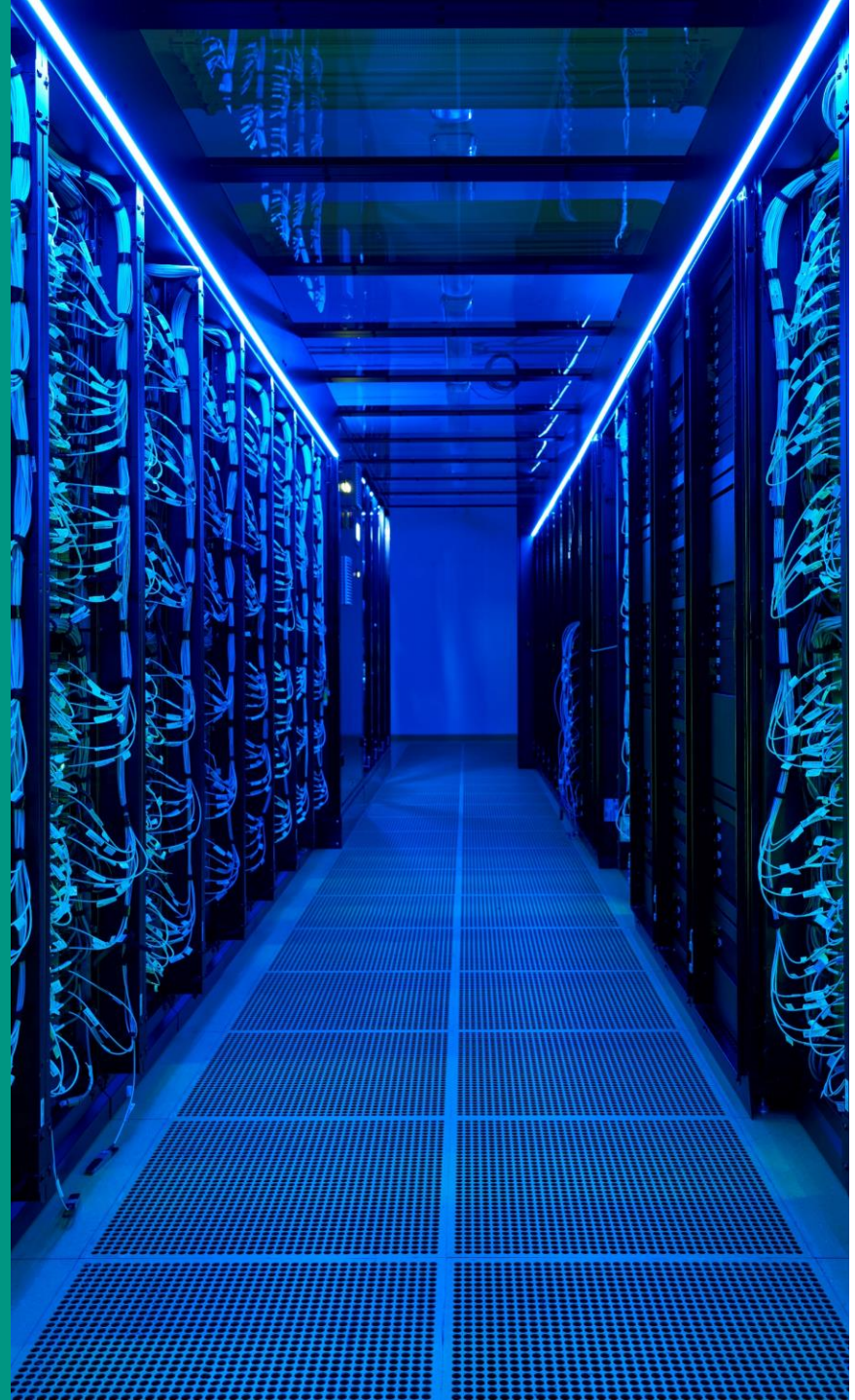
bwCampusnetz Netzwerkarchitektur



Julian Schuh, Scientific Computing Center SCC,
25.11.2025

Inhalte

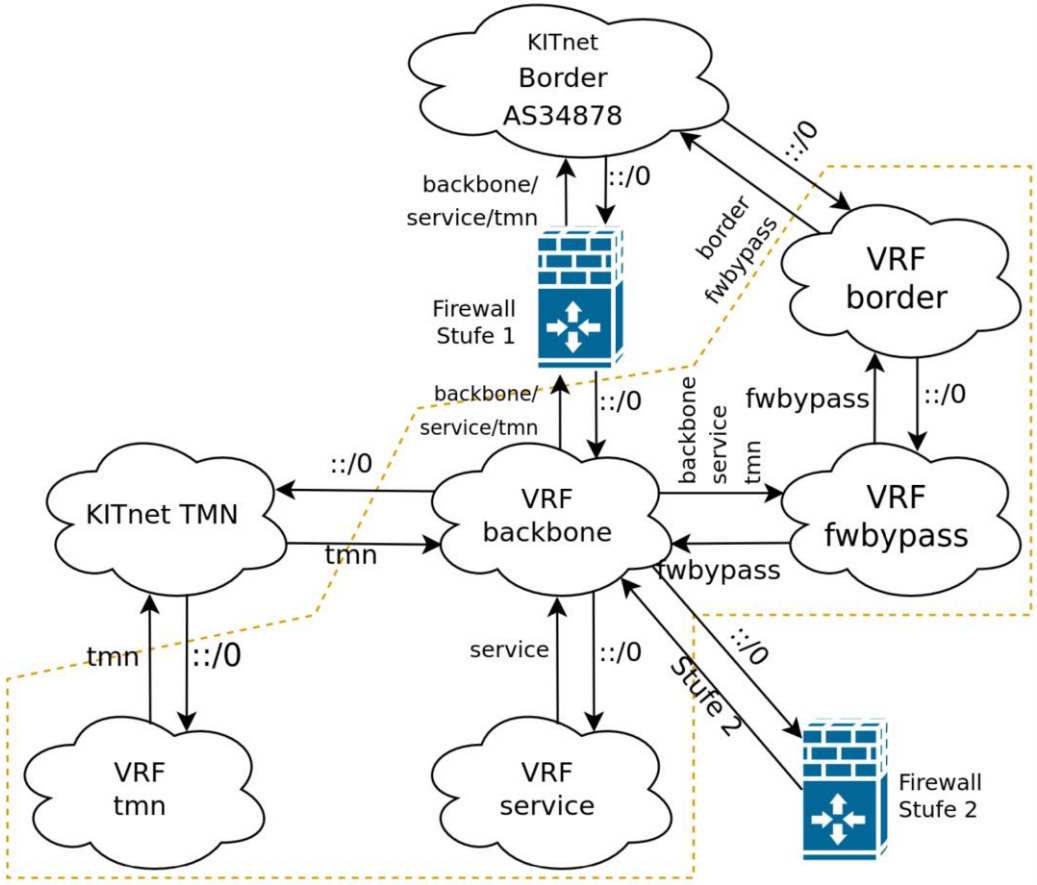
1. EVPN
   - Allgemein
   - Am KIT
2. EVPN InterOp / Open Source
3. Automatisierung
4. WLAN-Zugang für IoT-Geräte
5. Gedanken zur Zertifikatsauthentifizierung

EVPN/VXLAN

- Standardisierte Netzwerkvirtualisierungstechnologie
  - Verschiedene RFCs, Anwendung im Provider-, Datacenter- und Campus-Bereich
  - Implementiert von vielen Herstellern, InterOp teils herausfordernd
- Dataplane: VXLAN (Layer-2-Frames in VXLAN in UDP in IPv6/IPv4), Alternative: MPLS
  - VXLAN: basierend auf geroutetem Underlay, Unicast oder Multicast
- Controlplane: BGP
  - Erweiterungen um neue AFIs (Address Family Indicator)
    - Verschiedene route-Types definiert
    - Erweiterungen wie D-Path für Loop-Verhinderung in komplexen Topologien
  - iBGP oder eBGP
- Bereitstellung von L2VPNs und L3VPNs
  - L2VPN: Klassische Broadcastdomäne (Layer-2-Segment), das über mehrere Geräte gestretched sein kann
    - Nutzung optimaler Pfade im Underlay, Verzicht auf klassische Technologien wie STP
