BWCAMPUSNETZ

Zukunftsfähige Konzepte für die Campusnetze
an Universitäten und Hochschulen

LAN-Zugang für Benutzer, Geräte und IoT-Devices

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

Inhalt

1 Anforderungen 3

2 Erfahrungen 4

3 Fazit 9

Anhang 11

4 Versionsverlauf 15

1 Anforderungen

Der Einsatz von kabelgebundenem 802.1X wird momentan am Informationszentrum der Universität Stuttgart (IZUS/TIK) im Kontext des Projekts bwCampusnetz weiterentwickelt und praktisch erprobt. Ziel ist die Implementierung eines authentifizierten Netzzugangs im LAN ähnlich zu eduroam im WLAN. Aktuell besteht eine der Herausforderungen am IZUS/TIK darin, dass Netzwerkdosen praktisch ausnahmslos statisch konfiguriert werden, was sehr betreuungs- und beratungsintensiv ist. Insgesamt sind mehr als 50000 Switchports auf dem Campus der Universität Stuttgart vorhanden, die statisch konfiguriert werden, wobei Änderungen – z.B. wenn ein Raum und die darin vorhandenen Datenanschlüsse von einer anderen Organisationseinheit genutzt werden sollen – jeweils mit den Administratoren der beiden Einrichtungen abzustimmen sowie der Nutzung nachzuführen sind. Zudem gibt es immer weniger Administratoren, welche ausreichend Netzwerkkenntnisse vorweisen und die gegenüber dem Rechenzentrum als Ansprechpartner hinsichtlich Themen wie Netzwerksegmentierung oder Firewalling dienen könnten. Viele Institute steigen aufgrund dessen auf gemanagte Geräte um. Aus diesen Gründen wäre die Einführung eines Netzes mit so genannten „colorless ports“ wünschenswert, ähnlich zu „eduroam“ im drahtlosen Netz, in welches Nutzer nach abgeschlossener (bzw. erfolgter) Authentifizierung per 802.1X am Switchport gelangen und dem jeweiligen VLAN (d.h. Sicherheitskontext) zugeordnet werden.

Zusätzlich wird in Zeiten von Shared Offices die dynamische Zuordnung von Sicherheitskontexten über 802.1X immer notwendiger. Durch die Nutzung des 802.1X-Standards können Benutzer automatisch authentifiziert und autorisiert werden. Zudem ermöglicht die dynamische Zuordnung von Sicherheitskontexten, dass jeder Nutzer vollautomatisch die benötigten Berechtigungen erhält, ohne dass manuelle Eingriffe erforderlich sind.

2 Erfahrungen

Am IZUS/TIK wird 802.1X im kabelgebundenen Bereich momentan erprobt. Dabei kommen verschiedene EAP-Methoden zum Einsatz, darunter EAP-PEAP, EAP-TTLS und EAP-TLS. Diese Erprobungen werden und wurden auf unterschiedlichen Plattformen durchgeführt, einschließlich macOS, Linux (über NetworkManager und wpasupplicant) sowie Windows (mithilfe des nativen Supplicants sowie des Cisco Network Access Modules).

Eine wesentliche Herausforderung stellt dabei die manuelle Konfiguration der Client Betriebssysteme, insbesondere auf dem nativen Windows Supplicant, dar. Benutzer müssen diverse Schritte durchlaufen, um die korrekten Zertifikate und Anmeldeinformationen einzurichten, was nicht nur zeitaufwändig ist, sondern – trotz ausführlicher Anleitungen – erfahrungsgemäß auch häufig zu Fehlern führt, die zusätzlichen Support erfordern. Selbiges gilt für das Cisco Network Access Module, bei dem zunächst ein Profil erstellt werden muss. Aufgrund der Komplexität und des Aufwands bei der manuellen Konfiguration von 802.1X ist man hier auf zusätzliche Skripte angewiesen, die man den Endanwendern bereitstellen müsste. Diese Skripte automatisieren den gesamten Konfigurationsprozess, einschließlich der Auswahl von Zertifikaten und der Einrichtung der notwendigen Netzwerkeinstellungen. Die Einrichtung von 802.1X konnte dadurch deutlich erleichtert werden. Allerdings setzt dies, unabhängig davon, ob es sich um ein PowerShell- oder ein CMD-Skript handelt, voraus, dass der Nutzer auf dem entsprechenden Endgerät über Administratorrechte verfügt.

