ascent

Thought leadership from Atos

white paper

Internet evolution

Your business technologists. **Powering progress**

”A standalone computer is as useful as a standalone phone”. This provocative statement is a rather rough way of expressing the importance of data networks in today’s IT world. It is now inconceivable for most people to use a computer without an Internet connection and anecdotes about meetings not starting before most participants have managed to connect to their necessary online working tools are now abundant. Networks have become essential to both our professional and personal lives, and are becoming even more important with the appearance and impressive growth of Cloud computing, which relies on high-bandwidth networks to allow clients to use remote services easily. In addition, governments and companies consider networks to be strategic assets which must be protected and kept up to date in order to maintain competitivity and profitability.

Even though it is now a critical infrastructure that must be maintained, the Internet is changing. It is evolving in order to sustain more connected uses, in real time, and to ensure quality of service and reliability, both for mobile and low-capacity terminals, as well as the powerful servers that reside in a major Internet service provider’s data center. Atos, as a major online services operator and Cloud solutions provider, is monitoring this evolution and even anticipates it through its participation in the Future Internet Public Private Partnership as well as its own research and development (R&D) work on new protocols and network designs, in order to adapt to this ever-evolving environment. This white paper describes the changes that Atos has observed, from the initial experimental network designed in the 1970s to the infrastructure sustaining the online services we use daily. It then draws a picture of the Internet as it is today, before introducing research works and ongoing studies that are shaping the future of the Internet. This document is written for an audience of technologists interested in networking in general.

Published in December 2012

Internet evolution

Contents

About the Authors

This white paper was developed by Antoine Fressancourt, Research and development engineer and member of the Atos Scientific Community (Antoine.Fressancourt@atos.net).

About the Atos Scientific Community

The Atos Scientific Community is a network of some 100 top scientists, representing a mix of all skills and backgrounds, and coming from all geographies where Atos operates. Publicly launched by Thierry Breton, Chairman and CEO of Atos, the establishment of this community highlights the importance of innovation in the dynamic IT services market and the need for a proactive approach to identify and anticipate game changing technologies.

Uses evolution on the Internet

Since its invention as a data network connecting a few computers residing in universities and research institutions in the US, the Internet has evolved a lot. Once a relatively homogeneous network in terms of connectivity and edge peer capabilities, the Internet now allows very different peers, from mobile devices or objects to servers in large data centers, to communicate through a variety of fixed and mobile communication links. Below is a look at how the use of the Internet has changed in the last few years.

More people accessing the Internet, from more devices, for more uses

The Internet has grown from being an experimental research network implementing datagram commutation concepts to a major infrastructure used for critical applications, from communication to banking and commerce. The Internet is now accessed from servers, desktop computers and mobile devices to collaborate and access connected services. It is based on foundations established in its early days, such as the Internet Protocol (IP). While in the past, networked equipment from different backgrounds used different sets of networking technologies (e.g. the public switched telephone network or the GSM network), in the last few years, there has been strong convergence and IP has become ubiquitous. It is now used to connect set-top boxes, telephones and mobiles, far beyond the initial, best-effort uses of the Internet. Now, protocols from the IP stack are not only used for data communication, but also for real-time, multimedia, conversational communication services in both fixed and mobile networks.

At the same time, the number of devices connecting to the Internet using the IP protocol under its IPv4 version has dramatically increased. As a result, the number of potentially connected devices goes far beyond the available address space for IPv4, as shown in Figure 1.

The Internet Assigned Numbers Authority (IANA), the global address registrar responsible for the distribution of all IP address blocks, assigned its last IPv4 block to a regional registrar on January 31, 2011. The exhaustion of the IPv4 address space is urging networks to move to IPv6, a modified version of the IP-addressing protocol that provides a far larger address space to avoid limitations and addressing issues in the near future. This important shift will have a dramatic impact on the inherent structure of networks, as IPv6 carries functionalities that are operated by side protocols and mechanisms. This change will not appear overnight and major Internet infrastructure providers and network operators need to start preparing now to move to IPv6. Migration scenarios and their impact are currently being studied, while adoption is encouraged by public initiatives, such as the world IPv6 day. The world will have to cope with both IPv4 and IPv6 for a while.

With this new abundance of IP addresses, every object will be able to have a unique address for each of its interfaces to the Internet. This will certainly ease the resolution of issues related to network address translation (NAT) management, but the fact that addresses can now be associated to a device rather than managed by the network will lead to an increase in the size of routing tables: In routers managing the edge of the networks, a device's addresses may not be summarized easily in aggregate routes. This is a side effect of the deployment of IPv6 and will have an impact on the routing equipment that network administrators will have to manage alongside the 'pure' compatibility of their equipment and applications with IPv6.

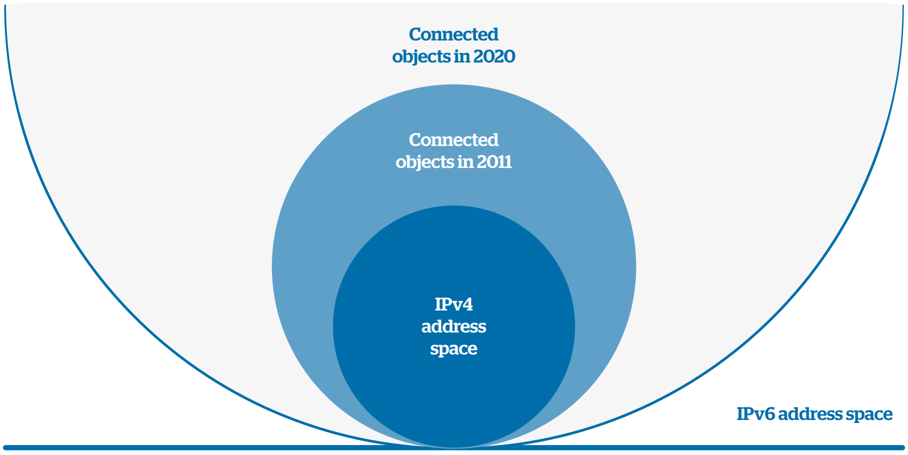

Figure 1: Comparison of IPv4 and IPv6 address spaces with number of connected objects (figures from the GSM Association (GSMA))

The Internet now connects more devices than ever and the growth rate of this figure is impressive. It is a challenging issue as most devices now connecting to the Internet now are mobile devices.

