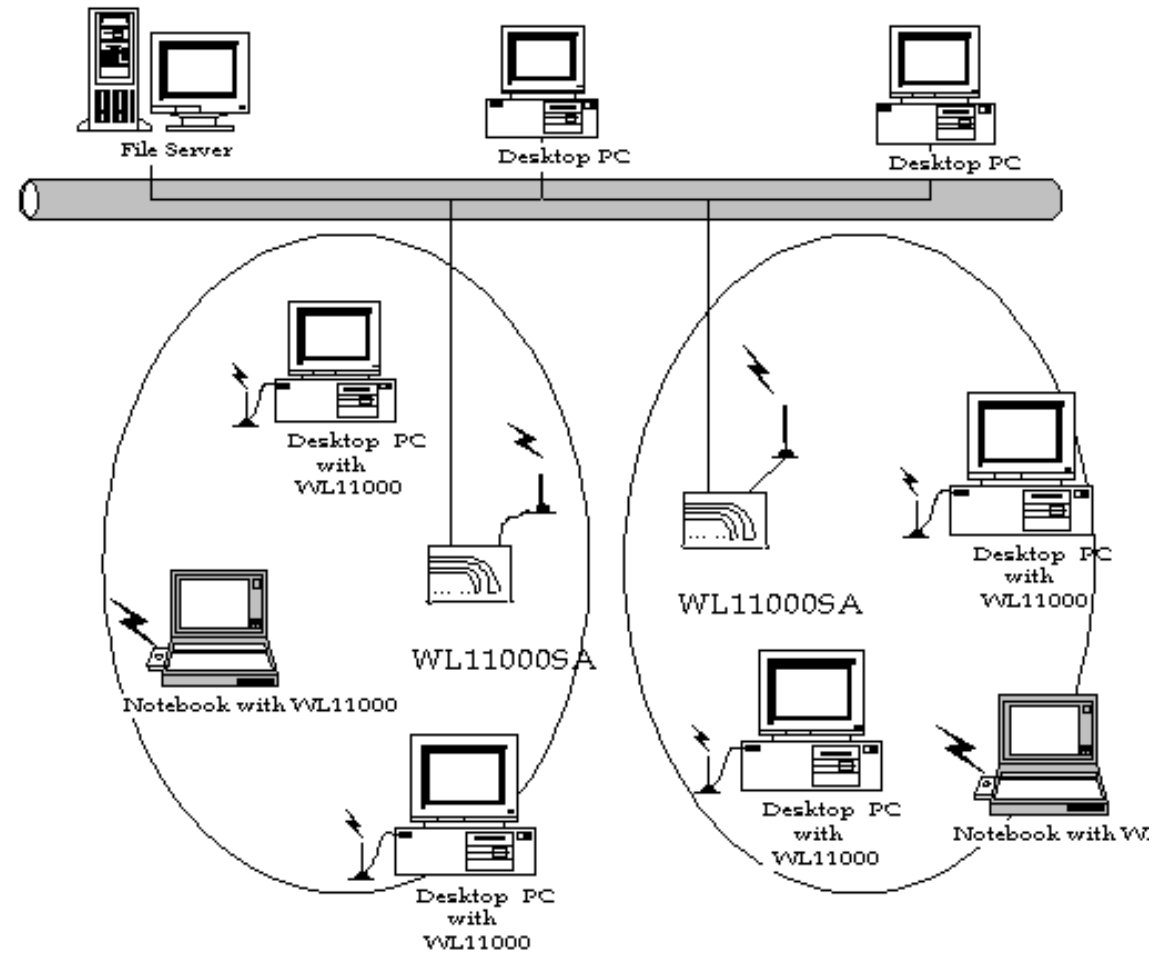


# Sicherheit in Wireless LANs

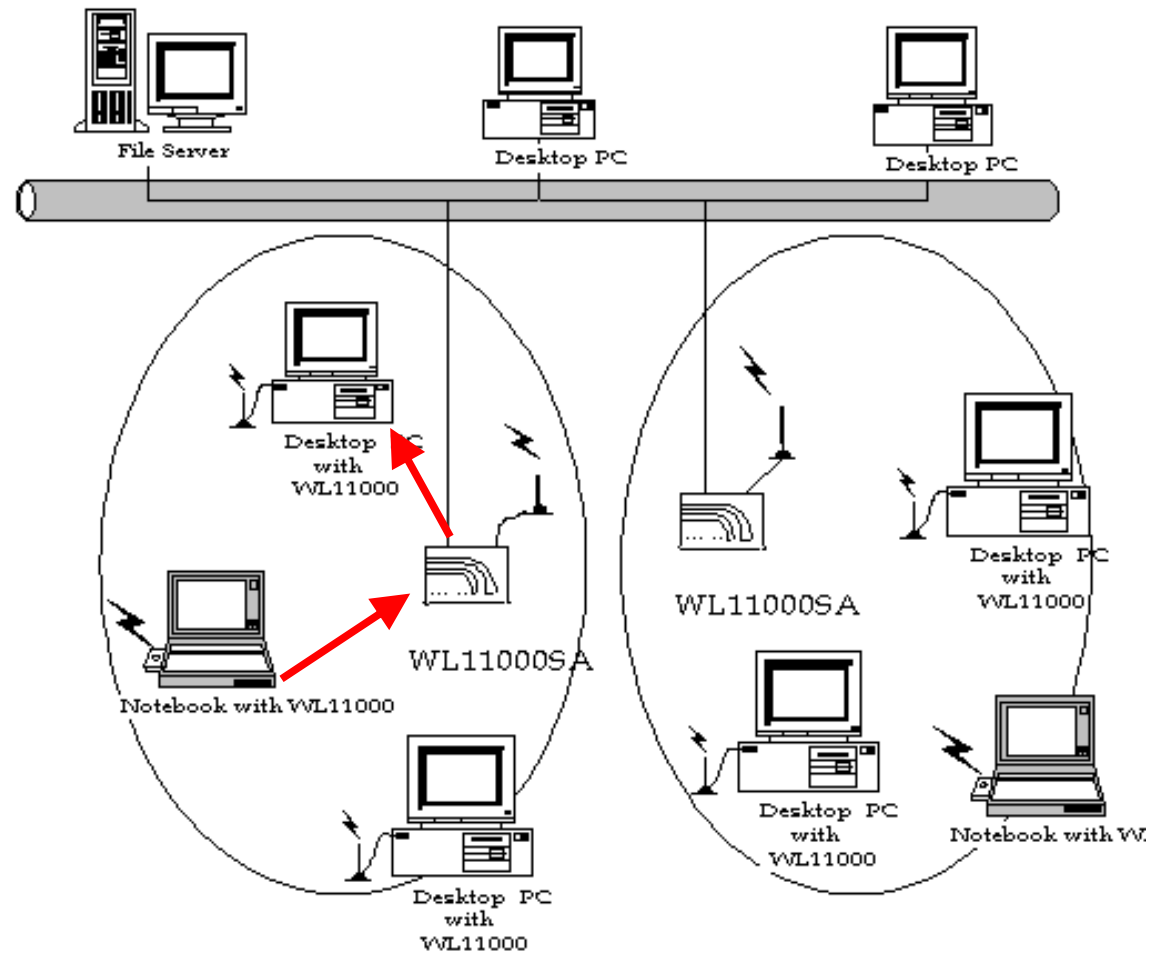
## ***VS-Seminar*** ***Wintersemester 2002/2003***

***Betreuer: Stefan Schmidt***

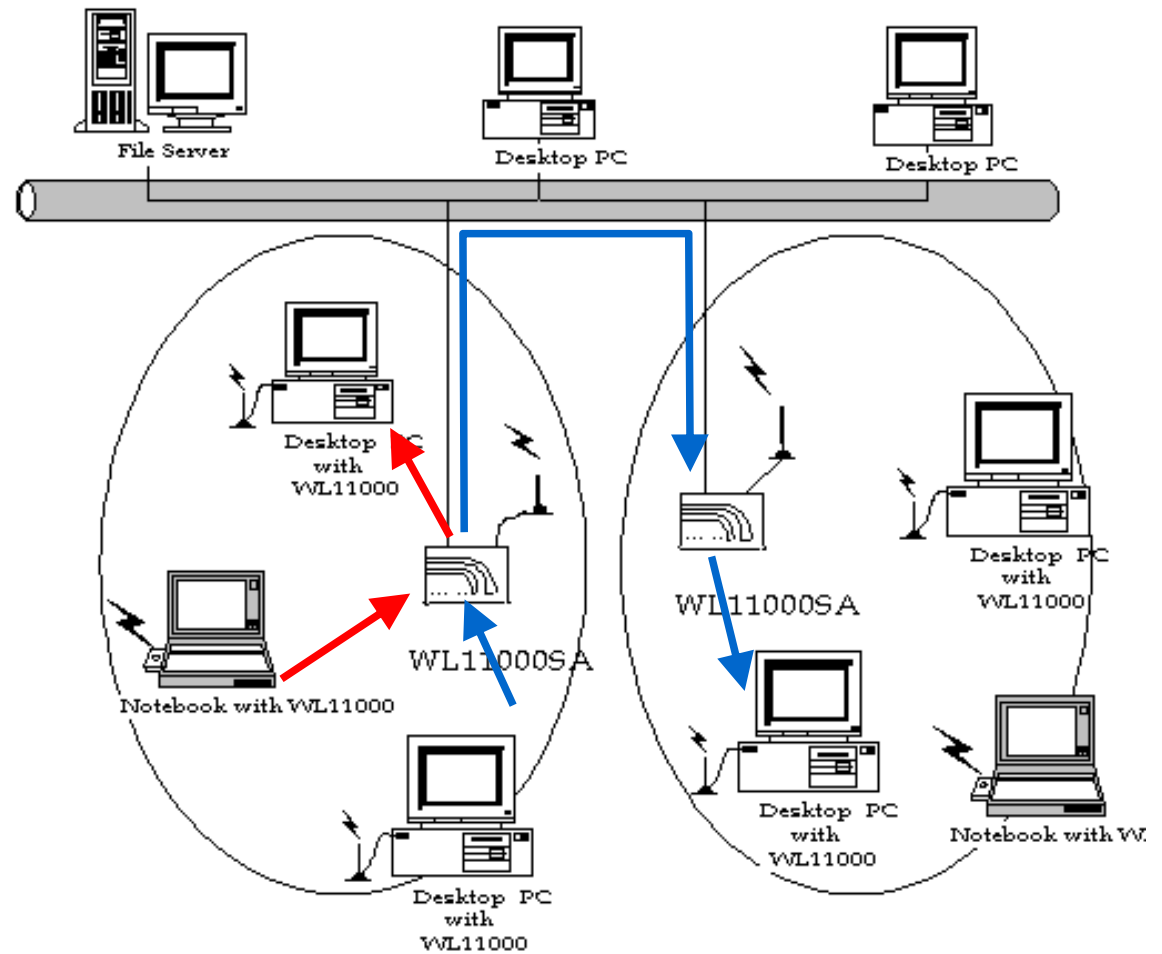
- Funktion und Aufbau von Infrastruktur Wireless LAN
- Sicherheit in Wireless LANs
- Sicherungsmechanismen in Wireless LANs
- Schwachstellen in den Sicherheitsmechanismen
- Verbesserung der Sicherheit
- Fazit



Kommunikation  
zweier Rechner in  
einem WLAN



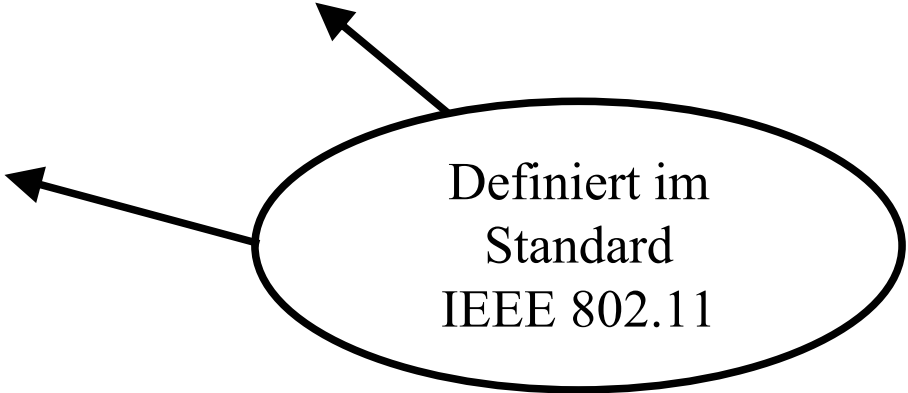
Kommunikation  
zweier Rechner in  
einem WLAN



- Integrität von Daten
- Authentizität von Daten und Benutzer
- Vertraulichkeit von Daten

- “geschlossenes WLAN“
- MAC-Adressen Zugriffskontrolllisten
- Wired Equivalent Privacy (WEP) Verschlüsselung
- Benutzerauthentifizierung

- “geschlossenes WLAN“
- MAC-Adressen Zugriffskontrolllisten
- Wired Equivalent Privacy (WEP) Verschlüsselung
- Benutzerauthentifizierung

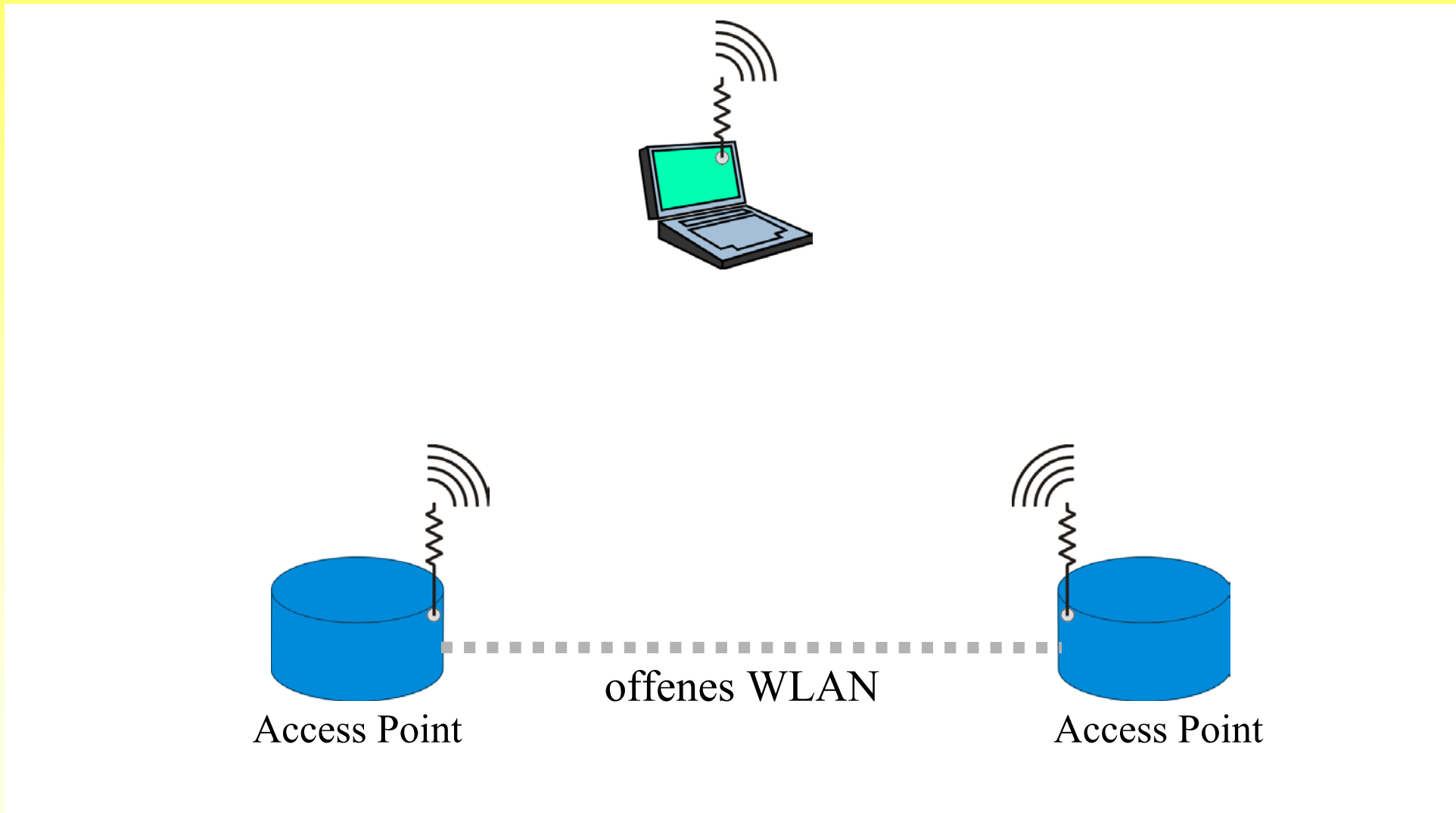


Definiert im  
Standard  
IEEE 802.11



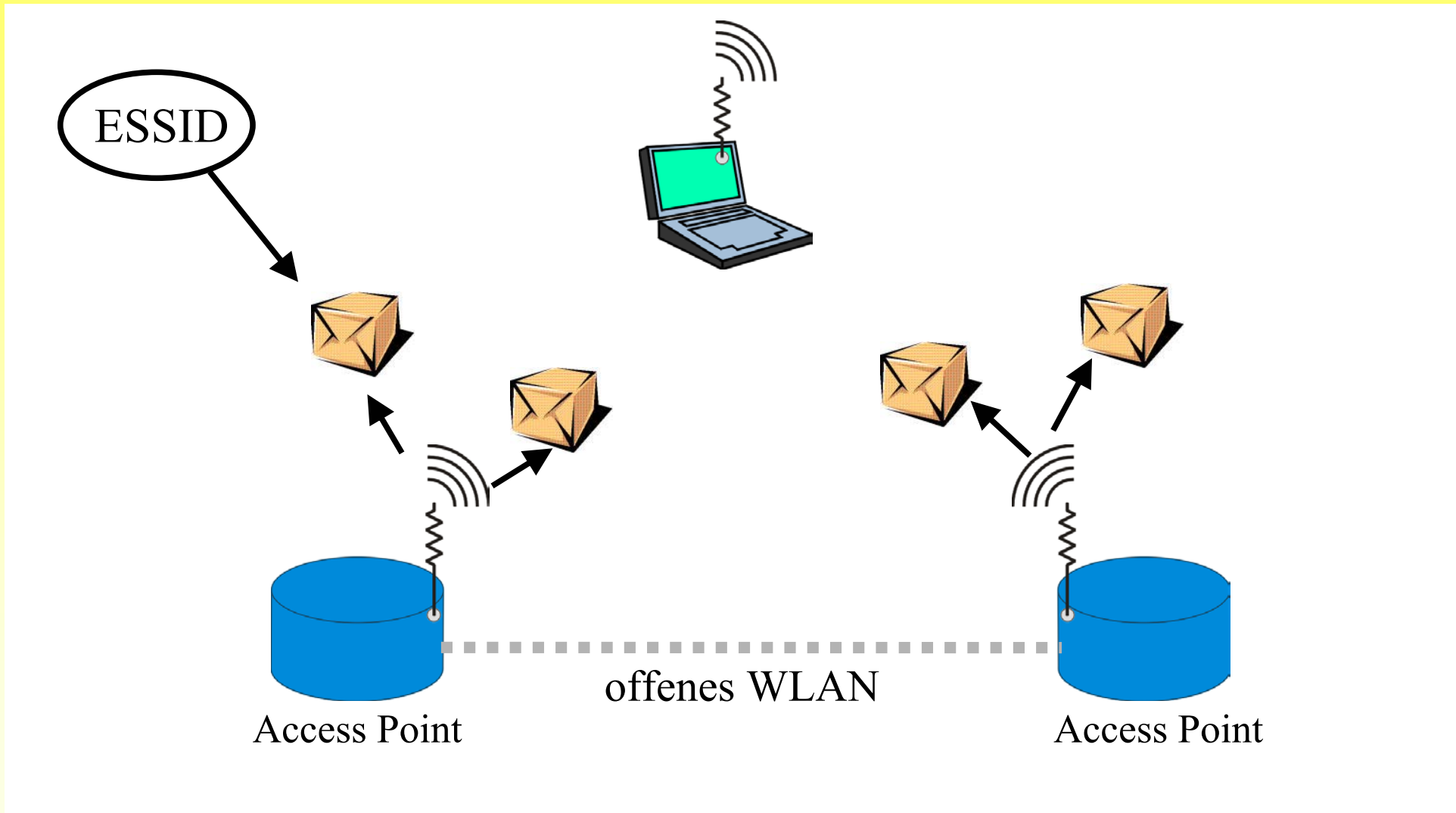
# Sicherungsmechanismen in Wireless LANs

## „geschlossenes WLAN“



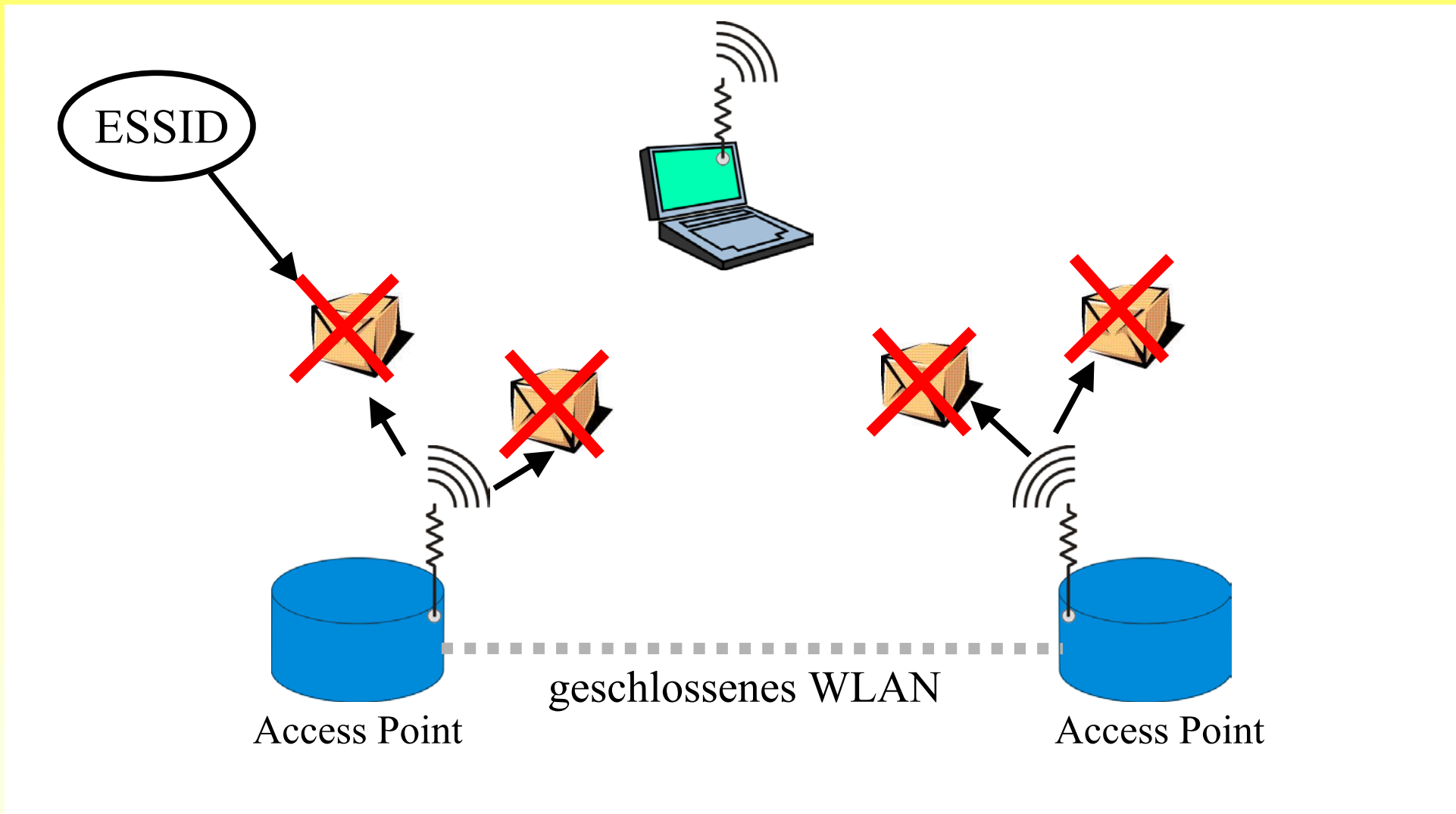
# Sicherungsmechanismen in Wireless LANs

