Authentifizierungsmethoden für leitungsgebundene breitbandige Zugangsnetze

Daniel Duchow, Thomas Bahls and Dirk Timmermann

Universität Rostock und Siemens AG Greifswald

11. Symposium Maritime Elektrotechnik, Elektronik und Informatik

Rostock, 3. - 4. Juni 2004

Agenda

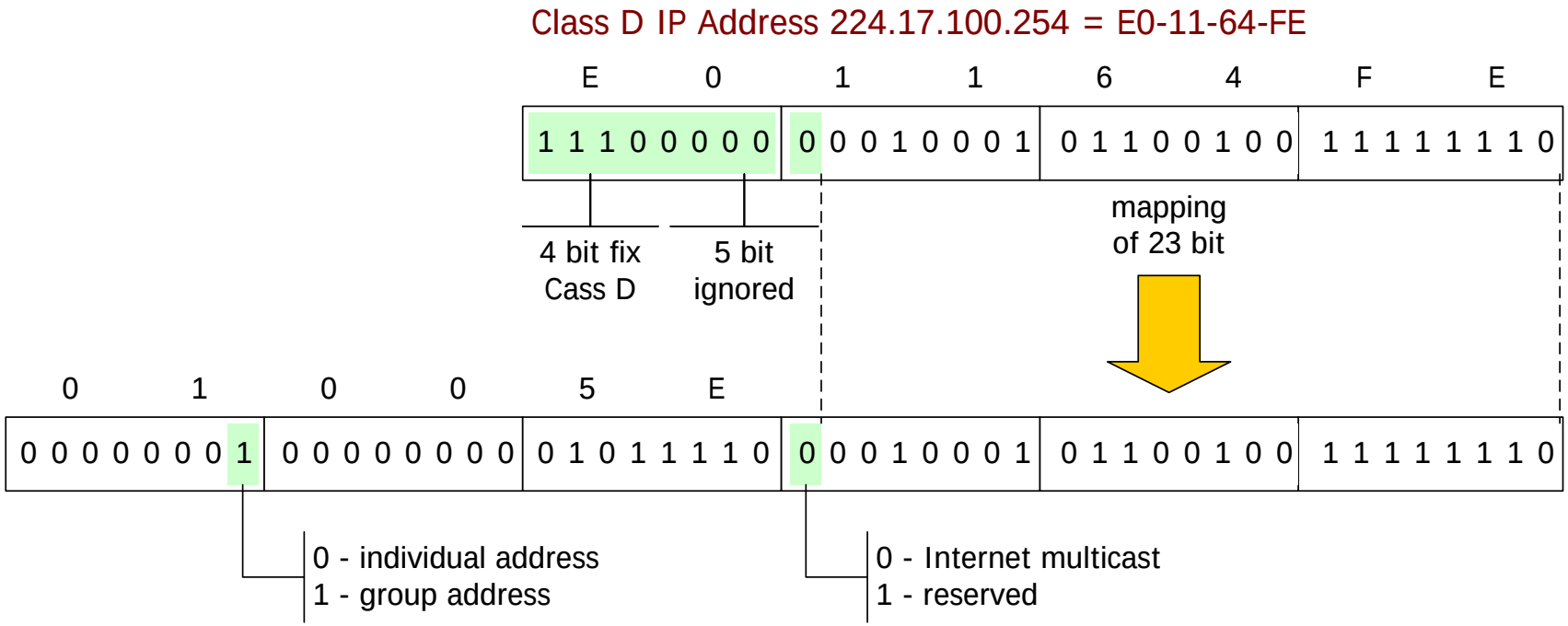
- Motivation
- IEEE Std. 802.1X – Port-Basierte Netzwerk-Zugangskontrolle
- 802.1X-Implementierung in Zugangsnetzen
- Ausblick und weitere Arbeiten

Motivation

- Neue Services in Access Networks erfordern ein Redesign der Netze in Struktur und Funktionalität
  Beispiel: IP Multicast Service
- Heutige ATM-Basierte Netze werden durch preiswerte Ethernet-Technologie ersetzt werden
- Authentifizierung und Autorisierung sind wesentliche Bestandteile von Zugangsszenarien
- Derzeit wird Authentifizierung mittels Point-to-Point-Protocol (PPP) vorgenommen
- Nachteil von PPP:
  - PPP kapselt IP-Datenpakete
  - Dadurch kein effizienter IP Multicast möglich

