The bridging virtualization approach to Next Generation Broadband Access Networks

JON MATIAS, EDUARDO JACOB, MARINA AGUADO, JASONE ASTORGA

University of the Basque Country, Department of Electronics and Telecommunications, Spain
{jon.matias, eduardo.jacob, marina.aguado, jasone.astorga}@ehu.es

Keywords: broadband access networks, NGN, network virtualization, Ethernet services, Carrier-Grade Ethernet, security

Next Generation Broadband Access Networks (NGBAN), the next evolutionary step of current broadband access, have experienced a great evolution in the last few years. The NGBAN architecture is based on the reference model introduced by the Broadband Forum in TR-144, while the Next Generation Services (NGS) are based on the Ethernet Services defined by the Metro Ethernet Forum in its 6.1 technical specification. In this context, network convergence means that the same network must be capable of transporting all the existent telecommunication services (voice, video and data). This paper introduces Carrier-Grade Ethernet as transport technology to achieve convergence in provider networks. A new approach for network convergence is also presented, the bridging virtualization, which uses the concept of instances to deal with service requests. Then, a secure instantiation mechanism for NGBAN is explained, which is based on the EAPoL protocol (IEEE 802.1X). Finally, a profile-based configuration service is introduced, which defines the services through XML profiles inspired on the MEF specifications (UNI, EVC per UNI and EVC).

1. Introduction

Provider networks have experienced significant improvements due to the developments carried out around the concept of *Next Generation Networks* (NGN). Architectural evolutions in access and core networks are the main results of all this effort. There have been different approaches to NGN, but convergence, security, ubiquity and mobility are constants in all of them.

The concept of network convergence involves drastic changes of the traditional way of thinking. This concept implies that the same network must be capable of transporting all the provided services, instead of using different network architectures and technologies for each service or type of services. Even though circuit-switched services are not taken into account, the challenge is not trivial, since each service has its own particularities.

Currently, IP/MPLS and *Carrier Ethernet* [1,2] are the main alternatives for achieving network convergence. This paper has been focused on Ethernet proposals, specifically on *Carrier-Grade Ethernet* (CGE) [3,4] developments in which Ethernet is used as transport technology (opposite to Ethernet as service or interface). In fact, multiple technological components [5] are involved, such as Provider Bridges (PB), Provider Backbone Bridges (PBB), Provider Backbone Bridges – Traffic Engineering (PBB-TE) or Shortest Path Bridging (SPB).

All of them are IEEE standards (the last two in draft status), where PB and PBB address scalability and management issues, PBB-TE adds traffic engineering and SPB contributes with a link-state protocol [6] approach. However, there are also a few other standards covering different aspects that Ethernet technology (which emerged from LAN environments) must fulfill if it is to succeed as a transport technology. This is the case of Operations and Maintenance (OAM) capabilities, which are introduced by Connectivity Fault Management standard [7] (IEEE 802.1ag) and ITU-T Y.1731 [8] recommendation. Connectivity verification, rapid recovery and performance measurement are some of their improvements, essential procedures as carrier class technology.

In order to improve the coexistence of all these proposals, we have analyzed virtualization techniques to achieve a complete platform, in which real benefits can be obtained from this cooperation between different technologies, and we have developed a testbed based on Click tool [9] with promising results. The prototype consists of several layer 2 nodes (bridges), each with multiple simultaneous instances of different CGE technologies running on the same machine (or split up in several machines). This is what we call the *bridging virtualization* approach.

The bridging virtualization approach was introduced at ConTEL 2009 [10]. Based on this initial work, further improvements are presented at this paper. Our most relevant contributions are: the concept of Next Generation Services based on the Ethernet Services defined by the Metro Ethernet Forum [11] and the complete description of the *secure instantiation process*. In the later contribution we also introduce the *service port* concept, as well as the single-step and two-step AAA instantiation, and the profile-based configuration process.

The scope of this paper covers both access and aggregation networks, where Broadband Forum is the main meeting point for vendors and service providers. The aim of this organization is to assure development and deployment of broadband networks. There are several technical recommendations [12] from this forum with special relevance that must be taken into account: Multi-Service Architecture & Framework Requirements (TR-058), Migration to Ethernet-Based DSL Aggregation (TR-101) and Using GPON Access in the context of TR-101 (TR-156). The last two establish the introduction of Ethernet into provider networks, as well as practical aspects for QoS, Multicast, OAM and security.

Future Internet (FI) related initiatives are another important source of contributions to this new perspective of what broadband networks should be. In some cases, the proposals deal with Post-IP scenarios, where new network architectures are designed. All these approaches arise from the necessity of new paradigms for current Internet in order to overcome its limitations. The recently created Future Internet Assembly [13] (FIA), promoted by the European Commission, collects all those restrictions as conclusions in the Bled Manifesto [14].

Regarding the worldwide activities, different research programs about Future Internet have been promoted by both the National Science Foundation (NSF, in USA) and the European Commission. There are also several initiatives in Asia, led by Japan and Korea, which revolve around Future Internet. GENI (Global Environment for Network Innovations) and FIND (Future Internet Design) are the main programs funded by the NSF, whereas the AKARI Project is the most important one in Japan; meanwhile 4WARD, DICONET, FEDERICA and EIFFEL are some of the projects funded by the 7th European Commission Framework Program (FP7), which are focused on similar issues.

The structure of the paper is as follows. Firstly, Section 2 introduces the architecture of the system; a solid alternative to achieve network convergence by using Carrier Grade Ethernet; and the concept of Next Generation Services. Afterwards, Section 3 presents our proposal, the bridging virtualization approach, which is based on virtualization techniques and implemented with Click tool. Finally, Section 4 specifies how we have defined the secure instantiation process for service authentication and authorization, and Section 5 summarizes the paper with some conclusions.

2. Next Generation Broadband Access Networks

2.1 System architecture

Even today, it is quite common to find solutions where clients access each service (or each group of the same type of services) through different networks. This is the case of telephone service (voice), Internet access (data) or TV broadcast systems (video). Since the beginning, the three of them have been operated as diverse business models, where they must also deal with connectivity issues.

Nowadays, both telcos and cable companies offer bundled telecommunication services, which include voice, video and high speed data. Introduced as triple-play, the idea behind this concept is the provisioning of several broadband services over a single broadband connection.

This type of paradigm has three different actors, with three specific functions to cover. On the one hand, the client (C) is the final user that wants to access a service. On the other hand, the service provider (SP) is the entity that offers a telecommunication service to its customers. Between them, the connectivity provider (CP) gives an added value to services, such as security, ubiquity, mobility, multicast or QoS. The real challenge for CPs is to provide all the services through the same network efficiently and in a cost effective way.

