bwCAMPUSNETZ

Zukunftsfähige Konzepte für die Campusnetze
an Universitäten und Hochschulen

Verwaltung von (Sicherheits-)Kontexten und VLANs für Nutzerbasierter Zuordung

Federführung bei der Erstellung dieses Dokuments: Universität Ulm
Kontakt: team@bwcampusnetz.de

Inhalt

Abstract

In komplexen Netzwerkumgebungen wie denen von Universitäten treffen eine Vielzahl von Nutzergruppen mit unterschiedlichen Anforderungen aufeinander: Studierende, Mitarbeitende, Institute, externe Dienstleister sowie IoT-Geräte müssen sicher, effizient und kontextsensitiv in das Campusnetz integriert werden. Klassische VLAN-Zuweisungen auf Basis physischer Standorte oder statischer Konfigurationen stoßen hierbei an ihre Grenzen. Dieses Whitepaper untersucht die Herausforderungen und Anforderungen an die dynamische Verwaltung von Sicherheitskontexten und VLAN-Zuweisungen in nutzerzentrierten Netzwerken. Im Fokus steht die kontextabhängige Netzwerksegmentierung, bei der Nutzer – unabhängig von ihrem Standort oder Zugangsweg (z. B. WLAN, VPN) – dynamisch in den für sie vorgesehenen logischen Netzwerkbereich eingebunden werden. Darüber hinaus wird aufgezeigt, wie Fremdfirmen und IoT-Infrastrukturen sicher in das Netzwerk integriert werden können. Ziel ist eine systematische Darstellung möglicher Lösungsansätze unter Berücksichtigung von Sicherheits-, Skalierbarkeits- und Verwaltungsaspekten.

1 Einleitung

Universitätsnetzwerke stellen eine besondere Herausforderung für die IT-Infrastruktur dar: Sie vereinen eine heterogene Nutzerschaft mit vielfältigen Anforderungen, wechselnden Geräten, mobilen Zugriffsszenarien und einem hohen Maß an Autonomie innerhalb einzelner Organisationseinheiten. Gleichzeitig sind Sicherheitsanforderungen, Datenschutzbestimmungen und administrative Vorgaben zu erfüllen.

In der Praxis bedeutet dies, dass beispielsweise ein Mitarbeitender eines Instituts – unabhängig davon, ob er sich über WLAN auf dem Campus, aus dem Homeoffice via VPN oder von einem Seminarraum in einem anderen Gebäude einwählt – stets dem gleichen logischen Netz (z. B. VLAN) zugeordnet werden sollte. Diese "Nutzerbasierte Kontextzuordnung" erlaubt eine konsistente Netzwerkumgebung, vereinfacht die IT-Administration und erhöht die Sicherheit.

Zusätzlich stellt der Zugriff externer Akteure – wie Fremdfirmen oder Dienstleister – sowie die zunehmende Anzahl an IoT-Geräten eine weitere Komplexitätsebene dar. Diese benötigen Zugang zu bestimmten Ressourcen, ohne dass das Gesamtnetz kompromittiert wird.

Dieses Whitepaper widmet sich der Frage, wie durch den gezielten Einsatz moderner Netzwerktechnologien – wie z. B. 802.1X, RADIUS, NAC-Systeme, SDN, VXLAN oder Identitätsmanagement – eine flexible, sichere und nutzerzentrierte Netzsegmentierung erreicht werden kann. Es werden verschiedene Ansätze, deren Vor- und Nachteile sowie Praxisbeispiele aus dem Hochschulumfeld beleuchtet, um eine Entscheidungsgrundlage für die Implementierung solcher Konzepte zu schaffen.

Auf Basis der Implementierunsansätze für eine dynamische Zuweisung von Kontexten an den teilnehmden Universitäten entstand diese Guideline, die es ermöglich, ein skalierbares System zur Verwaltung von Nutzerkontexten zu implementieren. Dabei wird, wie üblich im Projekt bwCampusnetz, auf ein Baukastenprinzip gesetzt. Die dargestellten Ansätze sind nicht als umfassende Lösung zu verstehen, sondern vielmehr als Sammlung von Tools.

Zunächst werden zum besseren Verständnis der Komplexitäten in dieser Thematik verschiedene User-Stories vor gestellt. Davon werden Anforderungen abgeleitet. Diese werden dann mit den bestehenden Systemen verglichen, um Weiterentwicklungsmöglichkeiten aufzuzeigen.

Aus den bestehenden Architekturen ergeben sich auch neue Herausfoderungen, die am Ende betrachtet werden sollen. Schlussendlich werden für einzelne Teilprobleme Lösungsansätze präsentiert.

1.1 Zielgruppe

Die Zielgruppe dieses Papiers sind zum einen Administratoren an größeren Einrichtungen. Technische Grundkenntnisse sind vorausgesetzt. Da das Thema allerdings auch die Anknüpfüng an Prozesse innerhalb einer Einrichtung sowie einen interdisziplinären Austausch mit Verwaltungselementen erfordert, wird auf zu tiefgehende technische Betrachtungen – sofern möglich – verzichtet.

2 Anforderungsanalyse

In diesem Kapitel sollen beispielhaft einzelnen Use-Cases, die sich an den teilnehmenden Universitäten ergeben, in Form von User Stories erläutert werden. Daraus werden dann Anforderungen an den technischen Aufbau sowie an die Verwaltungsprozesse abgeleitet.

2.1 Epic: Nutzerbasierte Verwaltung von Sicherheitskontexten und VLAN-Zuweisung in Universitätsnetzwerken

2.1.1 Beschreibung

In modernen Hochschulnetzwerken mit einer Vielzahl von Nutzern, Instituten, Gastzugängen, IoT-Geräten und externen Dienstleistern ist eine statische Netzwerksegmentierung nicht mehr zeitgemäß. Dieses Epic beschreibt die Entwicklung und Implementierung eines dynamischen, kontextbasierten Netzwerkkonzepts, das die sichere und flexible Zuweisung von VLANs und Sicherheitszonen auf Basis von Benutzeridentitäten, Zugriffswegen und Rollen ermöglicht. Ziel ist es, dass Nutzer und Geräte – unabhängig von ihrem Zugriffsstandort (WLAN, VPN, LAN) – automatisch in ihre definierten logischen Netzbereiche eingebunden werden. Dabei sollen auch Anforderungen an Sicherheit, Datenschutz, Skalierbarkeit und Integrationsfähigkeit externer Akteure berücksichtigt werden.

