

# K1: Netz-Zugangskontrolle mit 802.1X und RADIUS

---

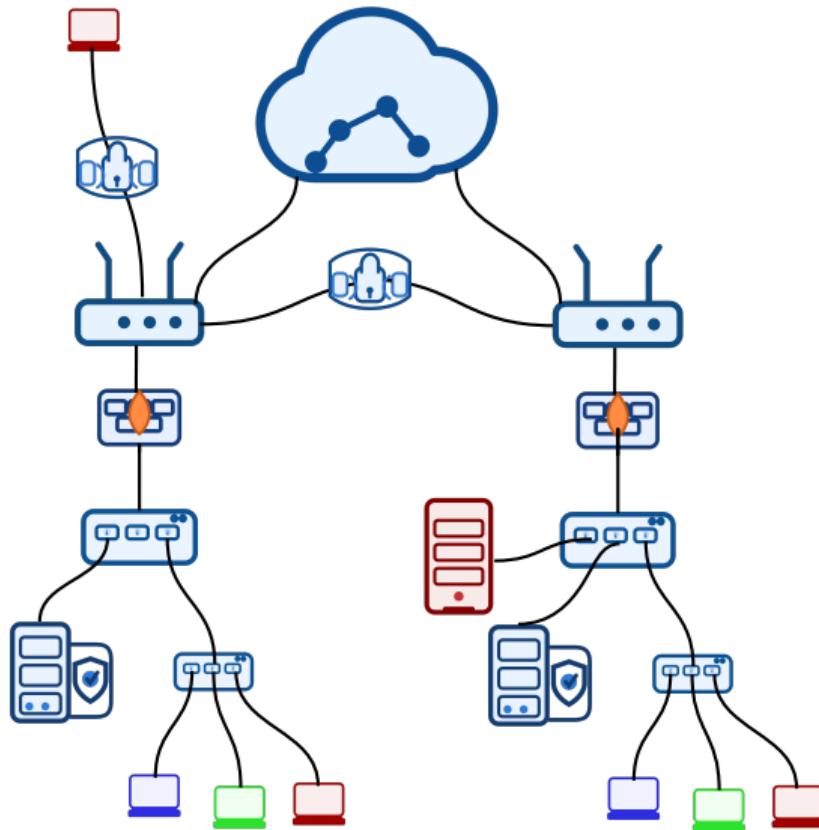
Christopher Scherb <[christopher.scherb@fhnw.ch](mailto:christopher.scherb@fhnw.ch)>

FHNW Hochschule für Technik

17. September 2025

## Attack Szenario

---



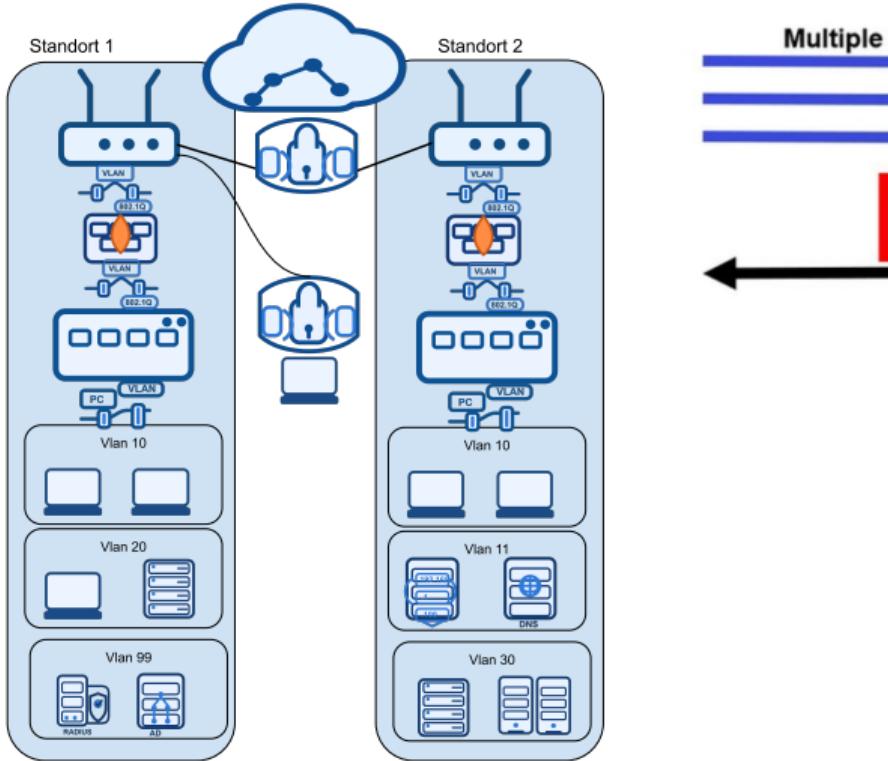
## Ziele und adressierte Bedrohungen

---

- ▶ **Zugriff kontrollieren:** Nur verifizierte Benutzer und Geräte dürfen produktive Netze erreichen.
- ▶ **Layer-2-Angriffe abwehren:** Rogue Devices, VLAN-Hopping, ARP/DHCP-Spoofing früh blockieren.
- ▶ **Lateral Movement begrenzen:** Dynamische VLANs, ACLs und Segmentierung verringern Ausbreitung im LAN.
- ▶ **Compliance sichern:** Policies für Gäste, BYOD und kritische Systeme nachweisbar durchsetzen.
- ▶ **Monitoring stärken:** Authentisierungs- und Policy-Entscheide zentral protokollieren und auswerten.

