

---

# IEEE 802.1x Erfahrungsbericht aus der Fraunhofergesellschaft

---

**Dipl.-Ing. Mathias Gärtner**

Sachverständigenbüro Prof. Pausch & Partner  
Heinheimer Strasse 38

D-64289 Darmstadt

Tel.: +49 6151 9712640

Fax.: +49 6151 9712641

Email: [Mathias.Gaertner@it-svbuero.de](mailto:Mathias.Gaertner@it-svbuero.de)

<http://www.it-svbuero.de>

**Dipl.-Ing. Mathias Gärtner**

Leiter CC-LAN der Fraunhofergesellschaft

Fraunhofer IGD

Fraunhoferstrasse 5

D-64283 Darmstadt

Tel.: +49 6151 155-316

Fax.: +49 6151 155-399

Email: [Mathias.Gaertner@igd.fraunhofer.de](mailto:Mathias.Gaertner@igd.fraunhofer.de)

<http://www.igd.fraunhofer.de>



**SACHVERSTÄNDIGEN-BÜRO FÜR COMPUTERWESEN**

**PROF. DR. PAUSCH & PARTNER**

öffentlich bestellte und vereidigte Sachverständige

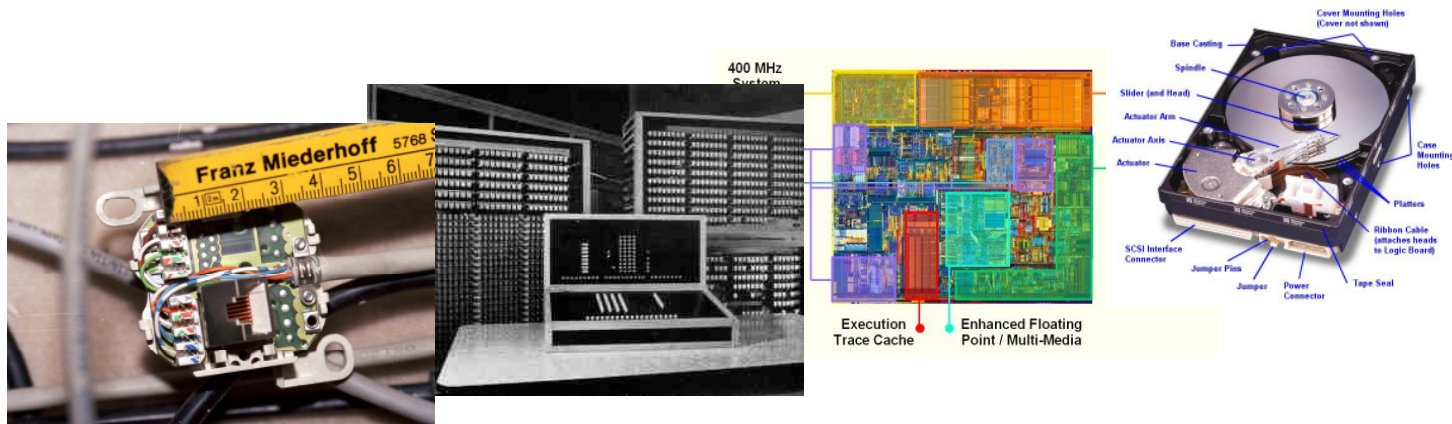


**Fraunhofer**

Institut  
Graphische  
