NGN Platforms for Networked Service Delivery

D. Toelle[1], E. Areizaga[2], C. Sauer[3], C. Liss[4], T. Banniza[5], E. Jacob[6], F. Geilhardt[7]

[1] Fraunhofer Institute for Communication Systems ESK, Hansastrasse 32, 80686 Munich, Germany, E-Mail: dietmar.toelle@esk.fraunhofer.de

[2] Robotiker-Tecnalia, Zamudio, Spain, [3] Infineon Technologies, Munich, Germany, [4] University of Paderborn, Germany, [5] Alcatel-Lucent R&I, Stuttgart, Germany, [6] University of the Basque Country, Bilbao, Spain, [7] T-Systems, Berlin, Germany

Abstract. The network infrastructure within the Access and Aggregation domains of provider networks are subject to significant changes, both in technology as well as in their business model. Recently, a number of research initiatives, most notably MUSE and PlaNetS, have promoted the development of a unified broadband access and aggregation network platform. It is based on Ethernet and features various access technologies such as DSL, WiMAX, etc. End-to-end-communication is based on IPv6, and the communication procedures within the Ethernet domain ensures, that QoS is provided and maintained for the IP-layer. Important functions to ensure the IPv6-communication with the necessary QoS-properties are implemented autonomously, e.g. the extended IEEE 802.1X AAA and the resource admission and control functions (RACF).

Keywords: Ethernet-based Provider Networks, IPv6, Next Generation Networks, Service delivery, Unified Broadband Access Networks

1. Introduction

The deregulation of the telecommunication market and the resulting decline in prices will ultimately result in a paradigm shift of the Carrier's business model. All communication services, including speech, video, and data, will be shifted to a single unified network platform, which is based on IP. However, this requires an extended network architecture to support all the different services with heterogeneous requirements. This extended IP-based network architecture is called Next Generation Network (NGN).

An essential property of an NGN is the separation of the transport and service layer. The ultimate design objective for the transport layer is cost-efficiency. This can be achieved by establishing a unified transport platform based on packet switching technologies such as IP and Ethernet. In contrast, the service layer must be as flexible as possible to implement multiple heterogeneous services and combinations thereof fast and efficiently. Furthermore, existing services such as classical fixed/wired telephony must be integrated. In order to combine these two layers efficiently a signaling and control framework is necessary. Currently, the favored approach is the IP Multimedia Subsystem (IMS).

However, establishing a new network platform and shifting all the services to this unified, worldwide applicable and reachable platform will force the carriers and providers to modify their business models and their business roles. A key issue is the specification of emerging business roles and their related responsibilities. Another important issue is the specification and development of a unified transport platform and the required functional blocks within. There is the consensus that this transport platform is based on IP (global scale) and Ethernet (local scale). However, there are still severe shortcomings of these packet switched technologies, including Quality of Service (QoS), availability, scalability, and security, which must be overcome to use them for carrier-grade transport. Another issue is the adaptation of other networking equipment to be seamlessly integrated in this platform, e. g. mobile devices or home entertained equipment. The requirement for cost-efficiency also drives the development of autoconfiguration and self-management principles of the platform.

The objective of this paper is to present the contribution of the PlaNetS project to solve these problems. PlaNetS (Platforms for Networked Service Delivery [13]) is a Medea+ labeled European research project that covers future aggregation network architectures, network access solutions and appropriate access nodes, home (or residential) gateways, in-house networking solutions, and service-enabling network equipment and management integration. The developed network concepts and equipment prototypes are brought together in a large lab trial. The consortium gathers important European network operators, equipment vendors, and research institutions from Spain, the Netherlands and Germany.