Alternativ kann die Konfiguration auch zentralisiert und automatisiert über Mobile Device Management (MDM) Lösungen oder Gruppenrichtlinienobjekte (Group Policy Objects, GPO) für alle Rechner, die in ein Windows Active Directory (AD) integriert sind, erfolgen. Zudem kann die automatische Verteilung und Verwaltung der benötigten Zertifikate über das Simple Certificate Enrollment Protocol (SCEP) realisiert werden. Technisch sind diese Ansätze umsetzbar, doch sie erfordern entsprechendes Personal für die Planung, Implementierung und vor allem laufende Betreuung. Darüber hinaus sind, wie eingangs erwähnt, solche zentralisierten Ansätze in BYOD-Umgebungen nicht ohne Weiteres umsetzbar. Geräte stehen nicht unter zentraler Verwaltung und so lassen sich weder GPOs noch MDM-Lösungen flächendeckend einsetzen. In solchen Szenarien bleibt die manuelle Konfiguration oder die

Bereitstellung von Skripten oft die einzige praktikable Option - mit den bereits beschriebenen Herausforderungen.

Die praktischen Erprobungen am IZUS/TIK haben ergeben, dass – anders als unter Microsoft Windows - 802.1X im kabelgebundenen Bereich mit bereitgestellten Profilen unter macOS sowie unter dem Linux NetworkManager problemlos funktioniert. Unter macOS können Administratoren vordefinierte Profile erstellen und bereitstellen, die alle notwendigen Einstellungen und Zertifikate enthalten, sodass die Benutzer diese Profile einfach importieren und sich ohne weitere Konfigurationen sicher mit dem Netzwerk verbinden können. Auf Linux-Systemen bietet der NetworkManager eine benutzerfreundliche Oberfläche zur Verwaltung von Netzwerkeinstellungen, einschließlich 802.1X-Authentifizierung.

Zusammengefasst wäre ein kabelgebundenes 802.1X-Profilmanagement eine skalierbare und effiziente Lösung für Hochschulen, die eine App, sei es für das Smartphone oder den Laptop, für verschiedene Anwendungen wie Mensa-Services oder Lern-Management nutzen. Für Einrichtungen, die bereits über solche Apps verfügen, könnte das 802.1X-Profilmanagement nahtlos integriert werden. Falls eine solche zentrale Multifunkions-App nicht vorhanden ist, ist die Einführung einer dedizierten App nur für die 802.1X-Konfiguration grundsätzlich denkbar; es muss jedoch Aufwand und Nutzen abgewogen werden, wobei bei den Aufwänden nicht nur die Erstellung der App zu berücksichtigen sind, sondern auch Informationskampagnen und Support für eine neue, bis dato unbekannte App.

Darüber hinaus muss beachtet werden, dass gerade bei der Nutzung von EAP-TLS, auf Seiten der Netzwerkabteilung ein erheblicher Supportaufwand, insbesondere wenn eine unternehmensinterne Public Key Infrastructure (PKI) betrieben wird, entsteht. Der Lebenszyklus der Zertifikate erfordert eine regelmäßige Erneuerung und Pflege der Client-Profile, was den administrativen Aufwand steigen lässt. Auch müssen neben der Ausstellung, Verlängerung und Sperrung von Zertifikaten gegebenenfalls Certificate Revocation Lists (CRL) oder Online Certificate Status Protocol (OCSP) Responder aktuell gehalten werden.

Des Weiteren kann es notwendig sein, die CA zu wechseln, etwa aufgrund ablaufender Root-Zertifikate oder einer Migration auf eine modernere PKI-Lösung. Als Folge dessen müssen alle Endgeräte mit neuen Zertifikaten versorgt werden, weshalb oft eine manuelle Neukonfiguration erforderlich ist.

Darüber hinaus erfordert der Betrieb einer privaten PKI gegebenenfalls regelmäßige Sicherheitsüberprüfungen, Audits sowie die Einhaltung von Compliance Vorgaben, was zusätzliche

personelle und finanzielle Ressourcen bindet. Auch die Verwaltung von Schlüsselmaterial, Hardware Security Modules (HSM) und die Schulung der IT-Administratoren stellen weitere Herausforderungen dar, die nicht zu unterschätzen sind.

