Segmentierung von Schulnetzwerken / WLAN-Infrastruktur

Netzwerksegmentierung bezieht sich auf die Aufteilung eines Computernetzwerks in kleinere Teile, um Leistung, Sicherheit und das Management zu verbessern. Diese Segmentierung kann auf verschiedenen Ebenen und mit verschiedenen Technologien erfolgen. Hier sind einige Schlüsselaspekte der Netzwerksegmentierung, insbesondere als Grundlage einer WLAN-Infrastruktur.

- Verbesserte Sicherheit: Durch die Segmentierung eines Netzwerks können sensible Daten oder Systeme in separaten Segmenten isoliert werden. Dies hilft, die Ausbreitung von Sicherheitsbedrohungen zu begrenzen und ermöglicht eine genauere Überwachung und Kontrolle über die Zugriffe auf verschiedene Netzwerkbereiche. In einem WLAN ist die Trennung von Netzwerksegmenten besonders wichtig, um sicherzustellen, dass nur autorisierte Nutzer Zugang zu sensiblen Daten oder Diensten haben. Durch die Segmentierung können Gastnetzwerke von internen Netzwerken getrennt werden, was verhindert, dass externe Nutzer Zugriff auf interne Ressourcen erhalten.
- Leistungsmanagement: Netzwerksegmentierung kann die Netzwerkleistung verbessern, indem sie den lokalen Verkehr innerhalb eines Segments hält und somit die Belastung des Gesamtnetzwerks reduziert. Dies kann besonders in großen Netzwerken mit hohem Datenaufkommen wichtig sein. Drahtlose Netzwerke können durch zu viele Geräte oder hohe Datenübertragungsraten überlastet werden. Durch die Segmentierung können Bereiche des Netzwerks (z.B. Abteilungen innerhalb einer Firma oder unterschiedliche Stockwerke in einem Gebäude) isoliert werden, um die Netzwerkleistung zu optimieren.
- Fehlerisolierung: Bei Problemen in einem Netzwerksegment ist es einfacher, die Fehlerursache zu identifizieren und zu beheben, ohne das gesamte Netzwerk zu beeinträchtigen. Dies kann besonders in komplexen Netzwerken mit vielen Nutzern und Geräten hilfreich sein.
- Zugriffskontrolle und Compliance: Segmentierung erleichtert die Durchsetzung von Zugriffskontrollrichtlinien und kann dabei helfen, Compliance-Anforderungen zu erfüllen, indem sie sicherstellt, dass nur autorisierte Benutzer Zugang zu bestimmten Netzwerkressourcen haben.

Technisch kann die Netzwerksegmentierung auf verschiedene Weise umgesetzt bzw. unterstützt werden:

- VLANs (Virtual Local Area Networks): Hierbei werden logische Unterteilungen in einem physischen Netzwerk vorgenommen. Jedes VLAN hat seine eigene Broadcast-Domäne, was die Netzwerkleistung verbessert, und die Sicherheit erhöht.
- Subnetting: Durch die Aufteilung eines größeren Netzwerks in kleinere Subnetze können IP-Adressen effizienter verwaltet und der Netzwerkverkehr besser kontrolliert werden.
- Firewalls und Netzwerkzugangskontrolle (NAC): Diese Technologien können eingesetzt werden, um den Verkehr zwischen Netzwerksegmenten zu überwachen und zu kontrollieren.

Segmentierungsmöglichkeiten an Schulen

In Schulen gilt es, individuelle Anforderung hinsichtlich des Lehrprofils und der Anzahl der Endgeräte sowie deren unterschiedliche Einsatzzwecke zu berücksichtigen. Die wesentlichen Bereiche dürften folgendermaßen abgedeckt sein:

- Default-VLAN: Dieses Segment ist für die Verwaltung der Netzwerkinfrastruktur wichtig und sollte streng abgesichert sein, um unbefugten Zugriff zu verhindern.
- Ressourcen: Dieses Segment für Dienste wie Drucker und Mirroring-Adapter ist sinnvoll, um diese Ressourcen zentral zu verwalten und den Zugriff darauf zu kontrollieren.