2.1.2 Ziele

- Entwicklung eines Frameworks zur nutzerbasierten dynamischen Netzsegmentierung.
- Integration bestehender Authentifizierungs- und Autorisierungsinfrastrukturen (z. B. RADIUS, LDAP, Shibboleth).
- Ermöglichung kontextsensitiver VLAN-Zuweisung (z. B. via 802.1X).

- Anbindung externer Dienstleister und IoT-Geräte unter Einhaltung hoher Sicherheitsstandards.
- Bereitstellung eines skalierbaren und wartbaren Architekturmodells.

2.1.3 Business Value

- Erhöhung der Netzwerksicherheit durch fein granulare, rollenbasierte Zugriffssteuerung.
- Entlastung der IT durch automatisierte VLAN-Zuweisungen.
- Bessere Unterstützung von Mobilität und Homeoffice für Mitarbeiter und Studierende.
- Reduzierung des Risikos durch klar abgegrenzte Netzbereiche für Fremdfirmen und IoT.
- Grundlage für zukünftige Netzwerkmodernisierung (z. B. SDN oder Zero Trust).

2.1.3.1 Stakeholder

- Zentrale IT-Abteilung
- Fakultäten und Institute
- Datenschutzbeauftragte
- Externe Dienstleister
- Betreiber von IoT-Infrastrukturen
- Netzwerkadministratoren

2.1.3.2 Akzeptanzkriterien

- Nutzer werden anhand ihrer Identität und Rolle automatisch dem richtigen VLAN/-Sicherheitskontext zugeordnet.
- Der Zugriff über verschiedene Zugangswege (LAN, WLAN, VPN) funktioniert konsistent.
- Fremdfirmen können sicher, zeitlich begrenzt und segmentiert auf definierte Ressourcen zugreifen.
- IoT-Geräte werden segmentiert und können nur auf freigegebene Dienste kommunizieren.
- Die Lösung ist skalierbar, dokumentiert und in bestehende Systeme integrierbar.

2.2 User Story 1 – Institutsangehöriger im Homeoffice

Zugriff auf Laborgeräte aus dem Homeoffice mit identischem Sicherheitskontext:

Als Institutsmitarbeiter, möchte ich, dass mein Zugriff aus dem Homeoffice auf Laborgeräte dieselben Firewall-Regeln und Netzwerkrechte wie im Institut verwendet, damit ich ohne Einschränkungen und sicher auf meine Arbeitsumgebung zugreifen kann.

2.2.1 Akzeptanzkriterien

- Bei VPN-Verbindung wird automatisch mein Instituts-VLAN oder Kontext zugewiesen.
- Die gleichen ACLs und Firewall-Regeln wie im Campusnetz gelten für meine Verbindung.
- Die Verbindung wird protokolliert und entspricht den IT-Sicherheitsrichtlinien.
- Die Authentifizierung erfolgt über die zentrale Identitätsinfrastruktur.

2.2.2 Technische Implikationen

- Dynamische VLAN-Zuweisung via RADIUS und/oder VPN-Gateway
- Nutzung von Rollen- oder Gruppeninformationen (z. B. LDAP/AD)
- Durchsetzung von Firewall-Policies unabhängig vom Zugriffsstandort

2.3 User Story 2 – Externer Dienstleister(Gebäudeleittechnik)

Sicherer Remote-Zugriff für externe Dienstleister auf Steuerungssysteme

Als externer Techniker eines Dienstleisters für Gebäudeleittechnik, möchte ich, remote auf bestimmte Steuerungssysteme zugreifen können, damit ich Wartungs- und Konfigurationsaufgaben durchführen kann, ohne vor Ort sein zu müssen.

2.3.1 Akzeptanzkriterien

- Zugriff ist auf bestimmte IP-Adressen oder Dienste limitiert.
- Die Verbindung ist zeitlich begrenzt und protokolliert.
- Nur definierte VLANs oder Zonen sind erreichbar.
- Zugriff erfolgt über zertifikatsbasierte oder multifaktorbasierte Authentifizierung.

2.3.2 Technische Implikationen:

- Einsatz eines Netzwerkzugangskontrollsystems (z. B. NAC)
- Temporäre VLAN-Zuweisung oder Microsegmentation (z. B. per SDN)
- Integration mit Ticket-/Freigabesystem für zeitlich gesteuerten Zugriff
- VPN- oder Reverse-Proxy-Zugriff mit strikter Policy Enforcement

2.4 User Story 3 – Mitarbeiter mit wechselndem Standort oder mehreren Rollen

Nahtloser Netzwerkzugriff für Mitarbeitende mit mehreren Büros auf dem Campus

Als Mitarbeiter mit mehreren Arbeitsplätzen, möchte ich, an jedem Ort im Campusnetz automatisch meinem jeweiligen Netzkontext zugeordnet werden, damit ich überall unter den gleichen Bedingungen arbeiten kann. Dabei muss ich den Kontext, in dem ich arbeiten will, selbst wählen können.

2.4.1 Akzeptanzkriterien

- VLAN-Zuweisung erfolgt standortunabhängig anhand der Benutzeridentität.
- Zugang über LAN und WLAN bietet identische Rechte und Zugriffsmöglichkeiten.
- Die Konfiguration muss ohne manuelle Intervention durch die IT erfolgen.
- Drucker, Dateifreigaben und andere Ressourcen sind überall erreichbar.
- Wahl des Kontext durch den Nutzer ist möglich.