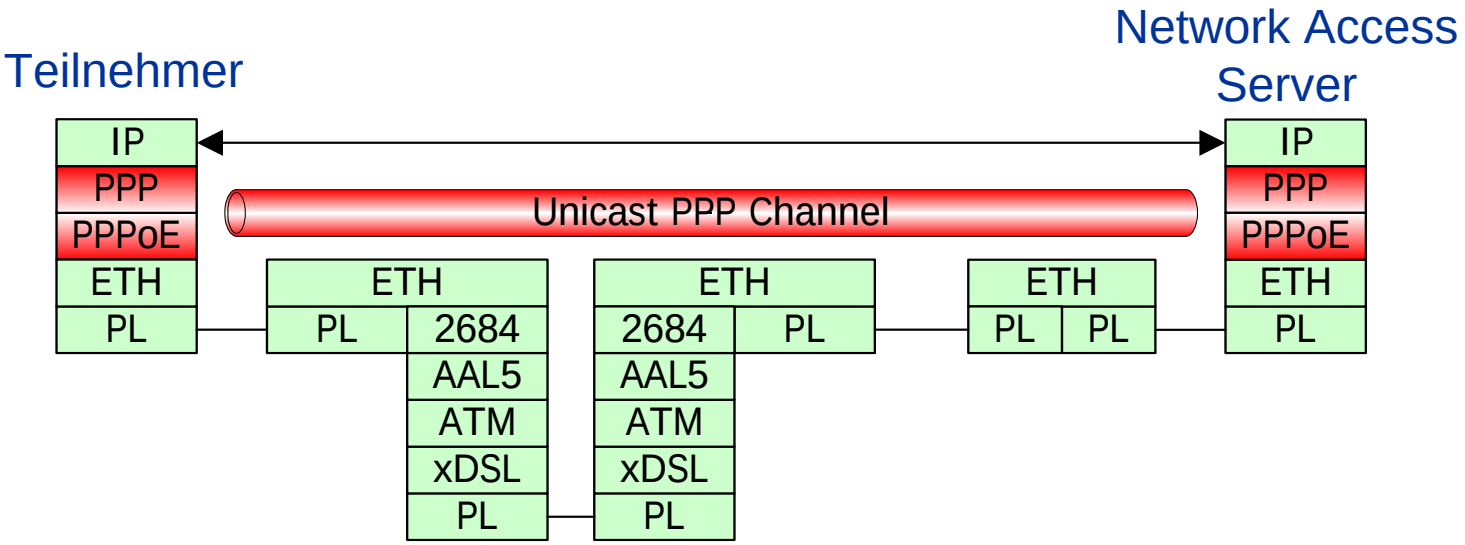
Beispiel: Multicast Kommunikation

- Beteiligte Schichten: Data Link und Network Layer
- Adress-Mapping zwischen IP und Ethernet Layer



Nachteil des PPP

- kein IP/Ethernet Multicast Support mit PPP möglich



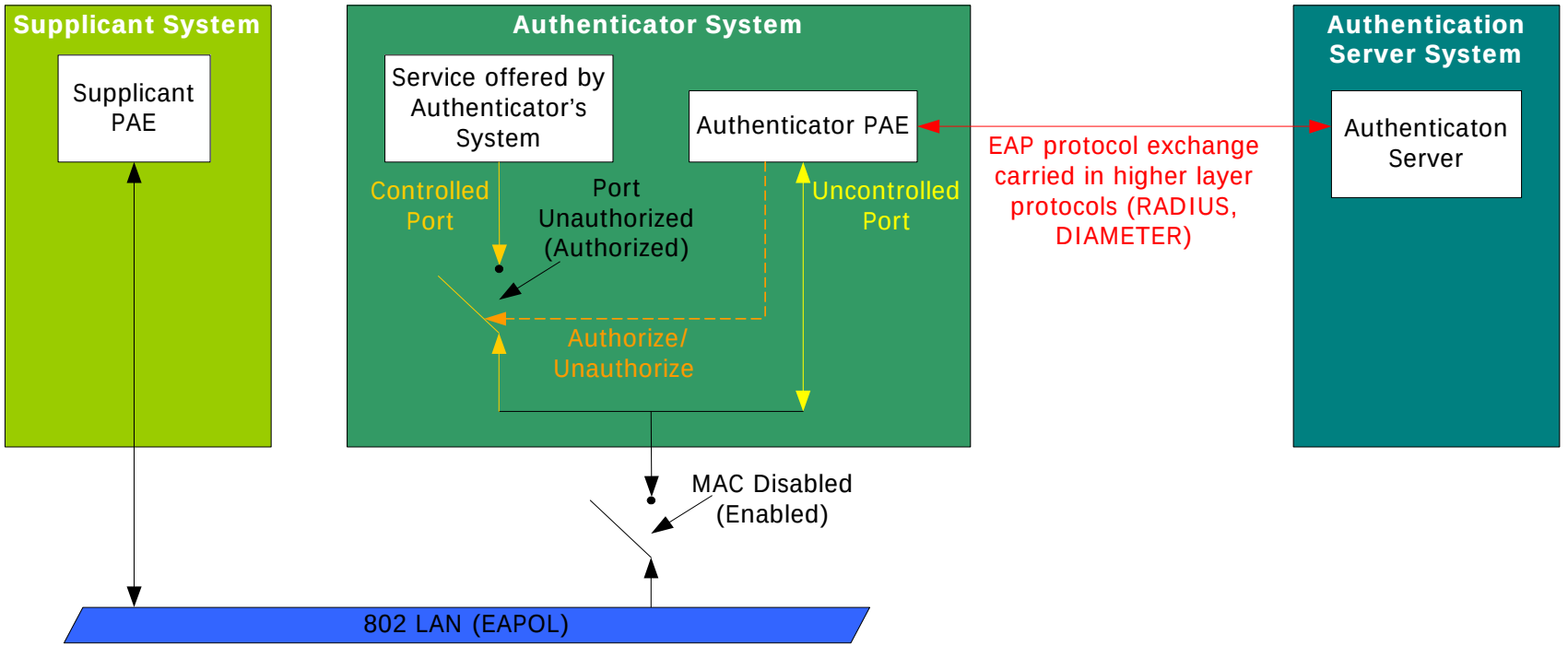
Problem: PPP blockiert Multicast zwischen Layer 2 und Layer 3

