutes the X-Road system, enables the user to search data from national databases that have joined the system, provided s/he is entitled to do so.

The system can be used in different ways (see diagram). In order to introduce oneself to the system (to authenticate oneself), an ID-card or the authentication service of commercial banks must be used.

Every **citizen** can use the system via the so-called citizen portal (more information in "e-Citizen project" below).

Civil servants can enter the X-Road system through the information system of their agency in order to perform their duties.

As an additional option for organizations with data security problems, a free standard mini-information-system-portal (MISP) has been developed, functioning as a secure system, and organizations can also use ASP services to use it.



Functional scheme of X-Road

The databases themselves remain functioning in a standard way; they are connected to the X-Road system by a special user interface. Thanks to the unified user interface it is now easier to use databases.

As to data security, the functionality of X-Road is very carefully designed and developed. The security servers of databases and information systems connected to X-Road communicate over encrypted channels. All users must go through authentication and authorization.

- **The citizen** can obtain and submit information within his/her rights;
- **The civil servant** can use all national databases in the decision-making process within his/her limits of authority;
- **The entrepreneur** can use the information of national databases for carrying out business within his/her limits of authority.

No citizen can read the data of another citizen, and no civil servant can read data not related to his/her work tasks.

The number of components that can be connected to the data exchange layer of X-Road is not limited.

When the project application was submitted more than two years ago, project development was planned to last three years – 2001-2003.

In 2001 the architecture and main functions of the whole system were designed. On the basis of a public procurement competition, all necessary software components of the X-Road environment were elaborated and tested, and the technical and user records of the project were drawn up. In December 2001 the **X-Road administration centre** was launched within the Estonian Informatics Centre.

In cooperation with other priority projects (e-citizen, e-elections, etc.) a number of information services available for all on the Internet were elaborated. Every citizen can see his/her data in the registers and notify necessary corrections to his/her statistical personal data (nationality, education, native language, field of activity, etc.)

In 2002 the development of X-Road continued in several different directions. Firstly, the existing technical basis was improved and several new functions were realized. Secondly, extensive work was carried out to link up new databases and the information systems of agencies with X-Road, and new services were also elaborated. Thirdly, various amendments, which are inevitable from the viewpoint of technological development, were proposed for the legislation and work organization of data processing and databases.

Development of the technical basis of X-Road was necessary in order to add new functions that appeared to be necessary in launching X-Road as well as to catch up with modern technological development. Work carried out in 2002 included the following:

- elaboration of the monitoring system
- realization of the simple object access protocol (SOAP) of distributed systems
- addition of an interface to the citizen portal to enable the use of ID-card
- application of ID-card in the mini-information-system-portal (MISP)
- development of MISP into an independent information system of an agency
- unification of the user interface for users of different databases
- addition of a transport system for XML-format documents
- addition of a system for entering data in databases
- addition of a system for making complex inquiries
- automation of portal updates over the Internet
- software expansion of security servers for identifying malfunctioning of a server and offering possible solutions to problems
- new solution for inquiries to the citizen portal for the population register in order to improve the quality of data
- design of the new State register of databases, which would take account of the technological opportunities of X-Road
- activities related to the unification of the functions of two national IT projects – X-Road and Citizen IT Environment (CIT)
- various activities related to the development of concrete databases.

All technical solutions for the development of X-Road were contracted through the public procurement system. The value of all contracts exceeded ten million Estonian kroons (over EUR 640 000).

The linking of agencies and databases to X-Road did not take place as quickly as the programme's contracting agency – the State Information Systems Department (RISO) of the Ministry of Economic Affairs and Communications – had planned. The main impediment was not the software developed or hardware installed, which both functioned perfectly, but various legal and organizational barriers. By the end of the year about 17 agencies with 23 databases had joined X-Road. Joining and using X-Road to obtain data is free of charge.

Information on the materials used in the X-Road project and conditions for joining are available on the Internet: http://www.riik.ee/ristmik/ (only in Estonian); the database of X-Road services is available at http://x-tee.riik.ee/eteenused/ (only in Estonian).

2.1.2.3 e-Citizen project

The third project – **the project e-Citizen** (in the narrower sense known also as the **citizen's IT environment project)** is a form of cooperation between State institutions to help make the State more citizen-oriented by means of ICT and the IT environment. The project's preparatory work started in 2000, public procurement was carried out in 2001 and concrete contracts with involved actors were made in April 2002. The public contracting authority and organizer of the project is the Department of State Information Systems (RISO) of the Ministry of Economic Affairs and Communications. As a result of public procurement, several Estonian IT companies and experts participate in elaboration of the project. The preliminary two-year project for the creation of a citizen portal on the Internet is developing into a unique future solution for the citizen to participate in the information society. The project is, in a sense, a follow-up to as well as a "roof project" for several national e-projects, such as the Records Management Program, X-Road, ID-card, and state portals www.riik.ee, http://tom.riik.ee/ etc.

Present Estonian information systems and legislation (e.g. the Public Information Act) foresee the future information society primarily as a collection of numerous websites, information systems and portals that all provide services for the citizen. Poetically speaking, the citizen will, as it were, walk down the "avenue of services" looking for the required service on the Internet. Commonly speaking, this mentality still follows the same State tradition whereby the civil servant is king and the citizen goes from one civil servant (web) to another civil servant (web).

The citizen's IT environment values the citizen. Every citizen has his/her own information system (office). The citizen's information system is equivalent to that of a ministry, city government or bank. The citizen can communicate with all the national information systems through his/her personal information system (office). All information systems will have the possibility and obligation to communicate with the citizen's office and reflect the performance of the citizen's "business" in his/her office. The citizen needs no longer to search for the service but has the opportunity and right to order the service and monitor the performance of the service "without leaving his/her office".

The essence of the project lies primarily in the elaboration and implementation of rules, agreements and standards. The project is complicated in the sense of information technology. This is necessary in order to ensure the synchronized functioning of thousands of processes. It is complicated also in the organizational sense. We cannot hope that introduction of the e-Citizen mentality suggested here would be easy for civil servants and citizens. The success of the project greatly depends on how much the State and local government agencies and the private and tertiary sectors are willing to accept and implement these ideas. Naturally, the project which has an impact on the whole of society implies legislative as well as organizational changes.

Transition to the information society is a revolution. Realization of the e-Citizen project presumes great changes in the functions of national institutions within the next five years. Many of these institutions will disappear; or their role will change radically. Overcoming the passive resistance of institutions is one of the most crucial risks of the project.

The **results** of the citizen's IT environment **by the end of 2002**:

- the citizen's manual covers approximately 20% of planned topics;
- every citizen has the opportunity to use the e-mail address *forename.surname_XXXX@eesti.ee*;
- every citizen has the opportunity to use his/her own personal secure information system;
- direct services of X-Road (checking/changing one's own data in the databases);
- option to attend to some business with the State and the private sector in one's virtual office;
- every citizen has the option to use a simple digital signature environment.

The vision of the citizen's IT environment supports the broader e-Citizen vision according to which:

- by 2004 all State and local government agencies will be providing services via the Internet;
- nearly 60% of the population will be using the Internet in everyday life;
- a major part of the population will have started to use the secure and convenient citizen's IT environment ("virtual office");
- e-services provided by the public and private sectors will be easily accessible to the citizen in the one-stop information portal.

The citizen's IT environment (CIT) is a set of information technology devices available for use through the Internet browser by all citizens (more precisely, all inhabitants) for communication with the information systems of State and local government agencies, private enterprises and tertiary sector institutions (hereafter referred to as agencies).

The broader goal of establishing CIT is to allow all people to obtain information about their rights and obligations, and to actively participate in public life at national, regional as well as local level – to be an "active" citizen.

The devices of CIT can be divided into three:

- citizen's part (citizen's portal and tools),
- core part (core tools for services),
- public part (information portal).

Citizen's portal: every citizen can directly use the following basic components: citizen's records management system, electronic forwardable mailbox, and a secure environment for accessing services, including digital signature.

Core tools for services: rules and core tools will be elaborated for realization of and easy access to the citizen-oriented e-services of the information systems of agencies.

The information portal is a free access website to inform people of their rights and obligations; it is also the citizen's gateway to e-services.

The services provided through CIT are divided into information services and e-services.

Information services are administered in the information portal. There are no restrictions to use of the information portal. If the information portal refers to a service that requires authentication, the user must authenticate him/herself to use the service.

Information services are hierarchical and are divided into layers.

The citizen's part of CIT tools consists of the following components:

- **User's archive** – citizen's records management system. Every user has his/her own private area with data that can be administered only by the citizen him/herself. The records management system can be used only through the authentication system. The user may archive operations initiated by him/herself. All information systems of State and local government agencies and private enterprises send notices of e-services to the user's archive. A "case" can be initiated by the user as well as by the information system of an agency. All subsequent operations of a certain "case" are connected with the initiation document in the citizen's portal.

- **The citizen's mail system** is necessary for communication with service providers. Every citizen has an e-mail address *forename.surname_XXXX@eesti.ee*, assigned to the citizen by the ID-card. The citizen chooses the user name him/herself – the default user name is the citizen's personal identification code. In order to avoid junk mail, only authorized information systems can send mail to the address. The citizen will presumably use that address for forwarding.

- Via the website which can be tailored to the citizen's individual needs, the citizen can access his/her **records management system**. The citizen can adjust the form and content of his/her website and include links to services s/he is interested in. In addition to the website, the citizen can also have other environments, such as wireless application protocol (WAP).

  The citizen's records management system also includes an area for the digital signing of documents and for exchange of signed documents with partners. The citizen's part allows the citizen to submit documents (applications, proposals, complaints, etc.) to the State (any agency that has joined CIT) and monitor the procedure in the State machinery according to the status of the "case" (e.g. Approved, In process, Waiting, Under coordination, Under review, Completed).

Additional information about the project, documents, solutions and components is available at http://www.riik.ee/ekodanik/ and at the website's links (in Estonian with a short overview in English). New versions of the CIT information portal are also under preparation in English (http://www.eesti.ee/eng/) and in Russian (http://www.eesti.ee/rus/) but at the time of preparing this report they were not yet open for public use.

2.1.2.4 ID-card programme

Of other government programme and projects realized, the first we should address is the ID-card programme.

On 28 January 2002 the first ID-cards were issued to Estonian citizens. Thus, the Estonian ID-card project was completed. By 11 December 2002 100 000 ID-cards, and by 24 April 2003 200 000 ID-cards, had been issued.

The Citizenship and Migration Board already started preparatory work for the development of ID-card in 1997. The initiative developed into a national programme a year later and since then it has been under constant scrutiny and discussion by the public and media. On 18 December 2001 the Parliament established the ID-card as a compulsory identity document and the Estonian passport is thus only a travel document for travelling abroad.

The Estonian ID-card project focused on the digital signature, which is equivalent to the ordinary signature on paper. At the same time the technologies and standards for creating digital signature have to be uniform nationwide. The signature should identify a person directly in order to facilitate verifying signatures, without additional contracts being necessary. To achieve this aim the Identity Documents Act and Digital Signatures Act were amended, resulting in the following:

- a certificate, allowing documents to be signed according to the Digital Signatures Act, is inserted in the ID-card chip;
- certificates inserted in the ID-card have no field-of-use restrictions and therefore can be applied in the public as well as private sectors, and also in any kind of mutual relations between individuals;
- the certificate inserted in the ID-card includes the personal identification code, allowing the individual to be identified at once.

The primary purpose of information on the ID-card chip is to allow the digital, unambiguous identification of the individual and creation of the digital signature. The certificate includes only minimum information about the individual – names and the personal identification code. A firm decision was made initially not to add additional information to the ID-card, and not to include information that requires updating. All other necessary information can be stored in separate databases to which access rights can be limited on a system-centred basis once the person who uses the system has been unambiguously identified.

The national ID-card project was elaborated in cooperation with private sector representatives, thus creating preconditions for the implementation of a common signature practice. As the final result, digital signing must become easily usable for everyone but it must be cheaper and more effective than its main competitors – paper and pen.

The ID-card is generally suitable wherever a person needs to be authenticated or when documents have to be signed. This means ID-card has not been created for a specific service or application only.

The ID-card can also be used for signing and encrypting e-mails. Every authentication certificate includes the person's e-mail address *forename.surname_XXXX@eesti.ee* (XXXX is the random four-digit number assigned to the person). The person can register his/her daily e-mail address in the mail server and mail will be forwarded to that address. This service is developed together with the national e-Citizen project, which could also become the official communication channel between the State and individual.

In order to make the implementation of digital signature easier for all parties, the **DigiDoc project** was initiated in Estonia. This project comprises agreed file formats as well as program libraries and applications for handling them. The preliminary program libraries and applications have been elaborated (financed by the Look@World Foundation), allowing signatures to be effected and checked. These program libraries are meant for everyone to use, whether as a direct library or as samples of a useful code. This helps a common format to be followed in the applications of all parties. For example, a certificate issued by a bank must be suitable for submission and use in the Tax Board and vice versa. If a person who is a party to some contract downloads a document in his/her computer, s/he should have a client program allowing digital signatures to be effected and checked. This, in turn, would allow the digital signatures system also to be used separately, for example between other companies and individuals.

The free, secure **signing portal** has been elaborated as a primary application for ID-card owners. Provided a person has an ID-card and a computer with a properly adjusted ID-card reader, it is possible to upload a document, which will be digitally signed, in this portal. In addition to the

person's own signature this document can be opened for signing by other people, provided they have an ID-card. It is also possible to search for people in the catalogue. The parties can download the signed document from the portal to their computer and retain it.

The portal technology is also free for use by anyone. It has already been applied by banks in the development of signing environments, by *Eesti Telefon* (Estonian Telephone Company) for the establishment of archive and contract environments, as well as by the national e-Citizen portal (http://www.riik.ee/ekodanik - only in Estonian).

In addition to the portal checked technology, the DigiDoc-Client applications have been developed, allowing documents to be signed and signatures in the workplace computer. As the signed file format is also a file in a specific format, it can be applied without changing the daily work process. Most of the documents are drawn up on the computer anyway. Now there is no need to print them out even for signing – it can be done directly on the computer. They can be forwarded by e-mail and loaded in records management systems. If hitherto mainly paper documents have been archived, attention should now be focused on the retention of signed files. The overall result should be savings in terms of transmission time and costs, as well as retention costs.

At the beginning of 2003 *Sertifitseerimiskeskus AS* in cooperation with *Eesti Telefon* launched the message gateway of *DigiDoc*-portal. Using the message gateway it is also possible to digitally sign faxes and calls; and to save fax or voice messages in the *DigiDoc*-portal and sign them with the ID-card afterwards.

Additional information on the ID-card and its applications is available at www.id.ee (summary in English); information on applying for the ID-card is available at www.pass.ee (in Estonian, English and Russian) and on the technological infrastructure at www.sk.ee (in Estonian and English).

2.1.2.5 e-TaxBoard

The second important project implemented thus far is the e-TaxBoard.

The Tax Board was one of the first government agencies in Estonia to offer Internet-based e-services to citizens and enterprises for filling in income tax returns and for other contacts and communication between taxpayers and the Tax Board.

Following the cooperation initiative of commercial banks and *Eesti Telefon* in 1999, the modernization plan for the work organization of the Tax Board and the general e-strategy of the Tax Board were developed by the beginning of 2000. The e-strategy comprised several smaller projects and the **first stage** of one of the e-projects aimed at providing self-employed taxpayers with the opportunity to submit their 1999 income tax returns to the Tax Board in March 2000 via the Internet portals of the commercial banks *Hansapank* and *Ühispank*. This was the beginning of the present e-TaxBoard. The project was successful and citizens reacted positively – over 10% more declarations were submitted than had been expected.

The **second stage** of the project aimed at elaborating a package of electronic services that would provide self-employed and legal persons with the option to electronically communicate with the Tax Board via the above-mentioned banks and the Tax Board's portals. During this stage of the project, electronic communication consisted in the electronic submission of the most frequent documents and obtaining a real-time overview of one's tax liabilities.

Instead of the temporary technological solution of the first stage, a new one was created, which, like the previous one, ensured the authenticity of taxpayers and the confidentiality and integrity of data. The system requirements called for taking into account the needs of different taxpayer groups and handling them separately. Attention was also paid to ensuring sufficient system capacity and to drafting the necessary information materials for taxpayers.

As a result of the second stage, the e-TaxBoard application was launched in November 2000 and the e-TaxBoard portal was opened on the Tax Board's homepage. As for income tax and social tax declarations, the Tax Board set the goal of receiving electronically 10 000 of the 30 000 declarations submitted every month.

In the **third stage** of the project, the Tax Board organized a taxpayers' awareness campaign at the end of 2000.

In March 2001 over 36 000 personal income tax returns were submitted – three times more than in 2000. The number of electronically submitted income tax and social tax declarations has constantly increased. In addition, e-TaxBoard allows self-employed taxpayers to see the amount of social tax that has been calculated for them, paid, and transferred to the Social Insurance Board.

By the beginning of 2001 the e-TaxBoard project had achieved its initial goal: taxpayers had the option of communicating electronically with the Tax Board. The project laid the foundation for servicing taxpayers at a new level and since launching the application the Tax Board has continued to develop it further.

The project lasted until September 2001. In the **fourth stage** the Tax Board elaborated separate e-TaxBoard service packages for the Central Criminal Police and the Public Procurement Office in the summer (June-September) of 2001. At the same time the elaboration of similar applications, which proceed from the needs of different agencies, was started for the bailiffs, Police Board, Health Insurance Fund and other agencies which, pursuant to the Taxation Act, are entitled to make inquiries in the register of taxpayers and withholding agents.

The improvement of the e-TaxBoard subsequently continued according to planned development, including improvement of the IT environment to make the use of e-TaxBoard even more convenient for taxpayers.

In summer 2001 the Taxation Act amendment entered into force. The amendment obliges State, rural municipality or city agencies to submit declarations electronically to the Tax Board, provided that the agencies have the necessary information technology tools. The further goal is to also make it obligatory for large companies to use Internet for communication with the Tax Board.

Since February 2002, ID-card owners have the option of entering the e-TaxBoard with the ID-card via the Tax Board's homepage (*www.ma.ee*). If the taxpayer has not previously concluded an agreement for using e-TaxBoard, it will be concluded electronically at the first entry with the ID-card.

Taxpayers could do the following in e-TaxBoard in 2002:

- file, view and correct their VAT returns (1999-2002);
- file, view and correct their social tax and income tax returns (2000-2002);
- send their income tax returns as a file (this option is only through the Tax Board's homepage);
- view precepts on imposing VAT (1999-2002), income tax and social tax (2000-2002);
- submit VAT refund applications;
- view decisions, transfers and payment orders on submitted VAT refund applications (since 1999);
- submit personal income tax returns;
- view previous income tax returns;
- view social tax calculated, paid and transferred to the Social Insurance Board by employers;

- view tax account balances and tax account cards;
- send notices, proposals and questions;
- receive information about the tax arrears of certain persons.

More information on e-TaxBoard is available at *http://www.ma.ee/ema/* (information in Estonian and English).

2.2 Public procurement

The first regulation on public procurement in Estonia concerned the purchase of IT means and services, which was enforced from 1 August 1993. Only two years later the general Public Procurement Act was adopted. The Public Procurement Office has been an independent executive agency since 1996. One of its tasks has been the establishment and operation of the public procurement information system and publication of the public procurement information bulletin.

In 1997 elaboration of the electronic public procurement information system started. Firstly, the local network of the agency was created to organize the use of information resources and data exchange within the agency. Secondly, a Phare project, which included elaboration of the public procurement information system, was completed in 1998.

In April 2001 there was significant progress in the development of the information system. A Government's decision provided the establishment of the **State Procurement Register**, which became the basis for carrying out public procurement. As a result, all activities related to public procurement in Estonia are Internet-based. The register was launched on 1 April 2002.

In order to be able to enter one's public procurement notice, tender or any other document in the register, the purchaser has to register him/herself in the register.

The purchaser registered in the State procurement register enters a preliminary notice, notice, tender or tender for design contest through the link on the register's homepage. Entered documents are checked by the employees of the register and if the information is in conformity with the Public Procurement Act, it will be confirmed and the next working day the confirmed document will be available for all Internet users on the register's homepage under "Electronic Bulletin".

Since the document is available for everyone on the Internet, all those interested in public procurement can turn to the purchaser on the basis of this information to apply for participation in the public procurement, receive the tender documents from the purchaser and make their tender.

The described procedure presumes daily monitoring of the public procurement information system. In order to make it easier for tenderers to get information they are interested in, the register's homepage includes an option to subscribe for receiving this information at the tenderer's e-mail address. The tenderer registers him/herself as a user of the register and notes also his/her topic of interest on which s/he wants to receive information at the e-mail address. The notice containing brief information on a given public procurement is sent in the morning of the first working day after entry of the tender in the register.

Following the public procurement procedures the purchaser must also enter the declaration and report on the public procurement in the register. Information concerning disputes is entered by the employees of the management division of the Public Procurement Office.

All the information in the register is public and available to everyone interested in public procurement. The homepage of the State procurement register is in Estonian and English. The homepage of the Public Procurement Office *http://www.rha.gov.ee,* which is the connecting link between contractors of public procurement (purchasers) and companies (tenderers), includes all information of interest to both parties.

The Estonian Informatics Centre provides a service to assist public agencies in working out invitations to tender and/or to carry out tenders to order and purchase complicated IT project solutions.

According to the order of the State Secretary, the director of the Estonian Informatics Centre is authorized to negotiate on behalf of the Government of the Republic and to sign framework agreements on State deliveries of information technology, financed from the State budget. Based on this the Estonian Informatics Centre has concluded framework agreements with several large software and hardware producers, thus securing remarkable price reductions for central and local government agencies in acquiring software, training, and obtaining technical support. In addition to price reductions, the framework agreements also cover the terms of delivery, installation and payment, and other general conditions.

2.3 Increasing dissemination and use of ICT

2.3.1 Government programmes to develop the ICT infrastructure for the public sector

The development of the use of computers and the Internet would be inconceivable without the development of the respective infrastructure. Development of the Estonian ICT environment has been progressive. In addition to the various private sector ICT services, which are based on modern data communication networks and tools, government-established and State-financed ICT structures have also rapidly developed their information technology possibilities, and the nomenclature, scope and quality of services.

The first example would be the development of the **backbone network *PeaTee*** (in English EEBone) for providing State and local government agencies as well as other State-financed institutions with data communication services. *PeaTee* is administered by the Data Communication Department (**ASO**) of the Estonian Informatics Centre. The development of *PeaTee* was based on the enhancement of the backbone network ASONet elaborated by the Border Guard Administration, Customs Board and Police Board in 1993 and it was developed as a Government's target programme in the years 1997-2000.

The *PeaTee* backbone network connects all Estonian county centres and several nodes in Tallinn. *PeaTee* has Internet connection; it uses TPC/IP technology and 16 Mbps bandwidth. The bandwidth of the backbone network between cities is 4-50 Mbps, connections to Estonian Internet service providers (ISPs) are 100 Mbps and 1000 Mbps, and traffic within Tallinn 100 Mbps up to 1 000 Mbps.

PeaTee is a public network. Every State and local government agency has the right to use *PeaTee* but they are not obliged to use it. A State agency decides upon joining *PeaTee* depending on which bandwidths and access services it needs and whether it would be more useful to outsource them from public service providers or from the Data Communication Department (ASO) of the Estonian Informatics Centre.

Use of the backbone network is financed centrally from the State budget and is free of charge for subscribed clients. The client has to pay only for access to the backbone network. The client designs his/her own access connection service. The quality and price of the connection is mainly determined by the chosen technical solution of the access connection, as one of the solution's components is the rent of a data communication channel from the client's location to the *PeaTee* node. ASO deals also with the administration of clients' access connections.

PeaTee was launched in October 1998. At present *PeaTee* has over 850 end-users and around 14 000 computers from all over the country have been connected to the network. Further information on network services is available at http://www.aso.ee/ (in Estonian). Since the end of 2002 *PeaTee* has also been providing Internet telephone or Voice over Internet Protocol (VoIP) services. The VoIP solution can in some cases significantly reduce communication costs.

During 1999-2001, **the target programmes *KülaTee*** (in English "Village Road"**) and Internetization of Public Libraries**, both being a continuation of the *PeaTee* project, were implemented to provide local government agencies, public libraries and municipal schools with data communication services. An infrastructure was built in rural regions to provide the above-mentioned institutions with data communication and leased line Internet connections. Local government agencies got switches to *PeaTee* network nodes; schools, libraries and other cultural institutions were connected to **the Estonian Educational and Research Network (EENet)** or commercial ISPs.

EENet, which was established by the Ministry of Education in 1993, provides educational, research and cultural institutions with data communication services.

The aim of the data communication network EENet is to develop and organize the data communication network of educational, cultural and research institutions and to manage and coordinate the related activities in Estonia. EENet participates in the drafting and implementation of national data communication policy, in national informatics programmes and in the international data communication organizations CEENet, TERENA, etc., and manages the Estonian top-level domain (".ee").

On 1 January 2003 475 agencies had leased line connection to EENet; there were 345 virtual homes, 930 e-mailboxes and 104 thematic mailing lists of agencies and educational, cultural and research projects in the service server *nw.eenet.ee*. In the ".ee" top-level domain controller 14 965 domain names had been registered by 1 January 2003. According to estimations, EENet serves over 200 000 researchers, students, teachers, persons engaged in cultural activities, etc.

Traffic speeds between the nodes (cities) of the backbone network are usually 2-8 Mbps. The bandwidth of the Tallinn-Tartu line is 60 Mbps and 155 Mbps for the external line Tallinn-Stockholm (GEANT).

At the end of 2002 EENet launched the 100 Mbps leased line Internet connections of 23 educational institutions in Tartu. The Estonian IT College's new 100 Mbps leased line connection to the academic network was launched as well. In February 2002 the Tallinn Technical University was connected to the academic network by an optical cable at the speed of 100 Mbps. Thus all larger Estonian universities, except for the Estonian Agricultural University, are connected to the academic network by fast optical channels.

2.3.2 Development of ICT infrastructure and technology in the private sector

The main part of the ICT infrastructure, especially that providing services to the population, has been developed by the private sector, e.g. *AS Eesti Telefon* (Estonian Telephone Company), a company with considerable market force providing telephone, leased line and interconnection services.

In the early 1990s during the restructuring of the State enterprise for providing telephone services, a private company Eesti Telekom was established. Under the Concession Agreement from 1993 to 2001 the company's main telephone services provider AS Eesti Telefon (ET) established a new digital telephone network (78.4% of all lines were digital in 2002) and fulfilled the conditions for

providing sophisticated telephone and Internet services across the country. However, building high-quality telephone network has also raised the prices of telephone services for customers. Therefore some ET clients have given up fixed telephone services in favour of the services of mobile operators, which have lower monthly payments and no additional call set-up charge.

As the company had held a monopoly position for 8 years, it was able to secure its position in the market even after the market was liberalized in 2001. In 2002 ET succeeded in keeping 89.2% of the fixed telephone market and more than half of the market of international calls. ET has also established itself as the market leader for the Internet dial-up service and ADSL connections (72.8% share of leased line services market).

The main competitors of ET are *Tele2* and *Uninet (Radiolinja Group)*.

Following the liberalization of the telecommunication market for fixed and basic services too, new operators have entered the Estonian market. In 2001, 64 operators and 110 companies joined the existing 47 operators and 146 service providers. The largest increase has been among data communication service providers – 53 companies received a licence in addition to the existing 44 companies.

According to estimations (2001) the total dial-up market has 65,000 clients with ET's share being 41 000 clients. Internet connection through DSL-modem is increasingly popular – in September 2002 ET had 24,100 ADSL clients (over half of them individuals). According to the *AS Emor* survey[3] the main Internet service providers for companies having Internet connection were *Atlas* (ET) 59%, *Tele2* 10%, *MicroLink* 8%, *Uninet* 4%, and *KPNQwest* 3%.

Starman, the main operator providing Internet over CaTV cable, has 8 000 clients, 90% of them individuals.

In 2002 Eesti Telefon was successful in organizing the worldwide live Internet broadcast of the Eurovision Song Contest held in Tallinn in May 2002. By that time ET increased the capacity of international Internet connections by over 2.5 – up to 555 Mbps – and through its network node in London established a new 155 Mbps bandwidth international Internet connection with the global telecommunication company Sprint. In addition, ET has international Internet connections to Great Britain (Teleglobe), Sweden, Latvia and Russia. The total capacity of all ET's international connections is more than 12.5 Gbps, comprising voice as well as data communication.

ET is the reseller of the international telecommunication services of the Infonet Services Corporation (*www.infonet.com*) in Estonia, providing access to services and infrastructure in more than 60 countries all over the world and to telecommunication networks in more than 180 countries.

At the end of November 2002 ET completed the building of a new national data communication backbone network, which is 64 times faster than before and will result in a multiple increase in the number of leased line Internet connections in Estonia. The Siemens DWDM (*Dense Wavelength Division Multiplexing*) equipment applied in the data communications backbone network enables the network's capacity of one fibre optic pair to be expanded from the previous 2.5 Gbps to 160 Gbps, as now it is possible to transmit information through one pair of the optical line on different bands. ET's transmission network for the optical line connects all county centres and bigger cities on the ring topology principle. This makes it possible to automatically redirect the network traffic without any interruption of data communication in case of breakdown.

---

[3] Survey by AS Emor, "Information Technology and Internet in Estonian Companies", April 2002 (in Estonian).

The mobile operators' market is divided mainly between three operators – EMT (Estonian Mobile Telephone), Radiolinja Eesti and Tele2. Today EMT struggles to maintain half of the market. The main operators have covered the entire country with mobile networks. The mobile phone penetration rate is currently over 60 subscribers per 100 people in Estonia.

The continuous development of mobile communication is furthered by new services through mobile phones, such as mobile parking (original solution by EMT), mobile payments and other bank operations, mobile inquiries to databases, reservation/purchase of tickets by mobile phone (M-ticket in public transport in Tartu City and SMS-ticket in public transport in Tallinn, since August 2002), but also Internet connection through GPRS-based (*General Packet Radio Service*) mobile communication. Various alarm systems have been applied within the use of mobile communication technologies. In Estonia car alarm systems based on MobiKIT have become popular. In addition, new technological solutions are also entering the market and it is possible to purchase innovative equipment and services based on the mutual convergence of mobile phone and computer.

As a result of cooperation between EMT and ET a joint wireless Internet connection service was introduced in December 2002, allowing the use of Internet without limit nearly anywhere in Estonia for a fixed monthly fee.

Fast Internet connection is offered within up to 2 Mbps WiFi (*Wireless Fidelity*) propagation areas (there are over 40 such areas in Estonian ports, airports, hotels, etc., with new ones being added constantly) and up to 54 kbps GPRS-based Internet connection within other mobile propagation areas in Estonia. The service is primarily for mobile teleworkers, and in order to ensure maximum security for their work the virtual private network (IP-VPN) service is offered as well. There are approximately 35 000 teleworkers in Estonia who need such a service.

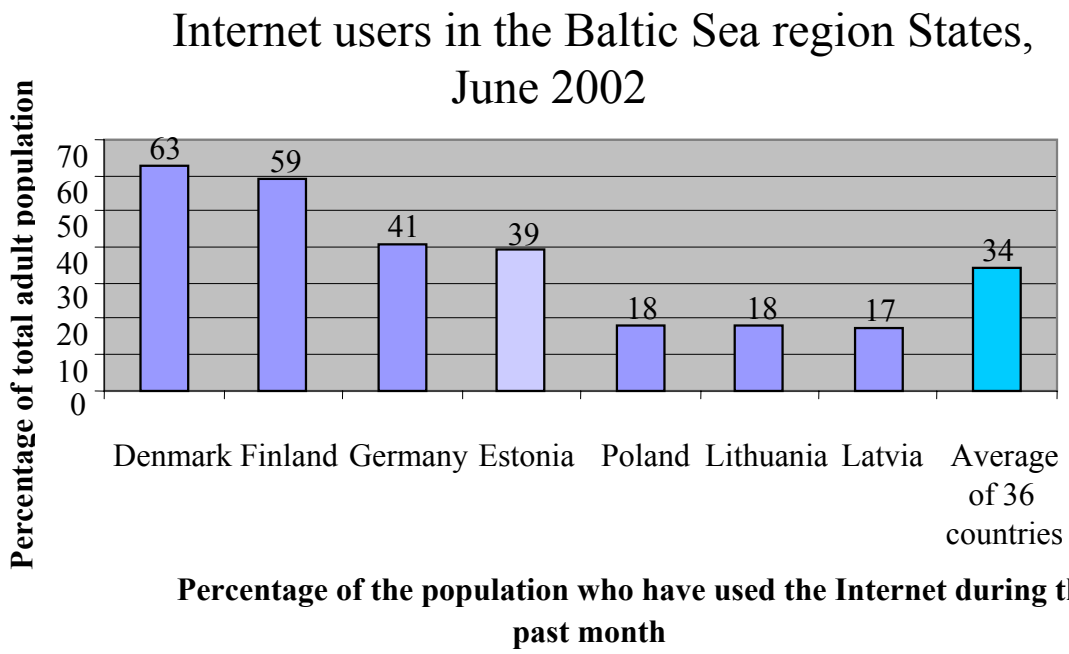
For stationary Internet users in rural regions without the necessary cable network for Internet connections, ET provides, since July 2002, new fixed wireless access Atlas RDSL, which allows a downloading speed of up to 256 kbps and uploading speed of up to 128 kbps through radio links. The latter is primarily for home users as private customers and small business customers. As the service provided by ET is relatively expensive, local operators and the consortium *Valvesilm OÜ*, who won the public procurement tender for the internetization of public libraries, try to organize the provision of alternative services for lower prices in rural regions.

2.3.3 Technology dissemination to individuals and households

The number of computer and Internet users has increased rapidly in Estonia within the last years. The percentage of people (aged 15 to 74) who have used the Internet during the last 6 months was 45% (469 000) according to a survey conducted in March-May 2003. The percentage of people to have used the Internet during the last 7 days was 35% (367 000)[4]. Of children (aged 6 to 14), 67% had used the Internet during the last 6 months according to a survey in spring 2003. As to the percentage of Internet users among the population (576 000 or 42.5%), Estonia outstrips several EU countries and is one of the leaders among the EU candidate countries.

---

4 AS Emor: E-track survey, September - November 2002.



Percentage of the population who have used the Internet during the past month

Data source: *Global eCommerce Report 2002 by Taylor Nelson Sofres Interactive*

The number of PCs in households has also increased significantly, as well as the share of PCs with Internet access – 35% of respondents aged 15-74 had a PC at home of which 69% were connected to the Internet in May 2003[5].

As shown in the analysis[6], Estonians spent 4.9% of their monthly income on telecommunication and nearly 3% on purchasing IT equipment in 2001. These indicators can be regarded as high even on a world scale[7].

The use of PCs is more widespread than the use of the Internet. The percentage of people (aged 15 to 74) to have used a computer during the last 6 months was 53% according to a survey conducted in March - May 2003 by AS TSN Emor and 40% of the respondents had used a computer during the last 7 days. The number of people (aged 15 to 74) who have never used a computer has decreased to 47%, i.e. nearly 492 000 inhabitants. The number of people who have never used the Internet has decreased to 53%, i.e. nearly 555 000 inhabitants.

---

5 AS TNS Emor: E-track survey, March - May 2003

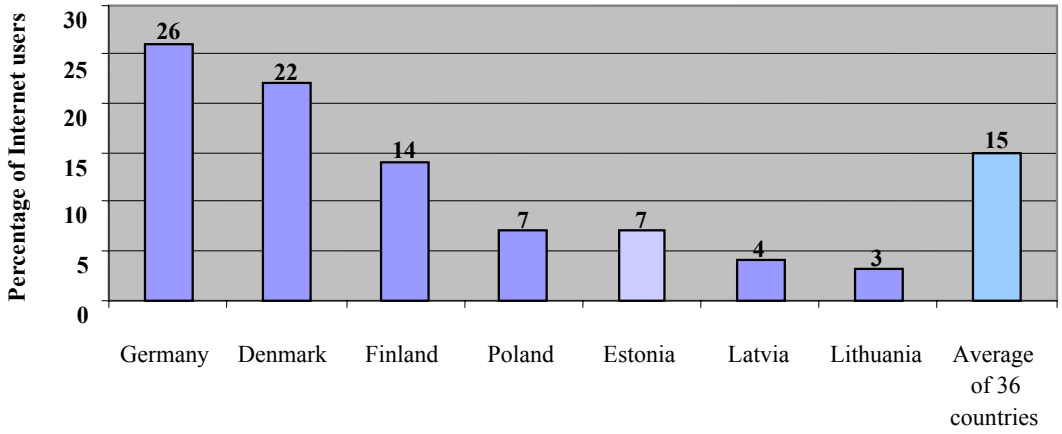
6 Estonian Statistical Office, 2002

7 PRAXIS Center for Policy Studies: ICT Infrastructure and E-Readiness Assessment Report: Estonia; 2002-2003.

Surveys show that Estonians use the Internet prevailingly for sending/reading e-mails (76%), searching for concrete information (70%), using Internet banking (61%), reading Internet publications (57%) and for communication (33%)[8]. According to surveys in September - November 2002 only 4% of all respondents (9% of all respondents who have used the Internet during the last 6 months) used the Internet for ordering/purchasing products/services. At the same time 19% of those who have used the Internet during the last 6 months visited Internet department stores to obtain information without purchasing anything.

In Estonia the biggest group of Internet users are persons aged under 20. These people, as world experience shows, are the least likely to buy goods and services via the Internet. The attitude towards e-commerce depends also on the general attitudes of the population towards this new way of providing services. The survey indicates that among the age group of 15 to 74, 66% of respondents are not interested in e-commerce at all, 16% are generally not interested, 5% cannot say, 11% are generally interested and only 2% are very interested in e-commerce. At the same time, reasons for not using e-commerce in Estonia are not so much related to the fear of insufficient Internet security (8%), as in many Western European countries, but to the fact that it is not possible to check the quality of goods (30%) or that the traditional way of shopping is preferred and customary (41%)[9].

Online shoppers in the Baltic Sea region States, June 2002



Percentage of Internet users who have bought goods or services online

8 AS Emor: E-track survey, September - November 2002

9 Global E-Commerce Report, 2001.

Data source: *Global eCommerce Report 2002 by Taylor Nelson Sofres Interactive*

Most Estonians use the Internet at home (49%), at their workplace (48%), at school/university (24%), but also in the households or workplaces of their acquaintances (24%), in public Internet access points (PIAPs) (16%) and elsewhere (6%)[10]. But still, according to the digital divide report[11], one of the barriers to Internet access was the absence of computers at home due to the high cost of equipment and Internet connection.

The number of PIAPs increased in 2002 and according to the data of *Look@World* there were 459 PIAPs with altogether 1,294 computers at the end of the year, which makes 0.34 PIAPs per 1,000 inhabitants. According to *AS Emor* the number of PIAP users has doubled compared with 2001.

The majority of PIAPs were opened in public libraries within the framework of the internetization programme of public libraries launched by the Ministry of Culture. According to the plan all public libraries should have leased line Internet connection in the first half of 2003. The main purpose of the programme is to establish an integrated Internet-based information system of libraries, which would serve as a channel for obtaining and using information on the services of libraries.

Nearly all schools have been provided with computers and Internet connections through the financing schemes of the Ministry of Education and the Tiger Leap programmes. In the academic year 2002/2003, primary and secondary schools (ISCED classification) were provided with computers for study purposes with an average of 3.6 computers per 100 pupils at the primary level and 4.4 computers per 100 pupils at the secondary level. The average in tertiary-level establishments (high schools, universities) was 5.0 computers per 100 students. All computers in schools and universities are connected to the Internet.

The following Reasons for reaching the present level of computer and Internet use may be noted (the reasons are listed in random order):

a) education programmes oriented towards the use of computers and the Internet; realization of the Tiger Leap Programme to provide schools with computers and Internet connections;

b) extensive development of public internet access points with public funds;

c) extensive promotion of Internet banking services provided by banks;

d) information provided to the public on the Government's information policy and information society development trends; generation of positive attitudes towards information society in the media; enactment of legislation promoting ICT development;

e) joint steps and cooperation projects of the Government and private companies to create convenient options for use of the ICT infrastructure (issuing of ID-cards and launch of necessary PKI infrastructure, development of e-government services, implementation of projects such as *Look@World*, etc.);

f) highly developed telephone communication and networks, and the provision of alternative data communication options (wireless Internet);

---

[10] AS TNS Emor: E-track survey, March - May 2003.

[11] Mari Kalkun (Emor), Tarmo Kalvet (PRAXIS), Report: Digital Divide in Estonia and How to Bridge It, PRAXIS 2002.

g) reduction in the prices for Internet usage charged by ISPs and provision of a variety of services for different Internet user groups;

h) general fall in prices of PCs with multimedia applications;

i) geographical proximity of highly developed ICT countries (Finland, Sweden, etc.) and close and good neighbourly relations; foreign investment in the development of the Estonian ICT infrastructure;

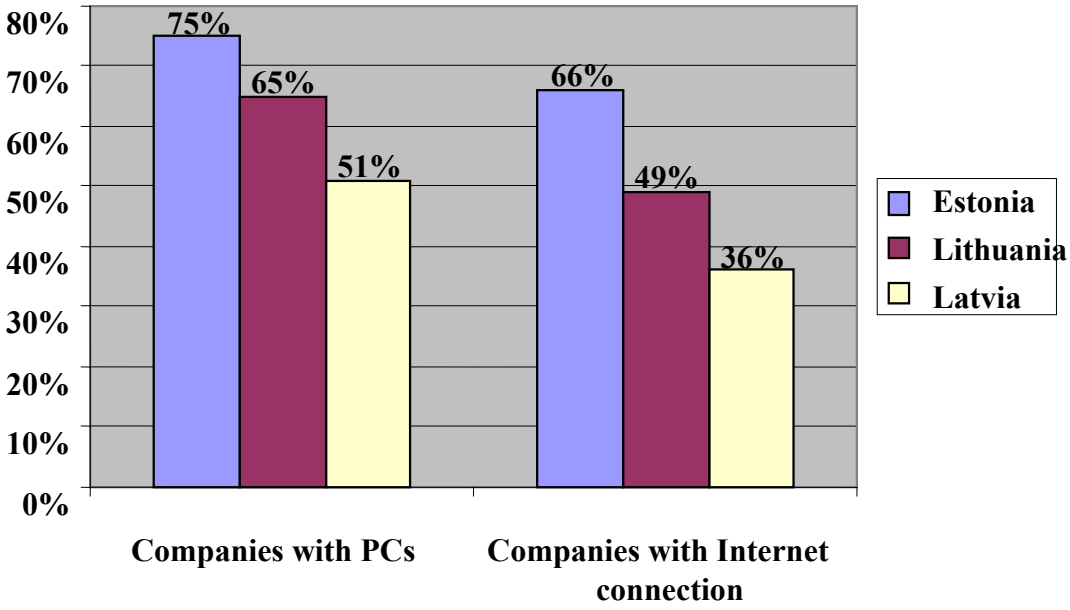
j) continuous economic growth, improvement of quality of life, etc.

The results of the cluster analysis of the Estonian ICT sector[12] also indicate that the State has played the most important role in building up the information society in Estonia. The business sector and the tertiary sector have followed when it has been in line with their objectives.

2.3.4 Technology dissemination to businesses

In April 2002, 75% of companies (about 25 000) registered in the Estonian Business Register had at least one computer and 89% of those (about 23 000) also had access to the Internet (40% using dial-up connection)[13]. Fifty per cent of companies had 1-3 computers, 21% had 4-20 computers and 3% had over 20 computers. A total of 7 700 companies have an Internet homepage, i.e. 35% of companies with an Internet connection. About 3 200 enterprises have an intranet solution, and approximately 1 300 companies have both – a homepage and intranet.

The majority of companies have not integrated their Internet and intranet solutions with other IT systems in the company. Approximately 1 100 companies have integrated at least some systems and about 1 800 companies are planning to integrate the systems in the near future.



[12] eVikings, Estonian ICT Cluster: Present State and Future Outlooks, http://www.esis.ee/eVikings.

[13] Survey by Emor Ltd.: Information Technology and Internet in Estonian Companies, April 2002 (in Estonian).

Source: Baltic E-track survey, Feb-March 2002.

No special policy or programme is needed to realize the increasing computerization trends in business.

On the other hand e-commerce in Estonia has developed slowly. Despite the numerous domestic B2B and B2C websites on the Internet, e-commerce statistics showed that in 2001 only 12% of enterprises have sold their products or services via Internet and 23% of enterprises bought materials, goods or services via Internet. The habits of the population in use of the Internet for buying goods and services were shown in the previous section.

2.3.5 Professional/managerial ICT skills

In the quite extensive ICT development process, the urgent need for competent ICT staff has become a serious problem. Taking into account the infrastructure, aspirations and tasks that have been developed, intellectual capital and professional staff are undoubtedly the key factors in further development. The problem is extremely complicated and typical (as in several developed countries). Taking account of economic possibilities, an influx of professional staff is unlikely to occur – instead, there is reason to expect a smaller growth in information society development projects and an acknowledgement of staff problems at the institutional level too. Recognizing the problem, the biggest Estonian universities, major IT companies and Estonian Telecom on one hand and the Estonian Republic on the other agreed to create a new institution of applied higher education, the Estonian IT College. The College is financed from a special fund created for the purpose. The Swedish Government gave significant support to the project as well.

The IT College provides a three-year applied higher education. This combines both IT and telecommunications, is of very high quality and has a strong applied focus. Up to 150 students will be prepared every year, although capacity lies at about 250. After finishing IT College, the majority of students will go into industry, both in Estonia and abroad. Students may also continue at universities, pursuing a bachelor's, master's and finally doctor's degree. The college enrolled its first students in autumn 2000.

In the academic year 2001/2002, at the universities and higher schools of Estonia, 4 269 students, of whom 335 were graduates, majored in ICT-related specialities (ICED classifier codes 481, 482 and 523).

In general education the national Tiger Leap Programme (1996-2000) for the computerization of Estonian schools, launched in 1996 by President Lennart Meri, set the following goals:

- help local governments to develop the IT infrastructure in schools, including support for the establishment of Internet connections in schools;
- help Estonian teachers to acquire basic computer skills and guide them to utilization of up-to-date resources of information and communication technology in subject teaching;
- support the updating of curricula by means of an interactive learning environment, promoting learning skills;
- encourage the creation of original software dealing with Estonian language, culture, history and nature in compliance with the national curriculum.

In order to achieve these goals, the Tiger Leap Foundation was created in 1997. From 1997 to 2000, the Foundation administered financial resources allocated to the programme from the national budget, in the amount of EEK 164 517 000 (EUR 10 515 000).

Several initiatives in addition to the Tiger Leap Programme promoted IT development in schools from 1996 to 2000:

- A Phare project with a budget of EUR two million, Information Systems in Education (ISE), has created a network of 20 pilot schools with the main task of introducing into local schools the school management software Extens, acquired within the framework of the project. Phare ISE has supported the training of more than 1 800 teachers in the use of computers in the classroom and organized the Telematics conferences in 1996, 1998 and 2000, which have proved to be popular among teachers. Phare ISE initiated the introduction of the European Computer Driver's Licence in Estonia.
- Cooperation projects of the Nordic countries and the Baltic countries: "BaltNet" (NOK 1 416 000 and USD 44 646), "Distance Training for Teachers" (EEK 1.6 million), and "School Development in the Information Era" (EEK 160 000).
- *Miksike*, which has a virtual learning environment with a wide circle of users and virtual assistant teachers, as well as popular virtual educational services, including electronic worksheets, a pupils' factory, story-telling and drawing competitions and academic competitions, was funded with EEK 1.5 million from Tiger Leap.
- Almost 100 Estonian schools are actively organizing and participating in learning projects such as the European School Project, I'EARN and Globe, mediated by international organizations. At the initiative of the Active Learning Centre at Tartu University, simulation games have been organized via Internet since 1993, and have been attended by almost 250 schools and 4 000 pupils over the years.
- The Open Estonia Foundation has funded several extensive educational projects promoting ICT infrastructure in schools and universities and teacher training with a budget of almost EEK 5 million.
- Within the framework of the Village Road Programme (*KülaTee*), the installation of Internet connections in many county schools has been financed.

In the year 2000, the Estonian schools were furnished with information and communication technology to the following extent:

- twenty-five pupils per computer on average (15 in Hiiumaa and 48 in Tallinn); there are no upper secondary schools or basic schools without computers.
- seventy-five per cent of all the schools have got online Internet connections and the remaining schools have a dial-up option.

These resources were mainly used in informatics classes, but each year more and more are being used in other subjects. According to the national curriculum, informatics is an optional subject, yet in the majority of computerized basic schools and upper secondary schools it is already being taught at the basic school stage of study.

The **teacher training** curricula at Tartu University and Tallinn Pedagogical University include a basic course in informatics; additionally, a number of specialities provide courses in subject didactics dealing with computer applications and/or courses in the basics of educational technologies. For example, Tartu University offers a two-year informatics teacher-training programme, and BCS and *IT Koolitus* deliver training to the information managers/network administrators of schools. Within the framework of in-service teacher training, ICT application courses are organized by universities. For example, Tartu University offers courses for the teaching of mathematics and science. Since the spring of 1999, the Tiger Leap Foundation has offered subject teachers ICT application training in biology, chemistry, mathematics, physics, astronomy, elementary studies, history, Estonian, English and German. Computer training that was started in the pilot schools of Phare ISE and Tiger Leap is now also provided in many other schools.

The Tiger Leap Plus (henceforth referred to as TL+) development plan (2001-2005) focuses on support for ICT development in Estonian general education and teacher training.

The TL+ development plan proceeds from the information policy of the Estonian Government and the development concept of the Estonian educational system, being the implementation document of the latter in the field related to ICT. The objectives of the development plan are in compliance with the action plan of the EU initiative, eEurope – Information Society for All.

As a vision in the year 2005 the Estonian educational system will be shaping the educational environment consciously and purposefully, helping Estonia to compete in the global information society.

The educational system will guarantee:

- premises for the development of the personality of the learner in accordance with his/her abilities and needs, for the development of self-expression, cooperation and communication skills and decision-making ability, so as to enable active participation in the life of society and ensure the ability to constantly learn and adapt to changes;
- equal opportunities for all learners, including the opportunity to study in a contemporary learning environment, and the development of necessary competencies;
- upgrading of the school, proceeding from the needs of learners and society, as well as cooperation between the school, parents and general public;
- expansion of the circle of decision-makers in education, both at the school and national level;
- monitoring the quality of educational processes;
- integration of Estonia into European and global educational space.

Implementation of the TL+ development plan should proceed from the principle of reasonable decentralization, promoting the emergence of ICT solutions appropriate for Estonian schools, offering teachers a choice of high-quality in-service training courses and taking into consideration the economic factors of hardware procurement.

2.3.5.1 Policies to reduce the "digital divide"

Against the background of fast Estonian ICT development and its reflection mainly in technological indicators, not enough attention has been paid to so-called "digital divide" problems, i.e. the socio-economic differences between individuals, households, enterprises and geographical regions and their unequal opportunities to use ICT.

As 47% of adults in Estonia have never used a computer and 54% have never used the Internet, the social factors that have prevented the application of new means of communication among this part of the population are now under scrutiny in order to find channels and opportunities for involving everyone in the further development of the information society.

It is possible to distinguish between several social groups among the non-users of the Internet. The largest group includes the so-called "people who are happy just to get through the day" and blue-collar workers.

The first group comprises primarily people over the age of fifty, mainly pensioners with little interest in what is going on outside their everyday life; those who do not wish to change their customary way of life, and who lack the motivation and material resources to start learning how to use the Internet.

The second group includes mainly skilled and unskilled workers, but also middle-level specialists and people engaged in customer service, the so-called "blue collars", who do not use a computer at their workplace and who do not find the Internet attractive (or useful) enough to motivate them to learn how to use it. In addition, there are social, psychological and economic barriers (fear of unknown technology, lack of language and computer proficiency, low income, etc.).

Sixty-five per cent of the above-mentioned risk groups (nearly 400 000 people) do not see a connection between their life and the Internet; they lack any motivation to use the Internet and therefore a different approach is necessary to create at least a slight motivation in them.

Thirty-five per cent of non-users (nearly 200 000 people) would like to use the Internet, yet lack skills and access so far. The involvement of these people in using the Internet would be relatively more successful.

In addition to public sector projects focused on providing e-services to citizens, the joint project of the public and private sector *Look@World* (*http://www.vaatamaailma.ee/* - also in English) aims to expand Internet access for non-users by establishing new PIAPs and providing PIAPs with IT tools (up to 450 computers to PIAPs in 2002). In addition, the action plan of *Look@World* for 2002 aimed to find options to change non-public Internet access points into public Internet access points, to decrease prices for Internet connection for PCs, to involve entrepreneurs to enable more households to purchase PCs or to establish closed Internet access points within enterprises for creating learning and using opportunities for their "blue collars".

As for training, *Look@World* started to organize free elementary training courses on computer and Internet use for 100 000 people within 3-4 years. The target group includes manual workers, civil servants, pensioners and others who have not independently used the Internet. A total of 219 teachers were recruited from all over Estonia to teach in 185 classrooms (17 classrooms were specially established for these courses). By 30 December 2002, 3 057 training courses with 28 649 course participants had been organized all over Estonia and 4 811 people had registered for the next courses. Seventy-two per cent of the courses were in Estonian and 28% in Russian. The preliminary feedback survey in August 2002 indicated that 58% of the course participants had started to use the Internet within a short time.

Look@World also organizes the training of PIAP staff, the so-called PIAP support persons. During 2002, up to 300 support persons were trained.

2.3.6 Government online

Besides the current Government's programmes and projects described above, a number of public web-based information systems have been implemented and are providing everyday online services. Some of these services will be described below.

2.3.6.1 The e-Government portal and its services

In 1998, as part of the project *"Vahetu Riik*" (in English "Direct Government"), a common access point for Estonian government agencies and constitutional institutions was created through an Internet domain *riik.ee* (*gov.ee*) and the Virtual Estonian Web Centre was established for administering it. Together with the fast development of Internet services the domain *riik.ee* has in five years become an inseparable part of Estonian e-government and the symbol of Estonia on the Internet. The portal "e-government" (*http://www.riik.ee/en/*) has time and again been changed and improved; new topics, databases, links, etc., have been added. In addition to the role of being the State portal, it has also acquired the role of an integrator and coordinator of national information systems. In 2000, the project went through several organizational changes and new development trends were prepared, most of which have now been realized.

Addresses like *http://tom.riik.ee* (portal "Today I Make Decisions; in Estonian), *http://ats.riik.ee/pub/* (public document system, in Estonian), etc., have been added to the domain. Several virtual servers and websites of State institutions and projects use the domain's resources. Although there have been only a few changes to the portal's content during the last year, its administrative organization has stabilized and the quality of the content improved. At the same time it has served as a basis for several new projects, such as the "e-Citizen" and "X-Road" described earlier.

The fact that the system has an average of over 100,000 visitors per day on weekdays proves the popularity of the portal. During peak hours there are over five visits per second, about 18% of them from abroad. Besides Estonian the working languages of the portal are English (*http://www.riik.ee/en/*) and Russian (*http://www.riik.ee/ru/*)*;* the data capacity of the latter two is, however, limited compared with the former.

The e-government portal should not only be the receiver of data but it should also become a data store and an interactive cooperation tool for government agencies.

Thus, to facilitate compliance with the Public Information Act, local governments have been provided with the option to disclose their documents in the common and integral server. The Ministry of Economic Affairs and Communications has provided a free server at *http://ats.riik.ee/pub/* (in Estonian only) for public sector agencies that have to meet the requirements of the Public Information Act but lack sufficient technology and finances.

Since the beginning of 2000, every State agency and local government has the option to use the modules of public services on the e-government server. The following modules are available: guest-book, voting, discussions, and questionnaires. All State and local government agencies can use these modules free of charge. These so-called communication modules can be used for organizing discussions and polls on the web.

2.3.6.2 TOM.riik.ee

The aim of the e-government portal's website TOM or "*Täna Otsustan Mina*" (in English: Today I Make Decisions) at *http://tom.riik.ee* is to enhance the population's participation in the State's decision-making processes. One can submit ideas, guidelines, thoughts and comments on draft legislation submitted by others or elaborated by ministries during the creation phase. Ideas that have found support among users will be submitted by Prime Minister's resolution to the relevant agencies to be executed. The public can constantly monitor what happens to the idea. In order to submit, comment, vote and sign ideas prior, registration is required. Everyone can read the ideas and comments.

The fact that in January 2003 371 ideas that had been submitted to TOM were undergoing legislative procedure in different government agencies, five acts based on submitted ideas were at the signature stage and ten draft legislations were under elaboration in the ministries, proves the popularity of TOM.

TOM also earned a European Commission award at the e-government conference in November 2001 in Brussels.

2.3.6.3 Service "forms on the Internet"

This service was elaborated as an independent project in cooperation with the Open Estonian Foundation, the State Chancellery and Phare public administration development programme; it was launched back in 1998. After the establishment of the virtual Estonian Web Centre the service was integrated with the latter and at present it is the most frequently used service in the e-government portal (average of 5 800 visits a day in January 2003).

The service has made document forms available for citizens to communicate with State agencies. Forms are in PDF-format and can be printed out (over 400) or filled in directly on the screen (around 80). At present the citizen can personally submit forms obtained from the Internet or filled in on the screen, or can send them by mail to a State agency, which will then process them. Thus the service saves time for the citizen. However, it is not yet possible to transmit documents directly to State agencies via the e-government portal owing to the lack of a secure authenticating transmission system for digital documents. Presumably there will be such an option after the implementation of the records management programme for government agencies and realization of the e-Citizen project.

The service is available at *http://www.riik.ee/blanketid/* and general information about the application of the service is also available in English and Russian.

2.3.6.4 Electronic "Riigi Teataja"

On 1 June 2002 an important new register was launched in Estonia – the electronic *Riigi Teataja* (State Gazette). Pursuant to the Riigi Teataja Act, *Riigi Teataja* is the official publication for the legislation, international agreements, reasoned judgments of the Supreme Court, notices and other documents of the Estonian Republic. The act stipulates that *Riigi Teataja* (hereafter eRT), which is one of the main national registers, will be published electronically as well as on paper. eRT is an Internet-based information system with public access that allows inquiries to be made within the whole legislation information system.

Legislation, notices and other documents published electronically and on paper have equal legal force.

Electronic *Riigi Teataja* includes the initial texts, whole texts, relationship between initial and whole texts, and additional information about changes and changers of documents and relevant data in the information system.

The users of the eRT information system can be divided into three main groups:

- **users of public services** are users of the Internet-based information system of *Riigi Teataja* entitled to search for and print documents;
- **authorized users** or users with access to data processing to the extent prescribed by law. eRT allows authorized users to electronically submit documents directly to the information system.

Users can access eRT at *http://www.riigiteataja.ee/ert/ert.jsp* (in Estonian) and also via links in the e-government portal *http://www.riik.ee/* and other Estonian web portals. In addition to eRT, initial texts and whole texts of legislation can also be accessed through free ESTLEX-online services directly via the e-government portal or via the web address *http://lex.andmevara.ee/estlex/kehtivad/AktSearch.jsp* (in Estonian). Specialists can use a search engine with special options through paid ESTLEX-online services.

2.3.6.5 National Land Information System (NLIS) e-services

The National Land Information System (NLIS), which was initiated in the Estonian Land Board (ELB) in 1995 on the basis of a strategy elaborated by a Phare project (EU Phare 1997-1999 Land Information System Development in Estonia), can also be regarded as an important step towards e-government. The system makes the administration of information related to Estonian lands easier, conveniently available and usable over the Internet.

The system has been developed further and the application options have been improved. The land Information System (LIS) has grown out of the Cadastral Information System (CIS) or data production system, which mainly serves as the basis for the maintenance of land cadastre. In addition to CIS, LIS also includes data management and application via public services on the Internet. The Public Service System is a tool for achieving one of ELB's main objectives, i.e. to provide society with land-related information, by enabling public access to spatial data maintained by ELB. The Public Service System is a group of services based on the Land Board's databases and map server available on the Internet.

Public services of LIS are divided into undirected and directed public services. **Undirected services** are meant for use by everyone. Access to services is free. **Directed services**, however, are meant for use by certain user groups (such as land surveyors, land advisers of local governments, etc.). Access to such services is limited and users must have a user name and password to access them.

The Land Information Service for the public consists of a simple web map application for users: using navigation tools it is possible to see administrative boundaries and the Estonian Base Map at the scale of 1:50,000 as a topographic background map. Zooming further the user can choose the display of either the Estonian Basic Map or digital orthophotos, both at the scale of 1:10,000. Cadastral and geodetic information is available as well. It is possible to display on the screen geodetic points and the parcel boundary layer, and by clicking on the point or parcel the alphanumerical information is displayed in a pop-up window or as a tool tip.

- The service is accessible through the Land Board's homepage http://www.maaamet.ee/teenus/maainfo.php

Two new layers were added to CIS and land information public service at the beginning of 2002: land price zones and productivity zones. Using this information every landowner can see directly on the Internet the exact taxable value of his/her land.

The Cadastral Unit Data Service, a.k.a. fast inquiry from the Cadastral Register, is also designed for public usage and is free of charge. Using different queries it is possible to get alphanumeric cadastral data. The service is suitable in cases when graphical cadastral data are of no interest.

The service is accessible through ELB's homepage *http://www.maaamet.ee/teenus/maainfo.php* (only in Estonian). It is also possible to query information by mobile phone using WAP protocol at *http://wap.maaamet.ee/ky/*.

Since the end of 2002 this service is also available trough the X-Road environment (see above).

2.3.6.6 Estonian Government of Ministers Session Infosystem

The Estonian Government of Ministers Session Infosystem (*http://www.riik.ee/valitsus/viis/viisengl.html* – in English) is an Internet-based information system for preparing and realizing Cabinet meetings and informing the public. The system was elaborated and implemented in 2000. Implementation of the system established preconditions for organizing digital records management in the Government after the implementation of digital signature and e-records management. The system has been improved with respect to the application of the results of the Records Management Programme (RMP) in the State Chancellery.

2.3.6.7 e-State Treasury

The e-State Treasury is an Internet application providing agencies maintained by the State Treasury with the option to communicate with the State Treasury via the Internet (*http://www.fin.ee/index.html?id=2078* - in Estonian only).

In e-State Treasury, agencies can make payments and reservations, send notices and receive statements of payments. All this is performed quickly and securely using the authentication service provided by banks.

The services of e-State Treasury comprise operations that enable agencies to submit data (reservations, payments, notices) to the State Treasury and receive data (daily journal, statements) from the State Treasury.

2.3.6.8 Centre of Registers of the Ministry of Justice

The Centre of Registers is a state agency under the administration of the Ministry of Justice. Its main functions include the administration of central databases of court registers (commercial register, land register, register of non-profit associations and foundations, etc.) and also other databases. In 2002 the Centre of Registers started to provide several electronic services, such as replying to name inquiries of enterprises, receiving electronic annual reports of enterprises, or information on compulsory dissolution, etc. Access to the e-services is available at *https://info.eer.ee/ari/ariweb_package.avaleht* in Estonian, German and English.

2.3.6.9 Services of the Register of Court Settlements

The Register of Court Settlements (*http://kola.just.ee*, in Estonian only), which functions as a part of the courts information system, is mainly an Internet-based means of cooperation for the employees of courts and the Ministry of Justice. The entry into force of the Public Information Act makes the register partly available to the public too. The database makes the settlements of civil, criminal and administrative matters available to the public through the search system after their entry into force, if no disclosure restrictions have been provided by law. It is also possible to view statistical reports on case procedures.

2.3.6.10 e-projects in Customs Board

Information technology has played an important role in the Customs Board's work since the establishment of the agency and its role has increased in time.

Today Estonia's accession to the European Union is inevitable. Therefore the Customs Board has launched several development projects and their successful completion is actually a precondition for accession. The time frame of these projects is more than tight – everything must be introduced before the targetted accession date, i.e. by December 2003.

There are over thirteen different EU systems that the Estonian Customs Board must be able to work with after the accession. Two of the most extensive projects in progress are:

- NCTS (New Computerized Transit System), i.e. the transit project. This is a system for keeping transit goods moving within the EU economic area under customs control until the end of the transit. Technically the system is based on the exchange of messages within all EU member states, between the customs offices at the points of entry and exit of the transit and all customs offices en route.
- MTS (Master Tariff System), i.e. the introduction of tariffs. Tariffs can be regarded as a set of all customs policies, including information on commodity codes, rates of duty, quotas and restrictions, special advantages, special permits, licences, etc., which have been listed in the legislation of different offices.

Technically it is a relational database (TARIC) administered in Brussels, which forwards changes to member states on a daily basis. All possible goods have been grouped and coded in the database and the above-mentioned information has been added to them in a way that allows the information to be processed in the information system and taxes to be automatically calculated when declarations are drawn up.

Taking into account the intensity of development projects, it is not really a consolation that the burden on the main system – drawing up declarations – actually decreases, expectedly by up to 70%, after accession to the EU, as most of the goods will be exchanged with EU member states. At the same time, Estonia will become the external border of the EU and requirements regarding the reliability, availability and functionality of systems will only increase.

2.4 International cooperation in IT development

Estonia's continuous fast IT development has been recognized all over the world. Estonia takes part in international cooperation projects and organizations; delegations from different countries have visited us in order to examine the present ICT strategy and development processes; Estonia's achievements have been presented at numerous international conferences. In addition, several reports on Estonian ICT development have been drawn up.

In summer 2002 the Government of the Republic of Estonia, United Nations Development Programme (UNDP) and the Open Society Institute (OSI) signed a memorandum of understanding to jointly set up a Regional e-Governance Centre in Estonia. The main aim of the training centre is to provide training in ICT coordination, organization and usage for the public sector managers and specialists and representatives of the tertiary sector of former Soviet republics, Central and Eastern Europe, and Asia. The training project offers the practical information and experiences of Estonia, the know-how of EU international experts and the exchange of experiences by participants in the training. Thus the project is important at foreign policy level too, as it has a positive influence on Estonia as a developed ICT country. The project also offers excellent potential for Estonian IT enterprises to introduce their products.

The activities of the e-governance centre comprise 8-10 training courses per year for 10-15-member groups. So far courses for the ICT managers of Kyrgyzstan, Sri Lanka, Albania and Bulgaria have been successfully organized. According to estimations, a total of 400 people will be trained within three years. Development of the information society in these countries facilitates the enhancement of democracy and effective functioning of the State machinery, and better provides citizens with public services.

Estonia continues to participate in the eEurope+ cooperation project of the EU candidate countries. The project aims to accelerate the modernization and reformation of the economy in the candidate countries, promote increase in administrative capacity and organizational structure, and improve general competitiveness. In spring 2002 the first progress report on the Estonian ICT situation was drafted (see *http://www.riso.ee/et/eEurope+_1stprogressreport.htm*).

Within the framework of the Northern eDimension project – joint project of the Baltic Sea States and the European Commission (*www.riso.ee/nordic*) - Estonia has actively participated mainly in the following two work groups: ICT security (Estonia is the lead country of the work group: see also the report at *http://www.riso.ee/en/nordic/eSecurity/2002aug.doc*); and e-government (led by Sweden).

The project offers new options for the development process of Estonian information systems – in the above-mentioned fields as well as in e-commerce, e-skills, indicators, and high-speed research networks and advanced broadband applications.

Estonia is a full member of ICA – the International Council for IT in Government Administration (*http://www.ica-it.org*). The aim of this prestigious organization is to promote intergovernmental exchange of information, ideas and experiences. The next ICA annual conference will be held in September 2003 in Tallinn and preparations for the conference have already started. The ICA Round Table Report 2002 reflecting Estonian information policy and ICT coordination is available at *http://www.riso.ee/et/ICARoundTableReport2002.htm*.

Estonia has several options for participating in EU projects. The European Commission launched the eContent programme to enhance the implementation of information technology and made a proposal to Estonia to join the project. The accession negotiations went well and now Estonia is the first EU candidate country to have full membership in the project. eContent is a multiannual programme for the elaboration, distribution and use of digital information content. The programme comprises the following three main topics: facilitation of access to and use of public sector information, promotion of creation of information content in different languages and for different cultures, and development of digital information content market. These, in turn, can be divided into various subtopics. The programme lasts for five years (2001-2005) and the EU will finance it to the extent of EUR 100 million. Projects can be submitted by all information content producers in the public and private sectors. The national contact point for the programme in Estonia is the Archimedes Foundation (*http://www.archimedes.ee/english/*).

One of the globally important events is certainly the World Summit on the Information Society , which will be held in two parts under the auspices of the Secretary-General of the United Nations: on 10-12 December 2003 in Geneva (a declaration of principles and action plan will be adopted) and in 2005 in Tunisia (implementation of the action plan will be under discussion). Estonia will participate in the Summit. The aim of the Summit is to bring together parties in the fast developing information society (government and private sector representatives, non-governmental organizations, media, etc.) to discuss the options and future of the information society and adopt an action plan satisfying the interests of all parties.

Compiled by Ivar Odrats Tallinn, 27 June 2003

Estonian Informatics Centre,
Senior Expert on Statistics of State Information Systems
tel.: +372 693 8212
e-mail: ivar.odrats@ria.ee

Attachment 4

Contribution by Professor Michael Geist

University of Ottawa, Faculty of Law

Director of E-commerce Law, Goodmans LLP

Table of contents

Page

A GUIDE TO GLOBAL E-COMMERCE LAW

I INTRODUCTION

What is e-commerce?

E-commerce is the use of electronic systems to engage in commercial activities. Businesses use e-commerce to buy and sell goods and services create greater corporate awareness and provide customer service.

What kinds of e-commerce business models exist?

A new lexicon has developed for the different e-commerce business models. "Brick and mortar" companies are those that have a presence only in the physical world and are without a commercial Internet presence (virtually every major company now has a website but a brick and mortar company typically uses its site for passive promotional purposes rather than to engage in online commercial activity). "Bricks and clicks" companies are brick and mortar companies that combine a physical offline presence with one online. Examples in the United States include Barnes and Noble and Wal-Mart who sell from both their physical stores and their web stores. "Pure-play companies" or "dot-coms" operate exclusively online. Examples include Amazon.com, which operates websites in the United States, United Kingdom, France and Japan and Monster.com, a global online job search service with sites in India, Singapore, Australia, Europe and North America.

Are there different e-commerce market categories?

Yes. Business-to-consumer companies (B2C) are involved with individual consumers in a retail or service setting. Business-to-business companies (B2B) provide goods or services to other businesses. Although B2B has less public prominence than B2C, most analysts agree that the B2B sector garners a much higher volume of business than does B2C. Consumer-to-consumer companies (C2C) facilitate transactions between individual consumers. eBay, an online auction site that serves the C2C market, generates revenue from transactional fees, ancillary services and advertizing. Also relevant are government-to-business (G2B) and government-to-consumer/citizen (G2C).

How large is e-commerce?

Despite the recent instability of many Internet companies, most analysts remain optimistic about the long-term future growth and critical importance of e-commerce and the Internet economy. By 2004, global Internet commerce is expected to swell to USD 3 trillion. As these numbers increase, it becomes apparent that e-commerce is developing into an integral component of the world economy.

How has e-commerce changed in recent years?

The e-commerce marketplace has witnessed dramatic shifts in recent years. During the late 1990s, venture capital flowed freely into Internet-based ventures, leading to thousands of novel and not-so-novel companies chasing dreams of cashing out with a quick initial public offering (IPO). The Internet market staged a stunning reversal in late 2000 and early 2001, however, as decline valuations for Internet companies led to the collapse of hundreds of companies with insufficient capital reserves. As a result, headlines touting the latest dot-com IPO success were replaced with news of yet another dot-com failure. While many successful e-commerce companies remain, their valuations and business models more closely resemble traditional businesses.

What are the most important elements of e-commerce law?

The most important elements of e-commerce law relate to the fundamental components of commercial transactions – how to ensure that an online contract is as valid and enforceable as one consummated offline. The building blocks of e-commerce law therefore focus on both enforcing the validity of electronic contracts and ensuring that the parties can be held to their bargains.

Once the contractual issues have been addressed, e-commerce law analysis shifts to a series of legal issues that may govern the transaction. These include jurisdiction (which court or arbitral tribunal can adjudicate a case), consumer protection issues, taxation, privacy, domain name disputes, as well as the role and potential liability of intermediaries such as Internet service providers.

II WHO SETS THE RULES FOR E-COMMERCE?

Who addresses e-commerce law at the international level?

As discussed in greater detail below, several organizations contribute to the development of global e-commerce law at the international level. Different organizations have tended to take the lead on different issues:

- UNCITRAL has played a leading role in developing model laws for e-commerce transactions;
- OECD has been at the forefront of Internet taxation, e-commerce consumer protection and privacy;
- WIPO has been the international leader on digital copyright and trademark issues involving domain names;
- ICANN has implemented the Uniform Domain Name Dispute Resolution Policy, which has addressed thousands of domain name disputes;
- APEC has worked on digital divide concerns and small and medium-sized enterprise (SME) e-commerce adoption;
- The Hague Conference on Private International Law has been the worldwide leader on Internet jurisdiction issues;
- WTO has considered e-commerce trade barriers.

Who addresses e-commerce law at the national level?

E-commerce law frameworks at the national level vary by country. In some countries, such as Japan, India, Malaysia, South Africa and Columbia, most of the e-commerce law and policy initiatives come from the national government. The United States and Canada use a dual approach whereby both the federal and state/provincial governments play a role, while in the European Union, directives applicable in all Member States are often the most important source of legal guidance.

How important are NGOs in the e-commerce law and policy development process?

On certain issues, such as jurisdictional rules and consumer protection, NGOs play a critical role in the development of e-commerce law and policy as they are often accorded a place at the negotiating and drafting table. At other times, the role of the NGO is more reactive, responding to new proposals and lobbying on behalf of business or consumer interests.

1 What international organizations are involved in e-commerce law? What do they do?

a) UNCITRAL[1]

What is UNCITRAL?

UNCITRAL is the United Nations Commission on International Trade Law. Established by the United Nations in 1966 to harmonize the law of international trade, it is a core legal body of the United Nations system that works to create accessible, predictable and unified commercial laws.

The Commission is composed of 36 Member States elected by the General Assembly, are chosen to represent the world's various geographic regions and its principle economic and legal systems. Members are elected for terms of six years, with the terms of half the members expiring every three years. The UNCITRAL secretariat is located in Vienna and carries out its work in annual sessions, which are held in alternate years in New York and Vienna. All States and interested international organizations are invited to attend as observers and participate in sessions of the Commission and of its working groups.

What does UNCITRAL do?

UNCITRAL focuses on law reform and creating model commercial laws that are both accessible and predictable. This is accomplished through:

- Conventions, model laws and rules which are acceptable worldwide
- Legal and legislative guides and practical recommendations
- Updated information on case law and enactments of uniform commercial law
- Technical assistance in law reform projects
- Regional and national seminars on uniform commercial law.

The Commission has established six working groups to perform the substantive preparatory work on a range of topics, including: international sale of goods; international transport of goods; international commercial arbitration; public procurement and infrastructure development; construction contracts; international payments; cross-border insolvency and, most important for current purposes, electronic commerce.

What is UNCITRAL's involvement with e-commerce?

UNCITRAL created a Model Law on Electronic Commerce in 1996 to enhance the use of paperless communication. In 2001, it created a Model Law on Electronic Signatures. Future electronic commerce work will focus on: electronic contracting, with a view to creating a draft convention; online dispute settlement; dematerialization of documents of title; and a convention to remove legal barriers to the development of electronic commerce in international trade instruments.

---

1 http://www.uncitral.org.

b) OECD[2]

What is OECD?

The Organisation for Economic Co-operation and Development (OECD) grew out of the Organisation for European Economic Cooperation, which administered American and Canadian aid to Europe after World War II. Established in 1961, OECD today has 30 member countries and maintains active relationships with 70 more. Its goals are to build strong economies in its member countries, improve market systems, expand free trade and contribute to development in both industrialized and developing countries. The governing body of OECD, the Council, is led by a secretary-general and is made up of representatives of member countries, who provide guidance on the work of OECD committees and decide on the annual budget.

What does OECD do?

OECD facilitates the creation of international instruments, decisions and recommendations in areas where multilateral agreements may create progress for individual countries in a globalized economy. Its various directorates and committees analyse issues, identify policies and deal with a wide range of economic and social issues from macroeconomics to trade, education, development and science and innovation. Among its other functions, OECD:

- has published more than 4 000 publications including research reports, conventions, working papers, country surveys and statistics spanning the spectrum of socio-economics;
- promotes and develops international statistical standards and coordinates statistical activities with other international agencies;
- fosters good governance in the government and private sectors through the hosting of conferences and the development of policy and guidelines;
- identifies and analyses issues surrounding emerging economies, sustainable development and aid.

What is OECD's involvement with e-commerce?

E-commerce has become an area of focus for OECD because of its transborder nature and its potential for all countries in the areas of economic growth, trade and improved social conditions. It has developed policy in areas ranging from telecommunication infrastructure and services to taxation, consumer protection, network security, privacy and data protection, as well as emerging markets and developing economies.

Following its "OECD Action Plan for Electronic Commerce", endorsed by its members in 1998, its work programme focus is to build trust for users and consumers; establish ground rules for the digital marketplace; enhance the information infrastructure for e-commerce; and maximize the benefits of e-commerce. Some of the activities currently under way in the area of e-commerce include:

- implementing aspects of the OECD Guidelines for Consumer Protection in the Context of Electronic Commerce;
- promoting the use of privacy-enhancing technologies and user education and awareness about online privacy issues;

---

2 http://www.oecd.org.

- studying the effects of e-commerce on cross-border trade in financial services, on contract law and on electronic delivery of insurance products;
- studying access to high-bandwidth information and communication technologies at affordable costs in rural as well as in urban areas;
- researching the needs for and constraints to, capacity development for trade faced by developing countries; and
- disseminating its work on e-commerce to member and non-member countries through other international organizations.

c) WIPO[3]

What is WIPO?

The World Intellectual Property Organization (WIPO) is an international organization that promotes and protects original works in the realms of art, science and technology.

Headquartered in Switzerland, WIPO is one of the 16 specialized agencies of the United Nations. It administers 23 international treaties dealing with different aspects of intellectual property protection (both industrial protection and copyright) and has more than 170 Member States.

Although WIPO was formed in 1970, its roots go back as far as the 1883 Paris Convention for the Protection of Industrial Property. In 1974, WIPO became a specialized agency of the United Nations with the mandate to administer intellectual property matters recognized by the Member States of the United Nations.

What does WIPO do?

WIPO's main objective is to develop international standards for the protection of intellectual property in keeping with ongoing advances in technology and business. Through its treaties, it seeks to:

- harmonize national intellectual property legislation and procedures;
- provide services for international applications for industrial property rights;
- exchange intellectual property information;
- provide legal and technical assistance to developing and other countries;
- facilitate the resolution of private intellectual property disputes; and
- marshal information technology as a tool for storing, accessing and using valuable intellectual property information.

What is WIPO's involvement with e-commerce?

WIPO has created a Digital Agenda to respond to the confluence of the Internet, digital technologies and the intellectual property system. Through international discussions and negotiations, WIPO is formulating new ways in which intellectual works can be disseminated, while at the same time ensuring the rights of their creators remain protected.

---

3 http://www.wipo.org.

The Digital Agenda also aims to:

- integrate developing countries into the Internet environment through such tools as the use of WIPOnet and the electronic delivery of information and services;
- rethink how intellectual property law works in Internet transactions and examine emerging new norms in this respect;
- facilitate the creation of effective online systems to resolve disputes; and
- coordinate and ensure the development of efficient and consistent responses to common concerns across national and multi-sectoral boundaries.

d) ICANN[4]

What is ICANN?

The Internet Corporation for Assigned Names and Numbers (ICANN) is a technical coordination body for the Internet. Created in October 1998 by a broad coalition of the Internet's business, technical, academic and user communities, ICANN has assumed responsibility for a set of technical functions previously performed under United States Government contract by other groups.

As a non-profit, private-sector corporation, ICANN is dedicated: to preserving the operational stability of the Internet; to promoting competition; to achieving broad representation of global Internet communities; and to developing policy through private-sector, bottom-up, consensus-based means. ICANN welcomes the participation of any interested Internet user, business or organization. The Board of ICANN is currently composed of nineteen directors: nine at-large directors, nine selected by ICANN's three supporting organizations and the president/CEO (*ex officio*). Five of the current at-large directors were selected by an Internet users' vote.

What does ICANN do?

ICANN coordinates the assignment of the following identifiers that must be globally unique for the Internet to function:

- Internet domain names
- IP address numbers
- protocol parameter and port numbers.

In addition, ICANN coordinates the stable operation of the Internet's root server system.

What is ICANN's involvement with e-commerce?

Future ICANN work is likely to address several key issues including institutional reform, the participation of Internet users in the policy-making process, the establishment of new top-level domains and amendments to ICANN's domain name dispute resolution process.

e) The Hague Conference on Private International Law[5]

What is the Hague Conference on Private International Law?

The Hague Conference is an intergovernmental organization that works to unify private international law rules. The first session of the Hague Conference was held in 1893; after seven more sessions, a statute came into force in 1955 making the Conference a permanent organization.

---

4 http://www.icann.org.

5 http://www.hcch.net/

The Conference, which has 59 Member States, holds plenary sessions every four years to discuss and adopt draft conventions and recommendations and make decisions on the working agenda of the Conference. Non-Member States invited to participate on an equal footing with Member States can vote at plenary sessions. The Conference is organized by a secretariat (the Permanent Bureau) which has its seat at The Hague and whose officials must be of different nationalities. The Bureau organizes the plenary sessions and maintains contacts with Member States, international organizations and users of the conventions.

What does the Hague Conference do?

The principal role of the Conference is to negotiate and draft multilateral treaties (conventions) in the different fields of private international law (e.g. international judicial and administrative cooperation; conflict of laws for contracts, torts, maintenance obligations, status and protection of children, relations between spouses, wills and estates or trusts; jurisdiction and enforcement of foreign judgments). Currently, its areas of concern include:

- conflict of jurisdictions;
- applicable law and international judicial and administrative cooperation regarding civil liability for environmental damage;
- problems of private international law raised by electronic interchange; and
- maintenance (support) obligations.

What is the Hague Conference's involvement with e-commerce?

In 1999, the Conference held a round-table discussion (in conjunction with the University of Geneva) with experts in various fields on issues arising from e-commerce and Internet transactions. A series of recommendations were adopted in such areas as online contracts, business-to-business and business-to-consumer transactions and online dispute resolution. In June 2001 the Conference held its Nineteenth Session to work towards a new Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters and to decide on its future work programme. Delegates based their discussions on both a Preliminary Draft Convention drawn up in October 1999 and on the results of formal and informal meetings of experts on e-commerce and intellectual property.

f) WTO[6]

What is WTO?

The World Trade Organization (WTO) is the international organization that deals with the rules of trade between nations. Based in Switzerland, WTO was formed in 1995 as the successor of the General Agreement on Tariffs and Trade (GATT), which set up a multilateral trading system shortly after World War II. Today WTO has over 130 member nations, more than 75% of which are developing or least-developed countries.

A series of rounds of trade negotiations under GATT and WTO have led to agreements between governments on various aspects of trade, tariffs, telecommunications and financial services. These agreements help set the ground rules for international trade and commerce. Decisions are made by the entire membership, generally by consensus. WTO hosts a ministerial conference that generally meets every two years. Several other levels of councils and committees work on a wide variety of issues.

6 http://www.wto.org.

What does WTO do?

The primary functions of WTO are to:

- administer WTO trade agreements;
- act as a forum for trade negotiations;
- handle trade disputes;
- monitor national trade policies;
- provide technical assistance and training for developing countries; and
- work together with other international organizations.

What is WTO's involvement with e-commerce?

At the 1998 ministerial meeting, WTO members agreed to study trade issues arising from global electronic commerce, focusing on three questions:

- how do existing WTO agreements impact e-commerce?
- are there any weaknesses or omissions in the law which need to be remedied?
- are there any new issues not now covered by WTO system on which members want to negotiate new disciplines?

Since then, issues related to e-commerce have been examined by WTO councils in the areas of services, goods, intellectual property and trade and development. A seminar on "Government Facilitation of E-commerce for Development" was held in June 2000, at which speakers from developing and developed countries, international organizations and the private sector addressed issues related to e-commerce and development. Each of WTO bodies working on e-commerce issues has produced progress reports for the General Council.

2 What national or regional entities are heavily involved in e-commerce law?

a) European Union (EU)

What are the most important European Union e-commerce law directives?

The European Commission has shaped e-commerce law throughout Europe and around the world since the mid-1990s. Essential directives include:

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases
- Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts
- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce")
- Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society.

b) Council of Europe

Who sits on the Council of Europe?

Although it is frequently confused with the European Union, the Council of Europe is a distinct body that encompasses a far larger group of countries than the EU. It includes 41 countries from Andorra to the United Kingdom. Several non-European countries, including the United States, Canada and Japan, enjoy observer status with the Council.

What is the Council's involvement with e-commerce issues?

The Council of Europe is best known for having successfully completed negotiations on a global cybercrime treaty in 2001. The treaty covers a wide range of online criminal activity including fraud and computer hacking. It also addresses Internet service provider liability and copyright concerns. In late 2001, the Council announced plans to develop an additional protocol dealing with racism and xenophobia online.

c) APEC[7]

What is APEC?

The Asia-Pacific Economic Cooperation (APEC) was established in 1989 in response to the growing interdependence of Asia-Pacific economies. It began as an informal ministerial-level dialogue group with 12 members and has grown to include 21 member economies comprising some 2.5 billion people, a combined gross domestic product of over USD 18 trillion in 1999 and over 47 per cent of world trade. Its goal is to advance economic dynamism and sense of community within the Asia-Pacific region.

APEC operates by consensus. The APEC chair rotates annually among members and hosts an annual ministerial meeting of foreign and economic ministers. At each year's ministerial meeting, members define and fund the work programmes for APEC's various committees, subcommittees, working groups and forums. APEC also has a Business Advisory Council composed of up to three senior business people from each member economy to provide advice on APEC action plans and specific business/private sector priorities.

What does APEC do?

APEC's goal is to achieve "free and open trade and investment in the Asia-Pacific by 2010 for developed member economies and 2020 for developing ones." In Osaka in 1995, APEC leaders established the three pillars of APEC activities: trade and investment liberalization, business facilitation and economic and technical cooperation. In 2000, APEC's objectives included:

- managing globalization through economic and technical cooperation and through participating in international forums;
- an Action Agenda for the New Economy, focusing on an e-Commerce Readiness Assessment, paperless trading and capacity building for both people and institutions;
- ensuring individuals from rural and urban communities alike have access to the Internet by 2010, including a pledge to triple the number of people with such access by 2005; and
- strengthening the multilateral trading system through a new WTO round.

---

7 http://www.apecsec.org.sg

What is APEC's involvement with e-commerce?

APEC's E-Commerce Steering Group is currently working on a range of issues, including:

- a Digital Divide Blueprint for Action to address issues of the digital divide and reliable, affordable access to the information infrastructure;
- paperless trading;
- a review of the 2000 APEC Action Plan to Support the Use of Electronic Commerce by SMEs;
- development of APEC voluntary online consumer protection principles;
- development of policy regarding the creation of an environment conducive to e-learning; and
- reviewing and updating the 1998 APEC Blueprint for Action on Electronic Commerce.

d) United States

Which United States agencies and organizations have been at the forefront of e-commerce law and policy development?

The United States has been a leader in developing e-commerce law policy since the Internet's inception. Agencies and organizations leading the way include:

- The Department of Commerce, which continues to play an oversight role over the Internet's infrastructure including the domain name system;
- The Federal Trade Commission, which has played the role of privacy and consumer protection enforcer;
- The Department of Justice, which administers United States competition law policy;
- The State Department, which leads the United States delegation at the Hague Conference negotiations;
- The Federal Communications Commission, which regulates communications infrastructure;
- The American Bar Association, which has developed policy documents on jurisdiction, privacy and e-commerce law; and
- The National Conference of Commissioners on Uniform State Law, which has drafted the Uniform Electronic Transactions Act, the United States version of the UNCITRAL Model Law on Electronic Commerce.

e) Canada

Who regulates e-commerce activity in Canada?

No single agency or entity can be said to regulate the Internet or e-commerce in Canada. Agencies that play a significant role in Canadian Internet and e-commerce law and policy include:

- Industry Canada (privacy, electronic commerce, electronic signatures, copyright)
- Justice (jurisdiction, cybercrime)
- Canadian Heritage (copyright)
- Competition Bureau (consumer protection, marketplace regulation)
- Canadian Internet Registration Authority (dot-ca domain names)

- Canadian Copyright Board (copyright)
- Canadian Radio-television and Telecommunications Commission (broadcast, Internet regulation)
- Uniform Law Conference of Canada (e-commerce, jurisdiction).

f) Australia

What is the most prominent e-commerce regulatory activity in Australia?

Although Australia has enacted e-commerce, privacy and online gambling legislation, it is perhaps best known for its online content regulation. The Australia Broadcasting Authority has been granted the power to order offensive content removed from Australian-based websites and to request that Australian Internet service providers take steps to make such foreign-based content inaccessible to Australian users. Despite dire predictions about the likely effect of such legislation, few sites have been removed from the web and the number of complaints has been relatively limited.

g) Singapore

How early did Singapore adopt e-commerce legislation

While dozens of countries have enacted e-commerce legislation, Singapore stands as one of the very first to establish an e-commerce legal framework. The country enacted the Electronic Transactions Act of 1998 in June of that year. Moreover, the first digitally signed international government document between Singapore, Canada and the State of Pennsylvania was signed in April 1998.

h) Colombia

Has Columbia enacted e-commerce legislation?

Yes. Colombia approved a law on electronic commerce, digital signatures and certification authorities (Proyecto de Ley Sobre Comercio Electrónico, Firmas Digitales y Autoridades de Certificación) in August 1999. The law is based on the UNCITRAL Model Law on Electronic Commerce. Further regulations concerning requirements for certificate authorities (discussed further below) have also been adopted.

i) Argentina

Is it too late to adopt e-commerce legislation at the national level?

No. While much of Europe, the United States and Canada have enacted their legislation, many countries are still working on appropriate domestic e-commerce statutes. For example, Argentina enacted its digital signature law in December 2001. The Argentinian law addresses the licensing and liability of certificate authorities and the legal effects of electronic documents signed by digital signature. Moreover, the Government has prepared amendments to the Civil Code in order to adjust requirements of form to electronic commerce.

j) Tunisia

How broad is Tunisia's e-commerce legislation?

Tunisia enacted the Electronic Exchanges and Electronic Commerce Law in 2000. Much like its counterparts around the world, the law covers electronic contracting and the validity of electronic signatures. In addition, the law boldly creates a National Agency for Electronic Certification, an administratively independent public agency designed to address electronic signature and certification issues.

3 What NGOs are involved in e-commerce law?

a) Global Business Dialogue on E-commerce (GBDe)[8]

Who belongs to GBDe?

Established in January 1999, the Global Business Dialogue on E-commerce counts dozens of the world's largest companies as its members including Disney, Vivendi Universal, BCE, AOL Time Warner, NEC, NTT, Hitachi, Toshiba, Alcatel, Deutsche Telkom, Daimler Chrysler and Nokia.

What are GBDe's areas of concern?

GBDe focuses on providing governments with the business perspective on e-commerce law and policy development. The organization has identified eight areas of concern: consumer confidence, convergence, cybersecurity, digital bridges, e-government, intellectual property rights, taxation and trade.

b) Internet Law & Policy Forum (ILPF)[9]

What is ILPF?

Founded in 1995, the Internet Law and Policy Forum is an international non-profit organization of major, Internet-oriented companies, including Verisign, Microsoft, BCE, Fujitsu and Deutsche Telekom, dedicated to promoting the global growth of electronic commerce and communications by contributing to solutions of the particular legal issues which arise from the cross-border nature of the Internet and electronic networks. ILPF provides information, calling upon the legal, business and technical expertise of its member companies and other companies, from governments and intergovernmental organizations and from the practice of law around the world.

What are ILPF's key issues?

ILPF addresses issues of concern through working groups consisting of representatives from member organizations. It currently has four such working groups:

- Working Group on Jurisdiction
- Working Group on Electronic Authentication (a combination of the original Working Groups on Certificate Authorities and on Digital Signatures)
- Working Group on Content Regulation and Intermediary Liability
- Working Group on Self-Regulation.

---

8 http://www.gbde.org

9 http://www.ilpf.org

c) Consumers International[10]

What is Consumers International?

Founded in 1960, Consumers International supports, links and represents consumer groups and agencies all over the world. It has a membership of more than 260 organizations in almost 120 countries. It strives to promote a fairer society through defending the rights of all consumers, including the poor, marginalized and disadvantaged.

How is Consumers International involved in e-commerce?

Consumers International identified e-commerce as an issue of concern in 1998, calling on governments to establish global protections for consumers who are engaged in e-commerce. Since that time, the organization has played a leading role in crafting e-commerce consumer protection policy and in working to establish effective and fair dispute resolution processes.

d) Electronic Privacy Information Centre (EPIC)[11]

What is EPIC?

EPIC is a public interest research centre in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment of the United States Constitution and constitutional values.

In what cases has EPIC become involved?

EPIC acts predominantly on cases of interest to the United States. It has appeared on some of the Internet and e-commerce's leading-edge cases including the Scarfo case on key stroke monitoring, the Microsoft antitrust case and the case challenging the constitutionality of the Children's Online Protection Act. EPIC has also played an important role in global awareness campaigns involving privacy issues.

e) International Chamber of Commerce (ICC)[12]

What is ICC?

The International Chamber of Commerce is a world business organization that speaks on behalf of enterprises from all sectors in every part of the world. ICC promotes an open international trade and investment system and the market economy. It often works with its member companies to develop global business codes of conduct. It also provides essential services, foremost among them the ICC International Court of Arbitration, a leading arbitral institution. Within a year of the creation of the United Nations, ICC was granted consultative status at the highest level with the United Nations and its specialized agencies.

How is ICC involved in e-commerce law and policy?

ICC is involved in e-commerce law issues on several fronts. Given its leading role in dispute resolution, ICC has shown a keen interest in developing dispute resolution for both B2C and B2B e-commerce. It has adapted for e-commerce its leading international trade rules, such as the Incoterms and the Uniform Rules for Documentary Credits (UCP 500). The organization has also become involved in jurisdictional negotiations, privacy and electronic contracting.

---

10 http://www.consumersinternational.org

11 http://www.epic.org

12 http://www.iccweb.org

III E-COMMERCE LAWS

(i) UNCITRAL MODEL LAW ON ELECTRONIC COMMERCE

1 Origins

The Model Law, adopted in 1996, is intended to facilitate the use of modern means of communication and storage of information, such as electronic data interchange (EDI), electronic mail and telecopy, with or without the use of such support as the Internet. It is based on the establishment of a functional equivalent for paper-based concepts such as "writing", "signature" and "original".

2 Key provisions

How does the Model Law treat electronic transactions?

The key principle underlying the Model Law is the concept of "electronic equivalence," found in Article Five. Although the Model Law does not deem electronic communications valid (just as with paper documents, legal validity depends upon more than a document's form), it provides that information or documents will not be denied legal effect or enforceability solely because they are in electronic format.

How does the Model Law achieve electronic equivalence?

A series of functional equivalency rules specify what conditions must be met for an electronic communication to constitute a legally effective substitute for a conventional, paper-based communication. For example, Article Six provides that a legal requirement to provide information or a document sent "in writing" is satisfied by its electronic equivalent if it is in a form that can be subsequently accessed and used by the recipient.

Article Eight states that electronic documents will satisfy a legal requirement for "original" documents if there is a reliable assurance as to the integrity of the information and that the information is capable of being displayed to the person to whom it is to be presented. The question of whether an assurance is reliable is to be determined in the light of all the circumstances, including the purpose for which the document was created.

How is the integrity of the information determined?

Article Eight also addresses this issue. It provides that the criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change that arises in the normal course of communication, storage and display.

Does the Model Law address the admissibility and evidential weight of electronic communication?

Yes. Article Nine creates an electronic equivalence standard for evidentiary purposes as it provides that evidentiary rules shall not deny the admissibility of an electronic communication solely on the grounds that it is in electronic form.

What conditions does the Model Law set for data retention?

Article Ten addresses the issue of data retention. It provides that data retention requirements are met where the information contained with the electronic message is accessible so as to be usable for subsequent reference, the message itself is retained in the format in which it was generated and any information indicating origin, destination, date and time of the message is retained.

Does the Model Law address online contracts?

Yes. The most interesting section of the Model Law focuses on online contracts. Although thousands of contracts are entered into daily through the Internet, some sellers and consumers remain uncertain of the legal implications of clicking the "I agree" button on a website. Article Eleven of the Model Law removes any doubt that this popular form of online consent is valid by stipulating that unless the parties agree otherwise, an offer or acceptance of an offer can be expressed in electronic form.

3 National implementations

a) United States

Has the United States implemented the UNCITRAL Model Law at the national or state level?

Yes, both. Nevertheless, most of the activity initially occurred at the state level, with dozens of states using the Uniform Electronic Transaction Act (UETA), developed by the National Conference of Commissioners on Uniform State Law, as a model. When some state laws began to deviate from UETA, the United States Congress stepped in to create a uniform standard by enacting the Electronic Signatures in Global and National Commerce Act (E-SIGN) in 2000.

Are there any important differences between the UETA and the UNCITRAL Model Law?

Yes. First, UETA includes a consent provision that clarifies that the Act does not require a record or signature to be created, generated, sent, communicated, received, stored or otherwise processed or used by electronic means or in electronic form. Second, it facilitates the use of electronic signatures for notarization of documents. Third, Section 10 of UETA features rules for where a change or error in an electronic record occurs in a transmission between parties to a transaction.

How does E-SIGN co-exist with the state law versions of UETA?

E-SIGN specifically provides that if there is a modification to UETA, state statutes that incorporate that modification supersede the federal statute.

What are some of the provisions that distinguish E-SIGN from UETA?

First, E-SIGN includes strong consumer consent provisions. These provisions require that consumers affirmatively consent before electronic records can be used to provide them with information that, under other law, must be provided or made available to them in writing. Consumers are also granted the right to withdraw their consent.

Second, E-SIGN contains some fairly expansive provisions related to contracting by electronic agents. The statute provides that a contract may not be denied legal effect solely because its formation or creation involved one or more electronic agents, provided that the action of the electronic agent is "legally attributable" to the person to be bound.

b) European Union

Has the European Union addressed the issues found in the UNCITRAL Model Law?

Yes. The EU's Electronic Commerce Directive contains several articles that bear direct similarity to principles found in the Model Law. Although it falls to Member States to implement the directive into national law, the directive does have direct effect in those States that fail to enact e-commerce legislation in a timely manner.

How does the E-commerce directive treat electronic contracts?

Article 10 of the directive speaks to contracts concluded by electronic means. It provides that Member States shall ensure that their legal system allows contracts to be concluded by electronic means. In particular, Member States are warned not to create obstacles for the use of electronic contracts.

c) Canada

Has Canada implemented the UNCITRAL Model Law on e-commerce into national law?

Yes and no. Although the Model Law has not been enacted into federal law, with one exception all provinces and territories have enacted versions of a Canadian model based on the United Nations model.

What is the Canadian model law?

The Uniform Electronic Commerce Act (UECA), a project of the Uniform Law Conference of Canada (ULCC), obtained official approval in 1999, providing Canada with a legal model for electronic commerce transactions. The subject of more than two years of negotiation, UECA brought much needed certainty to the world of e-commerce. Based largely on the UNCITRAL Model Law, it clarifies issues such as the enforceability and formation of online contracts, the use of electronic agents in the contracting process and at what point an electronic contract is presumed sent and received.

Have all provinces and territories enacted the Canadian model into law?

Not quite. UECA has received widespread approval from Canadian provinces and territories. As of March 2002, all Canadian provinces, with the exception of Quebec, had enacted legislation based on the UECA model. In November 2001, Quebec enacted its own e-commerce legislation that departs from the UECA model.

d) Other countries

What other countries have enacted the UNCITRAL Model Law into national law?

Dozens of countries from virtually every continent worldwide have used the Model Law as the basis for establishing national e-commerce legislation.

In South America, **Colombia** passed the Electronic Commerce Law 527 in 1999, based on the 1996 UNCITRAL model law. It establishes the validity and admissibility for "data messages," as well as the enforceability of contracts that contain data messages. Additionally, it provides for the validity of digital signatures and delineates standards for the licensure of certification entities and for the issuance of certificates.

In Asia, **Thailand** also passed its own Electronic Commerce Law in 1999. It addresses electronic signatures along with all electronic communications.

In the Americas, **Bermuda** enacted the Electronic Transactions Act in 1999 to address the legal validity and enforceability of electronic signatures and records as well as their admissibility as evidence in any legal proceeding.