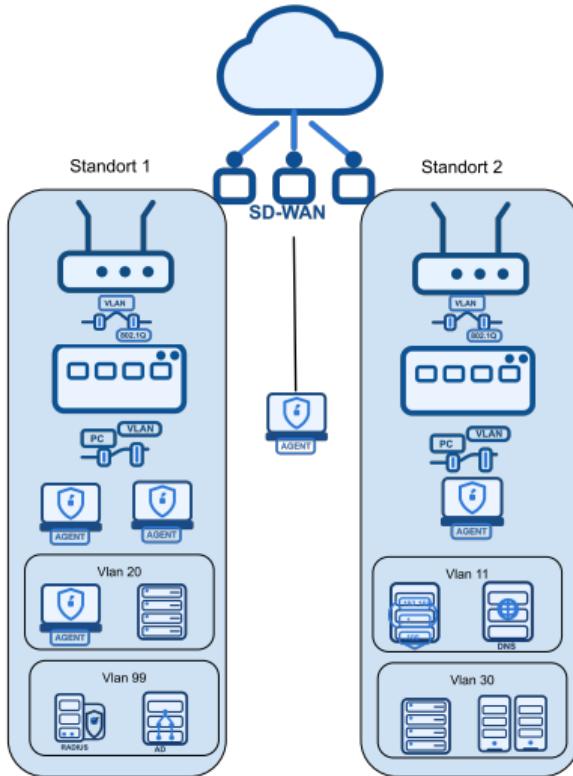
# Einordnung: Klassische Netzsicherheit

- NAC mit 802.1X und RADIUS setzt Identitäts- und Gerätekontrollen vor jeden Zugriff.
- Härtung von Layer-2 und WLAN verhindert Rogue Devices, VLAN-Hopping und Man-in-the-Middle.
- Firewalls, Segmentierung und Site-to-Site-VPNs schützen die produktiven Zonen und Services.
- Hands-on: FreeRADIUS-Deployment, dynamische VLAN-Zuordnung und OpenSense-Zonenaufbau.



# Sneak Peek: Moderne Netzwerk-Security

- ▶ Secure Access Service Edge verbindet Connectivity, Policy Enforcement und Inspection aus der Cloud.
- ▶ Security Service Edge stellt SWG, CASB und DLP für SaaS- und Webzugriffe bereit.
- ▶ Zero Trust Network Access ersetzt klassische VPNs durch identitäts- und kontextbasierte Sessions.
- ▶ Automatisierung und Telemetrie (SOAR, APIs) orchestrieren Reaktionen über Edge, Endpoint und Cloud.



# Motivation und Überblick

# Warum Network Access Control?

---

- ▶ Firmen-LANs sind keine vertrauenswürdigen Zonen mehr; Gerätezahl und Angriffsfläche wachsen kontinuierlich.
- ▶ **Ziel:** Gerätidentität überprüfen, bevor Zugriff auf produktive VLANs gewährt wird.
- ▶ NAC integriert Endpoint-Compliance, BYOD-Regeln und Gästezugang in einen einheitlichen Prozess.
- ▶ Kombination aus Richtlinien, Authentisierung und dynamischer Netzsegmentierung.

## Beispiel: Ungeschützter LAN-Port

---

- ▶ Meetingraum mit frei zugänglicher RJ45-Dose: unbekanntes Gerät verbindet sich mit dem internen LAN.
- ▶ Ohne 802.1X erhält der Port sofort vollen Layer-2-Zugriff auf produktive VLANs und Dienste.
- ▶ Angreifer kann DHCP/ARP-Spoofing ausführen oder sensible Systeme per SMB/RDP scannen.
- ▶ Incident Response kostet Zeit — NAC blockiert bereits beim Link-Up und erzwingt Authentisierung.



