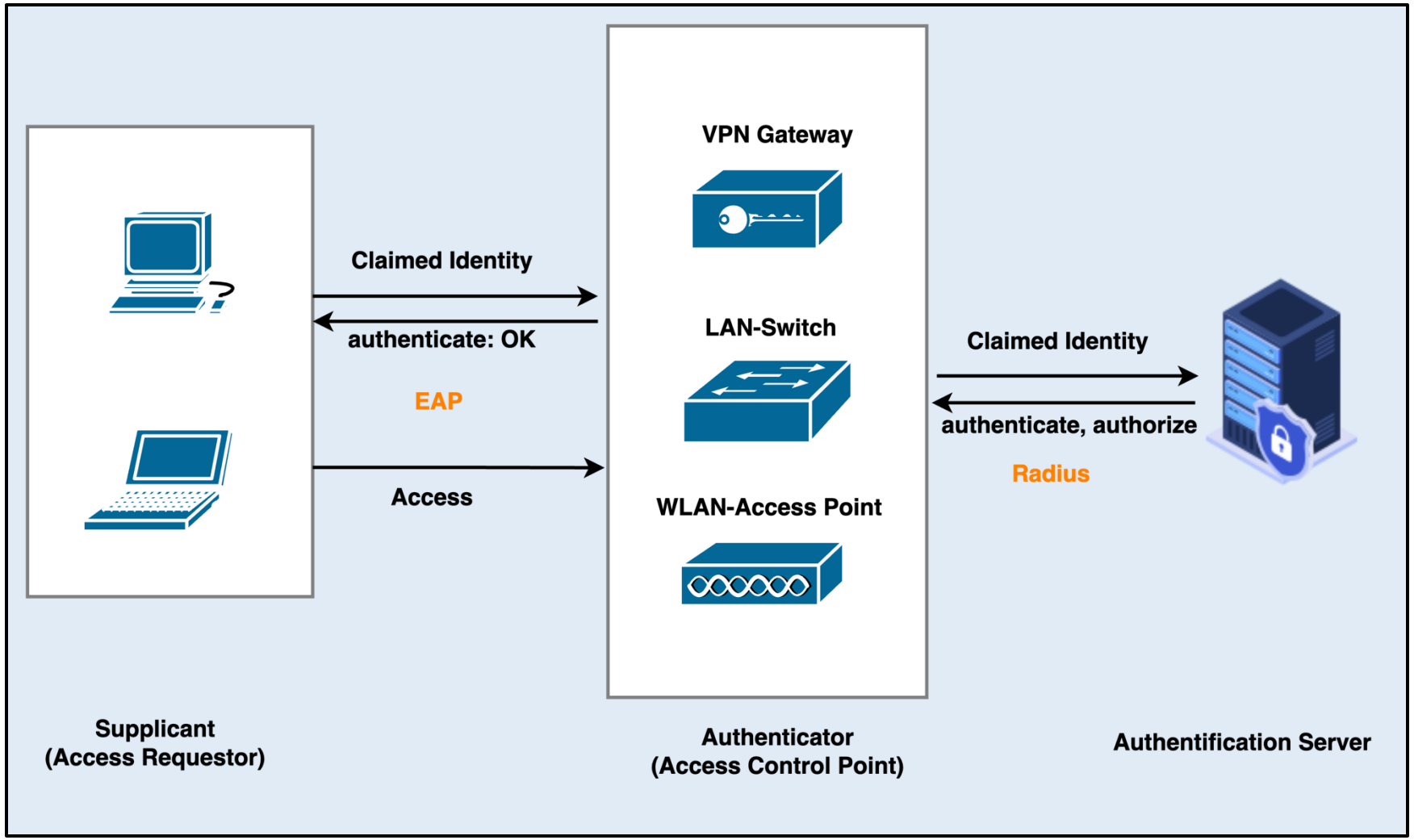
Kapitel 3: Netzwerkbasierte Authentifizierung und Autorisierung

Lernziele:

- Funktionsweise der folgenden Verfahren und Protokolle erklären und umsetzen können
  - NAC und IEEE 802.1X
  - EAPoL, EAP, RADIUS
- Threads und Sicherheitsmaßnahmen zum Absichern von NAC erklären können.

Überblick:

3.1 Network Access Control



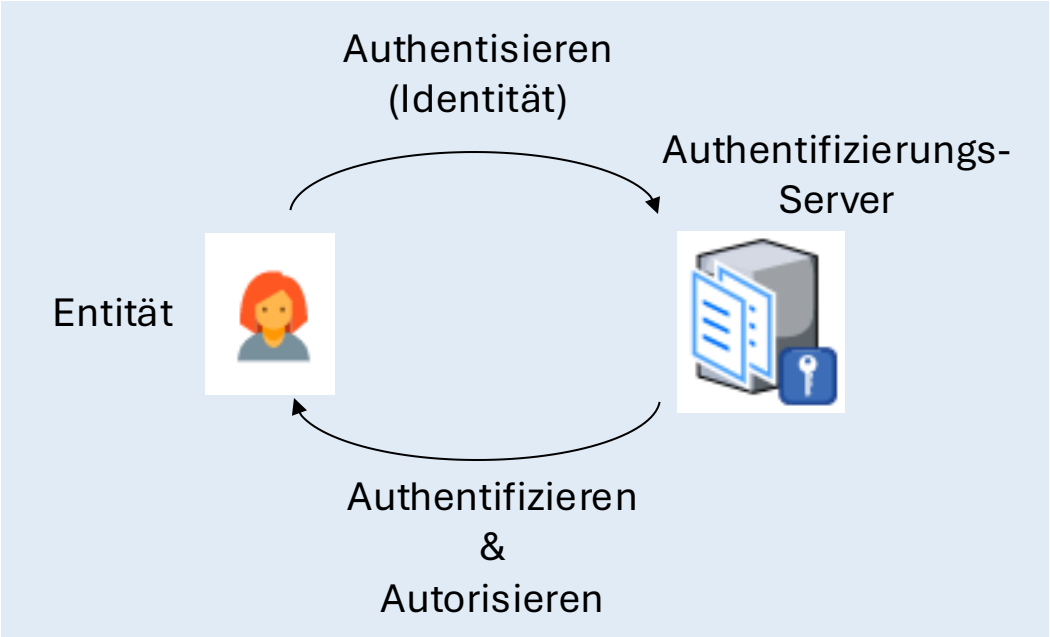
Access-Control: Authentifizierung & Autorisierung

- Begriffe
  - Entität: Eindeutig identifizierbare Person oder IT-System.
  - Digitale Identität: Menge von Attributen (Benutzername, Passwort, Computername, dig. Zertifikat, MAC-Adresse, IP-Adresse ...) die eine Entität in einem bestimmten Authentifizierungssystem eindeutig repräsentiert

Die Authentifizierung ist der Prozess, der die behauptete Identität einer Entität überprüft.

Der Authentifizierungs-Prozess besteht aus zwei Schritten:

- Authentisierung: Entität liefert den Nachweis für eine behauptete digitale Identität (z.B.: Benutzername & Passwort) an den Authentifizierungsserver (z.B.: Active Directory).
- Authentifizierung: Der Prozess zur Überprüfung einer übermittelten Identität, durch einen Authentifizierungsserver.



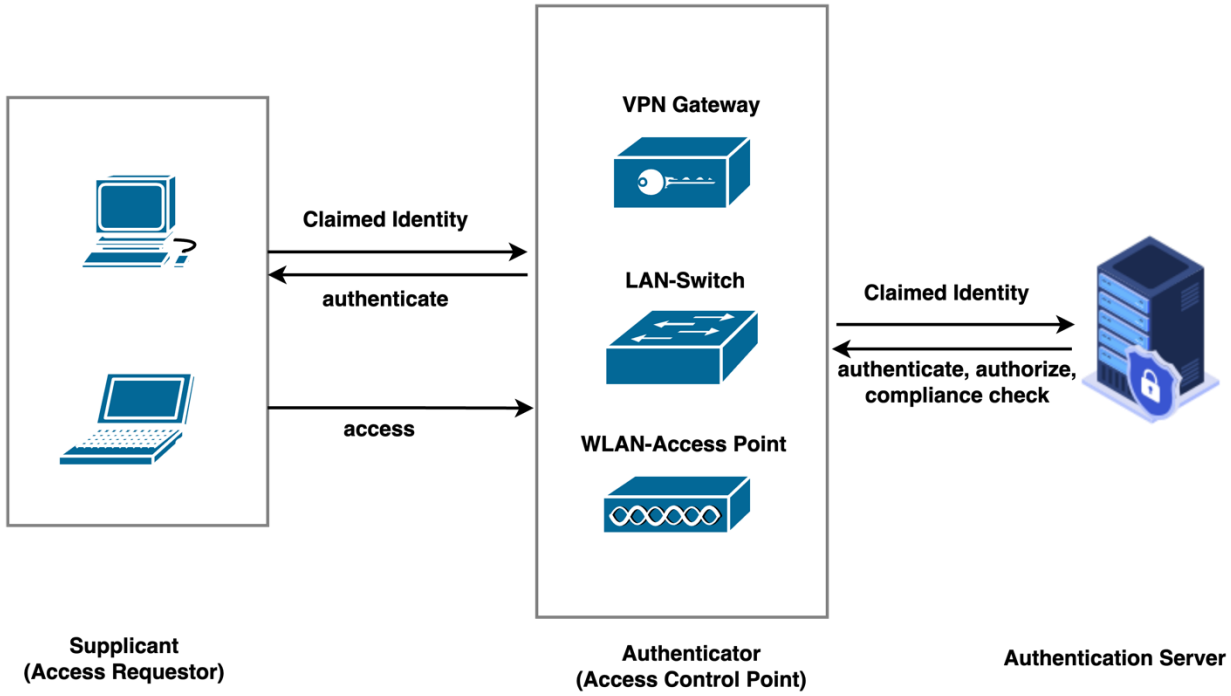
Die Autorisierung ist der Prozess, der einer authentifizierten Entität Zugriffsrechte auf ein IT-Asset einräumt.

Das Security Prinzip "Complete Mediation" fordert die Durchführung einer Zugriffskontrolle (Access Control) bei jedem Zugriff auf ein IT-Asset.

Access-Control = Authentifizierung & Autorisierung

Network Access Control (NAC)

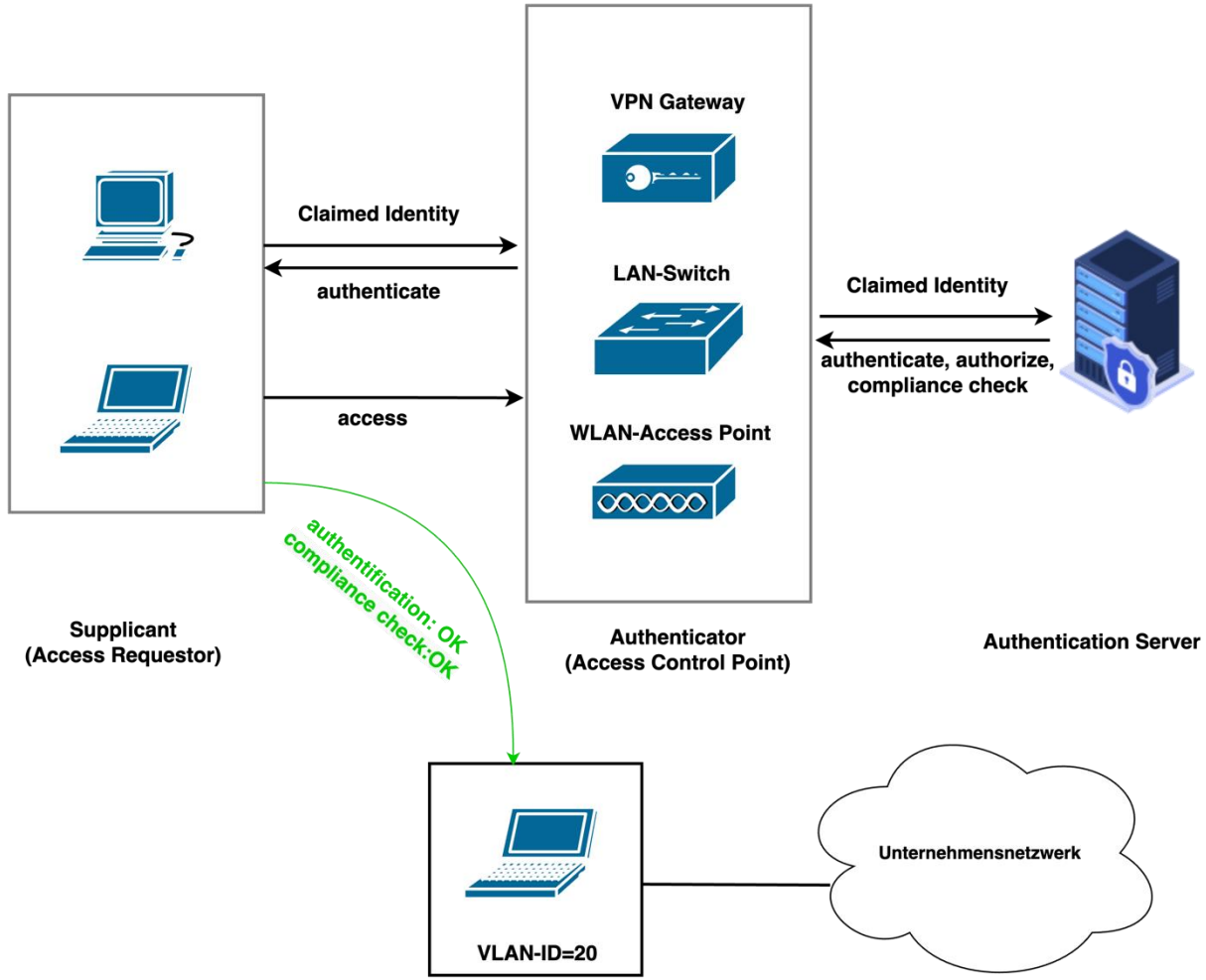
- Um ein sicheres Netzwerk zu erreichen, muss gewährleistet sein, dass jeder Zugriff auf ein Netzwerk über eine sogenannte Network-Access-Control (NAC) erfolgt:
  - Authentifizierung: Netzwerkteilnehmer wird durch einen Authentifizierungs-Server authentifiziert.
  - Autorisierung: Nach erfolgreicher Authentifizierung erhält der Teilnehmer Zugriffrechte auf das Netzwerk.
- Der Zugriff kann
  - Remote (Remote Access Control): Zugriff über öffentliche Leitungen auf ein Unternehmensnetzwerk.
    Beispiel: IPsec, TLS
  - Local (Local Access Control): Zugriff auf das LAN mittels eines Switch Ports oder per Funk via Access Point.
    Beispiel: 802.1X Port basierende Zugangskontrolle



NAC-Architektur

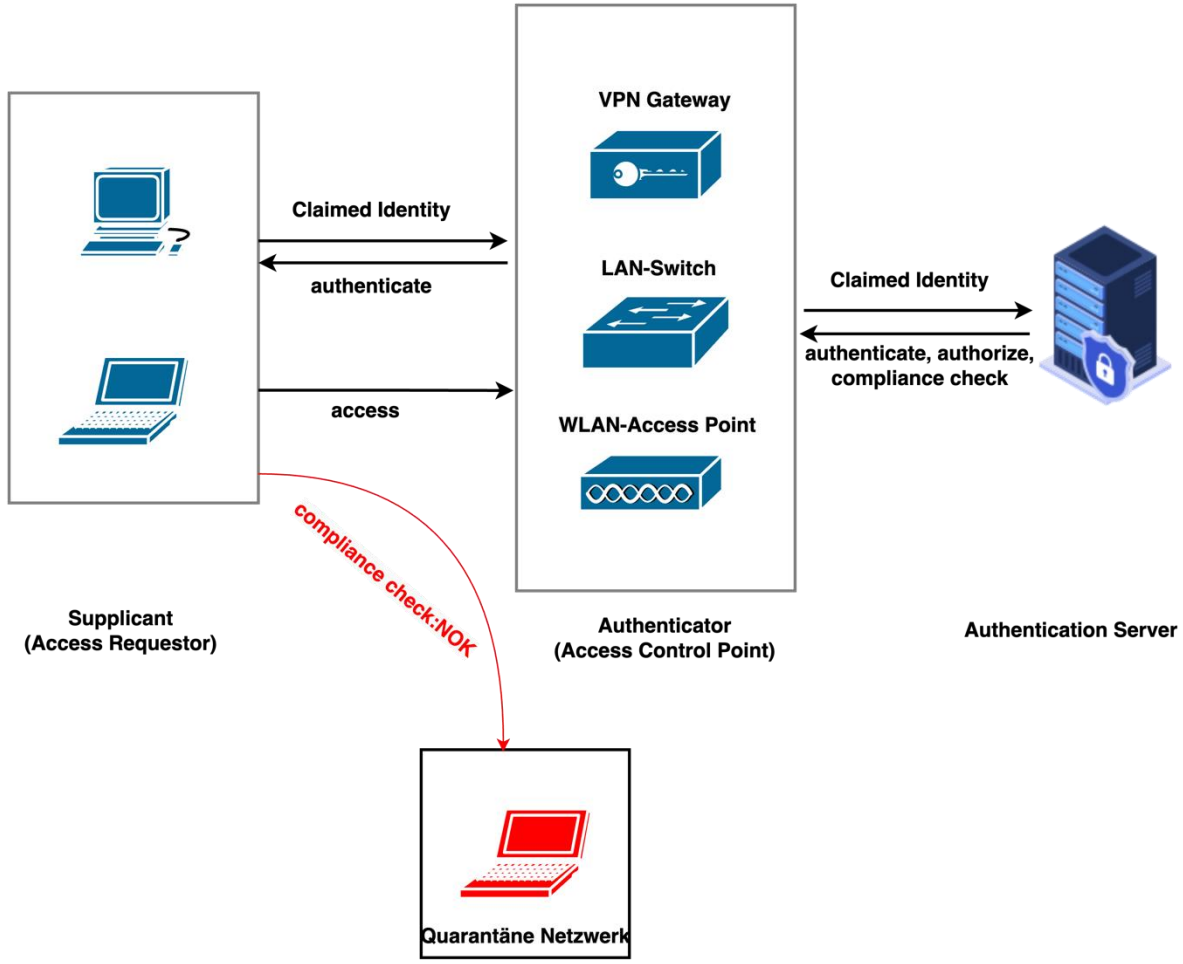
NAC-Systeme bestehen im Wesentlichen aus 3 Rollen:

- Supplicant (Access Requestor (AR)): Der AR ist der Endpunkt (PC, Notebook, Smart Device, Server, ...), der versucht, auf ein Netzwerk zuzugreifen.
- Authentificator (Access Control Point (ACP)): Der ACP ist der Zugriffskontrollpunkt für den AR. Der ACP steuert den Zugriff auf das Netzwerk eines Unternehmens. Er stellt für den AR den erlaubten Netzwerkbereich zur Verfügung.
  - Beispiele für ACPs sind: Router, Switche, WLAN-Access-Points, VPN-Gateways.
- Authentification Server (AS) : Verifiziert die Anmeldeinformationen und die Gerätekonfiguration des AR anhand von Sicherheitsrichtlinien. Informiert den ACP über das erlaubte Netzwerk. Beim AS handelt es sich beispielsweise um einen RADIUS-Server (alternativ: TACACS+ / Kerberos).



