Emerging Issues in Current Future Internet Design

Phuoc Tran-Gia, Tobias Hoßfeld, Michael Menth, Rastin Pries

Institute of Computer Science, University of Würzburg, Germany

Abstract – From its inception, the Internet was not intended as the worldwide universal communication platform. It developed over almost four decades to its current state. As a result of this unplanned evolution, we currently witness scalability problems, increased complexity, missing modularity as well as missing flexibility for emerging services. In this report we focus on two selected issues: i) the changing routing paradigm and ii) edge-based intelligence. We will then present a variety of projects on future Internet and finally assess recently established experimental facilities and their role in the Future Internet design.

Keywords – Next Generation Network, Future Internet routing, edge-based intelligence, experimental facilities

Neue Aspekte des Future Internet Designs

Ursprünglich war das Internet nicht als weltweite, universale Kommunikationsplattform geplant. Es hat sich vielmehr über vier Jahrzehnte zum aktuellen Stand entwickelt. Als Ergebnis dieser ungeplanten Entwicklung sind wir jetzt mit schlechter Skalierbarkeit, erhöhter Komplexität, fehlender Modularität und fehlender Flexibilität für zukünftige Dienste konfrontiert. In diesem Artikel behandeln wir zwei ausgewählte Aspekte bezüglich Forschung für das zukünftige Internet: i) skalierbareres Internet Routing und ii) intelligente Applikationen. Danach stellen wir eine Reihe von Future Internet Projekten vor und zeigen welche Rolle deren Experimentalplattformen für das Future Internet Design spielen.

Schlüsselwörter – NGN, Future Internet Routing, intelligente Applikationen, Experimentalplattformen

1. Introduction

Today’s Internet has a large economic influence but is based on legacy mechanisms and algorithms from the 70ies and 80ies. Routing tables are increasing fast and emerging applications have high demands for which the original Internet architecture was not designed for. Currently, several projects have been set up worldwide and are working on research towards the future Internet. These projects mainly focus on experimental-driven research, aiming to evaluate new architectures in large experimental facilities. In this paper, we present two selected aspects examined in the project G-Lab [http://www.german-lab.de].

The first issue describes how to face scalability problems of interdomain routing. The locator/identifier concept has been proposed to solve this problem at the expense of an indirection between identifiers and locators. The latter requires a powerful, reliable, and secure mapping system which is currently under study in G-Lab.

Along with the increasing number of Internet-capable devices, the bandwidth requirements of emerging applications increase. New services such as Video on Demand (VoD) or IPTV consume not only a large amount of bandwidth but also have high quality requirements. Currently, performance studies are conducted to get an insight how real-time applications react on the changing bandwidth conditions.

Finally, we present some projects in the area of future Internet design. We elaborate why experimental facilities are required and simulative or analytic approaches are not sufficient to get to the future Internet. This paper is organized as follows. Section 2 explains the scalability problem in Internet routing, the locator/identifier split as a potential solution to that problem, and an overview of mapping systems. Section 3 shows emerging paradigms of Internet applications. Besides different projects on future Internet, Section 4 is devoted to current future Internet testbed initiatives. Finally, some concluding remarks are given in Section 5.

2. Future Internet Routing

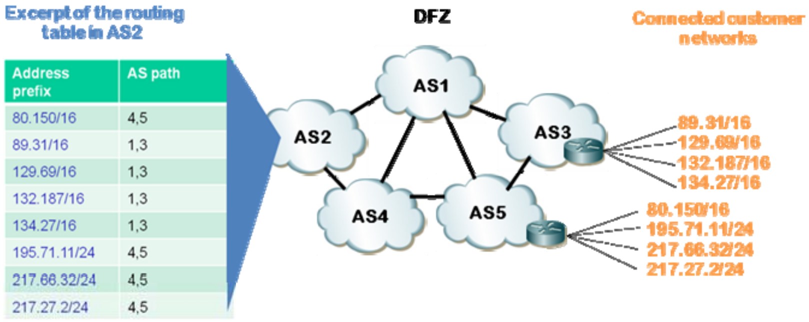
Today's routing in the Internet is not likely to scale in the future. The locator/identifier (Loc/ID) split is a potential solution to that problem, but it requires a mapping system to map identifiers to locators. Such mapping systems are currently developed in G-Lab.

The Internet's Scalability Problem

Currently, interdomain routing in the Internet does not scale well. The routing tables already keep 300,000 entries today and grow quickly. In addition, core routers are faced with a high border gateway protocol (BGP) update frequency. This problem is a main driver for many new future Internet routing proposals. We illustrate them and give some insights in this section.

The Problem. The Internet is an interconnection of multiple autonomous systems (AS) using IP as a common base to exchange messages. In general, destination-based forwarding is used in IP networks, i.e., routers look up the next hop for a packet in their forwarding information bases (FIBs) which are derived from their routing tables. The FIB entries consist of address prefixes and next hops. The longest prefix match for a destination address determines the interface over which the packet is transmitted. A default route can be provided that is taken when no matching prefix is found.

The composition of the routing table works differently for intra- and inter-domain routing. Each AS may use its own method to generate entries in the routing tables for intra-domain routing. Usually, they assign administrative costs to all links within the AS and forward the traffic along least-cost paths. This is mostly realized by distributed routing protocols like OSPF or IS-IS. For larger ASes, a subdivision of the network into several routing areas helps to manage the routing complexity and to keep intra-domain routing scalable.



Excerpt of the routing table in AS2

Address prefix	AS path
80.150/16	4,5
89.31/16	1,3
129.69/16	1,3
132.187/16	1,3
134.27/16	1,3
195.71.11/24	4,5
217.66.32/24	4,5
217.27.2/24	4,5

Figure 1: Reachability information about connected IP ranges exchanged in the Internet using BGP to construct distributed routing tables for inter-domain routing.

