ACIP: An Access Control and Information Protocol for Ethernet-based Broadband Access Networks

Daniel Duchow* and Dirk Timmermann
University of Rostock, 18051 Rostock, Germany
Tel/Fax: ++49 381 498-7276/52
{daniel.duchow, dirk.timmermann}@uni-rostock.de

Thomas Bahls
Siemens AG Communications
17489 Greifswald, Germany
thomas.bahls@siemens.com

Abstract

Ethernet-based broadband access network nodes like an IP DSLAM are required to provide many new Ethernet/IP-based features for, e.g., end user device autoconfiguration by DHCP, authentication and authorization based on IEEE 802.1X, and multicast distribution. At control plane, a lot of information exchange is needed to configure, administer, and control these features and services. Cost-effective access network and system structures highly depend on an efficient and optimized feature positioning. ACIP is a new Access Control and Information Protocol which enables optimized, cost-effective functional decomposition of features without loosing feature options and supports optimized feature positioning. It provides transport of configuration and control information in Ethernet networks, e.g., for providing DSL line identification used for DHCP relay agent option 82 to centralized systems and for transmitting control information to remotely control DSL user ports by a centralized 802.1X authentication mechanism. ACIP is designed for being as simple as possible and open for new extensions to provide future network control functions.

Preferred Topic Areas: 4b – network topology design and optimization at different layers

1. Background

In the last few years, a functional redesign of access network topology and system structure from Asynchronous Transfer Mode (ATM)-based to Ethernet-based network technologies has taken place. In context of the development of IP Digital Subscriber Line Access Multiplexer (DSLAM), based on layer 2 switching technology and some additional Ethernet/IP-based features, pure layer 2 access networks are originated. Figure 1 illustrates cascaded access network architecture and points out systems and modules involved. Support of Quality/Class of Service (QoS/CoS) [1][3], end user network interface card autoconfiguration based on Dynamic Host Configuration Protocol (DHCP) [6][2][3], and port-based network access control with IEEE 802.1X [5][4] are examples of these additional features. These functionalities have to be placed on DSLAMs line cards to completely perform all tasks in a standards-compliant way. The DSL user ports, which have to be controlled within authentication and authorization process, are directly located at the line cards. A DHCP relay agent is required to provide a DSL line identification sequence (referenced as port-ID in the following) within DHCP option 82 [6] – relay agent information option – to DHCP server. This port-ID is only available on the line card itself without additional means. And user-specific QoS/CoS parameter must be interpreted from line cards, e.g., for a priority-based handling of user traffic. In contrast to centrally located Ethernet switching cards (called central card in the following), line cards of a DSLAM are highly cost-sensitive modules and make fewer resources available. Line cards usually provide for hardware-based implementations. However, some of the additional features of IP DSLAMs have high functional complexity and cannot be implemented as pure hardware solutions. These applications would functionally overload the cost-sensitive line cards. Thus, functions must be implemented at a central and highly aggregated position, i.e. the central card of a DSLAM. The processing capacity of the less cost-sensitive central card usually provides for these functional implementations.

If a central card will perform the function of a DHCP relay agent with option 82, it will need the unique port-ID for a DSL user which is available for every DSL access loop on the line card. E.g., the user to port-ID correlation on a central card can be uniquely extracted by using of 1:1 Virtual Local Area Network (VLAN) assignment for all DSL ports. But 1:1 VLAN solution might not be suitable for all scenarios which use no or other VLAN assignment, or it might be not efficient enough with regards to traffic distribution such as multicast support. To have a VLAN-independent solution, the port-ID must be extracted by another method.

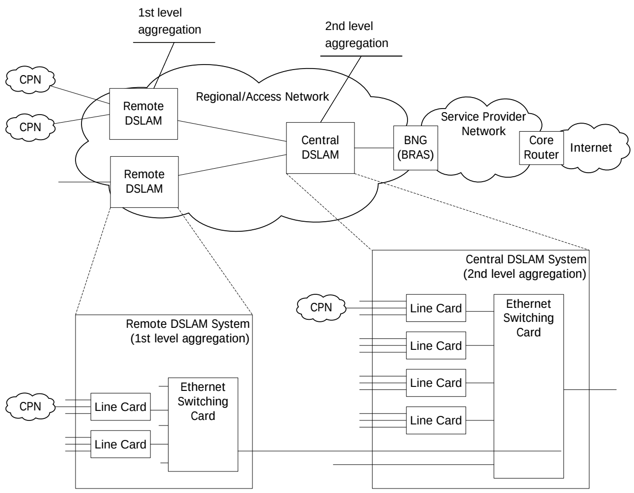

Figure 1. Cascaded Access Network

General requirements and procedures for DHCP relay agent processing on DSLAM level are described in [2] and [3], but no standardized solution for the port-ID problem on central card or DSLAM module level is given.