The work done by the Broadband Forum must be considered as reference point, since it has defined a complete architecture which covers both retail and wholesale scenarios with a complete study of current and future possible alternatives. This forum has gener-

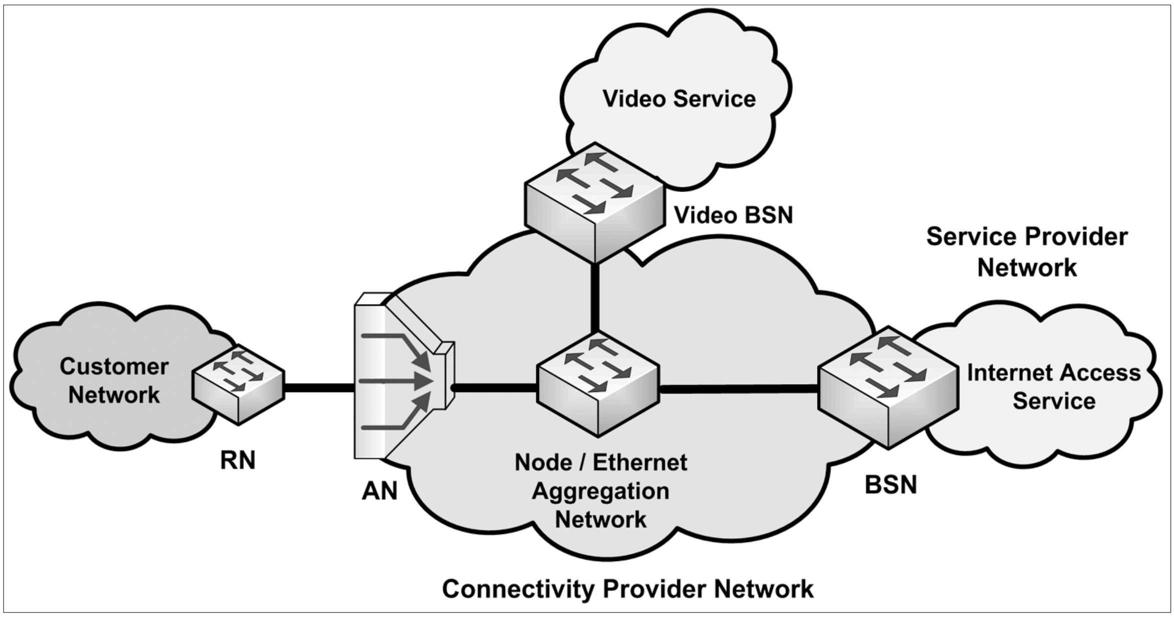


Figure 1. NGBAN architecture

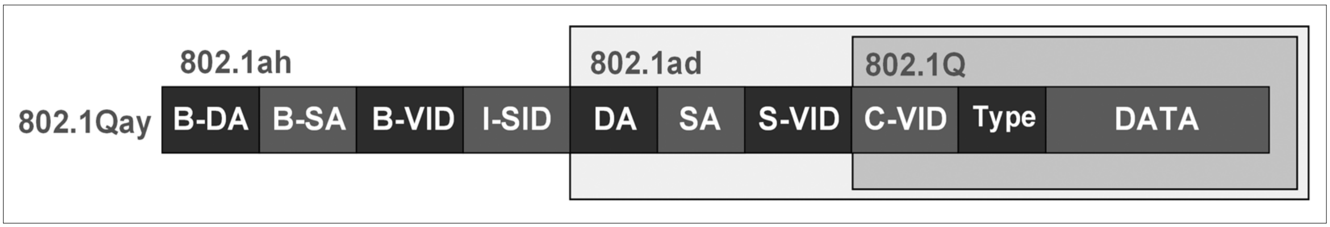


Figure 2. Carrier-Grade Ethernet frame format

ated several technical recommendations which have been turned into de facto standards by the telecom industry.

Regarding the architecture, there are two basic technical reports: TR-058 (Multi-Service Architecture and Framework Requirements) and TR-144 (Broadband Multi-Service Architecture and Framework Requirements). The TR-058 addressed the evolution from previous deployed DSL architectures to actual Multi-Service DSL architectures, but on top of an existing legacy ATM access network. Afterwards, the TR-101 (Migration to Ethernet-Based DSL Aggregation) was introduced as the next evolutionary step in the process of upgrading the access network to support Ethernet transport and switching capabilities. Therefore, the TR-144 extends the scope of TR-058 from a DSL centric architecture to a generic converged Broadband Multi-Service network architecture, which is exactly the aim of NGBAN.

As previously mentioned, there are three main entities in the reference architecture (*Fig. 1)*: the customer, the network provider and the service provider. The system allows the customer to access a set of service providers through the infrastructure and resources offered by multiple network providers.

The customer network has two types of elements: the Customer Premises Equipment (CPE) and the Residential Node (RN). The RN is a layer 2 device which carries out some essential adaptation functions between both entities. A layer 2 RN is one of the alternatives proposed by the TR-144.

The first element of the network provider is the Access Node (AN). The connection between the RN and the AN is known as the First Mile, local loop or access network. There are multiple technologies (i.e. xDSL, cable or FTTx) available in current deployments. Beyond the AN, the aggregation network is the part of the network provider which aggregates the traffic coming from multiple Access Nodes, and it is crucial for network convergence. It is very challenging for the transport technology to deal with the diverse nature of diverse service traffic. The Broadband Service Node (BSN) is the last element of network provider. It is also a layer 2 device and covers some essential adaptation functions.

The Service Provider is the entity which manages its customers (identity and credentials) and provides the services. A service is an agreement between the customer and the service provider. This means that the network provider must not impose any restriction over the service definition. The concept of Next Generation Services (NGS) is introduced as a new way of understanding what a telecommunication service could be. A NGS is a Layer 2 connection between a customer and a service provider (end-to-service), totally independent of Layer 3. This means that the connectivity provider relies only on Layer 2 (Ethernet) to join customers and services. Following this approach, Internet access (or IP connectivity) is just another service, whose multiple instantiations do not cause any collision in connectivity provider networks since IP Layer is transparent for them. Therefore, IPv4 and IPv6 (or multiple IP address schemes) coexistence becomes a reality, just as new paradigms where IP is not present (such as High Definition video directly over Ethernet).

2.2 Network convergence

Network convergence is one of the main challenges that Next Generation Networks must face. There are several initiatives and proposals dealing with this issue and all of them share some points: convergence, security, ubiquity, mobility and quality of service.

There are some different definitions for convergence; in this case, the concept is applied to the network scope: the same network to transport all the services (NGS) between the final client and the service provider. With the system architecture in mind, the convergence has a direct effect on the connectivity provider. This means that the architecture and technology selected by this provider must assure the multiplicity of services over the same physical network, what results in a multi-service and multi-provider solution.

For this purpose, IP/MPLS and Carrier Ethernet are the most realistic alternatives. The first one has been discarded because it prevents Next Generation Services (Layer 3 dependence). Moreover, IPv4 and IPv6 (or multiple IP address schemes) coexistence is not trivial. However, Carrier Ethernet fits right in with the requirements imposed by NGS (Ethernet services) and relies on a Layer 2 alternative endorsed by Metro Ethernet Forum [11] (MEF), later covered.