2.4.2 Technische Implikationen

- 802.1X-basierte Authentifizierung an Switchports und WLAN
- Zentrale Benutzer-/Gruppenzuordnung über RADIUS/LDAP
- Identity-Aware Network Access
- Dynamisches VLAN-Mapping auf Basis der Benutzerrolle

2.5 User Story 4 – Kontextverantwortlicher verwaltet Zugriffsrechte für sein Team

Delegierte Rechtevergabe durch Kontextverantwortliche

Als verantwortliche Person für einen bestimmten Kontext (z. B. Institut, Organisationseinheit), möchte ich, dass ich meinen Mitarbeitenden eigenständig Zugriffsrechte und Netzwerkkontexte zuweisen kann, damit ich flexibel und ohne zentrale IT-Einbindung mein Team verwalten und auf wechselnde Anforderungen reagieren kann. Ich möchte auch die Möglichkeit eines automatisierten Offboardings haben.

2.5.1 Akzeptanzkriterien

- Ich kann bestehende Nutzer aus meinem Kontext verwalten (z. B. Sicht auf meine Mitarbeiter).
- Ich kann VLAN-/Ressourcenzugriffe über eine Weboberfläche rollenbasiert zuweisen (z. B. Laborzugang, Forschungsnetz, Drucker).
- Alle Änderungen werden protokolliert und sind für die zentrale IT einsehbar.
- Nur innerhalb meines eigenen Kontextes kann ich Änderungen vornehmen.
- Es gibt klare, technische und organisatorische Begrenzungen meiner Rechte.

2.5.2 Technische Implikationen

- Delegationsmechanismus im IDM zur Zuweisung administrativer Rechte auf Kontext-Ebene

- Rollen-/Gruppenbasierte Zugriffskontrolle über ein zentrales Policy-System (z. B. NAC, Firewall, RADIUS)
- Webportal zur Self-Service-Rechtevergabe mit rollenbasiertem Zugriff
- Automatisierte Provisionierung und Policy-Updates nach Änderungen
- Auditing- und Logging-Funktionalität für alle durchgeführten Aktionen

2.6 Zusammenfassung

Aus den dargestellten User-Stories ergeben sich einige Anforderungen, die ein System sowohl technisch als auch organisatorisch abbilden können muss. ### Technische Anforderungen an das Netzwerk Zusammengefasst muss für ein möglichst flexibles System die Möglichkeit bestehen, Nutzer- und Sicherheitskontexte überall anzubieten, egal welchen Zugriffsweg ein Nutzer nimmt. Dabei muss ein Nutzerkontext nicht notwenigerweise heißen, dass es sich im eine Layer2-Domäne handelt. Vielmehr muss gelten, dass für einen Kontext die gleichen Voraussetzung hinsichtlich Firewalling und Routing bestehen. In Einzelfällen ist jedoch auch ein Layer2 Durchgriff erfoderlich, besonders in Gebäudeleittechnick und IoT-Netzen, in denen oftmals stark veraltete Technik zum Einsatz kommt. Die angesprochenen Kontexte müssen unabhängig vom Standort erbracht werden. Dazu muss das Konzept von verschiedenen Vendors unterstützt werden.

Schlussendlich muss – je nach Zugangsweg – das Netzwerk dynamisch Informationen zum angestrebten Kontext erhalten und die Nutzer*in in diesen Kontext mappen. Hier kommen vor allem die klassische Technologie 802.1X mittels RADIUS in Frage.

2.6.1 Anforderungen an ein Identitäts Management System

Es muss eine verlässliche Source of Truth (SoT) geben, die Nutzer und ihre jeweiligen Kontexte verwaltet und diese Informationen über eine Schnittstelle zur Verfügung stellt. Dabei ist es vor allem wichtig, dass es eindeutige Nutzeridentitäten gibt, die im Idealfall organisationsübergreifend gelten. Damit kann sicher gestellt werden, dass keine widersprüchlichen Informationen aus verschiedenen Quellen vorliegen. In dieser SoT muss die Zuordnung von Nutzer*Innen zu Rollen bzw. Kontexten gepflegt werden. Dabei können einzelnen Nutzern mehrere Rollen oder Kontexte zugewiesen werden. Wichtig ist, dass Nutzer mit mehreren Kontexten auswählen können, in welchen Kontext sie zu einer gegebenen Zeit aktiv

sein möchten. Zusätzlich muss die Möglichkeit gegeben sein, temporäre Accounts sowie Gast-Accounts zu verwalten. Darüber hinaus muss, um modernen Sicherheitsstandards zu genügen, die Möglichkeit einer Mehrfaktor-Authentisierung (MFA) gegeben sein. Damit eine effiziente Verwaltung von Rechten erfolgen kann, müssen Verantwortliche eigenständig (z. B. in einem Self-Service Portal) Nutzerkontexte zuweisen können.

2.6.2 Anforderungen an das Nutzermanagement

Nutzer möchten in aller Regel nicht zu sehr mit technischen Details überlastet werden. Deswegen muss es eine einfache Möglichkeit des Roll-Outs für Profile geben, sodass ein Nutzer an seinem Client möglichst wenig ändern muss. Daraus resultiert auch, dass es eine Möglichkeit geben muss, einen Client eindeutig zu identifizieren. Dabei gibt es verschiedene Möglichkeiten, einen Nutzer zu identifizeren.

3 Kontexte und Zuordnungen

Ein Kontext beschreibt im Netzwerkumfeld die Menge an Rechten, Ressourcen und Parametern, die ein Benutzer oder Gerät nach der Authentisierung erhält. Er kann auf verschiedenen Attributen basieren, beispielsweise der Gruppenzugehörigkeit im LDAP, der Rolle eines Benutzers, Standortinformationen oder sogar Endgeräteprofilen. Dadurch lässt sich sehr granular steuern, welcher Zugriff und welche Netzwerkressourcen für bestimmte Identitäten gelten. In diesem Kapitel wird noch detailliert darauf eingegangen, wie solche Kontextmappings in unterschiedlichen Netzwerk-Architekturen konkret umgesetzt werden können.