With port-based network access control according to IEEE 802.1X, an 802.1X authenticator and a RADIUS client perform port-based user authentication and authorization. The controlled port is located on the authenticator system itself. The line card has physical point-to-point connection characteristics to the port of the 802.1X supplicant system locating on customer's access device. A line card is the natural implementation point for an 802.1X authenticator and RADIUS client compared to the standard. However, implementing these functions at this non-central position is not a cost-effective solution. Functions would be implemented multiple times on the same DSLAM. If a central card is performing these functions, DSL line identification information on the central card of a DSLAM is required. Such an authentication procedure is described in [4]. The authenticator at the central card uses the port-ID to control (authorize/unauthorize) a DSL user port at the line card in the same or a remote system. Therefore, the authenticator must be able to communicate with all line cards.

These examples illustrate that based on the redesign of access network and systems additional control and communication features are needed. Therefore, we provide a solution for Ethernet-based communication between system modules within an access network – the *Access Control and Information Protocol*.

The reminder of this paper is organized as follows. In Section 2, we give an introduction to ACIP. Section 3 describes the protocol architecture. We explain protocol operation of the ACIP base protocol in Section 4 and ACIP protocol extensions in Section 5. Finally, the paper is summarized and concluded in Section 6.

2. ACIP – Introduction

The new communication protocol – *ACIP* – carries information in a well-defined manner through the entire access network and through every Ethernet network. Between systems or system modules where ACIP protocol entities are implemented, ACIP distributes the information by using several messages and attribute value pairs (AVP). The kind of information carried or its purpose is defined by specific ACIP extensions. In general, these can be control information from a controller device, e.g. a central card, to a controlled device, e.g. a line card, or other configuration or management information. Because ACIP is based on Ethernet transport mechanism, it can be used in every Ethernet environment. Furthermore, ACIP is designed as an as-simple-as-possible and extensible protocol.

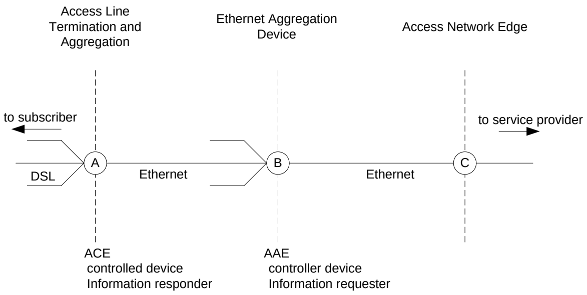

Figure 2. ACIP Generic Network Model

ACIP consists of an ACIP Client Entity (ACE) and an ACIP Agent Entity (AAE). However, ACIP is not designed being a pure client-server protocol because both ACE and AAE can initiate a protocol exchange. ACE and AAE can be installed on any Ethernet-capable network system within an Ethernet broadcast domain. Figure 2 shows a generic installation and usage model for ACIP where ACE and AAE are installed on two different neighboring aggregation points. ACE is located at system module A which aggregates a number of DSL connections, and AAE is located at system module B which is a higher aggregation point and handles a bigger number of user connections. This generic model can be specialized in different ways.

Figure 3 exemplifies a potential configuration within a cascaded network architecture consisting of a centralized DSLAM and one or more remote DSLAMs. An AAE is placed at the central card of the centralized DSLAM. ACE protocol entities are located on every line card of the centralized and the remote DSLAM. An AAE is not required to be installed on remote DSLAMs because both centralized

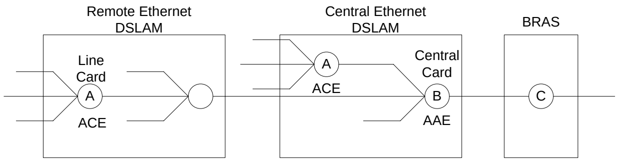

Figure 3. ACIP Specific Network Model

and remote DSLAM are within the same Ethernet broadcast domain. The network topology pointed out by Figure 3 matches the scenario in Figure 1 that was initially described.