## „geschlossenes WLAN“



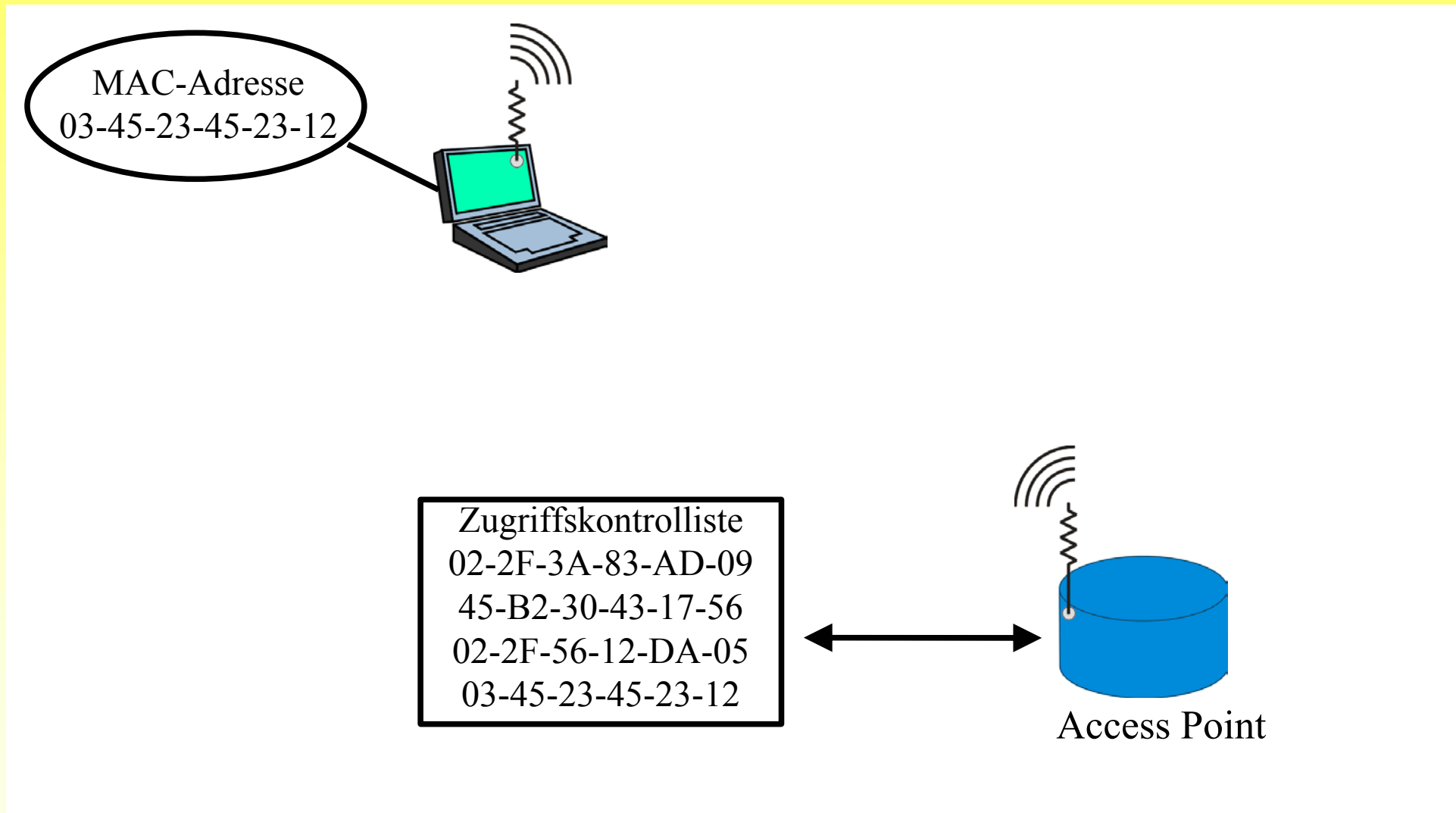
# Sicherungsmechanismen in Wireless LANs

## „geschlossenes WLAN“



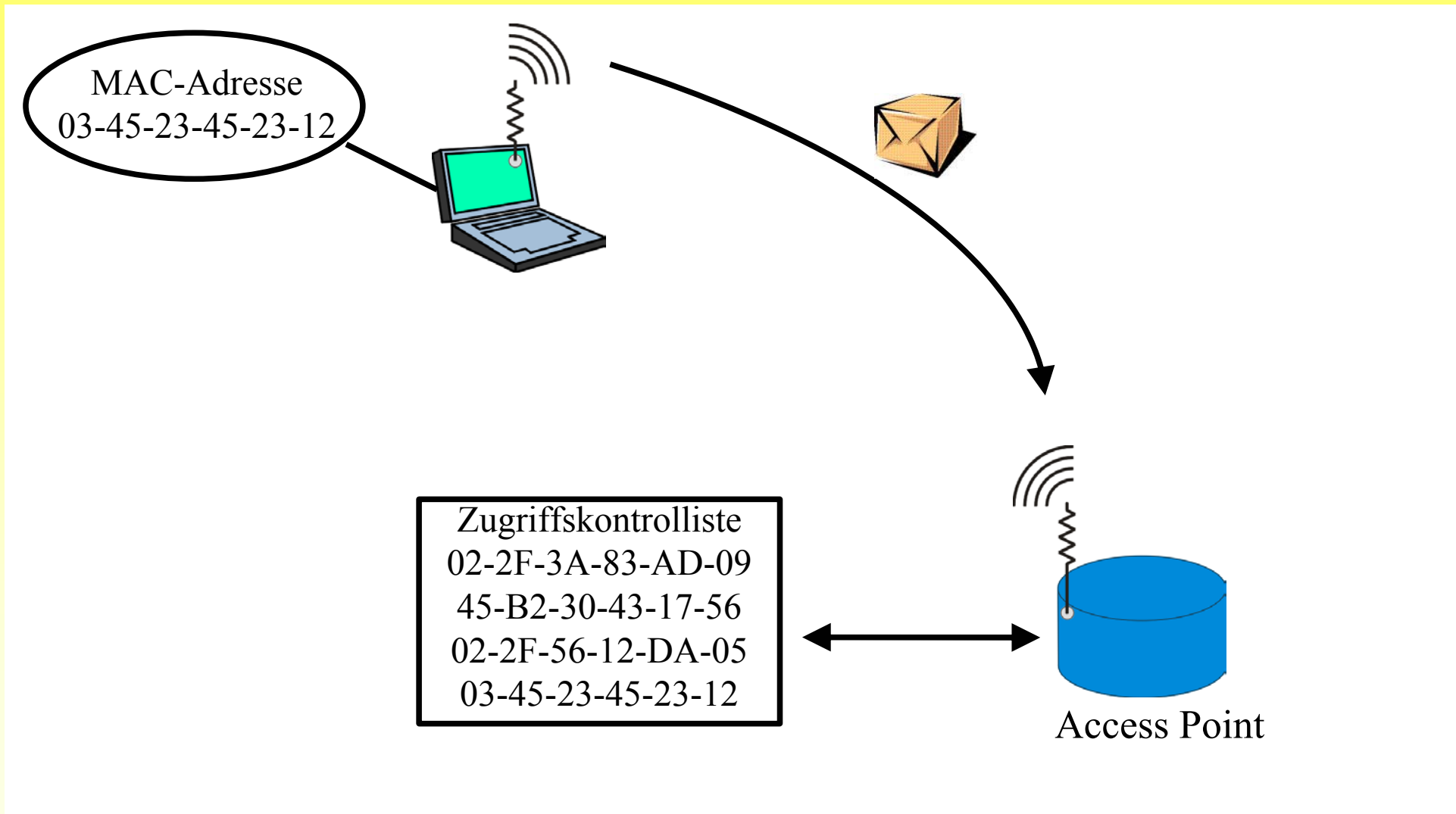
# Sicherungsmechanismen in Wireless LANs

## MAC-Adressen Zugriffskontrolllisten



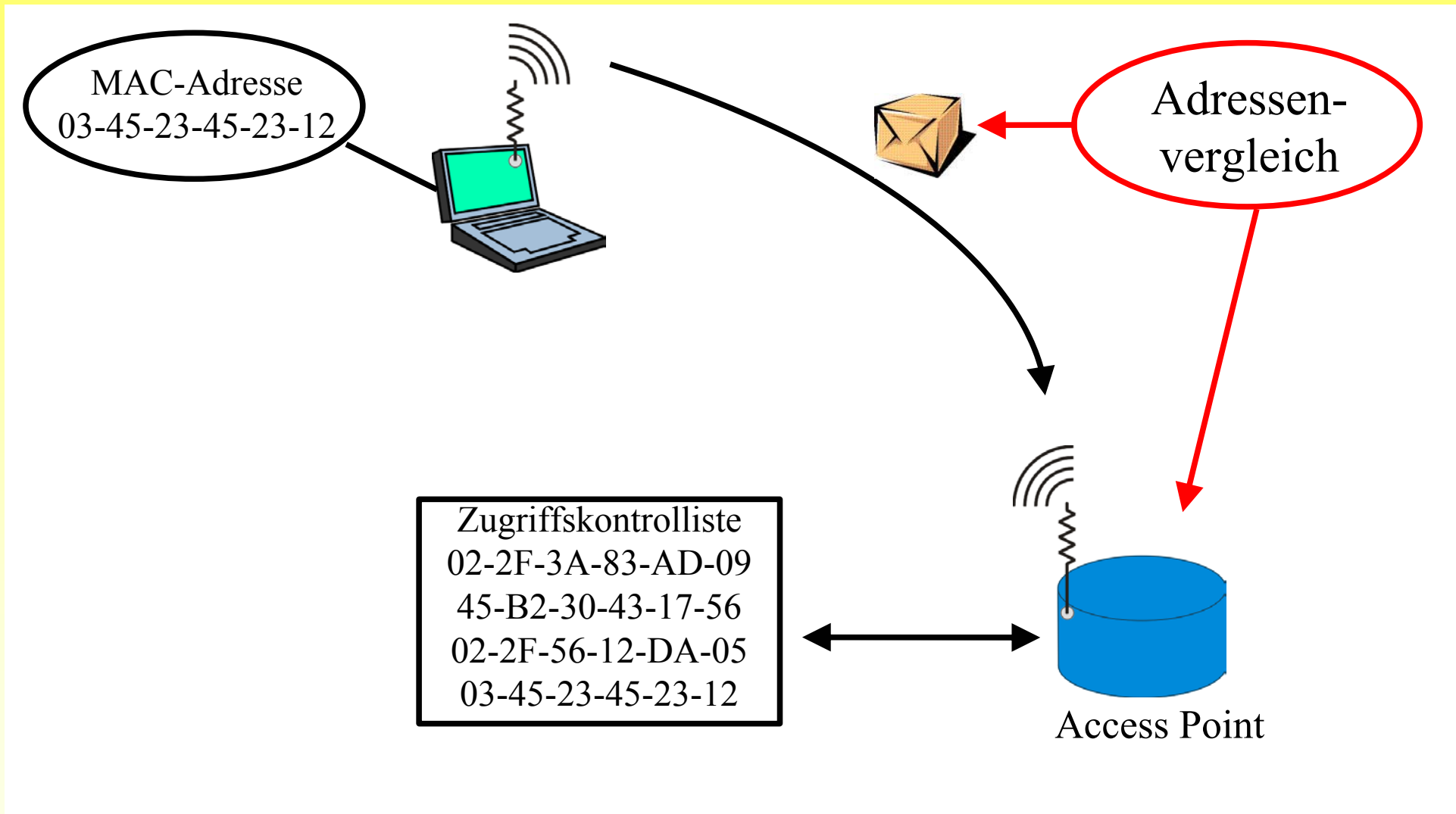
# Sicherungsmechanismen in Wireless LANs

## MAC-Adressen Zugriffskontrolllisten



# Sicherungsmechanismen in Wireless LANs

## MAC-Adressen Zugriffskontrolllisten



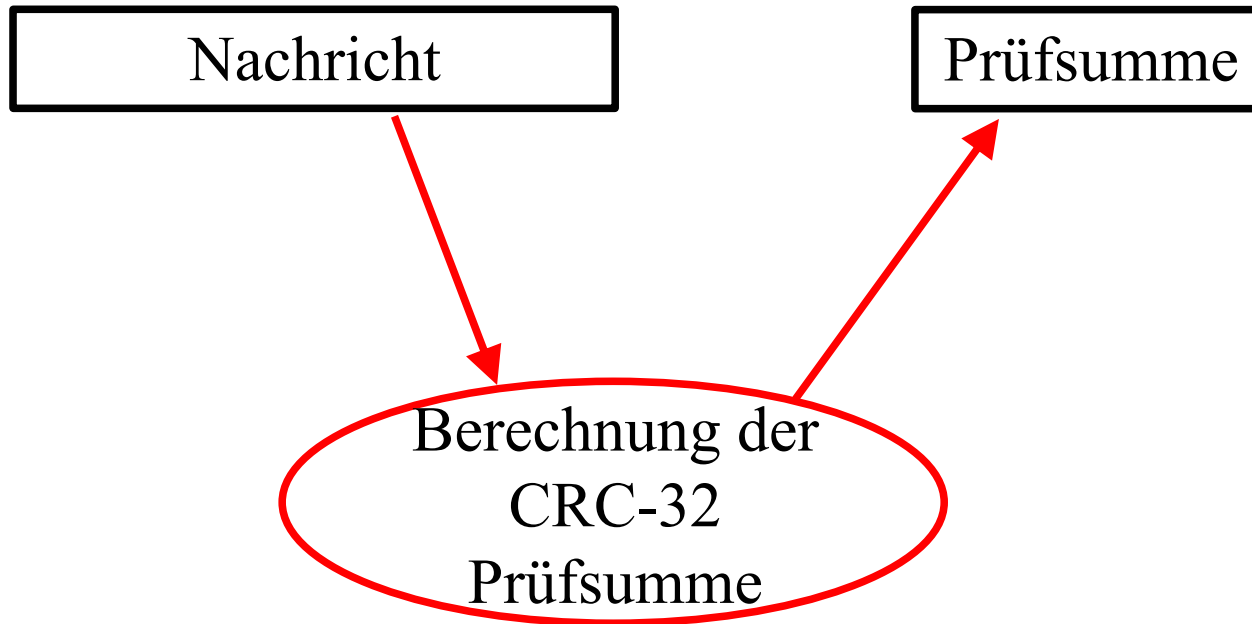
# Sicherungsmechanismen in Wireless LANs

## Wired Equivalent Privacy Verschlüsselung

Nachricht

# Sicherungsmechanismen in Wireless LANs

## Wired Equivalent Privacy Verschlüsselung





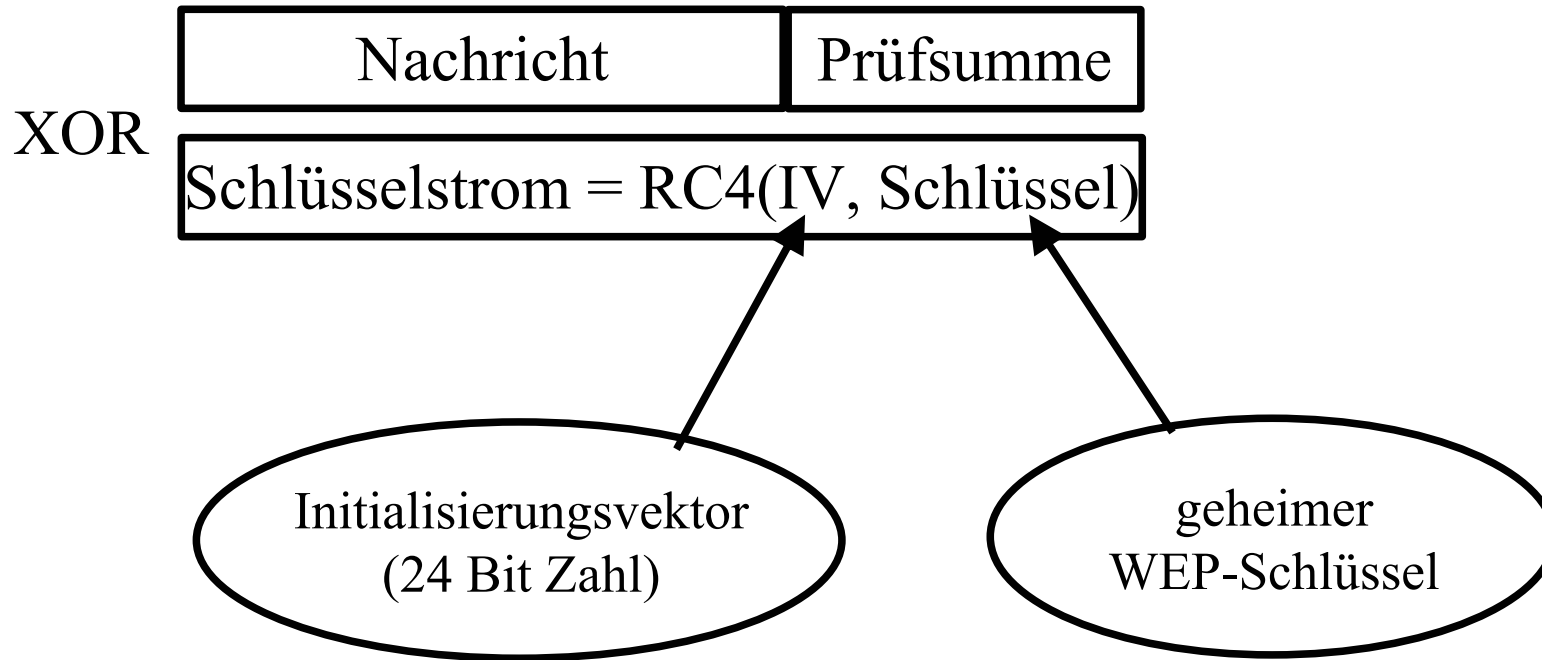
# Sicherungsmechanismen in Wireless LANs

## Wired Equivalent Privacy Verschlüsselung



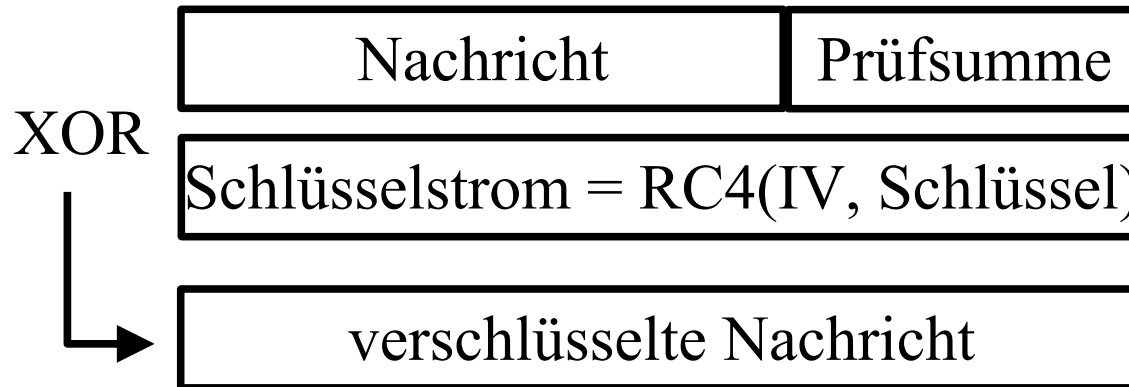
# Sicherungsmechanismen in Wireless LANs

## Wired Equivalent Privacy Verschlüsselung



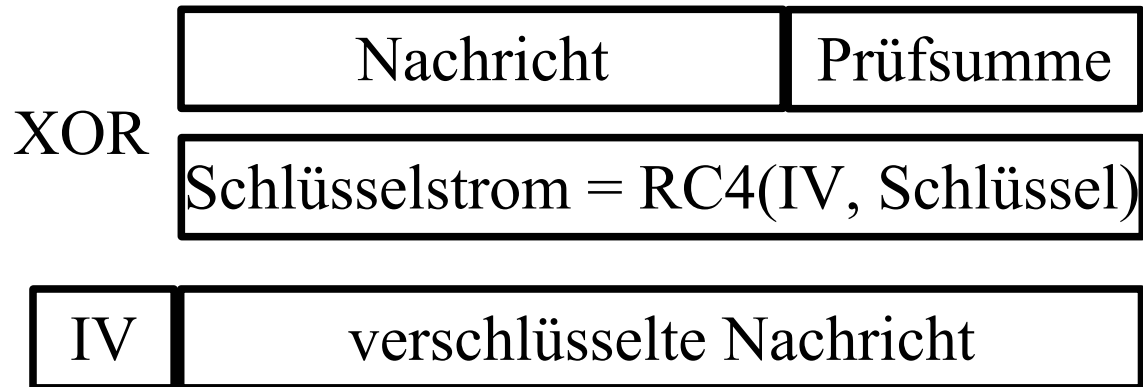
# Sicherungsmechanismen in Wireless LANs

## Wired Equivalent Privacy Verschlüsselung



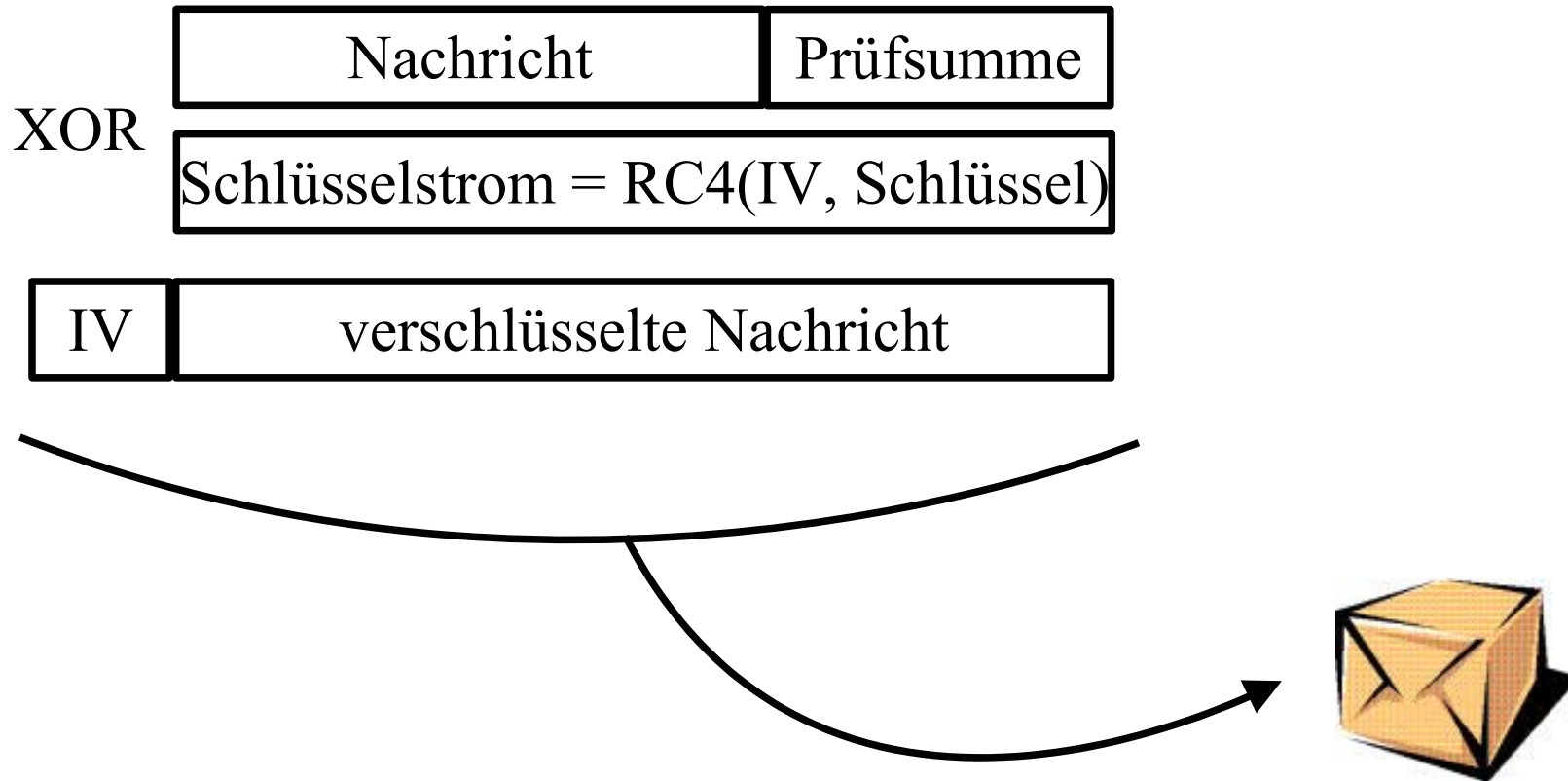
# Sicherungsmechanismen in Wireless LANs