The mobile Internet boom

In the last years, the Internet has moved from an essentially fixed network to a network accessed from mobile devices, using Wi-Fi connections as well as data connections using cellular mobile communication networks (GPRS, Edge, 3G, and LTE (Long Term Evolution) are currently deployed). The boom in Internet usage via mobile devices stems from the popularity of Apple's iPhone, followed by the emergence of a wave of smartphones. These devices have allowed mobile Internet services to become more usable. In addition, their launch has been accompanied by mobile flat fee data plans which contributed to the democratization of mobile Internet.

The boom in Internet access from mobile devices has also raised a number of issues. First, mobile devices move and change location, this is problematic from an Internet traffic routing perspective as the address and routes to reach mobile devices change frequently. This potentially results in multiple connection resets on moving devices while networking elements need to refresh their routing table frequently.

Beyond the need to manage spatial mobility, most mobile devices can also jump from one access technology to another. Many mobile devices embed both Wi-Fi and 2G (GPRS, Edge) or 3G connectivity. Today, this multiplicity is not well exploited and jumping from one data connection to another is poorly managed by most mobile terminals and operating systems (OSs). Yet, when properly managed, such connection multiplicity could dramatically enhance our mobile devices' capacities to operate and access data quickly. It is expected that in the future mobile devices and networks will allow for the proper management of handover operations between multiple access technologies. Yet, this handover suffers from issues related to the limitations of the IP protocol. IP is used both to address a particular interface and identify the host carrying multiple interfaces at the network level. This dual role is an issue, thus there is a need for an alternative to IP as a host identifier.

Finally, with the deployment of LTE networks, mobile networks are completely moving away from circuit switching to packet switching. As a consequence, most voice communication services will be operated over IP. While the exact solution that will be adopted to operate this service is still unclear, the move underscores the need for an appropriate quality of service, or at least a service level that allows the real-time constraints of voice services to be translated into appropriate network management and traffic prioritization policies.

The development of mobile uses of the Internet has highlighted a set of issues related to device mobility and multiple connection management. While some of these issues can be solved using over the top solutions, some limitations that have appeared are inherent to the structure of the Internet and the functionalities of its protocols. Some of these challenges may become even more important if the number of devices connecting to the Internet expands while the capabilities of these devices decline. This situation will prevail with the development of the Internet of Things (IoT).

The rise of machine-to-machine (M2M)

The Internet of Things, which has been introduced in a previous Scientific Community white paper[1], refers to "Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental and user contexts"[2]. Concretely, it means that multiple objects, which were not in the scope of the Internet when it was created, will join the network, send information, receive commands, collaborate and become interfaces between the physical world and the Internet. Today, the Internet of Things is still a burgeoning concept, but more and more objects are appearing, such as the Nabaztag (now called the Karrotz) that prefigures future applications and uses. At a session of the Mobile World Congress, car manufacturers made several announcements showing that they envision a connected future for the cars they are about to sell.

As more and more objects will be connected to the Internet, a proper way to address them and communicate with them should exist. The deployment of IPv6 and its extensive address space will be particularly useful. Even if the TCP/IP protocol suite has been designed for rather simple hosts, connecting objects to the Internet raises a number of challenges concerning how devices' scarce resources (limited energy, poor computing power, unstable and low bandwidth connection to the network) can be adapted. Some adapted versions of protocols running on top of IPv6 are designed and tested within the Internet Engineering Task Force (IETF) that focuses on a minimal computing, networking and energy footprint. Among these protocols, 6LoWPAN and the Constrained Application Protocol (CoAP) should be mentioned. 6LoWPAN is an adaptation of IPv6 that tackles the specificities of transmission over low-power, wireless, short-range links. CoAP can be used to address resource-constrained networks, while translating easily to HTTP. These protocols often come from various industries or result from a specific use case which have had a limited view of ongoing efforts in other verticals. To counter biases in these specific approaches, standard bodies, such as the GSM Association (GSMA), are currently working on generic use cases and common sets of needs, which will give birth to generalized service discovery and communication protocols.

The Internet of Things will put a lot of objects at the reach of computers and services through the use of the Internet, provided that appropriate addressing and protocols are used to connect to them, discover the services they can offer and the data they may provide. While the Internet has to adapt to reach such low capabilities and low connectivity peers, it also faces the opposite challenge of accompanying the Cloud computing wave.

[1] Atos Scientific Community, Internet of Things, http://atos.net/en-us/about_us/insights-and-innovation/thought-leadership/bin/internet_of_things.htm

[2] European Commission, Directorate General for Communications Networks, Content and Technology (DG CONNECT)

The Cloud computing wave

Cloud computing is a major trend in today's IT market. It has been defined by the National Institute of Standards and Technology (NIST) as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." From an Internet perspective, Cloud computing translates into the capacity to access an application which is operated remotely in a large data center with a similar experience to using a desktop or local application. The Cloud computing trend appeared when social network services gained popularity and media websites such as YouTube, DailyMotion, Deezer or Soundcloud began to attract a large audience. Given the popularity of these services, a growing share of overall Internet traffic flows to the data centers hosting them, as shown in Figure 2 that depicts the relative importance of web services.

This power of services tends to break the peer-to-peer, reciprocal model of the Internet, because de facto large data centers operated by Internet giants that hold the major cloud offerings (i.e. Amazon, Facebook, Google or Microsoft) attract a large portion of Internet traffic. This trend is here to stay, as Cisco, in a recent study[3], says that by 2015, IP traffic over data center networks will reach 4.8 zetabytes a year, with Cloud computing accounting for a third of it, while regular IP traffic flowing between peers will reach a zetabyte by then.

Given the popularity of the services they host, data centers have become some sorts of 'black holes' for Internet traffic. This results in a strong asymmetry in Internet traffic, which questions the original design of the Internet as will be discussed later in this paper. The growth of Cloud computing and associated hosted applications also results in a universal use of the Hypertext Transfer Protocol (HTTP). This protocol is now widely used as a transport method because most application programming interfaces (APIs) to access remote services are developed on top of it, and HTTP traffic is generally allowed by most enterprises or personal firewalls, contrary to other more specific protocols.

The development of Cloud computing introduces a set of peers to the Internet that have a particular role given the popularity of the service they operate and the privileged relationships among them. This small number of powerful, heavily connected peers, benefiting from vast resources and bandwidth, operate today on the Internet with the same protocols as mobile devices or objects, which gives room for optimization and tweaks at both ends of the usage spectrum.

