EFFICIENT PORT-BASED NETWORK ACCESS CONTROL FOR IP DSLAMS IN ETHERNET-BASED FIXED ACCESS NETWORKS

Daniel Duchow[+], Thomas Bahls[*], Dirk Timmermann[+], Stephan Kubisch[+], Harald Widiger[+]

[+] Institute of Applied Microelectronics and Computer Engineering
University of Rostock, 18051 Rostock, Germany
Tel: ++49 381 498-7276, Fax: ++49 381 498-7252
daniel.duchow@uni-rostock.de

[*] Siemens AG Communications, 17489 Greifswald, Germany
thomas.bahls@siemens.com

Keywords: Access Network, IP DSLAM, IEEE 802.1X, Authentication, Authorization

Abstract

This paper focuses on establishment of new authentication and authorization mechanisms in Ethernet-based fixed Access Networks. We provide approaches for an efficient usage of IEEE Standard 802.1X mechanisms in an Access Network environment for authentication and authorization purposes. We explain how 802.1X Authenticator functionality can be integrated in different Access Network systems such as IP DSLAMs and discuss pros and cons of several approaches that we analyzed. Our main goal is to specify a cost-effective system design by strictly complying with the 802.1X standard on Access Network edges. We describe a design approach of a distributed 802.1X Authenticator which is divided into two parts, implemented on different DSLAM system modules, and extended by an Access Controller. Furthermore, we explain necessary extensions for interworking of the new distributed 802.1X Authenticator parts which also offers solutions for further problems in the range of fixed broadband Access Networks.

1 Introduction

The support of new services like IP multicast in fixed broadband Access Networks [4] requires a functional redesign of these networks compared to the traditional Point-to-Point (PPP) access architecture [3]. In this case, one of the main aspects is customer authentication and authorization. We provide a new functional approach for authentication and authorization, which is based on a distributed 802.1X mechanism, in new structured Access Networks. In most cases, customers are connected via PPP to Broadband Remote Access Server (BRAS) or Broadband Network Gateway (BNG) [3] respectively of their Internet Service Provider in today's ATM- and Ethernet-based Access Networks. PPP provides IP layer connectivity for customer premises equipment (CPE) and is used for customer authentication purpose. However, this PPP channel forces a non-flexible network structure and prevents the necessary mapping of IP and Ethernet layer address information. Thus, an efficient IP multicast service is not supported in a scenario as shown in Figure 1. If IPv6 is adopted this problem will be intensified, because IPv6 intensively uses multicast communication. Removing PPP solves this problem. However, customer authentication and authorization have to be performed by another sophisticated procedure like IEEE 802.1X. Furthermore, ATM is substituted by Ethernet more and more in the field of Access Networks. For this reason, we have developed an 802.1X-based design approach for customer authentication and authorization by meeting all requirements of Ethernet-based Access Networks. The structure and the system design of Ethernet-based Access Network systems require an effective functional solution for each new implementation. Systems and modules, e.g., line cards of a Digital Subscriber Line Access Multiplexer (DSLAM),

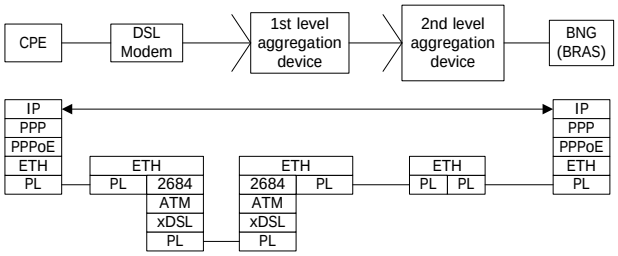

Figure 1: Typical Configuration of Ethernet-based Access Network with PPP Layer

which are non-centrally located, are often very cost-sensitive devices. Thus, this analysis suggests locations and devices on DSLAM module level where the new decomposed authentication functionality should be placed. Advantages and drawbacks of several options are discussed, demonstrating necessity, benefit, and feasibility of distributed port-based network access control.