Ein weiteres, Windows-spezifisches Problem besteht darin, dass unter dem nativen Windows Supplicant nicht zwei Profile für denselben Netzwerkadapter festgelegt werden können, sondern man ein anderes Windows-Benutzerprofil verwenden muss. Dieser Bedarf besteht, wenn eine Person mehrere Rollen innerhalb der Einrichtung oder gar einrichtungsübergreifend innehat und abhängig davon in unterschiedliche Sicherheitskontexte eingebunden werden muss. Diese Einschränkung erhöht den Aufwand und die Komplexität für die Benutzer erheblich. Daher wird eine Lösung benötigt, die sowohl die internen Bedürfnisse und Anforderungen der Organisation als auch die Fähigkeiten der Nutzer berücksichtigt und gleichzeitig eine praktikable Servicability gewährleistet.

Hinzu kommt, dass wenn ein Rechner, der für 802.1X konfiguriert ist, den Standort wechselt und sich an einem Nicht-802.1X-Port anmeldet, dies je nach Betriebssystem dazu führen kann, dass der Client keine Netzverbindung mehr erhält. Unter Linux muss beispielsweise ein anderes Netzwerkprofil verwendet werden, um an Nicht-802.1X-Ports eine Verbindung herzustellen. Dies bedeutet, dass Benutzer manuell zwischen Profilen wechseln müssen, was jedoch mit dem NetworkManager kein Problem darstellt.

Bei der praktischen Erprobung und der damit verbundenen Fehlersuche und -analyse hat es sich als problematisch herausgestellt, dass in vielen Fällen es nicht immer eindeutig ist, ob das Problem auf der Switch-Seite, der Client-Seite oder sogar auf der RADIUS-Seite liegt. Diese Unklarheit kann die Fehlerbehebung erheblich erschweren.

In Forschung und Lehre, insbesondere im Bereich der Natur- und Ingenieurwissenschaften, gibt es neben den Endgeräten der „klassischen“ Informations- und Kommunikationstechnik einen sehr hohen Bedarf an - und dementsprechend eine sehr hohe Verbreitung von – „Internet of Things“ (IoT) - Geräten, z.B. Messgeräten, Robotern, Werkzeugmaschinen usw. mit eingebauten Steuer-Rechnern und Netzwerkanschluss. Viele dieser Systeme verfügen über einen – verglichen mit normalen PCs – reduzierten Funktionsumfang des Betriebssystems bzw. eingeschränkte Konfigurationsmöglichkeiten. Im Zusammenhang mit 802.1X stellt dies eine weitere Herausforderung dar, da viele dieser Geräte kein EAP-PEAP, EAP-TTLS oder EAP-TLS unterstützen. Ein möglicher Lösungsansatz wäre die Implementierung einer MAC-basierenden Authentifizierung (als Fallback zu 802.1X). Dabei werden die MAC-Adressen der IoT-Geräte in einer Whitelist auf dem RADIUS-Server bzw. einer Datenbank hinterlegt, welche der RADIUS-Server dynamisch abfragt. Sobald ein Gerät eine Verbindung herstellt, sendet der Switch eine Anfrage an den RADIUS-Server, welcher wiederum ein Access-Accept oder Access-Reject an den Switch zurückgibt.

Hierbei stellt sich allerdings die Frage, inwiefern eine auf der MAC-Adresse basierende Authentifizierung einen ausreichenden Schutz darstellt. Diese Abwägung ist dabei organisationsintern unter Berücksichtigung aller relevanten Schutzziele zu treffen.

Ebenfalls könnte ein separates VLAN für IoT-Geräte mit spezifischen Zugriffsrichtlinien eingerichtet werden. Dabei kann es sich auch um ein so genanntes Guest Vlan handeln, in welches Geräte gelangen, die kein 802.1X konfiguriert haben, auch wenn 802.1X auf dem Port konfiguriert ist. Die Problematik hierbei ist allerdings dieselbe, wie bei Ports ohne 802.1X, dass dadurch jeder Zugang zu diesem Netz erlangen kann, der sich nur mit einer der entsprechend konfigurierten Dosen verbindet.

