

Muster-Leistungsbeschreibung

Aktive Netzwerkkomponenten

Zweck

Aktive Netzwerkkomponenten spielen eine tragende Rolle in der Netzwerkinfrastruktur der Schulen und erfüllen verschiedene Zwecke, um den reibungslosen Betrieb und die effiziente Kommunikation innerhalb des Netzwerks sicherzustellen. Das vorliegende Muster enthält Leistungsbeschreibungen zentraler aktiver Komponenten für pädagogisch genutzte schulische Netzwerke, inklusive eines Servers. Diese und weitere Muster-Leistungsbeschreibungen in diesem Modul verstehen sich als Ergänzung und Vertiefung gegenüber den Empfehlungen des Bitkom in der Handreichung Hardware produktneutral ausschreiben für den Schulbereich – Leitfaden für den öffentlichen IT-Einkauf¹ (Stand: Juli 2023).

Anwendungsempfehlung

Die in dieser Muster-Leistungsbeschreibung aufgeführten Anforderungen müssen in der Vorbereitungsphase zur Beschaffung mit dem Zielbild des Schulträgers für die konkreten Leistungsanforderungen an die pädagogisch genutzten Netzwerke der betreuten Schulen angepasst werden. Zur Unterstützung und Orientierung für die Arbeit mit den Muster-Leistungsbeschreibungen empfehlen wir zudem die Anleitung zur Nutzung der Muster-Leistungsbeschreibungen².

Die vorliegende Muster-Leistungsbeschreibung stellt ein beispielhaftes Musterdokument dar. Die darin enthaltenen Inhalte und Empfehlungen müssen stets vor einer Ausschreibung für den konkreten Anwendungsfall der betreffenden Organisation geprüft und angepasst werden. Die PD übernimmt keine Gewähr für die Richtigkeit der Angaben.

¹ Bitkom e.V. (2023): Hardware produktneutral ausschreiben für den Schulbereich. Leitfaden für den öffentlichen IT-Einkauf.
URL: <https://www.bitkom.org/sites/main/files/2023-09/ITK-Beschaffung-Leitfaden-Hardware-produktneutral-ausschreiben-fuer-Schulbereich-2023.pdf>

² Schul-IT-Navigator (Website): „Anleitung zum Umgang mit den Muster-Leistungsbeschreibungen“ (Modul „IT-Service-Management“)



Schon gewusst?

Mehr Fachwissen zum Thema Schul-IT finden Sie auf unserer Webseite:

 www.schul-it-navigator.de

Haben Sie Feedback zu den Umsetzungshilfen für uns? Fehlt Ihnen noch etwas?

Ihre Rückmeldungen sind für uns wichtig, da die Umsetzungshilfen kontinuierlich überarbeitet werden. Wir freuen uns auf Ihre Rückmeldung.

 feedback@schul-it-navigator.de

Inhaltsverzeichnis

Zweck	1
Anwendungsempfehlung	1
Beschreibung Beschaffungsgegenstände	3
Router	5
Switch	7
Access Point (AP)	9
WLAN-Controller (Gateway)	11
Glossar	13
Abbildungsverzeichnis	14
Autorinnen und Autoren	14

Beschreibung Beschaffungsgegenstände

Es gibt eine Vielzahl von aktiven Komponenten, die in Netzwerkinfrastrukturen eingesetzt werden. In diesem Dokument werden die folgenden, zentralen Netzwerkkomponenten fokussiert:

