Zugangskontrolle zum Ethernet mittels IEEE802.1X

Portbasierte Benutzerauthentisierung im Ethernet
auf der Basis von EAP

Maximilian Riegel

Inhalt

- 802.1X Motivation und Geschichte
- 802.1X Überblick
- Definitionen
- Generelle Architektur
- Prinzipielle Funktionsweise
- Volle Kontrolle und partielle Kontrolle des Ports
- 802.1X Protokoll Überblick
- 802.1X Message Flow
- Weitere mögliche Funktionen
- Zusammenfassung

802.1X Motivation und Geschichte

- Verstärkte Verwendung von 802 LAN (Ethernet) im öffentlichen und halb-öffentlichen Umfeld
- Wunsch nach einem Mechanismus zur Verknüpfung einer Benutzer-Identität mit einem LAN Port
  - Bereitstellung eines kontrollierten LAN-Zugangs
  - Ermöglichung einer benutzungsabhängigen Abrechnung
  - personalisierte Netzumgebung am LAN
- Existierende Ansätze sind nicht ausreichend.
  - Einfaches add-on zu existierenden Geräten und Systemen
  - PPPOE – zu viel Overhead
  - VPN – zu viele herstellerspezifische Lösungen
  - DHCP – nur für Addressierung und Konfiguration

802.1X Motivation und Geschichte, Forts.

- Wiederbenutzung der vorhandenen AAA (Authentication, Authorization, Accounting) Infrastruktur
  - weit verbreitet für Modem-Einwahlzugänge
- Ursprünglich als Erweiterung der Bridging-Spezifikation IEEE802.1D vorgesehen
  - eigene Spezifikation IEEE802.1X, nachdem mehrere andere Anwendungsmöglichkeiten aufgetaucht sind
- Entwurf stammt von 3Com, HP, and Microsoft
- IEEE P802.1X PAR wurde im Januar 1999 gestartet
- Anerkannt als IEEE Standard im Juni 2001
- Die Specification gibt es unter: http://www.drizzle.com/~aboba/IEEE/

Was ist Authentisierung des Netzzugangs?

- Ein Mechanismus, durch den der Zugang zum Netz auf berechtigte Personen/Geräte beschränkt wird
  - Typischerweise wird ein Benutzername als Identität benutzt.
    - *Jeder Benutzer auf einem Multi-User Rechner erhält Zugang zum Netz sobald der Link aktiviert wurde.*
  - Nach erfolgter Authentisierung wird eine Authorisierung fällig, die die Berechtigungen für den Zugang konfiguriert.
    - *Die Berechtigungen können Eigenschaften wie VLAN-ID, Bandbreite, Filter, Tunnels, etc. sein*
- Zur Verhinderung von ‘Hijacking’ ist die Authentisierung eines jeden Pakets notwendig.
  - keine Verschlüsselung der Daten notwendig
  - Der Message Integrity Check (MIC) basiert auf einen während der Authentisierung erzeugten Schlüssels
  - In PPP und in WEP gibt es keinen MIC!

Warum Authentisierung auf dem Link Layer?

- Es ist einfach, billig und schnell
  - PPP und IEEE 802, die verbreitesten Link Layer Techniken unterstützen die Authentisierung.
  - Niedrige Kosten werden bei der hohen Zahl Ports sehr bedeutsam.
- Der Client benötigt keinen Netzzugang um sich zu authentisieren
  - Authentisierung funktioniert auch ohne DNS und DHCP.
- Der Network Access Server (NAS) braucht maximal Layer 3 Funktionalität.
  - Authentication und AAA Support kann normalerweise mit einem Software-Update in bestehender realisiert werden.
- Die Link Layer Authentisierung funktioniert identisch für alle Protokolle.
  - Im IP Layer wären getrennte Methoden für IPv4, IPv6, AppleTalk, IPX, SNA, NetBEUI, … fällig.
  - Layer Interaktionen resultieren in höheren Delays.