  - L3VPN: Stretchen von VRFs (Routing-Kontexten) über mehrere Geräte
    - Erlaubt die Implementierung unabhängiger oder verbundener Routing-Kontexte

EVPN/VXLAN am KIT

- Vollständig ausgerollt im Kern-Netz
- Nächste Generation Campusnetz: EVPN/VXLAN bis zum Access Port
  - Ähnliche Struktur wie Kernnetz, deutlich komplexer
- L2VPNs zur Bereitstellung von Broadcastdomänen
  - Mit Routing-Interface (Anycast auf allen beteiligten Routern)
- L3VPNs zur Abbildung verschiedener Firewall-Zonen
  - VRF „vor“ der Firewall, im Intranet, als Stufe-2-Netz oder als Management-Netz
- Mittlerweile: Jedes Netz hinter der Stufe-2-Firewall in eigener VRF innerhalb eines VRF-Komplexes



EVPN/VXLAN am KIT: Anbindungen

- Anwendung der Architekturbausteine aus bwCampusnetz
  - Firewall: VRF-Komplex mit eigener VRF pro Sicherheitszone
    - Anbindung der Firewall via L3 in zwei „Head-VRFs“ auf den Border-Leaves
    - BGP für den Austausch der Routen
  - WLAN: Übergabe als L2-Trunk
  - VPN: Übergabe als L2-Trunk
    - Zukünftig: Umbau auf einen L3-Ansatz mit dynamischem Routing
- Interconnect Campus/Core-Fabric
  - Auf EVPN/VXLAN-Layer mittels EVPN-Gateway