To exchange reachability information about address ranges in other ASes, inter-domain routing uses BGP. Each AS tells its neighbours which destination prefixes can be reached over its own network and also provides a list of ASes that need to be traversed on the path towards the destination AS. This principle is illustrated in Figure 1. Routers in edge networks usually have a small number of prefixes in their routing tables and packets to unknown destinations are forwarded to a default router. However, BGP routers in the core of the Internet do not have default routes. They constitute the so-called default-free zone (DFZ) of the Internet. The number of entries in the routing tables over time is illustrated in Figure 2. It is increasing at an alarming rate. To cope with larger routing tables, routers need to be more powerful in the future, but it is not clear whether the performance of future hardware will suffice. In any case, it will be more expensive. Furthermore, a system with that many entries cannot be expected to be stable over long time. Currently, 1 – 10 BGP updates per second are propagated through the global routing system and peak rates with up to 10,000 changes per second are observed. This yields to another problem since BGP speaking routers must be able to cope with these update frequencies in addition to packet forwarding.

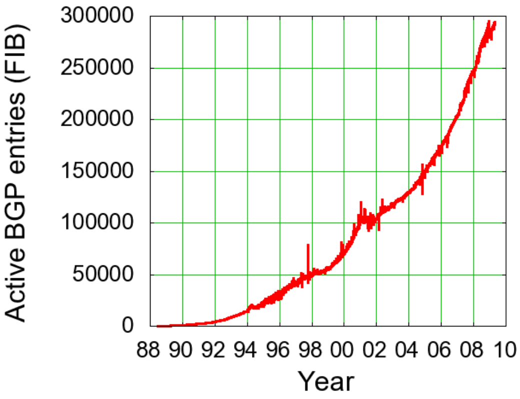


Figure 2: Growth of the routing tables in the DFZ.
[Source: http://bgp.potaroo.net/as2.0/]

When the Internet finally runs out of IPv4 addresses, the introduction of IPv6 eventually brings an almost unlimited number of IP addresses. This solves the problem of address depletion, but routing tables will grow even faster because the vast amount of available IPv6 addresses require even more prefixes to be announced in the DFZ.

Causes of the Problem. Experts discussed and analyzed the problem of increasing routing table sizes at the IAB Workshop on Routing and Addressing [1] and came to the following conclusions. The main causes for the current growth of the routing tables in the DFZ are the use of provider-independent addresses, multi-homing, traffic engineering for edge networks, and countermeasures against prefix hijacking. We explain some of these issues in more detail.

IP address space can belong to providers or to customers. In the first case, the addresses are called provider-aggregatable (PA). The Internet service provider (ISP) lends IP address subspace, i.e. IP prefixes, to customers for the duration of their contract, but the ISP stays the owner of the IP addresses. When the contract between the customer and the ISP is over, the ISP lends the IP prefixes to other customers. This has no impact on inter-domain routing because packets to these prefixes are still routed into the same AS. PA addresses limit the fragmentation of the address space, i.e., they preserve the aggregation of IP addresses such that short prefixes, i.e. large address blocks, continue to be announced through BGP. However, when a company using PA address space changes its ISP, all its devices must be renumbered to the address subspace of the new ISP. This is a time-consuming, error-prone, and expensive task. Therefore, companies prefer to obtain their own address space, i.e. so-called provider-independent (PI) addresses. They allow them to change providers without renumbering. For the global routing system, a provider change with PI addresses requires BGP updates to withdraw the path to the old ISP and announce the path to the new ISP in the Internet. In addition, the moved prefix was possibly aggregatable in the announced address space of the old ISP, but it is not aggregatable in the announced address space of the new ISP. As a result, a new entry is created in the interdomain routing tables. Furthermore, customers with PI addresses like to be connected to more than one ISP (multi-homing) to increase the reliability of their Internet connection or to perform traffic engineering. This introduces additional entries into the routing tables.

The Locator/Identifier Split

The locator/identifier (Loc/ID) split is expected to solve the problem of rapidly increasing routing tables. We explain it using the Locator Identifier Split Protocol (LISP) [2] as an example. However, there are many more proposals for more scalable Internet routing that implement the Loc/ID split idea. One of them is currently developed in G-Lab [12].

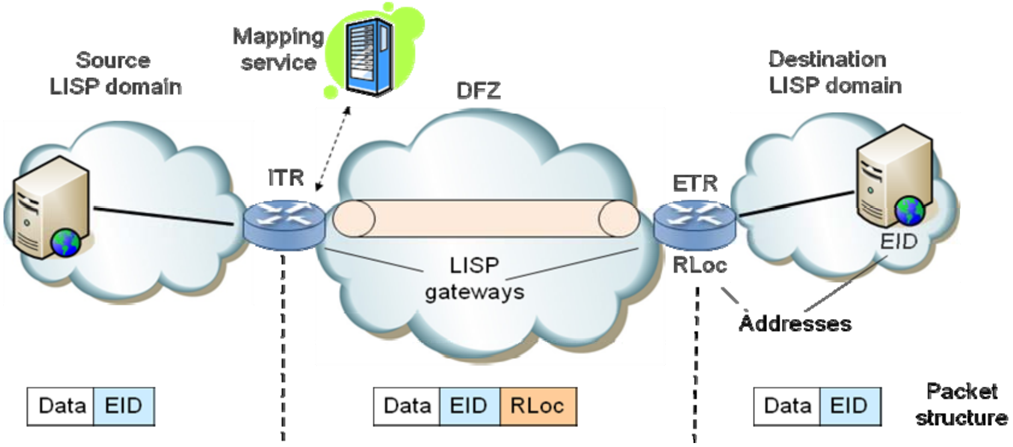


Figure 3: Data are tunneled between LISP gateways through the core of the Internet.