- Verwaltung: Ein spezielles Segment für die Schulverwaltung ermöglicht es, sensible Daten und Anwendungen zu schützen, die für die Verwaltung der Schule notwendig sind.
- BYOD/Gast: Dieses Segment für Bring Your Own Device (BYOD) und Gäste gewährleistet, dass der Zugang zum Internet isoliert vom restlichen Netzwerk erfolgt, was die Sicherheit erhöht.
- Unterricht: Ein spezielles VLAN für den Unterrichtsbereich ermöglicht es, Lehrmaterialien und Anwendungen sicher und effizient zu verteilen.

Zusätzlich können noch weitere Segmente in Betracht gezogen werden:

- Multimedia-/Labor-Bereiche: Für spezielle Klassenräume oder Labore, die auf Multimedia-Inhalte oder spezielle Software angewiesen sind, könnte ein eigenes VLAN sinnvoll sein.
- Sicherheit und Überwachung: Für Sicherheitskameras und andere Überwachungsgeräte könnte ein separates VLAN sowohl aus Sicherheitsgründen als auch zur Leistungsoptimierung vorteilhaft sein.
- Haustechnik: Diverse Teile der Gebäudetechnik erfordert Anschluss an die Netzwerkinfrastruktur.
- Schüler- bzw. Unterrichtsgruppen: separate Netzwerksegmente für Schüler in unterschiedlichen Kursen oder Jahrgangsstufen könnte Service und Sicherheit bieten, insbesondere wenn es um die geschützte Nutzung des Internets und den Zugriff auf bestimmte Ressourcen geht.
- Lehrer/Fachschaften: Ein eigenes Segment für Lehrkräfte könnte hilfreich sein, um ihnen Zugriff auf Lehrmaterialien und administrative Ressourcen zu geben, die für andere Kollegen oder Schüler nicht zugänglich sein sollen.

Um ein für die Schule passendes Segmentierungskonzept zu erstellen ist ein Verständnis für die Komplexität und die Auswirkungen notwendig:

Vorteile bei zunehmender Segmentierung	**Nachteile bei zunehmender Segmentierung**
• Bessere Netzwerkperformance: Mehr Segmente können die Netzwerkleistung verbessern, da der lokale Verkehr innerhalb der Segmente bleibt und so weniger Bandbreite auf Hauptverkehrswegen beansprucht wird. • Erhöhte Sicherheit: Mit mehr Segmenten lässt sich der Netzwerkzugriff genauer kontrollieren. Sensitive Bereiche können effektiver isoliert und geschützt werden. • Einfachere Fehlersuche und Wartung: Probleme lassen sich in kleineren, gut definierten Segmenten schneller identifizieren und beheben. • Bessere Skalierbarkeit: Ein segmentiertes Netzwerk kann einfacher erweitert und an veränderte Bedürfnisse angepasst werden. • Effektivere Zugriffskontrolle: Die Segmentierung ermöglicht eine feingranulare Zugriffskontrolle und hilft bei der Durchsetzung von Compliance-Vorschriften.	• Größerer initialer Planungs- und Implementierungsaufwand: Die Einrichtung eines stark segmentierten Netzwerks erfordert eine sorgfältige Planung und ist zeitintensiver. • Erhöhter Verwaltungsaufwand: Mehr Segmente bedeuten auch mehr zu verwaltende Einheiten, was den administrativen Aufwand erhöht. • Komplexität in der Wartung: Mit zunehmender Anzahl an Segmenten kann die Netzwerkwartung komplizierter und zeitaufwendiger werden. • Erhöhte Kosten: Mehr Segmente können zu höheren Kosten führen, sowohl in Bezug auf die benötigte Hardware als auch bei der laufenden Wartung und Verwaltung.