NAC - Sicherheitsdienste

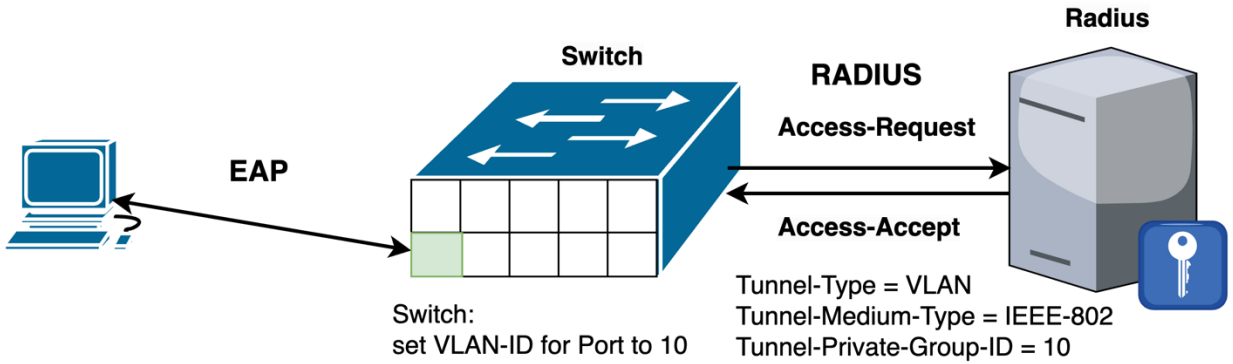
- Network Access Control (NAC) stellt zwei wichtige Sicherheitsdienste bereit:
  - Access-Control: Authentifiziert den Supplicant (PCs, Smart Devices, ...), der auf das Netzwerk zugreifen möchte, und bestimmt anhand der hinterlegten Zugriffsrechte, auf welche Netzwerksegmente ein Gerät zugreifen darf.
  - Compliance-Control: Überprüft die Konfiguration des Supplicants auf Konformität mit den Sicherheits-anforderungen (Patch-Level, Virenschutz, ...) des Unternehmens und verschiebt den Supplicant ggf. in ein Quarantäne-Netzwerk.



NAC – Autorisierung via RADIUS und VLAN

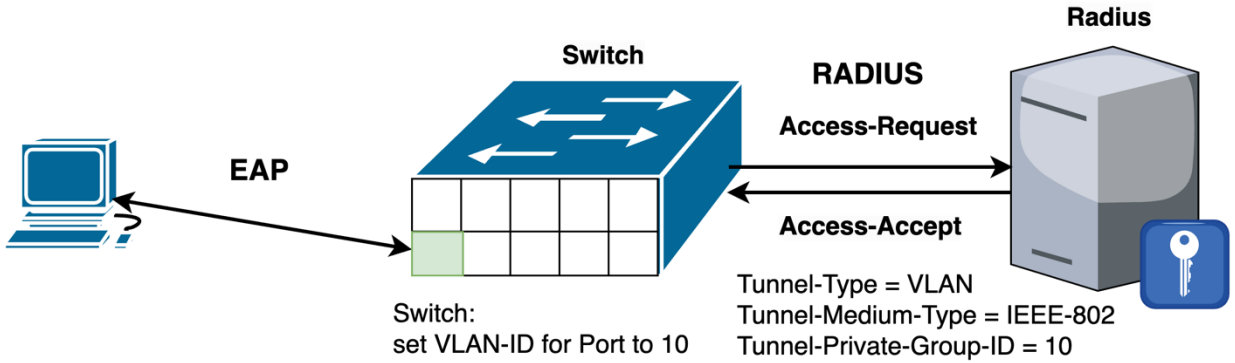
- NAC kann im Zusammenspiel mit einem RADIUS-Server als Authentication Server und einem VLAN-fähigen Switch als Authenticator, dem Switch-Port des Supplicants eine spezielle VLAN-ID zuzuweisen.
- Anwendungsfälle:
  - Segmentierung von Benutzerrollen: Weisen Sie Benutzern VLANs basierend auf Abteilungszugehörigkeit oder Funktion zu.

    Beispiele: Mitarbeiter im Bereich Forschung, Personal oder IT-Mitarbeiter, Gäste erhalten ein separates Netzwerk.
  - Segmentierung von Geräten: Geräte mit gleichen Diensten (Zeiterfassungsterminals, Drucker, ...), werden in separaten Netzwerken zusammengefasst.



VLAN-Tagging und RADIUS-Tunnel-Attribute

1. Client-Initiierung
   a. Ein Client-Gerät stellt eine Verbindung zu einem Netzwerkport an einem Switch oder einem WLAN-Access Point (AP) her.
   b. Client sendet eine Authentifizierungsanfrage.
   c. Der Switch/AP initiiert den Authentifizierungsprozess und leitet die vom Client erhaltene Authentifizierungsinformation an den RADIUS-Server weiter.
2. RADIUS-Authentifizierung und Autorisierung
   a. Der RADIUS-Server wertet die Authentifizierungsinformation aus, und übermittelt dem Switch bei erfolgreicher Authentifizierung mit einer Access-Accept-Nachricht, eine dem Benutzer (Gerät) zugeordnete VLAN-ID zu.
   b. Die Übermittelung erfolgt mit sogenannten RADIUS Tunnel-Attributen des RADIUS-Protokolls:

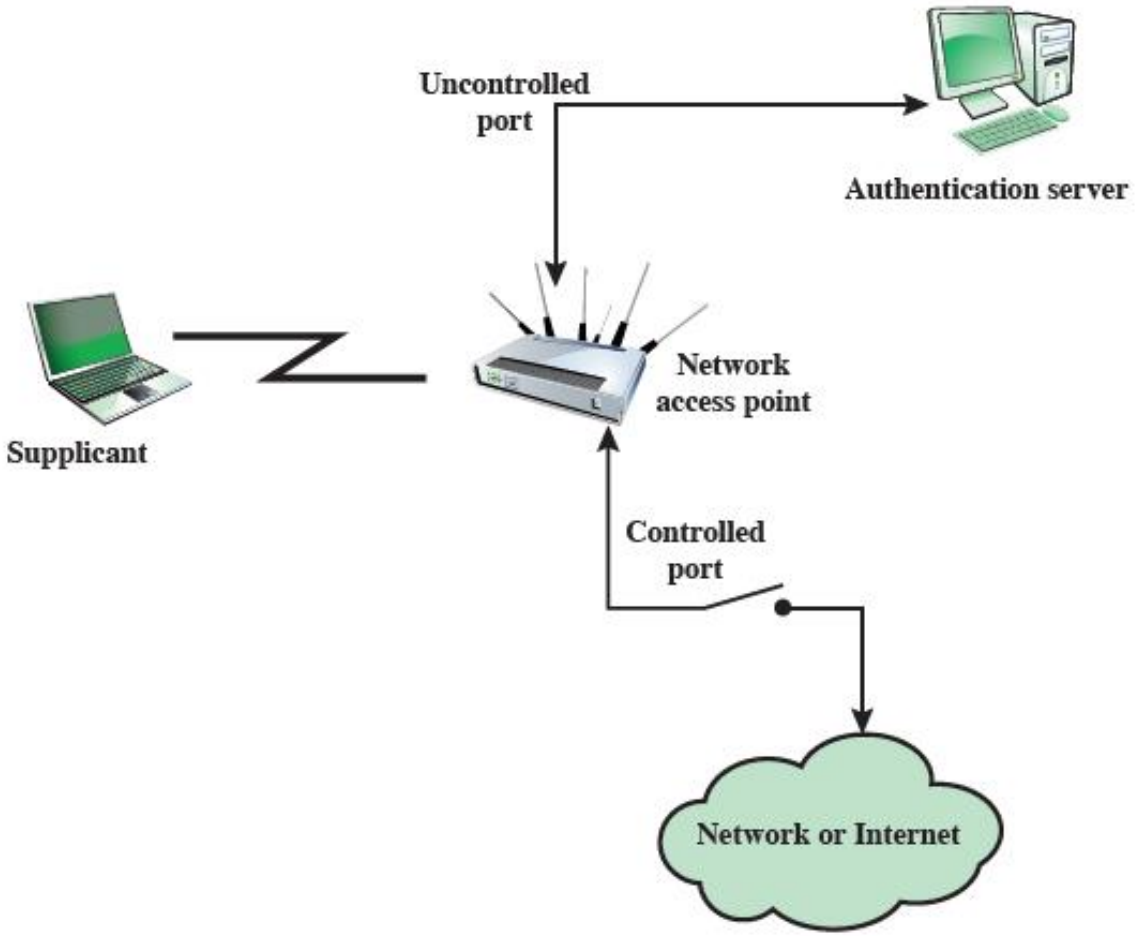


Tunnel-Type = VLAN

Tunnel-Medium-Type = IEEE-802

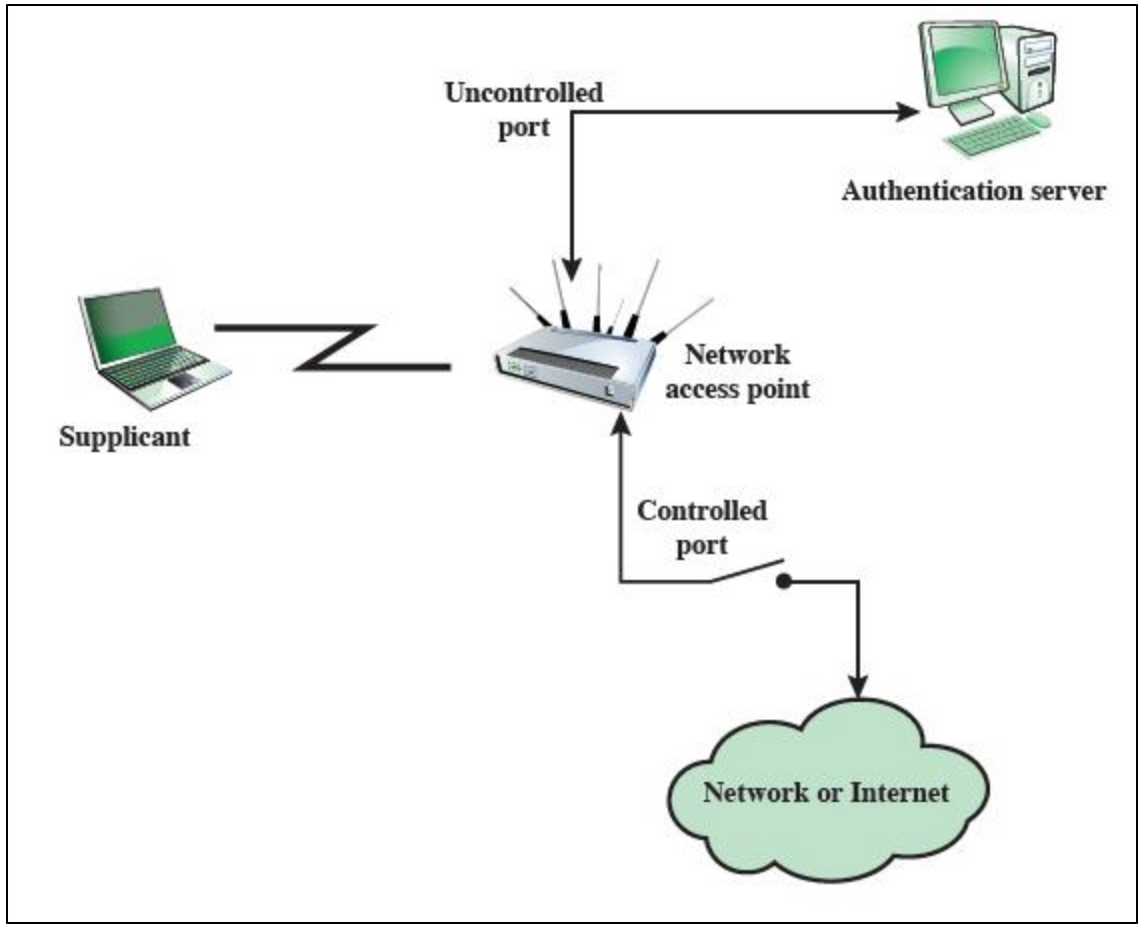
Tunnel-Private-Group-ID = 10

3.2 IEEE 802.1X Port-Based NAC



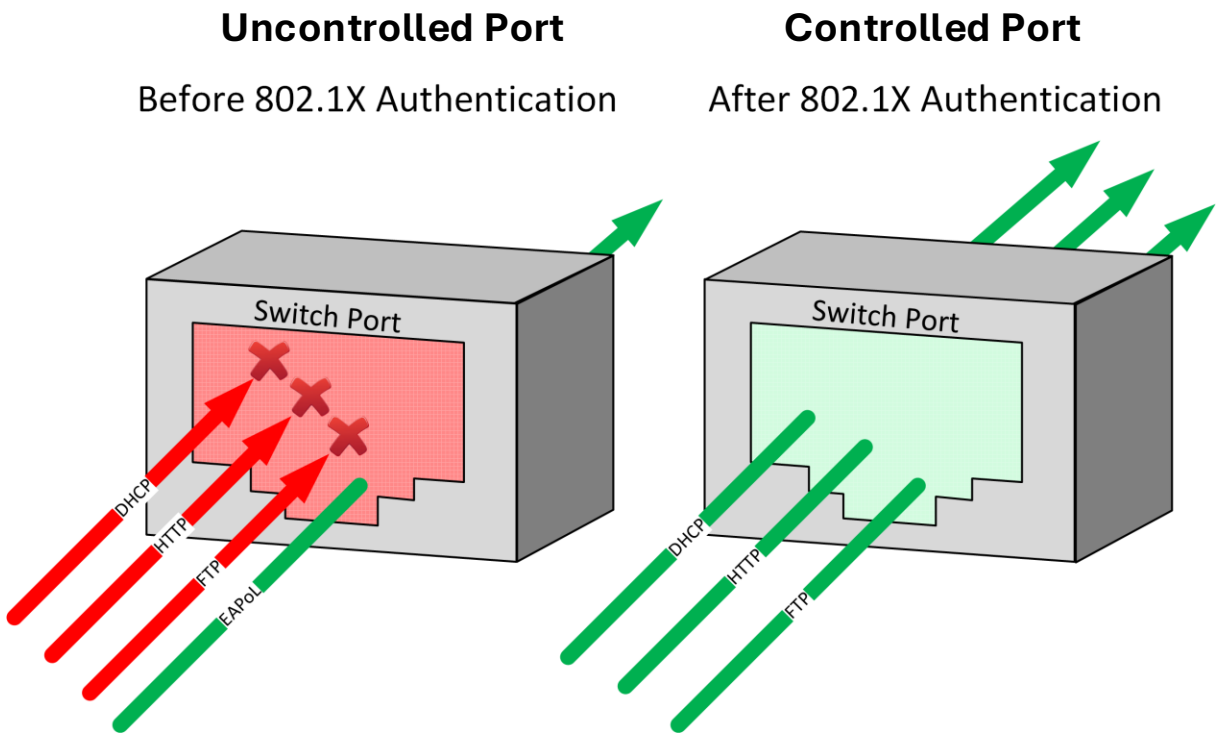
IEEE 802.1X

- IEEE802.1X ist ein IEEE-Standard für die port-basierte Netzwerkzugriffskontrolle (PNAC) für ein LAN oder ein WLAN – Netzwerk.
- Der Standard definiert ein Transportprotokoll "EAP over LAN" (EAPoL) für die Authentifizierung in einem LAN oder WLAN.
- Weiterhin definiert IEEE 802.1X im Authenticator ein Access-Control Verfahren mittels sogenannter controlled und uncontrolled Ports.
  - Switch: Ethernet-Port für den verkabelten Client
  - WLAN-AP: Logischer Port für den per Funk verbundenen Client.
- Vor der Authentifizierung befindet sich der jeweilige Port im Zustand "uncontrolled". Nach der erfolgreichen Authentifizierung befindet sich der Port im Zustand "controlled".



IEEE 802.1X Controlled and uncontrolled Ports

- Ein Authenticator (Switch, Router, Firewall) arbeitet als einfache Firewall.
- Ein uncontrolled Port ermöglicht nur den Austausch von Nachrichten zwischen dem Supplicant und dem Authentication Server, unabhängig vom Authentifizierungsstatus des Supplicants. Supplicant kann mit keinem weiteren System kommunizieren.
- Ein controlled Port ermöglicht den Austausch von Nachrichten zwischen einem Supplicant und weiteren Teilnehmern im Netzwerk.



Port Access Entity (PAE) in LAN

- Port Access Entity (PAE) bildet einen Zustandsautomat am Port des Authenticator (Switch-Port, WLAN-Port) ab.
- Der IEEE 802.1X sieht für die Konfiguration eines Switch-Ports auf einem Authenticator drei mögliche Zustände vor:
  - force-authorized (default):
    Deaktivierung von NAC via 802.1x. Der kontrollierte Port ist immer autorisiert Daten zusenden. Es erfolgt keine Autentifizierung.
  - force-unauthorized:
    Der Port ist immer nicht autorisiert und blockiert den gesamten Datenverkehr. Dient zur Isolierung eines Ports.
  - auto:
    Aktiviert die 802.1X-Authentifizierung und erfordert eine Authentifizierung des Supplicant (Client), bevor dieser Zugriff erhält.