Basic Description of LISP. LISP is designed that it can be incrementally added into today's Internet and first prototypes are already running [3]. LISP domains are connected to the Internet by a border router that works as a LISP gateway. The IP addresses used within a LISP domain are called endpoint identifiers (EIDs). They are not announced via BGP to the global Internet. Thus, they are routable only within its LISP domain but not in the general Internet. Local traffic within LISP domains is carried like today. Traffic between LISP domains is carried over tunnels between their gateways. The ingress and egress of the tunnel are called ingress and egress tunnel router (ITR, ETR). The IP addresses of the ITR and ETR are called routing locators (RLocs). Outbound traffic is forwarded to an ITR of a LISP domain. The ITR queries a mapping service for the RLoc of the destination EID of an outbound packet, encapsulates it and sends it to the ETR with the corresponding RLoc which is shown in Figure 3. This operation is called "map and encaps". The packet is decapsulated by the ETR in the appropriate LISP domain and delivered to the destination LISP node using the locally routable EID. A disadvantage of this particular implementation of Loc/ID split is that the packet size increases under way through additional headers which may cause packet fragmentation on the way and lead to issues with maximum transfer units (MTUs). There are also other solutions without this property.

Interworking with the legacy Internet. Nodes in LISP domains with only locally routable identifiers also need to communicate with the legacy Internet. To that end, two basic interworking principles exist: one is based on network address translation (NAT) while the other is based on proxy gateways.

First, we present the NAT solution. When a LISP node establishes a connection with a node in the legacy Internet, the ITR does not find an RLoc for the destination node. Then, it substitutes the source address of the LISP node with one of its own addresses which has a global locator function and changes the source port if needed. This information is stored in a translation table. The destination node receives a packet and can treat it like a packet from any legacy node. Responses are just replied to the source address which is the ITR. The ITR substitutes the destination address and port of the response packet with the address and port of the LISP node that initiated the communication. Although NAT is complex, it is a well established technique and equipment outside LISP domains is not needed for interworking.

Another interworking method requires proxy gateways. Communication from a LISP node to the legacy Internet is rather trivial because the destination address is a conventional IP address which has global locator function. Communication from the Internet to a LISP node is more complex. Proxy gateways announce strongly aggregated address prefixes for EIDs in BGP so that if a legacy node sends a packet to a LISP node, the packet is forwarded to a proxy gateway. Anycast may be used for this purpose so that packets destined to the same EID prefix are forwarded to different proxy gateways depending on their location. When a proxy gateway receives a packet destined to a LISP node, it requests the corresponding RLoc from the mapping system and tunnels it to the appropriate ETR in the appropriate LISP domain. Also the interworking solution with proxy gateways has drawbacks. Figure 4 illustrates the communication pattern. The involvement of a proxy gateway leads to triangle

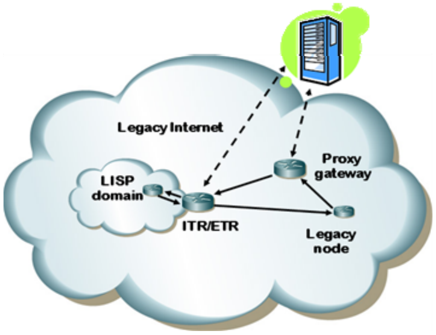


Figure 4: LISP interworking with proxy gateways.

routing, i.e. longer paths than today. In addition, extra equipment outside the LISP domain is required for interworking and the business model for the operation of proxy gateways is not clear. Announcement of EID prefixes into BGP is needed which again increases the routing table size if the announced EID address space is not highly aggregated.

Impact of Loc/ID Split on Core Routing. With Loc/ID Split, customer networks have their own address or identifier space which they can keep when changing ISPs. Therefore, renumbering of devices in the customer network is not needed, and the new ISP still does not need to announce new prefixes into BGP. In a similar way, multi-homing and traffic engineering can be supported without inflating the global routing tables and propagating BGP updates through the entire Internet.

Principles of Mapping Systems for Future Internet Routing

Most proposals for future Internet addressing and routing implement the Loc/ID split principle and require a mapping system. We present general and specific requirements for mapping systems, discuss the use of the mapping system as relay function, and review early approaches.

General Requirements. Mapping systems must support a high query load. Therefore, caching mapping information at the locations where the mappings are needed is indispensable. They must be able to support a large number of mapping entries and still respond fast. They need to be redundant and consistent to be robust against failures. Loc/ID split is another level of indirection for Internet communication. That raises new security issues. For example, means are required to validate the correctness of the mapping information and cache poisoning with wrong mapping information needs to be prohibited. Possible design rules are that foreign parties should not control mapping information or answer mapping queries. Moreover, mapping systems must introduce only little overhead to be efficient. When mapping information changes, this information should be propagated quickly to the mapping device, e.g. the ITRs in LISP. While information push leads to faster updates, pull models cause less signaling overhead. Apart from these issues, it is not clear which entity is authoritative for introducing the mapping information into the mapping system. Some proposals assume that ISPs need to announce to the mapping system that certain identifiers are reachable via a locator under their control. Others assume that the owners of the identifiers need to tell the mapping system over which locators they are reachable.

Requirements Depending on the Specific Routing Architecture. Depending on the routing paradigm, mapping systems must have additional features. In general, every identifier may have a different locator depending in which networks they currently are. However, some proposals live with the assumption that all identifiers of a common prefix must have the same locator. They take advantage of this limitation in the construction of the mapping system as it often suffices to provide a single mapping for an entire edge network. When mobility should be supported, every identifier must have its own locator. Moreover, changes in the mappings must propagate very fast to the mapping devices. The mapping system can contribute to the availability of a site by providing primary and backup locators for multi-homed networks. They need to be managed appropriately, i.e., if the primary locator does not work anymore, queries are answered using one of the backup locators. Mapping systems may be part of traffic engineering systems, e.g. load balancing can be achieved by answering queries for multi-homed networks with varying primary locators.

Mapping System with Relay Function. Most of the proposals for future Internet routing require an intermediate node along the path from source to destination to add the locator information to a packet. In that case, fast responsiveness of the mapping system is of utmost importance so that local caches with mapping information are advantageous again. In case of a cache miss, there are several options to handle the respective packet.

- Discard the packet. Discarding the packet is dangerous as it can have a detrimental effect on the communication, e.g. when a TCP SYN packet is lost.

- Store the packet until the mapping is available. Storing the packets is challenging as additional buffers are required and the management of a mapping node becomes more complex. Moreover, buffers can fill up quickly and packet loss occurs when many packets without locally available mappings arrive. This can be provoked by sending many packets to destinations with unknown mappings or even wrong identifiers.