## Wired Equivalent Privacy Verschlüsselung



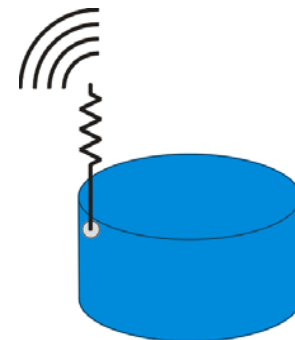
# Sicherungsmechanismen in Wireless LANs

## Wired Equivalent Privacy Verschlüsselung



# Sicherungsmechanismen in Wireless LANs

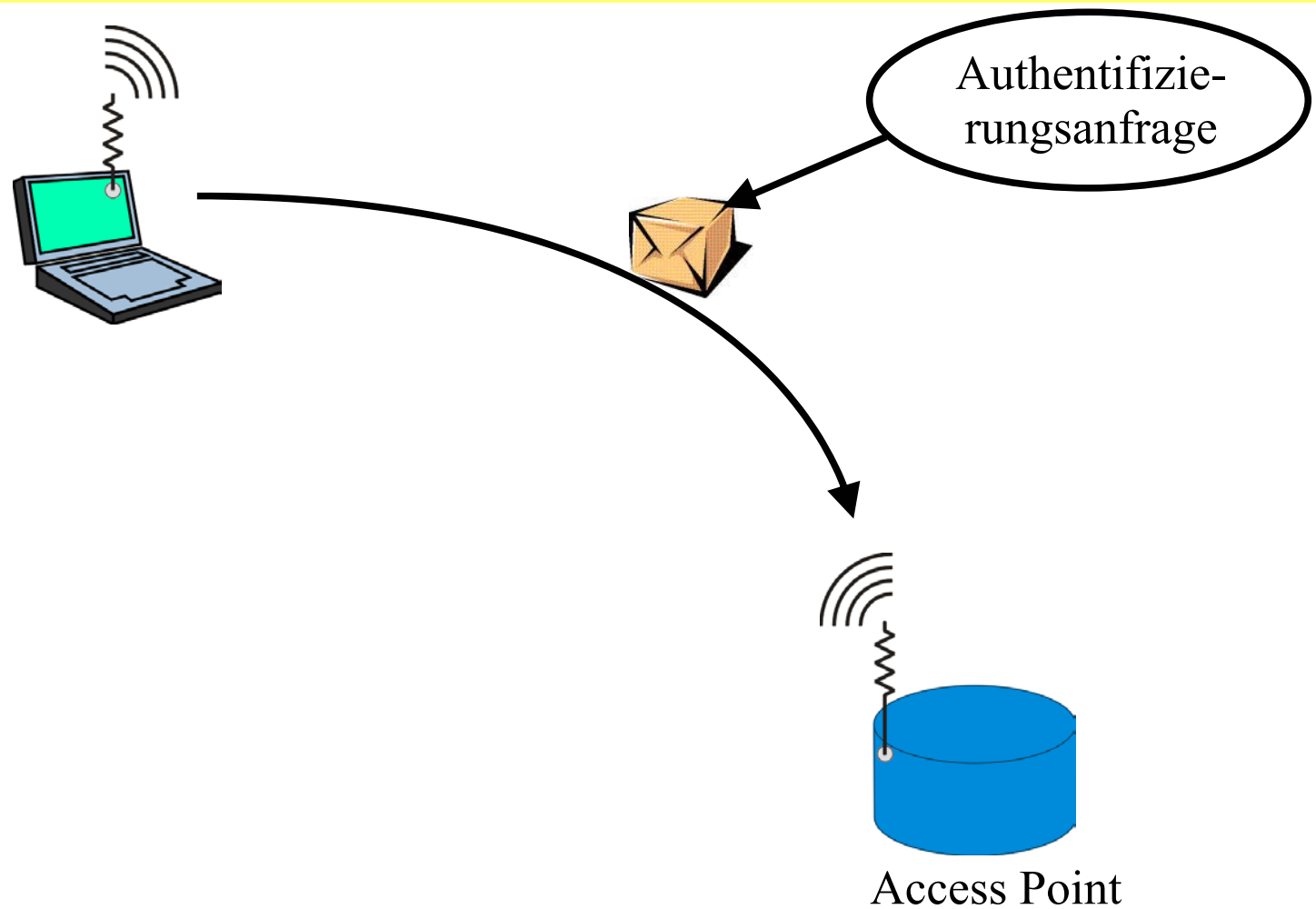
## Benutzerauthentifizierung (Shared Key)



Access Point

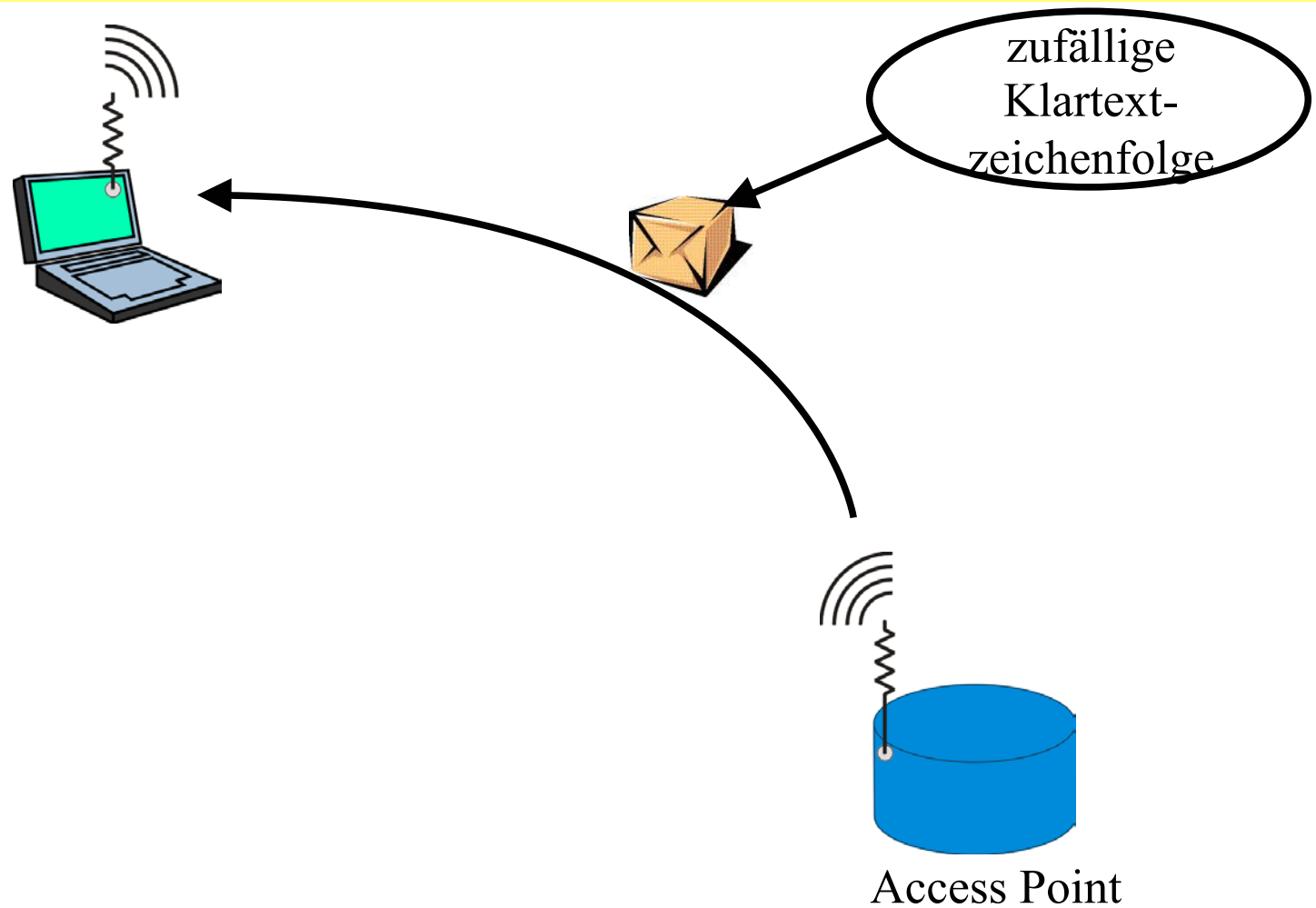
# Sicherungsmechanismen in Wireless LANs

## Benutzerauthentifizierung (Shared Key)



# Sicherungsmechanismen in Wireless LANs

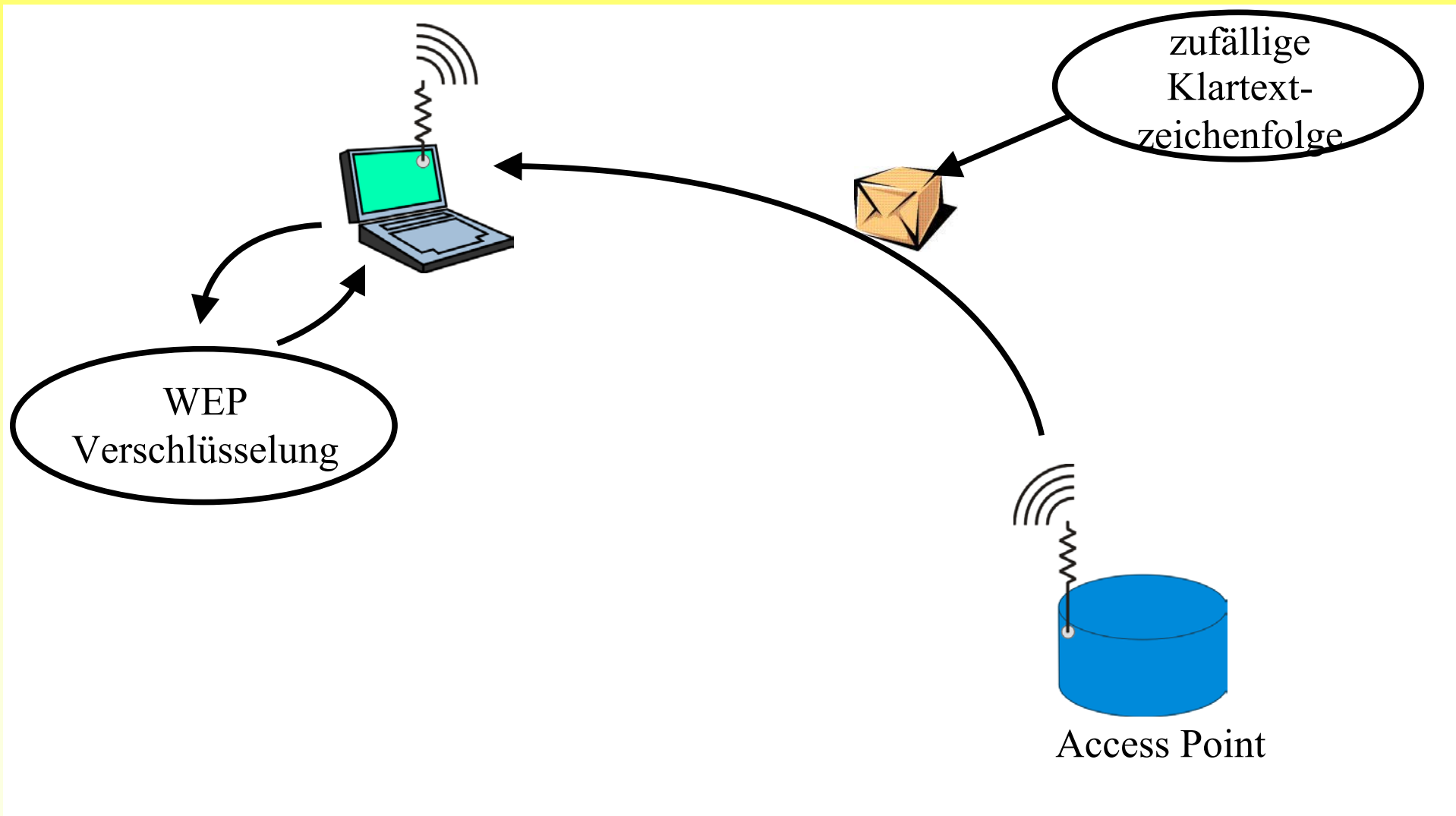
## Benutzerauthentifizierung (Shared Key)





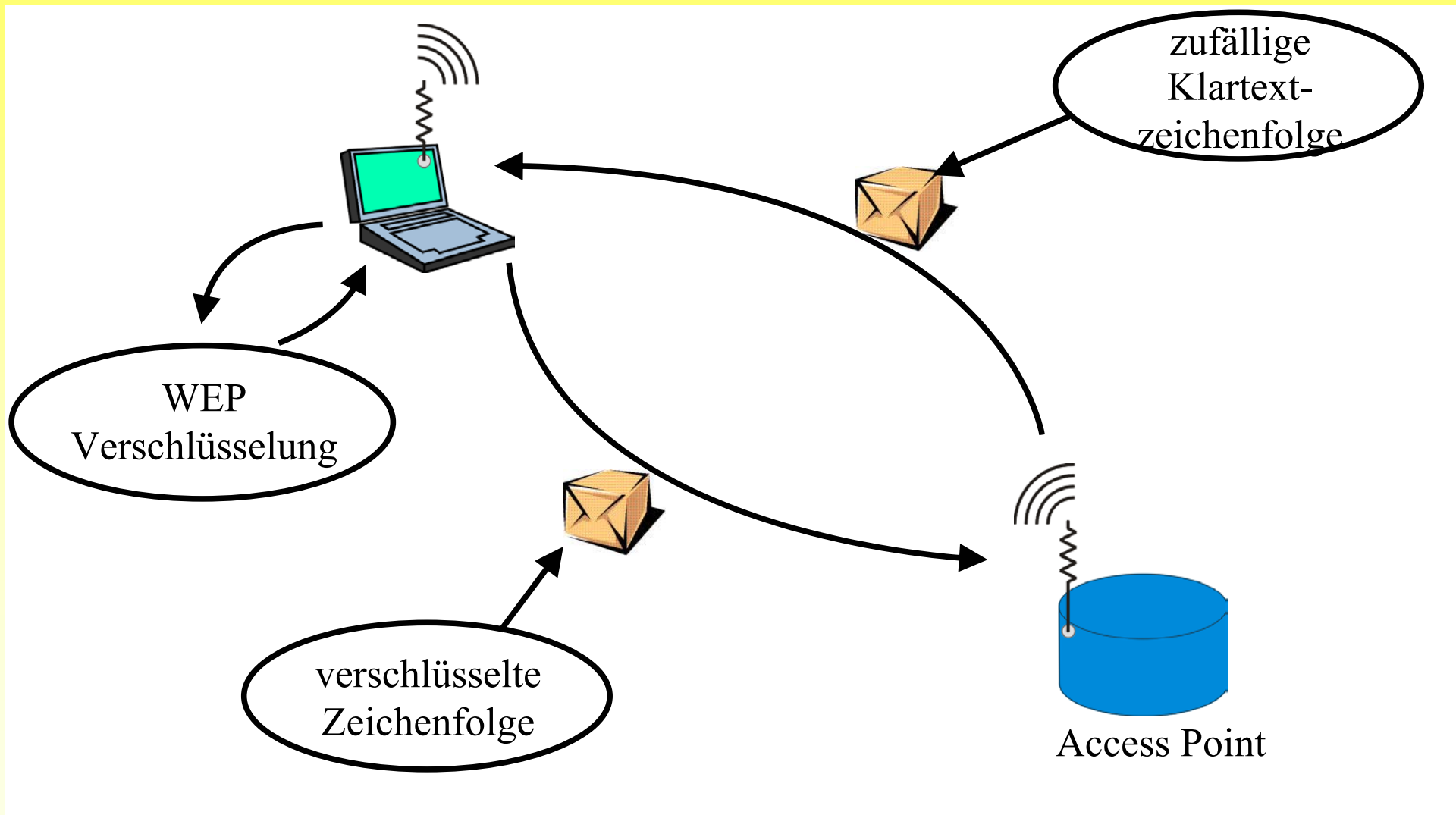
# Sicherungsmechanismen in Wireless LANs

## Benutzerauthentifizierung (Shared Key)



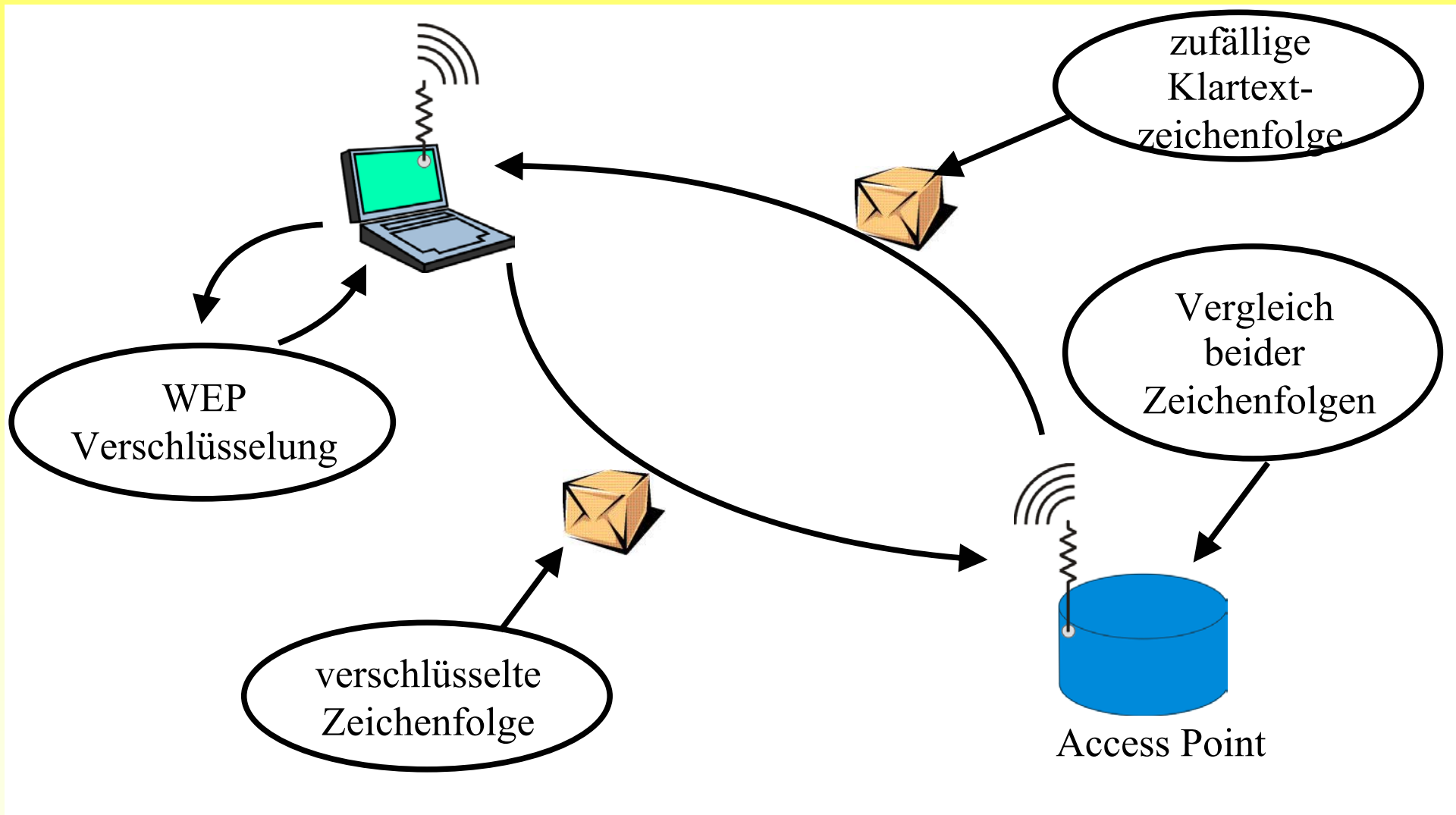
# Sicherungsmechanismen in Wireless LANs

## Benutzerauthentifizierung (Shared Key)



# Sicherungsmechanismen in Wireless LANs

## Benutzerauthentifizierung (Shared Key)



- Abfangen der ESSID
- MAC-Adressen Zugriffskontrolllisten
- Wired Equivalent Privacy (WEP) Verschlüsselung
- Shared Key Authentifizierung
- Denial of Service (DoS) im WLAN

# Schwachstellen in den Sicherungsmechanismen

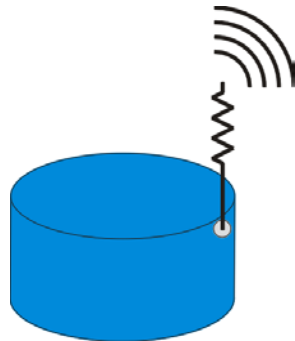
## Abfangen der ESSID im „geschlossenen“ WLAN