There are three main options for Carrier Ethernet as transport technology: Ethernet over SONET/SDH, Ethernet over MPLS, and Carrier-Grade Ethernet (CGE). The CGE technology is the best one to fulfill all the requirements imposed by Next Generation Services, and has overcome several significant challenges that traditional Ethernet (as LAN technology) evidences as carrier technology. Actually, CGE involves multiple technologies to accomplish all these challenges, such as: IEEE 802.1ad (PB), IEEE 802.1ah (PBB), IEEE 802.1Qay (PBB-TE), IEEE 802.1aq (SPB), or IEEE 802.1ag (OAM).

The necessity for network differentiation has firstly emerged in LANs environments, where companies want to isolate the traffic of each department. Virtual LANs standard [15] (IEEE 802.1Q) defines a new frame format *(Fig. 2)* that allows to differentiate Ethernet frames through Q-tag (12 bits) in order to split up the network in a logical way.

However, the same necessity appears at connectivity providers, which motivates the development of Provider Bridges standard [16] (IEEE 802.1ad), also known as Q-in-Q. This solution provides a new level of hierarchy, where customers' and providers' identification tags coexist in the same frame (Fig. 2) by encapsulating client tags (C-VID) in service tags (S-VID). Apart from this new technique, Spanning Tree Protocol (STP) and Independent VLAN Learning (IVL) are still used, limiting the scalability of developments based on PB. This restriction is motivated by a shared and flat MAC addressing scheme and the restriction of a maximum of 4096 service instances due to only 12 bits capacity in VID tags.

Because of these scalability restrictions, a new standard has been developed: Provider Backbone Bridges [17] (IEEE 802.1ah) or MAC-in-MAC. PBB overcomes PB's restrictions by encapsulating 802.1ad frames (Fig. 2) into a new provider's MAC header. In this case, instead of using a 12 bit Q-tag, a new field of 24 bits called I-SID (I-tag) is used to differentiate the services; achieving wide deployment scalability. The forwarding is based on the new header's fields (B-DA, B-SA and B-VID), totally isolated from customer's addressing scheme. So, PBB improves PB through scalability and isolation, but it maintains flooding and STP mechanisms.

Both 802.1ad and 802.1ah rely on the Spanning Tree Protocol [18] (IEEE 802.1D) to avoid loops. However, STP is not a suitable protocol for provider environments, because its goal is to get a loop-free topology by disabling those links that are not part of the tree. The generated final situation is very inefficient because it causes congestion on certain links, while others are not used at all. As an alternative, Multiple Spanning Tree Protocol (MSTP) could be introduced to get a better load balancing, but the limitation still remains.

Provider Backbone Bridges – Traffic Engineering [19] (IEEE 802.1Qay) improves CGE through traffic engineering capabilities.It is based on the MAC-in-MAC encapsulation (Fig. 2) defined in PBB, but operationally differs from it. PBB-TE disables some well known mechanisms of Ethernet like flooding, broadcasting or MAC learning, and also ignores STP associated states. On doing this, another mechanism is needed to fill the forwarding tables and assure a loop-free topology. The answer is a management system. PBB-TE achieves a connection-oriented behavior from a packet switched network by exploiting bridging forwarding mechanisms.

The forwarding decision is made according to the destination MAC address and VLAN ID (60 bits), providing great capacity to traffic engineering. The local scope of VLAN ID (B-VID) is the main difference from traditional VLAN schemes where this ID is global. This fact allows the reutilization of identifiers, which can obtain a global meaning by adding the destination address.

Shortest Path Bridging [20] (IEEE 802.1aq) is another recent development that proposes an alternative to STP dependence. SPB is a draft standard that uses PBB data plane combined with the well-known link state protocol IS-IS [6]. This enhancement adds carrier-grade any-to-any infrastructure capabilities by using the shortest path from any source to any destination.

Regarding quality of service, it is supported over 802.1p [18] efforts (included in IEEE 802.1D), and is a DiffServ based approach to provide QoS. There are eight different priorization schemes, which are included in a specific field of the VLAN tag (3 bits).

There are several developments regarding management capabilities, namely IEEE 802.1ag [7], which provides a mechanism for service fail proactive signaling; IEEE 802.3ah, which defines OAM capabilities for the first mille; IEEE 802.1AB, which allows topology discovery; ITU-T G.8031, which adds Ethernet protection mechanisms; and ITU-T Y.1713 [8], which gives additional management capacities to 802.1ag.

Definitely, Carrier-Grade Ethernet is supported by all these improvements to become the transport technology for connectivity providers. Some of the characteristics that CGE has acquired are future proof capacity for multimedia, quality of service support, scalability and hierarchical solutions, OAM capacities, and cost-effectiveness. Therefore, access and aggregation networks can be faced by native Ethernet solutions.

2.3 Next Generation Services

As previously introduced, a Next Generation Service (NGS) has been defined as an Ethernet Service. In this case, the work done by the MEF must be taken into account. This forum develops technical specifications and implementation agreements which could be considered as reference model for NGS.

The previously introduced architecture defines an end-to-end Ethernet scenario in which multiple broadband technologies could be used for service delivery. There are three different visions of Ethernet: an interface between two nodes, a service or a transport technology. Ethernet as a service means that all the Ethernet frames that enter a network provider must be delivered unmodified when leaving the provider, whereas Ethernet as a transport means that Ethernet technology is used to deliver the packets across the network provider. The former is the basis of NGS, while the latter is addressed by Carrier-Grade Ethernet (CGE).

NGS is focused on the Ethernet Services definition done by the MEF. Therefore, some terminology of MEF must be introduced. A User to Network Interface (UNI) i s a physical interface or demarcation between the network provider and the customer or subscriber (located between RN and AN). An Ethernet Virtual Connection (EVC) is a logical representation of an Ethernet service as defined by the associate between two or more UNIs. The most common way of implementing an EVC is through an S-VLAN ID of IEEE 802.1ad. A fundamental characteristic of this definition is that multiple EVCs can be multiplexed on the same UNI, which is essential to enable broadband service multiplicity over the first mile.

Three types of EVCs have been defined. The E-Line Service Type is a point-to-point EVC connection between two UNIs. In this regard, site-to-site layer 2 VPNs or Ethernet Internet access are some examples. The E-LAN Service Type is a multipoint-to-multipoint EVC connection among multiple UNIs (two or more). Multi-site layer 2 VPNs or Transparent LAN Service are examples. Finally, the E-Tree Service Type is a rooted multipoint connection (or point-to-multipoint) among multiple UNIs (two or more). E-Tree defines two different roles for a UNI: root or leaf. Each leaf is able to connect with all the root UNIs, whereas the connectivity between leaves is not allowed.

The MEF Ethernet service definition framework specifies the Ethernet Service attributes and parameters which define the UNI and EVC requirement for each Ethernet Service Type.