Figure 4 illustrates a use case for ACIP. We want to exemplify it for a better understanding. A DHCP relay agent shall be installed on a centralized Ethernet aggregation module and shall use DHCP interface information option (option 82) with agent circuit id sub-option. The DHCP relay agent inserts the interface information in any DHCP message received on a user interface and relays the message towards the next DHCP relay agent or server on service provider side. In the field of DSL access network, a unique subscriber port identifier (SP-ID) which uniquely identifies an access node and an access line must be used for the interface information option. SP-ID is only available on the line cards that host the respective ports. However, the centrally located DHCP relay agent must gain access to this information. Thus, interface information has to be made available to the centralized modules, too. Therefore, to request SP-ID, an ACIP message will be sent from AAE on the central module to ACE on the non-central module. These modules are the central card and the line cards of a DSLAM in the shown configuration of Figure 4. ACE sends the requested information back to AAE. As an important fact, ACE (using layer 2) implementation requires much less resources than a DHCP relay agent (using layer 5) and no TCP/UDP/IP stack is needed. We would like to point out that the structure of SP-ID is just an example. Currently, [3] defines the use of `‘‘Access-Node-Identifier L2-type slot/port[:vlan-id]’’` for syntax when Ethernet/DSL is used, which could easily adapted to any specific need as ACIP provides for a generic information exchange mechanism.

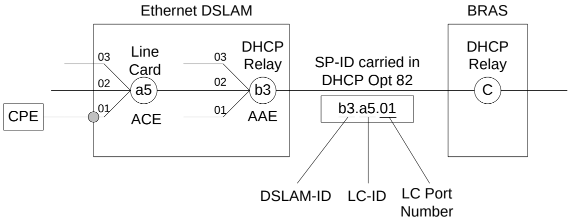

Figure 4. ACIP DHCP Relay Example

The important and essential properties of ACIP are as following:

- As simple as possible design approach
- Based on a strict design and using frames, messages, and AVPs
- Modular, extensible concept
- Comparable low demand with regards to system resources

Because of its properties, ACIP is especially qualified for systems within a hierarchical network topology and system structure where low resources are available on less-level aggregation points. Moreover, a hardware-based implementation of ACE within an FPGA, for instance, is facilitated.

3. Protocol Architecture

The general protocol structure of ACIP is devided into a base protocol part and protocol extension parts. The base protocol part establishes the underlying communication association between the protocol entities ACE and AAE. Within the base protocol, necessary parameters required for a reliable communication are exchanged. All control or any other information is carried in protocol extensions. Because of the protocol division, only the base protocol part and the extension parts needed for a dedicated system are required to implement for this system. In the current ACIP specification, two protocol extensions are defined – the *ACIP 802.1X Extension* and the *ACIP Port Information Extension*.

4. ACIP Base Protocol

The ACIP base protocol part establishes a communication relationship between ACE and AAE. An ACE will be bound to an AAE. After the establishment, information exchange between the two protocol entities is possible. During the protocol initiation phase at first, an ACE discovers all available AAEs. After receiving of a response from an AAE, ACE will be bound on this AAE and initialization will be completed. Further communication is realized by the available and implemented protocol extensions. If the binding shall be abolished and the communication relationship shall be ended, a logoff mechanism initiated by ACE or AAE will be used in the protocol logoff phase. After the logoff phase is concluded, no binding between ACE and AAE exists and no message exchange between the protocol entities is possible.

4.1. Addressing

Two different methods are used for addressing and ACIP frame identification. ACIP frame are marked with an ACIP

Ethernet type value (Ethertype). Additionally, a dedicated multicast destination address can be used, if no address information about the target is available or more than one protocol entity should be addressed at the same time. Both ACIP Ethernet type and ACIP group address are to be defined. Because ACIP will use a new Ethertype value, ACIP Ethernet frames can be easily identified in the traffic flow and, therefore, rapidly processed by the systems.

4.2. Frame Format

The frame format for ACIP for use in 802.3/Ethernet is shown in Figure 5. Five new protocol fields are defined. ACIP Ethernet Type is the Ethertype value for ACIP. The protocol version the sending protocol entity is using is inserted in the Protocol Version field. Packet Type field characterizes the type of packet/message carried in the Packet Body field. Currently, four different packet types are supported. ACIP-Start type is used within initialization phase. ACIP-Logoff type denotes logoff messages. ACIP-Packet-802.1XExt and ACIP-Packet-PortInfExt types are used for protocol extensions defined in current protocol version. Packet Body Length indicates the length of Packet Body field in numbers of octets. The Packet Body field contains exactly one ACIP message.