In Africa, **Tunisia** enacted the Electronic Exchanges and Electronic Commerce Law in 2000. Although the law addresses the general organization of electronic exchanges it also governs electronic contracts including the validity and execution liability that may arise from that form of contract.

(ii) UNCITRAL MODEL LAW ON ELECTRONIC SIGNATURES

1 Origins

When was the Model Law finalized?

The Model Law was approved by the UNCITRAL Working Group on Electronic Commerce at its thirty-seventh session, held at Vienna from 18 to 29 September 2000. It took effect in 2001.

2 Key provisions

What is the scope of the Model Law on electronic signatures?

Article One of the Model Law states that it applies where electronic signatures are used in the context of commercial activities. It does not override any rule of law intended for the protection of consumers.

How does the Model Law define "electronic signature?"

Article Two of the Model Law defines electronic signature as "data in electronic form in, affixed to, or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and indicate the signatory's approval of the information contained in the data message."

Does the Model Law also establish an electronic equivalence standard?

Yes. Article Six of the Model Law provides that where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used provided that the signature is as reliable as was appropriate for the purpose for which the data message was generated or communicated. The reliability is determined in the light of all the circumstances, including any relevant agreement.

When is an electronic signature considered reliable under the Model Law?

The Model Law treats an electronic signature as reliable provided that it meets four criteria. First, the signature creation data are linked solely to the signatory. Second, the signature creation data was under the sole control of the signatory. Third, any alteration of the electronic signature, made after signing, is detectable. Fourth, where the purpose of the signature is to provide assurance as to the integrity of the underlying information, any alteration of that information must be detectable.

What obligations does the Model Law place on users (signatories) of electronic signatures?

Article Eight of the Model Law provides that signatories must use reasonable care to avoid unauthorized use of their electronic signature. If they become aware that the security of their electronic signature has been compromised, they must notify any person that might be affected without delay.

What obligations does the Model Law place on parties that rely on electronic signatures?

Article 11 of the Model Law provides that a relying party will bear the legal consequences of its failure to take reasonable steps to verify the reliability of an electronic signature or to observe any limitations that may be placed on a certificate. A certificate is a data message that confirms a link between the signatory and the signatory creation data. It provides verification that the person who electronically signed a document is who they say they are.

What is a certification service provider?

A certification service provider is a person that issues certificates and may provide other services related to electronic signatures.

What requirements does the Model Law place on certification service providers?

Article Nine of the Model Law establishes several conduct requirements for certification service providers including:

- to act in accordance with States' policies and practices;
- to exercise reasonable care to ensure the accuracy of any information found on its certificates;
- to provide reasonably accessible means whereby parties relying on a certificate can confirm certain information pertaining to the certificate; and
- to utilize trustworthy systems.

How does a system meet the trustworthy standard?

Although the Model Law does not create firm standards, it does provide that the following factors should be considered when determining trustworthiness:

- Financial and human resources of the provider
- Quality of hardware and software systems
- Procedures for processing certificates.
- Availability of information to signatories and relying parties
- Regularity and extent of independent audits
- Regulation or licensing by government authorities.

(iii) EU DIRECTIVE ON E-SIGNATURES

What is the purpose of the EU Directive on E-signatures?

The purpose of this directive is to facilitate the use of electronic signatures and to contribute to their legal recognition. It establishes a legal framework for electronic signatures and certain certification services in order to ensure the proper functioning of the internal market.

Does the directive ensure that electronic signatures are legally valid?

Yes. It states that Member States must ensure that electronic signatures meet certain legal and technological standards to satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and that such signatures be admissible as evidence in legal proceedings.

Does the directive set rules for the potential liability of certificate authorities?

Yes. It provides that at a minimum, Member States must ensure that by issuing a certificate as a qualified certificate to the public or by guaranteeing such a certificate to the public a certification service provider is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate being accurate.

Does the directive contemplate electronic signatures certified by non-EU Member State authorities?

Yes. The directive provides that Member States shall ensure that certificates which are issued as qualified certificates to the public by a certification service-provider established in a non-EU country are recognized as legally equivalent to certificates issued by a certification-service provider established within the EU provided that the provider meets certain conditions.

Have any non-EU members worked toward obtaining certification?

Yes. Hungary adopted electronic signature legislation in May 2001. The law, which took effect in September 2001, is said to fully compliant with the EU principles. The Hungarian legislation creates two types of electronic signatures – a simple electronic signature and a qualified electronic signature. The legislation appoints the Minister of Education to administer future issues that may arise within the context of the certification of electronic signatures.

IV E-COMMERCE LEGAL ISSUES

(i) JURISDICTION AND APPLICABLE LAW

Are e-commerce and the Internet borderless?

The development of cyberlaw has long been shaped by the belief that the Internet is borderless. Many observers argue that without borders, the Internet is impervious to the real-space laws that mirror traditional geographic boundaries. Courts have generally accepted the vision of a borderless Internet as evidenced by their reluctance to even consider the possibility that geographic distinctions might be possible online. In *ALA v. Pataki*, for example, a 1997 United States case challenging a New York state law that sought to regulate obscene content found online, the court argued that "[t]he Internet is wholly insensitive to geographic distinctions. In almost every case, users of the Internet neither know nor care about the physical location of the Internet resources they access."

Although the court's view of the Internet may have been correct at the time, the Internet has not remained static. Providers of Internet content increasingly *do care* about the physical location of Internet resources and the users that access them, as do legislators and courts who may want real space limitations imposed on the online environment.

In the business world, Canada's JumpTV has garnered considerable publicity for its plans to use geographic identification technology to limit its Internet retransmission signal to Canadians. Other companies already using the technology for similar purposes include CinemaNow, a California-based online distributor of feature-length films that uses geographic identification technology to limit distribution of its films to ensure it is compliant with distribution-licence rules that vary by country.

How does applicable law differ from choice of forum?

Although occasionally discussed interchangeably, applicable law and choice of forum are distinct concepts that must both be addressed when addressing Internet jurisdiction concerns. Applicable law refers to which country's law will be applied to a particular dispute. While some contracts will specify which law governs should a dispute arise, where such a clause has not been included, it is left to the courts to determine which law should be applied.

Choice of forum refers to which court will decide a particular dispute. The majority of Internet jurisdiction cases address this latter issue, as courts struggle with the question of whether they can

assert jurisdiction over a particular dispute. Once the appropriate court has been identified, the court will then be asked to determine which law should be applied.

Are there international rules or treaties that govern Internet jurisdiction?

Not yet. The Hague Conference on Private International Law has been actively working toward developing an international convention on jurisdiction and the enforcement of judgements. If successful, the convention would address a range of issues including jurisdictional rules for consumer and business transactions.

What rule would the Hague Conference convention adopt for Internet jurisdiction?

As of March 2002, the Hague Conference convention approach was still subject to negotiation. Although delegates have succeeded in negotiating many aspects of the convention, the Internet issues have proven to be particularly difficult. The primary issue of contention surrounds whether to adopt a "country of origin" or "country of destination" jurisdictional approach to Internet consumer disputes.

The United States, alongside most business groups, support a "country of origin" approach under which jurisdiction would always rest with the jurisdiction of the seller in an online transaction. Most European countries, alongside consumer groups, meanwhile, support a "country of destination" approach that ensures that consumers can always sue in their home jurisdiction. The origin versus destination debate has polarized both groups, making it difficult to reach a compromise.

Are there alternatives to country of origin or country of destination being considered?

Yes. There has been some support voiced for a "targeting" approach that would allow consumers to sue in their home jurisdiction where sellers target their jurisdiction. This middle ground might allow businesses to confine their online activities (and thus their legal risk) to a limited number of jurisdictions, while ensuring that consumers retain the right to apply their local consumer protection laws to e-commerce transactions.

Has the European Union addressed Internet jurisdiction or applicable law issues?

Yes. The European Union has adopted several regulations that are relevant to the Internet jurisdiction issue. The primary source of law is the 1980 Rome Convention, which distinguishes between business and consumer contracts.

The Convention presupposes that most business transactions will include a governing law clause such that the parties may determine for themselves whose law will apply. Where the parties have neglected to include a governing law clause, the Convention provides that the law of the country most closely associated with the contract will apply.

Consumers are more likely to be able to rely on local law under the Rome Convention. It provides that where there is no governing law clause and the seller advertized its goods or services to the consumer, the law will be that where the consumer is resident. Moreover, even if there is a governing law clause, the Convention provides that such a clause will not exclude mandatory rules such as consumer protection regulations.

While the Rome Convention addresses which law applies, the 1968 Brussels Convention on Jurisdiction along with the 1998 Lugano Convention address which court may assert jurisdiction. The Brussels and Lugano Conventions provide consumers with similar protections since they are entitled to sue in either their resident jurisdiction or in that of the seller. In the case of business transactions, the Conventions stipulate that the parties may decide themselves by way of a contractual provision. If they fail to do so, a business may be sued in the State in which it is domiciled.

How have the courts addressed Internet jurisdiction issues?

Courts in the United States and around the world have been somewhat inconsistent in their treatment of Internet jurisdiction issues. Although some courts have been willing to assert jurisdiction to virtually any website accessible within their jurisdiction, others have adopted a more cautious approach that sets some limits on when a court will assert jurisdiction over a foreign or out-of-state entity whose ties to the jurisdiction are limited to the Internet. This latter approach is often referred to as the "Zippo test."

What is the Zippo test?

The Zippo test arose out of a Pennsylvania federal court case involving a trademark dispute over the zippo.com domain name. Zippo Manufacturing was a Pennsylvania-based manufacturer of the well-known "Zippo" brand of tobacco lighters. Zippo Dot Com was a California based Internet news service that used the domain name "Zippo.com" to provide access to Internet newsgroups. Dot Com's contacts with Pennsylvania occurred almost exclusively on the Internet since the company maintained no offices, employees or agents in the state. Dot Com had some success in attracting Pennsylvania subscribers. At the time of the action, approximately 3 000 or two per cent of its subscribers resided in that state. The issue before the court was one of personal jurisdiction arising out of a claim of trademark infringement and dilution.

Rather than using Internet analogies as the basis for its analysis, the Court focused on the prior, somewhat limited Internet case law, generating the following conclusion:

– "With this global revolution looming on the horizon, the development of the law concerning the permissible scope of personal jurisdiction based on Internet use is in its infant stages. The cases are scant. Nevertheless, our review of the available cases and materials reveals that the likelihood that personal jurisdiction can be constitutionally exercised is *directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet*. This sliding scale is consistent with well developed personal jurisdiction principles. At one end of the spectrum are situations where a defendant clearly does business over the Internet. If the defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction is proper. At the opposite end are situations where a defendant has simply posted information on an Internet website which is accessible to users in foreign jurisdictions. A passive website that does little more than make information available to those who are interested in it is not grounds for the exercise of personal jurisdiction. The middle ground is occupied by interactive websites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the website."

Although the Court may have conveniently interpreted some earlier cases to obtain its desired result, its critical finding was that the jurisdictional analysis in Internet cases should be based on, as the Court states, the nature and quality of the commercial activity conducted on the Internet. There was a strong argument that prior to *Zippo*, the jurisdictional analysis was based upon the mere use of the Internet itself, a finding that might easily produce a somewhat inappropriate analogy and lead to the subsequent application of legal doctrine unsuited to the circumstances. In the aftermath of the *Zippo* decision, in which the Court used its analysis to find that jurisdiction was proper due to Dot Com's subscription sales to state residents, Internet legal analysis underwent a significant shift in perspective.

Have courts in other countries adopted the Zippo test?

Yes. Canadian courts signalled their approval of the *Zippo* approach in *Braintech Inc. v. Kostiuk*. This 1999 British Columbia Court of Appeal case, the first Canadian appellate-level decision to address the Internet jurisdiction issue, involved a series of allegedly defamatory messages posted on a stock chat site by a B.C.-resident. Braintech, a B.C.-based company, sued the poster in a Texas court, which awarded the company roughly $ 400 000 in damages.

When the company returned to B.C. to enforce the judgment, the B.C. courts examined the appropriateness of the Texas court's assertion of jurisdiction over the dispute. Adopting the passive versus active test by citing directly from the *Zippo* case, the B.C. Court of Appeal ruled that the Texas court had improperly asserted its jurisdiction. It argued that the postings were passive in nature and thus provided insufficient grounds to grant the Texas court authority over the case. Braintech's appeal to the Canadian Supreme Court was denied in early March 2000.

Is the Zippo test still valid?

Despite the widespread acceptance of the *Zippo* doctrine (and indeed the export of the test to other countries including Canada), cracks in the test began to appear late in 1999. In fact, closer examination of the case law indicates that by 2001, many courts were no longer strictly applying the *Zippo* standard but rather were using other criteria to determine when assertion of jurisdiction was appropriate.

Numerous judgments reflect that courts in the United States moved toward a broader, effects-based approach when deciding whether or not to assert jurisdiction in the Internet context. Under this new approach, rather than examining the specific characteristics of a website and its potential impact, courts focused their analysis on the actual effects that the website had in the jurisdiction. Indeed, courts are now relying increasingly on the effects doctrine that was established by the United States Supreme Court in *Calder v. Jones*. That doctrine holds that a court may assert jurisdiction over an out-of-state entity where the effects of that entity's activities are felt within the court's jurisdiction.

What was the controversial French case involving Yahoo.com about?

Few Internet law cases have attracted as much attention as the Yahoo! France case, in which a French judge asserted jurisdiction over the world's most popular website, ordering it to implement technical or access control measures blocking auctions featuring Nazi memorabilia hosted on the California-based Yahoo.com site from French residents. Yahoo! reacted with alarm, maintaining that the French court could not properly assert jurisdiction over the matter. It noted that the company maintains dozens of country-specific websites, including a Yahoo.fr site customized for France that is free of Nazi-related content. These country-specific sites target the local population in their local language and endeavour to comply with all local laws and regulations.

The company went on to argue that its flagship site, Yahoo.com, was targeted primarily toward a United States audience. Since Nazi memorabilia are protected under United States free speech laws, the auctions were entirely lawful there. Moreover, the Yahoo.com site featured a terms of use agreement which stipulated that the site was governed by United States law. Since the Yahoo.com site was not intended for a French audience and users implicitly agreed that United States law would be binding, the company felt confident that a French judge could not credibly assert jurisdiction over the site.

Judge Jean-Jacques Gomez of the Court of First Instance of Paris disagreed, ruling that he was entitled to assert jurisdiction over the dispute since the content found on the Yahoo.com site was available to French residents and was unlawful under French law. Before issuing his final order, the judge commissioned an international panel to determine whether the technological means were

available to allow Yahoo! to comply with an order to keep the prohibited content away from French residents. The panel reported that though such technologies were imperfect, they could accurately identify French Internet users at least 70 per cent of the time.

Based on that analysis, Judge Gomez ordered Yahoo! to ensure that French residents could not access content on the site that violated French law. Failure to comply with the order would result in fines of USD 13 000 per day. Soon after, Yahoo! removed the controversial content from its site, but the company proceeded to contest the validity of the French court's order in a California court.

(ii) CONSUMER ISSUES

Why are online consumer protections different from those offline?

Unlike the offline environment, where consumers enter a store, inspect potential purchases and judge for themselves the trustworthiness of a seller, the online world does not provide the same opportunity to use a "buyer's instinct." Rather, many consumers are forced to proceed on faith, knowing precious little about the seller to whom they are entrusting their credit card data.

What are the OECD Consumer Protection Guidelines?

OECD's Council approved the Guidelines for Consumer Protection in the Context of Electronic Commerce in December 1999. These are designed to help ensure that consumers are no less protected when shopping online than they are when they buy from their local store or order from a catalogue. The guidelines establish the core characteristics of effective consumer protection for online business-to-consumer transactions, thereby eliminating some of the uncertainties that both consumers and businesses encounter when buying and selling online.

What general principles are found in the OECD Consumer Protection Guidelines?

The guidelines feature eight categories of general principles. They are:

- Transparent and effective protection – Consumers who participate in electronic commerce should be afforded transparent and effective consumer protection that is not less than the level of protection afforded in other forms of commerce.
- Fair Business, Advertising and Marketing Practices – Businesses engaged in electronic commerce should pay due regard to the interests of consumers and act in accordance with fair business, advertizing and marketing practices.
- Online Disclosures – Clear and obvious disclosures. A complete description follows.
- Confirmation Process – To avoid ambiguity concerning the consumer's intent to make a purchase, the consumer should be able, before concluding the purchase, to identify precisely the goods or services he or she wishes to purchase; identify and correct any errors or modify the order; express an informed and deliberate consent to the purchase; and retain a complete and accurate record of the transaction.
- Payment – Consumers should be provided with easy-to-use, secure payment mechanisms and information on the level of security such mechanisms afford.
- Dispute Resolution – Consumers should be provided meaningful access to fair and timely alternative dispute resolution and redress without undue cost or burden.
- Privacy – Business-to-consumer electronic commerce should be conducted in accordance with the recognized privacy principles set out in the OECD Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data (1980) and taking into account the OECD Ministerial Declaration on the Protection of Privacy on Global Networks (1998), to provide appropriate and effective protection for consumers.

- Education and Awareness – Governments, business and consumer representatives should work together to educate consumers about electronic commerce, to foster informed decision-making by consumers participating in electronic commerce and to increase business and consumer awareness of the consumer protection framework that applies to their online activities.

What online disclosures do the guidelines recommend?

The guidelines prescribe three types of online information disclosures. First, information about the business including identification of the business, its legal name, address, contact information and government registration or licence numbers. Second, sufficient information about the goods or services to enable consumers to make an informed decision about whether or not to enter into the transaction. Third, information about the transaction including terms, conditions and costs associated with the transaction. This may include making the information available in multiple languages, an itemization of costs, terms of delivery, as well as details on any limitations or warranties.

What consumer protection measures has the EU adopted that are particularly relevant to consumer e-commerce transactions?

The 1997 EU Distance Selling Directive, which was to be implemented by all Member States by May 2000, is particularly important from an e-commerce perspective. The directive mandates that consumers be provided with the following information before the conclusion of any distance contract:

a) the identity of the supplier and, in the case of contracts requiring payment in advance, his address;

b) the main characteristics of the goods or services;

c) the price of the goods or services including all taxes;

d) delivery costs, where appropriate;

e) the arrangements for payment, delivery or performance;

f) the existence of a right of withdrawal;

g) the cost of using the means of distance communication, where it is calculated other than at the basic rate;

h) the period for which the offer or the price remains valid; and

i) where appropriate, the minimum duration of the contract in the case of contracts for the supply of products or services to be performed permanently or recurrently.

Does the directive provide consumers with the right to withdraw from otherwise valid distance contracts?

Yes. Article Six of the directive provides that consumers have a period of at least seven working days in which to withdraw from a distance contract without penalty and without cause. The only charge that may be made to the consumer is the direct cost of returning the goods.

Does the directive require the supplier to complete the transaction within a given time frame?

Yes. Article Seven of the directive requires the supplier to execute the order within a maximum of 30 days from the day following that on which the consumer forwarded their order to the supplier.

(iii) TAXATION

Can countries tax e-commerce sales?

Since countries and states frequently rely on sales taxes as an important source of revenue, increasing sales on the Internet raise important taxation policy considerations. Unless the transaction takes place between a buyer and a seller residing in the same taxing jurisdiction, collection of sales tax rarely, if ever, occurs. Sensing that the Internet could cause tax dollars to be lost, some countries and states have begun to consider enacting Internet taxes. Opposition to such schemes is fierce, however, as it is feared that such taxes would severely dampen the growth of electronic commerce.

Proponents of a tax-free Internet fear that governments view the Internet as a lucrative new source of revenue and will rush to impose new taxes on transactions taking place within their jurisdiction. Given the Internet's distinctly non-geographic design, collection of new taxes would pose significant enforcement challenges since it is frequently unclear precisely where a transaction occurs when it is conducted online. Moreover, consumers and businesses might be dissuaded from embracing the Internet's commercial potential due to concerns with compliance and cost.

Why is the concept of a "permanent establishment" relevant?

The issue of a permanent establishment in an e-commerce context is both complicated and critically important from a tax policy perspective. Many states and countries use the existence of a permanent establishment as the basis for their right to levy corporate income or sales taxes. The definition of permanent establishment for e-commerce purposes will therefore be a key determinant for whether a country may tax an online business.

How does OECD propose to define a permanent establishment within the e-commerce context?

OECD has issued guidance on when a computer server might be considered a permanent establishment for taxation purposes. The guidance notes that computer equipment at a given location may only constitute a permanent establishment if it meets the requirement of being fixed. In the case of a server, what is relevant is not the possibility of the server being moved, but whether it is in fact moved. In order to constitute a fixed place of business, a server will need to be located at a certain place for a sufficient period of time.

Moreover, the guidelines also provide that where an enterprise operates computer equipment at a particular location, a permanent establishment may exist even though no personnel of that enterprise are required at that location for the operation of the equipment. The presence of personnel is not necessary to consider that an enterprise wholly or partly carries on its business at a location.

While this guidance suggests that businesses may increasingly find themselves deemed to have a permanent establishment in multiple jurisdictions, there are some important limitations. For example, the guidelines are careful to note that retaining an Internet service provider to host a website does not, on its own, constitute the creation of a permanent establishment.

What position has the United States adopted on e-commerce taxation?

The United States has assumed a leading role as a key proponent of a tax-free Internet. In 1998, the United States Congress passed the Internet Tax Freedom Act, which established a three-year moratorium on both Internet access taxes as well as new Internet taxes. That policy came under fire in 2001 when policy makers considered a permanent extension to the moratorium. Although most federal officials supported the moratorium, many state and local officials feared that revenue losses would be substantial and began to raise the prospect of new Internet taxation schemes. The law was temporarily allowed to lapse, though an extension was subsequently negotiated.

Has the European Union established a bit tax for Internet downloads?

No. Early European proposals focused on a "bit tax" which would levy tax based on the amount of digital content downloaded. Critics pointed out that the size of download bore little relation to the value of the downloaded content and thus the tax scheme was inherently unfair. The proposal was eventually abandoned.

Does the European Union apply value-added tax (VAT) to online purchases from non-member country merchants?

Not yet, but it has announced its intention to do so by 2003. In early 2002, it approved a plan that would impose VAT for all online purchases. The EU believes this will create a level-playing field between vendors located in EU member countries who already collect VAT and those located outside the EU which do not. Under the plan, vendors located outside the EU who sell goods or services to EU residents will be required to register for VAT collection. The proposal has yielded condemnation from United States e-commerce businesses, which argue that the plan will harm the development of e-commerce throughout Europe and place an unfair obligation on non-European businesses.

(iv) PRIVACY

What are the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data?

The OECD privacy guidelines were created in 1980, well before the Internet boom and the emergence of e-commerce. Although more than 20 years old, the principles found in the guidelines continue to serve as the basis for most privacy initiatives worldwide.

What are the principles found in the OECD privacy guidelines?

The guidelines feature eight privacy principles:

1) Collection Limitation Principle

There should be limits to the collection of personal data. Such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2) Data Quality Principle

Personal data should be relevant to the purposes for which they are to be used. To the extent necessary for those purposes, data should be accurate, complete and kept up-to-date.

3) Purpose Specification Principle

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified at each occasion of change of purpose.

4) Use Limitation Principle

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the data quality principle except with the consent of the data subject; or by the authority of law.

5) Security Safeguards Principle

Personal data should be protected by reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification or disclosure of data.

6) Openness Principle

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data and the main purposes of their use, as well as the identity and usual residence of the data controller.

7) Individual Participation Principle

An individual should have the right to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him or her. An individual should have the right to receive that data and to challenge it if incorrect.

8) Accountability Principle

A data controller should be accountable for complying with measures that give effect to the principles stated above.

What is the EU Data Protection Directive?

The EU Data Protection directive was enacted in 1995 with Member States required to implement its provisions by October 1998. The directive's primary goal was to create a common European standard of privacy protection for the processing of personal data. The directive establishes a series of protections for individuals including the right to know why information is being collected and how the information will be used and disclosed. Individuals are also entitled to compensation for any damages that arise from failure to abide by the directive's requirements.

Is the Data Protection Directive applicable outside the EU?

Although the directive does not have direct effect outside the EU, it does contain an "adequacy clause" that has had a significant effect on the privacy law frameworks of non-EU countries. Article 25 provides that Member States must ensure that the transfer of personal data to non-EU countries takes place only if the non-EU country provides an adequate level of privacy protection.

How is this adequacy standard determined? Which countries have obtained EU approval for their privacy law frameworks?

Article 25 of the directive provides that the adequacy of the level of protection of personal data provided by a non-EU country shall be assessed in the light of all circumstances surrounding the data transfer, with particular consideration given to the nature of the data, as well as the purpose and duration of the data processing. As of March 2002, only Switzerland, Hungary and Canada had obtained EU approval for their privacy law frameworks.

Has Hungary enacted data privacy protection law?

Yes. Hungary enacted the Protection of Personal Data and the Public Interest Act in 1992. The purpose of the Act is to guarantee personal control over personal information. Much like the OECD guidelines, the Hungarian privacy law contains provisions that address the need to provide a specific purpose for data collection, rights of access to personal data, limitations on data transfers outside the country and the possibility of compensation where damage occurs.

What are the origins of Canada's private sector privacy legislation?Hb

The Personal Information Protection and Electronic Documents Act received Royal Assent in April 2000 and came into force on 1 January 2001. The Act establishes the rules for the protection and management of personal information that is collected, used or disclosed by private organizations during the course of commercial activities.

The fundamental tenets of the Act are:

i) organizations that collect, use or disclose personal information during the course of commercial activity must do so only with the prior knowledge and consent of the affected individuals; and

ii) such information may only be used for the purposes for which consent has been given.

The Act limits the collection, use and disclosure of personal information to purposes that a "reasonable person" would consider appropriate in the circumstances. It will apply to any private enterprise that collects, uses or discloses personal information and will not be limited to businesses engaging in e-commerce or the electronic collection of data. Thus, information collected in a ballot box located in a supermarket will enjoy the same protection as personal data collected through online surveys.

The Act is based on the fair information principles set out in the Canadian Standards Association's Model Privacy Code for the Protection of Personal Information (the "CSA Code"). The CSA Code is the product of a collaborative effort between businesses, governments, academics, consumer associations and other privacy stakeholders. The principles of the CSA Code are incorporated (with some modifications) into the Act as Schedule 1 and private sector organizations must adhere to them.

Has the United States enacted private sector privacy legislation?

The United States does not have comprehensive privacy legislation at the federal level. It has enacted a series of industry or data-specific privacy laws. These include:

- the Gramm-Leach-Bliley Act, which covers financial privacy;
- the Health Insurance Portability and Accountability Act, which covers health privacy;
- the Children's Online Privacy Protection Act, which provides children under the age of 13 with special privacy protections.

What is the EU – United States Safe Harbour Agreement?

In addition to the industry or data-specific privacy laws referred to above, the United States and the European Union have entered into a safe harbour agreement that is designed to ensure the free flow of personal data between the two parties. Without such an agreement, there were fears that the EU might begin to block data transfers to the United States on the grounds that it did not meet the Data Protection Directive's adequacy standard.

Although the Safe Harbour agreement has been in place since 2000 and was thought to provide an effective solution bridging the United States – European privacy divide, United States support for the agreement has been tepid, at best. President George W. Bush has publicly questioned the agreement, noting his concern with the perception that the European Union is dictating United States privacy policy. With the notable exceptions of Microsoft and Intel, United States corporations have thus far been slow in signing up for the Safe Harbour Agreement.

(v) INTERNET GOVERNANCE AND DOMAIN NAMES

1 Domain name dispute resolution

Who ran the Internet's domain name system before the creation of ICANN?

The Internet Assigned Numbers Authority (IANA), headed by the late Jon Postel, initially managed the Domain Name System (DNS). Growing demand from businesses and individuals, however, together with the increasing administrative burden of maintaining the system resulted in changes to

the system in 1992. That year, the United States Government granted Network Solutions, Inc. (NSI) the exclusive right to register three generic top-level domain names (gTLDs) -- dot-com, dot-net and dot-org. As part of the registration right, which was initially scheduled to last for five years, NSI was charged with managerial responsibility for the maintenance of DNS.

With the first agreement set to expire in 1997, the United States Department of Commerce granted NSI a two-year extension. In return, NSI agreed to create a Shared Registry System that would allow competing companies to register dot-com, dot-org and dot-net domains. Moreover, once a competitive registrar system was established, NSI agreed to apply for accreditation through the same process as other registrars, thereby relinquishing its competitive advantage over the domain name registry market.

Was there a domain name dispute resolution process before the creation of the ICANN UDRP?

NSI did not have a formal dispute resolution mechanism to address domain name disputes when it took over the registry responsibilities from IANA. As disputes began to mount, NSI recognized the need for a dispute resolution policy. Early efforts, however, became a source of frustration for trademark owners and domain name registrants alike since the dispute policies focused primarily on protecting NSI from liability.

Prior to 1995, NSI maintained that domain name registrants bore the responsibility for ensuring that their domain name did not infringe upon any trademark rights, but otherwise did not provide a formal dispute resolution policy. NSI released its first formal domain name dispute policy in July 1995. It allowed trademark owners to challenge the registration of a domain name by presenting NSI with evidence that the domain name infringed upon its trademark rights. The policy required the trademark holder to present evidence that its trademark was identical to the registered domain name. The domain name registrant could successfully defend its right to the domain by presenting a valid trademark of its own. If it was unable to produce evidence of a registered trademark, NSI would allow the domain name registrant to retain the domain for 90 days as part of a transition process. If the domain name registrant refused to accept an alternative domain, NSI would place the domain "on hold" so that neither party could use it.

NSI issued its first amendment to the policy in November 1995. The revised policy addressed situations where the domain name registration pre-dated the issuance of a trademark. In those situations, the domain name registrant was entitled to keep the domain, provided that it agreed to post a bond to indemnify NSI from any liability.

NSI revised its dispute resolution policy yet again in September 1996. The new policy required trademark owners to notify domain name registrants of their legal claim before commencing a dispute resolution action. Moreover, the policy established limitations on the domain name registrants' defense of a competing trademark by requiring that the trademark be issued prior to the commencement of the dispute resolution action. This latter change was needed after domain name registrants began obtaining quick trademark registrations from Tunisia.

NSI revised its dispute resolution policy for the final time in February 1998. That revision enabled trademark owners to place domain names "on hold" pending the resolution of the dispute. The domain name registrant, if challenged, could prevent the domain name from being placed on hold by submitting evidence that established that (1) the domain name was registered before the complainant's trademark or (2) the domain name holder owned a competing trademark in the domain name.

How was the ICANN UDRP created?

As the number of domain name lawsuits mushroomed and concerns over the stability of DNS increased, the National Telecommunications and Information Administration (NTIA), an agency of the United States Department of Commerce, issued a draft discussion paper in February 1998 titled "A Proposal to Improve Technical Management of Internet Names and Addresses", better known as the "Green Paper." Following the Green Paper consultation, a final report entitled "Management of Internet Names and Addresses" or the "White Paper" was published by NTIA in June 1998. A key concern expressed during the Green Paper public consultations was the fear that the United States would seek to impose United States trademark law on the Internet for the resolution of domain name disputes.

In an attempt to alleviate this concern, the White Paper committed to a WIPO-led, international process to develop recommendations for a uniform approach to resolving trademark and domain name disputes. WIPO published its first Request for Comments (RFC-1) in July 1998, followed soon after by two further Requests (RFC-2 and RFC-3) calling for public consultation. WIPO released its final report in April 1999. Using the WIPO final report and the White paper as its guide, ICANN moved quickly to draft a policy to address cybersquatting and related issues. Only months after the completion of the WIPO consultation, the ICANN Board of Directors approved the Uniform Domain-Name Dispute – Resolution Policy (UDRP) and its accompanying rules on 24 October 1999.

Who administers domain name disputes?

While ICANN establishes the policies pertaining to the UDRP, administration of the dispute resolution process is largely "outsourced" to several accredited dispute resolution providers. As of April 2002, there were five such providers – the World Intellectual Property Organization (Switzerland), the National Arbitration Forum (United States), eResolution (Canada), the Asian Domain Name Dispute Resolution Centre (China) and the CPR Institute for Dispute Resolution (United States). The arbitration providers provide full case management services including case intake, panelist assignment and publication of decisions.

Is a domain name registrant required to participate in the ICANN UDRP process?

Yes. Domain name registrants are required to submit to a mandatory administrative proceeding conducted by a dispute-resolution service provider approved by ICANN where a complainant asserts that:

1) the domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; and

2) the registrant has no rights or legitimate interests in respect of the domain name; and

3) the domain name has been registered and is being used in bad faith.

To succeed, the complainant must prove that all three elements are present.

What constitutes bad faith registration and use of a domain name?

The policy provides some guidance as to what constitutes evidence of bad faith registration and use of a domain name. They include:

1) circumstances indicating that the registrant has acquired the domain name primarily for the purpose of selling, renting or otherwise transferring it to the complainant who is the owner of the trademark or service mark, or to a competitor of the complainant, for valuable consideration in excess of "out-of-pocket" costs directly related to the domain name; or

2) the registrant has registered the domain name in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name, provided that a pattern of such conduct is evidenced; or

3) the domain name has been registered primarily for the purpose of disrupting the business of a competitor; or

4) the domain name has been registered primarily for commercial gain through creating a likelihood of confusion.

How do domain name holders prove that they have a legitimate interest in the domain name?

A domain name holder can demonstrate rights or a legitimate interest in a domain name by presenting evidence that:

1) before any notice to the respondent of the dispute, the respondent used or prepared to use the domain name or a name corresponding to the domain name in connection with a bona fide offering of goods or services;

2) the respondent has been commonly known by the domain name, even if no trademark or service mark rights have been acquired;

3) legitimate non-commercial or fair use of the domain name, without intent to divert consumers or tarnish the trademark or service mark for commercial gain, is being made.

What is the process for an ICANN UDRP complaint? How are the arbitration panelists determined?

A proceeding commences when the complainant submits a complaint to an ICANN approved dispute resolution service provider of their choosing. The complainant must specify whether the dispute is to be decided by a single-member or three-member panel. The fee for a single-member panel is paid entirely by the complainant. In the event that a three-member panel is requested, the complainant must submit names and contacts of three candidates from a roster of any ICANN-approved provider to serve as one of the panelists.

Following a compliance review, the provider forwards the complaint to the respondent.

The respondent must submit a response to the provider within 20 days of commencement of the proceeding. If no response is submitted, the panel decides the case based solely upon the evidence furnished by the complainant.

Even if the complainant has requested a single-member panel, the respondent has the right to have the dispute decided by a three-member panel instead. If either the complainant or respondent requests a three-member panel, the respondent must provide the names and contact details of three candidates to serve as one of the panelists, which can also be drawn from any ICANN-approved provider's roster. Where the complainant has elected to have the dispute decided by a single-member panel and the respondent requests a three-member panel, the respondent is required to pay one-half of the applicable fee for a three-member panel.

If the complainant requests a single-member panel and the respondent does not object, the provider alone assigns a single panelist from its roster to the case. If a three-member panel is selected, one panelist is selected from the list of candidates provided by each of the complainant and the respondent. The third panelist is appointed by the provider from a list of five candidates submitted by the provider to the parties, the selection from among the five being "made in a manner that reasonably balances the preferences of both Parties". The typical approach is to allow each party to strike out up to two names from the list of five.

2 ccTLD domain name dispute resolution

What is a ccTLD?

A ccTLD is a country-code top level domain. Unlike gTLDs (generic top level domains such as dot-com, dot-net and dot-org), hundreds of countries have their own domain name suffix. Popular ccTLDs include dot-uk (United Kingdom), dot-fr (France), dot-jp (Japan), dot-sg (Singapore), dot-au (Australia), dot-ca (Canada) and dot-br (Brazil). Often ccTLDs have their own registration rules distinct from those found for gTLDs.

Do ccTLDs have domain name dispute resolution rules?

Many do. Although some simply use the ICANN UDRP, some variations exist, particularly among the larger ccTLDS. Countries that use the ICANN UDRP as their national dispute resolution policy include Antigua, Belize, Ecuador, Laos People's Democratic Republic, Mexico, Namibia, Philippines, Romania and Venezuela.

How does India's dispute resolution policy differ from the ICANN UDRP?

The dispute resolution policy for India's dot-in domain, administered by the National Centre for Software Technology, is much broader in scope than either the ICANN UDRP or the ccTLD dispute resolution policies examined above. The dot-in process allows for disputes to be launched for the following reasons:

- the domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rightful claim;
- the domain name holder has no rights or legitimate interests in respect of the domain name;
- the domain name holder has sold/auctioned/transferred the domain name to a third party without the approval of the domain registrar;
- the domain name has not been used by the holder for over one year;
- a trademark holder alleges cybersquatting; and
- any other dispute, accepted by the domain registrar at his or her own discretion.

Once a complaint is launched, the domain registrar advises the domain name holder that a third party complaint has been filed with him giving details of the complaint (name, address, cause of complaint) through a registered letter as well as by e-mail. The domain name holder has 15 days from receipt of the notice to reply. An oral hearing may also be granted where both parties could present their cases arising out of such a dispute. A decision in writing is communicated by the domain registrar within one month of the final hearing.

How does Canada's dispute resolution policy differ from the ICANN UDRP?

The Canadian Internet Registration Authority (CIRA) approved the Canadian Dispute Resolution Policy (CDRP), a Canadianized version of the ICANN UDRP in October 2001. CDRP creates a domain name dispute resolution process for dot-ca domains that maintains many of the benefits of the ICANN UDRP, while at the same time addressing concerns about the ICANN UDRP's procedural fairness.

The policy differs in several material respects. First, unlike the ICANN UDRP, CDRP contains explicit provisions protecting good faith commercial usage of the domain, good faith non-commercial use of the domain such as websites engaged in criticism or news reporting and good faith use of a generic domain or a domain that references a geographical place. It is noteworthy that if the registrant demonstrates a legitimate interest in the domain, they are entitled to retain it even if the complainant has proven confusion and bad faith.

Second, unlike the ICANN UDRP, CDRP also contains a reverse hijacking clause with some teeth. The clause, which can be invoked where the complainant commences an action in bad faith, provides that the complainant can be ordered to pay up to $ 5 000 to the respondent to defray the costs incurred by the respondent in defending an action that should never have been brought in the first place.

Third, the CDRP Rules provide that all contested cases will be decided by three-member panels to be paid for by the complainant. Where the respondent fails to respond, the complainant has the option of requesting a less costly one-person panel.

How does the United Kingdom's dispute resolution policy differ from the ICANN UDRP?

The dot-uk dispute resolution procedure, administered by Nominet.uk, features several variations on the ICANN UDRP model. First, unlike the ICANN UDRP, which has its disputes addressed by third party arbitration providers such as WIPO and the National Arbitration Forum, Nominet.uk runs its own dispute resolution mechanism. Claims are launched directly with Nominet.uk, which proceeds to appoint an expert from its own roster to address the case.

Second, the dot-uk approach includes a mandatory mediation period, where the parties are required to work to negotiate a resolution to their dispute.

Third, unlike the ICANN UDRP and the CIRA CDRP, both of which reference bad faith by the domain name registrant, the dot-uk approach is premised on the presence of an "abusive registration." An abusive registration refers to a domain that was registered or otherwise acquired in a manner which, at the time when the registration or acquisition occurred, took unfair advantage of or was unfairly detrimental to the complainant's rights or has been used in a manner which took unfair advantage of or was unfairly detrimental to the complainant's rights.

Fourth, the dot-uk approach includes an appeal process whereby either party is permitted to appeal against a decision on the basis that the matter be re-examined on the facts or that the proper procedure has not been followed.

(vi) INTERMEDIARY LIABILITY ISSUES

Why has intermediary liability emerged as an important issue in recent years?

With governments and regulators generally frustrated with their lack of control over Internet activities, the potential for intermediaries, particularly Internet service providers, to carry out the regulatory function is viewed by some as a possible solution to Internet regulation. Particularly if one accepts the important role that technology can play in regulating Internet activity, then the role of the ISP becomes quite crucial. Although certain technologies can be implemented at the level of the individual browser or by an individual website, there are times when technological implementation falls to the ISP, if to anyone at all.

How has the United States' addressed the issue of intermediary liability?

The United States provides very broad protection from liability to ISPs and other intermediaries. Section 230 of the Communications Decency Act provides that no provider of an interactive computer service will be liable for any good faith action designed to restrict access to obscene content.

Has the European Union followed the United States' lead on this issue?

Yes. The EU Electronic Commerce directive also provides intermediaries with important protections from liability. The directive exempts intermediaries for liability for online content where the intermediary merely plays a passive role in transmitting and storing website information. An exemption is provided for network providers who act as "conduits" to the information but serve no editorial or controlling function in its creation or dissemination.

Attachment 5

WHITE PAPER INTERNET KOREA 2004

As the leading agency for national informatization, the National Computerization Agency provides policies and state of the art technology that will guide us to the successful construction of e-Korea.

White Paper Internet KOREA 2004

For more than ten the people of National Computerization Agency(NCA) have kept helping the public and private sector to make the best of new and exciting opportunities brought by information and communication technology all over the country.

National Computerization Agency
Ministry of Information and Communication

WHITE PAPER INTERNET KOREA 2004

As the leading agency for national informatization, the National Computerization Agency provides policies and state of the art technology that will guide us to the successful construction of e-Korea.

White Paper Internet KOREA 2004

For more than ten the people of National Computerization Agency(NCA) have kept helping the public and private sector to make the best of new and exciting opportunities brought by information and communication technology all over the country.

Message From the Minister

Korea has established a world-class information and communication infrastructure thanks to the joint efforts of the government and private sectors to build an IT powerhouse during the 1990s. Korea's leading infrastructure in the information and communication sector has enabled Korea to achieve unprecedented developments in all areas including political, economic, social and cultural spheres.

As of the end of 2003, 11.18 million households - more than 73% of the total number of households - subscribed to broadband Internet and 29.22 million people - 66% of the total population - had access to the Internet. According to the "ITU 2003 Internet Report," Korea ranks first in terms of broadband Internet penetration rate, has the third largest population of Internet users, and has the fourth highest PC penetration rate in the world. These statistics well illustrate Korea's firm standing as a leading Internet country.

The Internet has become an essential part of our everyday lives as more and more people rely on the Internet for their daily economic activities such as online shopping or Internet banking. Furthermore, an increasing number of parents are also depending on the Internet to provide education for their children.

For small-to mid-sized businesses, the Internet has become a useful tool in embracing information technology. The deployment of world-class Internet infrastructure in Korea has enabled SMEs, which lack capital and labor resources compared to their larger counterparts, to take advantage of the advance of IT technologies and readily introduce them to their own businesses.

On the other hand, the government has spurred its efforts to build an e-Government, thereby making more effective and interactive administrative process possible. The establishment of e-Government has allowed citizens to enjoy convenient public services online at the click of a mouse. The government has also created an environment to establish a Broadband convergence Network (BcN) since 2003 to prepare for a future ubiquitous society and is pushing ahead with plans to migrate to a new Internet protocol system, known as Internet Protocol version 6, or IPv6.

The 2004 Korea Internet White Paper will be useful in gaining a basic understanding of the present and future Internet environment of Korea. It provides a structured outlook on the future development of the Internet environment, trends in the Internet sector, and the current status of Internet usage by companies and citizens.

I congratulate the publication of the 2004 Korea Internet White Paper and extend by gratitude to everyone who participated in the publication of this white paper. Thank you.

July 2004
Daeje Chin, Ph.D.
Minister,
Ministry of Information and Communication

Preface

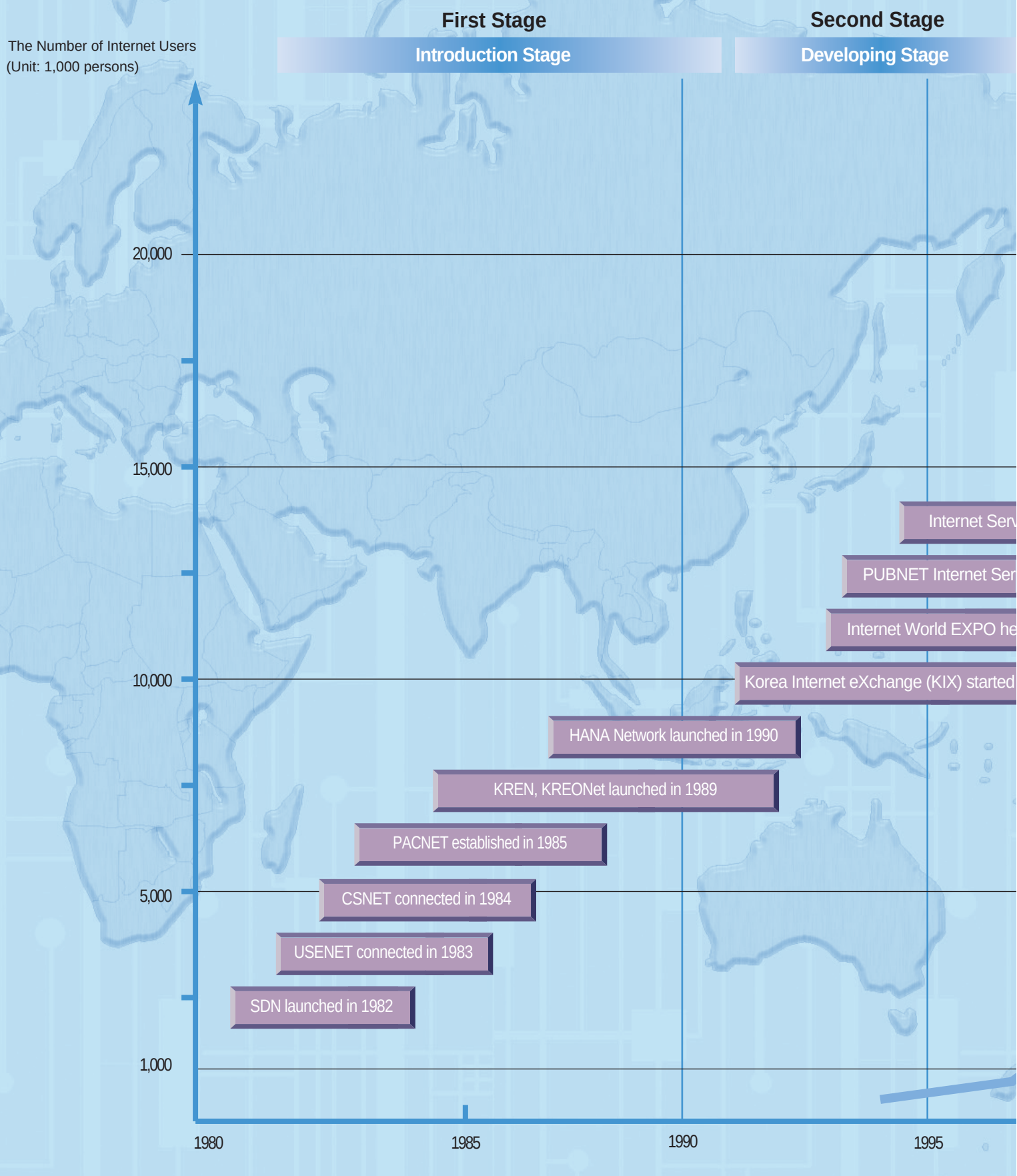
This year marks the 5th anniversary of the publication of the Korea Internet White Paper. After the Internet became commercially available in 1996, the Internet sector has faced its share of ups and downs; it has developed and diversified but also underwent the burst of the dotcom bubble. 2003 was a good year for the Internet sector as it saw great increases in profits despite the overall economic recession and gained the reputation as a genuine value-added industry. The number of Internet subscribers now reaches 30 million and full-scale movements to realize a ubiquitous environment integrating wired and wireless networks are being carried out.

The Internet sector experienced rapid growth in 2003 as can be seen through the growth of the online education market and the online game market that respectively amounted up to 100 billion won and 600 billion won. Information searching through large portals and new services such as blogs (web logs) have become popular while Internet financial services such as mobile banking and electronic money have started to become widely used. Such examples go to show that the Internet has become an essential part of our everyday lives. Additionally, the quality of wired and wireless telecommunication services went up and the development of handsets became more diverse. On the back of such developments, plans to establish a Broadband convergence Network (BcN) - the first step in realizing a ubiquitous environment in the future - and plans to provide and facilitate IPv6 - a next-generation Internet address system - were announced and various cooperative efforts to execute these plans are being carried out by the government, business and academia.

The 2004 Korea Internet White Paper provides diverse perspectives on domestic and international Internet issues and trends. I hope that the 2004 Korea Internet White Paper serves as useful material to people at home and abroad in providing insights on the current Internet issues and trends of Korea. I would like to thank everyone who contributed to the publication of the 2004 Korea Internet White Paper and would especially like to thank the compilation committee for their helpful advice and editing. Thank you.

July 2004
Suh, Sam Young
President
National Computerization Agency

Milestones in Korea's Internet Evolutio

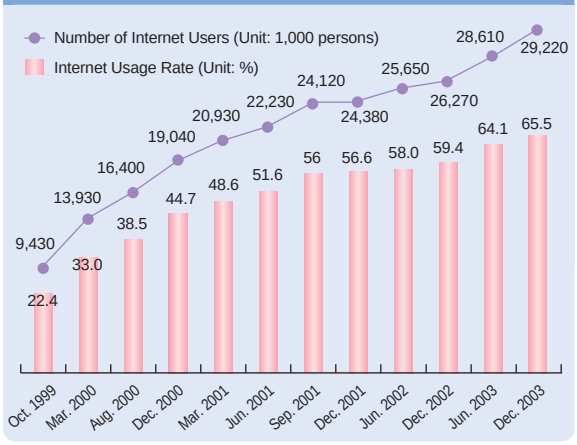


on


Third Stage
Expansion Stage
Law on Management of Internet Addresses and Resources Enacted in 2003
Broadband Internet subscribers reach 10 million in 2003
e-Government Service launched in 2002
Allocation of IPv6 addresses and launch of service in 2002
2 million internet-enabled mobile phones are sold in 2001
Second Stage of Broadband Internet Project Completed in 2000
Internet population over 10 million, KRNIC launched in 1999
vices over ATM launced in 1998
vices started in 1997
ld in 1996
in 1995
2000
2001
2002
2003
2004

Internet at a glance

Number of Internet Users



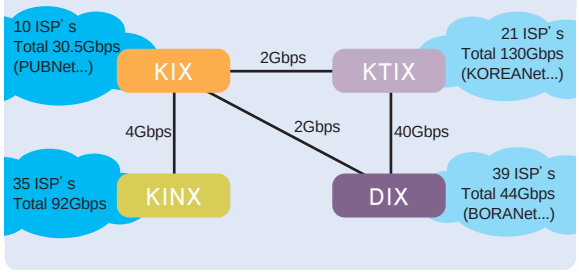
Source: KRNIC (December, 2003)

Number of Broadband Internet Subscribers (Unit: persons)

	xDSL	Cable Modem	Apartment LAN	Satellite Services
Number of Subscribers	6,435,955	3,828,166	909,542	4,836

Source: MIC (December, 2003)

IX Connectivity Diagram



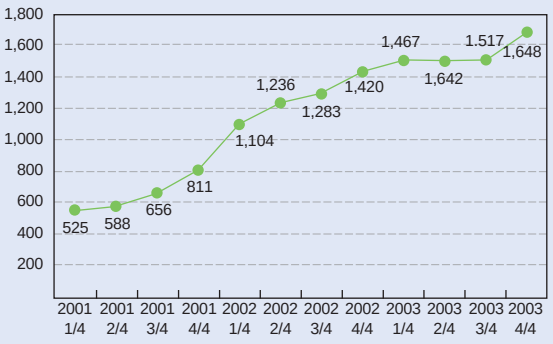
Source: NCA (December, 2003)

e-Commerce Market (Unit: ten billions of won, %)

	2002	2003		Change from Previous Year	
	3Q of 2002	3Q of 2003	Distribution Ratio		Rate of Change
Total Revenues from e-Commerce	44,926	55,833	100.0	10,907	24.3
Business to Business (B2B)	40,551	50,028	89.6	9,478	23.4
Business to Government (B2G)	2,990	4,195	7.5	1,204	40.3
Business to Consumer (B2C)	1,283	1,517	2.7	234	18.2
Other	102	92	0.2	-9	-9.3

Source: NSO (February, 2004)

Trend of B2C Market (Unit: ten billions of won)



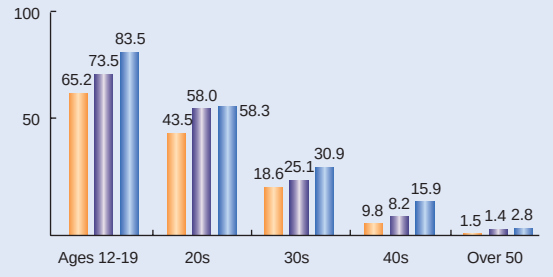
Source: NSO (February, 2004)

Frequently Used Mobile Contents (Unit: %)

Rank	Contents	Ratio
1	Bell Sounds	45.3
2	Games	12.5
3	Ringtones	9.2
4	Music	7.3
5	Characters	5.5
6	GIS	2.7
7	Sing Along	2.6
8	Traffic Information	2.3
9	Stock Information	1.4
10	Sports News	1.4

Source: Yonsei University HCI Lab (October, 2003)

Wireless Internet Users by Age (Unit: %)



Source: KRNIC (June, 2003)

Number of Wireless Internet Subscribers (Unit: persons)

Type		SK Telecom	KTF	LG Telecom	Total
By Delivery Method	WAP/ME Method	16,094,336	9,526,328	3,981,803	29,602,467
	ISMS Method	695,946	765,862	224,926	1,686,734
	Total	16,790,282	10,292,190	4,206,729	31,289,201
By Network	95A/B	2,715,902	2,939,543	1,363,857	7,019,302
	CDMA2000 1X *	14,074,380	7,352,647	2,842,872	24,269,899
	Total	16,790,282	10,292,190	4,206,729	31,289,201

* Note: CDMA 2000 1X subscribers include EV-DO subscribers (SK Telecom has 3,201,445 subscribers, and KTF has 696,199)

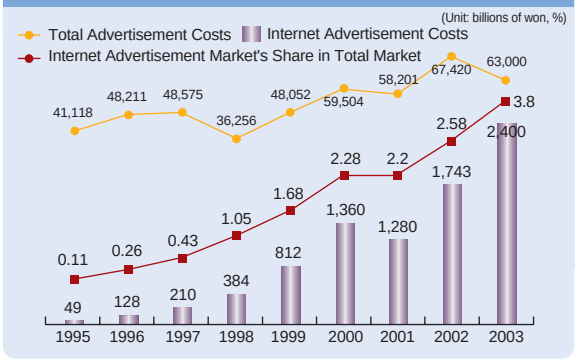
Source: MIC (November, 2003)

Best Selling Items among e-Retailers

Rank	Items	Ratio
1	Home Appliances/ Electronics/ Telecommunications	18.3
2	Computer Equipment and Peripherals	12.9
3	Daily Necessities/ Automobile Supplies	11.6
4	Clothing/ Fashion-related Goods	10.3
5	Travel and Reservation Services	7.4
6	Cosmetics/ Perfume	6.6
7	Others	5.9
8	Books	4.9
9	Sports/ Leisure Goods	3.9
10	Total	85.9

Source: NSO (December, 2003)

Internet Advertisement Market's Share in Total Advertisement Market

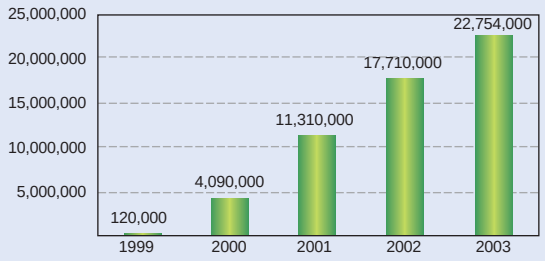


Note: Internet advertisement costs are the added sum of web and e-mail advertisement costs

Source: IMCK (December, 2003)

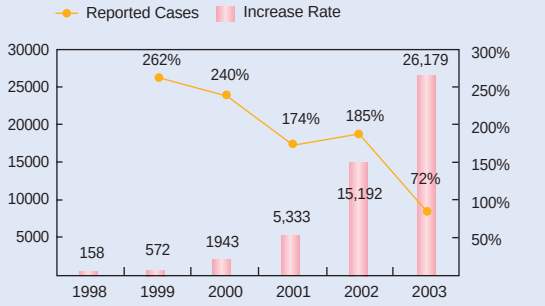
Number of Internet Banking Customers

(Unit: persons)



Source: BOK (December, 2003)

Trend of Computer Hacking Cases



Source: KPR (December, 2003)

Amount of Spam Mail (Daily Figure)

(Unit: reported cases)

	2001	2002	2003	Total
Request for Correction	165	2,853	7,918	10,936
Reported to ISP	-	42,555	26,281	68,836
Reported to the Ministry of Information and Communication	43	2,162	1,688	3,893
Reported to Investigative Bodies	-	-	516	516
Total	208	47,570	36,403	84,181

Source: KPR (December, 2003)

Cases of Spam Relay

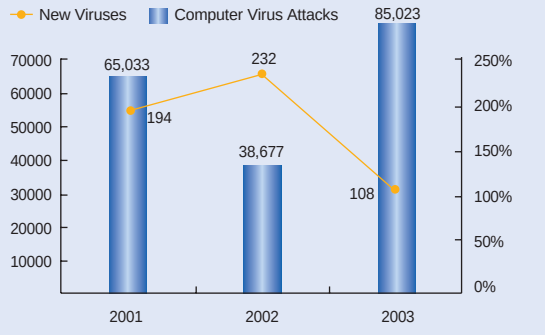
(Unit: reported cases)

	2001	2002	2003
Reported Cases	65	5,537	8,276

Note: Spam Relay is the act of sending spam mail by hiding one's actual mailing address in ways such as using someone else's mail server in order to pass a spam mail filtering system

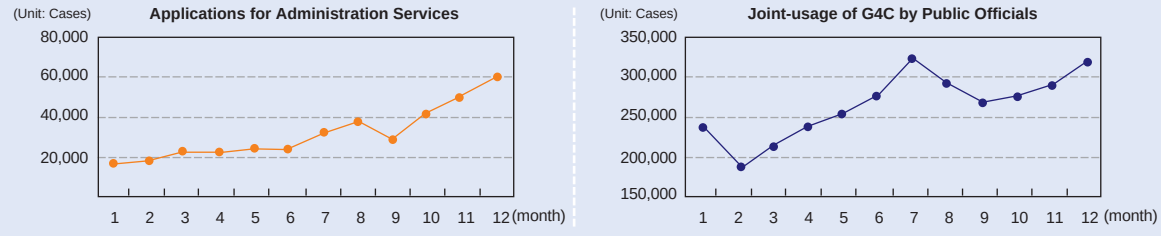
Source: KPR (December, 2003)

Cases of Computer Virus Attacks and New Viruses



Source: KPR (December, 2003)

Usage Rate Trend of e-Government's G4C in 2003



Source: NCA (December, 2003)

The Year in Review

01 Rapid growth of the Education Market in e-Learning

- Internet broadcasting of EBS Scholastic Ability Test (SAT)

The online education market has recently been expanding at a rapid speed. The college entrance market for an online Scholastic Ability Test (SAT) has grown to 100 billion won in 2003 from 1 billion won in 2001. And in 2004, analysts expect this market to double its current value to reach 200 billion won. In addition, the markets for online education or online test preparation for obtaining certificates will also increase in value.

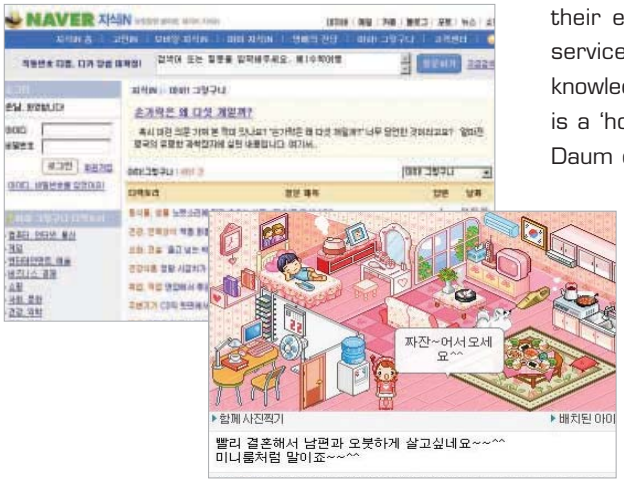
In particular, the 'EBS broadcasting and Internet service for the SAT' plans to have a 24-hour SAT preparation channel via satellite and rebroadcasts segments on the Internet (EDUNET) so that students can access all the shows from any place at any time they want.

※ 1$ ≒ 1,200 won

02 Creation of a New Profit Model for Internet Portals

- Information search, blog, keyword search advertisement

In 2003, despite the general economic slump, sales figures of leading portals have doubled from the previous year. In 2003, portal companies exerted all their efforts into service areas by introducing personal media services such as blogs and portal search services. Currently, knowledge searches where people can ask and answer questions is a 'hot trend'. The growth of leading portals such as NHN and Daum communications, Neowiz and Auction owes much to them being able to obtain various sources of profit and advertisements on search sites. Portal search services limited to listing website addresses was a 100 billion won-market in 2003, and prospects are that it will increase to 200 billion won in 2004.



※ 1$ ≒ 1,200 won

Number of Internet Users Soon to Exceed 30 Million

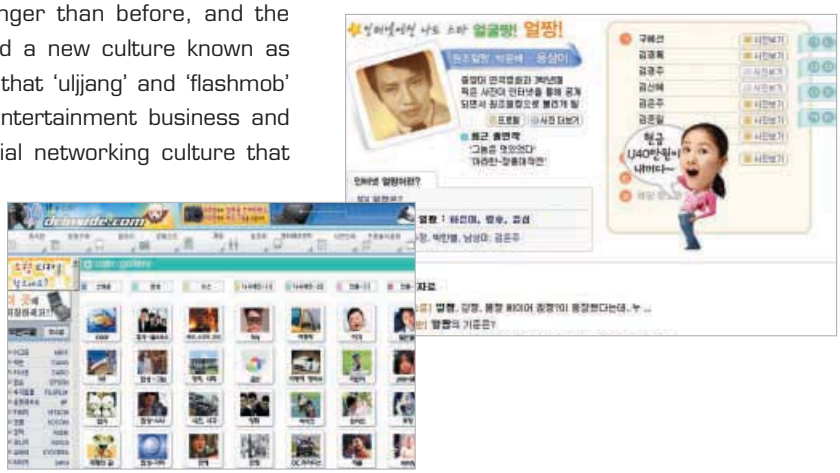
03

The number of Internet users in Korea entered an age of 30 million Internet users as the figure stood at 29.22 million as of the end of 2003 according to the Ministry of Information and Communication (MIC). Internet users as a percentage of the population reached over 65%, and in 2003 those in the mid-aged group (mainly in their 40s) increased by over a million since 2002 making 51.6% of the people in their 40s are now using the Internet. Furthermore, among Internet users, about a quarter have used fee-based services and, buying goods online such as clothes and miscellaneous goods (52.2%) and books (34.5%) is gaining popularity. The Internet no longer just has the role as a community in cyber space but also has become a necessary tool in our daily lives for economic activities such as shopping, Internet banking, and education.

Netizen Culture at the Center of Public Culture

04

Uploading a photo of oneself on the Internet to be voted on by netizens has now become an established gateway towards stardom. The spontaneous gatherings known as 'Flashmob' are a cultural phenomenon where people hold various gatherings from candlelight vigils to concerts. The power of images has become stronger than before, and the popularity of digital cameras has created a new culture known as 'jjang' for best face, best body. The fact that 'uljjang' and 'flashmob' have become catchphrases in society, entertainment business and other areas means that the unique social networking culture that emerged on the Internet has now become mainstream culture. In 2003, the Internet not only emerged as a gateway to stardom but also developed into an effective medium.



05 New Financial Services including Mobile Finance

In 2003, new financial services and various payment methods such as e-money, mobile banking and smart card, were introduced. Although the financial sector's IT investment was dampened by the insolvency of credit card companies, cooperation between mobile companies and mobile carriers became more active in the case of mobile banking which led to a convergence between finance and telecommunications. In addition, the three mobile carriers, which used to operate their own mobile payment infrastructure (mobile merchant) for the last three years, agreed to make the infrastructure compatible for reasons of cost sharing and common technical standards. As a consequence, a wide range of mobile banking services such as checking the balance of an account, wire transfers and cash advances will be available, and credit card services using a mobile phone is expected to be widely used.

06 Korea at the Forefront of the Global Online Gaming Industry

In 2003, the market size of the online gaming industry was 600 billion won with a high annual growth rate of 30% on average. After Hangame took over the Japanese online gaming market, Chinese Internet companies such as Sina.com and China.com have tried to buy shares of domestic game companies. Thus, Korean game companies have established a foothold in the global gaming market in 2003 and will start to make strong inroads in the U.S. and European markets in 2004.

※ 1$ ≒ 1,200 won

07 The Internet at the Center of Political Participation

- Allow for online election campaigns online and enforce 'Internet Real-Name Laws' to mandate the use of real names on Internet bulletin board

As the Internet started to have a greater influence on opinion making and politics, a legal framework was laid out for online election campaign processes for the first time in the world. The election law that was amended in February 2004 permitted the use of the Internet to encourage effective but lower cost campaigns while also imposing new regulations on Internet media. Thus, the 17th General Assembly Elections was the first election to be held centered on the Internet. Furthermore, Internet media companies developed a technology that could match the name and resident registration number of a person with his or her web postings on political discussion boards.

Establishment of Korea Internet Security Center (KRCERT)

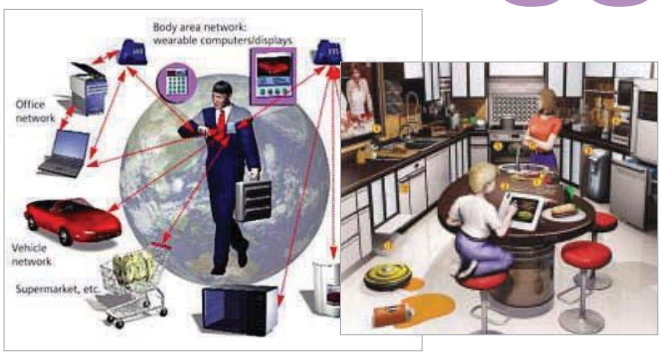
08

After the '1.25 Worm Incident' that affected the nationwide Internet network, the Ministry of Information and Communication (MIC) has been preparing various ways to prevent similar incidents and, as a result, in December 2003, established the 'Korea Internet Security Center' (KRCERT) for the early detection and analysis of cyber attacks against the Internet. Through this center, the government is able to monitor major Internet traffic of ISPs at all times to detect and analyze any unusual activity. In addition, the center is also responsible for issuing an alert or warning to the public before and after any signs of computer intrusions or attacks.

Establishment of Broadband convergence Network (BcN) and Migration to IPv6

- First step towards a ubiquitous environment

09



With the plan to set up the BcN and promote IPv6, the government decided to upgrade the Internet infrastructure to make it a foundation for next generation industries. To this end, following the development of IPv6 applications and equipment, the government plans to start a pilot project in the area of fixed-line telecommunications such as broadband Internet in 2005 and expand into the wireless telecommunications sector in 2006. In addition, through the establishment of BcN, it plans to create an integrated service environment that converges wired and wireless telecommunications, broadcasting, and voice and data.

Korea Placed 10th in Informatization Level

10

Korea's informatization levels makes international informatization rankings as can be seen in its steady rise over the years. In 2003, Korea's average ranking was 10th, and in the rankings for ITU's 'Digital Access Index (DAI)' Korea came in fourth place. Korea was ranked near the top with respects to a nation's underlying infrastructure was evaluated. On the other hand, Korea received a low rank in the e-Business World Rankings, which took into consideration political, economic and societal environments. The implications of this are straightforward-Korea must enhance the effectiveness of Internet use.

< International Informatization index >

(Institute) Index Name	Purpose/ Characteristic	Korea's ranking (Number of Surveyed Countries)	Latest Announcement Date	Ranking of Major Countries
(ITU) Digital Access Index(DAI)	Survey of IT infrastructure and usage focusing on Internet and telecommunication	4 (178)	Nov. 18, 2003	Sweden 1st, US 11th, Japan 15th
(EIU) E-business World Ranking	Survey of e-business environment	16 (60)	Apr. 1, 2003	Sweden 1st, US 4th, Japan 24th
(NCA) National Informatization Index	Survey of informatization by countries	12 (50)	Jul. 22, 2003	Sweden 1st, US 2nd, Japan 16th

Contents

1. ASP [Application Service Provider]

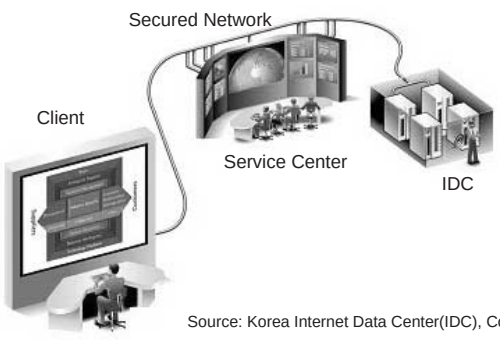
Special Report

In the past, in order to apply information technology to our work and daily lives, we had to purchase application software stored on a CD-ROM or other storage device, and install them on our hardware. However, with the advent of ASPs, the information paradigm is gradually moving towards the provision of access services that eliminate the need to own both hardware and software applications. Using ASP services delivered through the network, we can use the service anytime, anywhere, as much as we want on a 'pay-as-you-go' basis.

Concept

An application service provider (ASP) is a company that offers individuals or enterprises access over the Internet to applications and services that would otherwise have to be purchased or located in their own personal or corporate computers. Sometimes referred to as software as a service (SaaS), ASP is a new business concept that allows companies to access business applications ranging from emails to groupware, ERP, SCM and to CRM, directly from a website for a rental fee.

Figure 01 ASP Service Concept



Source: Korea Internet Data Center(IDC), Corio

Background

Since computers were introduced 40 years ago, companies have gone through three evolutionary stages of information technology: proprietary software development (1960~), package purchase (1970~), and outsourcing (1980~). Now, they are undergoing the 4th stage shifts from purchasing and installing to 'pay as you go'.

The emergence of ASPs, which brought in access-oriented information paradigm, is attributable to the growing demand to eliminate the need to maintain in-house IT applications forced to constantly keep up with evolutions in Internet infrastructures evolution including broadband network and IDCs. Companies have also recognized the need for new network-based IT services in order to respond quickly to the ever changing business environment, to overcome limits in time and space, to lower investment burden in IT and to address the problem of the lack of IT experts.

Composition of ASP

ASP is composed of several level each offering a necessary component of the service.

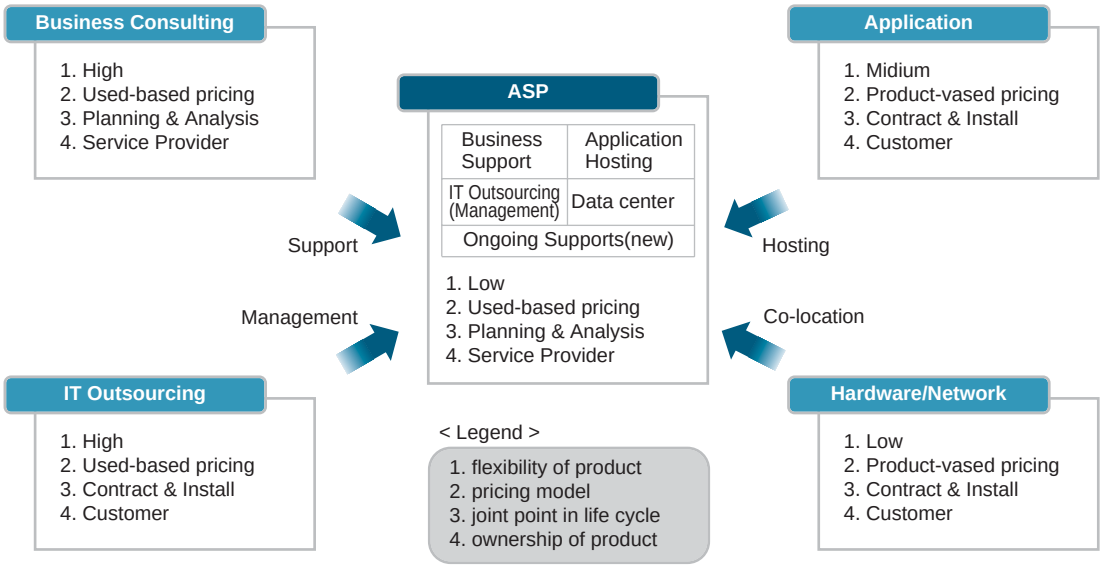
■ H/W and N/W

At the hardware layer sit hardware providers who supply servers and equipment. As for software, providers provide software products including management applications. From these two providers, ASP' s can consequently offer clients applications such as servers, operating systems, firewalls, middleware, and technology platforms. Data centers offer hosting facilities and management functions, which includes server management, network management, power management and security management. The network layer provides a physical network access service that can recognize applications. Companies involves in this include traditional telecommunications providers and ISPs (Internet Service Provider).

■ Application

The ASPs host applications from system developers and independent software vendors (ISVs) and offer both off-the-shelf applications and customized solutions while continuously maintaining them. Application users can categorize ASP, as follows.

Figure 02 Composition of ASP



Source: Internet Data Center(IDC)

Table 01 ASP Classification by Application Types

Classification	Content	Example
Personal ASP	Solution that can support many individual clients at low cost	Web mail, web office programs etc.
Collaboration ASP	Solution designed to support internal collaboration	Groupware, e-billing system etc.
Relation ASP	Solution that supports external relations such as customer management and exchange of information with partners	CRM, SCM etc.
Internal operations ASP	Solution that supports a company's basic operations and business management of a company such as finance, H/R, accounting and marketing	ERP, MIS etc.

Source: Korea Association of Information and Telecommunication(KAIT), Jul. 2003

Evolution of ASPs

The evolution of ASPs can be divided into the following three stages.

■ 1G ASP

In the early stage, ASPs offered software packages over the Internet. The application packages were either installed in a client's office as in-house solutions or hosted on the server to provide ASP services. When you installed the software in your office, you were charged a license fee and ongoing support and maintenance fees. Most ASP contracts were similar to the traditional maintenance outsourcing contract.

■ Web Native ASP

Following the first wave of ASPs, new applications made their debut as a service over the Internet, and they are classified as web native applications. These web applications were built to have a one-to-many delivery channel in their Internet service system and were developed fit to special network services rather than in-house solutions. Suppliers did not customize the service to each client's environment, and one consolidated bill was issued for both S/W license fee and the hosting fees.

■ Web Services ASP

Web services application refers to a unit application that can be delivered as a service by itself or in combination of other units of softwares or applications. Providers can host these web services and applications and deliver them to users via one-to-many service channels. In the future, many web-based applications are expected to migrate to a web service architecture.

Furthermore, unit applications that comprise application packages will be developed and provided in a web service format, allowing easier integration of application packages to enhance the IT system's efficiency.

As ASP services evolve into web-based services, ASPs are expected to overcome their rigidity and provide customized services, catering to the specific needs of each customer. At the same time, web-based ASP services will make it easier to integrate applications within and between companies, thereby increasing the efficiency of the IT system.

Obstacles to the Expansion of ASP Services

Initial software providers triggered the following problems in the process of repackaging large applications, which were subsquently

Table 02 Evolutionary Stages as a Service

Stages		Description	Period (Year)
1st Generation ASP		Focus on the delivery of software packages over the Internet	1998-2000
Web-based ASP		Advent of Internet-based software development companies	1999-2001
Web service ASP	1G web service	Ensure interoperability through alliance based on the standards like SOAP, UDDI and WSDL	2000-2003
	2G web service	Provide components-based web service	2003-2005
	3G web service	Provide business process-based web service	2005-2010

Source: Korea Internet Data Center(IDC), 2002

installed and run on the client's system as ASP services. First, systems were often delayed or local servers needed to be installed at the client site due to complex application, both of which les to failure in accommodating network access or multiple user access. Second, ASP's faced excessive requests from clients for customization as clients experted ASP's services to be as personalized as in-house solutions. Further, pricing was still based on 'per-seat' basis due to lack of expertise in sophisticated pricing and service volume measurement. ASPs offer centralized network services that integrate facilities and applications, which used to be owned by individual companies. Accordingly, ASP services have not yet gained confidence and reliability compared to in-house information systems.

Small Business Network Project

The small business network project targets 3.02 million small businesses with less than 50 employees, as well as solution developers who serve small businesses. A total of 71.4 billion won

Table 03 **Service Delivery Per Consortium in 2003**

Classification		Current Status
KT (36 participating companies)	Basic Service	VPN+bizmeka solution, KORNET+bizmeka solution, Megapass+bizmeka solution
	Value-added Service	Lite Alzzapack, Groupware, Business management, Business management POP, shopping mall builder, homepage builder, Credit card, information management, B2BI, SCM, ERP, platform rental service, marketplace, semuro national pension, health insurance, medical insurance, iPOS, mobile
	Specialized Service	Automobile management, beauty salon management, food materials management, interior, sports club management, real-estate management, church management, optician's shop management
Hanaro Telecom (67 participating companies)	Basic Service	Merchant, Soho
	Value-added Service	4 insurance, handy account book, comprehensive payroll management, groupware, CRM, CRM plus, card master, mail hosting, establishment of home page, home page building plus, CRM, e-Business card, domain registration service
	Specialized Service	Hair salon management, optician's shop management, car service center management, soho mall, kindergarten management, institutes management
Dacom (10 participating companies)	Basic Service	Fund management, MagicFax, CMS
	Value-added Service	Foreign currency information, legal information, legal counseling, shopping mall, home page, video conference, vidual web, call center, CRM, personnel/salary management, webhard, WebTAX21, web hosting, mail hosting, OnNet21, settlement service, trade EDI, eSCM21
	Specialized Service	Marketing/logistics management of distributors, accommodation management, RentPRO, wedding hall management, vending machine marketing management, apparel/furniture dealer management
Korea Information and Communication (2 participating companies)	Basic Service	Card sales manager
	Value-added Service	In preparation
	Specialized Service	In preparation
ELION Information Technology (2 participating companies)	Basic Service	Automobile-related contents & web-mail
	Value-added Service	Shopping mall
	Specialized Service	Car service center management

Source : Ministry of Information and Communication(MIC), Jul. 2003

will be invested from 2001 to 2004 to develop and distribute 50 business models and solutions as well as to support digital training for 180,000 small companies.

The small business network project is designed to develop business solutions that can serve the needs of small businesses in the early stage and provide integrated services in connection with broadband Internet services. At the same time, the project plans to provide small businesses with training on how to use the services to acquire enough subscribers so as to reach critical mass, allowing the network to be expanded autonomously.

Conclusion

ASP has entered a stable growth stage and is expected to evolve leveraging web services as key driver. As software has evolved into a utility service through ASP service, a great change is expected to occur in the overall information environment for individuals and enterprises. Especially, ASP is likely to contribute a great deal towards addressing intellectual property issues of software including piracy.

ASP should be used extensively to facilitate corporate competitiveness and realize an advanced information society, with the world's best IT infrastructure. Korea, therefore, plans to enhance global competitiveness of traditional small-and mid-sized companies and the ASP industry.

2. BcN [Broadband convergence Network]

The recent ICT environment is rapidly moving towards digital convergence, which brings together the industries of telecommu-nications, broadcasting and the Internet. At the same time, the trends of intelligence, convergence and broadband are being reinforced in the services and

Table 04 Prospects for the Advance towards Ubiquitous Information Environment

Narrowband Network (2.4kbps~9.6Kbps)	Broadband Network (1.5~2Mbps)	Broadband convergence Network (50~100Mbps)
· Voice & text services · Focus on electronic information process & distribution · Low Integration among devices	· Broadband Internet service · PC-based service · Some IT products are networked	· Various integrated IT services · IT convergence in all areas · All products are interconnected
· Narrowband technology · Single media technology	· Broadband Internet technology · Web-based service technology · Stand alone type IT technology	· Broadband network technology · Digital convergence technology · Ubiquitous computing technology · Convergence technology with other industries
1990	2000	2010

Source: Ministry of Information and Communication(MIC), Dec.2002

devices of information and communication networks. In order to respond to such a drastic change in the ICT environment the Korea Government has set forth a plan to aid the creation of the Broadband convergence Network (BcN).

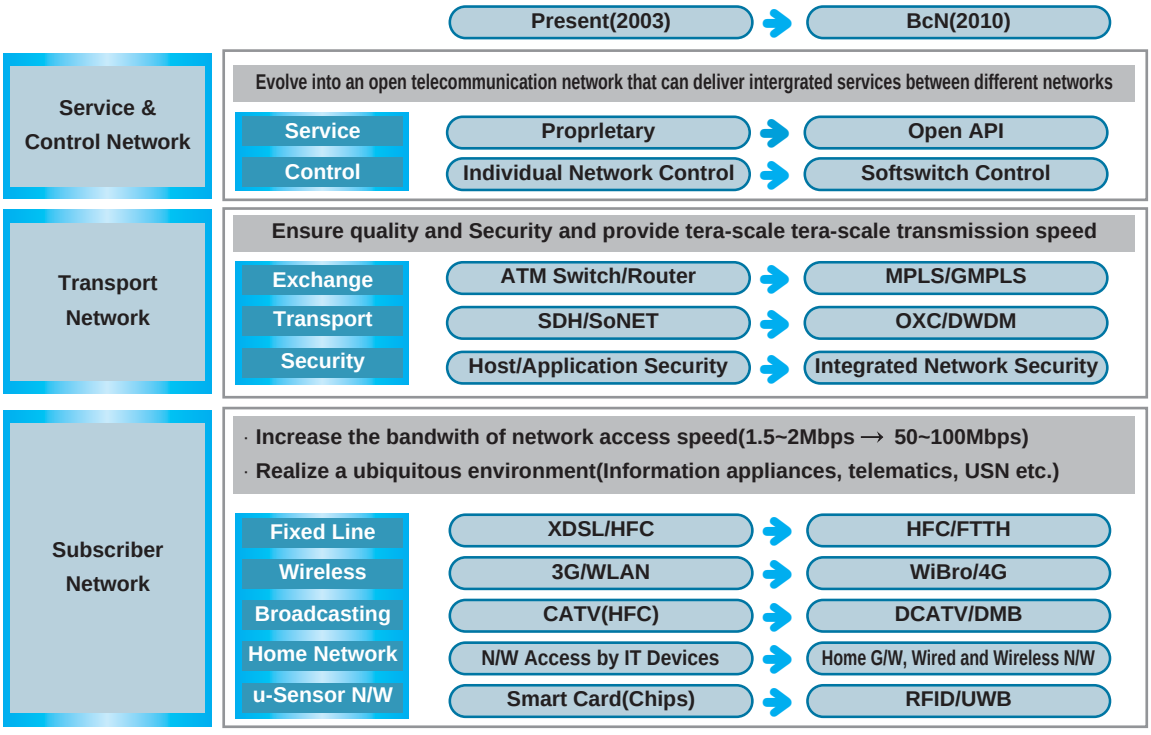
※ Ubiquitous Network : Ubiquitous refers to the quality of 'being available anytime anywhere', and ubiquitous network means a network environment in which networks exist everywhere, offering always-on connectivity.

Table 05 **Prospects for the ICT Service Market (1995~2010)**

Classification	1995	2003	1995~2003 Growth rate	2004	2010	2004~2010 Growth rate
Fixed-line (0.1B won)	66,789	204,951	15.9%	219,449	337,280	7.4%
(Voice)	(58,276)	(57,449)	(-0.01%)	(57,334)	(56,490)	(-0.25%)
(Data)	(8,513)	(147,502)	(47.1%)	(162,115)	(280,790)	(9.7%)
Wireless (0.1B won)	17,101	163,897	35.2%	170,953	198,857	2.6%
(Voice)	(17101)	(146,048)	(33.6%)	(144,533)	(109,339)	(-4.0%)
(Data)	(-)	(17,849)	(81.3%)*	(26,420)	(89,518)	(26.1%)
Broadcasting	27,555	79,793	15.2%	88,452	153,886	9.8%
Total	111,445	448,641	17.9%	478,854	690,023	6.3%

N.B. 1) Fixed-line voice : General call services including local, long-distance and international calls
Fixed-line data : Except the areas of fixed-line voice, Internet telephony, premise communications and the entire value-added communications
Wireless data : Portable Internet, mobile phone Internet service, wireless data service
(*) : Year 2000~2002
Source : Korea Association of Information and Communication(KAIT) (1995~2001), Ministry of Information and Communication(MIC)(2002), Korea Information Strategy Development Institute(KISDI)(2003~)

Figure 03 **Evolution of BcN**



Source: Ministry of Information and Communication(MIC), Dec.2002

Growth Outlook for the ICT Service Market

The size of the ICT service market grew from 11 trillion won in 1995 to 45 trillion won in 2003, a remarkable 18% growth per year on average. As a result, a variety of application services such as VoIP and MMoIP are hitting the wired and wireless telecommunications market with the wide penetration of digital broadcasting and two-way broadcasting. The market is expected to maintain an average annual growth rate of 6%, expanding the volume of business to 69 trillion won in 2010.

Growth Outlook for BcN

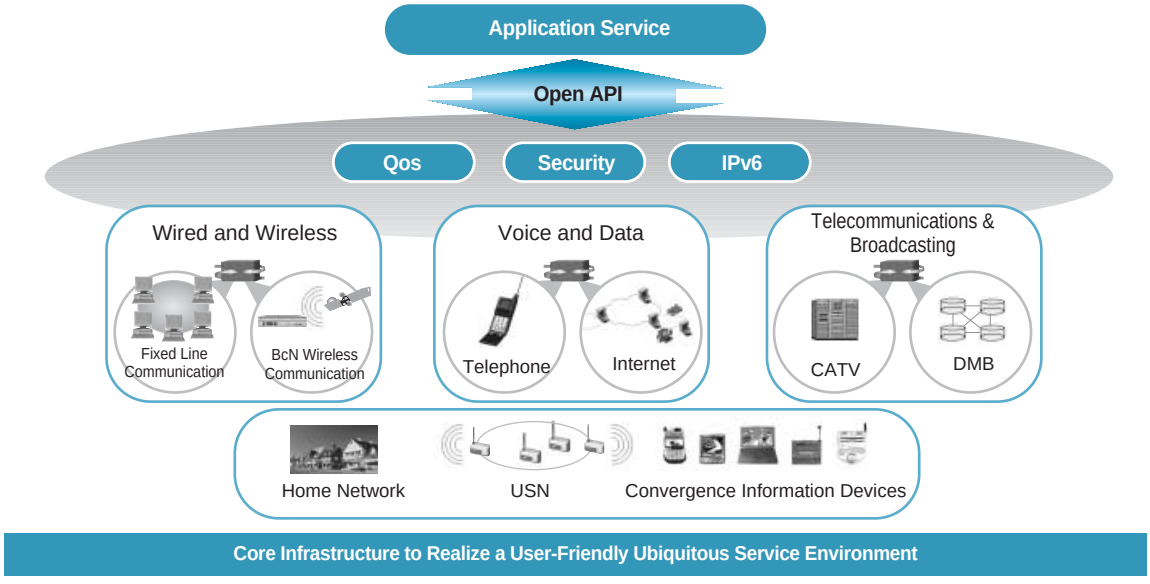
The Control Network (CN) of BcN is expected to develop into an open network that delivers a variety of convergence services of voice and data, wired and wireless, and telecommunications and broadcasting. As for the Transport Network (TN), the tera-scale transmission speed will be available, and the Subscriber Network (SN) will turn into a broadband subscriber network that can send and receive a wide array of broadband multimedia information. The home network is predicted to evolve into a structure in which various home appliances are interconnected to provide a set of integrated services. And the development of ubiquitous access network will be mainly driven by the advance of integrated terminals, smart tags, UWB and sensor technology.

BcN will allow a wide range of applications and services to be easily developed based on open API. This convergence network ensures security and QoS while supporting IPv6. In addition, BcN offers a ubiquitous service environment where users can enjoy seamless service regardless of their handset or network operator.

■ Transport Network

Transport networks will be built to guarantee end-to-end QoS, which differs depending on the

Figure 04 Composition of BcN



Source: National Computerization Agency(NCA)

service quality requirement by users. The network also will efficiently carry out the functions of intrusion detection, intrusion response, and traffic control. As the Internet spreads of to include, information terminals, home appliances, and sensor networks, a new Internet address system, IPv6 (128bit, Some 3.4×1038 addresses) is necessary to enable this cusent estimates project that IPv6 will be functional by 2006. Against this backdrop, in order to introduce IPv6 in all the layers including a variety of information devices and digital home appliances, IPv6 is being applied to new businesses like portable Internet and digital home, and the migration from the existing IPv4 network to IPv6 network is taking place on a gradual basis. Open API services will be introduced through standardized interface among all network layers, so as to create an environment where services can be developed and used regardless of the types of telecommunications networks.

■ Subscriber Network

Currently, more than 100 million households subscribe to a broadband subscriber network, which uses technologies like DSL, HFC and LAN ; but, there are a limits to what the bandwidth can deliver contents, interactive services like P2P (Peer To Peer) and digital home services.

In order to accommodate a wide range of telecommunications then, broadcasting and convergence services such as HD-quality VOD, P2P, webcam chatting and games, 50~100Mbps bandwidth will be required in 2010. Accordingly, the existing subscriber network is expected to broader its bandwidth, and eventually lay optic cables from a carrier's office directly to a subscriber's residence, thereby achieving FTTH (Fiber-to-the-Home).

The Korean Government plans to roll out high-speed WLAN service with a goal of building the wireless network that ensures 50~100Mbps of bandwidth both at a standstill and on the move. At the same time, portable Internet service also will be introduced, offering 30~50Mbps transmission speed in low to medium speed moving environments. In addition, a service that ensures transfer speeds of up to 10Mbps while moving at high-speeds will come through IMT-2000, and New Mobile Access(4G mobile communications service) will be commercially available with the speed of 100Mbps around 2008~2010.

Upgrading the broadcasting network by interworking telecommunications and broadcasting networks will allow the provision of high-quality (HD-quality pictures and CD-quality sound) two-way intelligent services that can be used anytime, anywhere. Such a network upgrade will contribute to creating various business models including T-Gov and T-Commerce, and lead the existing broadcasting infrastructure such as terrestrial, cable, satellite, and DMB broadcasting into going digital while developing into the convergence network of telecommunications and broadcasting.

■ Home Network

In order to create a large consumer base along with the early expansion of the home network, the government is encouraged to develop and distribute the standard model and low-cost core equipment that befit residential environments like cyber apartments, general apartments and houses. Cyber apartments uses premise wiring, Ethernet, and power line communications (PLC) for their home networks. Mobile devices like mobile terminals and laptops are connected through wireless LAN, and as for A/V devices are connected using IEEE1394.

Growth Outlook for the ICT Service Market

The size of the ICT service market grew from 11 trillion won in 1995 to 45 trillion won in 2003, a remarkable 18% growth per year on average. As a result, a variety of application services such as VoIP and MMoIP are hitting the wired and wireless telecommunications market with the wide penetration of digital broadcasting and two-way broadcasting. The market is expected to maintain an average annual growth rate of 6%, expanding the volume of business to 69 trillion won in 2010.

Growth Outlook for BcN

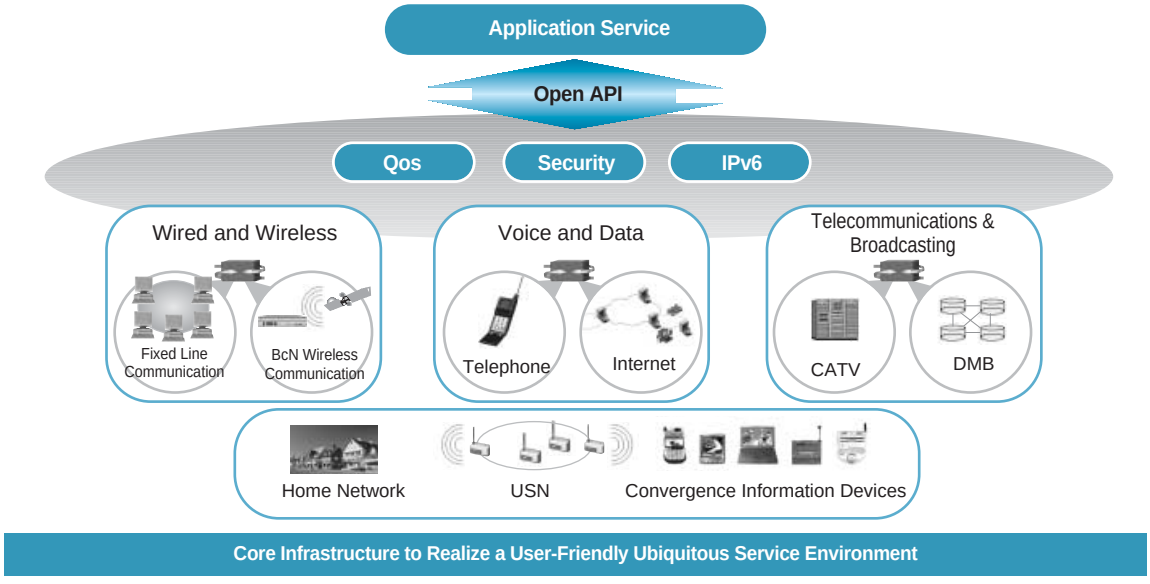
The Control Network (CN) of BcN is expected to develop into an open network that delivers a variety of convergence services of voice and data, wired and wireless, and telecommunications and broadcasting. As for the Transport Network (TN), the tera-scale transmission speed will be available, and the Subscriber Network (SN) will turn into a broadband subscriber network that can send and receive a wide array of broadband multimedia information. The home network is predicted to evolve into a structure in which various home appliances are interconnected to provide a set of integrated services. And the development of ubiquitous access network will be mainly driven by the advance of integrated terminals, smart tags, UWB and sensor technology.

BcN will allow a wide range of applications and services to be easily developed based on open API. This convergence network ensures security and QoS while supporting IPv6. In addition, BcN offers a ubiquitous service environment where users can enjoy seamless service regardless of their handset or network operator.

■ Transport Network

Transport networks will be built to guarantee end-to-end QoS, which differs depending on the

Figure 04 Composition of BcN



Source: National Computerization Agency(NCA)

service quality requirement by users. The network also will efficiently carry out the functions of intrusion detection, intrusion response, and traffic control. As the Internet spreads of to include, information terminals, home appliances, and sensor networks, a new Internet address system, IPv6 (128bit, Some 3.4×1038 addresses) is necessary to enable this cusent estimates project that IPv6 will be functional by 2006. Against this backdrop, in order to introduce IPv6 in all the layers including a variety of information devices and digital home appliances, IPv6 is being applied to new businesses like portable Internet and digital home, and the migration from the existing IPv4 network to IPv6 network is taking place on a gradual basis. Open API services will be introduced through standardized interface among all network layers, so as to create an environment where services can be developed and used regardless of the types of telecommunications networks.

■ Subscriber Network

Currently, more than 100 million households subscribe to a broadband subscriber network, which uses technologies like DSL, HFC and LAN ; but, there are a limits to what the bandwidth can deliver contents, interactive services like P2P (Peer To Peer) and digital home services.

In order to accommodate a wide range of telecommunications then, broadcasting and convergence services such as HD-quality VOD, P2P, webcam chatting and games, 50~100Mbps bandwidth will be required in 2010. Accordingly, the existing subscriber network is expected to broader its bandwidth, and eventually lay optic cables from a carrier's office directly to a subscriber's residence, thereby achieving FTTH (Fiber-to-the-Home).

The Korean Government plans to roll out high-speed WLAN service with a goal of building the wireless network that ensures 50~100Mbps of bandwidth both at a standstill and on the move. At the same time, portable Internet service also will be introduced, offering 30~50Mbps transmission speed in low to medium speed moving environments. In addition, a service that ensures transfer speeds of up to 10Mbps while moving at high-speeds will come through IMT-2000, and New Mobile Access(4G mobile communications service) will be commercially available with the speed of 100Mbps around 2008~2010.

Upgrading the broadcasting network by interworking telecommunications and broadcasting networks will allow the provision of high-quality (HD-quality pictures and CD-quality sound) two-way intelligent services that can be used anytime, anywhere. Such a network upgrade will contribute to creating various business models including T-Gov and T-Commerce, and lead the existing broadcasting infrastructure such as terrestrial, cable, satellite, and DMB broadcasting into going digital while developing into the convergence network of telecommunications and broadcasting.

■ Home Network

In order to create a large consumer base along with the early expansion of the home network, the government is encouraged to develop and distribute the standard model and low-cost core equipment that befit residential environments like cyber apartments, general apartments and houses. Cyber apartments uses premise wiring, Ethernet, and power line communications (PLC) for their home networks. Mobile devices like mobile terminals and laptops are connected through wireless LAN, and as for A/V devices are connected using IEEE1394.

■ u-Sensor Network

u-Sensor Network links users to the wired and wireless subscriber network by attaching RFID or sensor to the objects, thereby allowing them to collect information of anytime, anywhere.

※ WPAN (Wireless Personal Area Network) : Short-distance wireless network represented by a Bluetooth technology and provides connectivity among mobile devices within the vicinity of the user whether stationary or in motion.

※ RFID (Radio Frequency Identification) : Composed of tag, antenna, and reader. Can be applied to many applications, say, to identify individual objects and surroundings, and provide support for logistical management. International and domestic standards related to spectrum used and output power need to be set up.

■ Building of the Advanced BcN R&D Network

The advanced BcN R&D Network is a network that develops and verifies technologies and services by providing a test-bed for pilot projects. To build such a network, KOREN, which is deployed in six major cities across the nation, will be upgraded. And in order to allow Korean research institutes to conduct international joint studies, Korea should spur efforts to develop Korea into an R&D hub so that international research networks like APII Testbed and TEIN can be interconnected centered around Korea.

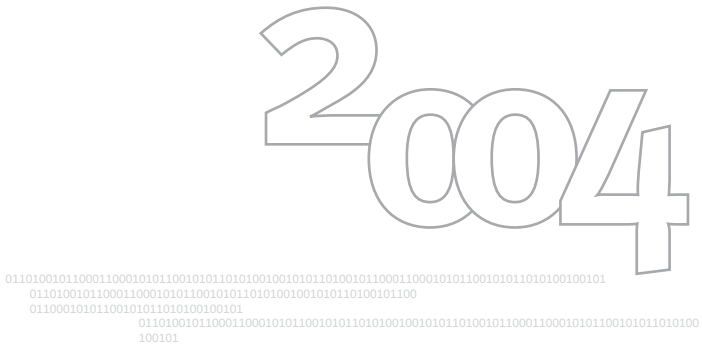
※ As of the end of May, 2004, the interconnection of Korea-U.S. (1Gbps), Korea-Japan (1Gbps), Korea-Singapore (12Mbps) and Korea-France (34Mbps) is under construction.

■ BcN Pilot Project

Core BcN pilot projects are developed with the focus on voice/data, wired/wireless, telecommunications /broadcasting, users business, QoS, security, telematics, home network and u-commerce that can create a new service market and create a large demand base in the new IT growth engine sectors.

Creating an Environment for the Building of BcN

In order to successfully build the BcN, the government plans to facilitate the development of services to realize u-Life across the nation including all the public and private sectors. And the government will work on the development of a digitalization model by setting out a plan to build a BcN model city, and explore the pilot projects related to e-Logistics, virtual office, e-Learning, home network and telematics. Further, the government will encourage the use of BcN services by building e-Government communications network and providing the foundations for advanced e-Government services such as m-Gov, t-Gov, and u-Gov.


2004

1. General Overview of the Internet Industry in 2003

Chapter 1 Introduction

2003 was a meaningful year for the Internet. For one, the domestic Internet industry that had sunk as the dot.com bubble burst discovered the potential to become a 'profit-generating business'. And secondly, the Internet has come to play a greater role in our daily lives. In the meantime, 2003 was also a year that searched for measures to resolve the counter-effects of the Internet.

1.1 Era of High Profit for the Portal Business

Major domestic portal sites such as NHN, Daum communications, Neowiz and Empas posted record earnings due to efforts to diversify their revenue sources and search engine advertising business. In particular, the sales figures of these four companies for the first half of 2003 exceeded the total sales figure for the whole of 2002 and profit rate reached close to 40%. Neowiz leads with a growth rate of 210% compared to the first half of 2002, recording sales of 41.5 billion won, followed by NHN, Empas and Daum which have grown by 158%, 107% and 103% with sales figures of 76.5 billion won, 11.3 billion won and 61.8 billion won respectively. Moreover, the total amount of sales of NHN, Daum and Neowiz in 2003 reached over 400 billion won.

The profit rate of the Internet business draws a sharp contrast with the profit rate of domestic manufacturing companies, which stands at a level of 2-5%. Such a comparison shows the high added value aspect of the Internet business in the sense that it can be run with only labor and marketing costs. This wipes out the uncertainty of the Internet business and proves that it has risen to the ranks of the category of high value-added businesses.