Nutzer



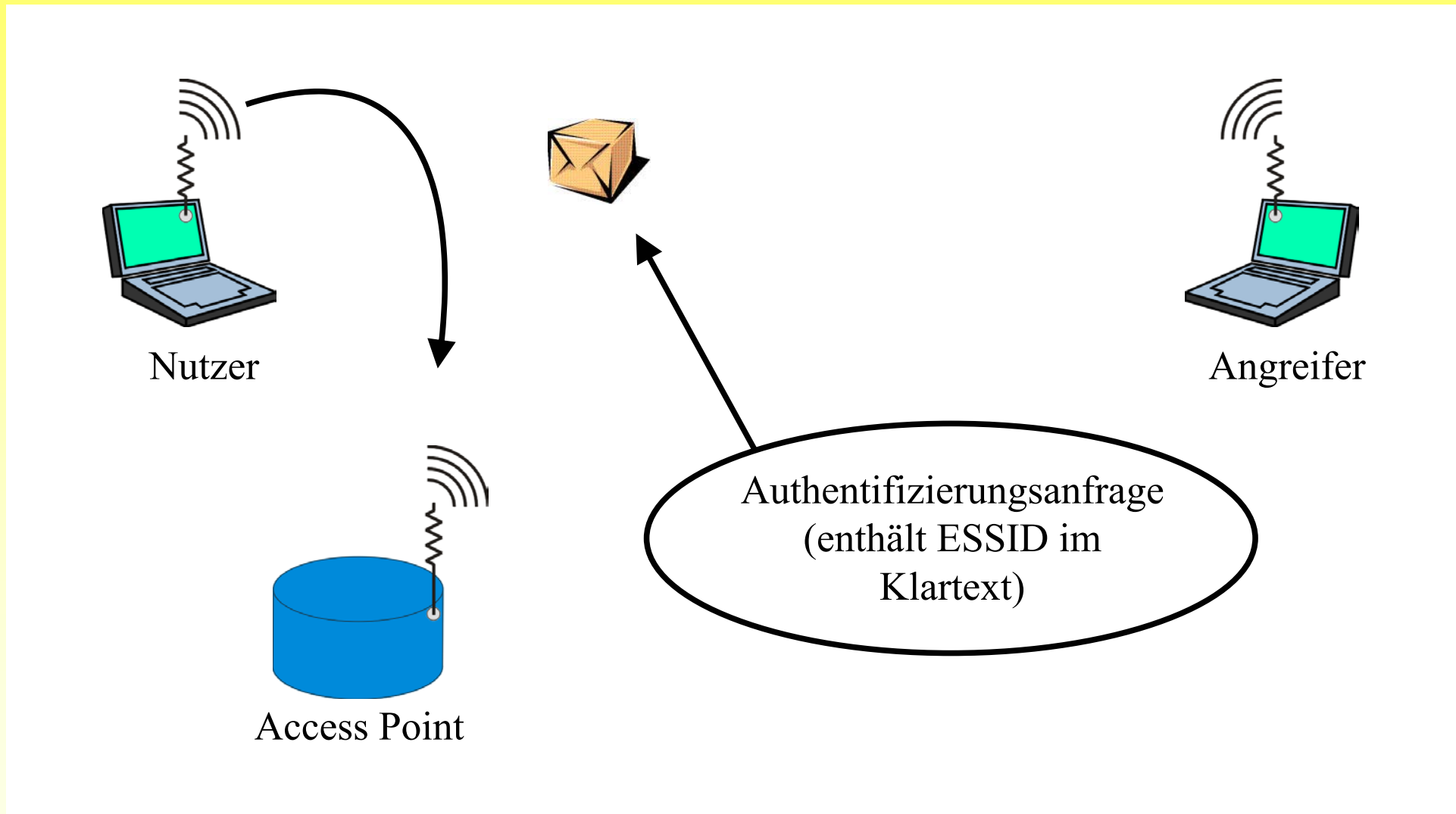
Angreifer



Access Point

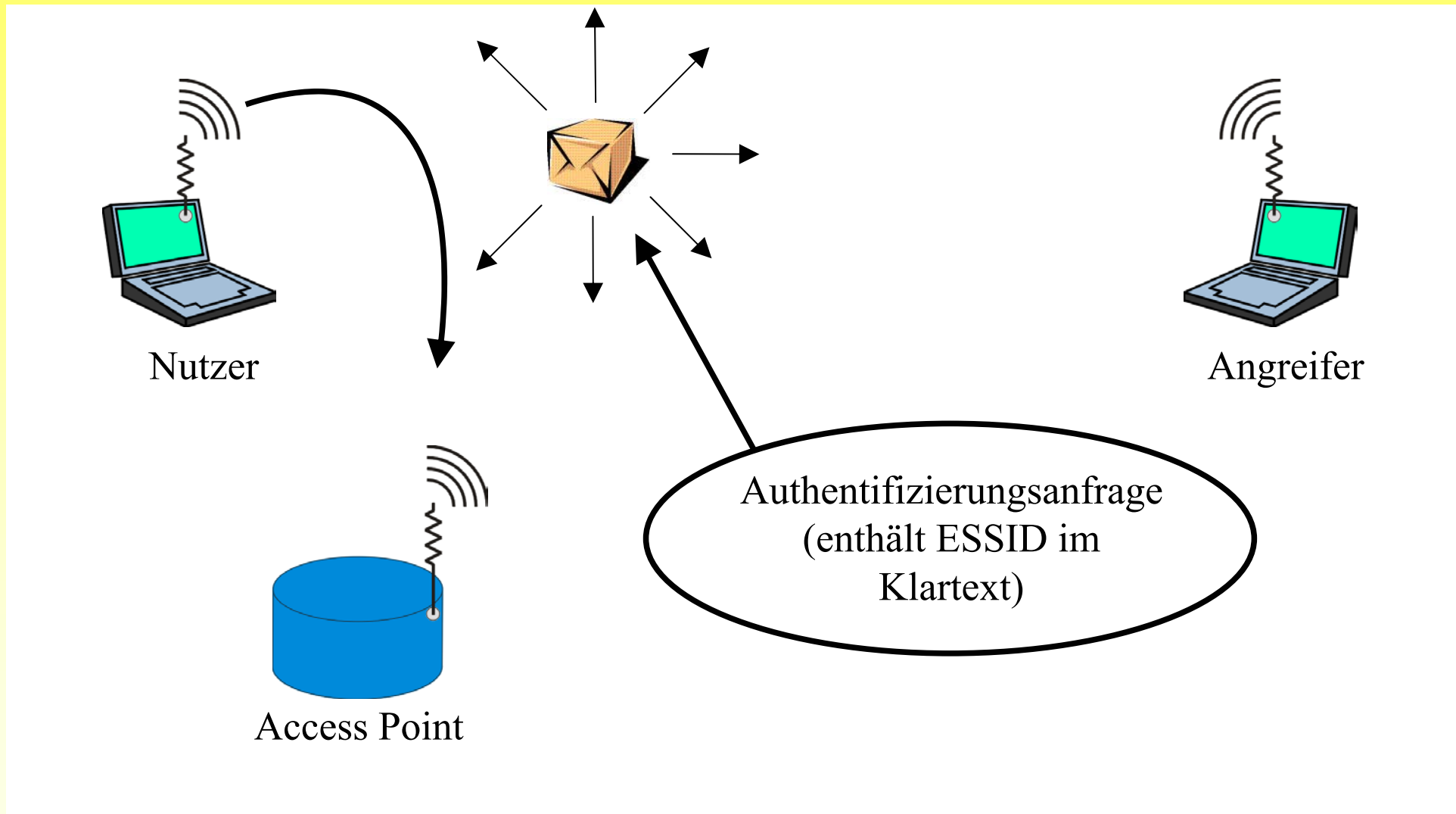
# Schwachstellen in den Sicherungsmechanismen

## Abfangen der ESSID im „geschlossenen“ WLAN



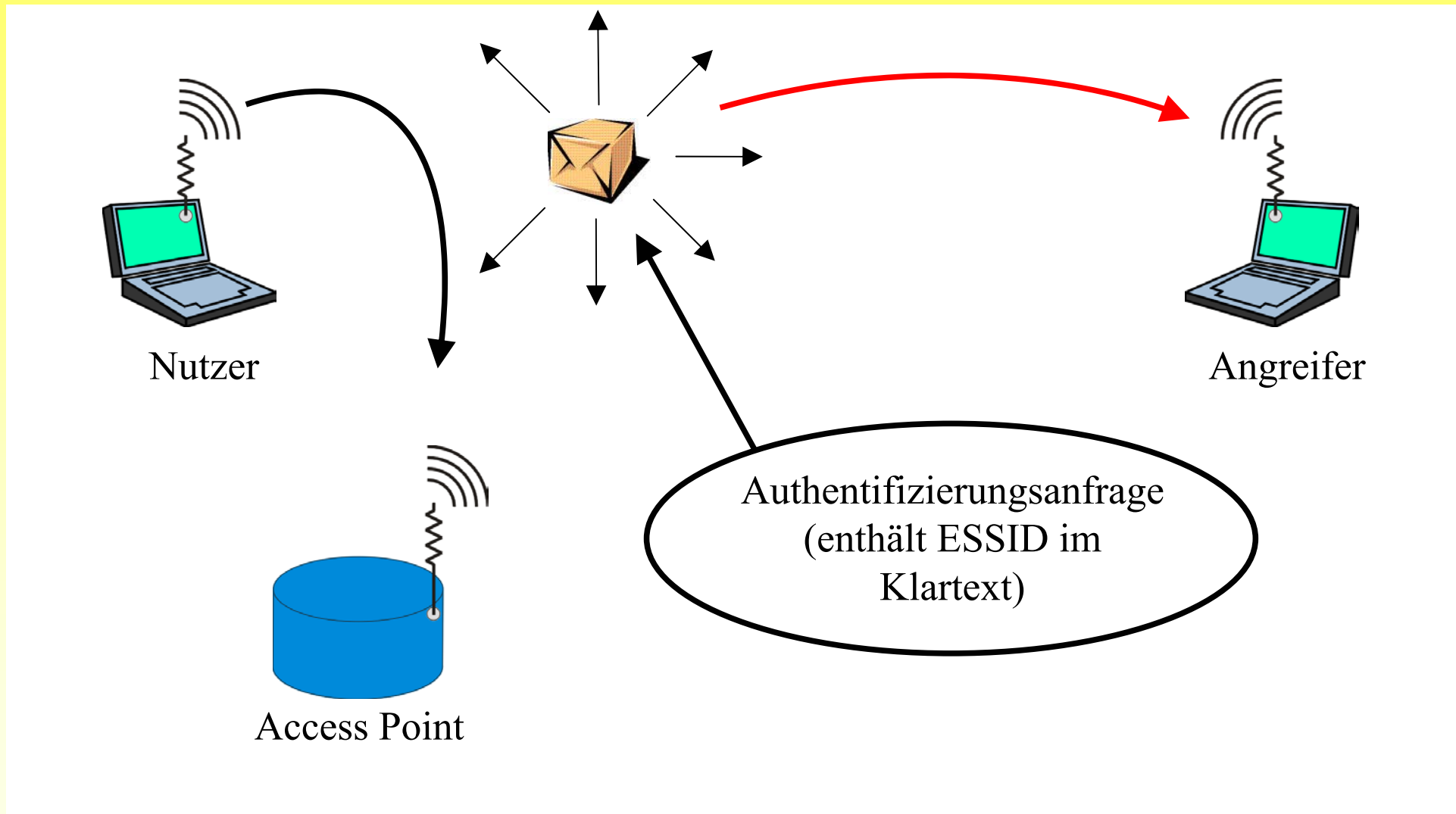
# Schwachstellen in den Sicherungsmechanismen

## Abfangen der ESSID im „geschlossenen“ WLAN



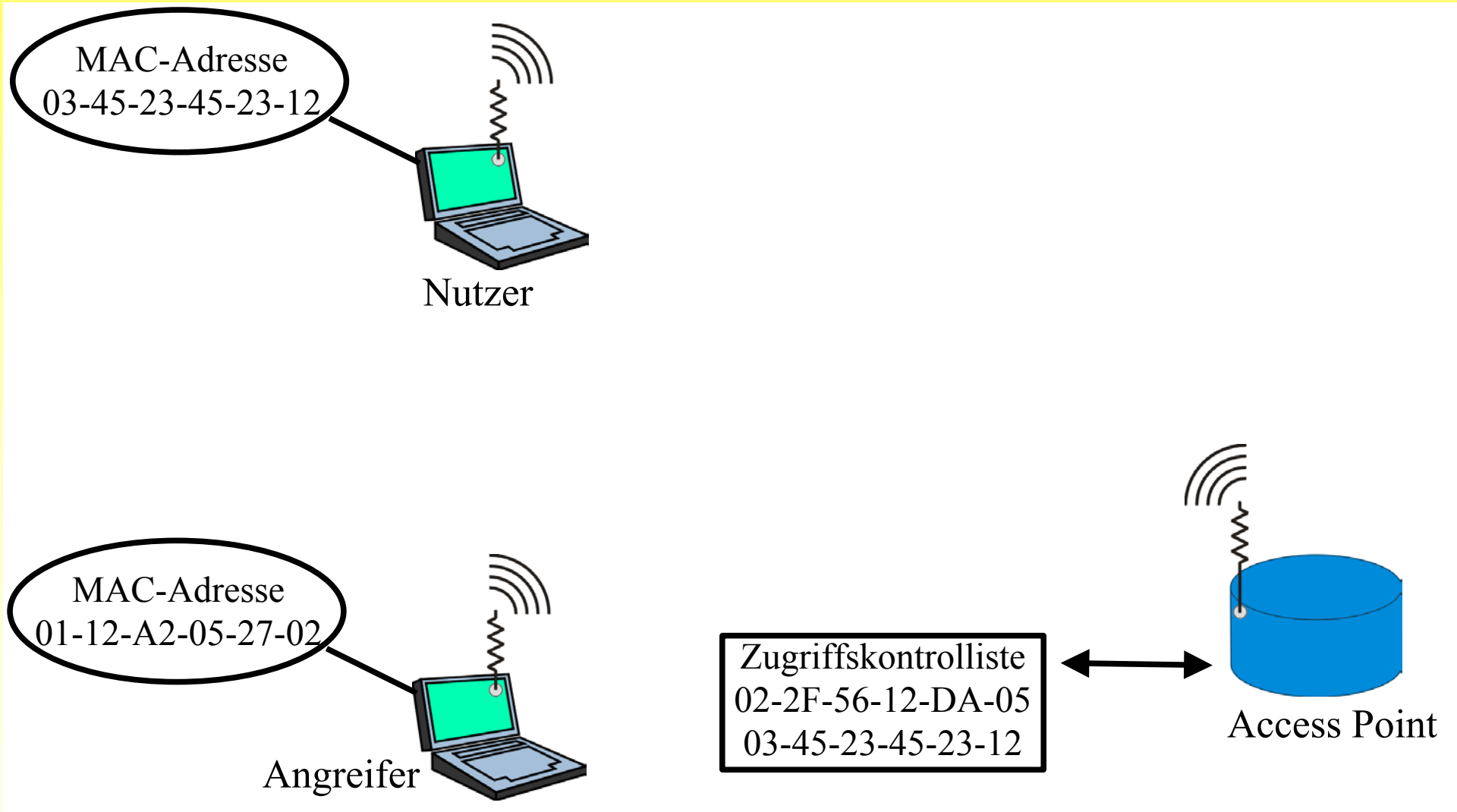
# Schwachstellen in den Sicherungsmechanismen

## Abfangen der ESSID im „geschlossenen“ WLAN

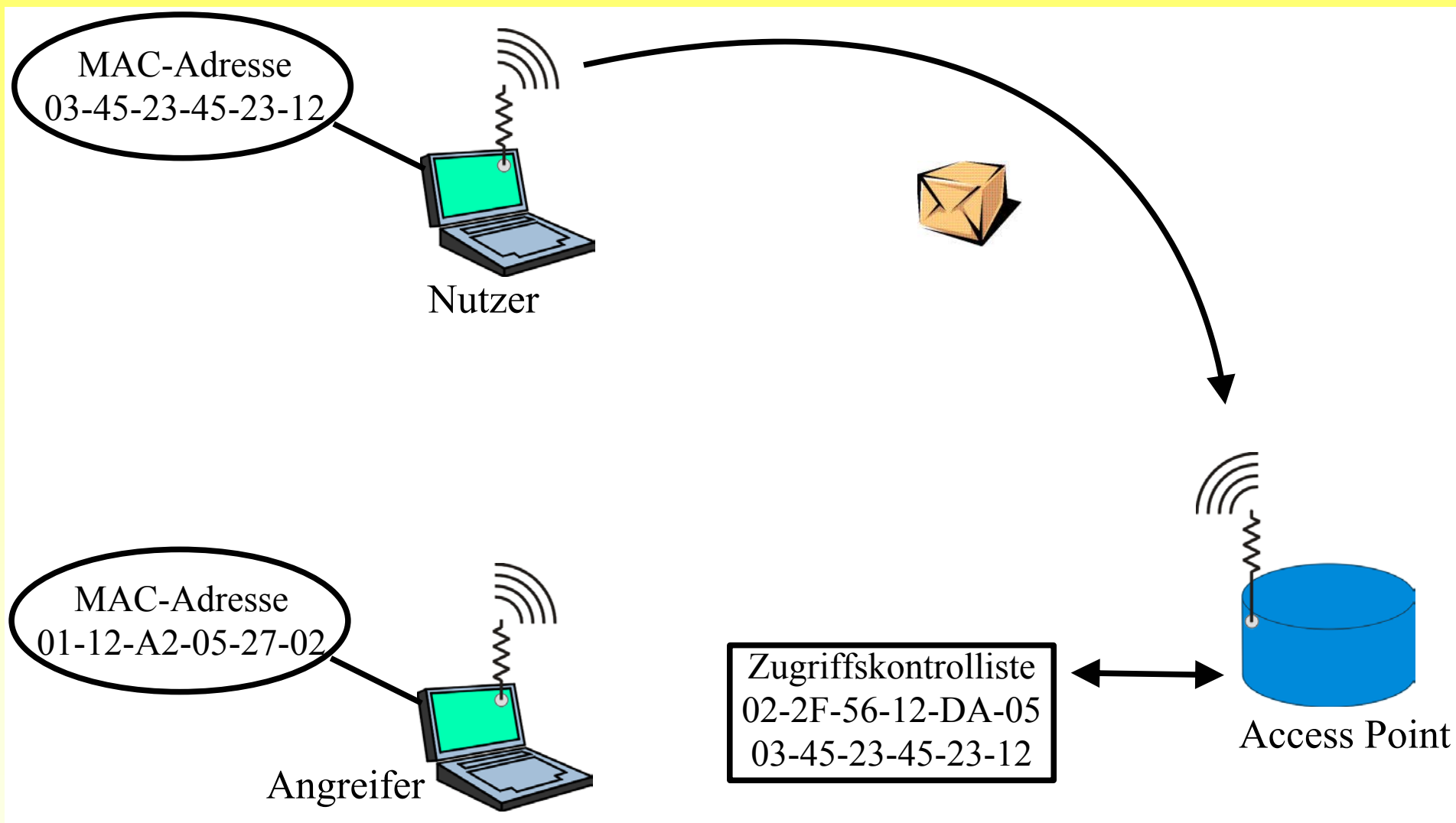




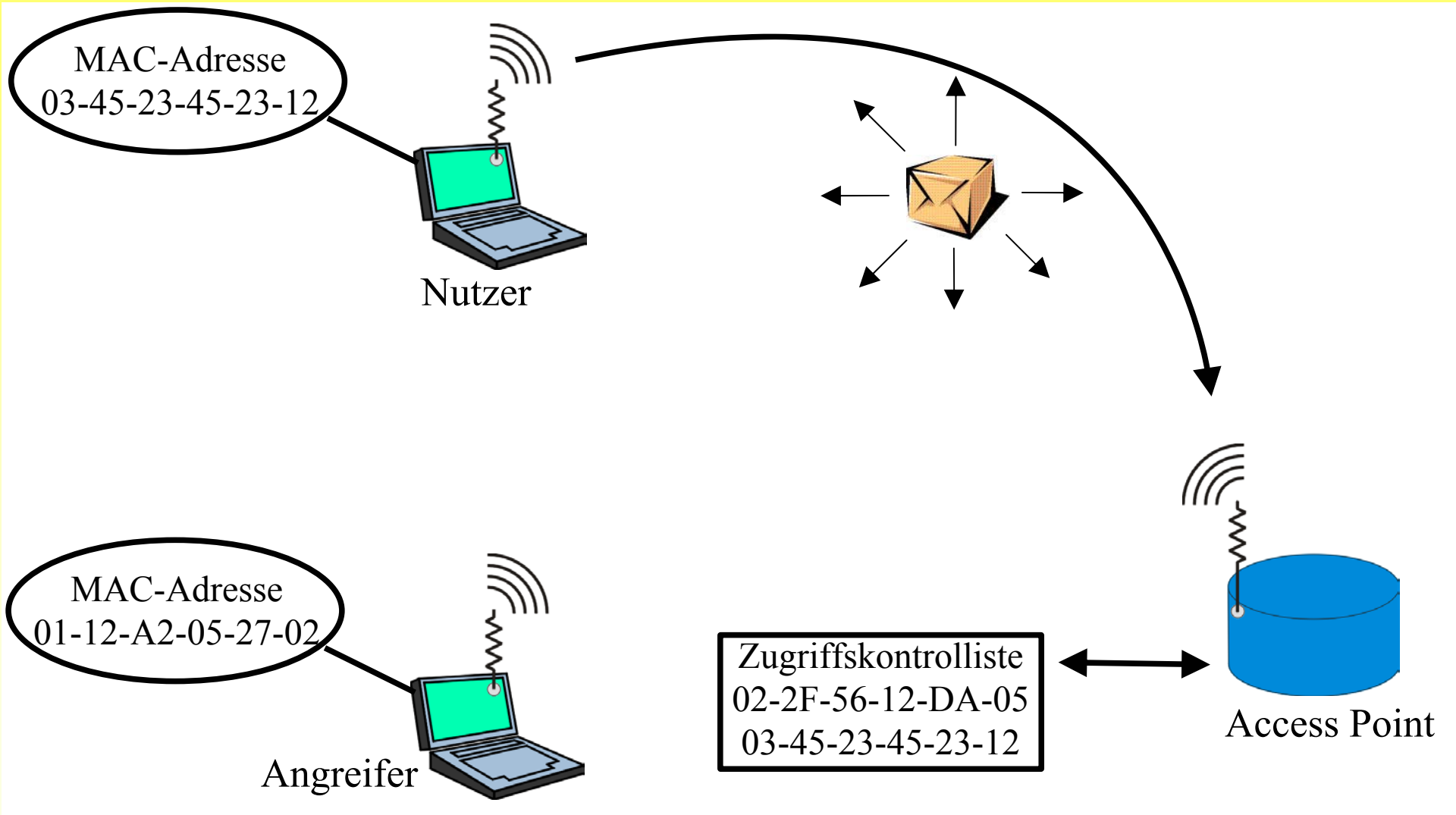
# Schwachstellen in den Sicherungsmechanismen MAC-Adressen Zugriffskontrolllisten



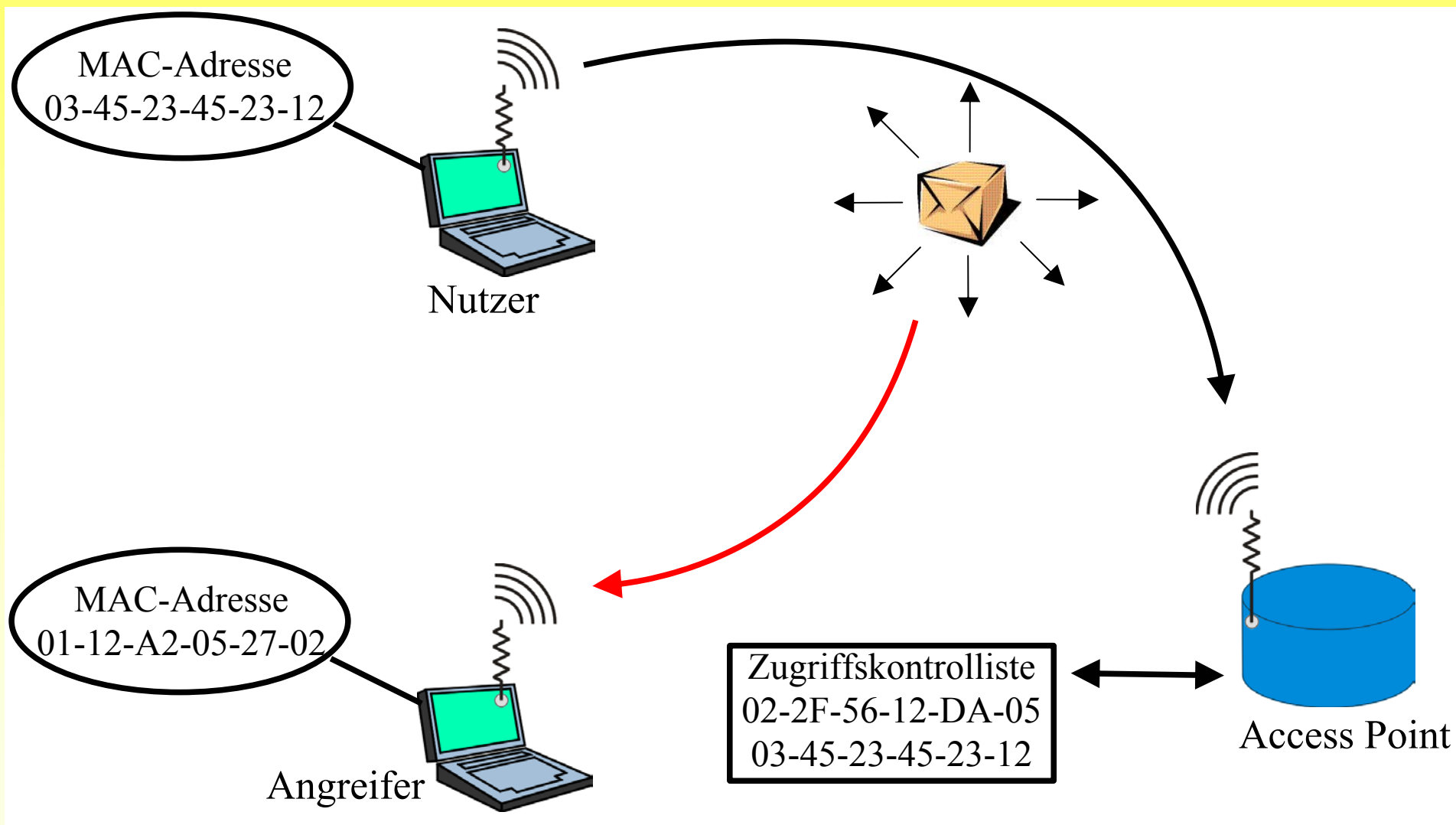
# Schwachstellen in den Sicherungsmechanismen MAC-Adressen Zugriffskontrolllisten



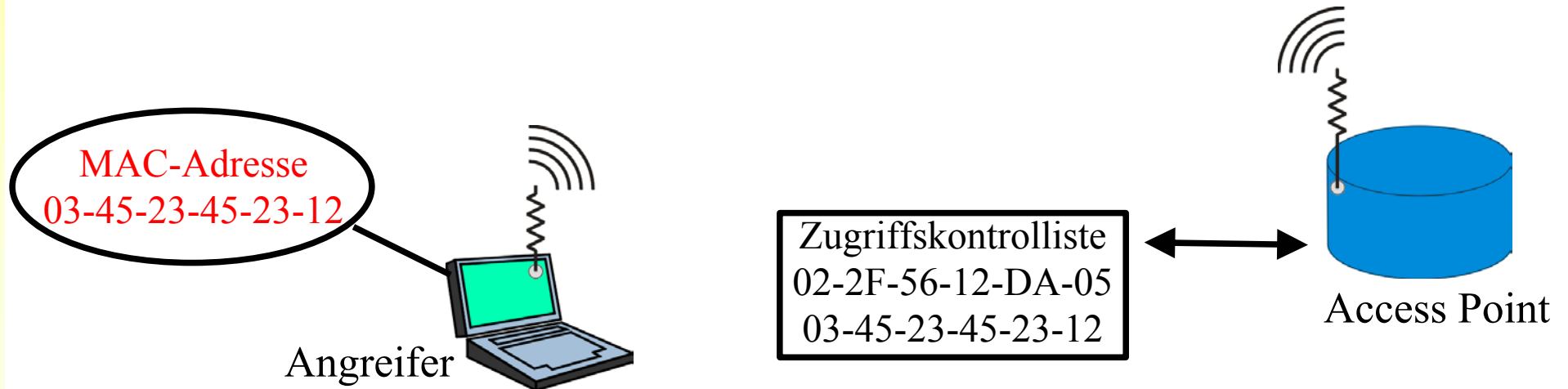
# Schwachstellen in den Sicherungsmechanismen MAC-Adressen Zugriffskontrolllisten