Darüber hinaus muss erwähnt werden, dass 802.1X zwar eine wichtige Grundlage für die Netzwerksicherheit darstellen kann, es jedoch allein nicht ausreicht, um alle Sicherheitsanforderungen innerhalb eines LAN-Segments zu erfüllen. Aufgrund dessen ist es notwendig, 802.1X mit weiteren First-Hop-Security Mechanismen zu kombinieren. Dies können beispielsweise Schutzmaßnahmen gegen MAC-, DHCP- oder ARP-Spoofing sein. Möchte man zudem eine vollständige Client-Isolation sicherstellen, sodass Clients im selben Layer-2-Segment nicht miteinander kommunizieren können, kommen Technologien wie Private VLANs (PVLANs) zum Einsatz.

3 Fazit

Das 802.1X-Protokoll bietet eine nutzerbasierte Authentisierung und Autorisierung für einen sicheren und kontrollierten Zugang zum Netzwerk, der – zumindest auf dem Papier – sowohl in drahtgebundenen als auch in drahtlosen lokalen Netzen eingesetzt werden kann. In der Praxis hat sich jedoch gezeigt, dass diese Technik nur in drahtlosen WLAN-Netzen eine gute Unterstützung in den Client-Betriebssystemen hat und erfolgreich großflächig eingesetzt werden kann (z.B. bei „eduroam“); in den drahtgebundenen Ethernet-Netzen gilt es hingegen eine Reihe von Herausforderungen zu lösen.

Für zentral gemanagte Endgeräte stellt 802.1X eine praktikable und effektive Lösung dar. Durch eine zentralisierte Verwaltung und vordefinierte Profile kann die Implementierung von 802.1X auf diesen Geräten effizient durchgeführt werden.

An einer Universität bzw. Hochschule gibt es jedoch eine Vielzahl unterschiedlicher Geräte, die von dezentralen Beauftragten an den Instituten verwaltet werden, sowie von Studierenden mitgebrachte Privat- Geräte (BYOD) und „Internet of Things“ (IoT)-Geräte. Die Vielfalt der Geräte, deren unterschiedliche Betriebssysteme sowie Konfigurationen führen hierbei zu einer Steigerung der betrieblichen Gesamtkosten.

Eine mögliche Alternative ist es, für „klassische“ Endgeräte der Informations- und Kommunikationstechnik, insbesondere für Laptops, einen Netzwerkzugang ohne 802.1X-Authentisierung bereitzustellen, der keinen direkten Zugang zum Internet oder anderen schützenswerten Ressourcen bietet, sondern nur den Aufbau einer VPN-Verbindung zum VPN-Server der Universität bzw. Hochschule ermöglicht. In Zeiten von verstärktem ortsunabhängigem Arbeiten („home office“) kann davon ausgegangen werden, dass auf der Mehrzahl der Geräte bereits ein VPN- Client konfiguriert wurde, so dass der Zusatzaufwand für Konfiguration und ggf. Fehlersuche bei 802.1X entfallen kann. Für die IoT-Geräte, die im Regelfall keinen VPN-Client unterstützen können, bietet sich MAC- Authentication-Bypass als vergleichsweise einfach zu administrierende Lösung an, die gegenüber einem gänzlich ungesicherten Netzzugang dennoch einen gewissen Sicherheitsgewinn darstellt. Eine wichtige Entwicklung im Bereich der Campusnetze ist, dass drahtloser WLAN-Zugang nicht mehr nur als Ergänzung der drahtgebundenen Anschlüsse – z.B. für gelegentliche Nutzung im Besprechungsraum – verstanden wird, sondern verstärkt als primärer, oft auch einziger Netzzugang verwendet wird. Die

