Diameter

KM-/VS-Seminar

Wintersemester 2002/2003

Betreuer: Martin Gutbrod

TECHNISCHE UNIVERSITÄT
CAROLO-WILHELMINA
ZU BRAUNSCHWEIG
Institut für Betriebssysteme und Rechnerverbund
http://www.ibr.cs.tu-bs.de http://www.ibr.cs.tu-bs.de

Übersicht

- Einleitung
- AAA
- Szenarien
  - Remote dial-in
  - Mobile dial-in
  - Mobile telephony
- Design von Diameter
  - Features
  - Protokoll Layout
  - Anwendungen
- Ausblick

Einleitung

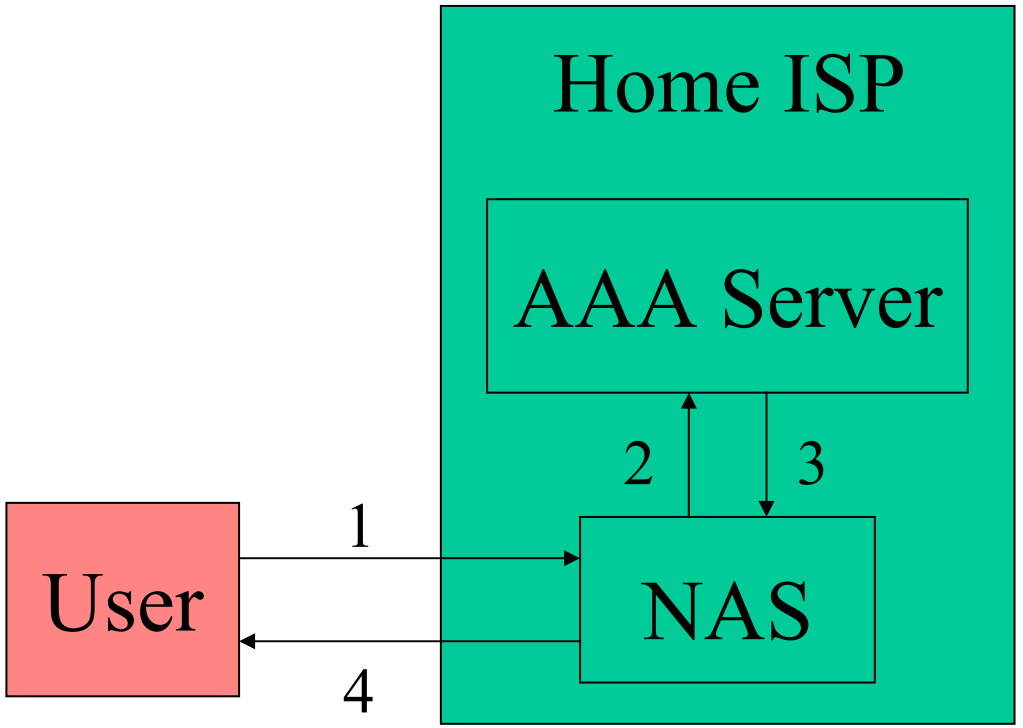
- Diameter
  - Netzwerk Protokoll
  - IETF „proposed standard“ seit 27. Januar 2003
  - Ersetzt RADIUS
  - Anwendungen in verschiedenen Umgebungen durch Modularität

AAA

- Authentication
  - Die Identität eines Nutzers überprüfen
- Authorization
  - Herausfinden, ob dem Nutzer Rechte gewährt werden
    - Netzwerkzugang
    - Zugang mit hoher Bandbreite
    - Nutzung von Diensten
- Accounting
  - Daten zur Nutzung von Ressourcen sammeln, z.B. für
    - Verkehrskontrolle
    - Abrechnung

TECHNISCHE UNIVERSITÄT
CAROLO-WILHELMINA
ZU BRAUNSCHWEIG
Institut für Betriebssysteme und Rechnerverbund
http://www.ibr.cs.tu-bs.de