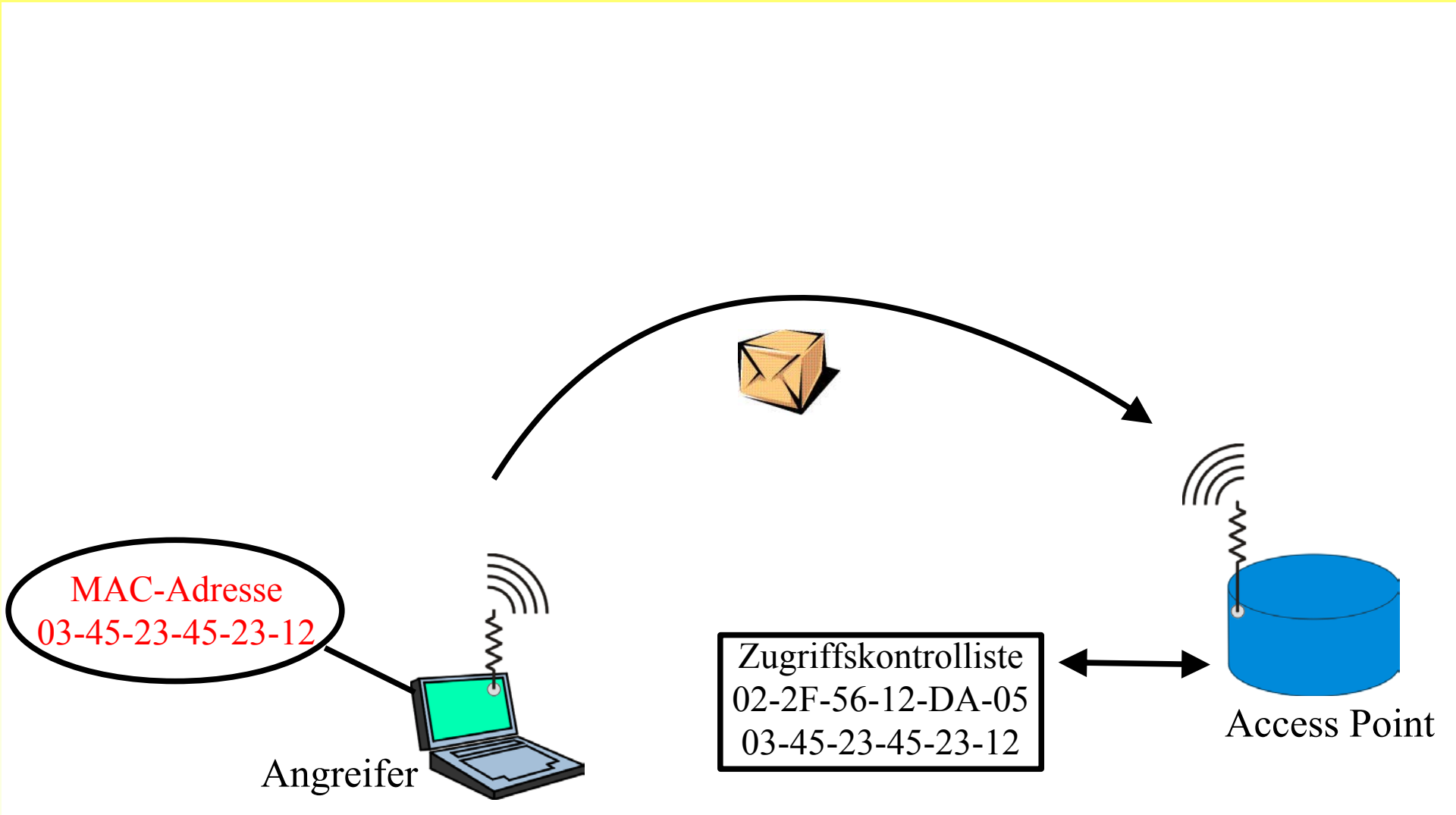
# Schwachstellen in den Sicherungsmechanismen MAC-Adressen Zugriffskontrolllisten



# Schwachstellen in den Sicherungsmechanismen MAC-Adressen Zugriffskontrolllisten



# Schwachstellen in den Sicherungsmechanismen MAC-Adressen Zugriffskontrolllisten



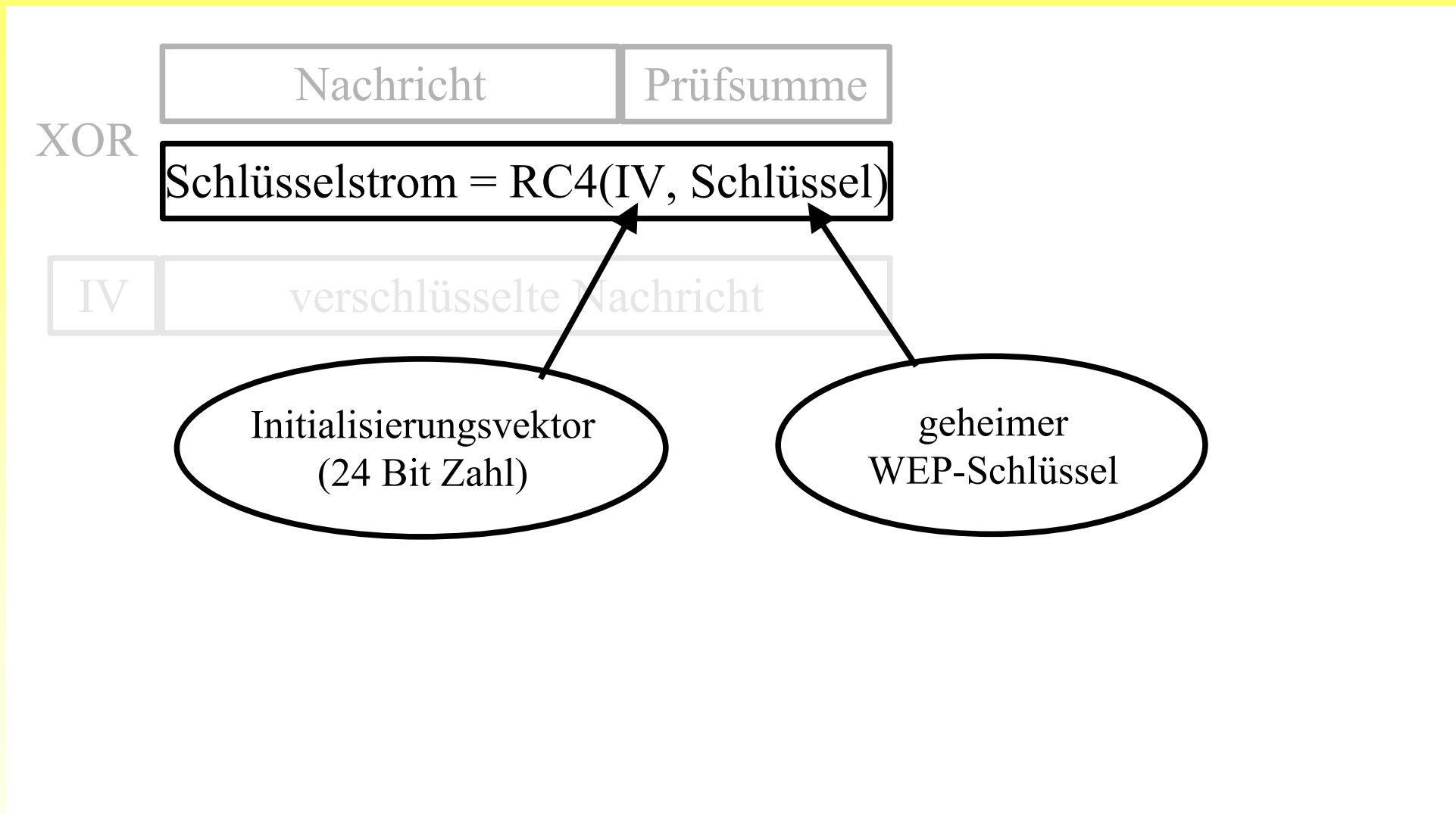
# Schwachstellen in den Sicherungsmechanismen

## Wired Equivalent Privacy Verschlüsselung



# Schwachstellen in den Sicherungsmechanismen

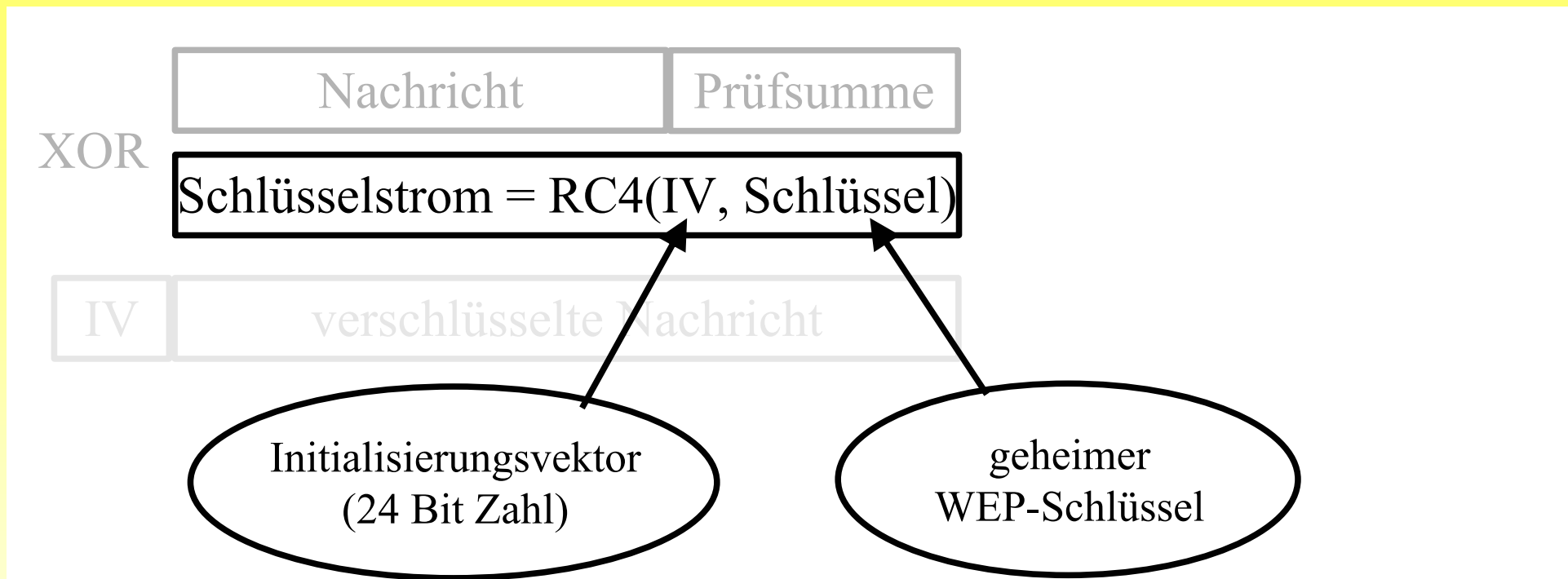
## Wired Equivalent Privacy Verschlüsselung





# Schwachstellen in den Sicherungsmechanismen

## Wired Equivalent Privacy Verschlüsselung



Datentransferrate von 5Mb/s  $\hat{=}$  436 Datenpakete/s mit je 1500 Bytes  
Nach 12 Stunden Datenübertragung  $\Rightarrow$  mehr als  $2^{24}$  Datenpakete übertragen

# Schwachstellen in den Sicherungsmechanismen

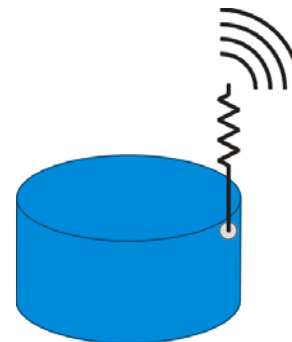
## Wired Equivalent Privacy Verschlüsselung



Nutzer



Angreifer



Access Point

# Schwachstellen in den Sicherungsmechanismen

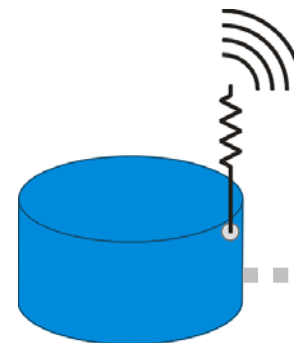
## Wired Equivalent Privacy Verschlüsselung



Nutzer



Angreifer



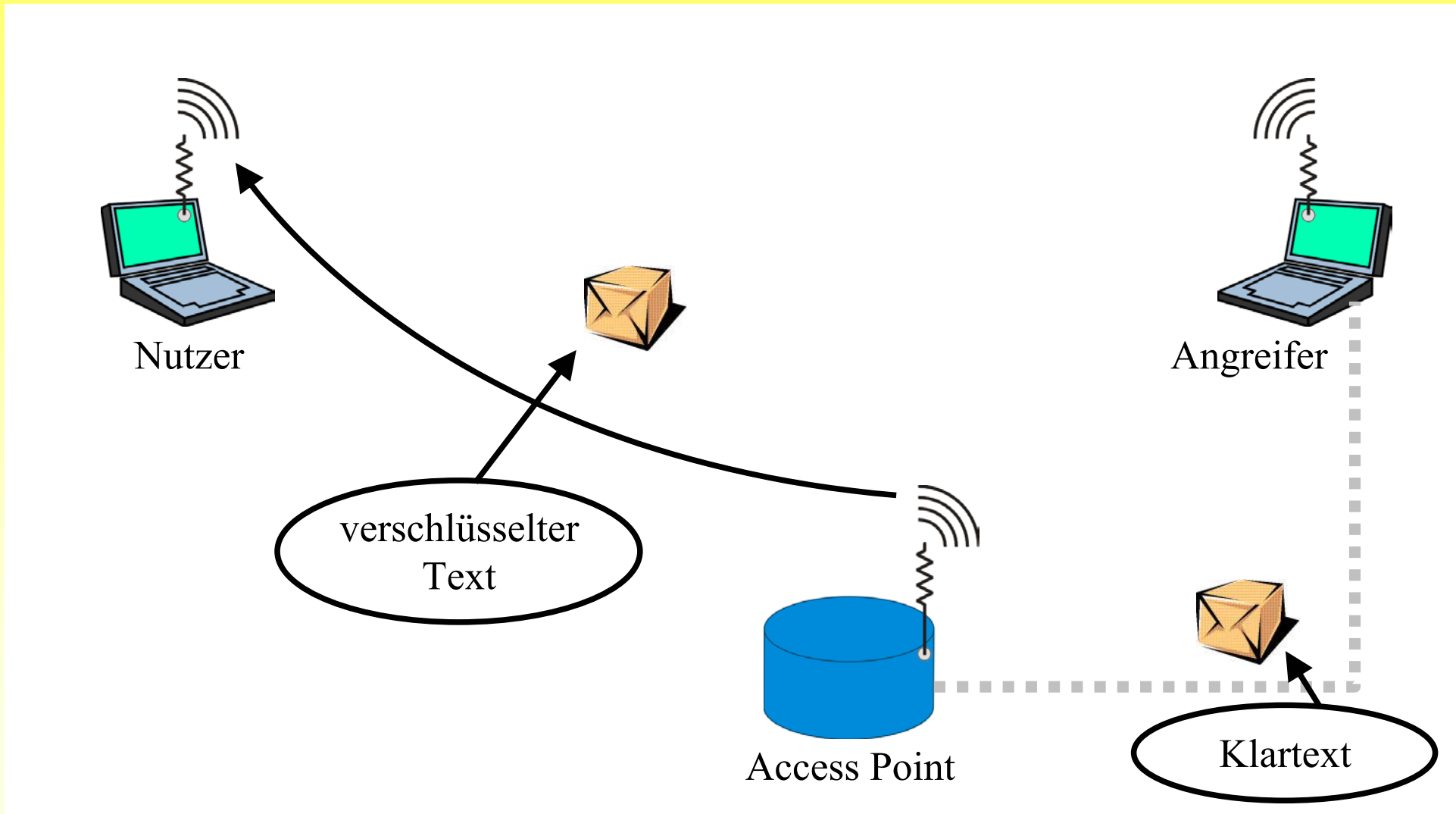
Access Point



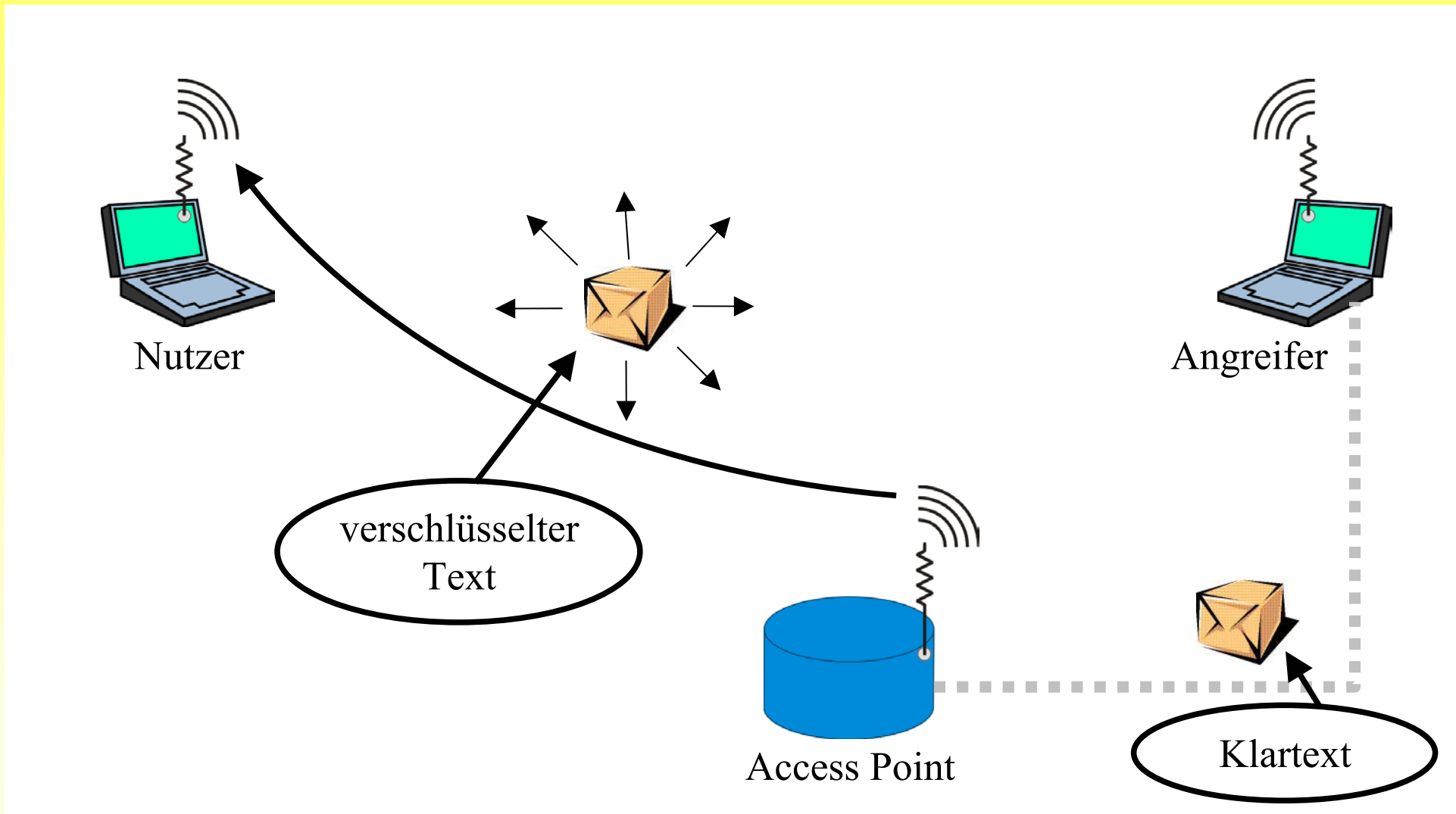
Klartext



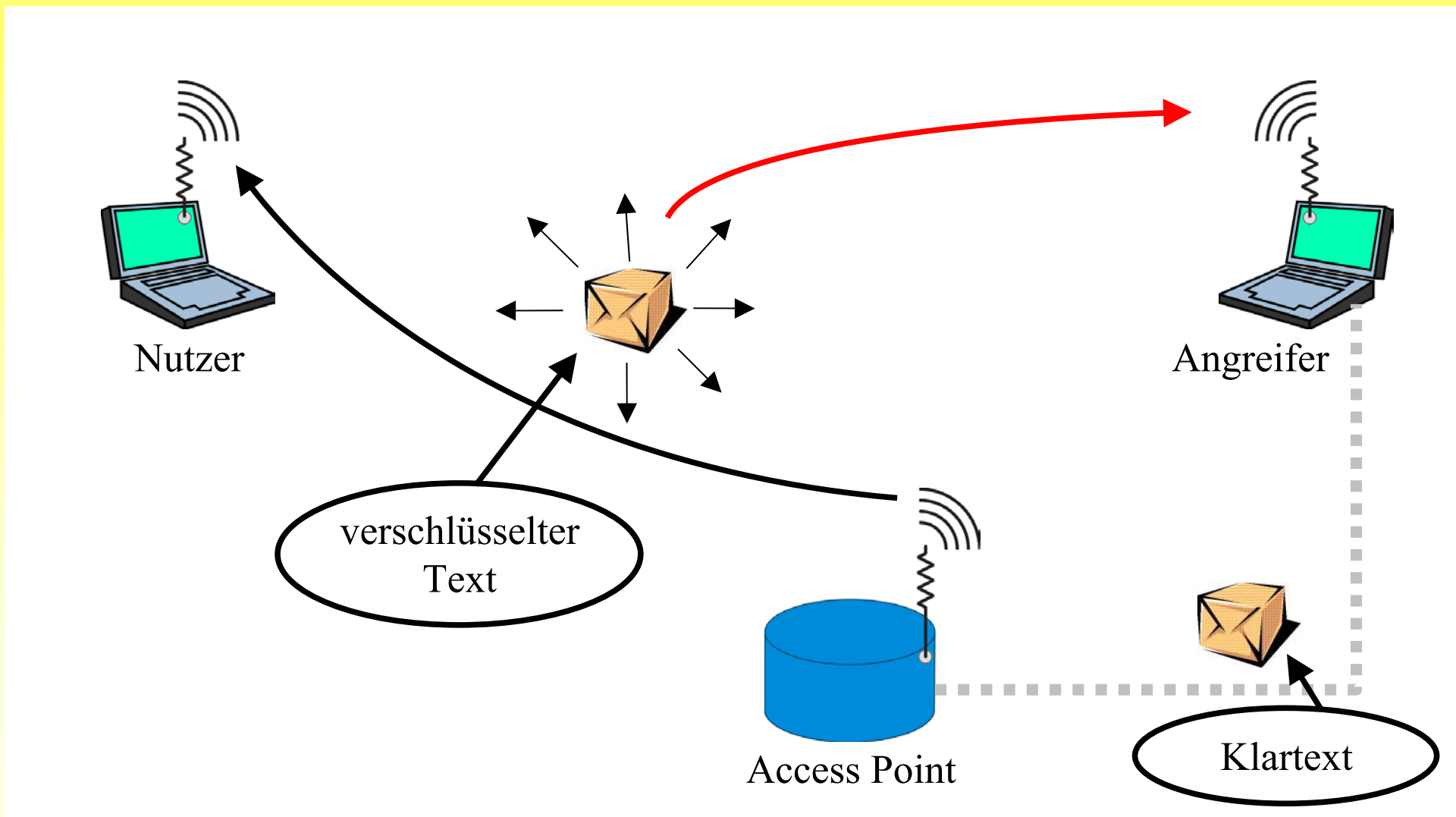
# Schwachstellen in den Sicherungsmechanismen Wired Equivalent Privacy Verschlüsselung