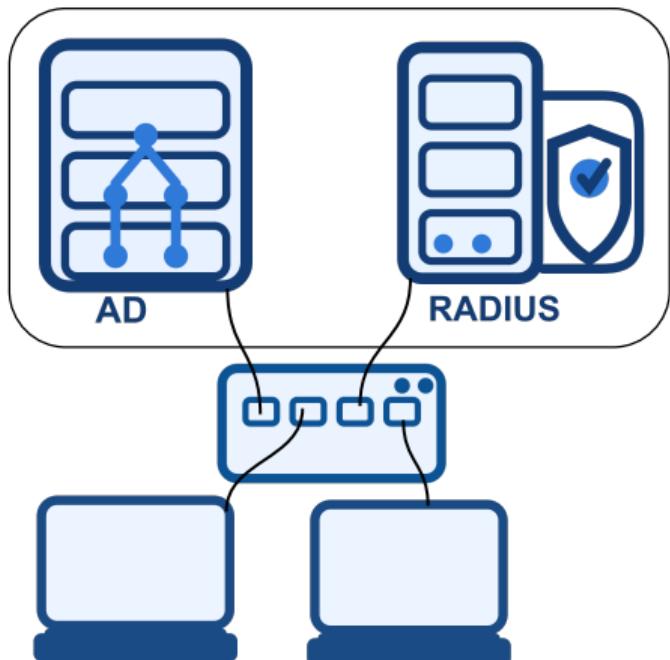
## Warum MAC-Based NAC nicht reicht

---

- ▶ MAC-Adressen laufen im Klartext in Broadcast- und ARP-Verkehr mit und lassen sich passiv mitschneiden.
- ▶ Ein `ip link set dev eth0 address <MAC>` klont die Adresse in Sekunden – ohne kryptografische Prüfung.
- ▶ Aktuelle Betriebssysteme rotieren ihre Private-MACs pro SSID/VLAN; Whitelists werden schnell veraltet oder zu weit gefasst.
- ▶ 802.1X mit Zertifikaten oder EAP-TLS liefert nachweisbare Identität und Policy-Attribute (VLAN, ACL, SGT).

# Kernkomponenten einer NAC-Lösung

- ▶ 802.1X-fähige Switches und WLAN-Controller agieren als Authenticator am Access Edge.
- ▶ RADIUS-Policy-Server übernimmt Authentisierung, Autorisierung und Accounting (AAA) **für Ports und Admin-Logins**.
- ▶ Identity Stores (AD/LDAP) liefern Benutzer-, Gruppen- und Geräteattribute.
- ▶ Posture-/MDM-Systeme ergänzen Compliance-Daten und stoßen Remediation an.



# Lifecycle einer 802.1X-Sitzung

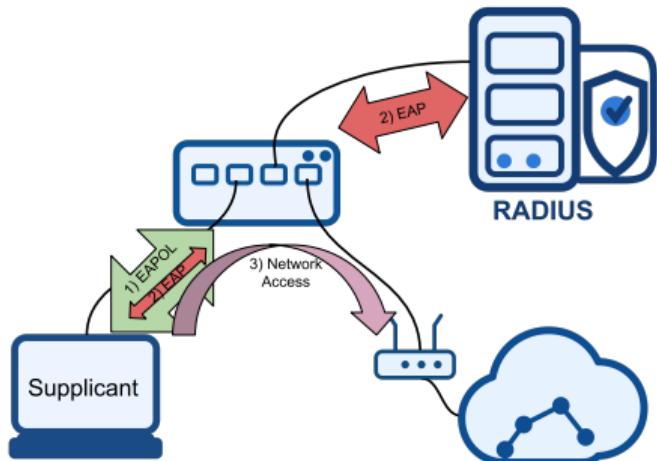
---

1. Port im **unauthorized**-State akzeptiert nur EAPOL.
2. Supplicant meldet sich beim Authenticator an und startet EAP-Aushandlung.
3. Authenticator kapselt EAP in RADIUS und fragt beim Server an.
4. Entscheidung (Accept/Reject) bestimmt VLAN-Zuordnung und ACLs.

# IEEE 802.1X im Detail

# Rollenmodell in 802.1X

- ▶ **Supplicant:** Endgerät mit EAP-Client (z.B. Windows, wpa\_supplicant).
- ▶ **Authenticator:** Switchport oder WLAN AP, kontrolliert den Link.
- ▶ **Authentication Server:** RADIUS, entscheidet über Zugang und Attribute.
- ▶ Kommunikation erfolgt über EAPOL (Layer 2, EtherType 0x888E).



## Port-Zustände und Steuerung

---

- ▶ **Unauthorized:** nur EAPOL erlaubt, Datenverkehr geblockt.
- ▶ **Authorized:** nach erfolgreicher Authentisierung, voller Datenpfad.
- ▶ Reauthentifizierung zyklisch oder ereignisgesteuert (Link-Down, VLAN-Änderung).
- ▶ MAB (MAC Authentication Bypass) als Fallback für Geräte ohne Supplicant.

# EAP-Verfahren im Überblick

---

- ▶ **EAP-TLS:** beidseitige Zertifikate, höchste Sicherheit.
- ▶ **EAP-PEAP:** TLS-Tunnel, innen MSCHAPv2; verbreitet für Benutzerkonten.
- ▶ **EAP-TTLS:** generischer Tunnel, flexibel für Legacy-Auth.
- ▶ **EAP-FAST:** Cisco-Variante mit Protected Access Credential (PAC).

