Horizon Project

ANR call for proposals number ANR-08-VERS-010
FINEP settlement number 1655/08

Horizon - A New Horizon for Internet

WP4 - TASK 4.1: Internet Service Requirement Analysis and Case Study
(Annex J)

Institutions

Brazil
GTA-COPPE/UFRJ
PUC-Rio
UNICAMP
Netcenter Informática LTDA.

France
LIP6 Université Pierre et Marie Curie
Telecom SudParis
Devoteam
Ginkgo Networks
VirtuOR

Contents

List of Figures

List of Tables

Chapter 1

Introduction

The Internet is a great success. Since it was created, the Internet has expanded and been used for many different applications. In the end of 2008, the Internet had exceeded the 1.5 billion user mark. This growth is also a reality in Brazil, as shown in Table 1.1. Even though this expansion indicates approval and acceptance by users, some limitations appear in order to attend requirements such as security, mobility, and quality of service. These limitations result from the "ossification" of the original Internet design, which means that it is hard to modify the network core due to operational and economical issues.

The Internet requirements were initially defined according to the usage scenario in the 70's. The network connected universities inside the USA and users were trustworthy and owned technical knowledge and skills about the network. Nowadays the reality is different because people with all kinds of education and distributed around the world have access to the network, creating a totally distinct environment with plenty of conflicts [2].

Month/year	**Number of Users**
12/2005	12,25 million
12/2006	14,49 million
12/2007	21,3 million
12/2008	24,5 million

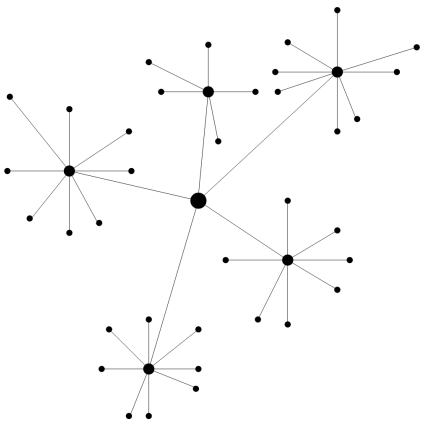
Table 1.1: Estimates of active residential Internet users in Brazil [1].

The first packet switching network was ARPANET (Advanced Research Projects Agency NETwork)[1], which was ordered by the Department of De-

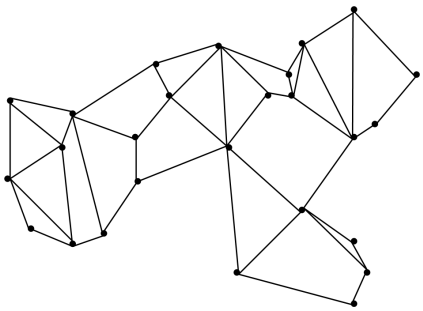
[1]The first communication system to use the ideia of packet switching was the ALOHA network proposed by Abranson in 1960. The ARPANET was the first packet switching

fense (DoD) of the United States in 1969, due to the "Cold War". The U.S. government, fearing a Soviet attack to the Pentagon, started to design a communication network that was more robust than the telephone network. Telephone networks were organized in central points, as shown in Figure 1.1(a), so an attack to one of these points could affect the entire network. Thus, ARPANET was design and built to be highly distributed and fault-tolerant, with a topology similar to the one on Figure 1.1(b), using packet switching. ARPANET links supported at most 56 kb/s,

where each node, consisting of a station and a switch called Interface Message Processor (IMP), should be connected to two other nodes to create alternative paths and guarantee reliability in case of node failures. The IMPs segmented and forwarded packets. Communication protocols for network nodes and final stations were also designed. Network protocols defined the communication between adjacent IMPs and the communication protocol defined the communication between the source and destination IMPs. Figure 1.2 shows the initial network project.



(a) Example of the centralized telephone system topology.



(b) Example of a distributed topology according to the ARPANET design.

Figure 1.1: Differences between the telephone system and the ARPANET topologies.

In the early 70's, many nodes were added to ARPANET and the difficulties to connect different networks became clear. As a solution, Vint (Vinton Gray) Cerf and Bob (Robert) Kahn proposed the Transmission Control Program (TCP), which introduced the concept of gateways that interconnect two

network.

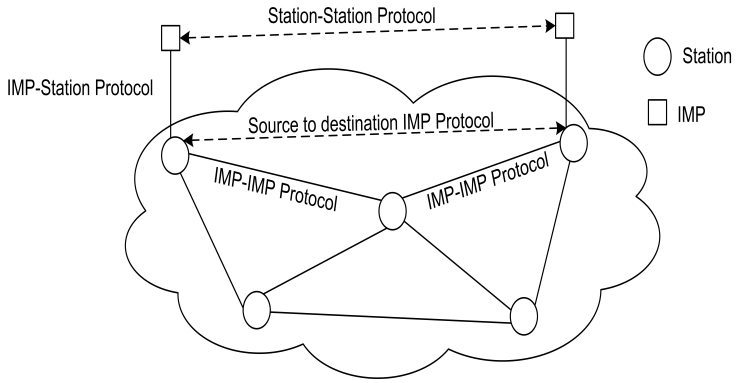


Figure 1.2: Protocols designed for ARPANET.

packet-switching separated networks. Besides, TCP specified the creation and destruction of logical connections between processes using packets of different sizes, the detection and recovery of transmission errors and packet-sequencing flaws, in addition to flow control and end-to-end error verification. This program also handled node addressing and packet forwarding. Hence, TCP is considered the beginning of the Internet [3, 4]. Later, in the early 80's, the Transmission Control Program was divided into two protocols, the Transmission Control Protocol (TCP) and the Internet Protocol (IP), which, respectively, transports and forwards data in the network. This was the beginning of the TCP/IP model, which became the reference model for the Internet architecture. Many consider ARPANET the mother of Internet and the TCP/IP model the origin of the current Internet.

The Internet was designed emphasizing generality and heterogeneity in the network layer. Its structure is based on the principles of a simple and transparent network core with intelligence in the endpoint systems. Besides, the network

was decentralized and divided into multiple autonomous administrative regions [5]. Nowadays, however, these principles make users frustrated when something doesn't work, because the nodes in the core are simple and don't provide much information about the network operation. This also leads to a high overload in manual configuration, debugging and design of new applications. The design of new applications, at first, should be easy because the network is simple and doesn't impose many restrictions. Nevertheless, applications are responsible for implementing all needed functionalities, which makes their development much more complex. In this scenario, new applications appear bringing requirements that are incompatible with the current network architecture, such as a higher interference of the network core.

Due to difficulties recently found in the network, there is a consensus that the Internet needs to be reformulated, creating the "Internet of the Future". This new Internet must keep principles that led the current Internet to its success, such as easy deployment of new applications and protocol adaptability, and also hold new concepts, such as self-healing and self-management, and may acquire principles of intelligence and knowledge.

This report is organized as follows. In Chapter 2, the principles of the Internet and the modifications in its core, called patches, will be discussed. In Chapter 3, the main limitations of the current Internet and the requirements of the new Internet are pointed out. At last, Chapter 4 presents our final considerations.

Chapter 2

Current Internet and its Evolution

2.1 Architectural Principles of the Internet

These requirements, established to attend military and university networks, allowed the creation of a large scale network, composed of different networks, each one with its own administrative entity. To fulfill these requirements, some principles and solutions were chosen, which are:

- adoption of a multi-layer model, which later became known as TCP/IP Model
- utilization of packet-switching and the best-effort delivery models
- transparency
- complexity in the end-points
- the immediate delivery of packets
- subnet heterogeneity
- the use of global addressing

After, new requirements were added, such as:

- distributed control
- global routing calculation
- region division

- minimal dependency

These principles ruled the development of today's Internet architecture and protocols.

