Neue Authentifizierungsmethoden für leitungsgebundene breitbandige Zugangsnetze

Daniel Duchow [I], Thomas Bahls [II], Dirk Timmermann [I]
[I] *Institut für Angewandte Mikroelektronik und Datentechnik*
Universität Rostock, Richard-Wagner-Str. 31, D-18119 Rostock
Tel.: +49 381 498-3630, Fax: +49 381 498-3601
{Daniel.Duchow, Dirk.Timmermann}@etechnik.uni-rostock.de
[II] *Siemens AG, Information and Communication Networks, D-17489 Greifswald*
Thomas.Bahls@siemens.com

1 Einleitung

Die Etablierung neuer Services wie IP Multicast in leitungsgebundenen breitbandigen Zugangsnetzen erfordert ein Redesign dieser Netze in Struktur und Funktionalität. Einer der wesentlichen Aspekte ist dabei die Authentifizierung von Teilnehmern. Wir stellen in dieser Arbeit einen Ansatz vor, wie die Authentifizierung in neu strukturierten Access Networks (AN) funktional vorgenommen werden kann. In heutigen ATM-Basierten AN, die den Teilnehmern durch xDSL-Technologien einen breitbandigen Zugang bereitstellen, erzeugt das Point-to-Point-Protokoll (PPP) in Verbindung mit dem PPP-over-Ethernet-Protokoll (PPPoE) einen Kommunikationskanal von den Geräte-Interfaces der Teilnehmer bis hin zu einem Network Access Server am Rande des AN. PPP(oE) konfiguriert nach erfolgreicher Authentifizierung die Network Interface Cards und stellt so IP Connectivity der Teilnehmergeräte her. Abbildung 1 zeigt die grundlegende, von uns verwendete Netzstruktur und die wichtigsten Teile des Protokoll-Stack in einem Netzkonzept, in dem bereits Ethernet-Technologie anstelle von ATM für einen Großteil des AN angenommen wird.

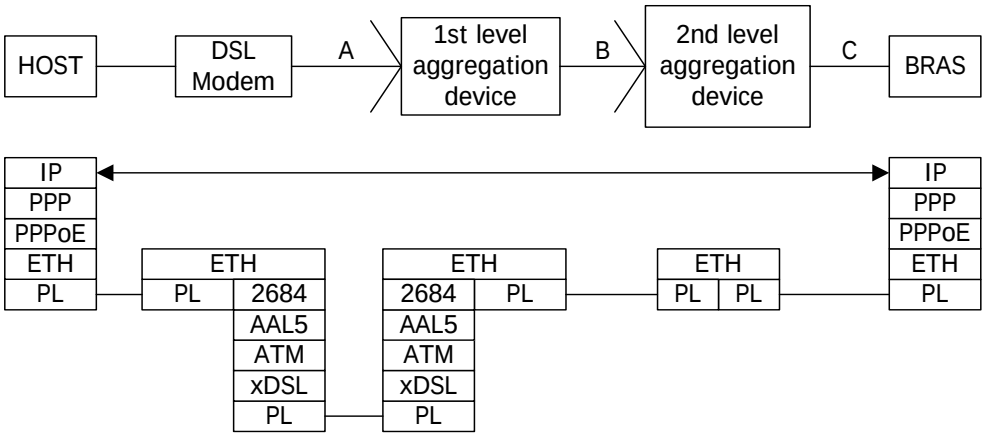

Abbildung 1. Ethernet-Basiertes Zugangsnetz mit PPP(oE)

Der wesentliche Nachteil von PPP(oE) als Methode zur Authentifizierung und Konfiguration besteht darin, dass PPP(oE) eine Kapselung der IP-Datenpakete vornimmt und diese innerhalb des etablierten PPP-Kanals resp. -Tunnels über das Netz transportiert. Für die Einführung eines IP-Multicast-Service ist jedoch die gegenseitige Sichtbarkeit und Erreichbarkeit von Ethernet und IP Layer eine dringende Voraussetzung für den effizienten Einsatz von Multicast-Verfahren. Die Datenübertragung mittels Ethernet und IP Multicast erfordert ein Mapping der IP-Multicast-Adressen auf Ethernet-Multicast-Adressen und umgekehrt. Abbildung 2 veranschaulicht die Konvertierung exemplarisch.