2. Overview of NGN activities

Besides the IEEE, the Metro Ethernet Forum (MEF), the DSL-Forum, the ETSI, and the ITU-T are currently engaged in the specification of Ethernet-based provider networks. For this purpose, the different standard bodies and forums elaborate recommendations, which specify the general functional requirements to fit into the overall communication landscape. The most important recommendations are those of the ITU-T Y-series [8][9][10] and the ETSI TISPAN series [17][18]. Both the ITU-T and ETSI are specifying general reference models for future service networks to achieve traffic parameters as specified by the MEF [12] or by MUSE [1][7]. These so called Next Generation Networks (NGN) are based on packet switching (IP as convergence layer, Ethernet as general transport layer) as well as the IP Multimedia Subsystem (IMS) as global signaling and control layer. Fig. 1 depicts the general architecture of an NGN based on IMS. The European standardization body ETSI specifies a similar approach, which is called Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN) [17].

The IMS serves as a signaling and control framework, spanning multiple, heterogeneous domains. Carriers will use their own instances of IMS with the different IMS instances being interconnected via gateways.

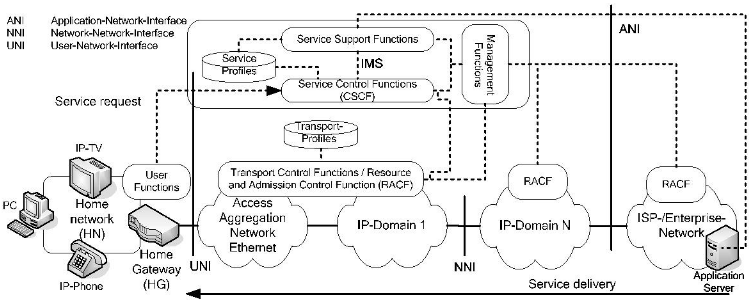

Fig. 1.: Basic IMS Architecture

The IMS provides a multitude of important service enabling functions. These comprise besides the user management (AAA functions) and the application management the complete signaling functions (based on an improved version of the Session Initiation Protocol (SIP), often in conjunction with associated protocols such as the Session Description Protocol (SDP)) as well as the resource and admission control requests (Resource and Admission Control Function (RACF [10][18])) across all involved domains.

Business Roles

Within one of the largest European research initiatives in IST FP6, MUSE [7], the business roles for the Access and Aggregation Networks (AAN) have been defined.

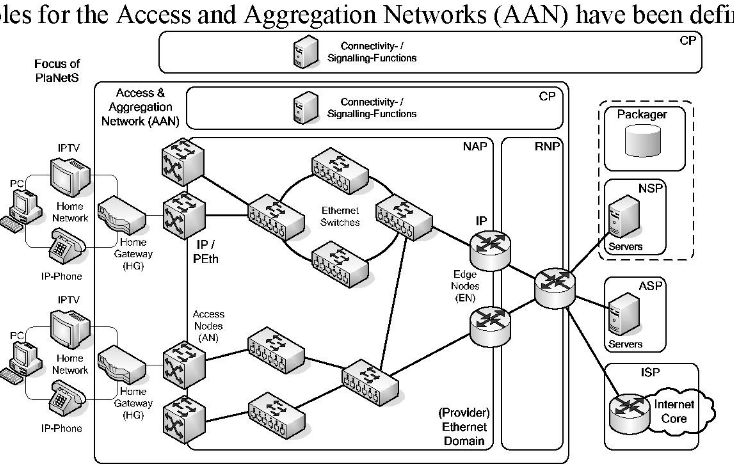

Fig. 2.: MUSE / PlaNetS architecture

Seven of these business roles were elaborated including concepts of how these collaborate in various network models. PlaNetS takes these concepts and develops concrete realizations thereof. However, PlaNetS focuses on the AAN domain as indicated in Fig. 2.

From the seven business roles the Network Access Provider / Regional Network Provider (NAP/RNP), Network Service Provider (NSP), Internet Service Provider (ISP), and Application Service Provider (ASP) are standard in current service network implementations. The other two roles, Packager and Connectivity Provider (CP), are new in the concept of converged service networks and key within the MUSE project. The Packager's role is mainly business-related and should be as technology-agnostic as possible. It directly collaborates with both the network / internet service providers and application service providers and defines and manages Service Level Agreements (SLA). The Packager links the applications with the required network services, effectively separating the applications from the network services. It maintains the Customer-profiles and is therefore involved in the AAA-procedures. The Packager may also interface with other Packagers and Connectivity Providers in order to provide "cross-domain" services. A Customer can be connected to several Service Providers simultaneously and therefore can have relationships with different Packagers.