Immer Authorized:

```
#interface GigabitEthernet0/1
#dot1x port-control force-authorized
```

Immer Unauthorized:

```
#interface GigabitEthernet0/1
#dot1x port-control force-unauthorized
```

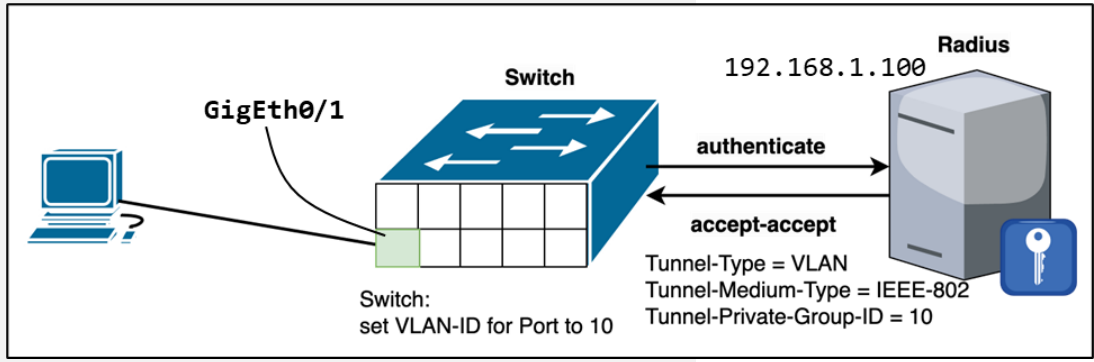
802.1X-Authentifizierung:

```
#interface GigabitEthernet0/1
#dot1x port-control auto
```

IEEE802.1x Switch-Port Konfiguration

- Switch-Portkonfiguration: Damit ein Switch-Port in der Lage ist eine dynamische Port-Konfiguration per EAP/RADIUS durchzuführen, ist die folgende Konfiguration nötig:

```
!Activate AAA globally on the Switch
Switch(config)# aaa new-model
!Enable 802.1X authentication globally on the Cisco switch
Switch(config)# dot1x system-auth-control
!Configure a specific port in access mode
Switch(config)# interface GigabitEthernet0/1
Switch(config-if)# switchport mode access
!Set Port As Authenticator (PAE)
Switch(config-if)# dot1x pae authenticator
!Automatically start authentification when device connects
Switch(config-if)# dot1x port-control auto
!Fallback VLAN if RADIUS server is not down
Switch(config-if)# authentication event server dead action authorize vlan 100
!Define the  RADIUS server and a shared secret key to encrypt messages
Switch(config)# radius-server host 192.168.1.100 key <sharedSecretKey>
```



Port Access Entity (PAE) in WLAN

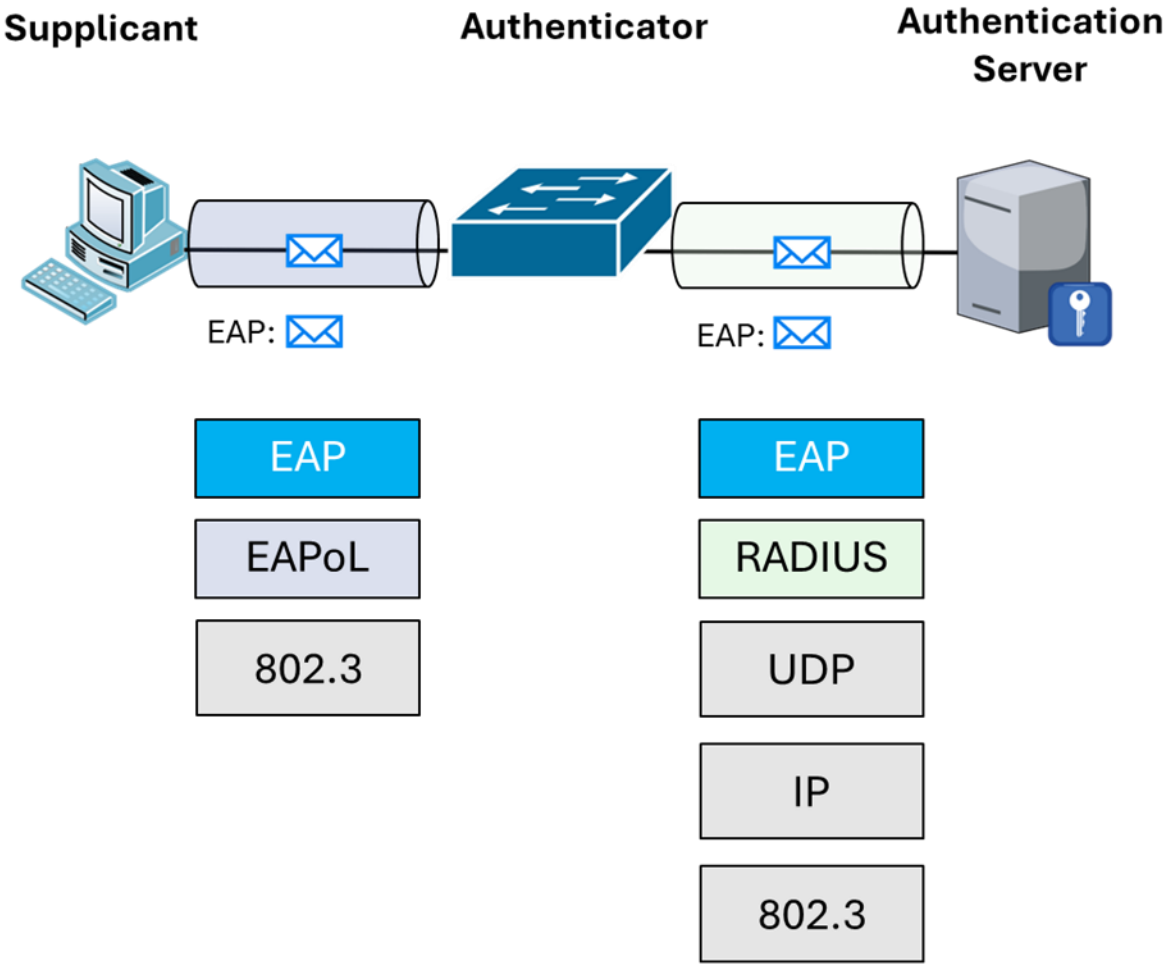
- Um die Port Access Entity (PAE) im Zustand auto auf einem WLAN-Access Point zu aktivieren, muss dort unter Sicherheit
  - WPA2-Enterprise

    oder
  - WPA3-Enterprise

  aktiviert werden.
- Unter Authentifikation Key Management kann dann 802.1X und die gewünschte EAP-Authentifizierungsmethode ausgewählt werden.

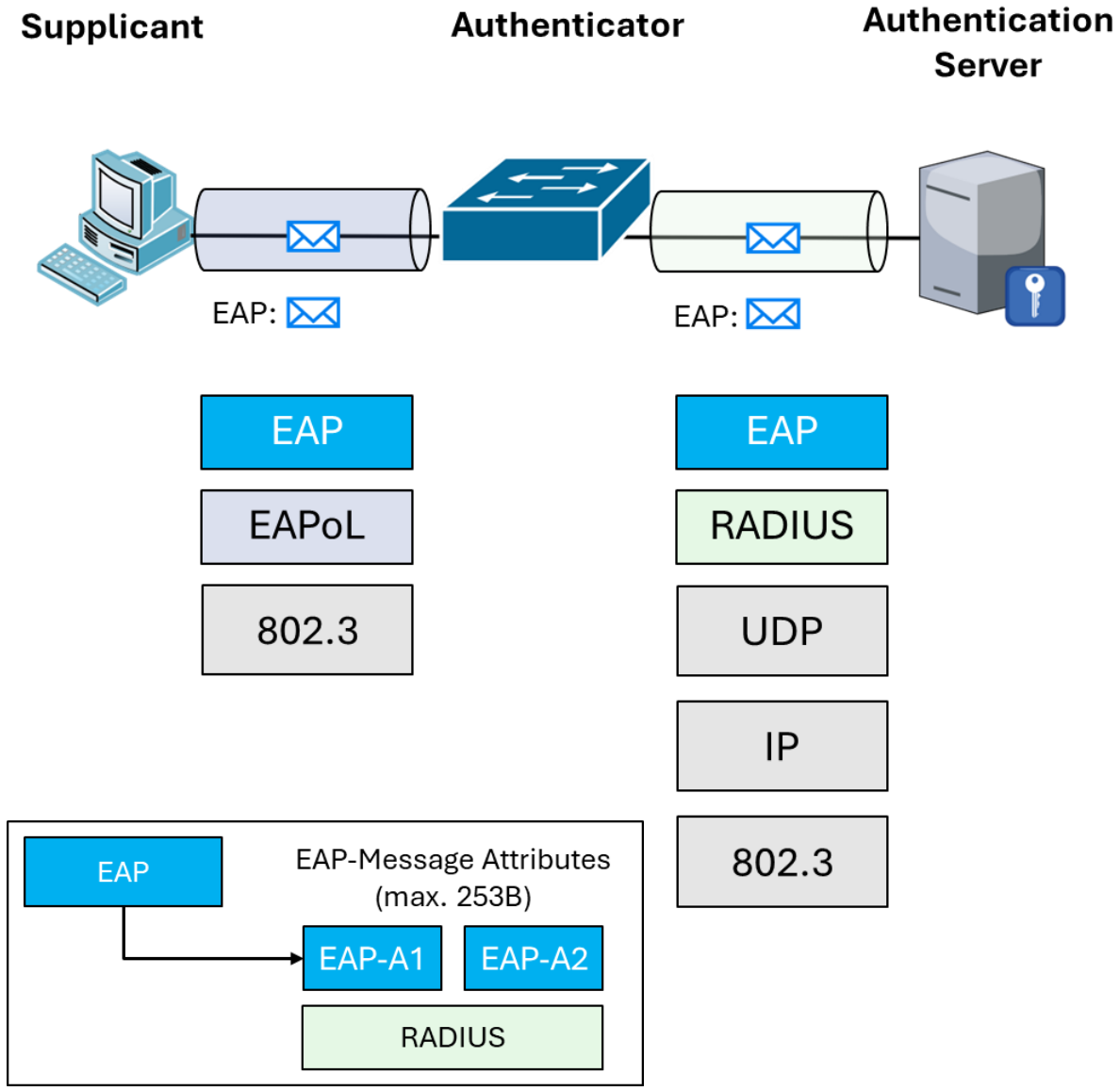
Port-Based NAC in LAN und WLANs

- Der Prozess der Authentifizierung erfolgt über dedizierte Authentifizierungsprotokolle
  - EAPoL (EAP over LAN) dient als Transportprotokoll für EAP in LANs und WLANs.
  - EAP (Extensible Authentification Protocol) übermittelt den Authentifizierungs-Payload (Authentifizierungsdaten und Algorithmen) und ist unabhängig vom Transportprotokoll.
  - RADIUS (Remote Authentification Dial-In User Service) transportiert den Inhalt der EAP-Nachricht (Benutzer-name & Passwort) und übermittelt Access-Control-Information an einen zentralen RADIUS-Server.



Port-Based NAC: Nachrichtentransport

- EAPoL-Nachrichten transportieren die EAP-Nachrichten in lokalen IEEE 802.X-Netzwerken vom Supplicant zum Authenticator.
- Die EAPoL-Nachrichten werden wiederum durch das jeweilige Layer-2-Protokoll transportiert
  - IEEE802.3 : Ethernet in LAN
  - IEEE802.11 : WLAN
- Wenn ein Authenticator ein EAPOL-Paket vom Supplicant erhält, entfernt er die Kapselung (EAPOL/802.X).
- Anschließend speichert er den EAP-Nachrichteninhalt in Form von mehreren 253B großen EAP-RADIUS-Attributen und sendet diese als RADIUS Nachricht an den RADIUS-Server.
- Das RADIUS-Protokoll verwendet UDP als Transportschicht.



EAPOL-Nachrichten

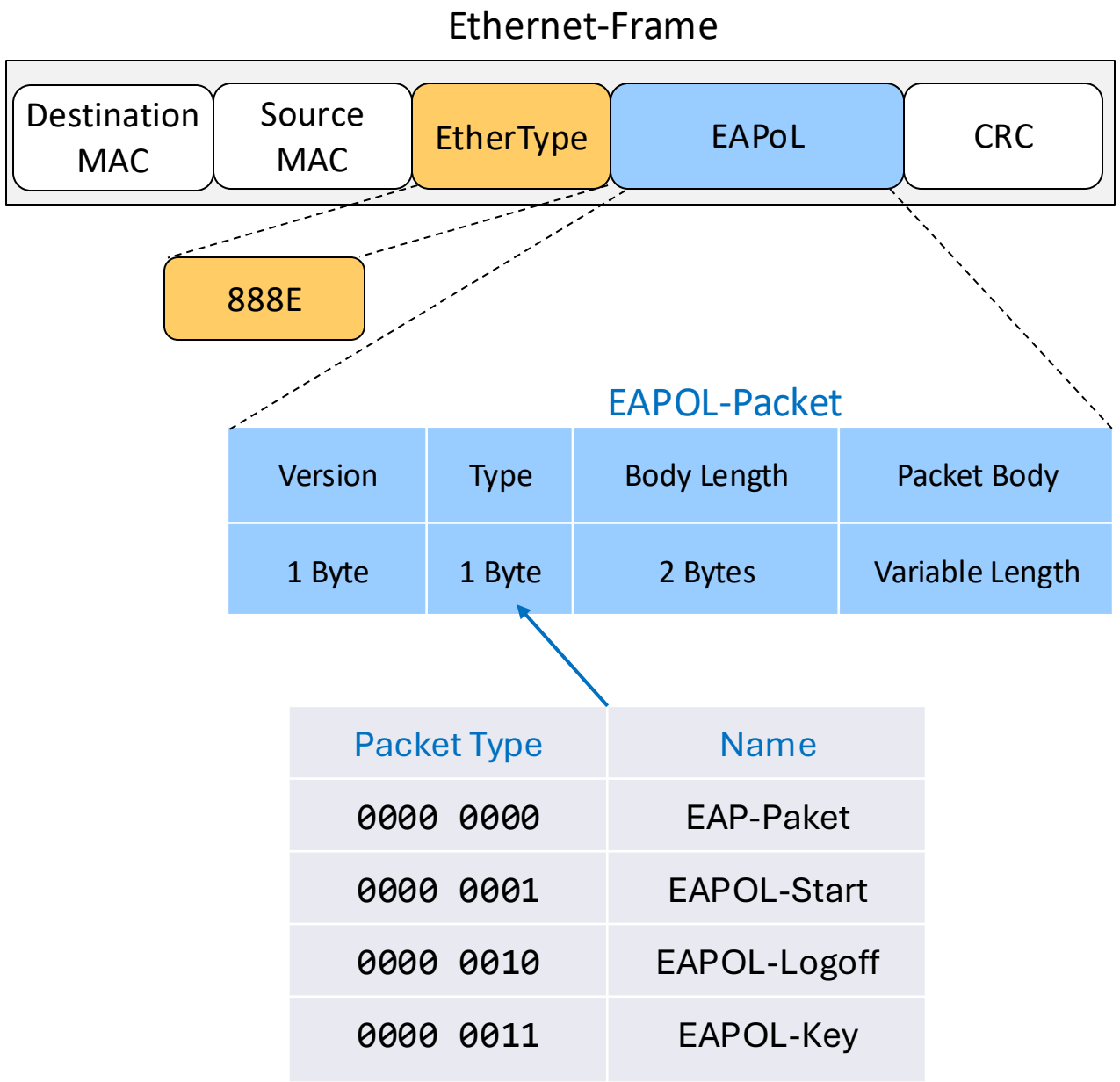
- Nebenstehende Abb. zeigt eine EAPoL – Nachricht, die mittels einem Ethernet-Frame transportiert wird.
- Das Ethernet-Frame zeigt über den EtherType an, das es ein EAPOL-Packet transportiert:
  - EtherType (2 Byte): 0x888E für das EAPOL-Protokoll
- Die EAPoL-Nachricht besteht aus den folgenden Feldern:
  - Version (1Byte): 2 (fixer Wert für aktuelle Version 2)
  - EAPOL Type (1 Byte): Beschreibt den Nachrichten-Typ

    EAPoL-Paket: 0x00

    EAPOL-Start: 0x01

    EAPOL-Logoff: 0x02

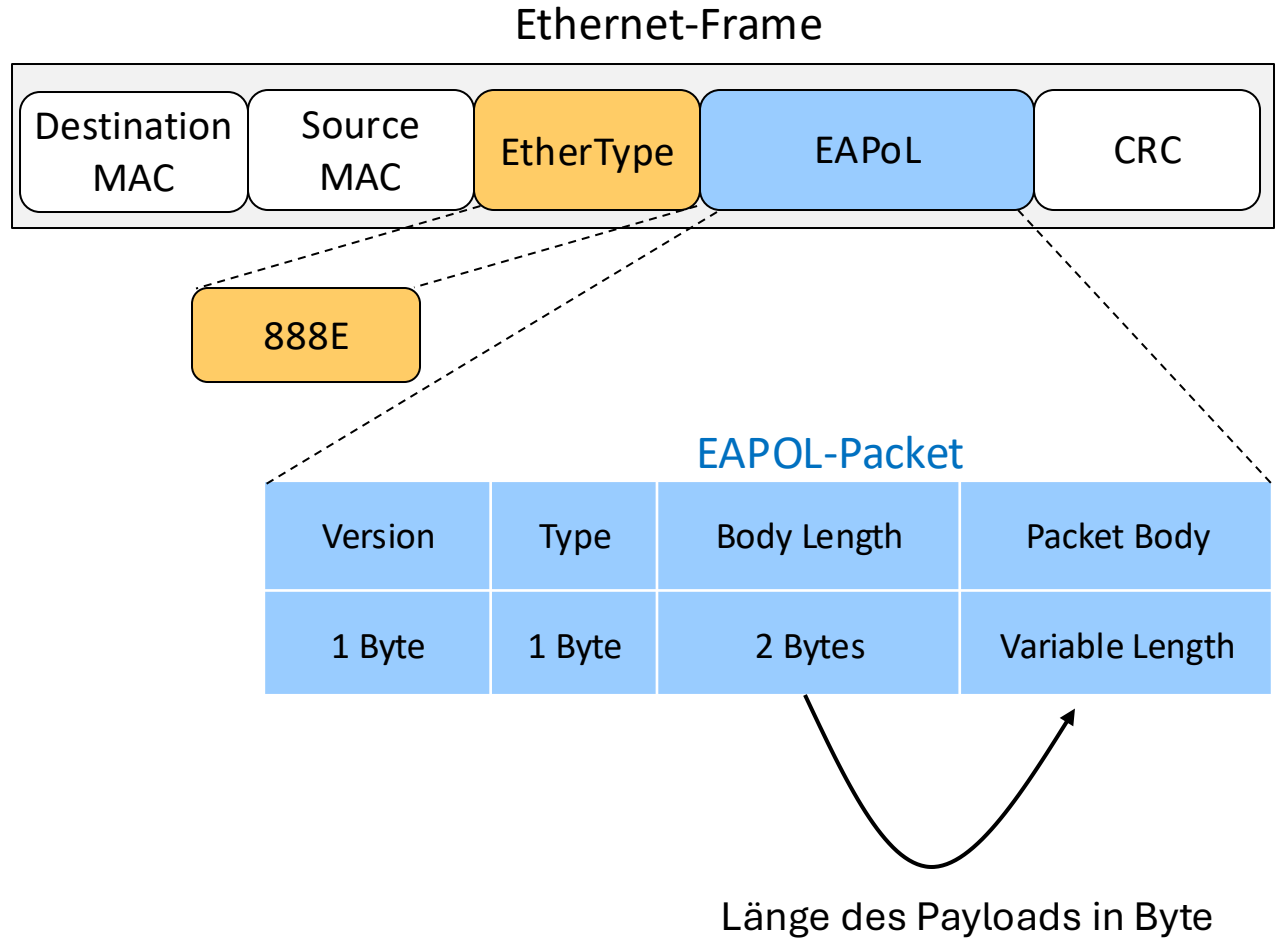
    EAPOL-Key: 0x03



EAPOL-Nachrichtenformat

- Body Length: Länge des EAPOL-Packet-Bodys in Byte.