EVPN InterOp / Open Source

- Die meisten Aspekte von EVPN sind standardisiert
  - Implementierungen auf Protokollebene kompatibel
  - Trotzdem: Viele Unterschiede in der Implementierung im Detail, Networking OS muss Optionen bereitstellen, um Verhalten anzupassen

- InterOp-Test im Rahmen des Projekts
  - Verschiedene Vendor-Implementierungen und Open-Source-Implementierung Free Range Routing (FRR)
  - Für einfache Anwendungsfälle (L3VPN) und Topologien erfolgreich
  - L2VPN deutlich komplexer als L3VPN
  - Zusätzliche Herausforderung: Anycast Gateway
    - Schwierig, gleiches Verhalten zwischen verschiedenen Herstellern und Linux zu erreichen

- Free Range Routing (FRR)
  - Implementierung von L2VPNs (bridges) und L3VPNs (vrfs) auf Linux
  - VXLAN-Implementierung im Linux-Kernel, einige Plattformen unterstützen VXLAN Offloading

Automatisierung

- Mehr Konfigurationsaufwand bei Nutzung von Netzwerkvirtualisierungstechnologie
  - Underlay, Overlay, L2-Segment (BCD), SVI, L3-Segment (VRF)
  - Zusätzlicher Identifier-Space muss verwaltet werden (VXLAN ID)

- Automatisierung unabhängig davon, ob Netzwerkvirtualisierungstechnologie eingesetzt wird
  - ASCII-Konfiguration im Ganzen generieren und auf das Gerät laden
    - Von vielen Herstellern nicht sinnvoll unterstützt, Gerät kann bei Fehler in ungültigem Zwischenzustand landen
  - Konfiguration via NETCONF/YANG bzw. OpenConfig
    - Standardisierte Datenmodelle für den Betrieb von Routern
    - Oft proprietäre Erweiterungen durch Hersteller
    - Oft nicht transaktional

- Für Standardtopologien sind oft proprietäre oder offene Automatisierungslösungen durch die Hersteller erhältlich

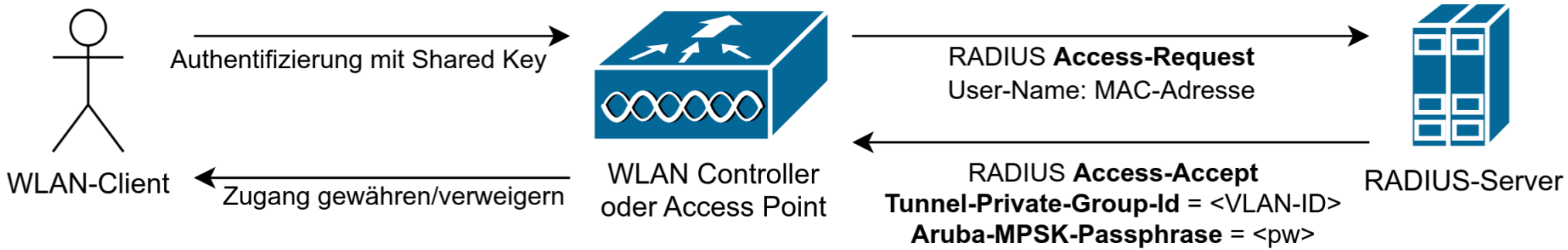
WLAN-Zugang für IoT-Geräte

- Problemstellung: IoT-Geräte, welche nicht an einen Nutzenden gebunden sind und WLAN, aber kein WPA-Enterprise unterstützen

- Lösung: SSID mit WPA2-PSK, eigenes pre-shared secret für jedes Engerät
- Proprietäre, aber ähnliche Implementierungen durch mehrere Hersteller
  - Verschiedene Namen, z. B. IPSK/MPSK
  - Bei Verbidungsaufbau eines Engeräts Abfrage eines RADIUS-Server auf Basis der MAC-Adresse des Endgeräts
  - RADIUS-Server gibt pre-shared secret für Endgerät zurück
  - Verbindungsaufbau mit eigenem pre-shared secret wird abgeschlossen

- Lösung nicht standardisiert, jedoch verwendetes Protokoll (RADIUS)
  - Implementierung mittels Open-Source-Lösungen (z.B. FreeRADIUS) möglich

WLAN-Zugang für IoT-Geräte



Zertifikatsauthentifizierung

- Ziel: Nutzung von Zertifikaten für 802.1X mit EAP-TLS im WLAN oder drahtgebundenen Netzzugang
  - Vermeidung von Mehrfachnutzung von Credentials (Username/Passwort)
  - Automatische, sichere Provisionierung von Client-Systemen, ohne Client-Credentials kennen zu müssen

- Eigenes Zertifikat für jedes Endgerät eines Nutzers
  - Entkopplung von Nutzer und Device
  - Zugang zum Netz kann je Device, nicht nur je Nutzer, eingeschränkt werden

- Zentrale Zuordnung von Netzsegment ↔ Zertifikat ↔ [Nutzer / OE]
  - Kein Ändern der Credentials um den Client in eine andere BCD zu bringen
  - Self-Service-Portal im Rahmen von ZKI AK Netzdienste aktuell in Entwicklung