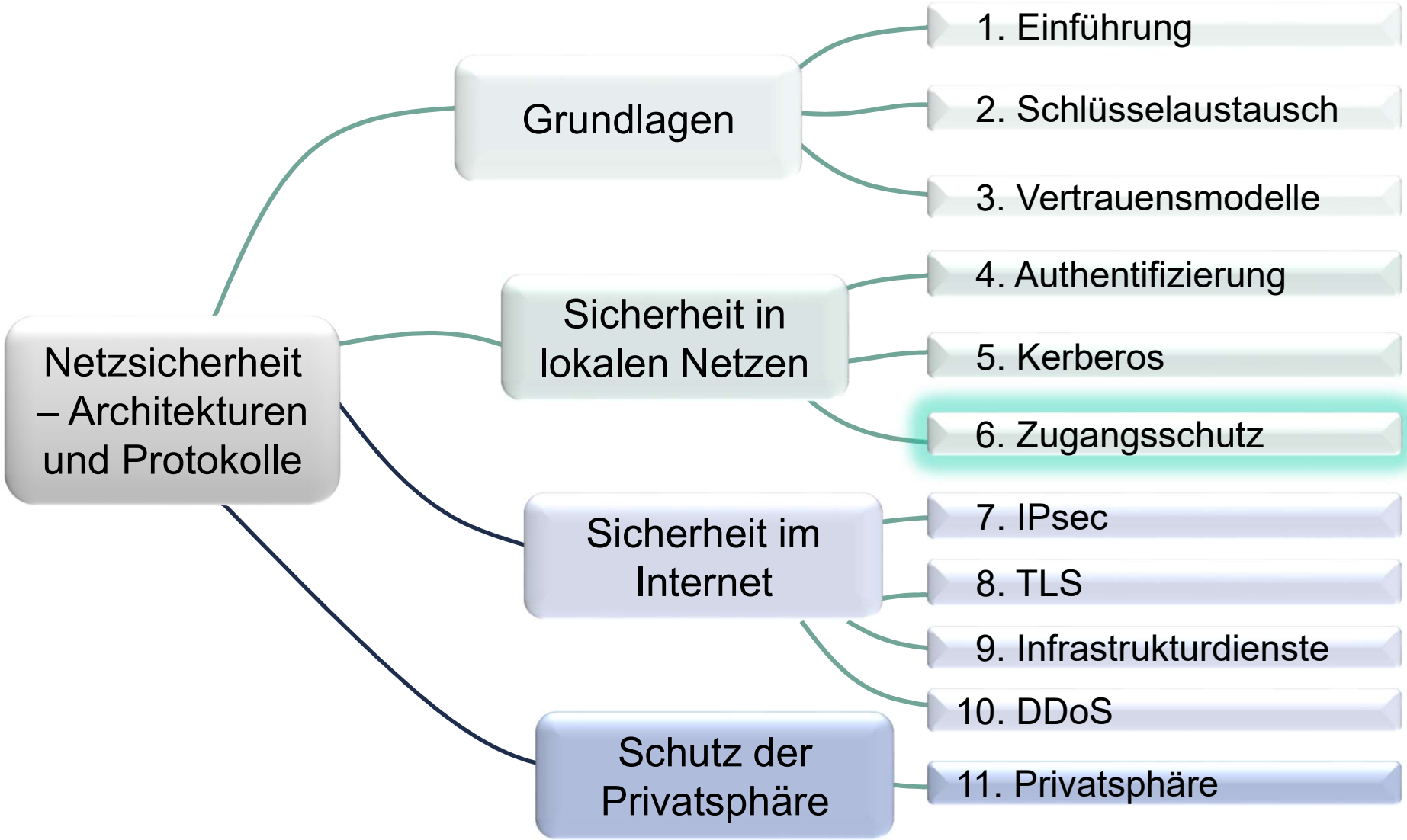
Karlsruher Institut für Technologie

Vorlesung Netzsicherheit
Kapitel 6 – Zugangsschutz

PD Dr. Ingmar Baumgart, PD Dr. Roland Bless, Matthias Flittner, Prof. Dr. Martina Zitterbart
baumgart@fzi.de, [bless, flittner, zitterbart]@kit.edu

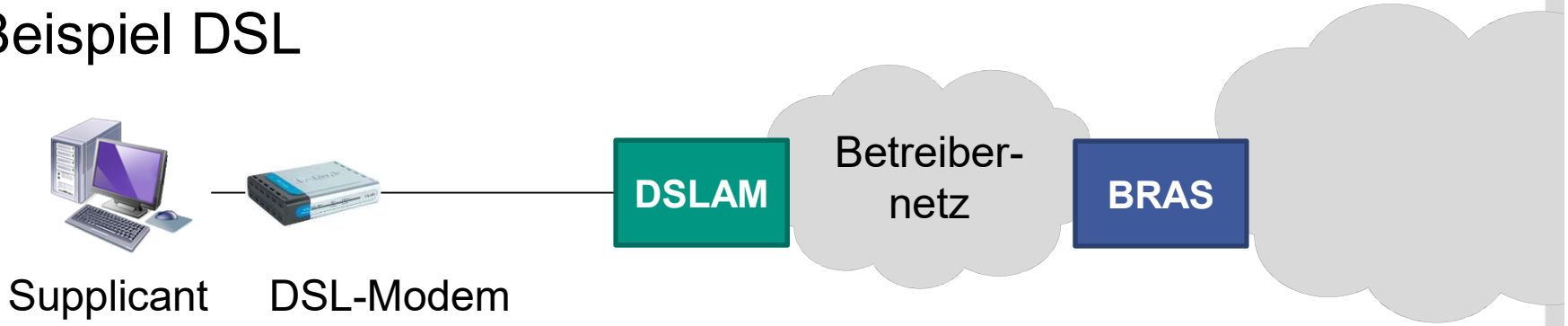
Institut für Telematik, Prof. Zitterbart

Inhalte der Vorlesung

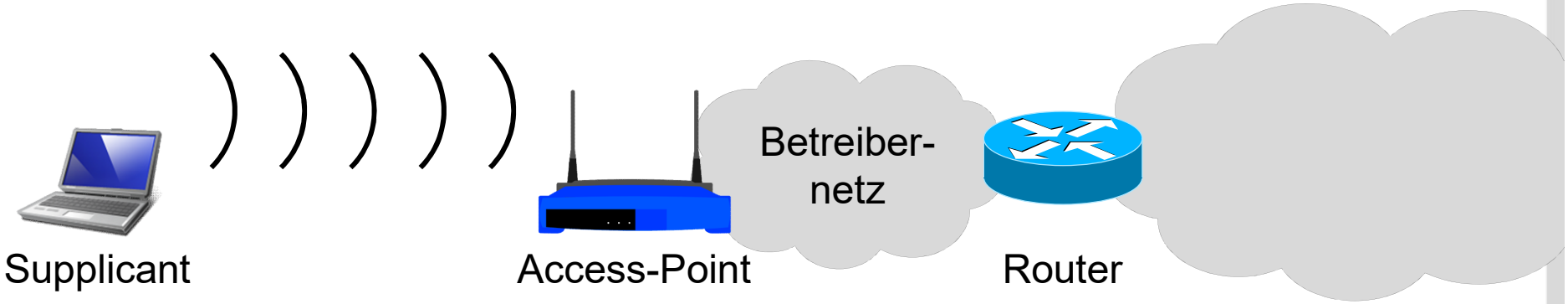


Netzzugang – Motivation

- Beispiel DSL

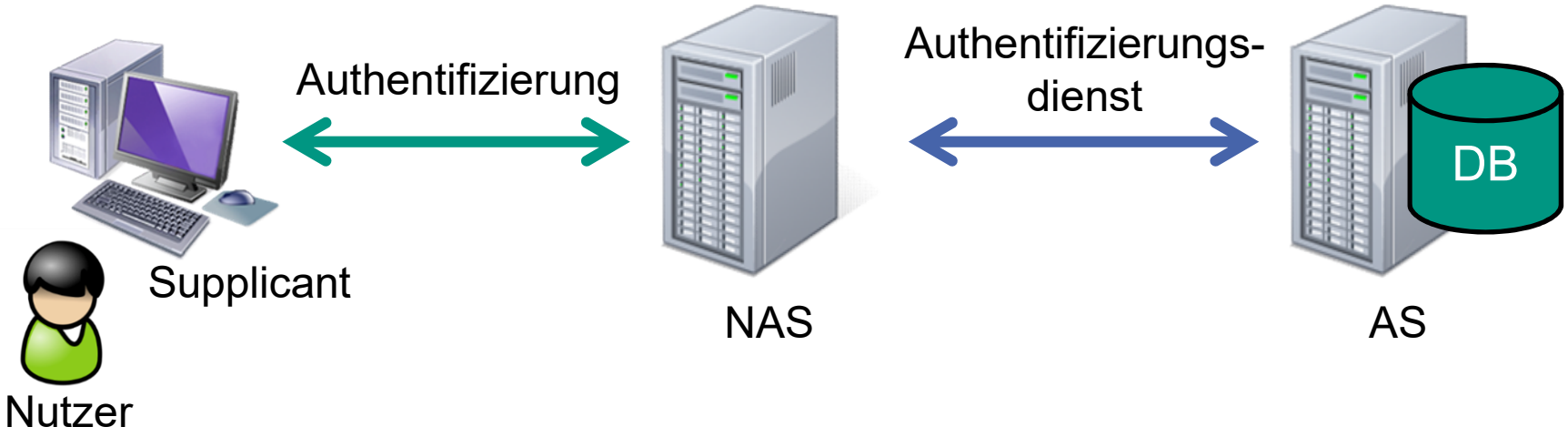


- Beispiel WLAN



Bestandteile Zugangsschutz

- Network Access Server (NAS)
  - Einwahl- / Verbindungspunkt für Nutzer
- Authentication Server (AS)
  - Verfügt über Datenbank mit Nutzerdaten

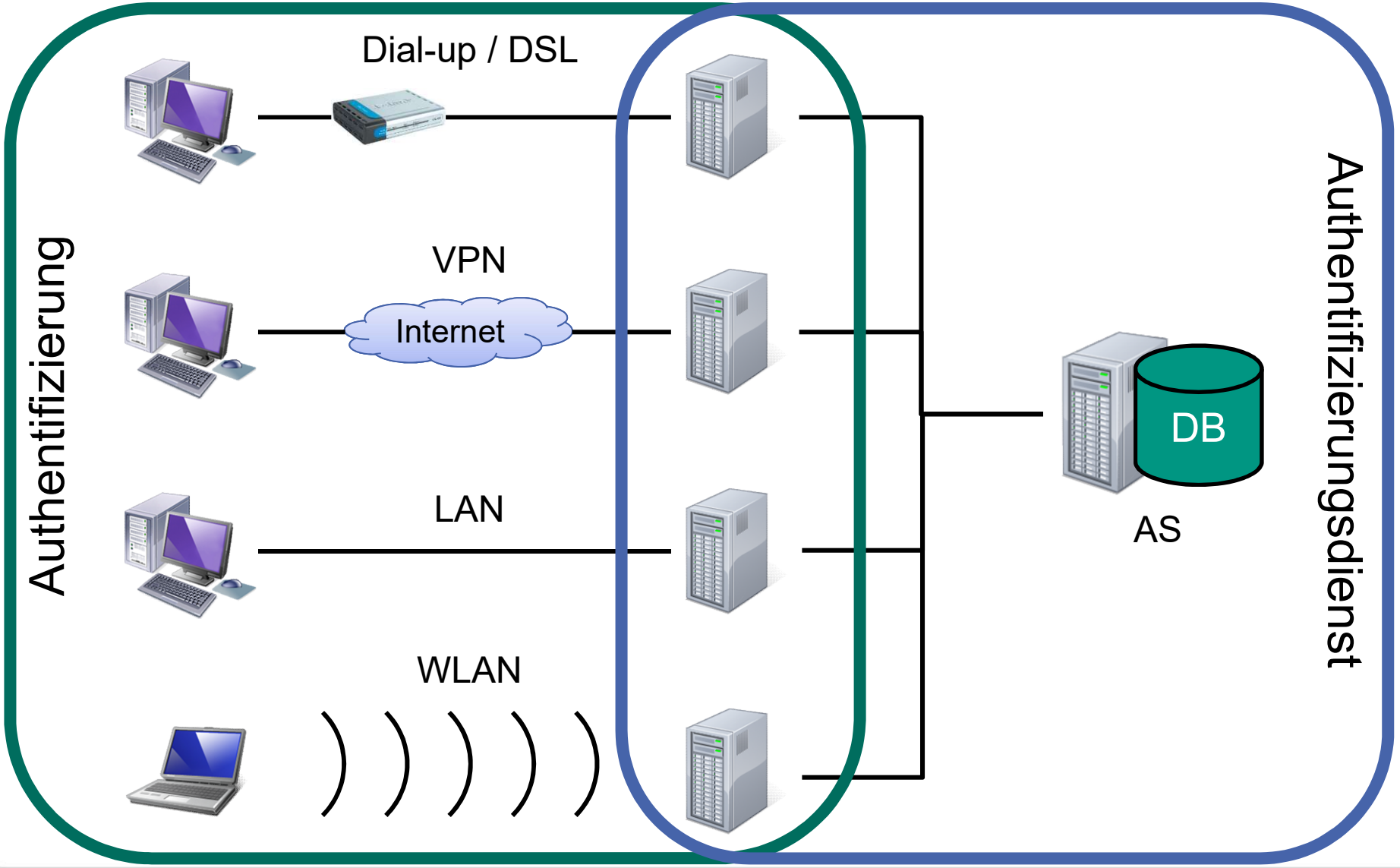


- Authentifizierung: zwischen Supplicant und NAS
- Authentifizierungsdienst: zwischen NAS und AS