The remainder of this paper is organized as follows. In 2, we give a brief overview of IEEE 802.1X with the main conditions that are significant for our solution. Section 3 describes the design approaches for a cost-effective port-based network access control implementation for IP DSLAMs, the new distributed 802.1X Authenticator parts for a decomposed 802.1X solution, and the communication extensions which are required for our favor design approach. We discuss advantages and solutions for further Access Network issues which are addressed by our approaches, too, in Section 4. Finally, the paper is summarized and concluded in Section 5.

2 Port-based Network Access Control in Ethernet Networks

The Ethernet layer has direct access to the IP layer and vice versa by removing the PPP layer in the entire Access Network. Authentication based on the IEEE Standard 802.1X [6] is well suitable in such a network structure, because 802.1X is designed for 802 media, e.g., 802.3 Ethernet.

A Supplicant port, i.e., a port of customer equipment, is authenticated and authorized by an 802.1X Authenticator. The Authenticator is implemented on the switching system the Supplicant port is directly connected to. 802.1X necessarily requires a point-to-point port characteristic. The Authenticator typically relays Extensible Authentication Protocol (EAP) messages between the Supplicant and a backend authentication server, using RADIUS [1] [2] or DIAMETER [5] as the authentication protocol, for example. The authentication server sends an *accept* message back to the Authenticator after the Supplicant was successfully authenticated. The Authenticator authorizes the controlled port. Figure 2 shows the network and system structure of this procedure.

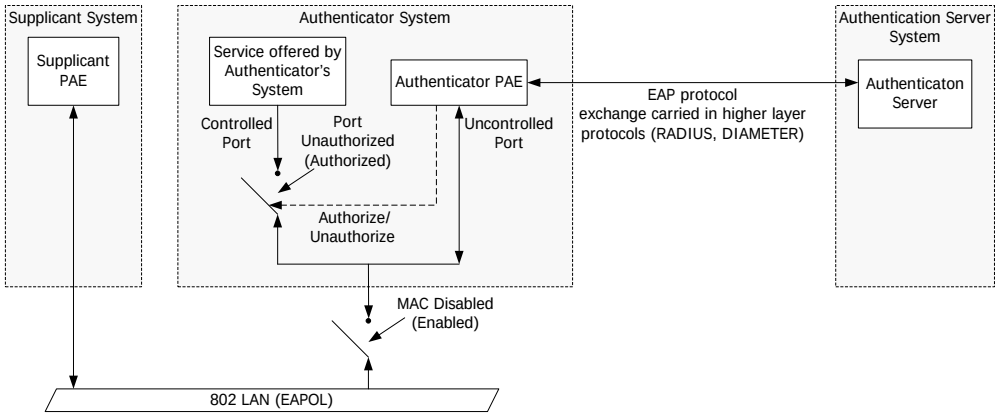

Figure 2: IEEE 802.1X System Architecture ©

802.1X provides a port-based network access control. Therefore, a port of Authenticator or Supplicant system respectively is authenticated and authorized. As a result, the use of 802.1X requires compliance with the following main conditions:

1. Both authenticated and the authenticating system have direct physical or logical point-to-point connection.
2. The authenticating system has a filter functionality to perform access control.
3. The authenticating system has a port controller functionality which can authorize and unauthorize a port (set the filter functionality).
4. The authenticating system has IP layer support for authentication server packet exchange.

In the next section, we explain how an 802.1X procedure can be integrated in an Access Network architecture.

3 Using 802.1X in an Access Network

3.1 Concept-Overview

A physical or logical point-to-point port connection characteristic is required by using 802.1X. Every 802.1X implementation must support this. Figure 3 exemplifies a cascaded network infrastructure with central and remote Ethernet DSLAM systems (generally known as IP DSLAMs) on first and second level of aggregation. A DSLAM consists of one