The CP is responsible for realising the network connectivity and resource requests of the Packager. As such it must receive the required resources for the requested service and be able to identify the resources already used inside the involved network domains and take the appropriate measures to provide the corresponding technology-specific service bindings. While the Packager role is technology-agnostic, the CP role is technology-specific. The CP also takes responsibility for providing the necessary means for AAA and legal intercept. A CP may deal with multiple administrative network domains, e.g. combine one or more types of access network with a regional network in order to establish end-to-end-connectivity. Multiple CP per network domain should be possible, and multiple CPs must support interworking to cover larger networks. Another responsibility of the CP is the configuration of Customer's equipment using an Autoconfiguration Server (ACS) as well as the provisioning of network addresses.

Other research initiatives such as the German research project ScaleNet [16] pursue a similar approach, although the project main focus is based on IP rather than on Ethernet. While the main objective of the project is the unified access of mainly mobile technologies such as WLAN or UMTS using IP, the traffic aggregation is also based on Ethernet. An essential requirement for the aggregation network accrues from the mobility of the users: the organization of the Ethernet-based aggregation network must be flexible and dynamically reconfigurable. During the lab trial the PlaNetS network will be connected to the ScaleNet IMS (cf. Fig. 6).

3. The PlaNetS project

PlaNetS is a Medea+ project which contributes to the overall goal of providing cost-efficient broadband access to residential and business customers. The broadband access will be based on a converged network unifying the current heterogeneous networks. The unification also includes wireless access technologies. The converged network is centered around the Internet Protocol IPv6 and an end-to-end solution will be elaborated and tested during lab trials.

Within the Access and Aggregation Network (AAN) domain, Ethernet is the most promising, cost-efficient transport platform due to the efficient multiplexing capabilities, pricing for optical Ethernet interfaces, reuse of technology, and simplified interworking. For new first mile technologies such as VDSL and PON, Ethernet has been chosen as link layer. The challenge for this project is to evolve the standard Ethernet technology to a unified carrier-grade transport platform and provide interworking concepts with the IMS control layer and the service layer. An important aspect thereto is to develop solutions to shortcomings of Ethernet. This includes a supplement to the Ethernet-based prioritization in order to control the overall load within the network domain. This is especially important in conjunction with resilience, as the standard Ethernet solutions such as Spanning Trees do not support restoration with service survivability. Furthermore, AAA function must be implemented at the provider edge to cope with the shared nature of Ethernet and intelligent filtering mechanisms must be applied at the provider edge.

3.1 Overall Architecture and Features

The overall architecture used in the PlaNetS project is depicted in Fig. 2. In this paper the focus is on the center part of the architecture which is the Ethernet-based AAN domain. The business roles included in this domain are the NAP and the CP and might also include the RNP role depending on the geographical dimension of the domain. The essential requirement for this domain is the utilization of standard Ethernet components, either legacy Ethernet [3] or Provider-Bridged Ethernet [5][6]. It is assumed that customer service frames are entering and leaving the Ethernet domain through IPv6-nodes. Customers are attached to a certain class of network elements (NE), called Access Nodes (AN). These ANs are responsible for customer port access control and limitation of the number of MAC addresses the Ethernet domain has to handle, thereby solving the MAC scalability problems. The connection to the IP core network is done using Edge Nodes (EN), which are IP edge routers being involved in the routing process. The ANs are not involved in the routing, their IPv6 address prefixes are derived from the IPv6 EN prefix(es) through prefix delegation. These AN-EN pairs effectively form end-to-end traffic relations within the Ethernet domain. The traffic relationships between servers and customers are based on the IPv6 prefixes, which in turn are used to automatically determine the traffic relationship between AN and EN within the Ethernet domain. This procedure simplifies the configuration of the Ethernet domain, as the prefix delegation can be coupled to the automatic creation of AN-EN-bitpipes (explained below) within the Ethernet domain. The traffic classes within the Ethernet domain (802.1p) can be derived from the IPv6 Traffic Class. For PlaNetS – as well as for MUSE – four traffic classes are specified: LowLatency, RealTime, Elastic, Best Effort (2 inelastic, 2 elastic) Class [13]. The configuration effort is targeted to be as low as possible. The traffic handling within the Ethernet domain should be independent of the IP-layer and mainly self-configuring. This pushes the processing overhead towards the edges of the Ethernet domain, reducing the complexity of the Ethernet-based processing. The QoS maintenance problem within the Ethernet domain is tackled by automatically providing and supervising AN-EN-bitpipes and regulating access to these bitpipes. A RACF assigns spare bandwidth to these bitpipes. This enables the AN to perform the Network Admission Control (NAC) instantaneously on authentication and/or service requests. The bitpipe assignment is dynamic and rearranged, if necessary.