To sum up

The evolution of the uses of the Internet has had a significant role in shaping the Internet as it is today. Today's Internet architecture and network characteristics have been inherited from design constraint decisions that were taken 30 years ago that couldn't predict the success the Internet would become. The development of mobile access to the Internet and the importance of data center and Cloud-related traffic to today's Internet have highlighted a set of issues related to mobility management, interface multiplicity, latency and traffic management in a network that has evolved from a rather homogeneous infrastructure to an assembly of links that differ heavily in terms of stability, capacity and latency.

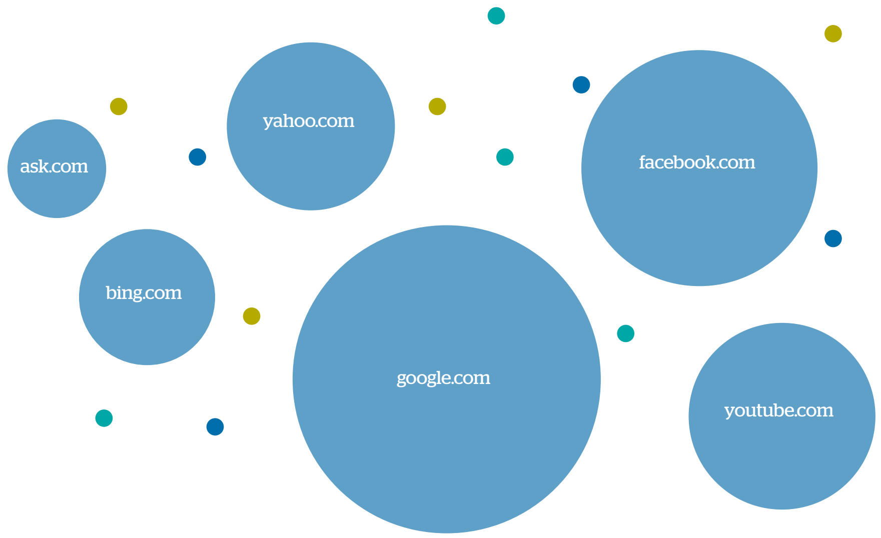

Figure 2: The Internet map. Source: http://internet-map.net/

[3] http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns1175/Cloud_Index_White_Paper.html

How is the Internet evolving?

While the technologies behind the Internet have provided a framework for uses to develop, the trends and evolution of those same uses have had a strong influence on how the Internet has evolved from an experimental research network to what it is today. Among the trends that have shaped the Internet Cloud computing is the most important as it has contributed to flattening the Internet's architecture.

A flatter Internet

In the beginning of the 2000s the Internet and its topology followed a rather pyramidal structure. Few intercontinental operators had peering agreements with regional operators, which then connected to national and access network operators, as shown in Figure 3.

Among the different operators, Internet traffic was exchanged at IP exchange points according to agreements where the dissymmetry in traffic was compensated.

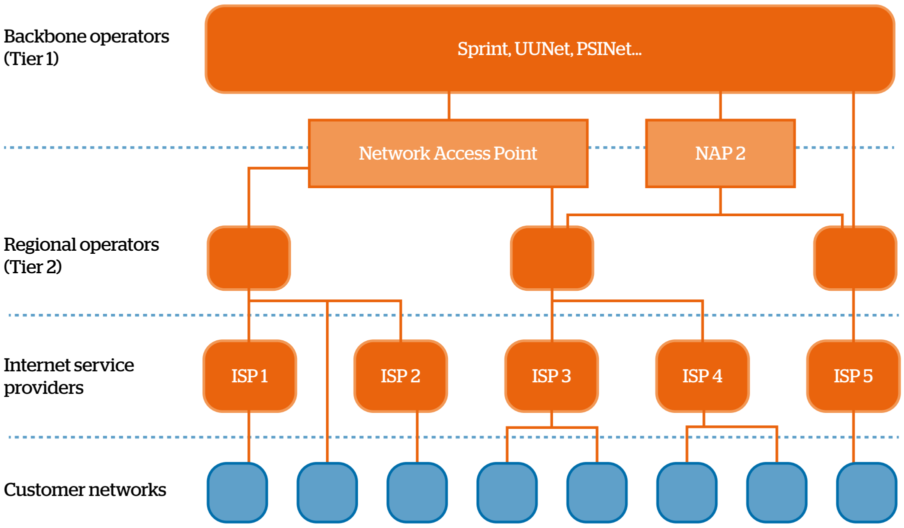

Figure 3: Internet architecture circa 2000. Source: Internet inter-domain traffic

However, researchers have shown[4] that during the last ten years this pyramidal structure has been bypassed by Internet services providers, such as Google, Facebook, Amazon or Yahoo!, and content delivery network operators, such as Akamai. As a result, the Internet's backbone has a flatter infrastructure where there are fewer autonomous systems (the routing units associated to major Internet services providers) connected to the many others, resulting in a more diverse situation where Internet content providers tend to get as close as possible to their customers' access networks, as depicted in Figure 4.

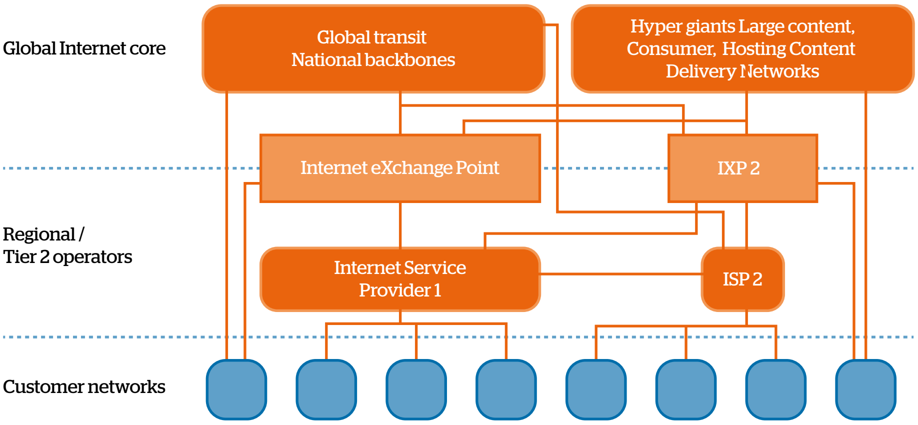
Global Internet core
Global transit National backbones
Hyper giants Large content, Consumer, Hosting Content Delivery Networks
Internet eXchange Point
IXP 2
Regional / Tier 2 operators
Internet Service Provider 1
ISP 2
Customer networks

Figure 4: Current Internet architecture. Source: Internet inter-domain traffic

[4] Craig Labovitz, Scott Lekel-Johnson, Danny McPherson, Jon Oberheide, Farnam Jahanian, Internet inter-domain traffic, Proceedings of the ACM SIGCOMM 2010 conference on SIGCOMM, August 30-September 03, 2010, New Delhi, India

If this move continues, the Internet will consolidate into a network where end-user hosts will connect for the most part to a relatively small number of data centers hosting popular services. In this topology, the links connecting data centers to each other and to access networks become more important than other links. Given the way these links are operated, it will be necessary to use them at maximum efficiency to avoid bottlenecks and the waste of networking resources, especially in an economic context where the need for networking resources increases more quickly than the growth of most Internet service providers[5].