## Ablauf EAP-TLS

---

1. Supplicant sendet **EAPOL-Start** an den Authenticator.
2. Authenticator fordert mit EAP-Request/Identity die Identität des Supplicants an.
3. Supplicant antwortet mit EAP-Response/Identity.
4. Authenticator kapselt die Identität in einen RADIUS Access-Request und leitet ihn an den RADIUS-Server weiter.
5. RADIUS-Server präsentiert sein Zertifikat und initiiert den TLS-Handshake.
6. Supplicant präsentiert sein Client-Zertifikat zur gegenseitigen Authentifizierung.
7. RADIUS verifiziert das Client-Zertifikat und sendet bei Erfolg Access-Accept inkl. MSK und VLAN/ACL-Attributen.
8. Authenticator sendet EAP-Success an den Supplicant.
9. Authenticator setzt den Port auf authorized und wendet die erhaltenen Policies an.

# RADIUS-Architektur

# AAA-Grundlagen

---

- ▶ **Authentication:** Wer bist du? Prüfung der Identität über Credentials, Zertifikate oder Tokens.
- ▶ **Authorization:** Was darfst du? Ableitung von Zugriffen, VLANs oder ACLs aus Richtlinien.
- ▶ **Accounting:** Was hast du getan? Protokollierung von Sitzungsbeginn, Dauer, Datenvolumen.
- ▶ AAA bildet die Basis für nachvollziehbare und steuerbare Netzwerkzugriffe.

## AAA mit RADIUS

---

- ▶ **Authentication:** Prüfung von Credentials via Backend (AD, Zertifikate, Kerberos).
- ▶ **Authorization:** Zuweisung von VLAN, ACL, QoS-Profil über RADIUS-Attribute.
- ▶ **Accounting:** Sitzungsstart/-ende, Datenvolumen für Compliance.
- ▶ Policy Engine setzt kontextbasierte Regeln um (z.B. Endpoint-Gruppe, Uhrzeit).

## RADIUS Grundprinzip

---

- ▶ UDP-basiert (Ports 1812/1813), Request/Response-Modell.
- ▶ Nutzdaten in AVPs (Attribute Value Pairs), klar strukturiert.
- ▶ Shared Secret schützt Integrität, TLS-Variante (RadSec) für Transportverschlüsselung.
- ▶ Erweiterbar durch Vendor-Specific Attributes (VSA).

## RADIUS-Attribut-Beispiele

---

- ▶ Tunnel-Type (64) = VLAN (13), Tunnel-Medium-Type (65) = IEEE-802 (6), Tunnel-Private-Group-ID (81) = 20 für VLAN-Zuordnung.
- ▶ Filter-Id zur Zuweisung vordefinierter ACLs.
- ▶ Session-Timeout erzwingt Reauthentisierung nach Zeit X.
- ▶ Class oder Vendor-Attribute für Policy-Metadaten (z.B. Rollen-ID).

# Standardattribute im Access-Accept

Attribute	Funktion
Tunnel-Type (64) VLAN (13)	= Aktiviert VLAN-Tunnel (Ethernet).
Tunnel-Medium-Type (65) = IEEE-802 (6)	Gibt Medium des Tunnels an.
Tunnel-Private-Group-ID (81)	VLAN-ID für den Port (z.B. 10).
Filter-Id (11)	Verweist auf ACL- oder Policy-Set auf dem Switch.
Session-Timeout (27)	Startet Reauthentisierung nach X Sekunden.

## Beispiel Access-Accept

```
Tunnel-Type := VLAN,  
Tunnel-Medium-Type := IEEE-802,  
Tunnel-Private-Group-ID := "20",  
Filter-Id := "ACL-Employees",  
Session-Timeout := 28800
```

# Vendor Specific Attributes (VSA)

Hersteller	VSA Zweck
Cisco	Cisco-AVPair='ip:dacl=Allow-Users' für Downloadable ACLs. Cisco-AVPair='vlan-id=20' oder 'ssid=Corp' für VLAN/WLAN-Policies.
HPE/Aruba	Aruba-User-Role setzt rollenbasierte Firewall- Policies.
Microsoft NPS	MS-Quarantine-IPFilter für Quarantäne-Netz.