Aufgaben von NAS und AS

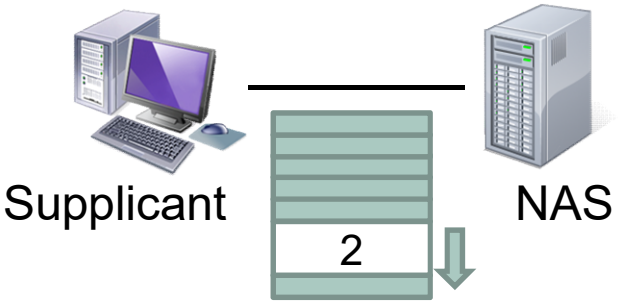
- Network Access Server (NAS)
  - Blockiert zunächst Zugriff auf das Netz bzw. Dienste
  - Gewährt nach erfolgreicher Authentifizierung und Autorisierung des Supplicants Zugriff auf das Netz bzw. Dienste
  - Weiterleitung von Dateneinheiten
- Authentication Server (AS)
  - Speichert Informationen zum Nutzer
    - z.B. Erlaubte Dienste, Berechtigungen, Nutzungsvolumen
  - Nimmt Authentifizierungsanfragen entgegen und bestätigt diese (oder lehnt sie ab)
  - Verteilt eventuell kundenspezifische Merkmale
    - z.B. IP-Adresse, Namensserver, Gateway

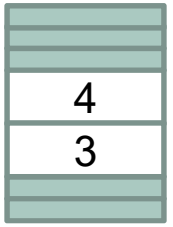
Netzzugangstechniken



Verschiedene Netzzugangstechniken

- Dediziertes physisches Medium
  - Direkte Punkt-zu-Punkt-Verbindung
  - z.B. bei POTS, ISDN, LAN
- Geteiltes Medium
  - Hier: Drahtgebunde Punkt-zu-Mehrpunkt-Verbindung
  - z.B. bei DSL, DOCSIS (Kabelnetz), LAN (Bus)
- Broadcast Medium
  - Hier: Drahtlose Punkt-zu-Mehrpunkt-Verbindung an alle in Empfangsreichweite
  - z.B. bei WLAN, GSM, UMTS, LTE
- Netzwerkübergreifend (z.B. über Internet)
  - Supplicant ist nicht im gleichen lokalen Netz wie NAS
  - z.B. bei VPN





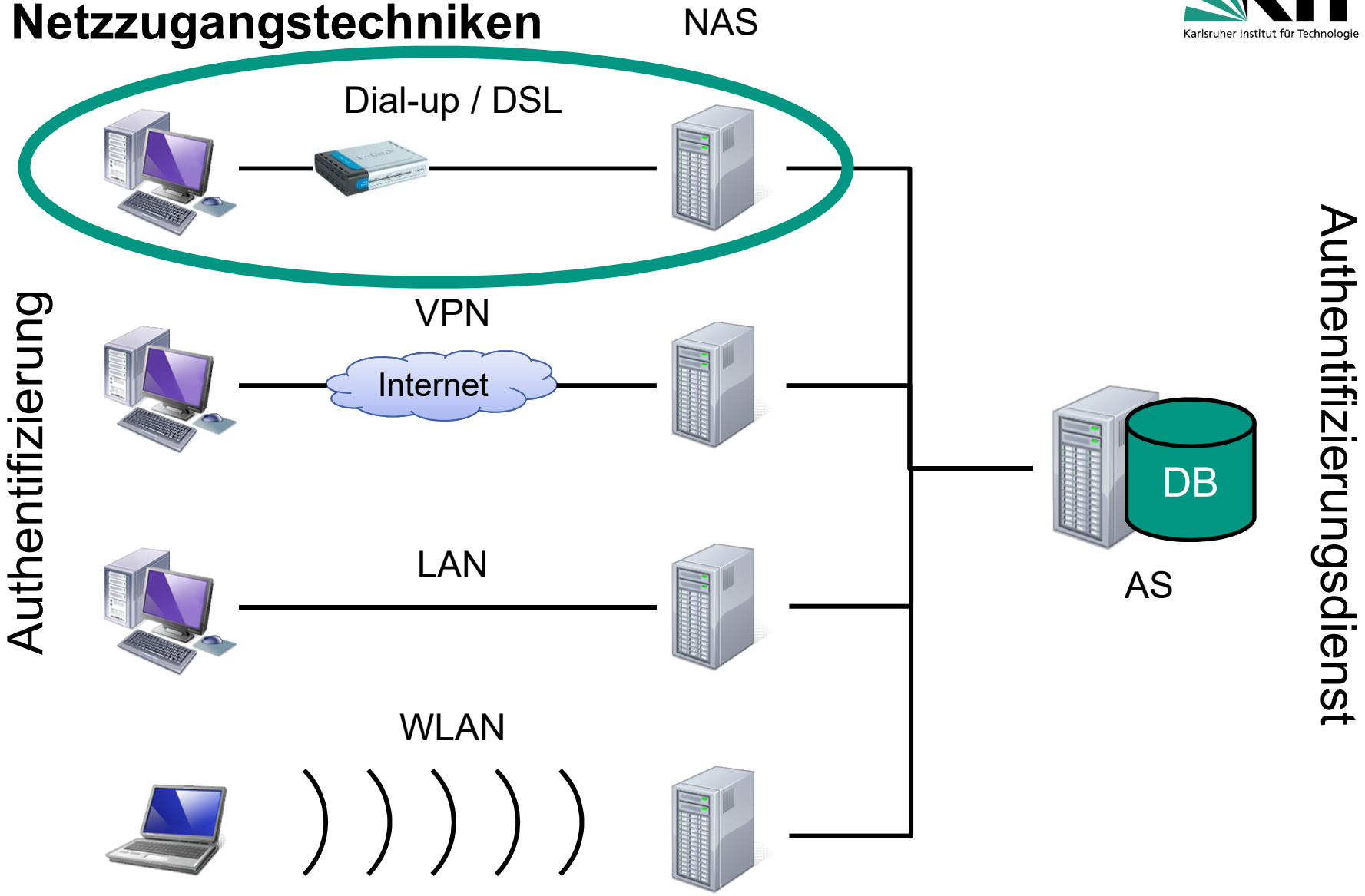
Sicherheitsbetrachtung

- Dediziertes physisches Medium
  - Angriffe schwer
  - Erfordern physischen Zugriff auf dediziertes Zugangsmedium
- Geteiltes Medium
  - Angriffe für Insider leicht (z.B. ARP- / IP-Spoofing)
  - Externe Angriffe benötigen physischen Zugriff auf Medium
- Broadcast Medium
  - Angriffe für Insider leicht
  - Externe Angreifer müssen nur in Empfangsreichweite sein (z.B. vor dem Haus des Opfers)
- Netzwerkübergreifend (z.B. über Internet)
  - Angriffe leicht, viele weitervermittelnde Netzwerke

Exkurs: MAC-/ ARP- / IP-Spoofing

- Sicherheit von Ethernet/IP-Dateneinheiten?
  - Absender MAC-Adresse – Kein Integritätsschutz
  - Absender IP-Adresse – Kein Integritätsschutz
- Jedes System kann sich für jemand anderen ausgeben!
  - Zum Beispiel um Sitzung zu übernehmen / unterbrechen
  - Um Daten zu verändern
  - Für Man-in-the-Middle-Angriff
- Abhilfe
  - Z.B. Firewalls, VLANs, …
  - Verwendung von 802.1x / IPSec
    - Sichert Integrität von Ethernet bzw. IP-Dateneinheiten

Netzzugangstechniken



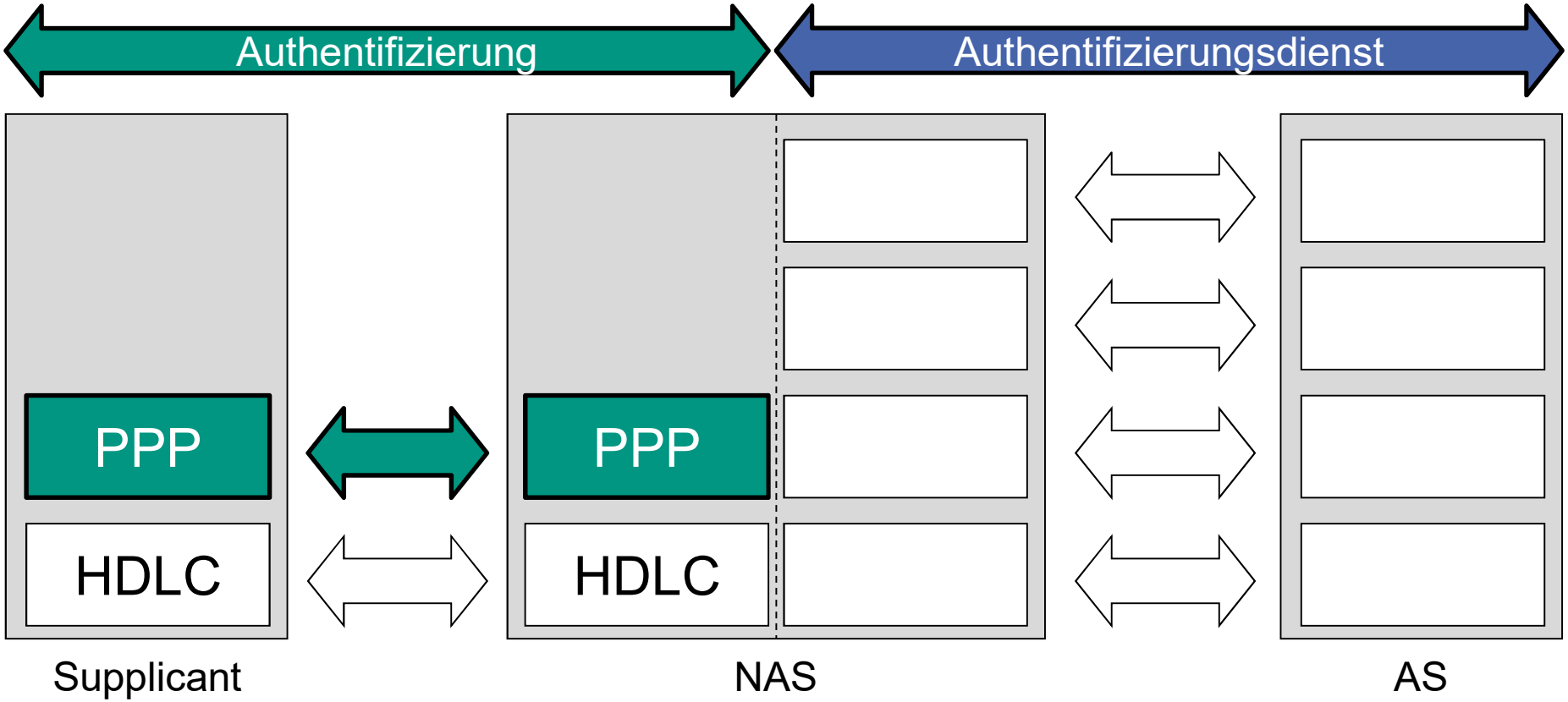
Einwahlverbindung per POTS / ISDN

- Dediziertes physisches Medium
  - Zwischen Supplicant und NAS
- Annahme: Angriffe schwer, da direkter Zugriff benötigt
- Protokoll zum Aufbau von Punkt-zu-Punkt-Verbindungen
  - Point-to-Point Protokoll (PPP) TM
- Unterteilt in
  - Link Configuration Protocol (LCP)
    - Medienzugriff
    - Zuständig für Authentifizierung von Nutzern
  - Network Configuration Protocol (NCP)
    - Einrichtung der Schicht 3 (z.B. IP)

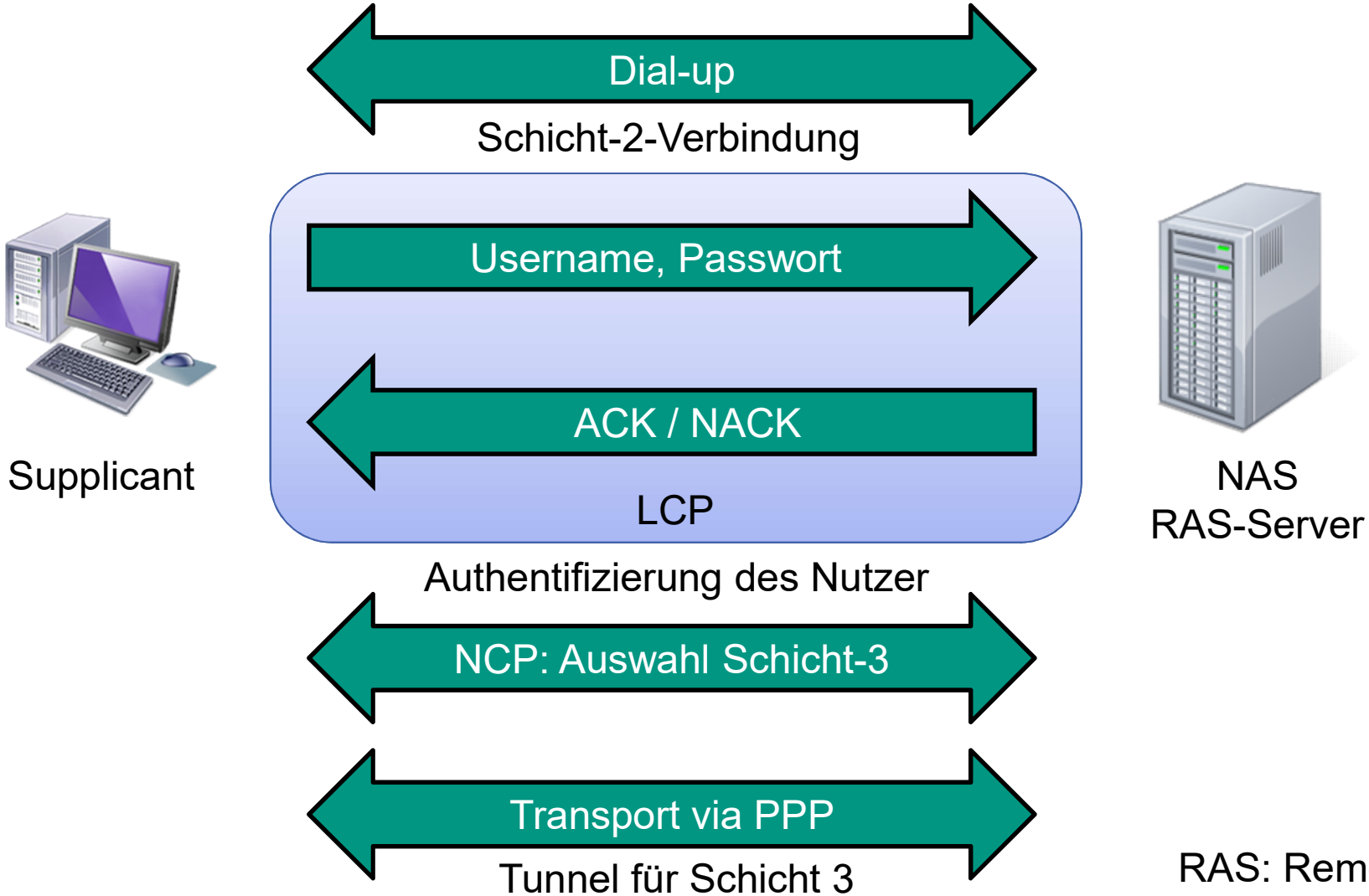
[RFC1661]