Multi-layer model - The choice of a multi-layer model aims at reducting system complexity by dividing and isolating network features, allowing each layer to have specific roles and serve[1] its upper layer. This results in a communication model based on encapsulation, in which data pass through upper to bottom layers in the sender, and through bottom to upper layers in the receiver, as seen in Figure 2.1.

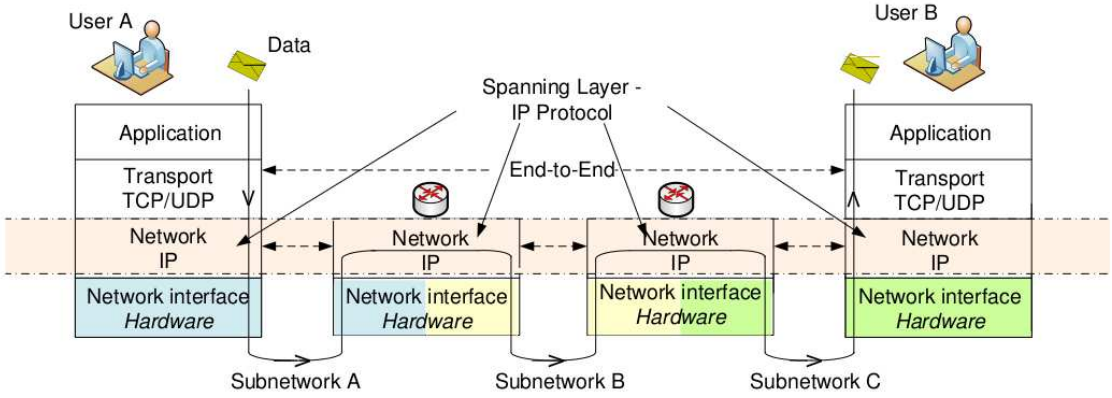


Figure 2.1: Representation and use of TCP-IP protocol stack.

TCP/IP is the multi-layer model that specifies the protocol stack of the Internet architecture, which is the main reason of of today's internet success but also determines several problems. Among its successes, a lesser number of layers in comparison with de OSI (Open System Interconnection) model and the interoperability among different technologies stand out. In comparison with the OSI model, which consisted of seven layers, the Internet divides the communication system in just four layers, allowing a simpler and cheaper implementation. The definition and semantics of the IP allows the translation of the transport layer to a variety of bottom-layer technologies,

[1]A service defines the visible functions of a layer to its upper layer. The TCP protocol offers a reliable data transfer "service" and therefore guarantees the delivery of the data with no errors. The application layer, which sits on top of the transport layer, just handles the data to the transport layer (TCP protocol) for it to be delivered with no errors on the destination. To provide this feature, the TCP protocol has several mechanisms such as error control, flow control, packet segmentation, which are transparent to the application layer. Therefore, the multi-layer model simplifies the project, the development, and the error debugging in a communication system.

which is called Spanning Layer [6], ensuring interoperability between various technologies in the Internet. The IP layer is considered an efficient spanning layer because it allows packets to be transmitted to any network technology through a uniform interface, interconnecting a variety of applications to the many existing network technologies. In addition, the simplicity of the TCP/IP model implies a dummy network, which allowed fast evolution of applications and the fast growth of the network. On the other hand, the simplicity of the model is also responsible for the ossification of the Internet, because the absence of intelligence in the network implies restrictions to application development, also hindering the resolution of structural problems such as scalability, management, mobility, security, etc. Thus, although the TCP/IP model is efficient and meets the original requirements of the Internet, it may not be the best solution for the Future Internet.

Packet Switching and best effort - Packet switching was preferred over circuit switching to provide a robust network that could survive disasters and still be efficient, through the sharing of available bandwidth [7]. The robustness is obtained through alternative path redundancy from the source to the destination. The datagram technique, used in packet switching, in addition to a mesh topology, allows finding alternative paths after some infrastructure fault. Efficiency is obtained from sharing available bandwidth between all packets, because the circuit switching implies in idle time in network links, due to dedicated bandwidth. Packet switching technique segments data in little units of variable size, called packets, that contains a destination address to be forwarded through the network. In the Internet, as a project option, each packet is forwarded according to the best effort discipline, independently of other packets. The choice for the best effort service results in simple and low cost nodes since it lacks error correction and resource allocation policies. The best effort service, however, doesn't offer admission control, maximum delay guarantee, and not even the delivery of the packets to the destination [8]. Thus, packets that pass through different node queues in its path from the source to the destination suffer different delays depending on the queue occupation. In addition, packets that meet full queues are discarded, never reaching its destination. Since packets are independent units of data, packets with the same source and destination may be forwarded by different paths and also arrive at an order different than that sent, due to different delays through the network. Besides the greater efficiency in the utilization of available bandwidth, the choice of packet switching and the best effort model allows stateless forwarding systems, ensuring scalability and low cost in implementation and maintenance. These were important factors for the success of this scheme.

Transparency - Today's Internet provides syntactic transparency, meaningthat a packet is forwarded from source to destination without suffering data modification from the network. Thus, user data, in the absence of transmission errors, is transferred from source to destination without any modification.

End-to-end principle - The end-to-end principle implies a simple core network with endpoint intelligence. This principle is a fundamental part of the Internet architecture and suggests that application layer specific functions should not be part of lower levels of the network core, since these functions can only be implemented correctly and completely just with application knowledge in the endpoints of the communication system [9]. Thus, the network function is only to forward packets. This ensures a simple and flexible network structure, in which only the endpoints are responsible for the communication functions, thus making the network more robust. Hence, problems such as loss of a communication state implies only in problems for that application, not in network fault. As consequence, all delivery control and retransmission, the packet storage for loss recovery, and flow control are performed only by the endpoints without network interference [6].

Immediate delivery - Another ruling principle of the Internet is the immediate delivery of a packet in the absence of network failures or overloads, according to the best effort model. There is no persistent storage of the message inside the network. Thus, connectivity must be continuous over time, which means that undefined delays should not exist in packet delivery, and also there should be no intermittent connections, as suggested for Delay and Disruption Tolerant Networks (DTN) [10].

Subnet heterogeneity - According to this principle, there are basic premises regarding network interface layer features. For instance, a subnet must be capable, at least, to transfer a data unit, a burst of bytes, and support synchronization of the data unit. Then, a subnet is responsible for the synchronization of packets and frames that cross the subnet. Thus it is possible to connect different subnet technologies, through basic feature premises of the network interface layer. Each subnet may have its own features such as bandwidth, latency, error patterns and Maximum Transmission Unit (MTU), without the need for whole network changes.

Global addressing - The architecture of the Internet, in principle, depends directly on the existence of a global address space in which unity of each address is ensured. Packet forwarding decisions are also taken based in this addressing space. In fact, the IP address, besides identifying nodes, provides a convenient global localization of nodes on the Internet, due to the address hierarchy.

Distributed control - According to this principle, there should be no single points of failure in the network control algorithms. These algorithms must be fully distributed, to ensure the robustness of the network.

Global routing calculation - To fulfill the requirement of robustness in the network with regard to data delivery, the Internet must perform global route calculation in a hierarchical manner to support packet forwarding with no loops based only on destination address.