Lösung

Neue Authentifizierungsverfahren anstelle von PPP-Authentifizierung

IEEE Std. 802.1X

- Port-Basierte Netzwerk-Zugangssteuerung für IEEE-802-Netze (z.B. Ethernet)



- Wichtige Bedingung: 1:1-Beziehung von Supplicant und Authenticator Port, weil Port-Basierend

IEEE 802.1X in Zugangsnetzen

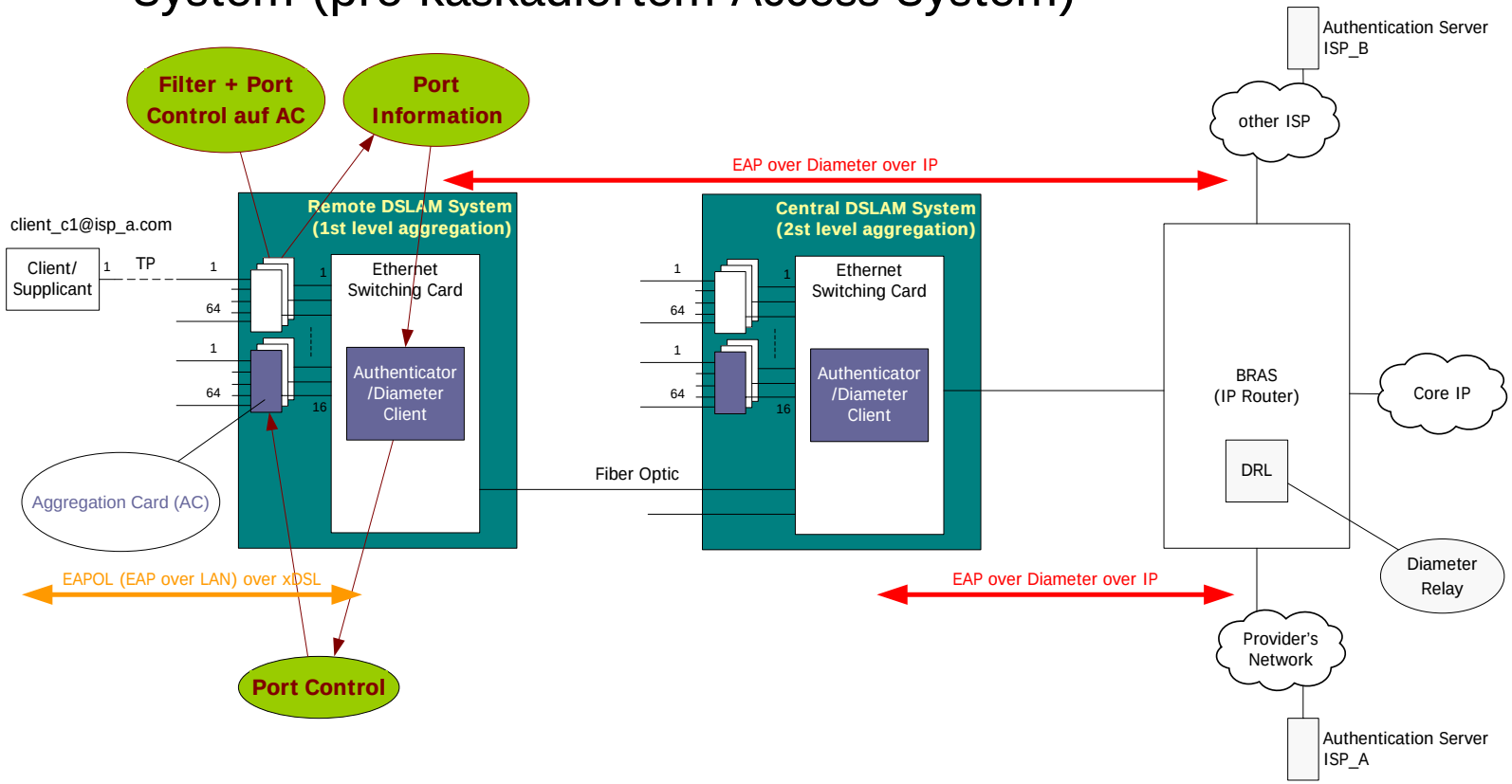
- Wichtige Bedingung: 1:1-Beziehung der Supplicant und Authenticator Ports muss realisiert werden
- Zuordnung der 802.1X-Funktionseinheiten zu den Elementen eines Access Systembildes