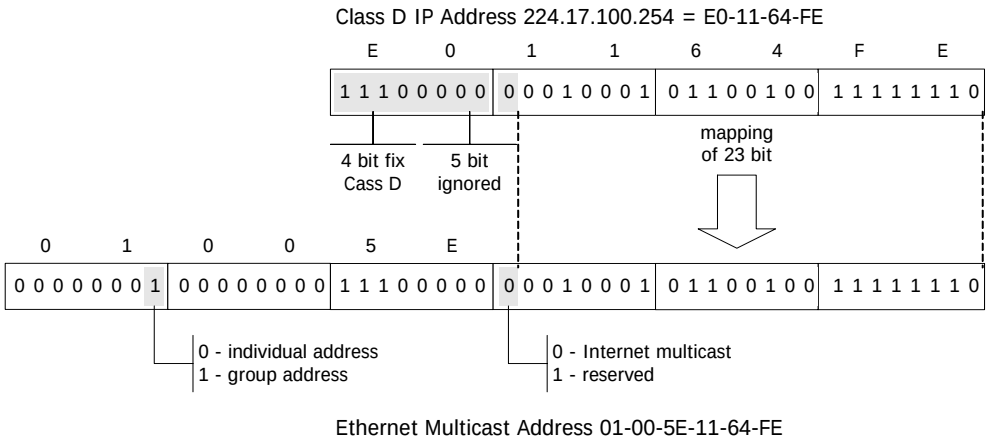

Abbildung 2. Abbildung von IP-Multicast- auf Ethernet-Multicast-Adressen

Aus diesem Grund befürworten wir für zukünftige Netze und Systeme die Ersetzung des PPP(oE) durch andere, Ethernet- oder IP-Basierte Methoden zur Authentifizierung und Konfiguration. Im Folgenden zeigen wir eine Möglichkeit auf, wie durch den Einsatz neuer Methoden zur Authentifizierung und Autorisierung auf den Einsatz von PPP(oE) als Authentifizierungs-mechanismus gänzlich verzichtet werden kann.

2 Authentifizierungsverfahren für künftige Access-Netze und –Systeme

Eliminiert man PPP(oE), so besteht nach Abbildung 2 eine direkte IP-over-Ethernet-Verbindung über das gesamte AN hinweg. Für eine solche Struktur bietet sich der Einsatz des IEEE Std. 802.1X als Authentifizierungskonzept an. Bei dieser Port-Basierten Authentifizierung wird ein Supplicant – das Endsystem des Teilnehmers – von einem Authenticator, der eine Funktionseinheit auf einem Vermittlungssystem darstellt, authentifiziert und für den Netzzugang autorisiert. Der Authenticator kann dabei die Authentifizierung selbst vornehmen, indem er die erforderlichen Informationen aus einer lokalen Datenbasis entnimmt. Eine andere und weitaus flexiblere Möglichkeit wird durch die zusätzliche Verwendung eines Authentication Backend Servers offeriert. An diesen reicht der Authenticator die Authentifizierungsanforderungen der Supplicants unverändert weiter. Dabei können die verschiedensten Verfahren zwischen Authenticator und Authentication Server eingesetzt werden. RADIUS ist ein weit verbreitetes Authentifizierungsprotokoll. DIAMETER ist eine aktuelle Weiterentwicklung von RADIUS und wird in zukünftigen Systemen relevant sein. Beide Verfahren dienen unter anderem dazu, die Authentifizierungs-Messages des Extensible Authentication Protocol (EAP) über IP zwischen einem Client und einem Server zu vermitteln.

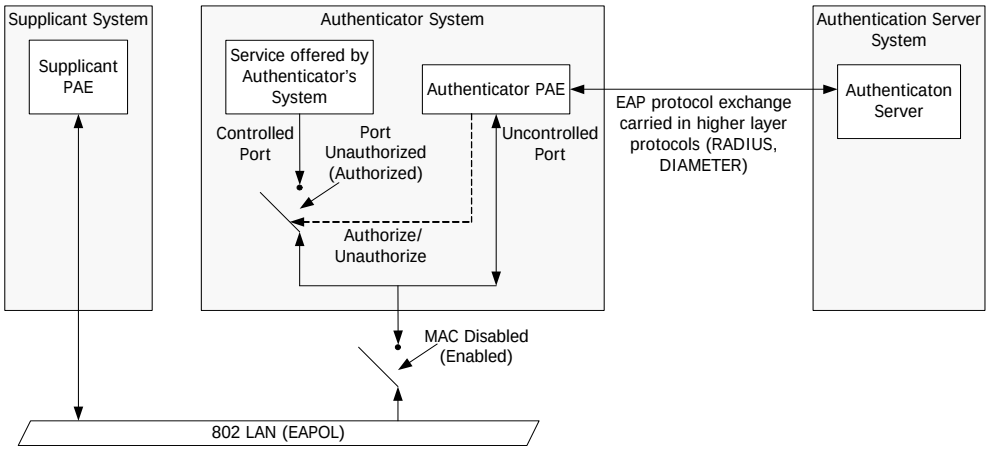

Abbildung 3. IEEE 802.1X - Port based Network Access Control

Die Authentifizierung selbst nimmt ein Backend Server vor, der die notwendigen Informationen aus einer zentralen Datenbasis entnimmt. Nach erfolgter Authentifizierung sendet der Server eine positive oder negative Bestätigung an den Supplicant zurück. Der Authenticator als zwischengeschaltetes System erkennt das Ergebnis des Authentifizierungsprozesses, indem er die Kommunikation zwischen Supplicant und Authentication Server untersucht. Je nach Zustand des Ergebnisses – positiv oder negativ – nimmt der Authenticator die Autorisierung des Supplicant für den Netzzugang vor. Abbildung 3 zeigt die System- und Netzstruktur dieses Verfahrens.