Szenarien: Remote dial-in



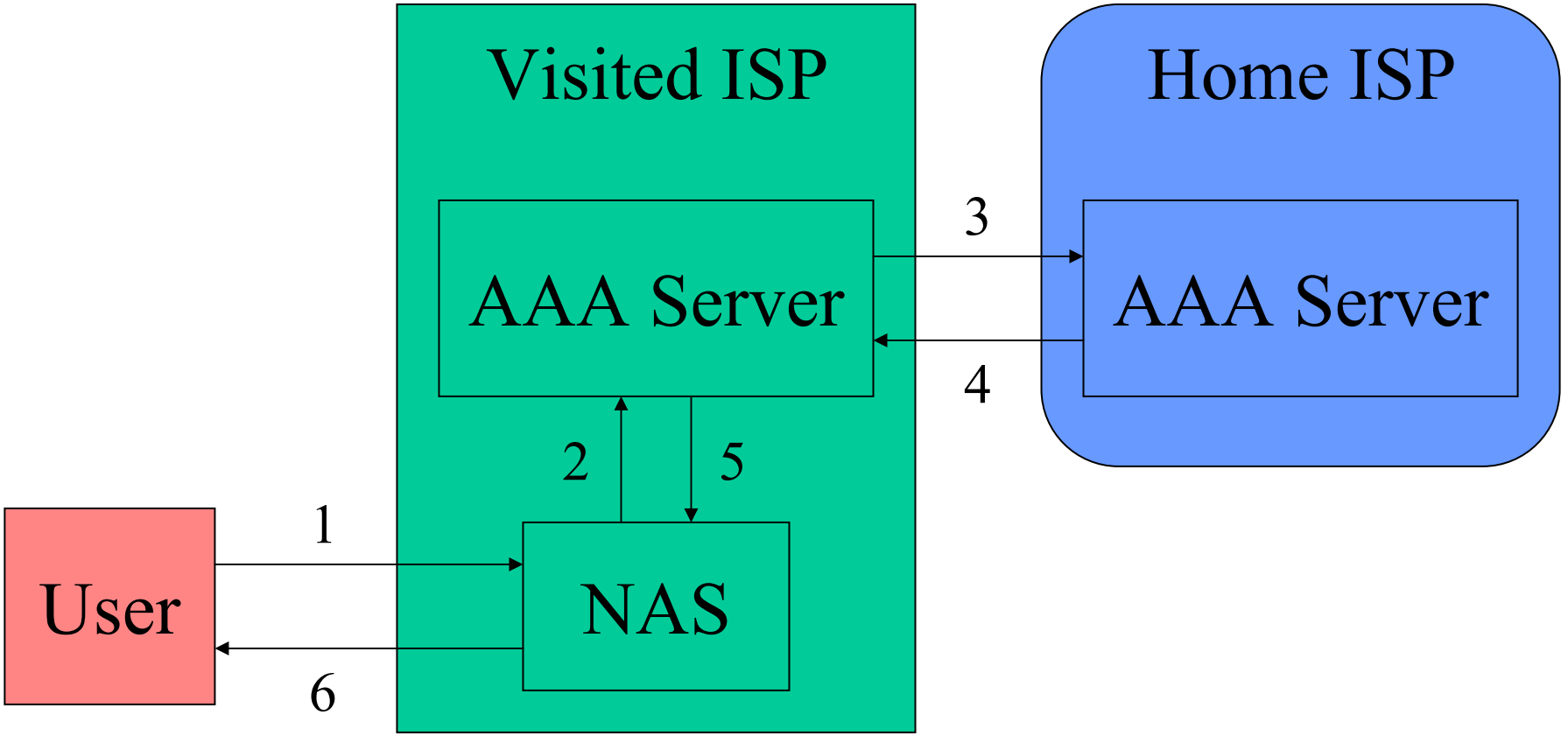
TECHNISCHE UNIVERSITÄT
CAROLO-WILHELMINA
ZU BRAUNSCHWEIG
Institut für Betriebssysteme und Rechnerverbund
http://www.ibr.cs.tu-bs.de http://www.ibr.cs.tu-bs.de

Szenarien: Remote dial-in

- Beispiel: Anwender wählt sich von zu Hause im Firmennetzwerk ein
- Bisheriger de facto Standard hierfür: RADIUS
  - Ermöglichte erstmals Zentralisierung von AA Funktionen auf einem Server
- Probleme
  - Langsam in großen Netzen
  - Keine Staukontrolle