- Forward the packet to some default node that probably knows the mapping. In particular, the packet could be sent to some part of the mapping system that has packet forwarding capacity [4].

Early Approaches. Some mapping systems have been proposed in the LISP context. Others proposals reuse the DNS infrastructure or assume distributed hash tables (DHTs). However, this area is currently not well researched and more insights are needed. We briefly describe LISP+ALT as it seems to be the preferred option in LISP. LISP+ALT stands for the LISP ALternative Topology [4]. ETRs communicate the mapping information for the EID prefixes they are responsible for to a network of so-called ALT routers. These ALT routers compose the ALT and are arranged in a hierarchical fashion with potential shortcuts among routers of the same hierarchy level. The ETRs communicate the reachability of the EID prefixes they are responsible for only to bottom-most routers in the ALT. ALT routers communicate which aggregated IP prefixes are reachable through them to peering ALT routers on the same hierarchy level and to superordinate ALT routers on a higher hierarchy level. BGP is used for that purpose. The structure of the ALT should be chosen such that the reachability information can be aggregated as much as possible. To query mapping information for some EID, an ITR connects to some ALT router which forwards it either to subordinate or peering ALT routers using the obtained reachability information or to a superordinate ALT router if no such information is available. Eventually, the query reaches an authoritative ETR which responds the mapping information directly to the ITR.

In the next section, we describe how the applications hedge against traffic fluctuations and against the increased user requirements.

3. Newly Emerging Paradigms for Internet Applications

Over the last years, new paradigms have emerged in telecommunication systems that are currently being realized in the Internet. Among those are the overlay, Peer-to-Peer (P2P), and Quality of Experience (QoE) paradigms. An **overlay** or an **overlay network** is a flexible, logical network that is built on top of an existing substrate network. Overlays are used to overcome technical limitations of the Internet, e.g. multicast, or to facilitate simplified implementation of sophisticated new mechanisms on a logical layer, e.g. re-routing on application layer in case of congested end-to-end paths. Note that the Internet itself has evolved as an overlay on top of the plain old telephone system to support new packet-switched data services.

In a **Peer-to-Peer (P2P) network**, the nodes of this network, called peers, share common resources, e.g. bandwidth or memory, in order to provide or support a certain service, like content distribution networks (CDN) or distributed lookup systems. Typically, the peers form an overlay for communicating with each other. The capabilities of P2P facilitate the deployment of new functionalities, like direct any-to-any communication or sharing of user-generated contents, as well as help to overcome restrictions on resources, e.g. in terms of storage capacity for a CDN. To this end, the application of the fundamental P2P paradigm fosters the realization of future Internet applications and allows saving infrastructure costs by using existing resources in a more efficient way.

Furthermore, the technological advances in high-speed Internet access enable the realization of the P2P potential and propel the use of the Internet into a new era. New applications have emerged that are bandwidth intensive or have strict Quality of Service (QoS) requirements. The most popular applications up to now are P2P file sharing applications that serve as a new medium for CDNs like eDonkey or BitTorrent. Recently, new types of overlay applications have appeared and gained popularity, such as P2P-based voice and video services. Examples are the popular Skype Voice-over-IP application or online video recording systems.

The user's satisfaction with a particular application is expressed by the **Quality of Experience (QoE)** measure [10]. Degradation in QoS, like packet loss, packet reordering, and large jitter in the network, may lead to strong decrease in QoE, which is the case for VoIP applications for instance. Beside such objective end-to-end QoS parameters, QoE focuses rather on subjective evaluations of service delivery by the end users. It addresses service reliability comprising service availability, accessibility, access time and continuity, as well as service comfort including session quality, ease of use and level of support. From this perspective, QoE will be the major criterion for the subscriber to select a specific service.

Multi-Network Services and Edge-based Intelligence

The composition of these paradigms may result in multi-network services with edge-based intelligence. In future telecommunication systems, we observe an increasing diversity of access networks and the fixed to mobile convergence between wireline and wireless networks. This implies an increasingly heterogeneous networking environment for applications and services. The separation of transport services and applications or between different services leads to **multi-network services**. A future service has to work transparently to the underlying network infrastructure and independently of the user's current location and access technology. In this sense, a multi-network service establishes a logical overlay on top of different access networks.

The Internet Protocol is currently the smallest common denominator for such multi-network services. Still, roaming users expect these services to work in a satisfactory way, i.e. a good QoE, regardless of the currently available access technology. Thus, a true multi-network service must be able to adapt itself to its environment to a much stronger degree than what is supported by the Internet protocol suite. Streaming multimedia applications for example face the problem that their predominant transport protocol UDP does not take any feedback from the network into account. Consequently, any quality control and adaptation has to be applied by the application itself at the edge of the network. This is referred to as **edge-based intelligence**. The network providers have to cope with the fact that these edge-based applications dynamically determine the amount of consumed bandwidth. In particular, applications such as Skype do their own network quality measurements and react to quality changes in order to keep their users satisfied. This edge-based intelligence is established via traffic control on application layer which is reasonable from the view point that the application knows its service requirements best. For example, a voice application knows its used voice codec and thus the corresponding required minimum throughput.

The shift of the control intelligence to the edge is accompanied by the fact that the observed **user behavior** also **changes**. A user can appear either altruistic or selfish. Selfish user behavior means that the user or the application tries to maximize the user-perceived QoE rather than to optimize the overall network QoS. Very often such selfish behavior is implemented in the software downloaded by the user without his explicit notice. In contrast, altruistic users, whose behavior is mostly influenced by the network provider's traffic control protocols (like TCP) help to maximize the overall system performance in a fair way. In the case of file sharing platforms, an altruistic user is willing to upload data to other users, while a selfish user only wants to download without contributing to the network. For VoIP, altruistic users would reduce the consumed bandwidth in the case of facing congestion, while selfish users would continuously try to achieve a high goodput and QoE, irrespective of the consequences for other users.