MEF Services are classified into two categories: port-based and VLAN-based. Port-based category implies a single service instance per UNI, which means that the network resource is dedicated to the same EVC. Consequently, this type of services can be identified on a per port basis. On the other hand, VLAN-based category implies multiple service instances per UNI, which means that the network resource is shared among multiple EVCs. Therefore, a new mechanism is needed to differentiate the services. MEF proposes the use of VLAN tags at data layer, which enables service differentiation on a per C-VLAN ID (Customer VLAN identifier) basis.

VLAN-based services make use of multiplexing attribute previously introduced, which allows multiple EVCs on the same UNI. On the other hand, port-based services make use of a special case of bundling attribute, the all-to-one bundling. The bundling service attribute enables two or more C-VLAN IDs to be mapped to a single EVC at a UNI. Moreover, both types of services are able to use two additional attributes: the C-VLAN ID preservation and the C-VLAN CoS preservation. Both preservation attributes define whether the C-VLAN ID or C-VLAN CoS is preserved unmodified across the EVC. This four attributes give great flexibility to the final system.

Another significant contribution of MEF is the complete definition and classification of Ethernet Services based on three set of attributes. The UNI attributes specify the physical interface capabilities, the service multiplexing capability or the C-VLAN bundling capability. The EVC per UNI attributes specify the C-VLAN mapping to EVC or the ingress and egress quality of services parameters (CIR, CBS, EIR and EBS). Finally, the EVC attributes specify the EVC type, the list of UNIs, the VLAN or CoS preservation or the service frame delivery behavior.

The NGS definition profile is composed of UNI, EVC per UNI and EVC attribute definitions, plus a new attribute which defines the Service. This last element has not been defined by the MEF and is an agreement between the service provider and the customer.

3. Bridging virtualization

3.1 Network virtualization

This section introduces a new approach to network convergence, which is based on virtualization techniques. Current developments on systems virtualization have allowed a new approach: the achievement of network convergence through network virtualization *(Fig. 3)*.

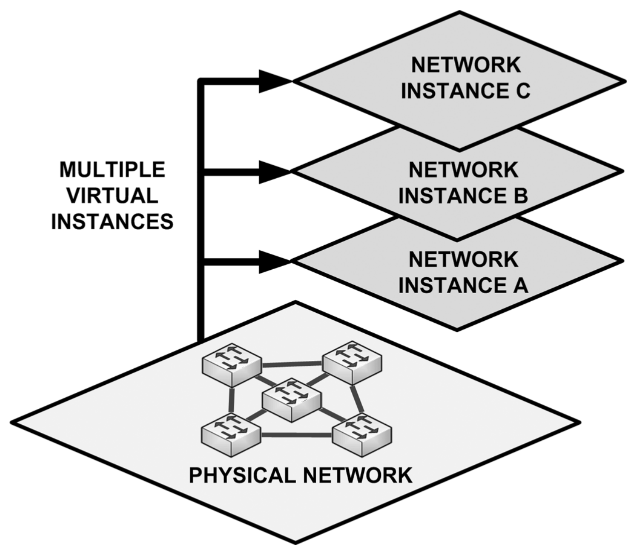


Figure 3. Network virtualization

The idea behind any kind of virtualization is the sharing of the same resources (hardware and/or software) by several instances. In the case of network, this means that the physical links (bandwidth), network interfaces and network devices (bridges in this case) are shared by different virtual network instances which use the same network infrastructure at the same time.

Sometimes it is difficult to get the same network fulfilling all the different requirements imposed by each service. Carrier-Grade Ethernet, for instance, faces this challenge by developing several different solutions like PB, PBB, PBB-TE, or SPB. In this case, all of them are proposed by the same organism that has taken care of making them compatible with each other. However, this is not always possible.

Next Generation Services will demand different behaviors from the connectivity network, and also complete isolation between services. This type of service does not depend on Layer 3, instead end-to-end (customer-to-service) connectivity relies exclusively on Layer 2 (CGE). This way, any Layer 3 protocol could be used transparently for connectivity provider network. Therefore, the final architecture would consist entirely of bridges (as has been described in Section 2).

The improvement of network efficiency, the reduction of capital and operational costs (CAPEX and OPEX), or the enhancement of provider agility are some of the ideas behind network virtualization. Resource sharing could be applied to get a network that has different behaviors depending on the instance in which the service resides. In this case, the network resources (like links, bandwidth, or equipment) are shared between all the Next Generation Services, where each instance is isolated, secured and managed by a different virtualization process.

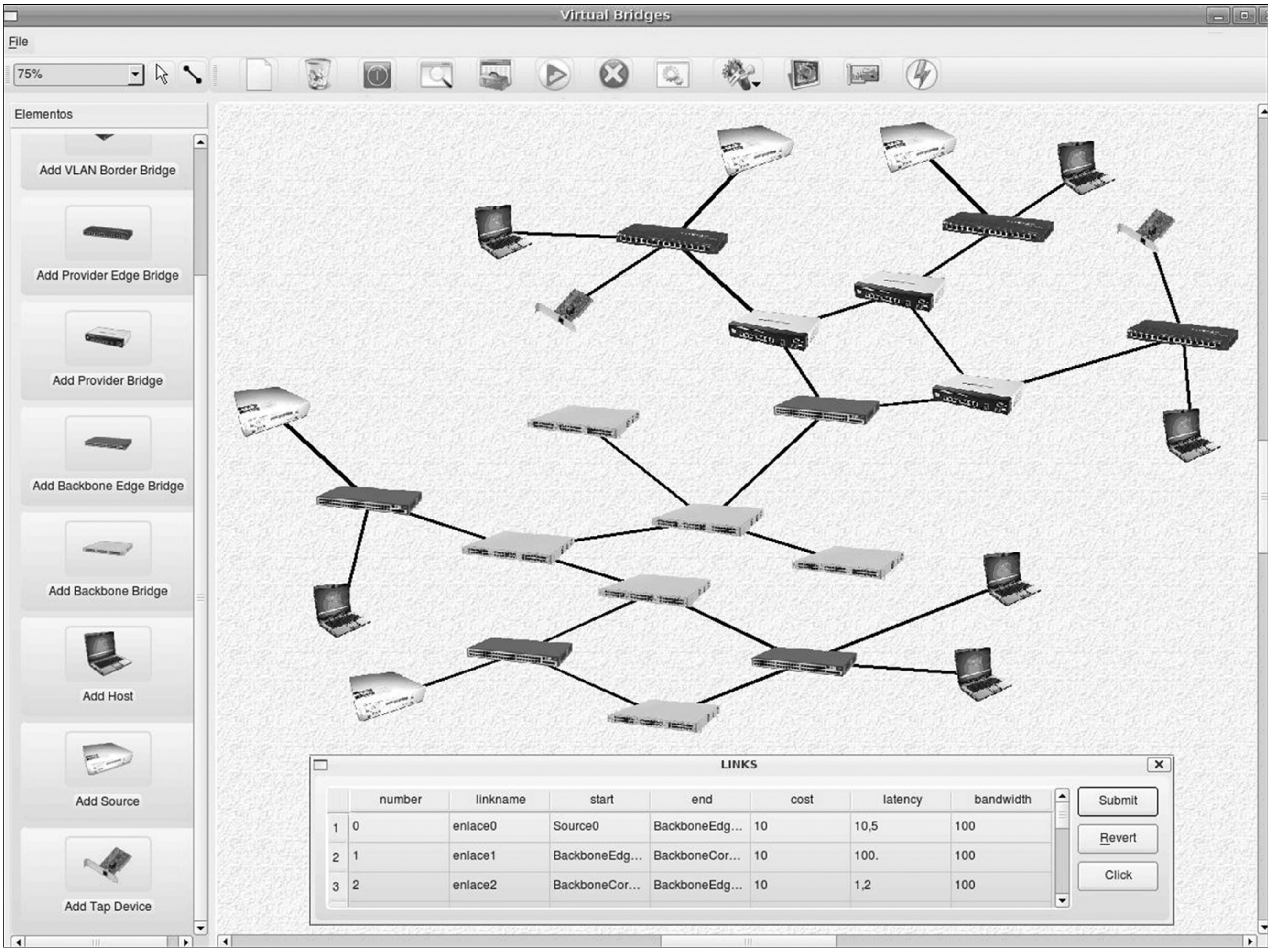
This paper proposes a solution where connectivity provider network achieves a convergence model by bridging virtualization. The data plane of each instance would be differentiated from others by using the VLAN identifier present in all Carrier-Grade Ethernet packets, which means that each VID can be associated with a different instance of the network. The control plane of each instance would manage the behavior of the bridges depending on the associated virtualization process that rules the forwarding engine. One instance could be controlled by Provider Backbone Bridges, other by PBB-Traffic Engineering, other by Shortest Path Bridging, other by a new proprietary development, and so on.