TECHNISCHE UNIVERSITÄT
CAROLO-WILHELMINA
ZU BRAUNSCHWEIG
Institut für Betriebssysteme und Rechnerverbund
http://www.tu-bs.de http://www.ibr.cs.tu-bs.de

Szenarien: Mobile dial-in



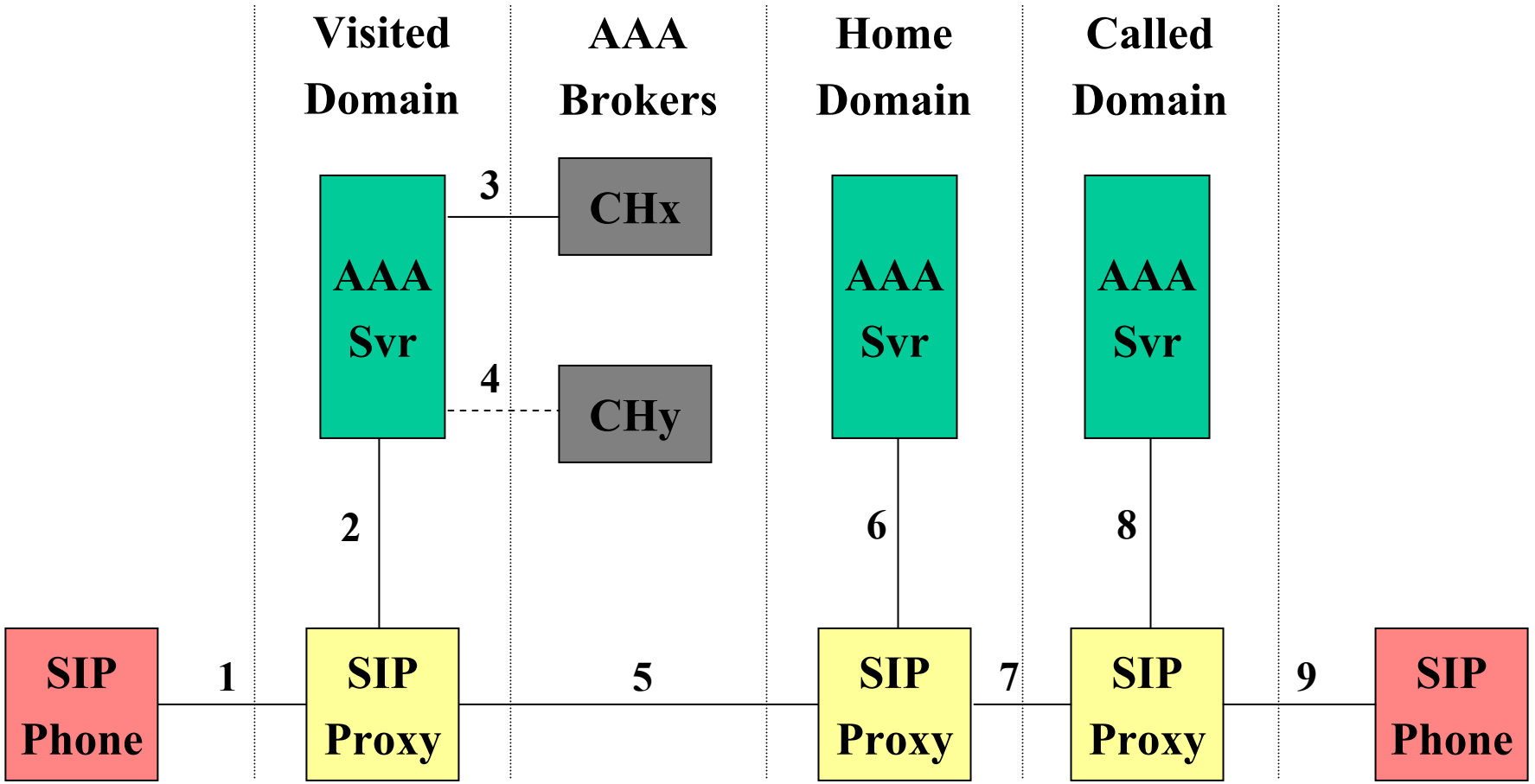
TECHNISCHE UNIVERSITÄT
CAROLO-WILHELMINA
ZU BRAUNSCHWEIG
Institut für Betriebssysteme und Rechnerverbund
http://www.ibr.cs.tu-bs.de http://www.ibr.cs.tu-bs.de