3.1 Attributbasierte Zuordnung

Grundsätzlich können Kontexte basierend auf verschiedenen Attributen zugeordnet werden. Diese Möglichkeiten sollen hier erläutert werden.

3.1.1 Nutzerbasierte Zuordnung mittels Nutzername

Jedes Mitglied bzw. jeder Gast einer Einrichtung besitzt in aller Regel schon einen Nutzernamen oder ein anderes indentifizierendes Attribut. Dieses kann ebenfalls für die Zuordnung zu einem Kontext genutzt werden. Diese Methode hat den Vorteil, dass sie zum einen bestehende Infrastruktur einfach nutzen kann. Darüber hinaus kann hier durch Anbindung an das IDM eine eindeutige Zuordnung eines Nutzers zu einem Kontext gewährleistet werden. Dabei ist die Zuordnung nicht an das Endgerät gebunden. Jedoch ergeben sich Probleme, wenn ein Nutzer mehreren Institutionen oder Kontexten zuordenbar ist. Eine reine Zuordnung basierend auf einem Nutzernamen ist daher nicht ausreichend. Eine reine Zuordnung auf Nutzerbasis ist mit erheblichem Aufwand verbunden, was die Pflege von Listen angeht.

3.1.2 Gruppenbasierte Zuordnung

Kontexte werden losgelöst von einzelnen Nutzern und es wird eine Gruppierung vorgenommen. So werden Gruppen gepflegt, denen jeweils ein Kontext zugeordnet werden kann. Allerdings ergibt sich dadurch eine geringere Granularität. Prinzipiell sind auch hier Zugehörigkeiten zu mehreren Gruppen problematisch.

3.1.3 Zuordnung mittels Realm

Eine Erweiterung des Gruppenkonzepts ist das Konzept des Realms. Zur Zuordnung von Kontexten werden wieder Gruppen gebildet. Ein Nutzer kann nun zu mehreren Gruppen gehören. Beim Login kann der Nutzer nun selbständig seinen Realm angeben. Beispielsweise kann als Nutzername “user@realm” verwendet werden.

3.1.4 Zuordnung via Zertifikat

Eine Alternative zu AAA mittels Nutzername und Passwort, ist die Nutzung von Zertifikaten.

3.1.4.1 Zuordnung von Geräten

Gerätebasierte Zertifikate erlauben es, Geräte sicher einem Kontext zuzuordnen. Hierbei verliert man allerdings die Möglichkeit, mehreren Nutzern das Teilen einer Gerätes zu ermöglichen. Vor allem, wenn Trusted Platform Modules genutzt werden.

3.1.4.2 Nutzerzertifikate

Alternativ können an Nutzer*Innen gebundene Zertifikate ausgestellt werden. Diese ermöglichen dann eine Zuordnung. Auch hier stellt sich die Frage, wie ein Nutzer seinen Kontext wechseln kann. Darüber hinaus erfodert die Verwaltung von Zertifikaten einiges an technischem Know How.

3.2 Zusammenfassung

Aus der User-Stories ergibt sich klar, dass eine Anforderung ist, dass eine Nutzer*In selbstständig und ohne technisches Wissen die Möglichkeit haben muss, den jeweiligen Kontext zu wechseln. Dies ist vor allem durch Nutzung von Realms möglich. Je nach Netzzugangstechnologie ist eine technische Umsetzung leicht mölich: Die meisten RADIUS-Server ermöglichen problemlos das Verarbeiten von Nutzernamen.

4 Relevante Technologien

4.1 Authorisierungstechnologien

4.1.1 Authentisierung und Autorisierung mit IEEE 802.1X

Das Protokoll IEEE 802.1X dient als Grundlage für portbasierte Zugangskontrolle. Es definiert ein Verfahren, bei dem ein sogenannter Supplicant (z. B. ein Endgerät) seine Identität gegenüber einem Authentifizierungsserver nachweist, bevor der Zugriff auf das Netzwerk freigegeben wird. Switches oder Access Points fungieren dabei als Authenticator und blockieren den Datenverkehr so lange, bis die Authentisierung abgeschlossen ist. In diesem Kontext können dynamisch VLANs zugewiesen werden, abhängig von Rolle, Nutzergruppe oder Sicherheitsstatus des Geräts.

4.1.2 RADIUS und TACACS als AAA-Infrastruktur

Die Kommunikation zwischen Authenticator und Authentifizierungsserver erfolgt typischerweise über das Remote Authentication Dial-In User Service (RADIUS)-Protokoll. RADIUS stellt dabei die Funktionen Authentication, Authorization und Accounting (AAA) bereit und ist etabliert für die Integration mit 802.1X. Über RADIUS-Attribute können Netzwerkgeräte dynamisch Konfigurationen wie VLAN-IDs oder Access-Control-Listen erhalten.

Neben RADIUS findet auch TACACS+ Verwendung, vor allem bei der Authentisierung von Administrationszugriffen auf Netzwerkgeräte. Während RADIUS stärker auf den Zugriff von Endgeräten in ein Netz ausgerichtet ist, bietet TACACS+ eine feingranularere Trennung von Authentisierung und Autorisierung im Gerätemanagement. Beide Protokolle sind somit komplementär und tragen in unterschiedlichen Szenarien zur kontrollierten und kontextabhängigen Ressourcenzuweisung bei.

4.1.3 Zuordnung mittels Realm

Um Nutzer*innen die Möglichkeit zu geben, ihren Netzwerkkontext aktiv mitzubestimmen, können sogenannte Realms eingesetzt werden. Dabei handelt es sich um ein Namenspräfix oder -suffix, das im Rahmen der Authentifizierung – typischerweise über 802.1X – an den Benutzernamen angehängt wird. Durch diesen Zusatz lassen sich unterschiedliche Kontexte, Organisationseinheiten oder Nutzungsszenarien explizit kennzeichnen.