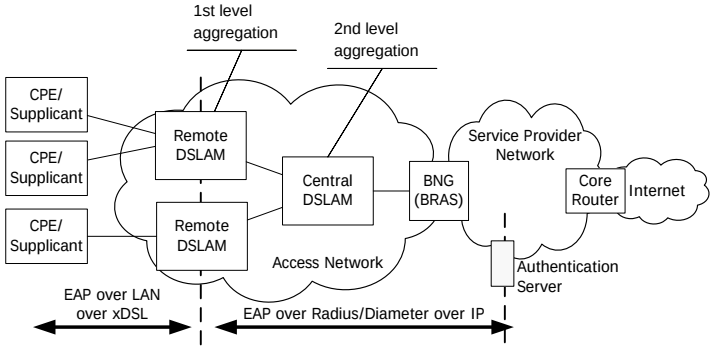

Figure 3: Access Network Architecture

central positioned Ethernet switching card and, e.g., 16 aggregation line cards as shown in Figure 4. The 802.1X Authenticator functionality can be implemented at the following positions in this system design:

Design Approach A: Authenticator implementation on every aggregation line card
The aggregation line cards have physical point-to-point connection characteristics to the ports of the Supplicant systems. The controlled ports are located on the aggregation line card itself. Thus, this is the natural implementation point for an 802.1X Authenticator compared to the functional structure of Figure 2. A complete Authenticator implementation is needed on every line card in the entire Access Network in this scenario.

Design Approach B: Authenticator implementation on Ethernet switching card of every DSLAM system
In this approach, an 802.1X Authenticator implementation on a DSLAM's Ethernet switching card provides a network access control service for every attached line card. Just a single implementation on each DSLAM is required. However, the controlled ports are still located on the aggregation line cards. For this reason, we extend the 802.1X procedure by a simple Access Controller on every line card. Additionally, information exchange by communication between the Access Controller on the line cards and the new Authenticator on the Ethernet switching card is essential. These extensions are responsible for keeping all requirements for a standard-like 802.1X implementation as mentioned in Section 2.

Design Approach C: Authenticator implementation on Ethernet switching card of the highest level aggregation DSLAM system

This solution extends design approach B. Only a single Authenticator functionality implementation which is placed on the Ethernet switching card of the highest level aggregation DSLAM system, this is the central DSLAM pointed out in Figure 3, is used for the entire Access Network. Implementation extensions, which are described in the second scenario, are also defined for this approach. But these implementation extensions result in higher complexity compared to scenario B. Communication between the Access Controller and the Authenticator part is not only intra-system communication in a DSLAM, but it can pass several layer 2 network devices.

3.2 Authenticator Implementation on each Aggregation Line Card

The aggregation line card has physical point-to-point connection characteristics to the port of the Supplicant system locating on customer's access device. The controlled port is located on the Authenticator system itself. This is the natural implementation point for an 802.1X Authenticator compared to the functional structure as shown in Figure 2. This approach meets the main requirement for an 802.1X implementation as mentioned in Section 2. In the system

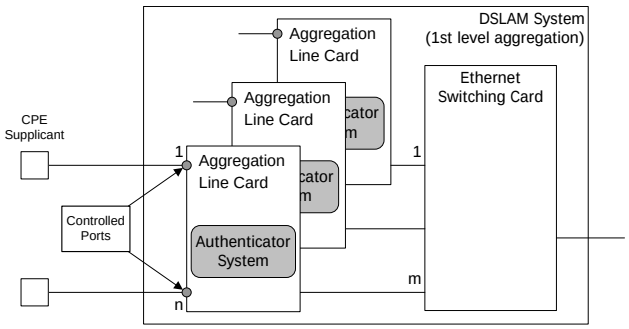

Figure 4: Design Approach A: 802.1X Low Level Aggregation Concept in Access Networks

design which is illustrated by Figure 4, the Authenticator exercises control on all line card ports directly. It performs access control, authorizes and unauthorizes the controlled ports, and has authentication message exchange with the authentication server. All these functionalities together require a lot of resources on every line card. For the most part, an 802.1X Authenticator implementation is a software application which requires CPU processing time or system cache and central memory, for example. However, aggregation line cards are very cost-sensitive devices. For that reason, a complete Authenticator functionality implementation at this non-central position does not seem to be a cost-effective solution. For this reason, we favor a distributed design approach.