Szenarien: Mobile dial-in

- Beispiel: Einwahl ins Firmennetz per Internet Service Provider
- Probleme
  - Quality of Service sicherstellen
  - Staukontrolle
  - Abrechnung
  - Authentication ohne „shared secret“

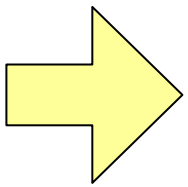
TECHNISCHE UNIVERSITÄT
CAROLO-WILHELMINA
ZU BRAUNSCHWEIG
Institut für Betriebssysteme und Rechnerverbund
http://www.ibr.cs.tu-bs.de http://www.ibr.cs.tu-bs.de

Szenarien: Mobile telephony



Szenarien: Mobile telephony

- Beispiel: Zugang zum Firmennetz aus dem fahrenden Auto
- Zusätzliche Probleme
  - Konstante IP-Adresse
  - Shared Secret
  - Kontakte/Verträge zwischen allen möglichen Domains



Broker

Diameter

- Features
  - SCTP statt UDP
    - Flußkontrolle
    - Staukontrolle und -vermeidung
    - Zuverlässiger Transport
    - TCP möglich, aber ohne SCTP Vorteile
  - Keep-alive messages
    - Versagen eines Peers wird schneller erkannt
  - Peer-to-Peer Architektur
    - Auch „Server“ dürfen Anfragen stellen oder Verbindung abbrechen

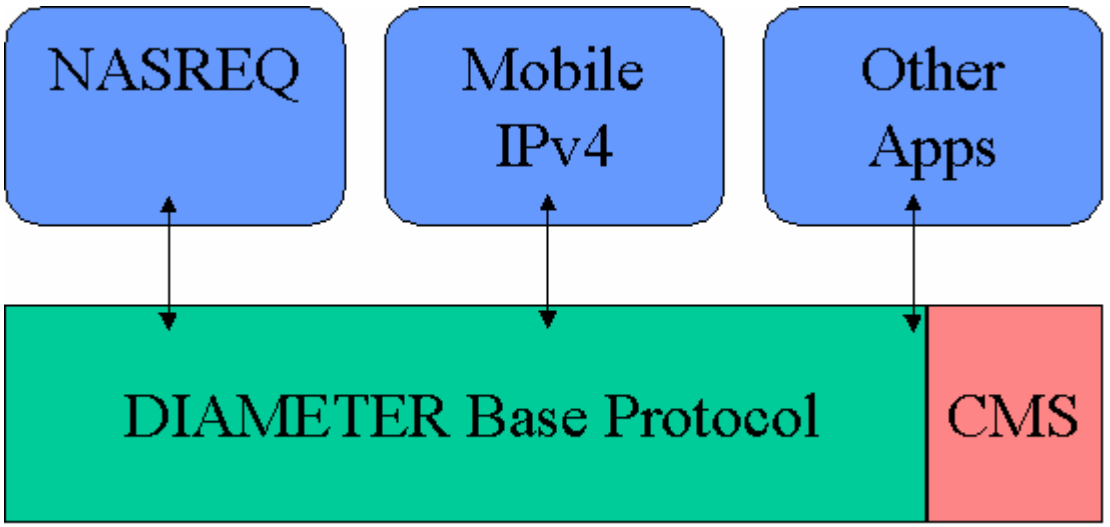
Diameter

- Zeitstempel
  - Verhindert Replay-Attacken
- Platz für Erweiterungen
  - Hersteller-definierbar
  - Garantiert zukünftige Erweiterbarkeit
- IPSec und TLS
  - Dank IPSec und Transport Layer Security ist kein „shared secret“ mehr nötig
- End-to-End Sicherheit mit CMS
  - Verhindert Manipulationen auf dem (unsicheren) Übertragungsweg durch Verschlüsselung