  Wenn der Pakettyp EAPoL-Start oder EAPOL-Logoff ist, wird dieses Feld auf 0x0000 gesetzt, und es folgt kein Feld für den Packet-Body.
- Packet-Body: Payload z.B. ein EAP-Frame.



EAPOL-Frames

- EAPoL verwendet primär die folgenden 4 Pakete, um die EAP-Nachrichten vom Supplicant zum Authenticator zu transportieren.
  - EAPoL-Start: Um die Authentifizierung zu starten schickt der Supplicant eine EAPOL-Start-Nachricht an den Authenticator.
  - EAPoL-Packet: Das EAPOL-Packet-Frame transportiert alle EAP-Request-/Response Nachrichten und die finale EAP-Success- oder EAP-Failure-Nachricht zwischen dem Supplicant und dem Authenticator.
  - EAPoL-Logoff: Supplicant schickt dieses Frame, um die Verbindung zu beenden.
  - EAPoL-Key: Das EAPOL-Key Frame transportiert alle Frames zum Aushandeln einer verschlüsselten Daten-verbindung nach der erfolgreichen Authentifzierung. Beispiel: **4-Wege-Handshake** für **WLAN (WPA2, WPA3)**.

EAPOL-Start

Version	Type	Length	Packet Body
0x02	0x01	0x0000	(empty)

EAPOL-Packet

Version	Type	Length	Packet Body
0x02	0x00	nn	EAP-Nachricht

EAPOL-LogOff

Version	Type	Length	Packet Body
0x02	0x02	0x0000	(empty)

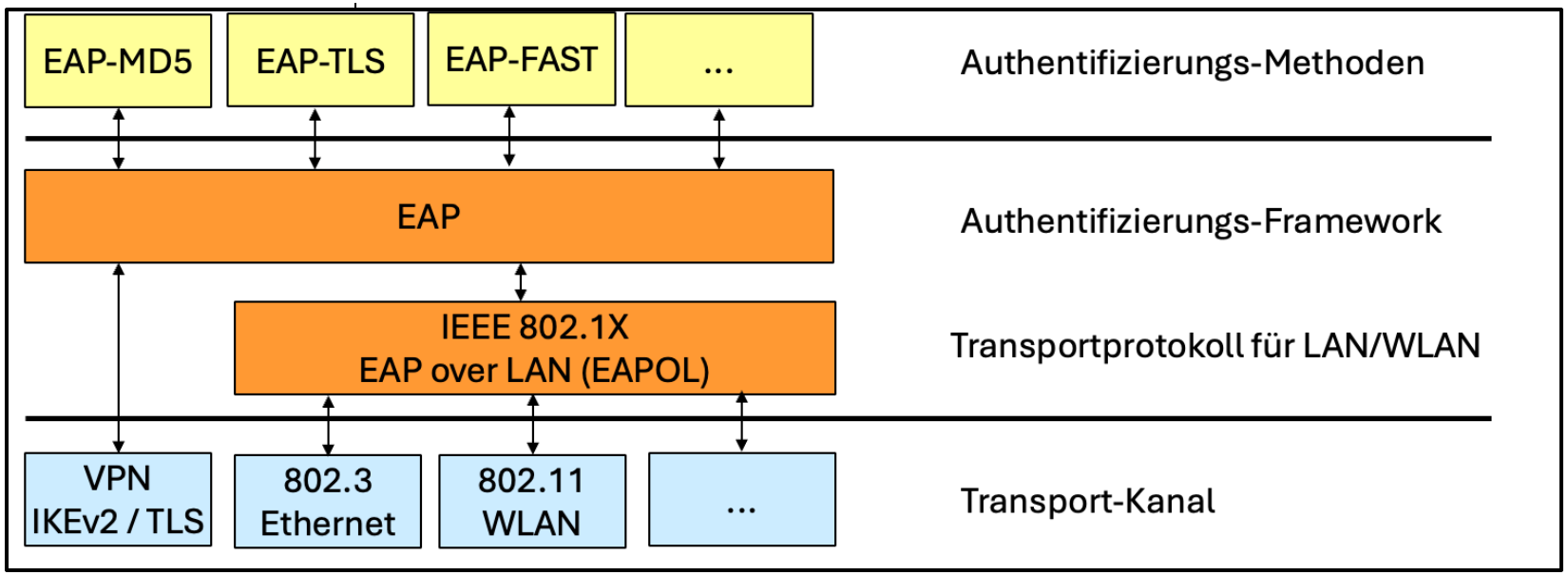
EAP (Extensible Authentication Protocol)

- EAP ist ein Internetstandard RFC3748 .
- EAP unterstützt verschiedene Authentifizierungsmethoden, z.B. EAP-TLS, EAP-OTP, EAP-MD5,... und ist erweiterbar ("extensible") um neue Authentifizierungsmethoden.
- Die EAP-Nachrichten transportieren die eigentlichen Authentifizierungsdaten auf Basis der vorkonfigurierten Authentifizierungsmethode (z.B.: EAP-TLS).
- Die EAP-Nachrichten werden als Payload von verschiedenen Transport-Protokollen übertragen:
  - LAN / WLAN via EAPoL
  - IPSec-VPN via IKEv2
  - Web-VPN via TLS

FAST: Flexible Authentication via Secure Tunneling

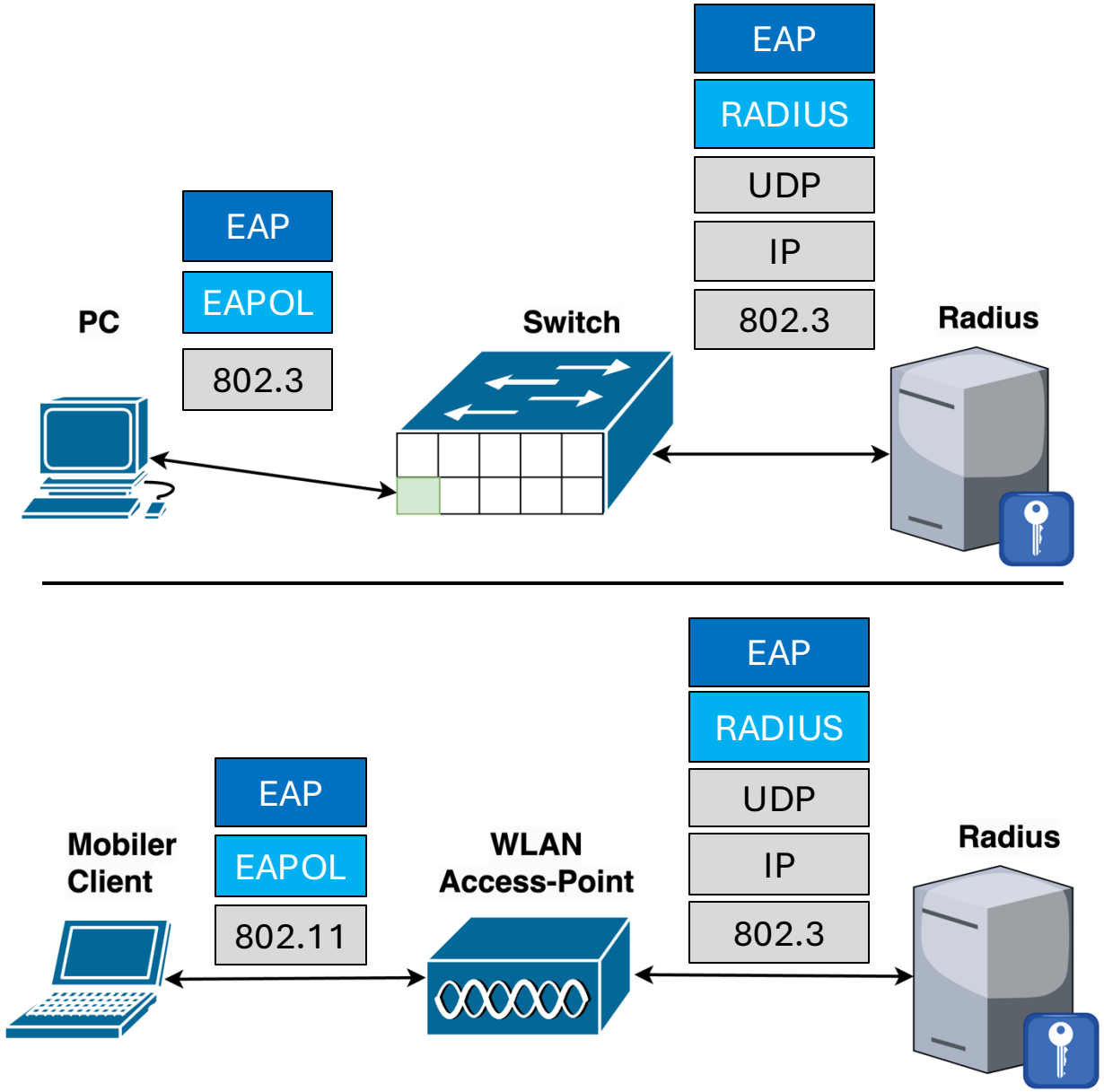
Beispiele für Authentifizierungsmethoden:

- EAP-TLS: Verwendet das TLS-Handshake-Protokoll zum Aufbau eines verschlüsselten TLS-Kanals, Authentifizierung erfolgt über digitale Zertifikate.
- EAP-Fast: Verwendet ein pre-shared Credential (Protected Access Credential) zwischen Authenticator und Authentication Server zum Aufbau eines verschlüsselten TLS-Kanals. Authentifizierung erfolgt dann mit Username und Passwort.



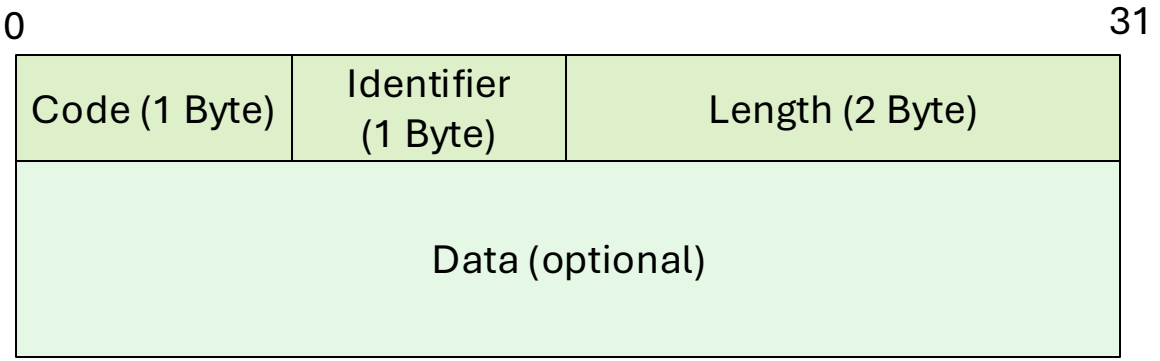
EAP: Pass-Through-Mode

- Der RADIUS-Server fungiert als zentraler Authentifizierungs-server, der für alle Authenticator (Switch, Router, Firewall) in einem Unternehmen Authentifizierungsanfragen annimmt und diese authentifiziert und ggf. autorisiert.
- Der jeweilige Authenticator empfängt die EAP-Anfragen von einem Supplicant (PC) und leitet diese als Gateway an den RADIUS-Server weiter.
- Dieses Verfahren wird auch als EAP-Durchgangsmodus (Pass-Through-Mode) bezeichnet.
  - Zwischen dem Supplicant und dem Authenticator wer-den die EAP-Nachrichten in Pakete des Transportproto-koll (Ethernet, WLAN: EAPOL) eingepackt und übertragen.
  - Zwischen dem Authenticator und dem RADIUS-Server werden die EAP-Nachrichten über das RADIUS-Protokoll in Form von EAP-Message-Attribute transportiert.



EAP-Nachrichtenformat

- Das EAP-Nachrichtenpaket besteht aus einem Header mit den Feldern Code, Identifier und Length und einem optionalen Data-Bereich, der die Authentfizierungsdaten enthält.
- Code (1Byte) - Identifiziert den Typ der EAP-Nachricht. Die folgenden 4 Typen werden für die Authentifizierung verwendet:
  - Code=1: EAP-Request - Nachricht vom Authenticator an den Supplicant.
    z.B.: Anfordern der Identität
  - Code=2: EAP-Response - Nachricht vom Supplicant zum Authenticator.
    z.B.: Senden der Identität, eines Passwortes oder digitalen Zertifikates
  - Code=3: EAP-Success - Nachricht vom Authenticator an Supplicant bei erfolgreicher Authentifizierung.
  - Code=4: EAP-Failure – Nachricht vom Authenticator an Supplicant bei fehlerhafter Authentifizierung.

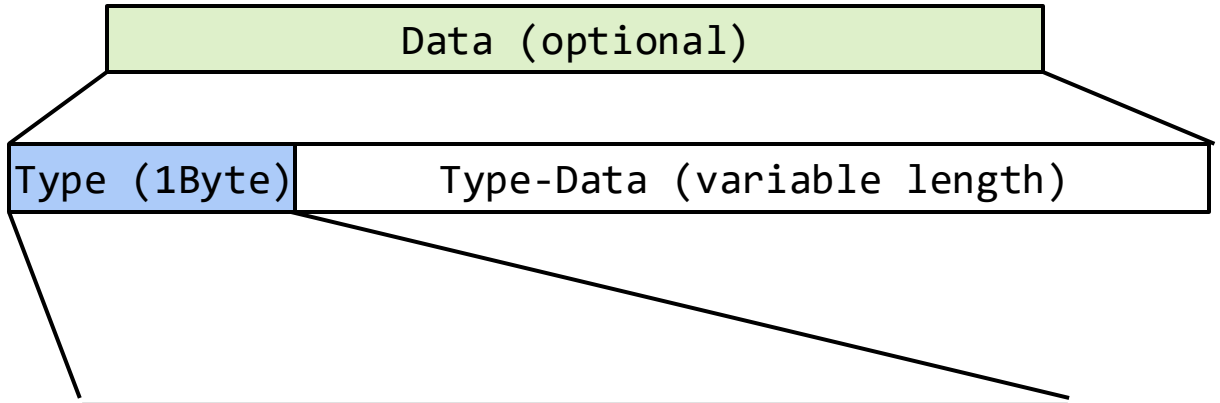


- Identifier (1Byte) - Enthält eine vorzeichenlose Ganzzahl, die für ein Response- und Request-Nachrichtenpaar gleich sein muss und für jedes neue Paar um 1 erhöht wird.
- Länge (2Byte) - Enthält die Anzahl der Bytes des gesamten EAP-Paketes (Header & Data)
- Daten - Das Datenfeld hat eine variable Länge zwischen 0 und $(2^{16} - 4)$B.

"Success"- und "Failure"- Nachrichten enthalten kein Daten-Feld.

EAP-Nachrichtenformat

- Data: Das Datenfeld ist optional. Das Datenfeld besteht aus einem Type-Feld, das den Typ des Dateninhaltes beschreibt und den zugeordneten Type-Data.
- Type (1B): Dieses Feld gibt den Typ der Request- oder Response-Nachricht an.
  - Für jede EAP-Anfrage oder -Antwort MUSS ein Type angegeben werden.
  - Der Response-Typ muss mit dem Request-Typ überein. Ausnahme: NAK-Frame
- Type Data: Enthält die eigentliche Nutzlast. Der Inhalt hängt vom Type-Wert und der Phase des Authentifizierungs-prozesses ab.



Value	Description	Reference
0	Reserved	
1	Identity	[RFC3748]
2	Notification	[RFC3748]
3	Legacy Nak	[RFC3748]
4	MD5-Challenge	[RFC3748]
5	One-Time Password (OTP)	[RFC3748]
13	EAP-TLS	[RFC5216]
...	...	...

Beispiele für Type-Werte

EAP Nachrichtenformate

- Mögliche Varianten an EAP-Response und EAP-Request Nachrichten:

Feld	Länge	Beschreibung
Code	1B	1 = Request, 2 = Response
Identifier	1B	Request- und Response-Zuordnung oder Identifier der letzten Response
Length	2B	Länge der gesamten Nachricht
Type	1B	Gibt die EAP-Methoden-ID an (z. B. 1 = Identity, 4 = MD5-Challenge, 13 = TLS)
Data	variabel	Abhängig von der verwendeten EAP-Methode (z. B. Benutzername, Zertifikat, Challenge).