3.2 Components

DSL Access Node

The most crucial component of the Ethernet domain is the Access Node (AN) as it caters for the customer authentication and authorization (effectively it becomes a distributed BRAS) and keeps the processing required within the Ethernet domain as low as possible.

The PlaNetS AN is based on a revolutionary concept [11] that brings to the users access to "all services" and "all connectivity providers" in just one plug (in contrast to the current bundled model where the user is stuck to a wholesale provider). This independence from the providers is brought by the NAP.

The AN is mainly a combination of Port Functions (or functions per port) applied to every access line in combination with a simple Ethernet core that will aggregate the traffic and prepare it for its transport within the Ethernet domain.

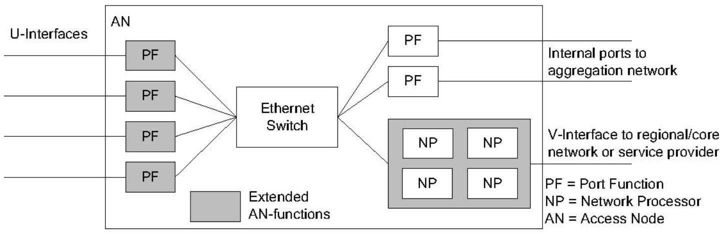

Fig. 3.: Access node architecture

A Port function (PF) implements different rules at the incoming and outgoing ports. At the incoming port PF is responsible to generate a new Ethernet header from the information stored in the forwarding tables. Basically, it is the generation of the suitable source and destination MAC addresses from the IP address source and destination addresses, as well as the QoS mapping from the header information. Additionally, it can implement some network layer functions, such as blocking outgoing packets based on simple routing information at the outgoing ports, preventing the flooding caused by the Ethernet Switch Core.

Basically, the PF blocks must implement the following features:

- It must segregate the first-mile (FM) from the aggregation network on layer 2, by implementing IP awareness during packet forwarding.
- PFs must establish connection between neighboring layer 2 segments, by the generation of new Ethernet frames based on the IP header information available.

Finding an Resource-efficient Hard- and Software Platform for Access Nodes

The focus of this challenging task is an easily programmable next-generation network processor platform that is tailored to the growing and persistently changing requirements of the access domain, composed modularly from both commodity modules and performance optimized building blocks.

To achieve the required cost-efficiency an application-driven approach to the exploration of platform alternatives is followed that starts from reference implementations of the desired system function(s) such as the Media Proxy below and

Ethernet- or IPv4/6-based DSLAMs [14] on a generic and fully programmable multiprocessor platform. Fig. 4 depicts the exploration process.