1.2 Fierce Competition for the Top Place between 'the Big 3'

The competition between Daum, NHN, Neowiz, Knowledge power station, Yahoo! Korea (Yahoo), Nate etc. for the top three spots in the industry that is currently held by Daum, NHN and Yahoo, has become fiercer than ever before.

As the competition between web portals increases, the distinct business areas in the portal business have merged and today web portals provide a one-stop comprehensive service. In other words, if one web portal provides a service within a couple of months, most of the other portals start to offer similar services. Conventional search portals such as NHN and Empas are concentrating their investment on community services which is expected to be the next major service. As NHN's 'Hangame' achieved great success, Daum, Empas and Freechal also competed to start a game portal and Naver's knowledge search service has also mostly expanded to portal services.

1.3 M&A Frenzy

M&A has become one of the most important management strategies for survival and expansion in the portal industry. Just as Naver and Hangame merged into one company to become NHN, such a trend is gaining momentum since merging with another company that possesses a different technology and an established user base, is more profitable and easier than entering the new market as a new entrant.

1.4 Fusion of the Wireless Internet Content.

The main topic of conversation among industries dealing with mobile content is 'fusion.' While user demand for more diverse mobile content is growing, the overall wireless Internet content market is growing rapidly. The fusion of business items as well as advancement into new areas has become a common interest for mobile content businesses. This reflects the acknowledgement of mobile content businesses that they will not be able to survive or take a leading role in an era of network interworking between wired and wireless just by providing contents such as bell music and games. In particular, the business structure that guaranteed stable profits started to come under pressure as mobile content, fixed-line portals, mobile communications businesses and other players started to face fierce competition with the opening of wireless network.

1.5 Full-fledged Use of the Hangeul Domain

As Hangeul.kr domain registration service started in August 2003, the era of the Korean domain opened in Korea's Internet market. Considering the fact that Hangeul.kr domain is a Korean domain that is superior relatively on recognition but due to legal rights' issues regarding trademark law and successive introduction of new services, its actual effectiveness as a domain was realized in November 2003 when its popularity was encroached upon by hangeul.com and Hangeul.net. But despite such difficulties, registered users of the Hangeul domain rose at an immense rate and in November 2003 '.kr domain reached 600 thousand'.

1.6 Game Craze Across the Internet Industry

2003 was a year when the Internet industry focused all its efforts on games. In the case of NHN that is operating Hangame as well as the Internet portal site, Naver has profit margins of 40% on revenues and its Hangame division contributed a substantial portion of these profits. The Internet community site, Neowiz of Sayclub, may have made a loss in the first quarter of 2003 but with the incredible response from Netizens for Saygame, their game business, not only could they overcome the losses but sales in 2003 continued to rise. The number of all small-and mid-sized portals, contents industries, companies that pursued projects related to games, amounts up to around 30.

1.7 Korean Mobile Games Sweeping the Global Market

Domestic mobile games have advanced into the top ranks for games in top communications industries and mobile portal sites in other countries. The mobile game 'Action Tennis' of Magic house technology ranked fifth out of the total downloads within a week of starting its services on Jamba!, a well-known European portal site, and gained widespread popularity. The mobile game 'Samgukji' which Manastone introduced in China, is a leading game among Chinamobile WAP games. The mobile game portal site 'Minigame Paradise' that was introduced in Japan by Com2us ranked number one among Java games. In this light, it seems that due to the rise in the value of Korean mobile game brands, the export prospects of mobile games is very bright, and it seems that mobile games will become the export item with the most potential in 2004.

2. The Internet, Penetrating into Our Daily Life

2.1 'Personal Media' Blog Craze

The blog craze which is a personal media, has over 2,000,000 new blogs being set up a day in about 30 portal blog services and special sites, and in November 2003 blog users reached over 10 million. The immense success of blogs are due to the attraction that you can be at the center of the site and create your own open community. At the end of 2002, the number of blogs hovered around 2 million but increased more than fivefold within a year. Given the total number of people who use the Internet, it means that one out of three Internet users have their own personal blog. Furthermore, with the introduction of the mobile blog (mobilog) which enables users to post photos taken on their mobile phones directly to their blog by connecting their blogs and mobile phone, users are becoming 'prosumers' who produce content as well as consuming it.

2.2 Expansion of the Internet Culture

2003 was a year when the Internet's role as a gateway was significant as the influence of images grew. The word 'uljjang' which means 'a good-looking face' became popular word in social, political and cultural areas and events related to 'uljjang' were held all the time on web sites and each web portal competed to set up related services too.

2.3 Internet Users: Rapid spread to those in their 30s and 40s.

There has been a significant increase in Internet users among 30-40 years of age. In particular, the middle aged group in their 40s who can be referred to as the generation caught in the middle of the digital and analog age, are rapidly surfacing all over the Internet. According to the outcome of

the 'survey on the current situation in informatization technology' carried out by the government in November 2003, Internet users in their 40s have increased by over 1 million and out of the total number of people in their 40s, 51.6% are shown to be using the Internet.

3. Exploring Policy Alternatives

3.1 A New Turning Point in the Internet Address Policy

The Internet Address Resources Act that was passed in the national assembly in November 2003 was announced in January 2004 and will be put into effect on July 30, causing the Internet address policy to reach another milestone.

The bill will provide a new opportunity to introduce and use a management system in the Internet address protocol that had been bogged by squatters and excessive competition that had been happening so far. In particular, it is significant in that the government allowed the limited number of Internet addresses to be used by all, thus making the best use of its strength as 'a country with well-deployed infrastructure' and established a legal basis to take the leading role in the Internet address system.

3.2 Strengthened Internet Security Policy

After the Internet break-down incident in January 25 2003, with wired and wireless Internet services grinding to a halt for about nine hours, the government formed a 'Computer Emergency Response Team (CERT)' to prevent such incidents from reoccuring. The government established a comprehensive war room and Korea Internet Security Center (KRCERT) involving the experts from the government, ISPs and information security companies. In particular, spam mail and spread of computer viruses through e-mail and most frequently used services have become a major issue that needs to be controlled in cooperation between private and government agencies and there has also been an increase in the number of people installing anti-virus programs. Government policies that had concentrated on expanding the underlying Internet infrastructure are now making efforts to ensure the security of the infrastructure and prevent various cyber attacks.

1. Trend in Internet Usage

1.1 Fixed-line Internet

■ Number of Internet Users

In Dec.2003, the percentage of Internet users nationwide was 65.5% with the number of Internet users among those with registered residence in Korea reaching 2,922 million. The number of Internet users has increased every year by more than 10%, only beginning to slowing after 2001 when the market became relatively saturated.

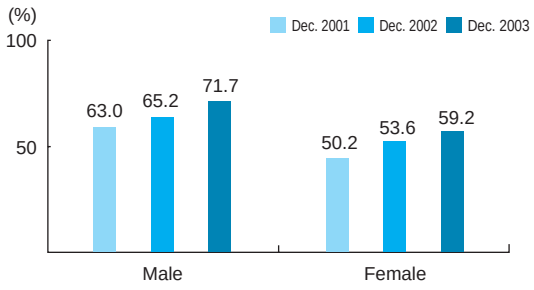
■ Gender/Age Groups

In Dec. 2003, approximately 72 out of a hundred Korean men and 59 out of a hundred Korean women used the Internet. As for age breakdowns, the percentage of Internet users aged 6~19 was the highest with 94.8%, followed by those in their 20' s with 94.5%, those in their 30' s with 80.7% and those in their 40' s with 51.6%. In comparison to Dec. 2002 surveys, usage among those in their 40' s showed the most growth, increasing by 12.3% (1.08million). the growth of internet use by those in their 30' s followed close behind with 11.3%(0.98million) growth.

■ Households with Internet Connection

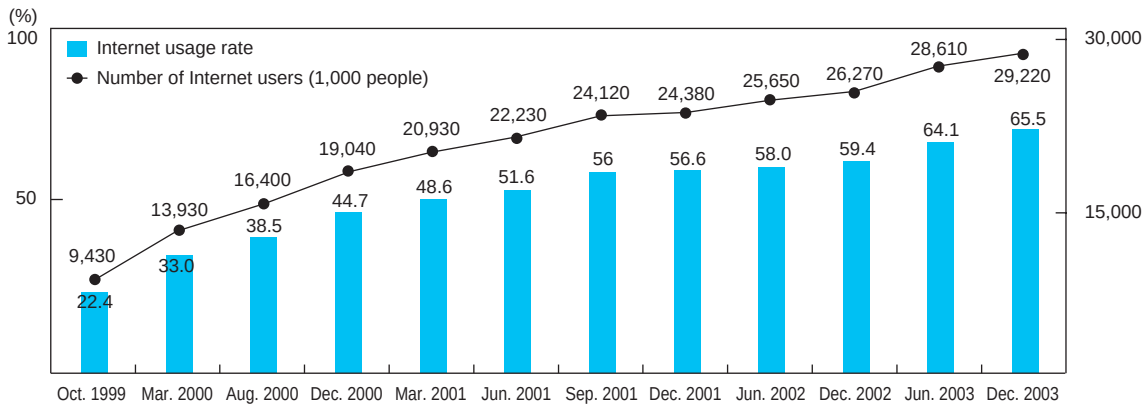
Among households, 68.8% had Internet connections, and 91.5% of the households with computers have suitable Internet use environments.

Figure 2-02 Internet Usage by Gender



Source: Korea Network Information Center(KRNIC), Dec. 2003

Figure 2-01 Changing Trend in the Number of Internet Users



Source: Korea Network Information Center(KRNIC), Dec. 2003

The total number of houses with computers is divided into 'Internet accessible households' and Internet access unattainable households'.

■ Internet Connection Type

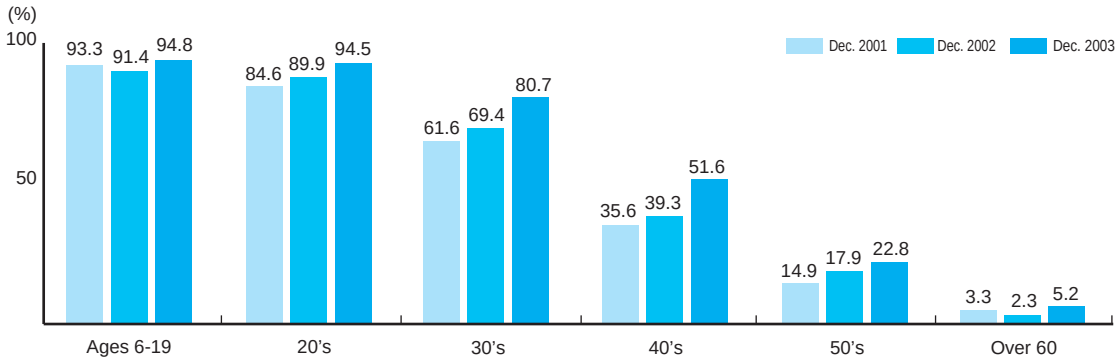
In Dec. 2003, the most popular type of Internet connection among families was the 'XDSL' type with 83.5%, the 'CATV' net (12.4%), 'Dial-up MODEM' (2.1%), 'ISDN' (1.0%) etc. In case of district regions, 88.2% of households with access to the Internet use the 'SDSL' type, 83.3% in middle and small cities and in major cities, 83.1% of the households connect into the Internet via 'XDSL'.

■ Internet Fee

The monthly average Internet usage fee among Internet accessible households is approximately 32,100 won, and among all households with Internet, the average monthly payment is 22,100 won.

By community, the monthly average costs in

Figure 2-03 Internet Usage by Age group



Source: Korea Network Information Center, Dec. 2003

Table 2-01 Ratio of Households with Internet Connection

(Unit: %)

	Households with a computer			Households without a computer
	Number	Internet connection	Non-Internet connection	
Total Households	75.2	68.8	6.4	24.8
Households with a computer	100.0	91.5	8.5	-

Source: Korea Network Information Center(KRNIC), Dec. 2003

Table 2-02 Types of Internet Connection among Households

(Unit: %)

	xDSL	CATV	Dial-up Modem	ISDN	Others	Don't know/no reply
Total	**83.5**	**12.4**	**2.1**	**1.0**	**0.5**	**0.5**
Major cities	83.1	13.6	2.1	0.8	0.2	0.2
Middle to small cities	83.3	12.0	1.6	1.1	1.0	0.9
Districts	88.2	5.1	4.6	0.7	0.0	1.3

Source: Korea Network Information Center(KRNIC), Dec. 2003

major cities is 24,800 won, significantly more than their counterparts in small and mid-sized cities and district regions.

■ Internet Usage Time

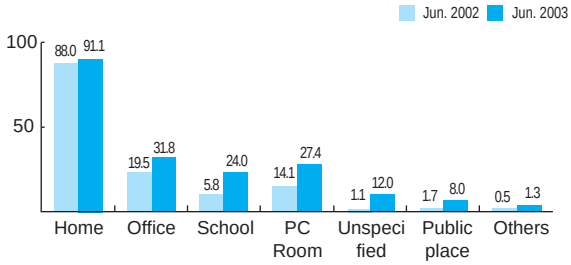
The average Internet usage time per week is 12.5hours with 46.9% of users using the Internet for more than 10 hours. The remaining 27.3% use the Internet for 4~10 hours or less, and 16.8% use the Internet for 2~4 hours or less.

■ Main Location for Internet Use

Surveys show that most Internet users (91.1%) connect to the Internet at home, followed by work (31.8%), PC rooms (27.4%), schools (24.0%) and the remainder at other places.

Figure 2-05 Main Location of Internet Access

(Unit: %)



Source: Korea Network Information Center(KRNIC), Dec. 2003

Table 2-03 Monthly Average Internet Usage Fee per Household

(Unit: %)

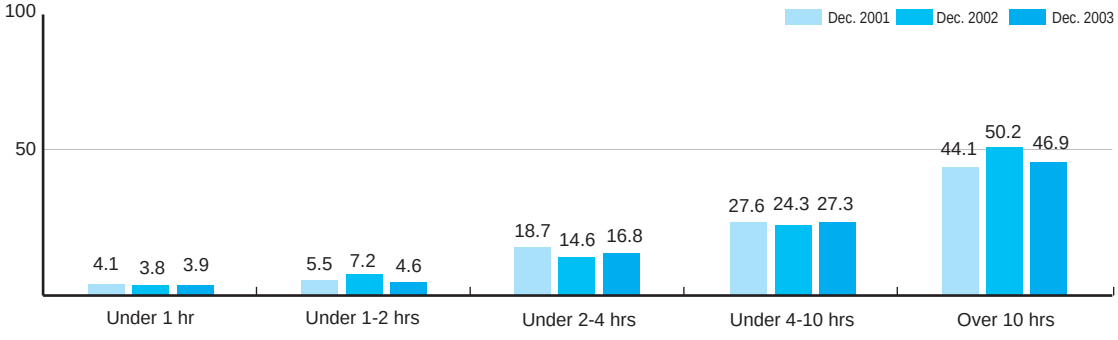
	Free of charge	Less than a 10,000won	10,000~ 20,000won or less	20,000~ 30,000won or less	30,000~ 50,000won or less	50,000won over	No reply	Total household average (1,000won)	Internet-enabled household average (1,000won)
Total	**0.3**	**0.4**	**1.9**	**17.2**	**76.6**	**2.9**	**0.6**	**22.1**	**32.1**
Major cities	0.0	0.4	2.4	14.8	78.0	3.7	0.5	24.8	32.8
Middle to small cities	0.7	0.3	1.1	21.4	73.7	2.1	0.7	21.0	30.9
Districts Regions	0.2	0.6	2.0	10.2	84.4	2.2	0.3	14.2	33.2

※ 1$ ≒ 1,200won

Source: Korea Network Information Center, Dec. 2003

Figure 2-04 Average Internet Usage Time per Week

(Unit: %)



Source: Korea Network Information Center(KRNIC), Dec. 2003

■ The Current Status of PC Rooms

Near the end of 1998, the number of PC Rooms in Korea stood at approximately 3,000. Afterwards, the figure showed continuous growth, expanding to 22,549 by 2001, In 2002 however, this figure decreased to 21,213 as the Internet infrastructure at homes improved.

Also in May 2003, according to a survey of 600 game players in Seoul and Gyeonggi Province, the average time spent at PC Rooms per trip was 2 hours. 43.3% of respondents said to have spent 1~2 hours in the PC Room playing games at costs of approximately 43,000 won monthly. By age group, those above 30 spend 61,042 won monthly at PC Rooms, the most on average. Male users spend approximately 55,000 won while female users spend approximately 17000 won.

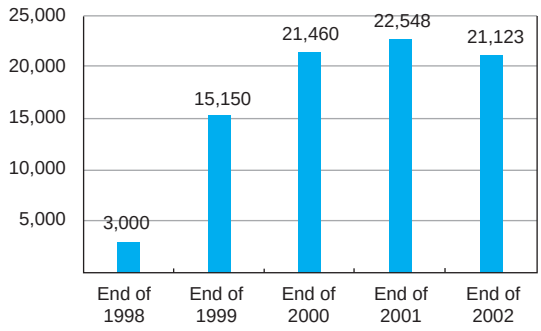
■ Current Status of Internet Shopping Malls and Fee-based Contents.

39.9% of Internet users above the age of 12 have within the previous 6 months conducted Internet shopping, either purchasing goods or pre-purchasing/reserving a ticket.

Most people use Internet shopping to purchase 'clothes/personal goods' (51.2%) followed by 'books' (34.5%), 'living/car supplies' (24.0%) and 'reservation/pre-purchased tickets' respectively.

Figure 2-06 Yearly Trend of PC Room

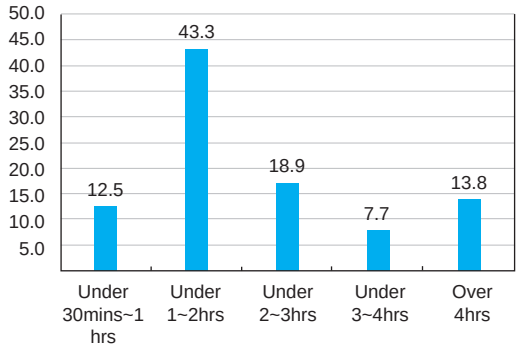
(Unit: No. of PC Room)



Source: Korea Entertainment System Industry Association, Jul. 2003

Figure 2-07 Average PC Room Usage Time per Trip

(Unit: %)



Source: Korea Entertainment System Industry Association, Jul. 2003

Table 2-04 PC Room Usage Fee

(Unit: 100won)

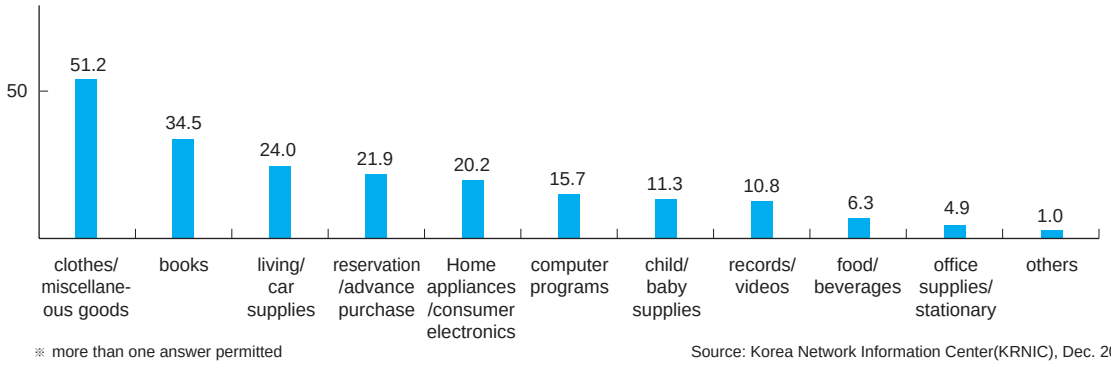
Category		Monthly average usage fee
Total		430.4
Age	10's	28.97
	20's	483.54
	Above 30's	610.42
Gender	Male	554.83
	female	175.32

※ 1$ = 1,200won

Source: Korea Entertainment System Industry Association , Jul. 2003

Figure 2-08 Items Purchased at Internet Shopping Malls

(Unit: %)



※ more than one answer permitted

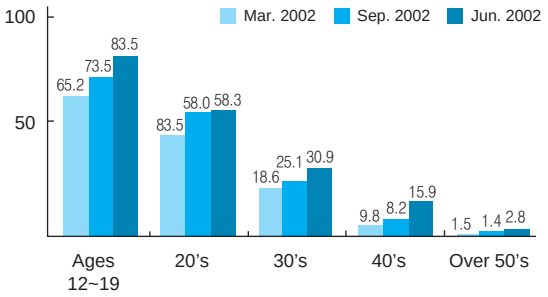
Source: Korea Network Information Center(KRNIC), Dec. 2003

1.2 Wireless Internet

In June 2003, 36.1% of wireless Internet users were mobile phone holders, and the number of wireless Internet users was 1.197 million (users above age 12). The ratio of male wireless Internet users was 34.1% and the same figure for females was 38.9%, a 4.8% higher usage figure than males.

Figure 2-09 The rate of Wireless Internet usage by Age Group

(Unit: %)



Source: Korea Network Information Center(KRNIC), Jun. 2003

■ Ratio of Use by Age

By age group, Koreans between 12~19 used wireless Internet the most (83.5%) and as the age group gets higher the ratio of wireless Internet use drops significantly with only 2.8% of those above their 50' s using wireless services..

In Sept 2002,the 12-19 age group experienced the largest usage increase levels..

■ Frequency of Use/Average Time Online

41.2% of wireless Internet users log on at least once every week and up to 10.4% said to have used wireless Internet 'nearly everyday.'

The average usage time per week for wireless Internet users is 1 hour 4 minutes (64.2 minutes). 51.4%, the highest figure in this grouping, said they used wireless Internet 10 minutes or less per week while 12.3% of respondent said they used the same services for 90 minutes or more.

Table 2-05 Usage Time of Wireless Internet

(Unit: %)

		Less than 10 mins	Less than 10~30 mins	Less than 30~60 mins	Less than 60~90 mins	More than 90 mins	Average time (mins/week)
Total		51.4	19.3	11.1	5.8	12.3	64.2
Gender	Male	48.4	18.8	12.0	6.9	13.9	79.0
	Female	55.0	19.9	10.1	4.6	10.5	46.8

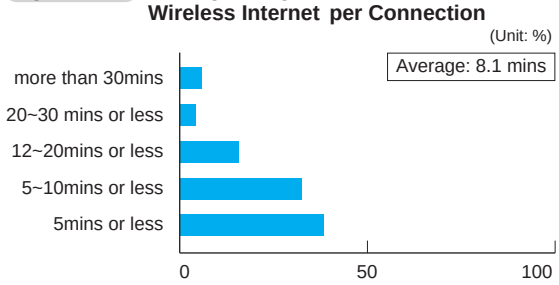
Source: Korea Network Information Center(KRNIC), Jun. 2003

Average connection times to wireless Internet, however, hovered around 8.1 minutes on average.

■ Contents of the Wireless Internet

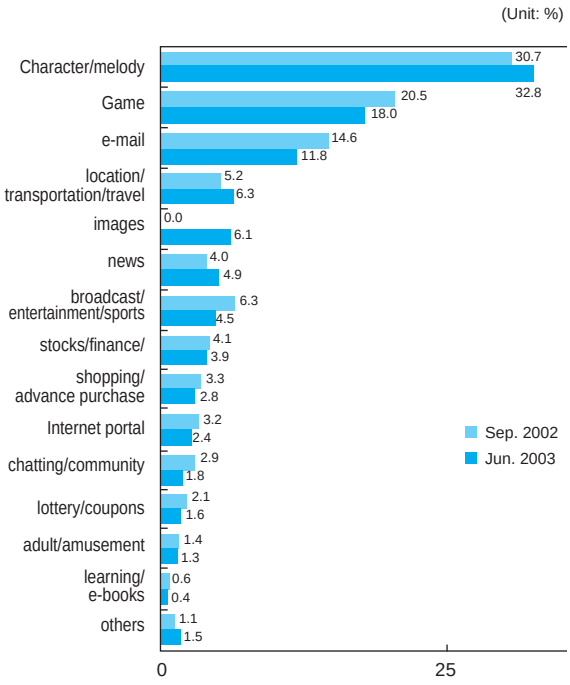
The most popular contents used by wireless Internet users are 'characters/melody/photo download' (32.8%), followed by' Games' (18.0%) and 'e-mail' (11.8%).

Figure 2-10 **Average Usage time of Wireless Internet per Connection**



Source: Korea Network Information Center(KRNIC), Jun. 2003

Figure 2-11 **Popular Wireless Internet Contents**



Source : Korea Internet information center, Jun. 2003

2. Current Status of Internet Usage by Sectors

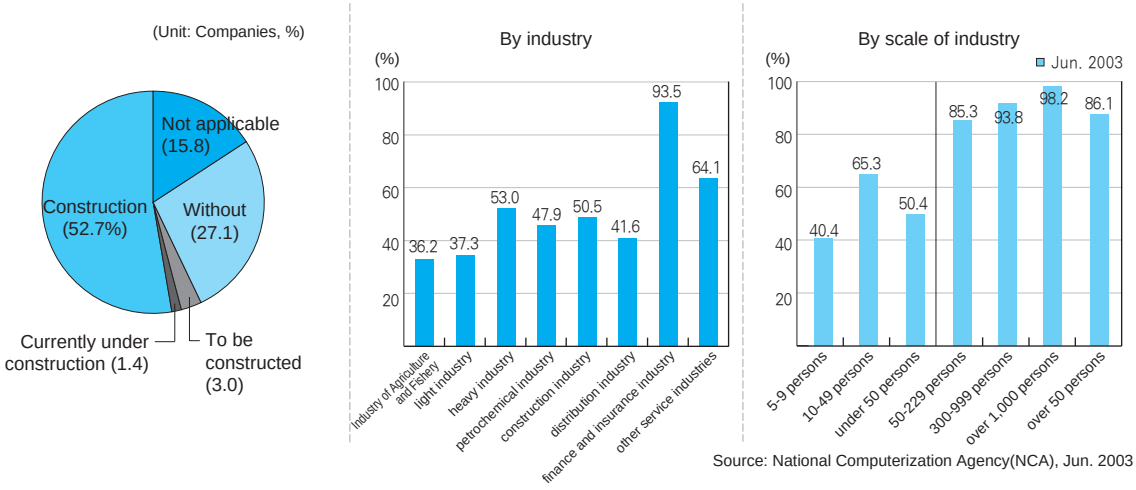
2.1 Industries

■ Network Construction and Current Status of Internet Connection

Among all the companies in Korea with more than 5 employees, those with established networks (communication networks excluding modems) came to 52.7% as of June 2003, and companies capable of Internet connection came to 79.7%

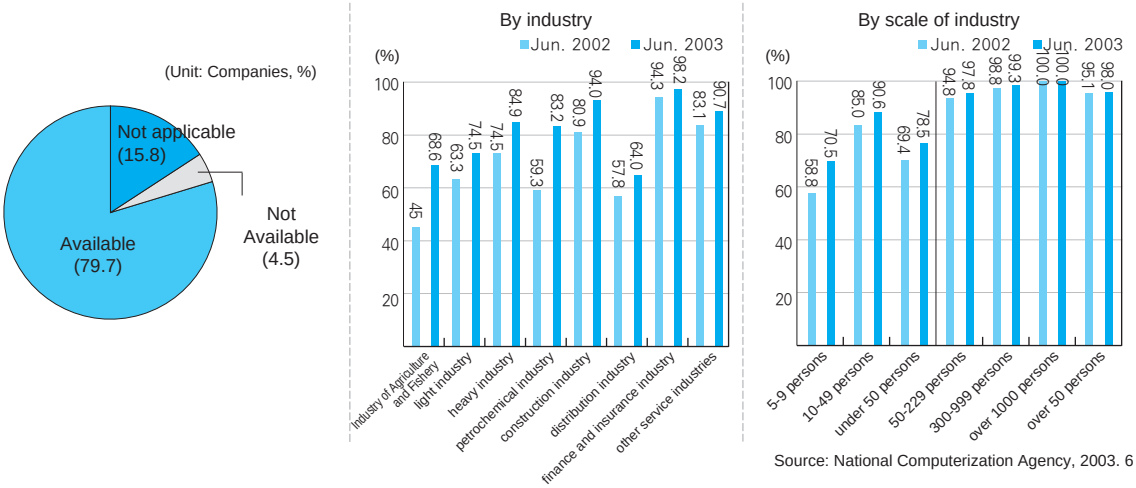
Looking at each sector, finance and insurance companies had the highest percentage of network

Figure 2-12 Network Construction Rate



Source: National Computerization Agency(NCA), Jun. 2003

Figure 2-13 Internet Access Availabilty by Industries



Source: National Computerization Agency, 2003. 6

construction and Internet connections while agriculture, forestry and marine product industries were lowest in both network construction and Internet connections. The larger the number of workers was the higher the percentage of network construction and ratio of Internet connections. And in comparison with 2002, there was a much larger increase in network construction among companies with less than 50 workers.

■ Main Internet Connection Type and Speed

In June 2003, 64.2%(241000) of the 375,000 industries able to have Internet connections used 'xDSL' to connect into the Internet, and 18.9% used 'leased lines'.

By industry, finance and insurance companies (52.3%) used leased lines as their main connection type. And by organization types, central and local governments (65.0%) used leased lines as their main connection type.

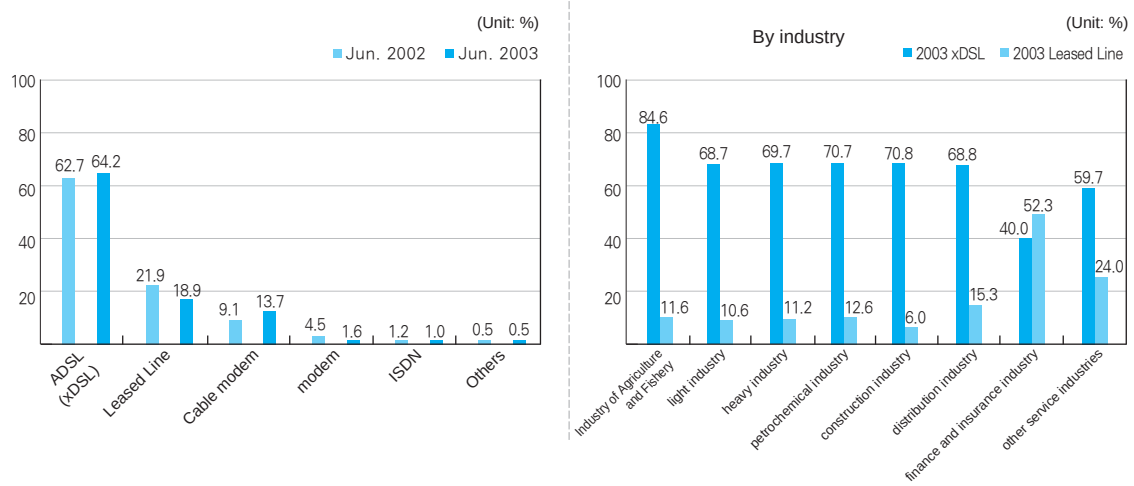
■ Proportion of e-Commerce Usage

According to our yearly survey on e-Commerce (subject to companies with more than 5 employees between Jul. 2002 and Jun. 2003), 23.5% of companies that have experienced electronic trading or roughly 111 thousand companies.

If we compare this to the same period in 2002, the proportion of those with experience in e-Commerce has increased by 13.7%, evidence of e-Commerce's increasing appeal. By industry, construction, finance and insurance industries and other service industries record slightly higher rates of e-Commerce use with light industries the lowest.

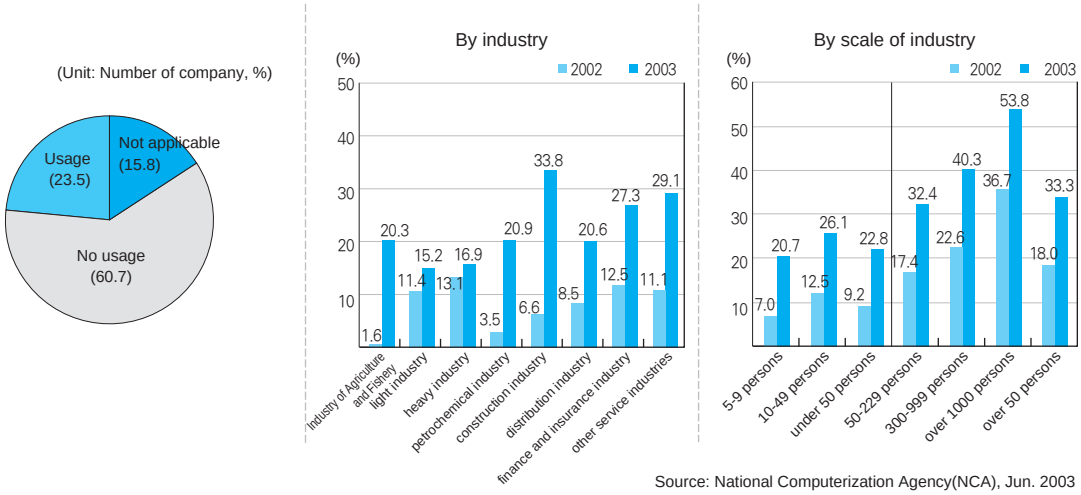
Gauging by the number of employees, for companies with less than 50 employees, the percentage who used e-Commerce is 22.0% while companies with more than 50 employees recorded a higher 33% use. In comparison to the same period in 2002, the proportion of e-Commerce usage by companies with less than 50 employees has increased by 13.6%.

Figure 2-14 Main Internet Connection Type by Industries



Source: National Computerization Agency, 2003. 6

Figure 2-15 e-Commerce Usage Rate



Source: National Computerization Agency(NCA), Jun. 2003

2.2 Public Organizations

■ Internet Connection Type

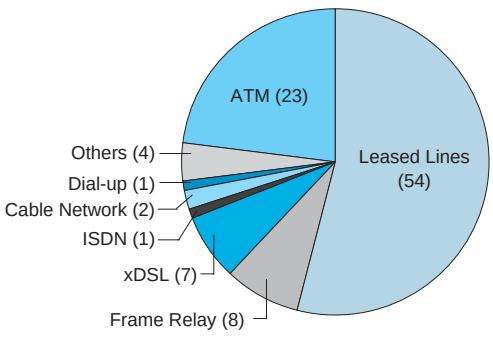
The method of Internet access mainly used by public organizations is via leased lines (54%), followed by ATM' s (23%), Frame Relay (8%) and Xdsl (7%). 76% of these Internet lines can handle 256Kbps or more.

■ Online Civil Services

In the public sector, 90% of institutions have introduced online civil services while 10% have not. The types of online civil services are verification and validation 27%, petition and inquiry proposal 26%, declaration and transfer 16% while authorization and permission came to 9% and registration and license identification came to 9%.

Figure 2-16 Connection Type of Internet Lines

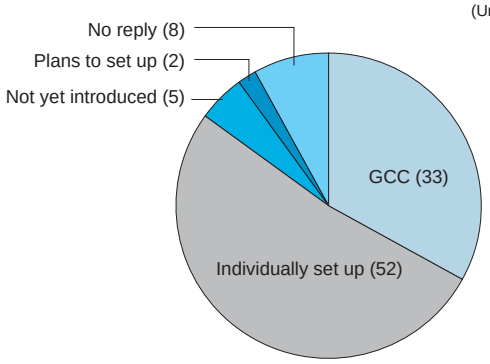
(Unit: %)



Source: National Computerization Agency(NCA), Dec. 2003

Figure 2-17 Current status of Building Public internet system for Civil Services

(Unit: %)



Source: National Computerization Agency, Dec. 2003

52% of all institutions have set up an individual public Internet system to deal with claims, and 33% responded affirmatively to having set up a claim system through the Government Computerization Center(GCC), bringing the total to 85% of all institutions.

2.3 Educational Institutions

■ Preschool and Special Education

Since 1999, preschool Internet education has grown in popularity. And since 2000, around 700 early education institutions were operating their own homepage. The homepages offered information on education plans, events and other educational activities and communication with parents and mailing classroom activities to homes via bulletin boards and counseling sections

The Internet also is being used for special education, targeting students with disabilities, special education teachers and parents. Out of the total 137 'special' schools, 132 are opening homepages providing services concerning related materials.

■ Elementary and Middle Schools

In Dec.2003, 1,2555,704 PCs were supplied to elementary and middle schools (an average of 2.6 PCs per student); and by 2005, these figures should reach to roughly 5 PCs per student.

As for Internet speed, 6,307 of all schools reached E1 grade (2Mbps) lines or more, and in 2003, 71% reached the same grade. As every elementary and middle schools is supplied with Internet lines and most schools have constructed their own homepage, the school and family are being closely connected, sharing teaching and learning materials through homepages.

Table 2-06 Year of Homepage Establishment at Pre-school Education Institutions

(Unit: Number of institution)

number of sub-menus	1996	1997	1998	1999	2000	2001	2002	2003
total	1	2	10	23	42	59	48	12
Kindergarten	1	1	6	10	28	26	19	4
Children's Home	-	1	4	13	14	33	29	8

Source: Ministry of Education & Human Resources Development, Nov. 2003

Table 2-07 Current Status of Education through Special School Homepages

Regional education office			Special schools		
Number of education office	Established number	Ratio of establishment	Number of schools	Operating staff	Ratio of operation
180	140	77.8%	137	132	96.4%

Source: Ministry of Education & Human Resources Development, Nov. 2003

Table 2-08 Current Status of Internet Speed at Schools

(Unit: Number of lines)

Category	256K	512K	2M	Over 3M	Other	Total
state schools	-	-	45	-	-	45
public and private schools	754	3,381	6,262	-	132	10,529
Total	754	3,381	6,307	-	132	10,574

Source: Ministry of Education & Human Resources Development-Korea Education and Research Information service, Nov. 2003

■ General Universities

Since 1996, after expanding electronic networks within campuses and establishing information education classes at preparatory teachers training institutions in 1999, e-Classes based on on-line learning have been constructed at 151 out of 376 universities. In 2003, about 11,568 classes (53.3%)

Table 2-09 Current status of e-Classes

Category	No.of school	No. of General classes	No. of e-Classes	Percentage of e-Classes
4 year state university	24	4,312	2,165	50.2%
State commercial university	8	619	190	30.6%
Education university	11	476	222	46.6%
State college	5	98	59	60.2%
4 year private university	156	16,158	8,932	55.2%
total	204	21,663	11,568	53.3%

Source: Ministry of Education & Human Resources Development-Korea Education and Research Information service, Nov. 2003

Table 2-10 Cyber University Curriculum

(Unit: %)

		Types of major	
IT related courses	Engineering Department	IT Division, IT Planning course, Computer course, Information Technology division, Computer Information Technology course, Digital Multimedia division/course, Multimedia division /course, Computer Media course, Digital Information course, Internet course, Internet Contents course, Digital Contents division, Education Contents course, International Authorized Computer Programming course, Information Protection course, Computer course.	15.5
	Design Department	Digital Multimedia division (majoring Design), Computer Design division, Multimedia Design division, Digital Design division, Digital Animation department, Space Design	4.4
	Game related	Game Planning course grouping, Game Contents course grouping	1.6
Social Science related courses	Management related courses	Management course grouping/ division /course, Management Information course, e-Business course, e-Management division /course, Management Information course, Venture Management course, Property Management course, Tax Accounting course, Industry System Management course	20.8
	Tourism Management	Hotel Management course, Tourism Hotel and Restaurant Management course	2.5
	Social Welfare	School of Cyber NGO (majoring Social Welfare), Social Welfare course	9.2
	Law/Administration/Society	Law division /course, Law Administration division, International Studies division, Digital Administration course, Advertising and Public Relations division, Cyber NGO course, Military Affairs course	9.8
Language related courses	Language	Foreign Language faculty, Practical English course, Practical Language course	10.9
Humanities related courses	Education / Culture	Digital Education course, Lifelong Education course, Education for Handicapped course, Care of Children course, Literary Creation course, Theatrical Movie course, Media Literary Creation course	4.2
Not Classified		Social Science course, Information Culture Industry course, Humanity and Society courses, Nature Engineering courses, Arts courses (Hard to classify due to big registration unit)	21.1
Total			100.0

Source: Ministry of Education & Human Resources Development-Korea Education and Research Information service, Nov. 2003

out of the 21,663 university classes researched were operated via the Internet.

■ Cyber Universities

As of 2003, 17 cyber universities had been established to provide advanced education. The curriculum provided at cyber universities is mainly economics (23.3%) and data communication related (21.5%).

■ Life-long Education and Internet classes for Parents

Since 2000, the government has been promoting a 'life-long education system.' As a result, from 2002, an education center homepage(ncle.kedi.re.kr) providing information on life long education programs and life long learning contents began operations, and cities and provinces built community life-long education center homepages. Government education on the Internet for parents began in 2001, aiming to narrow the digital divide and provide information concerning children's learning, schools and life, which are the main interests of parents.

Table 2-11 Current Status of Internet Classes

(Unit: persons)

Category	Elementary School	Middle School	High School	Total
Number of students	29,155	14,752	11,596	55,503

Source: Ministry of Education & Human Resources Development-Korea Education and Research Information service, Nov. 2003

1. Internet Address Policy

The current IP address is the Internet Protocol version (IPv4), a 32-bit system that can accommodate approximately 4.3 billion addresses. However, due to the increase in Internet users and diversity in media, demand for IP address is rapidly increasing and thus at the current rate of demand, all IP addresses will be allocated within the next 5 to 10 years. Therefore, we are promoting a plan to gain a clear verification and analysis of the current status of IPv4 that have been allocated when an oversight committee for allocating Internet address resources was absent.

Furthermore, the introduction and general use of the 128 bit IPv6 address system is being promoted to improve the quality of the next generation Internet by improving mobility, security and QoS (Quality of Service). In particular, as the wireless Internet service and digital home services among the next generation Internet services are being introduced on a trial basis, while telematics and mobile Internet services are becoming more common, more fixed IP addresses are being used in the next generation Internet environment. This is why the introduction of the IPv6 address system is being recognized as a critical step to address future issues. Therefore, the government is establishing a plan to facilitate the introduction of IPv6 across the nation.

1.1 Internet Governance

If the previous Internet was a physical infrastructure, today's concept of the Internet has expanded to include a social and cultural infrastructure. As a result, creating a governance system for all information-based society that will enable the effective operation of social and cultural infrastructures has become a very urgent issue. Internet governance now encompasser the technical aspects of the Internet such as protocol, to the political, social, economic and cultural aspects. To be more specific, Internet governance is a process through which related parties, including governments from each country, manage, regulate and control their decisions and implement Internet policies with consistent authority and means.

In December 2003, the first World Summit on the Information Society of the International Telecommunication Union stated that setting up an appropriate framework for Internet governance should be the main task for the development of the global information society and the authority of public policies related to the Internet are under each country's sovereignty. Furthermore, the conference demanded that the Secretary-General of the UN construct a framework for Internet governance and to submit a report by the second opening of the WSIS scheduled for November 2005. To this end, governments, industries, academic circles, civic organizations, and other groups are cooperating and carrying out research not only concerning Internet-based governance that is sometimes referred to as Internet governance (technical domain), but also in Internet support governance (social and economic domain), practical Internet governance (political and social

domain) and other sections. Research on Internet management models at the global and local level and new governance structures is being actively carried out.

1.2 Settling Disputes on Domain Names

For a faster settlement of domain disputes, supporting evidence such as the applications and letters of the parties involved in the disputes can be submitted online and the arbitrator can swiftly carry out the process through document screening.

An average period of 2 years is required to settle a case, whereas in cases of settling by arbitration cases, an average period of 50 days is required. The Korea Domain-Name Dispute Resolution Committee has 14 professional domain-name dispute arbitrators including experts from universities and research institutes, lawyers and patent attorneys. As of the end of 2003, 80 cases out of a total of 103 cases of dispute resolution complaints had been resolved (37 cases were removed, 34 cases cancelled, 9 cases dismissed), and 11 cases succeeded in reaching a settlement between the parties involved in the disputes.

1.3 New URI Environment

Recently, under the general concept of URI (Uniform Resource Identifier), there are ongoing debates concerning the various identification and approach system of the next generation Internet, and active discussions are also taking place over the following issues; 1) the International Domain Name System (iDNS), which allows non-English speakers to navigate the web by supporting their local language characters without using the plain English text (ASCII; 2) protocol ENUM (Telephone Number Mapping) that provides a variety of integrated services in a wireless Internet environment by converting the telephone number to URL; 3) and the mobile address system which is an approach that uses numbers. On the other hand, to ensure that digital content is efficiently delivered on the Internet, a standard identification system is being developed and a basis for a national URN is being created.

2. Policy for the Next Generation Internet

2.1 IPv6

■ Network Construction Policy

There are plans to construct a convergence test network of wired and wireless network (KOREAv6) and verification tools and techniques related to the IPv6. The backbone network will use the IPv6 network of KOREN and be linked with domestic and overseas IPv6 networks through the 6NGIX. There are also plans to construct an access network for subscribers such as the IPv6 exclusive network line, public wireless LAN network, xDSL network, CATV networks, mobile communication network and other access networks by incorporating key telecommunication carriers.

■ Providing and Promoting Services

In order to promote the development and provision of IPv6 application services, the facilitation of the next generation Internet service is being explored in the following ways. First, develop an IPv6-based P2P application and launch an IPv6-based home network trial service in liaison with home network businesses and FTTH pilot project. Second, develop an All IPv6-based VoIP service by gradually connecting WLAN (2.4GHz, 5GHz), mobile communication network, fixed-line or PSTN, and provide a high-quality IPv6-based Internet education service for elementary, middle schools, high schools and universities. Third, develop an IPv6-based telematics application service through a composition of various factors such as ITS, Mobile IPv6, mobile communication network, sensor network, location-based or wireless LAN, and develop and embrace wired and wireless e-Government services based on IPv6.

2.2 Home Network

A home network is a future-oriented family environment where all information electronic home appliances are connected to wired and wireless home networks in which anyone can have access to various home network services from any place at any time. Home networks are being promoted by many industries including the communication, broadcast, and construction industy in various ways. The government is planning to transfer 10 million households, 61% of all households, into a digital living space where various services can be provided by constructing home network by 2007.

Construction industries are planning to cooperate with electronic home appliance companies and ISPs to deliver the early stage of home network services, based on the experience of building cyber apartments that realized home-automation and remote control service for home-information devices. In the case of some luxury apartments, home gateways and Internet information devices are built into the building's structure and the early stage services such as home-automation service are being offered. In addition, telecommunication carriers and

broadcasters are competitively pushing ahead with their business strategies to create new sources of profit in response to the convergence trend of broadcasting and communications. The networks of broadcasting companies are going digital, and telecommunication carriers are exploring new business domains by providing a two-way multimedia service based on the existing wired and wireless network and satellite infrastructure.

2.3 u-Sensor Network

Recently, electronic tags and sensing technology is drawing much attention as next generation technology. This technology is used to check information of objects by attaching electronic tags to them. Electronic tags and sensing technology are the core technology of the government's project to foster new growth in the IT industry, and under the evaluation that it has big technological ripple effects and a large application area, a 'u-life policy' was established and is being promoted. According to the implementation plan, by the year 2005, a passive and active electronic tag product is to be developed and will start to be spread in line with formation of a foundation and standardization.

By 2007, low-powered, micro communication tags that allow communication between electronic tags installed with sensing functions are to be developed so that sensor network services can be provided by 2008. The development of u-Sensor Network technology is expected to be gradual as its adoption in the market depends on the development of the electronic tag technology in aspects such as price, size and function of the chip. If the electronic tag can be cheap and minitaurized but more intelligent, its application in every day life will be expanded in areas such as logistics, distribution and environment, clothes and food management.

■ Technology Development Policy

The leader for constructing the u-Sensor Network and the gradual development of tag technologies will be pursued through cooperation of industry, academia, and research institutes with government-funded research institutes at the center. Passive and active electronic tags will be developed by 2005, sensing type tags by 2007, and core technologies of ubiquitous sensor network and system by 2010.

■ Frequency Policy

Frequency for electronic tags used for constructing the u-Sensor Network basically uses the ISM bandwidth, but some frequency bandwidths cannot be supplied for electronic tags as frequency allocation varies by countries. Therefore, as for the 860~960MHz bandwidth that was suggested to be used for a Global TAG, the allotment of 910~914MHz return bandwidth of CT-2 is being considered as an alternative. And obstacles will be overcome by easing the regulation on the power output limitation.

2.4 Revenues in telematics

Revenues in the Korean wireless Internet market exceeded 2 trillion won in 2003 and the 'communication network evolution' that is heading for a Broadband convergence Network in order to accommodate various wired and wireless communication networks is accelerating the growth of the telematics market. The telematics industry in cooperation with the automobile

industry and mobile carriers, is expected to grow into a comprehensive information communication service industry that has related services with various traditional brick and mortars industries such as handsets, tool manufactures, SI, contents, safety, insurance, pre-owned cars, rental cars, and automobile repairs. Hence, the government, with the Ministry of Information and Communication (MIC) and the Ministry of Commerce Industry and Energy (MOCIE) at the center, is planning support measures to foster telematics as the core industry of next generation growth engines.

In Korea, Daewoo Motors first introduced Dreamnet services in 2002, followed by Nate Drive Service of SKTelecom, and Hyundai Motors recently released Mozen service. It is expected that 3.7 million cars, 23% of all cars registered, are to be equipped with telematics by 2005. As an infrastructure of telematics, Intellectual Transport Society and Location-based Services are being actively promoted, and telecommunication providers are working hard to secure related basic solutions. Also, Hyundai Motors, Samsung Renault Motors, Ssangyong Motors are making heavy investment in enabler technologies. In this process, the Korea Telematics Business Association (KOTBA) was launched to realize strategic partnerships between different industries and a community consisting of 30 different companies including major equipment companies, insurance companies, the three main mobile carriers and major motor companies was formed.

Table 3-01 **Eleven Main Telematics Projects**

	Plan of operation
1	Developing core technologies of telematics
2	Constructing industry clusters
3	Building R&D Hub
4	Supporting domestic standardization and leading international technology standards
5	Constructing a telematics information center(TELIC)
6	Constructing a testbed
7	Constructing a pilot city
8	Expansion of terminal installation
9	Policy on tax and fees for the expansion of service
10	Operating a cooperative system for related organizations
11	Fostering professional manpower

Source: Ministry of Information and Communication(MIC), Dec. 2003

The main works of the government in order to promote telematics services are launching core technology development projects, building an effective telematics industry cluster to create a cooperative system between different sectors, establishing an R&D cooperation system centered around Daeduk research center, and leading the efforts in domestic and international standardization activities. The total budget for these works is approximately 328.1 billion won.

2.5 National Grid Policy

Grid refers to an information and communication infrastructure that allows highly effective research resources, such as supercomputers, large capacity storage devices, high voltage electron microscope and others, to be selected on a user demand basis and for those resources that were selected like a local system to be easily used. Korea implements the policy on grid computing to integrate the grid industry with high-tech industries like bio and nanotechnology.

The key accomplishments of 2003 are △ the construction of computing grid database with the participation of 9 institutions including Seoul National University and Pohang University of Science and Technology △ ten test grid application researches including a bio grid aimed at finding a grid based industrial science technology application research model △ the development of a grid portal protocol type mainly for bio and nanotechnology grid

users △ the implementation of APEC APGrid construction △ a joint research on grid computing with iHPC of Singapore.

3. Internet Business Policy

3.1 Promotion of Internet Business

Internet-related the third quarter of 2003, the Internet supporting industry has grown by 10.1 trillion won and Internet application industries, such as Contents, e-Business (only open types are included in cases of B2B), have grown by 58.8 trillion won. Especially, the 'dot-com' industry (Internet application industry) has grown enormously in spite of a long economic slump.

In order for Internet businesses entering development stages to continuously develop, cooperation is required between the government and the industry to create a better business environment, protect consumers, and prevent adverse effects. The government is publicizing easier Internet service access for people in their 40s and 50s to help them access services needed in everyday life, since only business models for 10~20s (game, avatar, messenger) have been developed. Also for Internet enterprises that have superior technologies and business models but a weak management foundation, consultations on financial strategies and fund raising were held and through investment exhibitions a total fund of 9.2 billion won was raised.

3.2 Towards an Active m-Commerce

The gateway of mobile communication companies has been opened so that more portal providers and independent content providers (CP) can directly connect to wireless Internet networks and provide individual services. In short, by requiring three mobile carriers to outline terms and conditions that allow their gateways to be used by third parties, many portals have entered into the m-Commerce market in equal terms with mobile carriers, and introduced services interlinking wired and wireless platforms.

The terms and conditions for using gateway allow CPs, who are linked to the gateway, to use platform information, terminal information, location information, which were used only by mobile carriers or exclusive CPs. And upon the request of the linked CPs, mobile carriers are obliged to collect service fees from the end-user for the contents or services provided by those CPs on their behalf, so in the near future the appearance of more various and new m-Commerce services can be expected.

In addition, number portability has been enforced so people can keep their own numbers even if they switch the mobile carrier. As a result of this, the lock-in effect has been eliminated, inducing mobile carriers to provide more diverse m-Commerce contents and services.

4. Information Protection Policy

4.1 Creation of an Environment to Protect Information and Communications Infrastructure

■ The Protection of Major Information and Communications Infrastructure

The government established and enforced the Information Infrastructure Protection Act in January 2001 to protect major information and communication networks in finance, communications, transportatiory, energy the government, which have a significant influence on national security and the economy, from cyber attacks such as hacking and computer viruses. Especially in May 2003, emergency guidelines were distributed to allow people to swiftly counter cyber attacks against major information and communication facilities. Also, in response to the possible cyber crimes that are becoming increasingly more sophisticated over time, the organization responsible for managing information and communication facilities came up with information protection measures and introduced a policy to designate a consulting company for information protection in order to build a system to use advanced technologies of the private sector. In the future, in hopes to enhance service quality and reliance on professional information protection enterprises, there are plans to reinforce education training of technical manpower and internal protection measures. In this regard, there are 89 information and communication infrastructure facilities, which have been appointed by the government since 2001.

■ Hacking Virus Prevention and Countermeasures

In December, there were a total of 26,179 reported cases of hacking attacks in korea, and damage reports due to computer viruses record 85,023 cases. When compared with the same period in 2002, hacking has increased by 50% and virus attacks have increased by more than 100%.

As information and communication systems of key infrastructures are interconnected, even cyber threats such as hacking are being interconnected and shared. This kind of advanced information infrastructure environment has become the target for international hackers. Therefore, in order to effectively confront increasing cyber attacks, the Ministry of Information and Communication, along with the Korea Information Security Agency, is issuing alerts and early warnings regarding hacking attacks while supporting the operation of CERT to accelerate people's autonomous information protection activity.

In this regard, the government is planning to advance the cyber terror response system through joint action with the private sector, and to strengthen the efforts to tackle global cyber terrorism.

■ Toward the Active Use of Digital Signatures

To ensure the safety and reliance of electronic transactions and information distribution using the Internet, the government enacted the Digital Signature Act. The Digital Signature Act

introduced the concept of authorized electronic signature, which recognizes the same legal validity with a handwritten signature, and this law stipulates safety requirements that should be met. The authorized digital signature is verified by a digital signature certificate, which is issued by the accredited certification authorities. The current technology of authorized e-signature is based on an asymmetrical encryption technology.

Without regard to the issuing organizations, the government introduced an interlinking system that allows various electronic transactions to take place using just one authorized certificate. As the importance of digital signatures started to grow, certificate users that only numbered 50,000 at the end of 2000, exceeded 8.71 million at the end of December 2003 and the number of agencies that introduced authorized certificates increased to 390.

Korea at present, have people actively using digital signatures in Internet transactions such as e-Procurement and bidding, Internet banking, on-line stock transactions, e-Government services. It is expected that in the future, by using authorized certificates, people will be able to make safer electronic transactions in various fields by increasing the use of digital signatures in fields such as online payment and medical treatment.

4.2 Protecting Personal Information and Establishing a Sound Cyber Culture

■ Protecting Personal Information

Due to the increase in Internet users, building a healthy information society has become an important issue. In order to strengthen the protection of personal information, a foundation of laws and polices such as the Personal Information Dispute Mediation Committee (PICO) has been established. Also, the government set up a guideline, which it is distributing accross the industry that specifies the relevant laws and regulations for enterprises to abide by, in order to establish a self-regulation environment. A part of this initiative, the government has outlined a 'policy to protect the personal data of clients who have terminated contract with a mobile carrier'. On the other hand, by providing 'technical and administrative guidelines for preventing personal data violation,' and 'privacy mark system,' the possibility of abusing personal data has been blocked.

■ Ensuring a healthy information culture

In order to regulate mobile phone spam text messages, the government limited spam messages

Table 3-02 Current States of Authorized Digital Signature Users

(Unit: Persons)

Authorization certificate Issuing Agencies	2001	2002	2003
Korea Information Certificate Authority Inc.	260,996	558,806	771,272
Korea Securities Computer Corp.	281,634	748,840	1,865,042
Korea Financial Telecommunication and Clearings Institute	1,363,016	3,925,522	5,249,970
National Computerization Agency	11,992	485,388	697,857
Crosscert.Inc	-	53,092	117,803
Korea Trade Network	-	857	11,285
Total	1,917,638	5,772,505	8,713,229

Source: Ministry of Information and Communication(MIC), Dec. 2003

by amending the terms and conditions of the end user agreements in October 2003 among the three main mobile carriers so that no text messages can be sent without the consent of the user. Also to enhance a healthy information culture, in 2004, the government plans make information and communication service providers liable for the circulation of illegal and harmful information, implement an opt-in method for cellular phone spam and to improve the legal system to enhance the control of violators of the law and giving a more severe penalty. Also, countermeasures will be taken to confront harmful information circulation, and the 'evaluation system for self-regulation by service providers' will be introduced to allow the Information Communication Ethics Committee (ICEC) to monitor and deliberate the circulation of harmful telephone information services such as one-to-one indecent phone call service.

4.3 Laying the Foundation for the Information Security Industry

■ Technology Development and Standardization

Information security technology prevents information leaks, and forgery over communication networks, and these days, countries around the world increasingly focus on nurturing this technology. As for Korea, in 2004, the government will push ahead with the development of advanced network information security system, harmful information blocking system, and human recognition technology, investing 24.9 billion won, and from 2004 to 2007, it will place focus on the development of information security technology as a core strategic area.

■ Cultural Campaign for Information Security

For a year, in 2003, the government started education on information security by providing various curriculums to workers of information and communication industries and to the general public. In 2004, a Specialist for Information Security (SIS) system and various education programs will be introduced to constantly raise the awareness and level of information security.

■ Evaluating the Information Security System

In order to verify and safely construct the information security system, an information security evaluation system is being implemented. Starting with the evaluation of intrusion blockage system, the scope of subjects to be evaluated was expanded to include virtual private network products, operation security system, fingerprint recognition system and smart card. Also, in order to quickly correspond with evaluation systems that are being internationally standardized, Korea will outline the Common Criteria (CC) and make continuous efforts to secure CC-based evaluation technology, improve the evaluation system and to strengthen manpower.

4.4 Bridging the Digital Divide

■ Current Status of the Digital Divide

With the development of information technology, the widening gap between the technology-enabled and the technology-deprived has emerged as a new social problem. As a result, the government enacted an 'Act on Resolving the

Digital Divide' and has made vigorous efforts to reduce the information discrepancy such as providing a computer training to 10 million people, but it appears that neglected groups such as low-income households, the disabled, the elderly and people with a lower education have a significantly lower percentage of Internet users compared to the its Internet sawy group (information leading group). According to age group, academic background, vocation and the presence of a disability, the gap ranges from a low of 36.55% to a high of 80.3%. The discrepancy in the percentage of Internet users among those with and without disabilities, and those in their youth and elderly ranging from age groups between 10~50 years old, are each 37.0% and 82.1%, which are higher than the 14.8% and 31.5% of the U.S.. Also, the gap in Internet user proportion among those with and without disabilities, and those in their youth and elderly ranging from their 10s and 50s, is by 1.7 times higher than the average discrepancy level of advanced countries such as the U.S. and the U.K..

■ Efforts to Resolve the Digital Divide

In order to bridge the digital divide, the government set out a comprehensive government-wide digital bridge plan. In accordance with this plan, in 2004, 13 Ministries including the Ministry of Education and Human Resources Development are establishing and promoting a joint action plan to narrow the digital divide.

Table 3-03 **Current Status of the Digital Divide (based on the Internet Usage Rate)**

Category	Presence of disability	Gender	Age	Academic background	Income	Vocation	Region
Compared group	Total population	Male	20's	University graduates or higher	More than 2.5 million won	Office work	Big cities
Proportion of Internet users (%)	64.1	70.7	94.3	87.7	76.4	88.7	66.1
Weak group	Disabled	Female	Above 50's	Middle school graduates or lower	Less than 1.5 million won	Production work	District regions
Proportion of Internet users (%)	27.6	57.5	14.0	8.0	40.1	31.8	44.2
Discrepancy (% p)	36.5	13.2	80.3	79.7	36.3	56.9	21.9

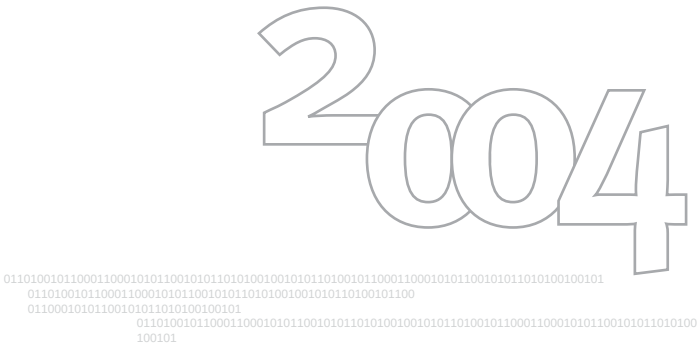
※ 1$ ≒ 1,200 won

Source: Korea Agency for Digital Opportunity and Promotion(KADO), Jun. 2003

Table 3-01 2004 Action Plan to Bridge Digital Divide

Orgranization	Content
Ministry of Education and Human Resources Development	Support of PC and communication fees for children in low-income households
Ministry of Foreign Affairs and Trade	Provide support in bridging digital divide in developing countries
Ministry of Justice	Provide information education for prisoners and children under juvenile protection
Ministry of Government Administration and Home Affairs	· Establish a test cyber town · Provide Information Education for local residents and public service personnel
Ministry of Culture and Tourism	Establish information DB for the visually impaired
Ministry of Agriculture and Forestry	· Support agriculture, informatization of rural areas, and e-Commerce of agriculture products · Information education for farmers · Expand support system for shipping and consultation system for farming
Ministry of Information and Communication	· Construct broadband networks in agriculture and fishing areas · Expand reduction of mobile phone fees for low-income groups and the disabled · Support establishment of free-of-charge information facilities · Provide support for PCs, support devices for the disabled, digital TVs · Develop and supply contents for the elderly and disabled · Provide information education for isolated groups · Carry out international cooperation to bridge digital divide
Ministry of Health and Welfare	Provide information education for the elderly
Ministry of Labor	· Provide information education for workers and the disabled · Operate employment information system for the disabled
Ministry of Gender Equity	· Provide advanced IT education for women · Hold digital contents' exhibition for women
Ministry of Maritime Affairs and Fisheries	· Provide information education for fishers · Establish an information community in fishing areas
Small and Medium Business Administration	· Provide information education for workers of small to mid-sized businesses · Construct a foundation for informatization in regions where many small to mid-sized businesses are located

Source: Ministry of Information and Communication(MIC), Dec. 2003


2004

1. Internet Content

1.1 Portal / Community

Web portals have been expanded to include not only search engines and directory services but also communication services (chatting, e-mails etc), community services (special interest clubs), entertainment (online games, VOD, Sports etc), information services (finance information, news etc), and online shopping. Furthermore, platforms have diversified from PCs to mobile handsets such as mobile phones and PDAs. The convergence of telecommunications and broadcasting is predicted to become a widespread phenomenon in the future. The domestic web portal industry posted record earnings growth in 2003 as leading companies diversified their revenue sources by charging for previously free services, attracting more advertisers, and receiving commissions from e-Commerce transactions. In line with this trend, the intense competition among leading web portals have led them to expand their mobile content offerings after mobile phone companies were ordered by the government to open their networks to third parties. Web portals have seized this new opportunity to beef up their entertainment content which also includes games and have also rolled out knowledge search services.

1.2 Online community

In 2003, online community experienced rapid growth and change. In particular, there are now over 6 million online communities hosted by numerous web portals. Furthermore, with the introduction of blogs, communities now feature personal online diaries, online photo albums, and video broadcasting. Blogs have also expanded into the wireless platform so now people can access a mobile blog (moblog) on their mobile phones.

In the past, many online communities were formed among close friends but the current communities are centered around people who share similar interests.

1.3 Game

The size of the domestic gaming market is approximately 4.43 trillion won and has posted a growth rate of 10.1%. The online gaming market is a 704.2 billion won-market that has a higher growth rate of 28 %. Korean online games account for 7.1% of the global online gaming market. In 2003, online games were exported to China, Taiwan and Southeast Asia countries. In 2003, Korean online games accounted for 60.8% of the total game export and compared to last year there has been a growth rate of 906%. As the domestic game market is expected to become saturated in 2006 or 2007, companies are focusing their strategies on foreign markets such as Southeast Asia.

1.4 Entertainment

■ Digital music

Total sales for the digital music industry grew to 185 billion won in 2003, which is a 37.6% increase from the previous year. The digital music market depends on wireless content (ringtones) for 70% of its sales. On the other hand, the market for streaming music and downloading songs is experiencing difficulties in wooing consumers due to the proliferation of free file-sharing services. As conflicts deepened between the online music services and record companies, the government gave the order that all online music services must charge a fee and pay licensing royalties for each song. Except for Bugs Music, the largest streaming music company, all other companies began to charge a fee for their services. However, none of them became profitable since Bugs Music refused to follow the government's order and still remains the largest and most popular service provider. The online music market still has a long way to go as it struggles with the problems posed by free music sites, file-sharing sites, and the reluctance of users to pay for songs that they can download for free on the Internet.

■ Internet movies

Domestic online movie market has grown from 70 billion won in 2002 to 80 billion in 2003 and total online movie website number over 300. Recently, online movie websites have been showing movies before or at the same time when the movie's video or DVD have been released. In the case of the movie "Desire," it was released at theaters and shown on online movie websites simultaneously for the first time in Korea. Meanwhile, the revenue structure of the online movie websites is changing. The sales ratio for adult movies and domestic feature movies was about 6:4 in 2002 but changed to 3:7 in 2003. This

Table 4-02 Revenue Portfolio of the Digital Music Providers (unit: million won)

Classification	Online		Offline	Total
	Wired	wireless		
Revenue	12,397	130,356	42,275	185,028
Proportion	6.7%	70.5%	22.8%	100%

Source: Korea IT Industry Promotion Agency, Dec. 2003

Table 4-01 Game Market Forecast

(Unit: 100 million won)

Classification		2000	2001	2002	2003	2004	2005	2006	2007	annual growth rate
Online game		1,628	2,985	4,656	7,042	9,330	11,168	12,406	13,145	28.0%
Mobile game		17	497	727	1,352	2,474	4,125	6,422	9,491	63.5%
PC game		1,323	1,810	902	1,275	1,276	1,277	1,278	1,278	-5.6%
Arcade game		5,844	3,528	4,142	3,984	3,894	3,830	3,782	3,745	1.0%
Console game	H/W	18	29	1,012	1,015	1,512	1,649	1,947	2,238	106.3%
	S/W	72	117	898	943	1,009	1,435	1,700	1,973	60.1%
	Total	90	146	1,910	1,958	2,521	3,084	3,647	4,211	75.1%
Subtotal		8,902	8,966	12,337	15,611	19,495	23,484	27,535	31,870	23.5%
Online Internet caf'e		13,343	19,832	19,441	22,763	23,873	24,446	24,731	24,870	3.8%
Computer game room		8,634	5,969	6,570	5,928	5,703	5,543	5,422	5,329	-1.9%
Total		30,879	34,767	38,348	44,301	49,072	53,473	57,688	62,069	10.1%

※ 1$ ≒ 1,200 won

Source: Korea Entertainment System Industry Association, Dec. 2003

indicates that there is more demand for domestic feature movies. The success of the online movie market will be determined by such factors as piracy, viewing environment, marketing, competition, hardware performance, and image and sound quality.

1.5 Internet media

■ Online newspaper/webzine

The competition in the online news business intensified in 2003. The online versions of the major dailies were threatened by Internet-only news websites. Some major dailies like "Joins.com", the subsidiary company of Joong Ang Daily and "Naver" agreed to form a strategic partnership to share content and provide each other with technical assistance. Such efforts to forge alliances among competitors have enabled companies to serve the market with more news content while showcasing cutting-edge multimedia technology.

In terms of performance, the Internet ventures of the major dailies recorded losses while Internet-only news websites became profitable. The Internet-only news companies have been able to diversify their revenue stream while reducing their dependency on advertisements. Furthermore, companies such as "OhmyNew.com" became an influential media company. Politically conservative-leaning Internet-only news websites also emerged in 2003 to challenge the majority of liberal-leaning news websites. However, these conservative websites were swiftly challenged by the established liberal players on a wide range of political and social issues.

■ Internet Broadcasting

Korea's Internet broadcasting industry started to grow in 2000 and reached its peak during 2001. The market stabilized in 2003. The Internet broadcasting business has experience many difficulties in many areas including the quality of content, cutthroat competition, business performance and government regulations concerning adult-oriented websites

As of 2003, the number of Internet broadcasting companies decreased drastically from previous years, and the Internet broadcasters accounted for 80% of the total of 719 Internet broadcasting-related companies while the remaining 20% were shared by broadcasting solution providers and production companies. The size of the industry has also declined. According to industry experts, the smaller and less profitable companies exited the market during the period of intense competition while only the larger companies that were able to weather the market downturn were able to survive and remain in the market today. In terms of broadcasting content, 28% of all content was entertainment content followed by educational content at 14.3% that targeted young school children. Among entertainment content, music was

Table 4-03 2003 Top On-line Newspaper Sites

(unit: persons)

Rank	Site	No. of Visitors
1	chosun.com	8,573,765
2	imbc.com	8,135,012
3	kbs.co.kr	7,855,645
4	joins.com	7,687,431
5	sbs.co.kr	6,587,180
6	donga.com	4,862,305
7	sportsseoul.com	4,807,197
8	stoo.com	4,504,887
9	hot.co.kr	4,426,054
10	mk.co.kr	3,867,551

Source: KoreanClick, Dec. 2003

the leading item and the large broadband subscriber base in Korea helped create momentum for Internet broadcasters who streamed movies and video to paying customers.

Table 4-04 Internet Broadcasting Industry

Classitication	2001	2002	2003
No. of companies related to Internet broadcast	1,218	865	719
Revenue of Internet broadcasting industry	500 billion won	427.9 billion won	250.8 billion won

※ 1$ ≒ 1,200 won Source: Korea Webcasting Association, Dec. 2003

Table 4-05 Classification of Internet Broadcasting

(Unit: Number of cases, %)

Classification	No. of Internet broadcasts	Proportion (%)
Education/Study	66	14.3
Vocational education	29	6.3
School	44	9.5
Sports	14	3.0
Animation	6	1.3
Entertainment	14	3.0
Movies	21	4.5
Music	60	13.0
Games	4	0.9
Other amusements	11	2.4
Public institutions	12	2.6
Companies/Organizations	10	2.2
Society/Culture/Welfare	30	6.5
Regional information/Living information	50	10.8
Current issues/Economy/Management	22	4.8
Arts	5	1.1
Religion	18	3.9
Teens	11	2.4
Hobby/Leisure	26	5.6
News	4	0.9
Health/Medicine	5	1.1
Total	462	100.0

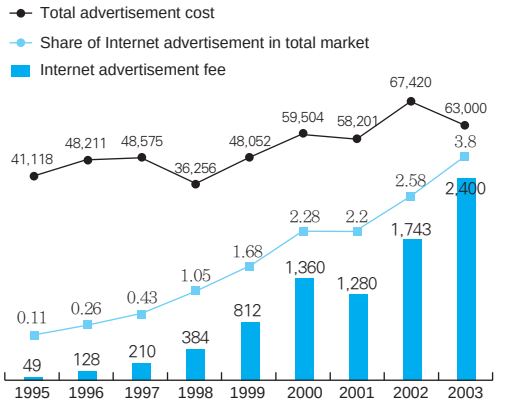
Source : IT Public Webcasting (http://www.webcst.or.kr), Dec. 2003

■ Internet Advertisements

Cross media advertisements that incorporate both online and traditional advertising methods has gained popularity. The Internet advertisement business remained strong as more companies chose to advertise their products online. According to a recent survey taken among advertisers, advertising on the Internet ranked second to TV advertisements as the most cost-effective and favorable medium. The actual money spent on Internet ads is still substantially lower than what advertisers spend on TV ads. However, the share of Internet ads in the overall advertising market is steadily growing. The Internet advertisement market grew by 38% in 2003 and the total volume reached 240 billion won. And if the 95 billion won from keywords search services are added, the market grew even larger than before. In 2003, the keyword advertising market grew by 260% compared to 2002.

Figure 4-01 Internet Advertisement Market Volume Vs. Overall Advertisement Market

(Unit: Billion won, %)



※ 1$ ≒ 1,200 won Source: IT Public Webcasting, Dec. 2003

1.6 Education content

The domestic e-Learning service of the industry market has grown from 30 billion won in 2001 to 78 billion won in 2003. The public education sector grew from 10 billion won in 2001 to 30 billion won in 2003, while the elementary, middle and high school education market grew from 32 billion won in 2001 to 130 billion won in 2003. In particular, it was shown that about 15.2% of domestic companies have introduced online training to educate their staff. Included in the benefits of online education are, improvement in job performance, reduction in training costs, better evaluation of employees, and a boost in morale among employees. Meanwhile, e-Learning companies adopted various strategies to adapt to the changing environment and strengthened their business partnerships with other industries. Furthermore, educational courses that can be delivered over mobile phones and PDAs is also being tested. The government has been exploring the implementation of supporting policies to promote the online education market. For example in December 2003, the "Promotion Act for the e-Learning Industry" was enacted. This act ensures that there is no discrimination between online and traditional forms of education and thereby encourages the active use of online education in educational institutes. In this regard, the government plans to pursue various policies that will help companies introduce an online education system while public institutes will also include online education in their courss.

2. e-Commerce

The total size of e-Commerce in 2003 was 235.25 trillion won. This is a 32.2% increase from 2002. B2B comprised 88% of all e-Commerce trade (206.854 trillion won) while B2G captured 9.2% of all transactions (21.634 trillion won). B2C came in last place with only 2.6% of the entire e-Commerce market (6.95 trillion won). Compared to 2002, B2B increased by 32.8% (51.147 trillion won), B2G by 30.1% (5.2 trillion won) and B2C by 20.9% (1.52 trillion won)

2.1 B2B

In 2003, the B2B market became a 206 trillion-won market posting a 32.8% increase from the previous year. A close look revealed that buyer-driven transactions came to 150.69 trillion won, taking up 72.8% of the total B2B market. This is a 33.1% increase on a year-on-year basis. Supplier-driven transactions increased by 33.6%, reaching a volume of 48.77 trillion won. Middle trader-driven transactions only recorded 7.4 trillion won, an increase of 24.5% from the previous year while only accounting for 3.6% of the total market.

Meanwhile, 96.4% of all B2B activity was

conducted over the Internet, indicating that Internet-based commerce will remain the most common form of commerce. The manufacturing industry is the leading industry in terms of volume after posting 37.939 trillion won (77.8%) in sales and followed by the electricity and electronics industries (32.8%) and primary metals such as steel (33.9%) make up two-thirds of the total market. Meanwhile at the end of 2003, the number of e-Marketplaces came to 260 and international trade had the most with 37 followed by electronics with 32, mechanical and commercial equipment with 31. The maintenance/repair/operation (MRO) sector had 24 e-Marketplaces, agricultural and marine area and food and drink sector had 22. Trading volume at e-Marketplaces in 2003 reached 7.4 trillion won, and according to business sector, the MRO (2.182 trillion won, 29.5%) led the industry followed by construction and building materials (1.362 trillion won, 18.4%), chemicals (1.24 trillion won 15.3%), and steel (697 billion won).

2.2 B2C (Shopping Mall)

The domestic B2C market that used to rely heavily on advertising to drive sales is now witnessing a new shift in the market as web portals have also set up online shopping sites in addition to rolling out fee-based content. The success of the large e-Retailers drove the growth of the B2C market in Korea. In recent years, the domestic B2C market increased by 20.9% (1,052 billion won) to generate about 6.95 trillion won in sales.

As of the end of 2003, large e-Retailers accounted for only 11% of total sales in the B2C market. However, in terms of sales volume, e-Retailers comprised 72.4% (5 trillion won) of all sales. Thus, small specialty e-Retailers are losing

Table 4-06 Volume of e-Commerce

(Unit: Billion won, %)

	2002		2003		Year-on-Year	
		Ratio		Ratio	Increased amount	Increase rate
Total volume of e-Commerce	177,810	100.0	235,025	100.0	57,215	32.3
Business to Business (B2B)	155,707	87.6	206,854	88.0	51,147	32.8
Business to Government (B2G)	16,632	9.4	21,634	9.2	5,002	30.1
Business to Consumer (B2C)	5,043	2.8	6,095	2.6	1,052	20.9
Others	427	0.2	442	0.2	15	3.5

※ 1$ ≒ 1,200 won

Source: Korea National Statistical Office(NSO), Feb. 2004

Table 4-07 Size of e-Commerce according to traders

(Unit: Billion won, %)

	2002		2003		Year-on-year	
		proportion		proportion	Increased amount	Increase rate
B2B	155,707	100.0	206,854	100.0	51,147	32.8
Buyer-oriented	113,254	72.7	150,688	72.8	37,434	33.1
· Open	23,281	(20.6)	34,270	(22.7)	10,989	47.2
· Cooperative	89,973	(79.4)	116,418	(77.3)	26,445	29.4
Seller-oriented	36,509	23.4	48,766	23.6	12,257	33.6
· Open	4,430	(12.1)	6,279	(12.9)	1,848	41.7
· Cooperative	32,078	(87.9)	42,487	(87.1)	10,409	32.4
Broker oriented	5,944	3.8	7,400	3.6	1,455	24.5

※ 1$ ≒ 1,200 won

Source: Korea National Statistical Office(NSO), Feb. 2004

Table 4-08 e-Market Place; Scale and Scope (third/fourth quarter)

(Unit: Number, Billion won, %)

	e-Marketplace			
	No. of companies		Amount of transaction	
		Ratio (%)		Ratio (%)
Total	260	100.0	7,400	100.0
Chemicals	20	7.7	1,124	15.2
Construction (Materials)	16	6.2	1,362	18.4
Agriculture, livestock, fishery products / Food & beverages	22	8.5	609	8.2
Steel	9	3.5	697	9.4
MRO	24	9.2	2,182	29.5
Textiles, clothes	12	4.6	11	0.1
Trade	37	14.2	187	2.5
Healthcare	11	4.2	337	4.6
Oil	5	1.9	432	5.8
Machinery and industrial material	31	11.9	113	1.5
Electronics	32	12.3	313	4.2
Others	41	15.8	34	0.5

※ 1$ ≒ 1,200 won

Source: National Statistical Office (NSO), Feb. 2004

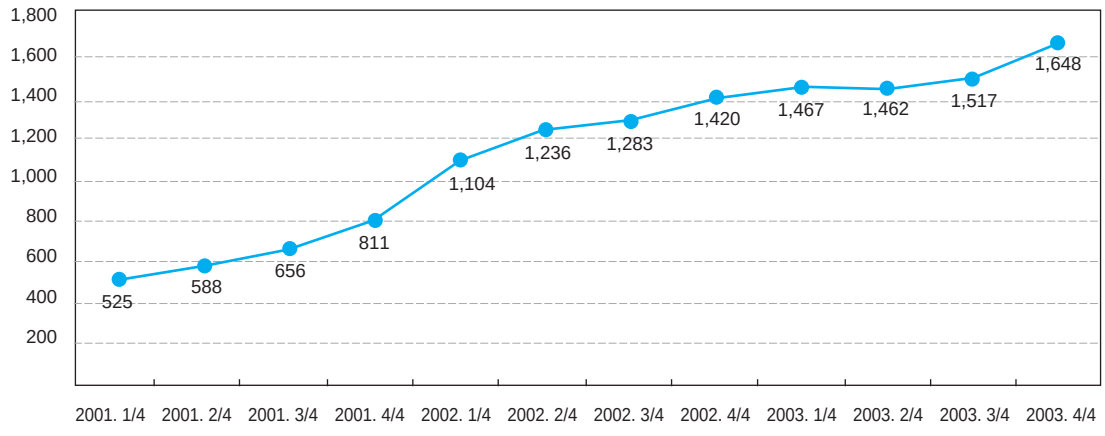
market share while a handful of large e-Retailers are dominating the market.

A breakdown of B2C trade shows that appliances/electronic/communication equipments (18.3%) was the leading category among consumers and was followed by computer and related equipments (12.9%), daily equipments/car equipments (11.6%), clothes/fashion and related products (10.3%), and travel and reservation services (7.4%).

With an average yearly growth rate of 100%, B2C is rapidly becoming a legitimate and profitable distribution channel along with cable shopping channels.

Figure 4-02 B2C Market Volume

(Unit: Billion won)



※ 1$ ≒ 1,200won

Source: National Statistical Office(NSO), Feb. 2004

2.3 B2G

In 2003, the volume of trade in the B2G market increased to 21.63 trillion won, which is an increase of 5.2 trillion won (30.1%) from the previous year. These numbers indicate that online bidding is becoming a standard procedure in the government procurement process. A breakdown of the types of trade showed that building materials had the largest share at 3.6 trillion won (42.8% of all B2G transactions), followed by tangible goods at 2.6 trillion won (31.0% of all B2G transactions), while equipment and machinery came in at 1.233 trillion won (14.7% of all B2G transactions).

2.4 Financial trading service

■ Internet banking

As of December 2003, Internet banking services were provided by 21 financial institutions (18 domestic banks, Citibank, HSBC and the national post office). In 2003, about 22.75 million people were registered as users of Internet banking services, which is an increase of 27.8% compared to 2002. About one million businesses are using online banking services recording a sharp increase of 44.2% compared to 700,000 in 2002.

Through online banking services, customers can check the balance in their accounts, make a wire transfer, apply for a loan, open a savings account, as well as send money to a foreign-based account. In addition, more banks are providing services such as accounts aggregation, electronic bill present and payment (EBPP), and mail banking.

In December 2003, the number of online transactions exceeded 6.16 million which means that over 85.3% of all bank transactions were conducted over the Internet. The number of transactions of electronic funds reached 1.06 million, accounting for 14.6% of all online transactions. Online applications for loans were miniscule in comparison to other online transactions. It only composed 0.1% of the total. However, 49.3% of these online loan applications were approved.

In December 2003, there were 2.56 million

Table 4-09 Market Volume by Medium

(Unit: 100 million won)

Classification	2002	2003	Year-on-year increase rate
TV home shopping	37,810	36,980	-2.2%
B2C	50,434	60,950	20.9%
Catalogue	11,510	7,000	-39.1%
M-Commerce	280	340	21.4%
Total	87,300	96,270	10.2%

※ 1$ ≒ 1,200won

Source: Korea e-Commerce & Direct Marketing Association (KEDMA), Feb. 2004

Table 4-10 B2G e-Commerce Volume

(Unit: Billion won, %)

	2002		2003		Year-on-Year	
		Rate		Rate	Increasing or decreasing amount	Increasing or decreasing rate
G2B	16,632	100.0	21,634	100.0	5,002	30.1
- Purchase of goods and services	6,792	40.8	8,411	38.9	1,619	23.8
- Construction	9,840	59.2	13,223	61.1	3,383	34.4

※ 1$ ≒ 1,200 won

Source: National Statistical Office(NSO), Feb. 2004

mobile banking transactions. The mobile banking service is provided by domestic banks and the post office. The number of mobile transactions using this service more than doubled since the year before. This is mainly because of the Bank-On Service of Kookmin Bank that was launched in September 2003. The Bank-On Service allows users to use his or her mobile phone to pay for public transportation fees, conduct transactions over a mobile phone, and withdraw money from an ATM machine.

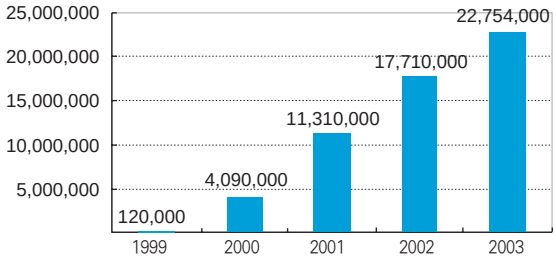
■ Online Stock Trading

Online stock trading is steadily gaining popularity and therefore the number of online trading accounts has been increasing. As of June 2003, the number of online accounts reached 5.59 million which is equivalent to 83.6% of the total number of accounts. Since the end of 1998, the total number of active accounts increased by 70% while online accounts increased 24-fold in the same period of 4 years. Online stock trading comprises 55.2% of all securities transactions including stocks, futures, and options.

36 out of 43 domestic securities companies provide online services and there are a few companies where more than 90% of all transactions are conducted online.

Figure 4-03 Upward Trend in the number of On-line Banking Users

(Unit: 10 thousand persons)



Source: Bank of Korea (BOK), Dec. 2003

Table 4-11 Number of Mobile Banking Transactions

	Inquiry	Electronic funds transfer	Total
Dec. 2002	1,081,262	14,482	1,095,744
Mar. 2003	1,106,000	25,000	1,131,000
Jun. 2003	1,176,000	23,000	1,199,000
Sep. 2003	1,272,000	58,000	1,330,000
Dec. 2003	2,173,000	387,000	2,560,000

Source: Bank of Korea (BOK), Dec. 2003

■ New services

Financial services have changed in many ways not only in terms of the trading format but also in the content of its services it aims to create a Financial Portal through horizontal and vertical expansion of services. Online financial services are converging with mobile financial services, adding a wider selection of convenient services to customers. In addition, to the existing financial services over the Internet such as online comparison charts of interest rates and information services regarding new financial instruments, financial portals accessed by mobile handsets provide a new form of financial services that combine the features of mobile technology with the financial web portals.

Table 4-12 Number of On-line Accounts and Customers' Active Accounts

(Unit: No. of accounts, %)

	On-line account	Active account	Ratio of online account
Dec. 1998	227,350	3,792,456	6.0
Dec. 1999	1,887,245	7,572,839	24.9
Dec. 2000	3,849,240	8,668,187	44.4
Dec. 2001	4,578,651	8,385,376	54.6
Dec. 2002	5,321,259	8,010,496	66.4
Jun. 2003	5,597,881	6,698,085	83.6

Source: Korea Securities Dealers Association(KSDA), Dec. 2003

Table 4-13 Trend of Total Stock Trade and On-line Stock Trade Amount

(Unit: Trillion won, %)

	On-line stock trade		Total stock trade		On-line ratio	Increase or decrease
	Amount	Increase rate	Amount	Increase rate		
1998	22.5	-	1,205.2	-	1.9	-
1999	684.3	2,845.8	3,607.5	199.3	19.0	17.1
2000	1,939.7	183.4	4,163.9	15.4	46.6	27.6
2001	2,189.5	12.9	4,185.0	0.5	52.3	5.7
2002	3,293.5	50.4	6,321.8	51.1	52.1	-0.2
First half of 2003	1,918.5		3,473.0		55.2	

※ 1$ ≒ 1,200 won

Source: Korea Securities Dealers Association (KSDA), Dec. 2003

3. Mobile Internet

Domestic mobile Internet market size has been showing an quarterly increase rate of about 10.6% in sales and is taking over 10% of the total sales of mobile communication services. Such growth is made possible by the introduction of diverse mobile content, taking advantage of network evolution to cdma 2000-1x and EV-DO.

3.1 Mobile Content

Ringtones is one of the most popular contents. Recently, ringtones that can produce 64 chords are being offered and many diverse application contents are being introduced.

A new m-card service delivers a ringtone with an animated character to mobile phone subscribers.

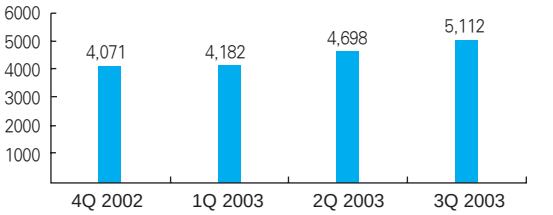
More than 30% of data traffic in mobile Internet is generated by games. The domestic market for mobile games has increased from 10 billion in 2000 to 250 billion won in 2003 and it will soon reach the industry sale levels of online and PC games.

The most common feature in the character (avatar) service is a downloadable character that can appear in the background of the mobile phone screen. The user can choose several photos and save them as a background screen or make a certain photo appear when there is an incoming call or while the user is accessing the wireless Internet.

MMS goes beyond simple text messaging by allowing users to attach photos, background pictures, images, and music to their text messages.

Figure 4-04 Quarterly Sales of the Korean Wireless Internet Market

(Unit: 100 million won)



※ 1$ ≒ 1,200 won

Source: Total of Mobile Carriers Quartely sales

■ Future services

First, an MMS service will allow users to send content such as video, photos, maps, and business cards. The service will also support large data files such as flash animation clips or video advertisements.

The current MMS market is centered around sending and receiving text messages while the technology also supports the transmission of photos, ring tones. In the future, it will become more diverse to allow communication between person and server using push technology for sending mobile advertisements and news.

Secondly, VOD is becoming a promising business as it delivers video streams to mobile phones that can also be downloaded. Since 2002, full-scale VOD service based on MPEC-4 technology has been expanding. SK Telecom and KTF are already providing multimedia content via EV-DO networks under the JUNE and FIMM branded service. Popular content among users is entertainment such as music video, movie trailers, soap operas, and sports.

Thirdly, various services and mobile content that use location-based information are becoming established. Services that can track the location of friends, family members, and cars while providing information about nearby restaurants and accommodations is gaining a lot of attention.

Table 4-14 Frequently Used Mobile Contents

(Unit: %)

Rank	contents	Ratio
1	Bell sounds	45.3
2	Games	12.5
3	Ringtones	9.2
4	Music	7.3
5	Characters	5.5
6	GIS	2.7
7	Sing Along	2.6
8	Traffic Information	2.3
9	Stock Information	1.4
10	Sports News	1.4

Source: Yonsei University HCI Lab, Dec. 2003

3.2 m-Commerce

In 2003 the registered users of cdma 2000 1x EVDO, which can be referred to as 3rd generation mobile communications, reached 24.8 million out of the total 33.6 million users in December 2003, thus establishing a basis for an active full scale data service market. Upon this momentum, the size of Average Revenue per User (ARPU) is increasing in the area of data services. The mobile Internet market size has grown to 2 trillion won while the W-CDMA network where full-scale investment is taking place, the rate of growth will accelerate even further. Following the introduction of a full-scale ubiquitous service environment and new convergence products, the m-Commerce market is becoming more active not only in the existing payment of small purchases and mobile trading but also in new m-Commerce markets such as MMS, LBS and telematics.

In line with the above trend,, the existing wired high speed internet companies, major portals, banks and financial institutions will be providing new products that merge the functions of telecommunication and finance, forming a competitive market structure. The mobile Internet network and accelerating convergence of telecommunication and finance.

Table 4-15 **Comparison of Micro Payment Service of Mobile Phone with Fixed-line Phone, ADSL and Credit Card**

(Unit : One million cases, 100 million won)

Classification	2001		2002		2003	
	No. of Settlement	Amount of Settlement	No. of Settlement	Amount of Settlement	No. of Settlement	Amount of Settlement
Fixed-line	234	217	1,736	1,365	2,081	1,926
Mobile phone	1,506	793	4,866	2,613	9,412	4,718
Credit card	16	433	67	2,803	78	1,080
ADSL			13	9	68	56
Total	1,756	1,443	6,682	6,790	11,639	7,780

※ 1$ ≒ 1,200 won

Source: SKTelecom, Dec. 2003

1. Backbone Network

1.1 Internet eXchange(IX)

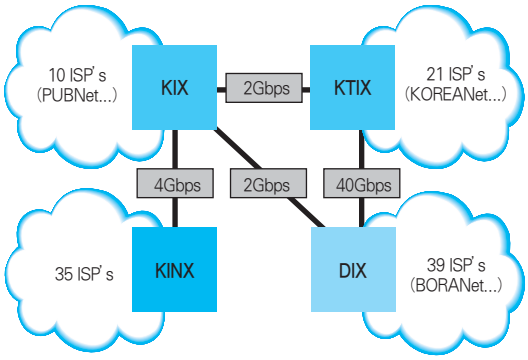
■ IX

At present, the Korea Internet eXchange (IX) service is provided by NCA (KIX, www.kix.ne. kr), KT (KT-IX, www.kornet.net), Dacom (Dacom-IX, www.bora.net), and KINX (KINX, www.kinx.net).

The non-profit public networks are interconnected to NCA's KI while the commercial ISPs are linked to KT-IX, Dacom-IX or KINX. KT-IX and D-IX were built by KT and Dacom respectively and are operated by these backbone providers, which are also ISPs. KINX is managed by KINX Inc., which was established by a consortium of small-and mid-sized ISPs.

In the meantime, IX in Busan is the nation's first regional eXchange (R-IX) that the government set up with the goal to improve Korea's Internet interconnection structure that is centered around Seoul, and bridge the digital divide by regions. Since May 2003, 13 ISPs of 11 organizations in this region have been interconnected, handling Internet traffic originating from Busan and South Gyeongsang Province.

Figure 5-01 IX Connectivity Map



Source: National Computerization Agency(NCA), Dec. 2003

■ ISP

Commercial ISPs emerged in 1994, and the number of small-sized ISPs has continuously increased by 2001. In particular, the presence of ISPs offering Internet services via CATV network like Thrunet has rapidly expanded. However, 2002 marked the turning point in the Korean Internet access service market as it reached a saturation point in terms of quantity. This in turn led to a full-fledged competition in the market, accelerating M&As targeting small-sized ISPs.

Korean ISPs have spurred efforts to introduce services using new technologies, based on which

Table 5-01 State of IX bandwidth

Classification	IX	Operating Entity	No. of ISPs connected	Total Connection Bandwidth
Public	KIX	NCA	10	30.5 Gbps
Commercial	KT-IX	KT	21	130 Gbps
	Dacom-IX	Dacom	39	92 Gbps
	KINX	KINX	35	44 Gbps

Source: National Computerization Agency(NCA), Dec. 2003

they tried to develop a profitable business model. In line with this, these providers have continuously pushed ahead with expanding their businesses into Internet telephony, contents business and portals while maintaining the existing server hosting and Internet data center (IDC) services. In addition, Korean ISPs are exploring ways to build a better profit structure and change their current flat-rate tariff policy by reviewing the Service Level Agreement (SLA) that is under discussion overseas.

Table 5-02 No. of IDC's ISP Members by Year

(Unit: Number of ISPs)

Year	2000	2001	2002	2003
No. of ISP members	83	99	82	78

Source : Korea Internet Data Center(IDC). Feb. 2004

1.2 Commercial Network

Currently, Korea commercial networks are provided by 78 ISPs including KT (KORNET), Dacom Corp. (BORANET), Onse Telecom Corp. (Shinbiro), Hanaro Telecom Corp. (Hananet),

Table 5-03 Major Commercial Network State

Company	Service Name	Network State	Network Connection	
			Domestic	Foreign
KT	KORNET	· Total nodes nationwide: 100 · Links between major cities: 2.5Gbps~10Gbps · Links between small and mid-sized cities: 155~622Mbps	(Total bandwidth of IX:42Gbps · DIX: 40Gbps · KIX:2Gbps) (Total connected ISPs:130.5G)	(Total 17.5Gbps) · U.S.(UUNET and 6 companies) : 13Gbps · Japan, China, Hong Kong, Australia, New Zealand, Southeast Asia: 4.5Gbps
Dacom	BORANET	· Total nodes nationwide: 71 · Links between major cities: 310Mbps~5Gbps, 2 lines · Links between small and mid-sized cities: 45~155Mbps	(Total bandwidth of IX:42Gbps · KTIX:40Gbps · KIX:2Gbps) (Total connected ISPs: 50Gbps)	(Total 5.2Gbps) · U.S.(Qwest, PAIX etc.) : 2Gbps · Asia(9 countries like Japan(555M) and China(555M) : 3.0G
Hanaro Telecom	HANANET	· Total nodes nationwide: 200 · Links between major cities: 40Gbps~800Gbps · Links between small and mid-sized cities: 155Mbps~2.5Gbps	(Total bandwidth of IX: 83.5Gbps · DIX: 25Gbps · KINX: 5Gbps · KIX: 1Gbps · KTIX: 52.5Gbps) (Total connected ISPs:25.7G)	(Total 5.2Gbps) · U.S. : 3.3Gbps · U.K. : 310Mbps · Asia : 1Gbps · Others : 620Mbps
Onse Telecom	SHINBIRO	· Total nodes nationwide: 19 · Links between major cities: 465M~5Gbps · Links between small and mid-sized cities: 45Mbps~310Mbps	(Total bandwidth of IX: 12Gbps · DIX: 4.5Gbps · KINX: 4Gbps · KTIX: 3.5Gbps) (Total connected ISPs: Total 4.7Gbps)	(Total 1,030Mbps) · U.S. (Onse US POP) : 975Mbps · Japan(Japan Telecom) : 45Mbps · Taiwan : 10Mbps · Hong Kong(NWT) : 128Kbps
Thrunet	Thrunet	· Total nodes nationwide: 124 · Links between major cities: 5Gbps~10Gbps	(Total bandwidth of IX: 19.5Gbps · KT-IX : 7.5Gbps · KNIX:5Gbps/KIDC:5Gbps · DIX: 2Gbps) (Total connected ISPs: 17.1Gbps)	(Total 1,705bps) · U.S.(Dacomcossing, Onse Telecom) : 1,395Mbps · Asia(Transit node, AGC) : 310Mbps

Table 5-03 Major Commercial Network State

Company	Service Name	Network State	Network Connection	
			Domestic	Foreign
Enterprise Networks	GNGIDC	· Total nodes nationwide: 63 · Links between major cities: 2.5Gbps node-to-node duplexing	(Total bandwidth of IX: 13.6Gbps · KT-IX : 7.5Gbps · KINX : 3Gbps · DIX: 2Gbps · KIX : 1Gbps · BIX : 100Mbps) (Total connected ISPs: 8.6Gbps)	(Total 775Mbps) · U.S.(MCI,Reach): 465Mbps · Japan(NTT): 310Mbps
SK Telecom	SK speedNet	· Links between major cities: 622MGbps · Links between small and mid-sized cities: 155MGbps · Jeju: 45Mbps	(Total bandwidth of IX: 6Gbps · KT-IX : 2.5Gbps/DIX: 2Gbps · KINX : 1Gbps) (Total connected ISPs: 2.545Mbps)	(Total 155Mbps) · Dacom-international: 155Mbps
Dreamline	DreamLine	· Between major node links: 45Mbps~2Gbps	(Total bandwidth of IX: 7Gbps · KIX : 5Gbps · KINX : 2Gbps) (Total connected ISPs: 7.4Gbps)	(Total 310Mbps) · Hanaro Telecom: 155Mbps · AGC: 155Mbps
Powercomm	POWER-COMM	· Total nodes nationwide: 75 · City links: 2.5Gbps · Subscriber network: 155Mbps	-	-

Source: National Computerization Agency(NCA), Dec. 2003

Thrunet Corp. (Thrunet), Enterprise Networks (GNGIDC), SK Telecom (SKSpeedNet), Dreamline (DreamX), and Powercomm Corp. (POWERCOMM). The total number of ISPs has decreased from 98 in 2001 to 78 in 2003. The following table shows the current status of Internet backbone networks in Korea with the nationwide backbone network operators.