In addition, an edge-based application is often controlled by an overlay network, which can change rapidly in size and structure as new nodes can leave or join the overlay network. Thus, **higher dynamics of the network topology** are observed and the application has to manage this. An edge-based application could use many networks with different technologies in parallel, raising the question which network has to maintain which portion of the agreed QoS. From this perspective, the QoE will be the major criterion for the subscriber of a service. As a consequence, the edge-based application is responsible (a) to evaluate the QoE at the end user's site and (b) to react properly on the performance degradation, i.e. that the application adapts itself to the current network situation to maintain the QoE.

Figure 5 illustrates the **QoE control scheme** of such an edge-based application. Users are connected to each other via the corresponding access technologies. The QoE is assessed during a period t_Q of time. Accordingly, the altruistic users and the selfish users react on feedback obtained from measurements. As an example for edge-based intelligence, we investigate the Skype VoIP service in more detail. This example shows the change in user behavior and bandwidth demand and discusses the QoE adaptation scheme, i.e. the way Skype reacts to keep the QoE.

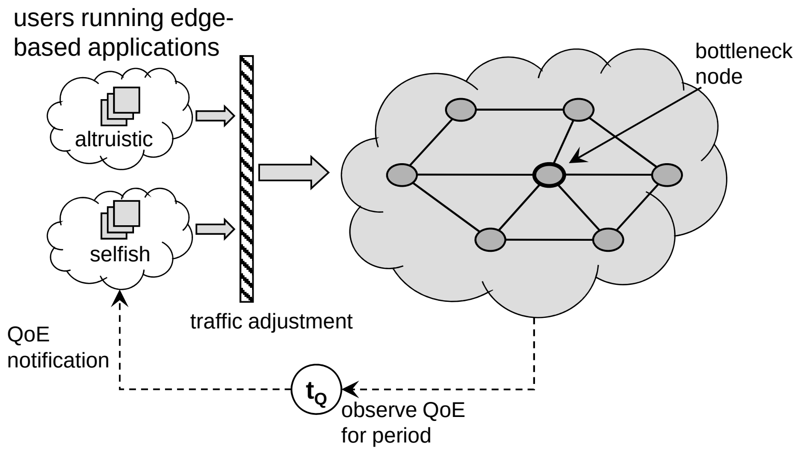


Figure 5: Quality assessment mechanisms for edge-based applications.

Example: Skype VoIP Service

In a measurement study in [5, 6], we emulated dynamic network changes by setting the packet loss and the delay on the end-to-end link between two Skype users. We captured the observed traffic pattern, i.e. Skype's reaction on the QoS changes in the network, as well as the QoE in terms of MOS at the end user site. As a result, we found that Skype selects an appropriate voice codec in order to maintain the voice quality. The power of the processing unit determines whether a constant-bit rate iLBC derivate or the more complex, adaptive iSAC codec is used. Another possibility is the adaptation of the bandwidth and the replication of information to overcome packet loss, even during a call.

Skype repeats voice samples depending on the perceived end-to-end loss. From the viewpoint of a single user, the replication of voice data overcomes the degradation caused by packet loss and enables to maintain a certain QoE. The cost for this achievement is a larger amount of consumed bandwidth. However, if the packet loss is caused by congestion in the network, this additionally required bandwidth even worsens the network situation. Altruistic behavior, on the other side, would reduce the bandwidth consumption in such a way that the pressure on the network is released and thus the overall network performance is improved.

However, if the direct end-to-end connection between two users is too poor, Skype initiates re-routing on application layer by relaying the traffic over a third-party machine. In our measurements, Skype used a different machine C in the Internet as a relay node. After 15 s, the traffic was redirected from A to C to B, instead of the direct, but disturbed connection, from A to B, see Figure 6. This variety of mechanisms to maximize the QoE reveals the edge-based intelligence of the Skype application. Traffic engineering in future Internet is expected to follow this new paradigm.

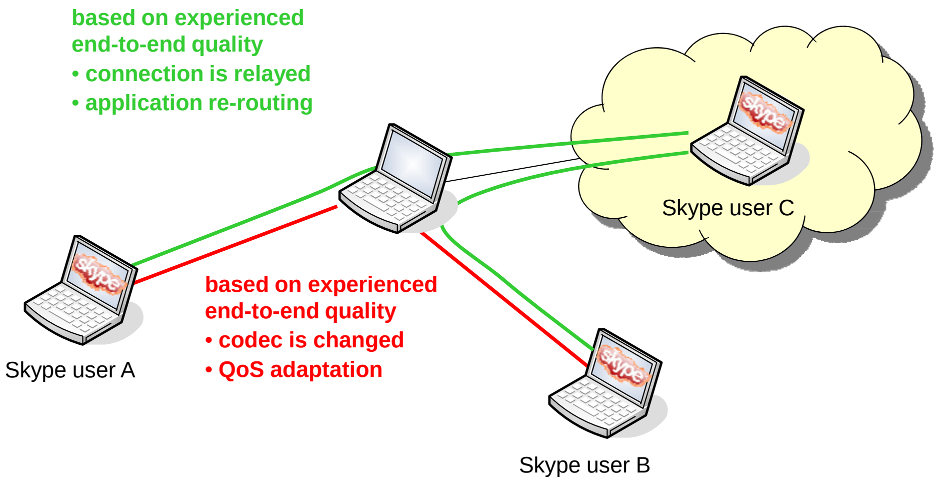


Figure 6: QoE adaptation and application-layer routing of edge-based Skype VoIP.

From an operator’s point of view, it will be an increasing challenge to cope with such new edge-based applications, which are already highly popular among the users for a variety of reasons. They offer good quality, are easy to use, and provide additional functionality, for example chatting and file transfer are implemented in Skype, but were not available in traditional telephony. Most importantly, the flatrate cost models for ubiquitous Internet access additionally make VoIP very affordable. Moreover, operators will not be able to stop user-driven applications at the edge of the network since the corresponding traffic cannot reliably be distinguished from regular IP traffic. However, as the traffic is transported via the Internet, there are no QoS guarantees like in regular circuit switched calls. Thus, if a network operator does not want to be reduced to a bit pipe, he needs to offer strict QoS and QoE guarantees and value-added services, like location based services in mobile environments. Therefore, QoE management and provisioning become a crucial task. In this context, network virtualization may be the apparatus which allows network operators to offer and realize QoE management and provisioning. It goes along with a new layering concept which will be discussed in the following.