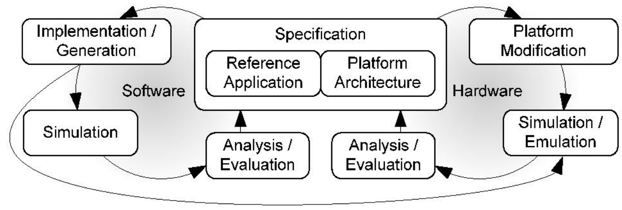

Fig. 4.: Hardware-software design space exploration process

Starting points are the specifications of the reference application on the software side and the specification of the generic multiprocessor on the hardware side. These specifications are independent, therefore requiring an explicit mapping of the reference application to the resulting platform. In the explicit mapping step application code that can be executed using the platform is generated. In this step, constructs that ease the mapping may be added as well, either as hardware-dependent software or as hardware building blocks. The resulting system can be executed using simulators or a rapid prototyping system and its performance can be analyzed. Results may be used to optimize the platform architecture or the mapping of the application onto it or both aspects. Application-specific platform optimization includes hardware accelerators for compute-intense tasks, application-specific instruction set extensions, memory layout and hierarchy, and chip- and board-level communication schemes.

In the PlaNetS project, the University of Paderborn and Infineon Technologies develop the Network-Optimized Versatile Architecture (NOVA) platform based on this approach [15]. The first prototype implemented on the RAPTOR2000 rapid prototyping system demonstrates a compact DSLAM with support for QoS.

WiMAX Radio Access Network in an IMS controlled NGN Environment

Network convergence enables cost saving synergies for operators, suppliers and end users while offering a unified service availability and quality if a suitable overall network architecture can be implemented. This asks for a generic approach in the definition of the interface functions between access networks and the service provision environment in the core. For the analysis of this interface, the WiMAX access technology was chosen as a prototype for a QoS controlled access network, which allows handling all interface aspects such as service / subscriber initiated QoS provision and supervision or mobility. As this project aims for convergence in service provision, focus of analysis will not be on WiMAX specific solutions, but the solutions and concepts found shall be adaptable also to other existing and upcoming access technologies. This will open an opportunity for service providers to reach subscribers in a multitude of access networks with a single service provision environment.

The work is split in two parts: the first one deals with the analysis and specification of needed functions at the interface towards the core network, the other one deals with the prototypical realization of a specific interface element, the Media Proxy part of a Border Gateway.

As already outlined in section 2, today there are two main bodies aiming for the definition of a coherent service provision environment: 3GPP defined the IP Multimedia Service (IMS) concept for the mobile access, whereas ETSI TISPAN set up their Next Generation Network (NGN) concept. Our analysis showed that the TISPAN concepts are best suited for the integration of WiMAX in IMS. The architecture proposed in PlaNetS offers a generic approach for integration of heterogeneous access technologies like WiMAX, public WiFi, DSL and UMTS. In this concept the IMS remains generic and access specifics are encapsulated in the lower TISPAN layers.

In general, Border Gateways are located at the border between two network domains. A Border Gateway separates different packet network domains on the transport layer while allowing applications to transit. To do this, a Border Gateway has to operate above the IP layer. It consists of 2 main blocks: the Signaling Part which terminates or relays signaling info, checks policies, controls and releases sessions with specified parameters and controls the Media Proxy, and the Media Proxy which classifies incoming packets, performs address/port translation, polices media streams and can do further application specific media stream processing like e.g. transcoding.

Today, Border Gateways are located in the core part of telecom networks to separate networks of different operators. As in the future more and more services will rely on connections with assured QoS parameters, Border Gateways will also be needed in the access at or near the subscriber entry point (e.g. DSLAM or base station) to control and separate the traffic coming from the subscribers. This would increase drastically the number of Border Gateways. At this point, a split of the Border Gateway will ease this scalability issue: The Signaling Part can be located rather central and controls a large number of Media Proxies which will be distributed to the subscriber entry points, where they can effectively protect the network. Within the project PlaNetS, work on the prototypical realization of such a detached Media Proxy is carried out. Furthermore, it is planned to integrate this Media Proxy together with an existing Signaling Part into the PlaNetS lab trial.