Region division – The Internet is as an interconnected collection of Autonomous Systems (ASs). Each AS is managed by an Internet Service Provider (ISP), which handles a backbone connecting the client to other ISPs [11]. The management of one AS is done apart from other ASes, allowing some options as the choice of routing protocols, management policy, and the type of provided service. The collaboration between ASes is accomplished by the Border Gateway Protocol (BGP), through which route announcements are exchanged between neighbors domains and, therefore, reachability information are propagated to the AS [12]. Thus, the routing tables are calculated based on the AS internal routing protocol (Interior Gateway Protocol) and on the data obtained by the BGP. The collaboration between different ASs guarantees the existence of a totally distributed network. An important positive consequence to the Internet success is that this kind of structure guarantees a robust network, because if one AS has a problem, the network builds alternative routes to avoid this AS.

Minimum dependence – This principle determines that the end-to-end communication must be provided if at least one minimum network service set is available. Thus, if two stations know each other address and there is a path between the two nodes, the communication must happen even if additional services, like name resolution by the Domain Name System (DNS), are unavailable. In addition, the minimum dependence also implies that, if two nodes are directly connected, they can communicate without the help of a router, because there is no specific network access protocol for the Internet [6].

2.2 Evolution through "patches"

Despite the Internet well defined project requirements, in these forty years, the network structure has been modified through patches to meet the new needs and requirements. To understand the problems caused by these modifications, it is necessary to analyze the network development, the emergence of new requirements and the impact of the modifications into the initial fundamental ideas. Moreover, the assessment of the Internet evolution

reveals the positive impact of the TCP/IP model, the transparency, and the end-to-end principles to the growth of the Internet but today are barriers to provide new services in the network.

During the 80's, more and more local networks were connected to the ARPANET, creating the need for network changes. Thus, the Internet started to be patched with the creation of the sub-networks, autonomous systems, and of the Domain Name System (DNS) to provide scalability [13]. Another patch related to the scalability was the adoption of Classless Internet Domain Routing (CIDR) in the 90's [14]. The sub-networks are presented as a solution to the universities and big companies demanding interconnection for their different local area networks. Then, the Internet changed from a two level hierarchy model, composed by the Internet on the superior level as a whole and the local network on the bottom level with its identifier, to a model of three hierarchy levels, in which a local network can be subdivided in many networks [15]. Thus, the mask concept was proposed and it is being utilized till today on the Internet.

The network division on Autonomous Systems (AS) was another consequence of the increase of the number of users in the early 80's. The increase of the network created a demand for the adoption of a hierarchic structure, because the information overload between the gateways became very high on every route update and the size of the routing tables greatly increased with the addition of new networks. Another problem that simultaneously arised was that a variety of routers were being used with implementations of different companies of the Gateway-to-Gateway Protocol (GGP), which made the maintenance and the failure isolation almost impossible. Hence, it was chosen to leave the one network model to the division of the network in many regions with their own administrative autonomy, called ASes. In addition, a classification was proposed to distinguish the backbone ASes from the ASes that connect the local networks to the Internet, called stubs ASes. Each stub AS must have at least one special router connected to the Internet backbone. Communication between these stub ASes is accomplished by special routers and the Exterior Gateway Protocol (EGP) was proposed, it is another patch to the architecture. The Interior Gateway Protocol (IGP) nomenclature was specified to the AS internal communication, which can be any routing protocol, as the Routing Information Protocol (RIP), the Open Shortest Path First (OSPF) and the Interior Gateway Routing Protocol (IGRP) [16].

In the late 80's, the Exterior Gateway Protocol (EGP) has already presented several limitations, like the need of a tree structure of ASes interconnection to not create loops, that are incompatible with the Internet growth. The EGP used a simple route calculation algorithm that indicated the next AS, like the distance vector algorithm. Due to the independence among au-

tonomous systems, each AS could choose the route metric according to the AS policy, which could cause inconsistencies and routing loop formation. So, the AS interconnection topology was restricted to trees and, as a consequence, without loops. With the increasing number of links, the ASes interconnection topology becomes increasingly rich and the inter-ASes topology has become a mesh, in which the EGP won't work. Thus, the Internet Engineering Task Force (IETF) introduced the Border Gateway Protocol (BGP) to work properly on a mesh topology, adopting a new route calculation algorithm, the path vector. In this algorithm, the announced routes contain the entire ASes path to reach the destination, rather than just the destination and next hop. Hence, the loop is avoided, even with the utilization of different metrics by the different ASes. The BGP has changed over the 90's and is currently on version 4. An interesting change brought by the BGP-4 was the support to the Classless Inter-Domain Routing architecture (CIDR), to avoid the fast Internet addresses consumption and the routing-table explosion. At the beginning of the Internet, it was chosen to use 32 bits addresses, in which 8 bits represented the network and 24 bits indicated the station. Due to the network growth, they soon realized that the 8 bits were insufficient to map all the networks. As a result, address classes were created as in the table below. The address classes division patch, however, was not efficient, because the demand for class C address was small, since most organizations had more than 254[2] machines. On the other hand, the class B address let many unused address, since most organizations had less than 65.534 machines. Thus, a run out of the class B network addresses happened. To improve the addresses distribution, the Classless Inter-Domain Routing architecture (CIDR) was proposed, representing a new patch [14]. With the CIDR, the addresses were better assigned and route aggregation could be done, decreasing significantly the routing-table size.

Table 2.1: Internet addresses classes before CIDR.

Class	**Network bits**	**Bits for *host***	**Available addresses**
A	8	24	167.777.216
B	16	16	65.536
C	24	8	256

Still on the network growth context, another difficulty found was the stations location. It wasn't possible anymore for a user to memorize the des-

[2]Despite the 256 possible addresses, the addresses with all "0" and all "1" are reserved for network address and broadcast address, respectively.

tination IPs, which led to the creation of the Domain Name System (DNS). The DNS is a distributed database which allows the name assignment to IP addresses. The DNS is considered as an important patch to the Internet architecture but due to its hierarchic structure in which there are root servers, goes against the original idea that the network wouldn't have central points, being a single point of failure.

Another important change in the 80's was the introduction of congestion control techniques [6] in TCP. In 86, the Internet suffers from the first series of congestion collapses, which led to the introduction of the following principles: the transport protocol at the last node must sensor congestion and reduce the transmission rate when it is needed; the packet transmission must be controlled by acknowledgement messages; and there must be sufficient buffer to a station operate the congestion adaptive algorithm with the Round Trip Time (RTT) control [17]. Such patches were of primordial importance for the Internet to continue working even with the network scale growth.

The IP protocol also received several patches over the years. The first patch attention was the the IP multicasting proposal[3] in the late 80's.

The IP multicasting aims at sending data from one station to a group of stations, denying the initial concept of sending information from just one station to another station. The multicast datagram must be sent utilizing the best effort principle like any IP datagram [18]. Another addition to the IP was the IPv6 [19] that aims at increasing the number of available addresses; simplifying the IP header, that had many unused fields; better support for options; allowing the identification of flows and adding authentication and privacy mechanisms at the IP layer. A "patch" to increase the number of stations on the Internet without allocating new addresses was the creation of Network Address Translation (NAT) [20]. With the NAT, the principle of unique global addressing is violated with the objective of using multiple equipments sharing a single valid address. Another addition, relative to security, on the IP layer is the IPsec [21], which objective is to introduce a security architecture that allows access control, integrity regardless of the connection, data-origin authentication , protection against replay attacks, and confidentiality. Another interesting "patch" is the Mobile IP [22]. Ipv4 assumes that the IP address identifies uniquely the point of connection of the node to the Internet. If the node changes this connection point due to mobility, it would be necessary to obtain a new IP address, due to the hierarchy of the addresses. Nevertheless, this would cause the loss of all the TCP connections that were established to the first IP address. Thus, Mobile

[3]IP Multicast is an IP address that identifies a group of stations. A multicast communication is from one to many.