The improvement of this model is that any other solution, apart from IEEE proposals, could be addressed; the only restriction lies on using the same data plane present in CGE. This means that any new scheme that enhances the performance of a service could be easily incorporated just by adding the new virtual instance. More than in deployment scenarios, this feature is lightly valuable for testing new developments; but deployment networks could also be benefitted by the system's modularity.

All these concepts have been proved in a testbed. For the implementation, the Click tool [9] (originally developed at MIT) has been used. This tool allows network emulation with real interaction between Click and network nodes. The main benefit of using Click is that lots of developments can be reused (or improved) to get a really complex device just by adding modular components, where some might need to be implemented from scratch. This is the case of Provider Bridges (802.1ad), Provider Backbone Bridges (802.1ah) or PBB-Traffic Engineering (802.1Qay), which have been developed as new components. All of them have been implemented starting from the Virtual LAN (802.1q) component.

Click tool is able to emulate multiple devices over the same hardware or distribute them over several machines. In order to validate the functionality of the proposal, it is required to test different architectures in access and aggregation networks. Therefore, a new graphical tool *(Fig. 4)* has been developed to make this process

Figure 4. Graphical interface for Click



	number	linkname	start	end	cost	latency	bandwidth
1	0	enlace0	Source0	BackboneEdg...	10	10,5	100
2	1	enlace1	BackboneEdg...	BackboneCor...	10	100.	100
3	2	enlace2	BackboneCor...	BackboneEdg...	10	1,2	100

more efficient. This new implementation is focused on network interconnection, while each node is based on previously described components. All the network devices of this graphical tool could be sniffed (being one of its strengths), assuring that everything is working correctly.

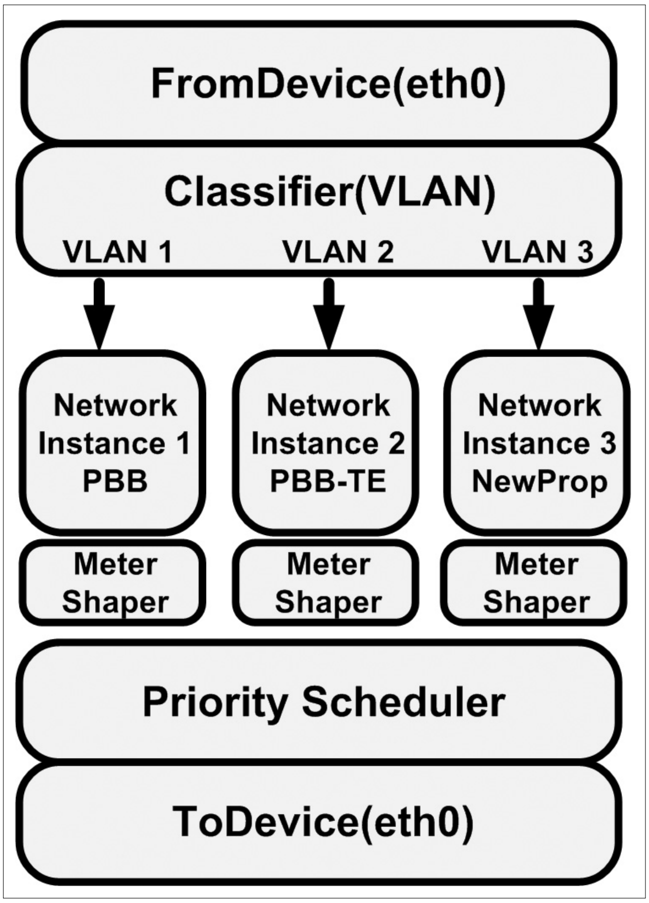


Figure 5. Bridging virtualization Click design

Fig. 5 introduces the click design that supports bridging virtualization, and therefore the network virtualization model for next generation network's convergence. Each packet goes through a classification process while entering the device through a “physical” port (it could be a real or virtualized port).

This classification determines the instance to which the packet belongs. As previously mentioned, this is done by associating VLAN identifiers and bridging instances, where each instance implements one possible CGE solution. On the other hand, the outcome of each packet goes through a prioritization process according to 802.1p developments. Previous to enforce this process, the definition of a QoS policy is needed to determine the interrelation between all the instantiated processes.

The flexibility of the model allows even the coexistence of a bridge based instantiation and a router based instantiation over the same node. This is a consequence of its modular design, where the forwarding decision of each packet is made after the classification process, and it could be taken at any level.

3.2 Click prototype

The prototype has three different parts: the click bridges, the GUI tool and the bridging virtualization technique. Each of them is analyzed in this section with more detail.

The basic element that emulates the behavior of PB, PBB and PBB-TE has been defined by creating new modules for Click. The design phase has been crucial to obtain the best reusability of the developed subsystems.

It is important to notice that in all the previously mentioned technologies, there is a remarkable difference between edge and core nodes. This results in each technology having two differentiated behaviors. The edge nodes have to encapsulate and forward packets, whereas core nodes only have to forward packets depending on the specific technology implemented. The encapsulation process is not as easy as it could seem, because a previous management process must configure the values of the new fields depending on the data that arrives in the packets. On the other hand, the forwarding process affects both the edge and the core nodes, which means that this module could be reused.