Thinning the Protocol Layer

In today’s Internet, performance problems are often solved with cross-layer optimizations or middleware concepts. However, these solutions are hard to support efficiently in heterogeneous environments. They are inflexible and result in troublesome enhancements or even incompatibility for future networks. If we consider the commonly used ISO/OSI layer model for communication networks, interoperability between different technologies is solved on network and transport layer but not optimized for future Internet (e.g. TCP over wireless, multicast …). Peer-to-Peer (P2P) overlays and technologies might solve these problems of heterogeneity and complexity by creating their own name spaces, overlay routing algorithms, load distribution mechanisms, and scalable functionality. However, they need to be adapted to the underlying layers in order to increase the overall efficiency (e.g. by including proximity into the overlay) and to increase robustness (e.g. by installing mechanisms to react to faults and node failures). As a result, cross-layer approaches are used to realize an efficient implementation of P2P mechanisms for today's technology. Additionally, in the de facto standard layer model of the Internet some layers are not used.

All these observations lead to our vision of the future Internet. The architectural design is minimized to three necessary layers addressing the above mentioned aspects: a connectivity layer, a mediation layer, and an application layer cf. Figure 7. The task of the connectivity layer is to optimize individual physical access networks while including the mobility of users to allow handovers between different access technologies. From the user's point of view this means a multi-network service. The future network is designed for and focused on services for end users, i.e., the end-to-end user perceived quality is taken into account. This necessarily requires autonomic networks and autonomic network management mechanisms which will be a task on the next layer, the mediation layer. The advantages of P2P technology are utilized to mediate signaling information and user data, resulting in self-organized routing (which includes also source-routing or content-based routing) and a distributed resource access (e.g. bandwidth sharing among peers). Additional tasks like security and storage of third-party information for billing and accounting have to be considered to allow dependable direct communication between users and to offer service and network providers the possibility to charge for their added value to the future Internet. The top-level layer is the application layer which is user-oriented and allows end-to-end QoS. A crucial task might be the context-awareness of applications to offer real mobile applications. Therefore, the intelligence is moved out of the networks to the edge enabling these multi-network services. If necessary, application-layer routing or content-based routing can be applied to certain services.

In order to design and test such a new architecture concept, an important issue is the question how this can be implemented. Experimental driven research is a key approach to research future Internet networks and applications. A European network implementation substrate might be necessary like the GEANT2 or the German G-Lab which may also federate with other international testbeds like GENI.

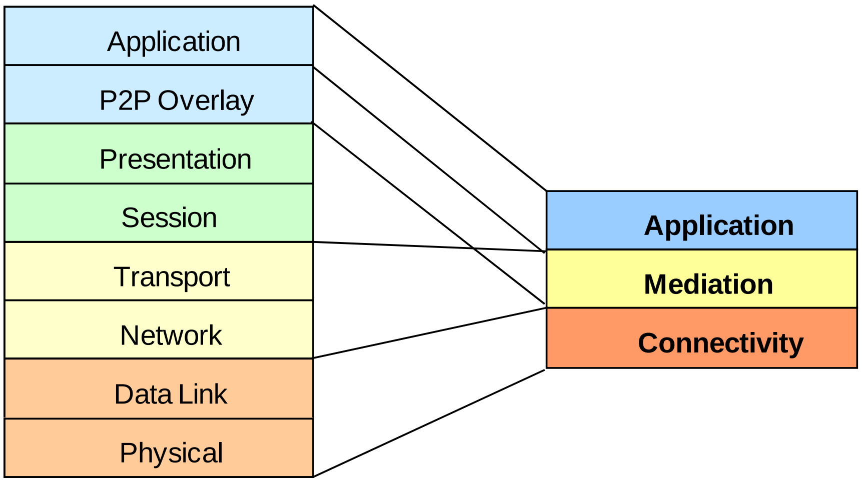


Figure 7: A new layering concept.

Virtualization

Network virtualization appears to be a promising solution for realizing the new layering concept by segregating the provisioning of services and applications from the physical infrastructure [9]. Thus, the mediation layer offers a virtual network to the application layer which is utilized by well-defined interfaces and APIs.

With the advances in microprocessor technology, virtualization has evolved into a viable option for managing and controlling several virtual entities on a shared physical resource. For instance, the Xen virtual machine monitor allows concurrent operation of Virtual Machines (VMs) on a single host PC running different isolated operating systems, each sharing the same physical CPU, hard disk, memory, and other resources using software for arbitration. This concept is now also entering the field of networking, where virtual networks are formed that are composed of interconnected virtual devices sharing the same physical substrate network. Naturally, the operation of such networks imposes much more sophisticated management routines for the access to the common resources, as the internal tasks of processing flows in routers becomes much more complicated than in conventional best-effort provisioning found in today's Internet.

In general, the concept of virtualization can be regarded as a high level abstraction principle that hides the underlying implementation details. This permits the construction of multiple coexisting virtual network architectures by different service providers, which all share the common physical substrate network managed by one or more infrastructure providers. This decoupling of service and infrastructure leads to a different view from the traditional concept of an ISP as they are known today. Users perceive each virtual network as tunnel and are free to choose their topology that suits best to their demands, whereas also infrastructure providers benefit from such concept by not having to be forced to deploy all new functionalities to support certain services at each node. This task can be shifted to the service providers to manage and reprogram their network architectures offering the end users a service-specific end-to-end quality. Therefore, an end user can connect to multiple service providers, which offer exactly their custom-made services without any interaction to the actual infrastructure. Thus, beside the technological benefits, the introduction of virtual networks would lead to entire different business and pricing models from an economical viewpoint.