Ein bekanntes Beispiel für ein realm-basiertes Authentifizierungssystem ist eduroam. Hier erfolgt die Anmeldung mit einem Benutzernamen im Format `<uid>@realm.tld`, wobei der Realm die Heimatorganisation des Nutzers identifiziert. Im Hintergrund findet eine hierarchische Authentifizierung statt, bei der die Anfrage zunächst an einen zentralen RADIUS-Föderationsserver und anschließend an den zuständigen RADIUS-Server der jeweiligen Einrichtung weitergeleitet wird. Der Realm fungiert in diesem Kontext als Routing-Information und als Grundlage für die Auswahl der entsprechenden Policy.

Dieses Konzept lässt sich jedoch nicht nur in föderierten Szenarien wie eduroam nutzen, sondern auch lokal, zur kontextsensitiven Policy-Zuweisung innerhalb einer Institution. So kann z. B. durch unterschiedliche Realms (@stud.example.edu, @staff.example.edu, @extern.example.edu) bei der Authentifizierung unmittelbar der gewünschte Nutzungskontext mitgeteilt und vom RADIUS-Server ausgewertet werden. Auf diese Weise entsteht eine einfache, aber effektive Möglichkeit, kontextabhängige Netzwerkzuweisungen flexibel und dynamisch umzusetzen – gesteuert durch den Nutzer selbst und ohne aufwändige Attributverwaltung im IDM.

4.1.4 Mac Authentication Bypass

Eine einfache Methode zur kontextbasierten Netzzuweisung, insbesondere für nicht-interaktive Geräte wie Drucker, Sensoren oder IoT-Komponenten, ist die MAC Authentication Bypass (MAB). Dabei identifiziert sich ein Gerät beim Verbindungsaufbau nicht durch Benutzeranmeldung, sondern allein durch seine MAC-Adresse, die vom Switch oder Access Point an einen RADIUS-Server übermittelt wird. Der RADIUS-Server ordnet dieser Adresse eine definierte Rolle oder Policy zu – etwa ein bestimmtes VLAN, eingeschränkten Zugriff oder spezifische Firewall-Regeln.

Diese Methode erlaubt es, Geräten auch ohne Benutzerinteraktion eine Netzwerkkontext zuzuweisen und ist besonders in Umgebungen nützlich, in denen keine 802.1X-Unterstützung vorhanden ist.

Ein wesentlicher Nachteil dieser Vorgehensweise besteht jedoch darin, dass die Rolle auf Basis des Geräts und nicht des Nutzers bestimmt wird. Das bedeutet: Sobald ein Gerät zugelassen ist, erhält es stets dieselbe Netzwerkkonfiguration – unabhängig davon, wer es verwendet oder in welchem Nutzungskontext es eingesetzt wird. Dadurch fehlt die Möglichkeit zur dynamischen, nutzerabhängigen Steuerung, was insbesondere in sicherheitskritischen Umgebungen problematisch sein kann. Zudem ist die MAC-Adresse leicht fälschbar, was zusätzliche Schutzmechanismen erforderlich macht.

Trotz dieser Einschränkungen kann MAB als Übergangslösung oder Ergänzung zu 802.1X-basierter Authentifizierung dienen, insbesondere für legacy- oder IoT-Geräte, die keine eigene Authentifizierungsfähigkeit besitzen.

4.2 Zuordnung von Kontexten in verschiedenen Netzarchitekturen

Grundsätzlich kann eine Gruppenzuordnung auf mehreren Ebenen geschehen, je nachdem, welche Netzarchitektur vorherrscht.

4.2.1 L2-zentrisches Netz

In der einfachsten Methode werden Nutzergruppen statisch einem festen VLAN zugewiesen. Diese Gruppen-VLAN-Zuordnung bleibt dabei unabhängig vom tatsächlichen Aufenthaltsort oder der Zugangstechnologie der Nutzer. Um dennoch eine konsistente Netzwerkkonfiguration zu ermöglichen, muss das entsprechende VLAN bis zu jedem potenziellen Endpunkt – sei es im LAN oder WLAN – gestreckt werden. Dadurch kann ein Nutzer etwa unabhängig davon, ob er sich in Gebäude A oder B befindet oder über VPN oder WLAN einsteigt, immer demselben logischen Netz zugeordnet werden.

Diese Herangehensweise bringt jedoch erhebliche Skalierungsprobleme mit sich. Zum einen müssen Layer-2-Broadcastdomänen campusweit gestreckt werden, was zu sehr großen Fehlerdomänen führt: Ein einzelnes Fehlverhalten (z. B. fehlerhafte Geräte oder Broadcast-Stürme) kann sich über das gesamte Netzwerksegment ausbreiten und die Stabilität beeinträchtigen. Zum anderen steigt der administrative Aufwand, da jede Änderung an der VLAN-Zuweisung manuell an vielen Stellen nachvollzogen werden muss.

Auch für WLAN-Zugänge existieren tunnelbasierte Ansätze (z. B. durch zentrale WLAN-Controller), bei denen der Datenverkehr des Clients an ein zentrales Gateway getunnelt und dort in das passende VLAN einsortiert wird. Diese Lösungen umgehen zwar teilweise die Notwendigkeit, VLANs physisch bis an jeden Access Point zu führen, doch auch sie stoßen bei wachsender Nutzerzahl oder großer geografischer Verteilung an ihre Grenzen: Sie verursachen zusätzlichen Overhead, sind zentralisiert und oft ein Engpass bei der Skalierung sowie bei der Redundanz.

Letztlich basieren all diese Ansätze auf statischen Zuweisungen, die nicht flexibel auf sich ändernde Nutzungskontexte reagieren können – etwa Rollenwechsel, Geräteklassen oder Sicherheitsstufen. Für moderne, dynamische Campusnetzwerke mit heterogenen Nutzergruppen ist daher ein flexibler, kontextabhängiger Ansatz erforderlich, der sich nicht mehr primär an physikalischer Infrastruktur, sondern an logischen Nutzerattributen orientiert.