IP was proposed as a solution to this problem assuring that a node can keep its communication with the other nodes even after the modification of the connection point of the link layer with the internet without modifying its IP address. The mobile IP work through tunnels[4], being considered, for this reason, another patch in IP. In Mobile IP, a mobile node has two addresses, its origin address (home address) and a dynamic address obtained in the network it is visiting (care-of-address – CoA). Besides that, there are types of routers with special functions, the Home Agent – HA and the Foreign Agent – FA. When a mobile station leaves its original network, the HA intercepts the packets sent to the mobile, and sends them to the network the mobile is visiting, adding a new header to the original packet, with the care-of-address. The FA is responsible to maintain the list of the CoA given to visiting nodes.

All these changes were largely due to the increase of the number of users in the network and the diversity of the applications. In fact, such growth is due to another "patch", the creation of the World Wide Web, which brought big changes to the network concerning the utilized applications and the type of user. In fact, in the 90's , with the commercialization of the network, the public was no longer composed of researchers, with specific technical knowledge about the network, and started to expand to every kind of public. Besides that, the usage of the network was no longer just file transfer, remote logon and messages exchange and started to be in its majority Web traffic.

Other interesting "patches" were mechanisms like Int-serv [23] and the Diff-serv [24] to ensure quality of service. Besides, caches were introduced in the interior of the network to reduce the amount of traffic and delay, which goes against the end-to-end principle of the network. The firewalls also present a change that goes against the transparency principle, because the packets that enter the network will not necessarily be transmitted to their final destination [25]. Therefore, the development of the Internet entailed changes in its original project so that the new requirements that appeared would be met. Even significant proposals, like Ipv6, experience difficulties to be deployed due to the "ossification" of the network core. One of the reasons is the need of modification in every AS interconnected to the network and the need of keeping the service robust to fails. First, there is no simple way to impose big structural changes to every AS, since the administrations are

[4]In Mobile IP, a mobile node has two addresses, its origin address (home address) and a dynamic address obtained in the network it is visiting (care-of-address – CoA). Besides that, there are types of routers with special functions, the Home Agent – HA and the Foreign Agent – FA. When a mobile station leaves its original network, the HA intercepts the packets sent to the mobile, and sends them to the network the mobile is visiting, adding a new header to the original packet, with the care-of-address. The FA is responsible to maintain the list of the CoA given to visiting nodes.

autonomoes. This implies that changes incompatible to previous versions suffers re4sistency to be deployed because of the required homogeneity in the network during the transition to the new service. Besides, the service providers are not willing to implement new services that are not guaranteed to be robust and safe, being able to cripple the network service, even temporarily. Then, new demands arise, showing that the "patched" architecture has unsatisfactory performance to some applications.

Chapter 3

Current Architectural Issues and Future Challenges

The patches in the architecture of the Internet show that the initial project no longer fits the current needs in the network. Moreover, the current architecture of the Internet already shows many unsolved problems, preventing the fulfillment of the requirements of new applications and services. Following, are shown the main problems of the current architecture of the Internet and the requirements to the development of a new architecture to the Internet.

3.1 Addressing

IP addressing has a series of structural principles that are in disagreement with current requirements and, consequently, addressing is one of the main challenges to the Internet of the Future. The shortage and the semantic overload of IP addresses, which accumulate localization and identification functions, are the two main problems.

The problem of the address shortage had its origin with the significant increase of the number of users in the network, incompatible with a 32 bits address. With 32 bits it is possible to address about 4 billion stations, and almost this entire total has been already allocated [26].

The IPv6 is proposed as a solution, by increasing the size of the address from 32 bits to 128 bits, which would solve the lack of addresses. Nevertheless, the non interoperability between Ipv4 and Ipv6 and the difficulty of convincing ASes, that are autonomous and do not risk implementing changes that would not bring immediate financial return, to invest in Ipv6, have hindered its implementation, in global scale, for more than 10 years. Other

adopted solutions to reduce address shortage are the dynamic allocation of addresses, with mechanisms like the Dynamic Host Configuration Protocol (DHCP), and the introduction of the Network Address Translation (NAT). NAT allows multiple devices access to the network using a single valid Internet address. This technique, however, is in opposite direction to two fundamental principles of the Internet Architecture, because the addresses in no more global and also an intermediary element, called middleboxe, is now mandatory between the communicating extremities, breaking the end-to-end principle. With NAT, the intermediary elements have the destination IP without being actually the extremities of the communication, violating the IP semantics. NAT severely restricts types of end-to-end communication that can be used in the Internet, requiring inspection and modification of higher layers protocols for applications to work properly [27, 28].

Besides the shortage of addresses, IP also implies other structural challenges on the Internet, like the naming of entities. One of the main problems related to the IP addressing is that the current semantic overloads the address as identifier and localizer of a node, indicating the point in which a node is connected to the network [29]. Due to this overload, the support to mobile nodes has become a challenge to the internet. Another point related to the overload of the IP semantics is the naming of the service or information identities. The Internet has only two global naming spaces, the IP addresses and the names in the DNS, which have a series of abstractions that allowed the success of the current Internet. Those global name spaces, however, also have many disadvantages created by the need of overloading their semantic and extending their functionality [30]. Both the IP addresses and the DNS names are linked to pre-existing structures, then being the administrative domains and the network topology, respectively. Due to this rigidity, the usage of DNS and IP to name the services and information implies faults like the association of the service or information in the machine were they reside instead of being associated to some denomination of their own. The main consequence of this is that changing a service from a machine may imply that the service name is not valid anymore. The use of Dynamic DNS can solve this problem inside a domain. Nevertheless, the exchange of domain of a service that uses DNS also implies the invalidation of the name. Thus, there is challenges to the replication of data in the and services in the network, because the names, instead of identifying just the service, identify the place and domain associated.

The naming and addressing scheme used on the Internet also causes security problems. On one hand, there is no obligatory authentication mechanism. One station can impersonate another by stealing its IP address. Moreover, the lack of authentication for the systems and for the datagrams allows

attacks such as denial of service on the network. On the other hand, besides the need for authentication, a consistent anonymity mechanism is also necessary. While the authentication protects the network, it is also necessary to protect the user privacy. One must avoid the possibility of gathering information that allows to profile a person through its network usage and using it to undesirable ends, for example, making directed propaganda. In vehicular networks applications, the release of information about the user could allow an attacker to track its position.

The definition of new premises to the identification and localization systems and the creation of an addressing space consistent with the needs of the network are requirements to the Internet of the Future.

It is worth mentioning that changes in addressing scheme would imply a different routing system, based in regions where addresses are valid inside each region. If the addresses are not global, there is the need of them to be distinguishable, at least in the context of the application. Besides, there are also proposals for systems in which the identification of users and devices is independent of the premises of packet forwarding.

3.2 Mobility

In the next years, a larger variety of Internet services is expected. The expectations are for increasing access from wireless devices due to the need for mobility. Indeed, the cellphones integration with the Internet raises expectations that the number of mobile devices connected to the network overcomes the number of fixed devices [31]. Therefore, the type of communication established in the Internet original project, based on the end-to-end principle, with point-to-point connections and immediate delivery, no longer addresses well the current network requirements.

The main question concerning mobility is the handovers, namely the mobile nodes transition between access points without loosing their active connections. The current IP addressing structure for the Internet not only identifies the end-point but also its location, overloading the IP address semantics. Hence, the connection fails when the destination IP address is modified by mobility, which brings change of location, and in consequence the change of IP address. Such change of IP address occurs, for example, in a wireless network when a mobile station changes access point. The transport layer should be able to exchange data between end-points without the need of information regarding the node location or the network topology [27].