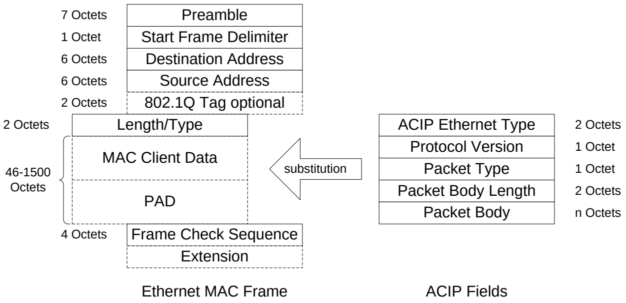

Figure 5. ACIP Frame Format

4.3. Message & AVP Format

An ACIP message consists of the fields depicted by Figure 6. The Msg Code (Message Code) field identifies the type of ACIP message. The Message Length field includes the total length of the message in number of octets including message header and data/AVP fields. The Identifier is used to identify the response to a particular request message. The number of AVPs carried in the data field of a message is recognized by the NoAVPs (number of AVPs). A value of NULL indicates that no AVP is included in the message. All data for a particular message are encapsulated in AVPs which are carried in the AVPs field of the message. If more than one AVP is present in a message, AVPs must be inserted in ascending order by AVP Code. This order alleviates message handling and analysis compared to random order. Furthermore, it provides additional error indication and a fast protocol processing.

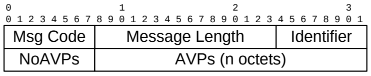

Figure 6. ACIP Message Format

Attribute value pairs consist of header and data fields and are used to encapsulate message-specific data. Figure 7 illustrates the ACIP AVP format. AVP Code uniquely identifies the type of attribute. The AVP Length field contains the total length of an AVP including AVP header and data. The Data field carries the data for a specific attribute. The length of the data depends on the AVP code which is used.

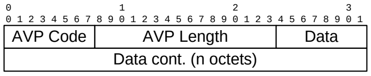

Figure 7. ACIP AVP Format

4.4. Base Protocol – Messages & AVPs

Figure 8 shows all messages for ACIP in current version defined for the base protocol part. Also the direction messages travel between the protocol entities is shown.

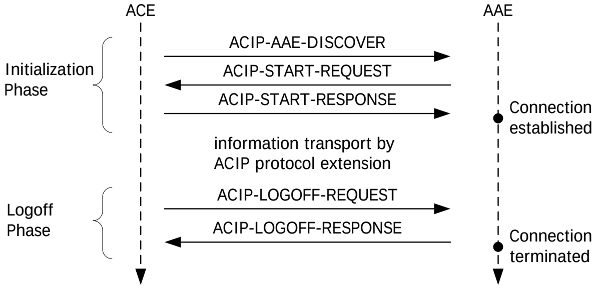

Figure 8. ACIP Base Protocol MSC

During the initialization phase, communication association between ACE and AAE will be established. An ACE transmits an AAE-DISCOVER message in order to discover an available AAE. ACIP group address can be used for the Ethernet destination address. In the AAE-DISCOVER message, an ACE provides its own MAC address carried in the LAD-MAC-ADDR AVP and a system identifier, for example a device ID or line card number, carried in the LAD-ID

AVP to an AAE. An available AAE which will receive the message creates an extra identifier named ACE-ID for this ACE which is locally unique within the scope of this AAE. A START-REQUEST message is sent by AAE to the MAC address of ACE. START-REQUEST message contains ACE-ID, the own AAE-ID of AAE, and AAE-MAC-ADDR in addition to all AVPs received in AAE-DISCOVER. At this time, an ACE is temporary bound to this AAE. In response, a START-RESPONSE message which also includes ACE-ID and AAE-ID is sent back to AAE by using the AAE MAC address, and communication association is established. The binding is kept until an explicit logoff based on ACIP logoff mechanism or an implicit logoff in case of network connectivity failure occurs. Both ACE and AAE can terminate the binding and close the communication association by using LOGOFF-REQUEST and LOGOFF-RESPONSE messages including ACE-ID and AAE-ID. An AAE may send a single LOGOFF-REQUEST message carrying only AAE-ID AVP to all ACEs bound by using ACIP group address. A state machine controls sending, receiving, and handling of messages. The state machine is responsible for re-binding and logoff in case of packet loss or any error indication. The following AVPs are used in but not limited to the basis protocol part:

LAD-ID includes a system identifier of the system or system module referred to as Local Access Device (LAD) in the scope of ACIP where an ACE is installed. This identifier is, e.g., a device or line card number. LAD-ID is used to identify an ACE device in addition to identification by MAC address.