802.1X	Access System
Supplicant System	Subscriber Device (Endgeräte der Teilnehmer)
Authentication Server System	RADIUS oder DIAMETER Server des ISP
Authenticator System	Verschiedene Möglichkeiten der örtlichen Implementierung

Anordnung des Authenticator Systems (AS) im Access-Systembild

Drei Fälle sind möglich:

1. Je ein AS pro Aggregation Card eines DSLAM
2. Je ein AS pro Ethernet Switching Card (pro DSLAM)
3. Ein AS auf der Ethernet Switching Card des Central DSLAM System (pro kaskadiertem Access System)



Fall 1: AS pro Aggregation Card

- Vorteile:
  - Aggregation Card konzentriert die DSL-Ports: Point-to-Point-Portcharakteristik vorhanden
  - Eindeutige Zuordnung der Supplicant Ports zu den Ports des Authenticator (1:1-Beziehung)
  - Standardkonforme Lösung
- Nachteile:
  - Starke Dezentralität
  - Hoher Aufwand, da je ein AS pro Aggregation Card (bei 64 Cards/DSLAM -> 64 AS)
  - RADIUS bzw. DIAMETER Client im AS erfordern IP-Layer-Support bereits auf Aggregation Card

Fall 2: AS pro Ethernet Switching Card

- Vorteile:
  - Nur ein AS pro DSLAM, der 802.1X den Aggregation Cards als Service anbietet
  - Weniger dezentral als Fall 1 -> Kostenreduzierung

- Nachteile:
  - Point-to-Point-Portcharakteristik geht verloren und muss innerhalb eines DSLAM-Systems durch weitere Mechanismen geschaffen werden (logische Point-to-Point-Verbindung)
    -> zusätzlicher Aufwand zum Fall 1

Fall 3: AS auf Ethernet Switching Card des Central DSLAM System

- Vorteile:
  - Höchste Stufe der Zentralität in einem kaskadierten DSLAM-Szenario
  - Nur eine AS-Implementierung nötig, die allen Aggregation Cards aller DSLAMs im System den 802.1X-Service zur Verfügung stellt
  - Geringster Aufwand -> geringste Kosten
- Nachteile:
  - Point-to-Point-Portcharakteristik geht verloren und muss durch weitere Mechanismen geschaffen werden -> aber hier nicht nur innerhalb eines DSLAM, sondern innerhalb des kaskadierten Szenarios -> zusätzlicher Aufwand zum Fall 1 und 2