The topology of the Internet has evolved through economic and technological optimization decisions to become a flatter structure where major content providers and distributors get as close as possible to the access networks used by their customers, bypassing intermediate Internet service providers. The result is a flatter topology for the Internet's backbone network. The trend towards flatter network architectures can also be found in the area of access networks.

The traffic/management split

While the flat architecture of the Internet's backbone resulted in uncoordinated optimization decisions being made by major Internet actors in order to optimize their operations, flattening the infrastructure's architecture has been advantageous to access networks for the design of the future LTE network architecture and modern data centers.

In LTE, the design of access networks is significantly flatter than the packet networking infrastructure architecture in both 2G and 3G.

LTE's core network, management and data transfer functional elements have been separated to split traffic operation from signaling and management. This design allows management equipment to have a more consistent view of the network load and state while taking routing or resource distribution decisions.

In a data center's internal network architecture, network administrators and engineers think about using the same kind of management - traffic operation split by using software-defined networking technologies. Software-defined networking is a term first coined by Technology Review[6] and refers to the design and implementation of interfaces and access methods to control the routing and switching operation of network equipment. In software-defined networking, traffic management decisions are taken on a central server and applied by switches and routers in the network.

OpenFlow[7], the flagship initiative in this area, was created as a research experimentation project and is now gaining ground as it is being adopted by both equipment vendors and

The topology of the Internet has evolved through economic and technological optimization decisions to become a flatter structure where major content providers and distributors get as close as possible to the access networks used by their customers.

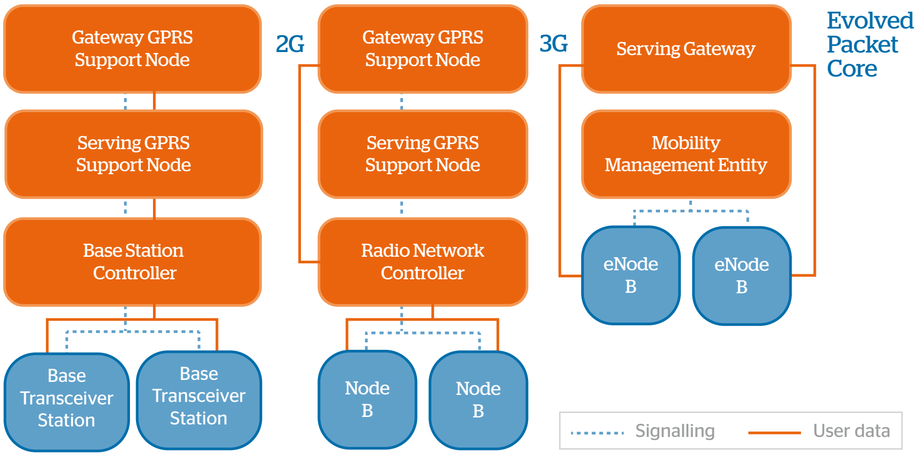

Figure 5: Comparison of mobile data network architectures

[5] Forrester Research, The Future of Data Center Wide-Area Networking, info.infineta.com/l/5622/2011-01-27/Y26, 2010
[6] TR10: Software-Defined Networking, http://www.technologyreview.com/biotech/22120/
[7] OpenFlow, https://www.opennetworking.org/standards/open-flow

infrastructure operators, such as Facebook, Yahoo! or Google. It is radically different from the original approach adopted in the design of the Internet. In this approach, routing decisions are taken locally to foster the independence of network nodes, which comes at the price of a more limited view of other elements in the network. The rise of software-defined networking shows that in an Internet that has become asymmetric, the result of the trade-off between the independence of routing equipment and centralized management of the routing policy needs to be studied carefully.

Flat network designs for access networks have emerged as some of the initial basics of the Internet have been questioned. Network management and data traffic relaying functions have been split, and some intelligence has been concentrated in the process, which harms the 'intelligence at the edge' principle of the initial Internet. In the long run, the question will be whether the Internet will continue to become increasingly concentrated, driving it towards a more centralized network, or if there will be a new wave of decentralization.

The question will be whether the Internet will continue to become increasingly concentrated or if there will be a new wave of decentralization.