IEEE802.1X Überblick

- Methode zur Kontrolle der Benutzer-Identität beim Zugriff auf das Ethernet
  - Idealerweise durchgeführt am Zugangspunkt (z.B. Switch-Port)
- Spezifiziert ein Protokoll zwischen Geräten, die den Zugang zum LAN suchen, und Geräten, die den Zugang zum LAN verwalten
- Beschreibt die Anforderungen an ein Protokoll zwischen dem Authenticator (Zugangspunkt zum LAN) und einen Authentisierungs-Server (z.B. RADIUS)
- Spezifiziert verschiedene Stufen der Zugangskontrolle und dem Verhalten eines Ports, der kontrollierten Zugang bietet.
- Beinhaltet auch Network Management Funktionen über SNMP

IEEE802.1X Überblick, Forts.

- Standardelemente und Definitionen

Supplicant

Authenticator

Authentication Server

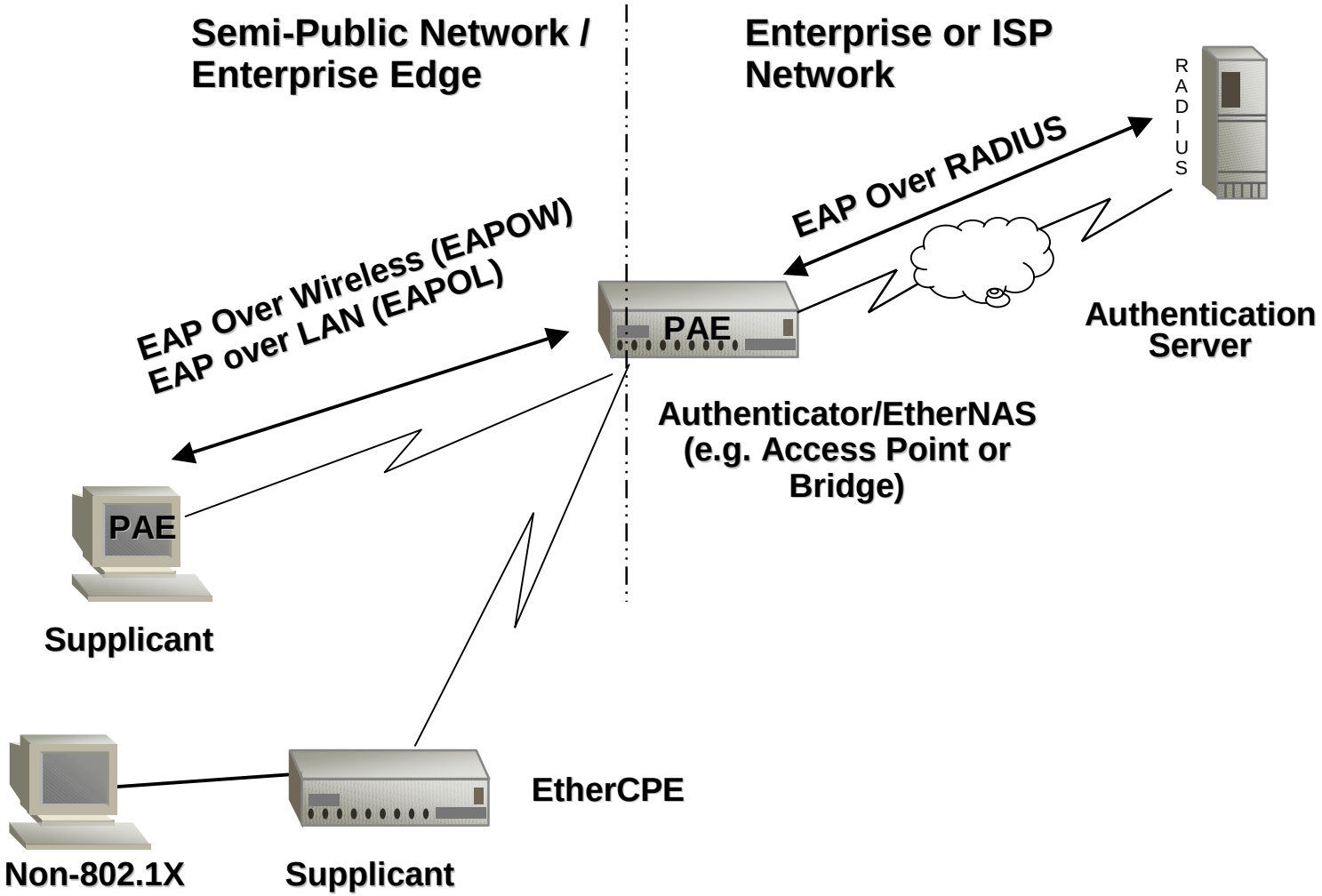
Definitionen

- Authenticator
  - Die Einheit, die die Authentisierung des Gerätes am anderen Ende der Verbindung anfordert
- Supplicant
  - Die Einheit, die Zugang zum LAN sucht und dafür durch den Authenticator überprüft wird.
- Port Access Entity (PAE)
  - Die Protokoll-Instanz die mit einem kontrollierten Port verbunden ist. Die Instanz kann die Funktionalität eines Authenticators, eines Supplicant oder auch beides gemeinsam umfassen.
- Authentication Server
  - Eine Einheit, die die Authentisierung durchführt und das Ergebnis der Authentisierung dem Authenticator mitteilt. Diese Einheit kann mit dem Authenticator integriert sein, ist aber meistens ein externer Server.