Von grundsätzlicher Bedeutung für den erfolgreichen Einsatz dieses Verfahrens ist das Erfordernis, dass zwischen Supplicant und Authenticator eine physische oder logische eindeutige Punkt-zu-Punkt-Verbindung (p2p) besteht, wie diese zum Beispiel bei switched Ethernet gegeben ist. Diese Eindeutigkeit ist erforderlich, da die Authentifizierung und Autorisierung Port-Basiert erfolgt und daher eine eindeutige Zuordnung von Port und Supplicant bestehen muss.

3 IEEE Std. 802.1X in einem Access Network

Die physische oder logische Zuordnung des Ports eines Supplicant zum Port des Authenticator System ist eine der wichtigsten Maßnahmen bei der Umsetzung des Standards in einem Access System.

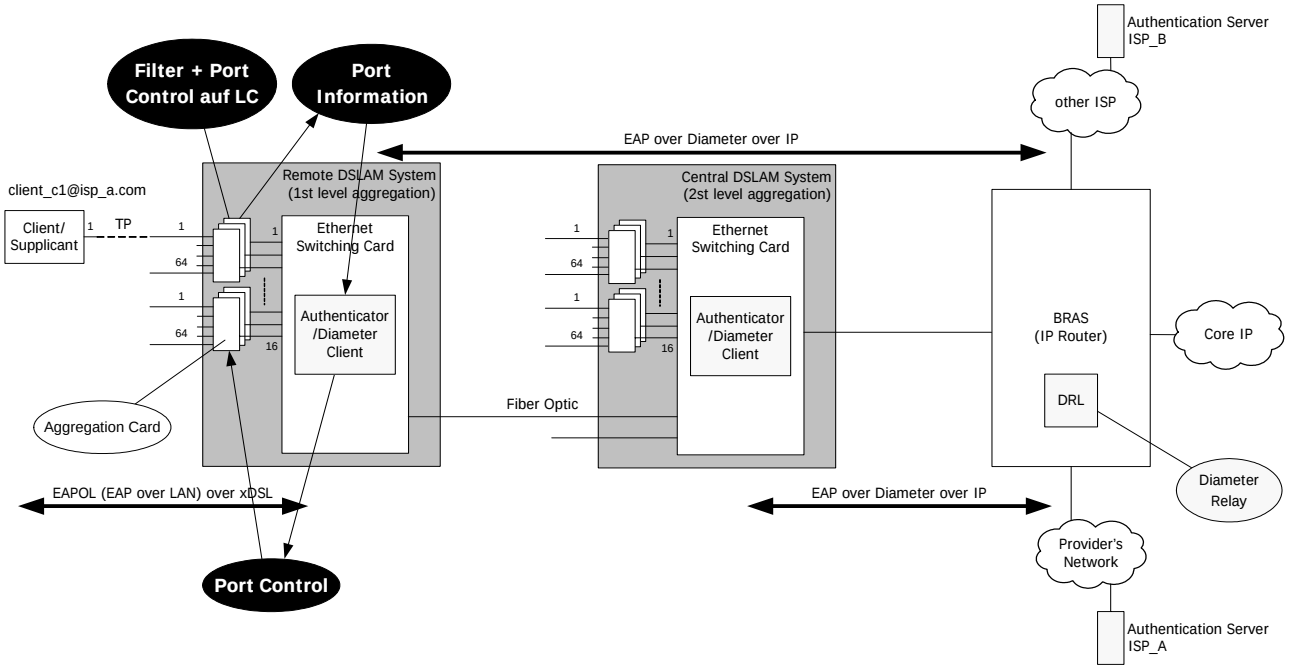

Abbildung 4. Implementierung des IEEE Std 802.1X in einem Access System

Abbildung 4 zeigt ein kaskadiertes Netzszenario mit Central und Remote DSLAM Systems als 1st und 2nd Aggregation Devices. Diese Systeme bestehen aus einer Anzahl verschiedener Karten. Die hier wichtigsten Karten sind die Aggregation Cards sowie die Ethernet Switching Cards.