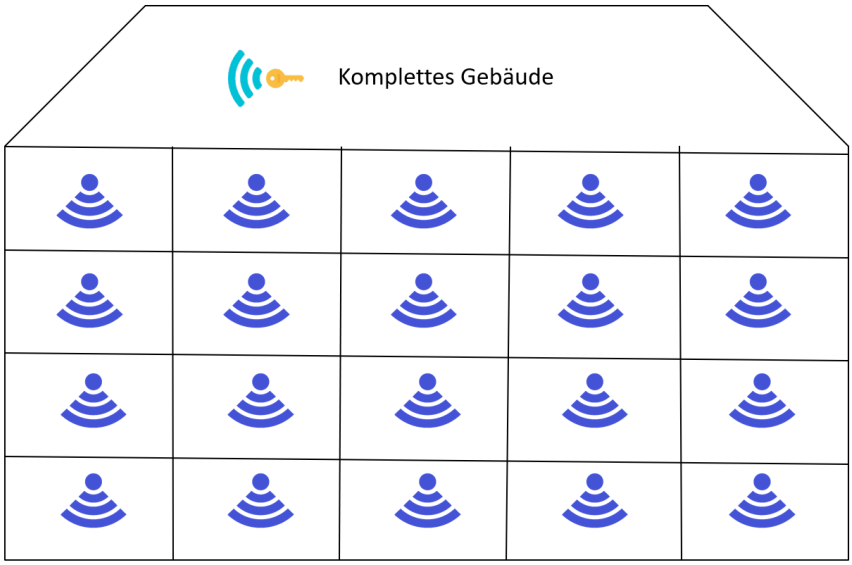
Insgesamt ist es wichtig, ein Gleichgewicht zwischen der Anzahl der Segmente, den Sicherheitsanforderungen, der Netzwerkleistung und den zur Verfügung stehenden Ressourcen zu finden. Die optimale Anzahl und Art der Segmentierung hängen von den spezifischen Bedürfnissen und Anforderungen des jeweiligen Netzwerks ab.

Beispiele für WLAN-Infrastruktur an Schulen auf Basis von Netzwerksegmentierung

Für jede Schule kann ein individuelles Segmentierungskonzept entstehen. Drei Beispiele, welche sich in manchen Belangen sehr deutlich voneinander unterscheiden, seinen folgend kurz vorgestellt:

Ein Segment

Ein Netzwerk für den kompletten Unterricht einer Schule.