3.3 Authenticator Implementation on Ethernet Switching Card of every DSLAM System

Ethernet switching cards are more centrally situated than aggregation line cards and, therefore, less cost-sensitive. All necessary resources such as memory or processing time can be concentrated at this centrally located system module and can be shared by all connected aggregation line cards. An 802.1X Authenticator implementation on Ethernet switching cards provides authentication and network access control service for all attached line cards. Just a single implementation on each DSLAM is needed. However, the controlled ports are still located on the aggregation line cards. For this reason, we extend the 802.1X functional model by an Access Controller on every line card and information exchange by communication between the line cards and the Ethernet switching card. These extensions are responsible for keeping all the requirements for a standard-like 802.1X implementation on network edges which were mentioned in Section 2. Figure 5 illustrates this approach. The Authenticator system itself does not have physical point-to-point connection characteristics to the port of the Supplicant system, which is located on customer's access device, but a physical n-to-1 relationship. With an additional communication between line cards and Ethernet switching card, a logical point-to-point connection characteristic is established. But it is insufficient to perform access control for a logical port correlation on the Authenticator system itself for a standard-like 802.1X implementation. Every data traffic coming from unauthorized Supplicants have to be blocked at the network entry. For this reason, a small function Access

Controller on the line card has a filter functionality for both up- and downlink direction. All necessary information is provided by the Authenticator to the Access Controller to control the line card ports and perform access control. The Access Controller opens the line card ports in case of positive authentication result, and otherwise it closes the ports. Only EAP over LAN (EAPOL) frames are allowed for forwarding from and to the Supplicant for an unauthorized port. A Supplicant port is unauthorized at the beginning of an authentication procedure. Either a Supplicant or the

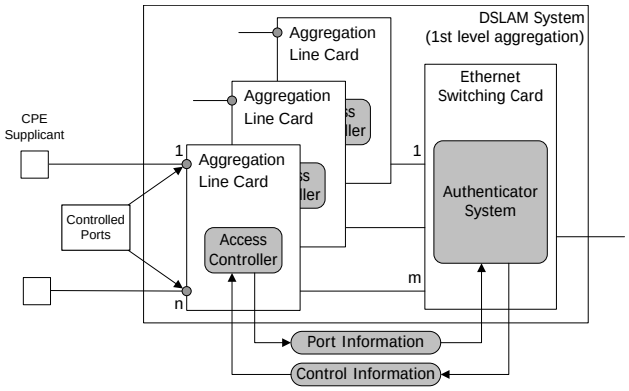

Figure 5: Design Approach B: 802.1X Medium Level Aggregation Concept in Access Networks

Authenticator initiates an authentication procedure. In both cases, the Access Controller recognizes the beginning of the authentication message exchange for a specific line card port and then sends an additional *port information* message to the Authenticator. Authentication is now processed by using an authentication protocol like RADIUS between Authenticator and authentication server. The Authenticator sends the outcome of the authentication process back to the Supplicant. This can be an *accept* or a *reject* message. Furthermore, Authenticator sends a *control information* message to the Access Controller. Thereby, the Access Controller can be explicitly set for a designated filter function to authorize or unauthorize a specific line card port. Due to the fact that the Access Controller and the Authenticator are parts of the same DSLAM system, only an in-band or intra-system communication is needed for the *port* and *control information* transmission. This can be achieved by existing in-band communication on the system management plan. However, a generic communication design with an independent layer 2 communication protocol, as pointed out in following sections, is a highly adequate solution. The decomposed design approach minimizes the functional complexity on cost-sensitive aggregation line cards compared to a full Authenticator implementation and concentrates main functionalities on the central Ethernet switching card. Usually, filter mechanisms already exist on line cards and have to be simply adjusted. Details about the new distributed Authenticator and communications design are described in more detail in following sections.

This scenario is especially qualified for Access Networks without remote DSLAM systems. Under these terms, design approach B represents a central and cost-effective solution. But also the usage in a network structure as shown in Figure 3 is adequate. Moreover, for such a cascaded network infrastructure with central and remote Ethernet DSLAM systems, a further centralization of the 802.1X Authenticator is possible. The next section describes this solution.