The concept of virtualization is also applied in future Internet testbeds. Normally, testbeds use a slice-based concept, where each node consists of slivers, realized as virtual servers. Several slivers on a set of nodes form a virtual network, called a slice. This is, for example, part of the design principles of the PlanetLab testbed [8]. In the next section, we describe the role of such testbeds for the future Internet design.

4. The Role of Testbeds for the Future Internet Design

Testbeds have attracted a lot of attention during the last years. The first, worldwide testbed, PlanetLab [http://www.planet-lab.org], was set up by the Princeton University in 2003. The slice-based software provides the possibility to perform tests on up to 487 locations all around the world.

Besides PlanetLab, a large variety of testbeds and future Internet projects have been set up. The testbed projects can be divided into Internet-integrated testbeds and homogeneous, private ones. Let us call the first category the social testbeds and the second one the dedicated testbeds.

Within a social testbed, the user behavior can be evaluated. A good example is here the testing of real-time and streaming services. Up to which video quality is the end user at home satisfied or when does he turn the service off? Besides the testing of real-time services, security and anomaly detection can be performed in a social testbed. Several anomalies would never occur in a dedicated testbed and cannot be simulated. The anomaly detection further implies the need for traffic measurements, traffic management, and traffic analysis. Traffic measurement tools for home users to analyze their broadband Internet connection are provided by the Measurement Lab (M-Lab) initiated by Google and the PlanetLab Consortium [http://www.measurementlab.net].

In contrast, dedicated testbeds help to create and evaluate new services and protocols. Future Internet routing protocols will never be set up on backbone routers before they are intensively tested in a dedicated testbed. From the industrial point of view, such dedicated testbeds help to decrease the time to market of new services and network topologies.

The different testbeds however are only a small step towards the future Internet. Besides testing, new protocols and mechanisms have to be designed and evaluated. Furthermore, due to the fact that large-scale testing is time-consuming and often not possible, simulation studies are required and analytical models have to be assembled. Thus, a kind of research cycle between testing, simulation, and analysis is needed. Routing, addressing, mobility control, and management concepts invented and evaluated via simulation can be executed in testbeds which are a lot closer to reality. New problems occurring in the testbeds can then be used to adapt the simulation. Furthermore, the complexity of new services, mechanisms, and technologies are high so that they are difficult to handle using an analytical model. This combination of Future Internet studies and experimentation is shown in Figure 9 and is applied in the G-Lab project [11].

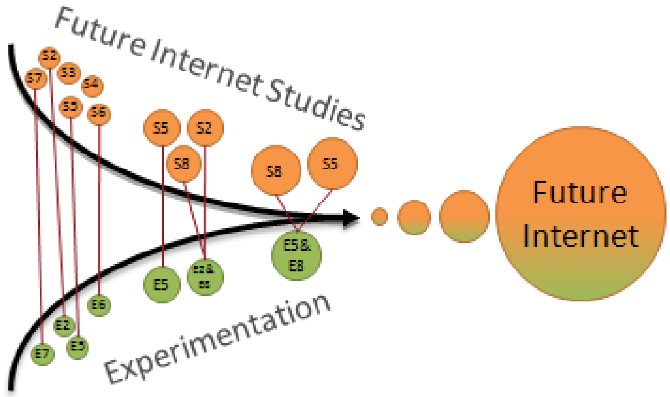


Figure 8: Future Internet studies and experimentation in combination leading to the Future Internet.

Future Internet Initiatives and their Testbed Projects

As already mentioned, the precursor of all testbeds was PlanetLab from Princeton University. Their software is widely used in several experimental facilities. Due to the huge amount of future Internet projects, we can point out only a few of them.

American Testbed Initiatives

Starting from PlanetLab, the US has now set up the successors Global Environment for Network Innovations (GENI), and the Measurement Lab (M-Lab). However, M-Lab is in contrast to the GENI not funded by the National Science Foundation (NSF). The goal of M-Lab is not to set up large, heterogeneous testbeds but to provide measurement tools to the end user.

Measurement Lab (M-Lab): The Measurement Lab was founded by the New America Foundation's Open Technology Institute, the PlanetLab Consortium, Google Inc., and academic researchers. M-Lab was developed in 2008 after Vint Cerf and others at Google initiated conversations with network researchers to learn more about challenges to the effective study of broadband networks.

M-Lab provides a number of servers and measurement tools. With their help it is possible to identify network problems, prioritization schemes of the ISP, and to see which traffic is blocked by the ISP. At the moment four tools are provided like the network diagnostic tool to test home connection speeds. Two further tools are coming soon.

Global Environment for Network Innovations (GENI): In contrast to M-Lab, GENI is the direct successor of PlanetLab and one of its goals is to improve the virtualization concept of PlanetLab to be able to handle heterogeneous testbed sites with wired and wireless access operating with different bandwidths. 29 partners are integrated in the project which is at the moment funded with USD 12 Mio. The sliced based software is now equipped with a clearing house which is responsible for the resource allocation. A user participating in the project can request resources from different testbeds and the clearing house controls the assignment.

GENI does not only provide an experimental facility with major knowledge from the PlanetLab project but also supports other projects like Future INternet Design (FIND). Furthermore, it will be possible to integrate other testbed initiatives like OneLab or Akari which are also based on the PlanetLab software.

FIRE: The European Testbed Initiative

Future Internet Research and Experimentation (FIRE) is the European Testbed Initiative and contains about 15 subprojects working on the development of the Future Internet, whereby five actions work on developing the testbeds and its software, see Figure 9.