Datenverarbeitung

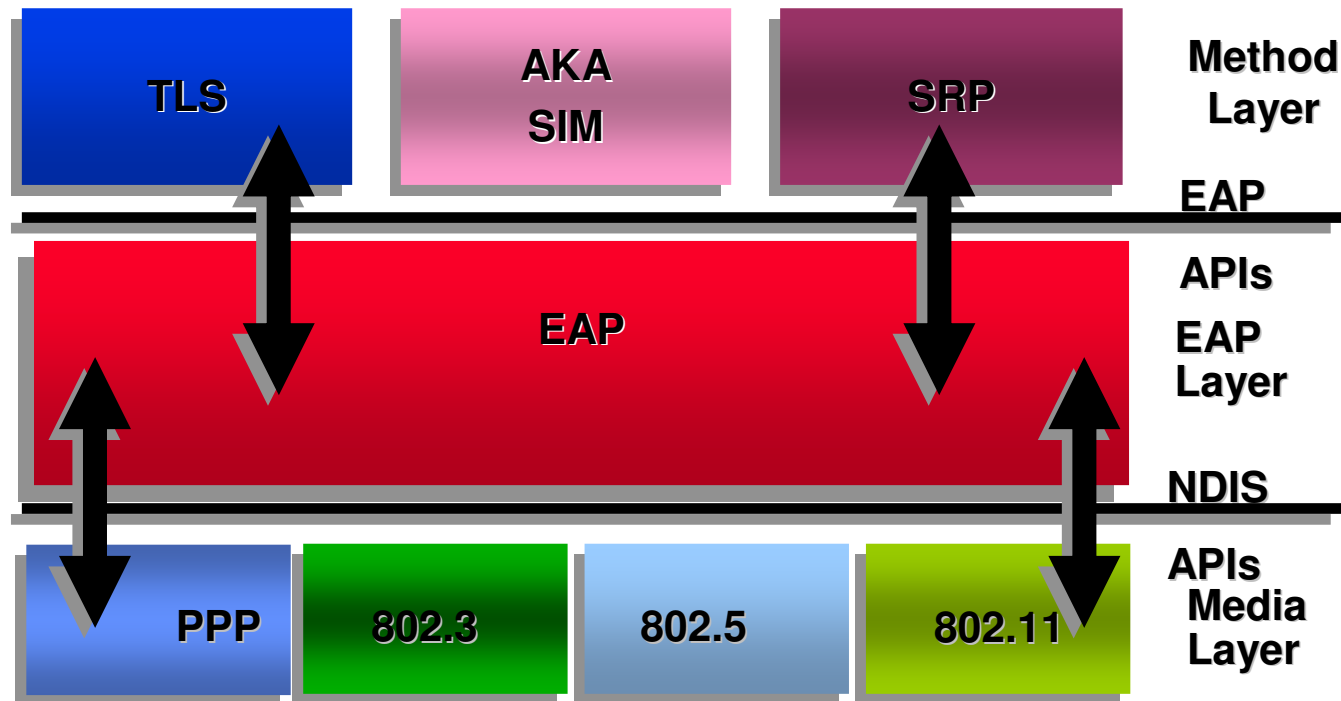
# Agenda

- Einführung in die Technik
- Vorteile
- Nachteile
- Zusammenfassung

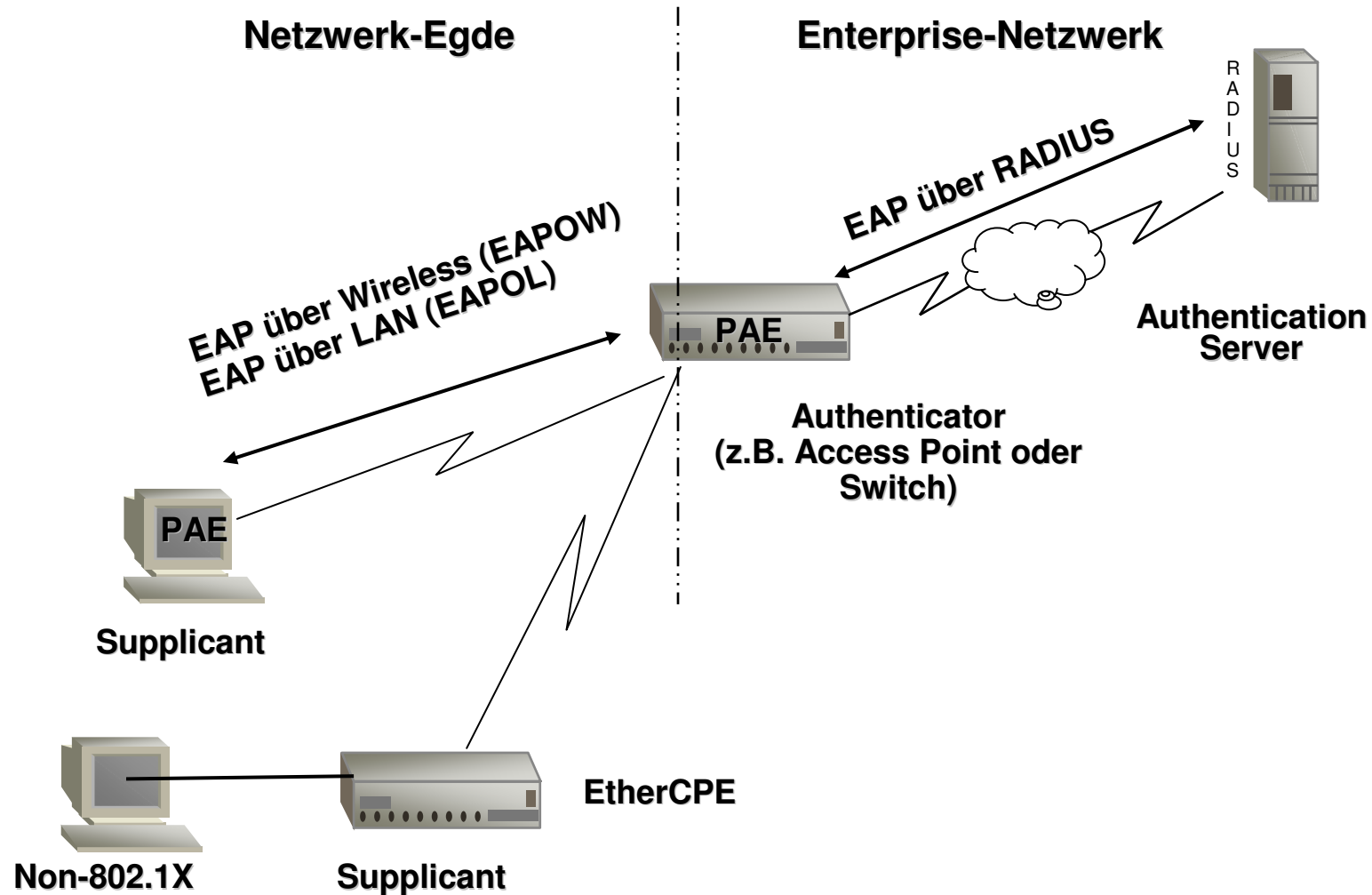


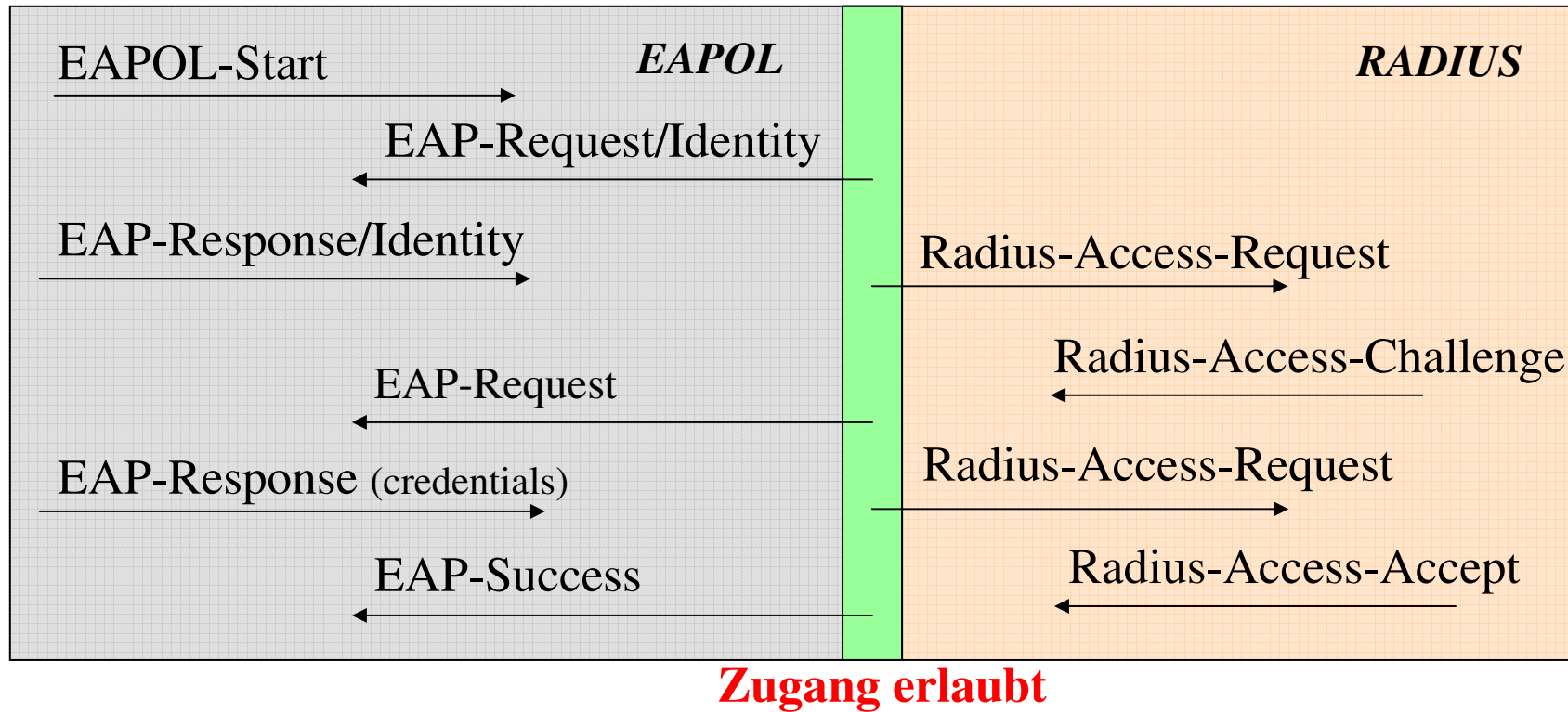
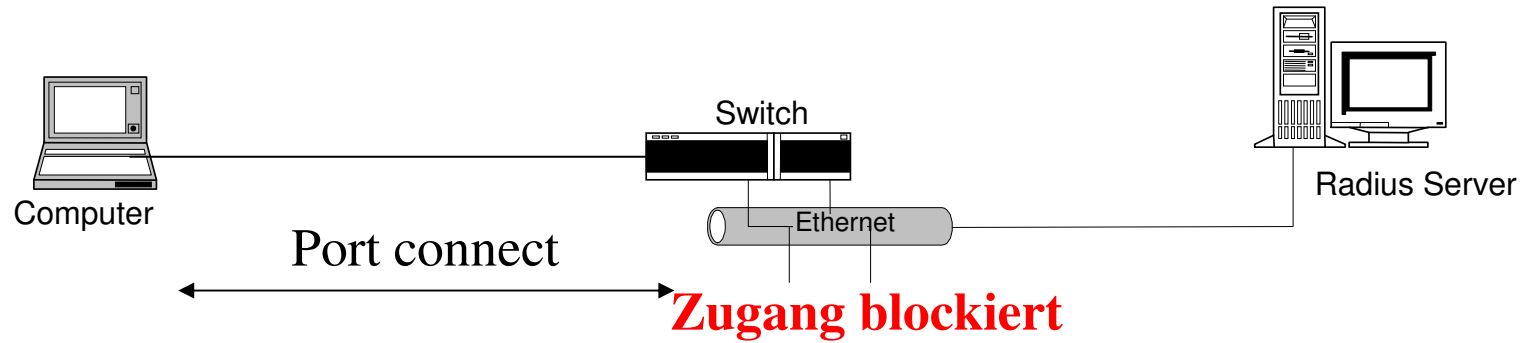
# Einführung in IEEE 802.1x