3.4 Authenticator Implementation on Ethernet Switching Card of the Highest Level Aggregation DSLAM

In a cascaded Ethernet-based Access Network design according to Figure 3, it is possible to implement only one 802.1X Authenticator functionality. This is the third option for an Authenticator implementation as illustrated in Figure 6. This solution extends the design approach B. Only a single Authenticator functionality implementation that is placed on the Ethernet switching card of the highest level aggregation DSLAM system is needed for the entire Access Network. Every aggregation line card performs access control for their controlled ports by using this new centralized Authenticator service of the central DSLAM. Implementation extensions that were described in the second scenario are also used by this approach. The Access Controller has the same capabilities and functionalities. Every line card comes with an Access Controller which controls the line card ports depended on the outcome of authentication process.

Communication between Access Controller and Authenticator establishes the necessary logical point-to-point port characteristic and is used to transmit *port* and *control information* messages. However, in contrast to design approach B, communication is not only intra-system communication in a DSLAM but can pass several layer 2 network devices between line cards of a remote system and the Ethernet switching card of the central DSLAM. For this purpose, we favor an independent layer 2 communication protocol which carries all required *port* and *control information* between layer 2 devices. A further description of this protocol follows in Subsection 3.6. Usually, remote DSLAMs connect

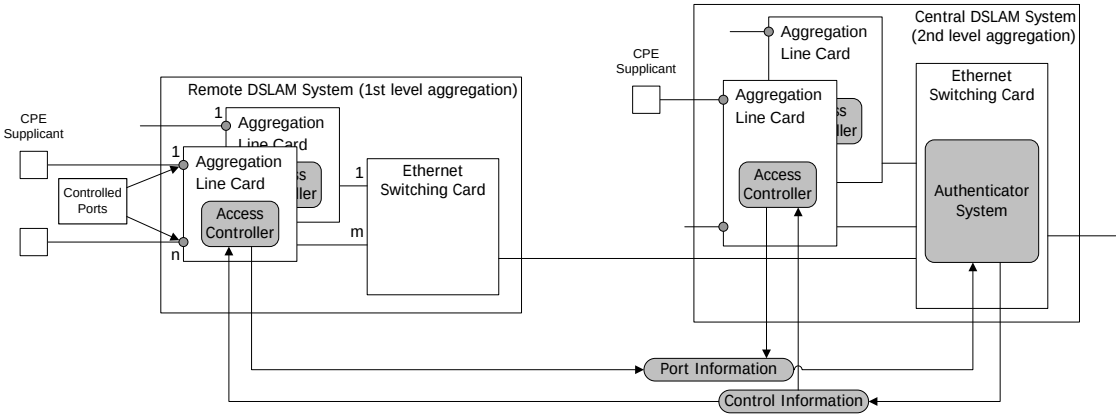

Figure 6: Design Approach C: 802.1X Highest Level Aggregation Concept in Access Networks

customers who are far located from the central office and, therefore, can not be directly attached to a central DSLAM. Because remote DSLAMs often consist of less line cards and, thus, have a smaller switching card, they have much less resources available than bigger central DSLAM systems. This solution relieves all remote DSLAMs from an Authenticator implementation in addition to the pros and cons of scenario B.

3.5 The New Distributed Authenticator Parts

An Authenticator system according to IEEE 802.1X [6] consists of the components and functional modules respectively controlled and uncontrolled ports, control mechanisms to authorize/unauthorize the controlled ports, access to service which is provided by the Authenticator, and all functionalities for authentication procedure purpose with Supplicant and authentication server. Our presented implementation approach divides these integral parts into two functional modules – the Access Controller module and the Authenticator module. The controlled port and its control mechanism are still implemented on the access device which is immediate connected to the Supplicant port. The new Access Controller comprises of these components. All other components are placed on a higher level aggregation system and form the new Authenticator. Figure 7 illustrates the decomposed functional result. A filter mechanism at the Access