1.3 Non-Profit Networks

■ PUBNET- KT

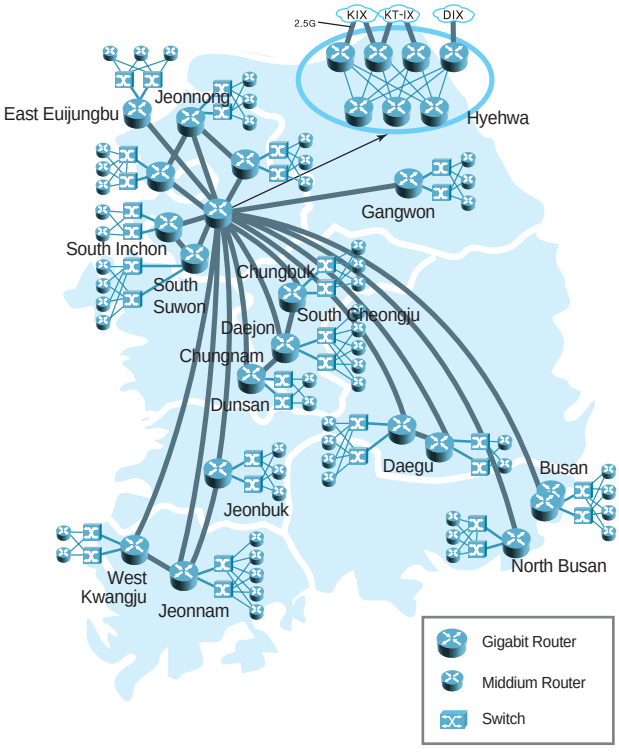
PUBNET has commenced providing commercial service in January 1998 to serve the need of the government and public sector. Since 1998, an Internet network based on ATM switch networks has been constructed and upgraded, and 18 nodes were completely built in the end of 2002. The subscriber access networks in 144 cities across the nation accommodate subscribers through ATM lines and frame relay lines. The backbone sector of the ATM switches networks is providing access speeds of 155~622 Mbps between major cities within the backbone sector of ATM switches, and 155 Mbps between small and mid-sized cities. The interconnected links between major nodes will be upgraded to speeds faster than 2.5 Gbps.

Table 5-04 Major Non-Profit Network State

Company (Service Name)	Network State	Service Targets	Network Connection	
			Domestic	Foreign
KT (PUBNet)	· ATM network-based nodes nationwide: 18 · Between majors cities: 155M~622Mbps · Between small and mid-sized cities: 155Mbps	· Public & non-profit organizations · Elementary & secondary schools	(Total bandwidth of IX: 13.6Gbps · KIX : 5G · KT-IX : 7.5G · DIX : 2.5G) (Connected ISPs: Connected to KIX, KT-IX)	· U.S.(KIX): 75Mbps
Dacom (PUBNET-PLUS)	· Between ATM network-based nodes nationwisde: 45Mbps, 155Mbps, 622Mbps	· Public & non-profit organizations	(Total bandwidth of IX: 4Gbps · 6KANet: 2Gbps · BORANet : 2Gbps) (Connected ISPs: Connected to KIX, DIX)	· U.S.(KIX): 75Mbps
NCA (6KANet)	· Between Seoul and Youngin: 45Mbps	· Central administration, judiciary & legislative bodies · Educational organization, organizations in leading application business	(Total bandwidth of IX: 1Gbps 6NGIX : 1G) (Connected ISPs: 2.5Gbps -Interconnected via 6NGIX)	· U.S.(6NGIX, KIX) :775Mbps
KERIS (EDUNET)	· Between the six nodes nationwide: 2Mbps~4Mbps	· All citizens including students, teachers, parents	(Total bandwidth of IX: 310Mbps · KT-IX : 155M · DIX: 155M (Connected ISPs: 400Mbps)	· 155M (Interconnection via KIX)

Source: National Computerization Agency(NCA), Dec. 2003

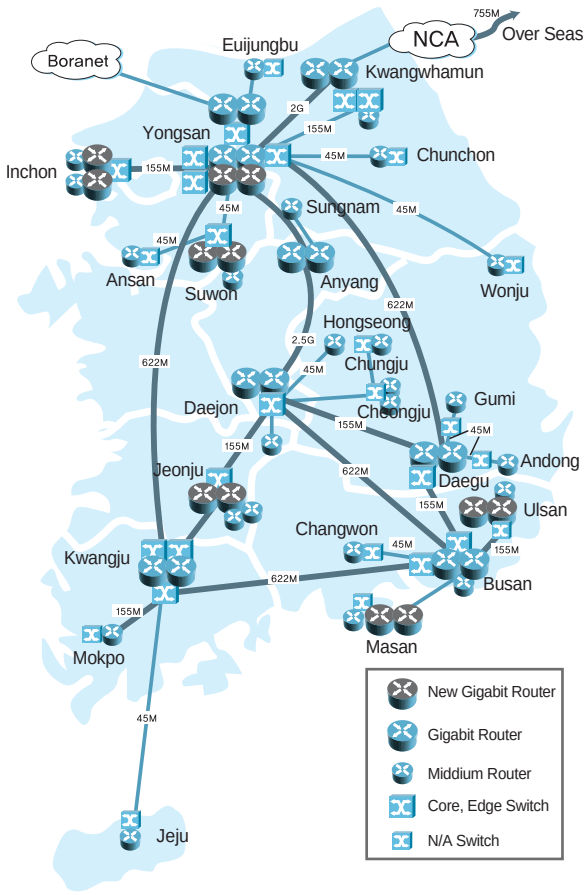
Figure 5-02 PUBNET Network



■ PUBNETPLUS - Dacom Corp.

PUBNETPLUS is offering broadband Internet services to the government and public agencies through ATM switch networks. Internet backbone networks have offered elementary and secondary schools nationwide ATM Metro service since 2003. In order to provide high-quality Internet services such as real-time multimedia streaming service and voice telephony service over the Internet, Dacom is vigorously working on the establishment of Multi-Protocol Label Switching (MPLS) networks based on ATM switch networks. The speeds of lines are mostly 45Mbps, 155Mbps, and 622Mbps while maintaining reliable service by dualizing the routes between the nodes.

Figure 5-03 PUBNETPLUS Network



■ 6KANet - National Computerization Agency (NCA)

The KOSINet service, which was delivered to the government and non-profit organizations was shut down, and a next generation Internet network, 6KANet, is replacing the KOSINet. 6KANet is a next-generation Internet network based on IPv6 and plans to provide high-quality Internet services to the government and public agencies by supporting IPv6 security functions, QoS and multicast. At present, a total of 47 agencies are using the 6KANet service. 6KANet network offers 6NGIX service along with such common services as IPv6 DNS, Web, IPv6 messenger and IPv6 streaming services. Services like IPv4/IPv6 Tunnel Broker, ISATAP, NAT-PT and Teredo are currently being provided or scheduled to be offered.

■ EDUNET - Korea Education Research Information Service (KERIS)

EDUNET offers a comprehensive information on education that is built up systematically, thereby allowing students, teachers, parents and citizens to have access to a wide range of academic information and research resources with ease anytime anywhere. Since EDUNET launched service in September 1996, it has offered teaching and studying materials as well as support for teaching activities. EDUNET provides educational resource service in alliance with Education Agencies in 16 cities and provinces. As of the end of 2003, EDUNET has about 5.16 million subscribers.

1.4 Advanced Research Networks

■ Korea Advanced Research Network (KOREN)

KOREN is a non-profit network that provides a research environment for universities, research labs, and corporations to develop high-speed communication equipment and new application services. For the access, backbone lines are provided for free, but subscriber lines are charged to the using subscribers. KOREN serves its subscribers via POP established in 6 areas nationwide, and the bandwidth of its backbone network is 40Gbps between Seoul and Daejeon, and 155Mbps in other backbone links.

Expectedly, the backbone will be upgraded to 1Gbps. KOREN is integrated with STAR TAP

(155Mbps) of the U.S., SingAREN (6Mbps) of Singapore, and RENATER(17Mbps)of France through APII Testbed to offer service for R&D activities.

■ Asia Pacific Information Infrastructure (APII)

APII has two main objectives. The first objective is to facilitate international collaboration project among countries in the Asia-Pacific region, and the second one is to build and operate APII Testbed. APII international collaboration project aims to liberalize investment in the ICT sector, strengthen cooperation in joint research projects, realize the Asia Pacific Information Society (APIS). As of December 2003, Korea operates APII Testbeds between Korean and Japan and between Korea and Singapore with the bandwidth of 1Gbps and 6Mbps respectively. The Korea-U.S. link is 155Mbps. The Testbed will be connected to CERNET of China and AARNET of Australia. The links with CERNET of China will be 45Mbps in the 1st half of 2004. Korea-Japan and Korea-Singapore networks are connected to KOREN and managed by NCA while Korea-U.S. APII Testbed is linked to KREONET of Korea Institute of Science and Technology Information(KISTI).

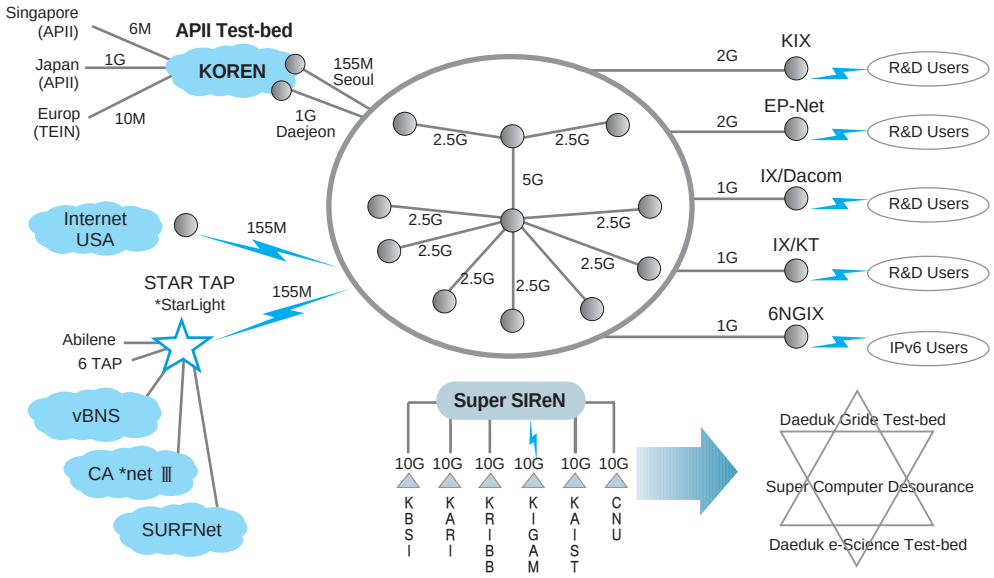
■ Trans-Eurasia Information Network (TEIN)

TEIN is a telecommunications infrastructure that facilitates joint research projects and shares information among ASEM members(between Asia & Europe). TEIN, which is the first inter-continental link between Asia and Europe, has enabled the dynamic exchanges of information between Asia and Europe and, in the long run, it is expected to improve the global telecommunications infrastructure where communications traffic is concentrated in North America. For better network service, TEIN was upgraded to the bandwidths of 10Mbps in March 2003, and to SCR 17Mbps and PCR 34Mbps in the end of 2003. There is also ongoing discussion between Korea, European and Southeast Asian countries over extending TEIN to Southeast Asia. In Korea, about 30 KOREN and 200 KREONET member institutes can access TEIN.

■ Korea Research Environment Open Network (KREONET)

KREONET, which was conceived as a nationwide network that allows researchers in science and technology to share databases, has built 15 regional network centers for the first time in Korea to introduce Internet services. KREONET has served as one of the nation' s key research networks by opening up direct international research links with the signing of the Science and Technology Agreement with other countries. (U.S.: 1991, CERFnet/NSFNET(SDSC), Europe: 1994, EuroPaNET(ULCC/UK), Japan:1995, IMNET(KDD/JST)) KREONET is connected to STAR TAP/Abilene with the capacity of 155Mbps and to KOREN with 1Gbps(Daejeon). The network is also linked to overseas BORANet(Dacome) at 55Mbps to provide research network services for R&D users at home.

Figure 5-04 KREONet Backbone Network



Sorce: KREONet, Dec. 2003

Table 5-05 International Submarine Optic Cables

	Cable	Constructed Sections	System Capacity	Length (km)	Beginning Date of service
Inter-natio-nal	JKC	Korea-Japan	36M	200	1980
	HJK	Korea-Japan-Hong Kong	280M×1	4,587	1999
	RJK	Korea-Japan-Russia	560M×2	1,762	1995
	CKC	Korea-China	560M×2	549	1996
	APCN	Korea-Taiwan-Malaysia-Australia and 10 countries	10G×2	11,839	1997
	FLAG	Korea-Japan-Hong Kong-Middle East-Europe and 13 countries	5G×2	27,943	1997
	SMW-3	Korea-Northeast Asia-Southeast Asia-Middle East-Europe and 35 countries	40G	38,000	1999
	CUCN	Korea-U.S.-China-Japan-Taiwan-Guam	20G×4	26,000	2000
	APCN-2	Korea-Japan-China-Hong Kong-Taiwan-Singapore-Malaysia	2.56Tera	20,000	2001
	KJCN	Korea-Japan	2.88Tera	500	2002
	EAC	Korea-Japan-Taiwan-Hong Kong	2.56Tera	10,600	2001
	C2C	Korea-Japan-Taiwan-China-Hong Kong-Taiwan-Singapore-Malaysia	7.68Tera	17,000	2001
	FNAL	Korea, Japan, Taiwan, Hong Kong	2.4 / 3.8Tera	9,600	2002
Dom-estic	No. 1 Jeju-Continental Korea	Jeju-Goheung	280M×3	169	1990
	Ullung-continental Korea	Ullung-Hosan	2.5G	159	1993
	No. 2 Jeju-Continental Korea	Jeju-Goheung	2.5G×4	191	1996
	No. 3 Jeju-continental Korea	Jeju-Namhang	2.5G×2	236	2000

Sorce: National Computerization Agency(NCA), Dec. 2003

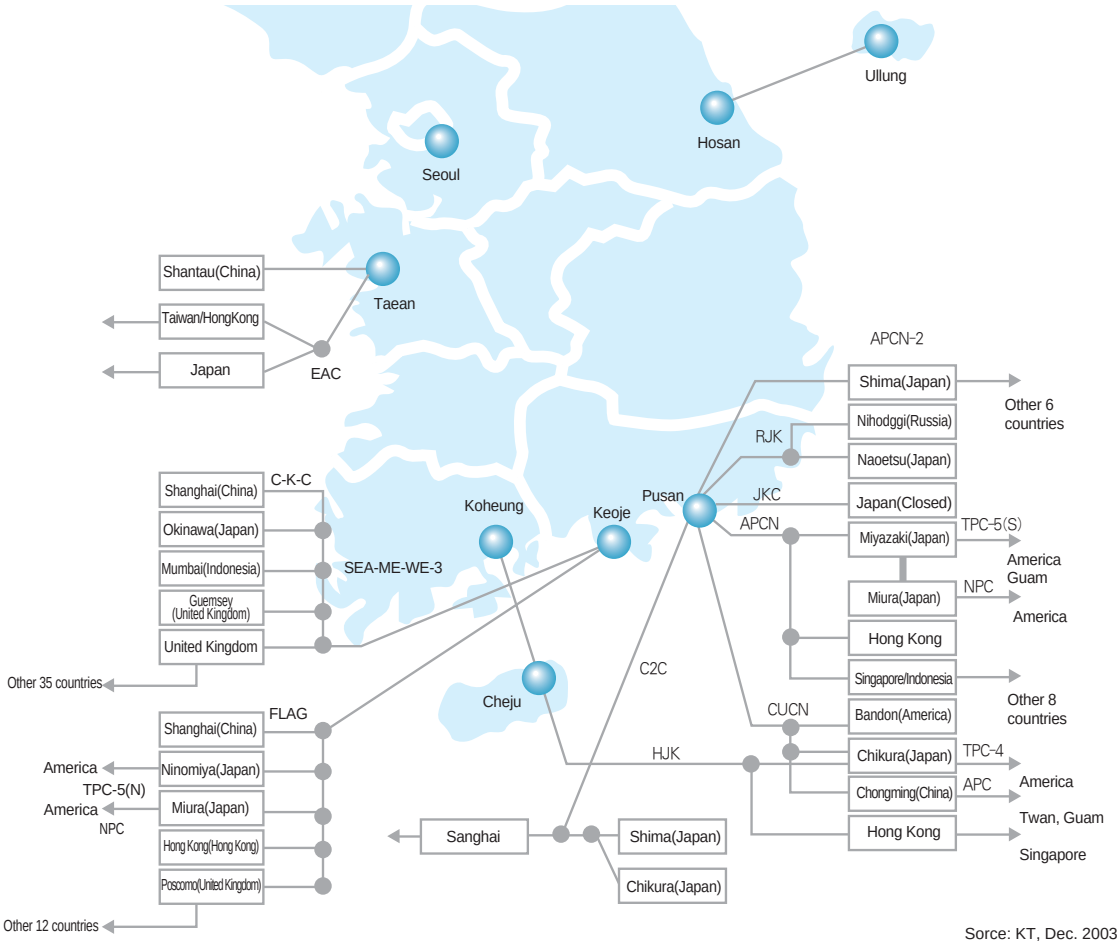
1.5 International Cables and Satellite Communications in Korea and Abroad

International submarine optic cables play an important role with satellite as a communications tool that connects countries with Tbps-scale submarine optic cables, thereby transmitting a large volume of data. General lifespan of submarine optic cables is 25 years on average, and there are all told 12 optic cables (HJK, RJK, CKC, APCN, FLAG, SMW-3, CUCN, APCN-2, KJCN, C2C, EAC, FNAL) under operation in Korea with a total capacity reaching 19Tbps.

With the global telecommunications market, which has been in the grip of a sweeping recession since 2001, the construction of new undersea cables is very slow in 2004, and most telecommunications operators across the globe are expected to meet the demands by increasing the current systems or acquiring bankrupt cable companies or leasing the lines in the short term from the cables market.

As part of global efforts to reasonably maintain the network since 2003, old and low-bandwidth cables have been removed across the world. Nevertheless, the number of international undersea optic cables connecting North American countries centered around the U.S. and Canada, and countries like the U.K., France and Germany in

Figure 5-05 Submarine Optic Cables in Korea



Sorce: KT, Dec. 2003

Europe, and Singapore, Malaysia, and Hong Kong in Asia surpass 24 and their total capacity reaches dozens of Tbps-scale.

2. Subscriber Network

2.1 Fixed-line Network

The fixed-line network can be classified into an xDSL based network (VDSL : Very high-bit[data] rate Digital Subscriber Line, ADSL, HDSL : High bit[data] rate DSL, SDSL : Symmetric DSL, ADSL : Asymmetric DSL), which uses copper lines, and a cable modem using a HFC (Hybrid Fiber Coaxial) network. Out among 11.1 million total fixed-line network users, 6.44 million people hook up to xDSL and 3.83 million people are connected to cable modems.

■ VDSL (Very high-bit[data] rate Digital Subscriber Line)

VDSL is one of the several types of DSL technology that is transmitted over copper lines. In the VDSL standard, T1.424, the asymmetrical transmission speed is 22Mbps on the downlink and 3Mbps on the uplink. As for symmetrical transmission speed, the service is provided at speeds of 6Mbps~13Mbps on the downlink and uplink. VDSL works only over relatively short transmission distance (0.3Km~1.5Km) compared to ADSL. Despite such a weakness, VDSL service is gaining great popularity as it can offer service with the speed of 13Mbps. Given the characteristics of VDSL, it has to maintain a short

Table 5-06 No. of Broadband Internet Service Subscribers

(Unit : Person)

Classification	xDSL	Cable Modem	LAN of Apartment	Satellite	Total	Market Share
KT	5,230,342	-	353,880	4,836	5,589,058	50.0%
Hanaro Telecom	1,093,261	1,290,150	342,152	-	2,725,563	24.4%
Thrunet	-	1,287,502	5,862	-	1,293,364	11.6%
Onse Telecom	-	419,293	3,769	-	423,062	3.8%
Dreamline	56,178	89,546	3,874	-	149,598	1.3%
Dacom	-	135,884	65,820	-	201,704	1.8%
Value-added telecom operators	3,362	605,791	9,950	-	619,103	5.5%
Resellers	52,812	-	124,235	-	177,047	1.6%
Total	6,435,955	3,828,166	909,542	4,836	11,178,499	100%
Market Share	57.6%	34.2%	8.1%	0.1%	100%	-

Source : Ministry of Information and Communication, 2003. 12

transmission distance. To this end, VDSL should evolve to FTTC and FTTH, so the networks of VDSL are formed mainly around high-density residential areas like apartments. VDSL chipset makers released a 20Mbps-scale VDSL product followed by 50Mbps-scale as a commercial service.

■ ADSL (Asymmetric Digital Subscriber Line)

ADSL is a communication tool that enables high-speed data communications using the existing copper lines. ADSL can send 1.5Mbps~8Mbps data rates downstream, and 16Kbps~640Kbps upstream. The fact that local exchanges in large cities are located within the radius of 3-4km offered an ideal environment to provide an ADSL service. And upon the introduction of the service, it has quickly spread across all users centering around densely populated apartment complexes. As a result, as of the end of 2002, the number of subscribers recorded 5.7 million people and the ADSL market got saturated in 2003. Now, the service is moving to VDSL.

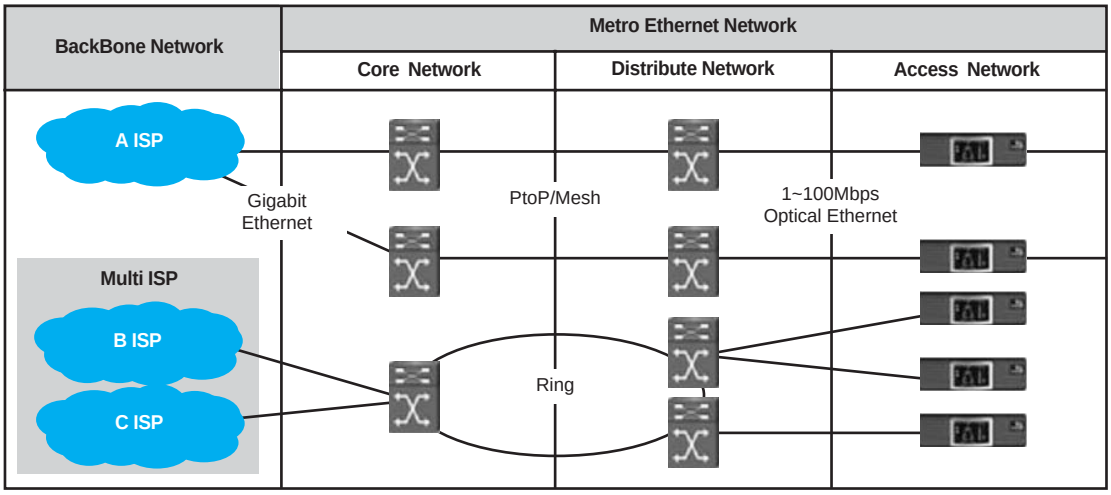
■ Cable Modem

Cable modem broadband Internet service uses a hybrid fiber coax (HFC) network that is composed of fiber optic cable connections and coaxial cable connections. Since the introduction, the service has continued to evolve, extending its lifespan and accelerating the technological development more than the existing services like ISDN, HomePNA and ADSL. In the existing service areas, service operators (SO), which used to retransmit broadcasting programmes using cable networks, and multiple system operators (MSO) started providing broadband Internet service either independently or in cooperation with ISPs. And those SOs and MSOs, which worked with ISPs to provide broadband Internet service in the initial stage, are now transforming themselves as an ISP taking a form of SO. They are expected to deliver 100Mbps-capable service around 2005.

■ Metro Ethernet Service

The existing leased line has offered the service with speeds of 256K, 512K, 1.544K, 2,048K, 45M and 155M, using the TDM (Time Division

Figure 5-06 Metro Ethernet Structure



Multiplexing) method. The TDM entails a high cost and triggers a bottleneck problem. In 2001, Metro Ethernet services commenced. Customers demanded access to a high speed Internet service at work or a PC room. Nowadays, the price of Ethernet-based equipment is stedily drooping and new Metro Ethernet equipment have been launched. Metro Ethernet service is composed of switch equipment that offers services in the various speed ranges of 1M, 3M, 5M, 10M, 50M and 100M~1G, and supports End-to-End QoS (Quality of Service), VoIP and VPN.

2.2 Wireless Network

■ Mobile Communications

Currently, mobiles communications services are offered in the form of mobile phones, radio paging, TRS and wireless data communications etc. And the cellular phone service subscribers account for 98.7% of the mobiles communications service. This figure shows that the penetration-to-population ratio stands at 70%, indicating that the mobile service market will reach a saturation point in no time unless a new variable emerges. Thus, mobile operators are expected to engage in a much fiercer competition with each other to secure more mobile subscribers. With the rapid take-up of mobile phone services, the radio paging service has seen a drastic decrease in its subscribers while TRS and wireless data communications services are maintaining a steady growth by attacking the niche markets. As of the end of April 2004, the number of wireless Internet service in Korea is 33.09 million people, taking up 94.5% of the total mobile subscribers that amount to 35 million. Out of which, the subscribers who have an exclusive wireless Internet browser or platform built-in such as WAP/ME, stand at 31.82 million or 96% of the total.

■ Wireless LAN

Wireless LAN allows the transmission of data by using radio frequency technology. In addition, wireless LAN consumes less power, and has a strong signal reception even in places where interference exists. As the price of wireless LAN products goes down, the technology is more widely used. Recently, KT and Hanaro Telecom launched their wireless LAN commercial services in the hotspot areas using the 2.4GHz ISM band, and SK Telecom is also providing trial service, paying attention to Wireless LAN as a complementary technology of mobile telephones as it offers far faster transmission speed than the

Table 5-07 No. of Mobile Communications Subscribers in Korea

Classification	End of Mar. 2004	Market Share	Carriers
Mobile Communications	35,003,983	60.0%	SK Telecom, KTF, LG Telecom
Radio Pager	63,597	0.1%	Real Telecom(nationwide provider), Seoul Mobile Telecom, Eyesvision, Selim, Centis(local provider)
TRS	304,852	0.5%	KT Powertel, Anam Telecom, Seoul TRS, Daegoo TRS, Powertel TRS, KB Telecom, Jeju TRS
Wireless Data Communications	105,718	0.2%	Air Media, Real Telecom
Total	58,324,664	100%	-

Source: Ministry of Information and Communication, Wired & Wireless Telecommunications Service Subscribers, 2004. 3

latter. At present, KT is leading the wireless LAN market in Korea followed by Hanaro Telecom. Dacom is providing free service in some subway stations and airports. As for SK Telecom, the company is delivering trial service in some 80 hotspot locations including universities, airports and horse racing tracks in pursuit of creating synergy effects with mobile phone services. However, in Korea, KT is the only carrier which is aggressively attacking the wireless LAN market. KT is providing not only wireless LAN products, but also wireless LAN services in areas where wireless LAN is set up through 'NESPOT-swing', and for other areas, KT is providing services that allow wireless data communications via mobile telephone networks. At the same time, in order to create a new income source in the fixed and wireless services, KT is pushing ahead with the business in cooperation with KTF.

■ Satellite Communications

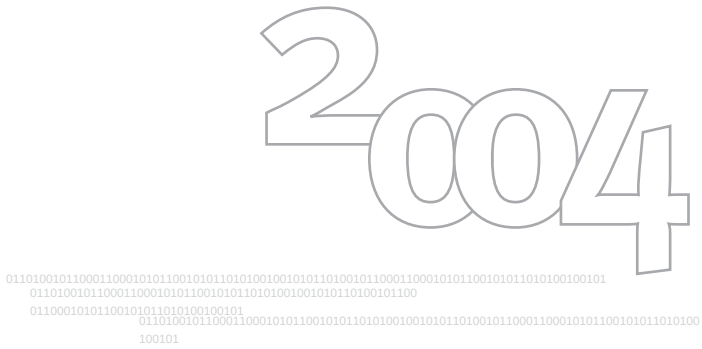
With the launch of Mugungwha Satellite in August 1995, the full-fledged satellite era has begun in Korea. A variety of broadcasting and telecommunications services are being provided through satellite communications such as DAMA/SCPC service, satellite VAN service of VSAT, digital satellite broadcasting service and on-the-spot news reports. Internet service via satellite uses Mgungwha Satellite, and achieves transmission speed up to 1Mbps anywhere in the country including remote areas where fixed-line infrastructure is difficult to be deployed. Satellite uplink transmissions are made over telephone lines or mobile telephone networks. As for areas like ordinary households and buildings, they use fixed-line networks like leased lines, PSTN, ISDN for the uplink, and satellite Internet on the move uses mobile telephone networks. And the downlink which carries a lot of traffic offers service using a satellite dish. Internet service via satellite is being offered as part of KT's broadband Internet service, 'Megapass', but is limited to remote areas which find it difficult to receive fixed-line broadband Internet services like xDSL, cable modems and apartment LAN, or areas where satellite broadcasting equipment is set up. These days, with the convergence of telecommunications and broadcasting, efforts are made to expand subscribers by combining satellite broadcasting with wireless Internet service.

Table 5-08 **No. of Wireless Internet Subscribers in Korea**

Classification	SK Telecom	KTF	LG Telecom	Total
WAP/ME Method	16,879,400	10,489,518	4,451,709	31,820,627
ISMS Method	482,993	605,474	184,001	1,272,468
Total	17,362,393	11,094,992	4,635,710	33,093,095

* ISMS method is not a mere SMS but a service that allows you to log on to the Internet and search the web without a web-browser by linking the ISMS system to the Internet gateway.

Source: Ministry of Information and Communication, 2004. 3


2004

A p p e n d i x

1. List of Internet-related Organizations

Field Related	Organizations	URL	TEL
Policy & Statistics	National Computerization Agency (NCA)	http://www.nca.or.kr	+82-02-2131-0114
	Korea Information Society Development Institute (KISDI)	http://www.kisdi.re.kr	+82-02-570-4114
	Information Communication Ethics Committee (ICEC)	http://www.icec.or.kr	+82-02-3415-0114
	Korea Network Information Center (KRNIC)	http://www.nic.or.kr	+82-02-2186-4500
	Information Culture Center of Korea (ICC)	http://www.icc.or.kr	+82-02-3660-2633
Technology & Research	Electronics and Telecommunications Research Institute (ETRI)	http://www.etri.re.kr	+82-42-860-6114
	Korea Institute of Science and Technology Information (KISTI)	http://www.kisti.re.kr	+82-02-962-6682
	Korea Information Security Agencu (KISA)	http://www.kisa.or.kr	+82-02-3488-4500
	Korea Association of Information and Telecommunication (KAIT)	http://www.kait.or.kr	+82-02-580-0580
	Telecommunications Technology Association (TTA)	http://www.tta.or.kr	+82-02-723-7073
	Institute of Information Technology Assessment (ITA)	http://www.iita.re.kr	+82-42-869-1114
Industry & Corporation	Korea Internet Corporations Association (Kinternet)	http://www.kinternet.org	+82-02-528-4114
	Korea Information & Contents Business Association (KIBA)	http://www.kiba.or.kr	+82-02-2264-3636
	Federation of Korean Information Industries (FKII)	http://www.fkii.or.kr	+82-02-780-0201
	Promissing Information & Communication Companies Association (PICCA)	http://www.picca.or.kr	+82-02-3424-6155
	Korea Venture Business Association (KOVA)	http://www.kova.or.kr	+82-02-562-5914
	Open Standards and Internet Association (OSIA)	http://www.osia.or.kr	+82-02-562-7041
	Korea ISPs Association	http://www.kispa.or.kr	+82-26007-6200
e-Commerce	Korea Institute for Electronic Commerce (KIEC)	http://www.kiec.or.kr	+82-02-3453-0404
	KOREA CALS/EC ASSOCIATION (KCALS)	http://www.kcals.or.kr	+82-02-551-1452
	CommerceNet Korea (CNK)	http://www.commercenet.or.kr	+82-02-774-8558
Infrastructure	Korea IT Industry Promotion Agency (KIPA)	http://www.software.or.kr	+82-02-3469-1500
	Korea Database Promotion Center (KDPC)	http://www.dpc.or.kr	+82-02-318-5050
	Korea Software Industry Association (KOSA)	http://www.sw.or.kr	+82-02-586-3411
	Korea Software Financial Cooperative (KSFC)	http://www.ksfc.or.kr	+82-02-3469-1100

2. List of ISPs

Non-Commercial Network

Network Operater	Service Name	Tel	E-Mail	URL
National ComputerizationAgency	6KANet	+82-02-2131-0757	ssy@nca.or.kr	www.ngix.ne.kr
KERIS	EDUNET	+82-02-3488-6471	ip-tech@keris.or.kr	www.keris.or.kr
KISTI	HPCNET	+82-042-869-0582	help@hpcnet.ne.kr	www.hpcnet.ne.kr
KISTI	KREONet	+82-042-828-5166	hjjung@kisti.re.kr	www.kreonet.re.kr
Korea Telecom-PUBNET	PUBNET	+82-331-260-2387~8	ip@pubnet.ne.kr	www.pubnet.ne.kr
DACOM-PUBNETPLUS	PUBNETPLUS	+82-02-6220-6695	uspark@dacom.net	www.pubnetplus.ne.kr

Commercial Network

Network Operater	Service Name	Tel	E-Mail	URL
KIC for Agriculture	AFFIS	+82-031-299-8833	hwangjs@affis.net	www.affis.net
HangaramNetworks	BITSRO	+82-42-670-4690	parkyj@hangaram.co.kr	www.hangaram.co.kr
Bittel	Bittel	+82-02-338-7942	help@bittel.net	www.bittel.net
DACOM Corporation	BORANET	+82-02-6220-7007,02-709-3700	market@bora.net	www.bora.net , www.chollian.net
BANDOCABLELINE	CABLELINE	+82-063-900-9051	modem@cableline.com	www.cableline.com
EZCEN	CENNET	+82-02-815-5651	ezcen@ezcen.com	www.ezcen.com
CPS	CNIDC	+82-02-3218-0782	sales@cps.co.kr	www.cps.co.kr
Kyonggi Cable TV	DigitalSystem	+82-031-910-1000	webmaster@digitalsystem.co.kr	www.digitalsystem.co.kr
ABN	DITIZONE	+82-031-710-8952	jspark@abn.co.kr	WWW.ABN.CO.KR
DreamcityMedia	DREAMPLUS	+82-1566-1234	ymjoo@dreamcity.co.kr	www.dreamcity.co.kr
DREAMLINE CO.	DREAMX	+82-1566-0606	ip@dreamx.net	www.dreamline.co.kr
KILT.,Co.Ltd	DUALLINE	+82-32-423-6100	psm@kilt.co.kr	www.dualline.net
eGIOS	eGIOSNET	+82-02-2116-8014	rnoh@egios.com	www.egios.com
ELIMNET, INC.	ELIMNET	+82-02-3149-4900	webmaster@elim.net	www.elim.net

Commercial Network

Network Operater	Service Name	Tel	E-Mail	URL
GNG Networks, Inc	GNGIDC	+82-1588-2464	sales@epnetworks.co.k	www.epnetworks.co.kr
ETRI	ETRI	+82-042-860-4847	mkshin@pec.etri.re.kr	www.etri.re.kr
eyesvision	EYES	+82-051-850-5000	ip@ns.eyes.co.kr	www.eyes.co.kr
NTT KOREA	GIN	+82-02-2016-5006	korea-ip-gl@ntt.com	www.ntt.com/kr
Hanaro Telecom Inc.	HANANET	+82-106	info@hanaro.com	www.hanaro.com
HANINTERNET	HANINTERNET	+82-02-860-8000	iservice@haninternet.co.kr	www.haninternet.co.kr
SERVERBANK	HANNET	+82-02-829-3333	martketing@e-serverbank.com	www.e-serverbank.com
HanQnet Co.,Ltd	HANQ	+82-80-211-1242	webmaster@hanq.net	www.hanq.net
hansol iGlobe	HANSOLNET	+82-02-3488-7770	sales@higlobe.net	www.hansoliglobe.com
Hanvitinb	HANVITINB	+82-031-414-4000	pslee@hanvit.net	www.hanvit.net
HANVITDIGITALPLUS	MAGICPOWER	+82-02-553-2130	hjlee@hanvitdp.com	www.hanvitdp.com
DAEJONTELECOM	HIPASS	+82-042-633-0033	ksi1202@daejon.com	www.daejon.com
IBSat Co.,Ltd.	IBSat	+82-080-555-7100	ibsat@ibsat.co.kr	www.ibsat.co.kr
ILINKKOREA	INDICLUB	+82-02-2109-5255	ip@ilinkkorea.co.kr	www.indiclub.co.kr
Inet Hosting, Inc.	INET	+82-02-2103-7500/7600	baram@inet.co.kr	www.inet.co.kr
PrismCommunications	INTELLICENTER	+82-02-310-0400	ip@prism.co.kr	www.intellicenter.co.kr
ISSAN CO.,Ltd	ISSAN	+82-02-789-9114	ykoh@issan.net	www.issan.net
IOSYSTEM	JIGUNET	+82-02-413-9005	jdm@iosystem.co.kr	www.jigu.net
INTERTNS	JLAN	+82-063-224-6774	intertns@intertns.com	www.intertns.com
Kwacheon Broadcasting Network	KBN	+82-02-507-4000	ceo@kbntv.co.kr	www.kbntv.co.kr
Kwan-ak Television Network Co	KCNET	+82-02-837-6008~9	webmaster@kcnet5.com	www.kcnet5.com
KOREAINTERNETDATACENTERInc.	KIDC	+82-02-6440-2900	market@kidc.net	www.kidc.net
KT Solutions Corporation	KITINET	+82-080-2580-410	lhwto@groupnet.co.kr	www.ktsolutions.co.kr
KOREAINTERNETTELECOM	KITNET	+82-62-511-6670	choi@kitclub.co.kr	www.kitclub.co.kr
KangNam CableTV	KNCTV	+82-02-2056-7777	sysop@knctv.co.kr	www.knctv.co.kr
Korea Telecom Hitel	KOLNET	+82-02-3289-2200	mkchoi01@hitel.net	www.hitel.net, www.nhitel.net
Korea Telecom	KORNET	+82-080-014-1414	ceo@kt.co.kr	www.kornet.net
KRISP	KRISP	+82-32-442-6000	sos@krisp.co.kr	www.krisp.co.kr
KrLine Internet Service Inc.	KrLine	+82-02-3461-3282	sgbang@krline.net	www.krline.net
Korea Telecom I com	KTiCOM	+82-02-3488-1333	webmaster@kticom.com	www.kticom.com
Korea Trade Network	KTNET	+82-02-6000-2119	doshin@ktnet.co.kr	www.ktnet.co.kr
ARISOO	Living114	+82-02-584-5363	ukyo@web114.com	www.living114.net
mire.net	MIRENET	+82-02-2009-2660	rlatjsska@mire-net.co.kr	www.mire-net.co.kr
Korea Mobile Internet eXchange	MIXNET	+82-02-563-3399	ix@kmix.net	www.kmix.net
Mouminfomation Co.,Ltd	MoumNet	+82-080-561-8888	jkim@moumnet.com	www.moumnet.com
KoreaMultinet	MULTINET	+82-02-3443-3006	johnjung@koreamultinet.com	www.koreamultinet.com
MINS	NCABLENET	+82-53-263-7000	jamesmin@ncable.net	www.mins.co.kr
Reach Network Service Korea	NETPLUS	+82-02-550-3709	contact@reach.co.kr	www.reach.co.kr
NETSGO	NETSGO	+82-02-3479-0700 +82-080-011-4295	lineinfo@netsgo.com	www.netsgo.com
NEXTEL	NEXTEL	+82-02-2202-9300	homerun@nexteline.co.kr	www.nexteline.co.kr
NOWCOM Co.,Ltd	NOWCOM	+82-02-590-3800	nowweb@nownuri.net	www.nownuri.net
OKSUNG TEL-Communication Co,. Ltd	OK-NET	+82-02-2107-3114	oksung@oksung.com	www.oksung.com
pacificcsi	PCSI	+82-02-776-3179	seo813@korea.com	www.pcsi.co.kr
QrixNetworks	QRIXNET	+82-02-999-8855	qrix-admin@qrix.com	www.qrix.com
GORayNet	RayNet	+82-02-2109-8282	ip@raynet.co.kr	www.raynet.co.kr
SAEROUNNET	SAEROUNNET	+82-02-2102-3345	hamm@saeroun.co.kr	www.saeroun.co.kr
ESOLTECH	SAFELINE24	+82-055-266-6924	network@esoltech.co.kr	www.safeline24.net
Samsung Networks Inc.	SAMSUNGNETWORKS	+82-02-1577-0300	ygpark@samsung.com	www.samsungnetworks.co.kr
ONSE Telecom	SHINBIRO	+82-083-100	kyh@onsetel.co.kr	www.shinbiro.com
KICA	SIGNGATE	+82-02-360-3003	asia44@signgate.com	www.signgate.com
SK Global co., Ltd	SKGNW	+82-1588-7555	bjlee1@skglobal.com	www.skglobal.co.kr
SK C&C Co., Ltd.	SK-NET	+82-02-2196-8254	mrdeer@skcc.com	www.sk-net.com
SK Telecom	SKSpeedNet	+82-02-2121-3457	jsg@sktelecom.com	www.sktelecom.com
SKTelink	SKTelink	+82-02-829-2968	lineinfo@sktelink.com	www.sktelink.net
SuperNet	SUPERNET	+82-02-568-3003	ysong@supercdn.net	www.supercdn.net
SKTelecom	SYNCROAD	+82-02-3709-1466	dreamtr@sktelecom.com	www.skwin.com
Thrunet Co., Ltd (THRUNET)	THRUNET	+82-1588-3488	abuse@thrunet.com	www.thrunet.com
Tomis Information & Telecom Corp	TOMISNET	+82-02-784-0110 (204)	ski21@tomis.co.kr	www.tomis.co.kr
Today and Tomorrow	TTNet	+82-1566-1577	iwlee@tt.co.kr	www.tt.co.kr
WEBURO	WEBURO	+82-631-284-4650	apply@weburo.net	www.weburo.net
cablei	XNET	+82-02-878-5481/2	cmpark@cablei.co.kr	www.cablei.co.kr
MCIWORLDCOM	XPRESSNET	+82-02-6281-7921	parksang2001@hanmir.com	www.wcom.co.kr

3. List of Government Agencies and Other Agencies

APNIC: Asia Pacific Network information Center (http://apan.net)
CRERIS: Korea Education and Research Information Service (http://www.kmec.net)
DDC: Domain Dispute Committee (http://dispute.nic.or.kr)
EC: Engineering Committee (http://ec.nic.or.kr)
ECRC: Electronic Commerce Resource Center (http://www.ecrc.or.kr)
ETRI: Electronics and Telecommunications Research Institute (http://www.etri.re.kr)
GIA: Government Information Agency (http://www.allim.go.kr)
ICANN: Internet Corporation for Assigned and Numbers (http://www.icann.net)
ICC: Information Culture Center Korea (http://www.icc.or.kr)
IETF: Internet Engineering Task Force (http://www.ietf.org)
Internet Appliance Promotion Council (http://iapc.kait.or.kr)
KAIT: Korea Entertainment System Industry Association (http://www.kait.or.kr)
Kinternet: Korea Internet Corporations Association (http://www.kinternet.or.kr)
KINX: Korea Internet Neutral eXchange (http://www.kinx.net)
KIPA: Korea IT Industry Promotion Agency (http://www.kipa.or.kr)
KIPO: Korea Intellectual Property Office (http://www.kipo.go.kr)
KISA: Korea Information Security Agency (http://www.kisa.or.kr)
KISDI: Korea Information Society Development Institute (http://www.kisdi.re.kr)
KISTI: Korea Institute of Science and Technology Information (http://www.kisti.re.kr)
KCCT: Korea Chamber of Commerce & Industry (http://www.korcham.net)
KCS: Korea Customs Service (http://www.customs.go.kr)
Korea Fair Trade (http://www.ftc.go.kr)
Korea Institute for Industrial Economics & Trade (http://www.kiet.re.kr)
Korea Meterological Administration(http://www.kma.go.kr)
Korea National Railroad (http://www.korail.go.kr)
KRPA: Korea Radio Promotion Association (http://www.rapa.or.kr)
KRNIC: Korea Network Information Center (http://www.nic.or.kr)
MIC: Ministry of Information and Communication (http://www.mic.go.kr)
Ministry of Culture and Tourism (http://www.mct.go.kr)
Ministry of Education & Human Resources Development (http://www.moe.go.kr)
Ministry of Labor (http://www.molab.go.kr)
Ministry of Maritime Affairs and Fisheries (http://www.momf.go.kr)
Ministry of Patriots & Veterans Affairs (http://www.pvaa.go.kr)
MOCIE: Ministry of Commerce, Industry and Energy (http://www.mocie.go.kr)
MOGAHA: Ministry of Government Administration and Home Affairs (http://www.mogaha.go.kr)
National Tax Service (http://www.nts.go.kr)
NC: Name Committee (http://namecom.nic.or.kr)
NCA: National Computerization Agency (http://www.nca.or.kr)
NNC: Number & Name Committee (http://nnc.nic.or.kr)
PAC: Protocol and Address Committe (http://namecom.nic.or.kr)
Personal Data Protection Center (http://www.cyberprivacy.or.kr)
PICCA: Promissing Information & Communication Company Association (http://www.picca.or.kr)
PPS : Public Procurement Servic (http://www.pps.go.kr)
SPPO: The Supreme Public Prosecutor's Office (http://www.sppo.go.kr)
Supreme Court of Korea (http://www.scourt.go.kr)
TTA: Telecommunications Technology Association (http://www.tta.or.kr)
The Constitutional Court of Korea (http://www.ccourt.go.kr)

WHITE PAPER INTERNET KOREA 2004

July 2004

Editor

Ministry of Information and Communication (MIC)

Director General	Kang, Jung-hyup (kangjh@mic.go.kr)
Director	Paek, Ki-hun (khpaek@mic.go.kr)
Deputy Director	Hong, Soon-hee (sooni@mic.go.kr)

National Computerization Agency (NCA)

Vice President	Shin, Sang-chul (ssc@nca.or.kr)
Director	Kim, Yoo-jeong (yikim@nca.or.kr)
Junior Researcher	Park, Dong-hwa (pdh@nca.or.kr)

Published by

National Computerization Agency (NCA)

Center for National Informatization

Department of Internet Policy Development

NCA Bldg, 77, Mugyo-Dong, Jung-Gu, Seoul, Korea, 100-170

tel: +82-02-2131-0248

http://www.nca.or.kr

Ministry of Information and Communication (MIC)

Informatization Planning Office

Internet Division

100, Sejong-Ro, Chongro-Ku, Seoul, Republic of Korea, 110-777

tel: +82-02-750-1247

http://www.mic.go.kr

Printed by

i will

tel: +82-02-2266-5124

fax: +82-02-2266-5125

Attachment 6

Contribution by the Electronic Communications Committee (ECC) of CEPT (009)

Implications for numbering, naming and addressing of the convergence of the Internet and telco networks

Table of contents

Page

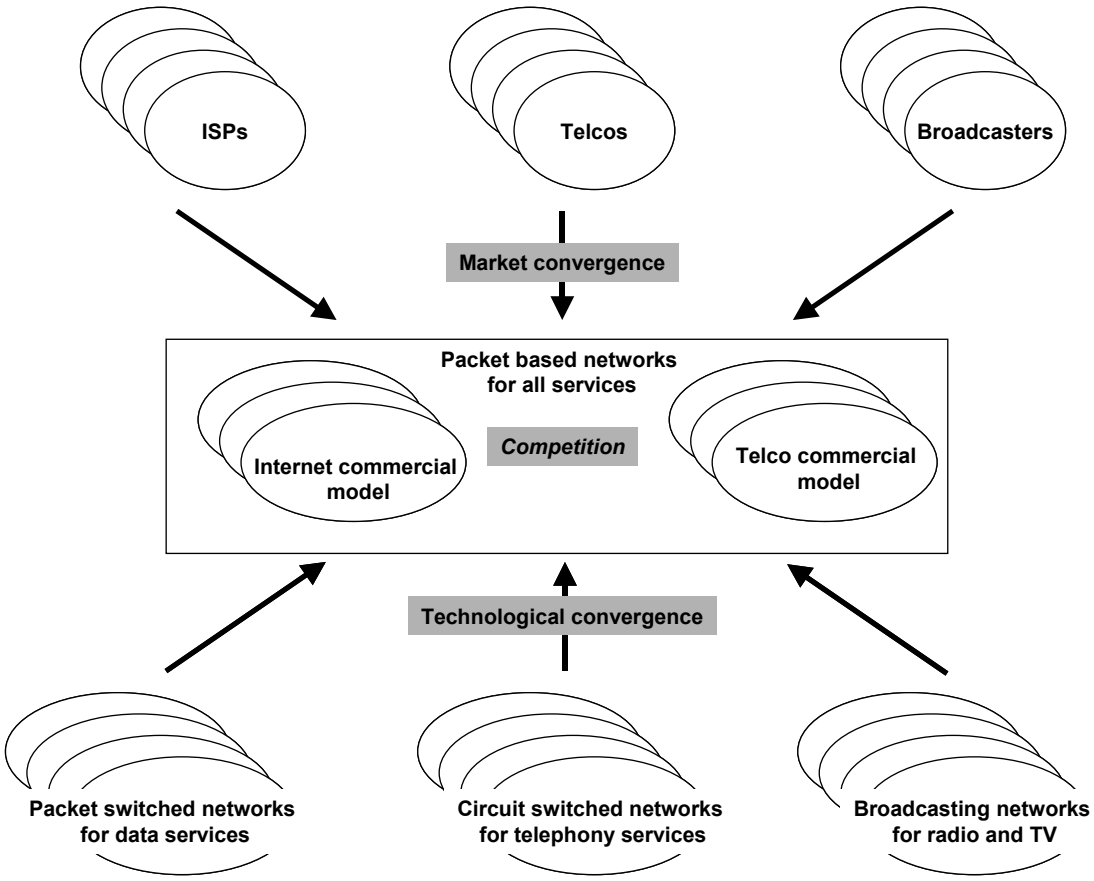
Page

ECC Report 26

Executive summary

This report is essentially in two parts.

The first part provides a general analysis of what convergence means and what are the likely ways in which the telecommunication market may develop. It pays particular attention to the growing competition between the traditional telco approach to networks and the Internet approach. The following diagram summarizes the process of convergence.



This analysis has led to the following conclusions, which are presented together with their implications for numbering, naming and addressing.

1) The public Internet will become increasingly important for communications including real-time communications such as voice.

Implication: Adequate management of the naming and addressing resources on the Internet is needed to satisfy the various commercial and governmental requirements.

2) The different economic models of the telcos (intelligent network with controlled usage and time-based charging) and the Internet (dumb network with open usage and subscription-based charging) will increasingly compete with each other, and there is a possibility that basic communications will become a subscription-charged utility in the future. This means that the future development of the DTN (developing telco network) based on the current telco commercial model is not assured, creating an unprecedented degree of uncertainty in the market-place. Consequently the development of future services will become increasingly diverse and unpredictable.

Implication: Adequate address space is needed to allow a variety of approaches to networks to be tried in the market-place even though some may fail.

3) E.164 numbers will be used in three ways for services that are provided over IP:

- Migration of telco services with E.164 numbers to IP
- New telco services on IP that will require E.164 numbers
- New services on the Internet that will require E.164 numbers.

Implication: These developments will lead to increased demand for E.164 numbers and increased diversity in the services that they are used for.

4) Whereas in the past new services were developed cooperatively by the telcos through standardization bodies such as ITU-T and ETSI, service development through these bodies for fixed networks has largely ceased, although it is continuing to some extent in the mobile area for third generation systems. Innovation in services is now focused on the Internet where services are created at the edge of the network and "terminal functionality" is provided through downloadable software. Service innovation is also fragmented with various companies developing similar but incompatible services such as Instant Messenger. The main area of growth at present is distributed customized applications.

Implication: Naming and numbering in the future will have to be able to support a much less stable service environment because they can no longer be related to well-defined services. This will in turn lead to a loss of the information that can be deduced from numbers such as service type, tariff level and location. Consequently there will be a need for more comprehensive directories and other sources of service-related information.

5) The availability of the Internet as a "dumb network", and the scope for creating and running services from outside the network is stimulating the development of intelligent software-based terminals that use general purpose hardware such as PCs and PDAs.

Implication: This will lead to reduced control over how numbers and names are used and increased threats to the integrity of the E.164 numbering scheme (i.e. use of numbers for services for which they have not been assigned, and the adoption of numbers without regard to the formal assignment processes).

6) There is growing user demand to make services more user-friendly especially as sophisticated telecommunications become a pervasive part of society and not just a tool for people who are better educated or interested in computing. These objectives are driving new initiatives to simplify identification and to reduce the number of identifiers that users have to handle. More information on the current concepts that are being developed is given in a later section.

Implication: There may be a need for better centralized directories and other support functions especially for information relating to new services in order to support greater user friendliness.

7) There is a strong trend towards the separation of network operation and service provision. This separation is already an integral part of the structure of the Internet but it is being adopted also by the telcos in their plans for DTNs. This separation of service provision is likely to result in services being provided from outside the country where they are used.

Implication: As above. There will also be problems in the loss of reliable geographic information, the control of services and the support of law enforcement, which relies heavily on numbers.

8) As networks become capable of supporting multiple different services there will be increasing pressure to use numbers for multiple services. This development will break the relationship between numbers and network operation and lead to requirements for a new approach to number assignment and personal numbering.

Implication: Numbers will become multi-service in the same way that Internet names are multi-service. This will create increased pressure for the individual/personal assignment of numbers and the need for adequate methods of validating people's rights to use a given number. It will also result in loss of information from numbers because the information normally relates to specific services.

9) Numbers are a very useful form of identifier especially for services that are potentially global and are used in a wide range of different cultures. Therefore there is likely to be increasing demand for E.164 numbers not only from both the telco and Internet-based communities, but also for purposes that go beyond communications.

Implication: The increased and diverse demands will put pressure on the structure of the E.164 scheme and it will become increasingly difficult to decide what range of numbers to use for new services. The demand for global numbers, i.e. numbers that are not country-specific, will increase. Demand will develop to use E.164 numbers for purposes that are beyond telecommunications.

The second part of the report explores these implications and makes various recommendations for future work within ECC. The recommendations are:

Recommendation – 1

CEPT as an independent organization should not become involved in the ongoing debate about government involvement in Internet naming and addressing. The issues are discussed in the Government Advisory Committee of ICANN and ITU with the European position being prepared in the Internet Informal Group (IIG) convened by the Commission, and there is little point in attempting to duplicate the discussions within CEPT. However, these arrangements do not provide scope for participation by all CEPT members who are not members of the EU, and CEPT administrations could ask the Commission to expand the membership of the IIG.

Recommendation – 2

Each national government should take steps to ensure adequate coordination between the people responsible for managing E.164 numbers and those responsible for managing domain names, irrespective of the legal and organizational arrangements.

Recommendation – 3

The Working Group Numbering, Naming and Addressing (WG NNA) should keep an active watch on the development of IPv6 and the usage of IPv4 addresses.

Recommendation – 4

WG NNA should study the issues that will be involved in the introduction of IPv6, preferably through a case study.

Recommendation – 5

WG NNA should develop guidelines to help national regulatory authorities handle the wide variety of applications for the use of E.164 numbers for voice communications over IP technology including the Internet.

Recommendation – 6

WG NNA should study in more depth the use of numbers for multiple different services and produce guidance on the problems that can arise and how they can be avoided.

Recommendation – 7

WG NNA should keep a close watching brief on the public and private sector developments for simplifying user identification.

Recommendation – 8

WG NNA should keep a watching brief on the development of directories and if necessary study in greater depth the scope for competition in basic telephony-related directories and the possibility of developing more comprehensive directories for new services.

Recommendation – 9

WG NNA should keep a watching brief on the development of number databases for use by network operators and public support functions.

Recommendation – 10

WG NNA should study the numbering and naming aspects of multichannel access to services.

1 Introduction

The aim of this report is to identify the main changes in telecommunications that come under the general title of "Convergence" and to analyse their implications for numbering and naming. The report is written from a top-down perspective and so necessarily includes an overview and analysis of the main economic and commercial developments and trends in the market and the likely technological developments that underlie them. This report should therefore:

- Help governments and NRAs to understand better the process of convergence and in particular the key developments that determine how rapidly convergence will proceed
- Analyse how users are likely to be affected by convergence and what new user requirements are likely

- Assess the significance of various recent developments including ENUM, UCI and new commercial identification schemes
- Identify the main issues for numbering and naming that ECC will need to study further, covering both policy and technical issues.

The scope of the report is only to identify issues that arise out of convergence. Further separate work is planned to resolve the issues identified. The scope of the report does not cover all forms of identifier, for example it does not include E.212 or E.118. These identifiers may be affected by convergence and assignment of these identifiers may be needed for services provided on the Internet but these issues are for further study.

Whilst the report contains a significant amount of material about future markets, it aims only to indicate the possibilities for commercial development and is not intended to predict exactly where the market will go and certainly not where it should go.

2 Definitions and abbreviations

2.1 Definitions

The analysis and discussion of convergence in this report uses the following terminology. Some terms may have more than one interpretation, depending on the context, origin or usage of such terms, and therefore the definitions below are noted accordingly.

Definitions used in this report

Term used	Definition
Assignment	"Assignment" is used for the process of authorizing the use of a number or name or range of numbers.
NGN	"Next Generation Network (NGN)" is used in the ITU-T sense of the goal of a near universal future network that lies some way beyond the current developments being undertaken in programmes such as TIPHON and 3GPP IP Multimedia. NGN will subsume the PSTN and most of the Internet and add many new capabilities.
DTN	"Developing Telco Network (DTN)" is a term coined specifically for this report to describe the current telco-led developments such as are being worked on in TIPHON and 3GPP as a pathway towards the NGN. Thus the term DTN will be used in many instances where the reader might expect NGN to be used in a loose sense. Furthermore, the term DTN is used to refer specifically to developments and investments aimed at the support of new services as distinct from the replacement of parts of the PSTN with packet based technology either to reduce costs or to provide public telephony in new building developments.
Quality	"Quality" when used on its own is used in a very broad user-orientated sense and includes concepts such as reliability and availability that are treated separately in standardization.
Service	"Service" is used as a description of the combination of the form of information transmission offered and the identification system used for the caller and called parties.

2.2 Abbreviations

The abbreviations in this section apply to the use of terms in this report. Some terms may have more than one interpretation, depending on the context, origin or usage of such terms, and therefore some of the abbreviations below are noted accordingly.

Abbreviations used in this report

Abbreviation used	Explanation
3GPP	Third Generation Partnerships Project
ADSL	asymmetric digital subscriber line
APNIC	Asia Pacific Network Information Centre
ARIN	American Registry for Internet Numbers
ATM	asynchronous transfer mode
CEPT	European Conference of Postal and Telecommunications Administrations
CLI	calling line identity
CLIP	calling line identification presentation
CLIR	calling line identification restriction
DNS	Domain Name System
DTN	developing telco network
E.XXX	Number of the appropriate ITU-T Recommendation, e.g. E.164
EC	European Community
EG	ETSI Guide
ENUM	electronic telephone number mapping
ETSI	European Telecommunications Standards Institute
EU	European Union
GPRS	general packet radio system
HF	human factors
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IIG	Internet Informal Group
IP	Internet protocol
ISDN	integrated services digital network
ISP	internet service provider
ITU-T	International Telecommunication Union, Telecommunication Standardization Sector
LACNIC	Latin American and Caribbean Internet Addresses Registry
LAN	local area network
NAPTR	Naming Authority Pointer
NAT	network address translator

Abbreviations used in this report *(end)*

Abbreviation used	Explanation
NGN	next generation network
NNI	network node interface
NRA	national regulatory authority
OSP	open system provision
PDA	personal digital assistant
PSTN	public switched telephone network
RFC	Request for Comments [IETF]
RIPE NCC	Réseaux IP Européens Network Coordination Centre
RIR	regional internet registry
SIP	session initiation protocol
SMS	short message system
STF	special task force
Telco	Operator of traditional telecommunication networks
TIPHON	Telecommunications and Internet Protocol Harmonization Over Networks
TLD	top level domain
TS	technical standard
TSB	Telecommunication Standardization Bureau
UCI	uniform resource locator
UK	United Kingdom
UNI	user network interface
VPN	virtual private network
WG NNA	Working Group Numbering, Naming and Addressing
WiFi	wireless fidelity

3 Policy and regulatory objectives

3.1 Introduction

Traditional public telecommunications and broadcasting have developed as licensed activities, coordinated at international level by governments in ITU and CEPT with national activities under regulatory control. Whilst competition and liberalization have changed the approach to public telecommunications and introduced many new freedoms, a clear overall framework has endured. All identification issues relevant to telecommunications and broadcasting such as numbering, naming and addressing have been handled within this "governmental" framework (nearly all have related to telecommunications rather than broadcasting, with E.164 numbers being the main scheme).

In contrast, several data networks especially the Internet have developed outside this framework on the basis of common interests with less formal associations and controls. The various identification schemes used in the Internet, principally Internet names and IP addresses, have been established under IANA and ICANN with little or no reference to government, and have sometimes positively discriminated against the involvement of representatives of Government. This situation is now changing to some extent with the proposed restructuring of ICANN but the Internet framework remains largely "non-governmental" compared to the ITU-T framework.

As the Internet becomes increasingly capable of providing an alternative[1] to the traditional methods of public telecommunications and broadcasting, there is a growing awareness of the inconsistency in the degree of involvement of governments in each framework. This has been highlighted by the proposals for ENUM which involve E.164 numbers from the government-run ITU-T framework being used within the Internet Domain Name System.

At the same time new commercial identification schemes such as Microsoft Passport are developing for use on the Internet but outside the control or supervision of ICANN or even any international governmental control. Figure 1 gives an overview of the changing scenario.

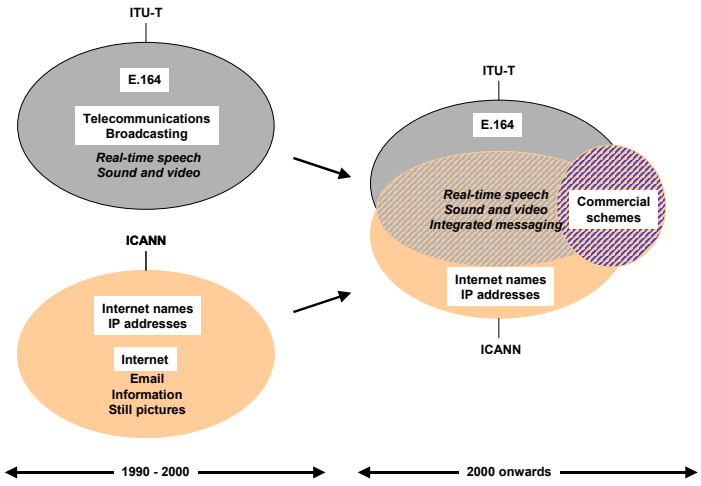


Figure 1 – The changing scenario

3.2 ITU-T objectives

ITU-T is involved in two ways in convergence between the public telco networks and the Internet:

- As a regulatory organization, it is concerned about the growth of the Internet and its organization and management that have occurred on a largely commercial or voluntary basis outside the ITU-T framework, and so undermine the long standing controls and practices that have been developed within ITU-T. This is especially the case in the areas of responsibility for naming and numbering, which has been brought sharply into focus by ENUM, and in the areas of tariffs and accounting rates, since the Internet is being used to bypass the accounting rate system for communications with developing countries. Network operators in countries that have liberalized their public telecommunications have already moved away from the accounting rate system to some extent.

[1] In terms of the functionality perceived by the user, e.g. an "approximate" alternative.

- As a standards organization, it is promoting the development of standards for NGN mainly through the work of Study Group 13, but also involving Study Groups 2, 12 and 16. This standards work partly competes with and partly is complementary to the work in ETSI 3GPP and TIPHON.

The role as a regulatory organization is the role of main relevance to this report.

ITU passed Resolution 102 (see Annex A) in 2002 on involvement with ICANN. The views expressed in ITU-T by European administrations are quite diverse. Some administrations want ITU-T to have more involvement with ICANN and the Internet especially with regard to ccTLDs, and others want to keep control of the Internet in the private sectors subject to national law. For example:

- Some register strong concern about the principles of the Internet and its naming and addressing operating under ICANN, which has developed historically in the private sector as a commercial organization run under Californian law. This view is taken even more strongly by developing countries, especially China.
- Others take a more pragmatic approach, being content that Internet naming and addressing is working satisfactorily in practice and think that it should stay in the private sector and that the reforms in ICANN are meeting the concerns of government.

Whilst it may be useful for the ECC to discuss these different positions, it is probably impracticable for the ECC to try to resolve them through a parallel debate.

In general terms the objectives of ITU-T for NGN have been summarized[2] as:

- facilitate the convergence of networks and services;
- promote fair competition;
- encourage private investment;
- define a framework for architecture and capabilities to be able to meet various regulatory requirements;
- provide open access to networks,

while:

- ensuring universal provision of and access to services;
- promoting equality of opportunity to the citizen;
- promoting diversity of content, including cultural and linguistic diversity;
- recognizing the necessity of worldwide cooperation with particular attention to less developed countries.

Overall the goal of NGN is the development of a single universal network platform that will support all the existing services without loss of performance and also support new services. The vision of NGN is shown in Figure 2.

---

2 Taken from SG 13, Q12/13 TD 19 of meeting 29 October - 8 November 2002.

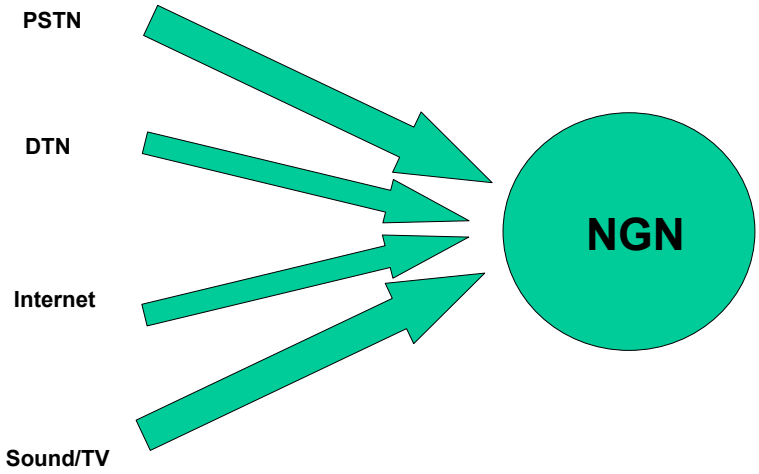


Figure 2 – The ultimate goal of NGN

3.3 European objectives

A new framework of directives was adopted by the European Union in 2002 and the deadline for implementation in national law is 25 July 2003. The general objectives are described in Article 8 of the Framework Directive (2002/21/EC).

Article 8.1 states that regulation should be **technologically neutral**.

This means that the aims of regulation as described in the EU directives have to be applied for all public telecommunication networks. This includes all packet switched networks such as the Internet.

Article 8.2 requires Member States to **promote competition** by:

(a) ensuring that users, including disabled users, derive maximum benefit in terms of choice, price and quality;

(b) ensuring that there is no distortion or restriction of competition in the electronic communications sector;

(c) encouraging efficient investment in infrastructure, and promoting innovation; and

(d) encouraging efficient use and ensuring the effective management of radio frequencies and numbering resources.

Article 8.3 requires them to **develop the internal market** by:

(a) removing remaining obstacles to the provision of electronic communications networks, associated facilities and services and electronic communications services at European level;

(b) encouraging the establishment and development of trans-European networks and the interoperability of pan-European services, and end-to-end connectivity;

(c) ensuring that, in similar circumstances, there is no discrimination in the treatment of undertakings providing electronic communications networks and services;

(d) cooperating with each other and with the Commission in a transparent manner to ensure the development of consistent regulatory practice and the consistent application of this Directive and the Specific Directives.

Article 8.4 requires them to **promote the interests of citizens** by:

(a) ensuring all citizens have access to a universal service specified in Directive 2002/22/EC (Universal Services Directive);

(b) ensuring a high level of protection for consumers in their dealings with suppliers, in particular by ensuring the availability of simple and inexpensive dispute resolution procedures carried out by a body that is independent of the parties involved;

(c) contributing to ensuring a high level of protection of personal data and privacy;

(d) promoting the provision of clear information, in particular requiring transparency of tariffs and conditions for using publicly available electronic communications services;

(e) addressing the needs of specific social groups, in particular disabled users; and

(f) ensuring that the integrity and security of public communication networks are maintained.

The accompanying Universal Services Directive (2002/22/EC) includes provisions specifically for numbering concerning:

- Comprehensive Directory Enquiry services (Article 5)
- Single European emergency number (Article 26)
- European international access code (Article 27)
- Number portability (Article 30).

These requirements of the Universal Services Directive, however, apply only to "publicly available telephone services[3]" and so only involve E.164 numbers. They would include IP technology only where it is used for "publicly available telephone services" but exclude voice communications over the Internet and more advanced services offered over DTNs that would not fit the description of "telephone service".

The accompanying Directive on Privacy and Electronic Communications (2002/58/EC) harmonizes the provisions of the Member States whereby the latter required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.

This means that the requirements of the Privacy Directive apply to all public telecommunications, including the Internet.

4 User objectives

No formal user objectives have been agreed for numbering but the following objectives have been proposed from time to time:

- The separate communications requirements of the end user originating a communication and the end user receiving a communication are addressed.
- The privacy of end users is protected.
- Both the end user originating a communication and the end user receiving a communication can be confident that the other's identity is authentic.
- The number of communication identifiers associated with an end-user is minimized.

[3] These services include facsimile and dial-up Internet access

- Communication identifiers associated with an end user are stable over time.
- End users are able to easily capture identifiers associated with other end users with whom they communicate.
- End users can easily control how and when they are communicated with by other end users.

  (Identified by ETSI Specialist Task Force STF180, "User Identification solutions in converging networks", at Numbering 2001 conference, June 2001.)
- Communication identifiers associated with an end user are easy to remember or to find.
- Communication identifiers associated with an end user may be retained when the end user changes location or changes the operator providing service to a particular identifier.
- Communication identifiers should, where they have a connection with call charges or location of an end user, enable such information to be readily identified.

  (Identified by Claire Milne, Antelope Consulting, "The Design and Management of Numbering Systems" in Telecom Reform: principles, policies & regulatory practices, edited by William H. Melody.)
- Communication identifiers have the possibility to be personal to a particular end user.

  (Identified by Knut Nordby, ETSI Human Factors, "User identification in future networks", presentation at Numbering 1999 conference, October 1999.)

In addition, work in the ETSI TIPHON project has identified the following aspects of user friendliness in non-numeric names:

- Ease of being remembered by a human
- Ease of identifying the person or terminal or line from the name
- Ease of being written (or input to a terminal) without error
- Ease of being generated from first principles if the name is not known or has been forgotten (this is an advantage only when there are inadequate directory services).

The work also drew attention to the issues of:

- Use in different languages
- Use in different alphabets
- Replication (i.e. non-uniqueness) of natural names.

and concluded that the scope for a user-friendly non-numeric naming scheme is quite limited unless the context is restricted such that there is a single language/alphabet and replication is very low. This work also commented that many of the benefits of user friendliness can be achieved in other ways by intelligent terminal software.

The objective for the future is a coherent multiservice network with a separation of service provision and network operation and a simple user-friendly identification system.

5 What convergence is and what is driving it

Convergence means "coming nearer together" but it is a term that is applied very loosely in telecommunications.

The main driver of convergence is digitization which reduces all telecommunication transport-services and applications to bit streams. Digitization is likely to become universal.

The secondary driver is the ability to provide both connection-orientated and connectionless communications on the same packet based infrastructure, where for example Internet protocols are becoming more widespread but not necessarily universal.

These two drivers are making new networks capable of supporting multiple or all services and applications. Therefore "multiservice" is a major element of "convergence". All services and applications converge on the same networks, and all networks become capable of providing the same services.

The trend towards networks becoming capable of supporting multiple different services has little impact on the use of Internet names as these are capable of being used in connection with multiple services. In respect of E.164 numbers, however, this trend creates pressure to use the same number with several services. One implication of such a development is that the connection that currently exists between numbers and network operation is no longer unique and, to a large extent, ceases to exist. This implication suggests the need for different approaches to assignment of numbers or the greater use of personal numbering, to ensure individual end users can exercise full control over how their numbers are used. A second implication of the use of the same number with multiple services is that information which may currently be derived from numbers, such as the associated type of service, is no longer reliable.

E.164 numbers are used for the routing of calls within and between traditional telco networks, in the same way that Internet addresses are used for the routing of packets on IP networks including the public Internet. However, there is no technical reason preventing services running over the Internet using E.164 numbers for identification of end users. There may be advantages for Internet-based services in using E.164 numbers, in that they are familiar to end users around the world, are simple, and can be used from legacy equipment (such as traditional telephone terminals) which may be supported by these services.

The drivers of convergence mean that E.164 numbers are likely to be used, not only for services provided on traditional telco networks, but also for:

- Services that are migrated by telcos from their traditional networks to IP networks
- Entirely new services provided by telcos on their IP networks
- Entirely new services provided on the public Internet.

There are some important differences between the various networks that are discussed further in section 5:

- The Internet is becoming capable of providing telephony and broadcasting services with only minor changes and a continual steady growth in its characteristics
- Telcos need to develop new capabilities, i.e. DTNs, to provide new services
- Broadcasters are investing in digital technology and new delivery methods, e.g. satellite, cable and the Internet, and additional capabilities, e.g. return channels, although they are not replacing their existing terrestrial radio broadcasting channels.

This technological trend of convergence is driving profound changes in the market-place. Because networks become universal transport networks, network operators who previously supported services in a single market gain the scope to play in markets that were originally served by quite separate network operators and organizational arrangements. This leads to market convergence where separate markets of the ISPs, telcos and broadcasters are all merging. However this market convergence is bringing the different historical commercial models of the telco and the Internet increasingly into direct competition as each becomes capable of supporting the same services. Figure 3 shows the overall process of convergence.

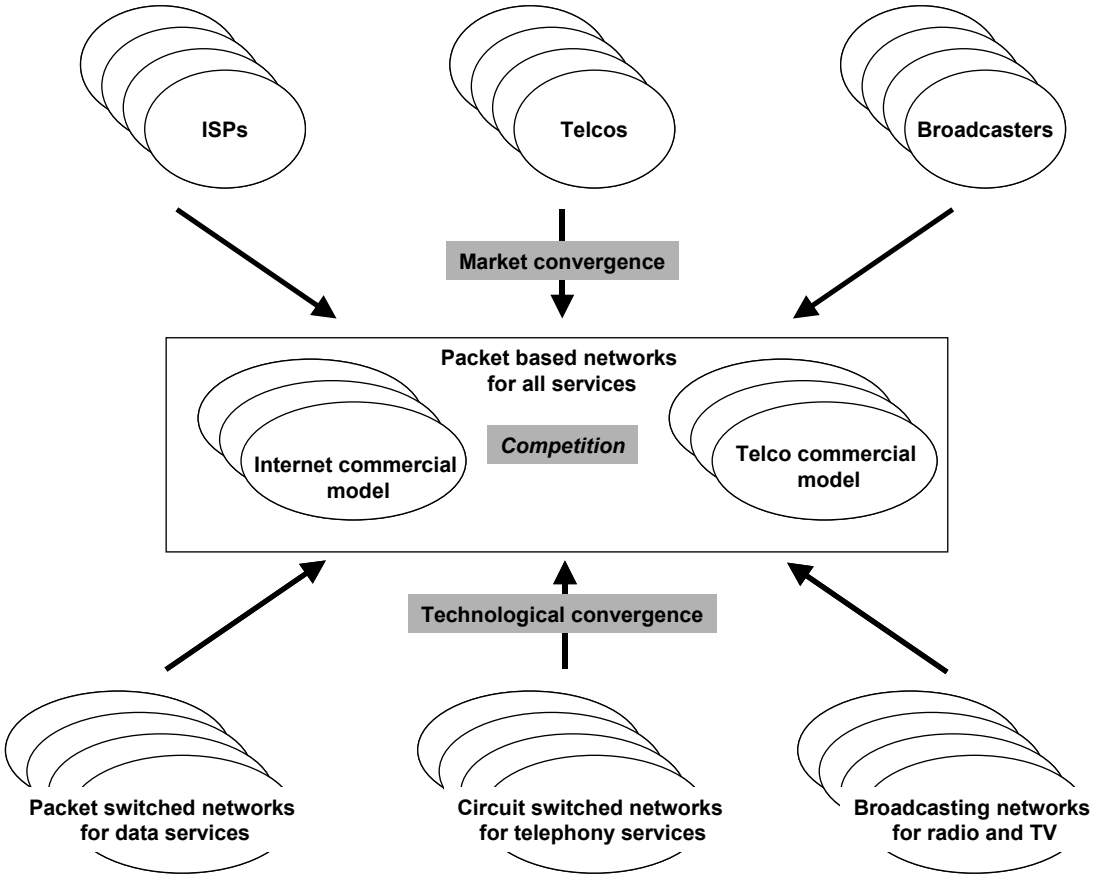


Figure 3 – The process of convergence

The word "convergence" may imply to many people a constructive convergence where different entities draw together and produce a synergy that creates new possibilities. The technological aspects of convergence are constructive in this sense as they allow a fuller spectrum of services and provide much more scope for the integration of different service types and roles.

The commercial aspects of convergence are quite different since they will lead to increasing competition between the players whose businesses were originally confined to single separate markets. Since broadcasting (terrestrial and satellite) will continue to be needed indefinitely and is funded by the programme distributors, it is not threatened by the ability to deliver programmes over the Internet and over DTN. In contrast the telcos are threatened significantly by the prospective loss to the Internet of telephony paid for by users according to their usage. This is why the main commercial competition will be between the different commercial models of the telcos, with largely usage-based charging, and the Internet, with largely subscription-based charging.

Overall, the word "convergence" does not seem to fit particularly well with the period of intense competition that is starting.

One of the main conclusions of the analysis of the market situation below is that although the telco and Internet worlds are competing, they are likely to continue in parallel for the medium-term future and it is not clear to what extent they will converge eventually to a single solution (the NGN). The effect of competition is likely to be that some traffic moves from the telco world to the Internet world and vice versa but both will continue for a period of time. The possibility of the two worlds converging to a single universal technical and commercial model is probably many years away. Thus in some respects the Internet and the telco networks are not converging at present but are staying far apart.

Convergence is not a simple process. Technologically networks are converging on the use of IP technology but the methods of managing the networks and the provision of services differ significantly, and the telco and Internet business models are coming increasingly into competition with each other. From a market perspective, convergence means that organizations that previously worked in distinct areas are increasingly becoming able to provide a wider range of services and compete with each other.

6 Current market situation and developments

Overall the market currently lacks direction. After a period of diverse investments, many of which have not been profitable, the top priority for many operators is to manage their debt situations.

In terms of fundamental resources:

- Local physical infrastructure remains expensive
- Transmission costs have fallen and are falling very rapidly thanks to a combination of absolute costs (cost per bit) and coding that enables more use to be made of a bit (e.g. voice coding)
- Switching costs are falling but faster for IP-based switches than for circuit switches
- Billing costs are falling only slowly, and the overheads of running a telecommunication business are increasing as a result of increased regulatory compliance costs including areas such as data protection.

This situation leaves telcos refocusing on core business, but with some developing broadband access networks.

There is a great deal of discussion and confusion about how telecommunication networks will develop at a technical level in the next few years. Three years ago everyone was expecting the rapid and near universal adoption of IP technology, but since then the whole investment climate has changed and the current situation is much less clear.

Communication services can be classified in many ways but there are two important distinctions:

- User-user services compared to user-host services
- Real-time services compared to store and forward services (real-time also means delay sensitive).

Figure 4 shows how services (grey ellipses) relate to these categories and which networks (coloured rectangles) are best suited to each category. In the past each network was designed for a particular service type, but now we are seeing the Internet becoming capable of providing real-time services such as speech and sound and video broadcasting, in other words it is spreading into these other service areas. In contrast, the DTN will be a new development starting from nothing and capable of providing all services.

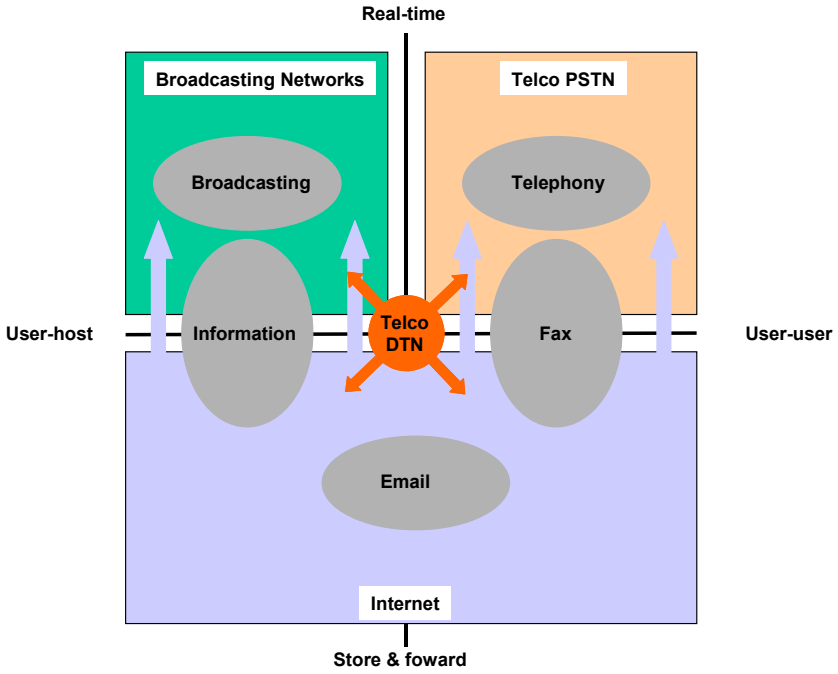


Figure 4 – Network developments in relation to services

In terms of total traffic volumes, the volume of "data" on the Internet continues to grow and is estimated to be several times the volume of telephony traffic, which is static and in some countries beginning to fall. The volume of broadcasting traffic is growing but it is difficult to make an appropriate comparison between broadcast and point-point traffic. Taking very approximate figures for the UK, 50 radio channels at 400 kbit/s and 30 TV channels at 10 Mbit/s give a loading of 320 Mbit/s one way. In comparison, the total telephony traffic is estimated to be around 320 Gbit/s in the busy hour[4] with 64 kbit/s per channel, some three orders of magnitude higher. The comparable figures for Switzerland are 514 Mbit/s and 30 Gbit/s.

Figure 5 shows a credible view of how networks will change. The diagram[5] is best viewed in colour as the colours are significant. The blue rectangle covering the whole diagram illustrates the dependence on a common IP-based transmission platform, the exception being the lop left hand corner where circuit switching is still used. The diagram shows the terrestrial and satellite broadcasting arrangements continuing unchanged but losing traffic to the Internet. The main economic issue is whether new services will develop on the DTN or on the Internet.

---

4 This is based on 60 billion minutes of traffic from fixed telephones per quarter as given by Oftel for Q2 2000/1, using 50 working days per quarter and 4 hours of traffic per day at the busy hour level, giving 5 million simultaneous conversations.

5 Adapted from a diagram produced by Mr Nozsek of Deutsche Telekom.

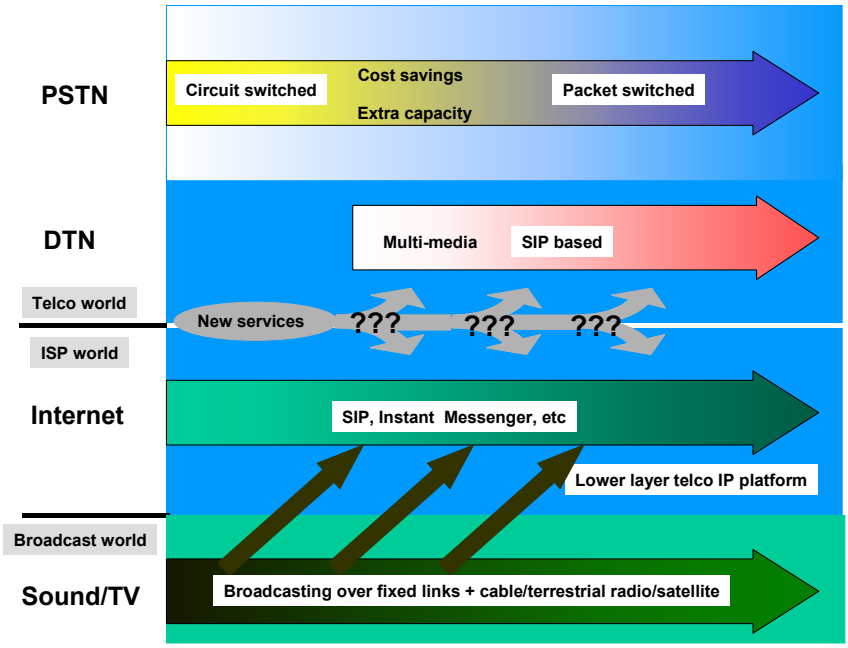


Figure 5 – Short to medium term network developments

6.1 PSTN and mobile networks

The PSTN/ISDN and the mobile networks are largely circuit switched. Public services currently offered using E.164 numbering are likely to continue largely unchanged for the indefinite future because they work well and are universal.

Technologically it is now possible to provide at least basic public services on a packet based network infrastructure that uses either IP or a combination of IP and ATM. The range of supplementary services available may be less than with circuit switching. Although some operators are already using packet based infrastructures in some places, these technologies are working as islands and nearly all interconnections currently remain circuit switched. There is general acceptance that, if there is a widespread migration to packet technology, the approach to network planning and network management will have to change and that there will be some challenges in satisfying all the requirements met hitherto by the circuit switched PSTN/ISDN.

The main justification for replacing circuit switches with packet based switches is economies of scope with new services and cost savings primarily in operational expenditure since the capital expenditure has already been made. This justification will grow gradually if manufacturers fail to supply adequate spares and if the expertise for software modifications is dissipated, but relatively few modifications will be needed and the current circuit switches could remain in use for at least another 10 years, at least at the local level. There are differing reports on the current scope for justifying replacement based on savings.

Where extra capacity is needed, it is less likely that operators will buy new circuit switches and some manufactures may no longer be able to supply them, so they will buy softswitches instead. Since PSTN/ISDN traffic is static or falling (except for Internet access and some calls to non-geographic numbers) there should not be too much need for additional capacity.

The solution to the growing Internet access traffic is to introduce xDSL, e.g. ADSL, and so remove this growing traffic from the local switches and handle it in a more appropriate manner. Some telcos are now pushing ADSL very actively.

Where circuit switches are replaced by softswitches, the aim will be to make the PSTN services appear unchanged. Thus the simplest solution will be to implement the No. 7 signalling protocols over IP with minimum changes. Manufacturers are already doing this for transit-level switches (Class 4) but few if any have yet developed softswitches with the full capability of local exchange circuit switches, but this will change.

At the international level, there are now several IP-based networks that handle international traffic including traffic from incumbents and the entry into the market of these networks has helped to create an active market in international call minutes. Some of this traffic is handled on dedicated IP networks and some on the public Internet.

Mobile operators are currently grappling with the introduction of GPRS to provide Internet access and better data services. The always-on GPRS Internet access is analogous to ADSL but much slower although higher speeds should be achieved with 3G technology. The GPRS backbone is at an early stage of development but operators are increasingly marketing it as a means of Internet access rather than as a bundle of operator-specific services. Mobile networks are increasingly substituting for fixed networks in terms of the provision of telephony, for example some households no longer have fixed telephones, but the cost of cellular mobile data access is likely to exceed that of fixed for the foreseeable future. The longer-term goal of IP multimedia services (3GPP Release 5) is closely analogous to the telco DTN.

The future of cellular mobile networks will be affected quite significantly by the recent and rapid growth in WiFi as a means of providing high bit rate low cost Internet access. WiFi is especially useful for laptops which are normally used in places that can easily be served by WiFi such as waiting rooms, airports, hotels, cafes.

Future developments of WiFi may also compete with fixed access if they can provide a greater operating range.

Figure 6 shows the trends for network access, comparing mobile and fixed networks and the circuit based and packet based forms of access. It shows circuit based access traffic to the fixed networks reducing as the traffic, mainly telephony, migrates to mobile access for greater ease of use or to the Internet over xDSL. A migration of voice communications from circuit switching to packet switching within mobile networks is less likely because mobile packet access is much more expensive than fixed packet access. In any case, the mobile operators have some control over the migration of mobile telephony to the Internet through the combination of their pricing policies and the quality of Internet access that they provide. Thus it is the telephony revenue of the fixed telcos that is most at risk from competition from the Internet.

Information services are currently provided on both the Internet (web) and as telephone response services accessed from the PSTN and mobile networks. These services have seen significant growth in both forms. For many users, access by telephone has been the only option but with the growth in both mobile and fixed data services, telephone access will reduce and be used only where the user prefers the telephone medium to the data medium.

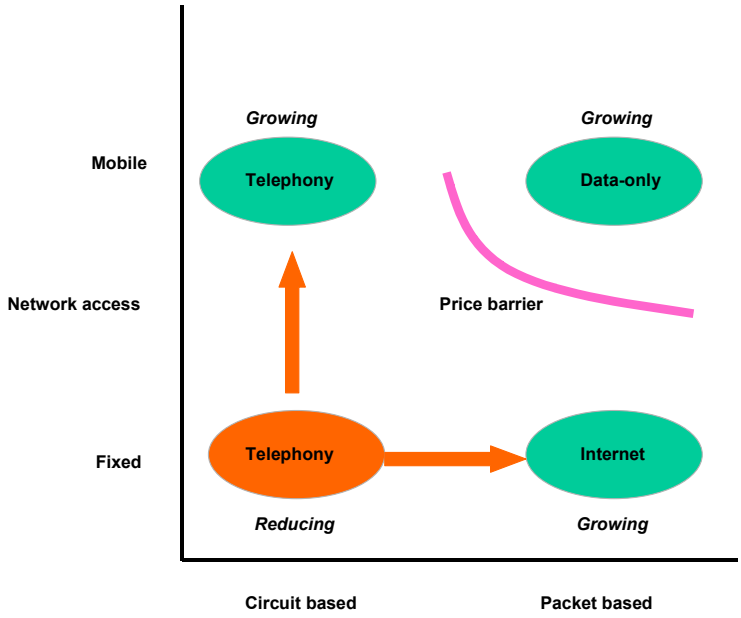


Figure 6 – Traffic trends on different forms of network access

In summary:

- the fixed PSTN/ISDN is likely to stay largely unchanged with slowly declining traffic volumes as traffic is lost to mobiles and the Internet. Its technology will migrate slowly to softswitches, driven by cost savings;
- mobile networks will see some further growth in telephone traffic. They may migrate to a packet architecture if it offers sufficient cost savings but this migration is some way off;
- packet based access in fixed networks is the key to enabling new services to be provided at low cost and is also a principal enabler for the migration of telephone traffic from the PSTN to the Internet;
- mobile data is likely to remain a specialist service on price grounds for the foreseeable future.

6.2 Broadcasting

Broadcasting networks use leased lines, satellite links and point-point microwave links with delivery to the customer via any of the following:

- Cable
- Terrestrial radio
- Satellite broadcasting.

Increasingly broadcasting channels are distributed to end users at lower bit rates over the Internet with reasonably long buffers to correct for the variable transmission delay.

Broadcasting technology is undergoing a major change from analogue to digital terrestrial and satellite broadcasting, and digital broadcast channels will be used for an increasingly wide range of data distribution, e.g. group paging services, and not only for traditional programmes.

Another change is the development of interactive programmes where viewers or listeners respond to the programme or interact with it in other ways. A variety of return channels are used including telephone (voice and direct modem), SMS, web forms and e-mail. The Internet will increasingly be used for the return channel, but the forward and return channels are likely to remain independent because of the diversity of forward channels needed.

Since broadcasting (terrestrial and satellite) will continue to be needed indefinitely and is funded by the programme distributors, it is not threatened by the ability to deliver programmes over the Internet and over DTNs.

6.3 NGN and DTN

The NGN description document produced by ITU-T Study Group 13 says that NGN can be defined by the following fundamental characteristics:

1) Packet-based transfer

2) Separation of control functions among bearer capabilities, call/session, and application/service

3) Decoupling of service provision from network, and provision of open interfaces

4) Support for a wide range of services (including real-time/streaming/non-real-time services and multimedia)

5) Broadband capabilities with end-to-end transparency, including access network utilization considerations

6) Interworking with legacy networks

7) Generalized mobility

8) Unfettered access from users to competing service providers and/or services of their choice.

The term DTN is used for the telcos' initial developments of IP-based networks as a step towards NGN.

There is confusion over whether the term DTN should be used from the perspective of the technology used or the services provided. There is no right answer, as the choice is a matter of definition. The use of the term in this report is primarily from the services perspective, i.e. the capability to provide new services not currently offered by the telcos. The reasons for this usage are:

- The main issue that is affecting the market is whether the telcos will be able to raise revenue from new services provided by the DTN in competition with the services and applications on the Internet. The view taken of these prospects will determine whether or not the telcos invest in DTN.
- Any investment made in DTN is likely to be targeted at the customers most likely to use the services and DTN would therefore be introduced as an overlay to the circuit switched PSTN, although the DTN infrastructure would also be used to provide public telephony to customers of DTN services.
- The "competition" between the DTN and the Internet is likely to be resolved before there is a good case for replacing the circuit switched PSTN with a packet based network on grounds of cost savings, mainly operational expenditure.

SIP is currently the favourite protocol for these developments and work on SIP is being undertaken in 3GPP for its IP Multimedia Platform.

One of the problems with DTN is that few people have clear ideas of what services will be needed. This is one reason why the manufacturers are perusing an "open services environment", as no one is very sure about what to do. In general the telcos want to pursue technical competition in service creation rather than standardization and they are resisting suggestions of service standardization in ETSI.

Figures 4 and 5 show the DTN arrow growing from nothing to indicate its gradual implementation.

6.4 Corporate VPNs

This is currently the area where telco IP-based services are growing most rapidly. The VPNs provide:

- Internal voice communications
- External PSTN access
- Services exclusive to the customer that relate to their operations
- Internet access.

The needs for corporate and public telephony are similar technically to the provision of public telephony over IP, however the protocol is likely to be QSIG over IP since it will be necessary to provide a smooth transition for services from circuit switching to IP.

VPNs are used primarily for telephony, Internet access and functions that relate specifically to corporate operations; there is as yet little innovation in services.

Continued expansion of the VPN market is likely and it is also likely that there will be a demand for interconnection between the VPNs of different organizations. However, this interconnection will only be of value where the "services" of both networks are similar at a technical level. This should be achievable for standardized services such as public telephony and its private counterpart. Where new DTN services have been developed such as video-telephony, interconnection between VPNs run by different telcos will be possible only if the "service" is similar at a technical level, which implies standardization.

6.5 Internet

The public Internet is the third area of development. It is by definition an open services environment but the commercial arrangements are quite different from those of the managed telco networks because the Internet provides a global platform with access paid largely by subscription.

The range of services available on the Internet is increasing and users are able to obtain services, including voice communications, at low or zero marginal price on the Internet, for which previously they had to pay usage based charges to the telcos. There will be differences in the quality of service but these differences may reduce to a level that is not a deterrent for users. Thus the fixed telcos are facing a steady migration of traffic away towards the Internet and also to mobile networks.

The Internet model represents a major threat to the traffic-related revenue of the telcos because the marginal costs of using the Internet are low or zero for many users who have already obtained the necessary equipment such as a PC. In the longer term this may lead to a revision of the economic models.

6.6 Comparison of the telco and Internet models

Figure 7 compares the "closed" telco networks with the "open" Internet. The most important difference is that the telco networks are aware of both the services that they are carrying and the users for whom they are carrying them, and is responding in different ways (e.g. charging) to this information, whereas the Internet is just transporting packets without this awareness.

Current telco networks	Current broadcast networks	Telco DTN networks – closed	Internet – open
• Circuit switched technology • User-user services centrally controlled by provider of transport service • Usage related charges and quality control • Access control for users and interconnection • Interconnection is service related and controlled • Few/no third party services • Intelligent network, dumb terminal[6]	• Circuit-orientated technologies • Delivery by cable, terrestrial radio or satellite • Distribution charges are normally based on the quantity of programmes distributed and not the quantity viewed • Well developed third party service market • Increasing provision of interactive programmes but forward and return channels are independent • Terminals become more intelligent	• ATM/IP-based technology • Run via APIs • Usage-related charges and quality control • Access control for users and interconnection • Interconnection may occur at various levels. Above the IP level it is likely to be service related and controlled • Intelligence focused in telco servers attached to the network	• IP-based technology • No service creation - services and applications run from edge • User-user services run by users themselves • Client-host services run y independent hosts at edge • Access control for users but otherwise open • Interconnection is open and only at IP level • No usage-related charges and little quality control • Gateways to telco networks have control and charging • Dumb network, intelligent terminal

Figure 7 – Comparison of telco networks and the Internet

The distinctions are illustrated in Figure 8, which compares the telco concept of the DTN with the Internet. The figure highlights the controlled and service-related interconnections between the telco networks and the use of APIs through which the "service-aware" telco networks obtain the information that they need about the services.

6 Mobile networks have more intelligent terminals than fixed networks, see section 6.7.

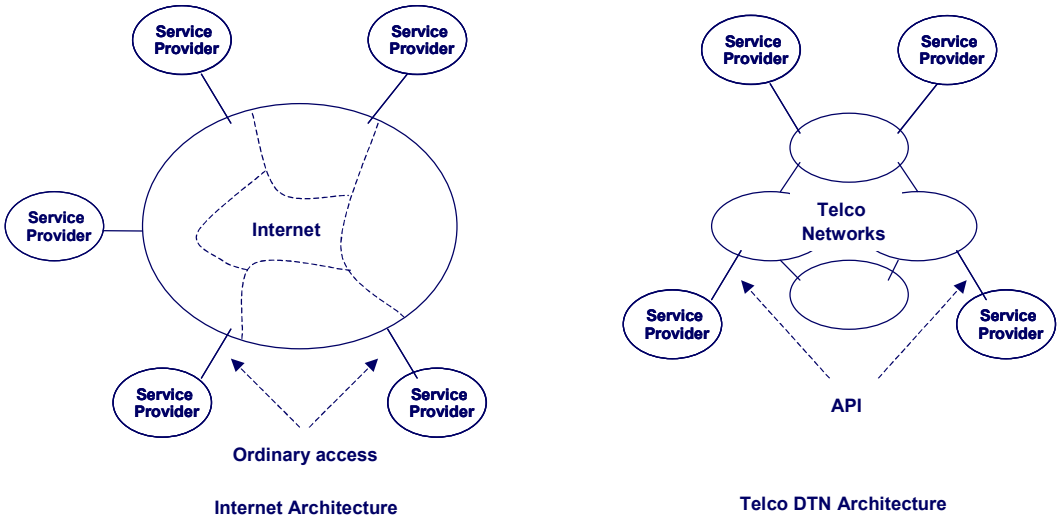


Figure 8 – Comparison of telco DTN architecture and the Internet

6.7 Network architectures and intelligence

The traditional PSTN had a strong degree of vertical integration in that the same organization provided the service, ran the network infrastructure and provided the access technology. The same was true to some extent for broadcasting since many broadcasters ran their own distribution networks.

In contrast, the Internet was always split horizontally into:

- Service providers or application operators
- Backbone network operators
- Internet access providers (ISPs)
- Physical access providers (e.g. the telcos which provided dial-up access circuits or leased lines).

Liberalization, with its focus on competition and opening unbundled access to dominant activities, coupled with the example of the Internet, has created a trend towards all networks becoming split horizontally (less vertically integrated). As the network and access technologies become more multipurpose, there are increasing opportunities for service providers and content distributors to use many different networks. For example messages can be sent and received using many different technologies, and radio programmes are distributed on the Internet as well as by traditional terrestrial and satellite technologies.

Terminals are becoming more intelligent. The functionality in mobile terminals has grown extremely rapidly with pressure from the large-scale consumer market. These terminals initially functioned with pre-loaded software but more recently they are becoming more like general purpose computers into which service providers can download software and upgrade the software when necessary with varying degrees of user visibility and control. The complexity of the software is likely to make this trend continue as new services may not be standardized and service providers will need the ability to add features and correct software bugs.

Intelligence in DTN will be handled differently from the way in which it was handled in PSTN. In PSTN the intelligence was distributed and often duplicated on each switch. In DTN the intelligence is expected to be centralized in a logically single server, with one server[7] for each network. The basic network infrastructure will be dumb and similar to the Internet, except that there will be call-related access control at the network boundaries.

6.8 Voice traffic

The telcos are heavily involved in the support of the Internet in that they supply the basic transmission facilities and dial-up access and in many cases also have large businesses as ISPs, and therefore the growth of the Internet is not wholly a commercial threat. Their main risk, however, is the loss of revenue from usage-based telephone traffic, which is typically some three times that of access line rental.

Voice traffic can be subdivided into three categories:

- Repeat calls to same people (family, friends, colleagues). This is the largest category and the one best suited to Instant Messenger services
- Calls to government, shops, services, schools. This will be a major application for webpages with click-to-talk services as call centres develop Internet access
- "Random other calls". These calls are likely to remain served by PSTN.