LAD-MAC-ADDR contains the MAC address of a LAD.

ACE-ID contains an identifier for an ACE which is generated by an AAE and locally unique within the scope of this AAE.

AAE-ID contains an identifier for an AAE configured by management function and unique within the Ethernet domain an AAE is presented. In addition to address an AAE by its own MAC address, AAE-ID is used to easily and reliably identify an AAE.

AAE-MAC-ADDR contains the MAC address of the system or system module where an AAE is installed.

5. ACIP Protocol Extensions

Subsequent to the creation of a communication association and binding of ACE and AAE, the following communication between ACE and AAE is based on the definitions of ACIP protocol extensions. The current protocol version defines the *ACIP Port Information Extension* and the *ACIP 802.1X Extension*. The following sections describe these two extensions briefly.

5.1. ACIP Port Information Extension

The ACIP Port Information Extension is used to transmit a port or interface information respectively for remote access line identification and is explicitly designed for being a VLAN-independent solution. The relevant port is located at the local access device (LAD) mentioned as a DSL line card on which an ACE must also be installed. An AAE which requires the user port-ID for providing it to a local application, e.g. a DHCP relay agent, requests the port-ID by sending a SUBSCRIBER-PORT-ID-REQUEST message to a dedicated or all ACEs bound. This message contains the LAD-PORT-MAC-ADDR AVP which carries a user MAC address associated with the requested port-ID. Corresponding LAD and, therefore, ACE has access to this information and encodes it for using in the LAD-PORT-ID AVP. ACE transmits a SUBSRIBER-PORT-ID-RESPONSE message which contains LAD-PORT-MAC-ADDR and LAD-PORT-ID back to requesting AAE. Figure 9 illustrates the message exchange. Messages also include ACE-ID and AAE-ID AVP defined within the base protocol.

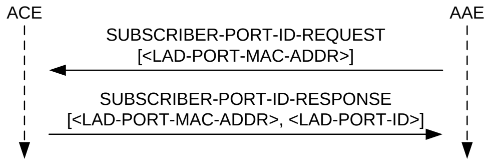
ACE
AAE
SUBSCRIBER-PORT-ID-REQUEST
[<LAD-PORT-MAC-ADDR>]
SUBSCRIBER-PORT-ID-RESPONSE
[<LAD-PORT-MAC-ADDR>, <LAD-PORT-ID>]

Figure 9. Port Information Extension MSC

5.2. ACIP 802.1X Extension

To gain a cost-effective solution for DSL users authenticating themselves based on IEEE 802.1X, an 802.1X authenticator has to be placed on a centralized system module [4]. The controlled ports, however, are still located at the non-central line cards and have to be remotely controlled. ACIP 802.1X Extension offers a centralized authenticator implementation instead of a highly replicated and, thereby, hard-to-manage decentralized implementation on all line cards throughout the layer 2 broadcast domain. The set of LAD-ID, LAD-PORT-MAC-ADDR, and LAD-PORT-ID which is unique in the whole access network is used for logical port association identification. The DSL user port can be remotely controlled regarding of the result of authentication process.

The messages and primary AVPs are illustrated by Figure 10. An ACE transmits a AUTH-8021X-START-REQUEST message to AAE if the begin of an authentication process is recognized by the local control function on LAD. This will be true, e.g., if a 802.1X start frame is recognized

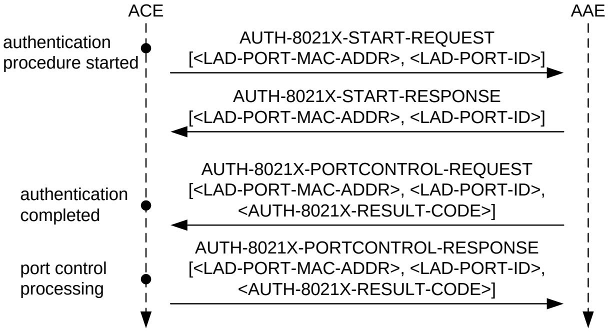
ACE
AAE
authentication procedure started
AUTH-8021X-START-REQUEST [<LAD-PORT-MAC-ADDR>, <LAD-PORT-ID>]
AUTH-8021X-START-RESPONSE [<LAD-PORT-MAC-ADDR>, <LAD-PORT-ID>]
authentication completed
AUTH-8021X-PORTCONTROL-REQUEST [<LAD-PORT-MAC-ADDR>, <LAD-PORT-ID>, <AUTH-8021X-RESULT-CODE>]
port control processing
AUTH-8021X-PORTCONTROL-RESPONSE [<LAD-PORT-MAC-ADDR>, <LAD-PORT-ID>, <AUTH-8021X-RESULT-CODE>]