Authentifizierung

- Zwischen Supplicant und NAS via PPP auf Schicht 2
  - NAS „prüft“ Authentifizierung mittels Authentifizierungsdienst



Beispiel: PPP und PAP



RAS: Remote Access Service

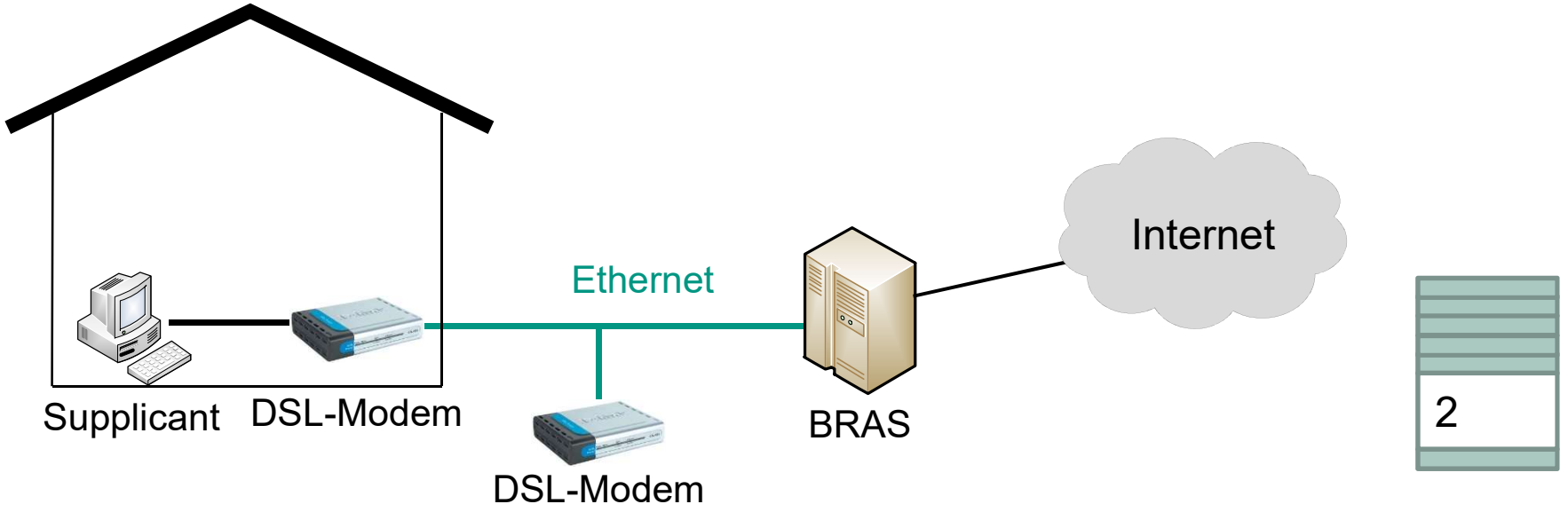
Zwischenfazit PPP

- Etabliertes Protokoll zur Einwahl
  - Entwickelt für dediziertes physisches Medium
  - Unterstützt verschiedene Transportprotokolle
  - Wird häufig bei Internet-Service-Providern eingesetzt

- Sicherheitsbetrachtung
  - PPP dient zur Authentifizierung von Nutzern
  - Keine Sicherheit auf dem Übertragungsweg Supplicant ↔ NAS
  - Keine Sicherheit für anschließende Kommunikation
  - Annahme: Angreifer hat keinen Zugriff auf Medium!

PPP und Digital Subscriber Line (DSL)

- Ethernet als Anschlusstechnologie
  - Kosteneinsparung für Betreiber
- Aber: fehlende Funktionalität in Ethernet
  - Authentifizierung, Aushandlung von Optionen, Accounting
  - Jetzt: Geteiltes Medium (Punkt-zu-Multipunkt)



BRAS: Broadband Remote Access Server

PPP over Ethernet (PPPoE)

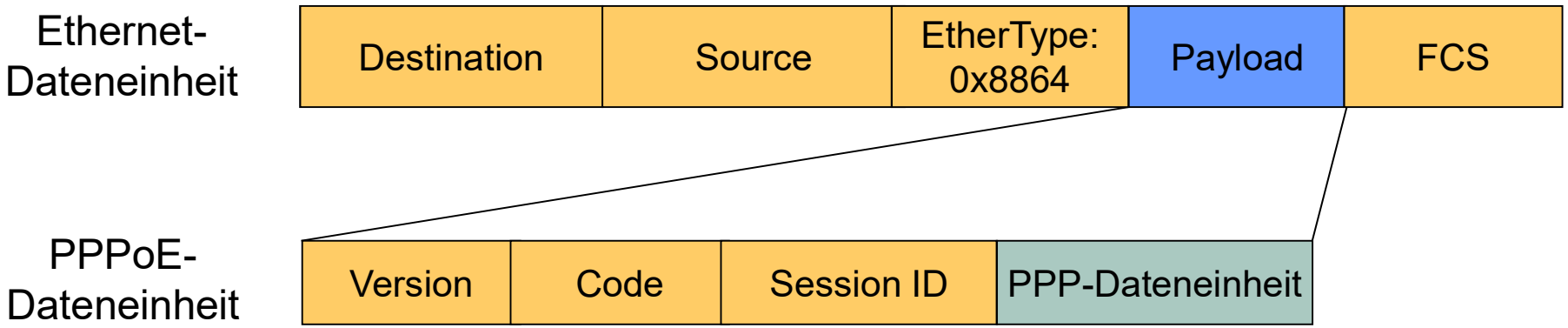
- Geteiltes Medium
  - Zwischen Supplicant und NAS
- Idee: Warum nicht einfach PPP wiederverwenden?


[RFC2516]

- Annahmen
  - Angriffe für Teilnehmer schwer
    - Zusätzliche Schutzmaßnahmen um z.B. Abhören anderer Teilnehmer zu verhindern (z.B. durch Modem selbst, durch VLANs, …)
    - Externe Angriffe benötigen physischen Zugriff auf Medium
- Problem bei Ethernet
  - Wie findet man die Gegenstelle zur Einwahl?
  - Welche MAC-Adresse hat NAS (BRAS) auf Seite des Betreibers?

Ablauf PPPoE

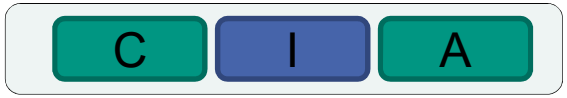
- Auffinden der richtigen Gegenstelle (NAS) zur Einwahl
  - PPPoE-Discovery
- Übertragung von PPP in Ethernet-Dateneinheiten
  - PPP-Session
    - Authentifizierung mittels PPP



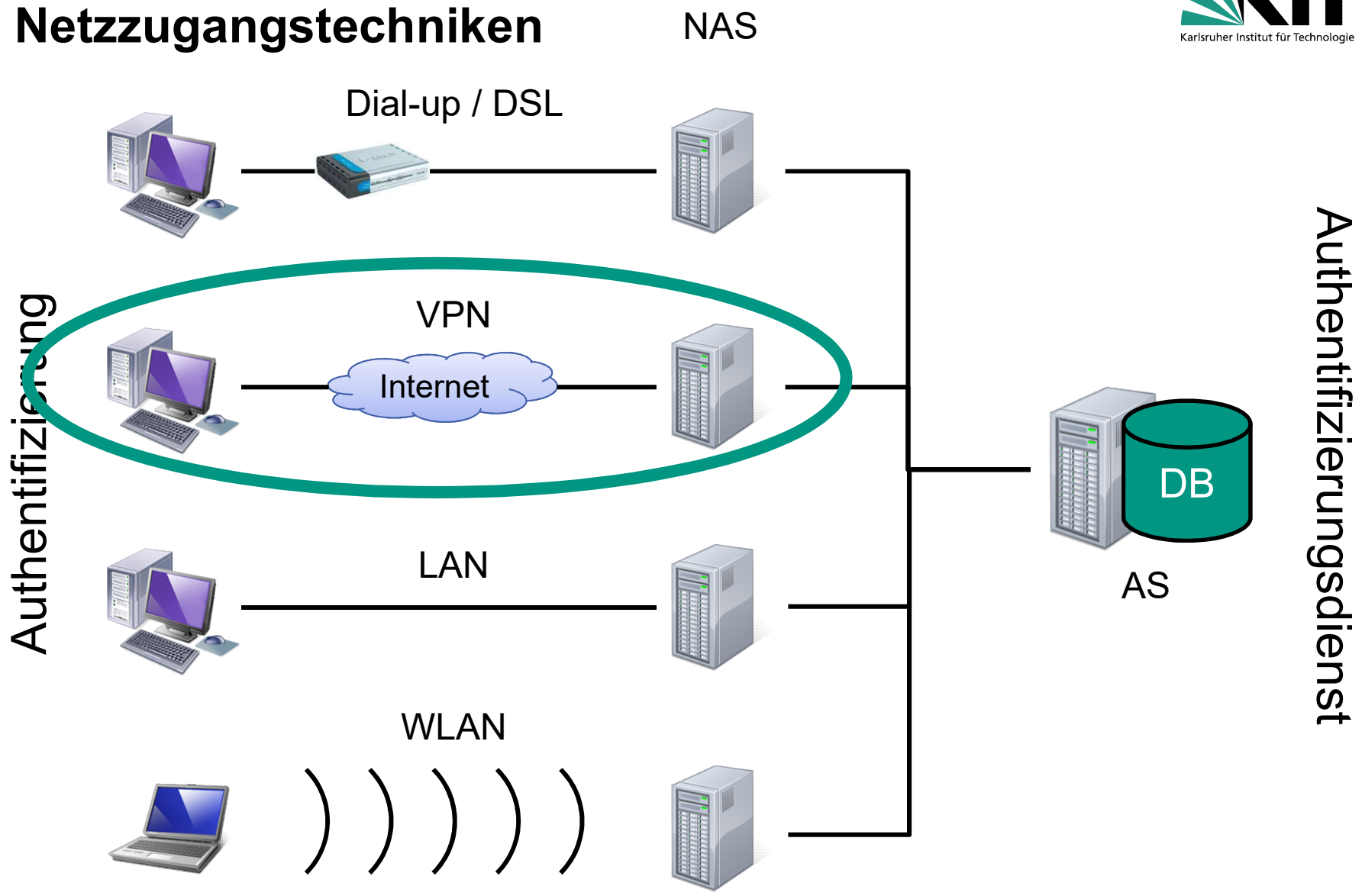
Zwischenfazit PPPoE

- Weiterverwendung von PPP bei geteiltem Medium
  - Wiederverwendung der Authentifizierung mittels PPP
  - Keine zusätzlichen Sicherheitsfeatures

- Sicherheitsbetrachtung
  - PPP dient zur Authentifizierung von Nutzern
  - Keine Sicherheit auf dem Übertragungsweg Supplicant und NAS
  - Keine Sicherheit für anschließende Kommunikation
  - Alles steht und fällt mit den Annahmen:
    - Teilnehmer können andere Teilnehmer nicht abhören (z.B. VLANs)
    - Externer Angreifer hat keinen Zugriff auf Medium

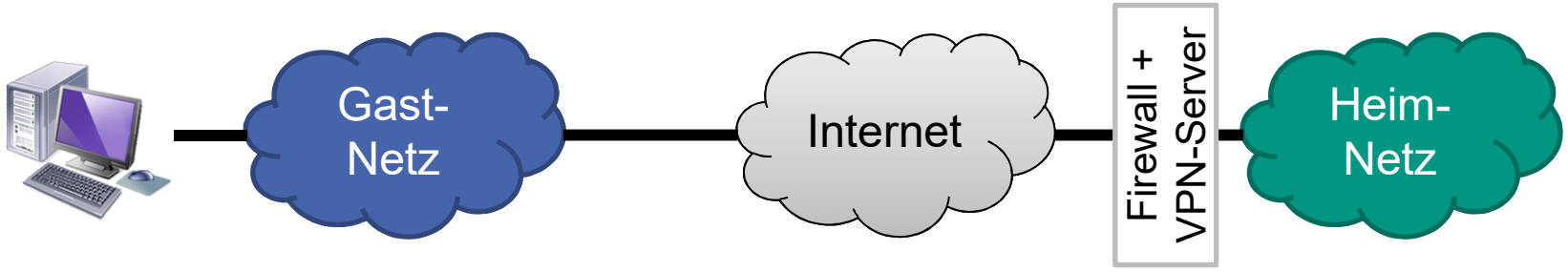


Netzzugangstechniken



Problemstellung bei Zugriff auf VPN

- Netzwerkübergreifend (z.B. über das Internet)
  - Zwischen Supplicant und NAS
  - Angreifer ggf. in weitervermittelnden Netzwerken