The development of the basic elements has been done in C++, a restriction imposed by the Click tool. Previous work and development of the VLAN modules have been taken as the starting point.

Apart from these new basic elements, tap devices (Layer 2 virtual network devices) have been used to achieve network connection virtualization between elements. A new tap interface is created when a new virtual link is defined between two nodes. Because of this, traffic can be sniffed from every port of every node. Having interactivity with real nodes is as easy as changing a tap device by a real interface. The real interfaces can be useful to test the platform with real nodes or to split up the platform in multiple machines.

Once those basic click elements are developed and tap devices are created, the bridges are composed by the creation of new .click files in which the interaction between both is defined. This .click files use specific nomenclature and are launched by the Click tool (that must be previously installed on the target machine) as independent processes. Afterwards, each process can be accessed by telnet to control and manage its behavior.

The problem is that the definition of those files could become very complex depending on the specific network architecture. Moreover, if this architecture changes, it could affect a huge amount of files which must be correctly configured in order to not have unstable schemes.

Because of this all, a new graphical tool has been developed. This new GUI is not only able to make network scheme composition more efficient, but also control the consistence of the final .click files (one per node) and the creation of all the required taps. The GUI is also very useful to define multiple different network schemes, without the complexity of doing all this by hand.

Apart form the bridge nodes, the GUI is also able to introduce source nodes (which generate traffic with specific characteristics and frame format) and capture devices.

Therefore, the GUI has several important tasks. First of all, it must create the tap devices needed to achieve network virtualization. Then, it must compose the .click files (one per node/element) depending on the graphically defined connections (or links) among them. Afterwards, it must launch the click processes, each of them associated with a virtual node defined by the .click files. Finally, the GUI tool has the ability to interact with the virtual nodes once they are running. This capability relies on specific handlers used by click, which have been defined in the previous mentioned design process of each element.

The last part is the one that introduces the bridging virtualization techniques. As it has been presented, it is a new radical approach for network convergence that can be useful for both research and deployment scenarios.

These techniques have a direct impact on .click files composition rather than basic elements development. This means that all the previous work defining CGE technologies can be reused only by extending the way in which the packets are handled when they come into or go outside the click processes.

It has been defined a data plane based on Ethernet, which uses 802.1ad or 802.1ah frame format. This means that all the packets carry a VLAN identifier which can be used to differentiate the specific instance of each of them. So, it is a restriction that any new definition of network behavior must support this frame format.

Focusing on the prototype, the VLAN identifier must be classified when a packet enters the bridge node (click process) in order to determine to which network instance it belongs. Once the packet is processed, the forwarding process of the specific CGE technology determines the outside interface. Since all the interfaces are shared by all the instances, a priority schedule is needed to manage the order in which the packets are sent through each interface. It is important to remember that all those interfaces can be real network devices or virtual tap devices.

The GUI tool must be also adapted to support the definition of this new type of nodes through the modification of previously used .click template files.

4. Secure instantiation process

This section is focused on the functional aspects of the service instantiation process to securely control the service delivery. There are two methods defined: the two-step AAA and the single step AAA. The latter one is common, and will be described in detail. The main difference between them is that the single step AAA only authenticates and authorizes the services, whereas the two-step AAA authenticates and authorizes both the network and the services. Both support multiple simultaneous processes of authentication and authorization of services.

A new extension of the Port-Based Network Access Control standard [21] (IEEE 802.1X) is also introduced, which defines the EAPoM (EAP over MAN or EAPoL-in-EAPoL) protocol. This extension adapts the 802.1X standard to a new scenario in which multiple services must be controlled, and is closely related to the *service port* concept.

4.1 Service port

The main restriction of IEEE 802.1X is that the standard can only control the access to the network, instead of being able to control the access of each customer to each service. It is an all or nothing access control to the network, while more granular control per service is needed.

Originally, the IEEE 802.1X standard defined the physical port of a device as the resource to be controlled; each physical port of a bridge must be authenticated by the supplicant (which is the client in an EAPoL scenario) that wants to access the network. Afterwards, with the development of IEEE 802.11i (security for WiFi networks), the physical port control was turned into a logical port control definition. With the introduction of the logical port, the IEEE 802.1X standard still remains the same, since each authentication process is univocally identified by the customer's MAC, and each customer traffic can be easily distinguished by this MAC even all the traffic goes through the same physical port.

In this new proposal, this logical port concept must be extended to address the new requirements. Following this tendency, the service port definition *(Fig.6)* is introduced as the basic element that enables the operation of the EAPoM protocol. The service port splits up the logical port into additional new ports, each of which has its own associated authentication process that rules the access to each service. This multiplicity of authentication processes is supported by EAPoM, which is able to differentiate multiple EAP processes from the same supplicant (or subscriber).

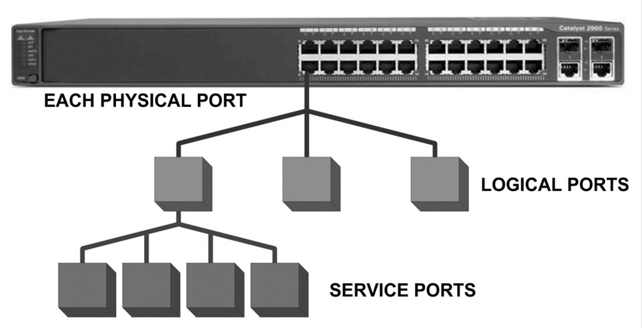


Figure 6. Service port

Another important definition associated with service ports, is the differentiation and identification of each service flow. Two are the main alternatives for this task: source-destination MAC address or VLAN identifier. The service flow identification based on source-destination MAC addresses could be used on point-to-point services or when the service is based on multicast traffic (and a multicast MAC address is defined). In both cases the access control definition is well restricted (source and destination); while in a multipoint scenario a certain variety of Access Control Lists (ACL) should be used (a list of multiple sources and destinations).

The second choice relies on IEEE 802.1Q standard [15] to identify each service flow through the use of different VLAN identifiers per service. In this case, the subscriber equipment must tag the traffic. Optionally, the Residential Node could make this tagging when customer's devices do not support it.

4.2 Two-step/single-step AAA instantiation

The two-step AAA instantiation process has two phases: the AAA process with the network provider and the multiple AAA processes with the service providers.

In the first AAA process, the subscriber is authenticated and authorized by the network provider. This procedure is similar to the standard IEEE 802.1X process. The only difference is that the EAP exchange between the subscriber and the Access Node is transported by the new EAPoM protocol, which uses a different Ethertype and MAC group address. This first network instantiation is demanded by the customer previous to any service instantiation procedure. The subscriber's identifier and associated credential are supplied by the network provider, and the concrete EAP method depends on its security policy. If this network's AAA process finalizes successfully, the subscriber is correctly configured to access the network; then, a new logical port associated with the subscriber is ready. This logical port is further divided into service ports by the subsequent service AAA processes.

As previously introduced, this first network AAA process could be omitted depending on the network's or the wholesale system's security policy. Each subsequent service AAA processes are equal, and the same as a single step AAA instantiation.