Figure 9 shows where voice traffic that has hitherto been carried as telephony on the fixed PSTN is migrating. The migrations are characterized by:

- Slow but accelerating substitution by mobile networks. An increasing number of customers no longer bother to have fixed lines and rely wholly on mobiles.
- Substitution of some short non-urgent calls by text messaging using either e-mail or SMS.
- A slow substitutionary migration of traffic to the public Internet and corporate VPNs. This traffic mainly comprises frequent calls between the same small group of people (e.g. teams at work or distant family members).

---

[7] For service control and call control in TIPHON terminology. There may be other facilities provided as well, such as voice response systems

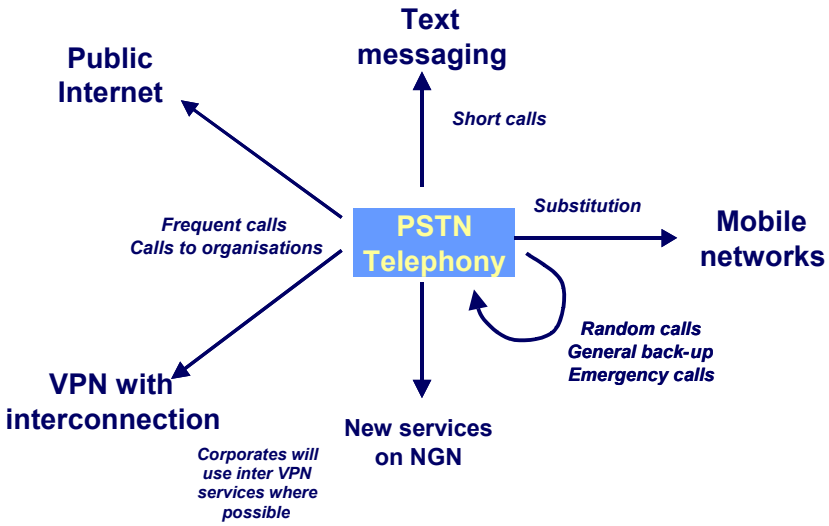


Figure 9 – Migration of telephony from PSTN

Some of the traffic that stays on the PSTN may be handled by IP if IP technology is introduced into the PSTN.

Figure 10 shows the differences in market pressure between the telcos and the Internet. The main pressure on the telcos is to reduce price, the main pressure on the Internet world is to increase quality (in the broad sense of the term).

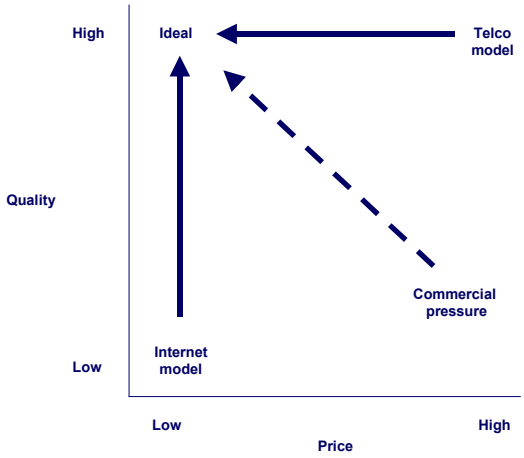


Figure 10 – Market pressures

Three main issues are slowing the migration of voice traffic to the public Internet:

- Transmission quality
- Ease of use
- Blocking by NATs and firewalls.

At present most of the codecs used in VoIP were designed for circuit switched applications and are badly affected by the packet loss that occurs on congested IP-based networks; however, new codecs designed to tolerate packet loss are becoming available and are expected to provide adequate quality even over the Internet.

Ease of use will then remain the critical factor. Voice communications over the Internet at present depend on services such as Instant Messenger to overcome the problem of dynamic assignment of IP addresses. This creates three problems:

- There are different proprietary solutions (e.g. Microsoft, AOL and Yahoo), which results in users having to register with multiple systems, which is not popular. (Interestingly this is the same problem that will be created by the competition in services that the telcos now seem to favour.)
- The call set-up arrangements of Instant Messaging is not as quite simple as making an ordinary telephone call.
- Only some users subscribe to Instant Messaging and so the capability to reach other users is more limited than for PSTN and also not easily predictable.

Dynamic assignment of IP addresses is likely to remain common for the next few years although it might reduce if there is rapid adoption of IPv6. The introduction of IPv6 is uncertain as there are a variety of issues that affect it. Whilst IPv6 will remove limitations in the availability of IP addresses, this may not lead to widespread use of permanently assigned addresses as dynamic assignment and the use of NATs offer some advantages in security that users will take into account.

The ease of use needs to be improved by better software but significant improvements are expected within the next two years.

In most cases, voice communications over the Internet are blocked by firewalls and NATs. Some of the causes of blocking can be solved by changing the policies of the relevant IT departments, but voice communications cannot currently traverse NATs because the NAT cannot be made to translate IP addresses and port numbers for the media streams as well as the signalling. Various activities aim to solve this problem and substantial progress is expected in 2003/2004. Advocates of an early introduction of IPv6 see the possibility of removing NATs as a major driver for its introduction, but its effect will depend on how quickly solutions to the NAT problem are developed for IPv4.

Other developments that facilitate the migration of voice to the Internet are:

- The growing popularity of broadband Internet access with always-on capabilities. Ironically this means that if telcos accelerate the roll-out of broadband access they may facilitate the loss of some voice traffic revenue.
- The rapid growth of WiFi Internet access and especially its provision in public places such as airports, railway stations, hotels and conference centres. WiFi is expected to have major implications for 3G mobile services as it offers better performance at lower prices for the mobile laptop market, and there is the possibility of the development of a large market for WiFi-based SIP telephones.
- Growth in the use of LANs in the home, whether wireless or wired. LANs are being sold in some do-it-yourself stores in some countries.

The main development that is likely to deter the migration of voice to the Internet is the introduction of flat-rate tariffs by the telcos. Such tariffs are becoming more common, whether for the whole day or just for off-peak times, and they remove the cost-saving incentive of using the Internet. Users seem to like flat-rate tariffs because they reduce vulnerability to unexpectedly high bills. Flat-rate tariffs also help the telcos to reduce their costs in handling customer complaints.

The overall conclusion is that voice traffic, which has limited potential growth capability within Europe, will continue to migrate away from the fixed networks to mobile networks and to VPNs

and the Internet. The migration to the Internet is likely to gather pace from late 2003 as the problems of traversing NATs are solved and new facilities make PC-based voice communications more user-friendly.

This migration of voice traffic is unlikely to reduce the demand for fixed access including access to the PSTN greatly as most smaller premises will require Internet access via ADSL or newer technologies and most users will wish to continue to have access to public telephony both for any-any connectivity and for use when other forms of communication fail.

6.9 Service multiplication and concentration

Service providers are multiplying and users are consequently facing:

- An increase in the number of different bills that they have to pay
- An increase in the number of subscriber identities and passwords that they have to use.

This is creating a new market for service and subscription aggregation. This market is not limited to telecommunication services but includes other utilities and the purchase of goods and services over telecommunication networks of all types.

Two of the various commercial identification schemes that are starting are:

- The Federated Network Identity being developed by the Liberty Alliance (www.projectliberty.org) supported by a wide range of commercial interests including credit card companies
- The Microsoft Passport introduced in 1999 with over 200 million registrations by April 2002.

ETSI is also studying a universal communications identifier (UCI) that will probably be based on a subset of E.164 numbers with additional information.

These schemes are concerned not only with identification but also with authentication and the collection and exchange of personal information, and each has its own unique features - they are not equivalents. They are of significant interest to governments who need to integrate their various dealings with citizens (e.g. tax, health, education, motoring, passports, law enforcement). Thus identification systems are being caught up in wider "multidisciplinary" issues. The following statements illustrate some of the conflicting forces at work:

- Users want simpler account and subscription management and billing
- Users want privacy
- Users need protection against identity theft
- Advertisers want information about users so that they can target advertisements, and operators of common identification schemes are in a prime position to collect this extremely valuable information
- Credit card companies want authenticated user identities that they can trust
- Banks and insurance companies want better information for credit ratings and risk assessment
- Governments want to integrate their dealings with citizens and this needs a common electronic identity
- Law enforcement authorities would benefit from any concentration of information about citizens as it would reduce the number of different bodies that they may have to interact with.

Because they are globally unique and understandable across a wide range of languages and cultures, E.164 numbers are potentially a very convenient identifier. For this reason, demand for E.164 numbers may be expected to increase. However, the particular types of numbers that will be sought, and the sources of demand, are likely to change. Requirements for global mobility (e.g. access to services from anywhere in the world) may increase interest in global numbers (i.e. numbers that are not country-specific). Telcos will remain a source of demand for numbers, but Internet application service providers will also seek E.164 numbers. Moreover, the attractiveness of E.164 numbers may result in interest in using them as identifiers for purposes unrelated to telecommunications.

In the telco and Internet worlds, the proposed ENUM scheme for mapping E.164 numbers to Internet names and URLs is receiving a great deal of attention but it is only a part of a bigger picture.

These developments are discussed further later in this report.

The "open" Internet commercial model is competing with the "closed" telco commercial model. Critical issues are how fast voice traffic will migrate on to the Internet and whether new services will use the Internet or the telcos' new networks.

7 Competition between DTN and the Internet

7.1 DTN developments

Whilst there is a clear case for migrating private and corporate networks to an IP platform to provide integrated voice and data, there is not a clear economic case for doing so for public networks. Several operators have undertaken studies of the economic benefits of replacing circuit switched networks with IP-based networks but have found that the benefits do not outweigh the costs.

The fundamental problem for fixed circuit switched network operators is that traffic levels are flat or decreasing slightly for almost all traffic other than dial-up Internet traffic[8]. The strategy of removing Internet access traffic as early as possible on to a separate network platform and leaving the circuit switched network in place therefore seems increasingly attractive and is likely to remain attractive until the maintenance costs of the circuit switches and concentrators become too high. This problem may occur earlier than "necessary" since many manufacturers have ceased, perhaps prematurely, manufacturing spares for this technology. Notwithstanding this, it is unlikely that a clear case will emerge for replacing circuit switches within the next 4-5 years. IP-based infrastructure will therefore be rolled out in parallel as an overlay network to serve:

- New developments
- Areas where high population growth cannot be served by the existing switches
- Customers who specifically need DTNs.

Two of the hopes of the telcos are that:

- Users will want to continue to have "guaranteed quality"
- Service providers will pay to host services on the new telco DTN platforms.

8 The growth of dial-up traffic is also distorting traditional network planning and changing the cost base of networks.

It is not clear whether these hopes will come to fruition. Adequate quality for a high proportion of cases may prove sufficient for most customers, and innovators of new services may prefer to use the Internet and gain global reach to prospective customers at the price of basic access rather than enter special arrangements with telcos whose history of helping third party service development in the intelligent network (IN) era was disappointing.

Within ETSI the support of TIPHON has reduced significantly and there are few signs that manufacturers are implementing the standards yet[9]

7.2 Internet developments

The critical question for the Internet is whether quality (all aspects including transmission) will continue to increase or whether it is currently at its peak, due to excessive "dot-com" investments, and will deteriorate in the future. The trend for increasing dependence on the Internet suggests that people will if necessary be willing to pay more overall for Internet access and so quality can be sustained or improved. In practice it seems that a large proportion of the costs are in the access arrangements and several countries are seeing quite high levels of demand for ADSL access which indicates willingness to pay more for better quality. The fact that most of the bottlenecks are in the access[10] means that it should be possible to achieve a fairly direct relationship between subscription levels and quality, giving the right economic signals to the market.

One of the main methods to improve Internet quality is to segregate traffic of different types (packet length and delay sensitivity) on to different virtual networks so that they queue separately for routers and some priority can be given to delay-sensitive traffic. Techniques for such segregation have been developed (e.g. diffserv) and may be introduced in the future.

7.3 Hybrid developments

There is a great deal of activity in hybrid PSTN-Internet services mostly from smaller new entrant operators. The main businesses established so far are Internet-based services for PSTN break-out that enable users with Internet access to make long-distance and international phone calls at reduced rates, especially into countries with high termination rates.

A group of operators called VisionNG are establishing a service for users with laptops to have both incoming and outgoing calls from Internet connections. They will be assigned numbers from the global code +878 10. Some of the technology developed is a spin-off from TIPHON.

Other potential developments are linkages between ISPs and local exchanges so that Internet users on dial-up access can be warned of incoming telephone calls and either clear to receive them or receive them on their Internet access.

In general the hybrid developments are either specialist services or short-term bypass services that will decline when better access to the Internet is available for more people.

---

9 Most examples of the use of TIPHON standards relate to the OSP protocol for billing and clearing house services, which was developed outside TIPHON and presented to ETSI for republication.

10 Especially in the routers and contention systems used behind the access line.

7.4 Parallel operation

Possibly the most likely outcome is that both the Internet and telco DTN platforms develop in parallel but with the DTN platforms for PSTN developing slowly. It is not at all clear how quickly the Internet will take traffic from PSTN because it is not clear how rapidly the ease of use and NAT problems of voice over the Internet will be solved. It is also unclear how rapidly new DTN services will develop (see next section).

Computer-based systems for voice over the Internet are unlikely to reach the levels of reliability of PSTN for a long time and many customers may choose to retain their traditional PSTN connections for use when the PC or LAN crashes, even when they use the Internet for most of their voice traffic. This combination could be the "best of both worlds".

It is not clear how the competition between the Internet and the new telco networks will develop. Both are expected to continue their developments in parallel and hybrid services that use both networks will also develop. The circuit switched PSTN is likely to remain indefinitely but with gradually reducing traffic volumes.

8 DTN network services

The telcos and their suppliers, who are supporting DTN developments, whether fixed or mobile, are planning to promote technical competition in the development of new services rather than the standardization of new services. Figure 11 shows the architecture planned. This approach applies to both mobile (e.g. 3GPP IP Multimedia) and fixed networks (e.g. TIPHON).

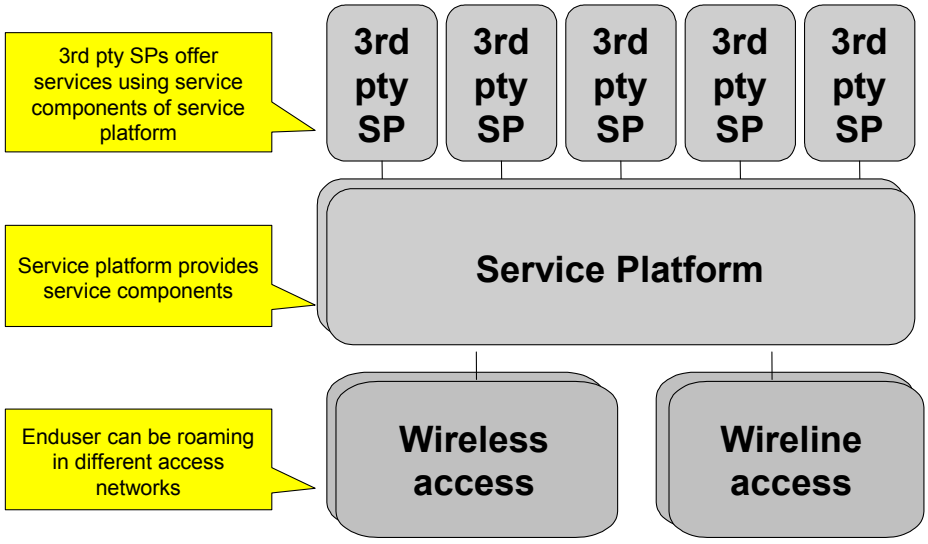


Figure 11 – Architecture of DTNs

The intention is that the network operators will provide a general purpose service platform for the creation of innovative services by themselves and third parties, and that the service platforms and third-party service providers will be able to charge customers on a usage basis.

The service providers will innovate in service creation and place contracts with service platforms for connectivity. This approach raises several issues:

- Network operators were unwilling to promote third-party service creation in the ISDN-IN era and have not yet demonstrated in practice a willingness not to favour their own vertically integrated services
- Service providers will have to negotiate connectivity agreements with the platforms of many different operators if they are to have wide coverage for their services and to have usage-based billing
- Where new client-client services are provided, communications may only be possible between the customers of the same service provider unless different service providers cooperate to offer the same technical service.

It is far from clear how these developments will work out. There is a huge advantage in having a standardized service with standardized UNI and NNI interfaces for public services and also for any "private services" that could be interconnected on VPNs. The standardized UNI interface creates a large independent terminal market, and the standardized NNI provides easy any-any interconnectivity between the customers of different service providers and facilitates the development of comparable reference interconnection offers. Standardization of these interfaces does not inhibit the development of new features that exist wholly within a terminal or wholly within a network. Yet, notwithstanding these advantages, there is currently no support from fixed network operators for producing technical standards for new services, probably because there is no consensus on what services to standardize but a fear of discussing proposals when the focus is on competition between different types of services.

The success of competitive service innovation compared to the traditional standardization route will depend on:

- The extent to which better technical characteristics in a particular service influence the choice of service provider when most customers take many or all services from the same provider
- The extent to which customers find that the loss of an any-to-any capability is a disadvantage when communications are possible only between customers of the same service provider. In other words, how well do the informal groups whose communications account for probably the majority of each person's communications map to the choice of service provider?
- The effect of competition from similar services on the Internet which may not have the same constraints
- The level of competition between service providers

Figure 12 shows some of the possible developments and their dependence on the main key issues.

If quality improves then service innovation is likely to take place on the Internet. If it deteriorates, then the telcos will have more incentive to invest in DTN platforms. If the new services start to develop on the DTN platforms then the main issues will be coverage and coverage and interconnectivity. If they are solved then the current telco model will prevail. If they are not solved then the telcos may have to offer an open platform of higher quality than the public Internet, i.e. an "Internet Mark 2" with higher access charges and higher charges for attaching services but without usage-based charging to simplify interconnectivity.

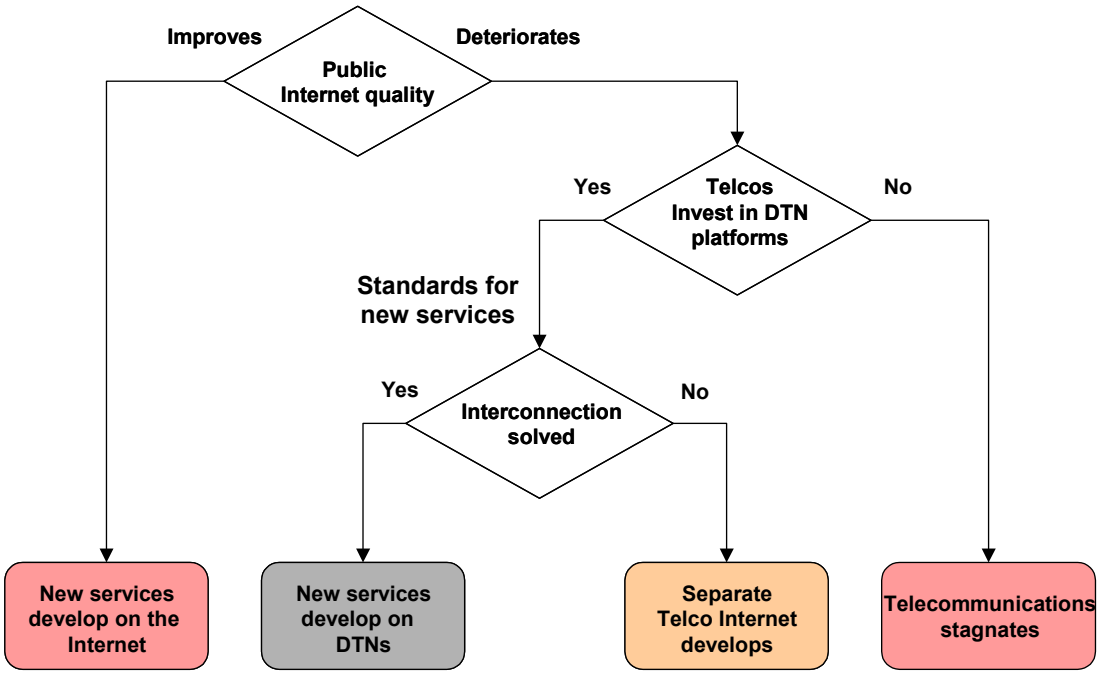


Figure 12 – Possible short- to medium-term developments

The DTN architecture is quite similar to the Internet architecture in terms of the separation of functions and layers and so it creates the similar issues for the commercial and operational relationships between the players . Figure 13 compares the two architectures.

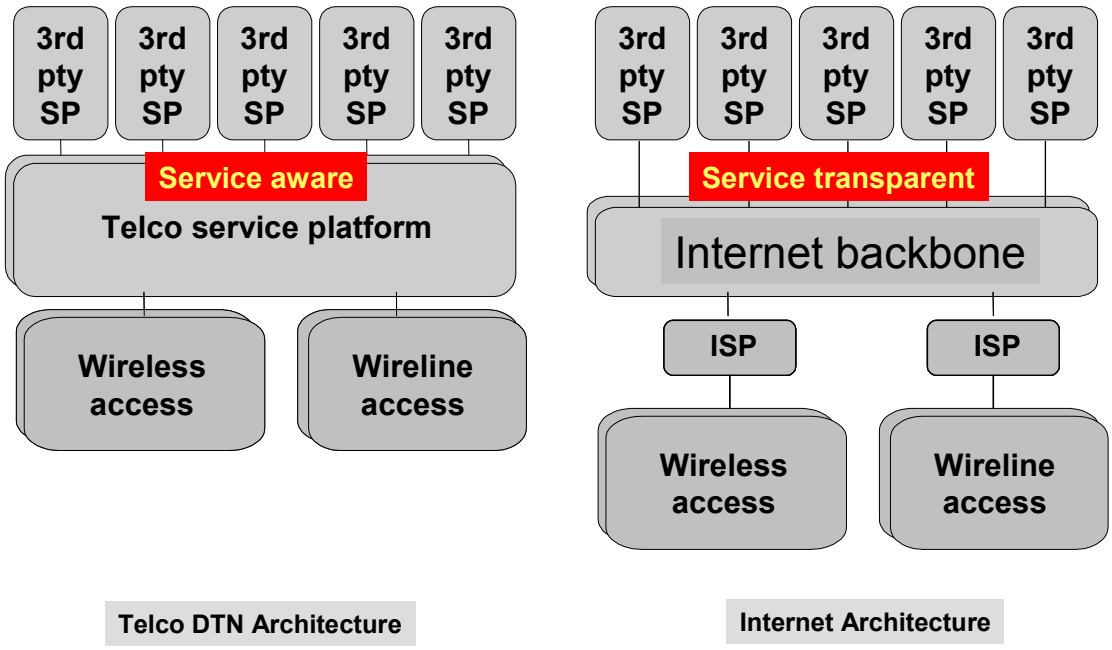


Figure 13 – Comparison of the telco and Internet architectures

The differences lie primarily in the commercial and organizational arrangements. In the Internet model, users pay for Internet access that is general purpose and has no knowledge of the services being used. They may then use any service anywhere and pay the service provider directly as necessary. Thus Internet access is totally decoupled from service usage and so:

- Interconnection between parts of the backbone and between ISPs and the backbone is simple
- Users have access to all service providers.

In contrast, with the DTN model:

- Interconnections between service platforms and possibly between access systems and service platforms are service-specific
- Users have access only to those services that are supported by their access provider and service platform through specific agreements.

Given the unavoidable multiplicity of service providers, the DTN commercial and operational model seems to be impracticably complex and restrictive. This line of analysis points towards the conclusion that the Internet commercial model of an "open" network platform may be the only viable commercial and operational model.

If the telco DTN does not develop because it is impracticable, then it is questionable whether the telcos will develop a "telco Internet" separately from the public Internet. If the quality of the Internet is poor then the telcos could run part of the Internet themselves with better quality and higher access charges. This could be preferable to developing a separate "telco Internet" because it would preserve global connectivity.

Politically the possibility or prospect of the DTN failing and all new services running over the Internet means a continuation and possible enhancement of the dependence of entities in Europe on essential facilities in the United States. This is not limited to DNS servers such as the root servers and .arpa but covers other facilities such as Instant Messenger servers and the servers used for Microsoft Passport. With increasing concerns about national security, this means that United States law enforcement could have better access to information on European citizens than is available to European law enforcement. Furthermore, trade-offs could be made to relax "anti-trust" concerns in return for better access to information for law enforcement.

The structure of the developing telco networks and the Internet both provide separation of service provision from network operation but the commercial arrangements of the closed telco network backbone will make connectivity on the telco networks difficult to achieve. These problems coupled with a lack of innovation in new services by the telcos makes the future of the new telco networks uncertain. The telcos may need to move to more of an Internet model and one possibility is the development of a "telco Internet" with higher charges and higher quality than the public Internet.

9 Conclusions and implications of the market developments

The preceding sections have described the current developments in the market. The second half of the report examines the current initiatives with respect to numbering, naming and addressing and the implications of the market developments for numbering, naming and addressing. Therefore at this point it is necessary to summarize the main conclusions and indicate the implications that are to be considered in the second half.

The main conclusions are:

1) The public Internet will become increasingly important for communications including real-time communications such as voice.

Implication: Adequate management of the naming and addressing resources on the Internet is needed to satisfy the various commercial and governmental requirements

2) The different economic models of the telcos (intelligent network with controlled usage and time based charging) and the Internet (dumb network with open usage and subscription based charging) will increasingly compete with each other, and there is a possibility that basic communications will become a subscription-charged utility in the future. This means that the future development of the DTN based on the current telco commercial model is not assured, creating an unprecedented degree of uncertainty in the market-place. Consequently the development of future services will become increasingly diverse and unpredictable.

Implication: Adequate address space is needed to allow a variety of approaches to networks to be tried in the market-place even though some may fail. The future service environment will become increasingly unstable.

3) E.164 numbers will be used in three ways for services that are provided over IP:

- Migration of telco services with E.164 numbers to IP
- New telco services on IP that will require E.164 numbers
- New services on the Internet that will require E.164 numbers.

Implication: These developments will lead to increased demand for E.164 numbers and increased diversity in the services that they are used for.

4) Whereas in the past new services were developed cooperatively by the telcos through standardization bodies such as ITU-T and ETSI, service development through these bodies for fixed networks has largely ceased, although it is continuing to some extent in the mobile area for third generation systems. Innovation in services is now focused on the Internet where services are created at the edge of the network and "terminal functionality" is provided through downloadable software. Service innovation is also fragmented with various companies developing similar but incompatible services such as Instant Messenger. The main area of growth at present is distributed customized applications.

Implication: Naming and numbering in the future will have to be able to support a much less stable service environment because they can no longer be related to well-defined services. This will in turn lead to a loss of the information that can be deduced from numbers such as service type, tariff level and location. Consequently there will be a need for more comprehensive directories and other sources of service-related information.

5) The availability of the Internet as a "dumb network", and the scope for creating and running services from outside the network is stimulating the development of intelligent software-based terminals that use general purpose hardware such as PCs and PDAs.

Implication: This will lead to reduced control over how numbers and names are used and increased threats to the integrity of the E.164 numbering scheme (i.e. use of numbers for services for which they have not been assigned, and the adoption of numbers without regard to the formal assignment processes).

6) There is growing user demand to make services more user-friendly especially as sophisticated telecommunications become a pervasive part of society and not just a tool for people who are better educated or interested in computing. These objectives are driving new initiatives to simplify identification and to reduce the number of identifiers that users have to handle. More information on the current concepts that are being developed is given in a later section.

Implication: There may be a need for better centralized directories and other support functions especially for information relating to new services in order to support greater user friendliness.

7) There is a strong trend towards the separation of networks operation and service provision. This separation is already an integral part of the structure of the Internet but it is being adopted also by the telcos in their plans for DTNs. This separation of service provision is likely to result in services being provided from outside the country where they are used.

Implication: As above. There will also be problems in the loss of reliable geographic information, the control of services and the support of law enforcement, which relies heavily on numbers.

8) As networks become capable of supporting multiple different services there will be increasing pressure to use numbers for multiple services. This development will break the relationship between numbers and network operation and lead to requirements for a new approach to number assignment and personal numbering.

Implication: Numbers will become multiservice in the same way that Internet names are multiservice. This will create increased pressure for individual/personal assignment of numbers and the need for adequate methods of validating people's rights to use a given number. It will also result in loss of information from numbers because the information normally relates to specific services.

9) Numbers are a very useful form of identifier especially for services that are potentially global and are used in a wide range of different cultures. Therefore there is likely to be increasing demand for E.164 numbers not only from both the telco and Internet based communities, but also for purposes that go beyond communications.

Implication: The increased and diverse demands will put pressure on the structure of the E.164 scheme and it will become increasingly difficult to decide what range of numbers to use for new services. The demand for global numbers, i.e. numbers that are not country-specific, will increase. Demand will develop to use E.164 numbers for purposes that are beyond telecommunications.

The implications of some of these conclusions overlap. The following is the list of implications that are considered further in the second half of this report. These implications are grouped in terms of their subject.

Management of the Internet names and addresses

1) Adequate management of the naming and addressing resources on the Internet is needed.

Availability of Internet addresses

2) Adequate address space is needed to allow a variety of approaches to networks.

Organization of the E.164 scheme and number assignment

3) Naming and numbering in the future will have to be able to support a much less stable service environment because they can no longer be related to well-defined services.

4) There will be increased demand for E.164 numbers and increased diversity in the services that they are used for.

5) The increased and diverse demands will put pressure on the structure of the E.164 scheme and it will become increasingly difficult to decide what range of numbers to use for new services.

6) Numbers will become multiservice. This will create increased pressure for individual/personal assignment of numbers.

7) There will be a loss of the information that can be deduced from numbers such as service type, tariff level and location.

8) The demand for global numbers, i.e. numbers that are not country-specific, will increase.

9) Demand will develop to use E.164 numbers for purposes that are beyond telecommunications.

Control of numbers and names and their use

10) There will be reduced control over how numbers and names are used and increased threats to the integrity of the E.164 numbering scheme (i.e. use of numbers for services for which they have not been assigned, and adoption of numbers without regard to the formal assignment processes).

11) There is a need for adequate methods of validating people's rights to use a given number.

12) There will be problems in the support of law enforcement, which relies heavily on numbers.

Databases

13) There may be a growing need for databases, other support functions and improved directory functions.

10 Naming schemes and their characteristics

From the perspective of numbering and naming, different systems have been developed in the Internet and telco worlds so far, and thus exist on opposite sides of the main axis of competition. The Internet world uses Internet names of the form "user@domain" supported by the Domain Name System (DNS) under the guidance of ICANN. The telco world uses E.164 numbers whose assignment is controlled under ITU-T. Both schemes can be supported on IP-based networks and the telcos may start to use Internet names more as they develop packet-based DTNs.

Figure 14 summarizes the main features of each naming scheme and adds the capabilities of an ideal scheme.

Feature	E.164	Internet name	Ideal scheme
Management	International: ITU-T National: Administrations	International: ICANN National: Mostly various not-for-profit organizations	Open, stable, accountable and responsive
Worldwide suitability	Well established worldwide	Popular in countries that use non-accented Roman alphabet but difficult for countries with other alphabets	Suitable for all cultures and character sets
Sharing	Geographic numbers are commonly shared by users who share an exchange line	Rare	None

Figure 14

Feature	E.164	Internet name	Ideal scheme
Relationship to addresses	Confused: some E.164 numbers are names only, others are both names and addresses	Totally separate	Totally separate
Memorability and user friendliness	Low, expect for golden numbers	Can be better than numbers as can include natural names but diminishing due to increasing number of TLDs, and non-uniqueness of many natural names (see ETSI EG 201 940)	Good
Tariff information	Can be inferred approximately in many cases	Not relevant with the current model	Best treated separately
Support from directory services	Good for geographic numbers	Poor	Good
Relationship to services	Number space is subdivided into ranges for different services and so many users have multiple numbers, one for each type of service	Names are intrinsically multiservice because the application is specified separately, but some users subscribe to services from more than one provider and so may have multiple names	Multi-serve to be simple for the users
Portability between locations	Not normally available between countries but normally available locally in fixed networks	Normally available wherever access to the ISP is possible	Probably both portable and not portable systems are needed as different users have different requirements
Portability between service providers	Supported within some services and some countries, but generally becoming more widely available	Supported if the user has their own domain name, but many users have Internet names of the form "user@service-provider" and so cannot port their name.	Supported
Authentication	Good	Poor	Good
Use by law enforcement	High	Low	High
Data protection (directory CLIP/CLIR)	middle / high	low	High

Figure 14 *(end)*

Ideally users want as few telecommunication identities as possible with each name being capable of being used for multiple services, with a separate mechanism for identifying the services available. This makes it easier for users to remember their telecommunication identities and give their identities to other users.

Figure 14 shows the current situation for a user of services in both worlds.

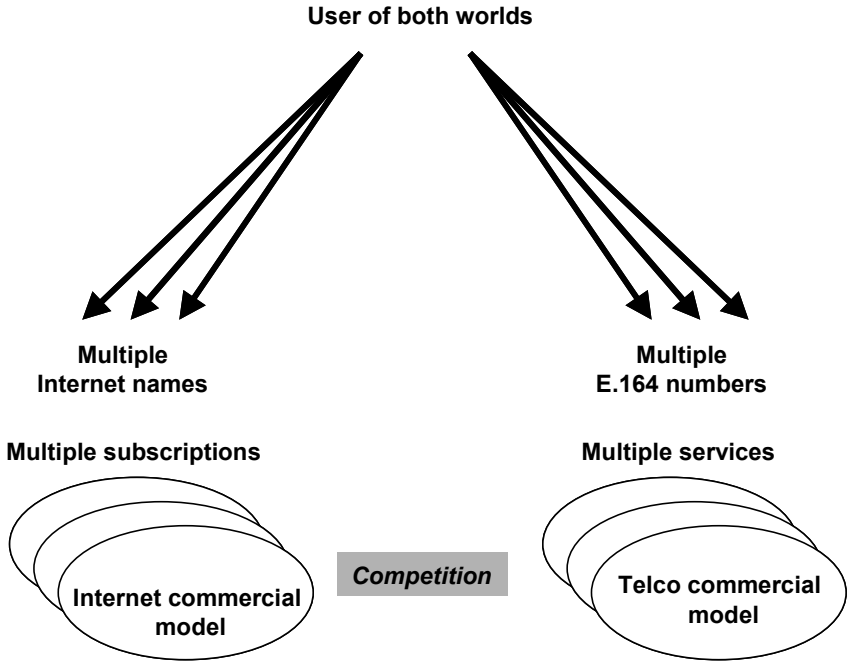


Figure 14 – Current situation for numbering and naming

The ETSI TIPHON project has studied the possibilities for non-numeric naming and has concluded that it is not possible to create a scheme that is significantly better than the Internet naming scheme since all the main problems associated with that scheme are:

- Intrinsic in the use of non-numeric names that are language and alphabet dependent and involve varying degrees of natural replication and intellectual property value
- The consequence of the scheme running on the basis of loose cooperation where anything that does not cause a major problem is tolerated rather than a more rigid system backed by regulation.

11 Current developments for identifiers

The main problem being worked on at present is the multiplication of different identifiers for the same users. This is true both for communication services and for services and transactions over communication services, e.g. purchases over the web. Solutions are needed that:

- Reduce the number of identifiers that need to be used and stored by users
- Simplify and increase the reliability and effectiveness of authentication
- Improve the ease with which users can find out how they can communicate with other users and what identifier to use
- Are adequate proof against fraud and impersonation.

We now review the different schemes that are being developed. There is, however, one fundamental problem that underlies all these developments: because the number of service providers has multiplied, only the users know their own list of identities and services used. Service providers have only a subset of this information and some of the information that they hold, e.g. a fixed telco's record of a user's e-mail address, may be out of date. Thus all improvements are dependent on persuading users to input their information and keep it up-to-date.

11.1 Customizable address books in terminals

Telecommunication terminals are becoming more intelligent and many mobile terminals and personal computers include customizable address books where users can store numbers and Internet names, including ones collected from incoming communications, and associate then with correspondents who can be known by short or nicknames. The availability of these features has gone a long way to make up for the absence of e-mail directories.

11.2 ENUM

ENUM is a proposal to populate the Internet Domain Name System under .e164.arpa[11] with telephone subscriber information using the E.164 number in reverse, thus information about the subscriber for:

+44 71 215 5000

would be held under:

0.0.0.5.5.1.2.7.1.4.4.e164.TLD

This information would use the standard DNS pointers and syntax and would enable a software agent to query DNS using an E.164 number and be pointed to, for example, the subscriber's:

- E-mail address
- SIP address
- Mobile telephone number
- Website
- Entry in a more extensive database.

Thus ENUM provides a one-way translation from E.164 numbers to Internet names and other identifiers. Figure 15 illustrates this.

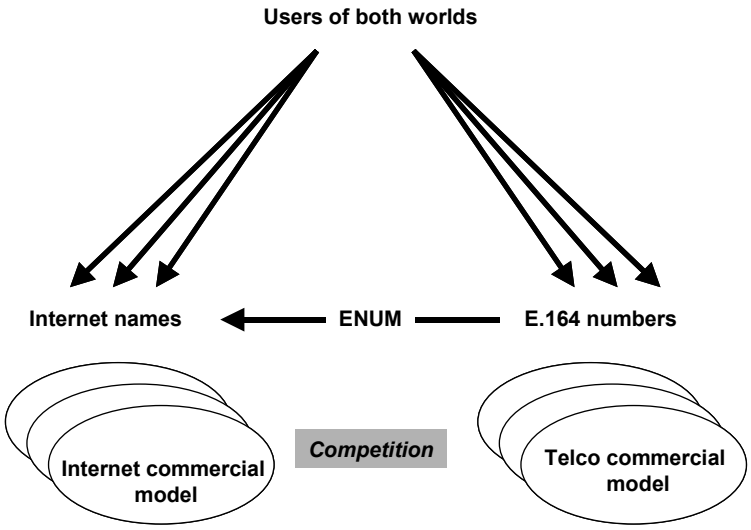


Figure 15 – Role of ENUM (RFC 2916)

[11] IETF has decided to use .arpa for ENUM but a number of administrations in ITU-T want a new TLD to be used, so the situation is not fully stable.

In addition, ENUM allows the E.164 number holder to input and update information about how they wish to be communicated with, e.g. a preference for e-mail.

Several countries including Austria, France, Germany, the Netherlands, Sweden and UK are running or planning trials of ENUM and ETSI has prepared an ETSI TS 102 172 on how information should be stored in the NAPTR records within DNS.

RIPE NCC in the Netherlands, which is also the regional Internet registry for Internet addressees in Europe, has been selected by the Internet Architecture Board as the registry for .e164.arpa and so registers the registries that are appointed for aE.164 country code or regional code.

ITU-T Study Group 2 has approved "Interim Procedures" to request ENUM delegations from RIPE NCC. According to this procedure ITU-T TSB is consulted by RIPE NCC and given an opportunity to object to any appointment. ITU-T TSB consults the relevant national administration and objects to any appointment that is not confirmed as satisfactory by the administration. This arrangement is designed to prevent an unauthorized organization becoming the ENUM registry for a country code. The Interim Procedures will be replaced by an ITU-T Recommendation currently under development.

The following are some fundamental practical issues that will affect the success of ENUM:

1) Correspondents need to know the E.164 number first so ENUM is not as good as directories

2) ENUM is designed only to translate one way and so does not provide a translation from say an e-mail address to an E.164 number. (It would take additional conventions and an expansion of DNS to introduce a reverse translation from Internet name to E.164 number since DNS does not hold Internet names of the form "user@domain", it holds only the "domain" part)

3) Many E.164 numbers are shared because they refer to exchange lines that are shared and ENUM does not handle sharing

4) Many potential users of ENUM do not have a stable relationship with E.164 numbers, e.g. students who move frequently between home, college and temporary accommodation for vacation jobs

5) Only users know all the information that needs to be entered into ENUM and so there will be a need to create incentives for users to populate ENUM, and at the same time a need to cover the costs of running ENUM

6) It will be difficult to ensure the continuing accuracy of information in ENUM.

In parallel with the official development of ENUM, various commercial organizations are offering or planning to offer similar mechanisms in other parts of DNS, i.e. not under .e164.arpa.

Within ITU-T there are a wide range of views about ENUM. Whilst a number of administrations support ENUM, or at least support enabling the creation of ENUM subject to normal market forces, other administrations have two major concerns:

- That most of the .arpa servers are located in the United States.
- That ENUM could facilitate the migration of telephony traffic from PSTN to IP-based networks and cause special economic problems for developing countries who collect substantial national revenue from incoming international calls that have high tariffs.

It is not certain how these concerns will be resolved.

11.3 Universal communications identifier (UCI)

UCI is a new identification system proposed by ETSI and supported by the European Commission that consists of:

A unique numerical identifier + a natural name (e.g. John Smith) + additional information

The unique numerical identifier is the main part of the proposed UCI and is the part that would be used by networks to identify the calling and called parties. The natural name is added to provide more meaning for the human user, for example when they see a CLI they could also see the name of the caller. The additional information would be designed to help directories or user agents and could include information about the preferences of the person identified. The unique numerical identifier is highly likely to be a new range of E.164 numbers. Different values of the unique numerical identifier could be used for personal and business life. This would make UCI an extension of E.164.

Figure 16 shows the function of the UCI in relation to other identification schemes and ENUM.

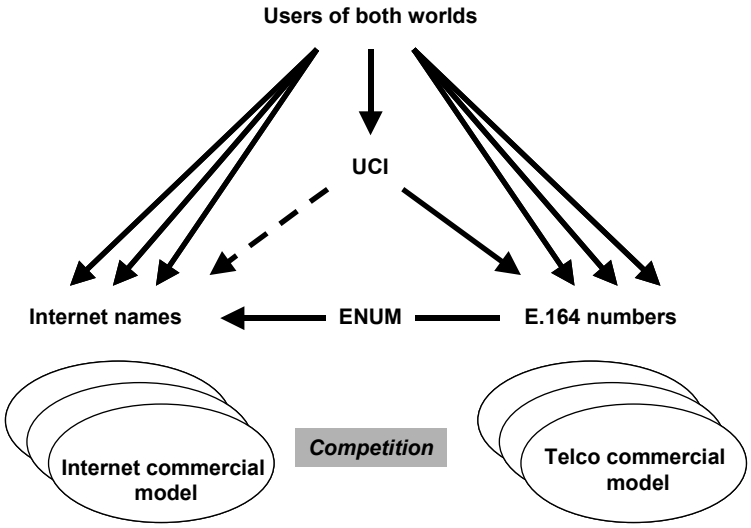


Figure 16 – Role of UCI

Two ETSI Guides have been produced so far:

- EG 201 795: Human Factors (HF); Issues concerning user identification in future telecommunications systems
- EG 201 940: User identification solutions in converging networks

Current work is covering the following issues:

- Downstreaming results of ETSI STF 180 on UCI Services
- Maximizing the usability of UCI-based systems
- Guidelines on the usability of UCI-based systems
- Placing UCI in context; Review and analysis of existing identification schemes
- Results of a detailed study into the technical areas for identification harmonization
- A web-based UCI demonstrator
- Using UCI-based systems to improve communications for disabled, young and elderly people
- Human factors guidelines for real-time person-person communication services.

The work in ETSI is also examining how to authenticate the user's natural user identity and to prevent impersonation and identity theft.

The prospects for UCI are difficult to assess. ITU-T is likely to assign a number range for its use and the current work in ETSI is examining the possibility of using the Internet to carry messages between user agents. It is however unlikely that PSTN will be upgraded to carry the full UCI. It is not easy to predict to what extent user agents will develop. Systems such as Instant Messaging already implement a form of user agent based on an Internet name and they may be reluctant to change to UCI. It is not yet clear exactly how the UCI will be used with Internet names. This is why the line to Internet names in the above figure is shown as dashes.

11.4 Microsoft Passport

The Microsoft Passport is an identification system based on an existing e-mail address supported by a password and run on Microsoft servers. When a user is online, software downloaded into the PC reports into the Microsoft servers which record that the user is online and the current value of the user's IP address. The user is then invited to sign in and does so with their passport (e-mail address and password). While signed in, if the user accesses any website that uses Passport, the access is redirected first to the Passport site where it is validated and returned to the site being accessed. Thus the site can use a different secret and validated identity from Microsoft and so does not need to apply its own separate user name and password system to identify and validate users.

These interactions give Microsoft an unprecedented opportunity to collect statistics on the web-use of users. Passport raises concerns similar to those raised by ENUM but far greater in magnitude.

NOTE – This description of the operation of Microsoft Passport has been deduced from information obtained form articles on the web and not from authoritative source materials.

11.5 Liberty Alliance

Liberty Alliance is an open cooperative initiative supported by a wide range of organizations including:

- American Express
- Cisco
- Ericssons
- France Telecom
- Mastercard
- Neustar
- Sun
- Verisign
- Visa
- Vodafone

It operates quite differently from Microsoft Passport as it has a distributed architecture and does not have a master identity for users.

The objectives are to:

- Enable consumers to protect the privacy and security of their network identity information
- Enable businesses to maintain and manage their customer relationships without third-party participation

- Provide an open single sign-on standard that includes decentralized authentication and authorization from multiple providers
- Create a network identity infrastructure that supports all current and emerging network access devices.

The protocols and software enable organizations to establish their own circles of trust within which users may federate (join up and share) their identities. Users can then sign on once with any member of the circle and then use the other websites in the circle without signing on separately. Existing local sign-on user names and passwords are preserved and can continue to be used for the initial sign-on. The system works by assigning temporary hidden aliases for use with the other sites in the circle of trust.

11.6 Conclusion

All the developments described here are rather different from each other and only Microsoft Passport and customizable address books have been implemented widely so far. Whilst customizable address books will improve and become more widespread as more terminals contain processors, it is not easy to predict whether the other concepts will take off and become well established or will fail. Thus the future developments are unclear.

12 Management of the Internet names and addresses

As the Internet grows in importance, it becomes increasingly important that the management of domain names and IP addresses is stable, effective and efficient, and takes adequate account of issues of public interest.

The following sections treat the political and regulatory issues separately. This is a loose distinction and the issues could be grouped differently.

12.1 Status of ICANN

ICANN is currently responsible for the management of the Internet addressing and naming scheme (IP addresses and Domain Name System DNS). The status of ICANN reflects the historical development of the Internet within the private sector as a network of networks based on voluntary cooperation. ICANN is a private not-for-profit organization based on Californian law but it receives significant inputs from governments on public policy issues through its Government Advisory Committee whose influence has grown over the last four years. The Government Advisory Committee is open to all countries but in practice only some 40 are represented.

A wide spectrum of views are held by various governments on the constitution of ICANN and the scope for governmental participation, and the following summarizes the different ends of the spectrum.

The interventionist view

This view is concerned that a private organization is managing an increasingly important global resource. It considers that the current arrangements on which ICANN is based are unacceptable and too much under United States influence. They think that an entity as important as the Internet needs to be adequately under the control of governments and that governments need to ensure that they retain full national sovereignty over their communications including in particular the use of their ccTLDs. Proponents of this view would like the views of governments to have more formal international authority and their decisions to be binding on ICANN and each other especially in relation to ccTLDs. They would like the arrangements for the Internet to be aligned much more closely with those of ITU.

The non-interventionist view

This view is that the Internet has flourished under self-regulation and has developed faster and better than traditional telecommunications have under the government-controlled ITU-based structures. It believes that the changes now being made in ICANN will provide adequate government oversight through cooperation, and sees no pressing need for stronger government involvement. It considers that national sovereignty is adequately protected by national laws, and that greater involvement would introduce risks of slowing developments and reducing market-led flexibility.

Recommendation – 1

CEPT as an independent organization should not become involved in the ongoing debate about government involvement in Internet naming and addressing. The issues are discussed in the Government Advisory Committee of ICANN and ITU, with the European position being prepared in the Internet Informal Group (IIG) convened by the Commission, and there is little point in attempting to duplicate the discussions within CEPT. However these arrangements do not provide scope for participation by all CEPT members who are not members of the EU and CEPT administrations could ask the Commission to expand the membership of the IIG[12].

12.2 Coordination between E.164 and domain name management

The development of the traditional telecommunication networks/services and the Internet have a totally different historical background. While the traditional telecommunication networks developed in a strongly regulated environment, the Internet developed mostly in the little regulated environment of one country. The same distinction applies to the numbering and naming schemes used by these networks/services. This is also a reason why most NRAs have legal responsibility only to manage the traditional "E.164 numbering plan". Only a few also have formal responsibilities in the field of Internet naming and addressing.

With the convergence of traditional networks and the Internet and/or next generation networks, NRAs are or will be confronted more and more with problems that need expertise in both numbering and naming schemes. This means that in the countries where the formal responsibilities for E.164 and IP/DNS matters are split between different authorities, good dialogue and cooperation between these different authorities is essential to ensure that the public interest is protected in the management of the involved numbering and naming schemes. ENUM is a good example where both E.164 and DNS expertise is important.

Whatever view is taken on the role of government in the management of domain names, the convergence of E.164 and Internet naming requires coordination at the national level between the people who are managing the schemes if incompatibilities and problems are to be avoided.

Recommendation – 2

Each national government should take steps to ensure adequate coordination between the people responsible for managing E.164 numbers and those responsible for managing domain names, irrespective of the legal and organizational arrangements.

---

[12] Norway and Switzerland are allowed to participate as observers.

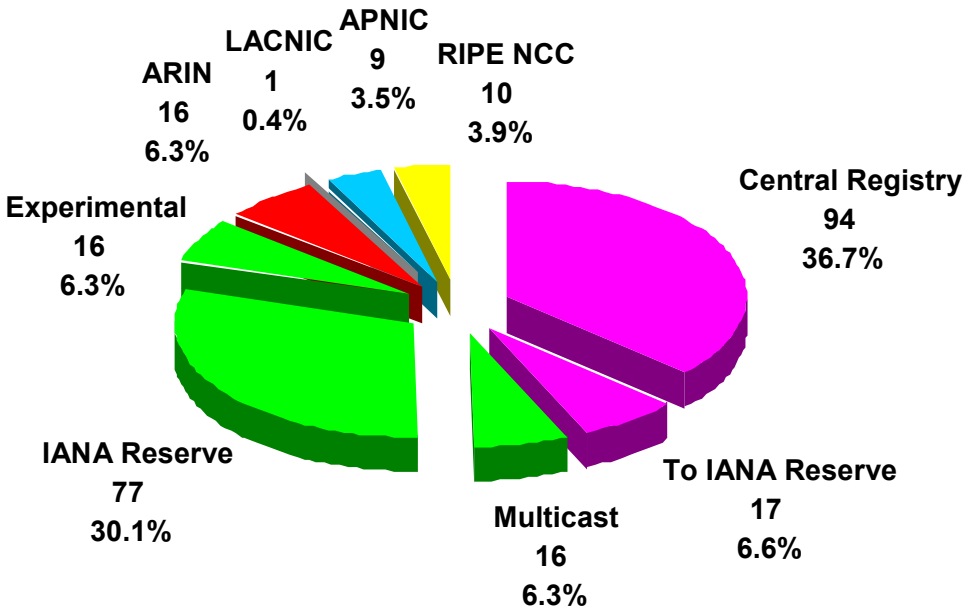
13 Availability of Internet addresses

There is much discussion about the prospect of shortages in IPv4 addresses and the need for IPv6 to replace IPv4. Concern is raised not only because of the growth of the Internet but the prospect of large-scale demand for IP addresses from mobile systems, despite the slow start to third generation systems.

Within Europe, the Commission is funding several pilot programmes based on IPv6. There is strong interest in the Far East, especially Japan. Overall the Far East seems to be the most advanced in terms of IPv6, Europe next and North America last.

IPv6 has a 128 bit address field, which is very much larger than the 32 bit field in IPv4, and therefore there should be no shortages in the availability of IPv6 addresses "forever".

Figure 17 shows the usage of IPv4 addresses in terms of the assignment of prefixes by the regional Internet registries (RIRs) as of early 2003.



Courtesy of RIPE NCC as presented to ITU-T Study Group 2 in May 2003.

Figure 17 – IPv4 assignments by 2003

Assignments are dominated by the profligate pre-RIR assignments to many entities (mostly United States) who do not need such large assignments (shown as "central registry"). This was done in good faith before the Internet reached the phase of rapid growth. All the main growth has been accommodated by the 14% assigned via the RIRs, which is not yet fully used up. Thirty-six per cent remains unassigned and will be assigned according to need by the RIRs who have adopted very strict criteria for assignment. A simplistic calculation would suggest that there could be capacity for 10-20 years of growth left, with more if steps were taken to recover some space form the pre-RIR assignments. The pessimists for IPv4 foresee rapid growth in areas such as China that will lead to much earlier exhaustion and the IPv6 Forum suggests that problems will start at some time within the next 5 years.

The other concern is that the growth of third generation mobile with many new data applications will lead to earlier exhaustion. This is a problem that many mobile operators would perhaps welcome in the current climate, and it may be a factor in the longer run.

The other drivers for a migration from IPv4 to IPv6 include improved functionality. Unfortunately the advantages are not yet adequately developed to become real commercial drivers to start the migration.

The migration from IPv4 to IPv6 will be complex and organizations will need to retain public IPv4 addresses to maintain IPv4 connectivity for a long time after starting to use an overlay of IPv6. Thus careful and adequate preparation will eventually be necessary. At this stage governments will need to ensure that users are fully aware of the issues.

Recommendation – 3

WG NNA should keep an active watch on the development of IPv6 and the usage of IPv4 addresses.

Recommendation – 4

WG NNA should study the issues that will be involved in migrating from IPv4 to IPv6, preferably through a case study.

14 Organization of the E.164 scheme and number assignment

14.1 The unstable service environment and growth in demand

Names and numbers are an essential part of the description of a telecommunication service because the type of identifier used delineates the set of parties that can be communicated with. In the past there were relatively few services and each service was well standardized through ITU-T or ETSI. Innovation in services is growing, but it is growing to a large extent outside the traditional standardization bodies, so a common and coherent approach is being replaced by a more fragmented and rapidly changing one. Thus the whole services environment is becoming less stable.

14.2 The structure of the E.164 scheme

The E.164 scheme is structured in terms of:

- Service (fixed, mobile, paging)
- Geographical location (country codes and regions within countries)
- Tariff (separate number ranges for different tariff types such as freephone, premium rate).

If users have a requirement to use E.164 numbers in connection with more than one type of service, then the assignment of number ranges to specific services will begin to lose its meaning and the structure will need to be reorganized to be more open and less service-specific.

The use of different ranges of numbers for services with different tariffs is quite important to users. With the falling costs of basic communications and the prospective growth in flat-rate tariffs on one hand, and the growth of sophisticated premium-rate services on the other hand, the polarization between low-cost calls and high-cost calls will grow and has to be taken adequately into account in the future development of E.164.

Providers of services on the Internet are starting to ask for assignments of E.164 numbers. For example providers of Internet telephony gateways would like E.164 numbers to assign to their subscribers so that incoming calls from the PSTN can be directed to subscribers through their gateways, and so that their subscribers can present a usable CLI when making outgoing calls to the PSTN. Guidance needs to be prepared for NRAs over the assignment of number ranges for these applications.

Recommendation – 5

WG NNA should develop guidelines to help NRAs handle the wide variety of applications for the use of E.164 numbers for voice communications over IP technology including the Internet.

14.3 Multiservice use for numbers

The multiplication of services could lead to a multiplication of different identifiers for users. This is not user-friendly and users would prefer to have fewer identifiers with each identifier being used for multiple services. The use of numbers for multiple services will break the uniqueness of the linkage between a number and a service provider. This will not matter if numbers such as personal numbers are used since these numbers are designed to be mapped to various different services and have no linkage to a specific service, but it is likely to cause problems if numbers that are linked to one service also begin to be used for another service.

Existing arrangements to facilitate the portability of E.164 numbers may need to be reviewed or re-shaped in order to encompass the following developments:

- the supply of services in connection with a single E.164 number by more than one service provider; and
- the supply of voice over IP applications by providers who are not based in the country in which the service is supplied, and who may benefit from the ability to access number portability databases in order to route calls sufficiently.

Recommendation – 6

WG NNA should study in more depth the use of numbers for multiple different services and produce guidance on the problems that can arise and how they can be avoided.

14.4 Loss on information from numbers

If E.164 numbers will be used in connection with Internet-based applications, it is likely that these applications could be supplied from and to anywhere in world (e.g. voice applications where an end user can log in from any location).

Such developments are likely to eliminate the association that exists in many countries between a particular series of numbers and a particular geographic area. The association between a given number series and a particular geographic area is, today, important:

- because it may enable callers to predict the cost of a call where this cost is distance-dependent;
- because it enables networks to accurately bill for calls; and
- in respect of porting of numbers, in that geographic numbers may be capable of being ported only within a specified geographic area with which a number series is associated.

Consequently, alternative methods of predicting call cost and billing for calls may be necessary; however, with tariffs dropping and becoming less distance-dependent this may not be a major problem. Similarly, technical considerations that impose geographic restrictions on porting of numbers may need to be overcome or the regulations will need to be altered.

If E.164 numbers are used in connection with Internet-based applications that can be accessed anywhere in world, the use of the calling line identification associated with an end user's service for providing location information to public service answering points of emergency services (in the event of an emergency call) or to support location-based services (such as services that rely on origin-dependent routing) will no longer be workable. In practice it may be necessary to advise users to continue to use the traditional PSTN or mobile networks and not Internet-based services for

accessing the emergency services because these networks have established mechanisms for location information. In the longer term it may become necessary to consider introducing means to contact the emergency services over the Internet if traditional services become less universally available than they are now.

14.5 Increased demand for global numbers

The separation of service provision from network operation is enabling services providers to offer services from one location to users in many different countries. Where these service providers need numbers to assign to their subscribers, assignment would be simpler if they could be assigned numbers from a global range without explicit country identification.

Users are also becoming more mobile and demand for non-country specific numbers could grow especially if the downward trend in tariffs continues and "international" numbers are less commonly regarded as expensive.

14.6 Demand for uses beyond telecommunications

The E.164 numbering scheme has high value as a global system of numerical identifiers that transcends cultural and language differences.

Names are used not only for identifying the source and destination of communications but also for identifying user profiles and preferences. For example, E.164 numbers are used extensively in the customer support systems of the telcos and can act as the entry point to other information and systems, some of which will contain information that is subject to various privacy laws. This means that E.164 numbers are being used outside the narrow role of identifying communication end-points and so the management and planning of E.164 needs to take account of this wider role. Developments such as ENUM, Microsoft Passport and Liberty Alliance are starting to consider these issues.

It is possible that new demands will arise for using E.164 numbers as keys in databases for applications outside telecommunications.

14.7 Direct assignment

Direct assignment of E.164 numbers to end users is likely to become increasingly desirable, including direct assignment of geographic and mobile numbers, as a way of:

- giving end users greater control over E.164 numbers they are assigned that they wish to use for more than one type of service, or in connection with which they wish services to be supplied by more than one service provider; and
- making it easier for end users to demonstrate their rights to use the E.164 numbers that they are assigned (e.g. when arranging to create, modify or delete ENUM records for their numbers).

Other means of giving users greater control may also be possible.

15 Control of numbers and names and their use

15.1 Loss of integrity

There may be reduced control over how numbers and names are used and increased threats to the integrity of the E.164 numbering scheme. Examples of loss of integrity are:

- use of numbers for services for which they have not been assigned;
- adoption of numbers by users or operators who have not been assigned them formally.

One of the main potential problems is that "pseudo-E.164 numbers" will start to be used widely with people becoming dependent on them before compatibility problems with properly assigned E.164 numbers start to be noticed. At that point some numbers will need to be changed and this will cause disruption to operators and users. This situation is similar in many ways to the unauthorized use of radio frequencies.

There is concern amongst some telcos and regulators that, without proper controls, ENUM may provide scope for the creation of "pseudo E.164" numbers in the domain name space, e.g. use of the domain name 1.0.0.5.5.1.2.7.0.2.4.4.e164.arpa when the number +44 207 215 5001 is not assigned.

15.2 Rights of use of numbers and names

Where the same E.164 number is used in connection with more than one type of service (such as a voice over IP application or applications that are initiated via ENUM), then one service provider will need to be able to verify the right to use an E.164 number that may have been assigned by another service provider. This is to ensure that additional services are supplied in connection with an E.164 number only with the express authorization of the end user to which the number is assigned and to ensure the integrity of a (national) numbering scheme. Such verification will require a robust means of proving that a particular E.164 number is assigned to an end user.

There are comparable issues when services are ceased since mechanisms may be needed to release numbers when users cease to have any service running on them.

The introduction of internationalized Internet domain names will need to be managed in such a way that conflicts are not created between holders of internationalized Internet domain names and holders of closely-related domain names that already exist (e.g. genève.com and geneve.com).

15.3 Support of law enforcement

For law enforcement purposes, it is sometimes necessary to be able to trace a particular end user or a service used by that end user. Methods for achieving this in telco networks, which usually rely on the end user's E.164 number as a key, are well-established. This is not the case for Internet-based applications, for which a particular end user may be identifiable by a given Internet name or address but for which there may be no simple or inexpensive means of relating the name or address to the end-user or finding what Internet-based applications are used by that end user.

It may be necessary to establish requirements and methods for tracing end users by means of an Internet name or address and tracing an Internet-based application used by a particular end user.

16 User identities, directories and databases

16.1 User identities

With the deployment of the Internet and the liberalization of the telecommunication market, the number of telecommunication identities identifying a single user is increasing. It is quite common for a subscriber to have more than one telephone number, e-mail address or other communication identifiers.

Ideally users want as few telecommunication identities as possible. Users want also be able to keep their telecommunication identities as long as possible (number portability in a general sense) because of the cost of changing identities.

Various initiatives are under way both in the government-funded sector such as UCI and in the private sector such as Microsoft Passport and Liberty Alliance. These initiatives could develop rapidly and lead to market power issues, especially in the case of Microsoft.

Recommendation – 7

WG NNA should keep a close watching brief on the public and private sector developments for simplifying user identification.

16.2 Directory enquiry services

The Universal Service Directive Article 5 requires the provision of directory enquiry services:

1. *Member States shall ensure that:*
   - *(a) at least one comprehensive directory is available to end-users in a form approved by the relevant authority, whether printed or electronic, or both, and is updated on a regular basis, and at least once a year;*
   - *(b) at least one comprehensive telephone directory enquiry service is available to all end-users, including users of public pay telephones.*
2. *The directories in paragraph 1 shall comprise, subject to the provisions of Article 11 of Directive 97/66/EC, all subscribers of publicly available telephone services.*
3. *Member States shall ensure that the undertaking(s) providing the services referred to in paragraph 1 apply the principle of non-discrimination to the treatment of information that has been provided to them by other undertakings.*

This requirement, however, is intended to cover only the E.164 numbers for publicly available telephone services, i.e. PSTN/ISDN and mobile. The various addressing or naming schemes used today are not subject to the same legal obligations.

E.164: legal obligations apply to service providers which assign E.164 numbers to subscribers (obligations to hold a directory and to give third-party access to directory data).

E-mail addresses: no legal obligations apply, and there is no initiative on the part of the e-mail service providers.

IM-id: no legal obligations apply but IM service providers are encouraging users to publish their data in a proprietary directory (like "Search for Friends" pages on ICQ, Yahoo! Messenger, MSN Messenger, etc.).

Directory service providers are also trying to enhance their services by incorporating other telecommunication identifiers besides E.164 numbers, such as e-mail addresses, website addresses and more rarely IM-id. However, because of privacy issues (e.g. SMS or e-mail spamming, etc.), subscribers are more and more reluctant to publish such data in publicly available directories. For example, in most European countries the number of mobile telephony subscribers who have published their mobile phone number in the public directory today is insignificant. This is unlikely to change if the subscribers have no means to protect themselves against unsolicited communications (e.g. e-mails or SMS).

As E.164 numbers are going to become more and more "multiservice", a better design of directory services would be needed. In particular, it will be necessary to specify which services can be used for a particular E.164 number (for example voice telephony, fax, SMS, etc.) instead of having separate directories for each service. Directory service providers could benefit from ENUM to enhance their services and products in such a way.

Advanced customized directory services in combination with ENUM and various time manager applications could also help customers to set dynamically the means by which they want to be reached.

It has also to be noted that currently the lack of competition in the market of directory services is preventing innovative services from being developed. One of the problems here is that users are highly familiar with a single number for calling directory enquiries and the introduction of competition would mean separate numbers would need to be assigned to different directory enquiry providers and a proportion of users would object to these changes.

There may also be a problem of the availability of information that relates to newer services. Some service providers may not be willing to reveal the relevant information about their customers and increasing tension is likely between privacy regulation and the need for directories.

The Internet has good search facilities for finding information on webpages and the registries for top level domains provide some information about the owners of domain names, but there is no comprehensive directory for Internet names such as e-mail or SIP addresses.

Increased functionality in terminals such as address books that automatically store information on callers will go some way to making up for the lack of directories.

Recommendation – 8

WG NNA should keep a watching brief on the development of directories and if necessary study in greater depth the scope for competition in basic telephony-related directories and the possibility of developing more comprehensive directories for new services.

16.3 Databases

The directories considered above are directories for users. There may be requirements for databases for routing that necessarily include all numbers but are not accessible by the public; an example is a central database for number portability. Such requirements are likely to grow as the structure of telecommunications becomes more international and more networks cross international borders. The ENUM concept could be used for the design of such databases.

There is also a need to use databases to support wider functions such as the provision of emergency services and these services may become more sophisticated in future for example by using location information or by providing links to medical information.

Recommendation – 9

WG NNA should keep a watching brief on the development of databases for use by network operators and public support functions.

16.4 Multichannel issues

Both the DTN and the Internet separate the role of service provider from that of network operator. This creates the possibility for a given service to be accessed or used from various different types of network. Two examples of this possibility are:

- Messaging systems that may be accessible from:
  - Voice response systems
  - Internet webpages
  - E-mail
  - SMS
  - Fax
- Sound and video programme distribution via:
  - Terrestrial radio broadcasting
  - Satellite broadcasting
  - Cable.

They may use various means such as the Internet and dial-up for responses to interactive programmes.

The mobile operators are currently introducing a multimedia messaging service (MMS) that is also multichannel.

The use of multiple network types is known as "multichannel". Strictly speaking, a service that integrates content and adds value is using multiple communication services with the possibility of using multiple identifiers that need to be mapped together. The growth of multichannel services will lead to increasing issues of relating different names and addresses together and the possibility of introducing overall "meta" identifiers to which existing identifiers may be linked.

This is an area for further study and is closely related to ENUM, UCI and the other commercial initiatives such as Microsoft Passport and Liberty Alliance.

Recommendation – 10

WG NNA should study the development of multichannel access to services.

17 Conclusions and recommendations for further study

17.1 Main conclusions and their implications

1) The public Internet will become increasingly important for communications including real-time communications such as voice.

Implication: Adequate management of the naming and addressing resources on the Internet is needed to satisfy the various commercial and governmental requirements

2) The different economic models of the telcos (intelligent network with controlled usage and time based charging) and the Internet (dumb network with open usage and subscription-based charging) will increasingly compete with each other, and there is a possibility that basic communications will become a subscription-charged utility in the future. This means that the future development of the DTN based on the current telco commercial model is not guaranteed, creating an unprecedented degree of uncertainty in the market-place. Consequently the development of future services will become increasingly diverse and unpredictable.

Implication: Adequate address space is needed to allow a variety of approaches to networks to be tried in the market-place even though some may fail.

3) E.164 numbers will be used in three ways for services that are provided over IP:

- Migration of telco services with E.164 numbers to IP
- New telco services on IP that will require E.164 numbers
- New services on the Internet that will require E.164 numbers

Implication: These developments will lead to increased demand for E.164 numbers and increased diversity in the services that they are used for.

4) Whereas in the past new services were developed cooperatively by the telcos through standardization bodies such as ITU-T and ETSI, service development through these bodies for fixed networks has largely ceased, although it is continuing to some extent in the mobile area for third generation systems. Innovation in services is now focused on the Internet where services are created at the edge of the network and "terminal functionality" is provided through downloadable software. Service innovation is also fragmented with various companies developing similar but incompatible services such as Instant Messenger. The main area of growth at present is distributed customized applications.

Implication: Naming and numbering in the future will have to be able to support a much less stable service environment because they can no longer be related to well-defined services. This will in turn lead to a loss of the information that can be deduced from numbers such as service type, tariff level and location. Consequently there will be a need for more comprehensive directories and other sources of service-related information.

5) The availability of the Internet as a "dumb network" and the scope for creating and running services from outside the network is stimulating the development of intelligent software-based terminals that use general purpose hardware such as PCs and PDAs.

Implication: This will lead to reduced control over how numbers and names are used and increased threats to the integrity of the E.164 numbering scheme (i.e. use of numbers for services for which they have not been assigned, and the adoption of numbers without regard to the formal assignment processes).

6) There is growing user demand to make services more user-friendly especially as sophisticated telecommunications become a pervasive part of society and not just a tool for people who are better educated or interested in computing. These objectives are driving new initiatives to simplify identification and to reduce the number of identifiers that users have to handle.

Implication: There may be a need for better centralized directories and other support functions especially for information relating to new services in order to support greater user friendliness.

7) There is a strong trend towards the separation of network operation and service provision. This separation is already an integral part of the structure of the Internet but it is also being adopted by the telcos in their plans for DTNs. This separation of service provision is likely to result in services being provided from outside the country where they are used.

Implication: As above. There will also be problems in the loss of reliable geographic information, the control of services and the support of law enforcement, which relies heavily on numbers.

8) As networks become capable of supporting multiple different services there will be increasing pressure to use numbers for multiple services. This development will break the relationship between numbers and network operation and lead to requirements for a new approach to number assignment and personal numbering.

Implication: Numbers will become multiservice in the same way that Internet names are multiservice. This will create increased pressure for the individual/personal assignment of numbers and the need for adequate methods of validating people's rights to use a given number. It will also result in loss of information from numbers because the information normally relates to specific services.

9) Numbers are a very useful form of identifier especially for services that are potentially global and are used in a wide range of different cultures. Therefore there is likely to be increasing demand for E.164 numbers not only from both the telco and Internet-based communities, but also for purposes that go beyond communications.

Implication: The increased and diverse demands will put pressure on the structure of the E.164 scheme and it will become increasingly difficult to decide what range of numbers to use for new services. The demand for global numbers, i.e. numbers that are not country specific, will increase. Demand will develop to use E.164 numbers for purposes that are beyond telecommunications.

17.2 Recommendations

Recommendation – 1

CEPT as an independent organization should not become involved in the ongoing debate about government involvement in Internet naming and addressing. The issues are discussed in the Government Advisory Committee of ICANN and ITU, with the European position being prepared in the Internet Informal Group (IIG) convened by the Commission, and there is little point in attempting to duplicate the discussions within CEPT. However these arrangements do not provide scope for participation by all CEPT members who are not members of the EU and CEPT administrations could ask the Commission to expand the membership of the IIG[13].

Recommendation – 2

Each national government should take steps to ensure adequate coordination between the people responsible for managing E.164 numbers and those responsible for managing domain names, irrespective of the legal and organizational arrangements.

Recommendation – 3

WG NNA should keep an active watch on the development of IPv6 and the usage of IPv4 addresses.

Recommendation – 4

WG NNA should study the issues that will be involved in the introduction of IPv6, preferably through a case study.

Recommendation – 5

WG NNA should develop guidelines to help NRAs handle the wide variety of applications for the use of E.164 numbers for voice communications over IP technology including the Internet.

Recommendation – 6

WG NNA should study in more depth the use of numbers for multiple different services and produce guidance on the problems that can arise and how they can be avoided.

Recommendation – 7

WG NNA should keep a close watching brief on the public and private sector developments for simplifying user identification.

Recommendation - 8

WG NNA should keep a watching brief on the development of directories and if necessary study in greater depth the scope for competition in basic telephony-related directories and the possibility of developing more comprehensive directories for new services.

Recommendation – 9

WG NNA should keep a watching brief on the development of number databases for use by network operators and public support functions.

Recommendation – 10

WG NNA should study the numbering and naming aspects of multichannel access to services.

---

[13] Norway and Switzerland are allowed to participate as observers.

ANNEX A

ITU Resolution 102

INTERNATIONAL TELECOMMUNICATION UNION — STUDY GROUP 13

TELECOMMUNICATION STANDARDIZATION SECTOR — **TD 15 (PLEN)**

STUDY PERIOD 2001-2004 — English only

Question(s): All/13 — Geneva, 29 October – 8 November 2002

TEMPORARY DOCUMENT

Source: TSB

Title: **RESOLUTION 102 (Rev. Marrakesh, 2002)**
Management of Internet domain names and addresses

The Plenipotentiary Conference of the International Telecommunication Union (Marrakesh, 2002),

aware

that the purposes of the Union are, *inter alia,* to promote, at the international level, the adoption of a broad approach to the issues of telecommunications in the global information economy and society, to promote the extension of the benefits of new telecommunication technologies to all the world's inhabitants and to harmonize the efforts of Member States and Sector Members in the attainment of those ends,

considering

a) that advances in the global information infrastructure, including the development of Internet Protocol (IP)-based networks and especially the Internet, are of crucial importance as an important engine for growth in the world economy in the twenty-first century;

b) that the private sector is playing a very important role in the expansion and development of the Internet, for example through investments in infrastructures and services;

c) that the development of the Internet is essentially market-led and driven by private and government initiatives;

d) that the management of the registration and assignment of Internet domain names and addresses must fully reflect the geographical and functional nature of the Internet, taking into account an equitable balance of interests of all stakeholders;

e) that Internet domain names and addresses, and more generally the Internet and global information networks, must be widely accessible to all citizens without regard to gender, race, religion or country of residence;

f) that the methods of assignment of Internet domain names and addresses should not privilege any country or region of the world to the detriment of others;

g) that the management of the Internet is a subject of valid international interest and must flow from full international cooperation;

h) that the expanding use of the Internet is expected to lead to the need for an increased capacity of IP addresses;

i) that Member States represent the interests of the population of the country or territory for which a country code top-level domain (ccTLD) has been delegated;

j) that Member States should play an active role in coordinating the resolution of management and administrative constraints arising with respect to their ccTLDs,

recognizing

a) that ITU is dealing with issues related to IP-based networks in general and the Internet in particular;

b) that ITU performs worldwide coordination of a number of name and address assignment systems and acts as a forum for policy discussion in this area;

c) that ITU can play a positive role by offering a platform for encouraging discussions, and for the dissemination of information, particularly to developing country governments, on the management of Internet domain names and addresses;

d) that through international cooperation, ITU should contribute to policy development related to the management of Internet domain names and addresses,

emphasizing

a) that the management of Internet domain names and addresses includes:

– technical and coordination tasks, for which technical private bodies can be responsible, and;

– public interest matters (for example, stability, security, freedom of use, protection of individual rights, sovereignty, competition rules and equal access for all), for which governments or intergovernmental organizations are responsible and to which qualified international organizations contribute;

b) that the methods of assignment of global and essential resources such as Internet domain names and addresses are of interest to both governments and the private sector;

c) that the role of governments is to provide a clear, consistent and predictable legal framework, to promote a favourable environment in which global information networks are interoperable and widely accessible to all citizens, and to ensure adequate protection of public interests in the management of Internet domain names and addresses;

d) that it is in the public interest that the system that manages Internet domain names and addresses has transparent rules and procedures, including dispute resolution procedures to facilitate the protection of intellectual property rights;

e) that governments are expected to promote, as appropriate, a fair competitive environment among companies or organizations responsible for Internet resource allocation,

resolves to instruct the Secretary-General

1 to take a significant role in international discussions and initiatives on the management of Internet domain names and addresses, taking into account associated developments and the purposes of the Union;

2 to encourage all Member States to participate in the discussions on international management of Internet domain names and addresses, so that worldwide representation in the debates can be ensured;

3 to liaise and to cooperate, in conjunction with the Bureaux, with the regional telecommunication organizations pursuant to this resolution;

4 to provide assistance, in conjunction with the Bureaux, to Member States, if so requested, in order to achieve their stated policy objectives with respect to the management of Internet domain names and addresses;

5 to report annually to the Council on the activities undertaken on this subject,

instructs the Director of the Telecommunication Standardization Bureau

1 to continue to liaise and to cooperate with appropriate entities on relevant Internet domain name and address management issues, such as the transition to IP Version 6 (IPv6), ENUM, and internationalized domain names (IDN);

2 to work with Member States and Sector Members, recognizing the activities of other appropriate entities, to review Member States' ccTLD and other related experiences;

3 to work with Member States and Sector Members, recognizing the activities of other appropriate entities, to develop a recommendation to clarify the management of the domain ".int";

4 to report annually to the Council on the activities undertaken on this subject,

instructs the Director of the Telecommunication Development Bureau

1 to organize international and regional forums, in conjunction with appropriate entities, for the period 2002-2006, to discuss policy, operational and technical issues on the Internet in general and the management of Internet domain names and addresses in particular for the benefit of Member States, especially for least developed countries;

2 to report annually to the Council on the activities undertaken on this subject,

instructs the Council

to take appropriate measures in order to contribute actively to international discussions and initiatives related to the management of Internet domain names and addresses,

invites Member States

1 to participate actively in the discussions on the management of Internet domain names and addresses and notably on progress being made in pursuit of their policy objectives;

2 to participate in and follow the policy, operational and technical developments of the management of Internet domain names and addresses;

3 to increase awareness at national level among all appropriate entities, and to encourage their participation in the management of Internet domain names and addresses.

ANNEX B

Principles for the Delegation and Administration of Country Code Top Level Domains

This is a formal text agreed in the ICANN Government Advisory Committee (GAC).

1 Preamble

In the five years since the issuance of RFC 1591, the Internet has evolved from a tool reserved for computer and networking research, to a global medium for commerce, education, and communication. The new realities of the Internet, including its increased importance as a vehicle for national economic growth, and the expanding and more diverse nature of the Internet community necessitated evolution in the traditional means of managing and administering Internet technical functions.

As a result, DNS functions, including the administration of the DNS root server system, the development of policies for the registration and allocation of domain names, the coordination of Internet Protocols, and the delegation of Internet Protocol numbers are becoming more clearly delineated and formalized through the ICANN process. Similarly, the procedures and framework of accountability for delegation and administration of ccTLDs need to evolve into a more robust, certain, and reliable system as well.

While evolution is needed, the principle of RFC 1591 remains sound: the manager of a ccTLD performs a public service on behalf of the relevant local community and as such the designated manager has a duty to serve this community. The designated manager also has a responsibility to the global Internet community. By "global Internet community" we do not mean any specific legal or international entity, but rather we interpret the term to refer to all of those who are affected by, now or in the future, the operation of the relevant TLD, because such operation may impinge on more than one jurisdiction and affect the interests of individuals and entities from both within the relevant country or territory and elsewhere. This is our interpretation of the meaning of ‘global Internet community' as it is used in RFC 1591.

2 Objective of this document

The objective of this document is to suggest principles that will assist in the development of best practice for the delegation and administration of ccTLDs. These principles are intended to contribute to the development of models of:

- a communication between the relevant government or public authority and ICANN;
- a communication between ICANN and the delegee; and
- a communication between the relevant government or public authority and the delegee.

3 Definitions

For the purposes of this document, the following definitions apply:

3.1 "Alternative Dispute Resolution" (or "ADR") means any system of resolving a dispute other than by court litigation, and includes arbitration, mediation, conciliation and processes of administrative dispute resolution.

3.2 "Communication" should include a law, regulation, agreement, document, contract, memorandum of understanding, or any other written instrument, as appropriate.

3.3 "Country code top level domain" or "ccTLD" means a domain in the top level of the global domain name system assigned according to the two-letter codes in the ISO 3166-1 standard, "Codes for the Representation of Names of Countries and Their Subdivisions."

3.4 "Delegation" means delegation by ICANN/IANA of responsibility for administration of a TLD in the DNS root.

3.5 "Delegee" means the organization, enterprise or individual designated by the relevant government or public authority to exercise the public trust function of a ccTLD and consequently recognized through a communication between ICANN and the designated entity for that purpose. The delegee for a ccTLD may be the relevant government or public authority itself or an oversight body designated by the relevant government or public authority, inasmuch as the administrative and management functions for a ccTLD may be contracted out by the delegee to another party and hence not performed by the delegee itself.

3.6 "Designation" means designation by the relevant government or public authority of the delegee.

3.7 "DNS" means domain name system.

3.8 "ICANN" means the Internet Corporation for Assigned Names and Numbers.

3.9 "Relevant government or public authority" means relevant national government or public authority of a distinct economy as recognized in international fora as those terms are used in the ICANN Bylaws and GAC Operating Principles.

3.10 "Relevant local community" means the local community in the context of the ISO 3166-1 code. This definition is specific to the purposes identified in this document and not broader.

3.11 "Top Level Domain" or "TLD" means a domain in the top level of the global domain name system.

4 Role of delegee

4.1 The delegee of a ccTLD is a trustee for the delegated domain, and has a duty to serve the residents of the relevant country or territory in the context of ISO 3166-1, as well as the global Internet community (as that term is interpreted in the Preamble to this document). Its policy role should be distinguished from the management, administration and marketing of the ccTLD. These functions may be performed by the same or different entities. However the delegation itself cannot be sub-contracted, sub-licensed or otherwise traded without the agreement of the relevant government or public authority and ICANN.

4.2 No private intellectual or other property rights should inhere in the ccTLD itself, nor accrue to the delegee as the result of delegation or to any entity as a result of the management, administration or marketing of the ccTLD.

4.3 Tradable goods and services may arise in the performance of other management and administrative functions attached to the ccTLD.

4.4 The delegee should recognize that ultimate public policy authority over the relevant ccTLD rests with the relevant government or public authority.

4.5 The delegee should work cooperatively with the relevant government or public authority of the country or territory for which the ccTLD has been established, within the framework and public policy objectives of such relevant government or public authority.

4.6 The delegee, and the delegee's administrative contact, should be resident or incorporated in the territory and/or jurisdiction of the relevant government or public authority. Where the delegee, administrative contact or technical contact are not resident or incorporated in the

territory and/or jurisdiction of the relevant government or public authority, it should nevertheless operate in a way that is consistent with the laws and public policy of that relevant government or public authority.

5 Role of government or public authority

5.1 The relevant government or public authority ultimately represents the interests of the people of the country or territory for which the ccTLD has been delegated. Accordingly, the role of the relevant government or public authority is to ensure that the ccTLD is being administered in the public interest, whilst taking into consideration issues of public policy and relevant law and regulation.

5.2 Governments or public authorities have responsibility for public policy objectives such as: transparency and non-discriminatory practices; greater choice, lower prices and better services for all categories of users; respect for personal privacy; and consumer protection issues. Considering their responsibility to protect these interests, governments or public authorities maintain ultimate policy authority over their respective ccTLDs and should ensure that they are operated in conformity with domestic public policy objectives, laws and regulations, and international law and applicable international conventions.

5.3 It is recalled that the Governmental Advisory Committee (GAC) to ICANN has previously adopted the general principle that the Internet naming system is a public resource in the sense that its functions must be administered in the public or common interest.

5.4 The relevant government or public authority should ensure that DNS registration in the ccTLD benefits from effective and fair condition of competition, at appropriate levels and scale of activity.

5.5 To give effect to governments' or public authorities' public policy interests, governments or public authorities should ensure that the terms outlined in Clause 9 are included in their communications with delegees.

5.6 In making a designation for a delegee, the government or public authority should take into consideration the importance of long term stability in the administration and management of the ccTLD and in the DNS. In most cases, such stability may be best served through the designation of an organization or an enterprise rather than a specific individual.

6 Role of ICANN

6.1 A primary function of ICANN is to establish, disseminate, and oversee implementation of the technical standards and practices that relate to the operation of the global DNS. In this capacity, ICANN administers a range of technical Internet management functions, including:

- establishment of policy for IP number block allocation;
- administration of the authoritative root server system;
- creation of policy for determining the circumstances under which new TLDs would be added to the root system;
- coordination of the assignment of other Internet technical parameters as needed to maintain universal connectivity on the Internet; and
- other activities necessary to coordinate specified DNS administration functions.

6.2 Specifically in relation to the administration and operation of ccTLDs, ICANN's role is to develop and implement policies that fulfil the provisions of Clause 10 below.

7 Principles relating to delegations

7.1 Where a communication between the relevant government or public authority and the delegee is in place, when ICANN is notified by the relevant government or public authority that the delegee has contravened the terms of the communication, or the term of the designation has expired, ICANN should act with the utmost promptness to reassign the delegation in coordination with the relevant government or public authority.

7.2 Notwithstanding the urgent need for a communication-based regime for ccTLD designation, delegation and administration, in the absence of such communication between the relevant government or public authority and the administrator of the ccTLD, ICANN should, upon the tendering of evidence by such government or public authority that the administrator does not have the support of the relevant local community and of the relevant government or public authority, or has breached and failed to remedy other material provisions of RFC 1591, act with the utmost promptness to reassign the delegation in coordination with the relevant government or public authority.

7.3 When ICANN notifies the relevant government or public authority that the ccTLD is being operated in a manner that threatens the stability of the DNS or of the Internet, or has otherwise breached and failed to remedy other material provisions of the communication between ICANN and the delegee, as outlined in Clause 10, the relevant government or public authority should cooperate with ICANN to remedy this situation or effect the reassignment of the delegation for the ccTLD.

7.4 With respect to future delegations or reassignment of delegations, ICANN should delegate the administration of a ccTLD only to an organization, enterprise or individual that has been designated by the relevant government or public authority.

7.5 Delegees should enjoy, in the execution of their responsibilities, the appropriate rights under applicable law, and should not be subject to discriminatory or arbitrary practices, policies or procedures from ICANN or the relevant government or public authority. In the event of a reassignment of delegation, registrants in the ccTLD should be afforded continued name resolution, or a reasonable period in which to transfer to another TLD.

8 Principles concerning the communication between the relevant government or public authority and ICANN

8.1 The communication between the relevant government or public authority and ICANN, as outlined in Clause 2, should include a designated point of contact within the relevant government or public authority, as well as the name and contact details of the recognized delegee and duration of this recognition. Either as part of this communication, or through a subsequent communication, the relevant government or public authority should copy to ICANN any communication established between it and the delegee, setting forth the terms and conditions of the designation and/or concerning the execution of the delegee's role and the management of the delegation.

8.2 The relevant government or public authority should communicate to ICANN how it will require the delegee to abide by the terms and conditions outlined in Clause 9 below.

8.3 Recognizing ICANN's responsibilities to achieve consensus in the creation of any new generic TLDs, ICANN should avoid, in the creation of new generic TLDs, well known and famous country, territory or place names; well known and famous country, territory or regional language or people descriptions; or ISO 639 Codes for representation of languages unless in agreement with the relevant governments or public authorities.

9 Principles concerning the communication between the relevant government or public authority and the delegee

9.1 The communication between the relevant government or public authority and the delegee should include the following provisions, a copy or summary of which should be forwarded to ICANN:

9.1.1 Term, performance clauses, opportunity for review and process for revocation.

9.1.2 A commitment by the delegee to operate the ccTLD in the interest of the relevant local community and the global Internet community.

9.1.3 A recognition by the delegee that the management and administration of the ccTLD are subject to the ultimate authority of the relevant government or public authority, and must conform with relevant domestic laws and regulations, and international law and international conventions.

9.1.4 Confirmation that the ccTLD is operated in trust in the public interest and that the delegee does not acquire property rights to the ccTLD itself.

9.1.5 Conditions to ensure the transfer of all relevant DNS data to a nominated replacement, if, for any reason, a reassignment to a new delegee is necessary.

9.1.6 Conditions for the efficient and effective resolution of disputes arising from domain name registration. In so far as ccTLD registration policies allow or encourage registrations from entities or individuals resident outside the relevant territory, then the delegee concerned should implement dispute resolution policies that ensure that the interests of all registrants, and of third parties, including those outside their territory and in other jurisdictions, are taken into account. Dispute resolution policies should, to the greatest extent possible, follow common principles, including due regard for internationally recognized intellectual property, consumer protection and other relevant law, and be implemented by all delegees. The delegee should, so far as possible, implement alternative dispute resolution procedures conducted online, without precluding access to court litigation.

9.1.7 The delegee's commitment to abide by ICANN developed policies as set forth in Clause 10.

9.1.8 Where ccTLD registration policies allow or encourage registrations from entities or individuals resident outside the relevant territory, the delegee commits to observe all ICANN policies applicable to such ccTLDs, not otherwise provided for in Clause 10, except where the delegee is prohibited by law from, or instructed in writing by the relevant government or public authority to refrain from, implementing such other ICANN policies.

9.1.9 The above terms and conditions shall apply to delegees, including delegees who are resident and/or incorporated outside the territory of the relevant local community.

9.2 A delegee should not sub-contract part or all of the technical operations of the ccTLD registry without ensuring that the sub-contractor has the technical qualifications required by ICANN, and informing ICANN.

9.3 In any sub-contracting of the technical operations of the ccTLD registry or administrative and management functions of the ccTLD, the sub-contract must state that the delegation itself is an exercise of a public right, not an item of property, and cannot be reassigned to a new delegee except in accordance with the provisions of Clause 7.

10 Principles concerning the communication between icon and the delegee

10.1 The communication between ICANN and the delegee should contain ICANN's commitment to:

10.1.1 maintain, or cause to be maintained, a stable, secure, authoritative and publicly available database of relevant information for each ccTLD (see below);

10.1.2 ensure that authoritative and accurate root zone information is generated from such database and ensure that the root servers are operated in stable and secure manner;

10.1.3 maintain, or cause to be maintained, authoritative records and an audit trail regarding ccTLD delegations and records related to these delegations; and

10.1.4 inform the delegee in a timely manner of any changes to ICANN's contact information.

10.2 The communication between ICANN and the delegee should contain the delegee's commitment to:

10.2.1 cause to be operated and maintained in a stable and secure manner the authoritative primary and secondary nameservers for the ccTLD, adequate to resolve names within the ccTLD for users throughout the Internet, and any sub-domains over which they retain administrative authority, and ensure that the zone file and accurate and up-to-date registration data is continuously available to ICANN for purposes of verifying and ensuring the operational stability of the ccTLD only;

10.2.2 inform ICANN in a timely manner of any changes to the ccTLD's contact information held by ICANN;

10.2.3 ensure the safety and integrity of the registry database, including the establishment of a data escrow or mirror site policy for the registry data managed by the delegate. The escrow agent or mirror site should be mutually approved by the relevant government or public authority and the delegee and should not be under the control of the delegee;

10.2.4 ensure the transfer of all relevant DNS data to a nominated replacement, if, for any reason, a reassignment to a new delegee is necessary;

10.2.5 abide by ICANN developed policies concerning: interoperability of the ccTLD with other parts of the DNS and Internet; operational capabilities and performance of the ccTLD operator; and the obtaining and maintenance of, and public access to, accurate and up-to-date contact information for domain name registrants; and

10.2.6 ensure the payment of its contribution to ICANN's cost of operation in accordance with an equitable scale, based on ICANN's total funding requirements (including reserves), developed by ICANN on the basis of consensus.

Attachment 7

Internet domain names and addressing

Internet domain names and addressing

The Domain Name System (DNS) is a distributed hierarchical look-up service. It is used on the Internet to translate between domain names and Internet protocol (IP) addresses and other identifiers like telephone numbers, e-mail addresses, instant messenger identifiers, etc.

ENUM converts the domain names into different identifiers like e-mail addresses, WWW pages, telephone numbers, instant messenger identifiers.

The DNS service consists of DNS data, name servers, and a protocol used to retrieve data from the servers. Clients of the DNS can be applications such as web browsers or mail transfer agents and even other name servers. Simple text data base records called ***resource records*** are placed into millions of files called ***zones***. Zones are kept on ***authoritative*** *name servers* distributed around the Internet, which answer queries according to the DNS network protocols. In contrast, ***caching*** *servers* simply query the authoritative servers and cache any replies. Most servers are authoritative for some zones and perform a caching function for all other DNS information. The DNS software implementation known as Berkeley Internet Name Domain (BIND) is the most commonly used domain name server on the Internet.

To understand the DNS hierarchy, it is helpful to examine the structure of Internet host names (see Figure 1). The last portion of a host name, such as .int, in the case of the **WWW.ITU.INT** (the ITU's website), is the top level domain (TLD) to which a host belongs. There are currently a set of *generic* top level domains (gTLDs), such as .com, .net, and .org, as well as *country code* top level domains (ccTLDs), such as .be for Belgium, .cn for the People's Republic of China, .mx for Mexico, and .us for the United States. Other top level domains such as .int, .gov, .mil and .edu do not neatly fit into either of these classifications – they form a set of "chartered" gTLDs since they have registration entrance requirements. For example, only intergovernmental treaty organizations are allowed to currently register under the TLD .int. Additional gTLDs have been recently created. ICANN plans to add new "sponsored" gTLDs.

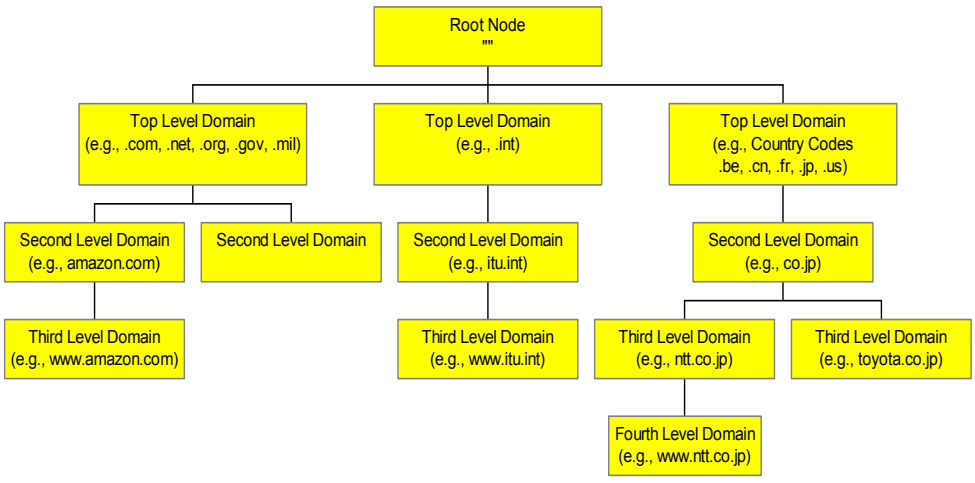


Figure 1 – DNS hierarchy

The root node of the Internet name space consists of a single file, the *root zone file*. The root zone file contains pointers to the master (primary) and slave (secondary) servers for all Internet top level domains (gTLDs and ccTLDs).

The master (primary) server is the *definitive* source of data for a DNS zone. This is where all changes to the zone's contents are made. The DNS protocol provides an automatic mechanism for propagating the contents of a zone to slave (secondary) servers. The provision of secondary servers provides robustness and prevents single points of failure. If one name server for a zone fails or is unreachable, there should be other name servers for the zone that can be queried instead. Usually a name server will only give up on an attempt to resolve a query when all the known servers for the zone have been tried and none respond.

At the top of the DNS database tree are 13 *root name servers* consisting of a primary server, "a.root-servers.net", and 12 secondary name servers. The location of the 13 root name servers is shown in Figure 2. Ten of these are in the United States, while the remaining three are located in Japan, Sweden and the United Kingdom.

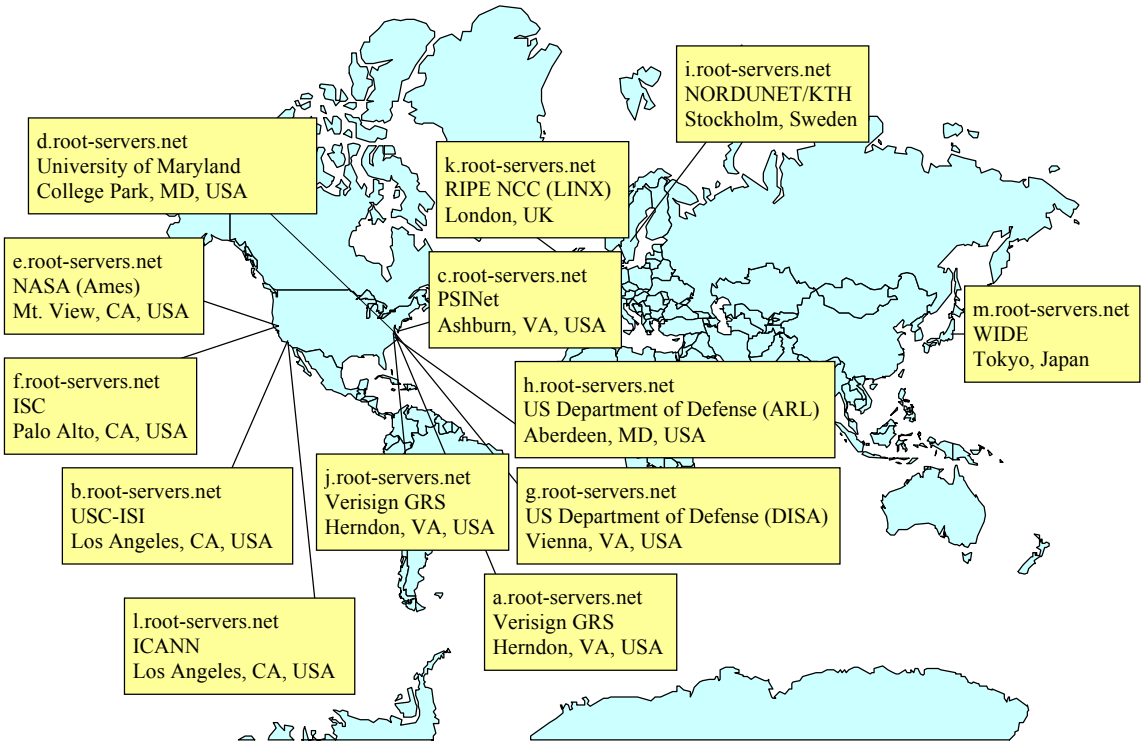


Figure 2 – Location of DNS root name servers

Currently, the primary root server, "a.root-servers.net", is maintained by Verisign Global Registry Services, a subsidiary of Verisign, Inc., located in the United States. The final authority for change control of the *root zone file* (e.g., addition or deletion of top level domains) is held by the United States Department of Commerce.

An example can be given of a DNS look-up to find the IP address of the ITU website: www.itu.int. When a server looks up www.itu.int, it will query the root name servers for a reference to the .int name servers. The local server then queries one of them for www.itu.int. A server for .int then returns a referral to the itu.int name servers. The server then repeats the query for www.itu.int a third time, this time to one of the itu.int name servers, which gives the final answer. This iterative process is known as *resolving*.

The answers a name server gets when it is resolving queries are *cached* and used to speed up subsequent look-ups. For example, if the name server that looked up www.itu.int was then asked to look up the mail server mail.itu.int, it would immediately query the itu.int name servers directly and not start resolving the query again from the root name servers.

There is often confusion about the difference between domains and zones. The difference between a domain and zone is subtle. A zone contains the domain names and data that a domain contains except for the domain names and data that are delegated elsewhere. Delegations means making someone else responsible for the subdomain. This delegation property is why DNS is often defined as a distributed database.

Attachment 8

IPv6

Table of contents

Page

IPv6

1 What is IPv6[1]

IPv6 (Internet protocol, version 6) was developed by the Internet Engineering Task Force (IETF), starting in 1993, in response to a series of perceived problems, primarily regarding exhaustion of the current, IP version 4 (IPv4) address space. It arose out of an evaluation and design process that began in 1990 and considered a number of options and a range of different protocol alternatives. The design process was essentially complete, and a protocol specified, in the first half of 1995, although refinement work continues[2]. The current version of the specification was published, after considerable implementation experience had been obtained, at the end of 1998[3]. Controversy continues to this day about some of the choices, but there are no proposals for alternatives that are complete enough for a determination to be made about whether or not they are realistic. The principal motivation for the new protocol was the address space issue on which the balance of this paper focuses. However, a number of other changes were made in formats and the interpretation of data fields. Those changes are intended to make the network operate better in the long term and to expand options for the design of efficient protocols, but their presence makes transition more complex than it would have been with address space expansion alone[4]. The driving motivation for IPv6 is to solve an address space exhaustion problem, but some communities have argued strongly that this problem does not exist or can be avoided by completely different approaches.

The remainder of this section contains a technical view of the policy issues.

2 The address space exhaustion problem: a history

2.1 Total address space, networks and classes

While one would prefer to make a given error only once and then learn from it, a few design errors have been repeated multiple times with what is now the Internet. Most of these have involved underestimating the rate or total scale of network growth. The original ARPANET design assumed

---

1 This material is based on a paper written by John Kleinsin, ITU-T Study Group 2 Information Document 15.

2 The history of the selection process, and its general conclusions, are described in Bradner, S., and A. Mankin, "The Recommendation for the IP Next Generation Protocol", RFC 1752, January 1995.

All "RFC" documents (the term originally referred to "request for comments" but has become simply the name for a publication series) are available online from a number of "mirror" locations. The official copies are located at ftp://ftp.rfc-editor.org/in-notes/rfcNNNN.txt, where NNNN is the RFC number.