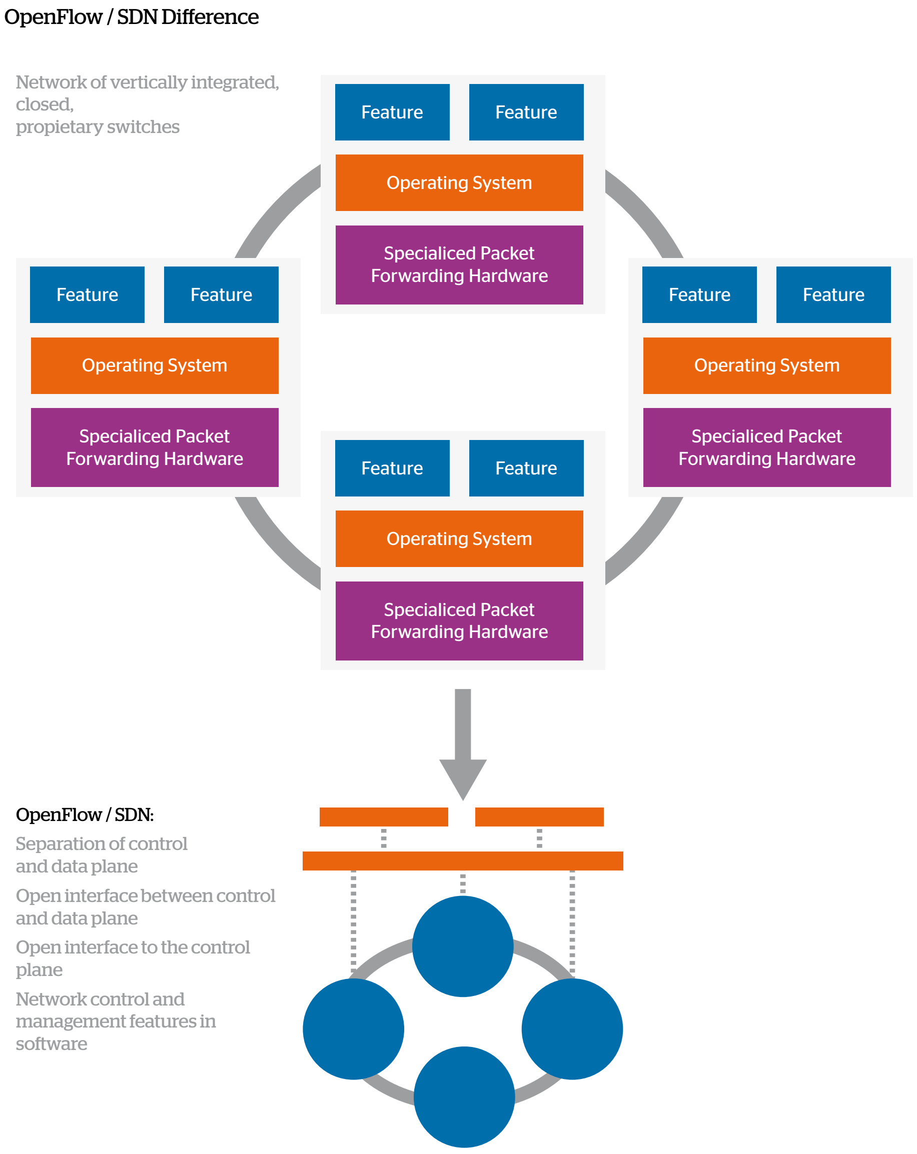
OpenFlow / SDN Difference
Network of vertically integrated, closed, propietary switches
Feature
Feature
Operating System
Specialiced Packet Forwarding Hardware
OpenFlow / SDN:
Separation of control and data plane
Open interface between control and data plane
Open interface to the control plane
Network control and management features in software

Figure 6: Description of software-defined networking (source: http://opennetsummit.org)

Concentration vs. distribution

The balance between centralized services and decentralized approaches has always been a topic of debate with regards to data networks. The Internet was initially designed to be a completely decentralized network, with intelligence located at the edge. Yet, connected services using the Internet have often wavered between fully-centralized architectures (terminal server, web services) and completely decentralized ones (meshed networks, peer-to-peer) with middle ways such as rich desktop applications or rich Internet applications.

Today's Cloud computing trend is associated with a rather centralized way of thinking about connected architectures as peer-to-peer protocols are declining as a result of the global struggle to enforce respect of copyright on media shared using those protocols. Meanwhile, new technologies such as WebRTC (Web Real Time Communication), a complement to the HTML5 standard, and plugins allow direct, peer-to-peer communication between applications deployed on the web. The development of such technologies will foster the deployment of connected services using a centralized approach, to keep the most critical or value-added services and connections under control, while bulk or delay sensitive data transfers will be done in a direct, decentralized mode.

Even if the Cloud computing trend moves toward a concentration of connections and a rather small number of central nodes, traffic optimization and offload policies could lead to the development of mixed approaches where bulk traffic will transit in a peer-to-peer mode while being controlled in a centralized way.

The Internet protocol mix

Today's Internet features a hegemonic use of the HTTP protocol on top of the Transmission Control Protocol (TCP). It has been shown that today HTTP and its secure counterpart HTTPS together account for 52 percent of inter-domain traffic on the Internet[8]. This impressive share of HTTP/HTTPS in the amount of overall Internet traffic is directly related to the use of this protocol to access Cloud 'as a service' applications either via a web browser or through dedicated Application Programming Interfaces (API). Application developers sometimes consider HTTP to be a transport protocol. That it is often simpler for a web or application developer to use HTTP to transfer data using the Extensible Markup Language (XML) or another structured data format comes at the price of a larger network footprint. The burden of web services access protocols compared to using tailored, lower level protocols is important and artificially introduces a need for a larger bandwidth.

The generalization of HTTP contradicts the need for mobile devices and objects participating in machine-to-machine (M2M) communication to benefit from lightweight protocols tailored to the applications' needs as well as to those devices' limited capabilities. Even in a data-center environment or in web applications, using a lightweight protocol can prove to be useful in order to reduce the protocol burden over well-identified protocol exchanges. Recently, several protocols have aimed at tackling these specific issues: Apache Thrift, a set of individual protocols that share object encoding and formatting properties that translate easily to more verbose protocols; Protocol Buffer, a method for exchanging structured documents over a dedicated TCP connection; MQTT (Message Queue Telemetry Transport), a lightweight publish/subscribe/notify protocol on top of TCP; and SPDY, a protocol developed by Google aimed at reducing webpage load latency by using compression and multiplexing techniques. Even if they have various scopes and uses, these protocols are alternatives to the hegemonic use of HTTP in more specific use cases.

Although several protocols have emerged from software development and M2M communities to address specific needs and use network resources efficiently, HTTP and HTTPS still dominate to the point that it can sometimes be considered as the transport protocol of the Cloud-computing Internet. As HTTP operates in a client/server mode, its importance is another crack in the initial peer-to-peer, reciprocal design of the Internet.

To sum up

The uses of the Internet have directed its evolution from the original desire to reconcile a resilient, datagram network with a network where some peers have a specific role as they offer popular contents or services. This evolution has led to several technological choices and optimization regarding the mechanisms and protocols used to communicate on the Internet.

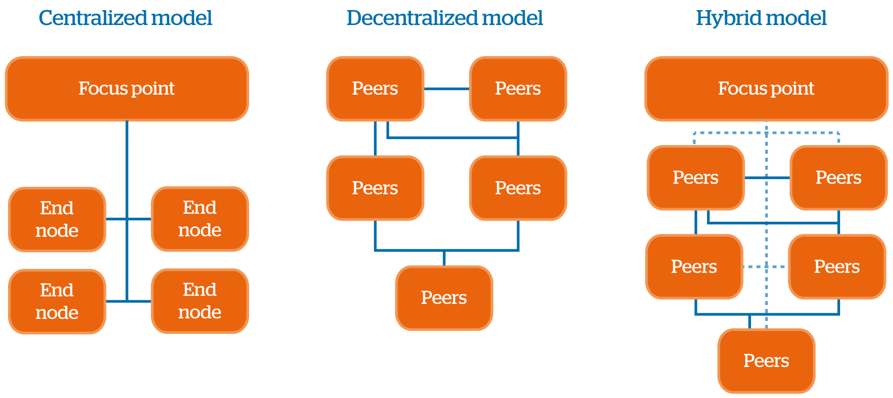

Figure 7: Comparing centralized, decentralized and hybrid models

[8] Craig Labovitz, Scott Lekel-Johnson, Danny McPherson, Jon Oberheide, Farnam Jahanian, Internet inter-domain traffic, Proceedings of the ACM SIGCOMM 2010 conference on SIGCOMM, August 30-September 03, 2010, New Delhi, India

Where is the research heading?