- Die Nachrichten EAP-Request/Identity vom Authenticator zum Supplicant startet die EAP-Authentifizierung.
- Der Supplicant antwortet in der EAP-Response/Identity mit seiner Identität.

EAP-Request/Identity

```
Code: 1 (Request)
Identifier: 5
Length: nn
Data:
 Type: 1 (Identity)
 Type-Data: ""
```

Authenticator → Supplicant

EAP-Response/Identity

```
Code: 2 (Response)
Identifier: 5
Length: nn
Data:
 Type: 1 (Identity)
 Type-Data: "bob@example.de"
```

Supplicant → Authenticator

EAP Nachrichtenformate

- Die Nachrichten zur Authentifzierung werden generell als **EAP-Request/Auth** und **EAP-Response/Auth**.
- Die nachfolgenden Nachrichten werden für eine EAP-TLS-Authentifizierung (Type=13) verwendet:

EAP-Request/Auth

```
Code: 1 (Request)
Identifier: 10
Length: nn
Data:
 Type: 13 (EAP-TLS)
 Type-Data:
  "TLS Handshake Nachricht"
```

EAP-Response/Auth

```
Code:  2 (Response)
Identifier: 10
Length:  nn
Data:
 Type: 13 (EAP-TLS)
 Type-Data:
  "TLS Handshake Nachricht"
```

- Der finale Status der Authentifizierung wird vom Authenticator mit den folgenden Nachrichten dem Supplicant mitgeteilt:
  - EAP-Success – Authentifizierung war erfolgreich
  - EAP-Failure – Authentifizierung war nicht erfolgreich

EAP-Success

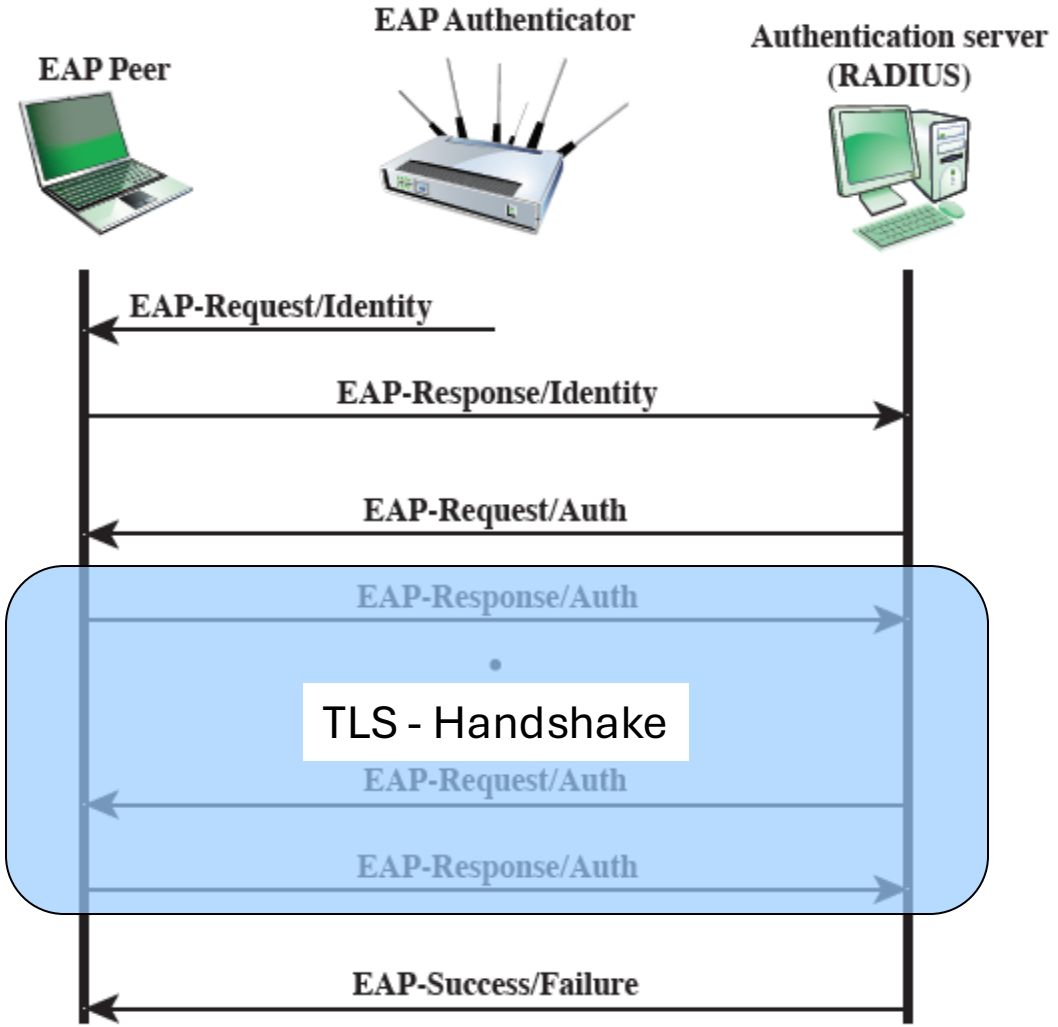
```
Code: 3 (Success)
Identifier: 10
Length: 0x0004
```

EAP-Failure

```
Code: 4 (Failure)
Identifier: 10
Length: 0x0004
```

EAP-TLS - Prozessschritte

- Ein sicheres Authentifizierungsverfahren ist die EAP-TLS Methode.
- TLS steht für das sichere Transport-Layer-Security-Protokoll.
- Hierbei wird nach dem initialen Austausch der Identität eines Benutzers oder eines Gerätes ein TLS-Handshake durchgeführt.
- Der TLS-Handshake wird mittels den EAP-Request/Auth- und EAP-Response/Auth-Nachrichten vom Typ=13 übertragen.
- Während des Handshakes werden die digitalen Zertifikate des Supplicants und des RADIUS-Server ausgetauscht und zur Authentifzierung verwendet.
- Ist die Authentifizierung erfolgreich oder die Authentifizierung fehlgeschlagen sendet der RADIUS-Server die finale EAP-Success- oder EAP-Failure-Nachricht an den Authenticator.
- Der Authenticator sendet diese an den Supplicant per EAP-Success oder EAP-Failure an den Supplicant.



EAP-TLS Nachrichtenformate

- Type =13 (EAP-TLS):

  Es handelt sich um eine EAP-Request und EAP-Response-Nachricht der EAP-TLS Authentifizierungsmethode.

- Type-Data enthält eine oder mehrere TLS-Nachrichten des TLS-Handshakes (ClientHello, ServerHello, Server Certificate, Client Key Exchange, ...), die im Rahmen des Handshakes sukzessive transportiert werden. Ist eine TLS-Nachricht zu groß, kann Sie auch fragmentiert werden.

EAP-Request/TLS-Start

```
Code: 1 (Request)
Identifier: 7
Length: nn
Data:
  Type: 13 (EAP-TLS)
  Type-Data: (empty)
```

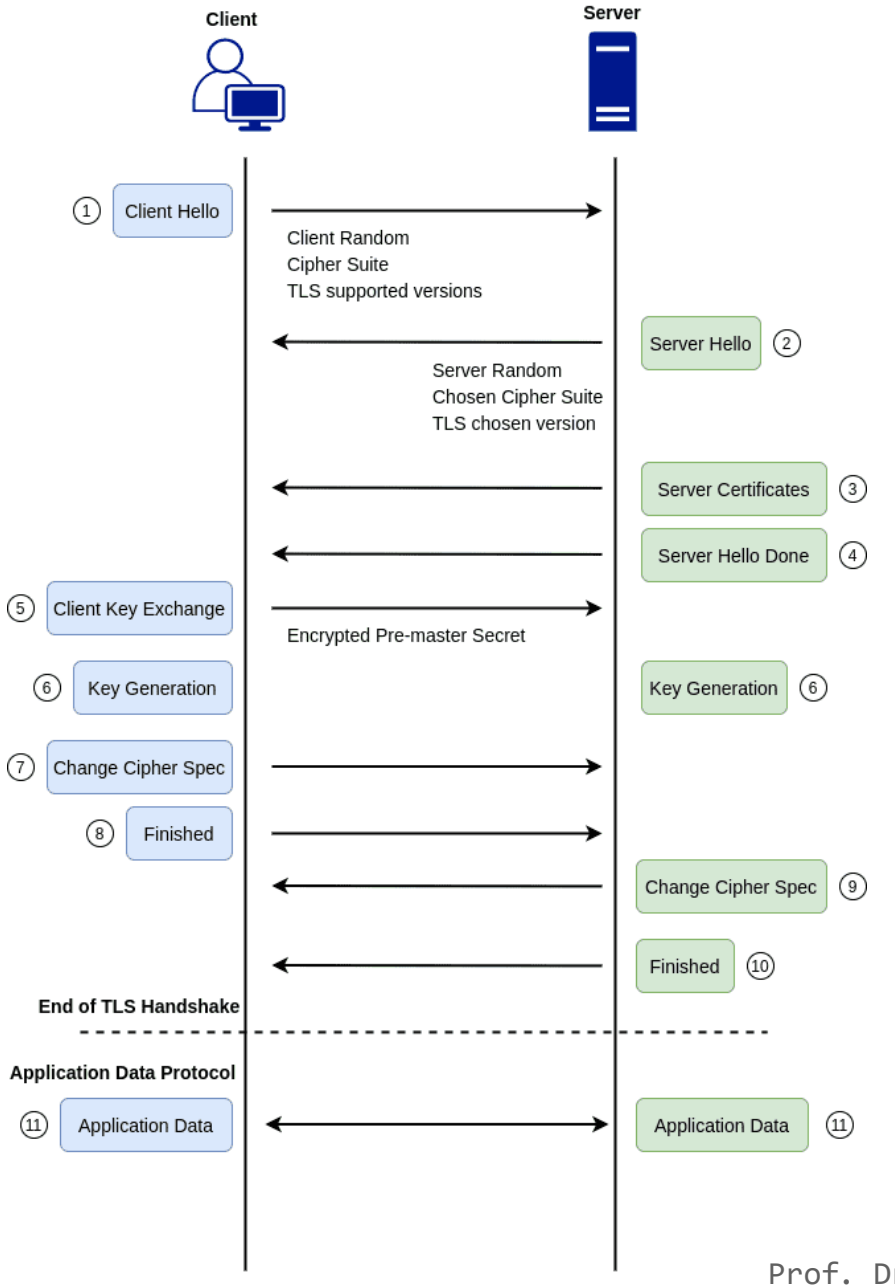
EAP-Response/TLS-ClientHello

```
Code: 2 (Response)
Identifier: 7
Length: nn
Data:
  Type: 13 (EAP-TLS)
  Type-Data: TLS-ClientHello Message
```

EAP-Request/TLS-ServerHello

```
Code: 1 (Request)
Identifier: 8
Length: nn
Data:
  Type: 13 (EAP-TLS)
  Type-Data: TLS-ServerHello Message
```

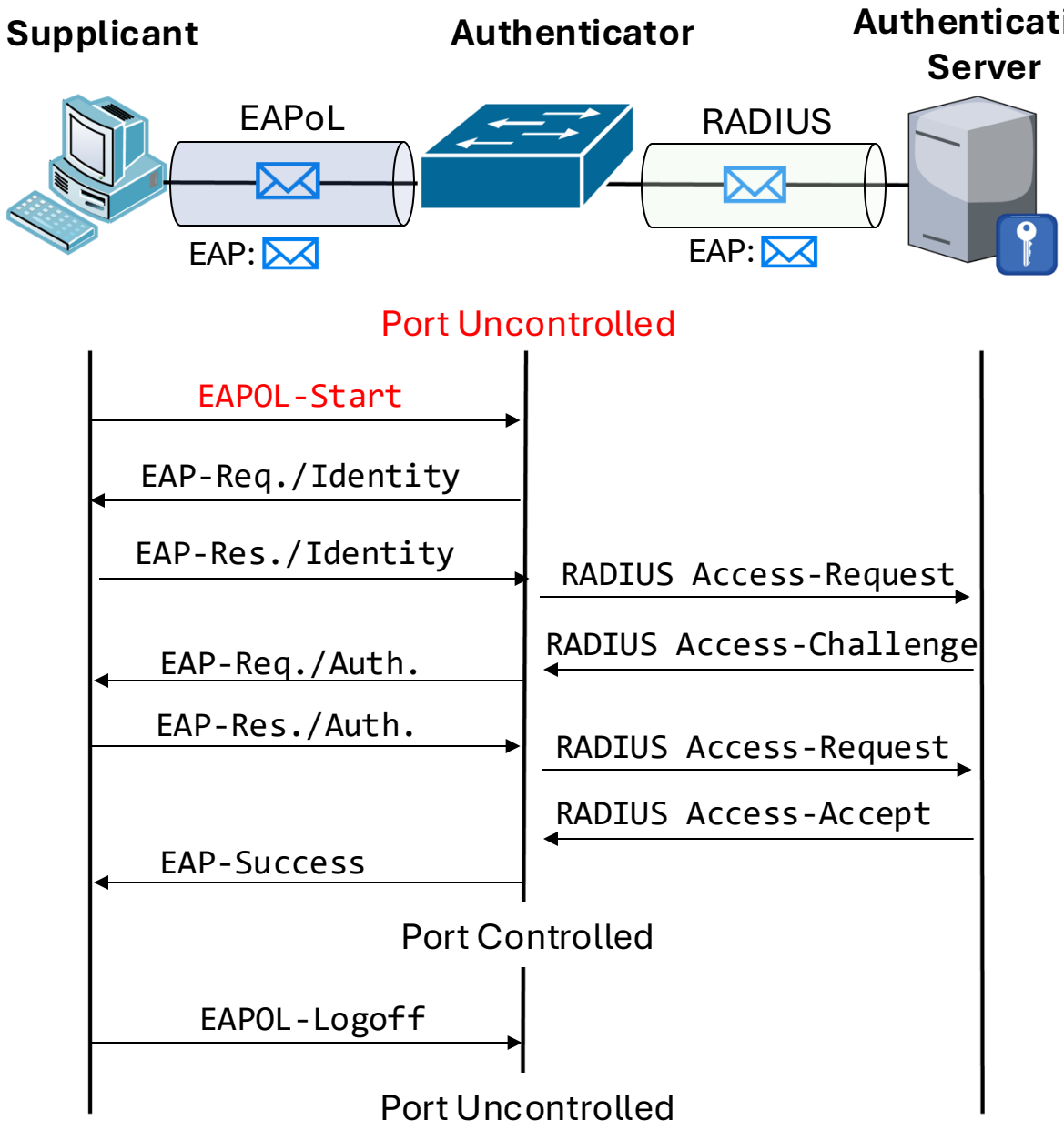
Einschub: TLS-Handshake mit allen Optionen



- **EAP-Request / EAP-TLS Start** (vom Authenticator → Supplicant)
  - Der Authenticator signalisiert, dass die Authentifizierung mit EAP-TLS beginnt.
- **EAP-Response / EAP-TLS ClientHello** (vom Supplicant → Authenticator → AAA-Server)
  - Der Supplicant startet die TLS-Handshake-Prozedur, indem er ein ClientHello sendet, das die unterstützten TLS-Versionen und Cipher-Suites enthält.
- **EAP-Request / EAP-TLS ServerHello + Zertifikat + ServerKeyExchange + CertificateRequest** (vom AAA-Server → Supplicant)
  - Der Authentifizierungsserver (z. B. ein RADIUS-Server) antwortet mit:
  - ServerHello (enthält die gewählte Cipher-Suite)
  - Server-Zertifikat (zur Authentifizierung des Servers)
  - (optional) ServerKeyExchange für Diffie-Hellman-Parameter
  - CertificateRequest (fordert das Client-Zertifikat an)
- **EAP-Response / EAP-TLS Client Zertifikat + ClientKeyExchange + CertificateVerify + ChangeCipherSpec + Finished** (vom Supplicant → Authenticator → AAA-Server)
  - Der Supplicant sendet:
  - Sein Client-Zertifikat zur Authentifizierung
  - ClientKeyExchange (enthält die für die Schlüsselerzeugung notwendigen Daten)
  - CertificateVerify, um zu beweisen, dass er den privaten Schlüssel des Zertifikats besitzt
  - ChangeCipherSpec, um die Verschlüsselung zu aktivieren
  - Finished, um den verschlüsselten Teil der TLS-Sitzung abzuschließen
- **EAP-Request / EAP-TLS ChangeCipherSpec + Finished** (vom AAA-Server → Supplicant)
  - Der Server sendet ebenfalls ChangeCipherSpec und Finished, um die verschlüsselte Sitzung zu bestätigen.