- 1. Router:** Ein Router ist ein Gerät, das den Datenverkehr zwischen verschiedenen Netzwerken steuert. Er leitet Datenpakete basierend auf IP-Adressen weiter und ermöglicht die Kommunikation zwischen Netzwerken.
- 2. Switch:** Ein Switch ist ein Gerät, das den Datenverkehr innerhalb eines Netzwerks steuert. Er verbindet verschiedene Netzwerkgeräte miteinander und leitet Datenpakete basierend auf MAC-Adressen weiter. Der Managed Switch ist eine leistungsstarke und vielseitige Netzwerkkomponente, die eine effiziente Verwaltung und Steuerung des Netzwerkverkehrs ermöglicht. Mit fortschrittlichen Funktionen und umfangreichen Verwaltungsoptionen bietet der Managed Switch eine optimale Leistung und Skalierbarkeit für Schulnetzwerke.
- 3. Access Point (AP):** Ein Access Point ermöglicht die drahtlose Verbindung von Geräten mit einem Netzwerk. Er stellt eine kabellose Schnittstelle bereit, über die Geräte wie Laptops, Smartphones oder Tablets auf das Netzwerk zugreifen können. Es werden ggf. zusätzliche Hardwarekomponenten benötigt, die aktiv das Netzwerk (LAN, WLAN, Internet) überwachen und Probleme an das zentrale Monitoring weitergeben (z. B. über LTE).
- 4. WLAN-Controller:** Ein WLAN-Controller ist eine Netzwerkkomponente, die für die zentrale Verwaltung und Steuerung von drahtlosen Netzwerken verantwortlich ist. Er wird häufig in Unternehmen, Bildungseinrichtungen und anderen Umgebungen eingesetzt, in denen eine große Anzahl von drahtlosen Zugriffspunkten (Access Points) verwaltet werden muss. Der WLAN-Controller bietet eine zentrale Schnittstelle zur Konfiguration, Überwachung und Fehlerbehebung des drahtlosen Netzwerks.