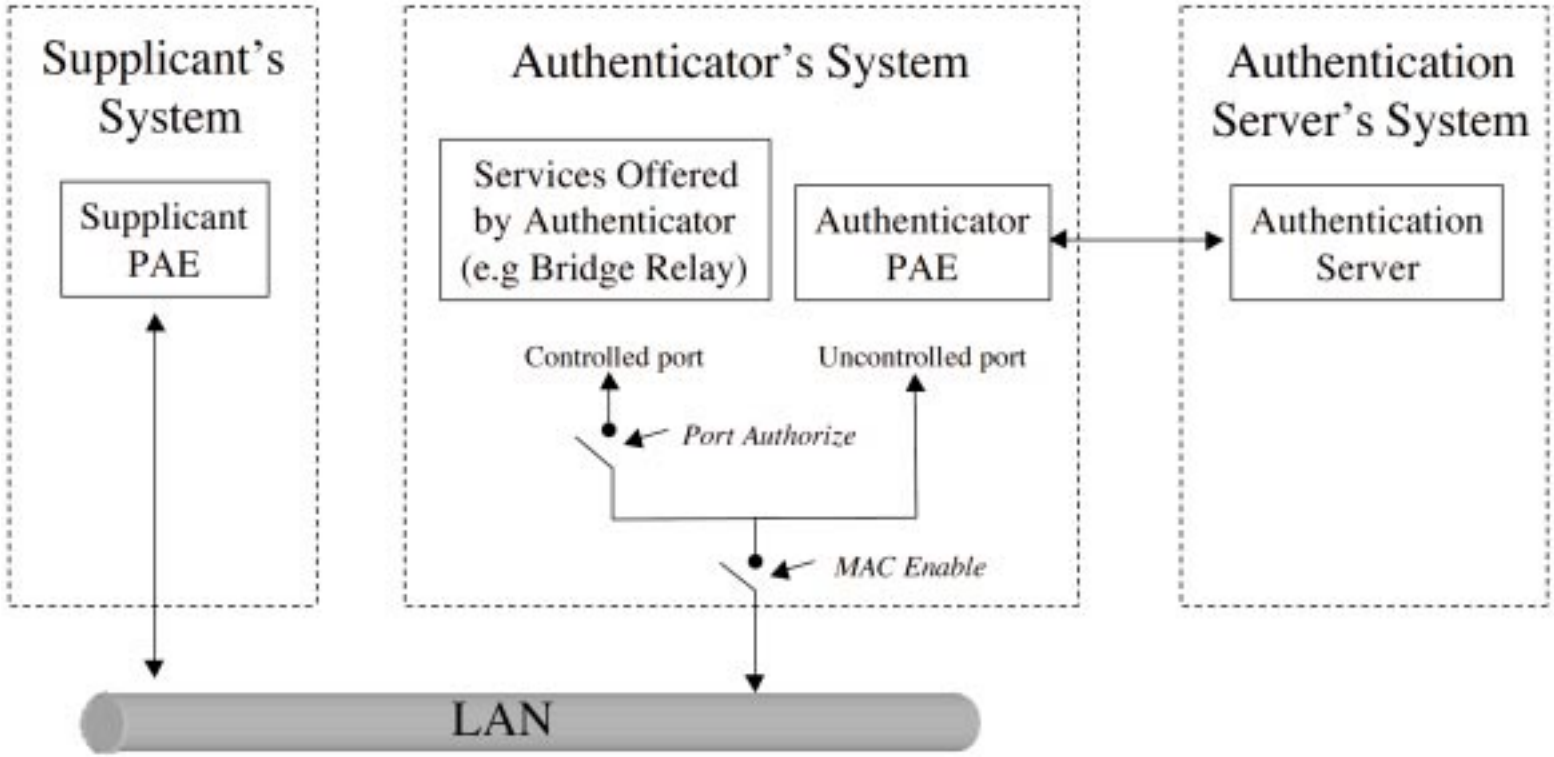
802.1X Sicherheitsphilosophie

- Konzept: ein flexibles Rahmenwerk für Sicherheitslösungen
  - Implementierung der Sicherheitsfunktionen in higher layer
  - Ermöglicht den Einsatz neuer Authentisierungsmethoden und Schlüsselgenerationsmehoden ohne Änderung der Netzkarte oder des Access Points.