4.2.2 L3-zentrisches Netz

In einem durch Layer-3-Grenzen segmentierten Netzwerk muss die Zuweisung von Nutzerkontexten über alternative, logisch übergeordnete Mechanismen erfolgen, da die klassische VLAN-basierte (Layer-2) Zuordnung nicht mehr flächendeckend möglich ist. Statt physikalisch identischer Netze wird in diesem Modell angestrebt, dass verschiedene Subnetze – etwa in unterschiedlichen Gebäuden oder Bereichen – logisch gleich behandelt werden. Dadurch kann ein bestimmter Kontext (z. B. „Studierender“, „Mitarbeiter“, „externe Firma“) unabhängig vom Aufenthaltsort oder Zugangspfad dem Nutzer zugewiesen werden.

Dieses Konzept eröffnet hohe Flexibilität und adressiert viele der Skalierungsprobleme, die in L2-zentrischen Architekturen auftreten. Kontextinformationen – etwa aus dem Identity Management, dem Authentifizierungsprozess oder dem Gerätetyp – werden zur Laufzeit ausgewertet und bestimmen die logische Netzzugehörigkeit des Nutzers. Technisch wird dies oft durch den Einsatz von Access Control Lists (ACLs), Policy-Based Routing, dynamischen

Firewalleinstellungen oder softwaredefinierten Netzwerkmechanismen (SDN) realisiert, die eine kontextbasierte Steuerung auf L3 ermöglichen.

Ein weiterer Vorteil dieser Architektur ist die einfache Integration unterschiedlicher Zugangstechnologien. Während kabelgebundene Geräte über dedizierte Zugriffsnetze eingebunden sind, können parallele logische Netzbereiche für WLAN-Clients oder VPN-Nutzer bereitgestellt werden, die über dieselben Rechte und Netzwerkzugriffe verfügen – obwohl sie sich in völlig anderen physischen oder logischen Netzen befinden. Dadurch entsteht eine einheitliche Nutzererfahrung, unabhängig vom Zugangsweg, und administrative Prozesse wie Rechteverwaltung oder Segmentierungsregeln müssen nur kontextbasiert und nicht mehr ortsgebunden gepflegt werden.

Darüber hinaus lassen sich durch dieses Modell auch externe Partner, Gäste oder IoT-Systeme sicher und kontrolliert einbinden: Über dedizierte Netzzonen mit gleichen Sicherheitsrichtlinien, aber unterschiedlichen physikalischen Voraussetzungen, wird eine konsistente Sicherheits- und Zugriffspolitik gewährleistet. Diese logische Entkopplung von Netzarchitektur und Nutzerkontext ist ein entscheidender Schritt in Richtung moderner, adaptiver Campusnetzwerke.

4.2.3 VPN und Overlay-Technologien

In Szenarien, in denen Benutzer über öffentliche oder nicht vertrauenswürdige Netze auf Ressourcen zugreifen, kommen Virtual Private Networks (VPNs) zum Einsatz. Ein verbreitetes Beispiel ist OpenVPN, das verschlüsselte Tunnel zwischen Endpunkten etabliert. Auch hier ist eine dynamische Zuordnung zu Kontexten möglich: So kann ein Nutzer je nach Berechtigung und Standort verschiedenen IP-Pools oder virtuellen Segmenten zugeordnet werden.

Darüber hinaus gewinnen Overlay-Netzwerke an Bedeutung, insbesondere im Kontext von Software-Defined Networking (SDN) und Cloud-Umgebungen. Hierbei wird eine logische Netzwerkstruktur über das physische Netz gelegt, um flexible Isolation und Segmentierung bereitzustellen. Über Overlays lassen sich dynamische Kontexte auch über unterschiedliche Infrastrukturen hinweg konsistent abbilden, etwa zur Trennung von Mandanten oder zur Realisierung sicherer Kommunikationsdomänen. An anderer Stelle des Projekts wird in diesem Zusammenhang ausführlich auf EVPN/VXLAN eingegangen.

4.3 Zusammenfassung

Die dynamische Zuordnung von Nutzern zu VLANs oder vergleichbaren Kontexten basiert auf einem Zusammenspiel etablierter Standards und Technologien. IEEE 802.1X bildet mit RADIUS die Kernarchitektur für portbasierte Authentisierung und VLAN-Zuweisung vor Ort, während TACACS+ ergänzend die Verwaltung von Administrationsrechten unterstützt. Für externe Verbindungen schaffen VPN-Lösungen wie OpenVPN sichere Tunnel, in denen ebenfalls kontextbasierte Steuerung möglich ist. Schließlich ermöglichen Overlay-Technologien die Abbildung solcher Konzepte über physische Grenzen hinweg, was vor allem in hochgradig virtualisierten und dynamischen Umgebungen entscheidend ist.

5 Implementierungsansätze und Architekturen

In diesem Kapitel werden basierend auf den bereits bestehenden Ansätzen, generelle Arichtekturmodell präsentiert.

5.1 Grundsätzliche Komponenten

Die kontextbasierte Zuordnung von Nutzern oder Geräten innerhalb eines Netzwerks erfordert grundsätzlich das Zusammenspiel mehrerer Komponenten.

Zunächst ist eine Datenquelle erforderlich, die die Beziehung zwischen einer Entität – beispielsweise einem Benutzer, einem Gerät oder einem Dienst – und ihrem zugehörigen Kontext abbildet. Diese Informationen stammen in der Regel aus einem Identity Management System (IDM) oder einem Verzeichnisdienst wie LDAP oder Active Directory. Sie enthalten zentrale Kontextmerkmale wie Rollen (z. B. „Studierender“, „Mitarbeiter“), Gruppenmitgliedschaften, Geräteklassifizierungen oder Sicherheitsstufen.