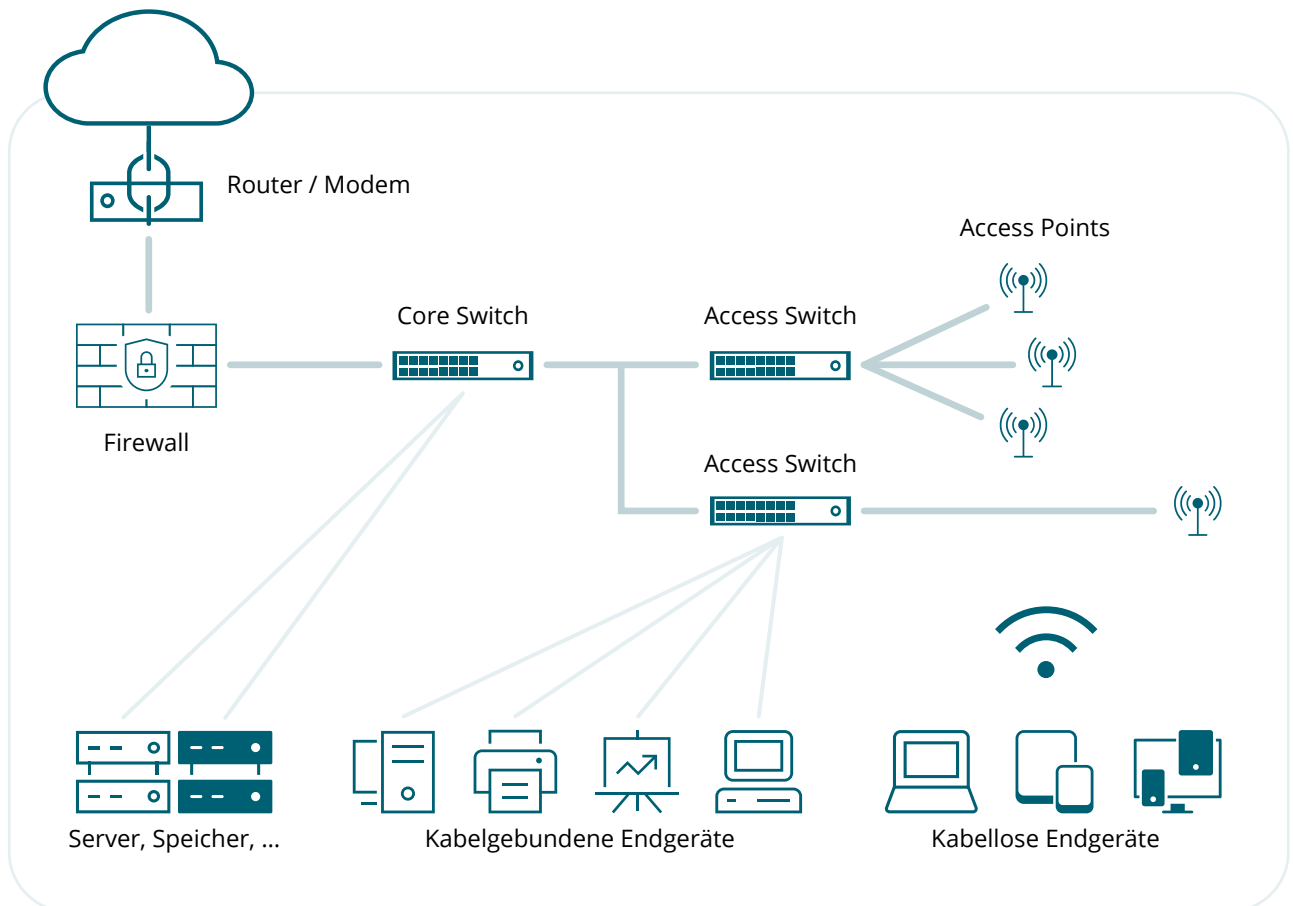


Abbildung 1: Beispiel für Server in schulischem Netzwerk



Hinweis

Bei der Beschaffung von Netzwerkkomponenten sollten immer sogenannte „Enterprise-Produkte“ eingekauft werden, um Leistungsfähigkeit, Ausfallsicherheit und Wartbarkeit auf höchstmöglichem Niveau zu ermöglichen. Von Geräten aus dem Home-Bereich sollte aus diesem Grund sowie im Sinne der Informationssicherheit abgesehen werden. Alle Netzwerkkomponenten müssen zentral überwacht und gemanaged werden können.

Für weitergehende Informationen zu technischen Anforderungen an aktive Netzwerkkomponenten für schulische IT-Netzwerke siehe den Leitfaden des Bitkom: Hardware produktneutral ausschreiben für den Schulbereich. Leitfaden für den öffentlichen IT-Einkauf, abrufbar unter: <https://www.bitkom.org/sites/main/files/2023-09/ITK-Beschaffung-Leitfaden-Hardware-produktneutral-ausschreiben-fuer-Schulbereich-2023.pdf>

Router

Ein Router ist ein wesentliches Gerät in einem Computernetzwerk, das dazu dient, den Datenverkehr zwischen verschiedenen Netzwerken zu steuern und zu lenken. Er ermöglicht die Kommunikation zwischen Geräten in einem lokalen Netzwerk (LAN) und anderen Netzwerken, wie dem Internet oder anderen LANs. Korrekt konfiguriert bietet der Router eine umfassende Sicherheit für Ihr Netzwerk³. Eine WLAN-Funktion wird in der Regel nicht benötigt, da das WLAN über einen WLAN-Controller separat realisiert werden sollte.

Grundlagen

Mindestanforderungen

Übertragungsgeschwindigkeit & Anschlüsse

- Der Router bietet mindestens die Übertragungsgeschwindigkeit, die auch der verfügbare Internetanschluss bietet.
- Unterstützung Glasfaseranschluss *oder* Unterstützung DSL-Anschluss (Kupferleitungen)
- Der Router unterstützt eine Übertragungsgeschwindigkeit von mind. 1 Gbit/s (Gigabit pro Sekunde).