  - Kryptographische Berechnungen übernimmt die Haupt-CPU
- Die Funktionsweise:
  - Die Sicherheitsfunktionen werden zwischen Supplicant und Authentisierungsserver realisiert.
  - Die Netzkarte und der Access Point leiten die Daten nur weiter.

802.1X Topologie



Prinzipielle Funktionsweise



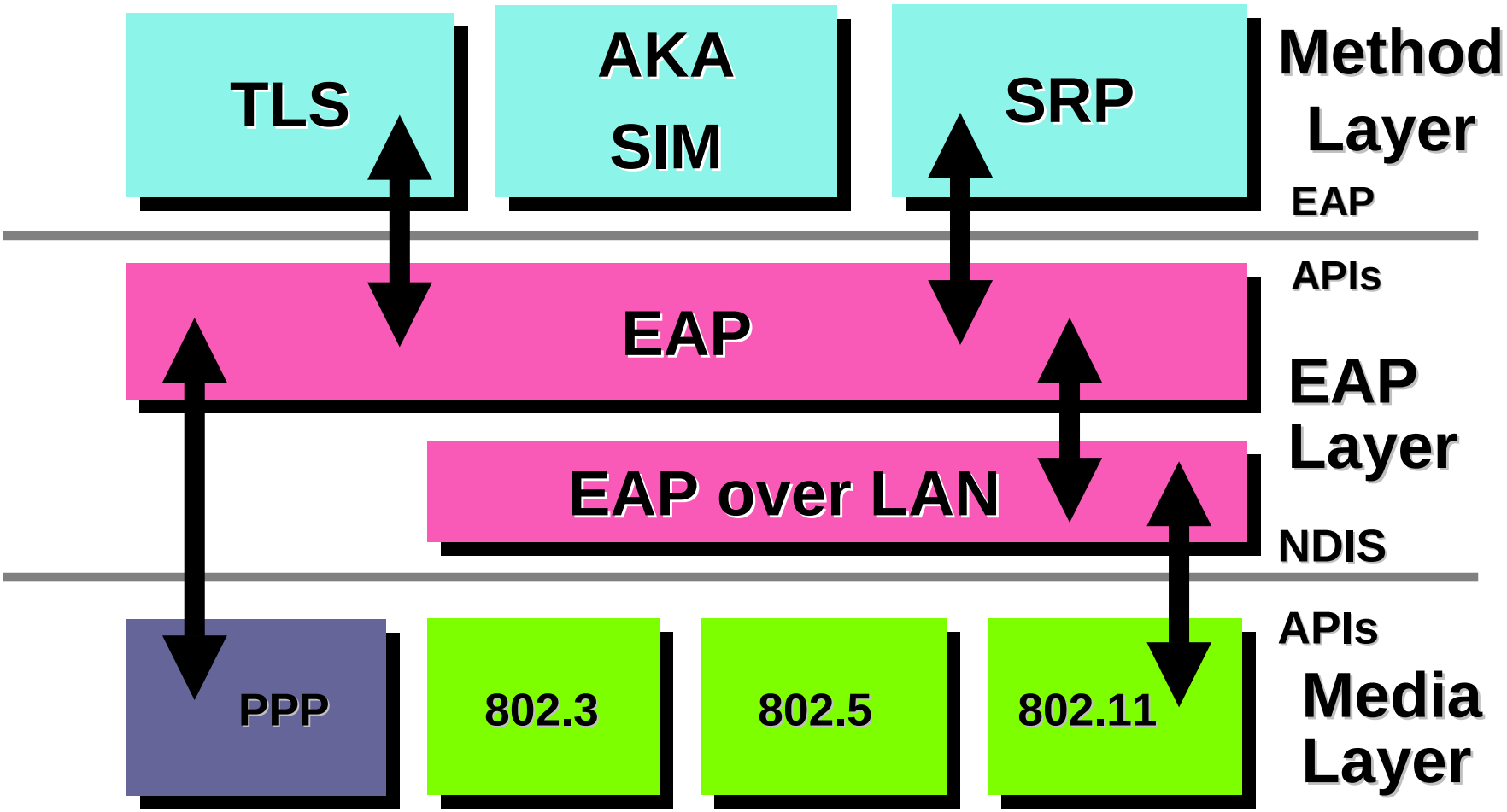
Volle Kontrolle und partielle Kontrolle des Ports