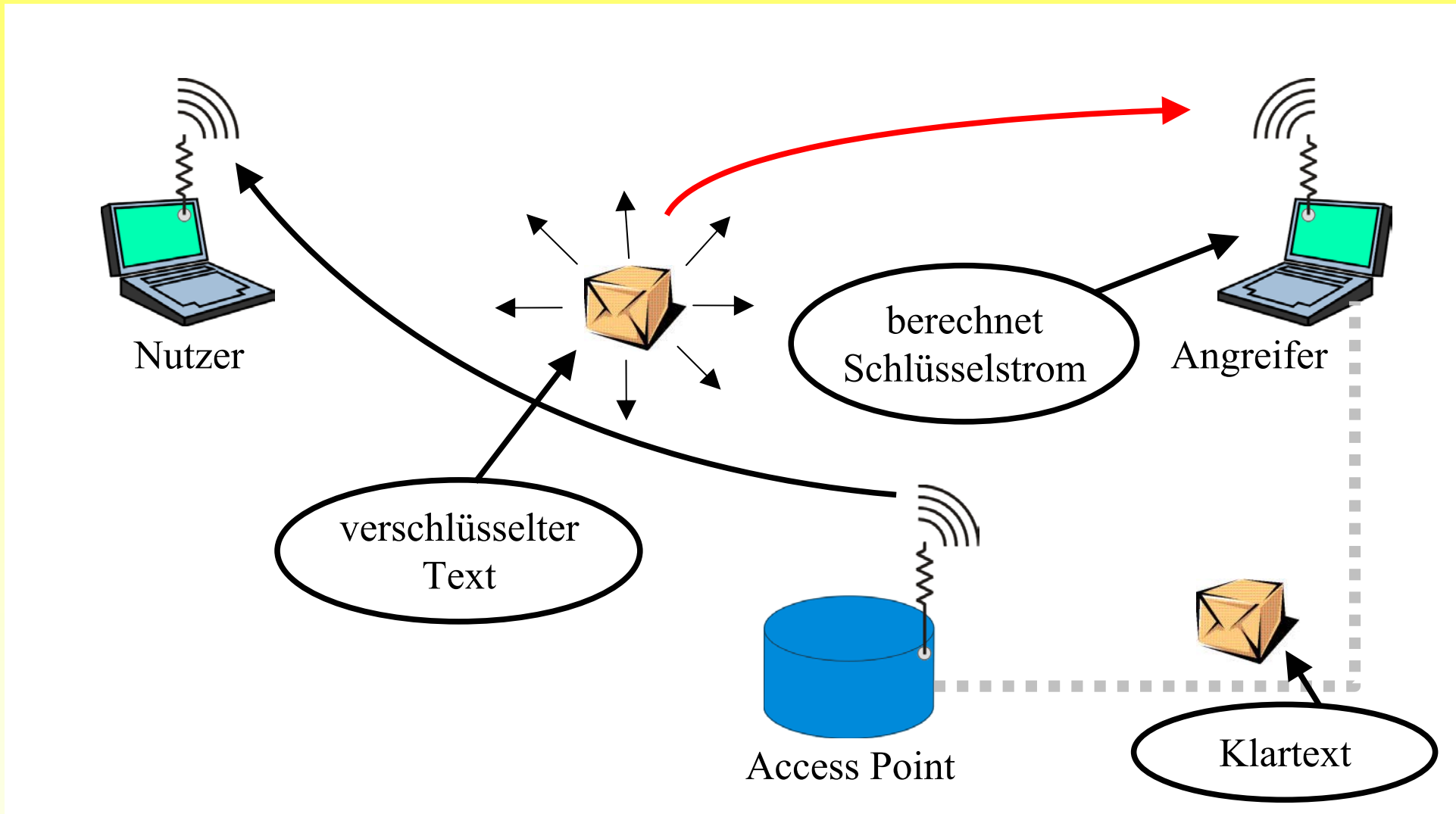
# Schwachstellen in den Sicherungsmechanismen Wired Equivalent Privacy Verschlüsselung



# Schwachstellen in den Sicherungsmechanismen Wired Equivalent Privacy Verschlüsselung



# Schwachstellen in den Sicherungsmechanismen Wired Equivalent Privacy Verschlüsselung



# Schwachstellen in den Sicherungsmechanismen

## Wired Equivalent Privacy Verschlüsselung

P = bekannter Klartext

C = bekannter verschlüsselter Text

C = P xor RC4(IV, Key)

---

C xor P  $\Leftrightarrow$  (P xor RC4(IV, Key)) xor P



# Schwachstellen in den Sicherungsmechanismen

## Wired Equivalent Privacy Verschlüsselung

**P = bekannter Klartext**

**C = bekannter verschlüsselter Text**

**C = P xor RC4(IV, Key)**

---

**C xor P <=> (P xor RC4(IV, Key)) xor P**

**<=> P xor (RC4(IV, Key) xor P)**

**<=> P xor (P xor RC4(IV, Key))**

**<=> (P xor P) xor RC4(IV, Key)**

# Schwachstellen in den Sicherungsmechanismen

## Wired Equivalent Privacy Verschlüsselung

**P = bekannter Klartext**

**C = bekannter verschlüsselter Text**

**C = P xor RC4(IV, Key)**

---

**C xor P <=> (P xor RC4(IV, Key)) xor P**

**<=> P xor (RC4(IV, Key) xor P)**

**<=> P xor (P xor RC4(IV, Key))**

**<=> (P xor P) xor RC4(IV, Key)**

**<=> 0 xor RC4(IV, Key)**

**P = bekannter Klartext**

**C = bekannter verschlüsselter Text**

**C = P xor RC4(IV, Key)**

---

**C xor P <=> (P xor RC4(IV, Key)) xor P**

**<=> P xor (RC4(IV, Key) xor P)**

**<=> P xor (P xor RC4(IV, Key))**

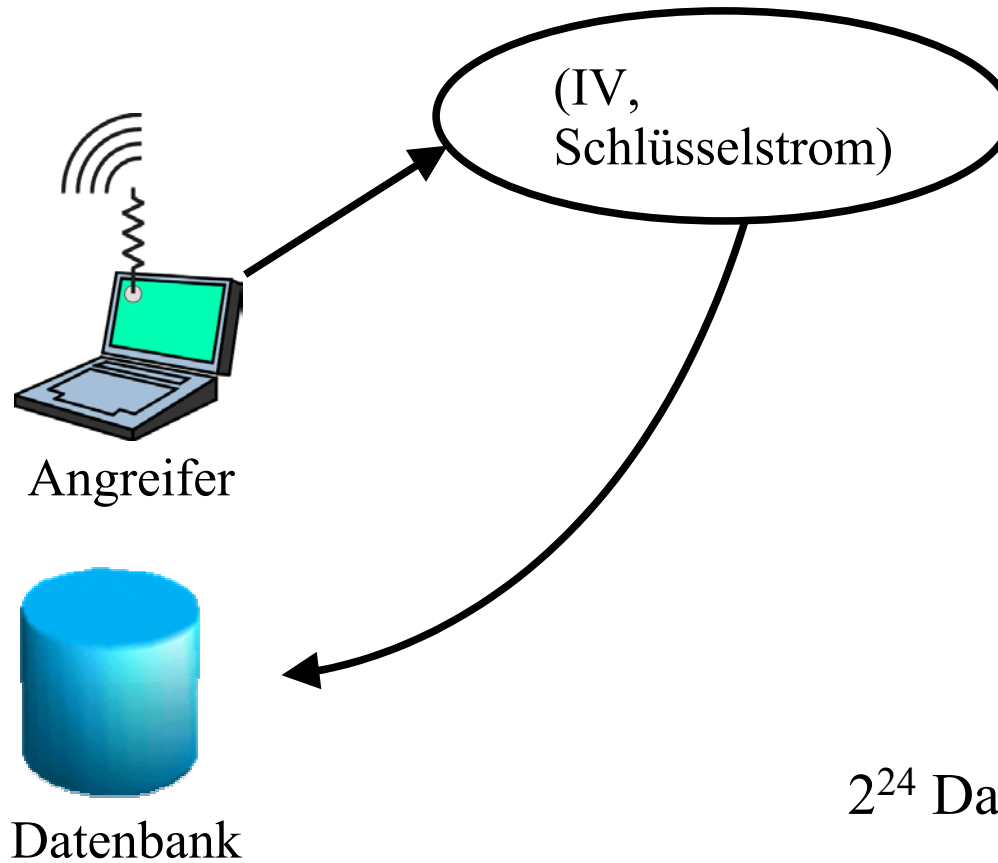
**<=> (P xor P) xor RC4(IV, Key)**

**<=> 0 xor RC4(IV, Key)**

**<=> RC4(IV, Key)**

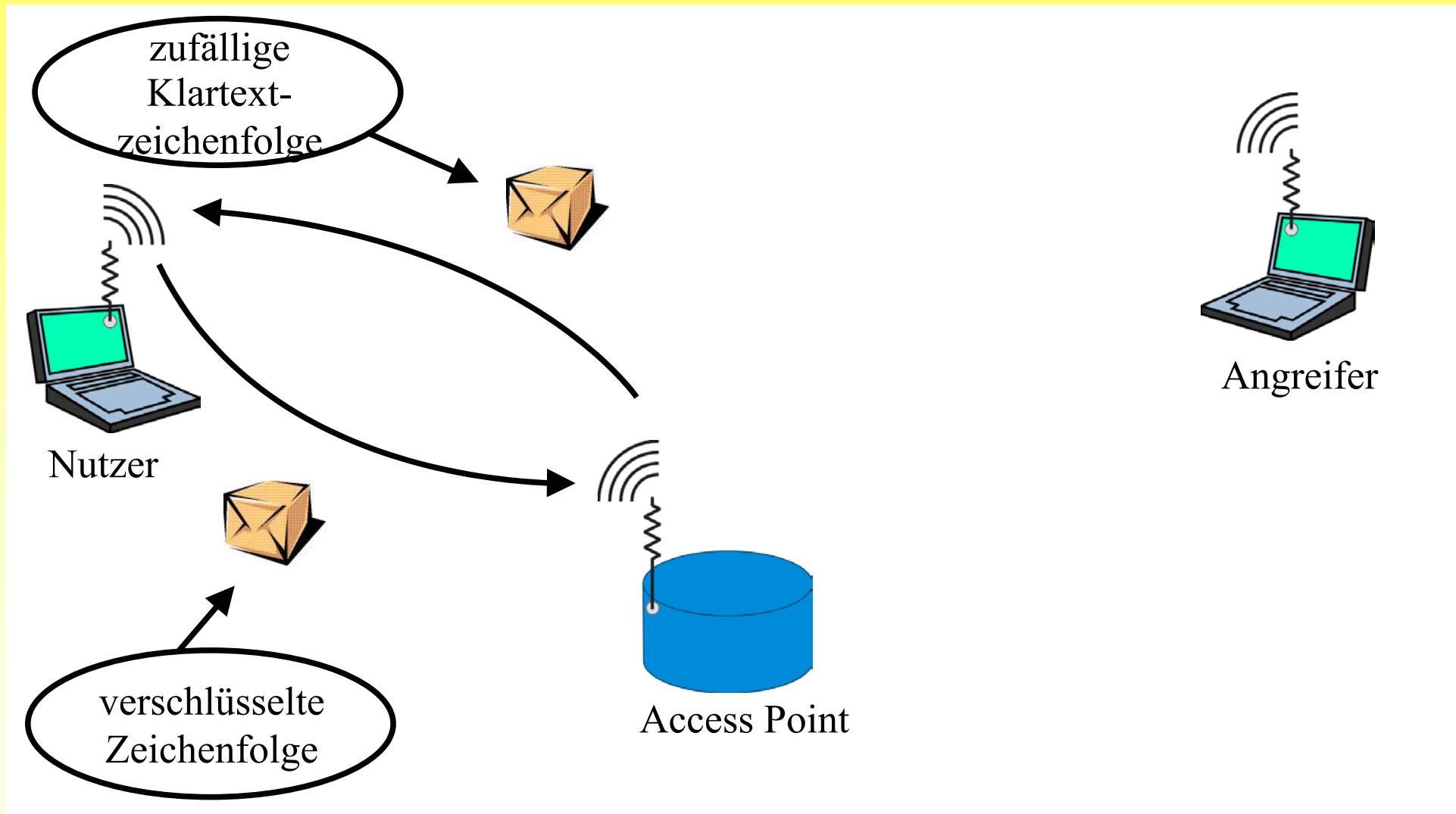
# Schwachstellen in den Sicherungsmechanismen

## Wired Equivalent Privacy Verschlüsselung

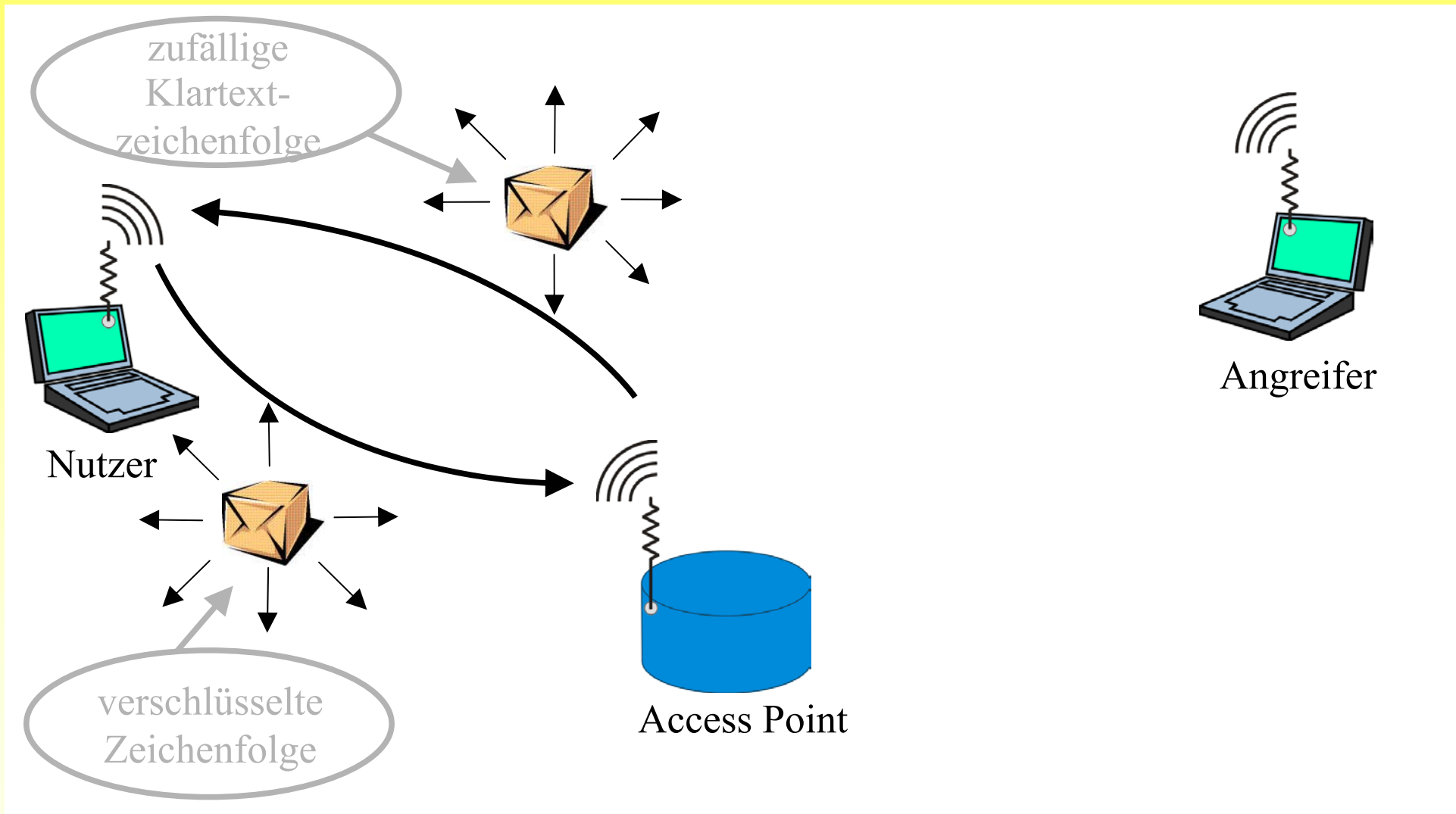


$2^{24}$  Datensätze  $\hat{=} 24\text{GB}$

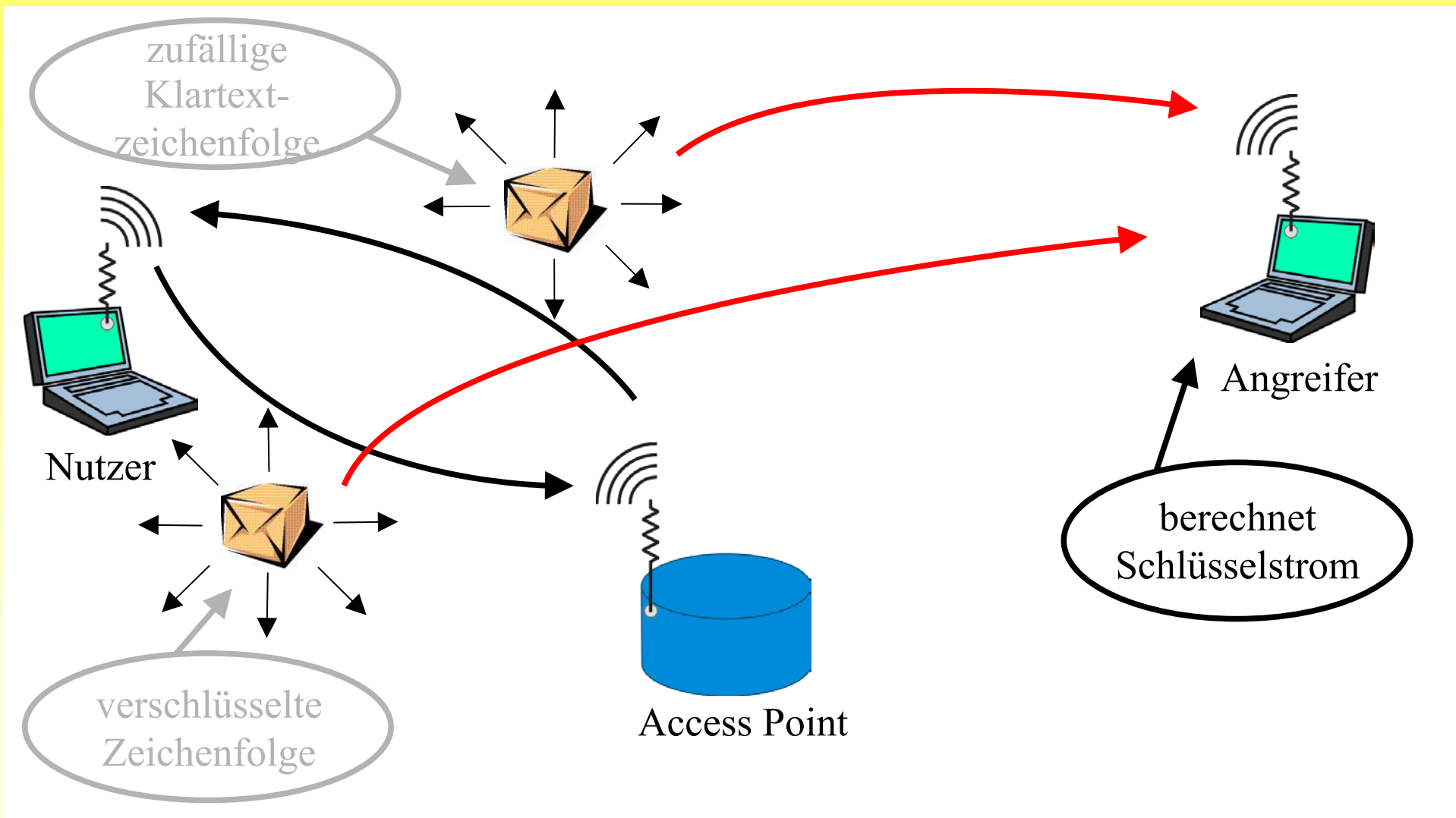
# Schwachstellen in den Sicherungsmechanismen Benutzerauthentifizierung (Shared Key)