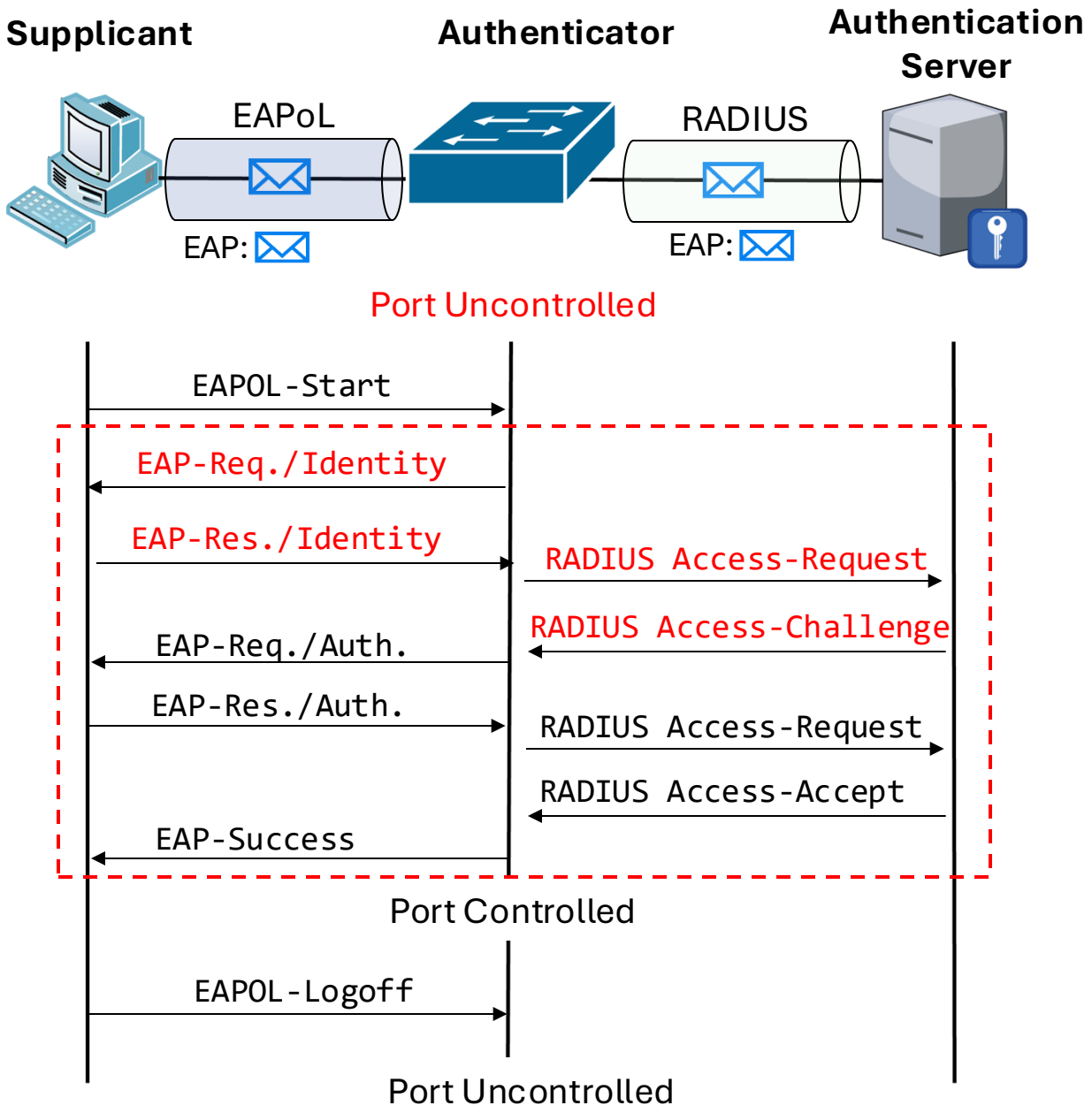
Nachrichtenfluss in IEEE802.1X

- Verbindet sich ein Endgerät initial mit einem 802.1X-fähigen Ethernet-Port eines Switches oder mit einem 802.1X-fähigen Wi-Fi-Netzwerk via WLAN Access Point, sendet der Client eine EAPoL-Start-Nachricht an die Multicast-Adresse `01:80:C2:00:00:03`.
- Der verbundene Switch oder der angefragte WLAN-AP lauschen auf Anfrage an diese Multicast-Adresse, und erkennen so dass eine EAPol-Start-Nachricht eingeht.
- Der Supplicant kann nur mit dem Authenticator Daten austauschen, da sich der Port im Zustand "uncontrolled" befindet.



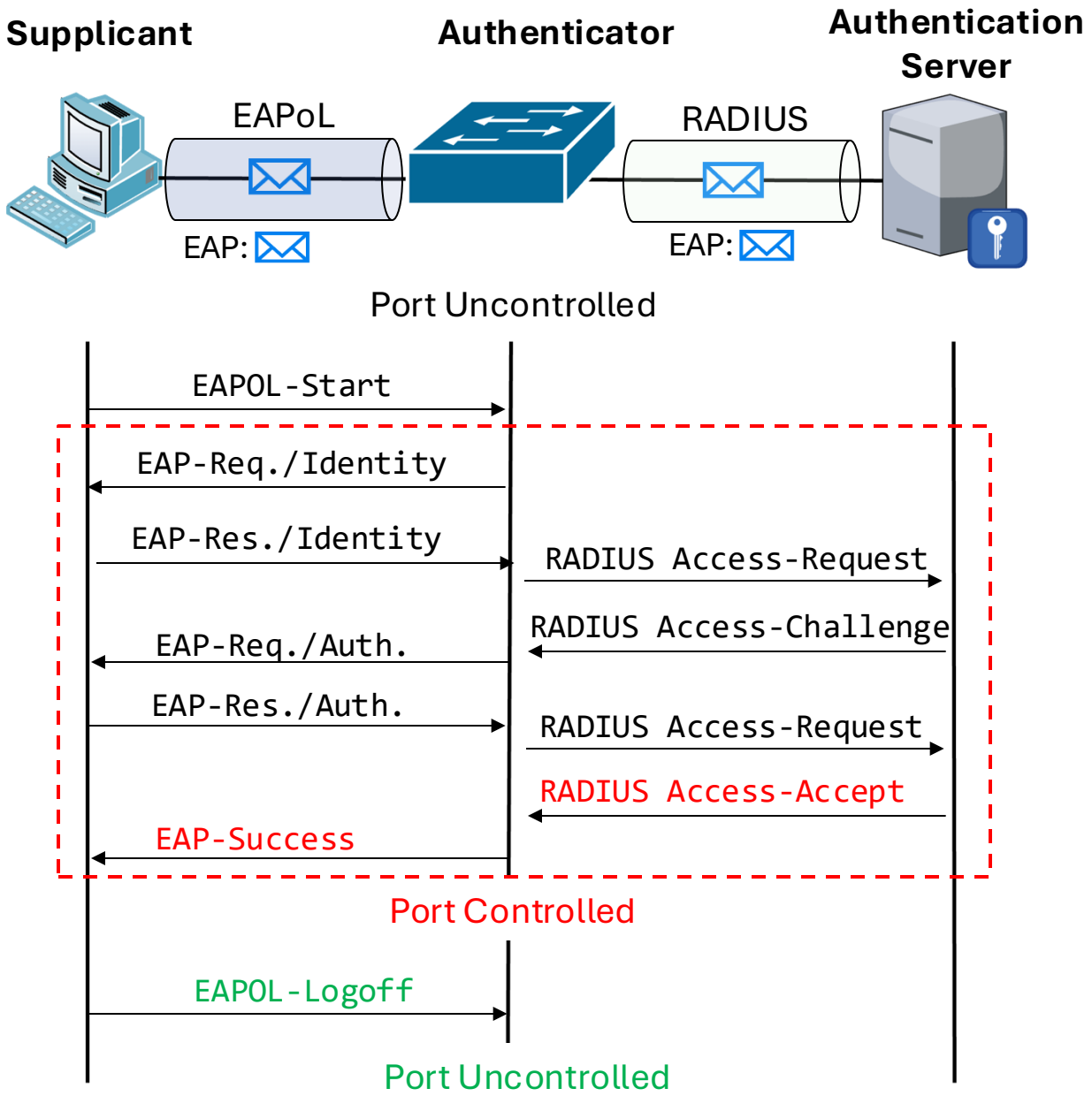
Nachrichtenfluss in IEEE802.1X

- EAPOL-Packet/EAP-Request-Identity: Der Authenticator fordert den Supplicant auf sich zu identifizieren.
- EAPOL-Packet/EAP-Request-Identity: Der Supplicant übermittelt dem Authenticator seine Identität (Username) und ggf. auch einen Nachweis (Password).
- RADIUS Access-Request: Der Authentificator leitet die Authentifizierungsdaten mit Hilfe des RADIUS-Protokolls an einen Authentifizierungsserver weiter.
- RADIUS Access-Challenge: Der Authentication Server überprüft die erhaltenen Authentifizierungsdaten und fordert optional zusätzliche Informationen an (z.B.: One-Time-Passwort).

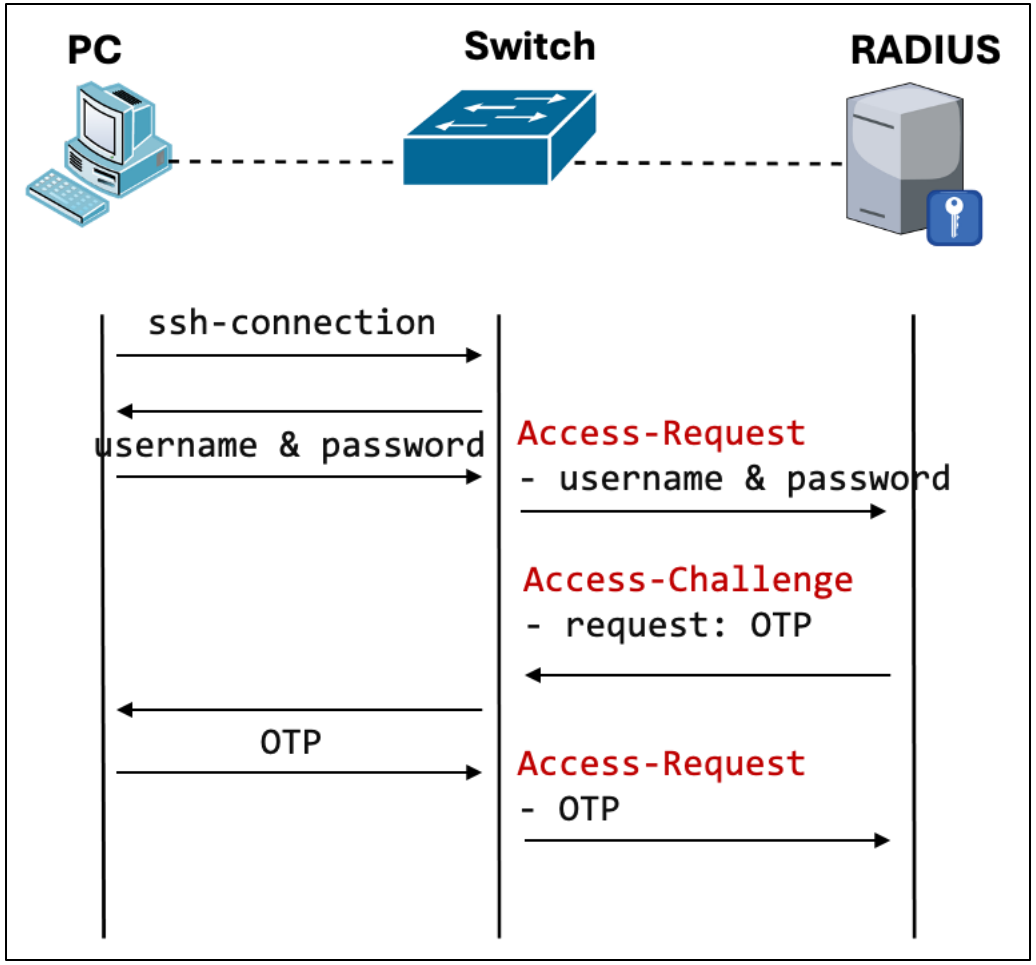


Nachrichtenfluss in IEEE802.1X

- Im Falle einer erfolgreichen Authentifizierung sendet der Authentification Server eine RADIUS Access-Accept an den Authenticator.
  - Der Authenticator setzt den Port in den Zustand Controlled und informiert den Supplicant mit einer EAPoL/EAP-Success-Nachricht.
- Im Falle einer fehlerhaften Authentifizierung sendet der Authentication Server eine RADIUS Access-Reject Nachricht an den Authenticator.
  - Der Portzustand bleibt im Status Uncontrolled.
  - Der Authenticatior informiert den Supplicant mit einer EAPoL/EAP-Failure – Nachricht.
- Zum Beenden einer Verbindung sendet der Supplicant eine EAPoL-Logoff-Nachricht, der Port geht in den Zustand uncontrolled.



3.3 RADIUS


PC
Switch
RADIUS
ssh-connection
username & password
Access-Request
- username & password
Access-Challenge
- request: OTP
OTP
Access-Request
- OTP

RADIUS

- RADIUS steht für Remote Authentication Dial-In User Service.
- Es handelt sich um ein weit verbreitetes Netzwerkprotokoll zur Bereitstellung zentralisierter Authentifizierungs-, Autorisierungs- und Accounting-Services.
- Bezeichnung: AAA-Services
- RADIUS verwendet
  - UDP/1812 für Authentifizierungs-, Autorisierungs-Services
  - UDP/1813 für Accounting-Services
- Die folgenden Vorteile bietet eine Radius-SW-Lösung:
- Zentralisierte sichere flexible Authentifizierung:
  - Anmeldeinformationen werden an einem sicheren Ort zentral gespeichert und zentral gepflegt.
  - Ein RADIUS-Server kann die Authentifizierung für viele Zugriffspunkte, Switches oder VPN-Gateways übernehmen.
  - Unterstützt starke Authentifizierungs- und Verschlüsselungsmethoden wie beispielsweise EAP-TLS, bei denen Zertifikate statt Passwörter verwendet werden.
- Zentrale Autorisierung:
  - Steuert den granularen Zugriff auf IT-Assets durch zentral pflegbare Zugriffsrichtlinien.
- Accounting und Auditing:
  - Aufzeichnen von Benutzeraktivitäten zu Fehlerbehebungszwecken.
  - Sicherstellung von Compliancevorgaben wie z.B.: unbefugtes Ändern eines Systems.
  - Aufzeichnen von Kundenaktivitäten zu Abrechnungszwecken.

RADIUS - Anwendungsszenarien

- Anwendungsszenarien für RADIUS sind beispielsweise:
- VPN-Authentifizierung:
  - Ein Benutzer stellt eine Verbindung zu einem Unternehmens-Netzwerk her. Das VPN-Gateway (Authentificator) verwendet RADIUS, um die Anmeldeinformationen des Benutzers zu überprüfen und Richtlinien durchzusetzen.
- Kabelgebundenes 802.1X-Netzwerk:
  - Ein Benutzer steckt ein Gerät in einen Ethernet-Port eines Switches. Der Switch (Authentificator) verwendet RADIUS, um das Gerät zu authentifizieren.
- WLAN-Zugang:
  - Ein Benutzer authentifiziert sich mittels seines Benutzernamens und Passwort an einem WLAN-AP. Der AP verwendet RADIUS, um den Benutzer zu authentifizieren und ihm anschließend ein WLAN-Netzwerk zuzuweisen.
- Zentralisierte Authentifizierung, Autorisierung und Accounting (AAA) für Netzwerkgeräte:
  - Bei einer Ammeldung eines Administrators an einem Switch, Router oder Firewall leitet das Netzwerkgeräte die Anmeldung an einen zentralen RADIUS-Server weiter.
  - Der RADIUS-Server kann sich zusätzlich eines Verzeichnisdienstes bedienen, um die Authentifzierung eines Benutzers via dem Protokoll LDAP (Lightweight Directory Access Protocol) durchzuführen.
- Begriffe:
  - Der Authenticator wird im RADIUS-Kontext auch als Network Attached Server (NAS) bezeichnet.
  - Der Supplicant wird im RADIUS-Kontext als Network Access Device (NAD) bezeichnet.

RADIUS - Authentifizierungsmethoden

- Password Authentication Protocol (PAP):
  - Authenticator sendet Benutzernamen im Klartext und "verschleiertes" Passwort an den RADIUS-Server.
  - Zur Verschleierung wird ein `sharedSecretKey`, sowie ein Authenticator verwendet. Der Authenticator stellt eine Zufallszahl dar, die jedes Mal neu generiert wird.

```
MD5-Hash = MD5(sharedSecretKey | Authenticator)
Verschleiertes Passwort = Passwort XOR MD5-Hash
```

  - Verfahren gilt als unsicher, sofern die Übertragung nicht über einen sicheren Kanal (z. B. TLS oder IPsec) oder innerhalb eines abgeschotteten Netzwerkes (Management-Netzwerkes) erfolgt.

- Damit ein Passwort nicht lesbar ist, wird es immer "verschleiert". Die Verschleierung funktioniert wie folgt:
  - 1. Der Authenticator und RADIUS-Server teilen sich ein gemeinsames Geheimnis ("shared secret").
  - 2. Ein 16-Byte-Request-Authenticator wird zufällig vom Authenticator generiert und in der Accept-Request-Nachricht an den RADIUS-Server übermittelt.
  - 3. Der Authenticator berechnet einen MD5-Hash aus dem gemeinsamen Geheimnis und dem Request-Authenticator .
  - 4. Wenn das Passwort kürzer als 16 Byte ist, wird es mit Nullbytes (0x00) aufgefüllt. Wenn das Passwort länger ist, wird es in mehrere 16-Byte-Blöcke aufgeteilt.
  - 5. Das Password wird dem MD5-Hash mittels XOR verknüpft.

RADIUS - Authentifizierungsmethoden

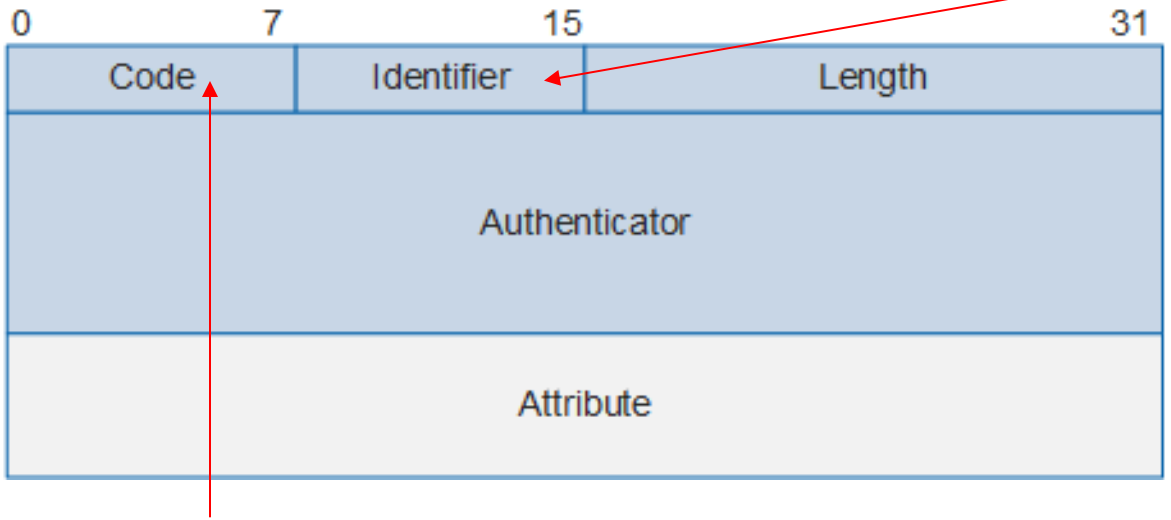
- Challenge Handshake Authentication Protocol (CHAP).
  - Nach der initialen Verbindungsaufnahme sendet der RADIUS-Server eine Challenge C (16B Random Number) an den Supplicant.
  - Der Supplicant berechnet für die Kombinaten aus Passwort und Challenge einen Hash-Wert (z.B.: MD5, HMAC-MD5, …) und schickt diese mit Hilfe des Authenticator an den RADIUS-Server weiter.
  - CHAP gilt jedoch nach modernen Standards immer noch als schwach und sollte ebenfalls nur in einem separaten Management-Netzwerk oder über einen über verschlüsselten Kanal verwendet werden.

```
HASH = H(Password | C)

HASH : Response vom Supplicant

C : Challenge (16B Zufallszahl) vom Server

H() : Hash-Funktion {MD5, HMAC-MD5, HMAC-SHA, …}
```

- Extensible Authentication Protocol (EAP)
  - EAP ist eine flexiblere und sicherere Methode, die häufig in modernen RADIUS-Implementierungen verwendet wird.
  - EAP unterstützt mehrere Methoden, darunter EAP-TLS, das den Datenverkehr verschlüsselt und zertifikatsbasiert authentifiziert.