- Volle Kontrolle verhindert jeden Datenaustausch über den kontrollierten Port solange der Teilnehmer nicht authorisiert ist.
- Partielle Kontrolle erlaubt den Datenaustausch über den kontrollierten Port soweit es für Wake-on-LAN benötigt wird
- Durch übergeordnete Funktionseinheiten kann die Partielle Kontrolle bei Bedarf auf Volle Kontrolle ausgedehnt werden (z.B.: durch spezielle Funktionen zur Detektion von Bridges um die Bildung von Rückkoppelschleifen beim Spanning-Tree Verfahren zu vermeiden)

Was ist EAP?

- Das ‘Extensible Authentication Protocol’ (RFC 2284)
  - Flexibles Link Layer Authentisierungsprotokoll
  - Einfacher Datentransport
    - *Keine Notwendigkeit zu IP*
    - *ACK/NAK, kein ‘windowing’*
    - *Fragmentierung wird nicht unterstützt.*
  - Nur geringe Anforderungen an den Link Layer
    - *Funktioniert über jede Art von Link Layer (PPP, 802, etc.)*
    - *Verlangt keinen sicheren Link*
    - *Benötigt kein ‘re-ordering’*
    - *Funktioniert über fehlerfreie und fehlerbehaftete Links*
- EAP Methoden auf Basis von IETF standards:
  - Transport Level Security (TLS)
  - Secure Remote Password (SRP)
  - GSS_API (including Kerberos)