Technik und Standardisierung der WLANs hat sich rasant fortentwickelt und ermöglichen hohe Übertragungsraten und eine hohe Zuverlässigkeit. Aus Sicht der Nutzer ergibt sich ein Komfort-Gewinn, da bei mobilen Geräten keine Netzwerk-Leitungen mehr ein- und ausgesteckt werden müssen; neuere Laptops haben dementsprechend oft gar keine Ethernet-Buchse mehr, aber auch stationäre PCs werden heute standardmäßig mit WLAN- Adapter ausgeliefert. Aus Sicht der Betreiber stellt diese Entwicklung zunächst eine gewisse Herausforderung dar – schließlich müssen für eine flächendeckende WLAN-Ausleuchtung sehr viele WLAN Access Points beschafft und installiert werden und dies erfordert Datenanschlüsse an der Decke. Langfristig kann diese Umstellung aber durchaus wirtschaftlich sein, wenn dementsprechend weniger drahtgebundene Anschlüsse und somit weniger Leitungen und Switchports benötigt werden. Bezüglich der nutzerbasierten Authentifizierung und Autorisierung beim Netzzugang lässt sich feststellen, dass die dafür benötigten Mechanismen im WLAN von den Herstellern deutlich besser unterstützt werden und deutlich weniger fehleranfällig sind als im drahtgebundenen Netz. Nicht zuletzt vor diesem Hintergrund erscheint eine „mobile first strategy“ – d.h. primärer Netzzugang für „normale“ Nutzer ist WLAN-basiert, drahtgebundene Anschlüsse nur für Sonderanwendungen (z.B. besonders datenintensive Graphikworkstations), die keine große Mobilität aufweisen und idealerweise keine nutzerbasierte Authentisierung und Autorisierung benötigen – eine sinnvolle Herangehensweise bei der Fortentwicklung der Campusnetze.

Anhang

Im folgenden Abschnitt werden die notwendigen Konfigurationsschritte für die 802.1X sowie nachrangig die MAC Authentication Bypass Authentifizierung auf Cisco Catalyst Switches (Version 17.12) sowie auf Aruba CX Switches (Version 10.13) beschrieben und erläutert. Die Konfiguration weiterer portbasierter Features, wie beispielsweise Spanning-Tree, wird nicht abgebildet. Es wird ebenfalls darauf verzichtet, alle vorhandenen Befehle in Zusammenhang mit 802.1X und MAB vollständig aufzuzeigen und zu erläutern. Für weiterführende Informationen zu diesen Themen wird auf die offizielle Cisco- sowie Aruba-Dokumentation verwiesen.[1] [2]

Cisco Catalyst IOS-XE

Initial muss, damit Clients per 802.1X am Switchport authentifiziert werden können, der folgende Befehl global konfiguriert werden:

```
dot1x system-auth-control
```

Im Weiteren ist dabei die port-spezifische 802.1X und MAB Konfiguration unter Cisco IOS-XE abgebildet, wobei hierbei standardmäßig der Single-Host Mode Anwendung findet. Neben dem Single-Host Mode, welcher es erlaubt maximal ein Gerät in der Data Domain sowie ein Cisco Telefon in der Voice Domain zu betreiben, existieren folgende weitere Authentifizierungsmethoden:

- Multi-Auth: Mehrere Geräte in der Data Domain sowie ein (Cisco- oder non-Cisco) Gerät in der Voice Domain.
- Multi-Domain: Maximal ein Gerät in der Data Domain sowie ein (Cisco- oder non-Cisco) Gerät in der Voice Domain.
- Multi-Host: Das erste Gerät wird authentifiziert, wobei bei erfolgreicher Authentifizierung alle weiteren am Port angeschlossenen Geräte zugelassen werden.

```
interface GigabitEthernet1/0/1
    switchport access vlan <vlan-id>
    switchport mode access
    switchport nonegotiate
    ! Setzt MAB als Fallback zu 802.1X
    authentication order dot1x mab
    authentication priority dot1x mab
    ! Aktiviert 802.1X
    authentication port-control auto
    ! Aktiviert MAC Authentication Bypass
    mab
    ! Konfiguriert Port als Authenticator
    dot1x pae authenticator
    dot1x timeout tx-period <sekunden>
    dot1x max-reauth-req <anzahl>
```

Darüber hinaus wurde MAB als Fallback zu 802.1X konfiguriert. Folglich werden alle Hosts, die 802.1X nicht unterstützen, per MAB authentifiziert. Dabei kann mittels **dot1x max-reauth-req** die Anzahl der Reauthentifizierungsversuche konfiguriert werden. Die Wartezeit zwischen Authentifizierungsversuchen kann mittels **dot1x timeout tx-period** konfiguriert werden. Abhängig von den Anforderungen kann hier eine höhere Anzahl an Authentifizierungsversuchen und/oder ein größerer Abstand zwischen den Authentifizierungsversuchen konfiguriert werden.