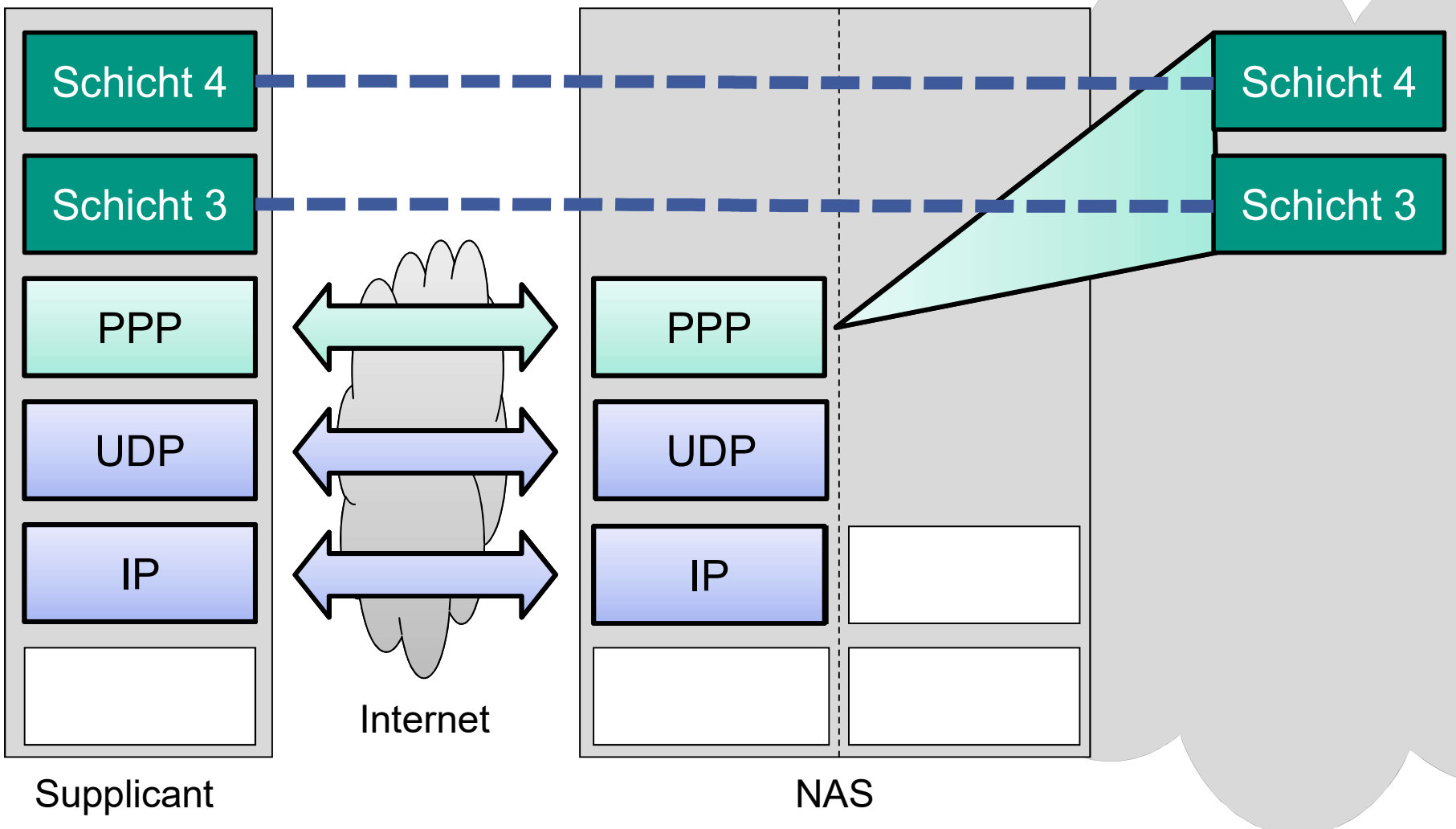
- Ziel
  - Gesicherter Zugriff auf Firmennetz von Remote
    - Virtual Private Network (VPN)
  - Zugriff nur für legitime Nutzer
    - Authentifizierung und Autorisierung der Nutzer
  - Schutz der Daten auf dem Transportweg

PPP über IP

- Idee („Rad nicht neu erfinden“)
  - Nutzung von PPP-Authentifizierung über IP/UDP
  - Herstellung von IP-Konnektivität zwischen Supplicant und NAS
  - Dann
    - PPP zur Authentifizierung und Konfiguration
    - Nutzung zum Transport von Daten ins/aus dem Netz
- Mögliche Realisierung
  - Point to Point Tunneling Protocol (PPTP)
    - Proprietäres Protokoll von Microsoft, später in IETF spezifiziert
    - Gilt als gebrochen (verwendet u.a. MS-CHAPv2)
  - Layer 2 Tunneling Protocol (L2TP)
    - Offener Standard (IETF)
    - Aufbau eines UDP-Tunnels zum Transport

[RFC2661]

PPP über IP


Schicht 4
Schicht 3
PPP
UDP
IP
Schicht 4
Schicht 3
PPP
UDP
IP
Internet
Supplicant
NAS

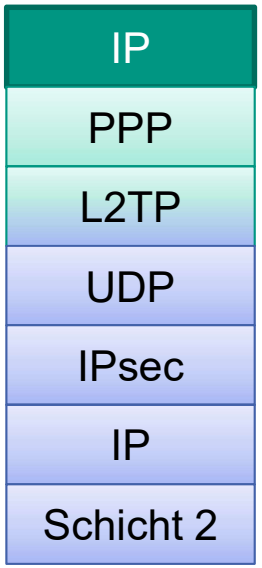
L2TP: Übersicht

[RFC2661]

- L2TP bietet
  - Virtuelle Punkt-zu-Punkt-Verbindung: Supplicant zu NAS
- L2TP nutzt UDP als Transportprotokoll
- L2TP bietet keine Vertraulichkeit!

- PPP über L2TP
  - Authentifizierung
    - z.B. mittels EAP
  - Einwahl in Heim-Netz
    - Etablierung von IP-Konnektivität

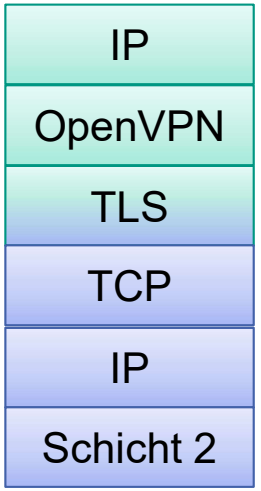
- Vertraulichkeit muss zusätzlich realisiert werden
  - In der Regel durch Nutzung von IPsec



OpenVPN mit TLS

- Ziel
  - Betriebssystem-unabhängige VPN-Einwahl
  - Bessere Konnektivität durch Firewalls und NATs hindurch
  - ➔ Verwendung von TLS

- OpenVPN Ablauf
  - Aufbau eines TLS gesicherten Tunnels zum NAS
  - Über TLS-Tunnel
    - Authentifizierung
      - Über Pre-Shared-Keys (PSK)
      - Benutzername und Passwort
      - Verwendung von Zertifikaten
    - Etablierung von IP-Konnektivität
      - Um Heim-Netz zu nutzen



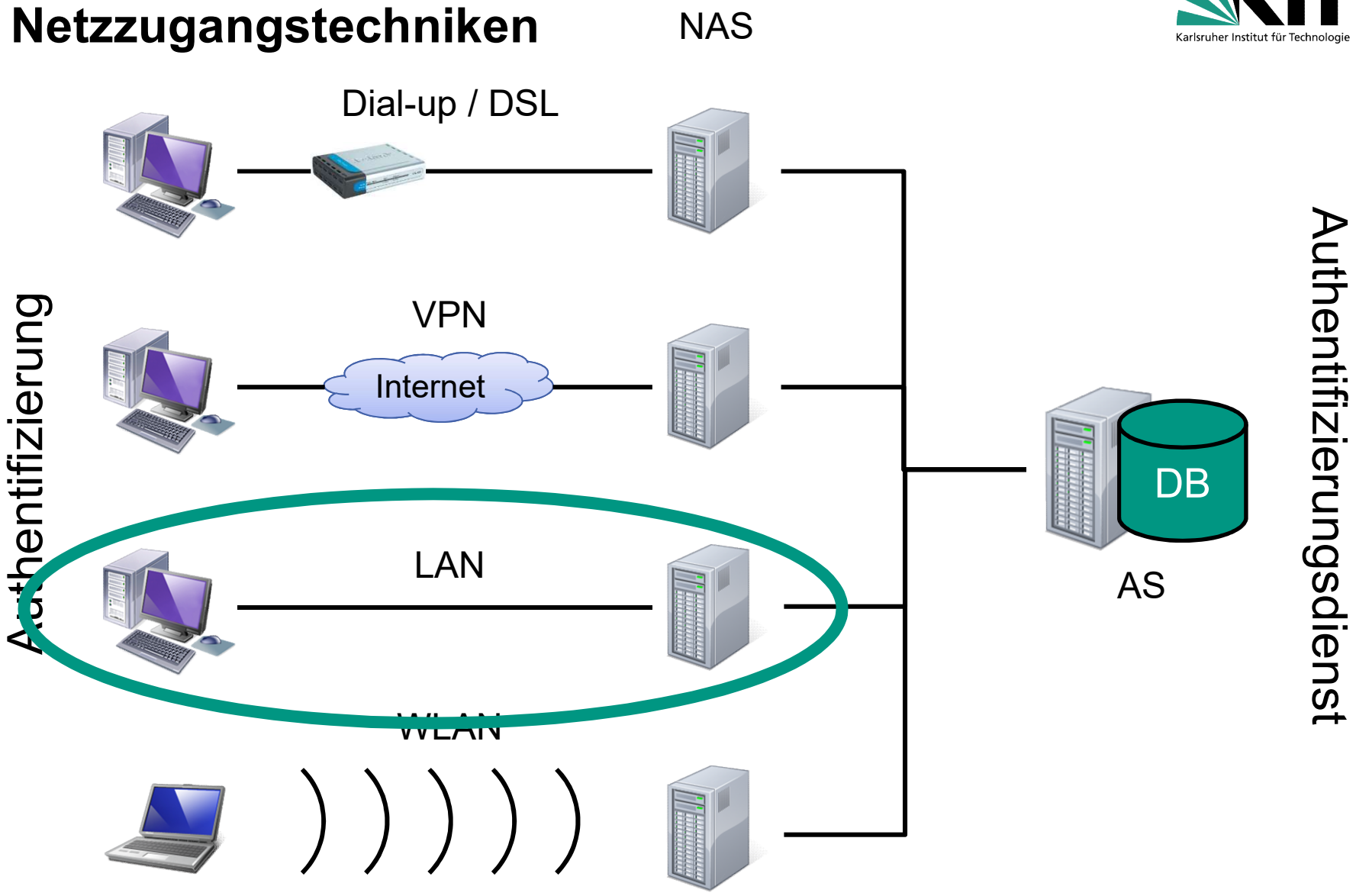
Zwischenfazit VPN

- Zunächst Aufbau eines gesicherten Kanals

- Authentifizierung des Nutzers
  - Weiterverwendung von PPP und damit verbunde Authentifizierung
  - Eigene Anwendung: Anwendungsspezifische Authentifizierung

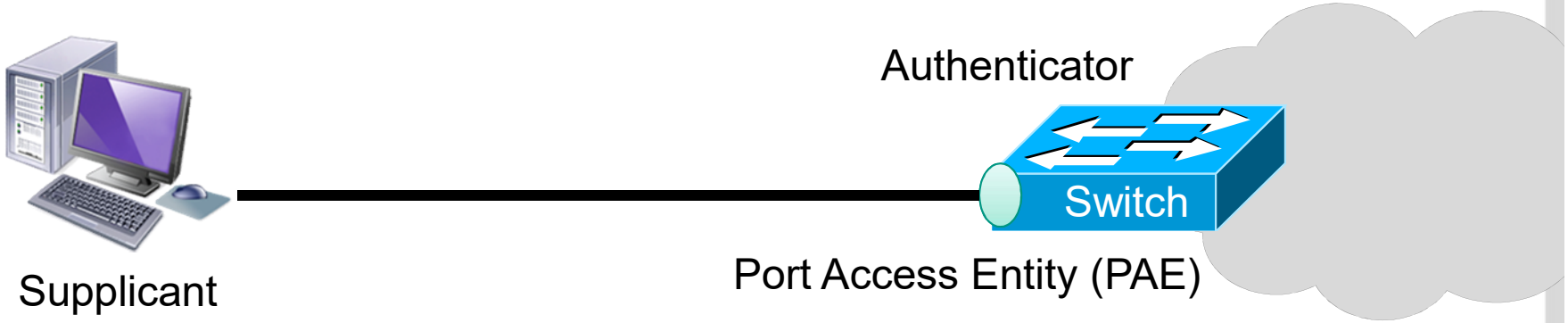
- Sicherheitsbetrachtung
  - Authentifizierung von Nutzern
  - Übertragungsweg Supplicant und NAS durch gesicherten Kanal geschützt (TLS/IPsec)
    - Gesamtsicherheit hängt somit auch an Sicherheit von TLS/IPsec

Netzzugangstechniken



Problemstellung bei LAN-Zugang

- Dediziertes physisches Medium
  - Konnektivität zwischen Supplicant und NAS (Switch)
    - Punkt-zu-Punkt-Verbindung mittels LAN-Kabel
    - IEEE 802.3 – Ethernet auf Schicht 2



- Authentifizierung und Autorisierung
  - Zum Schutz vor illegitimer Nutzung des LANs
    - z.B. Fremdnutzung konfigurierter Switch-Ports
    - z.B. Benutzung ungenutzter Switch-Ports