3 Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

4 A different, but complementary, view of some of the technical issues and challenges discussed in this paper may be found in Carmès, E., "The Transition to IPv6", ISOC Member Briefing #6, Internet Society, January 2002. A more general discussion of issues facing the Internet as it becomes more critical to commerce and society, including sections that address some of the topics covered here, appears in Computer Science and Telecommunications Board (CSTB), National Research Council, *The Internet's Coming of Age*, Washington, DC, USA: National Academy Press, 2001.

that there would never be more than a large handful of hosts and, hence, that permitting a total of 255 hosts (an 8-bit host address space) would be more than adequate. When the TCP/IP architecture for the Internet was designed as a replacement in the first half of the 1970s, a 32-bit address space was then believed to be adequate for all time. Since the Internet – and TCP/IP – are designed around the notion of a "network of networks", rather than a single, seamless, network, that 32-bit address space was originally structured to permit a relatively small number of networks (roughly 256), with a large number of hosts (around 16 million) on each. It rapidly became clear that there would be a larger-than-anticipated number of networks, of varying sizes, and the architecture was changed to support three important "classes" of networks (there was a fourth class, but it is not relevant to this discussion): 128 Class A networks, each accommodating up to 16 777 215 hosts, 16 384 Class B networks, each accommodating up to 65 535 hosts, and around 4 million Class C networks, each accommodating up to 255 hosts. As one might have anticipated, Class C networks turned out to be too small for many enterprises, creating a heavy demand on Class B addresses, but those were larger than any but the very largest enterprises or networks needed.[5]

The distinction between networks and hosts on a network was, and remains, very important because Internet routing is closely tied to the separation of routing within a network and routing between networks. Using the division of an address into a network number and a host number, a given host can determine whether a packet is to be routed locally (on the same network), using some sort of "interior" protocol or whether it must be routed, typically through a gateway (although there are actually slight differences in meaning, the term "router" is often used interchangeably with "gateway" or, more precisely, "network-level gateway"), to another, "exterior" network. Exterior routing protocols use only information about networks; they pay no attention to what goes on inside a network.

This network-based approach has very significant limitations as far as utilization of the address space is concerned. As indicated above, one doesn't really have nearly 2^{31} (somewhat over $2 \cdot 10^9$) addresses with which to work. Any hierarchical addressing system would have similar problems with density of address usage. Different subdivision methods permit addresses to be used more or less densely, but no system for allocating network addresses can achieve perfect density. Instead, the entire Internet could accommodate a much smaller number of networks, the vast majority of them very small. Worse, because class boundaries were fixed, if a network contained up to 254 hosts, it could use a network of Class C addresses, but, when the number of hosts rose even by two or three more, it became necessary to either allocate an entire Class B address space, potentially tying up sixty thousand or more addresses that could not be used for other purposes, or to allocate multiple Class C networks. The latter could be problematic in designing local network topologies, but also threatened explosive routing table growth and routing complexity.

This design nonetheless appeared reasonable for the early Internet, since the network was built around the assumption of relatively large, time-sharing hosts, each with large numbers of users. If one thinks about an enterprise computing environment as consisting of a small number of

---

[5] For a more extensive discussion on this subject, and the evolution of "CIDR" addressing, see, for example, Chapter 9 of Huitema, Christian, *Routing on the Internet*, 2nd Ed. New Jersey: Prentice-Hall, 1999. The authoritative documents on CIDR are Fuller, V., T. Li, J. Yu, and K. Varadhan, "Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy", RFC 1519, September 1993 and Rekhter, Y. and C. Topolcic, "Exchanging Routing Information Across Provider Boundaries in the CIDR Environment", RFC 1520, September 1993.

mainframes, each with an address and with terminal devices attached to them that were not connected using Internet or Internet-like protocols, a Class C network with capacity for 254 hosts is likely to be more than adequate. Even if the norm were departmental computers, rather than centralized mainframes, and a few machines per department, only very few enterprises would anticipate more than 75 or 100 departments, and the class-based addressing system, primarily allocating from the large number of available Class Cs, still seemed reasonable.

2.2 Class-based addresses, large networks and subnetting

Another disadvantage of the "class"-based addressing system that became obvious fairly early was that some of the networks – all of the Class As and many of the Class Bs – became quite large and complex. Interior protocols that would work well for subsets of them would not work for the networks as a whole. Especially when the networks became very large (geographically or in number of hosts), one might actually wish for exterior-type protocols to route between components. This problem led, in the early 1980s, to the introduction of "subnetting". Subnetting essentially provides for using the two-level network/host model within a network, so that one could now divide larger networks up into smaller ones and treat each as a separate (internal) network. This approach was particularly useful for enterprises with networks spanning very large areas, since it permitted multiple gateways and internal routing arrangements. But subnetting, like the change to class-based addresses, was largely a response to routing issues – not enough networks in the first case and the need to subdivide networks in the second – rather than to concerns about address space exhaustion.

Despite these changes, it was generally assumed that any computer using TCP/IP, whether connected to the Internet or not, would be assigned a unique address. For connected machines, this was necessitated by the need to reach the machine and have it reach others (and more generally, by the "end-to-end principle", discussed below). For machines and networks that were not connected, the term "yet" seemed applicable: a long-term trend emerged in which systems were built that were never expected to be connected, only to have plans changed, resulting in a need to connect those networks. Renumbering was considered undesirable, less because of the problems associated with changing the address of a single host, than because of the need to simultaneously renumber all of the hosts on a network when it was connected: remember that a host handles packets bound for its own network somewhat differently than it does hosts that are on a different network or, more specifically, use a different network address. Thus renumbering is done in response to changes in routing, or typically requires routing adjustments.

2.3 The advent of the personal computer and other surprises

The appearance of small and inexpensive desktop computers changed all of this. Fairly quickly, the assumption that an enterprise or department would consist of a few large computers with attached terminals – with the terminals using a different protocol to communicate with the computers than the computers used to communicate with each other – evolved to a vision of networks as consisting of machines, interconnected with TCP/IP, and hence needing addresses whose numbers were roughly proportionate to the number of people, rather than the number of departments. Increasing modem speeds, combined with protocols that supported dial-up use of TcP/IP with adequate authentication and management facilities for commercial use, made dial-up networks and general home use of Internet connections plausible. As a result of this combination, Internet growth, spurred on by the introduction of the web and graphical interfaces to it, exploded. Several techniques were

developed to reduce the rate of address space consumption below the rate of "Internet growth" (measured by the number of computers that were ever connected). The most important of these were:

(1) Dynamic assignment of addresses to dial-up hosts, reducing the number of addresses toward the number of ports on dial-up access servers, rather than the number of machines that might be connected.

(ii) Increased use of "private" address space, i.e. the use of the same addresses in different locations on the assumption that the associated hosts would never be connected to the public Internet.[6]

These two approaches caused problems in edge cases, problems that presaged the requirement for a larger address space. Private address spaces required renumbering when the associated networks were connected (as anticipated some years earlier) and, worse, tended to "leak" into the public Internet when attempts were made to connect the network through gateways that translated the addresses. Dynamic addressing, with a given host acquiring a different address each time it was connected to the network, worked fine but essentially prevented use of those hosts in environments in which other hosts needed to contact them (i.e. in peer-to-peer set-ups or as servers with client-server protocols). Patchwork solutions were developed in response to these problems, but they were not comprehensive in practice, or they introduced new or different problems. Those solutions, however, evolved into the alternatives to IPv6 discussed below.

2.4 Giving up on classes: the introduction of CIDR

The final step in this sequence of changes to IPv4 addressing to better utilize the address space was the abandonment of the classes and their fixed boundaries, replacing them with a classless system – Classless Inter-Domain Routing (see note 5). CIDR permitted the use of a variable-length network portion in the address, so that the remaining address space could be used more efficiently than the class-boundary network sizes permitted. An enterprise or network that needed, say, 500 addresses, could be allocated a network block with capacity for 511 or 1 023 hosts, rather than requiring a full Class B network and "wasting" the remaining sixty-four thousand (or so) addresses. When very small networks became common a few years later, such as for home or small office networks using cable television or digital subscriber line (DSL or xDSL) connections, CIDR also permitted address allocations to be made in blocks considerably smaller than the original Class C (up to 255 host) ones.

At roughly the same time CIDR was proposed, the regional address registries adopted much more restrictive policies toward allocating space for those who requested it. The approval of CIDR reinforced this space-conserving trend, which some enterprises considered excessive at the time. Applicants were required to document plans for space utilization and to justify, in fairly specific

---

6 The problem with privately-chosen address spaces was that they "leaked", i.e. the addresses ended up appearing on the public Internet, where they conflicted with addresses privately chosen by others or with allocated and registered addresses. This resulted, in turn, in routing problems, some security risks, and, if nothing else, confusion. This "leakage" finally became a sufficiently large problem that IETF and the regional registries decided to dedicate several address ranges to private use and recommend that Internet routers block these addresses if they appeared in the public network. The specification and some discussion appear in Rekhter, Y., B. Moskowitz, D. Karrenberg, G. J. de Groot, E. Lear , "Address Allocation for Private Internets", RFC 1918, February 1996. But those private allocation spaces did not completely solve the problem, as discussed above.

terms, the amount of space they would need. The intent was not to prevent anyone from getting needed space, but to slow the rate of allocations and ensure that space was used as densely as possible.[7] As discussed below, it is reasonable to assume that policies for conserving IPv4 space will become more aggressive as the available space is consumed.

3 Relationship to topology

To properly understand the Internet's address space issues, it is probably useful to understand what the addressing system is and is not. In particular, an analogy is often drawn between Internet addresses and telephone numbers, leading to discussions of number portability and alternate number routing. That analogy is, in most respects, incorrect. Given its routing implications in a packet environment and binding to a particular interface on a particular machine, an Internet address can be more accurately compared to a circuit identifier in the public switched telephone network (PSTN) than to an (E.164) number. With some further adjustments because of the difference in character between circuit-switched and packet-switched networks, the Internet analogy to a PSTN telephone number is, for most purposes, more accurately a domain name. This point is fundamental, so bears repeating: an IP address is tied to routing information; it is not a name. A telephone number is a name and not a route. So a telephone number is more similar to a domain name than it is to an IP address.

3.1 Analogies to the PSTN

For many years, the primary mechanism in the PSTN for mapping from the names of people to telephone numbers (and thence to routing information and circuits) has been a "white pages" service, supplemented by operator services. Although there have been local exceptions, there has never been a successful global, or globally interoperable, "white pages" service for the Internet. That situation is largely due to the competitive and regulatory environments of telephony services, which are still largely national, with international service being an additional service, priced at a premium and negotiated between carriers or countries on a bilateral basis.

By contrast, Internet services have been largely international from inception. While prices differ from one locale to another, there is essentially no pricing difference between national and international services.

These differences have had a number of implications, one of which has been additional confusion about the role of Internet domain names vis-à-vis host addresses. The confusion has sometimes been increased by the fact that IP address formats and usability are independent of the physical media by which the associated hosts are connected to the network: they are not physical-layer addresses. The next section discusses some of the additional issues associated with these distinctions.

---

[7] While the overall intent was the same, the regional registries adopted somewhat different policies to accomplish this goal. The instructions to the registries on the subject were contained in Gerich, E., ed. (IAB), "Unique Addresses are Good", RFC 1814, June 1995. The high-level policies adopted appear in Hubbard, K, M. Kosters, D. Conrad, D. Karrenberg, J. Postel, "Internet Registry IP Allocation Guidelines", RFC 2050, November 1996. The current policies of the RIPE NCC are probably representative and are implicit in their address space request "tips" memo, currently at http://www.ripe.net/ripencc/tips/tips.html.

3.2 Telephone numbers and the Domain Name System (DNS)

The Internet's Domain Name System (DNS) and telephone numbers provide a certain amount of portability of reference. One can retain a name and have the underlying address (or circuit) change and can even, at least in principle, change transport mechanisms, e.g. from wireline to wireless, with the same number. But IPv6 introduces something of a new twist, since, with its deployment in the network, a DNS name may be associated with one or more IPv4 addresses, one or more IPv6 addresses, any combination of them, telephone numbers and other universal resource identifiers.

3.2.1 Circuit identifiers and addresses

As mentioned above, historically the closest analogy to an IP address in the PSTN is a circuit identifier. However the analogy is not exact: the IP address does not directly represent a physical-layer entity. In addition, IP addresses are potentially visible to users and user-level applications. By contrast, circuit identifiers are not only invisible to the user but would normally be of no value if obtained (e.g. one cannot place a telephone call using a circuit number). And both systems have evolved somewhat in recent years, yielding different models of what their practical lowest-level identifiers actually represent.

3.2.1.1 Fixed addresses in some networks

With dedicated, "permanent" IP attachments, as with conventional, wireline telephone systems, an address identifies a particular terminal or host and conveys a good deal of the information needed to access it. The information is not volatile: while it can change, the nature of changes is that they are typically scheduled to occur over relatively long periods of time, and can be planned for and adjustments made on a fairly leisurely basis. For the telephone system, this is true even when number portability is introduced – changes do not happen overnight and without warning. In the Internet case, such addresses are typically configured into the machine itself: a change in address requires reconfiguring the machine in, depending on the operating system, a more or less significant way. Renumbering such machines, whether within IPv4 or IPv6 space, or from an IPv4 address to an IPv6 one, involves often-significant per-machine costs. IPv6 installations are expected to put more reliance on dynamic (really centralized-server-based or serverless automatic configuration) allocation of addresses than has been typical in IPv4 networks, partially to reduce these problems (the facilities to do this were not available when IPv4 was deployed).

From a routing standpoint, these addresses are completely stable: their network portions can safely be used as routing information, if the network's location changes with regard to the topology, the address will normally change as well.

3.2.1.2 Long-time-frame variable addresses in other networks

Other types of addresses are more volatile and less predictable by the user, but still involve relatively long periods of stability. Internet address assignments that are dynamic in nature, but bound to particular equipment, tend to be much longer lived than those that are likely to differ over very short times and be linked to transient phenomena, such as dial-up attachments.

Dynamic host configuration protocol (DHCP) assignments using DSL or cable "modems" or hardware ("MAC") addresses typically have these properties. The addresses are usually stable for many months, but can be reassigned, over a fairly short period, by a change in the tables of the

supplying Internet service provider. However, unless those tables are linked to the DNS records for the user site, the change will need to be reported to the user and the DNS changes made to correspond. Problems often occur during the period between the address change and the DNS changes. Finally, it is usually undesirable for the provider to operate the DNS entries for their customers – normally a requirement if address changes are to be immediately reflected in the DNS – since it prevents the administrators of the local area network (LAN) managing their own name spaces.

From a routing standpoint, these addresses are the same as the fixed ones – routing table updates occur on a per-minute or per-hour basis (or less) and these addresses are very long-lived by comparison to the network's ability to reflect routing changes.

3.2.1.3 Short-time-frame variable

Other types of addresses actually are dynamic, even as the Internet measures time. A mobile telephone that is actually moving between locations requires routing information that is dependent on more than its address, or requires rapidly-changing addressing or a different form of addressing. For many purposes, dynamic address assignment for dial-up connections, in which each connection is likely to acquire a different address than the host had on the previous connection, raises similar problems. Of course, rapidly changing addresses also have advantages (a least as seen from some perspectives), e.g. they make usage more private and the user somewhat harder to trace.

IPv6 will make enough address space available to expand the options in these areas; with IPv4, optimality is, of necessity, usually defined in terms of address space conservation.

3.2.2 New technologies

Just as telephone numbers have evolved from a tight binding to a circuit to a number of portability ideas and then to wireless access, there are some notions about mobility and reuse of IP addresses and their use independent of their apparent routing properties. Each has some unfortunate side effects – a globally accessible mobile phone number can lead to calls at unfortunate times of day if one is in a time zone far removed from one's normal location and a caller doesn't know that, but can also be very helpful. With IP addresses, there are specific mobility techniques that are not relevant to this discussion and a mechanism, called "network address translation" (NAT) that permits the addresses used within a particular network to be different from the global, routable addresses by which that network and its hosts are addressed from the broader Internet.

This translation capability can serve several purposes. If the addresses on a network need to be renumbered owing to a change in connectivity (whether voluntary or imposed by a provider), address translation may permit the "new" addresses to appear externally while avoiding reconfiguration of the machines on the network (proper use of DHCP is almost always a better solution to this problem). If there is an address shortage, address translation and port remapping may be used to permit several hosts on a LAN to share a single globally accessible address, thereby helping to conserve global address space, but with some costs and tradeoffs.

NATs, and address translations more generally, are discussed more extensively in subsequent sections.

3.3 Reviewing the end-to-end model

The design of the Internet depends critically on what is known as the end-to-end architecture and the associated "hourglass model"[8]. The key principles that impact IPv6 considerations can be summarized as:

(i) From an addressing and protocol standpoint, any host on the Internet should be able to identify and access any other host through a uniform set of protocols and global addresses. Of course, security considerations may restrict what, if anything, can be done with that access, but the principle remains important.

(ii) The network itself is "dumb", that is, it is insensitive to the applications and protocols being run on it above the IP level. Changes are not required to the network to add new applications or terminal device capabilities.

(iii) By consequence, the terminal devices are assumed to be as "smart" and capable as needed to support the applications that users intend to run. Uniformity of terminal device capabilities around the network is not necessary or assumed.

(iv) The architecture of applications above the IP layer is dependent on that layer only; applications do not depend on, nor are they aware of, the physical media, interfaces or interconnection devices being used. Consequently, introducing a new medium, or new link-level, has no impact on applications.

(v) The network does not change the content or other properties of traffic flowing through it, i.e. it is transparent to that traffic.

This combination of characteristics is actually one of the key differences (other than the obvious "circuit" and "packet" designs) between the design of the Internet and that of the PSTN. The latter is built around an assumption of an extremely dumb terminal with almost no local capability. Those terminals are also assumed to be fairly uniform as far as the network is concerned – additional capability in the terminal does not permit more sophisticated signalling into the network. Of course, ISDN and mobile systems change this model somewhat – the computational, routing and interface capabilities of even 2.5G cellular devices considerably exceed that of a PSTN desk phone and are equivalent to some Internet devices – but, for the base PSTN, the characteristic remains.

Oversimplifying somewhat, pressures on address space and responses to them pose three serious challenges to this traditional Internet model. The introduction of NATs to conserve address space implies that there is no longer a global end-to-end model, but, instead, that there are isolated hosts and LANs that can be accessed only through intermediaries. IPv6 itself is a disruptive technology, since it changes the IP layer and, inevitably, interfaces to it in ways that do require altering

---

[8] A more extensive and excellent recent discussion on the hourglass architecture and its implications was presented by Steve Deering at IETF 51; the presentation can be found online at:

http://www.ietf.org/proceedings/01aug/slides/plenary-1/index.html. A slightly different version appears in *The Internet's Coming of Age* report, op. cit.

applications or application services. And most of the transition strategies for a network containing a mix of IPv4 and IPv6 systems imply that some hosts will require more complex arrangements to reach others than the simplicity that the end-to-end architecture contemplates[9].

3.4 The 32-bit address space and exhaustion

3.4.1 Predictions about when we run out

Since the beginning of the last decade, predicting the date on which the IPv4 address space will be exhausted has been a popular sport, with a variety of estimates deriving from different assumptions and calculations. Under the most pessimistic of those estimates, we would have run out of addresses already. Some people observe that address exhaustion has not occurred and infer that there is no risk of ever running out. Early in the process that developed IPv6, IETF's working group on the subject estimated address exhaustion between 2005 and 2011, and some people believe we are still on that schedule. Others see a longer lifetime for the IPv4 space (largely because of CIDR and NAT), and still others continue to predict that catastrophe is right around the corner.

More realistically, we should understand that any estimate of an exhaustion date is made on the assumption that neither major technology nor policy changes will occur or, at best, with only the most tentative estimates of the impact of such changes. Looking back, those early, most pessimistic estimates did not fully take account of some of the effects of CIDR, or of provider refusal to route small blocks[10], or of more restrictive regional registry allocation policies, or of heavy use of NAT and private addresses, each of which has had a significant impact on the rate at which addresses have been allocated and consumed. Although there have been some extensions to NAT to expand the range of situations in which the technique can be applied, there are no further major technical tricks in the IETF queue that would reduce address space pressure. Applications could come along that would dramatically increase it. And it is sensible to anticipate that the regional registries will apply increasingly restrictive allocation policies as the available remaining space shrinks.

---

9 *The Internet's Coming of Age* report, op. cit., discusses end-to-end transparency issues in more detail. Some of the issues remain controversial; the introduction of many types of functions into the core network to mediate different functions (performance, security, efficiency of access to selected materials, etc.) can be seen as threats to the model even in the absence of IPv6 or NAT concerns. See, e.g. Carpenter, B., "Internet Transparency", RFC 2775, February 2000 and Kaat, M., "Overview of 1999 IAB Network Layer Workshop", RFC 2956, October 2000. A summary of the challenges and an argument that it is time to rethink important aspects of the model appears in M. Blumenthal and D. Clark. Rethinking the design of the Internet: The end to end arguments vs. the brave new world. To appear in *ACM Trans. Internet Technology*. Also to appear in *Communications Policy in Transition: The Internet and Beyond*. B. Compaine and S. Greenstein, eds. MIT Press, Sept. 2001. See also the presentation by Deering, referenced immediately above.

10 After CIDR was introduced, a few ISPs adopted policies, to protect their own routing tables and those of the Internet more broadly, that restricted the routes they would accept from other ISPs to networks they considered large enough. The net effect of this was that very small networks ("long prefixes") could not be reliably routed across the entire Internet. Those policies, in turn, further increased pressure to aggregate addresses into larger, ISP-dependent blocks. But those policies were adopted spontaneously by specific ISPs and were never mandated by either the registries or IETF.

In addition, there are very large blocks of addresses tied up in Class A and Class B blocks allocated in the early days of the Internet. Organizations that hold those blocks have little or no incentive to renumber out of them, and are typically very sensitive to the considerable costs of doing so. But it appears fairly obvious that, at some point, if there is enough pressure on the address space, economics will shift sufficiently to force exactly that renumbering. For example, several of the "legacy" Class A address blocks are held by private universities in the United States. Those institutions tend to be fairly insensitive to low-level economic pressures, but are not insensitive to legislative or significant economic ones (in, e.g. units of buildings or long-term endowment)[11]. One can easily imagine consortia formed to make financial offers for address space or mounting pressure for legislation if available address space becomes limited enough to impede significant new commercial ventures.

3.4.2 Consequences and how soon?

True address space exhaustion – with no additional space available for new hosts or new applications – would be a nightmare of the worst sort and, effectively, the end of the Internet, at least as a growing entity, since the time to deploy new protocols or applications would be significant, at least unless a significant portion had been converted to IPv6 (or, in principle, some other strategy) already. However, the expectation of changes in technology and policy, predicted long-term difficulties if NATs must be nested to preserve space or if additional NAT-resistant applications or work styles are deployed, and economic or other changes that might free up space that is poorly utilized by today's standards makes it unrealistic to make policy decisions based on the date at which the address space will be exhausted. Instead, it is useful to examine more likely outcomes if an address space expansion strategy is not deployed and globally accessible addresses continue to be necessary:

(i) The regional registries gradually shift toward allocation policies that require ever-stronger justifications for additional space and, in a potential reversal from today's stated policies, require explanations and justifications of why private space cannot be used. Their allocations from IANA (ICANN)[12] also gradually tightened up, requiring the registries themselves to prepare stronger justifications for allocations of space from the remaining pools. It is likely that governmental or other pressures on ICANN could introduce distortions in the policies and allocations to the registries in the interests of some perception of fairness.

(ii) A serious and expensive market opens up to recover underutilized space from legacy allocations, primarily in Class A and B space. Some sites and ISPs discover that the "network real estate" they occupy in address space has a higher market value than their business (based on any reasonable capital valuation of the latter) and they, or at least their server functions, are forced off of the network. This is likely to lead to additional pressures for legislative intervention in allocation policy decisions, but such interventions can ultimately only influence the price structure associated with mandatory renumbering and reallocation, or can allocate scarcity, but cannot create more address space.

---

[11] Stanford University did voluntarily try to set an example: it renumbered out of its original Class A allocation and returned the space to the general Internet community, but that action has, so far, been unique.

[12] IANA, the Internet Assigned Numbers Authority, was the original registry for all Internet protocol identifiers and the top-level allocation source for addresses and domain names. When the IANA function was moved out of the Information Sciences Institute of the University of Southern California and privatized, it passed to ICANN, the Internet Corporation for Assigned Names and Numbers.

There are some further complexities associated with the notion of a market in address space, even in large blocks (small blocks can encounter the practical restrictions discussed in note 10). For example, as a security measure (one that has proven important in resisting attacks in the past), some ISPs will only accept address and routing announcements from sources that are registered with the appropriate registry as authorized to utilize that space. This implies that a transfer, if made between an address-holding party and a party that wishes to acquire the space, may be useless unless the registries agree to it. Proposed new security policies and protocol modifications would reinforce this trend. On the other hand, if the available IPv4 address space reaches the end game contemplated by this section, it is hard to imagine the registries being able to adopt and retain overly restrictive policies relative to approval of transfers that extend the useful life of the address space[13].

The best way to look at the net result of these dismal scenarios is that one does not want to be the organization or enterprise that requests the last block of available IPv4 space, or even any blocks of space after things become significantly tight.

4 Some proposed alternatives

4.1 Application gateways

Most of the plausible suggestions for continuing to use the IPv4 packet and addressing for an extended period, potentially indefinitely, depend on localizing addresses and then using the same addresses in multiple locations around the network.

The classical version of this approach involves placing one or more application servers at the boundary of a network, using public addresses for those servers. Those servers then accept all inbound traffic, convert it as necessary, and transfer it, as needed, to the "inside" network. With this approach, it is not necessary that the "inside" network be using the same addressing arrangements as the "outside" one and, indeed, it is not necessary that it be running TCP/IP at all. It is believed that the first instances of this approach were developed when protocol conversion – for the network protocols, the applications, or both – was required, e.g. when one network was operating with SNA (originally, "system network architecture", an IBM proprietary protocol suite whose original versions focused on access to mainframes) and the other with TCP/IP or when e-mail arrived using an Internet protocol such as the "simple mail transfer protocol", better known just as SMTP, and e-mail on the "inside" network used a proprietary protocol such as cc:mail® or MSMail®[14].

---

[13] A further policy complication may be worth noting. Some people in the Internet community have seriously proposed that criteria for allocating IPv4 space should be considerably relaxed, and relaxed immediately. They suggest that the current restrictive model is distorting Internet growth and retarding important developments (such as extensive use of attachments by small networks to more than one ISP and protocol and security strategies that require multiple addresses per host). A subset of them suggest that the side effect of a more relaxed allocation strategy – rapid exhaustion of the IPv4 address space – would actually be an advantage, because it would force rapid movement to IPv6.

[14] cc:mail and MSMail are registered trademarks of IBM and Microsoft Corporation, respectively.

This "application gateway" approach had (and has) a few disadvantages. For example:

(i) It was necessary to locate the conversion ("gateway") servers at the boundary of the "inside" network, rather than inside it. Under many circumstances, this caused security and operational problems.

(ii) While some applications and protocols, such as e-mail, lend themselves to a "receive, store, convert, forward" architecture, the approach is hostile to anything that requires real-time communication at the packet level.

(iii) Hosts on the "inside" were subject to the same restrictions as those on the "outside", i.e. they could communicate only via the application gateways, not directly.

(iv) Since the gateways needed to accept the application traffic, understand it, and potentially convert it to other formats, any application, or application option, that was not preprogrammed into the gateway could not be accepted or accessed at all. Hence, the presence of such gateways tends to create huge impediments to deploying new types of applications.

For situations in which the network technology on both sides of the boundary was TCP/IP, Network Address Translation ("NAT"s or "NAT boxes") was developed. NATs solved some of the problems with application gateways used alone, but not others.

NAT advocates also turned a few of these problems into virtues as the notion of security firewalls evolved. For example, if an "inside" network was invisible to an outside one, and could be accessed only in terms of specific, permitted protocols, that provided a certain amount of protection against malicious actions, especially if other protocols were involved.

4.2 NATs, VPNs and private spaces

NAT arrangements, or, more often, firewalls with address translation and tunnelling capabilities, have been used to design and build virtual private networks, with the tunnels used to interconnect LANs that share a private address space. Such networks have proven quite useful to many enterprises. However, inevitable changes in business relationships, mergers, and sometimes spin-offs, have resulted in a need to consolidate previously independent private address spaces. That, in turn, has forced sometimes-painful renumbering when the addresses used have overlapped. If the networks involved were using IPv6 rather than IPv4, the much greater address space available would permit use of public addresses (even if the sites were administratively blocked and could not be accessed from the public network) so that these conflicts would not arise.

4.3 Implications for innovation and expansion

There are a few major difficulties with NAT-based approaches, difficulties that may or may not be issues for a given network and configuration. To state the issue positively, if the entire network "behind" a NAT consists of machines that are used only as clients of other Internet services, and there is only one NAT between that network and the uniquely-addressed Internet core, it is unlikely that problems will be encountered. Indeed, arrangements of that type are used in thousands of locations today and are essentially required when, for example, a cable model or DSL provider refuses to provide more than one address to a subscriber who actually has a home network, or makes excessive charges for additional addresses. Even in those "client-only" set-ups, it can be somewhat more difficult to diagnose problems that occur, since the addresses "inside" the local network are not visible from other Internet locations, and do not correspond to external addresses. In practice, this has not been a significant problem for most NAT users, possibly because few ISPs provide useful diagnostic help for problems within user networks even when public addresses are used.

On the other hand, there are many ways to violate the "client-only, no nested NATs" assumption. Some of the more significant examples include:

(i) The assumption that machines within the user network only support client functions impedes the use of any type of server or peer-to-peer function of the inside network intended to be accessed from the outside one. The Internet was designed for what are today called peer-to-peer functions and some protocols, including the famous Napster music exchange one, depend heavily on peer-to-peer functions. Operation of a home website or external access to home control capabilities typically require server functions on the home network. Remote access to computers on the local network also depends on either peer-to-peer or server functions. As an important example, the two protocols that support the use of telephony-like voice over the Internet – the SIP[15] protocol and the Internet adaptation of H.323 – do not work through NATs unless the NATs are extended with special modifications for those protocols. Finally, it is difficult or impossible to predict future protocol evolution – a new protocol could easily arise that requires peer-to-peer or server functionality on networks that are now behind NATs, requiring operators of those networks to switch to non-NAT (public address) or more complex arrangements and producing a rapid increase in demand for public addresses.

Newer NAT architectures do provide for servers on the network behind the NAT by doing what is often called "port mapping". With this facility, the NAT box appears to be a single server to the external network and provides internal connections to support particular protocols, with each chosen protocol mapping to a single internal server. This approach is fairly satisfactory (although having servers on the internal LAN increases the need for external problem diagnosis mentioned above) but limits the LAN to a single server for a given protocol or requires complex internal proxy functions. For example, a LAN that requires a primary and backup mail server to ensure availability or performance is extremely difficult to configure with a NAT.

A few (non-standard) protocols operate by trying to hunt for a port on which to operate and will operate on any port that supports their services. Since a NAT must typically be configured for each port and protocol for which services are to be provided to the external Internet, use of NATs would potentially make such protocols almost impossible to use.

(ii) The user will typically have no control over NAT nesting functions. If the supplying ISP decides to create a NAT set-up rather than provide public addresses to any of its customers, then the port mapping of server functions in the local LANs may become essentially unusable since the external NAT would be required to designate a single internal address (NAT or otherwise) for each protocol to be supported.

(iii) IP-level security protocols, notably the specific one called "IPSec", require end-to-end addresses and do not function properly in NAT environments in which either or both end-point hosts use private addresses. Where appropriate, this problem can be circumvented by assuming that hosts on the local LAN are trusted and operating IPSec only between the network boundary and the remote host or network. However, this requires a somewhat more sophisticated NAT box than many of those now available, since it must establish its own security associations, and will not work satisfactorily in a nested NAT environment in which the "outer" NAT is not controlled or trusted by the owner of the protected LAN.

---

[15] The name "SIP" is derived from "Session Initiation Protocol", a term that no longer accurately reflects the uses or function of that protocol.

Of course, each of these disadvantages might be considered as advantages if the operator of the NAT wanted to prevent use of server functions, IP-based security, or unanticipated protocols on the local LAN[16].

It may also be worth stressing a point that is implicit in the comments above. When NATs are nested, or need to support server functions, or involve other situations similar to the examples above, they often become quite difficult to configure properly and maintain, even for experts. That cost should not be ignored or underestimated; for some organizations, it may be a primary motivator for considering an early transition to IPv6.

5 Network problems and IPv6

5.1 Solving the address space issue

The obvious solution to a shortage of available address space is more address space. That, of course, isn't the only solution – others (most discussed elsewhere in this document) include reducing pressures on the address space by becoming more selective about which resources actually need addresses and determining ways to reuse addresses in different parts of the network. Nonetheless, while it provides some other benefits, IPv6 is essentially a "larger address space" solution. If the growth of the Internet – or, more specifically, the unique-address-using Internet – were to stop tomorrow, IPv6 would probably be unnecessary[17].

5.2 The routing problem

Many people have asserted that the key capacity issue with the Internet is not a shortage of addresses, but growth of the routing tables, i.e. the information that non-default routers must have and process in order to route packets to their destinations. IPv6 does not address routing problems in any direct way. IPv6 is designed to permit easier renumbering of hosts and local networks to accommodate changes in topology, but there is a great deal of scepticism about whether those facilities are going to be significantly useful in practice. Debate continues, in IETF and elsewhere, about whether the DNS mechanisms designed to complement the renumbering facilities should be retained.

For the last several years, routing table growth has been dealt with by brute force: availability of processing capability and memory in routers has managed to keep up with table growth, which slowed considerably after CIDR was introduced, and slowed further when some key ISPs started refusing to route traffic for very small, independent networks across their backbones. There is some evidence that growth rates have increased again in the last year, probably due to increased use of

---

16 A more extensive treatment of the implications and risks of using NAT set-ups appears in Hain, T., ed. (IAB), "Architectural Implications of NAT", RFC 2993, November 2000. D. Senie discusses ways to design applications that work better with NATs than some others in "Network Address Translator (NAT)-Friendly Application Design Guidelines", RFC 3235, January 2002, but, of course, most LAN administrators and users have little control over the design of the applications they would like to operate.

17 "Probably" is, unfortunately, a necessary qualification here. As discussed above, some potential applications, features and styles of network design are incompatible with NAT arrangements. No one actually knows how many hosts are "hidden" behind NAT arrangements today. It is possible that an abrupt conversion of all of them to public address space in order to accommodate NAT-hostile applications or features would essentially exhaust the existing IPv4 address space.

"multihomed" connections (connections of a host, LAN or subnet to more than one provider). While less readily measurable than table sizes, the length of (clock) time needed to make complete routing computations (or, more precisely, to have those computations converge) has also been rising, threatening a situation in which routing changes arrive at a higher rate than can be accommodated[18].

IPv6 may help with the routing table problems simply by giving us an opportunity to organize the address space in a more optimal way (from a routing standpoint), without having to deal with more than a decade of legacy allocations that did not follow a scheme we would consider appropriate today (see the next section). Also, most new research and developments in the routing area assume the larger address space of IPv6 and the associated flexibilities; if we reach a point at which major changes in Internet routing algorithms are needed, those changes are much more likely to be practical in IPv6 than in IPv4.

Even with IPv6, some decisions about addressing and routing may have profound implications. For example, an ISP (or multiple-ISP consortium) with global reach might prefer to have either a single prefix and a fairly complex routing policy or multiple prefixes that reflect a more regional network organization. Even if the first decision were made, it is likely that it would want to allocate addresses within its network according to some topological structure so that interior routing could be easily optimized.

5.3 Provider-dependency in addressing and multihoming

The key to CIDR's role as a routing table conservation strategy is that, to the degree possible, blocks of addresses would be allocated to ISPs, which would then allocate sub-blocks of them to their customers. If this worked perfectly, a single address block could be used to represent any given major ISP. Any other site or network would need to know only how to route to that network. And, once traffic reached that ISP, it would know how to reach its customers. Those customers, who might be yet other ISPs, would draw address space from the large allocations made to their parent ISPs and would reassign parts of it to their own customers or organizational locations. Consequently, smaller sites, and even smaller ISPs, would not be permitted to obtain space directly from regional registries and would be required to obtain it from their upstream ISPs. This model could not work perfectly for a number of reasons, and created many (predictable) resentments. A change in providers would mean renumbering, since the addresses belonged to the providers. A site that wished to connect to multiple providers (so-called "multihoming") for additional robustness or efficiency would either require provider-independent address space or would need to somehow "punch holes" in the CIDR block of one provider or the other (with equal, or worse, damage to routing table compactness). And, of course, much of the address space was already allocated to sites and networks that had, as discussed below, little incentive to disrupt their networks and give up flexibility in the general interest of Internet efficiencies that they wouldn't experience directly.

IPv6 may permit some rationalization of this situation, both by providing a way to start over on address allocations (without the legacy effects) and by providing somewhat cleaner mechanisms for allocations and renumbering.

5.4 Security

One of the characteristics of IPv6 that was controversial when the protocol was approved was the requirement that all implementations provide support for end-to-end security (privacy and integrity) of the data stream. That provision recognized the fact that security provisions to prevent intermediate sites or networks from tampering with, or eavesdropping on, packets in transit are increasingly important in today's Internet and that such provisions become much more useful when

[18] For a more extensive discussion of these issues, see, among others, the references mentioned in footnote 5.

supported by all sites. But, while it guarantees that the facilities are available, IPv6 does not intrinsically provide more security than IPv4: the IP-layer security ("IPSec") tools proposed for IPv6 were modified and designed to support both IPv4 and IPv6[19], and considerable configuration and key management are needed to make the security provisions work effectively with either protocol stack[20]. Nonetheless, by reducing or eliminating the need for NAT, IPv6 should facilitate use and deployment of end-to-end IPv6.

6 Space allocation policy proposals

The question of how the registries should allocate IPv6 address space to those who request it remains an ongoing controversy, at least at the detail level[21]. Some points seem clear:

(i) Allocations will continue to be made to the regional registries and then further allocated to ISPs and larger (in terms of network requirements) enterprises and user organizations, as they are today with IPv4. This differs from the telephony model in which numbers are allocated on a national basis, but, as with the address system itself, reflects routing necessities. The regional registries themselves will develop the detailed allocation rules, as has been the case for IPv4[22].

(ii) If allocations are made on the same basis as they have been with IPv4, i.e. by requiring plans and justification for a very high density of use of the space requested, the perception will be that IPv6 space is as difficult to obtain as IPv4 space, even though it will last a good deal longer. Such scarcity will impede the development of applications and approaches that require multiple addresses per host, many small-scale ("ubiquitous") IP-connected and globally accessible computers, and other address-consuming applications.

(iii) If allocations are made on an "anyone gets whatever they ask for" basis, we could, within a reasonably short period, be facing the same address space exhaustion and routing table problems we have with IPv4. As mentioned elsewhere, one of the attractions of IPv6 is that it permits us to start the allocation process over and in a way that is consistent with longer-term and more rational planning.

(iv) Some allocation requests and proposals have been made on a basis that make no sense given the constraints imposed by routing of network addresses. For example, the Internet is not the PSTN, nor is it the connection-oriented OSI network represented by E.121 addresses. While the management advantages of consolidating such addresses are obvious, each set has routing implications in its own context. The number of countries in which Internet routing and connectivity to the outside exactly parallels that of the other networks is very small, if not zero; the number in which that situation not only prevails today but can be guaranteed to continue is even fewer.

---

[19] The base architecture for IPSec is described in Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[20] A similar situation applies with quality of service (QoS) capabilities: while the ability to accommodate them was important to the design of IPv6, the protocols that have been designed and standardized will operate in either IPv4 or IPv6 environments.

[21] The general principles that the registries are expected to follow are specified in IAB and IESG, "IAB/IESG Recommendations on IPv6 Address Allocations to Sites", RFC 3177, September 2001. Two of the three regional registries have accepted those recommendations, and discussion is in progress in the third. However, that document specifies the sizes of blocks to be allocated, rather than details about the criteria to be used to accept applications for the allocations – those criteria will still need to be established and interpreted by the registries.

[22] See notes 7 and 21 for additional discussion and references.

In summary, whatever strategies for IPv6 address allocation are considered or adopted, the relationship between the network portion of those addresses (the address "prefix") and the Internet's current and likely future routing architectures is such that allocations and address assignment must follow the routing topology and neither physical or political geography nor the topology of other telecommunication networks.

7 Deployment difficulties and models

Any process for conversion to IPv6 requires mechanisms for operating the network with a mixture of IPv4 and IPv6 hosts and subnetworks. This section describes three possible mixed-protocol network approaches and then discusses the models by which conversion may occur. While the issues identified here are important, and will continue to be important as long as IPv4 hosts remain attached to the network, it is useful to understand that native IPv6 operation is no longer an experiment: the "6bone" (an IPv6 network running on top of the IPv6 one) now reaches almost a thousand sites in 56 countries and native IPv6 connectivity was available at the IETF meeting in March 2002.

7.1 Communication in a mixed-network environment

There are three major models for operation of a network that involves both IPv4 and IPv6 protocols. Even the most optimistic of IPv6 proponents now believe that there will be some IPv4-only machines on the Internet for a very long time, so at least some of these scenarios are important both for conversion and for long-term operations.

7.1.1 Dual-stack environments

In a dual stack environment, both IPv4 and IPv6 capability is available on every machine. When a pair of machines is capable of communicating using IPv6 (as noted for a remote machine by the presence of IPv6 information in its DNS entry), they do so, perhaps tunnelling across intervening IPv4-only networks; when one or the other is not, they communicate using IPv4.

When IPv6 was originally defined, and the period of transition was expected to be shorter, the dual-stack model was assumed to be the primary transition mechanism. However, a transition based on dual-stack tends to assume an edge-first transition process (see below), while other techniques may be more useful if IPv4 machines and LANs are to be connected to IPv6 networks.

7.1.2 Tunnels

As with many other network technologies, it is possible to embed IP packets "inside" other IP packets, so that part of the network is aware of carrying only the "outside" packet, with encapsulation occurring at one boundary and unpacking occurring at another. This technique, called "tunnelling" in many of its applications, is often used for security (the "inside" packet may be encrypted to hide its content and source and destination information) or to support some mobility and rerouting strategies, but it can also be used to embed IPv6 packets inside IPv4 ones and vice versa. In particular, two hosts or networks that are utilizing IPv6 can communicate with each other across an IPv4 network if the routers or other devices at the boundaries between the two network types encapsulate outgoing IPv6 packets in IPv4 ones and the corresponding devices unpack and discard the IPv4 "wrappers", leaving the IPv6 ones at the far end. Conversely, a similar technique can be used to permit a pair of IPv4 networks to communicate across an IPv6 infrastructure (although there may be good alternatives for that case that do not require tunnelling).

7.1.3 Conversion gateways

Finally, one can actually convert packets from one format into the other. This can, of course, be done at the applications level, viewing the activity as a protocol conversion one, but techniques have been proposed for reversibly embedding IPv4 addresses and packet structure within IPv6 ones that do not require tunnelling. For the medium term, these techniques are probably the preferred ones, where feasible, for communication between IPv4 and IPv6 networks and end-points. However, they do present some of the same issues as described above for NATs, although typically for NATs with the same number of addresses on the "inside" and "outside" networks and more obvious address mappings. For example, they should be much less problematic for problem diagnosis (from either side) than a multiple-inside-address NAT.

7.2 Converting the network themselves

The techniques discussed above outline mechanisms by which IPv4 and IPv6 networks can work interoperably during a period in which the Internet contains some instances of each. From a policy and economic standpoint, perhaps a more interesting question is how IPv6 might actually be introduced on a large-scale basis. Two models were proposed early in IPv6 development: conversion occurring first from the edges and conversion from the core of the network (the backbone ISPs) outward. Both of these depend on "tipping" behaviour after some critical mass is achieved. Conversion from the edges of the network has historically been considered the more likely although some opinion has been shifting toward the alternative of conversion from the core of the network. A third model – adoption by large connectivity "islands" – has recently appeared and is the primary model of IPv6 introduction today.

7.2.1 Conversion at the edges

In the edge conversion model, individual enterprises or LANs decide to convert, perhaps because they are feeling the address space restrictions for one reason or another – the perceived difficulty of obtaining IPv4 addresses typically being a major factor - and see too many disadvantages associated with classical NAT set-ups. These types of conversions have occurred already, but have been limited by, among other factors, the lack of availability of production-quality IPv6 "stacks" in popular desktop operating systems. For many LANs, NAT-based technologies provide a clear alternative to this type of conversion, especially when combined with security approaches that include NAT-capable firewalls and "DMZ" strategies that are installed anyway.

Another edge-conversion option, which has not proven popular, involves running "dual stack" on both machines within the LAN and on the routers at its edges.

Until the bulk of the network, and especially provider-ISPs, converts to IPv6, operating a LAN with IPv6 requires either dual-stack or some type of address and protocol translation at the LAN boundaries to communicate with other sites. On the other hand, as more "edge" customers convert, the presumption is that they would pressure their ISP suppliers to offer IPv6 service – or would select ISPs on the basis of IPv6 service being available to avoid doing conversions themselves – and that the implied economic forces would gradually spread IPv6 across the network.

7.2.2 Conversion at the core

The core-based conversion model suggests that larger ISPs may tire of the costs and problems of operating IPv4, and using IPv4 addresses, on their core networks. They would switch those networks over to IPv6, tunnelling the IPv4 packets they receive from their customers. In this approach, it is reasonable to assume that those ISPs would notice that it was less expensive to offer IPv6 service to customers (over their IPv6 network), since they would not need to provide

conversion or tunnelling services, and that they would eventually reflect this in discounts to customers presenting and receiving IPv6 packets at their routers. They might also conclude it was in their interest to offer more attractive peering arrangements to other ISPs who were able to handle IPv6 traffic. As the cost differentials increased, customers would be motivated to convert.

The economic forces and the relatively small number of core/backbone/ "tier 1" ISPs probably make the tipping properties of core-based models better than those of edge-based ones.

7.2.3 Adoption by large "islands"

An additional model was not anticipated in the early guesses about conversion scenarios but may turn out to be a major driver of IPv6. If one is anticipating putting TCP/IP into a major new area – geographical, enterprise, or technological – for the first time, it may make sense to go to IPv6 initially, rather than installing IPv4 and having to undergo conversion costs. The decision to use IPv6 for 3G wireless and active work on it in China and Japan seem to reflect these "island" factors as well as assumptions about increasing difficulties (or costs) in obtaining large quantities of IPv4 address space.

8 Potential roadblocks and solutions

Many of the issues covered in this section have been discussed, in context, above, so it may be considered a review of key issues.

8.1 Economical

Conversion to IPv6 will not be either painless or inexpensive. Remaining with IPv4, especially where networks are expected to grow or new applications will be deployed, will not be painless or inexpensive either. Economic incentives to convert will occur if the costs of IPv4 connectivity rise significantly above those of IPv6 connectivity (most likely with the "core-first" model discussed earlier), if a conversion is forced by technical factors, or if the costs of obtaining required address space become excessive. The economic risk of delay is that, while differential connectivity costs are likely to rise slowly, if at all, the others drivers could occur with catastrophic suddenness, requiring a conversion with little planning time once the catastrophe becomes apparent. Such conversions are almost always significantly more expensive than those that can be planned well in advance and carried out on a convenient schedule.

As long as the alternatives to IPv6, including the use of NATs to avoid needing more IPv4 address space and the use of a combination of address translation and protocol conversion to continue use of IPv4 even after significant fractions of the network have converted, are acceptable, the temptation to avoid converting will be very high. On first analysis, waiting would seem to have no consequences, the IPv4 environment will be more familiar than the IPv6 one, and, for at least the near future, all applications will support IPv4 and some may not support IPv6. Viewed this way, one might reasonably avoid converting until forced to do so. On the other hand, especially if the network continues to grow (both locally and globally), conversion costs later will almost certainly exceed those of an early conversion.

Finally, as discussed above, large enterprises or countries that are considering getting on the Internet for the first time, or that are considering very high growth rates in the foreseeable future, may want to consider early adoption of IPv6. Doing so would avoid the costs of adopting and deploying an IPv4 system and then having to convert or upgrade it, either to move to IPv6 along with the rest of the world or to obtain additional address space after serious scarcity sets in.

8.2 Technical

There is no longer any major technical obstacle to conversions to IPv6. Despite this, it is important to note that vendors and users are still trapped in a deadly embrace: from the user standpoint, the obstacle to conversion is a lack of experience with vendor-supplied software and facilities to the degree needed to test, build pilot implementations, and make firm deployment plans. From the vendor standpoint, those facilities are not being implemented and deployed because there is no strong user demand for them. Similar problems occur from the standpoint of ISPs: customers who perceive themselves as unable to construct realistic pilot and test programmes do not place demands on their ISPs for native and optimized IPv6 services; the absence of ISPs aggressively offering IPv6 services persuades many potential customers that they should defer planning conversions.

Enterprises and organizations that do decide to convert do, fortunately, find that tunnelling systems to link to other IPv6 environments across the IPv4 backbones are readily available (and that there have been many years of experience with them) and that protocol conversion and address mapping gateways are readily available.

There are also some technical risks that impact the economic considerations. To give only two examples: if a network is using a NAT arrangement to avoid asking for additional IPv4 address space, and a new protocol is deployed (or an older one becomes of interest) that will not work behind a NAT, an immediate network reconfiguration may be required, either to accommodate at least some hosts "outside" the NAT arrangement, to obtain and install a larger IPv4 address pool, or to go to IPv6. If new protocols come along that are of interest and that are, for whatever reason, supported only under IPv6, the enterprise will be faced with a choice between IPv6 support and access to the capabilities of that protocol. And, finally, as operating systems, software vendors and router manufacturers shift to IPv6, history leads us to predict rising maintenance and support costs for IPv4 versions of their systems.

All of these factors suggest that, while there may or may not be advantages of being an early adopter of IPv6, once significant conversions begin one does not want to be the last, or even in the last group, to convert – at least to an environment that can successfully interwork with IPv6 and, more likely, to IPv6 itself.

8.3 Policy/political

With the exception of the "islands" discussed earlier, most of the policy issues associated with IPv6 track the economic and technical issues discussed in the previous two sections. The islands are an interesting technical and policy challenge: is it better to be ahead of much of the world on IPv6 adoption or to adopt a more conservative plan, presumably with the expectation of later conversion? And, if one takes a conservative approach, will sufficient IPv4 address space be available to permit fulfilling reasonable projections about required addresses? The latter consideration was presumably important in driving third-generation wireless planning toward IPv6; similar considerations would presumably apply to any other applications – systems requiring fairly large per-residence home networks with peer-to-peer capability would be one possible example – that could be predicted to require very large amounts of globally-accessible address space. Finally, there are important features of IPv6 that this document does not address[23]. If some of them become important to some future application, there will be an important question as to whether to implement that application less efficiently with IPv4 (assuming that is possible) or to implement it for IPv6 alone.

---

[23] See the RFCs cited in notes 2 and 3.

9 Summary: thinking about conversion

Available globally-addressable space on the IPv4 Internet is decreasing. It is difficult to measure the rate of decrease, and even one or two very large-scale applications that require global address space could exhaust most of the space that can be allocated without disruption to existing users and applications. Even an expansion of dedicated Internet connections in China or India to the density now seen in several Scandinavian countries, if done using IPv4, could substantially exhaust the remaining IPv4 address space.

This implies, in turn, that, in thinking about conversion, there are two conditions under which IPv6 can safely be ignored:

(i) One concludes that, despite network growth and the technical factors and risks associated with the Internet's running out of space or having to request an allocation after free space has become very rare, that an address space crisis will never occur or is sufficiently far in the future that one can safely ignore that possibility.

(ii) Another concludes that one's supplying ISP will not make a conversion to IPv6 and subsequently either discontinue IPv4 service or offer it only at a prohibitive price. One could, of course, reach this conclusion after negotiating a long-term agreement with that ISP or assuming that ISPs will always be available that offer IPv4 service (and, if necessary, conversion and translation services to reach remote systems that are IPv6-only).

If neither of those assumptions applies, then the important questions are not about whether to convert to IPv6, but how and when to make the conversion. For the enterprise or other LANs, the major choices of "how" are whether to continue with an IPv4 network and address translation and protocol conversion gateways or to move directly to IPv6 with either a dual-stack environment on individual machines or address translation/ protocol conversion gateway capability from IPv6 to IPv4. The "when" question is even more complicated. In general, it will be less disruptive to convert at one's own convenience, rather than being forced into it by inability to reach and communicate with critical customers or correspondents or by pressing external economic considerations (unacceptable costs of additional IPv4 space or high ISP prices for IPv4 services). Also in general, if one waits, software may become more stable and per-station conversion costs may decrease somewhat as experience accumulates. On the other hand, if the patterns of growth in the Internet and Internet usage within organizations continue, the number of stations will rise over time, probably enough to more than wipe out any per-station savings.

Attachment 9

Internet for everyone: IPv6 2005 Roadmap Recommendations

Table of contents

Internet for everyone: IPv6 2005 Roadmap Recommendations[1]

1 Executive summary

The emergence of the Internet as a fundamental technology for commercial and social activity has been recognized by the European Commission with the launch of the eEurope initiative. The Internet has grown rapidly in the past five years, to a scale well beyond that which the original Internet designers envisaged over twenty years ago. It is imperative that the European Internet should be able to grow to meet the future demands of commerce and society, for business, for learning, to enable new markets to be realized, and to enrich the lives of European citizens.

The Internet relies on a data communication method called the Internet protocol (IP) to transfer data between machines on the network, be that data webpages, e-mail, online gaming or otherwise. All Internet applications communicate using IP; it is the basic enabler of every service on the Internet; it is thus critical that IP be able to scale for the Internet of at least the next decade.

Future network growth requires that Internet-enabled devices can be assigned and use a globally unique IP address, in a similar way to the telephone numbers that identify individual phones. The current version of IP, IPv4, has been in existence for over twenty years, but has a limited address space, not even enough for one IP address per person on the planet. Its successor, IPv6, in development by IETF for eight years, offers relatively unlimited address space. The IPv6 core standards were completed in 1999, and vendors started shipping commercial IPv6 products in earnest in 2000. As a result a number of early IPv6 deployments already exist, notably in Japan.

The scarcity of IPv4 address space, for example for both commercial and home users, restricts the applications that can be run into both business and home networks. A technique known as network address translation (NAT) allows multiple devices to be "hidden" behind one or more real IPv4 addresses, but NAT breaks the end-to-end principle of the Internet, preventing the evolution of next generation applications that demand IP address space, and connectivity *into* business premises and home networks (e.g. from IP-enabled mobile handsets). IPv6 delivers that address space, and is thus a key factor for the well-being of the future European Internet.

The wireless Internet (3G) will most likely lead the IPv6 revolution, though IPv6 will also pervade further, into the home, the workplace, into cars and into consumer electronic devices. IPv4 has been in use for over twenty years, yet the worldwide web was not conceived until ten years after the introduction of IPv4. By deploying IPv6, new, innovative applications will be realized, some of which can be developed now, but many of which will follow in years to come, as eEurope evolves.

This report overviews IPv6, describing the features of IPv6 that will be key enablers for new applications and services. It describes the road forward for IPv6, including the requirement to integrate IPv4 and IPv6 services as the gradual overall transition to IPv6 occurs. There is no IPv6 "flag day" as there was for Y2K, but the earlier that IPv6 transition is begun, the less costly that transition will be in the long run, and the sooner IPv6's benefits can be exploited in eEurope.

IPv6 is the only solution that provides the vastly increased IP address space that will allow the European Internet to grow and to scale into the next decade and beyond. The base IPv6 protocols

[1] This material was provided by BDT.

are ready now, but deployment, which should be led by market forces, requires a number of factors to be addressed, as recommended by this report.

2 Introduction

At the dawn of the twenty-first century, information and communication technologies (ICT) are revolutionizing the functioning of the economy and society, and are triggering new ways of producing goods, trading and communicating. The further development of ICT into the twenty-first century, will have a wide-range and long-lasting impact not only on the economy, but also on every aspect of people's lives, leading to radical transformations and far-reaching changes. Indeed these changes are not just about technology, they are primarily about creating wealth and generating new business opportunities, sharing knowledge, bringing communities closer together and enriching everyone's lives.

2.1 IPv6 and the future Internet

According to population estimates from the United States Census Bureau, the world will be home to about 9 billion people in 2050. Whatever the economic constraints may be, we must clearly plan technically for all of these people to have the potential for Internet access. It would not be acceptable to produce a technology that simply could not scale to be accessible by the whole human population, under appropriate economic conditions. Furthermore, pervasive use of networked devices will probably mean we will see many devices per person, not just one.

2.2 Internet communication and addressing

To a user of the Internet, computers are addressed by their domain name, e.g. in the web context you would use *www.microsoft.com* as the web address of Microsoft, or *someone@aol.com* as the e-mail address of an AOL e-mail user. While such domain names are easier for people to remember, the networked devices – such as web servers, e-mail servers or home PCs – communicate using a numeric address format and a protocol called the Internet protocol (IP). As a loose analogy, domain names and IP addresses can be compared to people's names and their telephone numbers. The Internet Protocol requires that communicating devices, anywhere on the Internet, have unique IP addresses, so that data packets can be carried (routed) between the devices across one or more Internet service provider (ISP) networks.

The current version of IP, IPv4, has been in use for over twenty years, having been developed by Internet pioneers such as Vinton Cerf. However, when IPv4 was designed in the 1970s, the vast growth in the Internet was not foreseen, and at the time the web was still many years away from conception. As a result, and given the limitations of hardware at the time, the original Internet designers only chose to use 32 bits to represent IPv4 addresses. Those 32 bits allow 2^32, or just over 4 000 million, IPv4 addresses. While the Internet of the late 1970s contained only a handful of hosts, mainly in the United States, the Internet today has reached over 400 million regular users.

There are not, at present, enough IP addresses for every person on the planet. When one considers that homes, offices, cars and other environments may all contain many IP-enabled devices in the near future, the pressure on IPv4 address space is evident, given that any one device on the network may wish to connect to any other (e.g. a computer system at a car dealership may remotely check the status of IP-enabled sensors in a car, to monitor performance and predict future problems). That pressure is heightened because IP addresses are never fully utilized, either because allocations per ISP or per site were too generous in the 1980s (some organizations have been allocated what amounts to 1/256th of the whole IPv4 address space), or because allocations have to be made in blocks of sizes that are multiples of two (computers being binary devices); thus a site with 129 devices will have to be allocated 256 IP addresses.

IPv6, in development since the early to mid-1990s, has now matured to the state where vendors are delivering early commercial products (e.g. Sun, Cisco, Microsoft, Juniper) and initial deployments are being made. IPv6's major advantage is that it uses 128-bit addresses, enough to offer a globally unique IP address to any device wanting it for the foreseeable future. Given that all Internet communications use IP, the importance of the availability of IP address space for all cannot be stressed enough.

3 IPv6 address allocations

In Europe, the IPv6 production address space is managed and allocated to ISPs by RIPE NCC[2]. To date, over 100 IPv6 prefixes have been assigned to top level providers worldwide, with, of the three regional registries, Europe having the most prefixes assigned, followed by Asia and then the Americas. An IPv6 prefix represents a hierarchical, aggregated block of addresses for a network, in a similar way to a telephone area code aggregating all telephone numbers in a city area (only the computer network may be spread over any distance, e.g. where a network prefix is used by a national or even multinational organization).

The three regional registries – RIPE, APNIC and ARIN – share a common IPv6 address allocation policy. While this policy is subject to change, it currently offers a top-level provider (ISP) up to 35 bits of network address space (i.e. the equivalent of more than the whole current IPv4 address space for a single IPv6 provider), and a site receives 16 bits of network address space, which should be ample for the vast majority of organizations.

The availability of IPv6 address space should, through market forces, lead to IPv6 addresses being cheap (compared to IPv4) if not free to the end user. Many ADSL users currently pay a fee to have a single, static IPv4 address for their home network (typically GBP 10 per month). With IPv6, not only does a home network user get a whole network of IPv6 addresses (rather than just one IPv4 address), IP address scarcity is no longer a reason for an ISP to charge for providing static IP addresses.

The combination of the availability of multiple globally reachable IPv6 addresses for a home network, along with broadband access (e.g. ADSL), enables a whole new range of remote home management applications (e.g. multiple web cameras, or wireless temperature sensors) that are not feasible with IPv4.

4 The digital divide

Most significantly IPv6 can help bridge the digital divide that currently exists between the developed world (in particular the United States, where IPv4 address space was in good supply in the early years of the Internet) and emerging Internet nations in Eastern Europe, Latin America, Africa and Asia. IPv6 promises a level playing field for Internet protocol application development and deployment where IP addresses are readily available the world over, not a luxury for a privileged minority.

Bridging this divide is now a global objective. But the uneven dissemination of technology is nothing new. There have long been huge differences among countries. The bitter irony of the Internet phenomenon is that while in theory the global network of networks is open to all, the vast majority of the world's population remain cut off from its economic and educational benefits. Only 8% of the world population has access to the Internet, compared to 20% to the phone system.

---

2 http://www.ripe.net.

Affordable technologies more appropriate to developing economies could include solar-rechargeable batteries that would allow mobile phones to be used even in areas lacking electricity lines. The Internet could achieve a far better penetration through wireless access technologies, due to their dual benefit of being faster to deploy in any area (wide-scale cabling is not required) and of "giving wings" to the Internet with their mobility.

The PC era will be overtaken by the non-PC world (PDAs, smart cell phones, personal network devices, etc). The I-Mode advanced mobile data communication initiative in Japan achieved more than 30 million users in just two years of deployment and is perceived by its users as the Japanese Internet. Now, adding IPv6 to it would give the developing world immediate access to not only the Internet but to many next generation applications currently under development. If we fail to provide access to digital technology to countries in the developing world we are, essentially, denying them an opportunity to participate in the new economy of the twenty-first century.

5 IPv6 benefits

Viewed from a technical perspective, IPv6 has many benefits, including the following:

1) Larger address space for end-to-end global reachability and Internet scalability; this is the key advantage of IPv6.
2) Simplified IPv6 data packet header for routing efficiency and performance.
3) Support for routing and route aggregation, making Internet backbone routing more streamlined and efficient (the IPv4 Internet backbone contains data routing information for over 130 000 networks; with IPv6 this number could be dramatically reduced).
4) Serverless ("stateless") IP auto-configuration, easier network renumbering, and much improved plug and play support.
5) Security with mandatory implementation of IP Security (IPSec) support for all fully IPv6-compliant devices (IPSec implementation is not mandated in IPv4). Note that *use* of IPSec is not mandatory, but its presence for implementation allows the user to have the option of secure communications.
6) Improved support for mobile IP and mobile (and ad hoc) computing devices.
7) Enhanced multicast networking support.
8) These benefits can be mapped to opportunities for improved business models and potential new application and system markets.

6 IPv6 in Europe

The question of when to begin a migration path to IPv6 is an issue of paramount importance to a wide range of industries, which will be producing goods with embedded Internet access, including cars and consumer electronics, as well as to fixed, mobile and wireless communications. The Communication from the Commission at the Lisbon Council Meeting 2000 states that:

1) Member States should make a commitment to progressively introduce IPv6 in their publicly owned networks, i.e. those for research and administrations.
2) The Commission would increase support for test beds through its research, TEN Telecom and IDA programmes.
3) The Commission would invite Member States to work together with industry in an ad hoc group, which should provide proposals by the end of 2001 in order to accelerate the introduction of IPv6 (the results of that group are presented in this report and those of the four associated working groups).

Responding to the conclusions of the Stockholm Summit, the Commission stepped up its R&D efforts notably in the context of the 5th Framework Programme. A large number of IPv6 projects totalling some EUR 65 million of community funding is currently operational with others due to come up online shortly (most notably 6NET[3] and Euro6IX[4]). In its preparatory work for the 6th Framework Programme, further opportunities will be provided to the research community to conduct research on IPv6 and develop innovative tools, services and applications.

7 IPv6 deployment around the world

Japan took political leadership in the design of the roadmap to IPv6 when back on 21 September 2000 in the policy speech by Prime Minister Yoshiro Mori to the 150th Session of the Diet the Japanese Government mandated the incorporation of IPv6 and set a deadline of 2005 to upgrade existing systems in every business and public sector. Japan sees IPv6 as one of the ways of helping them leverage the Internet to rejuvenate the Japanese economy.

Large-scale deployment networks and vendor implementations have been widely promoted. The IP research community has been supported by government initiatives. The Japanese initiative was very crucial to the Asian regions. Korea followed suit on 22 February 2001 by announcing plans to roll out IPv6. China and Japan, in their 7th Japan-China regular bilateral consultation, have declared jointly the further promotion of Japan-China cooperation in infocommunication fields such as IPv6.

The business case for IPv6 in the United States is not yet felt, as the technical case is not that apparent, though most of the design of IPv6 and vendor implementations has been done in the United States. The United States was, of course, first in the "land rush" for IPv4 address space, so is not yet in as critical a position as Asia or parts of Europe.

However, IPv6 infrastructure can and is being deployed today in the market on intranets and at access points on the edge of the Internet, in particular in the Far East. Deployment is in the initial stage; users can use commercially supported vendor IPv6 implementations that began shipping in earnest in 2000. IPv6 implementations are available for many major router, server and client products. These can be used to begin the infrastructure deployment, and can interoperate with existing IPv4 infrastructure elements. Application developers can begin porting IPv4 applications to IPv6, and undertaking innovative new IPv6 ventures.

8 The IPv6 2005 Roadmap Recommendations

The European Commission, further to the conclusions of the Stockholm European Council, established an industrially led IPv6 Task Force, tasked with examining the current state of the development and deployment of IPv6 and recommending priority actions to be undertaken at European level. The report of the IPv6 Task Force now issued (http://www.ipv6-taskforce.org) puts forward a number of key recommendations addressed to Member States, the European Commission and industry at large. Beyond the overall requirement to structure, consolidate and integrate European efforts on IPv6, the report calls notably for:

1) Increased support towards IPv6 in public networks and services;

2) Launching of educational programmes on IPv6;

3) Promotion of IPv6 through awareness-raising campaigns;

4) Further stimulation of Internet across Europe;

---

3 The 6NET Project: http://www.6net.org/.

4 The Euro6IX Project: http://www.euro6ix.org/.

5) Creation of a stable and harmonized IPv6 policy environment;

6) Strengthening of IPv6 activities in the 6th Framework Programme of R&D;

7) Strengthening of support towards the IPv6 enabling of national and European research retworks;

8) Acceleration of contributions towards IPv6 standards work; and

9) Integration of IPv6 in all strategic plans concerning the use of new Internet services.

Given the necessity for a concerted and timely effort to enable the overall competitiveness of Europe to be strengthened in this strategically important area, the report of the IPv6 Task Force advocates that its recommendations be brought to the attention of the Spring European Council to take place in Barcelona, from 15 to 16 March 2002, with a view to setting the deployment roadmap to be achieved by 2005.

The recommendations set out below are aimed at the recognized:

- Standards development organizations (ITU, 3GPP/3GPP2, ETSI, IETF, IEEE-ISTO, etc.);
- Forums (3G.IP, ASP Consortium, DSL Forum, IMTC, IPv6 Forum, MPLS Forum, MSF, MWIF, OIF, OMG, SDL Forum, TM Forum, TOG, UMTS Forum, World Collaboration CPR, etc.); and
- Industry associations (EICTA, ETNO, EURESCOM, EUCONTROL, GSM Europe, ISP associations, White Goods Associations, etc.), coupled with an ITU-T initiative[5].

Recommendations

It is critical that all standards-related initiatives and activities be harmonized for the timely and efficient introduction of common, interoperable IPv6 deployments.

Consider opportunities for partnerships on IPv6 projects for:

- Joint development/collaborative work (within and outside Europe);
- Common standards;
- Education and knowledge exchange;
- Market intelligence;
- Marketing and promotion;
- Profiling and implementation agreements;
- Interoperability and conformance testing;
- Feedback from market and forums to standards development organizations for:
  - Requirements;
  - Finished standards; and
  - Gaps analysis.

For more information: Mr Latif Ladid, IPv6 Task Force Chairman,
E-mail: latif.ladid@village.uunet.lu, Tele. +352 30 71 35

5 ITU-T initiative: http://www.itu.int/ITU-T/tsb-director/forum/.

Attachment 10

Additional information on ccTLDs

Table of contents

Additional information on ccTLDs[1]

1 Guinea-Bissau: present situation of ccTLD

Recognizing the importance of communications for the economic development of Guinea-Bissau, during the 1980s the Government of Guinea-Bissau started the process to reform the communication sector. This reached its peak with the creation in 1989, through a concession, of a contract to Guinea Telecom for the exclusive right to manage and exploit telecommunication services including the Internet.

Aware of the strong growth of the Internet and the new opportunity it provides to the social, cultural and economic development of the country, and the need to extend its use to all social levels of the population, the Government, through Guinea Telecom (incumbent operator, in which Portugal Telecom International is the major stockholder), opened the Internet service in 1997 in Guinea-Bissau.

Because of the sector monopoly held by Guinea Telecom at the time, ccTLD management was automatically given to it. The intention was to develop the service for all, but the expectation was not realized and hitherto the service provided has not been optimum.

Since inauguration of the Internet service up to the present date, Guinea Telecom has had only one server registered, providing only e-mail and Internet services. Guinea Telecom manages the ccTLD but does not provide the services related to it.

At present we are concerned by this situation and are trying to redeem this right held by Guinea Telecom in order to organize ccTLD management. Accordingly, the Government, in the pursuit of its goal to reform the sector, adopted a declaration of telecommunication sector policy wherein it expresses its firm decision to liberalize the sector. The legal framework definition is adapted to the existing global, regional and subregional context with the adoption in 1999 of the Basic Telecommunication Law creating the regulatory body, the Institute of Communications of Guinea-Bissau (ICGB), with the following attributes:

- To collaborate actively in defining telecommunication policy in Guinea-Bissau;
- To advise the Government in the exercise of its guardianship functions; and
- To exploit radio-frequency spectrum, numbering and other resources.

In view of the new legal perspective in the country and having regard to the constant growth in the number of users in the local Internet community, and considering the vital importance of this service in the context of globalization; considering also that the ccTLD is a strategic resource of public interest, and is therefore related to national sovereignty; the Government expressed its intention to redeem the ccTLD ".gw" with the objective of realizing its new global management.

Since its creation in 1999, ICGB has been collecting information about the redemption process for the management of the ccTLD, but unfortunately without success. This nevertheless remains a primary objective for us.

---

1 This material was provided by BDT.

2 Switzerland

2.1 Introduction

Over the past few years the Internet has become an essential factor in the economy, particularly through the development of electronic commerce and the information society more generally. As a result, the importance of domain names has greatly increased. For this reason, the Swiss Government (Federal Council) decided that it was necessary to create a formal legal framework for the registration of domain names in the ".ch" zone. A regulation on the subject was adopted with the Decree concerning Addressing Resources in the Telecommunications Sector (ORAT). This new regulation came into force on 1 April 2002.

The SWITCH foundation, responsible for the operation of the Swiss academic network, has taken an interest in the worldwide development of the Internet from its earliest days. At a time when Switzerland was without any legal framework for administering addressing resources, the foundation set up a technical and administrative organization for business and private users to register ".ch" domain names.

In the course of the preparations that led to formalization of the process of delegation of ".ch" domain names, consideration was given to the question whether the domain name registration market should be opened to organizations other than SWITCH. It was felt that consumers should have full freedom to choose from a diversified range of services, and service providers should be put in a position to supply a combination of services.

The Federal Office for Communications (OFCOM), the oversight authority for telecommunication in Switzerland, accordingly drew up a draft regulation for Internet domain names for the ".ch" zone, in which a partly distributed model was proposed under which service providers would compete to make those allocations (registry-registrar model). The draft was submitted for consultation to the groups concerned. Their reaction was, in general, that the registry-registrar model was not viable on the Swiss market and they did not wish to become providers. They wanted the existing sole-provider arrangement to be kept, with that provider having full latitude to promote or facilitate service provision by involving other organizations.

At that time the Federal Council concluded that it was neither desirable nor appropriate to open the allocation of ".ch" domain names to competition. Nonetheless, it is entirely conceivable that, sooner or later, the question of the sole provider will have to be looked at again, if the domain-name management and allocation market in Switzerland undergoes further changes.

2.2 Legal basis for formal delegation

Domain names are considered to be addressing resources under the Swiss Telecommunications Law (LTC). Under that law, OFCOM is responsible for managing addressing resources in Switzerland. In specific cases OFCOM may delegate the management and allocation of certain resources to another entity. This option was exercised in two cases, that of the management of telex numbering plan resources and that of Internet domain names. The arrangements are contained in the ORAT decree.

2.3 Form of delegation for the management of addressing resources in general and ".ch" domain names in particular

The following is a synopsis of the regulation governing delegation of the management of addressing resources in general and ".ch" domain names in particular.

- OFCOM designates one or more delegees, defining conditions that must be met to exercise the delegated activity or issuing a public call for offers. OFCOM determines any necessary arrangements for the delegation process, respecting the principles of impartiality, non-discrimination and transparency, while at the same ensuring the confidentiality of applicants' data is fully protected. Delegation of the management and allocation of addressing resources must take the form of an official authorization or a contract. Delegation is for a specified period of time. In the case of domain names, delegation takes the form of a renewable five-year contract under administrative law.
- When domain name reservations are abused, for example by registering domain names in bad faith, in deliberate violation of others' intellectual property rights or name rights (cyber-squatting), the possibilities for recourse include ordinary civil law but also a dispute resolution procedure, to be set up by the delegee.
- ORAT contains general rules governing the delegation of addressing resources by OFCOM (article 13 and following). Those rules apply to management and allocation of domain names as well, except where specific provisions to the contrary exist. This allows OFCOM to delegate management and allocation of addressing resources other than domain names without necessarily requiring any further revision of the decree. In addition, the general rules on delegation apply to telex addressing resources the management of which has been delegated.
- Specific rules have been set up to cover the delegation of domain name management and allocation (article 14 and following); their provisions cover gaps in, add detail to, and in some cases replace those of the general rules where the unique nature of domain names requires it.
- While the relationship between OFCOM and the delegees is governed by public law, the same is not true of the relationship between domain managers and the customers who make use of their management and allocation services for addressing resources. The latter falls under private law, and any disputes are subject to civil jurisdiction.
- In view of the nature of the task and the public interest involved, delegees have a responsibility to respect the principles and general rules of public law that apply to the management and allocation of addressing resources, particularly the principle of transparent, non-discriminatory allocation of those resources. The delegee must take the rules and principles into account in contractual, private law customer relationships.
- Delegees are free to determine the prices they will charge for their services in management and allocation of addressing resources if there is a situation of effective competition on a given market. The prices of certain services may in some cases be subject to approval by the Office, particularly if the manager does not have any competitors offering the same service - as is the case for domain names. In this case the registry determines the prices to be charged for those services, on the basis of incurred cost and fair profit.

2.4 Relations between ICANN, SWITCH and the Swiss Government (OFCOM)

Under the principles for delegation and administration of ccTLDs elaborated by the Governmental Advisory Committee (GAC) of ICANN, governments have ultimate authority over their ccTLDs. In Switzerland, the Telecommunications Law (LTC) provides the legal basis conferring this authority

over the top-level domain name ".ch" on the Government and its oversight authority, OFCOM. In addition, the delegated operator of the ccTLD ".ch", the SWITCH foundation, depends on the technical functions of ICANN/IANA to ensure the ccTLD functions correctly. There is thus a three-way relationship between the Swiss Government, SWITCH and ICANN/IANA.

To allow OFCOM to fulfil its role as ultimate authority, under the principles elaborated by GAC, SWITCH is obliged to submit for its approval any proposed contract with ICANN/IANA. This provision allows OFCOM, among other things, to verify that such a contract is in compliance with Swiss regulations concerning domain names.

For more details on the Swiss model for delegation. The complete texts in French, German and Italian are available under the following URLs:

French version: http://www.admin.ch/ch/f/rs/c784_104.html

German version: http://www.admin.ch/ch/d/sr/c784_104.html

Italian version: http://www.admin.ch/ch/i/rs/c784_104.html

3 Implementation of Resolution 102 of the ITU Plenipotentiary Conference (Marrakesh, 2002)

3.1 IP Symposium for CEE, CIS and Baltic States

Moscow Declaration: The ITU Plenipotentiary Conference (Marrakesh 2002) revised Resolution 102: Management of Internet Domain Names and Addresses, originally adopted at the 1998 Plenipotentiary Conference; it also adopted Resolution 133: Role of administrations of Member States in the management of internationalized multilingual domain names. Resolution 102 instructs the Director of the Telecommunication Development Bureau "*to organize international and regional forums, in conjunction with appropriate entities, for the period 2002-2006, to discuss policy, operational and technical issues on the Internet in general and the management of Internet domain names and addresses in particular for the benefit of Member States, especially for least developed countries".*

Following the instructions in Resolution 102, an IP Symposium for CEE, CIS and Baltic States was organized by the ITU Telecommunication Development Bureau in Moscow, Russian Federation, from 16 to 19 September 2003, at the kind invitation of the Ministry of Communications and Informatization of the Russian Federation.

The participants from ITU Member States have made the following recommendations as their contribution to the initiatives undertaken by ITU to implement Resolutions 102 and 133:

1) Next generation networks (NGN), representing the convergence of IP-based and PSTN network technologies and services, create new opportunities while representing challenges that need to be considered by national policy-makers and regulators. ITU is requested to provide an overview of the concepts behind NGN and their likely impact and considerations.

2) We recommend that national policy-makers and/or regulators need to pay particular attention to the issue of allocation/assignment of Internet names and addresses both within their national contexts and at regional and international levels, in particular, how they relate to convergence between PSTN and IP-based networks (e.g. ENUM, IPv6 deployment, potential allocation of ITU-T Recommendation E.164 resources to IP-based terminal devices).

3) For the consideration of national authorities, ITU is requested to provide examples of best practices and models of national organization structures and, if appropriate, model law frameworks with regard to administration of country code Top Level Domains (ccTLDs).

4) ITU is requested to provide assistance to ITU Member States, upon specific request, in the repatriation of the management of their ccTLDs as well as to provide technical and policy assistance concerning ccTLD management including dispute resolution considerations, the latter in partnership with WIPO.

5) Recognizing the sovereign and legitimate interests of ITU Member States with regard to the protection of their country names in the DNS, ITU is requested to keep Member States appraised of the current state of discussions concerning implementation of the WIPO recent recommendations in this regard.

6) ITU is requested to provide up-to-date information about the structure and responsibilities of Internet administration bodies and the current discussions concerning responsibilities for Internet management on a dedicated ITU website.

7) ITU is requested to summarize on a regular basis the experiences and best practices of various countries (e.g. Internet country case studies) in fostering the deployment of the Internet in their countries with regard to both the interest of administrations and the private sector, including, *inter alia*, best practices regarding deployment of VoIP in national contexts.

8) With regard to the international dimension of quality of service indicators and parameters of voice traffic transmission based on VoIP technology, ITU is requested to elaborate the appropriate recommendations that provide for a set of necessary technical requirements that meet the needs of users, operators and administrations. In this regard, ITU is requested to provide an overview of the current standardization activities and specific ITU-T Recommendations relating to QoS considerations for VoIP networks.

9) ITU is encouraged to enhance its training initiatives with regard to DNS and IP address management and recommend best practices, including with regard to deployment of IPv6, in cooperation with appropriate entities;

10) In accordance with Resolution 133, ITU is requested to keep Member States informed of possible policy considerations with regard to the deployment of internationalized domain names (IDNs) as well as to consider further cooperative initiatives at national and regional levels.

11) ITU is requested to provide reference material related to IPv6, its adoption and deployment.

12) Assistance should be rendered to the interested countries on the issue of regulatory and tariff policies with regard to advanced communication technologies in advance of joining WTO, in particular information should be provided about the activities of ITU-T Study Group 3 in this regard.

3.2 IP Symposium for Africa Region

Kigali Declaration: The ITU Plenipotentiary Conference (Marrakesh, 2002) revised Resolution 102: Management of Internet Domain Names and Addresses originally adopted at the 1998 Plenipotentiary Conference. Resolution 102 instructs the Director of the Telecommunication

Development Bureau "*to organize international and regional forums, in conjunction with appropriate entities, for the period 2002-2006, to discuss policy, operational and technical issues on the Internet in general and the management of Internet domain names and addresses in particular for the benefit of Member States, especially for least developed countries".*

Following the instructions in Resolution 102, an IP Symposium for Africa was organized by the ITU Telecommunication Development Bureau in Kigali, Rwanda, from 7 to 9 July 2003, at the kind invitation of the Ministry of Infrastructure of the Republic of Rwanda.

The participants from ITU Members States have made the following recommendations as their contribution to the initiatives undertaken by ITU to implement Resolution 102, the Istanbul Action Plan developed at the World Telecommunication Development Conference (WTDC-02) and the objectives of the New Partnership for African Development (NEPAD) initiative.

1) We recommend that the development of information and communication technologies (ICTs), including DNS management and IP address allocation, be considered at the highest political level including at national, subregional and African Union levels, in cooperation with ITU and other appropriate entities.

2) It was recognized that a national telecommunication infrastructure is much more important than just a platform for voice. Rather it must be considered as a fundamental enabling environment for the growth of ICTs, making possible new opportunities for improved access to government public services including, *inter alia*, education, health and socio-economic advancement.

3) We recommend that ITU develop an Internet policy handbook covering issues of concern to national policy-makers and regulators, with particular emphasis on the needs of developing countries. This could include, *inter alia*, VoIP, examples of current best practices and measures for dispute resolution.

4) It was recognized that indicators are essential to measure the evolution of ICTs, in particular the needs and performance of developing countries and their particular environments. It was considered necessary to have new indicators to measure and map the success of deployment of ICTs.

5) It was recognized that building human capacity and mainstreaming gender, youth and people with disabilities is an important factor in developing ICTs. We encourage the related national capacity building initiatives as well as ITU's related programmes.

6) It was recognized that there was a clear need for public-private partnerships that balance the commercial interests of the private sector with the responsibility of governments in promoting universal access to ICTs. The establishment of independent regulators was considered to be an important step in this regard.

7) We recommend the establishment of strategies and cooperation at regional and pan-African levels in the areas of infrastructure development, ICT manufacturing, capabilities and policy harmonization.

8) We recommend that national policy-makers and/or regulators pay particular and urgent attention to the issue of allocation/assignment of Internet names and addresses. It was emphasized that the Internet is a global resource. We strongly recommend that ITU engages itself in the establishment of an enabling international framework that fully recognizes the sovereign and legitimate interests of all ITU Member States. This includes, *inter alia*, the allocation and management of ccTLDs and the protection of country names.

9) We recommend that ITU, in partnership with the African Union, organize a symposium on issues related to AfriNIC as early as possible.

10) We recommend that ITU organize a symposium as early as possible on the topic of establishment of Internet Exchange (IX) points at national and regional levels to keep traffic local and thereby reduce international traffic and related costs. The symposium should address related topics including sharing of country experiences and the necessity of regional interconnection.

11) We recommend additional initiatives that reduce dependencies on non-regional services and international connectivity. Examples of such initiatives include encouraging the development of local content and services (e.g. local free e-mail services).

12) While recognizing that it is a national matter, it was considered important to establish a clear national policy and, as appropriate, regulatory framework concerning the use of VoIP. Furthermore, policy-makers and regulators are urged to consider the impact of convergence on the management of addressing resources affecting interoperability between VoIP and the PSTN (e.g. ENUM, E.164 resource assignment to IP terminals).

13) We recommend that open source software be considered as an enabling development for more affordable access to ICTs.

Attachment 11

Best Practice Guidelines for ccTLD Registries

Contribution by Richard Francis

Current Version

Status of this document

This document is a CENTR Position.

It has been developed in accordance with the CENTR Policy Development Procedures, as approved at the CENTR General Assembly in Budapest on 3 June 2003.

The paper labelled as a CENTR Position is a position paper developed by CENTR and CENTR Members.

This document is non-binding on CENTR Members.

Table of contents

Page

Best Practice Guidelines for ccTLD Registries

As at 19 September 2003

"CENTR Position"

I PREAMBLE

1 Basic objectives

This Best Practice document is intended to provide guidelines on the operation of country code top level domain name (ccTLD) registries and policies for such registries. It is intended to be a model for ccTLD registries. Whilst recognizing that managers of ccTLD registries do not necessarily fully conform, most of the ccTLD registry community subscribes to the essence of the guidelines set out in this document.

2 Basic principles

The Best Practice document closely follows established Internet principles such as:

a) self-regulation;

b) bottom-up authority (the Internet consists of cooperative networks);

c) consensus (requirement for self-regulation);

d) transparency (requirement for self-regulation);

e) cooperation based on trust and fairness.

Any interpretation of the Best Practice document must be consistent with principles a) to e) above.

3 Authority of the country code top level domain name registries

Historically, the identity of the ccTLD registry was recorded in the TLD database by the Internet Assigned Numbers Authority (IANA). In March 1994 the management of ccTLD registries was codified, under the guidelines published in RFC 1591 by IANA.

A ccTLD registry's authority derives from the local Internet community, as defined in clause II.1. of the Best Practice Guidelines below and from the acceptance of that authority by its local Internet community. That local Internet community has a responsibility to support and protect the ccTLD registry, and to assist the ccTLD registry to serve that community.

The function of IANA is recognized and supported by ccTLD registries. It is, however, felt necessary to stress the fact that the local Internet community and the law in the local jurisdiction takes precedence over any recommendations issued by IANA or other bodies.

II BEST PRACTICE GUIDELINES

1 Definitions

ccTLD – a country code top level domain in the global domain name system, using the two-letter code elements from the ISO 3166 standard.

ccTLD Registry – an entity that is responsible for administering and operating a ccTLD.

DNS – the Domain Name System (see RFCs 1034, 1035 and 2181).

Registrant – a company, organization or individual for whom a domain name under the ccTLD has been registered with the ccTLD registry.

Registry data – data held in the register database maintained by the ccTLD registry.

IANA – Internet Assigned Numbers Authority.

Local Internet community - the Internet industry, Internet users, governmental and other public authorities of the country or territory with which the ccTLD is associated. The definition of the local Internet community may vary from one country/territory to another, and is essentially a matter for the community in the country/territory.

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, published at www.ietf.org/iesg/1rfc_index.txt

2 Best Practice

2.1 Primary duty of ccTLD Registries

The primary duty of the ccTLD registry is to perform its function in the best interest of, and in consultation with, the local Internet community.

2.2 Consulting the local Internet community

For the purpose of consultation, the ccTLD registry should delineate the local Internet community. This process, as well as subsequent consultations, should be transparent.

2.3 Registration of domain names

ccTLD registries should:

- follow policies, rules and procedures that have been established and published, in a transparent manner;
- register domain names, in an efficient and timely manner;
- have a standard contract with registrants;
- provide a public WHOIS service.

2.4 Policies

Policies and procedures may vary from country to country owing to, for example, local customs, cultural values, local policies and objectives, law and regulations. However, registration policies should:

- oblige the ccTLD registry to be equitable and fair to all eligible registrants that request domain names;

- define which parties are eligible to register domain names under the ccTLD;
- require registrants to provide correct data and keep such data duly updated;
- base the registration on objective criteria which are transparent and non-discriminatory;
- be documented and publicly available.

2.5 Location

The ccTLD registry should be resident or established in the country/territory that the ccTLD relates to, specified in the ISO 3166 standard, unless otherwise accepted or agreed as being in the interest of the local Internet community.

2.6 Technical requirements

The ccTLD registry organizes the process of registration and maintenance of domain names, the operation of the domain name servers and the maintenance of the appropriate zone files for the ccTLD. There must be permanent (24 hours, 7 days) Internet protocol (IP) connectivity to an appropriate number of name servers (what constitutes an appropriate number is related to many different factors) and the registry servers. The ccTLD registry's contact details must be published and should be permanently accessible.

Duties such as the registration of domain names and operation of name servers must be done with technical competence (see RFC 2181). This includes operating with accuracy, robustness and resilience (see RFC 1591).

2.7 Changes to information in the IANA database

The ccTLD registry should inform IANA, in a timely manner, of changes to the information that is maintained in IANA's ccTLD database.

2.8 Financial basis of ccTLD registry operations

ccTLD registries should operate on a cost-effective, cost-recovery basis, unless otherwise accepted or agreed by the local Internet community.

2.9 Subcontracting of operations

If the ccTLD registry contracts out any or all of the operation and administration of the registry, then it should oblige its subcontractor to follow the requirements of this document.

2.10 Data security

ccTLD registries should take reasonable professional measures to ensure that all registry data is secured against damage or loss.

2.11 Domain name dispute policy

ccTLD registries should define and publish their domain name dispute policies and procedures.

3 Governing law and jurisdiction

The governing law of contracts between the ccTLD registry and registrants and/or registrars should normally be a system of law which obtains within the country or territory to which the ISO 3166 two-letter code relates; or - with the acceptance or agreement of the local Internet community concerned – an appropriate choice of law and jurisdiction from systems of law and jurisdiction commonly used in international commercial contracts.

4 Intellectual property rights

ccTLD registries may have rights to the intellectu al and other property developed by them as a by-product of managing the ccTLD registry. The ccTLD registry should take reasonable steps to safeguard any such rights.

Attachment 12

Model regulation or law for ccTLDs

Table of contents

Model regulation or law for ccTLDs

Article 1 Purpose

The purpose of these regulations is to set the public law framework conditions for an agency that assigns domain names under the national country code top level domain.

[Steps should be taken to facilitate the use of electronic means to form contracts for domain names. Means for incorporating electronic contracting provisions in national laws are, however, outside the scope of this model.]

Article 2 Definitions

The following definitions apply for the purpose of these regulations:

a) *Country code top level domains:* the uppermost domain in the hierarchy of the global Internet domain name system according to 2-letter codes under the ISO 3166-1 standard.

b) *Registry:* entity that by agreement with the international manager of top level domains is entitled to assign domain names under country code top level domains.

c) *Registrar:* an enterprise that has made an agreement with a registry for the right to send in applications and notices of alteration to the registry on behalf of applicants for/holders of domains under the national country code top level domain.

d) *Domain complaints board:* a board for handling complaints regarding domain names under the country code top level domain.

e) *Registered Data:* data regarding the applicant and applicant's enterprise required in connection with applications and notices of alterations.

Article 3 Designation

1 The national country code top level domain is administered by one registry which determines rules for the assignment of domain names (name policy) under the national country code top level domain.

2 The national telecommunications regulatory body shall define the conditions to be met by the registry and may issue a public call for tender in order to designate the registry.

3 The activities of the registry shall be subject to authorization by the national telecommunications regulatory body. The authorization shall be for a specific time period, normally five years. The authorization may be renewed. *[Depending on the national law and regulations, this authorization could take the form of a contract between the government and the registry, or it could take the form of a government decree.]*

4 The national telecommunications regulatory body may amend the provisions of the official authorization or contract prior to their expiry if there is a change in circumstances or in the law and such amendment is necessary to protect overriding public interests.

5 The registry shall be awarded an appropriate indemnity for any financial damages arising from such amendment of the official authorization or contract.

Article 4 Oversight

1 Supervision to ensure compliance with these regulations shall be exercised by the national telecommunications regulatory body.

2 If the registry fails to satisfy the requirements of these regulations, the national telecommunications regulatory body may order it to remedy the unlawful conditions or may order operations to cease within a specified time limit.

3 The registry shall not transfer its activities to another entity without prior approval by the national telecommunications regulatory body.

Article 5 Tasks

The registry's duties shall include the following:

a) provide for installation, management and updating of the technical infrastructure required for the allocation and management of the national country code domain;

b) provide for reliable and professional operation of the domain name system within the national country code domain in accordance with the applicable technical standards;

c) offer services in the allocation and management of domain names within the national country code domain;

d) provide for installation, administration and updating of a central public database providing any interested persons with guaranteed real-time access to information about domain name holders *[whether to include this provision, and the determination of which information to provide, will depend on national considerations, but should take into account existing practice, which is to publish the name, address, and e-mail of the domain name holders]*;

e) take the necessary precautions to ensure reliability, accessibility, availability, security and operability of the infrastructure mentioned in paragraphs a) and d) above;

f) ensure that the infrastructure mentioned in paragraphs a) and d) above conforms to the state of the art and is compatible with international standards used for the domain name system; and

g) in the context of its duties to allocate and manage domains, work towards the stability of the domain name system.

Article 6 Record of Activities

1 The registry shall maintain a record of all its activities in connection with the allocation, revocation and retirement of addressing resources.

2 The registry shall conserve the recorded data and supporting documents for a period of ten years *[modify duration in accordance with national law and practices]*.

3 The registry shall provide the national telecommunications regulatory body with any and all information and documents that may be necessary for the execution of the present regulations. In particular, the national telecommunications regulatory body may request a list of the allocated addressing resources and a copy of the record of activities.

4 The registry shall communicate free of charge to the national telecommunications regulatory body such information as may be necessary for the purpose of establishing official statistics.

Article 7 Rules for assigning domain names

1 Rules for the assignment of domain names (name policy) under the national country code top level domain shall be drawn up by the registry. *[Some countries may wish to engage in formal or informal consultations regarding the structure of names under the country code, for example, whether there should be second-level names reserved for specific purposes such as commerce, education, content for children, adult entertainment, etc.]*

[A key decision to be taken is whether the registration of domain names under the national country code should be restricted to entities or persons resident in the country, or open to anybody around the world. Both approaches have been taken in practice in different countries.]

2 The assignment rules shall be available to the general public and at a minimum shall be so designed that they:

a) ensure high technical quality;

b) are non-discriminatory;

c) are open to inspection;

d) promote predictability;

e) promote protection of personal data and consumer interests;

f) promote the interests of Internet users, individually and as a group; and

g) promote national interests and allow for international developments in the Internet.

3 Before assignment rules are adopted or altered, opinions shall be obtained from representatives of the users and from the national telecommunications regulatory body.

Article 8 Personal affirmation

1 The registry shall require applicants for registration of domain names under the national country code top level domain to furnish a personal statement affirming as a minimum that registration and use of the name applied for:

a) is not contrary to the assignment rules;

b) is not contrary to national law; *[in certain countries, this may prohibit registration of the names of places, for example, cities. Certain countries may also wish to consider a policy with respect to the names of persons.]*

c) does not conflict with the rights of a third party; and

d) does not unrightfully give the impression of pertaining to public administration or the exercise of public powers.

2 In this personal affirmation the applicant shall grant the registry the right to recall the assigned domain name if it is obvious that the assignment was contrary to paragraph 1 above.

Article 9 Non-payment of fees

If a domain name owner does not pay the fees agreed to by contract with the registrar or registry, the domain name shall revert to the registry.

Article 10 Transfer of domain names

A domain name registered under the national country code top level domain may be transferred at the request of the owner, by a will (provisions in case of death), by an administrative or judicial order, or by a decision of the domain complaints board.

Article 11 Registrars

[This article applies for countries wishing to introduce a competitive regime, through registrars. Other countries may prefer a single-supplier regime (no registrars)].

1 The registry shall delegate parts of the registration process, including forwarding applications and alteration notices on behalf of applicants for, and holders of, domain names, to the registrars and shall promote competition between them by granting all registrars the same terms.

2 Fees charged by the registry to registrars shall be fair and based on costs. They shall be submitted to the national telecommunications regulatory body for approval. Abusive pricing will be sanctioned in accordance with national law.

3 The terms of the standard contract proposed to registrars may be reviewed by the national telecommunications regulatory body in order to ensure fairness.

Article 12 Supervision of Registry

[This Article applies primarily to countries which have chosen a single-supplier regime (no registrars).]

1 Fees for the registration of domain names under the national country code top level domain shall be fair and based on costs. They shall be submitted to the national telecommunications regulatory body for approval. Abusive pricing will be sanctioned in accordance with national law.

2 The terms of the standard contract proposed to applicants for the registration of domain names under the national country code top level domain may be reviewed by the national telecommunications regulatory body in order to ensure fairness.

Article 13 Back-up copies

The registries shall ensure that copies are kept of all registered data, for at least five years. *[Modify duration in accordance with national law and practices.]*

Article 14 Data privacy

The privacy of personal information regarding domain name owners shall be safeguarded in accordance with national law.

Article 15 Complaints procedures

1 The registry shall establish a domain complaints board comprising at least three members.

2 The complaints board may handle complaints:

a) against decisions passed by the registry on applications for assignment of a domain name;

b) against decisions passed by the registry under paragraph 2 of article 8 of these regulations;

c) from registries that a name has been registered in contravention of a personal affirmation;

d) from a third party, under subsection c) of article 8 of these regulations; *[WIPO has published best practices in the area of handling complaints related to trademark infringement, see: http://web.itu.ch/itudoc/itu-t/workshop/cctld/cctld005.html This is the type of complaint that, to date, has arisen most frequently in practice.]*

e) from a public agency, under subsection d) of article 8 of these regulations; and

f) from the national telecommunications regulatory body claiming that registration of the domain name is contrary to the rules.

3 Complaints under subsection e) above must be filed no later than three months after the domain name is registered.

4 Opinions returned by the complaints board on complaints under subsection a) above shall be binding for the registry. Opinions returned by the board on complaints under subsections b) through f) shall be advisory.

5 The domain complaints board may be financed through an addition to the charge for registering the domain name and a charge payable by the complainant.

6 The registry shall define procedures for the complaints board in keeping with the above rules. Board decisions shall be open to the public in accordance with national law.

Article 16 Termination of activities

1 If the registry terminates its registration activities, whether voluntarily or by order pursuant to these regulations, or for other reasons, all registered data shall be transferred to a new registry.

2 The registry's duties may be taken over by the national telecommunications regulatory body until a new registry is established. In this case, the national telecommunications regulatory body shall take over the registered data free of charge and shall in turn transfer these data to the new registry free of charge.

3 The national telecommunications regulatory body shall decide whether operations in the interim period shall take place in accordance with the rules of the registry being terminated, and the rules concerning the complaints board, or whether new rules shall be adopted. In the interim period, the national telecommunications regulatory body is bound by these regulations wherever applicable.

Article 17 Sanctions

The national telecommunications regulatory body may impose enforcement fines in accordance with national law.

Attachment 13

Internationalize domain names (IDNs)

Table of contents

Page

Internationalize domain names (IDNs)

The Internet Engineering Task Force (IETF) has approved three documents which, taken together, provide a technical foundation for handling domain names with Unicode characters (that is, domain names which contain non-ASCII characters). These documents are:

- RFC 3490 "Internationalizing Domain Names in Applications (IDNA)";
- RFC 3491 "Nameprep: A Stringprep Profile for Internationalized Domain Names";
- RFC 3492 "Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA)".

1 Introduction

A domain name is used to identify an entity within the Internet in a format that humans can easily understand; it has been one of the fundamental addressing schemes in Internet use for over 15 years. At the most basic level, it maps a human-readable name such as "**WWW.ITU.INT**" to a machine-readable Internet protocol (IP) address (e.g. 156.106.134.92). In its current form, only a limited set of ASCII[1] characters, namely letters, digits and hyphens, can be used in domain names. Envisaged originally as a system of easily remembered identifiers to help network engineers address computers, there was no initial perceived need to expand the set of supported characters to include non-ASCII scripts.

However, the past decade has seen a wide global adoption of the Internet. Founded on innovative technological and economic principles, the Internet has experienced dramatic growth. It took 74 years for the telephone network to reach 50 million users. It took only four years for the worldwide web to reach that same number. Today, the Internet is a global network of more than 230 connected economies and more than 350 million users.

One consequence of this growth is that the number of users, as well as Internet content, from societies and cultures not familiar with ASCII is growing daily. To address this phenomenon, e-mail and web pages in many scripts and languages are supported by various pieces of Internet software. Yet domain names, arguably one of the most visible symbols of the Internet, are still in ASCII characters and pose a significant linguistic barrier. Although users of languages based on Latin characters, either natively (e.g. English) or in a transliterated form (e.g. Malay), do not have linguistic problems with the current domain name system, native speakers of Arabic, Chinese, Japanese, Korean, Tamil, Thai and others who use non-ASCII scripts remain at a considerable disadvantage. In an attempt to solve this problem, as well as generally provide for improved multilingual and multiscript support, a process of "internationalization" of the Internet's Domain Name System (DNS) has been under way.

---

1 ASCII (American Standard Code for Information Interchange) is the most common format for text files in computers and on the Internet. In an ASCII file, each alphabetic, numeric, or special character is represented with a 7-bit binary number (a string of seven 0s or 1s). 128 possible characters are defined. This format corresponds to the International Reference Alphabet (IRA) as defined in ITU-T Recommendation T.50 (ISO/IEC 646).

Since 1998, a number of technical solutions for this problem have emerged. More than a dozen commercial companies, as well as some country code[2] top level domain (ccTLD) administrators, have set up a variety of technical multilingual domain name solutions. In the commercial market, there is intense competition with no clear winners emerging with a *de facto* standard.