3.3 Procedures

Authentication Procedures

In a generic manner, authentication procedures should assure that only authorized users properly identified can attach to the network. The mechanism most widely used for authentication in L2 networks is IEEE 802.1X [4]. The elements that constitute an 802.1X solution are the supplicant (CPE), the authenticator (AN) and the authentication server. The authentication server can be located in any part of the network and, more importantly, can also act as a proxy on behalf of other servers.

In PlaNetS, one duty of the access node is to permit users and applications running over terminal equipments, in their respective local area networks, getting into the aggregation network.

IEEE 802.1X was designed to attach equipment to the network and get only a single service: L2 connectivity. The PlaNetS solution is much more complex. It is a multi service provider setup (cf. Fig. 5).

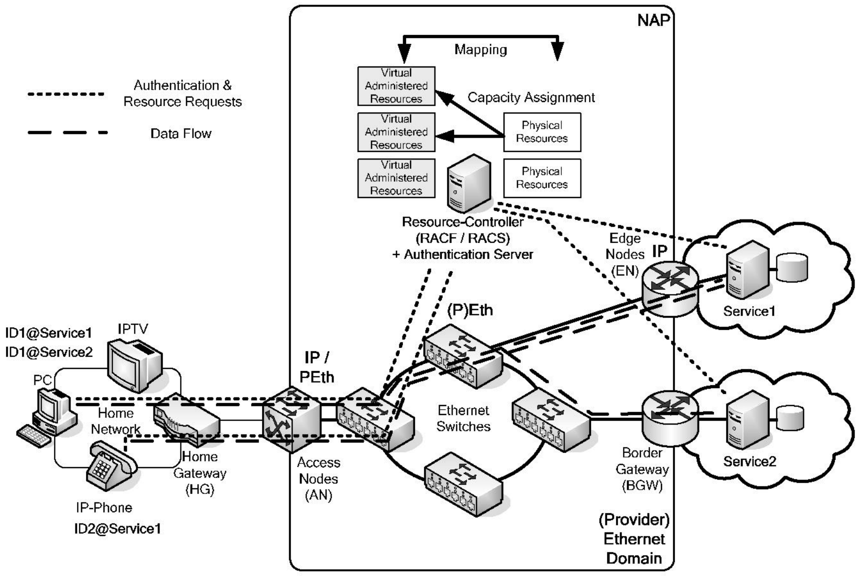

Fig. 5.: PlaNetS AAA and RACS procedures

Adapting IEEE 802.1X to this scenario necessitates several changes: it has to be modified to be able to support nested authentications. In first place authentication is necessary for using the access network (with some specific credentials), and later at the service level (with further credentials). An authentication server is used for the access network authentication which will, in turn, act as a proxy for each service provider authentication server. This gives the possibility to keep the connection to the access network blocked until getting the service level authentication. As a consequence of being able to subscribe the same user to several services, there must be a way to tag the different data flows from the same user to send them to the appropriate border gateway. This tag is a mix of MAC/IP addresses and VLAN IDs.

The third aspect of the adaptation deals with the fact that in the IEEE 802.1X specification only a single authentication process is run for each user. In PlaNetS, as a user can be subscribed to and access several service providers at the same time, several authentication processes will have to run at the same time.

Resource Admission and Control Function (RACF)

The RACF, as depicted in Fig. 5, is located on the same server as the authentication server for IEEE 802.1X. The server also processes the service requests and the related resource request.

The main function of the resource controller is the establishment and maintenance of virtual resources, called bitpipes. The capacity of the virtual resources is taken from the pool of physical resources within the Ethernet domain. It is important that the deactivated resources due to the Spanning Trees are considered only for restoration purposes. Capacity assignment is performed such that one network failure can occur without service interruption due to potentially resulting overload. Several capacity assignment schemes have been evaluated. In conjunction with the IPv6 prefix delegation and the processing mechanisms in the ANs and ENs the virtual resources are end-to-end bitpipes between each AN-EN pair. Each AN maintains a bitpipe to every EN within the domain and can perform Network Admission Control (NAC). A service request is admitted if and only if there is enough capacity left in the involved bitpipe. Otherwise the request is rejected or remapped to a lower traffic class. The resource controller actively monitors the utilization of the individual bitpipes and dynamically reassigns capacities.