Solutions that consider maintaining the IP during handovers to avoid interruptions in the connection would imply in an address hierarchy break.

Changing access points without changing IP would require the route for the node to be announced without aggregation. The absence of aggregation, in an environment where the routing-table size is already a concern, is not scalable. Hence, the Internet of today faces a great challenge on how to allow the nodes to move between access points without loosing their active connections.

Other problem related to TCP and mobility is the impact of high variability in the wireless link on TCP's congestion control mechanism. In wireless networks, the throughput in TCP is not optimal due the sender inability to find out the precise reason for packages loss. TCP assumes that losses are always caused by network congestion, reducing the congestion window every time a loss is detected. In wireless links, however, causes for the losses vary between link breaks due to mobility, transmission errors in wireless channel, and collisions in an attempt to access environment [32]. Thus, the congestion window ends up being inappropriately reduced as it would in a traffic jam. Therefore, errors caused by mobility, transmission and collisions require retransmissions attempts as soon as possible and, when interpreted as congestion, the retransmission attempts turn out to be incorrectly postponed. The result is a slow adjustment to load changes in links and a underutilization of the available bandwidth [6].

Another challenge related to mobility is the emergence of new mobile networks that need to deal with frequent delays and disconnections, called Delay and Disruption Tolerant Networks (DTNs) [10]. Examples of DTN networks are mobile sensor networks, underwater networks, interplanetary networking and rural networks. In these networks, there is no way to guarantee connectivity between all network nodes at a given time, which is incompatible with the IP principle of immediate delivery. Many data exchanges can only be performed if there is a tolerance with the existence of an end-to-end path in a time window. Hence, the use of TCP to establish connections does not apply to these networks, as an end-to-end path may not exist until the TCP connection timer expires. In fact, DTNs require the use of persistent storage mechanisms, through the network nodes, for the data during routing, besides the development of new forms of routing. Therefore, the TCP and the principle of immediate delivery are presented as problems for these next generation networks.

For the above mentioned reasons, the presence of mobility in new scenarios, such as mobile wireless networks, sensor networks and Delay and Disruption Tolerant Networks (DTNs) among others, presents itself as a key challenge for the Internet of the Future. In order to fully integrate these new technologies, the network must support highly variable features within short periods of time, or even extremely long propagation delays. In addition, we

need a restructuring of the characteristics of the network and transport layers in order to provide the services in mobile nodes.

3.3 Security

Users, service providers, industry, and application developers have been expressing increasing concern on safety aspects. The serious security threats that proliferate on the Internet can no longer be ignored, as the spread of viruses and Trojan horses, the denial of service [33] and the spams sending [34]. Future prospects in the war of defense systems against attackers are daunting. The forms of attack are becoming increasingly sophisticated and adaptable to improvements in defense systems, leading us to believe that this war won't end anytime soon. Nevertheless, the current Internet architecture doesn't provide a mechanism that limits the behavior of malicious end-stations and protect the non-malicious stations. By the time first attacks appeared on the Internet, advocates of the end-to-end paradigm said that security issues should be dealt with by the end-stations. Nevertheless, the dramatic growth of Distributed Denial-of-Service (DDoS) attacks indicate that minimalsecurity mechanisms should be provided by the network core. In addition, the current architecture doesn't provide any protection against attacks on their own network elements.

A major cause for all the current security problems is the lack of security in the design of the network architecture. As the network was initially used only by trusted users who had technical knowledge, there was no need to create mechanisms that protect the infrastructure or the network users. With the Internet commercialization, thousands of users started joining the network, bringing numerous threats. Malicious users aren't the only ones that cause problems, so do users who don't have enough technical knowledge to keep their machines updated and free of threats. In such cases, it's possible to use a non-malicious user's machine as a bot to perform distributed denial of service attacks or make it a viruses and other malwares spreader. Thus, the architecture that once provided a safe and reliable service now shows itself fragile and unable to provide robustness to the basic needs. The premise of an unalterable network core hinders the widespread implementation of security mechanisms [35].

The Internet security problems are not only restricted to the user's vulnerability, they also address to the security of network infrastructure. Currently, routing protocols don't use strong security premises, as well as authentication and monitoring systems are very far from what is needed in terms of delays, scalability, among others. As an example, there is the secure version of BGP,

which proposes the use of a shared secret key between each pair of neighboring routers. Although this measure restricts the sources that can route traffic, it doesn't protect the semantics of exchanged information and, as a consequence, don't prevent a malicious router to send false information [36]. Beyond this vulnerability in the routing level, TCP also shows vulnerabilities that could be used by malicious nodes to cause denial of service. There is a lack of security mechanisms in all network architecture layers.

One of the major architectural flaws on the Internet security is the absence of accountability mechanisms [37]. Accountability can be defined as the acknowledgment of the responsible entity for an action taken, which implies the need for correct correlation between actions and their sources. With accountability, you can punish or reward entities in accordance with the actions taken [38]. The Internet fails on accountability in basic principles, such as the source verification in a communication between two nodes, allowing problems such as IP spoofing, which creates difficulties to legally punish malicious users. Additionally, the use of IP as identification also hinders accountability in situations where NAT or mobile stations are used.

Another problem associated with malicious Internet traffic is the consumption of available bandwidth by unwanted data. This problem has been widely discussed for problems like spams and denial of service, but no effective solution has been found. The use of firewalls only prevents the arrival of unwanted traffic on the client but is unable to protect the network, showing the lack of mechanisms capable of filtering closer to the traffic sources. This type of filtering, combined with a global authentication system and with little cost, could bring great benefits to the Internet. To date, however, these systems only show up as great challenges.

Due to many problems associated with the current Internet architecture, many argue towards the need of creating a security architecture for the Internet. There is a consensus in which safety should be observed in all layers in order to obtain a safe environment, but the proposals toward security are still partial, not dealing with all problems jointly.

Thus we can identify new requirements for the new Internet, such as handling denial of service attacks, an efficient authentication of users and devices, creating a reliable system that modulates the level of transparency of the service provided by the network layer according to user preferences as well as the creation of an accountability system within the network.

3.4 Network Reliability and Service Availability

Service providers (Internet Service Providers - ISPs) are challenged to offer a network service that is reliable, robust and always available. The current network infrastructure, however, doesn't have the same reliability of the telephone network, which offers availability in the order of three nines, or 99.9%, and aims to reach more than five nine[1] through redundancies and high reliability equipment.

The Internet was designed to have service availability greater than the telephone network, due to the design decision to create a network with a lot of redundant paths between nodes, so that the failure of a link would not harm the entire network. The telephone network, which uses circuit switching, just physically connects source to destination, while in the Internet, which uses packet switching, nodes are devices that process and store information. Therefore, the complexity of the core and the services provided at the ends of the Internet is much larger than the telephone network, resulting in a lower availability. The frequent attacks on the many services and countless software failures considerably reduced the confidence of Internet users. Labovitz et al. measured the robustness of the Internet, to find out that only 35% of routes are available more than 99.9% of the time. A Gartner report estimates that the downtime of network services due to user and system error reaches 40% [39].

A service that is affected in a special way by this lack of trust is the IP telephony. With the advent of Voice over IP (VoIP), many believed that this would replace the conventional telephone service. Emergency services like police, fire and hospitals can't be based on a system with low reliability. In addition, many companies prefer to bear the cost of traditional telephony to have a reliable service. Another important issue is that many problems in the current Internet are detected due to user's notification of failure to administrators. The replacement of traditional telephony by VoIP service would interfere in this communication, further delaying the recovery of services and decreasing the availability of the network. This demonstrates the need for an architecture that is able to deal more efficiently with errors and that simplifies tasks to users, since the profile of people accessing the network has changed.