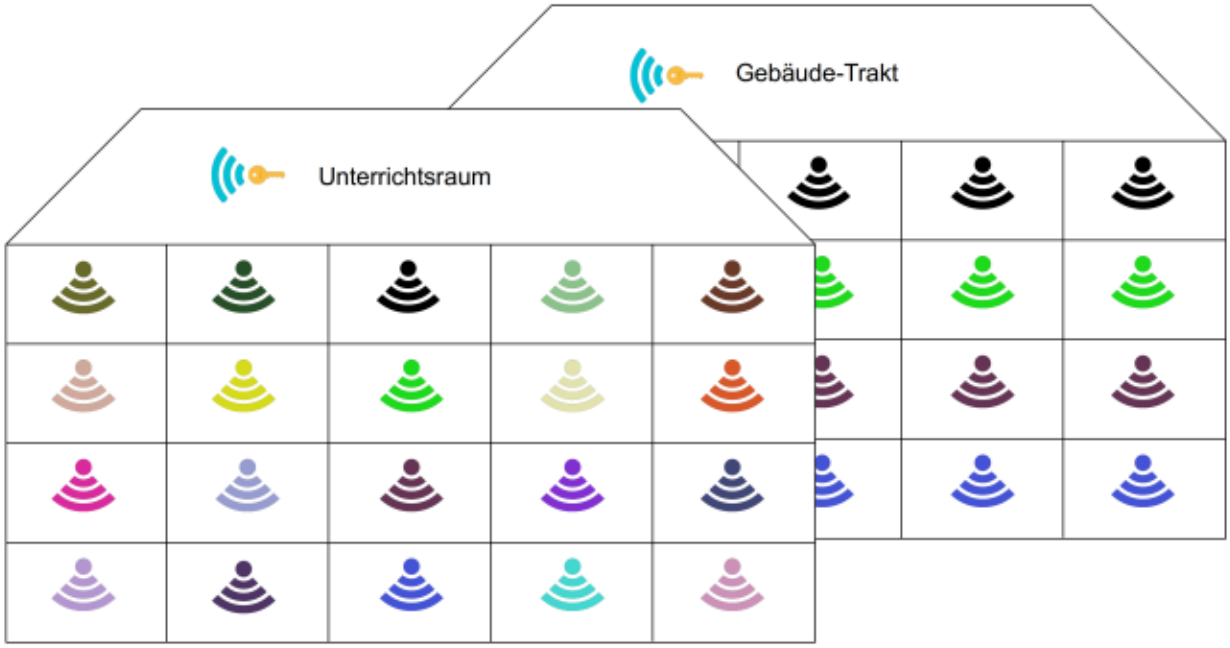


Wenn man für den kompletten Unterricht nur ein Netzwerksegment bereitstellt, muss das nicht unbedingt heißen, dass es keine Segmentierung per VLAN-Technologie an der Schule gibt. Das Verwaltungsnetz wird wohl vom Unterrichtsnetz verlässlich abgetrennt sein. Die notwendige Zahl an IP-Adressen wird durch die Verwendung einer 16-bit Netzwerkmaske (16.534 Adressen) sichergestellt.

Vorteile	Nachteile
• Einfache Einrichtung, geringer Verwaltungsaufwand. • Eine SSID im WLAN gewährleistet einen geringen WLAN-Overhead.	• Große Broadcastdomäne sorgt für einen hohen Anteil an Broadcast-Overhead im Datenverkehr. • Bei Störungen erstreckt sich das Troubleshooting über das ganze Gebäude. • Der Zugriff auf gegebenenfalls vorhandene Dienste bzw. Ressourcen kann man nicht auf Netzwerkebene regulieren.

Topologische Ansatz der Segmentierung

Segmentierung nach Etage/Gebäudetrakt oder pro Unterrichtsraum

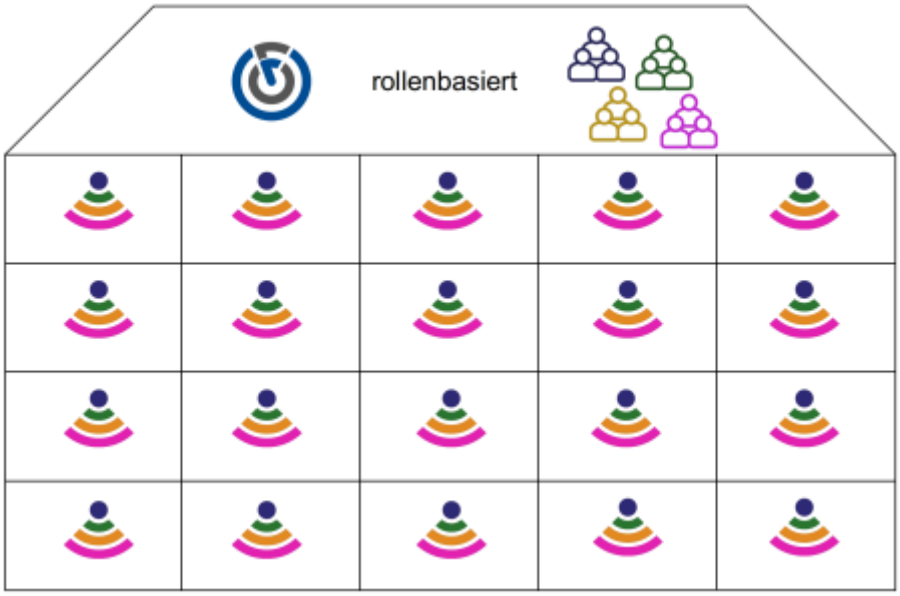


Beide von Ihnen beschriebenen Segmentierungskonzepte für Schulnetzwerke haben ihre eigenen Vorzüge und Herausforderungen und können je nach den spezifischen Bedürfnissen und Ressourcen der Schule sinnvoll sein. Lassen Sie uns beide Ansätze genauer betrachten:

Vorteile	Nachteile
• Klare physische Abgrenzung: Die Segmentierung entspricht den physischen/baulichen Abgrenzungen der Schule, was die Verwaltung und das Verständnis des Netzwerks vereinfachen. • Begrenzte Broadcast-Domänen: Dies reduziert den Netzwerkverkehr und verbessert die Leistung, da Broadcasts auf den relevanten Bereich beschränkt bleiben. • Erhöhte Sicherheit und Kontrolle: Jedes Segment kann individuell kontrolliert und gesichert werden, was die Risiken von Netzwerkstörungen und Sicherheitsverletzungen reduziert. • Bessere Roaming-Kontrolle: Nutzer haben eine klar definierte und konsistente Netzwerkverbindung in jedem Raum.	• Höhere Komplexität bei der Einrichtung: Jedes Segment erfordert individuelle Konfiguration und Wartung. • Potenzielle Verbindungsprobleme für Benutzer: Nutzer müssen sich beim Wechsel von Räumen oder Bereichen möglicherweise neu verbinden, was zu Unterbrechungen führen kann. • Erhöhte Anzahl von SSIDs: Kann für Nutzer verwirrend sein und die Verwaltung erschweren. • Höhere Anforderungen an Roaming.

Rollenbasierter Ansatz

dynamische VLAN-Zuweisung über Radiusserver



Vorteile	Nachteile
• Flexibilität und Benutzerfreundlichkeit: Nutzer können sich mit denselben Anmeldeinformationen überall im Gebäude verbinden. • Anpassungsfähigkeit: Das Netzwerk passt sich dynamisch den Bedürfnissen und Rollen der Benutzer an. • Erweiterte Sicherheitsfunktionen: Möglichkeit zur Implementierung von LAN-Port-Security und anderen fortgeschrittenen Sicherheitsmaßnahmen.	• Komplexität in der Einrichtung und Wartung: Erfordert einen Radiusserver und eine fortgeschrittene Netzwerkkonfiguration. • Potenzielle Störanfälligkeit: Zusätzliche Dienste können das System anfälliger für Störungen machen. • Höherer Verwaltungsaufwand: Die Pflege von Benutzerdaten und Zugriffsrechten kann aufwendig sein.

dynamische VLAN-Zuweisung über ‚private Preshared Keys'

Im Gegensatz zum Betrieb eines Radius-Servers lassen sich mit ‚privaten Preshared Keys' die gleichen Vorteile, wie bei der Verwendung eines Radius-Servers erzielen, der administrative Aufwand fällt jedoch deutlich geringer aus. Es werden pro Netzwerk unterschiedliche Preshared Keys erstellt. Bei der Anmeldung sind diese entscheiden, zu welchem Netzwerk Zugriff gewährt wird.

Fazit

In der Praxis könnte eine Kombination beider Ansätze sinnvoll sein, um die Vorteile beider Systeme zu nutzen und deren Nachteile zu minimieren. Beispielsweise könnte das Netzwerk in großen Gebäudetrakten topologisch segmentiert sein, während in häufig genutzten Bereichen wie der Bibliothek oder dem Lehrerzimmer ein rollenbasierter Ansatz verwendet wird. Letztendlich hängt die Wahl des geeigneten Segmentierungskonzepts von den spezifischen Anforderungen der Schule, dem vorhandenen Budget, den technischen Fähigkeiten des IT-Personals und den pädagogischen Zielen ab. Wird ein Schulnetzwerk noch von pädagogischen Systembetreuungen verantwortet, so lässt sich mit Reduzierung des Gesamtaufwandes ggf. ein geringerer Sicherheitsstandard rechtfertigen – vor allem wenn es sich um schlankes Netzwerk handelt, in dem so gut wie keine lokalen Ressourcen vorhanden sind, weil bereits in professionelle

Clouds ausgelagert.