## Beispiel Cisco VSA

```
Cisco-AVPair := 'shell:priv-lvl=15',
Cisco-AVPair += 'url-redirect=https://portal',
```

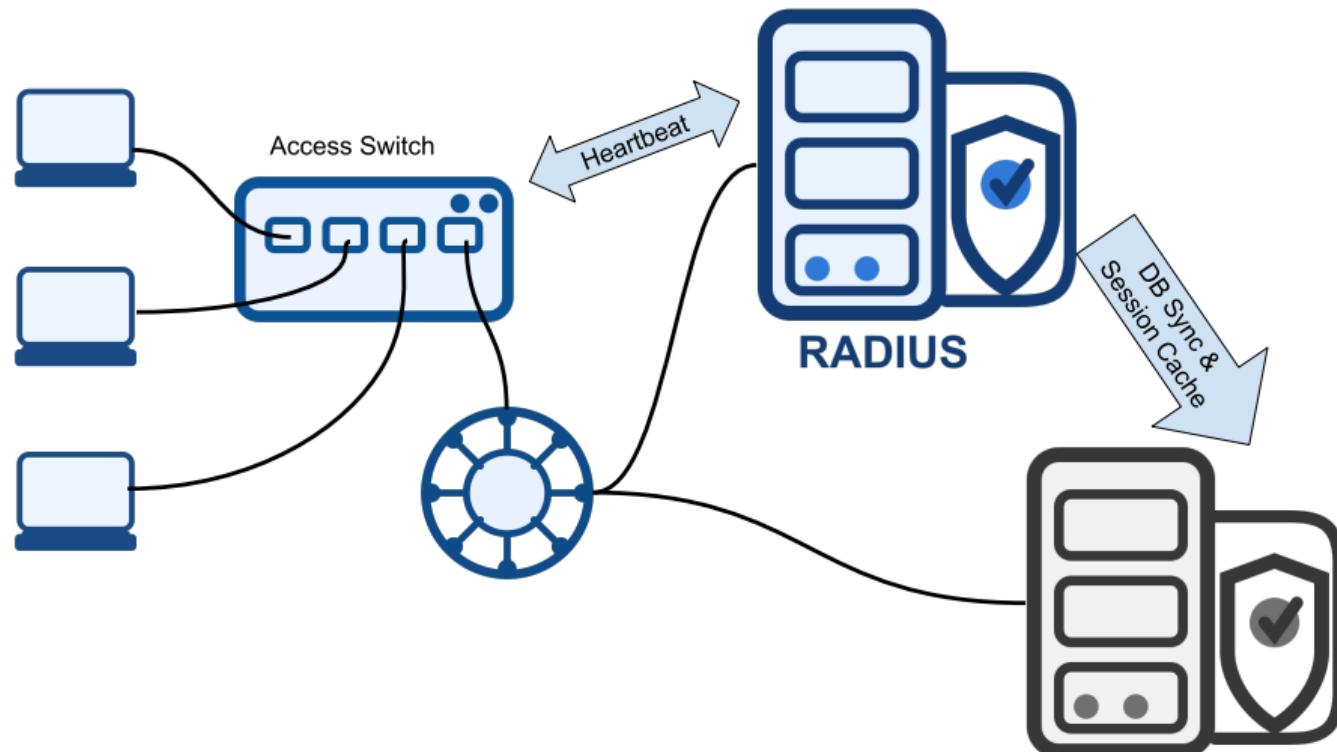
VSA erlauben granularen Zugriff auf Herstellerfunktionen – immer dokumentieren und

## Redundanz und Ausfallsicherheit

---

- ▶ Mehrere RADIUS-Server im Round-Robin- oder Active/Standby-Design.
- ▶ Nutzung von Keepalived/VRRP für virtuelle IPs.
- ▶ Datenbank-Backend redundant (MySQL/LDAP Master-Master).
- ▶ Device-Profile synchronisieren (z.B. via Git & CI/CD).

# RADIUS Active/Standby Topologie



# Richtlinien und NAC-Design

## Policy-Design Leitlinien

---

- ▶ Kategorien: Nutzerrollen, Gerätetypen, Standort, Tageszeit.
- ▶ Start mit wenigen, klaren Policies und kontrolliertes Wachstum.
- ▶ Konflikte mit Prioritäten oder bedingten Ausdrücken auflösen.
- ▶ Dokumentation der Entscheidungsbäume für Betrieb und Audits.

# Implementierungsschritte

# Projektphasen

---

1. Ist-Analyse: Gerätelinventar, vorhandene Identity Stores, Netzsegmente.
2. Pilot: Wenige Switches, dediziertes VLAN, begrenzte Benutzergruppe.
3. Rollout: Automatisierung via Templates, Change-Management beachten.
4. Betrieb: Monitoring, Reporting, regelmäßige Policy-Reviews.

# Integration in Cisco-Infrastruktur: AAA-Basis

---

## 1. AAA-Grundkonfiguration: aaa new-model

```
aaa authentication dot1x default group radius
```

```
aaa authorization network default group radius
```

```
RADIUS-Server definieren: radius server FREERADIUS address ipv4 10.10.10.20  
auth-port 1812 acct-port 1813 key SuperSecret  
optional radius-server vsa send accounting für dACLs.
```

## 2. 802.1X & CoA global aktivieren: dot1x system-auth-control, aaa server radius dynamic-author client 10.10.10.20 server-key SuperSecret.