Möchte man dem Nutzer ein Vlan zuweisen, auch wenn dessen Authentifizierung fehlschlägt (Authentication-Failed Vlan), keine Antwort vom Authentication Server kommt (Server-Dead Vlan) oder der Client kein 802.1X unterstützt (Guest Vlan), ist dies über folgende Interface Konfiguration möglich:

```
! Authentication-Failed VLAN
authentication event fail retry <anzahl> action authorize vlan <vlan>
! Server-Dead VLAN
authentication event server dead action authorize vlan <vlan>
! Guest VLAN: Falls keine Antwort vom Client kommt
authentication event no-response action authorize vlan <vlan>
```

Alternativ hat man mittels dem Statement **authentication open** die Möglichkeit, einem Nutzer bereits vor der Authentifizierung per 802.1X ein Vlan zuzuweisen.

HPE Aruba CX

Im Folgenden ist die port-spezifische 802.1X und MAB Konfiguration unter Aruba CX abgebildet, wobei hierbei standardmäßig der Client-Mode Anwendung findet. Hier müssen sich alle Geräte sowohl in der Data- als auch Voice-Domain authentifizieren. Darüber hinaus existieren folgende zwei Authentifizierungsmethoden:

- Device-Mode: Das erste Gerät wird authentifiziert, wobei bei erfolgreicher Authentifizierung alle weiteren am Port angeschlossenen Geräte zugelassen werden.
- Multi-Domain: Standardmäßig maximal ein Gerät in der Data Domain sowie ein Gerät in der Voice Domain, wobei das Limit auf bis zu fünf Geräte in der Data Domain erhöht werden kann.

Darüber hinaus kann der EAPoL Timeout, die maximale Anzahl an EAPoL Anfragen sowie die Anzahl der Reauthentifizierungsversuche mittels **eapol-timeout**, **max-eapol-requests** und **max-retries** konfiguriert werden.

```
interface 1/0/1
    no shutdown
    no routing
    vlan access <vlan-id>
    ! Aktiviere 802.1X
    aaa authentication port-access dot1x authenticator
        radius server-group dot1x
        eapol-timeout <sekunden>
        max-eapol-requests <anzahl>
        max-retries <anzahl>
        enable
    ! Aktiviere MAB
    aaa authentication port-access mac-auth
        enable
        radius server-group dot1x
```

Ebenfalls besteht die Möglichkeit dem Nutzer Port-Access Rollen und damit Vlans zuzuweisen, falls die Authentifizierung fehlschlägt (reject-role) oder der Authentifizierungsserver nicht erreichbar ist (critical-role). Allerdings müssen die Rollen vorher global definiert werden.

```
port-access role rejected
    vlan access <vlan-id>
port-access role critical
    vlan access <vlan-id>
interface 1/0/1
    aaa authentication port-access reject-role rejected
    aaa authentication port-access critical-role critical
```

Möchte man dem Nutzer bereits vor der Authentifizierung eine Rolle bzw. ein Vlan zuweisen, ähnlich **authentication open** unter Cisco IOS-XE, kann dies über die preauth Rolle konfiguriert werden.

```
port-access role preauth
    vlan access <vlan-id>
interface 1/0/1
    aaa authentication port-access preauth-role preauth
```

Global wird darüber hinaus PAP als Authentifizierungsmethode für MAB konfiguriert:

```
aaa authentication port-access mac-auth
    auth-method pap
    enable
```

4 Versionsverlauf

Version	Datum	Änderungen
1.0	22.03.2025	Initiale Veröffentlichung

Literatur

[1] *ISE Secure Wired Access: Prescriptive Deployment Guide*. Adresse: https://community.cisco.com/t5/security-knowledge-base/ise-secure-wired-access-prescriptive-deployment-guide/ta-p/3641515 (besucht am 31. 12. 2025).

[2] *Aruba AOS-CX 10.13 Security Guide*. Adresse: https://arubanetworking.hpe.com/techdocs/AOS-CX/10.13/PDF/security_6200-6300-6400.pdf (besucht am 31. 12. 2025).