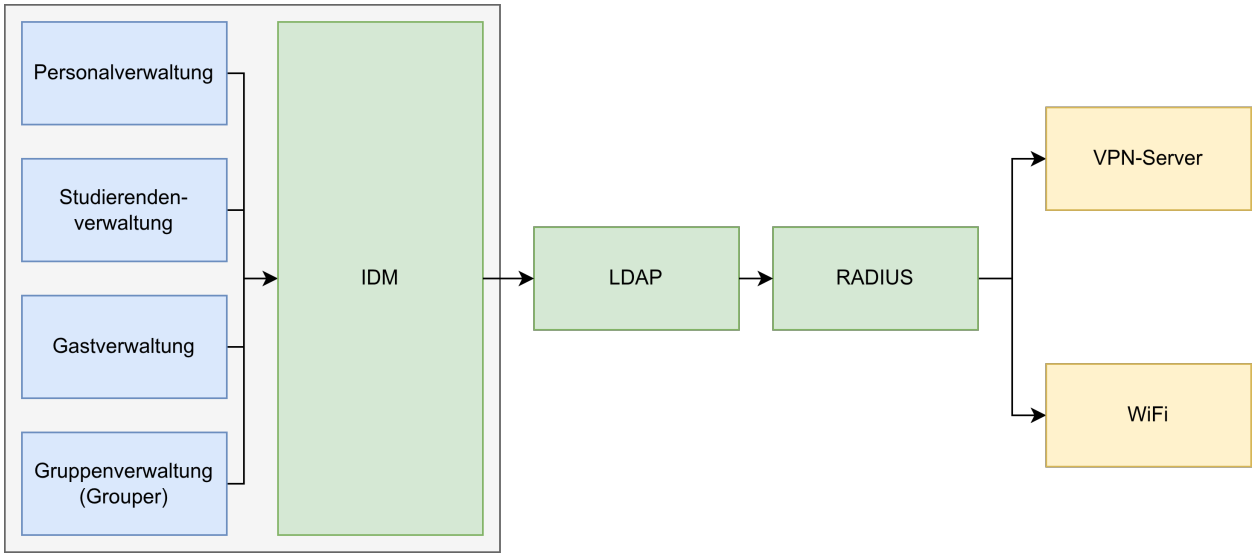
Darauf aufbauend wird eine Policy-Engine oder ein Vermittlungsdienst benötigt, der die Kontextinformationen in konkrete, netzwerktechnische Steueranweisungen übersetzt. In vielen Campusnetzwerken kommt hierfür ein RADIUS-Server zum Einsatz, der bei der Authentifizierung nicht nur den Zugriff erlaubt oder verweigert, sondern auch die zugehörige Policy (z. B. VLAN-Zuweisung, ACLs) dynamisch mitliefert. Moderne Systeme unterstützen zusätzlich attributbasierte Entscheidungen (ABAC), wodurch Policies noch granularer gesteuert werden können.

Abschließend ist eine Netzwerk-Infrastruktur erforderlich, die in der Lage ist, die übermittelten Policies auch tatsächlich umzusetzen. Das betrifft insbesondere Access Switches, WLAN-Controller oder Firewall-Systeme, die dynamische Zuweisungen wie VLAN-IDs, Access Control Lists (ACLs), Segment Tags (z. B. Cisco SGT, VXLAN-Tags) oder Quality-of-Service-Regeln interpretieren und anwenden können. Voraussetzung dafür ist, dass die eingesetz-

ten Komponenten die entsprechenden Standards unterstützen und in die zentrale Policy-Steuerung eingebunden sind.

Erst durch das Zusammenspiel dieser drei Ebenen – Datenquelle, Policy-Vermittlung und fähige Netzwerkkomponenten – kann eine flexible und kontextsensitive Netzwerkanbindung realisiert werden.

5.2 Beispielhafte Architektur für ein IDM-System



Die Grafik REFERENZ zeigt schematisch einen möglichen Aufbau zur Gruppenbasierten Zuordnung von Nutzer*Innen. Im Idealfall werden alle Benutzerkontexte in einem zentralen IDM gespeichert, dessen Daten sich aus verschiedenen Quellen speißen. Beispielsweise können aus Personal- und Studierendendatenbanken Daten importiert werden. Aus beiden Datenquellen ergibt sich automatisch die Zugerhörigkeit einer Person zu einer oder mehreren Organisationseinheiten. Die Zuordnung zu weiteren Gruppen sollte im Idealfall im self-service durch Verantwortliche Personne erfolgen können. Um die Anbindung an generische AAA-Dienste zu ermöglichen, können aus dem IDM Verzeichnisdienste befüllt werden. Als klassisches Beispiel dient hier ein LDAP-Server. Dieser kann dann wiederum als Datenquelle für einen RADIUS/TACACS Server benutzt werden, an den beispielsweise Wlan- oder VPN-Server angebunden werden können. Dabei kann der Radius-Server dann Zuordnungen zu Vlans/Profilen in seinem jeweiligen Auth-Flow an die Netzwerkgeräte übermitteln, durch die dann das entsprechende Mapping vorgenommen wird.

5.2.1 LDAP als Verzeichnisdienst

Ein LDAP-Server bildet Gruppenzugehörigkeit meist durch spezielle Objekttypen wie `groupOfNames`, `posixGroup` oder `groupOfUniqueNames` ab. Ein `groupOfNames`-Objekt enthält beispielsweise das Attribut `member`, das die Distinguished Names (DNs) der Benutzerobjekte referenziert.

Ein Benutzer mit dem Eintrag:

```
dn: uid=jdoe,ou=People,dc=example,dc=com
uid: jdoe
cn: John Doe
objectClass: inetOrgPerson
```

kann durch eine Gruppe zugeordnet werden, z.B.:

```
dn: cn=admins,ou=Groups,dc=example,dc=com
cn: admins
objectClass: groupOfNames
member: uid=jdoe,ou=People,dc=example,dc=com
```

Über eine LDAP-Abfrage wie:

```
(&(objectClass=groupOfNames)(member=uid=jdoe,ou=People,dc=example,dc=com))
```

lässt sich ermitteln, in welchen Gruppen `jdoe` Mitglied ist. Diese Information kann ein RADIUS- oder Kerberos-Backend wiederum verwenden, um Netzwerkkontexte zu mappen.