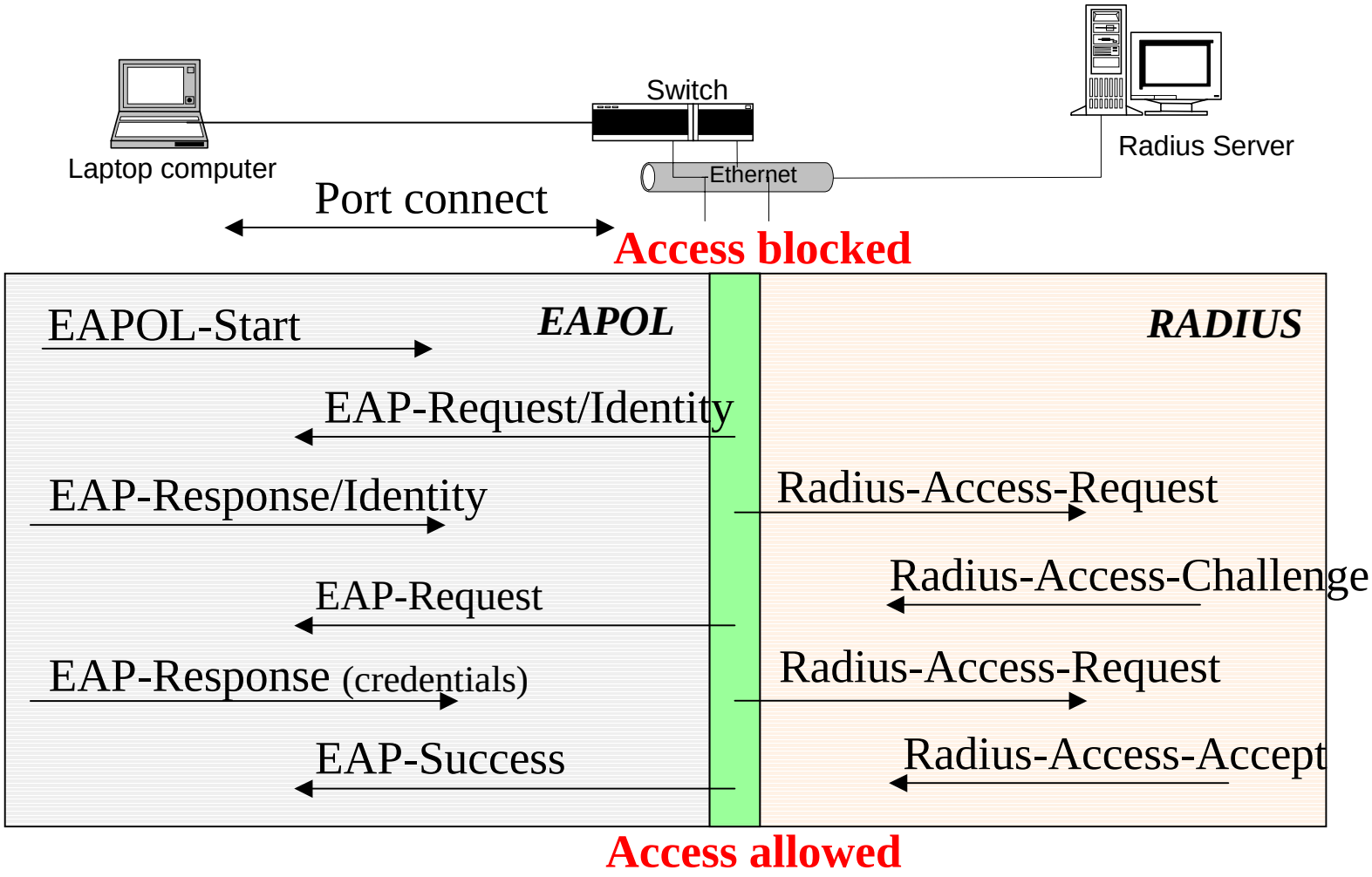
EAP Architektur



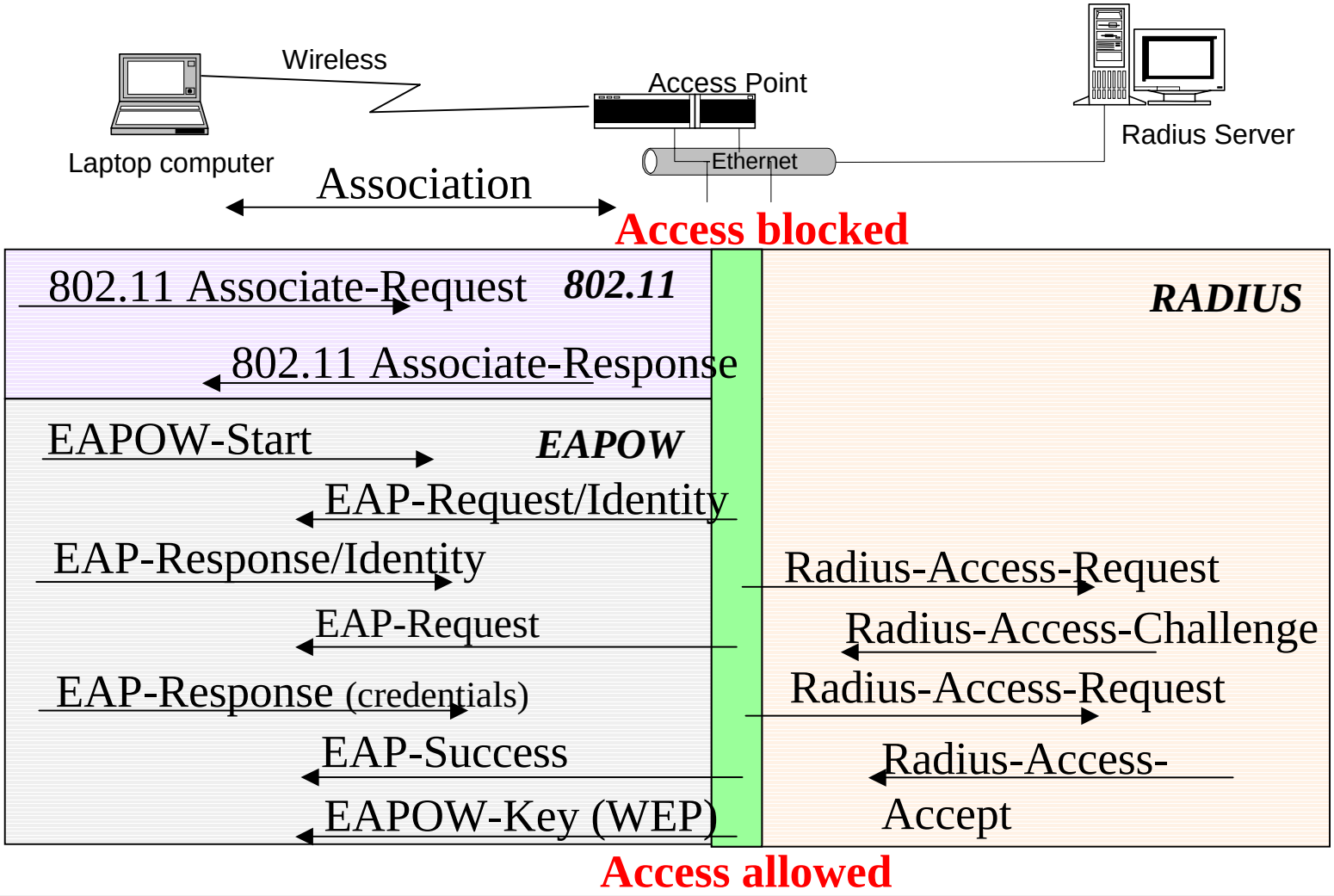
802.1X Protokoll Überblick

- Packt das Extensible Authentication Protocol (RFC 2284) in 802 Frames ein (EAPOL) und stellt einige Erweiterungen speziell für 802-LANs Verfügung
- EAP ist ein universelles Authentisierungsprotokoll, das die Verwendung verschiedenen Authentisierungsverfahren (z.B.: Smart-Cards, Kerberos, Public Key Verfahren, One-time password, statisches Passwort, usw.)
- Der Authenticator leitet die Authentisierung zwischen Supplicant und Authentisierungs-Server durch.
- Die PAE im Authentisator erwirkt den kontrollierten Zugang zum LAN anhand der Ergebnisse des Authentisierungs-verfahrens
  - wird vom Authentisierungs-Server an den Authentisator gemeldet