Consumer demand has been extremely strong – particularly in Asian countries. However, for the most part, these solutions remain technically non-interoperable among themselves. Recognizing the problem, an Internationalized Domain Names (IDN) Working Group was formed within the Internet Engineering Task Force (IETF) in early 2000 to define a technical approach and related standards. By 2000, various "test beds" had been deployed around the world to offer multilingual domain names.

There has also been an emerging realization that multilingualization of the DNS is far from being an exclusively technical problem – it is also one of administration, management and policy. By 2001, organizations such as the Multilingual Internet Names Consortium (MINC), Arabic Internet Names Consortium (AINC), Chinese Domain Names Consortium (CDNC), International Forum for IT in Tamil (INFITT) and Japanese Domain Names Association (JDNA), as well as a number of other nascent language groups, had emerged to occupy a policy vacuum.

In parallel, there have been major ongoing developments in administration and policy with respect to conventional ASCII-based domain names. In October 1998, the Internet Corporation for Assigned Names and Numbers (ICANN), a not-for-profit corporation, was established under the laws of the state of California, in the United States[3]. The following month, a memorandum of understanding (MoU) was signed between the Unites States Department of Commerce and ICANN[4]. Under the framework of this MoU, ICANN has provided for competition in the domain name registration market, a uniform domain name dispute resolution policy (UDRP)[5], and some new top level domains (TLDs).

More recently, in March 2001, ICANN formally launched a number of activities related to multilingual domain names. A recent survey conducted by an ICANN internal working group[6] has indicated that there is strong support for the rapid deployment of multilingual domain names.

Nevertheless, a great number of challenges and uncertainties remain as to when and how multilingual domain names will be deployed. At the time of preparation of this briefing paper (November 2001), IETF's IDN Working Group had not reached the consensus needed for technical standardization of multilingual domain names. Considering the related debates, even if an IETF standard does emerge, it is unclear whether it will be universally adopted. Equally unclear is whether new emerging naming technologies not based on the DNS, such as keywords, will emerge as a preferred solution. There is even the possibility that hybrid technologies merging the DNS and keywords will surface. One result is that users have been left in a state of considerable confusion by a multiplicity of technologies, "test bed" deployments and incompatible technologies.

---

2 Country code top level domains are based principally on the two-letter code set of the ISO 3166-1 Standard (e.g. .fr for France, .cn for the People's Republic of China). See http://www.din.de/gremien/nas/nabd/iso3166ma/ for a list of these codes.

3 For details on the organization and activities of ICANN, see http://www.icann.org.

4 See http://www.ntia.doc.gov/ntiahome/domainname/icann-memorandum.htm.

5 Principally developed by WIPO, see http://arbiter.wipo.int/domains/index.html.

6 See http://www.icann.org/committees/idn/final-report-28aug01.htm.

Finally, the appropriate model for the assignment, administration and management of multilingual domains, including multilingual top level domains, will need to be developed. ICANN, having only recently approached this problem, has not indicated any clear sense of the direction to be taken on this issue. In practice, national or regional approaches may differ widely according to local language requirements. In this case, there may be some sensitivity as to which authority would be responsible for what may be seen as national, localized or regional issues. Linguistic groups have also proliferated, adding yet another necessary level of coordination. All this suggests that the establishment of multilingual domain names may result in further challenges to the technology, policy and management aspects of the DNS.

2 Demand for multilingual domain names

As the Internet originated in the United States, the technology has, not surprisingly, been very much based on the English language. Even those outside of the United States who were pivotal in the development of the Internet typically had technical backgrounds and were familiar with English. Furthermore, ASCII codes have long been used at the core of computing and the Internet, especially early on, when resources such as central processing units and memory were limited. Because of these historical circumstances, even people in countries that do not use ASCII characters in their written languages have typically used ASCII characters when accessing services on the Internet. In addition, because users in the early stages of the Internet's development were from the research and academic communities, English language exclusivity did not prove to be significant obstacles to its expansion.

However, in more recent years, the Internet has grown to reach all corners of the world, to people of all ages and educational backgrounds, and is used by businesses and consumers alike. It is estimated that by 2003, two-thirds of all Internet users will be non-English speakers[7]. Furthermore, over 90 per cent of the world's population speaks a primary language other than English[8]. This means that, for an increasing number of people, English and the English alphabet will be considered barriers to becoming Internet users. These people will find it extremely unnatural to use the Internet in English with the English alphabet.

Therefore, the demand for Internet usage in languages other than English is growing and will continue to grow. Enabling the use of the Internet in one's native language, in which one is at ease, is important in extending the benefits of the Internet to all individual users. This is one more step toward bridging the "digital divide" – an expression commonly used to refer to the uneven global pace of progress in access to information and communication technologies.

It should be noted that, besides the disadvantages of using an alphabet with which they are not familiar, non-English speakers often face other issues of a more complex nature. For example, a Japanese person's name "博文" is transcribed as "hirofumi" in Roman letters. On the Internet, where only ASCII characters can be used, he is "hirofumi", just like other people named "hirofumi" but whose names may use different Japanese characters such as "博史" or "宏史". In fact, there may be over 100 different Japanese representations that will end up being denoted simply as "hirofumi" in ASCII space. Consequently, in the ASCII world, the person in question is just one "hirofumi" of many other Japanese "hirofumis", although in his native Japanese characters he would be clearly differentiated.

---

7 See http://www.icann.org/committees/idn/final-report-28aug01.htm and http://www.walid.com.

8 See http://www.walid.com.

This type of problem may also exist for people using Latin-based languages – for example, in the case of people with apostrophes, accents or other diacriticals in their names. The exact forms of these names cannot be represented as domain names either as the latter are restricted to alphanumeric characters and the hyphen. In other words, these people's real names are subject to mapping into a space where only alphanumeric characters and the hyphen can be used.

Over time, there has been a substantial evolution in the use of non-English languages in Internet content. For example, in the case of e-mail, the following developments have taken place:

Step 1: Expression of a native non-English language in e-mail texts using phonetic mapping from the language in question into the English alphabet (transliteration).

Step 2: Use of native language characters in e-mail texts.

Step 3: Use of native language characters in the subject field of e-mails.

What should the next step be? It is a natural step forward for people to want the name of the sender and receiver of e-mails to appear in their native language.

All machines connected to the Internet are given unique Internet protocol (IP) addresses, which are machine-readable, (e.g. 123.4.5.67 in the case of IP Version 4). An IP address can be made more human-friendly by using the Domain Name System which provides a simple, memorable string of characters, called a domain name, synonymous with a particular IP address. With the number of services that have emerged on the Internet, the need has arisen to address more than just machines. For example, with e-mail, we address *users* of machines. With the worldwide web, we address the locations of *documents*. Thus, in order to facilitate communication, objects on the Internet are named by means of uniform resource locators (URLs) such as **HTTP://WWW.ITU.INT/MDNS/** or e-mail addresses such as **SPUMAIL@ITU.INT**.

A domain name is a string of characters, such as "**WWW.ITU.INT**" or " **WWW.WIPO.INT**", in this case referring to Internet host computers. Given that domain names were devised as easily memorable strings to be used in place of IP addresses, there is no doubt that the requirement for memorability will grow into a demand to use native languages just as this is part of everyday life. Furthermore, the demand will grow for the use of other significant expressions such as company names and personal names. This means that domain names have evolved to a certain extent from simple identifiers to represent identities of entities. These days, domain names are considered equivalents to brand names, product names and service names. From a technical aspect, this is a major departure from the original purpose.

In addition to domain names, there are various other methods of naming the entities on the Internet. These include, *inter alia*, search engines and directories, such as the lightweight directory access protocol (LDAP) and common names resolution protocol (CNRP)[9]. However, only domain names have become so widely and consistently used, and therefore retain their role as the preferred naming scheme for the Internet.

The terms "multilingual domain names" and "internationalized domain names" are often used interchangeably, although Internet engineers and operators tend to prefer "internationalized domain names." This may reflect the view that they wish to avoid the semantics of natural languages into domain names and merely want to make it possible to use characters from all over the world in domain name scripts. However, generally this paper will use the term "multilingual", except where "internationalized" appears in a proper noun.

---

9 See http://www.ietf.org/html.charters/cnrp-charter.html.

3 Technical aspects of the multilingualization of domain names

The DNS domain name space has a hierarchical structure (see Figure 1 below) and is used to identify entities in the Internet. Each node in the structure corresponds to an entity in the Internet. A name given to a node in the structure is called a domain label. All nodes are given labels with one exception: the root node, as shown at the top of Figure 1, which has no label. The domain name of an entity (node) is a sequence of node labels starting from itself up to the root, and where labels are separated by periods. As to the length, a domain label should not exceed 63 octets[10] and an entire domain name should not be longer than 255 octets.

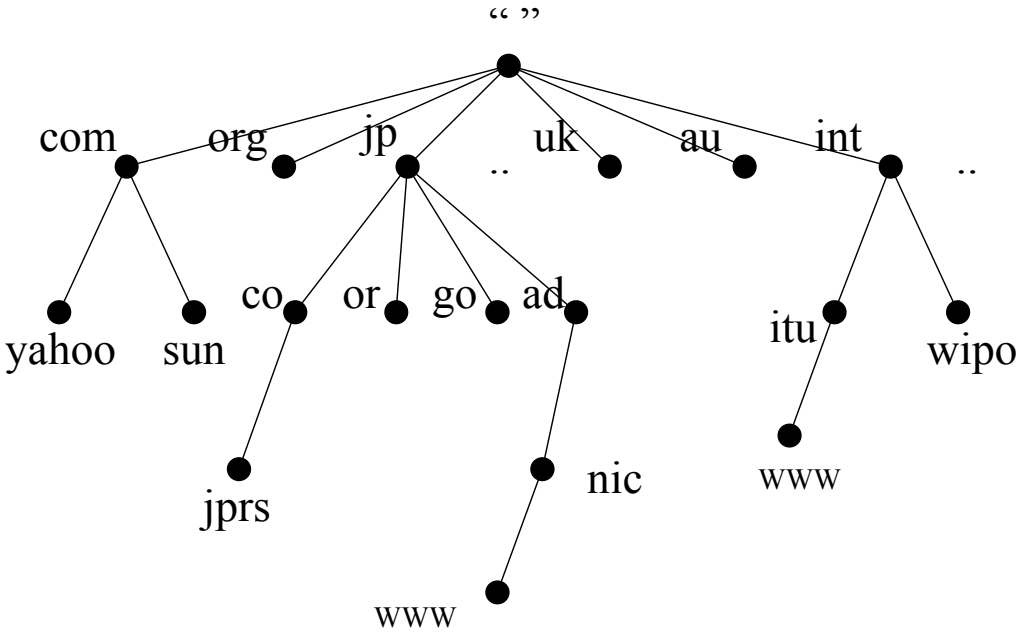


Figure 1 – The structure of domain names

Figure 2 (below) shows how an entity named by a domain name is identified on the Internet. Each node of the DNS structure can be considered as a table, called a name server, maintaining pairs of the node labels directly underneath the node and the corresponding IP addresses. Name servers correspond to organizations or units that are *authoritative* to manage the domain name corresponding to the node. For example, the root server is the authoritative source for the .int or .com names; the name servers for .int are the authoritative source for the .itu.int and .wipo.int names, and the name servers for .itu.int are authoritative for www.itu.int. The DNS is thus, in effect, a large globally distributed database from both an engineering and management viewpoint.

---

10 In computers, an octet (from the Latin *octo* or "eight") is a sequence of eight bits. An octet is thus an eight-bit byte. Since a byte is not eight bits in all computer systems, *octet* provides an unambiguous term.

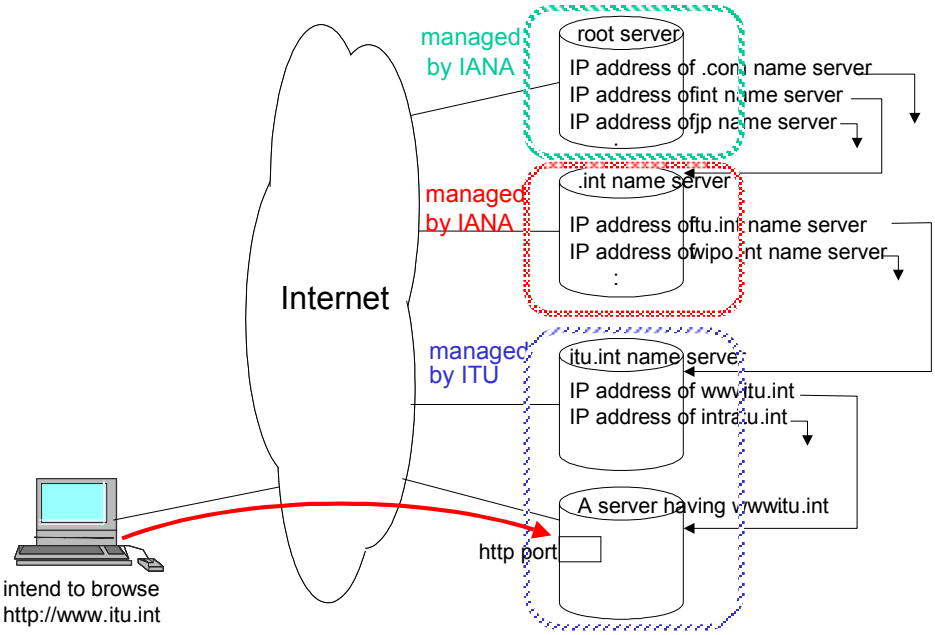


Figure 2 – How domain names are resolved

From the standpoint of the relationship between the Internet user and the DNS, a domain name is handled as shown in Figure 3 (below). With current protocols restricted to working with ASCII, users would be forced to limit themselves to using the ASCII characters permitted in domain labels. This effectively means that ASCII domain names would be used at all points, from the user to the website. However, with the introduction of multilingual domain names, the protocol between the user and the personal computer would be based on non-ASCII characters, while the current DNS is based on ASCII.

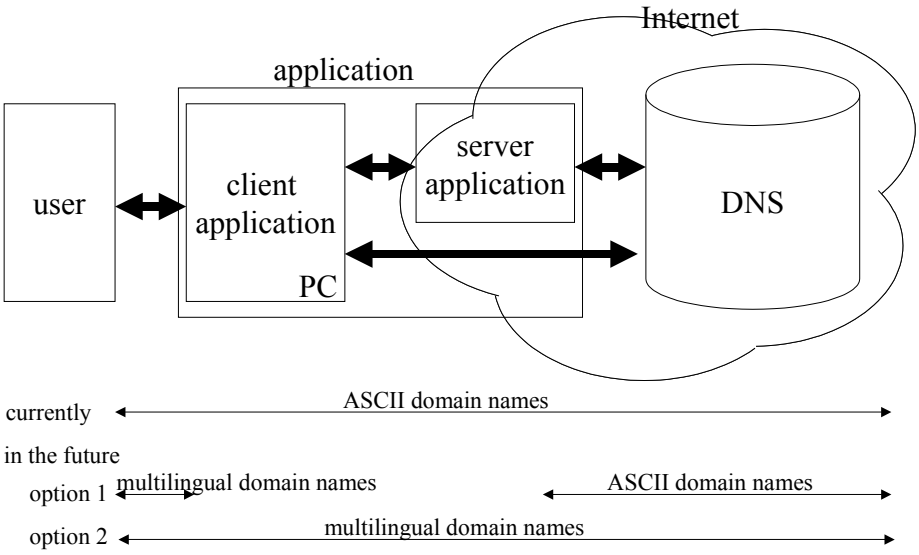


Figure 3 – Where multilingual domain names are recognized

The key technical questions are:

- How should non-ASCII codes be represented?
- Where should non-ASCII codes be recognized, in the client application or in the DNS server?
- What is the technical mechanism that maps multilingual domain names to current DNS technology?

The basic concepts of IETF's work on this problem are described in § 0 below. The first question is discussed in § 3.2; the second is discussed in § 3.3; the third is discussed in § 3.4-3.6.

3.1 Basic concepts of the IETF Working Group

As the DNS is one of the fundamental technologies deployed in the Internet, compatibility and interoperability of multilingual domain names is of critical importance. Any new technology should entail a minimal number of changes to the Internet, should coexist with the current domain names, and should allow a domain name to consistently designate the same unique entity throughout the Internet. This is achieved by means of appropriate standardization and compliance to standards by systems in the Internet. Standardization involves establishing a common protocol that promotes interaction between entities within the Internet; in the case of the DNS, this is carried out by IETF.

In January 2000, IETF set up the IDN Working Group for the standardization of multilingual domain name technology. Its charter can be summarized as follows[11]:

– the goal of the group is to specify the requirements for internationalized access to domain names and to specify a standards track protocol based on those requirements;

– a fundamental requirement in this work is not to disturb the current use and operation of the domain name system anywhere to resolve any domain name;

– the group will not address the question of what, if any, body should administer or control usage of names that use this functionality.

In processing the standardization of the technology of multilingual domain names, the basic requirements of the Internet Architecture Board (IAB)[12] are as follows:

– RFC2825: Preservation of compatibility with current domain names;

– RFC2826: Preservation of uniqueness of domain name space;

– The Internet must not be divided into islands.

3.2 Character codes of multilingual domain names

Only the letters of the basic Latin alphabet (non case-sensitive A-Z), the decimal digits (0-9) and the hyphen are permitted in domain names [RFC 1034[13] and RFC1035[14]]. Multilingualization of domain names entails the extension of this character set to one that includes non-ASCII characters.

---

11 See http://www.minc.org/events/yokohama2000/ppt/IETF_JamesSeng.ppt.

12 See http://www.iab.org.

13 See http://www.ietf.org/rfc/rfc1034.txt.

14 See http://www.ietf.org/rfc/rfc1035.txt.

To ensure that applications uniformly recognize and process the multilingual domain names, encoding and representations of such non-ASCII characters must be uniquely determined. To do this, a globally agreed-upon code set is needed for multilingual domain names so that all applications and systems relating to domain names scattered throughout the Internet cooperate with each other using a globally unique code set.

However, for various historical reasons, the fact is that many language scripts currently used in information systems have adopted national or proprietary standards. To give an example, the most popular Japanese character set used in Japanese devices is based on Japanese Industrial Standards (JIS) X 0208 and X 0201. Therefore, many PCs, personal digital assistants (PDAs), as well as Internet-enabled mobile phones in Japan can only display JIS and ASCII characters. This causes overlapping of codepoints and a lack of ability to uniquely define a type of encoding used, resulting in compatibility problems.

The most promising solution is the adoption of Unicode[15] (ISO/IEC 10646), which specifies the code sets of many scripts and therefore languages. Although Unicode may be the best current solution, it may have to be further developed to accommodate actual usage. Furthermore, when an application does not directly apply to Unicode for a representation of local characters, conversion of commonly used local code sets to and from Unicode is required somewhere in the computing environment.

There is also the possibility that mere adoption of Unicode will not be appropriate for domain names. For example, some Chinese characters have two representations – a traditional Chinese character and a simplified Chinese character. The fact that the correspondence between a traditional Chinese character and a simplified Chinese character is not one-to-one makes the situation much more complicated. Furthermore, although they are usually used in mainland China in place of traditional Chinese characters, simplified Chinese characters are seldom used in Taiwan or Hong Kong. The point has been raised as to whether or not these two character sets should be considered as one[16]. Some have argued that they should be treated as different characters if domain names are simply identifiers. Others argue that they should be regarded as the same characters if, in reality, domain names correspond to the identity of entities. Even if they are regarded as the same characters, other issues may arise in respect of whether it is merely a local code issue or a universal protocol issue; and whether a distinction should be made for such characters where used for traditional or simplified Chinese.

3.3 Client-side versus server-side solutions

As regards the question of *where* non-ASCII codes should be recognized in Figure 3, approaches to the solution of this problem are typically based on one of the following scenarios:

3.3.1 Client-side solution

In a client-side solution, translation between the multilingual script and the ASCII- compatible representation is performed in the user applications (e.g. a web browser). The client application translates multilingual scripts into ASCII strings, which can then be processed in the current Internet: the domain names are subsequently processed as ASCII domain names throughout the

---

15 See http://www.unicode.org.

16 This is often referred to as the TC/SC equivalence problem.

Internet. This category includes the case of an application that consists of both client-side and server-side software. But for the sake of convenience, the term "client-side" is used in the interest of consistency with the ICANN survey report[17].

Technically, a client-side solution is needed regardless of which approach is chosen. It is unlikely that an ASCII-only application will work immediately with multilingual domain names. Some form of upgrade will be necessary, either through provision of fonts, input methods or additional technical functionality to support internationalization.

3.3.2 Server-side solution

In a "server-side" solution, domain names are sent natively over the Internet by the client application in local encoding, such as UTF-8[18], GB or BIG5[19], or Unicode. Applications and services communicate with each other using non-ASCII domain names all the way along the path between them (sometimes referred to as "on the wire"). Note that the original implementations of IDN were actually proxy server solutions that intercepted local encoding from client applications and converted the encoding into an ASCII-compatible encoding so that the DNS server remained unaltered.

Some of the services, experiments and test beds currently deployed employ client-side, and others server-side solutions IETF has adopted standards based on a pure client-side solution. This is supported by the following arguments:

- First, the DNS is a huge, robust and distributed database, but one which works on the basis of a delicate balance. Too many pieces of Internet software and protocols make use of the DNS in its current form. Other than by carrying out exhaustive testing, modification of the DNS at a fundamental level may lead to a collapse of the entire system. In view of this, many Internet engineers think it is inadvisable to modify the core of the DNS, which may have disastrous consequences for the Internet. Therefore, it is argued that a client-side solution not requiring any significant changes to the DNS is much safer for the stability and growth of the Internet.

- Second, in view of the rapidly growing demand, the ability to use multilingual domain names should be made available as soon as possible. In general, deployment of servers takes much longer than deployment of client applications. In client-side solutions, only the entities intending to communicate using multilingual domain names must be prepared for multilingual domain names. Conversely, server-side solutions require that all components along the communications route, including the client, server and anything else in between, must be prepared for multilingual domain names. The deployment of a server-side solution may require reconfiguration of all of the servers throughout the Internet to accommodate the multilingual scripts, which would take a considerable amount of time.

---

17 See http://www.icann.org/committees/idn/final-report-28aug01.htm.

18 See http://www.ietf.org/rfc/rfc2279.txt.

19 GB and BIG5 are coding schemes for Chinese characters.

- Third, given the non-negligible time it would take to achieve server-side deployment, this approach could result in limited areas only of the Internet being able to accommodate multilingual domain names. This might lead into separation of the Internet into "islands" and the emergence of alternative roots[20]. This may result in confusion and inconsistency for users.

3.4 Standardization for compliance with the current DNS

Ideally, in technical standardization, all languages and characters that could potentially be used in multilingual domain names should be taken into account. However, many issues relating to a particular language are only identifiable by those who use the languages and characters in practice. Standardization will therefore be evolutionary, as all issues involved cannot be identified and solved at this time.

IETF has adopted standards based on a client-side solution, as described above. The technical elements that need to be standardized include:

- Preparation of internationalized host names (Nameprep);
- ASCII compatible encoding (ACE);
- Internationalizing host names in applications (IDNA).

In Nameprep, multiple multilingual string representations, which should be regarded as the same string, are combined into one string. After Nameprep, ACE converts the multilingual representation to an appropriate ASCII domain name. The roles of Nameprep and ACE are shown in Figure 4 (below). The architecture for application software to apply these two translations to the original multilingual domain names so as to be properly incorporated into the current Internet is called IDNA.

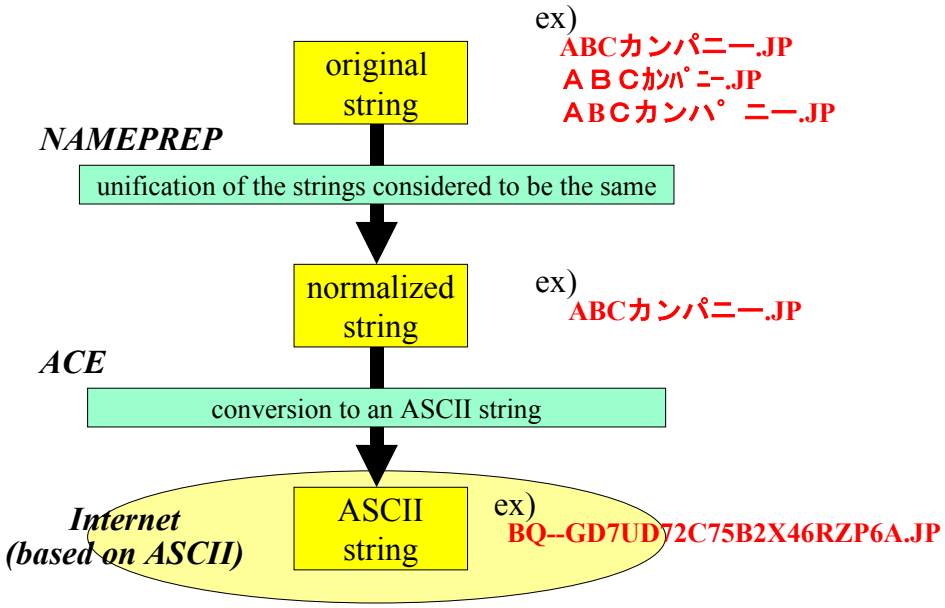


Figure 4 – The roles of Nameprep and ACE

20 Alternative root: a method of creating a separate domain name space from that of ICANN, by operation of proprietary root servers.

Preparation of internationalized host names (Nameprep)

The main functions of Nameprep are:

- Case folding: as the difference between uppercase letters and lowercase letters is insignificant in constituting ASCII-based domain names, the cases are merged into one form. This needs to be done not only for ASCII letters but also for non-ASCII letters. Other types of case folding may be needed for non-ASCII characters. Case folding is also called "a map" because it maps (a) character(s) onto (an)other character(s) which is(are) regarded as equivalent. The specifications of case folding rely on Unicode Technical Report #21[21].
- Normalization: many characters have several representations even if the human eye can see no difference. In domain names, these characters should be normalized into one representation in order to be regarded as the same character. For example:
  - the ligature "ä" and "a +¨" are canonically equivalent;
  - full-width "Ａ" and half-width "A" are compatibly equivalent.

  The specifications of normalization rely on Unicode Standard Annex #15[22].
- Prohibition: many characters in the Unicode character set are control sequences, formatting sequences or spacing characters, which are not appropriate for domain names.

The above demonstrates that Nameprep translates various representations that are regarded as the same string into a unique representation in the multilingual string space. If the outputs of Nameprep are the same, input strings are regarded as the same domain name. If the outputs are different, they are regarded as different domain names. To meet this goal, Nameprep should precede ACE. IETF is nearing the final stages of Nameprep standardization.

3.5 ASCII compatible encoding (ACE)

ACE encodes a non-ASCII string represented in Unicode into an ASCII string, which complies with the ASCII domain name format. This enables multilingual domain names to be properly processed as corresponding ASCII domain names. At the 49th IETF meeting in November 2000, the IDN Working Group was steered in the direction of choosing ACE, although arguments claiming the necessity of UTF-8 have still been a matter of debate in mailing list discussions. IETF is now reaching the final stages of ACE standardization.

RACE (Row-based ASCII compatible encoding)[23] was one of the earlier candidates among the proposed ACE algorithms. It was used in the registration and resolving services provided by, *inter alia*, VeriSign Global Registry Services (VGRS)[24] and Japan Network Information Center (JPNIC)[25]/Japan Registry Service (JPRS)[26]. Following RACE, various other algorithms were proposed and were evaluated by engineers as to their advantages and disadvantages using actual multilingual domain names registered in various test bed scenarios.

---

21 See http://www.unicode.org/unicode/reports/tr21/.

22 See http://www.unicode.org/unicode/reports/tr15/.

23 See http://www.i-d-n.net/draft/draft-ietf-idn-race-03.txt.

24 See http://www.verisign-grs.com.

25 See http://www.nic.ad.jp.

26 See http://jprs.jp.

At the August 2001 IETF meeting, an ACE system called AMC-ACE-Z[27] received significant support owing to its better compression efficiency. For example, AMC-ACE-Z can represent at least 18 Japanese characters as a domain label, while RACE can represent up to 17 such characters. As an example, the ASCII output strings for "日本語ドメイン名例JP" (meaning Japanese domain name example) produced by RACE and AMC-ACE-Z are respectively[28]:

– RACE: BQ--3BS6KZZMRKPDBSJQ4EYKIMHTKQGU7CY;

– AMC-ACE-Z: ZQ--ECKWD4C7CU47R2WFQW7A0ECL32K.

An ACE encoding maps multilingual domain name space into a subspace of ASCII domain names. In the reverse direction, it should be possible for the ASCII domain name using ACE to be uniquely re-mapped to a multilingual domain name. A subspace should therefore be reserved for multilingual domain names within the existing ASCII domain name space, as shown in Figure 5 (below). For this, a prefix, suffix or "tag" for a resulting ACE string needs to be defined. In this case, all strings having such an ACE tag will constitute a subspace defining multilingual domain names. The ACE tag has to be chosen taking into account the following conditions: there must be a 0 per cent possibility of coincidental existence of ASCII domain names with such a prefix or suffix, and the length of the prefix or suffix must be short enough to leave maximum space for long multilingual domain names. Under these conditions, the prefix or suffix could be simple strings, i.e. "??--", or "--??", where ? is an alphanumeric character. For example, if RACE is chosen, domain names starting with prefix "bq--" would indicate a multilingual domain name.

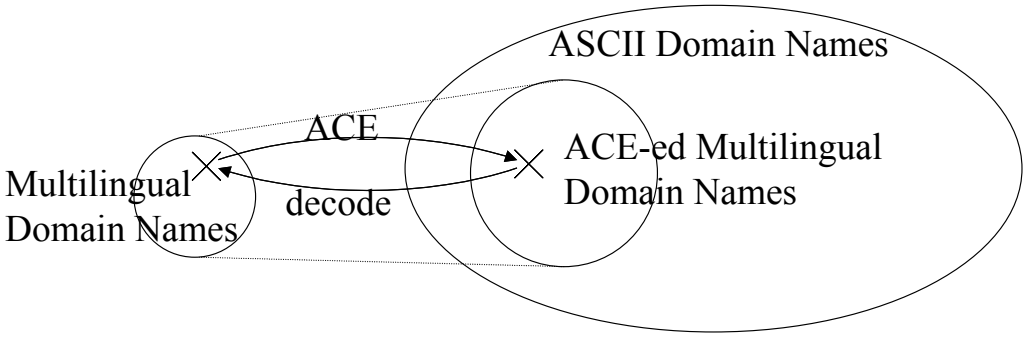


Figure 5 – Mapping from multilingual domain name space to subspace of ASCII domain name space

ACE has been standardized by IETF. Nevertheless, ASCII domain names should not be registered in the subspace reserved for multilingual domain names. For example, registration of ASCII domain names starting with "bq--" must be blocked if RACE is chosen. Second, as a domain label should not exceed 63 ASCII characters, it can only accommodate a limited number of multilingual characters – for example, 18 Japanese characters. This will restrict multilingual domain labels to being shorter in length than ASCII domain labels. In addition, deeper domain hierarchies cannot be achieved, as the length of a full domain name cannot exceed 255 characters.

---

27 See http://www.ietf.org/internet-drafts/draft-ietf-idn-amc-ace-z-01.txt.

28 The prefix of AMC-ACE-Z is assumed as "zq--" although it has not yet been specified.

3.6 Internationalizing host names in applications (IDNA)

To use the Internet as it currently stands, translations by Nameprep and ACE should be carried out before sending the domain name "down the wire" to the DNS or application server. The application architecture in which Nameprep and ACE are performed following the mapping from local code to Unicode is called IDNA, as shown in Figure 6 (below). At the August 2001 IETF meeting, many attendees supported the IDNA client-side solution.

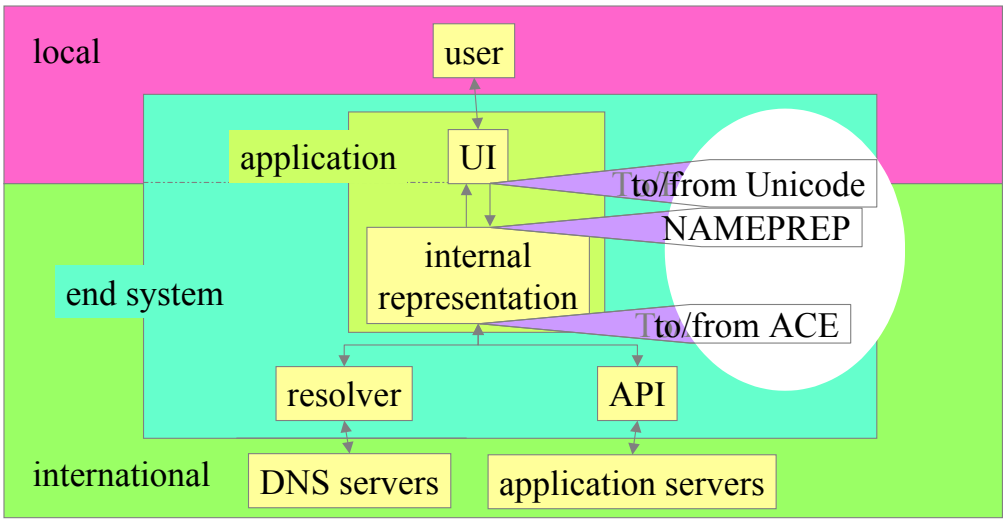


Figure 6 – The architecture of IDNA

3.7 Impact on the DNS structure

A basic requirement of the DNS is the ability to identify entities on the Internet. To meet this demand, the structure of the hierarchical domain name space must be administratively coordinated. This is currently performed by ICANN with oversight by the United States Department of Commerce[29]. This means that the authority of the DNS hierarchy root shown in Figure 1 on page 5 is ICANN. This root is sometimes called the *authoritative root*.

---

29 The stated policy of the United States Administration has been to transfer management of the DNS to ICANN. In practical terms, *inter alia*, this would entail transferring both policy and technical control of the authoritative domain name system server, where existing or new top level domains are defined and maintained, to ICANN or its subsidiary, IANA. On later occasions, the US Department of Commerce has stated that they have "no plans to turn over policy control of the authoritative root server" (see http://www.gao.gov/new.items/og00033r.pdf). Currently, the primary root server, "a.root-servers.net", is maintained by VeriSign Global Registry Services, a subsidiary of VeriSign, Inc. (http://www.verisign-grs.com), located in the United States. The final authority for change control of the *root zone file* (e.g. addition, modification or deletion of top level domains) is held by the United States Department of Commerce. See *Cooperative Agreement No. NCR-9218742, Amendment 11*, (Oct. 6, 1998) where it is stated: "While NSI continues to operate the primary root server, it shall request written direction from an authorized USG official before making or rejecting any modifications, additions or deletions to the root zone file. Such direction will be provided within ten (10) working days and it may instruct NSI to process any such changes directed by NewCo when submitted to NSI in conformity with written procedures established by NewCo and recognized by the USG." See http://www.ntia.doc.gov/ntiahome/domainname/proposals/docnsi100698.htm.

3.7.1 Alternative roots

An increasing number of software solutions are now offering so-called *alternative roots*. These encapsulate the public DNS and extend it by offering additional top level domains, thereby enabling Internet users to view domain names other than those recognized by ICANN. Unless there is some sort of global administrative coordination of top level domains[30], this could result in a fragmentation of the Internet into disparate name spaces.

In response to this concern, ICANN has recently issued position papers[31] arguing the need for a unique authoritative public DNS root, which should be managed as a public trust, and asserting that ICANN has assumed this public trust role. There is general agreement among technical experts that a unique public name space is necessary in order to maintain the integrity and global connectivity of the DNS. Here, a related statement of the Internet Architecture Board (IAB), documented in RFC 2826[32], is worth citing:

> *"To remain a global network, the Internet requires the existence of a globally unique public name space. The DNS name space is a hierarchical name space derived from a single, globally unique root. This is a technical constraint inherent in the design of the DNS. Therefore it is not technically feasible for there to be more than one root in the public DNS. That one root must be supported by a set of coordinated root servers administered by a unique naming authority".*

While the arguments stem from a variety of different perspectives as well as economic interests, there appears to be general agreement on the need for a DNS name space visible to a maximum of Internet users: a severely fragmented name space is of little value to anyone. As evidence, the managers of "unsanctioned" top level domains in alternative root systems have argued both a) for inclusion in the "authoritative root" and b), against ICANN introducing TLDs identical to their TLDs used in alternative inclusive roots. They also contend that it is possible to have an administratively coordinated root function that avoids collision between different top level domains based on multiple root systems. This suggests that the debate remains more about *who* is the *root* or *coordinating naming authority* rather than about the merits of a single coordinated name space.

3.7.2 Multilingual domain name resolution by alternative roots

Multilingual domain names cannot be supported by existing standard specifications. The deployment of multilingual domains with proprietary technology could encourage the emergence of alternative roots. From the user's perspective, this could result in one domain name referring to completely different entities in different name spaces under different root structures. In particular, because it is an extremely long process to introduce new top level domains, there is some question as to whether the market will simply overtake the current administrative arrangements.

One argument put forward by proponents of alternative roots for the resolution of multilingual domain names is that ICANN's authority is principally drawn from the United States having historically been considered the source of ASCII-based Internet domain names. It is argued that, as multilingual domain names originated elsewhere, alternative roots supporting multilingual top level domains may be more justifiable than some contend. Other proponents support the concept of an

---

30 Note that there does not necessarily have to be technical coordination.

31 See http://www.icann.org/stockholm/unique-root-draft.htm, http://www.icann.org/icp/icp-3-background/lynn-statement-09jul01.htm, and http://www.icann.org/icp/icp-3.htm.

32 http://www.ietf.org/rfc/rfc2826.txt.

"inclusive" root, which allows for top level domains not under ICANN's authority to be used for national or commercial deployment. In this case, as long as users point their applications to the inclusive root, they will be able to resolve ICANN domain names as well as non-ICANN domain names – giving direct access to new multilingual top level domains. Again, some see problems with this model in that there may be more than one party arguing that it manages the "inclusive root". This could lead to name space collisions that would need to be resolved by negotiation, arbitration, or possibly litigation. In the worst instance, this may lead to fragmentation of the Internet name space as predicted by the IAB in RFC 2826.

3.7.3 Pseudo-roots

There is a somewhat more subtle way to create a multilingual domain name space. This is achieved by making an "imaginary non-ASCII top level domain" in the authoritative domain name space. This method, called *zero level domain*, was suggested in IETF draft documents as early as in 1997. It conceals the upper part of the domain name space, assuming one top node of the unconcealed space as a virtual top level domain, and using the subspace governed by the virtual top level domain as the entire domain name space. For example, after creating a space {non-ASCII-string}.TLD under the authoritative top level domain ".TLD", users can access the Internet by using domain names like xxx.{non-ASCII-string} if the users' client application automatically detaches and/or re-attaches ".TLD" with each access to the Internet. This can make a (virtual) multilingual top level domain for users of such client applications. Even if zero level domains are somewhat more palatable than alternative roots, users still need to be conscious of the problem that different entities may apparently be designated by the same domain name if different client applications are used.

It is not multilingual domain names *per se* that lead to the creation of alternative or pseudo roots. Rather, it is the combination of commercial interests and user demand for early deployment of new TLDs; whether in English or multilingual scripts. If policies for the creation of new TLDs are able to meet user and commercial demands, the risk of fragmentation is reduced. This suggests that it is extremely important that ICANN find methods to address this demand effectively.

3.8 Policy and coordination issues raised by multilingual domain names

Technology is always the start of a process, not the end. Before a technology can be fully employed, it needs to be supported by policy and business. This section discusses the major policy issues related to multilingual domain names.

3.8.1 Consideration of multilingual domain names in various TLDs

In the present ASCII-based DNS, there are two basic kinds of top level domains: generic top level domains (gTLDs), such as .com and .info, and country code top level domains (ccTLDs), such as .uk and .jp. There are less than 15 gTLDs, and their policies are, for the most part[33], controlled by ICANN. There are currently about 245 ccTLDs[34], and the policies of each are, for the most part, controlled by a ccTLD management organization, typically in the respective country or region[35].

---

33 In fact, some "gTLDs", such as .mil, .gov, and .edu are not clearly under policy control of ICANN.

34 See http://www.iana.org/cctld/cctld-whois.htm.

35 However, there are a significant number of cases where management control of a ccTLD is outside the related country or territory.

3.8.2 Potential types of multilingual domain names

Several kinds of multilingual domain names may emerge, depending on the kind of TLDs they come under or represent. They could be same-language, same-script, or mixed-language, mixed-script, multilingual domain names. These might be represented as follows:

{non-ASCII-string}.{ASCII-ccTLD};

{non-ASCII-string}.{ASCII-gTLD};

{any-string}.{non-ASCII-ccTLD};

{any-string}.{non-ASCII-gTLD}.

The above notation is not formally defined here, as it is sufficient to have a grasp of the underlying principles. Furthermore, it is entirely possible that other types of multilingual TLDs could emerge. For example, language-related TLDs that indicate the language of the associated domain names: for example, {Chinese string}.{CHINESE} or {Japanese string}.{JAPANESE}, where "CHINESE" and "JAPANESE" represent the Chinese and Japanese characters for the name of the language.

3.8.3 Technical and non-technical issues

While obstacles to implementation of these multilingual domain names are mainly non-technical ones, a potential significant technical hurdle is the increased load on the DNS. This is because a {non-ASCII-string} is unusually long when encoded into an ACE format. Other technical hurdles include the necessity of multilingualization of related systems such as the *Whois* system, which displays associated attributes of domain names (e.g. registrant information). Non-technical obstacles, on the other hand, include:

issues related to responsibility for domain name registration;

issues to be resolved in the process of registration and usage.

The second of these obstacles will be discussed in subsequent sections. The first is described in this section by classifying the issues based on the kinds of top level domains.

3.8.4 Mixed multilingual.ASCII domain names

A number of organizations are already operators with regard to {non-ASCII-string}.{ASCII-ccTLD} and {non-ASCII-string}.{ASCII-gTLD}. For example, VGRS is offering {Chinese-string}.com registrations, and JPNIC/JPRS is offering {Japanese-string}.jp. These services are provided on the basis that the organization involved has "authority" over a ccTLD or gTLD and, if the DNS is internationalized, that same authority is sufficient to delegate {non-ASCII}.{ASCII} multilingual domain names under the corresponding TLD.

3.8.5 Multilingual.multilingual domain names

One example of {non-ASCII-ccTLD} is ".日本" ("日本" represents "Japan" in Japanese Kanji). If a {non-ASCII-ccTLD} and its management organization are coordinated with ICANN, there may be no problems regarding authority decisions as long as there is no dispute as to that organization being the legitimate authority. In the case of Japanese, therefore, as the seat of the language is in Japan, and no other country has designated the Japanese language as its official language, that decision is a clear-cut one. However, it should be noted that the same Japanese characters "日本" are also used in the Chinese character set and their glyphs are identical. Those particular characters could not normally also be designated as Chinese and assigned to another organization. The Japanese language also uses two other scripts, namely Katakana and Hiragana, but fortunately, as these scripts are not used by other countries, they are unlikely to give rise to complications. For other languages, the issues will be much more complex.

If a country or region corresponding to a country code has two or more official languages, it may need to decide which language is used to represent its country "code"{non-ASCII-ccTLD}, assuming that "country code" has an equivalent in that language. Even if a rule is established that two or more {non-ASCII-ccTLD}s can be assigned to one country or region, the issue arises as to the number of {non-ASCII-ccTLD}s to be assigned to the country or region for however many languages are official or are used in that jurisdiction. For example, in the case of India, there are more than 20 commonly used languages, each with their own script.

An example of {non-ASCII-gTLD} is ".企業" ("企業" is a traditional Chinese character string which means "a company"). One problem is that multiple languages may share characters. Because of this, identical strings may represent the same or different meanings in different languages. Also, similar characters exist in different languages. For example, both China and Japan use the word "企業", so people cannot tell whether the top level domain "企業" is in Chinese or Japanese. In other words, multilingual domain names may confuse people in spite of the goal to make domain names more memorable. It is very hard to decide who (and in which country) should be designated to manage these kinds of top level domains. Given the difficulties experienced when simply introducing new ASCII top level domains, it is not hard to imagine the challenges involved when introducing multilingual top level domains.

4 What are the languages that constitute multilingual domain names?

One of the issues that should be examined is the definition of languages from the viewpoint of multilingual domain names. Some languages have two or more kinds of scripts, and some languages have mixed scripts in the written form of the language. For example, Chinese Han characters, Japanese proprietary katakana and hiragana, Arabic numbers, and the English alphabet are all mixed in Japanese written documents. In this case, can all the possible strings in Japanese written documents be multilingual domain names? In which language are Chinese Han characters when used as a multilingual domain name in a Japanese document?

In addition, local rules such as the unification of traditional Chinese characters and simplified Chinese characters, as described in the last paragraph of § 3.2, will need to be addressed: even from the perspective of "whether they are the same language or different languages." For example, will the "folding" (see Preparation of Internationalized Host Names (Nameprep) under § 3.4) of traditional and simplified Chinese Han characters affect the usage of Han characters in other non-Chinese languages?

4.1 Who is the language authority for multilingual domain names?

A further question is whether the issues described in § 4 above are local issues or international issues. In the interest of eliminating confusion for the users, some advocate that the rules with respect to multilingual domain names should be the same even if they are under different top level domains. Therefore, a single domain name registry[36] should not be the ultimate authority for the

---

36 The registry of a domain name is an organization that is responsible for managing the registration of domain names under the domain name. For example, the registry of .com is VGRS.

rules on multilingual domain names. As an example, should the representation rules and conversion rules for Chinese domain names in .com and in .cn[37] be the same? In this case, the rules definition for Chinese multilingual domain names is inherently an international issue. However, should the international community that does not use the Chinese language be able to define localization issues for Chinese speaking people? And as the Chinese language is diasporic, used in different jurisdictions, countries and economies, how localized are these decisions?

It is extremely difficult (if not impossible), for those whose language is not concerned by this discussion to understand the sensitivity surrounding these kinds of issues. Understanding whether the issues in § 4 above are code problems or protocol problems is very difficult. But this understanding is necessary to lead to a decision as to the extent to which such issues need to be standardized internationally. Someone must decide which issues exist and how they are to be resolved. Perhaps a first step is resolving who is the relevant decision-making authority.

4.2 Matrix of authority

So far, a number of combinations of country/economy, language, script, and encoding systems have emerged and examples are listed in Table 1. Table 1 suggests that a "one size fits all" policy approach is very unlikely to succeed.

4.3 Models for a matrix of authority

The above table indicates that it will be important for language stakeholders to coordinate among themselves. Where needed, regional or international organizations may be appropriate forums. Generally, as a matter of principle, it seems appropriate that decisions affecting language users should be made by the language users themselves, where possible. Table 2 suggests some of the models that may need consideration.

Table 1

Script	Language	Encoding	Country/economy	Comment on administrative model
Chinese Traditional and Simplified	Chinese	GB BIG5 HW	China, Hong Kong, Taiwan, Macau, Malaysia, Singapore USA, Canada, UK, etc.	Diasporic language Official language of several economies Chinese Domain Name Consortium (CDNC)?
Hiragana Katakana Kanji	Japanese	JIS SJIS EUCS	Japan	>90% Japanese speakers in Japan JDNA/JPRS/JPNIC are obvious candidates Kanji needs coordination with CJK countries

37 .cn is the ISO 3166 alpha-2 country code for the People's Republic of China.

Table 1 (end)

Script	Language	Encoding	Country/economy	Comment on administrative model
Hangeul	Korean	KSC	People's Republic of Korea (South) Democratic People's Republic of Korea (North)	>80% Korean speakers in Koreas KRNIC is a potential candidate Hanji needs coordination with CJK countries
Arabic	Arabic Urdu Farsi Jawi		Algeria, Bahrain Djibouti, Dubai Egypt, France Jordan, India, Iraq Iran, Kuwait Lebanon, Libya Morocco, Malaysia Mauritania, Oman Palestine, Pakistan Qatar, Saudi Arabia Spain, Somalia Sudan, Syria Tunisia, Turkey UAE, Yemen and others	Diasporic language Multi-Country official language Arabic Internet Names Consortium (AINC) Arabic Languages WG, MINC Urdu Language WG, MINC
Tamil	Tamil	TAM TAB TSCII Many other proprietary fonts	India (Tamil Nadu state), Mauritius, Sri Lanka, Malaysia, Singapore, USA Canada, UK, etc.	Diasporic language minority in all countries Official language in a few Tamil Nadu State in India is recognized as seat of Tamil Language International Forum for IT in Tamil (INFITT) Working Group WG02
Thai	Thai	TSC	Thailand	>90% of Thai speakers in Thailand
Khmer	Khmer	Many proprietary fonts	Kingdom of Cambodia Thailand (Surin) Vietnam	>90% of Khmer speakers in Cambodia Official language in one
Lao	Lao	A few proprietary fonts	Lao PDR Thailand	10 times more Lao speakers in Thailand
Cyrillic	Russian		Russia and about a dozen other former USSR republics	>90% in Russia Russia recognized as seat of Russian language
Hebrew	Hebrew		Israel	>95% in Israel

Table 2

Model	Language
One language-one script-one country model	Hebrew, Thai, Russian
One language-one script-no country model	Tamil
One language-one script-many countries model	Arabic, Lao
One script-many languages-many countries model	Arabic-Urdu-Farsi-Jawi system, Han
One language-many scripts-one country model	Japanese, Korean
One language-many scripts-many countries model	Chinese (TS-SC), Urdu (Arabic-Hindi)
One country-many scripts-many languages	Many countries

5 Summary

To make multilingual domain names fully usable on the Internet, technical standardization is but the tip of the iceberg. In order to meet user requirements, it will be necessary to complete the following steps:

standardization of technology;

policy and coordination of registration and management rules;

deployment of applications and name servers.

The relationship between these steps, necessary for deployment of multilingual domain names, is illustrated in Figure 7 below.

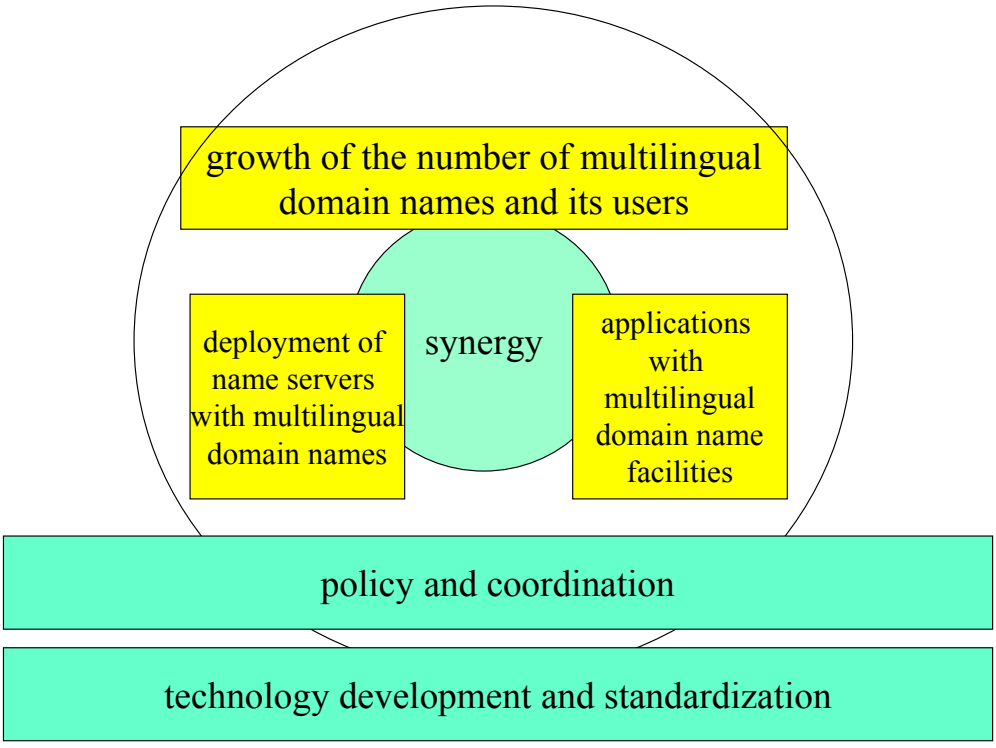


Figure 7 – The basis of multilingual domain name growth

As noted above, the base technical standards for IDN have been approved by IETF. However, as all languages of the world have yet to be considered, the specifications of the standard may need to evolve further. In addition, as the DNS itself is evolving, longer-term solutions such as server-based solutions or additional software layers may emerge (e.g. keywords) and prove to offer better solutions.

The policy and coordination issues discussed in § 3.8-4.3 above will need to be resolved in the very near future. However, with national, regional and international cooperation, solutions can be found.

The deployment of applications and name servers must rely on the dynamics of the business sector. In order to achieve satisfactory usage, it is important to promote deployment of both servers and applications. It is vital that application development be catalyzed and widely promoted. As one practical example, the Japanese Domain Names Association (JDNA), which was established in July 2001, has Japan-based members such as application vendors, network service providers and domain name registries. Within JDNA, necessary local specifications such as detailed representation of URLs and e-mail addresses will be determined.

To summarize, there is substantial market and user demand for multilingual domain names. To satisfy this demand, the whole environment needs to be developed to take into account technology standardization, policy and administrative arrangements, as well as new applications. The future of multilingual Internet names is imminent. We should not underestimate the significance of this activity, as it is part of a far nobler goal: the ongoing internationalization of the Internet.

Implementation of IDN raises some very complex issues. In particular, before accepting IDN-based domain names, registries should define a policy for what scripts they accept, that is, a policy for which subset of Unicode they accept. These issues are discussed in the Internet Draft "Internationalized Domain Names Registration and Administration Guideline for Chinese, Japanese and Korean" available at http://www.ietf.org/internet-drafts/draft-jseng-idn-admin-04.pdf. This document has not been approved by IETF and is currently undergoing review.

The Internet Draft "National and Local Characters in DNS TLD Names" available at http://www.ietf.org/internet-drafts/draft-klensin-idn-tld-00.txt reviews some of the motivations for IDN and the constraints imposed by the Domain Name System, and suggests an alternative, local translation, that may solve certain problems. This document has not been approved by IETF and has been offered for discussion.

The Internet Draft "Japanese characters in Internationalized Domain Name label" available at http://www.ietf.org/internet-drafts/draft-yoneya-idn-jpchar-01.txt provides guidelines to any DNS zone administrator who accepts Japanese as an IDN label. This document has not been approved by the IETF and has been offered for discussion.

ICANN has also published several reports and papers which discuss various aspects of IDN. See "IDN Committee Final Report to the ICANN Board" at

http://www.icann.org/committees/idn/final-report-27jun02.htm and the presentations referenced at the bottom of http://www.icann.org/committees/idn/

Attachment 14

ENUM

Table of contents

ENUM[1]

1 Introduction

The intent of this section is to provide some tutorial material to facilitate discussions of the requirements for the successful global implementation of ENUM, as described in IETF RFC 3761 (formerly RFC 2916).

Additional tutorial material can be found in Supplements 3 and 4 to ITU-T Recommendation E.164.

The ENUM protocol depends upon mapping parts or all of the ITU-T Recommendation E.164 international public telecommunication numbering plan into the Internet Domain Name System (DNS). At first glance a simple protocol, ENUM nevertheless raises a number of regulatory and policy issues.

One of the technical challenges raised by the ever-closer integration between circuit-switched and packet-switched networks is how to address calls that pass from one network service to another. Generally, it is assumed to be desirable that an integrated global subscriber access plan exists. For example, the same ITU-T E.164 telephone number would reach a subscriber regardless of whether IP-based or PSTN network technologies are used.

It is now widely possible to originate calls from IP address-based networks to other networks, but it is uncommon to terminate calls from other networks to IP address-based networks. Rather, calls are generally terminated on the PSTN, so the called party can only use a terminal device connected to those networks. In order to access a subscriber on an IP address-based network from the PSTN, some sort of global numbering/addressing scheme across both PSTN and IP address-based networks needs to be developed and implemented. ENUM could provide that numbering/addressing scheme.

This section is intended for readers who have a basic understanding of ENUM, the ITU-T E.164 international public telecommunication numbering plan and DNS. Section 4.2 provides a technical overview of how DNS works.

2 Background

The ENUM protocol, published in the standards-track document RFC 3761 (formerly RFC 2916), proposes mapping ITU-T Recommendation E.164 telephone numbers into DNS. An overview of how DNS works is given in § 4.2.

The ENUM protocol involves associating telephone numbers with network resources or services in DNS. For example, a specific E.164 number can be coupled with, *inter alia*, other E.164 numbers, such as fax and mobile numbers, voice mail systems, an IP telephony address, an e-mail address, a website or any other resources or services that can be identified through a widely-used Internet addressing scheme called uniform resource identifiers (URIs).

---

1 This section is based on a tutorial paper, ITU/T Study Group 2 Information Document 10.

he ENUM protocol requires that related services be looked up through a convention of one-to-one reverse mapping of digits in an ITU-T Recommendation E.164 number into separate DNS "zones" – which are then concatenated with another domain. The Internet Architecture Board (IAB), has proposed that this domain be "e164.arpa". At this time, there is not yet final consensus by ITU Member States on the usage of the e164.arpa zone or of a particular operator of this domain. With that disclaimer, the domain "e164.arpa", referenced in RFC 3761, is used below solely for the sake of discussion.

3 Description of ENUM

ENUM is a protocol which is the result of work by IETF's Telephone Number Mapping working group. The charter of the ENUM working group was to define a DNS-based architecture and protocol for mapping an ITU-T Recommendation E.164 telephone number to what are known as uniform resource identifiers (URIs) . A stable standards-track version of the ENUM protocol has been published as RFC 3761. URIs are strings of characters that identify resources such as documents, images, files, databases, e-mail addresses or other resources or services in a common structured format. The most commonly known types of URIs are uniform resource locators (URLs), which are used to locate resources using the worldwide web. For example, http://www.itu.int/infocom/enum/ is the URL for the ITU website providing an overview of ITU ENUM activities.

The ENUM protocol uses what are called naming authority pointer (NAPTR) DNS resource records as defined in RFC 2915 in order to identify the available methods or services for contacting a specific node identified through a Recommendation E.164 number. The ENUM protocol defines and uses a specific type of NAPTR service with the mnemonic "E2U" (E.164 to URI resolution).

The result of an ENUM query can be one or more URIs with their order of processing and preference indicated by values in the NAPTR records. These URIs are then used to reference resources or services associated with the Recommendation E.164 number. Possible examples of resources or services include fax number, mobile number, e-mail address, GPS coordinates, phone redirection services, unified messaging services, voice mail and public key for asymmetric encryption applications.

How are E.164 numbers mapped into the DNS?

The ENUM protocol requires that related services be looked up through a convention of one-to-one reverse mapping of digits in an ITU-T Recommendation E.164 number into separate DNS "zones" – which are then concatenated with another domain. The Internet Architecture Board (IAB), has proposed that this domain be "e164.arpa". As at 1 September 2001, there is not yet consensus by ITU Member States on the usage of the e164.arpa domain or of any particular operator of that domain but with that caveat, it is used below for the sake of discussion.

As an example, let us construct the related DNS domain to look up NAPTR resource records associated with the number +33 1 40 20 51 51, which corresponds to the information desk at the Louvre Museum in Paris, France:

- Write the E.164 number in its full form, including the country code, then remove all non-digit characters with the exception of the leading "+".
- Example: +33140205151
- Remove all characters with the exception of the digits and put dots (".") between each digit.

- Example: 3.3.1.4.0.2.0.5.1.5.1
- Reverse the order of the digits and append the ENUM Tier-0 zone to the end.
- Example: 1.5.1.5.0.2.0.4.1.3.3.e164.arpa

If the Louvre Museum had chosen to provision its number in the DNS for ENUM services, the client application could now perform a look-up on this name and, for example, retrieve the NAPTR records for a corresponding fax number, e-mail address or any other URI for the E.164 number +33 1 40 20 51 51.

4 ENUM tiers and roles and responsibilities

There is a range of options for describing ENUM administrative and technical levels and roles. However, some commonly used working definitions have emerged where Tier-0 refers to the root level of the ITU-T E.164 numbering plan, Tier-1 refers to the next level at the "country code" level, and Tier-2 refers to an actual subscriber telephone number.

The ITU Constitution and Convention set forth the functions and role of the ITU Telecommunication Standardization Sector (ITU-T), the world telecommunication standardization assemblies, as well as the Director of the Telecommunication Standardization Bureau (TSB). The role of the TSB Director and ITU Member States with respect to the allocation and management of numbering resources is defined in Resolution 20 – first issued by the World Telecommunication Standardization Conference (Helsinki, 1993) and most recently adopted by ITU Member States at the WTSA in Montreal (2000). Resolution 20 states "that the assignment of international numbering and addressing resources is a responsibility of the Director of the TSB and the relevant administrations", where the term "administration" is a term defined in the ITU Constitution as "Any governmental department or service responsible for discharging the obligations undertaken in the Constitution of the International Telecommunication Union, in the Convention of the International Telecommunication Union and in the Administrative Regulations."

In accordance with the above, it is agreed that the role of ITU Member States with respect to the allocation and management of their numbering resources, including the potential provisioning of those resources in the DNS, will be maintained. As ITU-T Study Group 2, Working Party 1/2, has stated, in a liaison statement to IETF/ISOC: "It is noted that most ENUM service and administrative decisions are national issues under the purview of ITU Member States, since most of the E.164 resources are utilized nationally."

If parts of the Recommendation E.164 numbering plan are to be authoritatively provisioned in the DNS, it is assumed that there is a requirement for an authoritative DNS infrastructure that parallels, at least to some extent, the hierarchical roles and responsibilities that currently exist for the E.164 numbering plan.

In the case of geographic resources, it is recommended that the legal authority for any ENUM Tier-1 domain corresponding to a country code resource be the corresponding ITU Member State or its designated delegates. Only in this case will the administration of the corresponding ITU Member State be able to legally exercise related policy, as well as coordinate the operational and technical management of the corresponding DNS zone.

In the case of E.164 network resources, it is recommended that the legal authority for any ENUM Tier-1 domain corresponding to a network resource should be the corresponding network operator or its designated delegates.

In order to ensure the sovereign role of each ITU Member States with respect to the allocation and management of their numbering resources, TSB ensures that each Member State has specifically authorized the inclusion of their Recommendation E.164 country code resource in the DNS, through

instructions from their administration. Upon this authorization, the management of E.164 resources in the DNS is considered to be a national matter and therefore administered by the ITU Member State(s) to which the country code is assigned. Furthermore, it is assumed that, based on the principle of sovereignty, in an integrated numbering plan, each country within the plan may individually administer their portion of Recommendation E.164 resources mapped into the DNS.

5 Policy and operational issues for ENUM implementation

As noted above, most of the issues related to ENUM implementation are national issues, to be addressed at the national level. The issues include the following:

- How to authenticate the identity of the subscriber for ENUM services?
- Who are ENUM registrars and what are they responsible for?
- How to validate ENUM data for potential subscribers (Add – Modify – Delete) in the NAPTR list of services and preferences?
- How are data provisioned in the country code name servers?
- How to obtain end-user agreement if necessary to enter a number in DNS?
- How to harden the ENUM zone data against data mining, especially for the purposes of spam?
- Competition models amongst suppliers of ENUM services, and related portability issues.

6 ENUM: potential policy implications[2]

ITU-T Study Group 2 is currently addressing principles and procedures for the administration of ENUM as well as defining a framework for the possible role of ITU. A key issue is implementing and maintaining the databases necessary for translation of the E.164 numbers into the Domain Name System so as to safeguard the integrity of the E.164 numbering system. National regulatory authorities or policy makers may wish to consider their appropriate level of involvement in these activities at ITU. More information on the ENUM protocol, and the issues related to it, can be found at www.itu.int/osg/spu/infocom/enum/.

6.1 ENUM standard

The ENUM standard, described in IETF's RFC 3761, defines a protocol and an architecture based on the Internet DNS, whereby it is possible to obtain a correspondence between E.164 telephone numbers and call service identifiers, with an order of priority (e-mail, website URL, SIP address of an IP telephony server, voice mail, other telephone numbers, …). Using the ENUM protocol, therefore, it is possible to find the various addresses of the target user on the basis of a simple telephone number. The subscriber or registrar may also customize the manner in which the subscriber may be reached, with a single E.164 number. It is easy to add to or modify such additional information without changing the number used for access. The ENUM protocol is thus seen as a technical gateway ensuring correspondence between the Internet and the switched telecommunication network, enabling interworking between the two.

The ENUM protocol and the use of DNS mechanisms do not give rise to any technical problems implying the incorrect functioning of services based on this functionality. However, the ability of the centralized and hierarchy-based DNS architecture to support requests generated by services

[2] The material in this section was provided by BDT.

requiring the transport of information in real time and with high quality will need to be determined at each level of the DNS architecture, according to the load and to the level of availability required by each service.

To find the DNS name of an E.164 telephone number, the RFC 3761 standard requires that the following steps be executed:

	Step	Example
1	Write the E.164 number in its complete form with the country code (IDDD)	+46-8-9761234
2	Delete all non-numeric characters except for the symbol "+"	+4689761234
3	Remove all non-numeric characters	4689761234
4	Insert a stop (".") between each digit of the number	4.6.8.9.7.6.1.2.3.4
5	Reverse the order of the digits of the number	4.3.2.1.6.7.9.8.6.4
6	Add the string ".e164.arpa" to the end of the number obtained in step 5	4.3.2.1.6.7.9.8.6.4.e164.arpa

Using the domain name obtained in the last step of the above procedure, the ENUM algorithm is applied in order to obtain the order of priority of the call service identifiers. The following figure shows an example of the ENUM protocol in the case of use of a conventional (analogue) telephone set via the switched network.

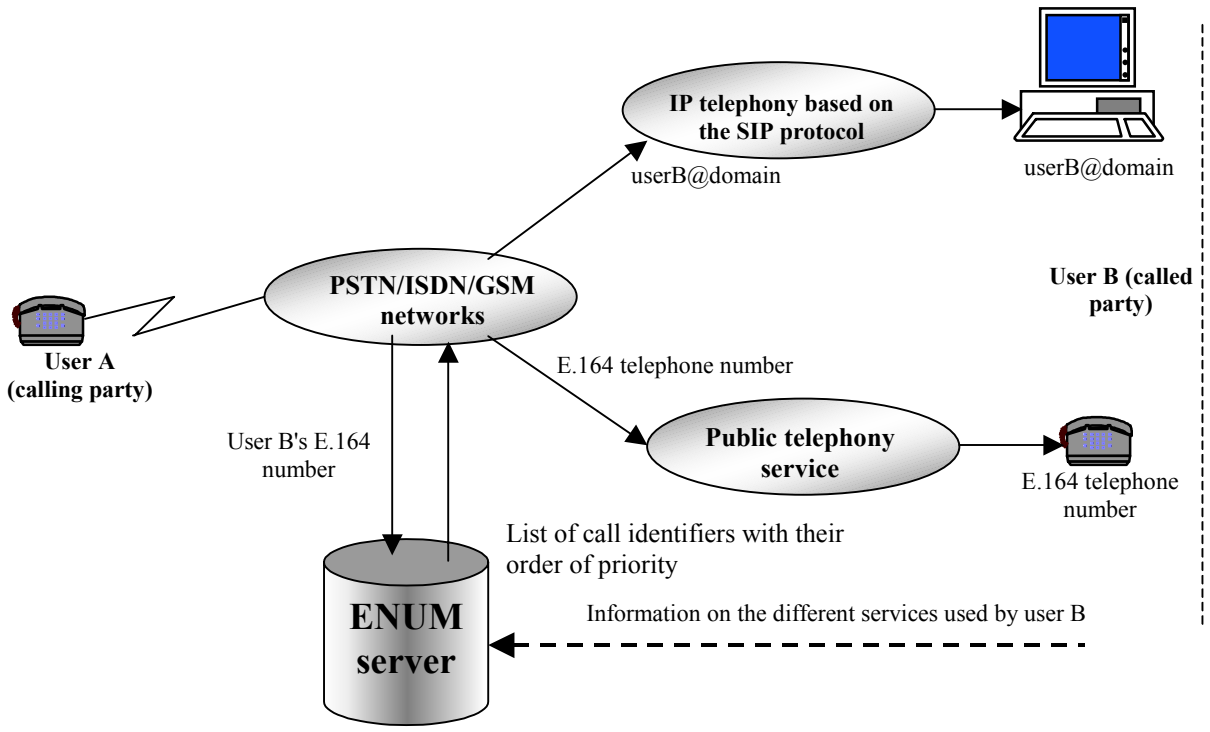


Figure 1 – Example of ENUM usage in the case of the switched telephone network

7 ENUM implementation status

List of ENUM national delegations[3]

E.164 Country Code	Country	Delegee	Date of TSB Approval dd/mm/yy
246	Diego Garcia	Government	12/08/02
247	Ascension	Government	12/08/02
290	Saint Helena	Government	12/08/02
31	Netherlands	Ministry	23/05/02
33	France	DiGITIP (Government)	28/03/03
353	Ireland	Commission for Communications Regulation	25/05/04
358	Finland	Finnish Communications Regulatory Authority	26/02/03
36	Hungary	CHIP/ISzT	15/07/02
374	Armenia	Arminco Ltd	11/07/03
40	Romania	MinCom	10/12/02
41	Switzerland	OFCOM	01/10/03
420	Czech Republic	Ministry of Informatics	24/06/03
421	Slovak Republic	Ministry of Transport, Post and Telecommunications	04/06/03
423	Liechtenstein	SWITCH	21/10/03
43	Austria	Regulator	11/06/02
44	UK	DTI/Nominum	16/05/02
46	Sweden	NPTA	10/12/02
48	Poland	NASK	18/07/02
49	Germany	DENIC	16/05/02
55	Brazil	Brazilian Internet Registry	19/07/02
65	Singapore	IDA (Government)	04/06/03
86	China	CNNIC	02/09/02
971	United Arab Emirates	Etisalat	13/01/03

Current status of the national ENUM delegations can be found at:
http://www.itu.int/ITU-T/inr/enum/.

Information on ENUM trials:
http://www.centr.org/kim/enum/index.html.

[3] As at 3 January 2005.

Attachment 15

IP telephony and voice over IP (VoIP)

Table of contents

Page

IP telephony and voice over IP (VoIP)[1]

1 Working definition of IP telephony

1.1 Technical motivations for IP telephony

Although IP telephony does not yet constitute a substantial percentage of the global worldwide telephony traffic volume, it is expanding rapidly as a result of the following technical motivations:

1) The circuit-switched network was designed and optimized to provide a single product – full-duplex 4 kHz switchable voice channels between points (64 Kb/s digital channels).

2) "Data", in general, are characterized by bursts of information rather than the constant bit rate flows typically associated with speech.

3) Data bursts can be most efficiently transported using packets of information that can be interleaved in time within a network with other packets being carried between other sources and destinations.

4) For more than 40 years, voice has been digitally encoded into 64 Kb/s streams that can be transported over the 64 Kb/s channels. However, advances in voice coding permit a wide range of options, e.g. from 5-8 Kb/s to higher quality audio at 64 Kb/s. Multiplexing voice at a rate other than 64 Kb/s is difficult over the 64 Kb/s circuit-switched network. However, IP telephony subscribers need to interconnect with the more than 1 billion worldwide classical telephony subscribers, and implementation of a transcoding mechanism makes it necessary to transform their lower bit-rate to the legacy 64 Kb/s encoding (much like what happened when the low-rate encoding of mobile networks was connected to fixed PSTN networks).

5) Significant work has been performed in IETF and elsewhere to provide real-time or near real-time capabilities using IP that permit voice to be transported over IP using the range of voice coding. Carrier-grade products that integrate those protocols are being introduced in the field to produce quality of service that satisfies their customers. IETF is currently working on protocols that ensure that QoS constraints are met in a consistent manner over a set of traversed networks.

6) This flexibility to transport a variety of user information streams, i.e. constant and variable bit rate, different speeds, etc., allows packet-switched networks to evolve towards the objective of one integrated network for a wide range of applications.

7) A single integrated network (packet-switching) can mean less operational and maintenance costs compared with multiple overlay networks. However, in the short term there may be additional expenses.

8) In addition the flexibility of packet-switched networks to accommodate new information streams, with a wide range of characteristics and based on the IP and the host of open, standardized interfaces and languages available to it, allows the introduction of new applications producing new revenue streams. In some cases those capabilities could be the real driver for the introduction of IP transport within telecomunication networks rather than the "reproduction" of existing telephony services.

---

1 The material in this section has been provided by BDT.

9) IP-based networks can use the same underlying lower layer transport facilities. i.e. twisted metallic pairs, cable, wireless, optical fibre, satellite. The evolution to IP-based networks can be accomplished economically by deploying IP-based packet switches/routers that can be connected by existing transport facilities. This was a tremendous vehicle for offering Internet access to mass markets in developed countries owing to the availability and ubiquity of those transport facilities.

1.2 Introduction to the different types of IP telephony

According to the nature of the IP network used, we may speak of two major categories for voice transmission over IP networks. The first is essentially based on the Internet, which is seen as the interconnection of a host of public or private networks on a global scale. The second is provided by service operators using managed IP networks, within which a number of pre-installed mechanisms (routing algorithms, coding, etc.) serve to ensure a quality of service level that is acceptable for speech.

There are three voice over Internet protocol (VoIP) usage scenarios according to terminal equipment and types of network:

1.2.1 Scenario 1: PC to PC

In this scenario, the calling and called parties both have computers[2] that enable them to connect to the Internet usually via the network of an Internet service provider (ISP)[3]. The two correspondents are able to establish voice communication only by prior arrangement, since both users have to be connected to the Internet at the same time (having fixed in advance the time at which they will communicate via the Internet, unless of course they are permanently online) and use VoIP-compatible software[4]. Furthermore, the caller must know the IP address of the called party; to overcome this correspondents must agree to consult an online directory server (updated with each connection) where users register prior to each communication or have other ways of locating and being aware of the availability of their correspondent's connection to the Internet (Instant Messaging technologies).

---

[2] Actually the term computer or PC indicates a device capable of executing a VoIP application software program. Today, we see the emergence of advanced user appliances like personal digital assistants (PDA) or advanced mobile handsets that are capable of running VoIP software; therefore the term PC used in the sequel is used for convenience and should be understood in the above general meaning.

[3] The role of the ISP is primarily to allow his subscribers to connect to his network and provision them with an IP address allowing them to use Internet applications. The case of accessing to the Internet through an ISP is cited here as the dominant example. Of course users connected directly to a LAN or WAN (enterprises or academia networks) can have an IP address – albeit a private one behind a network address translation (NAT) scheme – and use the Internet applications without the intervention of an ISP.

[4] The telephony softwares currently available on the market all have a similar structure, displaying a control panel from which the main telephony functions may be controlled and the configuration and options menus consulted. All such softwares provide access to Internet relay chat (IRC) areas, in which users can exchange text messages in real time, to which end a list of individuals using the same software and currently online is displayed. According to the product, there is also a menu which enables the user to make a call to a specific IP address that is permanent and corresponds to a machine that is already connected to the network. Some products may include encryption of voice communication. A voice-mail option enables voice messages to be recorded by the machine.

In this scenario, the ISP is generally accessed via the public telephone network by means of a simple telephone call. This means of access still predominates, even in developed countries. Alternative solutions, known as "broadband" and based on the telephone network (xDSL technology), a cable television network or a wireless access network (LDMS technology), are currently at the early stages of deployment, and are not yet in widespread use, even though certain countries are already well equipped[5].

The ISP's role in this scenario is limited to the simple provision of access to the network, which in turn enables the user to access the Internet. The voice application used by the customer is transparent for the ISP, which takes no specific measures to guarantee the quality of the voice service. In short, one cannot in such a scenario speak of "telephony" in the conventional sense of the word, i.e. the provision of a service by a third provider, but merely of the use of a voice application via the Internet, such usage having become as commonplace as any other network application. The protocol used between the two communicating parties is often the H.323 (see Annex F.1 to ITU-T Recommendation H.323) protocol defined by ITU-T (e.g. the NetMeeting application); however, IETF's SIP protocol (see Annex F.2) could see more widespread use in the future. This solution is illustrated in Figure 1 below.

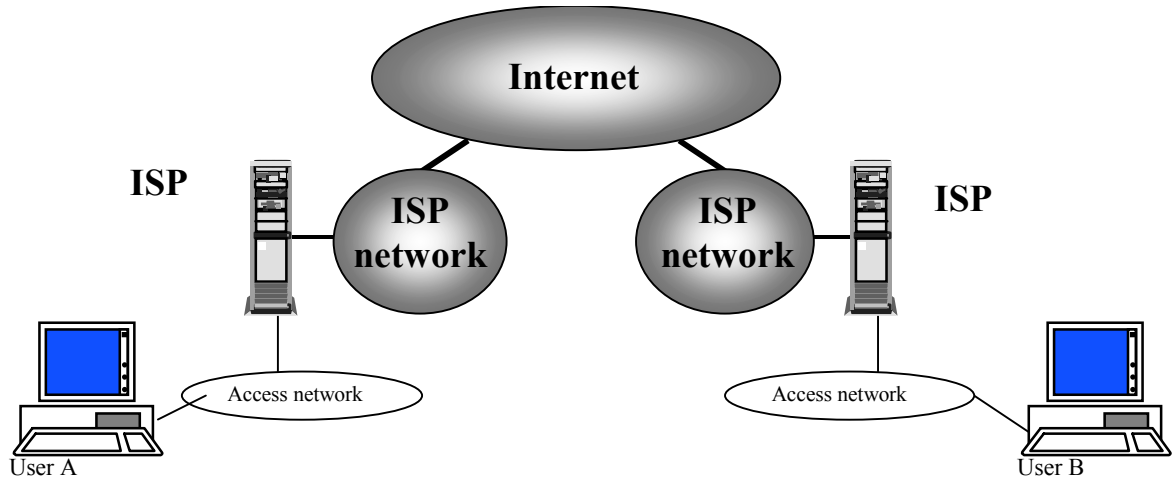


Figure 1 – PC-to-PC IP telephony

1.2.2 Scenario 2: Phone-to-phone over IP

In this case, the calling and called parties are both subscribers to the public telephony network (fixed or mobile) and use their telephone set for voice communication in the normal way. There are two methods for communicating by means of two ordinary telephone sets via an IP or Internet network.

---

5 The main European Union, North American and Korean operators already report an availability in the order of 90% ADSL access (see also ITU's "New Initiatives: Broadband" reports).

1.2.2.1 Use of gateways

This means that one or more telecommunication players have established gateways that enable the transmission of voice over an IP network in a way that is transparent to telephone users. What we have in this case is not the Internet but a "managed" IP network, i.e. a network which has been dimensioned in such a way as to enable voice to be carried with an acceptable quality of service. Figure 2 below illustrates such a scenario.

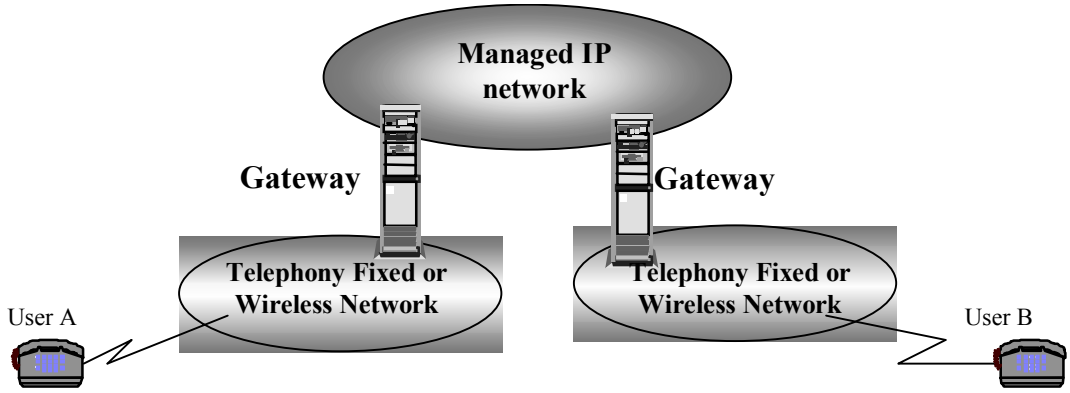


Figure 2 – Phone-to-phone IP telephony using gateways

In this scenario, the gateways and managed IP network could belong to different players, depending on whether we are looking at:

a) the purely internal use of VoIP within the network of a single telephone operator, which owns and manages the entire operation, handling both users A and B;

b) the provision of a long-distance voice service by a long-distance operator using VoIP technology (users A and B in this case belonging to different networks), in which case the whole operation belongs to and is managed by such a long-distance operator.

1.2.2.2 Use of adapter boxes

A number of companies market boxes which resemble modems and are installed between the user's telephone set and his connection to the PSTN.

In order for this arrangement to work properly, each of the two users needs to have a subscription with an ISP whose access parameters have been preprogrammed in the box.

The calling party initiates his call in the same way as in a conventional telecommunication network, and the first phase of the call is in fact set up on that network; however, immediately after this the boxes exchange the information required for the second phase. The conventional call is then broken off and the boxes, on the basis of the data they have exchanged and the pre-established parameters, establish a connection between each of the two correspondents and their respective ISP. Once the

call has been established, the boxes locally convert the voice signals into IP packets to be transported over the Internet as illustrated in Figure 3. This scenario is in principle very similar to scenario 1, except that the two users do not require a PC and the need for an Internet "rendezvous" is facilitated by the procedure being initiated in the form of a telephone call. However, this type of arrangement has been only marginally successful since it requires – as in the PC-to-PC case – that the two correspondents each be equipped with the same type of box.

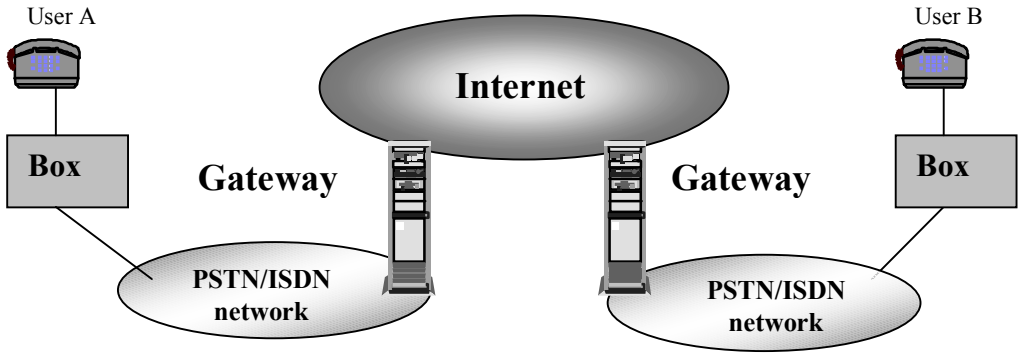


Figure 3 – Phone-to-phone IP telephony using adapter boxes

The two methods in this scenario call on two types of network to establish the telephone call, i.e. the Internet or a managed IP network, and the PSTN.

1.2.3 Scenario 3: PC to phone or phone to PC

In this scenario, one of the users has a computer by which he connects to the Internet via an access network and an ISP (in a similar way to scenario 1), while the other user is a "normal" subscriber to a fixed or mobile telephone network.

1.2.3.1 PC to phone[6]

When the computerized user wishes to call a correspondent on the latter's telephone set, he must begin by connecting to the Internet in the traditional manner via the network of his ISP. Once connected, he uses the services of an Internet telephony service provider (ITSP) operating a gateway which ensures access to the point that is closest to the telephone exchange of the called subscriber. It is this gateway that will handle the calling party's call and all of the signalling relating to the telephone call at the called party end.

It should be noted that the ITSP provides a one-way PC-to-phone service and does not manage subscribers as such; *in fact, the PC subscriber uses the ITSP's services solely for outgoing calls*. It should also be noted that the ITSP has a managed IP network, thereby ensuring a certain quality of service for voice as far as the gateway closest to the called subscriber, and that the ITSP also manages the interconnection with the latter's telephone operator. Despite their use of VoIP technology, ITSPs consider themselves to be telephone service providers and generally provide their services to individuals in the conventional manner, i.e. with a charge per minute.

---

6 The same remark noted for scenario 1 applies here; the ISP case is only the dominant example. The user can be connected to the Internet behind a LAN or WAN without the need of ISP mediation.

1.2.3.2 Phone-to-PC

In this case the calling party is the telephony user and the called party is the PC user. Since a telephony user can essentially dial an E.164 number to reach the called party, then somehow the PC user should have an E.164 number

– either indirectly: in case of its interconnection to the network behind an IP-technology private branch exchange (PABX) switch (actually in this case we can more properly speak about an "IP phone" rather than a PC device that is connected to the LAN managed by the IP PABX);

– or directly: in this case the IP-side subscriber has an E.164 address allocated by an IP telephony operator.

Technically speaking only the first of the above cases works today through the availability of IP PABX devices. The second case will work pending the availability of a translation mechanism between implemented by the IP side that translates the public E.164 number to the IP address of the called party. This will only be available pending the implementation of a technology like ENUM.

Figure 4 below illustrates this scenario.

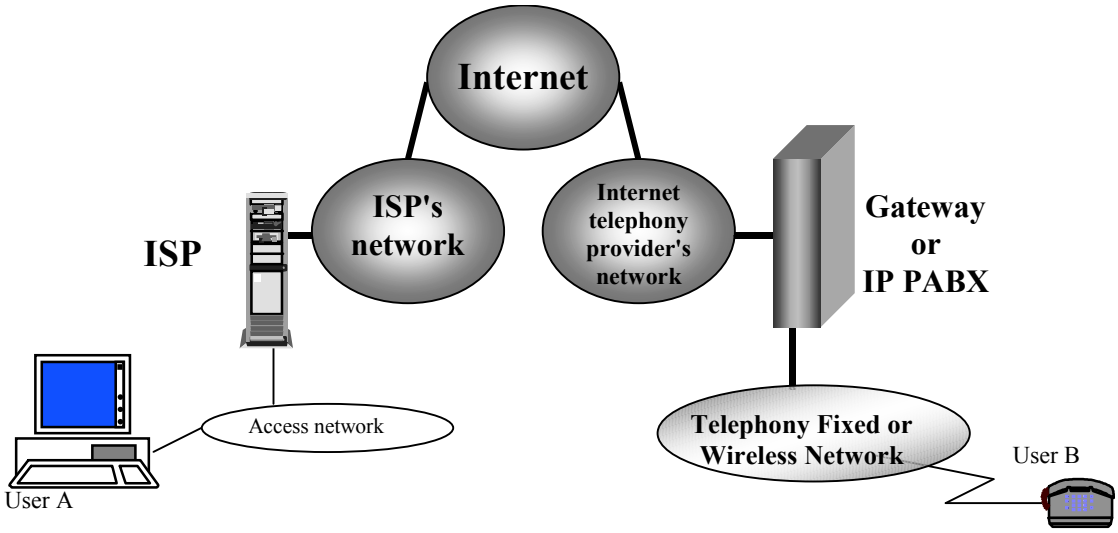


Figure 4 – PC-to-phone or phone-to-PC IP telephony

1.3 Working definition of IP telephony

ITU-T Study Group 2 issued the following explanations of the term "IP telephony":

"IP is an acronym for Internet Protocol. It is a communications protocol developed to support a packet switched network. The protocol has been developed by the Internet Engineering Task Force (IETF). **IP Telephony** is the exchange of information primarily in the form of speech that utilises a mechanism known as Internet Protocol"

The position of Study Group 2 regarding the term "Internet telephony" should also be noted:

"The combination of the term 'Internet' with the term 'telephony' is seen as inappropriate. The Internet offers many capabilities to users including the ability to carry bi-directional speech in real time or near real time. We consider this to be an intrinsic capability of the Internet and not a tele-communication service"

Apart from the possible use of the telephone network as a network providing access to the Internet, it is possible to categorize the scenarios presented above into two types:

Type 1: Those requiring the intervention of an operator and enabling, by means of a gateway, the partial (in one direction as in scenario 3) or full (in both directions as in scenario 2 with gateways) provision of communication to the global public switched network.

Type 2: Those requiring no intervention by a third provider (as in scenario 1 or scenario 2 with boxes) and without the need for a gateway; in this case, the application of VoIP is seen as one of the multiple applications of the Internet world.

Type 2 is close to what Study Group 2 considers as "Internet telephony" in the sense that it uses "the intrinsic capabilities of the Internet and [does] not [involve] a telecommunication service". Type 1 scenarios on the other hand use the Internet protocol as a bearer for speech but involve an intervention of an operator if only for the provision of an interconnection service towards a telephony network subscriber. They are closer to the above definition of IP telephony though that definition focuses only on the transport technology used for speech transmission (namely, the Internet protocol) and does not seem to address the other known attributes of telephony as a **service** provided by an operator.

It goes without saying that the first type of usage is the more advantageous, at least in the short and medium terms. It is alone in providing access to over one billion telecommunication network users throughout the world, thereby contributing to universal access to telecommunication services.

The second type of usage is of interest, in the short term, only to the community of Internet users, and will become valid as a long term universal communication model once all user equipment (particularly terminals) throughout the world has migrated to "native" IP technology for accessing the Internet, and once the technologies needed to implement the quality of service for applications involving interaction between individuals (whether by voice and/or other media) have been widely introduced in IP networks. Later in this document, we shall be focusing on the discussion of problems relating to implementation of the IP telephony service and to the ways in which the PSTN and networks using IP technology interact. We shall also be looking at the technological factors favouring migration by the telephony service to IP network technology and at the prospects that are opened up by that migration in terms of new services.

2 Review of current regulatory framework

2.1 General remarks

The introduction and growth of IP telephony raises a number of important policy issues. ITU-D is challenged with advising and assisting Member States and Sector Members in response to specific concerns and needs of developing countries regarding the policy implications that surround the introduction of "IP telephony".[7] In this report, expert advice and assistance is provided in three major sections:

1) review of current regulatory frameworks;

[7] Opinion D http://www.itu.int/ITU-D/e-strategy/internet/iptelephony/Documents/wtpf2001/Chaireport.html#OPINIOND

2) country case studies; and

3) shared experiences in developing new methods and approaches for the introduction of IP telephony.

This part of this report is meant to serve as a general guide, not a step-by-step plan. The Secretary General's report to, and the Chairman's report of, the third World Telecommunication Policy Forum (WTPF), http://www.itu.int/osg/spu/wtpf/wtpf2001/index.html provide useful background discussions of the many policy issues, as well as a survey of the varied domestic regulatory policy approaches of ITU Member States. The survey reveals that there is no single policy approach, and indicates that the policy issues will continue to evolve as IP telephony technology is enhanced and more widely deployed.

Aspects of the Secretary General's report and the WTPF Chairman's report have been included in this report where applicable. Readers are encouraged to consult the full reports as well as the source documents prepared for the WTPF for additional detail. However, as the underlying technologies and markets evolve, it is important to consider the effects of these changes on policies and to plan for change within the policy-making process.

2.2 Overview

As IP networks and IP telephony become more widespread, policy-makers face the challenge of evaluating whether current regulatory frameworks, developed initially for circuit-based networks, are relevant and appropriate for IP-based networks. This challenge is arising at a time when many Member States are lightening their regulatory regimes and moving to greater reliance on competition to ensure consumers the broadest possible access to telecommunication services.

Owing to the very different regulatory regimes created to address particular domestic economic, political and infrastructure challenges, Member States may want to focus their reviews on the rationale behind their policy frameworks, and especially the desired effects in the context of overall economic and social development. In particular, the existing level of network development and state of the communications market generally are issues that most likely will have to be taken into account. Countries that have very low teledensity levels must address the most basic difficulty of building a telecommunication infrastructure.

Within these broad policy frameworks, IP telephony may raise a number of specific questions for policy-makers and regulators requiring a careful and informed balancing of different and sometimes competing interests. As a threshold matter, it is useful to understand the short- and long-term economic consequences of any policy decision. It is also essential for regulators and policy-makers to understand that there is no policy model that is universally applicable. A number of approaches may be appropriate.

It is recommended that Member States consider the benefits of:

1) First, defining the broad telecommunication policy objectives for the country, within the context of overall economic development and social needs, and

2) Second, tailoring the regulatory regime to reach these objectives.

2.3 Areas for review

As the basis for determining policies specific to IP telephony, the Group of Experts believes that Member States may benefit from a review of their more general domestic telecommunications regulatory frameworks with the following in mind:

2.3.1 Achieving policy goals in the context of convergence and existing market conditions

Member States may need to evaluate their policy goals before determining what, if any, regulation is necessary in a converged market. For example, it may be appropriate to limit regulation in a converged, competitive market-place, employing regulation only when there is market failure.

2.3.2 Encouraging investment, spurring innovation, advancing development and opening markets

A competitive telecommunications environment allows for competition among multiple service providers and for multiple investors. Experience around the world reveals that competitive telecommunication models have been adopted to attract capital investment for telecommunication and IP-based network infrastructure build-out. It is also evident that policy-makers and regulators have successfully implemented a competitive model by ensuring appropriate safeguards against undue market power. Policies that allow multiple carriers and Internet service providers (ISPs) have been shown to stimulate infrastructure build-out and lower prices for business and consumer access.

2.3.3 Customer benefits

Competition has been shown to enhance end-customer choice by providing more options both in terms of price and quality. Consumer welfare is usually the greatest in an environment where there are no limits on the number of suppliers and services.

2.3.4 Universal service/access objectives for telecommunication services

In some circumstances the market may not function to provide telecommunication services to certain subsets of users. Universal access can be defined as government-sponsored programmes designed to provide access to specified telecommunication services for a community. Several countries in the developing world have adopted universal access models to provide access to a defined set of telecommunication services in rural and remote areas, and for low-income individuals. Without access to these services, Internet and other advanced IP services access and use is inhibited. Countries that implement universal access programmes may want to consider the following:

- A universal access programme that is created to promote the development of telecommunication infrastructure in rural and remote areas, and for low-income individuals.
- A universal access programme for telecommunications that is operated in a transparent, competitively neutral and non-discriminatory manner.
- Clear identification of the universal service requirements and provider obligations.
- When universal access to local services is funded by a cross-subsidy (for example, from long distance telecommunications), that any cross-subsidy be clearly and transparently identified.
- A funding mechanism that is clear as to whether the funds come from taxes or revenues.
- A universal access plan that promotes infrastructure development and is pro-competition.

2.3.5 Consideration of technological issues such as quality of service

The service and quality capabilities of IP telephony technologies are still evolving. To reach the full range of market needs, it is expected that IP technology will have functional capabilities similar to circuit-switched technology. Policies that allow flexibility in choice of technology and application to address user needs and to permit users to choose among different prices and qualities are more likely to encourage investment and stimulate development.

2.3.6 Interconnection and access policies

Within the context of network transition one role of policy-makers may be to ensure that existing services remain available as new services are introduced, as driven by market forces. Interconnection policy can play a critical role by ensuring that new and existing infrastructure can coexist, thus preserving and enhancing the value of both. In technology transitions, such as the one from circuit-switched to packet-switched communication transport mechanisms, there is usually a period of coexisting technologies. Policies that recognize transition by allowing multiple network platforms and encouraging their interconnection are preferable.

2.4 Agency contacts

ITU maintains a contact database of the regulatory agencies and key contacts of each Member State. Contact information can be found at

http://www.itu.int/GlobalDirectory/index.html An additional source of country-by-country contact information is available online at: http://www.totaltele.com/links/list.asp?CategoryID=267

3 Case studies and experience sharing

3.1 Introduction

While some developing countries have policies prohibiting IP telephony, others have policies embracing it. Some do not regulate IP telephony at all, while others have chosen to include it in a positive manner within their telecommunications regulatory framework. These countries may be motivated by a desire to encourage and stimulate emerging technologies that can lower costs, increase total revenue opportunities and promote innovation and national economic growth. These policies may be linked to concerns about imposing regulations on technologies that are not fully mature. Limitations placed on IP telephony may be seen as inconsistent with approaches designed to stimulate the deployment and migration to IP-based networks. Also, regulators may be hesitant to intervene in new markets unless there is evidence of market failure. Decisions to prohibit, regulate or not regulate IP telephony are often coupled with long-term policy objectives for the development of the communication infrastructure/network.

3.2 Results of policies embracing IP telephony

The World Bank has created an Internet Economic Toolkit for African Policy-makers addressing many of the above issues in the context of developing economies. This toolkit presents a model of the likely impacts of the Internet on African telecommunication companies and Internet service provider revenues, models of the cost structure and potential reach of Internet service, data on the extent of Internet development in Africa and examples of its current use. With this background, the toolkit goes on to discuss policy choices faced by countries that hope to expand Internet use within the context of needed telecommunication reform and government-private partnerships involving universities and NGOs. It is available in five pdf files and an Excel spreadsheet containing the model itself. It can be accessed online at: http://www.infodev.org/projects/finafcon.htm

3.3 Policies consistent with transition/convergence of networks

Case studies can provide useful insight into the impact of regulation on the development and expansion of the telecommunication market within a particular economy. Caution should be exercised, however, in extrapolating the findings to economies that do not share the basic characteristics of the studied economy. However, the methodologies used in these studies can be

particularly useful to others conducting their own case study. ITU has completed case studies of 5 Member States: Korea, China, Peru, Colombia and Canada. These studies are available on line through the ITU website at: http://www.itu.int/osg/spu/wtpf/wtpf2001/casestudies/index.htm

Over the past four years, the Organisation for Economic Co-operation and Development (OECD) has undertaken in-depth reviews of the telecommunication regulations in a number of economies. This work is aimed at producing, for each country reviewed, a multidisciplinary review of progress on regulatory reform based on international benchmarking, self-assessment and peer review. The recent reviews of Hungary, Poland and the Czech Republic are specially noted. The reviews of Hungary http://electrade.gfi.fr/cgi-bin/OECDBookShop.storefront/EN/Catalog/BO-1-13-xx and the Czech Republic http://electrade.gfi.fr/cgi-bin/OECDBookShop.storefront/EN/Catalog/BO-1-13-xx are available through OECD publications.

3.4 Sharing experience in developing new methodologies and approaches

3.4.1 General remarks

Countries have taken widely differing policy approaches toward IP telephony, which may be related to different prevailing market conditions or degrees of liberalization. The sharing of these different approaches can help policy-makers define and evaluate options to address issues specific to the environment in their country.

3.4.2 Approaches to technology-neutral, sector-specific regulation

Technological neutrality is a principle that is invoked by some policy-makers and regulators when addressing IP telephony and other emerging communication technologies. This concept can be generally characterized as an effort to apply regulations in an identical manner to like services, regardless of the technology used to provide these services in a competitive market. Unless other policy imperatives take precedence, the purpose of this concept is to support competition policy by ensuring that one provider is not given more favourable regulatory treatment than another when providing equivalent services. Others believe that policy-makers should not be indifferent to technology. They assert that emerging technologies might benefit from a "window", i.e. a form of asymmetric regulation during an introductory phase, which would allow them to develop and grow outside traditional regulation.

The principle of technological neutrality was widely discussed at the WTPF meetings and the Expert Group meetings. No consensus was reached. However, many believe that:

1) A country first must have effective competition in order to apply a principle like technological neutrality.

2) Technological neutrality is a legitimate consideration in policy and regulatory deliberations, but it should not override broader pro-competition objectives.

The European Union (EU) has concluded proceedings to create technology-neutral regulation. The Directive on access to, and interconnection of, electronic communication networks (COM(00)384final of 12 July 2000) harmonizes the way in which EU Member States regulate the market between suppliers of communication networks and services in the Community. The Directive lays down a framework of rules that are technologically neutral, but which may be applied to specific product or service markets in particular geographical areas, to address identified market problems between suppliers of access and interconnection.

The Directive "Interconnection and access in the new EU regulatory framework for electronic communications services" and additional material may be consulted at the EU website http://www.europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/index_en.htm

3.4.3 Application of domestic telecommunication regulation establishing effective competition, universal service/ access obligations including any other, further obligations, and other experiences

a) The United Kingdom's independent regulator, OFTEL, has had extensive experience with different regulatory approaches including price caps, and of adjusting the scope and intensity of regulation to take into account the level of competition in the market and technological change. Its website is: http://www.oftel.gov.uk/

b) In the United States there has been extensive competition in certain sectors of the telecommunication market since the 1970s, especially in long distance and enhanced or value-added services. In 1996, national legislation was adopted that specifically opened the local telecommunication market to competition. An overview of the United States experience is provided in:
http://www.itu.int/ITU-D/e-strategy/internet/iptelephony/Seminars/2ndEGM/documents/policy/IPTel-21.pdf

c) India is experimenting with IP telephony in limited applications. Under the NTP 1999, Internet telephony is not yet permitted in India. The Government of India has committed to monitor the development of IP telephony and its impact on national development and will review the issue at an appropriate time. The Government, at present, is working on various issues relating to the IP telephony. Meanwhile, the incumbent operator BSNL has plans to use IP technology for real time service for transit traffic between tandem exchanges, bypassing the tandems on an experimental basis at six locations in the country using a separate IP-based network. At present it is not envisaged to connect these links to the Internet. Only domestic long distance traffic is proposed for experimentation with VoIP and no international direct-dial calls are proposed in this experiment. This experiment will cover real-time voice and fax services, whereas data services will be transacted through the Internet.