In the single step AAA Instantiation process *(Fig. 7)*, each service is consciously requested by subscribers each time they want to access a specific service. The subscriber's AAA client sends a type 5 EAPoM packet, which means that an EAPOL-in-EAPOL frame is encapsulated in the packet. The inner part has a unique service identifier associated to this AAA process with packet type 1, EAPOL-Start. From this moment, the same outer part and the same service identifier in the inner part are used for every exchange associated to this process.

This EAPOL-Start encapsulated inside the EAPoM packet goes through the Residential Node and the access network, and reaches the Access Node. The Access Node, as the first device at the network provider's premises, captures the EAPoM packet based on Ethertype or MAC group address filter rules. Then a new service port is instantiated and associated to the subscriber's MAC and the service identifier that goes inside the EAPoM packet. After that, there is a common IEEE 802.1X exchange between the subscriber and the Access Node with the only particularity that all the messages are encapsulated inside EAPoM packets with the associated service identifier. This involves a variable group of EAP request-response exchanges, starting by the identity request-response.

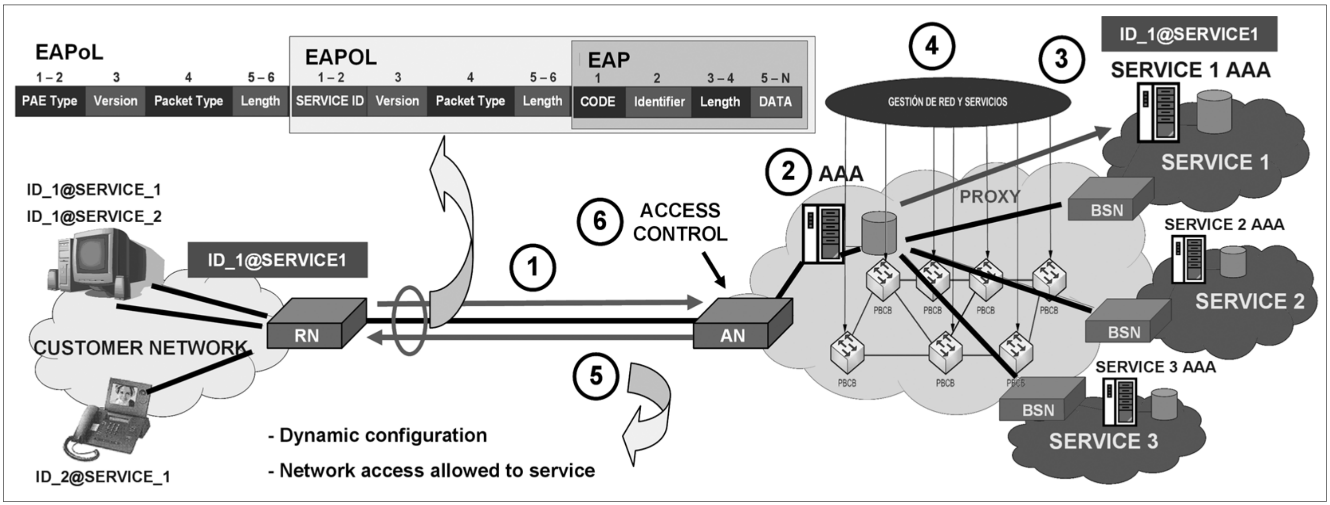
The subscriber identifier has two parts, the service provider identifier and the unique name that the customer has for this provider; this looks like ID@SERVICE (and is similar to other name schemes like e-mail or SIP ones).

Once the Access Node receives the identity response, the EAP packet is sent to the network authentication server using another protocol, in this case RADIUS. The network authentication server analyzes the subscriber identifier and depending on the service provider identifier part, it proxies the RADIUS packets to their respective service provider's authentication server. This means that the EAP exchange is made between the subscriber and the service provider; and therefore, the service provider is responsible for the authentication and authorization of the subscriber.

4.3 Profile-based configuration

Apart from AAA functions, this process is adapted to enable a configuration process. In this context, there is a secure relationship between the subscriber, the network provider and the service provider. This asso-

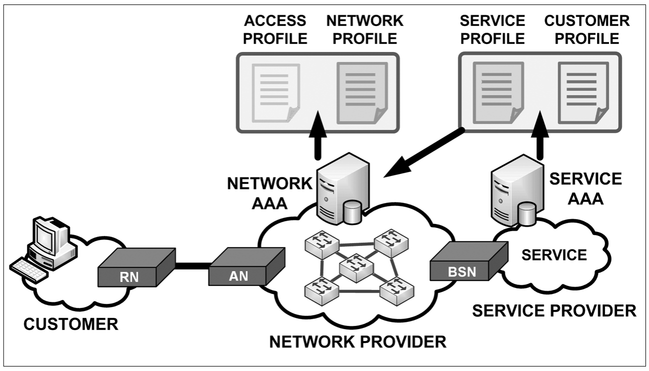
Figure 7. Secure instantiation of NGS



ciation can be used to define a set of configuration options that depends on the subscriber's identity.

This configuration process is based on the definition of profiles *(Fig. 8)*, which are XML files. This assures interoperability and a platform independent solution for configuration. Each provider has to create its own profiles associated with the service. Afterwards, the profiles are distributed together with the EAP success packet, once the AAA process ends successfully. The distribution of these profiles is done through new extended attributes of the RADIUS protocol.

Figure 8. Profile based configuration



The service provider defines two profiles: the service profile and the client profile. The service profile has all the parameters associated with the service and the subscriber's identity that must be interpreted by the network provider. The client profile has the parameters that must be configured by the customer.

The network provider also defines two profiles: the network profile and the access control profile. Both are dynamically synthesized from the service profile. The network profile defines the specific configuration that must be applied to the network in order to be able to assure the service requirements. The access control profile defines de access control policy that must be applied to the corresponding service port instantiated by the subscriber in the Access Node.

In case of using the IEEE 802.1ad standard (Provider Bridges), which has been recently adopted by the Broadband Forum, all the parameters of C-VLAN and S-VLAN associated to the service will be dynamically created and distributed to the Access Node through the configuration profile's mechanism.

A working prototype with all this concepts has been implemented in a Linux based environment. A standard development of IEEE 802.1X has been modified to support the new EAPoM protocol. The changes have been done quite easily because of its similarities with the standard, and both a supplicant and an authenticator with EAPoM support have been released. The authenticator has also been modified to support the new service port instances and a control access scheme associated with this concept. Finally, new RADIUS attributes have been defined in order to transport the previously introduced configuration profiles after a successful AAA exchange.

5. Summary

This paper introduces a new approach based on Carrier-Grade Ethernet to provide network convergence in NGBAN. The architecture recommended by Broadband Forum for Multi-Service is the reference point for the system architecture, where all the nodes are defined as bridges. Several Carrier Ethernet alternatives have been presented, among which Carrier-Grade Ethernet has been selected as transport technology for connectivity provider networks.