RADIUS-Nachrichtenaufbau

- Das RADIUS-Paket besitzt den folgenden Aufbau:



- Code (1B): Das Codefeld identifiziert den Typ einer RADIUS-Nachricht. Beispiel für RADIUS-Nachrichten sind in der folgenden Tabelle gelistet.
  - Die ersten vier RADIUS-Pakete werden für die Authentifizierung verwendet.
  - Die Autorisierungsinformation wird mittels des Access-Accept Paketes an den Authenticator übermittelt.
  - Das Accounting verwendet die letzten beiden Pakete.

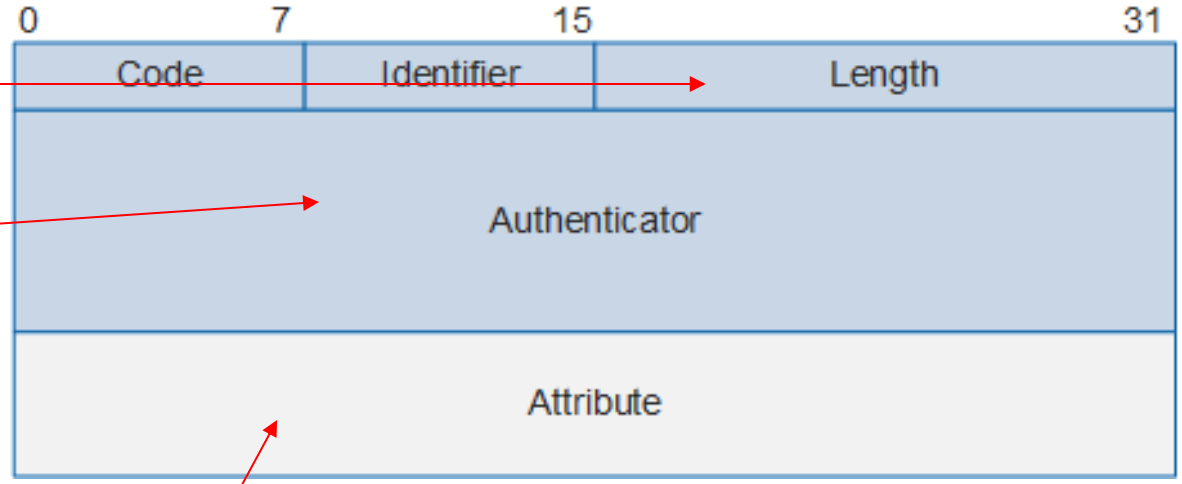
- Identifier (1B):
  - Das Identifier-Feld hilft dem RADIUS-Server, ein Paar aus RADIUS-Anforderungen (Access-Request) und RADIUS-Antworten (Access-Response) zu identifizieren, da Sie beide den gleichen Identifier erhalten.
  - Doppelte Anforderungen werden am selben Identifier-Authenticator Paar und derselben Kombination aus Source-IP/Source-Port bestimmt.

Code	Nachrichtentyp	Funktion
1	**Access-Request**	Authentifizierungsanfrage
2	**Access-Accept**	Authentifizierung erfolgreich. Übermittlung von Autorisierungsinformation
3	**Access-Reject**	Authentifizierung fehlgeschlagen
11	**Access-Challenge**	Zusätzliche Authentifizierung erforderlich
4	**Accounting-Request**	Sitzungsüberwachung starten/beenden
5	**Accounting-Response**	Bestätigung des Accounting-Datensatzes

RADIUS-Paketaufbau

- Length (2B):
  - Das Längenfeld gibt die Gesamtlänge eines RADIUS-Pakets an (Header & Attribute)
- Authenticator (16B): Das Feld besitzt unterschiedliche Inhalte.
  - Bei Access-Request-Nachrichten wird dieses Feld vom Anfragenden mit einem zufälligen 16-Byte-Wert gefüllt, der als Request Authenticator dient. Dieser Zufallswert wird auch bei der Berechnung des verschleierten Passwortes (siehe vorne).
  - Bei Access-Accept/-Challenge/-Reject-Nachrichten enthält dieses Feld den mit dem Request-Authenticator bestimmten Message Authentication Code (MAC) zur Echtheitsprüfung (Integritätsprüfung) der Antwortnachricht.

MAC = MD5(Code | Identifier | Length | Request Authenticator | Attribut-Liste | shared secret)



- Attribute
  - Das Feld „Attribute“ stellt den Payload der RADIUS-Nachricht dar
  - Es enthält eine Liste von null oder mehr Attributen.

RADIUS Attribute

- Attribute:
  - Die Länge eines Attributes ist variabel, aber maximal 255B.
  - RADIUS-Attribute enthalten die spezifischen Authentifizierungs-, Autorisierungs-, und Accounting-Daten für die RADIUS-Nachrichten.
  - Attribute werden im flexiblen Type-Length-Value-Format übertragen.
  - Type (1B): Definiert das übertragene RADIUS-Attribut, anhand einer Liste von vordefinierten Nummern im Wertebereich [1,255].
  - Length (1B): Das Feld Length gibt die Länge des RADIUS-Attributs-Values in Bytes an:

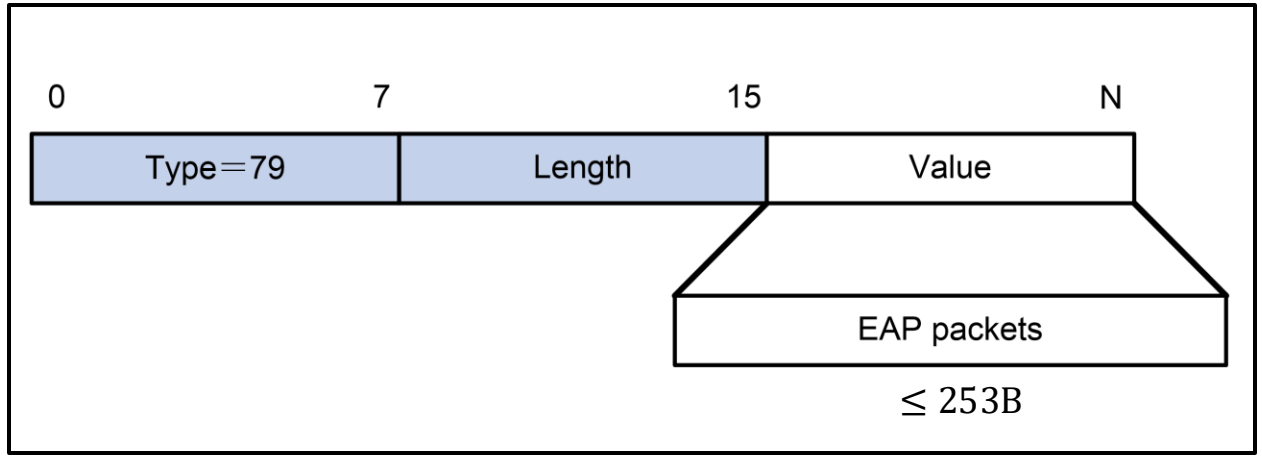
    Maximalwert Value: $2^8 = 255\text{B} - 2\text{B} = 253\text{B}$
  - Value (<253B): Das Feld Value enthält die spezifische Information zum jeweiligen RADIUS-Attribut.

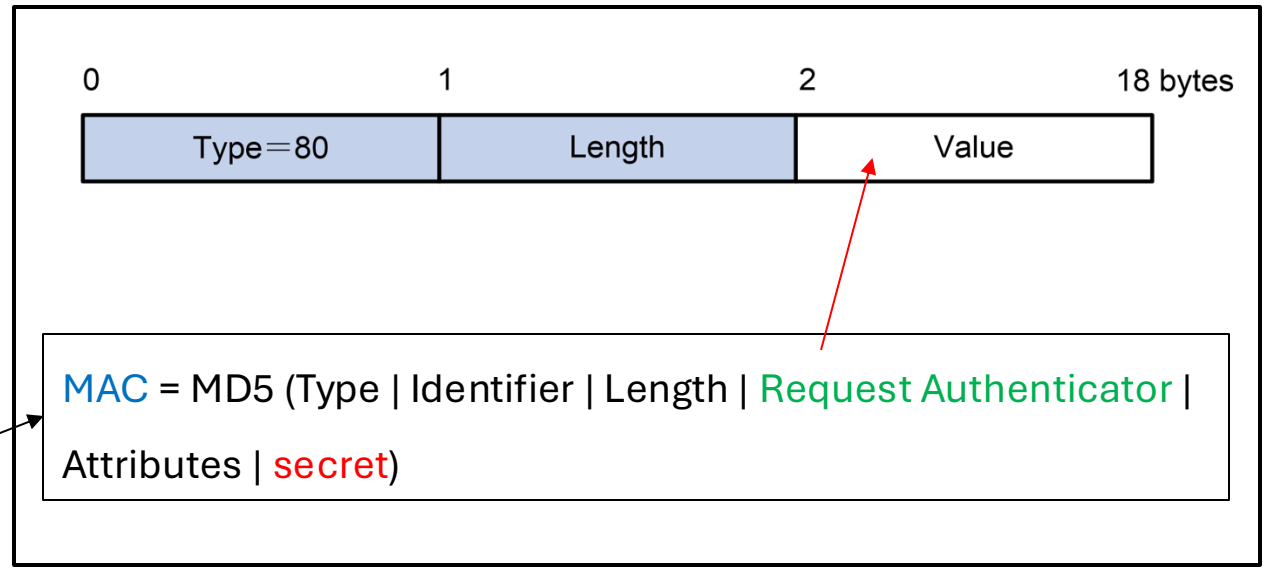
Beispiele für **RADIUS-Attribute**

Type (1B)	Name	Zweck	Beispiel
1	User-Name	Identität des Benutzers	admin klaus.meyer@example.de
2	User-Password	Verschleiertes Passwort des Benutzers.	9jduj39j399ksu1
3	Chap-Password	Chap Hash Response of Password	q3chuj39fjhsbs83spksu1
4	NAS-IP-Address	IP-Address of the NAS	10.10.5.20
5	NAS-Port	Physikalische oder logische Portnummer auf dem NAS	101 (WLAN logischer Port) 3 (vty line on device for a remote ssh connection) 0 (physikalischer Konsole-Port) 471 (VPN session id)
61	NAS-Port-Type	Art der Verbindung	19 (WLAN-Verbindung) 5 (remote virtual port: z.B.: ssh, ...) 29 (wired connection) 31 (vpn connection)
64	Tunnel-Type	Typ des Tunnels	13 (VLAN)
65	Tunnel-Media Type	Transport Medium	1 (IP4), 2 (IPv6) 6 (802.1x)

RADIUS Attribute & EAP

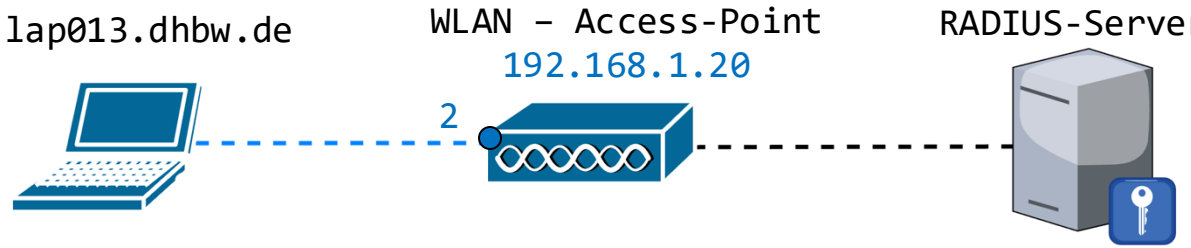
- RADIUS kapselt EAP-Pakete im sogenannten EAP-Message-Attribut.
- Das RADIUS EAP-Message-Attribut besitzt den Typ=79.
- Ein EAP-Paket wird vom Authenticator in das EAP-Message-Attribut geschrieben. Ist es länger als 253 Byte ist, werden mehrere EAP-Message-Attribute verwendet.
- Um die per RADIUS übermittelten EAP-Pakte-Inhalte vor unerlaubter Änderung in beiden Kommunikationsrichtungen zu schützen, wird ein weiteres RADIUS-Attribut, der Message-Authenticator (Type=80) verwendet.
  - Das Authenticator-Feld enthält dann immer eine Zufallszahl: Request-Authenticator (vom Supplicant erzeugt) oder einen Response-Authenticator (vom RADIUS Server erzeugt).
  - Das Message-Authenticator Attribut enthält den MAC der RADIUS-Nachricht (siehe vorne).

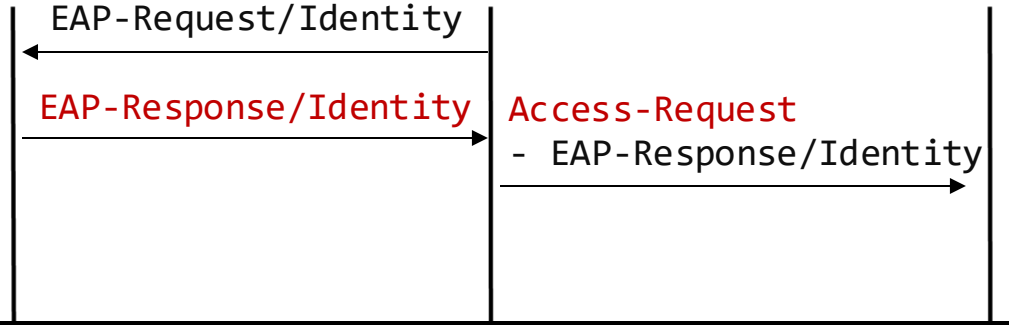




Beispiel: 802.1X-Authentifizierung über WLAN

- Szenario: Drahtloser Client (Laptop) möchte sich mit einer WLAN-Funkzelle verbinden, die eine 802.1X-Authentifizierung fordert (WPA2/3-Enterprise).
  - Als Authentifizierungsmethode ist die EAP-TLS-Methode konfiguriert. Im Falle eines Erfolges soll der Client dem VLAN 20 zugeordnet werden.
- Das initiale Access-Request-Packet vom WLAN-AP zum RADIUS-Server transportiert dessen EAP-Request-Identity Nachricht, die den Full-Qualified-Domain Name des Computers enthält:






```
EAP-Header:
 -Code: 2 (Response)
 -Identifier: 1
 -Length: <nn>
EAP Data:
 -Type: 1 (Identity)
 -Type-Data: "laptop013.dhbw.de"
```

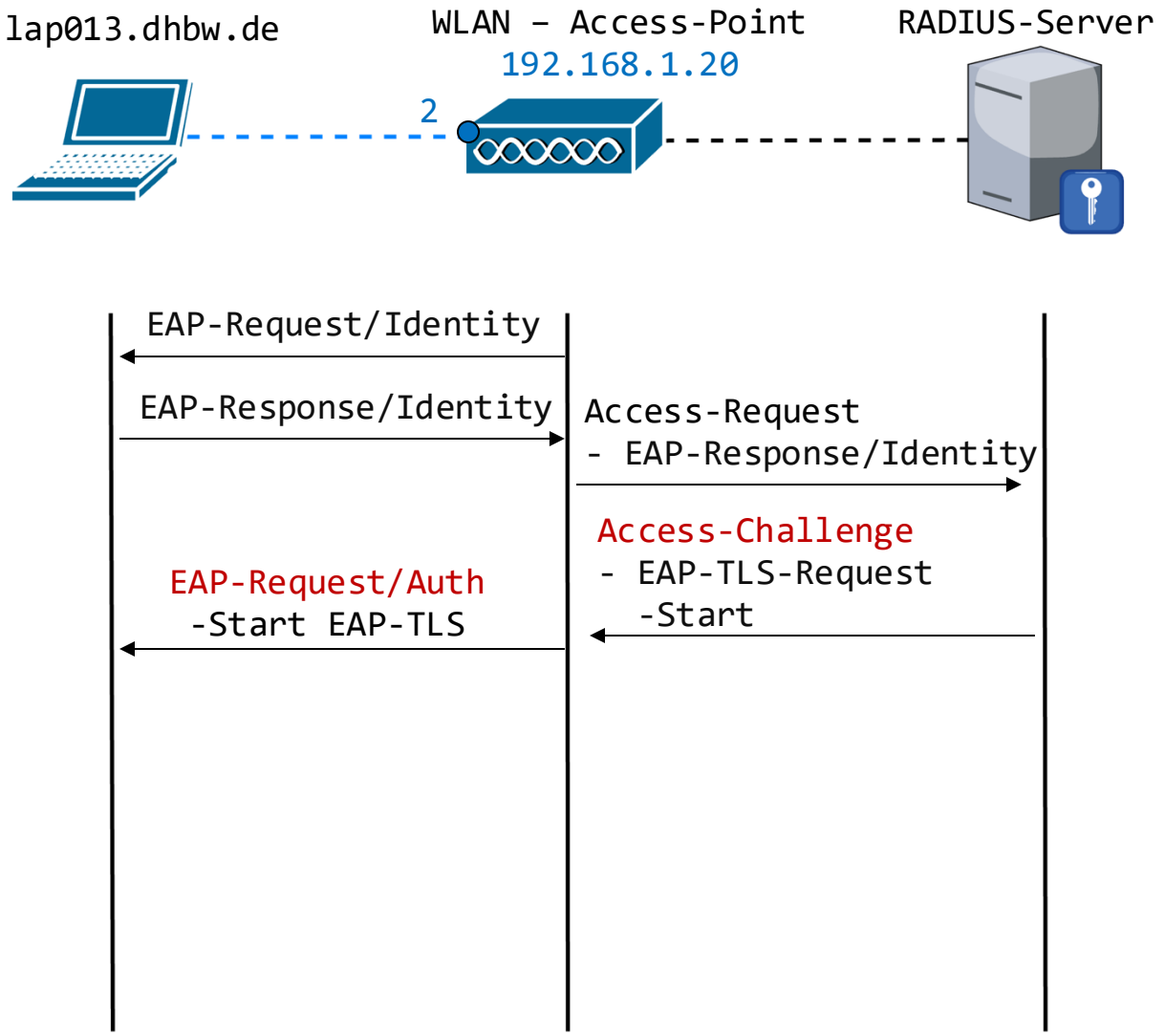
```
Code: 1 (Access-Request)
Identifier: 15
Length: <nn>
Authenticator: <Request Authenticator 16B value>
Attributes:
- Type:  1  (User-Name) laptop013.dhbw.de
- Type:  4  (NAS-IP-Address) 192.168.1.20
- Type:  5  (NAS-Port) 2
- Type: 61  (NAS-Port-Type) 19 (WLAN)
- Type: 79  (EAP-Message) EAP-Response/Identity
                                - "laptop013.dhbw.de"
- Type: 80  (Message-Authenticator) MAC
```