- Protokoll zur Authentifizierung des Netzwerkzuganges
- Authentifiziert Benutzer und Systeme am Netzwerk-Port oder Access-Point
- Benutzt RADIUS als Datenspeicher bzw. Protokoll
- Standardisiert im Juni 2001
- Basierend auf EAP nach RFC 2284



# IEEE 802.1x Topologie und Begriffe

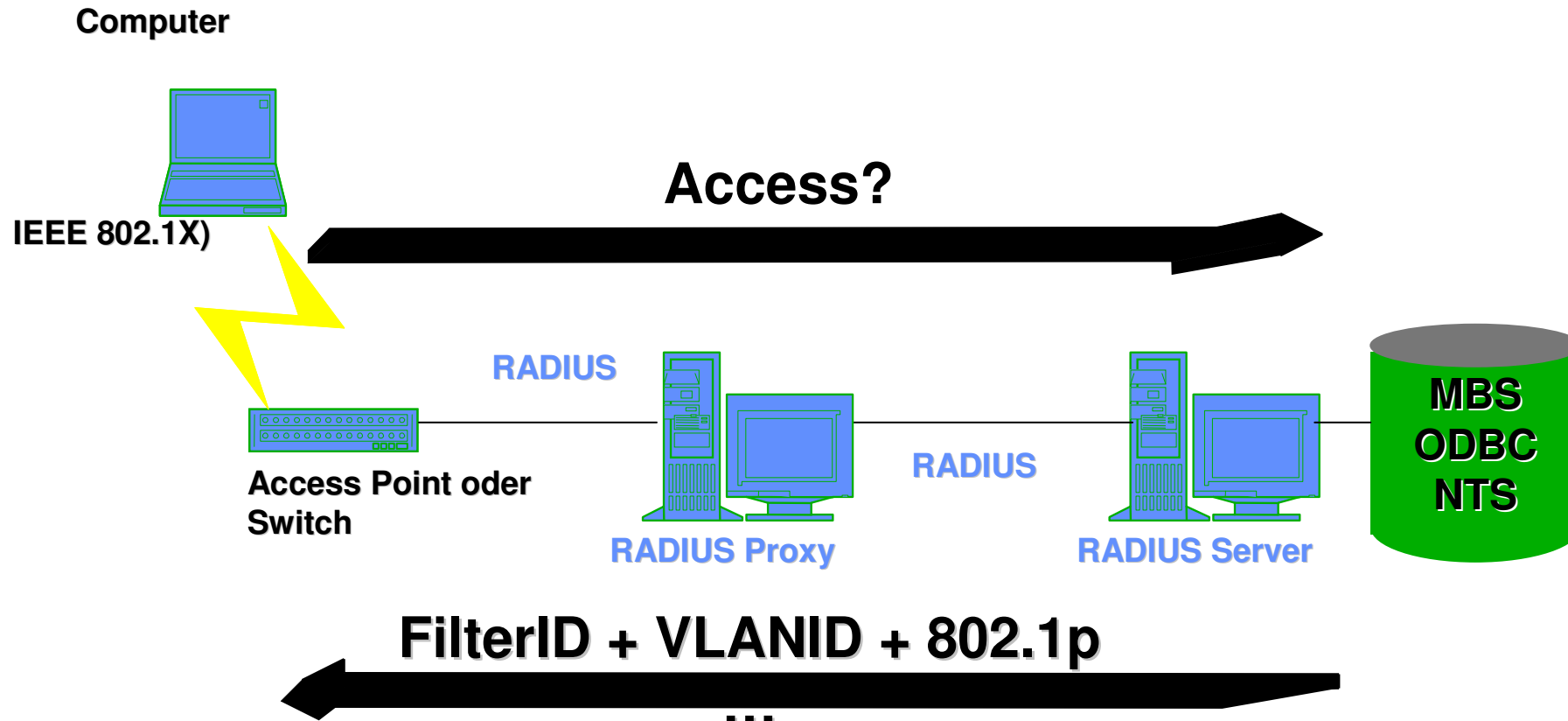






# Zusätzliche Informationen in der RADIUS Access-Accept-Message

- VLAN-ID
- Filterlisten
- Ratelimits



# Vorteile

---

- Nur autorisierte Entitäten haben Netzwerkzugang
- Entitäten können
  - Computer (MAC-Adressenbasiert) oder
  - Benutzersein
- Durch VLAN-IDs völlige Freizügigkeit der User im Netz bei immer gleichen Sicherheitsparametern
- Sehr feine Kontrolle des Netzzugangs möglich
- Verfügbar für (fast) alle Systeme
- Accounting möglich



# Nachteile

---

- Wake-on-LAN
- Softwareverteilung
- Multi-User-Systeme
- DHCP (bis einschließlich Windows XP SR1)
- Group-Policies (bis einschließlich Windows XP SR3, Vista?)
- Reines MAC-based IEEE 802.1x
- Spezielle Endgeräte



# IEEE 802.1x und Group-Policies bei dynamischen VLANs

---

- Nach dem Windows-Login wird eine verschlüsselte Verbindung zum Policy-Server (PDC, ADS) aufgebaut.
- Windows-Login wird als ID für Dot1x verwendet
- Nach erfolgreicher Authentifizierung wird ggf. das VLAN geändert
- Computer erhält neue IP-Adresse
  
- Und was macht der Tunnel?