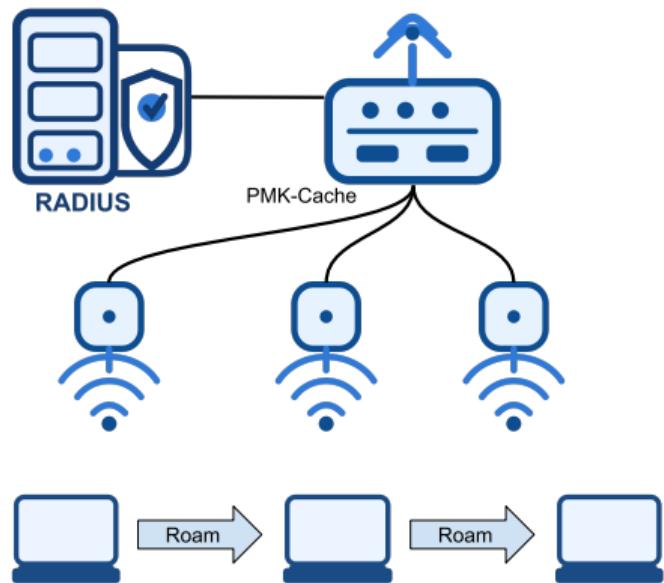
## Integration in Cisco-Infrastruktur: Access-Ports

---

3. Access-Port Beispiel: interface Gi1/0/11, switchport mode access, authentication port-control auto, optional mab, spanning-tree portfast.
4. Access-Accept: VLAN-Attribute Tunnel-Type = VLAN, Tunnel-Private-Group-ID = "20"; optional Cisco-AVPair = 'ip:dacl=Allow-Users'; CoA für Policy-Wechsel.

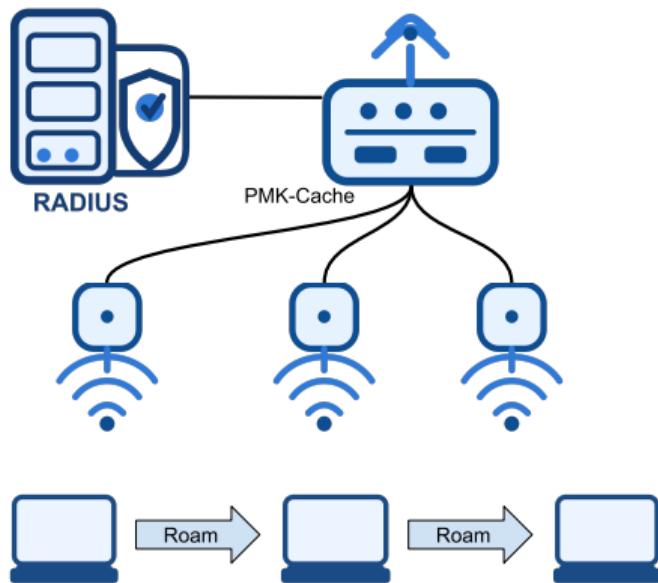
# Wireless NAC: Schlüsselaufbau

- WLAN-Controller agiert als Authenticator und startet den 802.11i 4-Way-Handshake nach erfolgreichem EAP.
- **PMK (Pairwise Master Key):** Aus dem EAP MSK abgeleitet; bleibt im Controller-Cache für erneute Verbindungen.
- **4-Way-Handshake:** Supplicant- und AP-Nonces + PMK → PTK; Schritt 3 überträgt den Group Temporal Key (GTK).
- Schlüsselhierarchie: PMK → PTK (Unicast) / GTK (Broadcast) → temporäre Sitzungsschlüssel im Access Point.



# Wireless NAC: Policy & Roaming

- ▶ Policy-Pakete kombinieren SSID, RADIUS-Profil, VLAN-/ACL-Zuweisung und QoS-Einstellungen.
- ▶ PMK-Cache, Opportunistic Key Caching (OKC) oder 802.11r Fast Transition beschleunigen das Roaming.
- ▶ Gast-/BYOD-Flows nutzen Captive Portal mit RADIUS Redirect; temporäre VLANs/ACLs werden per CoA aktualisiert.
- ▶ Monitoring: EAP-Fehlercodes, 802.11i-Key-Events und Session-Idle-Timer im Controller beobachten.



## Roaming und Sicherheit

---

- ▶ 802.11r/FT konfiguriert schnelle BSS-Transitions; 802.11k/v verbessern AP-Auswahl.
- ▶ PMKID-Cache oder Opportunistic Key Caching reduziert RADIUS-Last bei Bewegung.
- ▶ WPA3-Enterprise mit 192-bit Suite B für sensible Netze; Protected Management Frames (PMF) Pflicht.
- ▶ Monitoring: EAP-Timer, Failure-Reasons im WLC/RADIUS prüfen, dediziertes WLAN-Logging.

# Monitoring und Troubleshooting

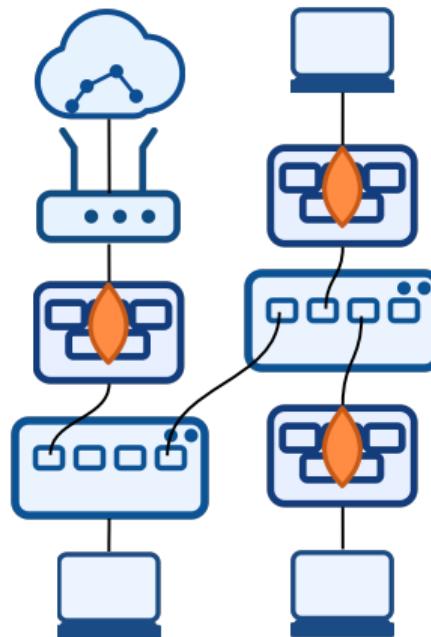
---

- ▶ RADIUS Debugging: freeradius -X im Testmodus.
- ▶ Switch: show authentication sessions interface Gi1/0/5 details.
- ▶ Packet Captures von EAPOL (Wireshark Filter eapol).
- ▶ Log-Korrelation mit SIEM (z.B. Splunk, Elastic) für Audit Trails.