A future Internet?

The previous chapters have shown that the Internet is facing several technical trends, needs and challenges that influence its development, adaptation and governance. Indeed, several research groups and global initiatives are seriously reconsidering the design of data networks in order to tackle the main issues related to security, reliability quality of service, manageability, mobility and energy consumption.

Among these initiatives, Atos is a member of the Future Internet Public Private Partnership, a European initiative that clusters European-funded projects and gathers academic as well as industrial researchers in an effort to redesign data networks according to the needs of several application fields. In this regard, Atos, through the Atos Research and Innovation unit, participates in research work and leads several projects within the frame of this assembly. In particular, Atos is part of the FI-WARE project, the aim of which is to build the core platform of the future Internet. This core platform will consist of a set of generic enablers that allow the development of future-proof connected services.

Around the world, other initiatives are also tackling the same issues. In the US, most of the research around future Internet protocols and architecture comes under the umbrella of the GENI (Global Environment for Network Innovations) initiative. GENI is a set of infrastructure elements deployed on a large scale across the US in which researchers can lead experiments to test network design assumptions or protocol implementations. In Japan, research on the implementation of a new-generation Internet is performed via the AKARI project. This project has similar goals to the Future Internet Public Private Partnership and has led to the identification of five different models for future networks which emphasize device heterogeneity, security or quality of service. The follow-up of this work is to identify the inconsistencies between the acknowledged models in order to reach a clear, future-proof Internet architecture.

In discussion groups around these initiatives, two approaches are being pushed. Some researchers support a clean-slate approach for the complete redesign of data networks. They believe that the issues that the Internet is facing are so important that they cannot be fixed using ad-hoc technologies. They would like to rebuild the Internet taking into account quality of service, real time, security and other concerns when designing data networks. This clean-slate approach is questioned by other researchers who would like to adopt an evolutionary approach to changing the Internet, as too much equipment and too many applications are already using the Internet in the way it was designed.

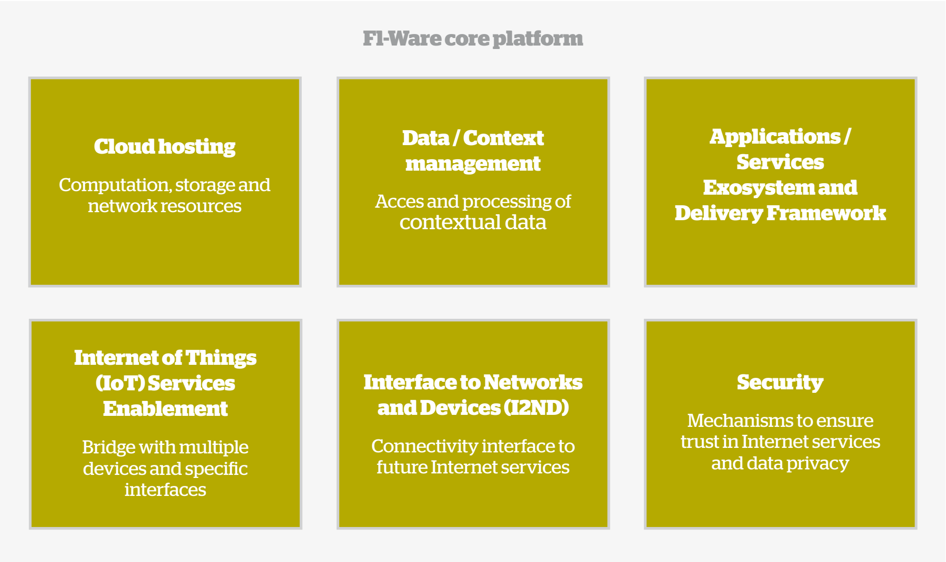
FI-Ware core platform
Cloud hosting
Computation, storage and network resources
Data / Context management
Acces and processing of contextual data
Applications / Services Exosystem and Delivery Framework
Internet of Things (IoT) Services Enablement
Bridge with multiple devices and specific interfaces
Interface to Networks and Devices (I2ND)
Connectivity interface to future Internet services
Security
Mechanisms to ensure trust in Internet services and data privacy

Figure 8: FI-WARE generic enablers

On the clean-slate approach side, researchers are designing several reference architectural models in order to address the concerns of the current Internet. These models base their design on various theoretical backgrounds to suggest a well-suited design for the Internet: for instance, the Real World Internet model applies concepts coming from the Internet of Things and suggests a mapping of the Internet architecture to real-world exchange patterns and methods. The Future Content Networks (FCNs) reference architecture pushes a content-centric approach to rethink the Internet, based on the fact that most uses of data networks are centered on collaboration around a document. This initiative shares some observations and concepts with the Content-Centric Networking concept which is promoted by Van Jacobson, among others. In these approaches, the network is tailored to ease the finding, retrieval and caching of contents or documents while the original Internet focuses on connecting hosts. This shift has big impacts on the way addressing, routing and resource naming is carried out.