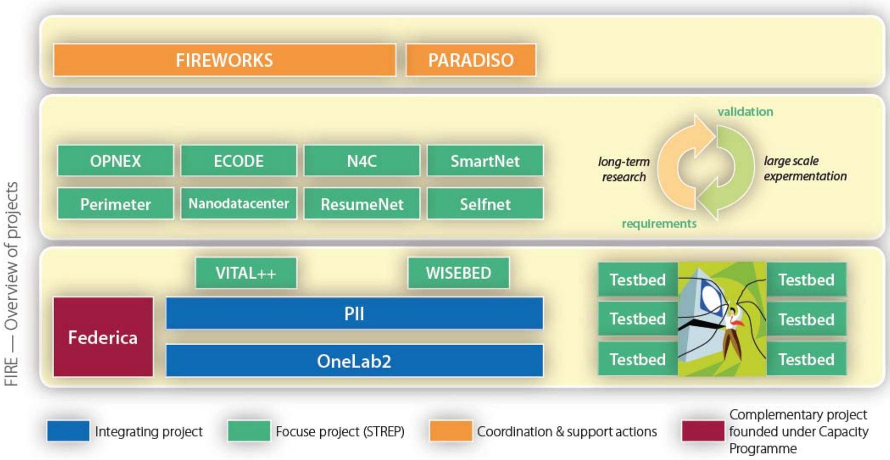


Figure 9: [*Source*] "An Overview of the European Fire Initiative and its Projects", European Commission, September 2008 [7].

OneLab: The OneLab consortium is a research-driven initiative with 29 partners from universities and industrial research institutions. Their aim is, similar to the GENI project, to extend the PlanetLab software to support heterogeneous testbeds. The partners operate the PlanetLab Europe, try to extend the PlanetLab services across Europe, and federate with other PlanetLab infrastructures worldwide.

Panlab: The Panlab project is an industry driven project working on the implementation of an infrastructure for federating testbeds. The tool called TEAGLE builds on the existing testbeds and should federate the regional innovation clusters in Europe. The testbed federation includes four core innovation clusters and three satellite clusters.

Federica: The third testbed-related FIRE subproject is called Federica. The aim is to develop a versatile technology-agnostic network infrastructure that can run over existing production networks such as GÉANT2 and national academic networks. In contrast to OneLab, it is not only possible to work on the upper layers of the ISO/OSI protocol stack but also to use the testbed platform to test routing protocols or even new MAC layer mechanisms.

WISEBED: The WISEBED experimental facility consists of a number of independent sensor networks throughout Europe. It offers not only the possibility to use a single sensor network through a portal server, but also to create virtual sensor networks built from physical networks and single nodes of networks.

VITAL++: The goal of the VITAL++ testbed is to embed P2P technology in next generation networks. Therefore, a combination between P2P and IMS is aspired where the IMS control-plane is used for AAA, security, and mobility management.

Local Testbed Initiatives

Several local testbed initiatives have been set up during the last years. Some of them focus more on wireless testbeds like the French **SenseLab** or the Finish **Converging Networks Lab**, whereas others focus on cloud/grid computing like the Netherlands **DAS-3,** the Israeli **IGT**, or the French **ALADDIN** project.

In Germany, the future Internet research project is called **G-Lab** and is coordinated by the University of Wuerzburg. The G-Lab project consists of a Germany-wide research and experimental facility used to investigate the interplay between new technologies and the requirements of emerging applications. The first phase of the project started in October 2008 and runs for three years. The G-Lab testing facilities consist of wired and wireless hardware with over 170 nodes which are fully controllable by the G-Lab partners.

5. Concluding Remarks

In this paper, we discussed issues in future Internet design. We showed trends in future Internet routing and the shift from multi-service networks to multi-network services supporting edge-based intelligence. These two issues are among others examined in the project G-Lab just started in Germany.

It is obvious that it is difficult or even impossible to predict, how the network of the future will emerge. However it is quite clear that some major architectural changes in the Internet will happen in the next years. According to our observations, the future Internet will be a network of applications emerging as a synthesis of evolutionary and clean-slate approaches. Clean-slate thinking determines shape and features of possible future networks, but their deployment will happen on an evolutionary path by adaptation of today’s reality.

References

[1] Meyer, D., & others. (2007). RFC4984: Report from the IAB Workshop on Routing.

[2] Meyer, D. (March 2008). *The Locator/Identifier Separation Protocol (LISP)*. The Internet Protocol Journal , 11(1).

[3] Meyer, D. (2008). *Lisp Interworking*. Requested on February 25, 2009 von http://www.lisp4.net/

[4] Farinacci, D., & others. (Nov. 2007). *LISP Alternative Topology (LISP-ALT). http://tools.ietf.org/id/draftfuller- lisp-alt-01.txt* .

[5] Tobias Hoßfeld and Andreas Binzenhöfer. *Analysis of Skype VoIP Traffic in UMTS: End-to-End QoS and QoE Measurements*. Computer Networks, Vol 52/3 pp 650-666, 2008, http://dx.doi.org/10.1016/j.comnet.2007.10.008.

[6] Tobias Hoßfeld, Phuoc Tran-Gia, Markus Fiedler. *Quantification of Quality of Experience for Edge-Based Applications*. 20th International Teletraffic Congress (ITC20), Ottawa, Canada, June 2007.

[7] European Commission. *An overview of the European FIRE initiative and its projects, September 2008*, http://cordis.europa.eu/fp7/ict/fire/

[8] Larry Peterson and Timothy Roscoe. *The design principles of PlanetLab.* ACM SIGOPS Operating Systems Review, Vol 40/1 pp 11-16, 2006.

[9] Thomas Anderson, Larry Peterson, Scott Shenker, Jonathan Turner. *Overcoming the Internet Impasse through Virtualization.* Third Workshop on Hot Topics in Networks (HotNets-III), San Diego, CA, USA, November 2004.

[10] Aad van Moorsel. *Metrics for the Internet Age: Quality of Experience and Quality of Business.* Fifth Performability Workshop, Erlangen, Germany, September 2001.

[11] Phuoc Tran-Gia, Anja Feldmann, Ralf Steinmetz, Jörg Eberspächer, Martina Zitterbart, Paul Müller, and Hans Schotten. *G-Lab White Paper Phase 1*, December 2008, http://www.german-lab.de/

[12] Michael Menth, Matthias Hartmann, and Dominik Klein. Global Locator, Local Locator, and Identifier Split (GLI-Split), work in progress, http://www3.informatik.uni-wuerzburg.de/~menth/Publications/papers/Menth08-GLI-Split.pdf