[1]It is worth mentioning that availability is measured with respect to time of operation without system failures. Availability of five nines means that in one year the system wasn't available for only about five minutes and fifteen seconds.

3.5 Debugging and Network Management

Currently, the Internet lacks diagnostic tools that allow the identification of sources of malfunction. Management is still a great challenge due to the fact that the Internet is managed in a distributed way and with intelligence only in the extremities and the absence of mechanisms to identify which network resources are being used by each application. As the network grows, the need for improvement or replacement in the network management systems to reduce delays and maintenance costs becomes more and more apparent.

The standard protocol for management of the Internet is the Simple Network Management Protocol (SNMP), created in the 80 decade and supported by most network equipment. SNMP works on an information model in which the data necessary for management is placed into modules called Management Information Base (MIB) by the equipment being managed. Although SNMP is widely known and used, its use is still restricted primarily to the monitoring of network devices, leaving open the problem of managing applications or servers. Even for network devices, SNMP has a limited application because it does not have a significant action in the area of configuration management. The network environment has changed considerably since the creation of SNMP, so that their features are insufficient to meet current needs. Given current technology, network devices could perform more complex management operations with a lower cost. Moreover, it is expected that routers and switches become increasingly programmable, making it possible to run more control functions directly from these devices [40].

Commercial aspects should also be considered when analyzing the management on the Internet. First, SNMP has a bad image with network administrators, who consider it unsafe, complex, slow and with limited functionality. In addition, the open management systems market is very limited, not bringing options to attract administrators. Thus, proprietary tools end up being used to manage individual devices, while the problem of managing complex networks remains open. The development of better management tools by companies often does not occur because management prime sector in equipment sales companies, so that the most experienced professionals tend to leave this sector to occupy more attractive functions for the company. In addition, the standards bodies tend to be very slow, in a way that the standards are published only after the creation of a management solution the company.

In addition to the management system, the Internet lacks effective control systems. This problem becomes more evident in next generation networks, which consist of devices such as sensors, cell phones and PDAs, where the energy should be saved. In such cases, distributed control mechanisms should

be designed in a way to conserve device battery level. Thus, the creation of a control plane that is able to optimize the operation of the network automatically and without overloading the connected devices is a major challenge.

In error diagnosis area, the user's view should also be emphasized. Once the profile of the majority of Internet users are people who have no technical knowledge, the lack of mechanisms for diagnosing and correcting network errors causes great discontent. In fact, most users can not distinguish when the error occurs on their own machine or on the network itself. Often, the errors could be identified and corrected in a simple and automatic way, but the absence of a structure in the Internet architecture that favors this type of service makes it impossible to create this kind of tool. Because of these restrictions in the field of management and error diagnosis, it is believed that the new Internet architecture must provide mechanisms that allow autoconfiguration of the political and administrative constraints based network. Thus, autonomy must be an important concept in the Future Internet. Research groups have put the existence of an intelligent control plan as a requirement for an increasingly complex network that must satisfy the non-technical users. Moreover, it is suggested to generalize the concept of routing domain to the notion of "region" [6] in order to express different interconnection policies, trust relationships, multiplexing mechanisms, etc.. The new concept of "region" could include a mapping between the boundaries in order to support different addressing schemes.

3.6 Quality of Service - QoS

The growing demand for voice and video transmission and entertainment applications, such as online gaming, makes clear the need to implement mechanisms that improve the quality of these services. However, the architecture of the Internet and its patches created various restrictions on the deployment of these solutions.

First, the current Internet architecture is based on the end-to-end principle. Therefore, the inclusion of equipment within the network to support quality of service goes against the initial design of the network which doesn't support a global implementation of this type of device. In addition, packet forwarding is based on the principle of "best effort", which means that any mechanism for bandwidth reservation or change of priority of packages also interfere in the operation established by the network project.

Despite these restrictions, the provision of quality of service is attractive to Internet Service Providers (ISPs), as it is a way to differentiate their service, which directly influences the fees charging and profits. To ensure quality

of service, it's necessary to guarantee bandwidth and delay characteristics in all the way from the content source to the receiver [41]. Nevertheless, due to the choice of a distributed management by dividing the network into autonomous systems, it's not enough that each ISP implements solutions to provide quality of service individually. There must be an agreement between all the ISPs from source to destination in order to provide the service with QoS. In addition, due to ossification of the network, global changes in the network core are extremely slow. Thus, although the issue of quality of service has been widely studied by the scientific community, it is unclear how and where to integrate different levels of QoS in the current network architecture [11].

3.7 Scalability

Due to exponential rising of number of station connected to Internet, some current architecture components have scalability troubles. An example is the routing system ,which has trouble with the frequent increasing and updating of routing tables [42]. Moreover, several applications have suffered the effects of increasing the number of users, such as the multimedia applications.

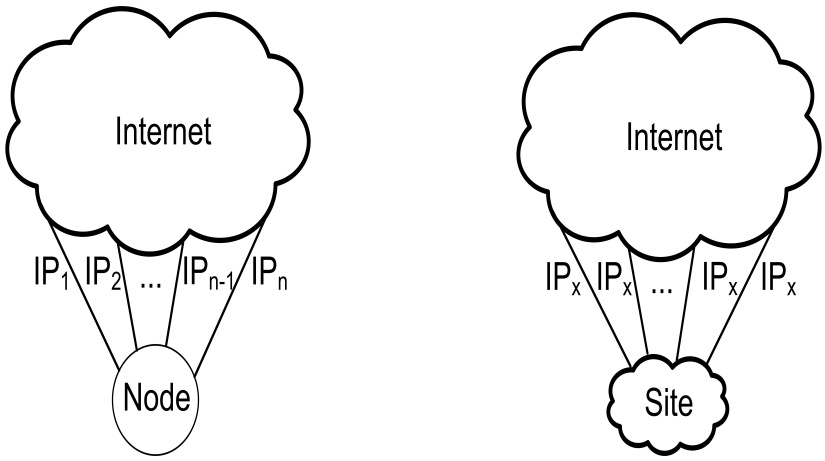
Video distribution is one of the most successful applications on the Internet. Sites that offers sharing and distribution services on demand are accessed by millions of users. Only the YouTube, the most famous of this kind of site, is accessed by about 20 million of users daily. The scalability and guarantee of quality of service requirements are the biggest challenges in the video distribution. Nowadays, the applications provide videos at about hundreds of kilobits per seconds and the number of simultaneous users is at about hundreds of thousands. In that way, the bandwidth resources required for a service provider are at about hundred of gigabits per second, considering use the client-server model. In the client-server model, more users and more video quality imply to higher costs of providers, so this model is inappropriate to the video distribution on the Internet [43]. Therefore, the utilization of middle boxes and peer-to-peer networks for improving the efficiency of new generation applications, as the video distribution in large-scale, is a requirement to the Future Internet.

Other problem related to scalability is the routing, due to increase in routing tables. This increase occurs because of the growth in the number of users and the practice of multi homing [44]. There are two basic perspectives for understand the multi-homing concept: the multi-homing host is the multi-homing site. In the multi-homing host, one station has several interfaces and each one can have one or more IP address. These IP addresses may all belong

to the same sub-net or they may have different prefixes. The multi-homing site aim to increase the availability of companies sites through the use of several ISPs [45]. In this case, the company advertises the same IP address or the same range of IP addresses on all outgoing connections, so that if the link of one of ISPs falls, the connectivity is not lost. Another use is the load balancing between the several ISPs. The configurations obtained using the multi-homing may be noted in the Figure 3.1.