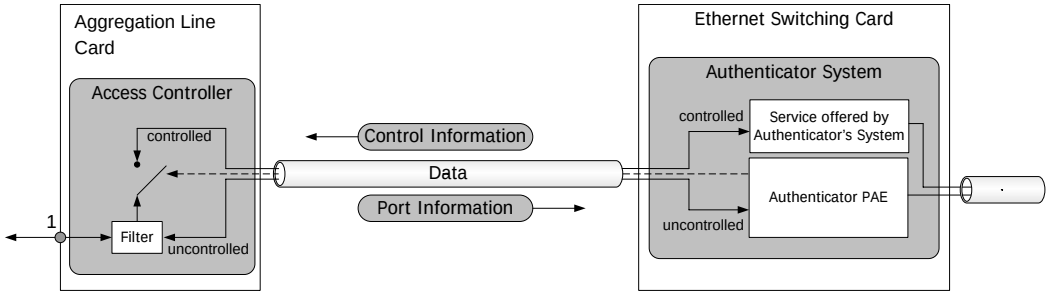

Figure 7: The new distributed Authenticator parts

Controller is responsible for logical creation of the controlled and uncontrolled ports. The uncontrolled port allows the uncontrolled exchange of exclusively EAPOL frames regardless of the authorization state. The controlled port

will allow the exchange of data frames, only if the port is authorized. The state of the controlled port is changed from unauthorized to authorized and vice versa regarding the transmitted *control information* from the Authenticator. If the controlled port is unauthorized, the Access Controller will silently discard all data frames sent by a customer on this port.

3.6 Communication Extensions

There are two principal reasons for communication extensions for the described solutions. First of all, no point-to-point port characteristic does exist on an Ethernet switching card. Therefore, a *port information* has to be transmitted in uplink direction. Secondly, the Authenticator has to provide a *control information* to the Access Controller which has to be transmitted in download direction from customers point of view. Two options are possible for the creation of a logical port relationship. The line card transmits a unique *port information* to the Ethernet switching card either by using a unique Virtual LAN (VLAN) Identifier (VID) per line card port or by creating of a unique Subscriber Port Identifier (SP-ID) regardless of the VLANs used.

If VIDs are used, no additional communication will be needed because VLAN tags are carried in Ethernet frames. But the use of per port VLANs only works on our second solution because VIDs are limited to a number of 4096. SP-IDs, which identify a line card port on a DSLAM uniquely in whole Access Network, better scale for both second and third solution. As an example, SP-IDs could be constructed by the set of DSLAM identifier, line card identifier, and line card port number.

Intra-system communication, on the system management plane, for example, can be used to transmit both *port* and *control information*. But this only works on the second scenario. Another option uses an independent communication protocol as a generic solution for all communication purposes in Access Networks. Only an inter-system communication across several layer 2 devices enables design approach C. Further, VID-based *port information* is no longer usable for the third solution.

A generic communication protocol to transmit the relevant *port* and *control information* between Access Controller and Authenticator in the first step can be specified as a connectionless layer 2 protocol as well as EAPOL with simple request and reply messages. This will minimize the complexity of protocol entities on the line cards and the Ethernet switching card. A fixed protocol structure might offer an optimized protocol implementation on the line cards. A Field Programmable Gate Array (FPGA) based hardware implementation of the line card protocol entity is possible, too. A new single Ethernet type value and a dedicated Ethernet multicast group address are useful for easy protocol frame recognition in the data stream. Up to now, no design and development has been done which considers additional constraints in Access Networks for such a solution. In a further step, we will work on a protocol specification for an "Access Control and Information Protocol".

4 Advantages and Solutions for further Access Network Issues

Other relevant issues in the field of Access Networks could be solved or optimized by using parts of the described mechanisms. A DHCP relay agent is often mandatory on new IP DSLAMs [3]. In this context, the transmission of a subscriber port identifier in the relay agent information option of DHCP (option 82) is mandatory. This identifier is the same like SP-ID using in our description. Thus, it is possible to implement a DHCP relay agent also on a higher level aggregation DSLAM by still having access to this subscriber port identifier.