After all this introduction of current technology, a new approach for NGBAN has been presented. It is called *bridging virtualization,* and two new developments around it have been shown: the implementation of a prototype that validates bridging virtualization, which is made by using Click; and a graphical tool that is able to compose all the nodes (real or virtual) to get a virtualized network. The functional validation of the approach has been carried out by the implementation of these tools.

This paper introduces a new Multi-Provider and Multi-Service framework, where subscriber's access to services is granted depending on the result of an AAA process. Therefore, security improvements are evident for both network and service providers, since only previously authenticated and authorized traffic gains access to the network. This control is made per service and based on *service ports* instances, which is an evolution of standardized IEEE 802.1X logical ports. The AAA exchanges between the subscriber and each service provider are carried by the new EAPoM protocol. Apart from security aspects of the AAA exchange, a profile based configuration procedure has been associated with it. This means that configuration process depends on subscriber ID and is done in a secure context.

Another important achievement is the nomadic access to services, which means that subscribers can access their services with any location or network provider restriction. The nomadism is supported by AAA proxy mechanisms and the dissociation between identities (customer and service) and network parameters.

Finally, some remarks about future work are presented. Currently, we are working on new models for network virtualization at data-plane, which are based on the MAC addressing scheme instead of the VLAN identifier. A detailed definition of the AAA policy and obligations (for policy enforcement) are also needed to complete the security proposal. Apart from this, the Openflow technology has been considered to implement the bridging virtualization approach instead of (or in addition to) Click tool.

Authors

JON MATIAS received his B.Sc. and M.Sc. Degrees in Telecommunication Engineering from the University of the Basque Country (UPV/EHU, Spain) in 2003. He currently works as a part-time lecturer and full-time researcher in the Department of Electronics and Telecommunications at the Faculty of Engineering of Bilbao (UPV/EHU). He is also pursuing the Ph.D. degree in Telecommunication Engineering at the same University focused on access networks and security. His research interests include Computer Networks, Broadband Access Networks, Wireless Networks, Services Provisioning and Security.

EDUARDO JACOB (IEEE Member): After obtaining his BSc and MSc Degrees in Electric Engineering in 1987, he spent a few years as network manager in an architecture firm. Later, he worked as R&D project leader in Teletek (now Robotiker Tecnalia) in the field of Telecomm Engineering. He came back to the Faculty of Engineering of the University of the Basque Country in Bilbao where he received his Ph.D. degree in 2001. He is actually a professor at the same University and teaches degree courses on Mobile Networks & Services and Ph.D. courses on Cryptography in Communications and Security in Wireless Systems. He also is the head of the I2T Research Lab at his university where has directed several public and private R&D projects and acted as reviewer for projects and articles. His research interests are security in distributed systems and experimental platforms for network research. He has been appointed as ICT expert in the Advisory Council of the Basque Data Protection Agency and currently holds its Presidency.

MARINA AGUADO received her B.Sc. Degree as Telecommunication Engineer from University of the Basque Country (UPV/EHU) in 1992 and her M.Sc. in Management of Manufacturing Systems from Cranfield University, England, a year later. She concluded her European Ph.D. degree in Telecommunications Engineering in 2009. She worked as a trainee in Ford Motor Company, UK in 1993. From 1994 to 2003, she worked at the traffic control center in several railway companies in Brazil (CVRD, MRS Logistics & BrasilFerrovias), first as network support analyst, and finally, as R&D manager responsible for IT projects on railway operation. At present she works as Assistant Lecturer at ETSI (UPV/EHU) and researcher in the I2T (Engineering and Research on Telematics). Her current research lines are Broadband Wireless access technologies, Ethernet and Mobile WiMAX networks and handover related issues in the transportation scenario.

JASONE ASTORGA received her B.Sc. and M.Sc. Degrees in Telecommunication Engineering in 2004 from the University of the Basque Country (UPV/EHU). She received another M.Sc. in Information and Communication Systems in Wireless Networks in 2008, also from the UPV/EHU. Currently she is a Ph.D. student in the Department of Electronics and Telecommunications in the Faculty of Engineering of Bilbao in UPV/EHU, where she also works as a full-time researcher and part-time lecturer. Her research interests include networking, security in distributed environments and mobility management.

References

[1] Minolti, D., Johnson, P., and Minolti, E.,
Ethernet-Based Metro Area Networks. Planning and Designing the Provider Network,
McGraw-Hill, 2002.

[2] Kasim, A.,
Delivering Carrier Ethernet:
Extending Ethernet Beyond the LAN,
McGraw-Hill, 2008.

[3] Meddeb, A.,
“Why Ethernet WAN Transport?,”
IEEE Com. Magazine, November 2005, pp.136–141.

[4] Allan, D., Bragg, N., McGuire, A., and Reid, A.,
“Ethernet as Carrier Transport Infrastructure,”
IEEE Com. Magazine, February 2006, pp.134–140.

[5] Fedyk, D., and Allan, D.,
“Ethernet Data Plane Evolution for Provider Networks,”
IEEE Com. Magazine, March 2008, pp.84–89.

[6] Allan, D., Ashwood-Smith, P., Bragg, N., and Fedyk, D.,
“Provider Link State Bridging,”
IEEE Com. Magazine, September 2008, pp.110–117.

[7] IEEE Std. 802.1ag,
Virtual Bridged Local Area Networks –
Connectivity Fault Management, 2007.

[8] ITU-T Y.1731,
OAM functions and mechanisms for
Ethernet based networks, 2006.

[9] Click Project,
http://read.cs.ucla.edu/click/

[10] Matias, J., Jacob, E., Aguado, M., and Astorga, J.,
“Enhancing NGN’s Versatility for Multi-Service Support: the Bridging Virtualization Approach,”
The 10th International Conf. on Telecommunications, ConTEL 2009.

[11] MEF TS 6.1,
“Ethernet Services Definitions – Phase 2,”
Technical Specification, April 2008.

[12] Broadband Forum Technical Reports,
http://www.broadband-forum.org/technical/download

[13] Future Internet Assembly,
http://www.future-internet.eu/

[14] Bled Declaration,
http://www.future-internet.eu/fileadmin/documents/bled_documents/Bled_declaration.pdf

[15] IEEE Std. 802.1Q,
Virtual Bridged Local Area Networks, 2005.

[16] IEEE Std. 802.1ad,
Virtual Bridged Local Area Networks:
Provider Bridges, 2006.

[17] IEEE Std. 802.1ah,
Virtual Bridged Local Area Networks:
Provider Backbone Bridges, 2008.

[18] IEEE Std. 802.1D-2004,
MAC Bridges, 2004.

[19] IEEE 802.1Qay,
Virtual Bridged Local Area Networks: Amendment:
Provider Backbone Bridge Traffic Engineering, 2009.

[20] IEEE 802.1aq/D2.5,
Draft Standard, Shortest Path Bridging, 2010.

[21] IEEE Std. 802.1X-2004,
Port-Based Network Access Control, 2004.