# Härtung von Netzwerkelementen

# Defense-in-Depth: Architektur

- ▶ Schutzebenen für Access, Distribution und Core festlegen – jede Ebene erhält eigene Kontrollen.
- ▶ Segmentierung über Firewalls, VRFs und dynamische VLANs begrenzt Laterale Bewegungen.
- ▶ Herstellerdiversität reduziert das Risiko gemeinsamer Schwachstellen.



# Defense-in-Depth: Prozesse

---

- ▶ Sicherheitsrichtlinien der Geschäftsleitung definieren Freigaben, Reporting und Eskalationen.
- ▶ Regelmäßige Penetrationstests und Architektur-Reviews halten Kontrollen aktuell.
- ▶ Incident-Playbooks und Übungen stellen sicher, dass Teams schnell reagieren können.



# Physischer Schutz: Infrastruktur

---

- ▶ Zutrittskontrollen für Racks und Technikräume, inklusive Protokollierung.
- ▶ Video- und Umgebungsüberwachung (Temperatur, Wasser, Rauch) frühzeitig alarmieren.
- ▶ Kabelführungen und Patchfelder dokumentieren, um Manipulationen zu erkennen.



# Physischer Schutz: Betrieb

---

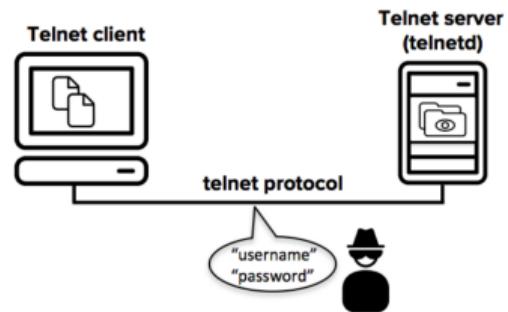
- ▶ Redundante Stromversorgung und Klimatisierung für kritische Standorte bereitstellen.
- ▶ Ersatzhardware, Konsolenadapter und Dokumentation in Reichweite lagern.
- ▶ Out-of-Band-Managementwege testen und in Incident-Playbooks hinterlegen.



## Lokale Zugänge: Dienste abschalten

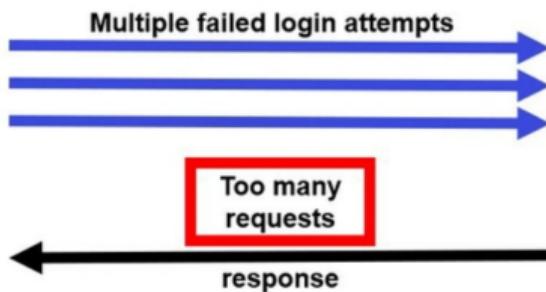
---

- ▶ Verwaltungsdienste ohne Verschlüsselung deaktivieren (HTTP, Telnet, AUX-Konsolen).
- ▶ Konsolen nur für Break-Glass-Szenarien freigeben und regelmäßig prüfen.
- ▶ Standardbanner setzen und Zugriffe protokollieren.



## Remote Zugriff: Netzwerksicht

- ▶ SSH als Standard-Protokoll, Legacy-Ports nur temporär freischalten.
- ▶ VTY-Zugänge auf Management-VLANS einschränken und per ACL absichern.
- ▶ Session-Timeouts und Login-Banner setzen, um Compliance-Anforderungen zu erfüllen.



# Rollen & Privilegien

---

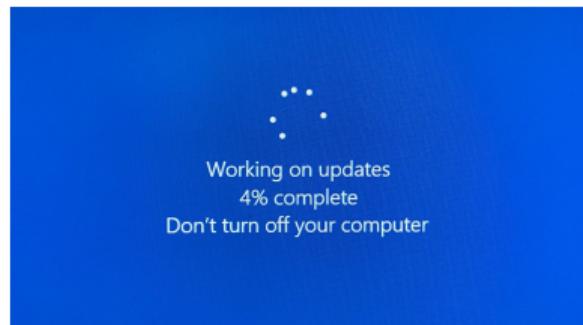
- ▶ Privilege Levels ordnen Konfigurationsbefehle abgestuften Rollen zu.
- ▶ Parser Views kapseln Befehle pro Team (Helpdesk, Netzwerkbetrieb, Security).
- ▶ AAA liefert Rolleninformationen per Cisco-AVPair oder CLI-Command-Sets.