# Schwachstellen in den Sicherungsmechanismen Benutzerauthentifizierung (Shared Key)

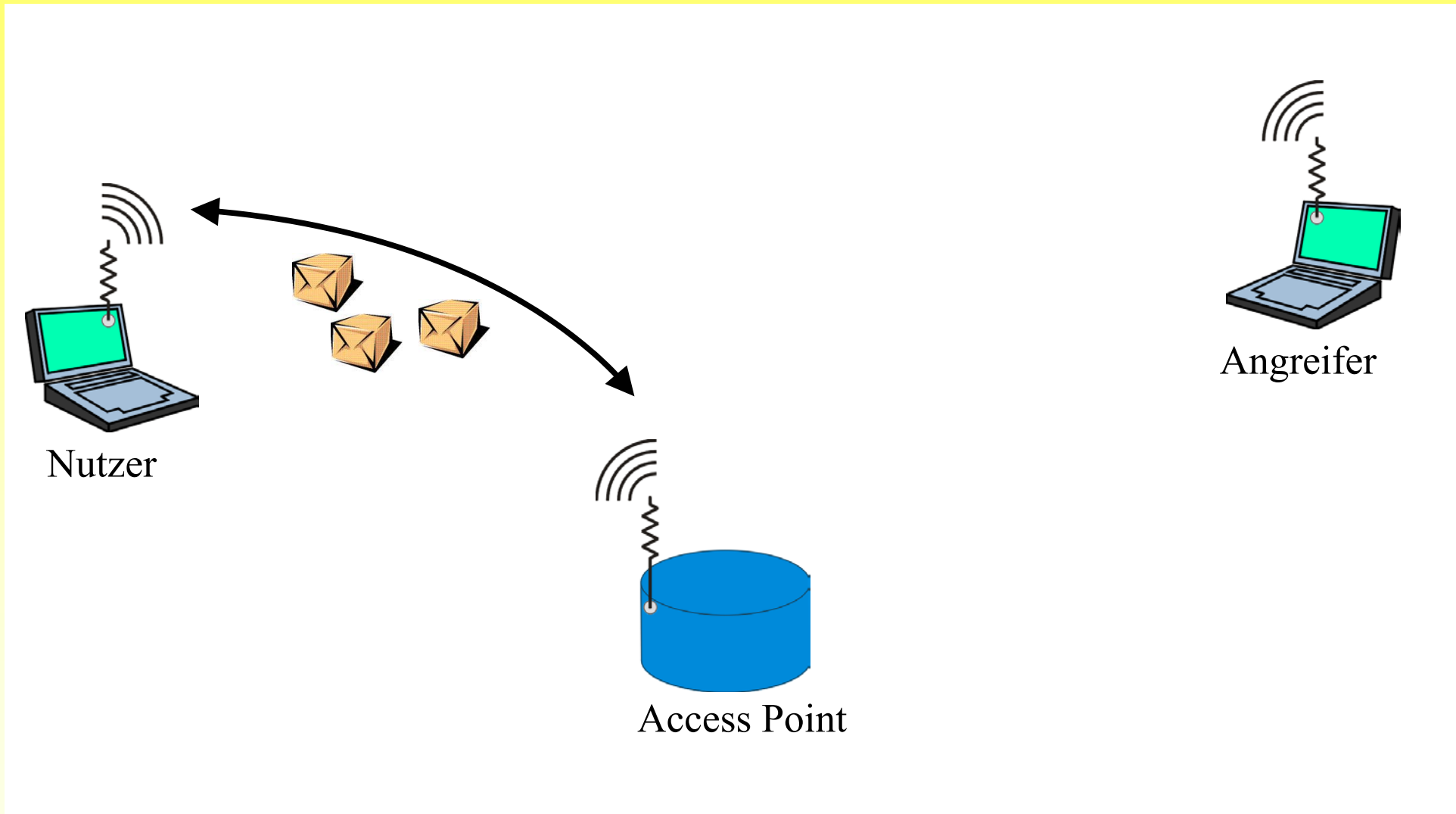


# Schwachstellen in den Sicherungsmechanismen Benutzerauthentifizierung (Shared Key)



# Schwachstellen in den Sicherungsmechanismen

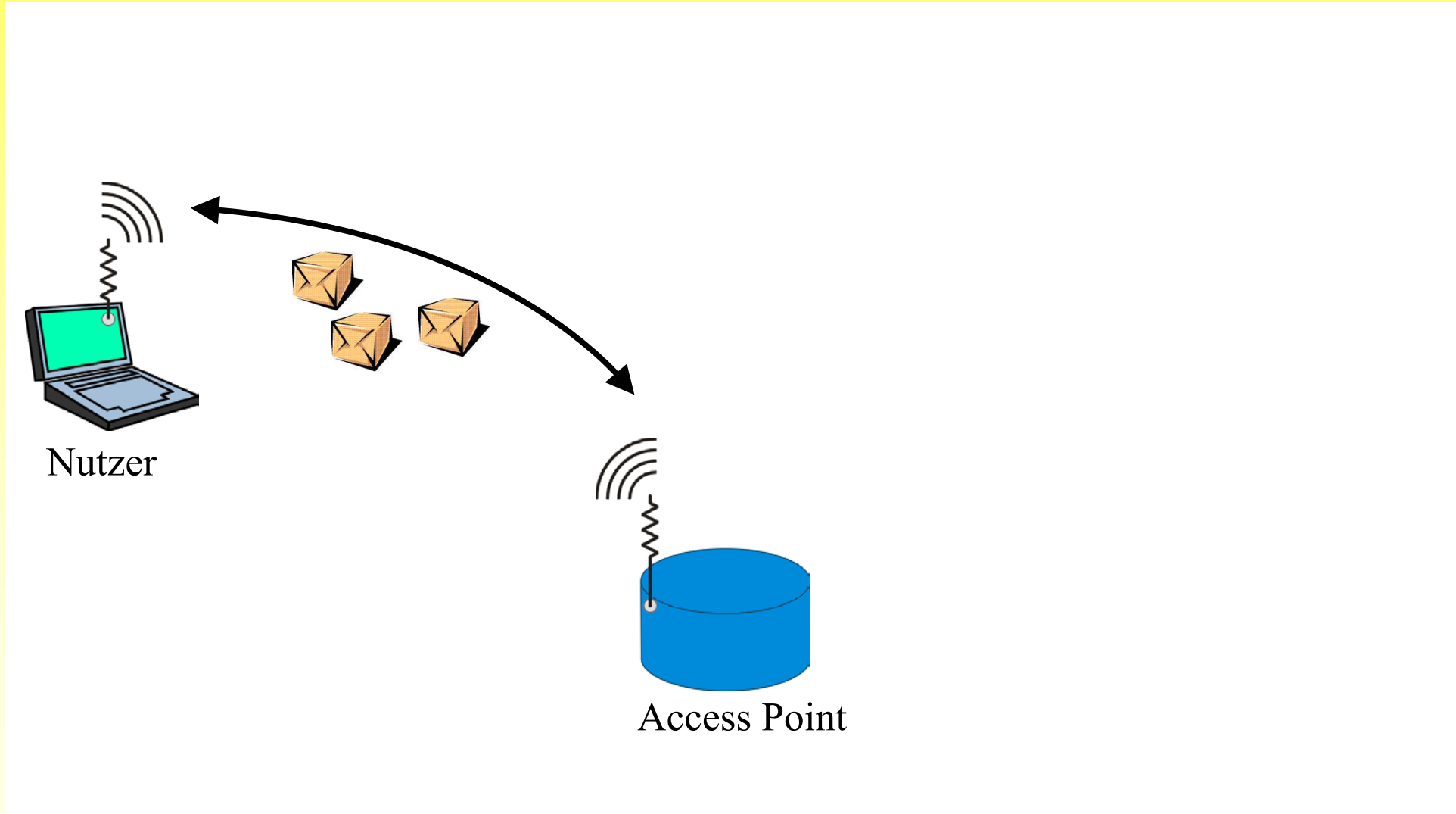
## Denial of Service





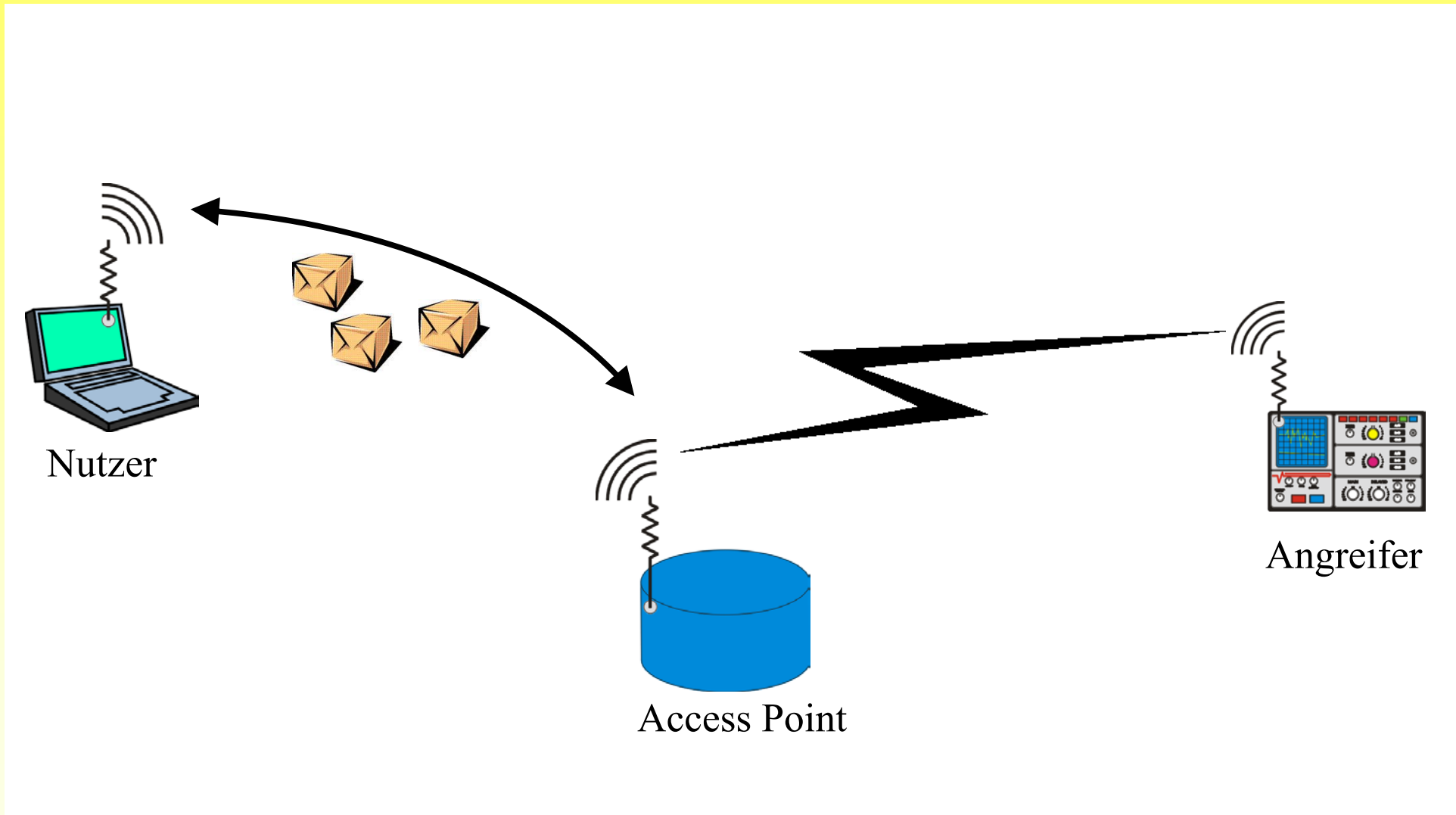
# Schwachstellen in den Sicherungsmechanismen

## Denial of Service



# Schwachstellen in den Sicherungsmechanismen

## Denial of Service



- Verschlüsselung auf höherer Ebene
- Verbesserungen am Standard IEEE 802.11
- IEEE 802.1X

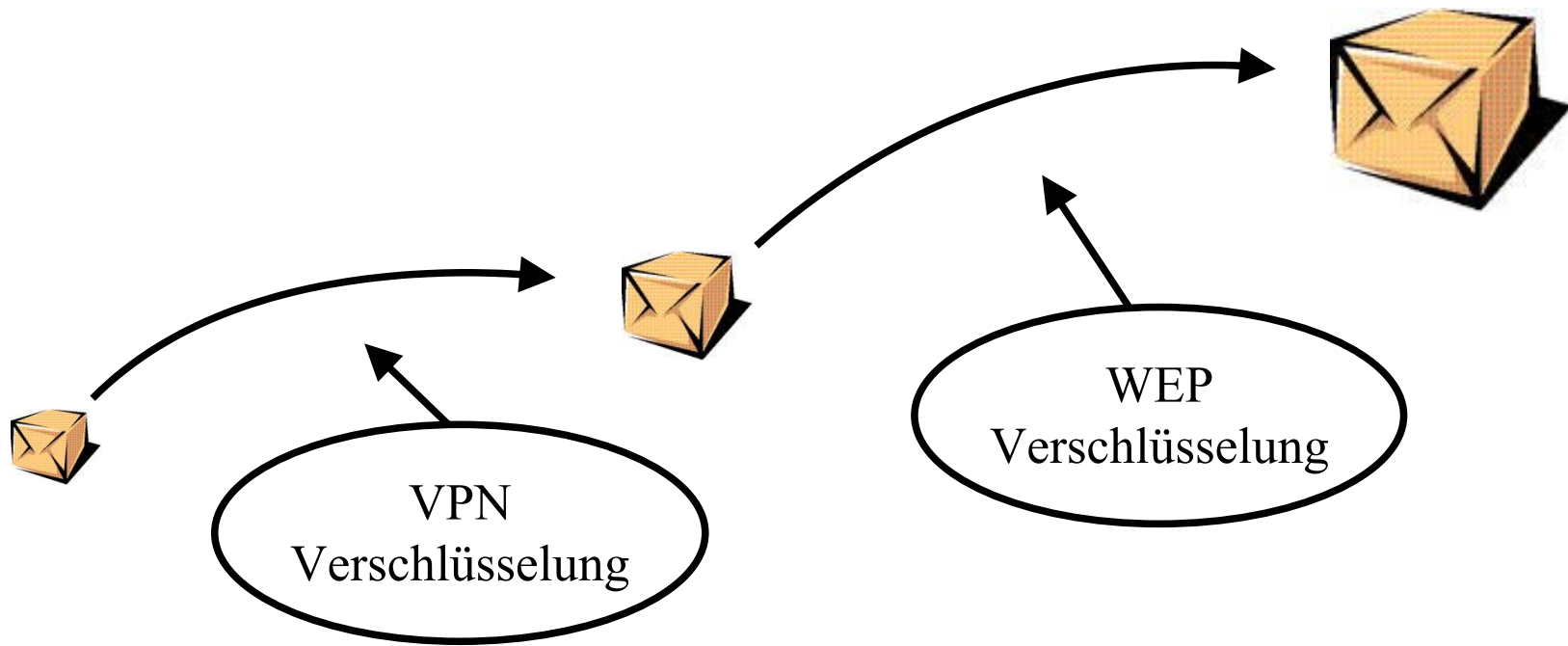
# Verbesserung der Sicherheit

## Verschlüsselung auf höherer Ebene

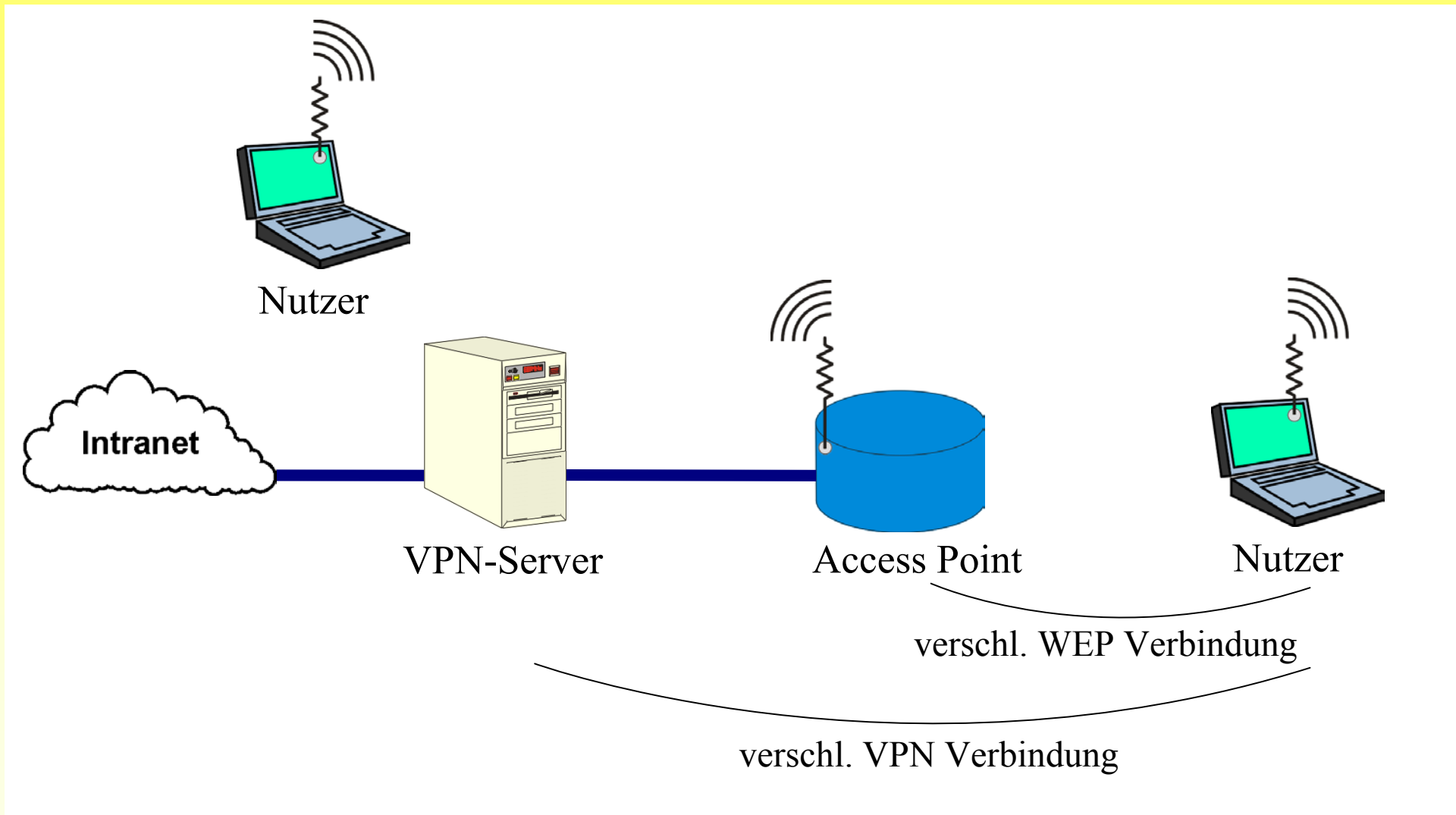
- Verschlüsselung wird über ein VPN realisiert
  - gebräuchliche Protokolle: PPTP, IPSec

# Verbesserung der Sicherheit Verschlüsselung auf höherer Ebene

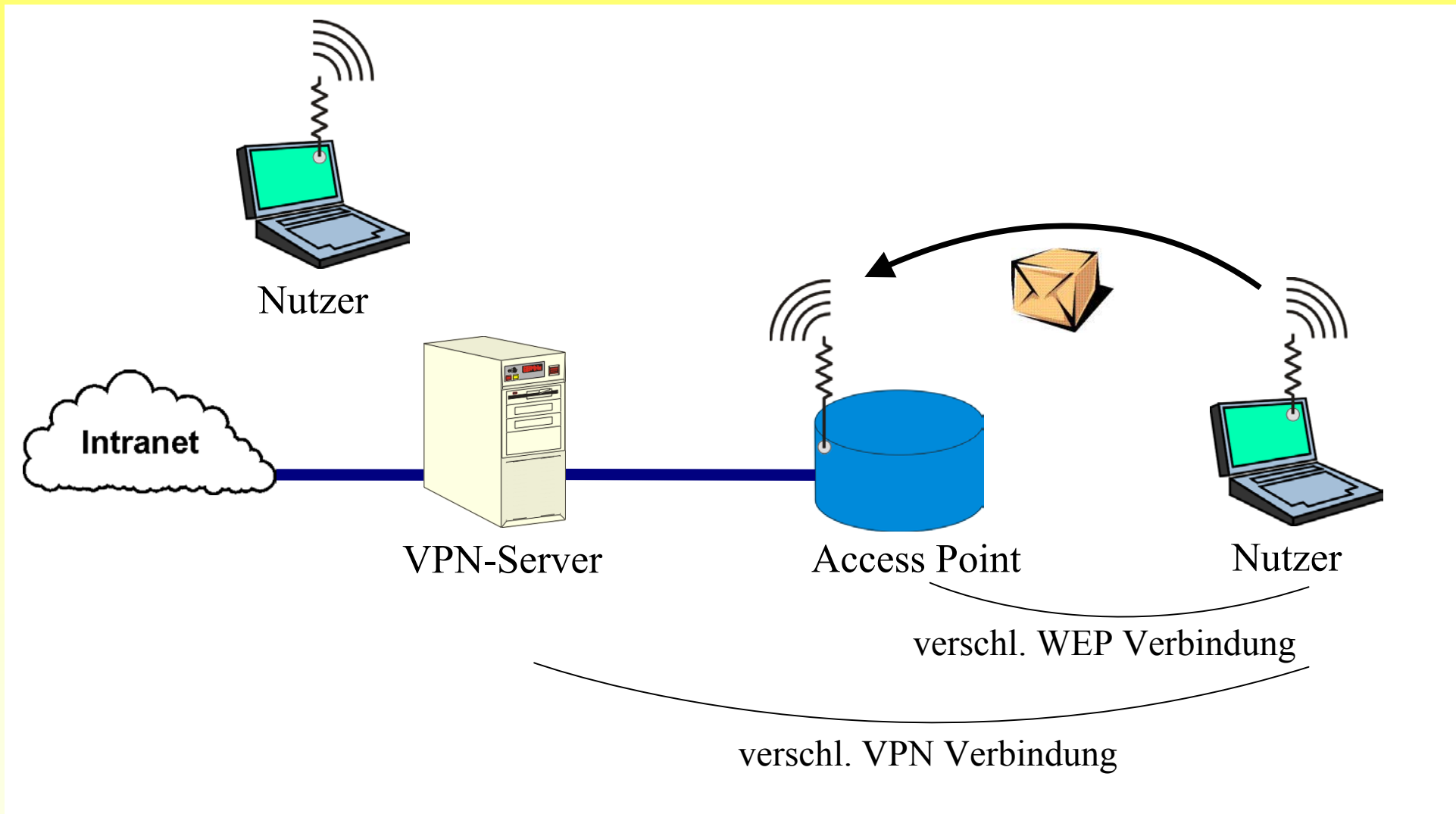
- Verschlüsselung wird über ein VPN realisiert
  - gebräuchliche Protokolle: PPTP, IPSec



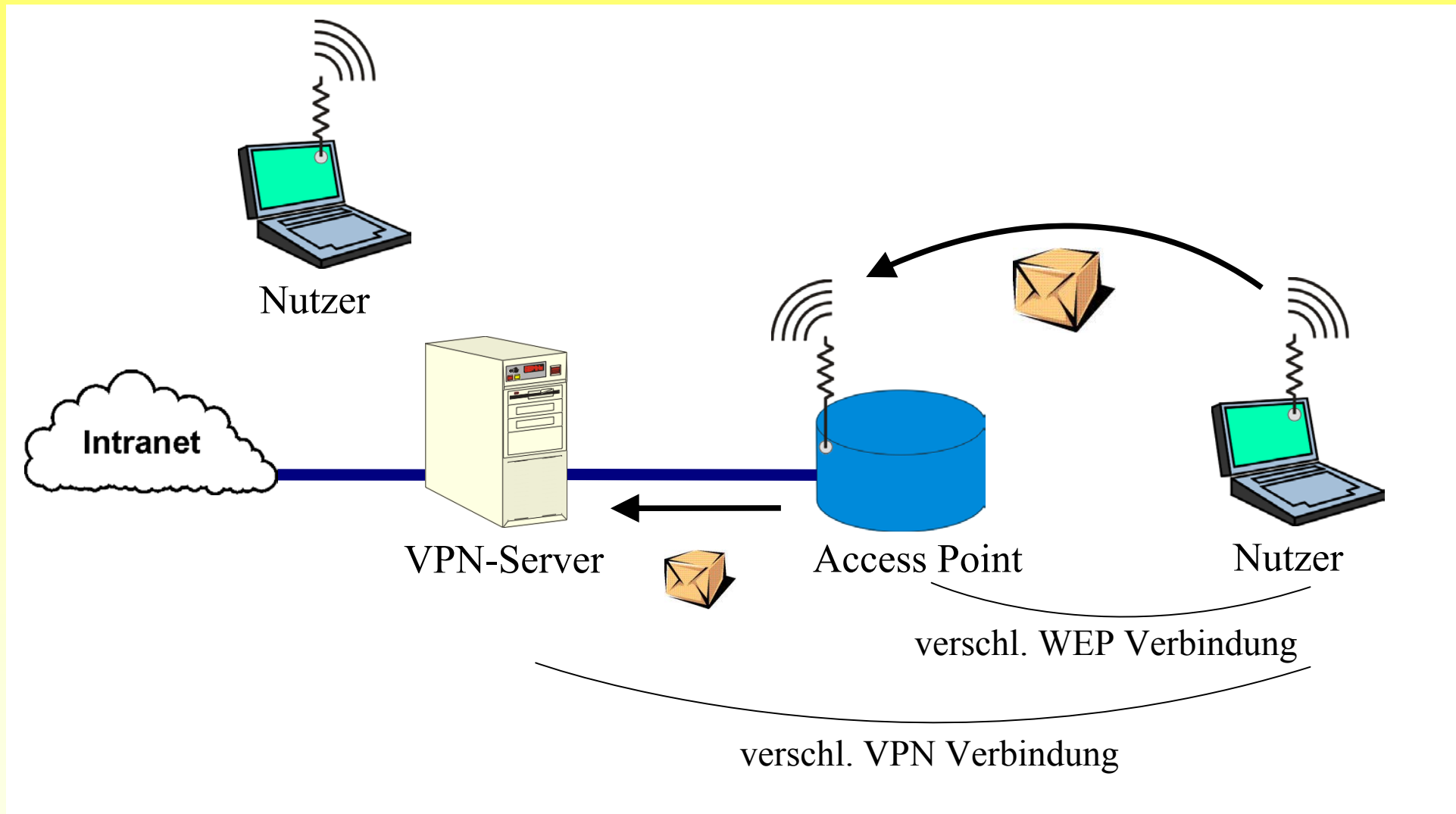
# Verbesserung der Sicherheit Verschlüsselung auf höherer Ebene