3.4 Lab Trial

Within the project PlaNetS a demonstrator will be realized and integrated at the T-Systems location in Berlin (Germany) as proof of concept. The PlaNetS demonstrator will be integrated as an extension of the MUSE trial but the PlaNetS part supports triple-play services with end-to-end IPv6 connectivity. So it is possible to show an IPv6 implementation additional to the MUSE IPv4 trial set-up.

The PlaNetS demonstrator will be realized with innovative prototype equipment which has been developed in PlaNetS including IPv6 Home Gateways provided by partner Stollmann, IPv6 aware VDSL2 Access Node (Robotiker and University of the Basque Country (AAA)), a purely Ethernet-based Aggregation Network with a Resource Admission and Control Function (RACF) provided by partner Fraunhofer ESK and a Border Gateway (BGW), provided by Alcatel-Lucent, supporting conversational services. In addition some advanced Home Network solutions will be integrated as well. The Fig. 6 shows the planned demonstrator setup including the interworking with the projects MUSE, MUPBED and ScaleNet.

A co-operation with ScaleNet provides an IMS overlay to support RACF and IMS services. The MUSE subproject B labs in Berlin and Huesca (Spain) are interconnected via Ethernet/IPv4 link provided by the research network of the IST project MUPBED.

The PlaNetS demonstrator covers the Home Network (HN) and Access & Aggregation Network (AAN) including the First Mile. Two HNs can be demonstrated in Berlin with typical terminal equipment. Each HN has access to the ‘Public Network’ via the Home Gateway (HG) with IPv6 protocol stack. The First Mile is based on VDSL2 links over telco copper cables. The AN will be operated in the MUSE IP forwarding mode with IPv6 stack. The AAN will be realized with Linux PCs running the Click Modular Router (CMR). The modules of the CMR have been modified and new modules have been added. The network performs Network Admission Control (NAC) by checking the required resources of a new requested service against the spare resources in the network. The BGW upgrades the MUSE demonstrator and allows SIP-applications to open communication paths across the network border.

Different use cases will be demonstrated to show the advanced features of the prototype technologies developed in PlaNetS including triple-play with IPv6 and Click-to-IMS services (IMS controlled services and IMS based session handover). A VPN service demo shows that also business services can be provided by the PlaNetS network. A test suite has been described that lists the main features to be tested in order to validate the PlaNetS prototype equipment and the network architecture. The test suite considers the functional blocks QoS, management, end-to-end connectivity and security.

The PlaNetS demonstrator will be set up in Q2/2007 and the test phase will be finished end of 2007. Detailed evaluation results are subject for further studies.

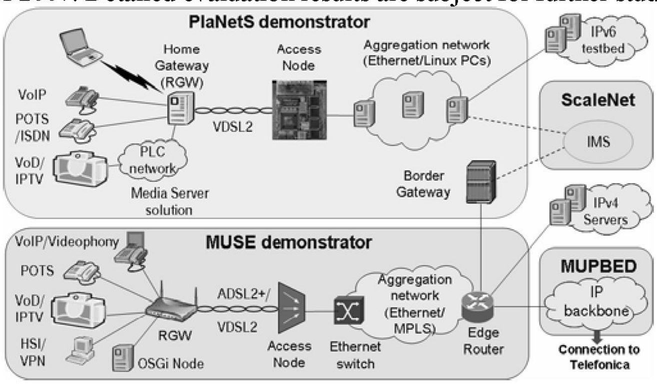

Fig. 6.: PlaNetS Lab Trial setup

As results we expect a significant improvement to the single provided mass market service, the internet access with best effort quality. PlaNetS focuses on a cost optimized broadband access solution based on VDSL2, Ethernet and IPv6 technologies enabling higher broadband coverage and higher data rates. PlaNetS specifies a solution for guaranteed QoS on demand for different IP flows on the basis of a resource management with RACS functionality embedded in an IMS overlay. Such an implantation allows a faster service provisioning and enables new multimedia service bundles by a higher level of service differentiation.