4 Conclusions: policy aspects

The policy implications of IP telephony should be examined within the context and complexity of the changes in the market environment. Developing countries face the additional challenge of addressing relatively low teledensity levels. As IP networks and IP telephony become more widespread, policy-makers may face the challenge of evaluating whether current policy frameworks, developed initially for circuit-based networks, are relevant and appropriate for IP-based networks. As the basis for determining policies specific to IP telephony, Member States may benefit from a review of their more general domestic telecommunications regulatory frameworks with the following in mind:

1) Member States may need to evaluate their broader policy goals before determining what, if any, regulation is necessary in a converged market.

2) Experience around the world reveals that competitive telecommunication models have been adopted to successfully attract capital investment for telecommunication and IP-based network infrastructure build-out.

3) Customer benefits are usually the greatest in an environment where there are no limits on the number of suppliers and services.

4) In some circumstances where the market may not function to provide telecommunication services to a certain subset of users, government-sponsored universal access/service programmes may be helpful.

5) Policies that allow flexibility in the choice of technology and its application to address user needs and to permit users to choose among different prices and qualities are more likely to encourage investment and stimulate development.

6) Consider, in competitive markets, whether to take a technology-neutral approach by applying regulations in an identical manner to like services, regardless of the technology used to provide these services.

7) Policies that allow for the coexistence of multiple network technology platforms and encourage their interconnection are preferred.

Countries have taken widely differing policy approaches toward IP telephony, which may be related to different prevailing market conditions or degrees of liberalization. No policy model is universally applicable. A number of approaches may be appropriate. The sharing of these different approaches can help policy-makers define and evaluate options to address issues specific to their country.

Training for policy-makers, regulators and operators is essential to help understand the implications of new technologies, new market structures and alternative regulatory models. A number of institutions, organizations and companies provide training programmes. Members are encouraged to take advantages of these programmes. Members are also encouraged to contact each other and to share first hand their experiences.

Attachment 16

E-Strategies – activities and progress report

Table of contents

E-Strategies – activities and progress report[1]

1 Introduction

To meet the objectives of Istanbul Action Plan (IsAP) Programme 3, six priority areas were identified by the 2002 World Telecommunication Development Conference (WTDC-02). The priorities domains are:

a) Foster the development of Internet protocol (IP) networks and services on all types of telecommunication networks.

b) Integrate the development of IP with the roll-out of societal applications to enhance governmental, medical/health, educational, agricultural, business and community services.

c) Enhance security and build confidence in the use of public networks.

d) Continue the development of multipurpose community telecentres (MCTs) and multipurpose platforms (MPPs) as mechanisms to provide wider and affordable access to ICTs.

e) Enhance ICT literacy and increase public awareness on the potentials of ICTs for socio-economic development.

f) Promote the establishment of a favourable legal environment for e-applications.

The activities presented in this report are grouped under four main categories below that are the deliverables for ITU/BDT E-Strategies activities for the period 2002-2003. The four main deliverables are:

a) E-applications *infrastructure*: Projects on e-services/applications.

b) *Capacity building*: Training on e-services/applications technologies.

c) *Policies and strategies*: Assistance in e-policies, e-strategies and e-legislation.

d) *Partnership*: Activities to facilitate the creation of mutually beneficial partnerships.

The following sections of this report highlight some actions undertaken to meet the four main areas' objectives. These activities have been carried out using mostly in-house expertise with priority given to least developed countries whenever it was possible for such activities to be undertaken and based on the demands from these countries. The years 2002 also marked the beginning of the transition from the Valletta Action Plan (VAP) to the Istanbul Action Plan (IsAP) especially for ITU-D study group Questions. Further information about these activities can be obtained from the website: http://www.itu.int/ITU-D/e-strategy.

Several LDCs from all regions have benefited from assistance provided by ITU/BDT and industry partners in various aspects of e-applications. BDT has actively participated in various workshops and seminars with particular emphasis on assisting LDCs in setting up their e-commerce endeavours.

---

1 This material was provided by BDT.

2 E-applications infrastructure

2.1 Ongoing and completed projects

During the year 2002, projects to deliver e-services were undertaken in most of the ITU regions. Most of these projects were aimed at implementing a secure IP infrastructure capable of delivering various types of e-service focusing on e-commerce. With developing countries represented by trade organizations, chambers of commerce, World Trade Centres and government ministries, projects in eight countries became operational during this period. Many other projects were launched and are still ongoing. For the activities reported, ITU/BDT provided assistance in respect of feasibility, technology strategies, project coordination and technical assistance in implementation.

For the first time, these countries benefited from ITU assistance in the deployment of infrastructure aimed at building security and trust (using digital certification, biometrics and digital signatures).

Bulgaria The first e-government project undertaken at the request of the Ministry of Transport and Communications (MTC). Launched in October 2002, the objective of this project was to enable highly secure communication including digital signatures and encryption for senior officials of the Bulgarian Government. Phase one of the project included the MTC, Council of Ministers, Communications Regulation Commission and Ministry of Finance. ITU provided guidance, technology strategies and recommendations for enabling technical and policy-level interoperability between other e-government initiatives in Bulgaria and the ITU/BDT project. This project is now operational. Funding, project coordination and implementation was provided by ITU/BDT with the participation and collaboration of the MTC.

Burkina Faso Project with the *Chambre de commerce, d'industrie et d'artisanat* (CCIA) for the deployment of a registration authority in the country. Funded mostly by ITU/ BDT and CCIA, this project became technically operational in December 2002. Even though operational, there are still issues related to business models and services necessary for sustainability that have to be addressed.

Cambodia Project to provide digital certification and value-added services/applications for the Ministry of Posts and Telecommunications of Cambodia (MPTC), including training. The project became operational in May 2002. Funded by the Swiss Federal Office for Communications (OFCOM), Cambodia became the first LDC to have an operational infrastructure for digital certification and e-applications.

Cameroon To address gender issues, ITU provided technical and financial assistance to a 3,500-member *Association pour le Soutien et l'Appui à la Femme Entrepreneur* (ASAFE) based in Douala, Cameroon and representing several countries. This project established sustainable e-commerce and Internet services. With financial aid from Japan for the physical infrastructure and that of ITU/BDT for the IP infrastructure and the support of the Government of Cameroon, this project has resulted in many other activities and international recognition. With expertise provided by ITU, the ASAFE project is one of the first projects in Cameroon where a wireless IP solution has been used to interconnect ASAFE to the national IP backbone. The ASAFE project became operational in 2002.

Cape Verde Project to build e-commerce infrastructure in Mindelo at the request of the Ministry of Transport and Habitat and the *Direccão Geral das Comunicações*. This activity has now been implemented. Additionally, there are plans for assistance in the introduction of a secure system for national and international e-transactions. This project has been postponed, because of a new Telecom restructuring.

Côte d'Ivoire Ongoing project to establish e-transaction infrastructure and services for the *Association pour la promotion des exportations* (APEX-CI). Funded mostly by BDT and APEX-CI, implementation commenced in December 2001 and was scheduled to be operational in the third quarter of 2002. Due to the political situation in the country in 2002, the finalization of this project was suspended in 2002.

Ecuador Project to provide digital certification and value-added e-services/applications for the *Corporación Ecuatoriana de Comercio Electrónico* (CORPECE), including training. The project became operational in February 2002 and was entirely funded by CORPECE. There need to be further actions in the area of marketing and the raising of awareness on the potentials of this secure e-transaction infrastructure for meeting the needs of various sectors in the domain of e-services.

Peru Project to provide digital certification and value-added e-services for LimaTel, the largest telecommunication operator in Peru. This project also included building local capacity through human resources development. This project's deliverable included the establishment of a registration authority for the provision of digital certification services and other value-added e-services and it became operational in February 2002. LimaTel provided the entire funding for this project.

Senegal Project to establish secure e-transaction infrastructure for SONATEL and Trade Point Senegal. This project was funded mostly by ITU/BDT and SONATEL and was completed in December 2002. Technically this project is operational but again, the next phase is to address services for vertical markets for the use of this infrastructure.

Turkey Funded by the World Trade Centre in Ankara (WTC Ankara) in Turkey, this project establishes the infrastructure for digital certification and value-added e-services/applications for WTC Ankara. The project became operational in the second quarter of 2002 and was entirely funded by the beneficiary organization.

Viet Nam This project was the first Asian Electronic Commerce Center operational at the Vietnam Trade Network. The project allowed the interconnection of other e-commerce projects in both developed and developing countries. The project was funded with in-kind contribution from ITU's industry partners. Owing to the high cost of Internet access, the sustainability of this project is endangered.

2.2 IP-based e-application projects launched in 2003

Azerbaijan ITU provided assistance in establishing a national policy framework for the development of e-business at the request of the Ministry of Communications. For 2004, ITU will be providing assistance to Azerbaijan in the establishment of an IP-based e-government infrastructure at the ministry.

Burkina Faso ITU provided technical assistance for the implementation of the "National IP Network Project for the Administration of Burkina Faso", Ouagadougou, Burkina Faso. This project will be implemented before the end of 2003.

Cameroon ITU is currently working on the implementation of an e-government infrastructure project with the Ministry of PTT aimed at creating efficiencies in government services and delivering e-administration services (e-payments, secure transmission of sensitive documents) to citizens. Funded by ITU, the European Union and the Government of Cameroon, this project is ongoing and scheduled to be operational in 2004.

Central America ITU is working on the elaboration of a regional strategy for ICTs in the Central American region in the domain of e-applications as part of the Connectivity Agenda for the Americas and Quito Action Plan. This activity was launched in the fourth quarter of 2003 and is ongoing.

Congo D.R. ITU will work on the implementation of e-services through the assessment of needs, the definition of technical and financial requirements and the proposal of a strategy, at the request of the Ministry of PTT. This project had to be cancelled on account of the current war and security risk in the region.

Georgia ITU worked on the implementation of an e-government infrastructure for digital certification and e-transactions capable of delivering e-services, at the request of the Ministry of Transport and Communications. Built on ongoing World Bank assistance in digitizing government documents, ITU's assistance provided highly secure IP-based solutions based on public key infrastructure to ensure data confidentiality, non-repudiation, data integrity and strong authentication. This project is operational.

Mauritania Funded mostly by ITU/BDT, this project aims to establish e-commerce legislation and an Internet access community centre (multipurpose community telecentre) for women in Mauritania during the first quarter of 2003. Legislation was adopted by the Parliament. The main deliverables of this project are e-commerce solutions for women through the community centre. ITU worked with the Government of Mauritania on another e-commerce project having a national scope, funded in most part by the Government of Mauritania. This project is now operational.

Mali This project aims to meet needs regarding technology, equipment and policy for the promotion of an e-learning service in Mali. ITU-D in partnership with Swisscom has started implementation of the IP project "Internet at school in Tombouctou". This project is operational.

Mongolia ITU worked on the implementation of an e-business infrastructure for digital certification and e-transactions capable of delivering e-services, at the request of the Ministry of Foreign Affairs. The project will be operational in the fourth quarter of 2003.

Paraguay ITU worked on the implementation of a digital certification infrastructure and applications for the delivery of secure e-applications for the Government of Paraguay. This project was partly funded by ITU/BDT with the participation of Paraguay. The project will be operation in the fourth quarter of 2003.

Seychelles — Implementation of an e-commerce infrastructure including secure e-payments to enable the sale of services and products. A first mission was undertaken by ITU in November 2002 to provide recommendations and a draft action plan to be adopted by the Government. Some ongoing and pending actions for this project include: refinement of the scope and requirements, the establishment of a task force and the identification of key stakeholders (e.g. merchants, banks and ISPs). This project is currently being implemented and scheduled to be operational in the first quarter of 2004.

3 Capacity building

3.1 Completed actions

Several training programmes have been undertaken to build local capacity in e-commerce, security and trust technologies and on the legal issues related to the use of these technologies. Training workshops have been organized for the Americas region, notably in Chile (for the Mercosur Member States), as well as for the Africa region, specifically in Senegal, and for the Asia and Pacific region, particularly in Pakistan. More than 27 courses and seminars on ICT have been given in the Centre for Training and Development created in Venezuela as a result of the ITU agreement with Fundandina. Some of these events are listed below:

Ecuador, Peru and Colombia — With the collaboration of ASETA, ITU gave basic training to public and private entities in Colombia, Ecuador and Peru on the legal aspects of e-commerce and secure e-transaction.

Switzerland — In November 2002, a World e-Trust Briefing Session for the Permanent Missions was held at ITU, Geneva, in order to inform them of the objectives of this new framework, the status, the activities and projects to be undertaken and how they could actively participate.

West African countries — *(Host country: Senegal)* – With the collaboration and assistance of SONATEL, ITU organized a subregional training workshop for Burkina Faso, Côte d'Ivoire and Senegal. The workshop addressed implementation and technology strategies for e-services infrastructure projects in these countries.

For 2003 and as in previous years, all project implementations have a capacity-building component.

4 Policies, strategies and e-legislation

4.1 Completed actions

Policy guidance and assistance to adopt appropriate strategies were provided to countries from all regions of the world through direct assistance, seminars, training workshops and conferences. Many countries have been assisted to adopt national (and regional) policies and strategies for the introduction of new technologies but more specifically, in the domains of Internet protocol and e-strategies. BDT also provided assistance to some countries to facilitate the adoption of a proper legal framework for e-applications. Some of these actions were undertaken in the Caribbean region, Pakistan, the Andean Community, Burkina Faso and Cape Verde.

In the face of rapidly evolving technology, a well-steered policy and a legal framework are critical to fostering an environment for secure e-services/applications to flourish in developing countries.

Activities to address e-application policies have taken place in Africa (Burkina Faso, Cape Verde, Cameroon, Mali, Mauritius, Morocco, Nigeria, Senegal and South Africa), Asia and Pacific (Islamic Republic of Iran, Lao PDR and Malaysia), Arab States (Algeria, Egypt, Kingdom of Saudi Arabia, the Sultanate of Oman, Tunisia and the United Arab Emirates), Europe and CIS (Azerbaijan, Belgium, United Kingdom, Romania, Russian Federation, Switzerland and Uzbekistan) and in the Americas region (Andean Community, Brazil, St. Lucia, United States and Venezuela). Some of these activities are highlighted below:

In 2002:

Andean Community — *Member States (Bolivia, Colombia, Ecuador, Peru and Venezuela) – March – April 2002:* At the request of the *Asociación de Empresas de Telecomunicaciones de la Comunidad Andina (ASETA),* discussed strategies and policy guidance towards the adoption of recommendations for a unique harmonized legal text on electronic commerce for the Andean Community Member States.

Burkina Faso — *(Host country) - November 2002* – Assistance was provided to regulators from Africa on e-commerce legislation with emphasis on a harmonized legal environment for the region. ITU provided training on the legal aspects of e-commerce and recommendations for the adoption of a law in this domain to representatives of the *Autorité de Régulation des Télécommunications* (ARTEL), the *Office National des Télécommunications* (ONATEL) and the Ministry of Communications, Burkina Faso.

Cape Verde — *September 2002*: At the request of the *Ministère des Infrastructures et Transports,* ITU provided a training session on the legal aspects of e-commerce and recommendations to representatives from the public and private sectors (businesses, telecom operator, banking) for the adoption of a law in this domain. This project was implemented and the law adopted by the Parliament.

Egypt — *December 2002:* A Regional Seminar on e-Business was organized to address the e-commerce policies and strategies for the Arab Region. Topics from e-security to business models, legal aspects and infrastructure were addressed with the objective of facilitating harmonized strategies for the region.

Romania — *May 2002:* ITU organized a regional event for the Central Eastern Europe (CEE) countries and the Commonwealth of Independent States (CIS) in cooperation with the Romanian Ministry of Communications and Information Technology (CIT), and the Secretary of State for CIT. This provided an exchange of views on e-commerce initiatives and the presentation of country projects, and it addressed challenges and successes and highlighted the need for regional strategies for the development of e-commerce. With the objective of addressing practical issues related to e-commerce, more than 20 presentations from countries, external experts and BDT were provided to cover security and trust, standards, legal issues, financial implications and national policy initiatives. The event also included panel discussions on best practices, appropriate strategies and successful models.

United States	*New York, January 2002: (Gender issues):* ITU, UNDP, and UNIFEM discussed and elaborated strategies for empowering African women in the use of information and communication technologies (ICTs) for socio-economic development.

In 2003:

Netherlands	*Amsterdam, October 2003:* A workshop was organized by the European Space Agency to establish cooperation on IP subsystems and applications with a view to future partnerships.
Cameroon	*Yaoundé, July 2003:* An international workshop on "South-South Cooperation and Cost-Effective Access to the Internet in Africa" was hosted by the Government of Cameroon and organized by ITU and UNDP with the objective of addressing policies and strategies for cost-effective Internet access in Africa.
Central America	E-applications (e-commerce, e-health, e-government and e-education) for Central America. The main objective of this activity is to assist countries in the Central American region in the elaboration of a regional strategy for e-applications. This activity will address the issues common to most e-applications and provide guidance and recommendations for the formulation of a regional policy and strategy for facilitating the implementation of projects in e-applications.
Mali	*Bamako, March 2003:* A workshop was held and attended by Malian officials, a Swisscom delegation and ITU to discuss implementation of the Internet at School in Mali project.
	Timbuktu, November 2003: Inauguration of the Internet at School in Mali project took place, hosted by Malian officials; both ITU and Swisscom participated in this event.
Mauritania	*Nouakchott, January 2003:* A colloquium on e-commerce was organized by the Secretary of State, the Ministry of Commerce, Crafts and Tourism and the Central Bank of Mauritania, ITU provided guidance and best practices on policies aimed at fostering the development of e-commerce in Mauritania.
Mexico	*Mexico City, November 2003:* ITU presented technology policies and strategies for building trust and confidence at the 5th Global Forum on Reinventing the Government, workshop on "New ICT and E-Government" hosted by the Government of Mexico.
Russian Federation	*Moscow, September 2003:* ITU organized an IP Symposium for CEE and Baltic States, hosted by the Russian Federation. This event resulted in a regional consensus on policy issues for IP addresses and ccTLD management as part of the Moscow Declaration.
Rwanda	*Kigali, July 2003:* An IP Symposium for Africa was organized by ITU and hosted by the Government of Rwanda. African countries met in Kigali to adopt the Kigali Declaration on IP Addresses and Domain Names. The Kigali Declaration was approved.

	Kigali, November 2003: A workshop was organized in the framework of the ITU/European Union partnership, to carry out a technical revision of the e-government project for Rwanda and to define actions, services and a timetable for implementation with the different stakeholders – IP-related.
Switzerland	*Bern, January 2003:* A meeting was organized by Swisscom in connection with the Internet at School in Mali Project and a further follow-up meeting took place in May 2003 – IP-related.
	Lausanne, February 2003: Visit to Lausanne of Burkina Faso delegation to the "*Centre Cantonal de Telecommunication du Canton du Vaud*" – VoIP communications in relation to the Burkina Faso National Project on IP Networks.
	Delemont, September 2003: Further follow-up meetings in connection with the Internet at School in Mali project took place. Swisscom, ITU and a delegation from the Ministry of Education of Mali were present.
	Fribourg, October 2003: A workshop was organized at Fribourg University on policy and IP connectivity within the framework of the DNS partnership with T-systems-Orange and Switch.
Tanzania	*Arusha, April 2003*: ITU Symposium: African ICT Roadmap in Support of NEPAD Objectives. The outcome of this meeting (Arusha Declaration) was a set of recommendations for policy-makers and international and regional organizations aimed at using ICTs to meet the NEPAD objectives. In the Arusha Delcaration, African delegates stressed the importance of ITU's support and active participation in providing assistance to Africa in the management of public Internet resources (IP addresses and ccTLD names).
Tunisia	*Carthage, October 2003:* A seminar was organized for the third round of ICANN meetings together with the Governmental Advisory Committee (GAC) meetings. ITU was represented – IP-related.
United Kingdom	*London, March 2003:* The annual meeting of the Global e-Sustainability Board meeting was hosted by BT, with the collaboration of UNEP and ITU. The output of ITU's contribution as one of the supporting organizations is the elaboration of strategies for dealing with the environmental impact of information technologies and telecommunications.
United States	*New York, June 2003:* A forum organized by UNICT on "Wireless opportunity for developing countries" with a view to preparing the "wireless access" WSIS side event – IP-related.
Uzbekistan	*Tashkent, October 2003:* Seminar on Standardization and ICT Development for the Information Society. This seminar was co-organized by ITU-D and ITU-T and resulted in guidelines for the elaboration of regional policies and strategies for IP and e-applications.
Syrian Arab Republic	For the Arab Region, ITU organized a regional seminar on e-education (including the use of the Arabic language) to address policies and strategies for fostering e-education in the Arab Region.

Tunisia As a global event, Tunisia will host the Third Telemedicine Symposium where strategies and policies to enhance the development of e-health will be elaborated. This event is planned for 2005 just before the second phase of the WSIS.

4.2 Actions launched in 2003

Azerbaijan *E-business infrastructure in Azerbaijan:* This activity is aimed at assisting Azerbaijan in the elaboration of a national policy to foster the cost-efficient development, deployment and use of e-business. Through a workshop organized by ITU and hosted by the Government of Azerbaijan, the main challenges faced by Azerbaijan were addressed. ITU provided guidelines and best practices on the technology aspects of e-business and also assisted in the formulation of an action plan for e-business implementation.

Burkina Faso *National IP-based network in Burkina Faso:* ITU provided technical assistance for the implementation of the "National IP Network Project for the Administration of Burkina Faso", Ouagadougou, Burkina Faso. This project will be operational in 2003.

Cameroon *E-government project:* Implementation of e-government infrastructure to enhance government services to citizens, enable cost-efficient and secure communication and exchange of government documents and provide solutions for the electronic payment of government services by citizens. Funded mostly by the European Commission, ITU and the Ministry of Posts and Telecommunications of Cameroon, the implementation and coordination of this project was carried out by ITU. Scheduled to be operational at the end of 2003, this activity also includes technical assistance provided by ITU in the elaboration of a national IT strategy for the Ministry of Posts and Telecommunications of Cameroon.

Congo D.R. *Creation of Internet Nodes in Congo D.R.:* Project aimed at implementation of Internet nodes and development of new information and communication technology applications in the Republic of Congo. Identification of needs for technical assistance within the general framework of IP-based networks and implementation of Internet nodes, bases for the convergence of multimedia networks in the Republic of Congo. Project to be implemented before end of 2003.

Islamic Rep. of Iran ITU is working with the Islamic Republic of Iran in elaborating policies and strategies for the implementation of e-commerce and e-finance. This action is to be funded by the Ministry of Post, Telegraph and Telephone (MTT).

Georgia *E-government project:* This ITU project addresses its challenges by delivering cost-effective solutions for the secure transmission, access and processing of digitized government documents thereby increasing the efficiency and transparency of government services. Senior officials of the Ministry of Transport and Communications of Georgia will be provided with solutions to enhance workflow automation, to enable officials to digitally sign and disseminate official documents thence replacing the slow and rather expensive paper-based methods. Authorized access to sensitive

documents will be made possible through security and trust solutions to establish the identities of authorized personnel within the ministry. The project also takes into account the interoperability of these new solutions with existing information technology systems at the ministry. Commenced in July 2003, this project is now operational.

Mongolia — *E-government project:* This action aims to assess the needs in the technology, policy and legal domains for the promotion of an e-government service in Mongolia. It also includes the implementation of e-government infrastructure to enhance government services to citizens and enable cost-efficient and secure communication and exchange of government documents. One of the deliverables is an intranet to enhance electronic collaboration within the Ministry of Infrastructure. The project will complement the efforts of the Government of Mongolia to facilitate the development and implementation of the e-government application by making specific inputs to it. This project will be operational before the end of 2003.

Mali — *E-education project:* This project aims to assess the needs in the technology, equipment and policy domains for the promotion of e-learning in Mali. ITU-D in partnership with Swisscom started the implementation of the IP project "Internet at school in Tombouctou" in Mali in March 2003. The project is now operational.

Krygzystan — *E-agriculture project:* Concerning the main sector in the country, this project aims to assess the needs of the agricultural sector in relation to the potentials of ICTs and work towards the implementation of a project in the rural area where ICTs can bring direct benefits to farmers and other stakeholders in the agricultural sector. ITU will assess needs, define technical and financial requirements and propose an action plan for the project implementation. With the participation of the Government of Kyrgyzstan, this project is planned to be operational before the end of 2003.

Paraguay — *E-government project:* Providing a secure and trusted Internet-based mechanism for operators and service providers to send sensitive information (such as income declarations) in electronic format to the national regulatory agency (CONATEL). Using ICT tools to facilitate the process of issuing licences to operators of public telephones. The solutions should also enable CONATEL to issue licences in electronic format, and to implement solutions to enable secure communication between CONATEL and its clients. This project will be operational before the end of 2003.

Seychelles — *E-commerce infrastructure/services in the Seychelles:* ITU worked on the implementation of secure electronic transaction infrastructure and e-services for the Government and business sectors, at the request of the Vice-President of the Republic of Seychelles. A first mission was undertaken by ITU to provide recommendations for the e-commerce strategy to be adopted

by the Government, and produced the following recommendations: a task force needs to be established to begin work on a pilot project; the interested stakeholders (merchants, banks and ISPs) need to be identified; the local acquiring banks need to provide required services for Internet merchants; actions should be started to better understand how to deal with some of the local challenges; there is a strong need for a common government strategy and vision on e-commerce; and the Government needs to roll-out e-government.

5 Partnerships

Working with partners is essential to meet the objectives of ITU/BDT especially in the domain of e-commerce. This is so because there are many components and skills required for the successful implementation of e-commerce services that need the collaboration of other partners. To this effect, partnership agreements have been established with FUNDANDINA of Venezuela, WISeKey, Goodwin Proctor LLP and World Trade Center Geneva.

FUNDANDINA

The partnership with FUNDANDINA of Venezuela, the first e-commerce partnership, has led to the establishment of a centre for IT training in Venezuela, the creation of more than 90 Internet portals and the establishment of e-commerce solutions.

WISeKey and World Trade Center Geneva

Activities in relation to the ITU-WTC-Geneva and WISeKey partnership have resulted in a number of beneficial services for the ITU membership including the workshop with the participation of more than 120 countries to discuss technology strategies for the implementation of secure and trusted IP-based infrastructure for e-business. This agreement also resulted in operational infrastructure for digital certification in a number of counties from most ITU regions.

Goodwin Proctor LLP

The agreement with Goodwin Proctor LLP expired and was not renewed after the first year. Goodwin Procter LLP provided pro bono assistance to Mongolia in e-legislation. To address the needs of Member States in e-legislation, ITU worked with United Nations Commission on International Trade Law (UNCITRAL) to assist Member States in establishing e-commerce legislation. This collaboration has already yielded positive results in Burkina Faso and was used for Cape Verde and Mauritania in 2003.

World e-Trust MoU

To address the needs of a multilateral, technology-neutral and inclusive framework where developing countries will work together with industry partners in the same spirit and towards the achievement of well-defined objectives, the World e-Trust Memorandum of Understanding was launched by ITU just before WTDC-02. As of March 2003, 48 entities represented by governments, industry and various associations from 35 ITU Member States have already embraced this framework. For developing countries, the signatories include 14 ministries (including 9 ministers) and heads of regulatory agencies. World e-Trust aims to bring together various stakeholders to work towards extending the deployment of e-applications (e.g. e-commerce, e-business, e-government, e-learning, and e-health) infrastructure and to provide the required security and trust for e-applications and other value-added services to bring the benefits of ICTs to developing and least developed countries.

Sysnet Ltd

This new partnership was signed in October 2003. Pakistan Development Gateway Foundation (the Foundation) is a World Bank initiative and an independent entity, of which the Government of the Islamic Republic of Pakistan is a founding member. Its mission is to harness the potential of information and communication technologies for sustainable development in Pakistan. ITU will assist in setting up an e-applications infrastructure using public key infrastructure (PKI)-enabled solutions in the Islamic Republic of Pakistan.

European Union

ITU has established an agreement with the European Union for the implementation of ICT applications to meet the Millennium Development Goals. Within the framework of this agreement, EC is providing more than USD 1.2 million to fund the implementation of e-government projects in three developing countries in Africa and Europe. ITU, Cameroon and Rwanda will sign the project documents during the World Summit on the Information Society in December 2003.

WHO

ITU and WHO are collaborating to establish health academies in developing countries worldwide. This partnership_will bring knowledge and know-how in health and disease prevention into the domain of the villagers, the community and the majority of the population of most countries and especially the underprivileged in the least developed countries.

6 Conclusion

6.1 Observations

The constantly changing technology environment and the low time-to-deploy for the roll-out of new technology services/applications imply several adjustments between the initiation and completion phases of a project.

The purpose of Programme 3 goes beyond the implementation of e-services/applications. These ICT solutions need to bring benefits to the populations of developing countries and in this regard they need to also address business models for sustainability. Some projects reported as implemented are facing new challenges in the provisioning of sustainable services. There is a need for the post-implementation issues of these projects to be addressed in the design phase.

Sound policies in the domain of the Internet are key to the successful implementation of IP application projects. In some of the countries, the absence of national IP policies is a barrier to the widespread use of the Internet.

In the area of e-commerce, there are several non-telecommunication services (such as banking, logistics, auditing, tracking and insurance) that play an equally important role in the deployment of such infrastructure. The absence of a direct relationship mostly with the financial sector, and the low level of awareness in the banking sector of several developing countries regarding e-payment services/applications, create additional challenges as banking services and private financial networks need to be directly connected to the e-commerce infrastructure for the delivery of secure e-payment solutions.

6.2 Proposals

a) E-commerce is one of several e-applications with much the same requirements as many others. Strategies and guidelines for their implementation need to take into account the synergies that exist between the various e-applications.

b) Some common challenges such as e-security and trust need to be addressed for all e-applications in order to reduce the overall cost of implementing the desired security for these applications and services. E-security strategies and policies need to take into account the overall needs of various e-applications.

c) Innovative ways of establishing partnerships that take into account the various sectors involved and their interests are necessary for meeting the challenges for implementing e-commerce solutions. World e-Trust has been put together to meet these challenges and could be an appropriate vehicle for meeting the common objectives of e-applications.

d) Even in cases where it is possible for these infrastructures to be remotely hosted in industrialized countries, it is important that efforts be made so that developing countries play an active role in acquiring the skills and enabling the transfer of these technologies. Emphasis needs to be put on having e-applications infrastructure hosted and run in developing countries.

e) As countries roll-out e-application services, it is necessary for appropriate business models to be developed that take into account local requirements in order to ensure long-term sustainability.

Attachment 17

Enabling e-commerce

Table of contents

Enabling e-commerce

The main issue of e-commerce is to understand how to secure all transactions between providers and clients and how to control that entire flow in a real application. The main goal of this chapter is not to discuss all possible ways to do e-commerce (see the tutorial for that) but to give practical security recommendations for implementation and application of selected relevant business models.

The following details use cases of the traditional business model known as super-distribution applied to digital e-commerce environments. Digital music purchase and consumption and distance learning are the usage scenarios taken into account. Functional and non-functional requirements for the correct exploitation of the trading cases are provided. An analysis of the security of the entire process in terms of intellectual property management and protection is performed and related security requirements provided. The use cases described are appropriate for adoption in trials of the technology being developed in "MOSES", a European project (IST 34144).

This document describes the "network system" requirements, trying as much as possible to avoid imposing a specific implementation model. Therefore, no reference is made to a specific content format or to any cryptographic processing.

Some main usage scenarios are described in more detail, and functional and non-functional requirements are provided. Different use cases for each usage scenario are detailed, every use case introducing new available options for content purchase, consumption and distribution. Lastly, requirements for safe (in terms of intellectual property protection) handling of the content and the process for its trading are presented, to be understood as an example for real field applications.

1 Usage scenario 1: digital music distribution

It is assumed that either a physical or an electronic commercial infrastructure to sell and deliver digital music (possibly stored on physical media) to the users is in place. It is also assumed that the user is equipped with a player that is able to play protected content according to the associated rules. The use cases described in the following paragraphs present an increasing level of complexity. Except where expressly specified, every new use case encompasses the features of all previous cases.

The user is supposed to be able to browse over the Internet by means of a web browser running on either a personal digital assistant (PDA) or a personal computer (PC).

2 Music production and distribution

The content is made available to customers by a producer (content author) and a distributor (service provider). The mechanisms protecting the music intellectual property ("tickets" and IPMP tools) can be provided either by one of the aforementioned parties or by a third party ("ticket" and IPMP tools provider).

3 Identity registration

Summary: Prior to executing any transaction within the considered network system, users must first register to receive their identity information. All processes require that users present their identity credentials in order to preserve a high level of security and trust between users and the various services.

However, since the network system is comprised of both "business-to-business" relationships (content distributors, content creators, web retail partners, network services) and "business-to-consumer" relationships (end consumers, web retail partners, network services), it requires that identity be managed differently for each type of relationship.

Thus, the registration of identity within the network system will support the characteristics of both *Consumer Identity* and *Agent Identity*.

3.1 Consumer Identity registration

Description: Consumers may typically choose to become members of the network as the result of a web promotion by a network business partner, as a by-product of choosing downloadable music/movies from a retail website, or as a student registering with the tele-education services offered at his/her school. In general, during the registration process the user will be asked to submit information about his/herself ("profile information") and to choose information that will be used by the network system during authentication (e.g. username/password or pass-phrase). Once received, the authentication service will construct the appropriate credentials to be used for subsequent network transactions. These credentials will be returned to the user and stored securely on the user's PC/PDA/set-top box.

Main flow: In order to satisfy the Create Consumer Identity request, the requesting entity must send the following information to the authentication server (*note: the user's information is typically, but not limited to, the following*):

1) User authentication information (e.g. network system username, password, etc.)

2) User profile information (e.g. e-mail address, street address, etc.)

When the authentication server receives the above information, it will create the appropriate records in the database for this user. The authentication server will then create the appropriate credentials that will be used to securely identify this user for all subsequent network transactions. This information will be returned to the user for safe storage on their local PC/PDA/set-top box file systems.

Error conditions: The following will cause exceptions to be raised during the processing of the Create Consumer Identity Request:

- User indicated by the supplied information is already an existing member of good standing in the network system and of the same type ("consumer").
- User indicated by the supplied information is a member whose privileges have been revoked by the system.
- User has supplied erroneous information that cannot be validated.

Security considerations: It is conceivable that the Create Consumer Identity request can be submitted only by those network affiliates that have gained appropriate security status (i.e. web retail partners, validated educational institutions, content owners, content distributors) and all other network requests of this type from unauthorized sources will be denied.

3.2 Agent identity registration

Description: Within the network of business partners (web retail partners, content distributors, etc.), it is desirable to allow certain transactions only to those members that have special security status within the system. Given the inherent financial, personal and copyright implications of the misuse of certain services, greater scrutiny may be necessary to ensure proper accountability and protection from malicious activity (e.g. denial of service attacks, improper licensing of content, invalid content created for unlawful distribution, etc.). Thus, it is conceivable that the registration of these business partners ("agents") will require a special case of the consumer identity registration scenario. Although these *agents* are still, in effect, *consumers* their business status should allow them to access enhanced services such as Content Preparation, Licensing Authorization, Consumer Registration services, Content-Metadata Registration, and so forth.

Main flow: Since the electronic registration of the network business partners should require greater scrutiny, it is conceivable that this will be a function of some prior "manual" business correspondence between the prospective affiliate and the network governing body (e.g. signed contract, licensing information, etc.). Once the proper arrangements have been made, the agent may commence the electronic registration process.

In order to satisfy the Create Agent Identity request, the requesting entity must send the following information to the authentication server (*note: the user's information is typically, but not limited to, the following*):

1) User authentication information (e.g. network username, password, etc.)

2) User profile information (e.g. e-mail address, business street address, etc.)

3) Affiliate type (e.g. web retailer, content distributor, etc.).

When the authentication server receives the above information, it will create the appropriate records in the database for this user. The authentication server will then create the appropriate credentials that will be used to securely identify this user for all subsequent network transactions. This information will be returned to the user for safe storage on their local PC/PDA/set-top box file systems.

Error conditions: The following will cause exceptions to be raised during the processing of the Create Consumer Identity request:

- User indicated by the supplied information is already an existing member of good standing in the network system and of the same type ("agent").
- User indicated by the supplied information is a member whose privileges have been revoked by the network system.
- User has not been activated by the network governing body as an "agent" user type.
- User has supplied erroneous information that cannot be validated.

Security considerations: The Create Agent Identity request can only be submitted by those members (or prospective members) that have obtained the appropriate security status. All other network requests will be denied.

3.3 Content distribution

In a content distribution system, it is possible to identify the following entities:

1) *Content author.* This is the author of mp4 content.

2) *Publisher.* This is the publisher of mp4 content.

3) *Distributor.* It takes the content from the publisher and gives it to the front-end seller.

4) *Front-end seller.* This is the actual seller of the content (i.e. online music store).

5) *Purchaser.* The purchaser can be either the end-user or a company that buys mp4 content from front-end sellers or from the distributor. They buy licences and give them free to users, asking in return for personal data about the users. These data are valuable information for companies: they may be used for future marketing actions.

How the aforementioned entities may interact in a real scenario is shown in the following example describing a contemporary commercial initiative.

3.4 Example of distribution

An example of a situation in which the purchaser is a company that after the purchase acts as re-distributor may be found in the action made by Sprite (Coca Cola Company) in Italy:

Buying a bottle of Sprite, a user finds a code on it. Linking to the Sprite site (http://www.thespriters.it/1sprite1song/index.php), the user has to subscribe first and then he has to write the code in a reserved area. In this way, he gets the chance to download an mp3 file free.

In this case, Sprite is the purchaser company that buys the copyright from the author and then distributes the content.

How the Sprite system works:

- Downloading a file
  - The user has to subscribe giving his personal data. He has to choose a username and a password to access the mp3 download area and the system that gives the licences to listen to music.
  - After the subscription, the user can choose his favourite music file among the available titles, and then has to click on *download*.
  - A window opens and the user has to enter username and password. Afterwards he has to enter a code: the one written on the purchased Sprite bottle.
  - The file download is authorized only if all the requested data are correct. After a confirmation message, the download starts automatically.
  - The file is saved on the computer with the .zip extension. The name of the zip is the same as the chosen mp3.
  - When the file is extracted, it is possible to listen to it on Windows Media Player. At the same time, the browser opens a window for the licence request. The user has to enter again username and password. If he is authorized to get the licence, it will automatically be installed on the computer to allow listening.
  - It is important to ask for the licence within 72 hours following the download, otherwise it is cancelled from the database.

- Rules and terms
  - The code has to be valid for this initiative.
  - Every code can be used only once.
  - The code cannot be used to download the same song more than once.
  - A user can download only 100 songs during the whole initiative, with a limit of 20 songs per day.
  - It is possible to download only 100 songs, with a limit of 20 songs per day on the same computer. This means that if several users share the same computer, they can only download the above-mentioned allowed number of files.
  - There has to be at least 15 minutes between downloads.
  - It is not possible to allow a new download if the previous one has not ended.
- What is a file licence?
  - To listen to the downloaded song, it is necessary to have a licence. For each new song there has to be a new licence.
  - All the music files are protected to respect copyrights. Only authorized users, upon subscription, can request and obtain a download licence to listen to their favourite song.
- How the licence works
  - The file licences bind the listening of the file exclusively to the computer where the file has been downloaded. The licence ends on 31 December 2002. If the user tries to modify the licence, it will be temporarily disabled and the file will not work any more.
  - Licences are completely free.

According to this structure, it is possible to define the following events:

- The author sells his content to a publisher and is paid for it. If the publisher is the music store, the author will receive a one-off fixed payment, or a fixed amount of money with a percentage according to how many copies of his "content" the publisher will be able to sell.
- The publisher will provide the front-end seller with the content through the distributor.
- The user will be able to purchase the content with the ticket mode.
- When the user purchases the content and the licence, he becomes the content owner. In this way, he can either distribute his own content to others (user becomes re-seller as in the case of Sprite), or simply be the end user of the purchased content.

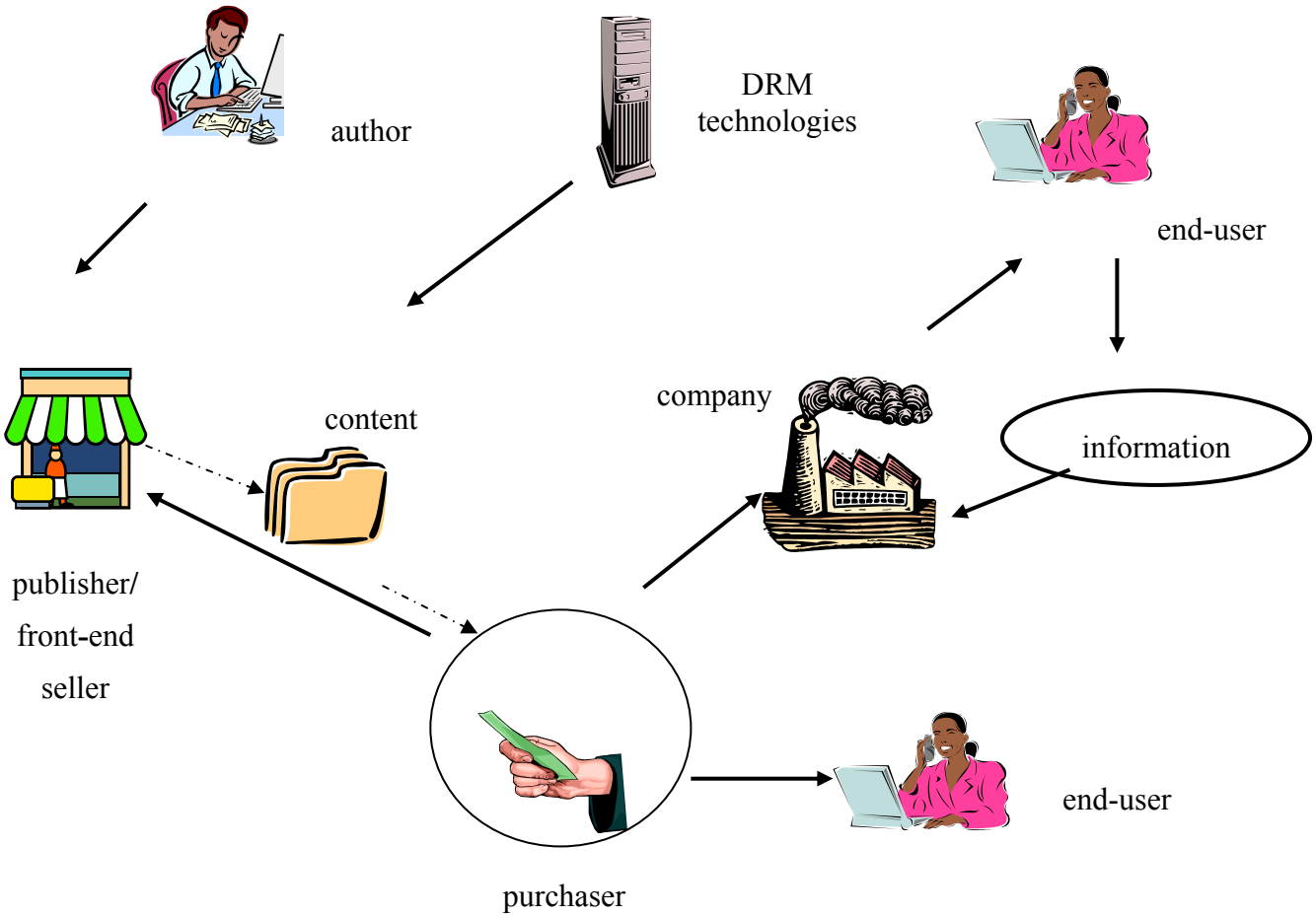


Figure 1 – Content distribution chain

In the knowledge that in some cases the publisher, distributor and front-end seller are the same entity, in Figure 1 the possible relationships partially described above are shown:

– Author sells content to distributor.

– Front-end seller buys content from distributor.

– Purchaser buys content from front-end seller.

– Front-end seller receives money from purchaser, who may receive information from end-user.

Front-end seller and purchaser can be the same entity if some kind of personal information is required to the end-user as payment. This can represent considerable added value for some companies.

4 Ticket production and association to content

Summary: In a response to a network request, the licence server checks the authorization for a particular user, for a specific right or rights, for access to a specific piece of content. If it is determined that the user has the appropriate security level, an authorized ticket is constructed on behalf of the network user that grants him/her the requested rights to that content only.

Physical tickets may be constructed by the licence server and delivered to the user in two ways:

1) When the content rights are purchased at the retail website, the associated licence authorization is saved to the database. The physical licence ticket is then constructed and returned to the user via his/her web browser and saved to the file system of the PC or PDA.

2) Content rights are purchased at the retail website and the associated licencing authorization is saved to the database. However, the physical licence ticket is delivered at a subsequent time (for example, during the rights validation process within the client playback scenario).

To facilitate the above, the licence ticket production process could be implemented in two steps:

- *Create licence authorization* – the licence authorization information is created and stored within the master databases for specific rights to specific content on behalf of specific users.
- *Create licence* – the licence server checks for existing licence authorization information in the database. The licence server then constructs a valid licence ticket, and returns this to the requestor.

5 Create Licence Authorization request

Description: A user browsing a retail website for downloadable music or movies may initiate the licensing authorization creation request to the licence server by choosing to purchase the offer being displayed. Once the payment has been authorized, the website may make a secure, authorized request to the licence server to create the database authorization information necessary to construct a physical ticket upon subsequent licence requests.

Main flow: In order to satisfy the Create Licence Authorization request, the requesting entity must send the following information to the licence server:

1) User's identity (or blank for "ALL" users)

2) Content identity

3) Rights information (all constraint information contained in the offer necessary to construct the licence authorization, e.g. expiry date, right (PLAY, BURN, etc.), number of plays).

When the licensing server receives the above information, it checks for the existence of the content by querying the database using the supplied Content Identifier. The licence server then checks for the existence of the user by querying the database using the supplied User Identity. If both are found, the licensing server constructs the appropriate licensing authorization in the database by linking the User Identifier to the Content Identifier, and finally to the rights information, limiting the licence by the supplied constraints.

The licence server responds to the requester with an appropriate response message indicating the results of the transaction.

Error conditions: The following will cause exceptions to be raised during the processing of the Create Licence Authorization request:

- User indicated by supplied User Identity is not a valid member in good standing or cannot be found in the database.
- Content indicated by supplied Content Identity is not valid or cannot be found in the database.
- Rights/constraints indicated by rights information in the request are invalid or disallowed by the content distributor.

Security considerations: The licensing server will satisfy requests for the creation of licensing information only from entities that have the appropriate security status. Only those retail partners that have authorized the user's payment for content may make this request.

5.1 Create Licence request

Description: As the result of an authorized purchase of content rights (as described above), an authorized entity may make a secure request for the licence server to create a physical licence ticket for a specific user.

Main flow: In order to satisfy the create licence request, the requesting entity must send the following information to the licence server:

1) User Identity

2) Content Identity

3) Rights information (optional. In general, the player will govern which "verb" the user has chosen (PLAY, BURN, etc.) based upon his/her actions.)

When the licence server receives the above information, it begins the process of checking for licence authorization for the specific content by querying the database by Content Identifier and User Identity. If the licence authorization information is found, a licence ticket is created for all the rights and constraints found within the licence authorization. The ticket is subsequently returned to the requester.

5.2 Licence components: A licence has the following characteristics/components:

– A licence may be used only by those principal entities designated within the licence. The authorization process must be able to prove ownership. The licence therefore contains the user's identity. (*Cryptographic example*: embedding the user's public key within the licence).

– It must be difficult to forge a licence. Proper techniques will be implemented to ensure that the licence was created by an authorized entity and has not been tampered with. Licence contains proof-of-authenticity. (*Cryptographic example*: hash of the licence bytes are encrypted with private keys of trusted hosts (CAs). Signatures are checked against locally calculated hashes).

– A content licence must be implemented such that content streams cannot be forged or substituted within licence structures. (*Cryptographic example*: during content preparation, hashes of the content streams are signed by trusted hosts. Content signatures are stored within the licence and checked during playback.)

– Licence contains all grants/constraints for the specific digital work.

Error conditions: The following will cause exceptions to be raised during the processing of the Create Licence Request:

- User indicated by supplied User Identity is not a valid member in good standing or cannot be found in the database.
- Content indicated by supplied Content Identity is not valid or cannot be found in the database.
- Licence authorization cannot be found for User Identity and Content Identity.
- Rights/constraints indicated by rights information in the request are invalid or defined in the licence authorization information.

Security considerations: The licensing server will satisfy requests for the creation of a licence only from entities that have the appropriate security status. Only those users that present valid security credentials will be allowed to make licensing requests to the server. All other network requests will be denied.

Use case 1: Limited play (free trial)

Summary: The user gets a free "ticket" that entitles him/her to play a piece of protected music either for a limited period starting from a fixed date and time or for a limited number of times.

Description: The user browses the website of a music site which offers a 24-hour free trial of the music tracks that are on sale. The user decides to try one free listening, so he downloads the protected music of his choice. The website informs the user that he will be able to listen to the music free for 24 hours; after that time the user will have to buy a proper licence.

The ticket is protected in such a way that it can be used only by the legitimate user. If the user copies the ticket and distribute it to his/her friends, they will not be able to use it.

When the user wants to play the music, he/she will be required to "show the ticket", and to prove his/her identity. The player then checks the validity of the ticket and the entitlements contained in the ticket, including in this case the time limitation of the entitlements. Once the ticket has expired, the ticket is automatically removed from the player storage. However, the system will record the fact that the free ticket has been used, and will not allow any further free ticket for the same music to the same user.

If all required conditions are met, the user is allowed to play the music.

Error flows: If one of the following arises, the player will refuse to play the content:

- the user is not the legitimate owner of the ticket
- the ticket entitlements do not match the operations required by the user (e.g. the user chose to EDIT the content, but the ticket entitles him/her only to PLAY it)
- the ticket is associated with a different content
- the ticket is not yet applicable
- the ticket has expired.

Use case 2: Unlimited play

Summary: Once the trial period has expired either in terms of number of consumptions or elapsed time the user buys a "ticket" that entitles him/her to use the protected content for an unlimited period. In the following, we assume that the user buys a ticket that allows the unlimited play of a specific content, with no other permission (e.g. the user cannot copy this entitlement to a friend). We also assume that all transactions are done electronically, however this does not mean that a permanent connection to the Internet is required in order to use the "ticket".

Description: The user browses the website of a service provider containing audio clips of his/her favourite band, and decides to buy one of them. The user then performs an electronic transaction and buys the "ticket" that entitles him/her to perform unlimited play on the selected audio clip.

The ticket is delivered to the user at the end of the transaction and it is then the responsibility of the user to keep the ticket in a safe place and to use it in an appropriate way. The user also downloads the audio clip, and stores it in his/her own "audio clip player".

The ticket is protected in such a way that only the legitimate user can use it. If the user copies the ticket and distributes it to his/her friends, they will not be able to use it.

When the user wishes to play the audio clip, he/she will be required to "show the ticket", and to prove his/her identity. The player checks the user's identity, then the validity of the ticket and the entitlements contained in it, and finally informs the user of the result of the check. For example, if the check detects that the user is the legitimate owner of the ticket and that the ticket entitles him/her to play that specific content, the "play" button is enabled.

The user then plays the audio clip.

Variants: If no e-commerce infrastructure is in place, the same operations can be performed using a physical distribution network. For example, once the user has selected the content he wants to buy, he goes to a shop where he buys both the "ticket" and/or the content on a physical support. The ticket is a piece of information either known or owned only by the customer (e.g. a sequence of numbers printed on a piece of paper or a hardware token to be inserted into the player). The first time the user requires the player to play the content, he will be required to "show the ticket"; he then "shows the ticket" according to the physical support chosen (inputs the sequence of numbers contained in the ticket or inserts the hardware token received at the moment of the purchase). The player validates the ticket, stores the ticket locally for future use, and then plays the content. Since the ticket is now stored in the player, the user doesn't need to repeat the ticket input when he wants to play that content again. Of course a hardware ticket will require that the player device supports it (i.e. embedded smart-card reader).

Error flows: If one of the following arises, the player will refuse to play the content:

- the user is not the legitimate owner of the ticket
- the ticket entitlements do not match the operations required by the user (e.g. the user chose to COPY the content, but the ticket entitles him/her only to PLAY it)
- the ticket is associated with a different content.

Use case 3: "Send a copy to a friend"

Summary: The user buys a "ticket" that entitles him/her to use the protected content and to transfer either the entire set or a subset of his/her entitlements to his/her friends or relatives. The operations can be for example PLAY, EDIT, MOVE, COPY, etc., or a combination thereof.

Description: Alice browses the website of a music store and decides to buy a "ticket" that allows her to play a piece of music she likes very much without limitations. Since she wants to share her music with her friends, the ticket she buys also allows her to distribute some copies of the protected content in a legitimate way. The number of allowed copies is limited, e.g. only 5 copies. The people receiving a copy of the ticket will not be allowed to make any further copy, so she is the only one who can distribute her own rights.

Variants: The copies could possibly have limitations that were not originally present in the original ticket, e.g. they could be valid for 30 days and then expire.

Error flows: The copy will not work when:

- the number of actual copies exceeds the limits imposed in the original ticket
- the original ticket has expired
- the original ticket does not allow copies.

Use case 4: "Crash recovery"

Precondition: The user owns a collection of "tickets" that entitles him/her to play without limitations his/her preferred music tracks. The tickets are stored on the user's portable device together with the content, and a backup copy is available on his/her PC. Unfortunately the user's portable device crashes, so he/she has to buy a new one. Now, the user wants to recover from the crash all his/her music collection, using the backup copy of his/her entitlements and of the related pieces of music stored on the appropriate storage devices (PC, CD, various memories supports etc.).

Description: Alice is a careful customer who knows the value of the goods she bought on the network, so she always makes a backup copy of the "tickets" she buys on her PC. One day, her portable music player crashes, and all tickets stored in the player are lost together with the music. Therefore she buys a new player and loads all backup copies of her tickets into the new player. Then she downloads the content from the network or from any other backup device she owns (CD, PC, other storage devices). She can then listen again to her preferred music.

Variants: The backup service could be provided by the e-commerce site selling the tickets, however if Alice buys music from several different music stores, probably she has to download the backup copies of the tickets from each of them. If the download is done automatically by the player, this is not a problem.

Error flows: Of course this scenario assumes that the new player has the same functionality as the old one, including the security-related features. The restitution of lost tickets will fail if:

- the user is not the legitimate owner of the tickets
- the ticket has expired
- the system requirements specified by the content vendor are not satisfied by the new device.

Comments: This use case has one main consequence: it is not possible to match the user identity with the identity of the player he/she uses.

Use case 5: "Floating licence"

Precondition: The user owns some "tickets" that do not allow copies. However, the user wants to be able to listen his/her favourite music on different devices, like his/her car stereo when he/she is driving, or his/her personal device when he/she is walking in the street.

Description: Alice owns two players, one is a portable device, and the other is a car stereo. Usually Alice downloads the music she likes on to her PC, and then copies it into the two players. However, since music is protected, she also has to download the associated ticket to the PC first (where she keeps a backup copy of all her electronic goods), and then into the two devices. Then, when she is travelling by car, she identifies herself to the car stereo, so that the car stereo can validate all her tickets and allow her to listen her favourite songs. When she leaves the car, she removes her identification token and plugs it into the portable device, so that the portable device can validate all her tickets. If her brother Bob uses the same car, when Bob identifies himself, the car stereo will validate Bob's tickets only, even if all Alice's tickets are stored in the car stereo memory.

Error flows: This scenario assumes that the car stereo has the same functionality as the personal device, including the security-related features. The use of tickets will fail if the conditions associated with the content are not met, as in the previous cases:

- the user is not the legitimate owner of the tickets
- the ticket entitlements do not match the operations required by the user
- the ticket is associated with a different content

- the ticket is not yet applicable
- the ticket has expired
- the device is not recognized as an authorized platform.

Functional requirements: This section provides requirements concerning the functionality needed so that the aforementioned use cases can take place as described. Since the aim of the entire system being studied is to achieve content fruition in accordance with acquired usage rules, the most important requirements deal with secure content management and its protection from abuse. Other requirements related to diverse infrastructures needed (connectivity, storage capacity, user interface) are also provided.

Security requirements: Within the domain of information technology (IT) systems security, the recognized tenets of security are:

- *Confidentiality*: protection from disclosure to unauthorized persons.
- *Integrity*: maintaining data consistency.
- *Authentication*: assurance of identity of person or originator of data.
- *Non-repudiation*:originator of communications cannot deny it later.
- *Availability*: legitimate users have access when they need it.

  Access control: unauthorized users are kept out.

Through the analysis of the different components of the systems, such requirements will be taken into account and detailed according to the different aforementioned use cases.

The player: The secure player must be able to

1) authenticate the user;
2) validate "tickets" (licences);
3) compare the rules associated with each protected content with the entitlements stored in the associated ticket owned by the user;
4) deny or allow content use accordingly;
5) allow secure transfer and handling of sensitive content (credit cards numbers, passwords).

The following paragraphs describe each item in more detail.

User authentication: The basis for the implementation of each usage scenario described above is the ability to identify the user in a secure way. Moreover, the user authentication must be repeated every time the user requires a privileged operation to be performed on the protected content, otherwise a user can identify himself on a device once, and then let all his/her friends use the device forever!

The user identification must be different from the identity of the device that is used to play the protected content, otherwise

- a crash of the player would be unrecoverable;
- using the content on different players would be impossible.

A simple solution is to use a physical token (i.e. a smart card) able to represent the user each time the user authentication is required. However, this requires a smart cart reader on each player device. The physical token shall be activated by the user every first time it is used after a device has been reset (player switched off and then on, or smart card extraction and re-insertion). A personal identification number (PIN) request by the token can implement this mechanism.

Another solution is to use a password that will expire after a while, e.g. every day, but this means that the user has to contact the service provider site each day to know his new password. It must be verified whether this is acceptable by users for a commercial service.

Ticket validation (integrity): This is a process whereby the player recognizes the user as the authentic owner of the licence stored in the form of a "ticket". For the user, the ticket can be just a sequence of numbers. But the player must be able to interpret the ticket, and to verify whether or not the user claiming to be the owner of the ticket is the real owner or false.

Rules parsing: There are rules associated with content ("content rules") which are generic, and rules specific to each single user ("user rules") contained in the "ticket".

Content rules: Content rules are generally embedded in the content itself. They contain at least the following information:

- the content unique identification,
- the unique identifiers of the IPMP components (e.g. crypto algorithms, watermarking algorithms) that must be employed by the player in order to use the content.

The first information allows the player to match content and user rules, while the second allows the service provider to associate every piece of distributed content with the best IPMP tools assortment that matches his/her security requirements. Such modularity of the protection system allows its easy update (i.e. to change a cryptographic algorithm when it is assumed to have been cracked). Of course, the update applies to new content only. In any case, this means that the player must have the ability to recognize that it needs a missing component, and to automatically download and install it.

User rules: Once the ticket has been validated, it must be parsed to extract the information contained in it. This information cannot be changed in any way by the player or any other entity, otherwise a user could entitle himself to do whatever he/she wants with the content without paying. The parsing process reads each field in the ticket structure, which may contain information like:

- the unique id of the content to which the ticket applies;
- the date from which the ticket is valid;
- the date of expiring;
- the operations that the user is entitled to perform on the content (e.g. PLAY, EDIT, RELEASE, etc.);
- for each allowed operation, the number of repetitions permitted;
- the secrets needed in order to perform the operations to which the user is entitled.

Great care must be taken by the player in handling this information, since it fully governs the use of the content and as such, it could be a possible point of attack by malicious users.

Rule enforcement (access control): The player evaluates the rules associated with content and the rules contained in the "ticket", and applies the result of a match between them. If the match is positive, the player applies the user rules granting or denying access to each specific content use as expected.

Secure transfer and handling of content (integrity, confidentiality): Every piece of sensitive information required during the process of content use shall be protected from abuse. Such protection includes:

- the content;
- the associated ticket;
- personal information related to the user (e.g. credit card number, electronic wallet PIN).

Techniques that are likely to be adopted include cryptography for the prevention of unauthorized access to sensitive information and watermarking in order to be able to track its illegitimate distribution.

Guarantee of quality of service (non-repudiation): If the service provided by the service provider is poor or not in conformity with the terms of the deal, the user shall be able to testify this in order to be guaranteed against content distributors' misconduct.

For instance, if the quality of the sound is very poor for reasons that are not of the user's responsibility (e.g. bad content storage or device handling), the service provider shall be made responsible for the provision of the adequate content quality or for a refund.

Availability: The implementation must maximize the service availability for the user, e.g. if a missing component is detected by the player, it should be able to upgrade automatically from a remote server regardless of the location and time the upgrade takes place. This means that suitable protection infrastructures shall shield the system from DDoS (distributed denial of service) attacks. Distributed denial of service attacks can bring down a network by flooding target machines with large amounts of traffic. Recently, several of the Internet's largest websites, including Yahoo, Amazon.com, eBay, and Buy.com, were disrupted for extended periods by DDoS tools. These new tools were detected in corporate networks, as well as in personal computers with high speed network connections. The prevalence of high speed DSL and the cable modem service magnifies these tools' potential effectiveness.

6 E-commerce infrastructure

The e-commerce infrastructure can be broadly defined as the collection of standards, guidelines, components and services that provide benefit to the online business community. One of the key questions in defining an e-commerce implementation approach is to determine exactly how this infrastructure can be optimally used to support the applications being deployed.

The infrastructure can be illustrated as a multitiered pyramid, in which each layer provides support for the layer above, as in Figure 2 below.

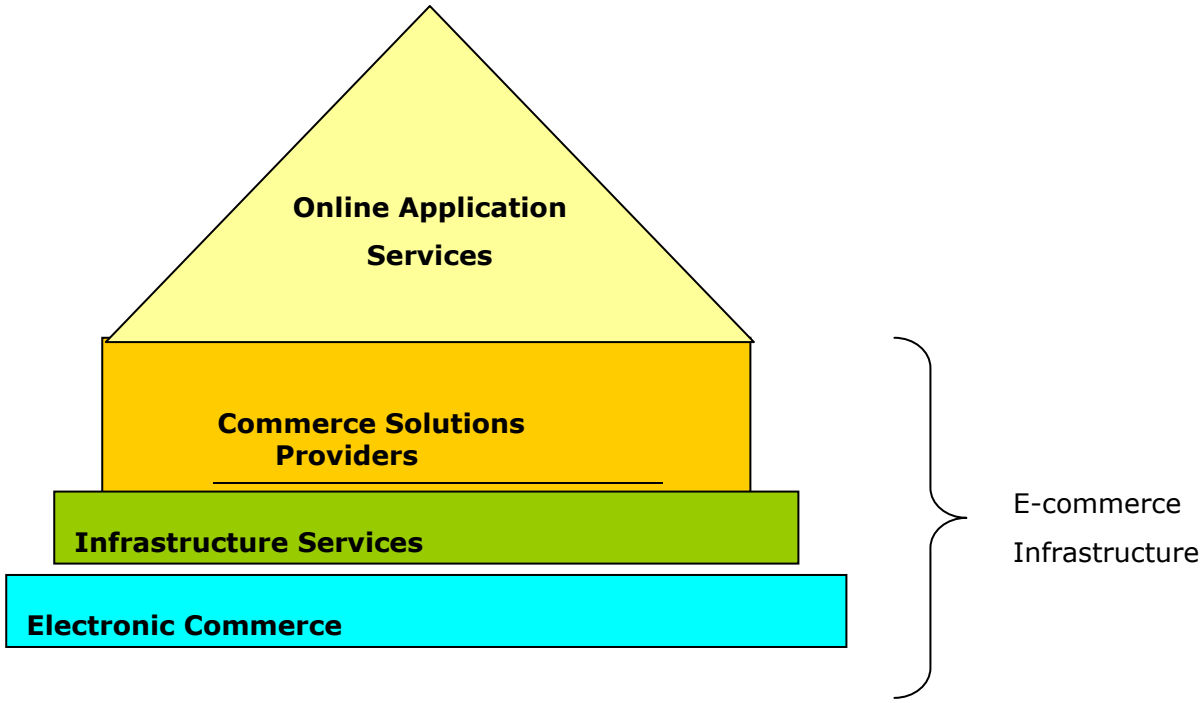


Figure 2 – Multitiered pyramid infrastructure

The e-commerce infrastructure can be categorized as follows:

- **Electronic commerce environmen**t – These are guidelines and frameworks designed to make a conducive environment for e-commerce. The environment includes technical standards, a legal and regulatory framework, and various incentive schemes.
- **Infrastructure services** – These are services that provide specific e-commerce functions, like user authentication or credit card payment processing. Typically, one or more infrastructure services are required by an electronic commerce solution. The infrastructure services can be further categorized as network services, directory services, security services and payment services.
- **Commerce solution providers** – These are organizations that offer complete end-to-end solutions, or packaged components of a solution, for businesses that choose not to implement electronic commerce systems on their own.

The infrastructure can be leveraged to enable e-commerce business applications more cost effectively, and with more predictable results than if an organization implemented the applications by developing all aspects of the solution on its own.

Each element of the e-commerce infrastructure is defined in more detail in the following paragraphs.

6.1 Electronic commerce environment

Online business applications, the infrastructure services and the commerce solution providers all exist within the structure's overall electronic commerce environment. The e-commerce environment is comprized of the following elements:

- **Legal and regulatory framework** – For electronic commerce to flourish there needs to be a conducive legal and policy environment. Businesses need to know that when they conduct business online, they enjoy the same legal protections as traditional businesses.
- **Standards** – It is necessary to establish a set of open, industry-led, technical standards in the areas of network protocols, security, e-mail and directories, electronic commerce, and information sources and exchange. The standards facilitate interconnection and interoperability of businesses over networks.

6.2 Infrastructure services

Infrastructure services comprise:

- **Network services** – These services provide the networks that link online businesses. These services are provided by Internet service providers.
- **Directory services** – These services allow customers to search for information or websites based on various search criteria.
- **Security services** – These services provide secure identification and secure communication over the Internet. Many tools for these purposes are available commercially.
- **Content protection services** – These services provide IPMP tools that supply the protection needed by content providers. These tools shall be as transparent as possible so that the entire process is not excessively weighed down in terms of time consumed. IPMP tool provider services shall be as efficient as possible (fast server for tools retrieval, light-weight tools to be downloaded, limited resource demanded on the local device).
- **Payment services –** These services enable secure payments over the Internet.

6.3 Commerce solution providers

Commerce solution providers (CSPs) are organizations that offer complete end-to-end solutions for businesses that choose not to, or do not have the capability to, implement e-commerce systems on their own. There are two categories of CSP:

- **Business to consumer services** – These CSPs create and host electronic commerce websites for merchants who sell directly to individuals.
- **Business to business services** – These CSPs provide services for electronic commerce between businesses.

7 The content and the ticket

Both the music and the related usage rules stored in the "ticket" shall be protected from abuse during their entire lifecycle after the deal has taken place. Cryptography and watermarking techniques are likely to be employed for this purpose.

8 General security recommendations

Many experiences in recent years have shown that protection mechanisms for products destined to the large consumer market are subject to an impressive amount of technically skilled attacks. Therefore, a fundamental requirement of security engineering is that the system shall be as "patchable" as possible. This means that the protection scheme shall not be "frozen" within the technology that implements it, otherwise the damages of a successful attack could not be repaired without changing the whole technology (e.g. players, physical supports, etc.). This happened with the digital versatile disk (DVD), where the encryption algorithm was very weak and unchangeable, and the entire set of possible keys was fixed and built into every disk.

Another important security principle driving the realization of systems devoted to information protection states that if one control in the system of controls is compromized, other controls shall provide a "safety net" to limit or prevent the loss. This implies that a break in a single component does not produce the spilling of all the information required to access the sensitive content. In other words, in order to bypass the protection mechanisms the attacker must break every component and possibly even then the attempt could partially fail owing to the lack of a correct interaction among compromized components.

9 Other functional requirements

Connectivity: Communication capabilities to be supported:

- wireless connection (e.g. Bluetooth, infrared);
- personal token interface (e.g. smart-card reader);
- TCP/IP protocol.

Storage capabilities: Two types of storage facility have to be present:

- *Volatile memory*: is a type of memory that loses its information when power is not present. It is required for those memory-consuming operations that take place only during player use and do not produce results that need to be stored for future use.

- *Non-volatile memory*: is a type of memory that preserves its information when power is not present. Such preservation can be either unlimited or for a lapse of time that is longer than the platform's lifetime. It is needed for the storage of those pieces of information needed by several successive uses of the device (content, usage rules, counters of different nature, etc.).

User interface: The user interface shall provide a friendly means to:

- browse content stored on the player for consumption;
- access the service provider for content purchase and download;
- manage content (COPY, MOVE, EDIT operations).

9.1 Non-functional requirements

HW/SW portability: The music is intended to be played also on embedded devices with limited processing power; therefore, the player code must be able to perform the decoding and additional processing (decryption and/or watermarking) of audiovisual information with real-time performances. The target platforms should be among those currently available on the market and compatible with the most popular configurations.

Performances: With respect to current established ways of accessing and consuming digital audio-video content, the additional options described here must provide an experience as close as possible to the current scenarios in terms of complexity of use.

The implementation must make efficient use of all the device resources, including CPU time. In order to achieve this goal, platform-specific development kits available from devices' manufacturers are likely to boost the process of optimization.

Interoperability: The player must be able to communicate with the servers used to support the upgrading service, and to install and run new components. In order to achieve this goal, the player, acting as a client, must support the most common communication protocols for client-server applications. The possibility of transferring the purchased content and all the related items (tickets, IPMP tools) to platforms that differ from the one of origin without need for repackaging seems to be of interest for the customer and shall be taken into account to the largest possible extent. In fact, this option would allow content transfer to different platforms without need to be online and to download all necessary items. If the content is to be transferred to other players in an offline scenario, the content protection scheme and any aspect connected to content consumption shall be as platform-independent as possible.

Deploying: In order to have a minimal impact on the ease of use, the player must have an installation procedure for the target platform. It will be able to upgrade automatically once installed on a device if upgrades are free of charge; otherwise the process of upgrading shall be as straightforward as possible.

Usage scenario 2: Tele-education

The final goal of the whole system is the creation of a virtual classroom where the different actors feel as if they are physically participating in the same event. According to the nature of the cognitive process the essential means through which knowledge is transmitted are speech, text and drawings. Even if not essential, support for video is likely to significantly contribute to the quality of the users' experience. In this section attention will be focused on a common university-style lecture where essential elements are the teacher's voice and the blackboard.

Various content distribution and use models will be examined according to the temporal and the spatial distance between service production and its consumption.

Precondition common to all of the several use cases: This scenario envisages an educational TV programme, "In a drug store", being played to a school class. The instructor, Kim, prepares the class using an educational broadcasting system (EBS) studio while some pupils prepare for the class in the same classroom as Kim or at home. Students that are going to follow the class from home are subscribed to Korea Satellite Broadcasting (KSB), which is a multichannel pay-TV company that provides digital broadcasting services over satellite. EBS is a professional broadcasting company that produces entire channels of educational programmes. In order to be allowed to follow the class, they have to identify themselves to the EBS. This identification process is likely to require that all the pupils belonging to the educational institution be provided with a personal identification device (e.g. smart card).

10 Content preparation

The educational institution where the class is taking place wishes to make it accessible to the largest number of pupils in the most flexible and comfortable way. This is the reason why a multimedia classroom is set up in order to best exploit the modern recording and telecommunication technologies. Such equipment will allow remote students to have an experience as close as possible to the experience of pupils attending classes in real classrooms. This requires that the classroom be equipped with a broadcasting system able to reach the largest number of pupils. Students can ask for a remote replay of the lecture not only as "live" transmission, but also for a later reviewing due to their unavailability at the time the class took place or for revision of the topics treated. This requires the possibility to store the recorded lesson on a server able to manage random requests for downloading according to the distribution policy established by the content owner.

The server hosting the content must provide basic functionality for content upload and activity monitoring. For example:

- Easy-to-use browser-based user interface
- Secure, instant access any time to site usage statistics, bandwidth utilization, etc.
- Real-time and historical reports, plus full access to log files
- Extensive viewer statistics available.

Use case 1: pupil at home attending "live" class

Precondition: A student, Hong, has a set-top box for broadcast communications reception at home. The set-top box is able to receive EBS transmissions and allows user identification and interaction (e.g. audio/video interfaces).

Description: Hong tunes his home TV to the EBS using a set-top box. When authenticating and accessing the service Hong can decide the degree of interactivity he wishes to reach. For example, he can decide whether he will record the programme or not, whether he wants to be able to ask questions or download Kim's notes or suggested support material. Any of these services may be provided following different distribution models; some of them can be free for a limited time or with limited operations allowed, others can be available only for purchase. For instance, before the beginning of the lesson Hong decides that he needs to be able to download free notes and a textbook for which he has to pay. During the class, he wishes to ask questions and get answers from Kim in order to write some important points made by Kim in the downloaded textbook.

Error flows: Since the pupil attending the class from home has exactly the same possibilities and the same obligations as those attending on site, the reasons for denial of service are the same as in the previous use case.

Use case 2: late class

Precondition: Cho was taking a sightseeing trip in Jeju with his relatives and missed the whole class. On his way back home, he would like to have a replay of the class on his PDA and have a look at Hong's notes and the textbook when he arrives home.

Description: Cho connects to the server where the recorded class has been stored and identifies himself to the system. Then he receives a replay of the class on his PDA, and downloads the textbook when he arrives home either from the EBS or from Hong's PC.

Error flows: In this case the pupil accessing the recorded class from home experiences a situation very close to that of pupils attending the class "live" from home. Therefore he has exactly the same possibilities and the same obligations; the reasons for denial of service are the same as in the previous use cases.

Functional requirements: As for the music distribution usage scenario, functional requirements here are provided with particular attention to intellectual property management and protection.

If the class is downloaded on a local storage device, the scenario is very close to that of music distribution where the sensitive content is an audiovisual stream and not just music. The functional and non-functional requirements for this case can be supposed to be the same as those listed in the previous sections. The case of streaming consumption of the content is taken into account here.

Secure streaming of digital content is the perfect selling model because there are no inventory or carrying costs, and it can be sold to anyone and delivered anywhere easily. This has far-reaching implications for both online retailers as well as corporations that own digital content such as training materials, digital rights for seminars, conferences, trade shows sporting events and so on. For these advantages to be real, it is of the utmost importance that only the persons entitled to access the service can do so and that their use of the content is in accordance with the terms of the deal. Therefore, particular attention is devoted here to security requirements in streaming scenarios.

Security requirements: In a streaming context where the content is likely to be available to a large mass of potential customers (e.g. over the Internet), the security principles already introduced in previous examples are applicable:

- *Authentication*: movie trailers, audio previews and other promotional media content can be secured so that they only play from the intended website.
- *Access control, confidentiality*: expire access to content to unauthorized users and enable authentication of media users.
- *Access control*: prevent unauthorized access of streaming content resulting from mass e-mailing of streaming URL links.
- *Integrity*: streamed reproduction shall actually be what is intended to be sent.
- *Non-repudiation*: Streamed information authenticity shall be certifiable after reproduction (if stored by the client).
- *Availability*: the streaming server shall be up and running 24x7.

In the following sections every component of the entire streaming system is described in terms of the functionality needed in order to achieve the above goals.

The player: The secure player, be it the set-top box or the PDA, must be able to:

1) authenticate the user;
2) check user rights on the selected content;
3) deny or allow content use accordingly;

4) allow secure transfer and handling of sensitive content (credit card numbers, passwords).

5) allow a secure streamed consumption of the content.

The following paragraphs describe each item in more detail.

User authentication: The basis for the implementation of each usage scenario described above is the ability to identify the user in a secure way. Moreover, the user authentication must be repeated every time the user requires to be allowed to see a streamed presentation on his local player. Otherwise, a user can identify himself on a device once, and then use the device forever or let all his/her friends do so!

The user identification must be different from the identity of the device that is used to play the protected content, otherwise:

- a crash of the player would be unrecoverable;
- accessing the content on different players would be impossible.

As for offline content consumption, a straightforward solution is to use a physical token (i.e. a smart card) able to represent the user each time the user authentication is required. Nowadays, if the presence of a smart-card reader in an STB is quite common, the same device for a PDA could engender some difficulties in terms of both cost and ease of use. Such a solution can be required for high-end devices destined for professional users where cost and ease of use are of secondary importance with respect to the value of the treated information.

The simpler solution of using a password that can expire after a while is more suitable for circumstances where ease of use and low cost are of primary importance.

User rights checking and packaging (access control, integrity): The server should be able to handle the different requests for streamed content and to check the rights held by the identified student asking for content. Different students belonging to the same educational institution may have different access rights on the available classes for several reasons (e.g. year of attendance, number of exams taken, etc.). Once the server has stated that the identified student holds the set of rights necessary to access the required class, it shall produce a "ticket" to be sent to the student together with the information stream. It will be the player's task to recognize the user as the authentic owner of the licence stored in the "ticket" by interpreting it, and verifying whether the user claiming to be the owner of the ticket is the real one or a faker.

User rights check (access control)

Rules parsing

As for offline content fruition, generic rules associated with content are designated as "content rules" and rules specific to each single user are called "user rules" and are contained in the "ticket". Content rules are embedded in the content itself and allow on one side the player to match content and user rules and on the other the service provider to associate every piece of distributed content with the best IPMP tools assortment that matches his/her security requirements.

Once the rules container (the "ticket") has been validated, it is parsed to extract the information contained in it. This information cannot be changed in any way by the player or any other entity, otherwise a user could entitle himself to do whatever he/she wants with the content without paying. The player can only evaluate the rules associated with the content and those contained in the "ticket", and then apply the result of the match.

Secure transfer and handling of content (confidentiality, integrity): In a streaming scenario it is of the utmost importance that the quality of the rendering is not affected by run-time operations such as buffering and information pre-processing (e.g. watermarking), so that the service provided to the user is actually what he/she expects to receive. This means that the protection layer that is supposed to guarantee information confidentiality and integrity is at the same time completely transparent for the user.

The pieces of sensitive information required during the process of content use shall be protected from access by unauthorized users (eavesdropping). Such components include:

- the content;
- the associated ticket;
- personal information related to the user.

Cryptographic and watermarking techniques are likely to be employed for these purposes.

Availability: The server shall be up and running as much as possible in order to allow users to access the content with no restriction of time (protection from DDoS attacks.

Other functional requirements

Connectivity: Communication capabilities to be supported:

- broadband wireless or wired (only for STB) connection.
- personal token interface (optional for PDA).

Storage capabilities: Two types of storage facility have to be present:

- *Volatile memory*: this type of memory that loses its information when power is not present is required here as a temporary buffer in case the bit rate of the downlink is higher than the bit rate of the presentation. It could be useful to prevent disturbances due to transient line interruptions. It is also likely to be filled with data produced by those operations that take place only during player use and do not produce results that have to be stored for use a second time.
- *Non-volatile memory*: this is not needed for normal situations of streaming but could be useful if the process of rendering should be forcefully interrupted by sudden external events (e.g. long connection breaks or device power supply failure). In fact it would keep important information required when the situation returns to normal.

User interface: The user interface shall provide a friendly means to:

- access the service provider for user authentication,
- browse content stored on the server for content selection and download,
- manage content (PLAY, STOP, PAUSE operations).

Non-functional requirements

HW/SW portability: The streamed class is intended to be played also on embedded devices with limited processing power. Therefore on one hand the device must support broadband connections and on the other the player code must perform decoding and additional processing (decryption and/or watermarking) of audiovisual information with real-time performances. The possibility of transferring the content from one device to another (from STB to PDA or from PDA to PDA) requires that adequate communication mechanisms be supported among those currently available in commercial products.

Performances: The recorded and streamed class shall provide an experience as close as possible to that of a pupil really attending it in the classroom. This applies to audio and video rendering quality. Such quality is affected by several factors that have to be taken into account:

- user-friendly interfaces;
- decoder(s) performances;
- protection scheme transparency;
- connection speed and reliability;
- adequate rendering devices (loudspeakers, displays).

All the device resources shall be efficiently exploited possibly by means of available development kits provided by original equipment manufacturers (OEMs).

Interoperability: Not only must upgrading services be supported by the client (the player), but also the IPMP infrastructure must be as flexible as possible. This includes the possibility of being downloaded from different available servers and fitting the widest range of platforms. The possibility of transferring the content without repackaging from one platform to another must be supported as much as possible. If current technology does not seem to be ready to completely fulfil this requirement, or if complete interoperability at the level of content seems to be too expensive to be supported, it can be left to high-end devices able to be extended in order to support future versions of the adopted protection technology.

11 Conclusions

The UML diagram in Figure 3 summarizes the functional requirements described above.

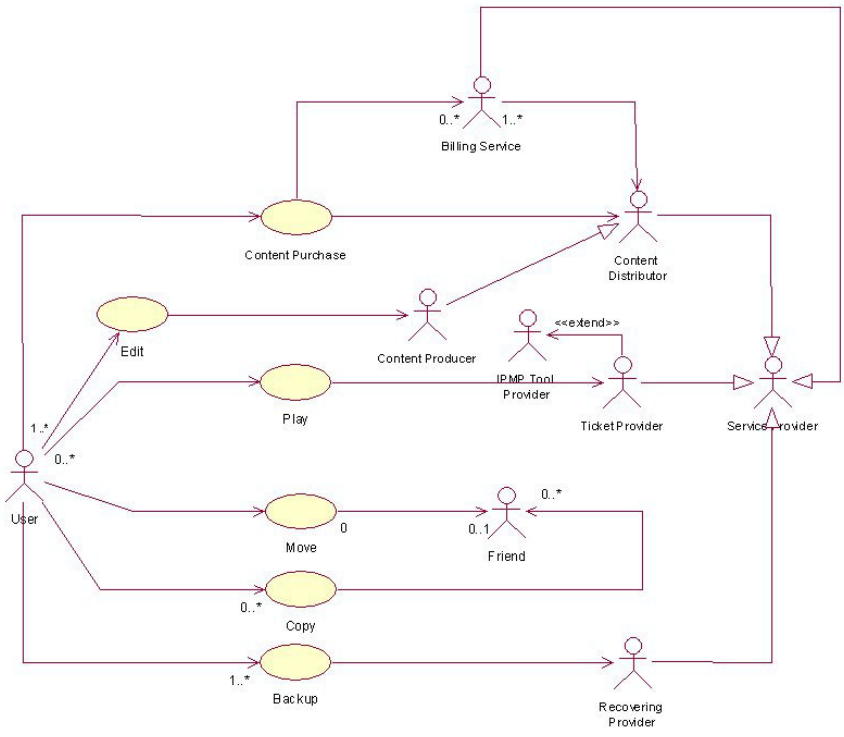


Figure 3 – Actors and functionalities of the MOSES system

The different actors involved can collapse into a generic *services provider* actor that will supply all the required business services. The diagram omits the entities needed in order to support the security requirements or to implement functionality. This is due to the UML approach that avoids specifying "*how*" components have to be put into practice. All the intermediate operations answering user requests must be transparent and, if additional options supporting specific features (e.g. confidentiality) are necessary, they must be as habitual as possible (e.g. to buy something I have to put my credit card in an ATM).

From this point of view, the music scenario seems to be the hardest challenge. In fact, the high degree of interoperability and flexibility required by the user must be satisfied in order to defeat the temptation of a monopolistic solution to the DRM problem.

The diagram in Figure 4 shows possible user interactions with digital content. Indexes near the association links (arrows) are called multiplicities; these count how many objects associated with a given entity or class can be present within a particular association. It is a concise way to describe scenarios where, for example, a music CD can be lent to a number of friends, and/or played on CD readers coming from different vendors (Panasonic, Sony, Philips, etc.) and in several devices (PC, DVD, etc.). The MOSES system is supposed to support such options to the largest extent.

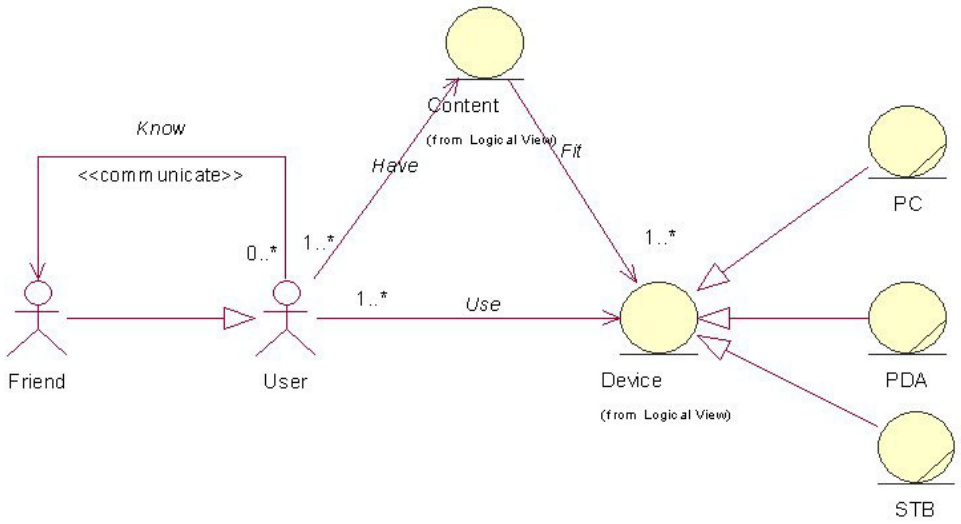


Figure 4 – User interaction with digital content

In the same context we will find a DRM system that reduces to a minimum the external interfaces required for the user's device. In other words, an audio CD does not need more functionality than power supply and a physical exchange to be played on different players.

To resume, the solutions will satisfy two fundamental requirements: different degrees of security for the vendors, maximum degree of freedom for the user.

Attachment 18

E-broadcasting: Broadcasting over the Internet

Table of contents

E-broadcasting: Broadcasting over the Internet

1 Digital video broadcasting

The broadcasting of digital multimedia content was boasted by the birth of two main technologies: the digital video encoding standard known as MPEG-2 and the definition of the transmission protocol known as **digital video broadcasting** (DVB).

DVB was originally born to replace the old analogue television, but it is now earning consensus for Internet-based broadcast (a.k.a. DVB over IP).

DVB is a transmission scheme based on the MPEG-2 video compression/transmission protocol and utilizing the standard MPEG-2 transmission scheme. It is however much more than a simple replacement for existing analogue television transmission. In the first case, DVB provides superior picture quality with the opportunity to view pictures in standard format or wide screen (16:9) format, along with mono, stereo or surround sound. It also allows a range of new features and services including subtitling, multiple audio tracks, interactive content, multimedia content – where, for instance, programmes may be linked to worldwide web material.

DVB is a European initiative. Equipment conforming to the DVB standard is now in use on six continents and DVB is rapidly becoming the worldwide standard for digital TV.

At the time DVB was being developed in Europe, a parallel programme of standards and equipment development was also being implemented in the United States by the Advanced Television Systems Committee (ATSC). Among other things ATSC adopts a different audio coding standard, and vestigial sideband (VSB) modulation. The United States has adopted a system based on ATSC, called digital TV (DTV). During standardization this evolved into a hot debate between the PC-based manufacturers (favouring a non-interlaced display) and the TV manufacturers (favouring an interlaced format). There is much in common between the United States and European standards and inter-operation between some DVB and DTV equipment has been demonstrated.

2 DVB over IP

DVB over IP is the expression used to describe delivery of digital television services (DVB) to homes over broadband IP networks. Typically this will be over cable so that the supplier can achieve the "triple play" bundling of voice (over-IP) telephone as well as Internet with the television service. This has great potential for interactive television as it includes a built-in fast return link to the service provider.

3 Example of a service scenario

A DVB-T/S broadcaster provides a service of high quality digital video delivery (MPEG-2 video). The well-known end-user terminals used in these scenarios are the set-top boxes.

The example depicted in Figure 1 shows how an IP network can provide the same services to the IP terminals it manages. The MPEG-2 transport stream is received and fed to an IP encapsulator. The encapsulator can process all or part of the MPEG-2 stream and encapsulate the MPEG-2 packets into IP datagrams. These datagrams are conveyed on a LAN to the end users that can directly retrieve and decode the MPEG-2 programme.

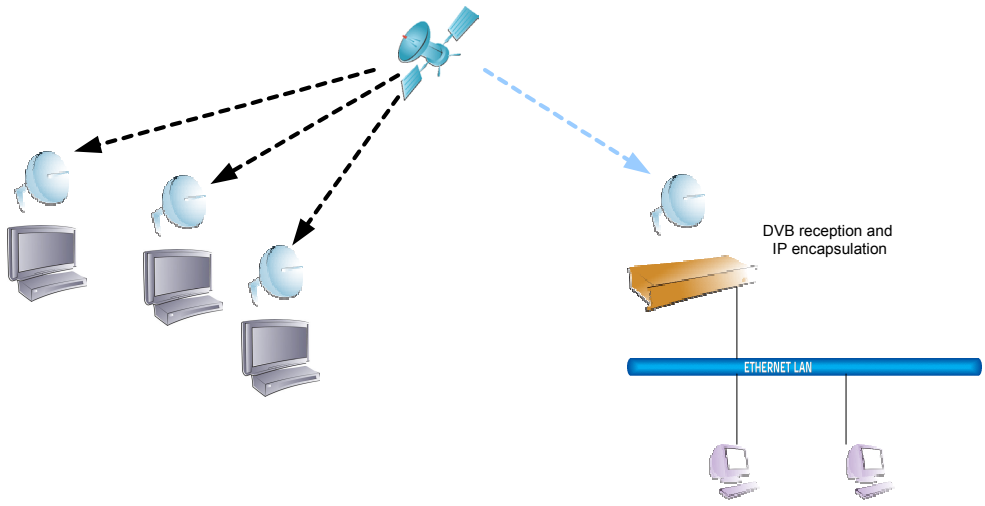


Figure 1 – DVB over IP

4 Service scenario parameters

Table 1 –Service scenario parameters for DVB over IP

Service type	Content type	Content format	Network/play out channel	Distribution/ usage mode	End-user terminal/device
Unidirectional broadcast of IP data Streaming of IP data	Audio video	MPEG-2 MPEG-2 over IP	DVB (T, S…) + LAN	Push	PC on LAN Set top boxes

5 Broadcast of IP over DVB

This expression normally designates the delivery of IP data and services over DVB networks. Also referred to as datacasting, this takes advantage of the very wideband data delivery systems designed for the broadcast of digital television, to deliver IP-based data services – such as file transfers, multimedia, Internet and carousels, which may complement, or be instead of, TV. As a result of DVB-Terrestrial's ability to provide reliable reception to mobile as well as fixed receivers, there are possibilities to send IP-style service to people on the move. For interactivity, a return path can be established by telephone.

5.1 Description of an IP over DVB scenario

In this scenario, content is streamed to an IP network in multicast. End users connected to the network can retrieve the services and visualize the content. A gateway allows a DVB hop to be effected by encapsulating the IP datagrams to MPEG-2 Transport Stream (TS) packets. On the reception side, a gateway retrieves the IP datagrams from the MPEG-2 packets and feeds them to another IP network. The streamed content is thus also available on the second IP domain.

Content streamed could be any format accepted by IP. It can be MPEG-2 over IP, MPEG-4 over IP or others.

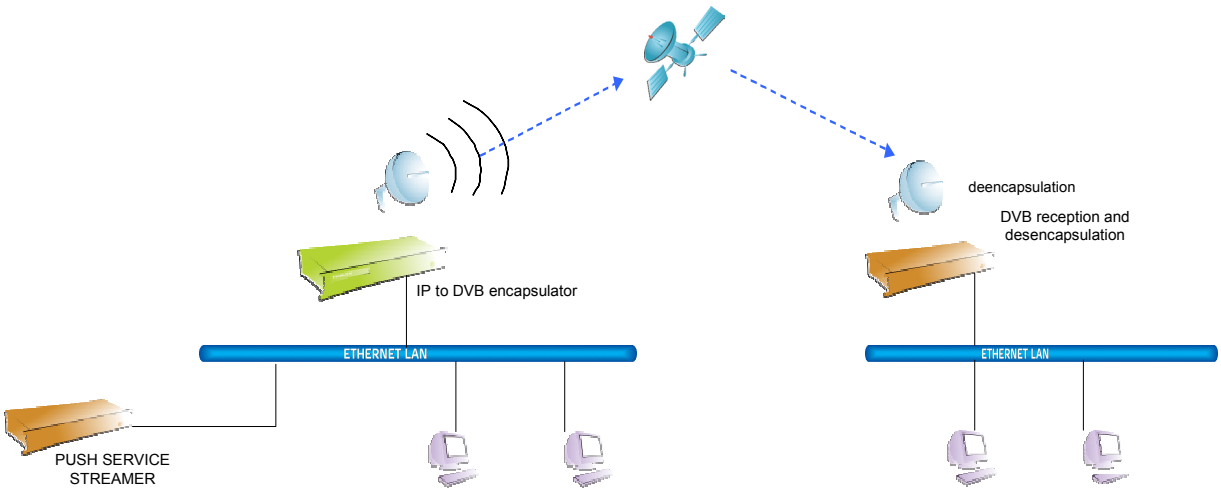


Figure 2 – Broadcast of IP over DVB

6 Service scenario parameters

Table 2 – Service scenario parameters for broadcast of IP over DVB

Service type	Content type	Content format	Network/play out channel	Distribution/ usage mode	End-user terminal/device
Unidirectional broadcast of IP data Streaming of IP data	Audio video	MPEG-2 over IP MPEG-4 over IP	DVB (T, S…) + LAN	Push	PC on LAN

6.1 Example of interactive IP over DVB

Multicast services implementation in a hybrid network may call for IP multicast protocols to be supported. One way but not the only way, to allow multicast services is to use the unidirectional link routing protocol (UDLR) which provides a mechanism that emulates bidirectional connectivity between the interfaces of a one-way channel through IP bidirectional return channel.

A DVB link is used to provide the incoming stream to an Internet client. The Internet client performs a request on an outgoing low bit rate request. The remote server receives the request and the response is routed to an IP to DVB encapsulator and then sent on the DVB link. On the receiving side, a router redirects the requested answer to the terminal. Several protocols exist to encapsulate IP into DVB (data piping, data streaming, MPE, ULE…).

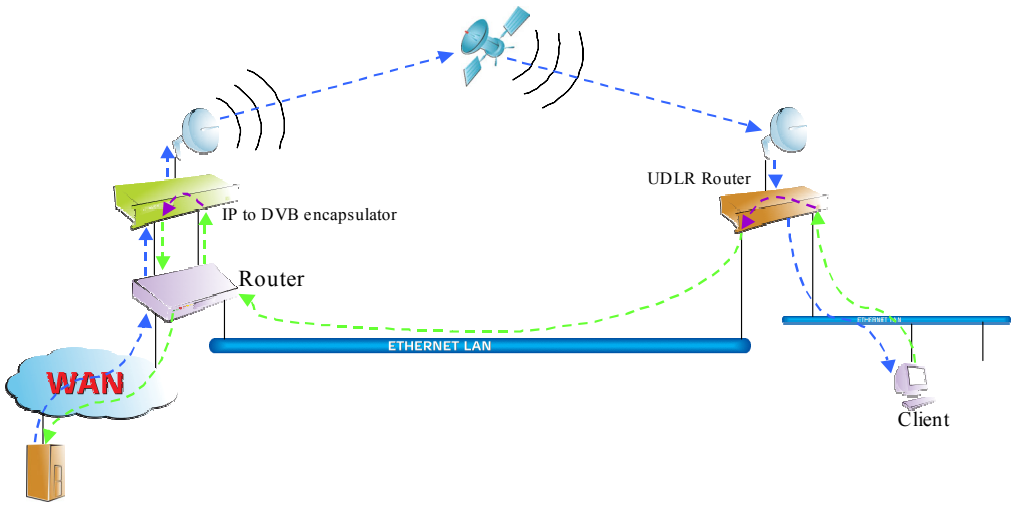


Figure 3 – UDLR usage for interactive broadcast of IP over DVB

6.2 Interactive IP over DVB parameters

Table 3 – Service scenario parameters for interactive IP over DVB

Service type	Content type	Content format	Network/play out channel	Distribution/ usage mode	End-user terminal/device
Unidirectional broadcast of IP data	Audio video	IP over MPEG-2 TS MPEG-2 over IP MPEG-4 over IP HTML MP2 audio Jpg, gif	DVB (T, S…) + LAN	Push Bidirectional Interactive	PC on LAN

7 Broadcasting of radio programmes

Digital audio broadcasting (DAB) technology provides a high capacity data broadcast network to mobile and fixed users. Broadcasters are now transmitting their existing services in high quality MPEG layer 2 format and new services are being offered exclusively to DAB listeners. Broadcast data services are also appearing in the form of broadcast websites, and other applications.

DAB is a digital radio system, which was developed by the Eureka 147 Project. It offers near CD-quality sound, more stations, additional radio and data services and therefore wider choice of programmes, ease of tuning and interference-free reception for the listener, plus the information potential of data, graphics and text. For the broadcaster, DAB provides a means of reaching listeners with sound quality on an equal footing with the CD player, and the ability to offer extra, potentially revenue-creating services. Transmission will also be cheaper. For other areas of industry, there will be a new market for receivers and transmission equipment.

8 Benefits for broadcasters

Broadcasters will accrue many benefits from DAB. Audiences will be able to enjoy better reception and find individual stations more easily–that means less complaints are likely to be received about these two topics! The near CD-quality sound that DAB offers means that radio will once again be able to directly compete against the perfect audio quality that the domestic CD or the very high quality cassette can reproduce. Unless broadcasters exploit this, they will lose listeners, particularly the younger generation, to these personal high-quality entertainment sources. Broadcasters will be able to offer more services, since DAB is flexible. Each package of radio stations (known as an ensemble) can be reconfigured at any time to allow new services to start and others to end. Extra sports commentaries can be added when matches start, or live classical music concerts can have extra digital capacity allocated to ensure that audiophiles receive the ultimate sound quality. Transmission will be cheaper too. DAB can be transmitted at lower power than today's FM and AM signals yet with no loss in geographic coverage, which means less cost to the broadcaster (and less power consumption means DAB is more environmentally friendly than conventional FM and AM). Another advantage of digital radio transmission is that it is a cost-effective and powerful advertising medium.

9 Not only digital radio

DAB was developed with the aim of improving radio reception. This is why audio transmission was at the forefront of the development process. But DAB, as a digital transmission system, can transmit other data as well as audio. In principle any type of information can be transmitted by DAB, provided simply that it is available in digital form and does not exceed the maximum available DAB data rate (approx. 1.7 Mbit/s). Examples of such additional services are still pictures accompanying radio programmes, digitized traffic messages (Traffic Message Channel), electronic newspapers, software updates and even animated video. This process leads to 'multimedia broadcasting' in which all forms of information can be conveyed via the common transmission medium DAB. In this context DAB could be described as the 'cordless information highway'. In contrast to multimedia applications via TV/cable, DAB additional services can also be received in a car and with portable equipment.

10 Pay-per-listen services

Because DAB receivers are intelligent, they can be configured to include pay radio services. Some broadcasters might offer special concerts available only on payment (because DAB is flexible, new services like pay channels – or extra conventional free-to-air channels – can be added without having to switch off the ones already on the air), which you would subscribe to on an individual or long-term basis. Specialist financial services might also be available on subscription via DAB. And then there are the futuristic possibilities which DAB might make a reality, like personal receivers that could correlate and compare the signals from global positioning system satellites in order to pinpoint your exact location. Because DAB is computer-based, it might also one day transmit and receiver computer files (like the Internet and e-mail) or fax transmissions. DAB's possibilities are endless.

Attachment 19

The Essential Report on IP Telephony

by the Group of Experts on
IP Telephony / BDT

http://www.itu.int/ITU-D/e-strategy/publications-articles/pdf/IP-tel_report.pdf

International Telecommunication Union
Place des Nations, CH-1211, GENEVA 20
Switzerland

Telecommunication Development Sector
(ITU-D)

Désiré Karyabwite
IP Coordinator, E-Strategies Unit
Telecommunication Development Bureau
(BDT)
Tel: +41 22 730 5009
Fax: +41 22 730 5484
E-mail: desire.karyabwite@itu.int
E-Strategies Unit: e-strategy@itu.int

Telecommunication Standardization Sector
(ITU-T)

Richard Hill
Counsellor, ITU-T Study Group 2
Telecommunication Standardization Bureau
(TSB)
Tel: +41 22 730 5887
Fax: +41 22 730 5853
E-mail: richard.hill@itu.int
Study Group 2: tsbsg2@itu.int

www.itu.int/ITU-T/special-projects/ip-policy/final/

Printed in Switzerland
Geneva, 2005