Drei grundsätzliche Möglichkeiten der Positionierung des Authenticator im Systembild nach Abbildung 4 sind wie folgt gegeben:

1 Da jede Aggregation Card eines DSLAM Systems mehrere DSL Ports konzentriert (in diesem Beispiel 64 Ports) und auf ihr die erforderliche p2p-Charakteristik mit den Ports der Supplicants standardkonform besteht, kann der 802.1X Authenticator direkt auf jeder Aggregation Card implementiert werden. Eine funktionale Umsetzung des Std 802.1X nach Abbildung 3 ist somit möglich. Ein wesentlicher Nachteil dieses Konzeptes ist die Dezentralität der Lösung und der damit verbundene hohe Kostenaufwand. Auf jedem DSLAM System mit einer Anzahl von x

Aggregation Cards müssen demzufolge auch x Authenticator Systems implementiert, konfiguriert und administriert werden.

2 Als weniger dezentrale Lösung lässt sich der 802.1X Authenticator auf der Ethernet Switching Card anstatt auf den Aggregation Cards selbst implementieren. Die Ethernet Switching Cards bietet den Aggregation Cards den Std 802.1X als Service an. Pro DSLAM System muss dadurch nur ein Authenticator System implementiert und administriert werden. Der Nachteil dieser Lösung besteht darin, dass die erforderliche p2p-Charakteristik der Ports verloren geht und nun zusätzlich durch die Implementierung weiterer Mechanismen geschaffen werden muss.

3 Die höchste Stufe der Zentralität besteht darin, in einem kaskadierten DSLAM-Szenario für alle DSLAM Systems gemeinsam lediglich ein einziges Authenticator System zu implementieren. Dieses wird auf dem Central DSLAM System realisiert. Auch bei dieser Lösung muss die p2p-Charakteristik der Port zusätzlich realisiert werden, was durch die Kaskadenstruktur des Systembildes noch aufwendiger ist als in dem zuvor beschriebenen Lösungsansatz.

Die von uns favorisierte Variante 2 zeigt Abbildung 4. Sie stellt eine zentrale und kostenoptimale Implementierung dar. Die notwendige Schaffung der p2p-Verbindung zwischen Supplicant Port und Authenticator Port kann wie folgt vorgenommen werden:

Die verschiedenen Karten zusammen ergeben das Gesamtsystem, das von einem Management System gesteuert wird und über systeminterne Kommunikation verfügt. Diese Kommunikation stellt sicher, dass die 802.1X-Funktionalität trotz der Zentrierung auf den Ethernet Switching Cards konsistent im System angeboten werden kann. Die verloren gegangene physische p2p-Charakteristik wird durch eine logische nachgebildet. Der Authenticator muss dafür für jeden einzelnen Authentifizierungsvorgang über eine Identifikationsinformation des Supplicant resp. DSL Ports verfügen. Diese Information wird ihm durch die systeminterne Kommunikation zur Verfügung gestellt (Port Information). Da die Aggregation Cards die Autorisierung der angeschlossenen Supplicants umsetzen müssen, stellt das Management System auch hierfür die notwendigen Informationen bereit (Port Control). Auf den Aggregation Cards sorgt ein Filter und Port Control Mechanismus dafür, dass die benötigten Informationen produziert und die Ports gesteuert werden. Diese drei Mechanismen (siehe Abbildung 4) sind vom Funktionsumfang her einfacher und somit kostengünstiger zu implementieren als ein gesamtes Authenticator System.

4 Zusammenfassung und Ausblick

Das vorgestellte Konzept eignet sich grundlegend sehr gut für die angestrebten Authentifizierungs- und Autorisierungsanforderungen, um PPP funktional zu ersetzen. Die beschriebenen Filter- und Port Control Mechanismen sowie ein Kommunikationsverfahren zwischen Aggregation und Ethernet Switching Card sind für die vollständige Umsetzung des Std 802.1X weiter zu spezifizieren. Alle anderen beteiligten Verfahren wie z.B. die Authentifizierungsprotokolle des DIAMETER (Client, Server, Relay) liegen als Spezifikation vor und können ohne Veränderungen in den Systemen implementiert werden. Ein sich ableitendes weiteres Erfordernis bei der funktionalen Ersetzung von PPP im DSL Access-Szenario ist die Implementierung eines Konfigurationskonzeptes, das zum Beispiel durch DHCP-Verfahren realisiert werden kann.

Quellen

[1] Duchow, D.; Bahls, T.; Timmermann, D.: “Enabling Multicasting for Access Networks”. University of Rostock, March 2004.
[2] IEEE Std for Local and Metropolitan Area Networks: “Port-Based Network Access Control”. IEEE Std 802.1X-2001, June 2002.
[3] Calhoun, P.; Loughney, J.: “Diameter Base Protocol”. RFC 3588, September 2003.