802.1X Nachrichtenfluss



802.1X im Zusammenspiel mit 802.11



Weitere mögliche Funktionen

- Ermöglicht die Zuweisung zu einem bestimmten VLAN anhand der Ergebnisse der Authentisierung
  - nicht authentisiertes VLAN
  - Management von Terminals nach fehlgeschlagener Authentisierung
  - Zuweisung zu einem bestimmten VLAN anhand der Benutzer Identität
- Ermöglicht die Einführung einer benutzerabhängigen Registrierung der LAN Nutzung
- Ermöglicht die Zuweisung von verschiedenen Traffic-Klassen zu bestimmten Benutzern
- Ermöglicht den Austausch von Schlüsseln zur Kryptisierung von Benutzerdaten

Zusammenfassung: IEEE 802.1X

- Der IEEE Standard für kontollierte LAN-Zugänge.
  - Verabschieded: June 2001
  - Basiert auf EAP, IETF RFC 2284
- Eine Architektur für Authentisierung und Key Management
  - IEEE 802.1X erzeugt Schlüssel für die ‘per-packet’ Authentisierung, Integritätsprüfung und Verschlüsselung.
  - Typischerweise wird sie mit bekannten Algorithmenten benutzt (e.g. TLS, SRP, etc.)
  - IEEE 802.1X kann auch im ‘weniger sicheren’ Umfeld eingesetzt werden.
    - *Authentisierung allein, oder Authentisierung und Encryption*
    - *Encryption alleine ist nicht ausreichend.*
- Was ist IEEE802.1X **nicht**!
  - Ein reiner Standard für Wireless
    - *Er ist für alle IEEE 802 technologies (e.g. Ethernet First Mile) einsetzbar.*
  - PPP over Ethernet (PPPOE)
    - *802.1X unterstützt nur EAP Methoden (kein PAP, keinCHAP)*
  - Eine Verschlüsselungstechnik
    - *Kein Ersatz für WEP, RC4, DES, 3DES, AES, etc, aber kann für die Schlüsselgenerierung eingesetzt werden.*

Zusammenfassung: IEEE 802.1X, Forts.

- Einfacher Mechanismus zur benutzerabhängigen Zugangskontrolle zum LAN
- Anwendbar fur eine Vielzahl verschiedener Geräte
  - 802.1D Bridges
  - 802.11b Access Points
  - Smart 802.3 Repeater
  - DSL Modems
- Verwendet existierende AAA Infrastruktur
- EAP ist offen für neue Authentisierungsverfahren

802.1X Implementatierungen

- Implementierungen sind verfügbar für:
  - IEEE 802.1X Support ist Bestandteil von Windows XP
  - Firmware upgrades gibt es von vielen AP and NIC Herstellern
  - Interoperability testing ist begonnen worden.
- 802.1X OS support
  - Microsoft: Windows XP
  - Cisco: Windows 9x, NT4, 2000, Mac OS, Linux
  - Open Source: Open1x

Links zu 802.1X Herstellern

- Microsoft, AirWave, Compaq, Dell, IBM, Intel, HP, Symbol, Toshiba, Telson, Wayport
  - http://www.microsoft.com/presspass/press/2001/Mar01/03-26XPWirelessPR.asp
- 3Com
  - http://emea.3com.com/news/news01/mar26.html
- Agere
  - http://www.networkmagazine.com/article/COM20010629S0009
  - http://www.lucent.com/micro/NEWS/PRESS2001/080801a.html
- Enterasys
  - http://www.dialelectronics.com.au/articles/c4/0c0023c4.asp
  - http://www.computingsa.co.za/2001/03/26/News/new07.htm
- Intersil
  - http://www.intersil.com/pressroom/20010403_802_1xWindows_XPFINAL_English.asp
- Cisco
  - Catalyst switches
    - *http://www.redcorp.com/products/09084608.asp*
  - 802.11 access points
    - *http://www.security-informer.com/english/crd_security_495312.html*
    - *http://cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1281_pp.pdf*

Das Ende

- Danke für Ihre Aufmerksamkeit.
- Fragen, Anregungen?

Maximilian Riegel *email: riegel@max.franken.de*
http://www.max.franken.de

- Links:
  - IEEE 802.1X
    - *http://grouper.ieee.org/groups/802/1/pages/802.1x.htm*
  - Bernard Aboba's WLAN Security site
    - *http://www.drizzle.com/~aboba/IEEE/*