<b>Rolle</b>	<b>Level / View</b>
n Helpdesk	Privilege 1 / view help
n Network Ops	Privilege 5 / view ops
n Security	Privilege 7 / view sec
n Architect	Privilege 15
n	

# Betriebssystem absichern

---

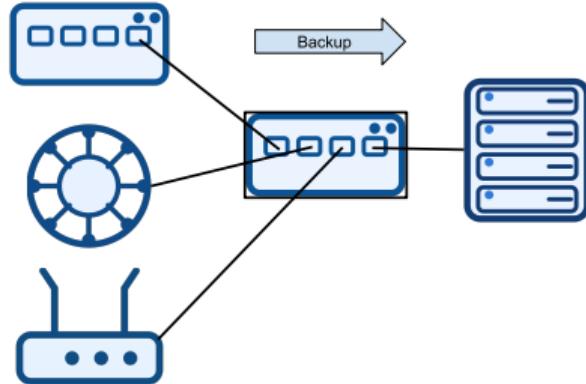
- ▶ Signierte Images und Secure Boot (`secure boot-image/config`) verhindern Manipulation.
- ▶ OS-Updates nach Wartungsfenster mit Rollback-Plan einspielen.
- ▶ Integritätschecks (MD5/SHA256) vor Deployments durchführen.



# Konfiguration archivieren

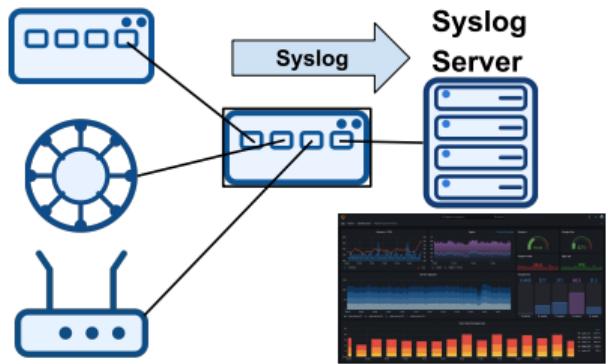
---

- ▶ Archivierung automatisieren:  
Konfigurations-Backups nach Changes und  
zeitgesteuert anstoßen.
- ▶ Sichere Ablage per SCP/SFTP in ein  
versioniertes Repository mit  
Zugriffskontrolle.
- ▶ Integrität und Wiederherstellung testen:  
Checksummen prüfen und regelmässig  
Restore-Proben durchführen.



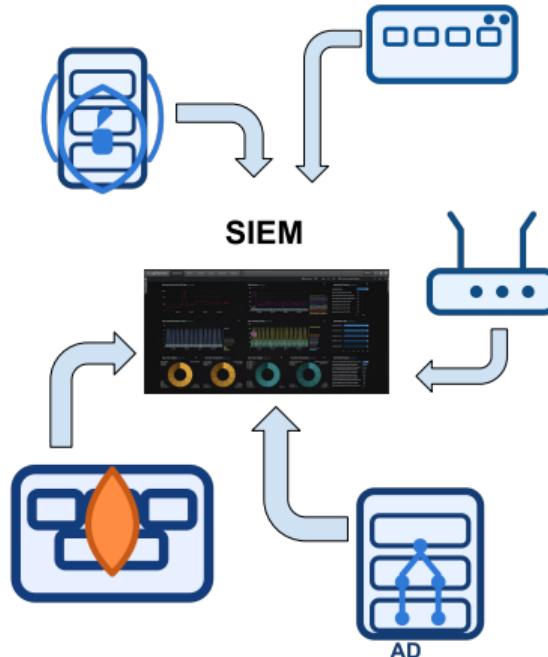
# Logging-Architektur

- ▶ Syslog-Quellen mit Severity-Filters definieren und an dedizierte Server senden.
- ▶ Quelle via `logging source-interface` setzen, damit ACLs greifen.
- ▶ Zeitnah Alerts für AAA-Fehlschläge und Config-Changes generieren.



# Telemetry & SIEM

- ▶ SNMP v3 mit AuthPriv und rollenbasierten Views
  - keine Community-Strings.
- ▶ Streaming Telemetry/NetFlow liefert Kontext für Anomalie-Erkennung.
- ▶ SIEM-Korrelation für Authentisierung, Config-Drift und Performance-Alarne.



# Zeit-Synchronisation

---

- ▶ NTP-Server redundant betreiben und mittels `ntp authenticate` absichern.
- ▶ Log-Server als Referenz für alle Netzwerkgeräte definieren.
- ▶ Zeitabweichungen überwachen (Syslog, SNMP), bevor Audit-Trails ungültig werden.



## Management-Netze

---

- ▶ Management-, Logging- und Monitoring-Verkehr in dedizierte VLANs/VRFs auslagern.
- ▶ ACLs und Firewalls lassen nur erforderliche Management-Protokolle passieren.
- ▶ OOB-Netze regelmäßig testen und mit MFA absichern.