Beispielsweise könnte ein Benutzer der Gruppe `admins` automatisch in VLAN 10 zugewiesen werden oder Zugriff auf administrative Dateifreigaben erhalten.

Praktisch bedeutet das: Die LDAP-Attribute `member` (bei Gruppen) und `memberOf` (bei Benutzern, sofern das Schema dies unterstützt) bilden die Schnittstelle zwischen LDAPs Gruppenlogik und der dynamischen Netzwerk- bzw. Ressourcensteuerung.

5.2.2 Abbildung von Policies mittels RADIUS-Server

Viele Netzwerkgeräte unterstützen die Zuweisung von Netzwerkprofilen im 802.1x Authentication Flow. Dabei übermittelt ein Radius-Server nach der Authentisierung eine Liste von Attributen. Um beispielsweise eine Zuordnung eines Nutzer zu einem Vlan zu ermöglichen, kann folgender Attribut-Satz an kompatible Geräte übermittelt werden:

```
        Tunnel-Type = 13,
        Tunnel-Medium-Type = 6,
        Tunnel-Private-Group-ID = 100
```

Statisches Mapping im RADIUS-Server

Im einfachsten Fall wird im RADIUS-Server eine feste Zuordnung von LDAP-Gruppen zu RADIUS-Attributen hinterlegt. So könnte definiert sein, dass Mitglieder der Gruppe `admins` stets VLAN 10 zugewiesen wird, während Mitglieder der Gruppe `guests` in VLAN 20 platziert werden. Die Logik liegt dabei allein in der RADIUS-Konfiguration und wird nicht dynamisch von externen Diensten beeinflusst.

Dynamisches Mapping durch externe Dienste

Alternativ kann der RADIUS-Server Abfragen an externe Policy-Dienste oder Directory-Backends stellen. Diese liefern auf Basis der LDAP-Informationen die korrespondierenden Attribut-Sätze zurück. Dadurch ist es möglich, komplexere Regeln anzuwenden, wie etwa rollenbasierte Policies, zeitabhängige Zuweisungen oder Standortprofilierungen. Ein Vorteil dieser Variante liegt darin, dass die Netzwerkkontexte unmittelbar durch die Logik externer Systeme bestimmt werden können, ohne dass jede Regel im RADIUS-Config-File gepflegt werden muss.

5.2.3 Schrittweise Implementierung

Die Einführung kontextbasierter Netzwerkzuweisungen erfordert nicht zwingend die Umsetzung eines vollständig integrierten Gesamtsystems von Beginn an. Vielmehr bietet sich ein schrittweises Vorgehen an, bei dem einzelne Komponenten nach und nach aufgebaut oder erweitert werden können.

Ein zentrales Identity Management (IDM) mit umfassender Rollen- und Attributverwaltung ist zwar langfristig sinnvoll, aber nicht zwingend für erste Implementierungsschritte erforderlich. In frühen Phasen kann die Zuordnung von Entitäten zu Kontexten auch lokal und statisch erfolgen, beispielsweise durch festgelegte Regeln direkt auf dem RADIUS-Server. So

lassen sich einfache Policies – etwa die VLAN-Zuweisung basierend auf Benutzername oder MAC-Adresse – bereits ohne komplexe IDM-Integration umsetzen.

Auch die Policy-Verarbeitung und Netzwerkintegration kann modular aufgebaut werden. Einzelne Zugriffspunkte, etwa bestimmte WLAN-Segmente oder Testbereiche im LAN, können zunächst pilotiert werden, bevor eine Ausweitung auf größere Netzbereiche erfolgt. Auf diese Weise lässt sich die neue Architektur inkrementell einführen, ohne bestehende Systeme sofort vollständig umzustellen.

Ein solches Vorgehen reduziert nicht nur die Einstiegshürde, sondern ermöglicht auch eine kontrollierte Evaluierung der eingesetzten Technologien und Prozesse im Live-Betrieb – mit der Möglichkeit, bei Bedarf nachzusteuern oder die Integrationstiefe schrittweise zu erhöhen.

5.3 Zusammenfassung

Die vorgestellten Konzepte und Methoden verdeutlichen, dass eine kontextbasierte Netzwerkzuweisung nicht als monolithisches Gesamtsystem implementiert werden muss, sondern schrittweise eingeführt werden kann. Durch die Kombination von flexiblen Authentifizierungsverfahren wie 802.1X mit Realms, der Nutzung von RADIUS-basierten Policy-Übersetzungen und der Unterstützung durch geeignete Netzwerkinfrastruktur lässt sich eine dynamische, nutzerzentrierte Segmentierung realisieren. Auch für Geräte ohne Nutzeranmeldung bieten Mechanismen wie MAB pragmatische Lösungen, wenn auch mit Einschränkungen. Insgesamt ermöglicht dieses Vorgehen eine skalierbare, sichere und anpassungsfähige Integration heterogener Nutzerkontexte in Campusnetzwerke.

6 Ergebnis

Zusammenfassend zeigt sich, dass Netzwerkkontexte und deren Mappings einen zentralen Ansatzpunkt für die flexible Steuerung von Zugängen und Ressourcen darstellen. Mit RADIUS und LDAP stehen bewährte Technologien als Cornerstones zur Verfügung, die eine klare Trennung zwischen Identitätsmanagement und Netzwerkkontrolle erlauben. Gleichzeitig macht die Analyse deutlich, dass die erfolgreiche Einbindung in unterschiedliche Netzwerkarchitekturen eine sorgfältige Planung und ein abgestimmtes Design erfordert. Ein weiterer wichtiger Befund ist, dass Kontextsysteme nicht zwingend als monolithische Gesamtlösung umgesetzt werden müssen, sondern sich auch schrittweise einführen lassen. Damit eröffnen sich praxisnahe Wege, um bestehende Infrastrukturen graduell anzureichern und zugleich die Grundlage für dynamische, zukunftsfähige Sicherheits- und Zugriffskonzepte zu schaffen.

7 Versionsverlauf

Version	Datum	Änderungen
1.0	15.09.2025	Initiale Veröffentlichung