The use of multi-homing affects the routing-table scalability due to the destruction of addresses aggregation by prefix based on the topology. Moreover, with this technique, the user may split his prefix in several more specific prefixes, further increasing the number of inputs in the tables.

Beyond the problems caused by multi-homing site, each interface of a node is seen as a totally different node when the multi-homing host is utilized. It implies more entries in the routing table to reach a single node, which makes both the routing and the mobility mechanism inefficient. This demonstrate that the problem of routing is implicitly linked to the problem of IP address semantics overload [46].



(a) *Host multi-homing*: single station with n interfaces that have different IPs in each interface.

(b) *Site multi-homing*: a site advertising the same IP to all output connections.

Figure 3.1: *Multi-homing* examples.

Therefore, the Internet have to deal with the challenge of keeping scalable the global routing system, even with the growth of the addressing space, the allocation of addresses independently of providers (site multi-homing) and the demand of load balancing [47].

Other scalability issues are related to new generation network. One such

case is ad hoc networks, which don't supports a large number of nodes due to using flat routing based in inundations. In the same way, the vehicular networks require authentication systems that work with a big number of users. It should be noted that the Future Internet must also support the scalable solutions to this type of networks.

3.8 Economic Model and Innovation Freedom

Besides technical issues, there is still the problem of the economic model of the Internet. The challenge is to allow network and service operators to be paid to ensure continued investments in infrastructure and new technologies. Network services, however, are provided end-to-end and the Internet is divided into autonomous systems, which means that no ISP has complete control over the connections of its clients [41]. Thus, the Internet was built in a way that difficulties service differentiation by ISPs, which sells to its clients only basic services such as e-mail in addition to providing bandwidth. The role of ISP is simply to forward packets, which makes its service a commodity. Without ways to differentiate service and with the competition from others ISPs, the service price ends up falling, inhibiting or difficulting investments in infrastructure and innovation [6].

One way to increase profit of ISPs is the insertion of middleboxes in the network to provide services to clients. Theses middleboxes can provide services such as caching, security, quality of service, and others. Middleboxes, however, damage the principle of end-to-end connection, besides the assumption of intelligence only at the edges. Other alternative to the ISPs is to analyze client's traffic so as to obtain information that could help to reduce costs or allow limitations on large volume traffic, such as the traffic generated by peer-to-peer (P2P) applications. This traffic analysis, though, constitutes a violation of user privacy. Due to these matters, the Future Internet architecture needs to offer ways to differentiate services to ISPs, without implying in architectural issues in the network core.

Another point that concerns the economic model and the innovation freedom is the treatment of conflicts in the network. The Internet is composed of entities with conflicting roles and interests: the users, that wants to exchange data and interact through the Internet; the ISP, that want to obtain profit from Internet services; the government, that want to apply the law, protect consumers, regulate the market, etc.; companies holding copyrights, that want to protect their content; content providers that look for profit,

and others [2]. The conflict type that may be happen is the one between parties with common interests trying to operate in the presence of a third, hostile or opposing, part. An example is the users' necessity of privacy, with the necessity of government supervision. The second conflict type happens when parts that want to communicate, but need a third part to solve some conflicting interest. As examples, there are the use of antivirus in e-mail systems to ensure secure communication between two users, or the utilization of certification authorities on the Internet. The third conflict type happens when several parts want to participate in an application, but they all want some other part to be excluded. The more typical example are e-mail users and spammers [6]. The interest conflicts can define strategies in the economic model of the Internet, apart from inserting several obstacles for innovation freedom.

In order to improve the economic model of the Internet, two main requirements are being raised: the use of a highly adaptable architecture and the separation of functions of service and infrastructure provision by ISPs.

It is argued that the new architecture design must predict actions that explicitly preserve the ability to change and evolve the network technologies [6]. The virtualization technique meets these requirements and, therefore, its use in the new architecture development has been widely defended by several research projects about Future Internet [48]. This decision, however, can result in reduced performance and efficiency. Thus, the challenge is to maintain generality and evolution capacity of the network and, in the same time, minimize implantation and maintenance costs.

The separation of current ISPs roles aims to providing a service through of whole path between source and destination. Today the ISPs are responsible for two tasks: network infrastructure management and the service providing to the end users. It is argued that the aggregation of these two functions by a single entity is one of the main causes of slow deployment of new protocols to the Internet [41]. Feamster et al. defend that the role separation could offer bigger innovation freedom to the service providers, enabling a faster evolution of the Internet protocols.

Chapter 4

Conclusion

In this document we perform service requirement analysis and a case study of the current Internet. It became evident that many design principles and requirements used in its early deployment were still present in the current internet, which combined with a "patch-based" maintenance, leads to a crescent "ossification" of early internet designs, making difficult major modifications on the network core.

Investigating the Internet's current features and functionalities, we were able to determine major causes for its success, such as the IP universality, simple network core and the minimal dependency of communication. In this process also became evident major architectural problems and flaws, such as mobility issues caused by IP's geographical hierarchy, difficulty of providing quality of service and security concerns, which weren't priority in the original design. The virtualization techniques meet many of these requirements, and its use in the new Internet design is defended by many research projects in the area.

Thus, this study promotes the need of a new Internet and, based on errors and successes from the past, points towards an ideal architectural design.

Bibliography

[1] *Internet no Brasil 2008 (dados e fontes)*, Accessed on November 2011. http://www.avellareduarte.com.br/projeto/conceituacao/conceituacao1/conceituacao14_internetBrasil2009.htm.

[2] D. D. Clark, J. Wroclawski, K. R. Sollins, and R. Braden, "Tussle in cyberspace: defining tomorrow's Internet," *IEEE/ACM Transactions on Networking*, vol. 13, no. 3, pp. 462–475, June 2005.

[3] V. Cerf and R. Kahn, "A protocol for packet network intercommunication," *IEEE Transactions on Communications*, vol. 22, no. 5, pp. 637–648, May 1974.

[4] V. Cerf, Y. Dalal, and C. Sunshine, *Specification of Internet Transmission Control Program*. RFC 675, Dec. 1974.

[5] D. D. Clark, C. Partridge, J. C. Ramming, and J. T. Wroclawski, "A knowledge plane for the Internet," in *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications (SIGCOMM '03)*, (New York, NY, USA), pp. 3–10, ACM, 2003.

[6] D. Clark, R. Braden, K. Sollins, J. Wroclawski, D. Katabi, J. Kulik, X. Yang, T. Faber, A. Falk, V. Pingali, M. Handley, and N. Chiappa, "New Arch: Future generation Internet architecture," tech. rep., USC Information Sciences Institute Computer Networks Division, MIT Laboratory for Computer Science and International Computer Science Institute (ICSI), Aug. 2004.

[7] P. Baran, "On distributed communications networks," *IEEE transactions on Communications Systems*, vol. 12, no. 1, no. 1, pp. 1–9, 1964.

[8] S. Shenker, "Fundamental design issues for the future Internet," *IEEE Journal on Selected Areas in Communications*, vol. 13, no. 7, pp. 1176–1188, Sept. 1995.

[9] M. S. Blumenthal and D. D. Clark, "Rethinking the design of the Internet: the end-to-end arguments vs. the brave new world," *ACM Transactions on Internet Technology*, vol. 1, no. 1, pp. 70–109, Aug. 2001.

[10] C. T. Oliveira, R. B. Braga, D. M. Taveira, N. C. Fernandes, and O. C. M. B. Duarte, "A predicted-contact routing scheme for brazilian rural networks," in *IFIP Wireless Days Conference*, (Dubai, United Arab Emirates), Nov. 2008.