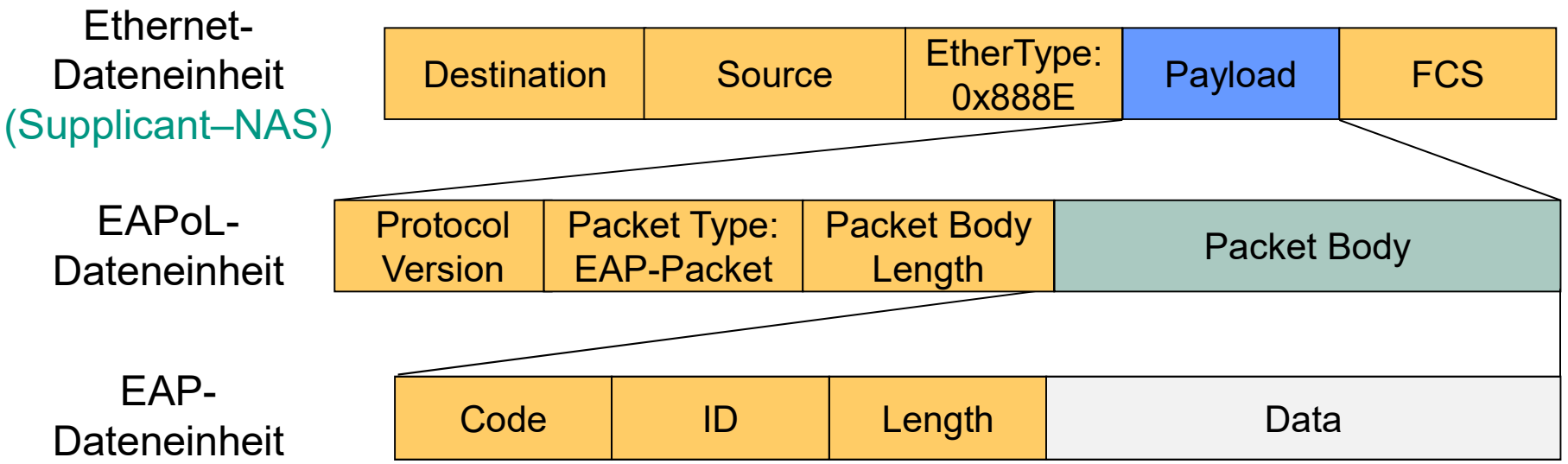
Port Based Network Access Control (PNAC)

- Ziel
  - Port-basierte Authentifizierung von Geräten
    - z.B. nach Anschluss an Switch-Port
- Protokoll für PNAC: IEEE 802.1X
  - Verwendung von EAP zur Authentifizierung (EAP over LAN)
  - Gewährt nach erfolgreicher Authentifizierung und Autorisierung Nutzung des Switch-Ports
  - Regelt Re-Authentifizierung
    - Nach definierter Zeitspanne
    - Wenn Port inaktiv wurde, z.B. durch Abziehen des Kabels

[IEEE802.1X]

EAP over Lan (EAPoL)

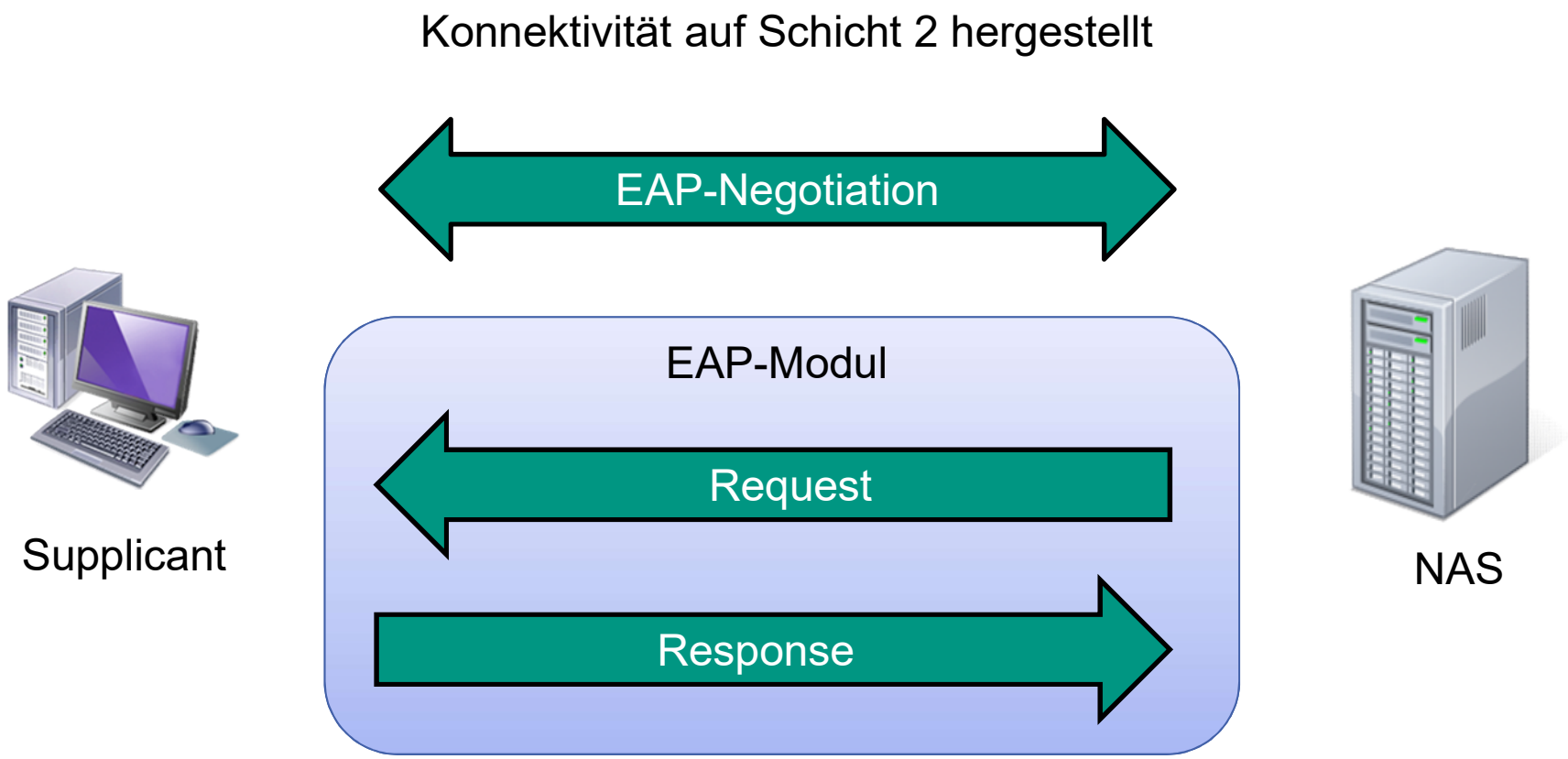
- Ethernet zwischen Supplicant und Authenticator / NAS
- Transport von EAP über Ethernet
  - Protokoll: EAP over LAN (EAPoL)



IEEE 802.1X – Aufgaben des Authenticators

- Authentifizierung und Autorisierung des Nutzers
  - Zunächst Datenvekehr über PAE blockieren
    - Authentifizierungsverkehr wird zugelassen
  - Nach Authentifizierung PAE für Nutzung des Netzes freischalten
  - Re-Authentifizierung
- Switch kann aber auch selber Supplicant sein
  - Wichtig zur Authentifizierung bei Konnektivität zwischen Switchen
    - z.B. mit Hilfe eines LAN-Kabels

IEEE 802.1X: Ablauf der Authentifizierung

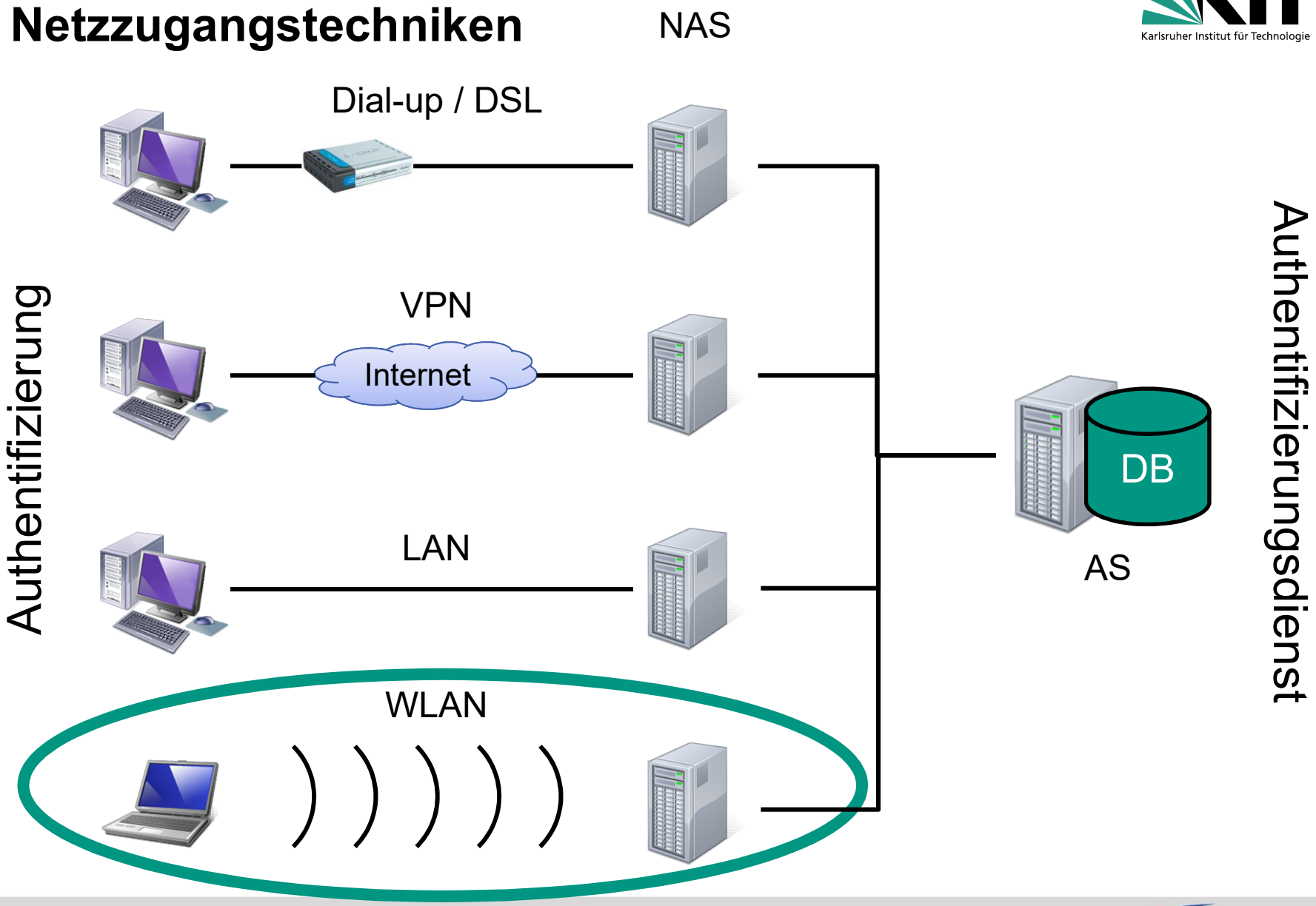


Port freischalten oder Nutzung blockieren!

Zwischenfazit 802.1X

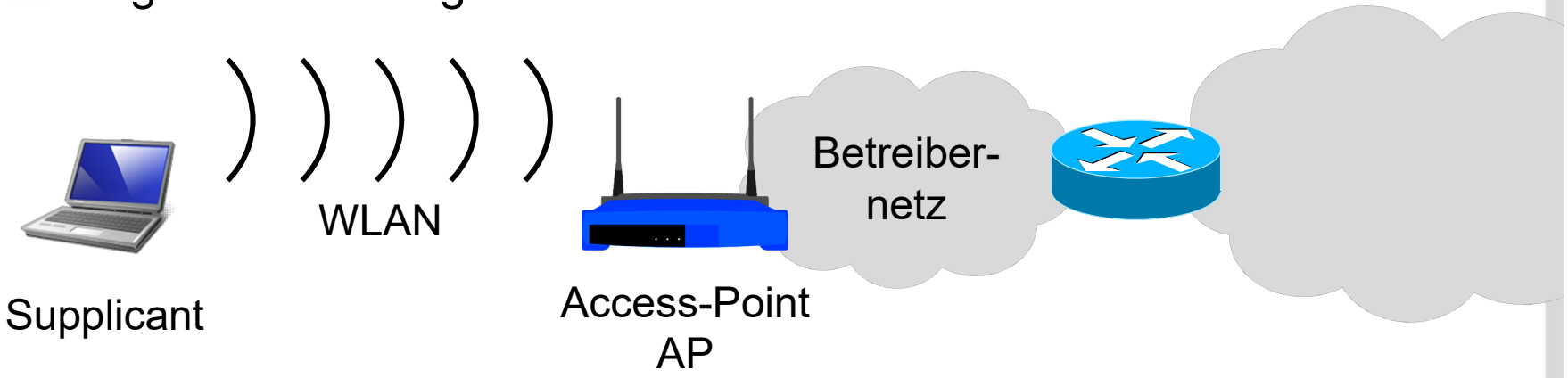
- Port-basierte Authentifizierung
  - Authentifizierung mit EAPoL
- Authentifizierung und Nutzung getrennt
- Sicherheitsbetrachtung
  - Einmal authentifizierter Port kann „entführt“ werden
    - z.B. wenn HUB zwischen Supplicant und PAE geschaltet war
  - Keine Sicherheit auf dem Übertragungsweg Supplicant und NAS
  - Keine Sicherheit für anschließende Kommunikation
  - Annahme: Angreifer hat keinen Zugriff auf Medium!