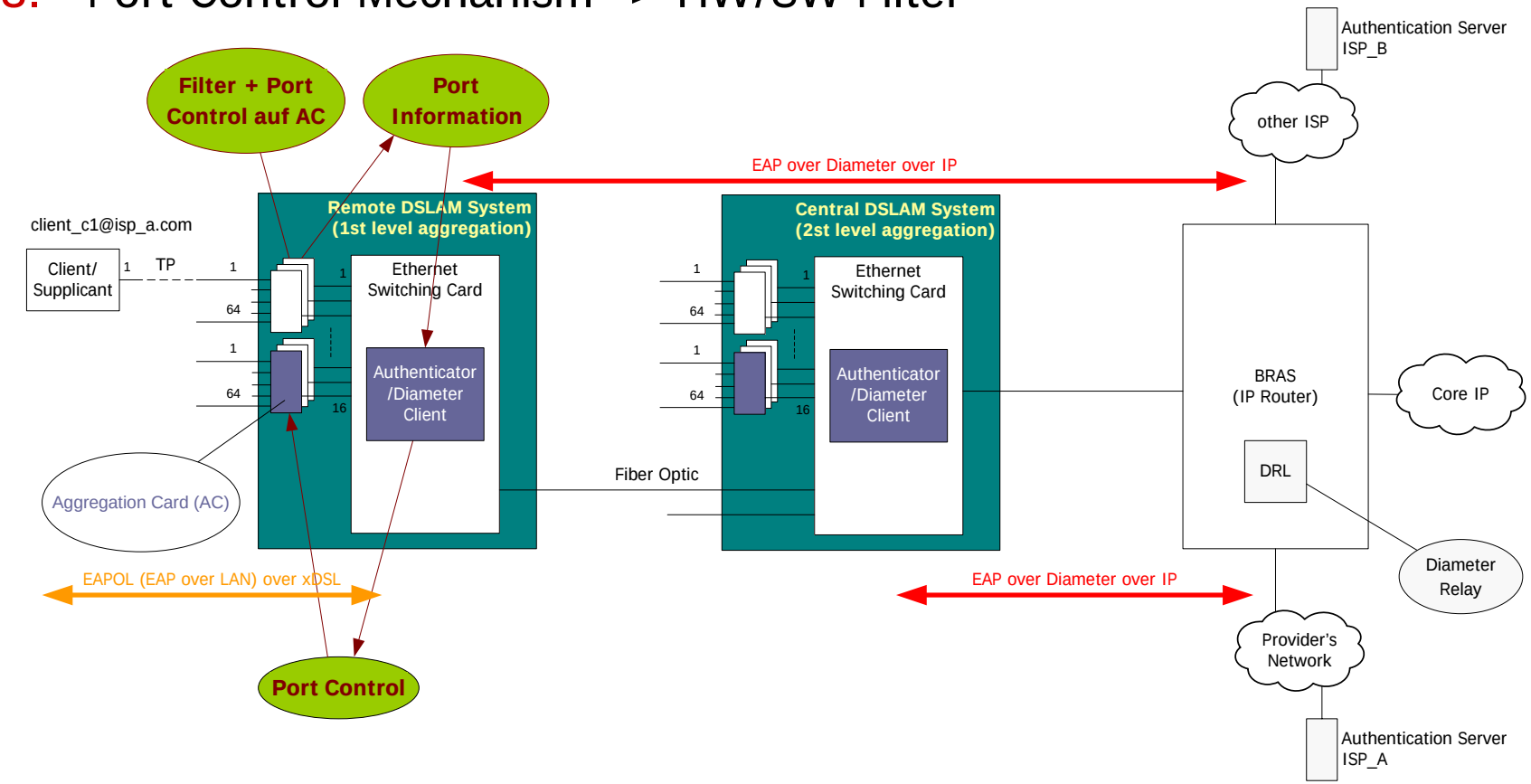
Favorisiert Lösung

- Fall 2: je ein AS pro DSLAM
  - Bestes Aufwand-Nutzen-Verhältnis
  - Zentral und kostenoptimal
- Schaffung der logischen Point-to-Point-Charakteristik
  - Systeminterne Kommunikation (wie z.B. Management)
  - Authenticator erhält für jeden Authentifizierungsvorgang eine „Port Information“
  - Authenticator sendet „Port Control Information“ an Aggregation Card zur Autorisierung
  - Aggregation Card öffnet/schließt Ports der Teilnehmer durch „Port Control Mechanism“

  -> weniger Aufwand als ein komplettes AS

Fall 2: Schaffung der logischen Punkt-zu-Punkt-Verbindung

1. Port Information -> EAPOL-Start/EAPOL-Logoff
2. Port Control Information -> EAP-Success/EAP-Failure
3. Port Control Mechanism -> HW/SW Filter



Ausblick und weitere Arbeiten

Für das vorgestellte Konzept

- Spezifizierung und Implementierung
  - der notwendigen Filter- und Port-Control-Mechanismen
  - der systeminternen Kommunikation

Erweiterung des Gesamtkonzeptes

- Ohne PPP ist die Einführung eines anderen Konzeptes zur automatischen Konfiguration der Network Interface Cards der Endgeräte der Teilnehmer erforderlich
  -> Entwicklung eines DHCP-Konzeptes für Zugangsnetze

Vielen Dank.

Fragen?