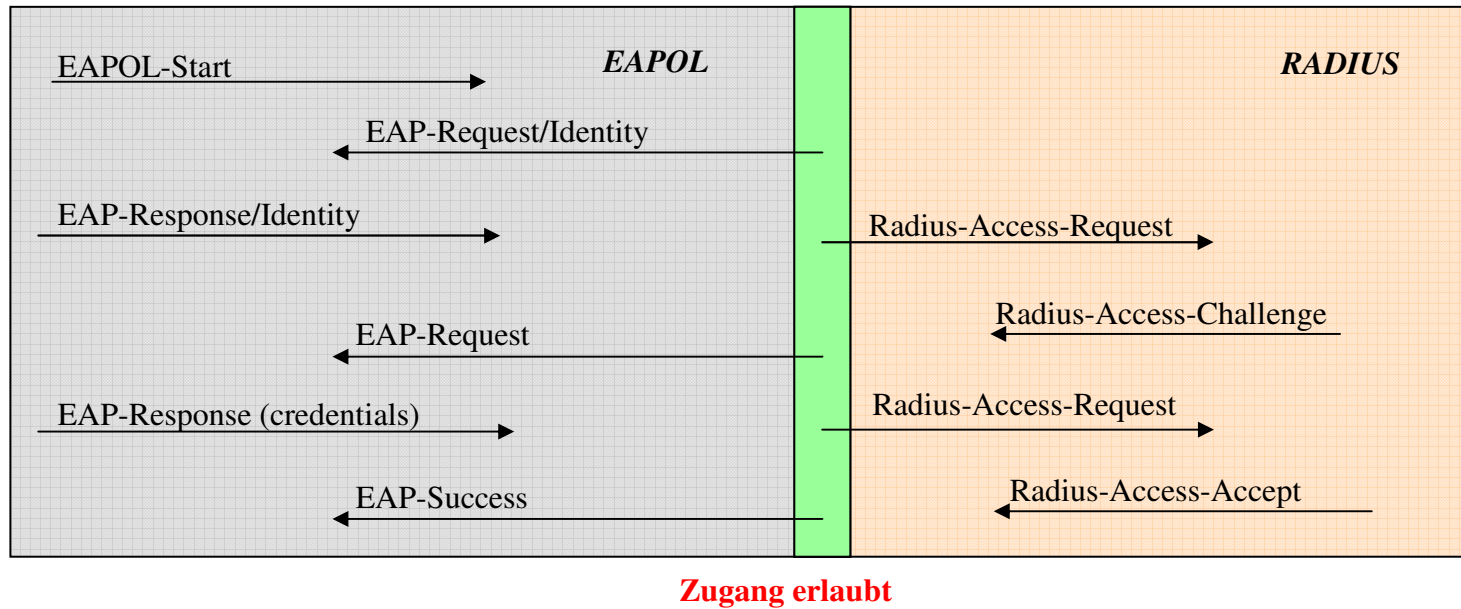
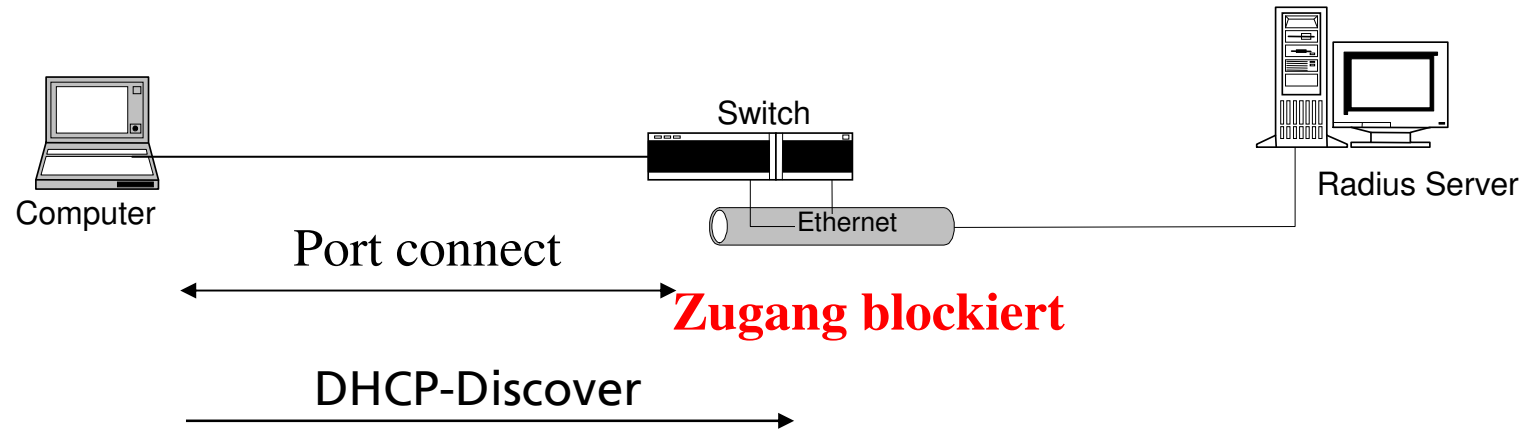
# Wake-on-LAN und Softwareverteilung

---

- Jeder Port ist im nicht authentifizierten Zustand NICHT verbunden
  - Keine Broadcasts
  - Keine Unicasts
  - Keine Multicasts
- WoL-Pakete kommen nicht an der Schnittstelle an
- Softwareverteilung ohne eingeloggten Benutzer?



# DHCP und IEEE 802.1x



# IEEE 802.1x mit Mac-Adressen

---

- Funktioniert problemlos, aber
- Wird ein Computer mit eingeschalteter Dot1x-Authentifizierung angeschlossen, dann
  - wird der EAP-Prozess gestartet und
  - es folgt meist ein „Reject“ vom Radius-Server
- Einige Switchhersteller stoppen dann den Prozess  $\Rightarrow$  Keine MAC-Adressauthentifizierung



# Spezielle Endgeräte

---

- Z.B. Drucker melden sich selten am Netzwerk, einen User gibt es auch nicht...
- Labormessgeräte dito



# Zusammenfassung

---

- IEEE 802.1x ist eine sinnvolle und funktionale Lösung zur Authentifizierung und Strukturierung des Netzwerkes
- Einige Endgeräte sind problematisch
- Bestimmte Techniken (z.B. WoL) sind problematisch
- Nicht immer stimmt die Reihenfolge beim Starten eines (Windows)-Rechners