IP DSLAMs currently offer multicast traffic handling by IGMP snooping for a number of groups without customer-based authentication or authorization mechanisms. For a port and multicast group address based multicast traffic authorization, a similar solution like the described port-based network access control approach can be used. If multicast traffic is dynamically restricted for line card ports, a multicast authentication service on the Ethernet switching card, for instance, has to be implemented. The multicast authentication service then has to control the customer authorization on the line cards, because the line cards are the final distribution and replication point for downlink multicast traffic. In this exemplified scenario, the Access Controller can be further extended and used for this purpose as well. The multicast authentication service can also be located outside the line cards.

5 Conclusions

All three design approaches presented are basically well suited to replace the PPP customer authentication model in an Access Network environment and to comply with the authentication and authorization concept according to IEEE 802.1X at the same time. Although the proposed concept A with a full Authenticator implementation on aggregation line cards is a strict standard-like solution, it drops out because of its too high demand on system resources on each line card. The pointed out necessary implementation extensions for concept B and C consist of a filter and port control mechanism within the Access Controller and an information exchange by communication between line cards and Ethernet switching card. With these extensions, a standard-like 802.1X implementation on network edges is achieved. In contrast to scenario A, these implementation extensions are insignificant additional expenses to have a solution with a distributed Authenticator implementation on line cards and Ethernet switching card that is described in concept B and concept C. The division of the original Authenticator into the two functional modules relocates the resource-intensive parts of the Authenticator on the central Ethernet switching card and, thereby, materially relieves the aggregation line cards from these tasks. The simple designed Access Controller is placed on the line cards. It merely transmits the *port information* to the Authenticator part on the Ethernet switching card and opens and closes its logical controlled ports dependent on the *control information* which are received from the Authenticator. The main part of the 802.1X Authenticator on the Ethernet switching card provides an authentication service for the line cards and takes over all authentication and authorization tasks including communication with the authentication server. Connection to and usage of existing AAA (Authentication, Authorization, and Accounting) service provider infrastructures can be set up without significant restrictions. All involved protocol operations are specified and standardized within authentication protocols, for example, RADIUS (client, server, relay). Thereby, an authentication server can be updated to handle 802.1X authentication. Further, many Supplicant implementations nowadays exist for different operating systems of customer equipment. These facts additionally support a port-based network access control application.

Furthermore, existing DHCP procedures will enable a new concept for customer network equipment autoconfiguration, if PPP is no longer supported for network access. New IP DSLAMs normally feature DHCP relay agents. So they are ready for providing DHCP services for the customers. The communication extensions into design approach B and C can be implemented by a separate layer 2 communication protocol.

A new “Access Control and Information Protocol” will provide message exchange between functional modules on different systems. It will be able to carry all information needed to be transmitted in the field of Ethernet-based Access Networks like *port* and *control information* for 802.1X authentication purpose. This generic protocol will additionally enable the implementation of other services, for example, a dynamically configuration of several multicast group addresses for each line card port. Then, a multicast service controller on the line cards will be able to grant or deny access to specific multicast traffic streams per customer port. In the course of protocol development, such extensions will be integrated. In field of Access Networks, many other applications and features are possible.

This work is done in cooperation with Siemens AG Communications, Greifswald, Germany.

References

[1] B. Aboba and P. Calhoun. RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP). RFC 3579 (Informational), Sept. 2003.

[2] P. Congdon, B. Aboba, A. Smith, G. Zorn, and J. Roese. IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines. RFC 3580 (Informational), Sept. 2003.

[3] DSL Forum. Migration to ethernet-based dsl aggregation. WT-101 Rev 10.1, Feb. 2006.

[4] D. Duchow, T. Bahls, and D. Timmermann. Enabling multicasting for access networks. In *Proceedings of 15th IEE International Symposium on Services and Local Access (ISSLS 2004) on CD-ROM*, Edinburgh, Mar. 2004.

[5] P. Eronen, T. Hiller, and G. Zorn. Diameter Extensible Authentication Protocol (EAP) Application. RFC 4072 (Proposed Standard), Aug. 2005.

[6] IEEE Std 802.1X^{TM}-2004, IEEE Standards for Local and Metropolitan Area Networks—Port Based Network Access Control.