Beispiel: 802.1X-Authentifizierung über WLAN

- Der RADIUS-Server initiiert den EAP-TLS Handshake indem er mittels einer Access-Challenge-Nachricht, eine EAP-TLS-Request "Start Nachricht" an den Supplicant schickt, mit dem EAP-Type 13 für EAP-TLS.

```
Code : 11 (Access-Challenge)
Identifier : 15
Length:  <nn>
Authenticator: <Response Authenticator 16B value>
Attributes:
- Type: 79 (EAP-Paket) EAP-Header, Type: 13 (EAP-TLS)
- Type: 5  (NAS-Port) 2
- Type 80  (Message-Auth.) <MAC>
```

```
EAP-Header:
- Code: 0x01 (Request)
- Identifier: 1
-  Length: nn
EAP Data
-  Type: 13 (EAP-TLS)
-  Type Data: <empty>
```

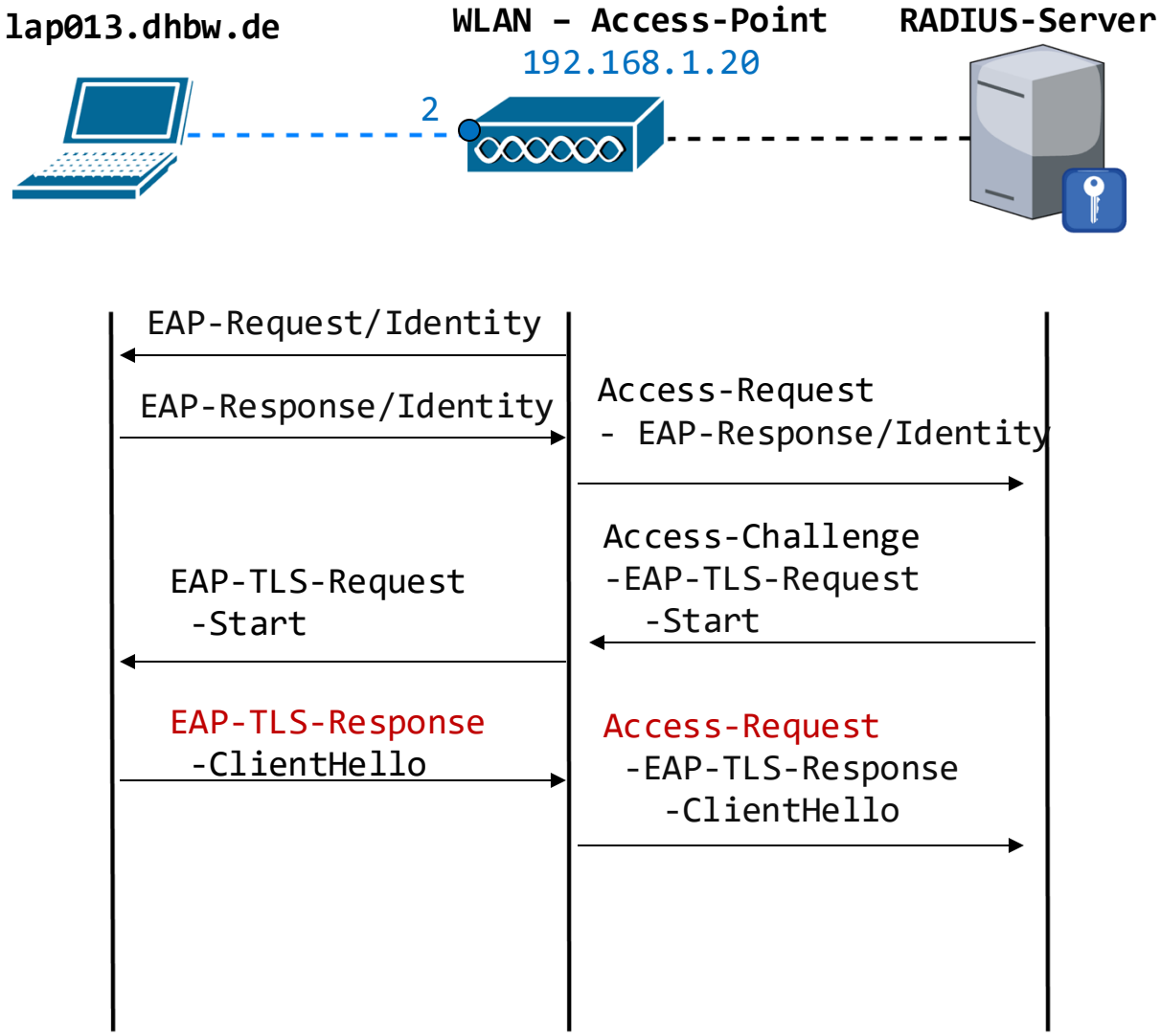


Beispiel: 802.1X-Authentifizierung über WLAN

- Supplicant antwortet dann mit der ersten TLS-Handshake-Nachricht, der Client-Hello-Nachricht (usw.).

```
EAP-Header:
- Code: 0x02 (Response)
- Identifier: 2
- Length: (Varies based on TLS data)
TLS Data:
- Type: 13 (EAP-TLS)
-  Type-Data: ClientHello-Nachricht
```

```
Code : 1 (Access-Request)
Identifier : 16
Length:  <nn>
Authenticator: <Request Authenticator 16B value>
Attributes:
 - Type: 79 (EAP-Message) ClientHello-Nachricht
 - Type:  4 (NAS-IP-Address) 192.168.1.20
 - Type:  5 (NAS-Port) 2
 - Type: 61 (NAS-Port-Type) 19 (WLAN)
 - Type: 80 (Message-Authenticator) <MAC>
```

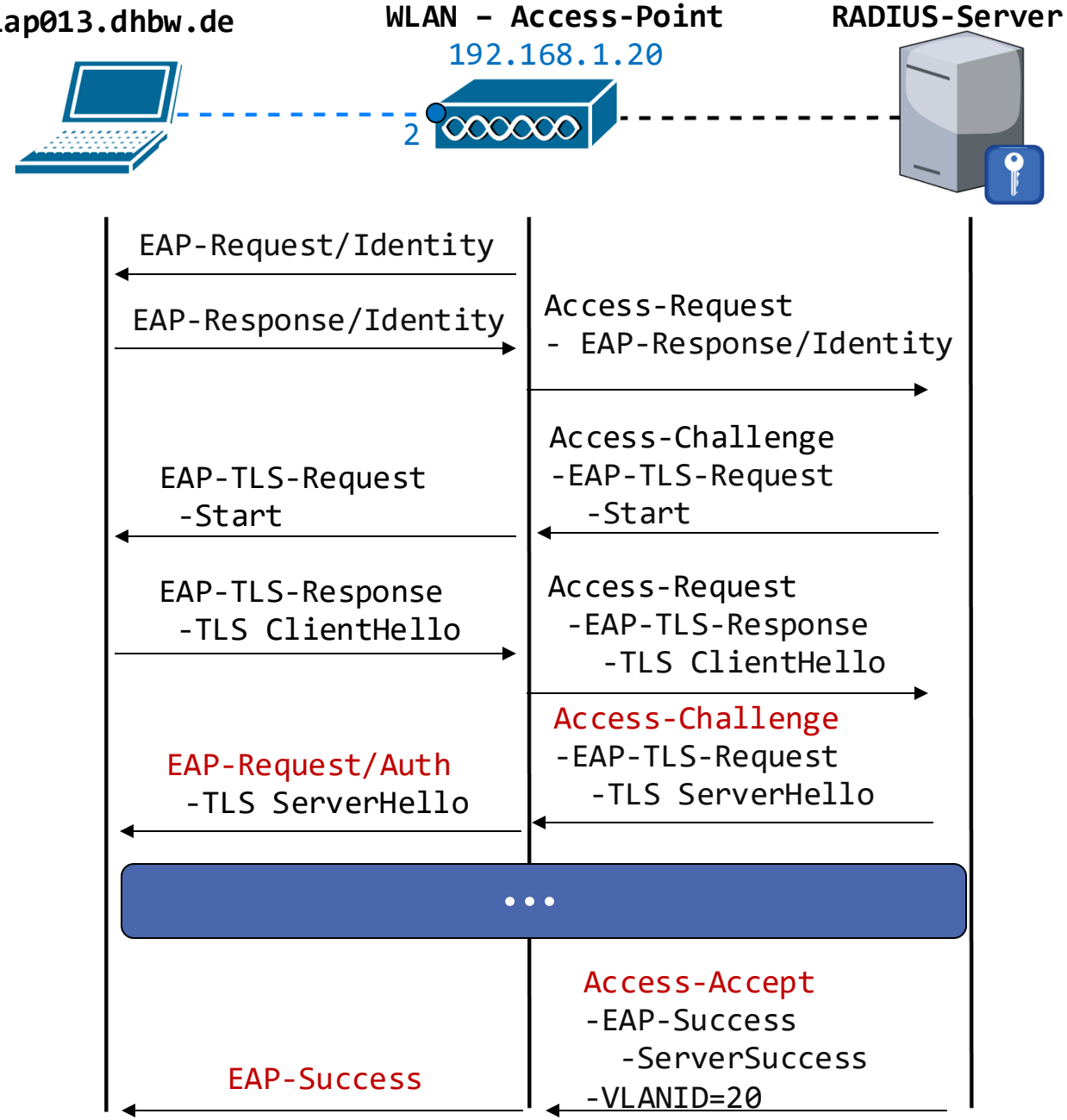


Beispiel: 802.1X-Authentifizierung über WLAN

- Der RADIUS-Server antwortet dann mit einer ServerHello-Nachricht mittels einer Access-Challenge – Nachricht, usw.
- Wird der TLS-Handshake erfolgreich abgeschlossen, schickt der RADIUS-Server ein Access-Accept-Paket mit einer EAP-Success-Nachricht und Autorisierungsattributen.

```
Code : 2 (Access-Accept)
Identifier : 17 (Match the last Access-Request identifier)
Length:  <nn>
Authenticator: <Response Authenticator 16B value>
Attributes:
 - Type: 79 (EAP-Message) EAP-Success
 - Type:  5 (NAS-Port) 2
 - Type: 64 (Tunnel-Type) 13  (VLAN)
 - Type:  65 (Tunnel-Medium-Type) 6 (IEEE-802.1X)
 - Type: 81 (Tunnel-Private-Group-ID) 20 (VLAN-ID)
 - Type: 80 (Message-Authenticator) <MAC>
```

```
EAP-Header:
- Code: 3 (EAP-Success)
- Identifier: 5 (Match the last EAP-TLS identifier)
- Length: 4 (Fixed Length)
```



Beispiel: 802.1X-Authentifizierung über WLAN

- Im Fall das der TLS-Handshake scheitert wird final vom RADIUS-Server ein Access-Reject-Paket verschickt mit den folgenden Attributen
  - Type 79 (EAP-Paket): EAP-Failure-Message (Code=4, Identifier=<ID>, Length=4, Type=13)
  - Type 18 (Reply Message): enthält einen anzeigbaren Text im UTF-8 Format.
  - RADIUS verwendet das Reply-Message-Attribut (Type=18) verwenden, um zusätzliche, menschenlesbare Nachrichten bereitzustellen.

```
Code : 3 (Access-Reject)
Identifier : 90 (Match the last Access-Request identifier)
Length:  <nn>
Authenticator: <Response Authenticator 16B value>
Attributes:
 - EAP-Message: Code=4, Identifier=12, Length=4, Type=13
 - Reply Message: "Authentification Failure"
 - Message-Authenticator: <MD5 Calculated value>
```

```
Code: 2 (EAP-Response)
Identifier: 7
Length: nn
Data:
  Type: 13 (EAP-TLS)
  Type-Data: "Authentification Failure"
```

```
Code: 4 (EAP-Failure)
Identifier: 90
Length: nn
```

Sicherheit von RADIUS

- Vertraulichkeit der Kommmunikation
  - Verschleierung des Benutzerkennworts: Das Attribut „User-Passwort“ wird mittels eines "Shared Secrets" und dem Feld „Request-Authentifikator“ verschleiert. Es handelt es sich hierbei nicht um eine Verschlüsselung im herkömmlichen kryptografischen Sinne.

Standard RADIUS-Sicherheit

1. Verschleiertes Benutzerkennwert mittels shared secret und Authenticator.
2. Integritätssicherung der Antwortnachrichten mittels Hash-Wert. HASH-Wert verwendet shared secret und Request-Authenticator

- Integrität der Kommunikation
  - Der Request-Authenticator in einer RADIUS Access-Request Nachricht ist ein 16B Zufallswert und wird zum RADIUS-Server übertragen.
  - Dieser Wert ist nicht statisch sondern wird für jedes RADIUS Request-Response-Paar (neuer Identifier) neu generiert.
  - Der Authenticator in der Access-Accept-/Challenge-/Reject-Nachricht ist ein 16-Byte-Hash-Wert der Antwortnachtricht, der zur Authentifizierung der Antwort und zur Sicherstellung ihrer Integrität verwendet wird.

Verbesserung der RADIUS-Sicherheit

- Zur Verbesserung der Sicherheit der RADIUS-Kommunikation können mehrere zusätzliche Methoden und Protokolle verwendet werden:
- RADIUS mit IPsec:
  - IPsec (Internet Protocol Security) kann verwendet werden, um die gesamte RADIUS-Kommunikation zwischen dem Authenticator und dem RADIUS-Server zu verschlüsseln. Dies gewährleistet die Vertraulichkeit und Integrität der Daten.
- RADIUS mit TLS (RadSec):
  - RadSec ist eine Erweiterung von RADIUS, die über TCP mittels TLS (Transport Layer Security) den RADIUS-Verkehr verschlüsselt. Es bietet eine vollständige End-to-End-Verschlüsselung der RADIUS-Nachrichten und schützt so vor Abhören und Manipulation.
- RADIUS mit EAP (Extensible Authentication Protocol):
  - EAP ermöglicht sicherere Authentifizierungsmethoden, die Anmeldeinformationen mithilfe starker Verschlüsselungsmethoden schützen können.
    Beispiel: Wi-Fi-Netzwerke
  - EAP-TLS beispielsweise verwendet TLS, um eine starke Verschlüsselung des Authentifizierungsprozesses bereitzustellen, und zu gewährleisten dass sowohl der Benutzername als auch das Benutzerkennwort verschlüsselt übertragen werden.

Aufgabe 3: IEEE802.1x mit EAP und RADIUS

1. **Grundlagen IEEE 802.1X**
   a. Erklären Sie das Sicherheitsziel von IEEE 802.1X in Netzwerken.
   b. Welche Komponenten sind in einer IEEE 802.1X-Authentifizierung involviert? Zeichnen Sie die zugehörige Topologie für ein LAN.
   c. Was versteht man unter **uncontrolled** und **controlled** Ports?
2. **Ablauf der Authentifizierung**
   a. Beschreiben Sie den Authentifizierungsprozess in IEEE 802.1X unter Verwendung der Begriffe **Supplicant**, **Authenticator** und **Authentication Server**.
   b. Welche Rolle spielt **EAPoL-**, **EAP-** und das **RADIUS-Protokoll** im 802.1X-Prozess?
3. **Authentifizierungsverfahren**
   a. Welche verschiedenen EAP-Methoden gibt es? Nennen Sie mindestens drei und erklären Sie kurz ihre Unterschiede.
   b. Welche Vorteile bietet das **EAP-TLS** Verfahren?
4. **Netzwerk-Sicherheit und Angriffe**
   a. Welche Sicherheitsrisiken gibt es bei der Nutzung von IEEE 802.1X?
   b. Kann ein Angreifer eine **Man-in-the-Middle-Attacke** in einem 802.1X-Netzwerk durchführen?
   c. Welche Maßnahmen können zum Schutz gegen solche Angriffe ergriffen werden?

Aufgabe 3: IEEE802.1x mit EAP und RADIUS

5. **Konfigurationsaufgabe (**Theoretisch oder Praktisch mit **CISCO Packet Tracer)**
   a. Skizzieren Sie eine typische IEEE 802.1X-Topologie mit Supplicant, Authenticator und Authentication Server.
   b. Welche Konfigurationsschritte sind notwendig, um IEEE 802.1X auf einem **Cisco-Switch** zu aktivieren?
   c. Wie kann man auf einem Windows-/LINUX-Client IEEE 802.1X konfigurieren?
6. **Fehlersuche & Troubleshooting**
   a. Ein Benutzer kann sich nicht am Netzwerk authentifizieren. Welche möglichen Ursachen könnten vorliegen?
   b. Welche Tools und Methoden können genutzt werden, um IEEE 802.1X-Probleme zu diagnostizieren?