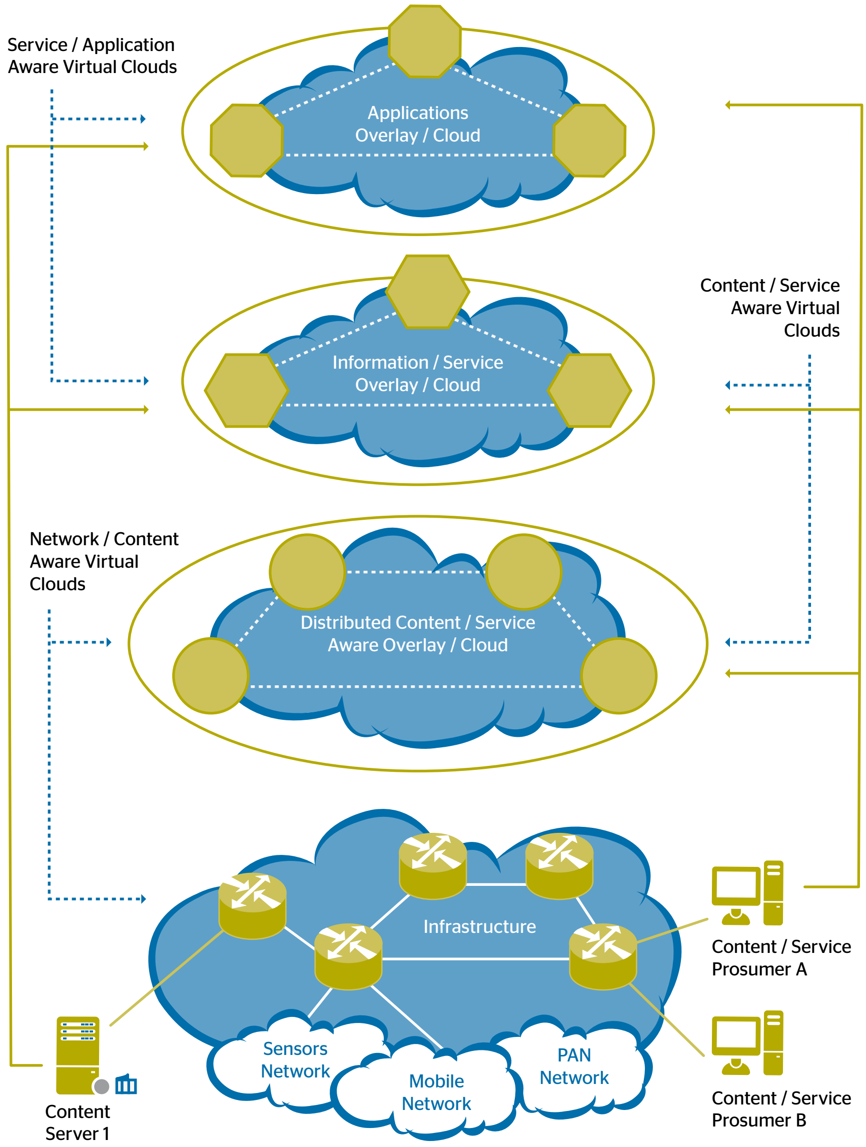

Figure 9: The FCN reference architecture

Most concepts used in the content-centric approach are already used in peer-to-peer overlay networks at a higher level in the architecture, which may indicate the potential use of this approach in an evolutionary scenario for the Internet.

Other approaches, such as the Management and Service-Aware Architectures (MANA) reference model or the Future Internet Service Offer (FISO) reference model, base their research work on the application of service-oriented architectures (SOAs), service orchestration and service reusability concepts, which make them particularly suited to accompany the move towards Cloud computing and centralized services in general. While these models are still quite abstract, they should be closely monitored as they reuse several key concepts of computer science, such as service orientation, polymorphism and virtualization in an effort to set up future data networks.

Several research initiatives in Europe, in the US and in Asia are trying to rebuild a better Internet from the ground up following a clean-slate approach to most current Internet issues. Yet, deploying these network architectures will take time and today's research projects are not yet adequately developed for the deployment to be envisioned. In the meantime, the Internet is currently suffering from several critical issues that need to be addressed to avoid dysfunction due to the growing number of peers using the network. Among these issues is the use of IP to both locate and identify hosts in the Internet, which is key to better addressing device mobility on the Internet.

The Locator - identifier split and its potential effects

Currently, IP addresses are used to reach a given network interface. Over time, these addresses have also been used to identify hosts. In an Internet where hosts have a single and fixed location to the network, this is not a real problem. Yet, issues arise when devices can move from access network to access network, or when they have multiple interfaces to the Internet. In such situations, IP addresses can either be provided to the device by the edge network equipment or fixed on the device. In the former case, the address is said to be connection-attached, while in the latter case, the address is device-attached. In a connection-attached model, when a device changes access network it changes its IP address. Therefore, all ongoing connections are disrupted and have to be re-established when the device gets its new address. In addition, a naming scheme has to be used and agreed upon to identify both sides of the connection, either for security or service continuity purposes. In the device-attached model, every time a new device joins an edge communication network, the router managing this edge connection has to manage this new address and advertise it together with the addresses of all other attached devices. As the probability that these addresses can be easily concatenated is low, the number of addresses advertised by the edge router up to the core of the network is extensive, which leads to an explosion of the core routers' routing tables. The same kind of issue appears when devices have two interfaces used in conjunction to access the Internet.

To solve this issue, several projects have proposed methods to dissociate the identification and locator roles of IP, such as Host Identity Protocol (HIP) and Site Multihoming by IPv6 Intermediation (SHIM6). These projects suggest solutions to the collision of the locator and identifier role of IP addresses on the existing Internet, either by suggesting endpoint solutions to the issue or by using intermediate network elements to minimize modifications made at the end hosts. One of the most advanced of these initiatives is the Location/Identifier Separation protocol (LISP). LISP is a 'map and encap' protocol; i.e. it uses encapsulation and mapping mechanisms to route traffic from one local area to another. In the local area, the IP address is used as an identifier and within this area, even if addresses cannot be easily aggregated, complexity is limited by the area scope. In the global arena, the IP address is a locator used to route packets efficiently. Border elements ensure gate operations between local and global areas, as depicted in Figure 10.

This now experimental approach still suffers from performance issues and is challenged by competing approaches, such as HIP, yet it gives a potential answer to the routing table expansion issue by isolating local addresses that can be used as identifiers from globally routable addresses.

Several projects have proposed methods to dissociate the identification and locator roles of IP.

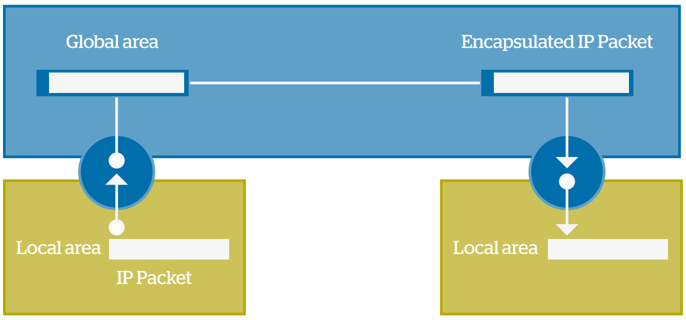

Figure 10: Simplified schema of a 'map and encap' protocol

Splitting the locator and identifier roles of IP addresses either at the Internet's endpoints or in some network elements can ease the management of mobility and multihoming, as has been shown by current experiments. Operations of transport protocols on top of this enhanced network layer could therefore benefit from lower layer optimization. These transport layer protocols can then be enhanced to take into consideration increase in bandwidth and stability of completely managed network links.