Netzzugangstechniken



Besonderheiten von Wireless LAN (WLAN)

- Broadcast Medium
  - Kommunikation über Luftschnittstelle
  - Jede gesendete Nachricht wird an alle Teilnehmer weitergeleitet
  - Angriffe leicht möglich



- Ziel: Illegitime Nutzer aus dem Netz fern halten
  - Zusätzlich: Schutz auf dem Transportweg (Supplicant<->AP)

WLAN: Übersicht der Zugangsverfahren

- Wired Equivalent Privacy (WEP) ab 1999
  - Authentifizierung: Gemeinsames Geheimnis
  - Verschlüsselung / Integrität: RC4
  - Gebrochen
- Wi-Fi Protected Access (WPA) ab 2003
  - Authentifizierung: Pre-Shared-Key (PSK) oder 802.1X
  - Verschlüsselung / Integrität: TKIP (basiert auf RC4)
  - TKIP sollte auch nicht mehr verwendet werden!
- 802.11i / Wi-Fi Protected Access 2 (WPA2) ab 2004
  - Authentifizierung: Pre-Shared-Key (PSK) oder 802.1X
  - Verschlüsselung / Integrität: AES-CCMP
  - Derzeit kein besserer Angriff als PSK erraten bekannt

Wired Equivalent Privacy (WEP)

- Ziel
  - Authentifizierung von Nutzern
  - Kein Fokus auf Vertraulichkeit / Integrität (Supplicant ⇔ AP)
    - Genau wie bei LAN
  - Umsetzung des Standards IEEE 802.11
- Unterstützt zwei Arten zur Authentifizierung
  - Open System - keine Authentifizierung
  - Shared Key – gemeinsames Geheimnis
    - Teilen sich AP und Gruppe aller legitimen Nutzer
- Schutz der Vertraulichkeit / Integrität

  - Nur gegenüber Nutzern die nicht Gruppenmitglied sind
  - Verwendung der Stromchiffre RC4

WEP: Authentifizierung

- Keine Authentifizierung einzelner Nutzer
  - Gruppe von legitimen Nutzern mit Gruppenschlüssel
    - Gruppenmitglieder teilen sich ein gemeinsames Geheimnis
    - Shared-secret (K)
    - Wahlweise 64 Bit, 128 Bit oder 256 Bit
  - ➔ Authentifizierung von Gruppenzugehörigkeit
- Authentifizierung eines Gruppenmitgliedes
  - Klassisches Challenge-Response-Verfahren
  - NAS wählt Challenge
  - Nutzer verschlüsselt vom NAS gewählte Challenge
    - Mit Hilfe eines Initialisierungs-Vektors und des Schlüssels K
    - Verwendung der Stromchiffre RC4

WEP: Verschlüsselung & Integritätssicherung

- Ablauf
  - Datenpaket P soll versendet werden
  - Zu P wird eine CRC-Prüfsumme Z berechnet (Integritätssicherung)
  - Anschließend wird ein zufälliger 24 Bit langer Initialisierungsvektor IV gewählt
  - P wird mit Hilfe der Stromchiffre $RC4$ unter Eingabe des Schlüssels K, IV verschlüsselt (XOR mit Schlüsselstrom)
    - $Enc \coloneqq RC4\ ;\ Enc_{K,IV}(P, Z) \coloneqq C$
  - Chiffrat C wird zusammen mit Initialisierungsvektor IV übertragen
    - $< C, IV >$
- Schutz nur zwischen Supplicant und AP
  - Gewählter IV wird im Klartext übertragen!

Angriff auf Authentifizierung

Supplicant

Auth

Challenge N_1

$IV_1, \mathrm{R}_1 \coloneqq RC4_{IV_1,K} \oplus N_1$

Nutzer authentifiziert

Access-Point

Angreifer

Auth

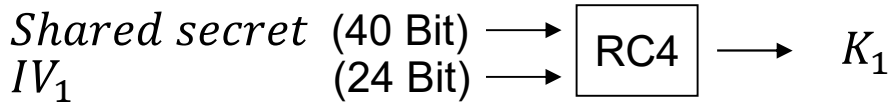
Challenge N_2

$IV_1, \mathrm{R}_2 \coloneqq \mathrm{N}_2 \oplus (N_1 \oplus R_1)$

Angreifer authentifiziert

Angriff auf Authentifizierung

- AP sendet Challenge N_1 an Supplicant
- Supplicant generiert IV_1, berechnet Schlüsselzeichen



- Supplicant berechnet Response $R_1 = N_1 \; XOR \; K_1$
- Supplicant sendet N_1, IV_1, R_1 an AP
  - Angreifer hört Nachrichten ab
- Angreifer berechnet
  - $N_1 \; XOR \; R_1 \; = \; N_1 \; XOR \; (N_1 \; XOR \; K_1) \; = \; K_1$
- AP sendet Challenge N_2 an Angreifer
- Angreifer berechnet Response $R_2 = N_2 \; XOR \; K_1$
- Angreifer sendet N_2, IV_1, R_2 an AP

WEP: Sicherheitsbetrachtung

- Probleme
  - Verwendung eines gemeinsamen Gruppenschlüssels
    - Nur kurze, statische Schlüssel (40 bzw .104 Bit), RC4 anfällig für Angriffe
  - IV wird im Klartext übertragen und enthält nur 24 Bit Entropie
  - Keine echte Integritätssicherung sondern Prüfsumme
    - Chiffrat kann passend modifiziert werden
  - Tools wie AirSnort und WEPcrack knacken WEP-Schlüssel

- TU Darmstadt, 2007 [TWPy07]
  - Breaking 104 bit WEP in less than 60 seconds

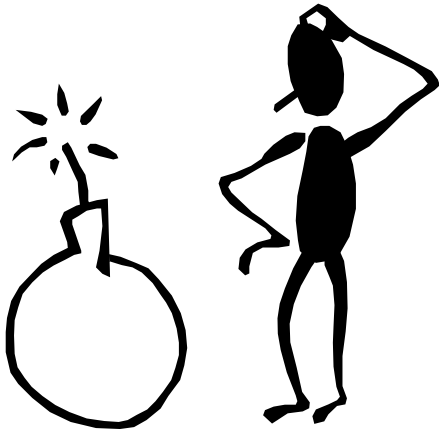
Wi-Fi Protected Access (WPA)

- Ab 2003
  - Schnelle Alternative zu gebrochenem WEP notwendig
    - Am Besten durch Softwareupdate der APs
  - Standardisierungsprozess von IEEE 802.11i am Laufen
  - IEEE 802.11i definiert verbesserte Algorithmen
    - Zur Authentifizierung
      - Pre-Shared-Keys (PSK) (Michael)
      - Unterstützung von 802.1X
    - Für Verschlüsselung / Integrität
      - Temporal Key Integrity Protocol (TKIP)
      - Individuelle Sitzungsschlüssel auf Basis von RC4
- Bereits standardisierte Teilmenge von IEEE 802.11i fand Umsetzung in WPA

WPA: Probleme

- Fehlende Unterstützung für starke Kryptomechanismen
  - Keine vollständige Umsetzung von IEEE 802.11i
- Verschlüsselung, Authentifizierung und Integritätssicherung gilt als gebrochen!
  - TKIP basiert auf RC4

- TU Darmstadt, 2008
  - Practical Attacks against WEP and WPA
- Hiroshima University, 2009
  - A Practical Message Falsification Attack on WPA



IEEE 802.11i – Robust Security Network (RSN)

- Abschluss der Standardisierung von 802.11i im Jahr 2004
  - Definition als Robust Security Network (RSN)
  - Authentifizierung:
    - Über Pre-Shared-Keys (PSK)
    - Oder 802.1X
  - Verschlüsselung: Zwingend AES-CCMP
    - Advanced Encryption Standard – Counter Mode with Cipher Block Chaining Message Authentication Code Protocol

- Ziel
  - Grundarchitektur für
    - Authentifizierung, Verschlüsselung, Integritätssicherung
    - Schlüsselgenerierung, Schlüsselaustausch, Schlüsselerneuerung

Wi-Fi Protected Access 2 (WPA2)

- Vollständige Umsetzung von IEEE 802.11i
  - Robust Security Network (RSN)

- Zwei Authentifizierungsmodi
  - Personal - Nutzung mit Pre-Shared Keys (PSK)
  - Enterprise - Nutzung mit 802.1X (z.B. im Unternehmen)
- Verschlüsselung / Integritätssicherung
  - Schutz auf Schicht 2 zwischen Supplicant und AP
  - Nutzung von AES-CCMP
  - Aushandlung von individuellen Sitzungsschlüssel je System

WPA2: Personal-Mode

- Vorbedingung
  - Access-Point und Supplicant verfügen über den gleichen PSK
    - 8-63 Zeichen lang
  - Service Set Identifier (SSID) des WLANs ist bekannt

- Hieraus Berechnung des Pairwise Master Key (PMK)
  - Mehrfachverwendung einer Hashfunktion (SHA1 / 4.096 Durchgänge)
    - $I_1 = H(PSK + SSID)$
    - $I_2 = H(I_1)$
    - …
    - $I_{4096} = H(I_{4095}) := \mathrm{PMK}$

WPA2-Personal: 4-Wege-Handshake

- Kombiniertes Verfahren
  - Authentifizierung über Kenntnis des PMK
  - Aushandlung / Verteilung von Sitzungsschlüsseln
- Ablauf
  - AP sendet Nonce N_A an Supplicant
  - Supplicant sendet Nonce N_S an AP
    - Plus dazugehörenden Message Integrity Code (MIC)
  - Anschließend Aushandlung von Schlüsselmaterial
- Authentifizierung indirekt, ähnlich wie bei WEP
  - Durch Berechnung des korrekten MIC, Nutzung des PMK

WPA2: Verschlüsselung und Integritätsschutz

- Für Unicast-Kommunikation: (Schicht 2: Supplicant ⇔ AP)
  - Individueller Pairwise Transient Key (PTK)
    - Abgeleitet aus PMK, Nonces aus Handshake, MAC-Adressen
      - $PTK := PMK + N_A + N_S + \text{SupplicantMacAdresse} + \text{APMacAdresse}$
- Für Multicast-Kommunikation: (Suplicant ⇔ Suplicants)
  - AP wählt je Gruppe zufälligen Group Master Key (GMK)
  - Hieraus abgeleitet Group Transient Key (GTK)
    - Wird vom AP an Gruppenmitglieder verteilt
    - Muss erneuert werden, wenn ein Mitglied die Gruppe verlässt
- Schlüssel werden während des 4-Wege-Handsakes ausgehandelt / übertragen

WPA2-PSK: 4-Wege-Handshake

Supplicant

AP

Auth ?

Nonce: N_A

Berechnung PTK

Nonce: $N_S + MIC$

Berechnung PTK

Verschlüsselt

GTK + MIC

ACK

Bewertung WPA2-Personal

- Erfüllt geforderte Schutzziele für WLAN
  - Authentifizierung von Nutzern
  - Schutz der Kommunikation zwischen Supplicant und NAS
- Allerdings wie bei WEP und WPA Authentifizierung nur auf Basis von Gruppenzugehörigkeit
  - Falls ein Mitglied die Gruppe verlässt müssen alle Nutzer Schlüssel austauschen
  - Schwierig einzelne Nutzer zu identifizieren
    - z.B. bei Rechtsstreitigkeiten

WPA2-Enterprise

- 802.1X basierter Authentifizierungsmodus von WPA2
  - Zum Einsatz in „Unternehmen“
- Ablauf
  - Supplicant stellt Konnektivität mit AP her
  - AP sperrt Nutzung des WLANs und lässt nur Authentifizierungsverkehr zu
  - Supplicant authentifiziert sich mittels EAP
  - Nach erfolgreicher Authentifizierung
    - Schlüsselverteilung wie bei WPA2-Personal
    - Freischaltung der Nutzung des WLANs

Bewertung WPA2-Enterprise

- Löst Probleme des Personal-Modus
  - Identifikation einzelner Nutzer
  - Sperren einzelner Nutzer
- Wiederverwendung etablierter Standards
  - 802.1X
  - EAP
- Ermöglicht
  - Authentifizierung von Nutzern
  - Schutz auf Schicht 2 zwischen Supplicant und AP

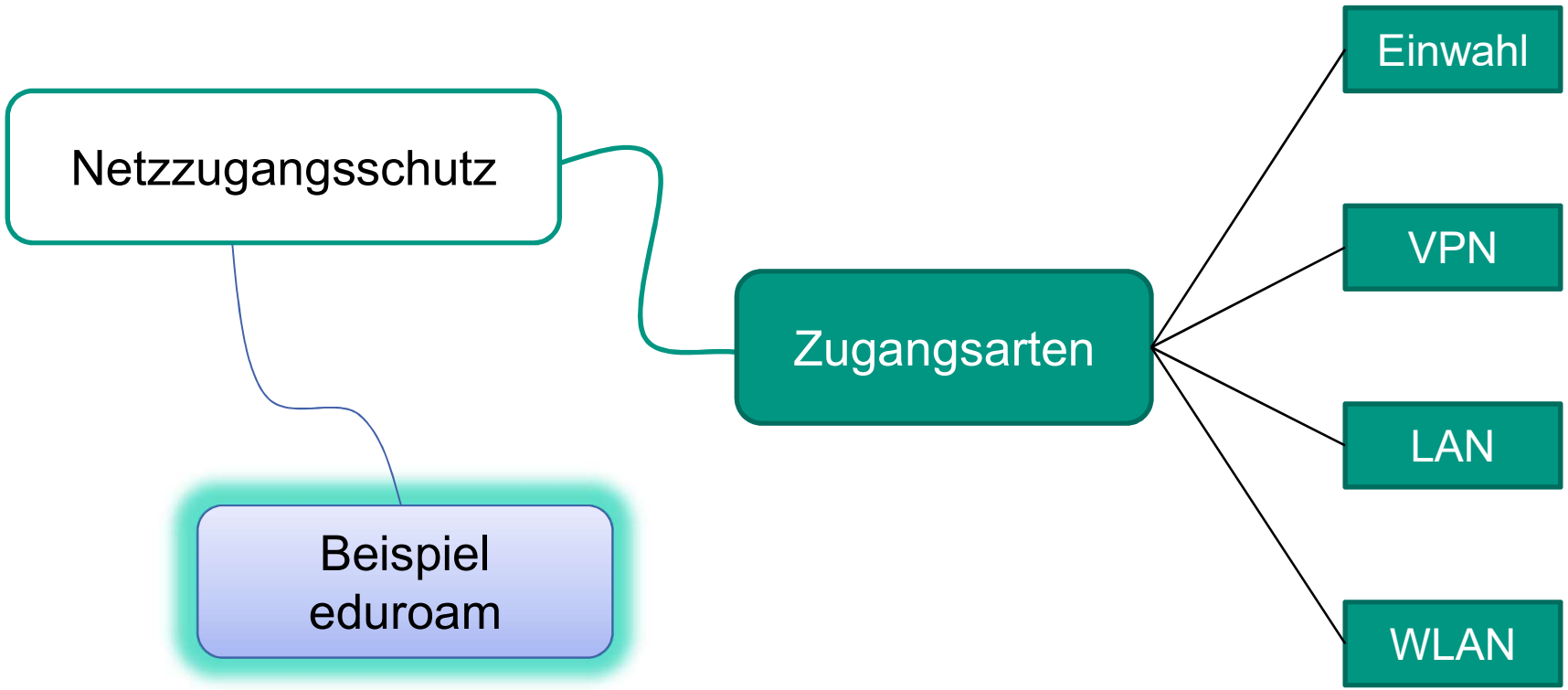
Ausblick auf WPA3

- Hauptsächlich verbessertes WPA2
  - Befindet sich noch in Standardisierung der Wi-Fi Alliance (WFA)
- Ausschluss von TKIP und WEP
- Umsetzung von Suite B

[RFC4869]

  - Konsequente Umsetzung gleichbleibend Sicherheitsniveaus
- Gegenseitige Authentifizierung mit Schutz vor Brute-Force-Angriffen (SAE)
  - Ähnlich wie Diffie-Hellmann jedoch symmetrisch
- Unterstützung für Protected Management Frames (PMF)
- Entwicklung: Alternativen zu Wi-Fi Protected Setup (WPS)

Überblick


Netzzugangsschutz
Zugangsarten
Einwahl
VPN
LAN
WLAN
Beispiel
eduroam

Authentifizierung: Beispielszenario

- Hier am Beispiel WLAN und eduroam
  - Föderativer Ansatz für Internetzugang über Universitäten
  - Soll allen Nutzern bei Teilnehmern WLAN-Nutzung ermöglichen
    - z.B. für Gaststudenten, Mitarbeiter auf Dienstreisen, …
  - Authentifizierung der Nutzer jeweils bei zugehöriger Universität
    - Dezentrale Speicherung der Authentifizierungsdaten!