# Verbesserung der Sicherheit Verschlüsselung auf höherer Ebene

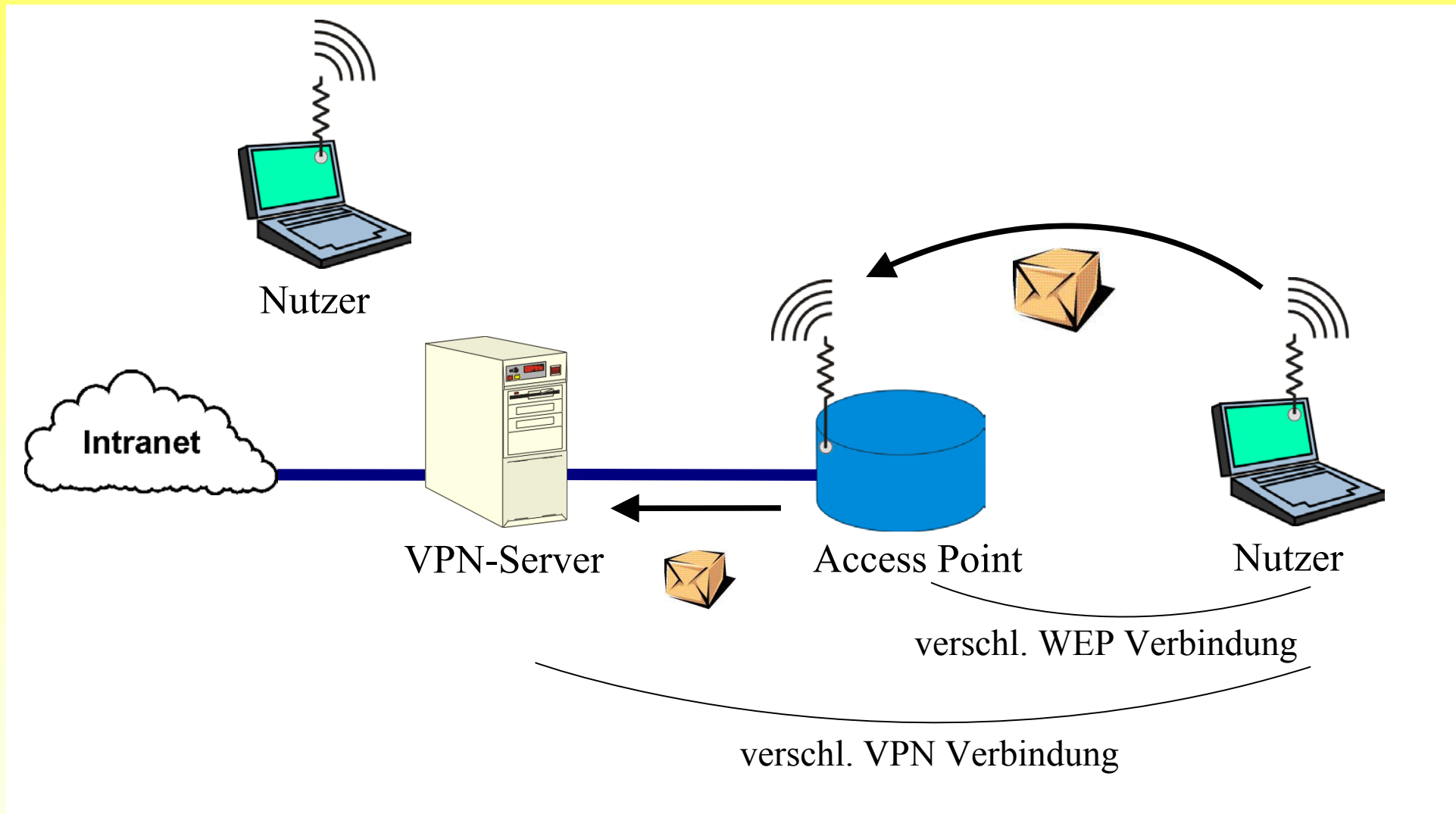


# Verbesserung der Sicherheit Verschlüsselung auf höherer Ebene

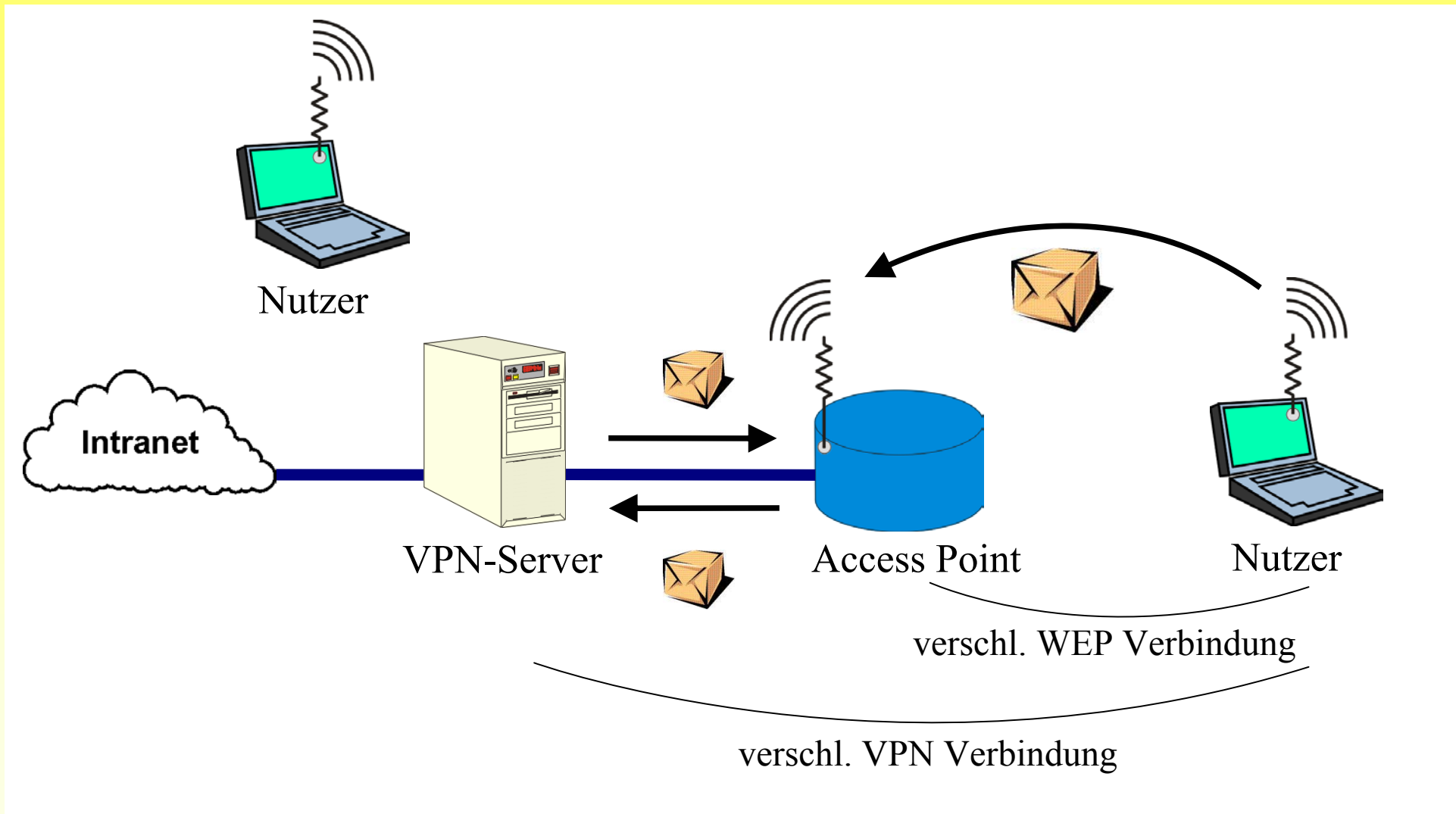




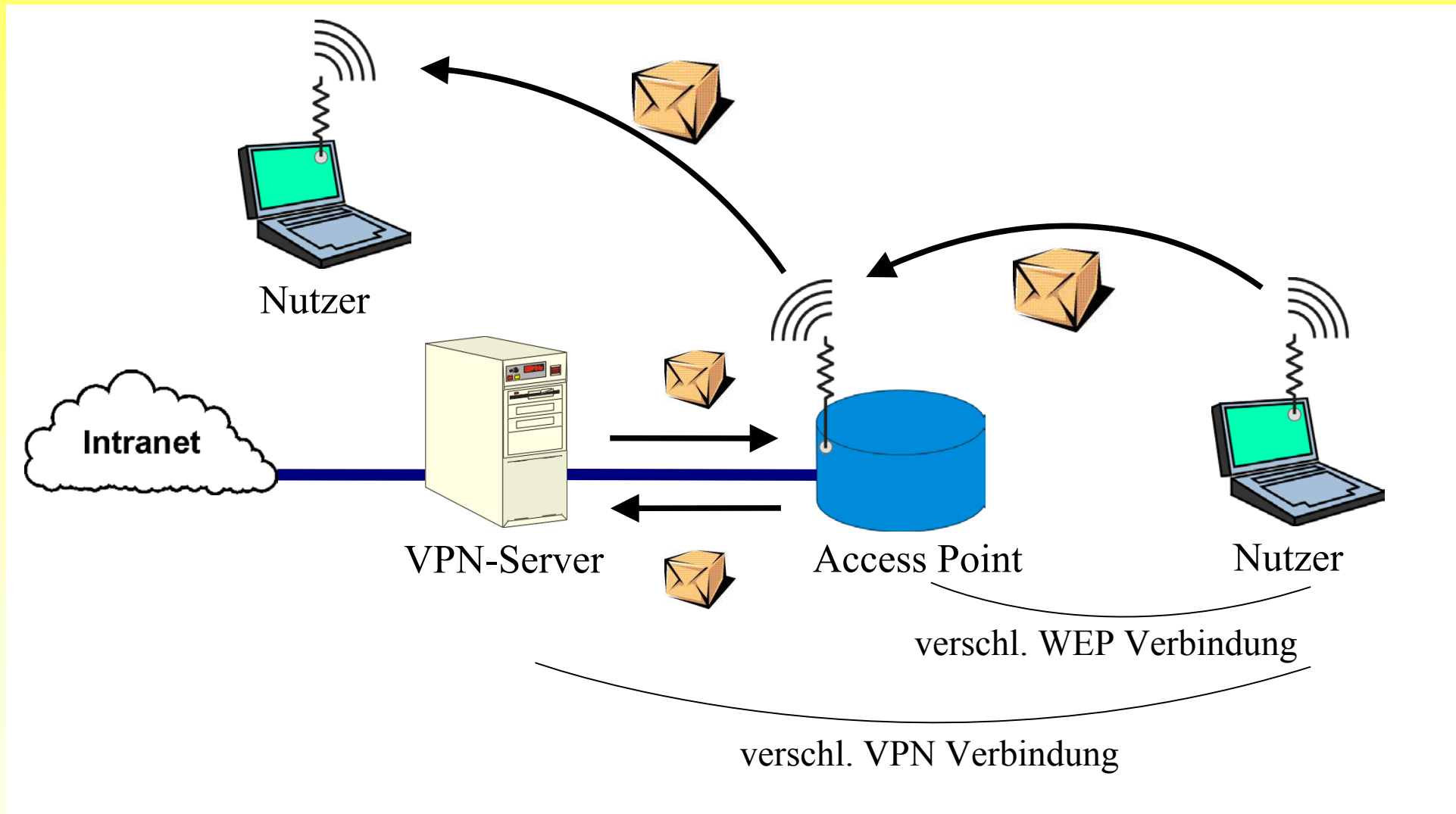
# Verbesserung der Sicherheit Verschlüsselung auf höherer Ebene



# Verbesserung der Sicherheit Verschlüsselung auf höherer Ebene



# Verbesserung der Sicherheit Verschlüsselung auf höherer Ebene



- Temporary Key Integrity Protocol (TKIP)

- Temporary Key Integrity Protocol (TKIP)
- Entwicklung eines neuen Sicherheitsstandard IEEE 802.11i
  - basiert auf IEEE 802.1X
  - vielfältige Authentifizierungsmechanismen
    - Benutzername und Paßwort
    - Zertifikate
    - SIM-Karte

- Temporary Key Integrity Protocol (TKIP)
- Entwicklung eines neuen Sicherheitsstandard IEEE 802.11i
  - basiert auf IEEE 802.1X
  - vielfältige Authentifizierungsmechanismen
    - Benutzername und Paßwort
    - Zertifikate
    - SIM-Karte
- neuer Verschlüsselungsalgorithmus: AES

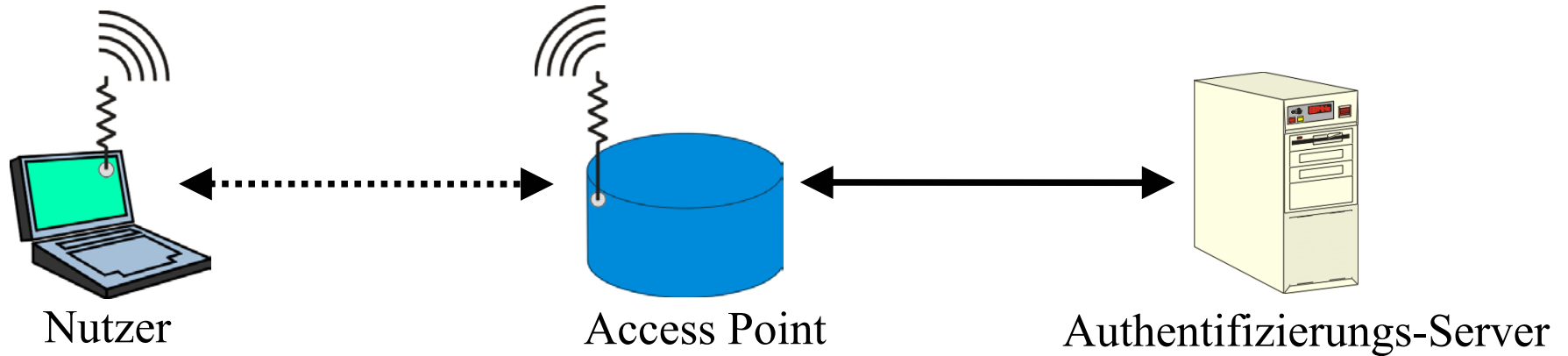
### Temporary Key Integrity Protocol

- Erweiterung des WEP-Standards
  - Verlängerung des Schlüssels
  - zusätzliche Sicherheitsmerkmale auf Paketebene
  - Algorithmus für regelmäßigen Schlüsselwechsel

# Verbesserung der Sicherheit

## Verbesserungen am Standard IEEE 802.11

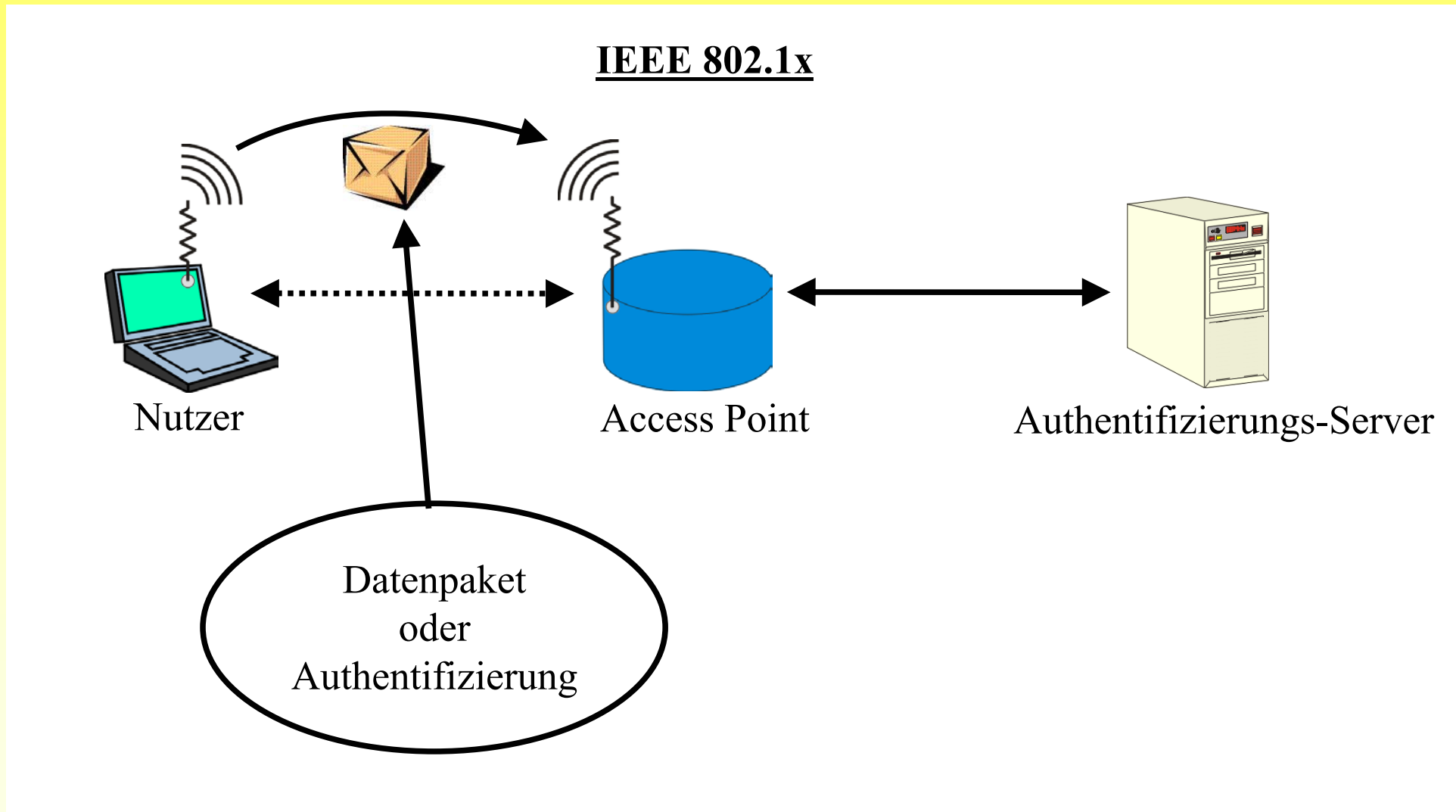
### IEEE 802.1x





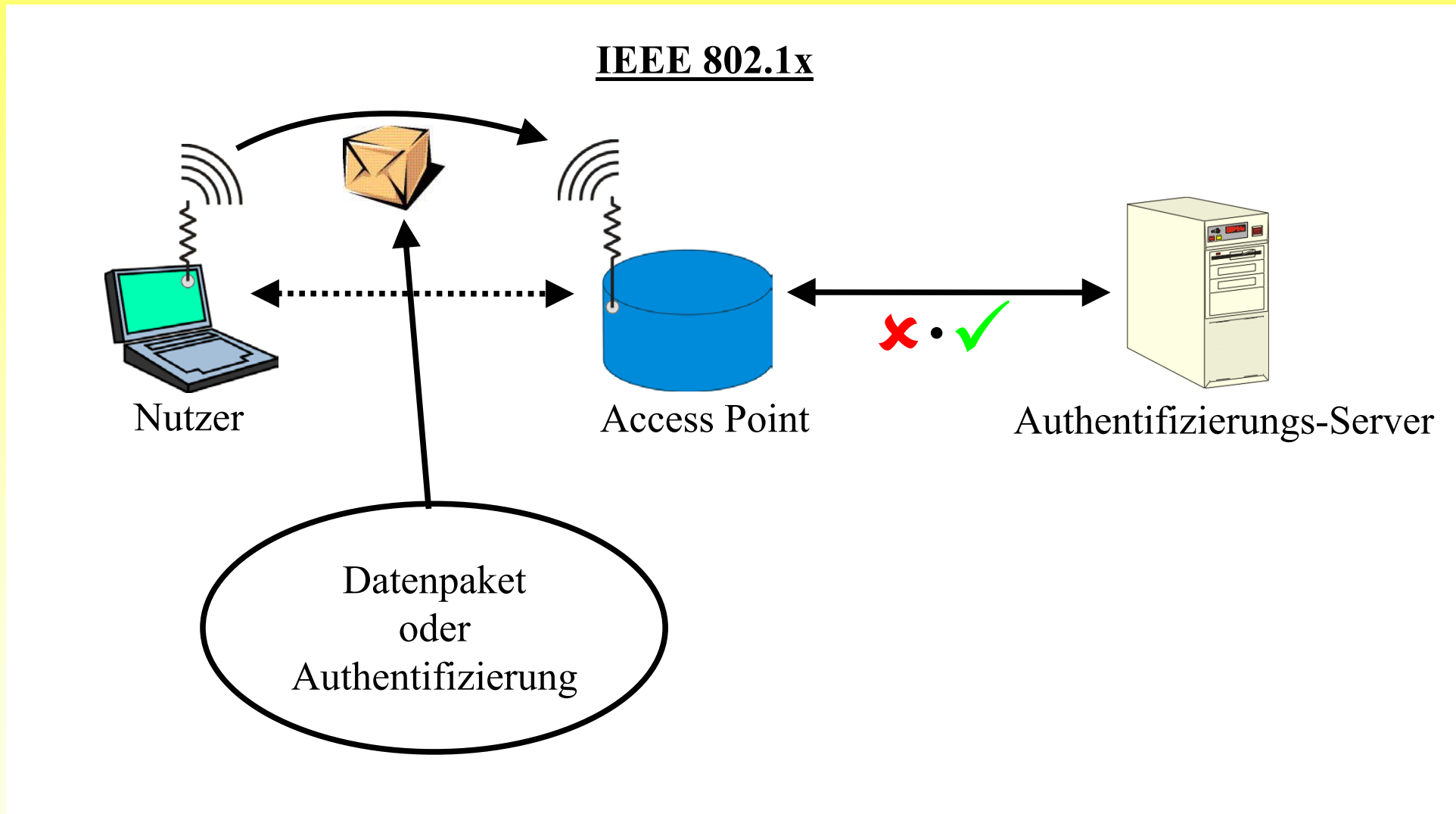
# Verbesserung der Sicherheit

## Verbesserungen am Standard IEEE 802.11



# Verbesserung der Sicherheit

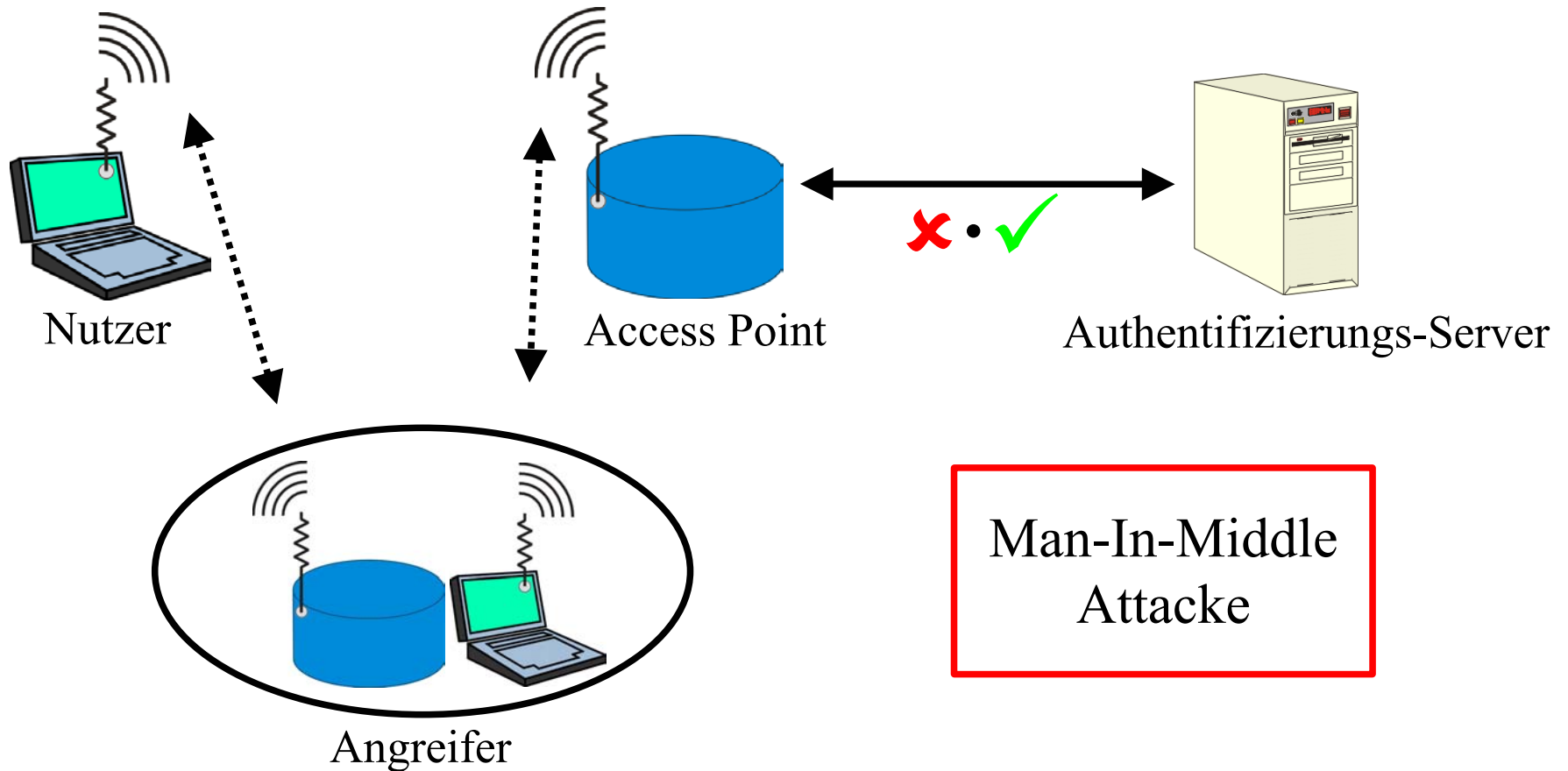
## Verbesserungen am Standard IEEE 802.11



# Verbesserung der Sicherheit

## Verbesserungen am Standard IEEE 802.11

### IEEE 802.1x



Man-In-Middle  
Attacke

- Sicherheitsmechanismen
  - Verstecken der ESSID ist nicht sicher
  - MAC Adressen Kontrollisten sind nicht sicher
  - WEP Verschlüsselung ist nicht sicher

- Sicherheitsmechanismen
  - Verstecken der ESSID ist nicht sicher
  - MAC Adressen Kontrollisten sind nicht sicher
  - WEP Verschlüsselung ist nicht sicher
  
- Neue Sicherheitsmechanismen noch nicht vollständig entwickelt
  - IEEE 802.1X ist angreifbar

- Sicherheitsmechanismen
  - Verstecken der ESSID ist nicht sicher
  - MAC Adressen Kontrollisten sind nicht sicher
  - WEP Verschlüsselung ist nicht sicher
  
- Neue Sicherheitsmechanismen noch nicht vollständig entwickelt
  - IEEE 802.1X ist angreifbar
  
- ↪ Sicherheit z.Zt. nur über VPN mittels IPSec gewährleistet