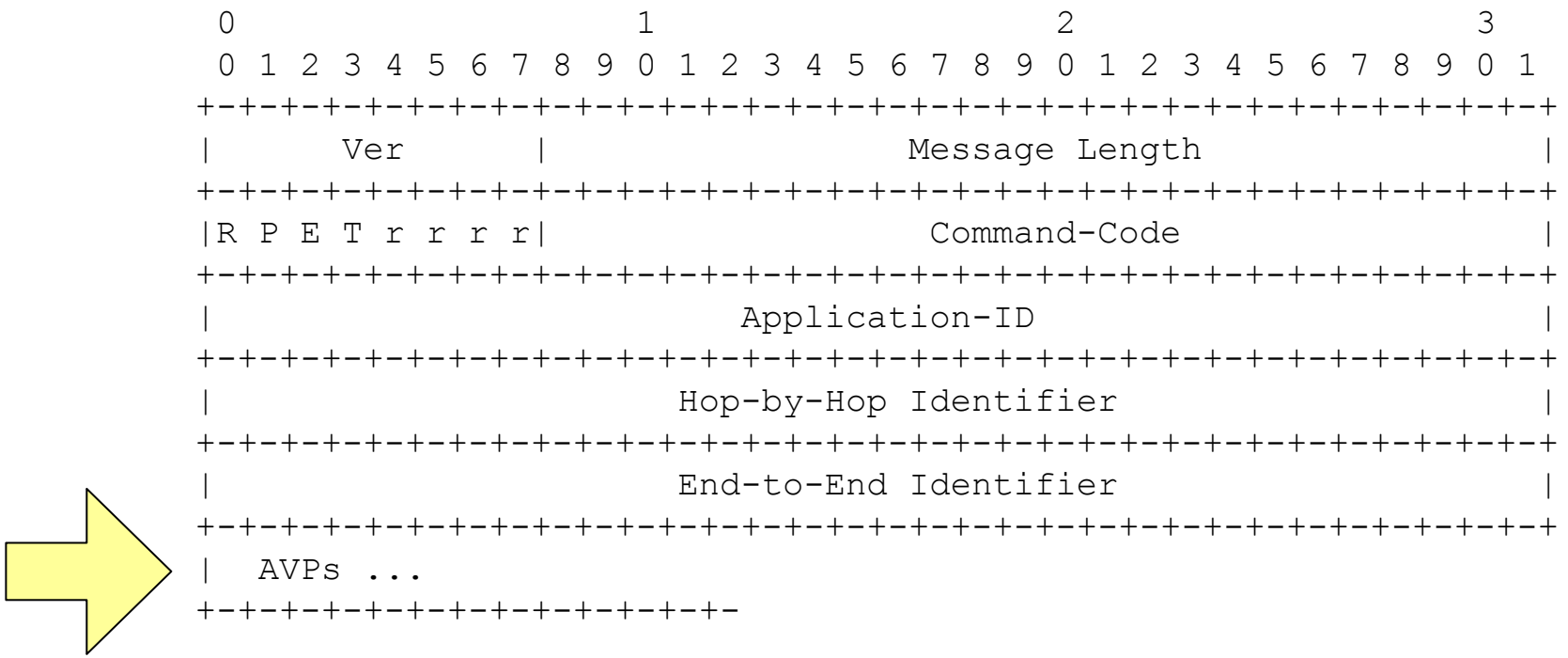
TECHNISCHE UNIVERSITÄT
CAROLO-WILHELMINA
ZU BRAUNSCHWEIG
Institut für Betriebssysteme und Rechnerverbund
http://www.tu-bs.de http://www.ibr.cs.tu-bs.de

Diameter

Protokoll Layout



Diameter


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Ver
Message Length
R P E T r r r r
Command-Code
Application-ID
Hop-by-Hop Identifier
End-to-End Identifier
AVPs ...

Anwendungen

- NASREQ
  - Network Access Server Requirement
    - Ersatz RADIUS
    - In allen dial-in Szenarien verwendet
- Mobile IPv4
  - Netzwerkzugang in Bewegung
- EAP
  - Extensible Authentication Protocol
    - PPP Protokoll
    - Verpackt in Diameters AVPs
- IPFIX
  - Datenflußinformationen sammeln

Ausblick

- IETF proposed standard
- Erste Implementierungen
  - Moby Dick Projekt
  - Open Source
- Ersatz für RADIUS
  - Implementierung komplexer
  - Sicherheitsbedingungen schwerer zu implementieren