- Betrachtung eines konkreten Netzzugangs
  - Nutzung von EAP
  - Realisierung von Schutzzielen
    - Schutz auf Schicht 2 (Supplicant ⇔ AP)
    - Schutz der Identität des Nutzers
    - Gegenseitige Authentifizierung (Supplicant / AS)

SSID: eduroam

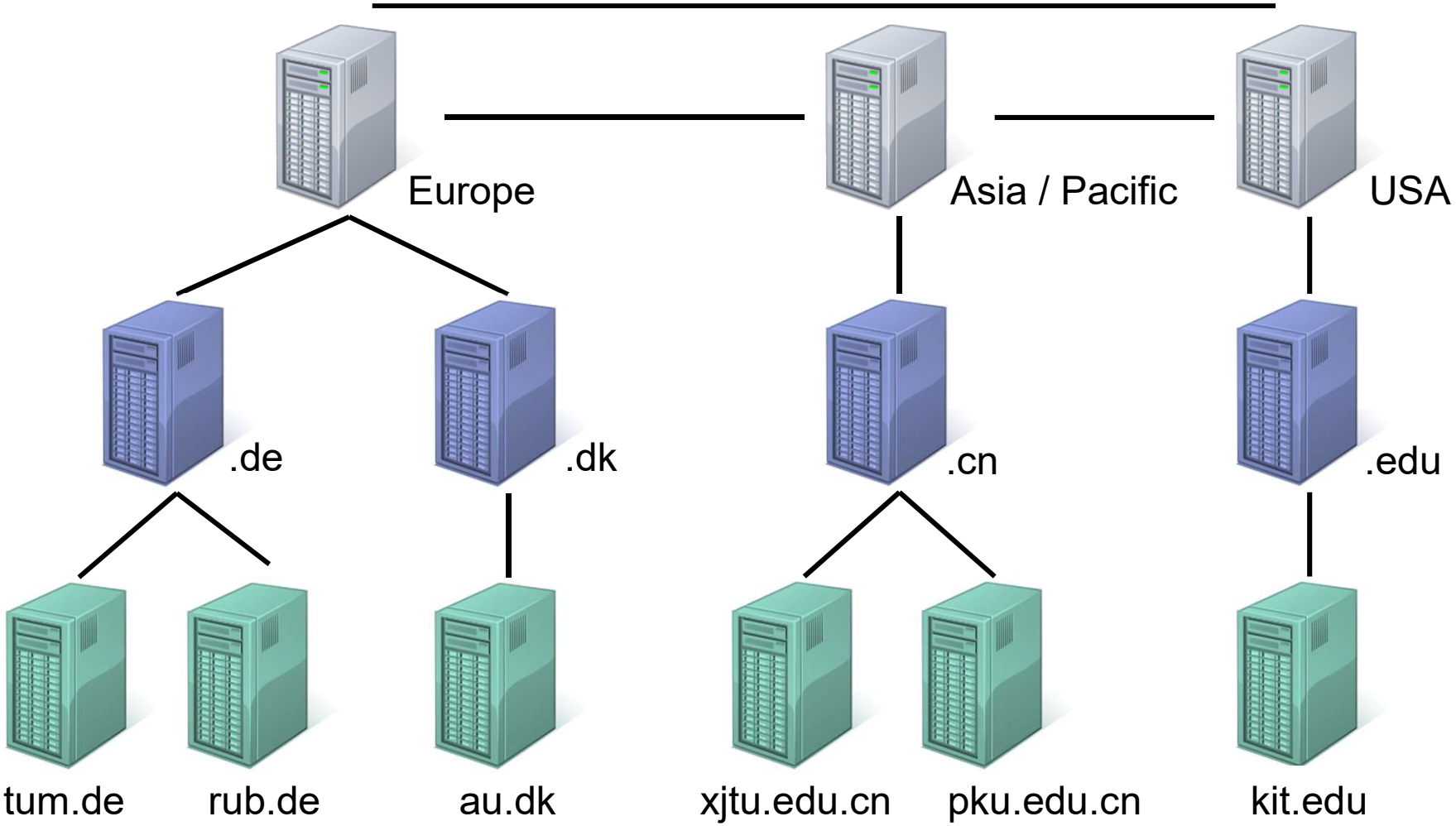
- Weltweite Verbreitung: 69 Länder

www.eduroam.org

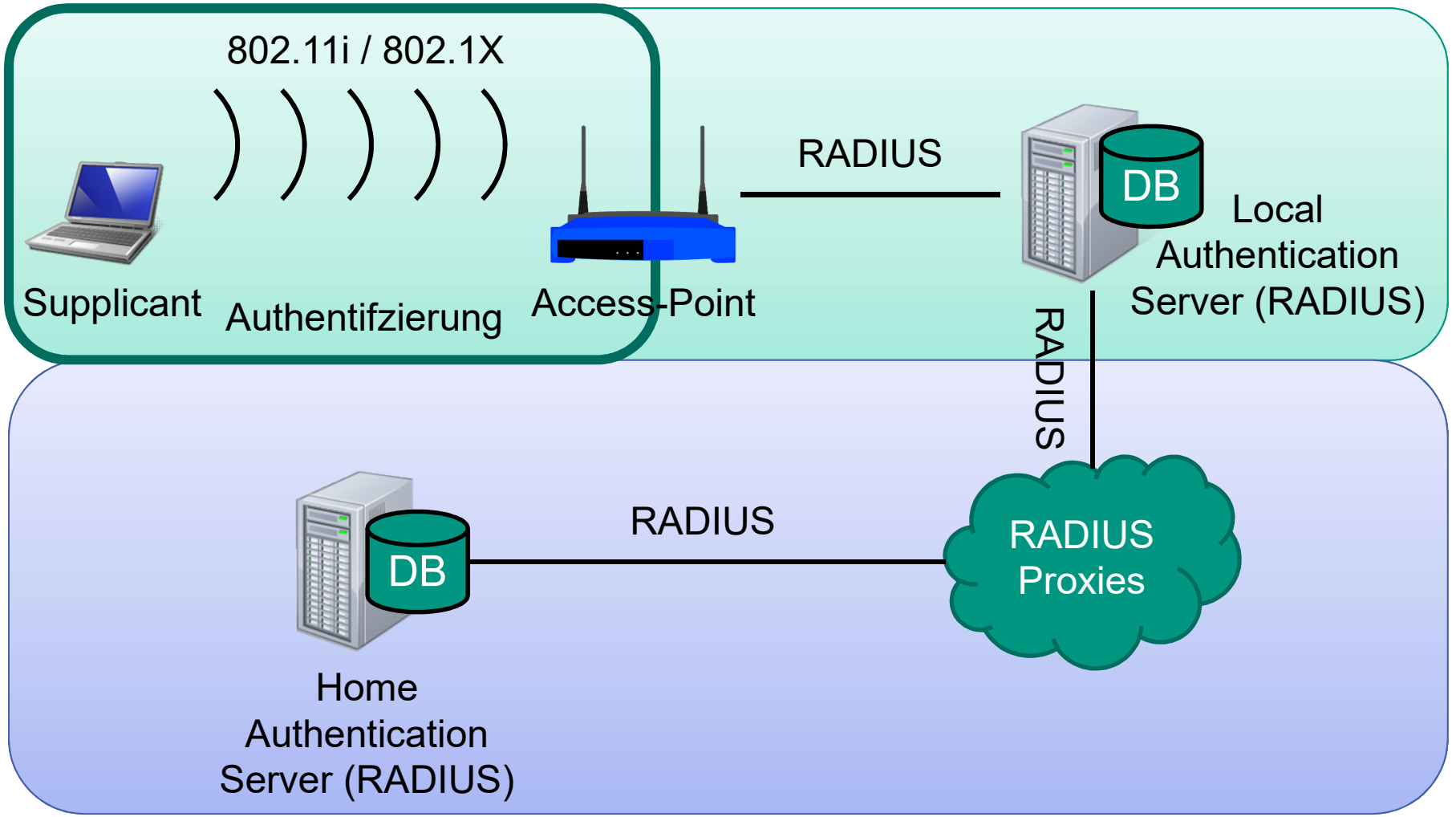
Education Roaming (eduraom)

- Aufteilung in Authentifizierungsdomänen
  - Sogenannte Realms
  - Jede teilnehmende Universität stellt eigenes AS (Identitätsprovider)
    - Institutional RADIUS-server
  - Hierarchischer Zusammenschluss je Land zur Föderation
    - National top-level RADIUS-server
  - Zusammenschluss der Föderationen zu Konföderationen
    - Europe top-level RADIUS-server
    - Asia-Pacific top-level RADIUS-server
    - United-States top-level RADIUS-server
    - Canada top-level RADIUS-server
- Eindeutige Identifikation der Nutzer
  - nutzer@universität.tld (nutzer@realm)