Figure 10. 802.1X Extension MSC

on the user port. In order to avoid unnecessary communication, the AUTH-8021X-START-REQUEST message already contains all parameters in terms of AVPs (LAD-ID, LAD-PORT-MAC-ADDR, and LAD-PORT-ID) needed for building the logical port association for supplicant and authenticator port. AAE transmits a AUTH-8021X-START-RESPONSE message for confirmation back to ACE. After authentication process is completed, AAE sends a AUTH-8021X-PORTCONTROL-REQUEST message to ACE. This message encapsulates the result of the authentication process in the AUTH-8021X-RESULT-CODE AVP. The result is decoded by ACE, and a port control command is executed by local LAD functions. The associated DSL user port at the LAD can now be opened or closed. ACE transmits a AUTH-8021X-PORTCONTROL-RESPONSE message back to AAE which signals the receipt of the authentication result. LAD-PORT-MAC-ADDR and LAD-PORT-ID AVP are the same as described in the ACIP Port Information Extension.

6. Conclusions

The migration from legacy ATM to Ethernet-based DSL access involves changes in network topology and system architectures combined with a lot of functional re- and new-designs in access networks. High bandwidth demands and new features like DHCP relay agents and authentication based on 802.1X are parts of the new Ethernet-based access networks.

A new *Access Control and Information Protocol* was introduced supporting and relieving integration, usage, and management of several new functionalities. Using ACIP as a generic and extensible protocol which can carry relevant information within access networks, the centralized positioning of resource-intensive functionalities on high level aggregation systems is possible. Functional moving relieves cost-sensitive systems from implementing and processing of functions demanding a lot of system resources. The effect of gaining fewer costs will be further intensified if the demand on bandwidth is further increased and, therefore, access nodes have to be moved toward the DSL user edge, e.g., for providing VDSL. This causes that the total number of access nodes to increase and, therefore, cost-effectiveness is further growing by using ACIP. ACIP can decrease and unify configuration and administration measures of networks. Centralizing as many as possible control functions facilitates comparatively ”dumb” peripheral equipment. ACIP base protocol part establishes the underlying communication relationship between ACIP protocol entities ACE and AAE. Two protocol extensions have been described. ACIP Port Information Extension is used to transmit a user port identifier. ACIP 802.1X Extension provides all information needed for having a distributed, centralized, and full-functional authentication mechanism based on IEEE 802.1X.

The protocol architecture used keeps ACIP very flexible referring to further development, i.e., additional messages and AVPs, and integration of new protocol extensions. Thus, it is possible to carry all information needed within access networks by ACIP as a central and integrative communication platform. As an example, a controlled multicast distribution through an access network is possible by defining a new extension. Moreover, a diversity of additional protocol extension for exchanging static data, parameter and configuration settings requests, or any other service-specific information and controlling will be possible.

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

References

[1] DSL Forum. Multi-Service Architecture & Framework Requirements. Technical report, DSLF: TR-058, Sept. 2003.

[2] DSL Forum. Use of DHCP Relay Agents and PPPoE Intermediate Agents for DSL line identification In Ethernet-based access networks. DSLF contribution: dsl2004.071.00, Feb. 2004.

[3] DSL Forum. Migration to Ethernet-Based DSL Aggregation. DSLF: WT-101 Rev 10.1, Feb. 2006.

[4] D. Duchow, T. Bahls, D. Timmermann, S. Kubisch, and H. Widiger. Efficient Port-based Network Access Control for IP DSLAMs in Ethernet-based Fixed Access Networks. In *Proceedings of World Telecommunication Congress (WTC 2006) on CD-ROM*, Budapest, May 2006.

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

[6] M. Patrick. DHCP Relay Agent Information Option. RFC 3046 (Proposed Standard), Jan. 2001.