[11] A. Feldmann, "Internet clean-slate design: what and why?," *ACM SIGCOMM Computer Communication Review*, vol. 37, no. 3, pp. 59–64, July 2007.

[12] Y. Rekhter, T. Li, and S. Hares, *A border gateway protocol 4 (BGP-4)*. RFC 4271, Jan. 2006.

[13] D. Clark, L. Chapin, V. Cerf, R. Braden, and R. Hobby, *Towards the Future Internet Architecture*. RFC 1287, Dec. 1991.

[14] V. Fuller, T. Li, and K. Varadhan, *Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy*. RFC 1519, Sept. 1993.

[15] J. Mogul and J. Postel, *Internet Standard Subnetting Procedure*. RFC 950, Aug. 1985.

[16] C. Huitema, *Routing in the Internet*. Prentice Hall PTR, 2 ed., 1999.

[17] V. Jacobson, "Congestion avoidance and control," in *Symposium proceedings on Communications architectures and protocols (SIGCOMM '88)*, (New York, NY, USA), pp. 314–329, ACM, 1988.

[18] S. Deering, *Host extensions for IP multicasting*. RFC 1112, Aug. 1989.

[19] S. Deering, *Internet Protocol, Version 6 (IPv6) Specification*. RFC 2460, Dec. 1998.

[20] K. Egevang and P. Francis, *The IP Network Address Translator (NAT)*. RFC 1631, May 1994.

[21] S. Kent, *Security Architecture for the Internet Protocol*. RFC 2401, Nov. 1998.

[22] C. Perkins, *IP Mobility Support for IPv4*. RFC 3220, Jan. 2002.

[23] R. Braden, D. Clark, and S. Shenker, *Integrated Services in the Internet Architecture*. RFC 1633, 1994.

[24] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, *An Architecture for Differentiated Services*. RFC 2475, Dec. 1998.

[25] R. Braden, D. Clark, S. Shenker, and J. Wroclawski, "Developing a next-generation Internet architecture," tech. rep., USC Information Sciences Institute Computer Networks Division, MIT Laboratory for Computer Science and International Computer Science Institute (ICSI), July 2000.

[26] *The IPv4 Report*, Accessed on November 2011. http://www.potaroo.net/tools/ipv4/.

[27] H. Balakrishnan, K. Lakshminarayanan, S. Ratnasamy, S. Shenker, I. Stoica, and M. Walfish, "A layered naming architecture for the Internet," in *Proceedings of ACM SIGCOMM Conference 2004*, pp. 343–352, Aug. 2004.

[28] B. Ahlgren, J. Arkko, L. Eggert, and J. Rajahalme, "A node identity internetworking architecture," in *25th IEEE International Conference on Computer Communications (INFOCOM 2006)*, pp. 1–6, Apr. 2006.

[29] N. Niebert, S. Baucke, I. El-Khayat, M. Johnsson, B. Ohlman, H. Abramowicz, K. Wuenstel, H. Woesner, J. Quittek, and L. M. Correia, "The way 4ward to the creation of a future Internet," in *IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2008)*, pp. 1–5, 2008.

[30] R. Moskowitz and P. Nikander, *Host Identity Protocol (HIP) Architecture*. RFC 4423, May 2006.

[31] S. Paul, R. Yates, D. Raychaudhuri, and J. Kurose, "The cache-and-forward network architecture for efficient mobile content delivery services in the future Internet," in *First ITU-T Kaleidoscope Academic Conference Innovations in NGN: Future Network and Services (K-INGN 2008*, pp. 367–374, May 2008.

[32] G. Holland and N. Vaidya, "Analysis of tcp performance over mobile ad hoc networks," *Wirel. Netw.*, vol. 8, no. 2/3, no. 2/3, pp. 275–288, 2002.

[33] R. P. Laufer, I. M. Moraes, P. B. Velloso, M. D. D. Bicudo, M. E. M. Campista, D. de O. Cunha, L. H. M. K. Costa, and O. C. M. B. Duarte, "Negação de serviço: Ataques e contramedidas," in *Minicursos do V*

Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais - SBSeg'2005, pp. 1–63, Sept. 2005.

[34] D. M. Taveira, I. M. Moraes, M. G. Rubinstein, and O. C. M. B. Duarte, "Técnicas de defesa contra spam," in *Minicursos do Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais - SBSeg'2006*, pp. 202–250, Aug. 2006.

[35] S. Bellovin, D. Clark, A. Perrig, and D. Song, "A clean-slate design for the next-generation secure Internet.," tech. rep., Pittsburgh, PA: Report for NSF Global Environment for Network Innovations (GENI) workshop, July 2005.

[36] R. Singel, *Pakistan's Accidental YouTube Re-Routing Exposes Trust Flaw in Net.* http://blog.wired.com/27bstroke6/2008/02/pakistans-accid.html, Accessed on November 2011.

[37] D. G. Andersen, H. Balakrishnan, N. Feamster, T. Koponen, D. Moon, and S. Shenker, "Accountable Internet protocol (AIP)," in *Proceedings of the ACM SIGCOMM 2008 conference on Data communication (SIGCOMM '08)*, (New York, NY, USA), pp. 339–350, ACM, 2008.

[38] J. Mirkovic and P. Reiher, "Building accountability into the future Internet," in *4th Workshop onSecure Network Protocols (NPSec 2008)*, pp. 45–51, Oct. 2008.

[39] Cisco Systems, Inc., "IP telephony: The five nines story," tech. rep., 2002.

[40] J. Schonwalder, A. Pras, and J.-P. Martin-Flatin, "On the future of Internet management technologies," *IEEE Communications Magazine*, vol. 41, no. 10, pp. 90–97, Oct. 2003.

[41] N. Feamster, L. Gao, and J. Rexford, "How to lease the Internet in your spare time," *ACM SIGCOMM Computer Communication Review*, vol. 37, no. 1, pp. 61–64, Jan. 2007.

[42] S. Buchegger and A. Feldmann, "ARCADIA - NeXtworking'07 workshop report," tech. rep., Deutsche Telekom Laboratories / TU Berlin, 2007.

[43] I. M. Moraes, M. E. M. Campista, M. D. D. Moreira, M. G. Rubinstein, L. H. M. K. Costa, and O. C. M. B. Duarte, "Distribuição de vídeo sobre redes par-a-par: Arquiteturas, mecanismos e desafios," in *Minicursos do Simpósio Brasileiro de Redes de Computadores - SBRC'2008*, pp. 115–171, May 2008.

[44] J. Abley, K. Lindqvist, E. Davies, B. Black, and V. Gill, *IPv4 Multihoming Practices and Limitations*. RFC 4116, July 2005.

[45] A. Mihailovic, G. Leijonhufvud, and T. Suihko, "Providing multihoming support in IP access networks," in *13th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, vol. 2, pp. 540–544, Sept. 2002.

[46] L. Loyola, P. Mendes, F. Romero, and M. Jimenez, "Multi-level distributed name resolution system based on flat identifiers," in *IEEE Global Telecommunications Conference (IEEE GLOBECOM 2008)*, pp. 1–6, Nov. 2008.

[47] D. Massey, L. Wang, B. Zhang, and L. Zhang, "A scalable routing system design for future Internet," in *SIGCOMM 2007 Workshop "IPv6 and the Future of the Internet"*, pp. 1–6, ACM, Aug. 2007.

[48] T. Anderson, L. Peterson, S. Shenker, and J. Turner, "Overcoming the Internet impasse through virtualization," *IEEE Computer*, vol. 38, no. 4, pp. 34–41, Apr. 2005.