4. Summary and Conclusions

This paper describes the Medea+ research project NGN PlaNetS which develops a unified access and aggregation network platform for service delivery. The project is closely related to the IST FP6 research project MUSE (Multi Service Access Everywhere), which provides the overall framework for the networking scenario by specifying business roles. PlaNetS focuses on the home, access and aggregation parts of this networking scenario and develops the IPv6 scenario, in contrast to the IPv4 scenario being developed in MUSE.

The central part of the work is based on the specification of a purely Ethernet-based access and aggregation network domain. The procedures specified for the Ethernet domain are designed such that the autonomous communication principles of Ethernet are maintained, hence, preserving the advantages of Ethernet such as cost-efficiency and low management complexity. Important procedures are the AAA procedures based on an extended version of IEEE 802.1X, allowing multiple parallel authentications to multiple service providers, and the RACF to perform Network Admission Control (NAC) in conjunction with the AAA procedures.

During the project, the developed principles and procedures will be implemented in prototype equipment and tested in a lab trial. The Access Node will play an essential role in this network scenario. While not covered in this paper, the equipment inside the home network is also important for the end-to-end provisioning of QoS-services. This equipment will also be integrated in the lab trial.

Acknowledgements

The authors would like to thank Susanne Baumer[1], Manuela Freese-Wagner[1], Arnold Plankl[1], and Dinh Khoi Le[4] for their valuable contributions. PlaNetS is partially funded by the German Ministry for Education and Science (BMBF, Project 01AK065D) and the Spanish Ministry for Industry, Tourist, and Commerce (Project FIT-330220-2005-111).

References

[1] A. J. Elizondo, et al., "Access network architecture III", T F1.6, MUSE Project Documentation, November 2006.
[2] DSL-Forum, "Migration to Ethernet-Based DSL Aggregation", TR-101, 2006.
[3] IEEE, "IEEE Standard for Local and metropolitan area networks: Virtual Bridges Local Area Networks", IEEE Std. 802.1Q-2005, 2005.
[4] IEEE, "IEEE Standard for Local and metropolitan area networks: Port-Based Network Access Control", IEEE Std. 802.1X-2004, 2004.
[5] IEEE, "Virtual Bridges Local Area Networks, Amendment 4: Provider Bridges", IEEE Std. 802.1AD-2005, 2005.
[6] IEEE, "Virtual Bridges Local Area Networks, Amendment 6: Provider Backbone Bridges", IEEE Draft Std. 802.1AH-D3.3, 2006.
[7] IST-FP6 Project Homepage, http://www.ist-muse.org.
[8] ITU-T Recommendation Y.2011, "General principles and general reference model for next generation networks", October 2004.
[9] ITU-T Recommendation Y.2012, "Functional requirements and architecture of NGN", September 2006.
[10] ITU-T Recommendation Y.2111, "Resource and admission control functions in Next Generation Networks", September 2006.
[11] Cs. Lukovszki, et al., "Revolutionary IPv6 optimized access solution", NOC 2006.
[12] MEF TS 10.1, "Ethernet Services Attributes Phase 2", Technical Specification, November 2006.
[13] PlaNetS Project Homepage, http://www.medea-planets.eu.
[14] C. Sauer, et al. "Application-driven development of concurrent packet processing platforms", IEEE PARELEC 2006, Bialystok, Poland, September 2006.
[15] C. Sauer, M. Gries, S. Dirk, "Modularity and Programmability of the NOVA Packet Processing Platform", DATE 2007, Nice, France, April 2007.
[16] ScaleNet Project Homepage, http://www.scalenet.de.
[17] TISPAN, "NGN Functional Architecture: Rel. 1", ETSI ES 282 001, August 2005.
[18] TISPAN, "Resource and Admission Control Subsystem: Functional Architecture", ETSI ES 282 003, June 2006.