Transport layer optimization

In addition to the birth of the Internet, the Transmission Control Protocol (TCP) was also designed to allow peers in an IP network to reliably send and receive data; i.e. ensure that even if packets are dropped, every bit sent to be transmitted from one end to the other is received. To manage such reliable transmission, TCP uses an algorithm to detect congestion along the path and avoid it - the slow start and congestion-avoidance mechanism - which directs the settings of the packet size sent between the hosts. This congestion-avoidance mechanism was based on the assumptions that hosts are not able to predict the path taken by packets sent over the network; hosts have a single interface to the network and links between the hosts are fundamentally unreliable. These assumptions were particularly apt in earlier days, but don't describe today's reality, in particular regarding data-center networking. In data centers, network links are rather homogeneous, benefit from a high availability of bandwidth and failures can be detected. In racks, servers are often connected using multiple network interfaces, and multihomed on switches depending on the same router. In this situation, the slow start and congestion-control mechanism used in the original TCP is suboptimal and sometimes its imperfect functioning leads to delays and the underutilization of network links. To address congestion management problems in specific use cases of the TCP protocol, several research teams have suggested alternative congestion-avoidance mechanisms, such as data-center TCP (DCTCP), which enhances the TCP congestion-control algorithm by leveraging a new feature of data-center switches called Explicit Congestion Notification (ECN). The analysis of ECNs gives the host hints with regards to the presence of congestion and its severity, which are used to shape the traffic sent over the connection.

Together with optimization efforts on the transport layer, other research teams are working on the possibility of scheduling the use of managed network resources in data centers. They base their work on the observation that inside data centers and between distant data centers, a large part of network resources is being consumed to convey traffic that does not originate from direct user interaction with the system: virtual machine transfer, backup, replication, etc. This traffic can be reordered and delayed in order to avoid charging the network at precise peak hours or in cases of a sudden service demand and to use the resource more efficiently when user-generated traffic is lower.

While perfectly suited to conditions at the birth of the Internet, the design decisions that drove the creation of the transport protocols used then are no longer applicable to today's Internet. Research is underway to enhance these protocols in particular situations, for instance in data centers where network is an important yet under-optimized resource. These research projects play a role in slowly changing the Internet while solving issues that arise in critical yet rather specific use cases. Taking into consideration these specificities is another way to underscore the need to stop considering the Internet as a homogeneous network of peers.

> We need to stop considering the Internet as a homogeneous network of peers.

Conclusion and Glossary

Conclusion

The Internet, which was created in the 1970s as an experimental research network connecting universities and research institutions has morphed from a reciprocal, peer-to-peer network where all the intelligence resides at the edges of the network into a more complex infrastructure mixing peers of very different nature and capabilities, connecting from fixed or mobile, using a low- or high-bandwidth access network. The huge development of Cloud computing and online services has led to technological evolutions that tend to break the symmetry of the Internet. Indeed, the Internet tends to resemble a network where a majority of the traffic is from a rather small set of peers; i.e. data centers hosting the providers of the most popular Internet content and services. These peers are accessed by a rather large number of devices connecting through diverse access networks and collaborating with a smaller set of peers also operated from large data centers with which they benefit from high-capacity links. This Internet is shaped by online-hosted services and Cloud offerings and is flatter than it used to be 10 years ago, as major service providers try to get as close to their clients' access networks as possible through direct peering or via content-delivery networks that bypass regional and national transit network providers.

While the increase in network-link capacity naturally enhances the quality of the connection to online services, several issues that are inherent to the way Internet protocols have been designed will remain unsolved until network operators and service providers question the design assumptions that have driven the Internet's creation. This is the aim of ongoing research efforts from the networking community which try to both rebuild the Internet from the ground up in a clean-slate approach and to develop incremental solutions to critical yet very specific issues.

Atos, as a major European online services operator and Cloud solutions provider is monitoring this evolution, and even anticipates it through its participation in the Future Internet Public Private Partnership research project and its own R&D tests of new protocols and network designs in order to adapt to this ever-evolving environment.

Glossary

API: Application Programming Interface

EDGE: Enhanced Data Rates for GSM Evolution, an evolution of GPRS

FCN: Future Content Networks

FISO: Future Internet Service Offer

FP7: Seventh Framework Program of the EU

GENI: Global Environment for Network Innovations

GPRS: General Packet Radio Service

GSM: Global System for Mobile communications, derived from the French "Groupe Spécial Mobile"

HIP: Host Identity Protocol

HSDPA: High Speed Downlink Packet Access, an evolution of UMTS

HTTP: Hypertext Transfer Protocol

HTTPS: Hypertext Transfer Protocol Secure

IANA: Internet Assigned Numbers Authority

ICT: Information and Communication Technologies

IETF: Internet Engineering Task Force

IP: Internet Protocol, used to route packets across networks

IPv4: Version 4 of the Internet Protocol

IPv6: Version 6 of the Internet Protocol

IT: Information technologies

LISP: Locator/Identifier Separation Protocol

LTE: Long Term Evolution, i.e. the evolution of mobile cellular networks beyond HSDPA

M2M: Machine-to-Machine

MANA: Management and Service-Aware Architectures

MQTT: Message Queue Telemetry Transport

NAT: Network Address Translation

NIST: National Institute of Standards and Technology

OS: Operating system

REST: Representational State Transfer

SDN: Software defined networking

SOA: Service Oriented Architecture

TCP: Transmission Control Protocol

UMTS: Universal Mobile Telecommunications System, a third generation mobile network technology

WebRTC: Web Real-Time Communication

Wi-Fi: Wireless Fidelity

WIMAX: Worldwide Interoperability for Microwave Access

XML: Extensible Markup Language

About Atos

Atos is an international information technology services company with annual 2011 pro forma revenue of EUR 8.5 billion and 74,000 employees in 48 countries. Serving a global client base, it delivers hi-tech transactional services, consulting and technology services, systems integration and managed services. With its deep technology expertise and industry knowledge, it works with clients across the following market sectors: Manufacturing, Retail, Services; Public, Health & Transports; Financial Services; Telecoms, Media & Technology; Energy & Utilities.

Atos is focused on business technology that powers progress and helps organizations to create their firm of the future. It is the Worldwide Information Technology Partner for the Olympic and Paralympic Games and is quoted on the Paris Eurolist Market. Atos operates under the brands Atos, Atos Consulting & Technology Services, Atos Worldline and Atos Worldgrid.

atos.net