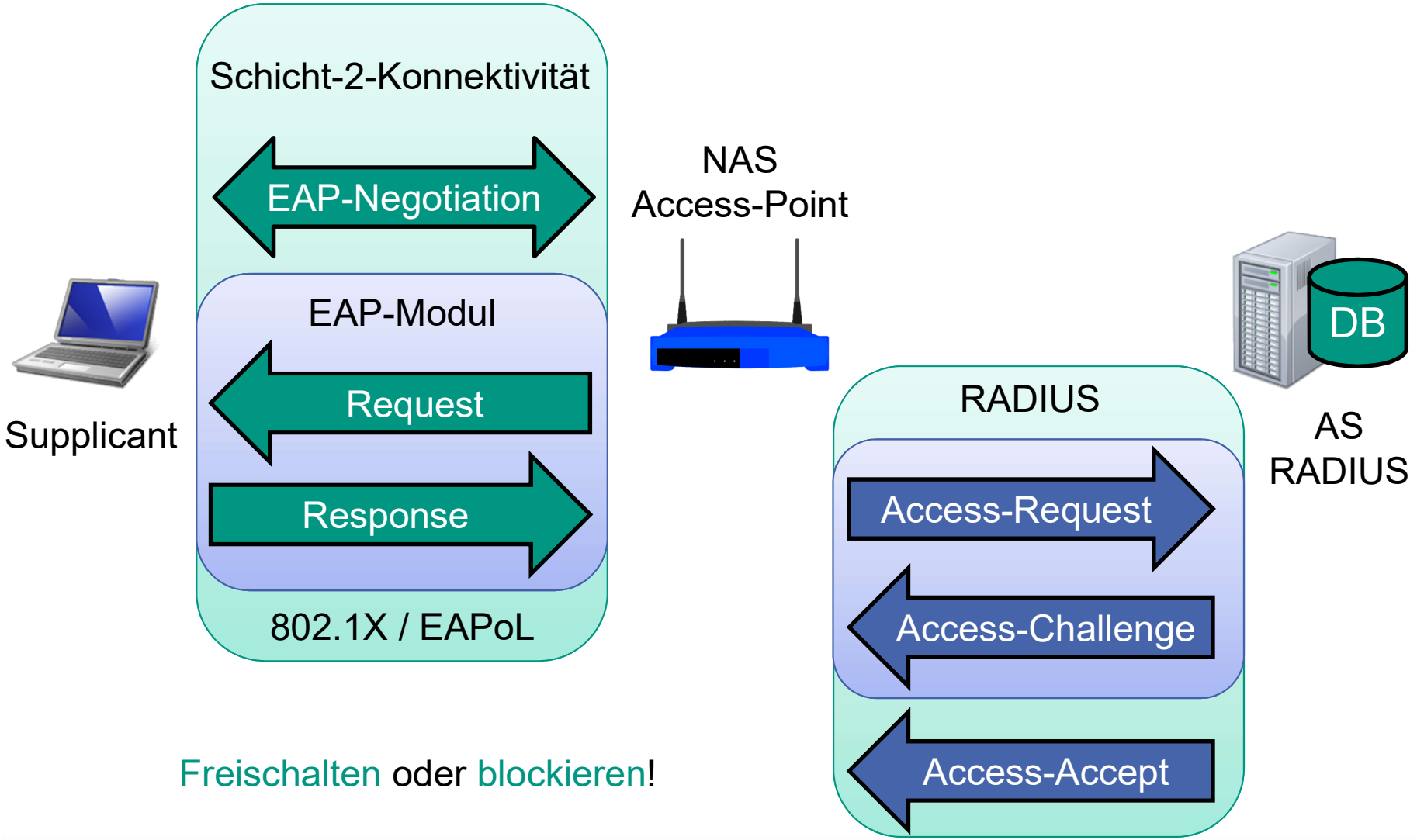
Hierarchischer Aufbau: eduroam



Authentifizierung schematisch mit eduroam

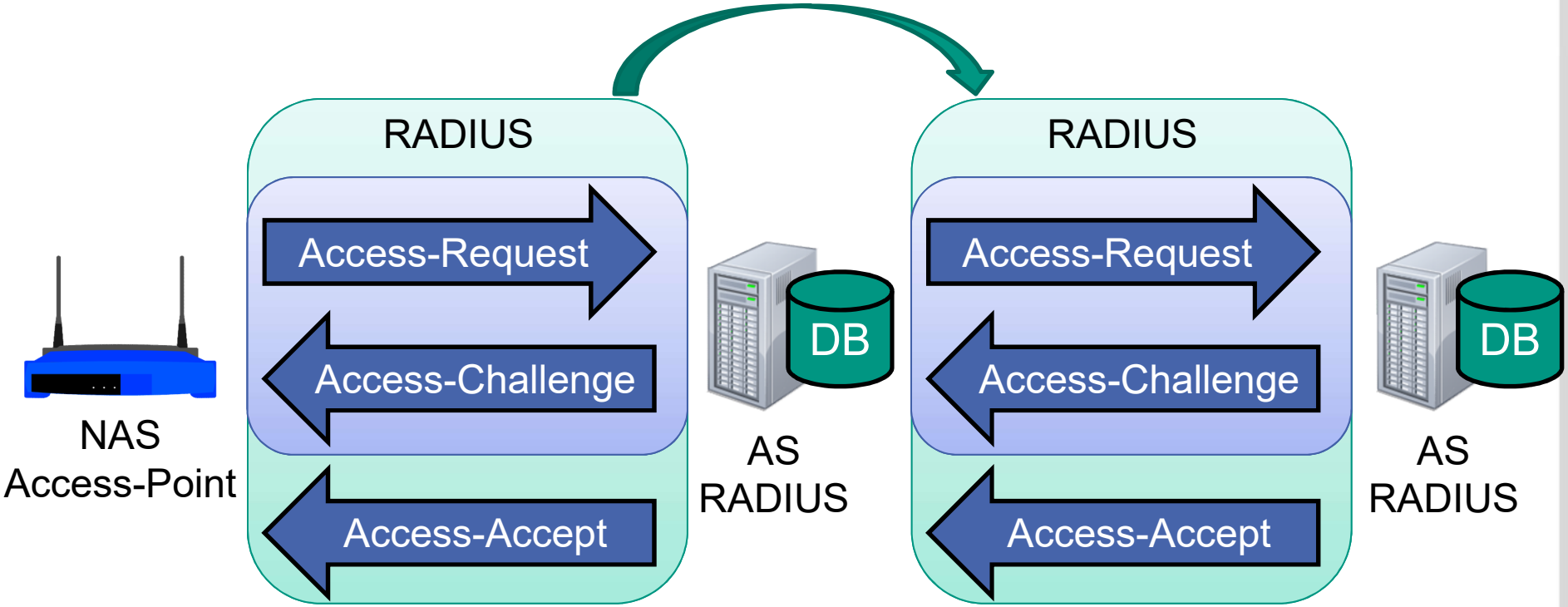


WPA2-Enterprise: Authentifizierung



Freischalten oder blockieren!

RADIUS-Proxies: Roaming

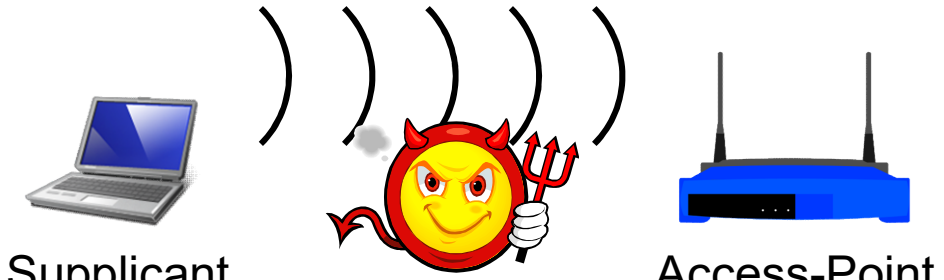


- Weiterleitung an RADIUS-Server des Realms
  - Auflösung über RADIUS-Hierarchie
  - Umkopieren der RADIUS-Nachrichten
  - TLS-Verbindungen über Internet

So weit mit bisherigen Mitteln…

- Schutz der gesamten Kommunikation?
  - Nur zwischen Supplicant und NAS, NAS und AS, AS und AS
  - Zwischensysteme können Daten abhören / verändern
  - ➔ Kein Schutz auf komplettem Weg zwischen Supplicant und Heimat-AS
- Schutz der Identität
  - Kein Schutz der Identität des Supplicants
    - NAS erfährt konkreten Nutzernamen
- Gegenseitige Authentifizierung
  - Authentifizierung des Supplicants
  - Keine Authentifizierung des Heimat-AS

Zusätzliche Probleme bei 802.1X und WLAN



- Passive Angriffe einfacher möglich
  - Identitäten beim initialen Austausch können mitgehört werden
- Aktive Angriffe einfach möglich
  - Man-in-the-Middle-Angriff während Authentifizierung
  - Fälschen von Dateneinheiten möglich
    - z.B. End-of-Session bei EAPoL
    - z.B. EAP-Success / Failure-Nachrichten

Baustein der noch fehlt

- Schutz des Authentifizierungsverkehrs
  - Schutz von EAP über NAS und RADIUS-Proxies bis zu Heimat-AS
  - Authentifizierung, Vertraulichkeit und Integrität
- Verschiedene EAP-Module als Lösung
  - Protected EAP (PEAP)
    - Proprietäres Protokoll von Microsoft und Cisco
  - EAP Tunneled TLS (EAP-TTLS)
    - Standardisiert von der IETF

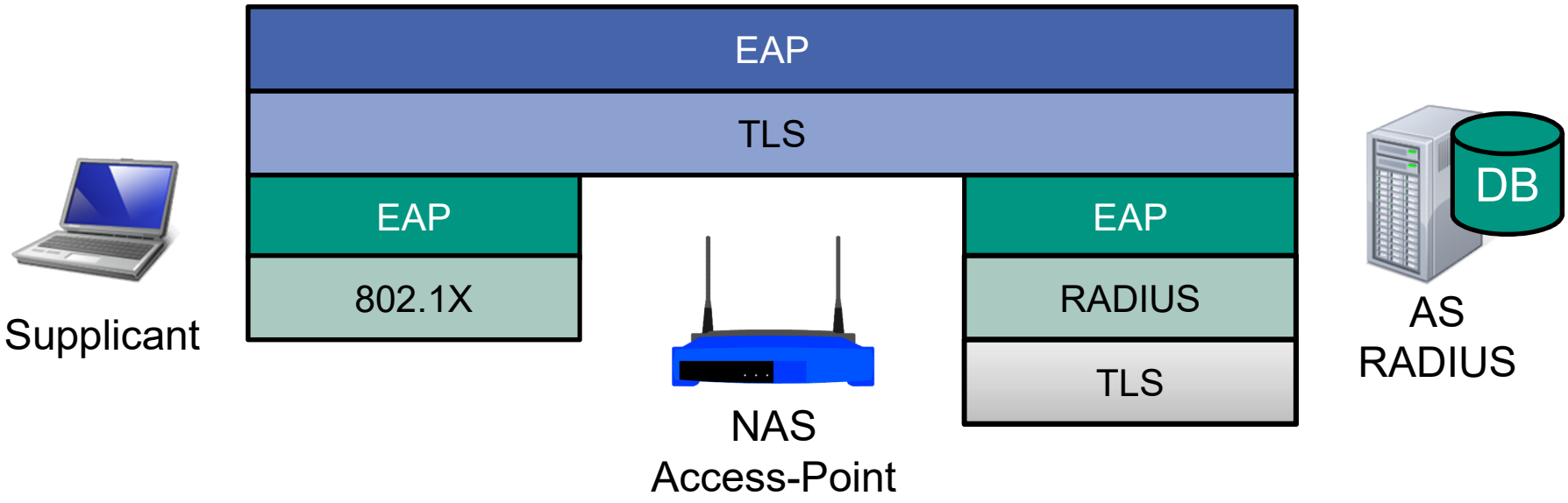
Modul: EAP-TTLS

- Ziel
  - Aufbau eines gesicherten TLS-Tunnels zwischen Supplicant und Heimat-AS über RADIUS-Proxies hinweg
  - Über TLS-Tunnel dann Authentifizierung mit EAP
- Unterteilt in zwei Phasen
  - Phase 1: Aufbau TLS-Verbindung (Wahl der Cipher Suite)
    - Supplicant anonym (anonymous@realm)
    - Authentifizierung des Heimat-AS über Zertifikat
  - Phase 2: Geschützte Nutzer-Authentifizierung mit EAP
    - Über TLS-Tunnel
- Verschlüsselung und Integritätssicherung wie gehabt
  - WPA2-Schlüsselverteilung

[RFC5281]

EAP-TTLS im Protokollstack

- TLS-Tunnel via EAP-Nachrichten (Supplicant ⇔ AP ⇔ AS)
  - Über NAS, diverse RADIUS-Proxies, bis zum Heimat-AS
- Über gesicherten TLS-Tunnel erfolgt Authentifizierung
  - Mittels EAP
- Authentifizierungsentscheidung wird zu NAS gesandt



EAP-TTLS: Austausch des PMK

- Nach erfolgreicher Authentifizierung muss PMK für Schutz auf Schicht 2 zwischen Supplicant ⇔ AP initialisiert werden
  - Für Verschlüsselung und Integrität mit WPA2
- Supplicant
  - Leitet PMK aus TLS-Schlüsseln und Informationen aus EAP-Authentifizierung ab
- AP
  - Empfängt PMK + Authentifizierungsentscheidung von Heimat-AS
  - Übermittelt über RADIUS-Proxies

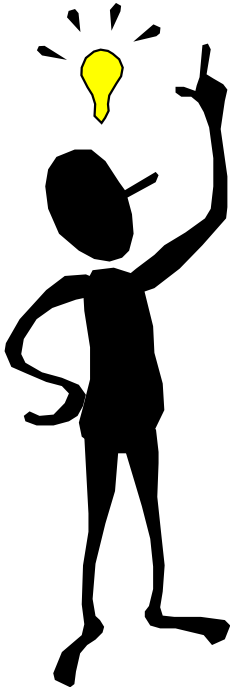
EAP-TTLS: Vor- / Nachteile

- Vorteile
  - Identität des Supplicant bleibt geschützt
  - Schutz des Authentifizierungsverkehrs bis zum Heimat-AS

- Nachteil
  - Ob AS-Zertifikats validiert wird hängt von Supplicant ab
    - Problematisch z.B. bei zurückgerufenen Zertifikaten

Fazit eduroam

- Gute Umsetzung von Netzzugangsschutz
  - Authentifizierung: IEEE 802.11i, WPA2 (PEAP/EAP-TTLS), 802.1X
  - Authentifizierungsdienst: RADIUS (mit TLS- und EAP-Erweiterung)
  - Verschlüsselung / Integrität: WPA2 (AES-CCMP)
  - Schutz der Nutzeridentität
- Also besser eduroam anstatt KA-WLAN nutzen!
  - Beide Verfahren authentifizieren Nutzer
    - KA-WLAN über Captive Portal
    - Eduroam über 802.1X, EAP und Radius
  - Aber nur eduroam sorgt für Schutz auf Schicht 2
    - Zwischen Supplicant und AP auf der Luftschnittstelle
    - Mit WPA2-Enterprise



Aber…

- Auch WPA2-Enterprise bei eduroam schützt nur
  - Authentifizierungsverkehr zwischen Supplicant und Heimat-AS
  - Daten auf dem Übertragungsweg zwischen Supplicant und AP
    - Schicht 2

- WPA2 schützt nicht
  - Daten auf dem weiteren Weg durch das Netz

- Wichtig: Supplicant muss zur Abwehr von MitM-Angriffen auf Authentifizierung unbedingt das Server-Zertifikat prüfen!

Zusammenfassung

- Effektiver Zugangsschutz für Netze ist möglich
  - Erfordert aber sorgfältige Planung
  - Angreifermodell und Schutzziele müssen klar sein
- Zugangsschutz schützt nicht
  - Kommunikation innerhalb des Netzes
  - Vor schadhaften Anwendungen auf Seiten des Supplicants
  - Initiale Aushandlung von Benutzername und Passwort
- Schutz muss so früh wie möglich etabliert werden
  - Authentifizierung und Autorisierung von Nutzern
  - Vertraulichkeits- und Integritätssicherung zwischen Supplicant ⇔ NAS

Literatur

[IEEE802.1X] 802.1X-2010 - IEEE Standard for Local and metropolitan area networks--Port-Based Network Access Control; 2010

[RFC2865] C. Rigney, S. Willens, A. Rubens, W. Simpson; Remote Authentication Dial In User Service (RADIUS); Jun. 2000

[RFC3539] B. Aboba, J. Wood; Authentication, Authorization and Accounting (AAA) Transport Profile; Jun. 2003

[RFC5281] P. Funk, S. Blake-Wilson; Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0); Aug. 2008

[RFC3579] B. Aboba, P. Calhoun; RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP); Sep. 2003

[RFC6614] S. Winter, M. McCauley, S. Venaas, K. Wierenga; Transport Layer Security (TLS) Encryption for RADIUS; May 2012

[RFC6733] V. Fajardo, J. Arkko, J. Loughney, G. Zorn, Diameter Base Protocol; Oct. 2012

Literatur

[RFC1661] W. Simpson; The Point-to-Point Protocol (PPP); Jul. 1994

[RFC2516] L. Mamakos, K. Lidl, J. Evarts, D. Carrel, D. Simone, R. Wheeler; A Method for Transmitting PPP Over Ethernet (PPPoE); Feb. 1999

[RFC2661] W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn, B. Palter; Layer Two Tunneling Protocol "L2TP"; Aug. 1999

[RFC3748] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, ; Extensible Authentication Protocol (EAP); Jun. 2004

[TWPy07] E. Tews, R.-P. Weinmann, A. Pyshkin; Breaking 104 Bit WEP in Less Than 60 Seconds; in Information Security Applications: 8th International Workshop; WISA 2007; Jeju Island, Korea, August 27–29, 2007, Springer, http://dx.doi.org/10.1007/978-3-540-77535-5_14

[eduroam] https://www.eduroam.org/

[openvpn] https://www.openvpn.net/