Auswahlkriterien

Einfache Einrichtung und Verwaltung

- Mit der benutzerfreundlichen webbasierten Benutzeroberfläche können Sie den Router schnell einrichten und konfigurieren. Sie haben die Möglichkeit, das Netzwerk zu überwachen, Einstellungen anzupassen und Firmware-Updates durchzuführen.
- Die WAN-Anbindung sollte 10 Gbit unterstützen
- Der Router unterstützt Load-Balancing
- Der Router unterstützt Mobilfunk-Fallback

Schnittstellen

Mindestanforderungen

LAN-Schnittstellen

- Mind. 1x Gbit Ethernet Ports, die eine schnelle kabelgebundene Verbindung zu weiteren Netzwerkkomponenten ermöglichen

Auswahlkriterien

- Serviceschnittstellen zum lokalen Zugriff auf den Router
- API-Schnittstellen für herstellerunabhängige Administration

Sicherheit

Mindestanforderungen

- Er unterstützt den Einsatz von mehreren VPNs (Virtual Private Networks) für eine sichere Verbindung zu entfernten Netzwerken.
- Regelmäßige Software-Updates müssen während des Lebenszyklus des Routers verfügbar sein, um Sicherheit gewährleisten zu können.

Auswahlkriterien

- Er verfügt über eine integrierte Firewall, um unerwünschten Datenverkehr zu blockieren

³ Siehe hierzu vertiefend die Handreichung „Einführung in die Informationssicherheit für Schulen“ im Modul „IT-Steuerung und Kooperation“ des Schul-IT-Navigators.



Hinweis

Sofern der Router keine Firewall-Funktionalität bietet, muss diese über ein anderes System bereitgestellt werden.

Quality of Service & Support

Mindestanforderungen

- Gewährleistung mind. 60 Monate
- Gerät muss für die Dauer der Nutzung/Abschreibung Herstellersupport (Softwarepflege) erhalten
- Hersteller verfügt über deutschsprachigen Service

Auswahlkriterien

- Der Router bietet QoS-Funktionen, mit denen Sie den Netzwerkverkehr priorisieren können. Sie können bestimmte Anwendungen oder Geräte priorisieren, um eine optimale Leistung für zeitkritische Anwendungen wie Videostreaming oder Online-Gaming zu gewährleisten.
- Garantie über den gesamten Lebenszyklus (Lifetime Warranty)

Switch

Der (Managed) Switch ist ein wesentliches Element in modernen Computernetzwerken, da er die Netzwerkleistung verbessert, die Effizienz steigert und die Übertragung von Datenpaketen zwischen den Geräten erleichtert. Der Core Switch ist der zentrale Schalter in einem Netzwerk und bildet das Rückgrat der gesamten Netzwerktopologie. Er ist normalerweise hochleistungsfähig und mit hoher Kapazität ausgestattet, um den Datenverkehr von mehreren Access Switches zu verarbeiten.

Die Hauptaufgabe des Core Switches besteht darin, den Datenverkehr zwischen den verschiedenen Access Switches weiterzuleiten und eine schnelle Kommunikation zwischen den verschiedenen Teilen des Netzwerks zu ermöglichen. Der Access Switch ist ein Schalter, der Endgeräte wie Computer, Telefone, Drucker und andere Netzwerkgeräte direkt verbindet. Er bildet die Schnittstelle zwischen den Endgeräten und dem Kern des Netzwerks. Der Access Switch ist oft an mehreren Ports mit verschiedenen Geschwindigkeiten ausgestattet, um eine Vielzahl von Geräten mit dem Netzwerk zu verbinden.

Grundlagen

Mindestanforderungen

VLAN-Unterstützung

- Der Switch ermöglicht die Einrichtung und Verwaltung von Virtual Local Area Networks (VLANs). VLANs bieten die Möglichkeit, das Netzwerk in virtuelle Segmente aufzuteilen, um den Datenverkehr zu isolieren, Sicherheit zu verbessern und die Netzwerkleistung zu optimieren.

Management Optionen

- Der Managed Switch bietet verschiedene Management Optionen. Dazu gehören eine webbasierte Benutzeroberfläche, die eine intuitive Konfiguration und Überwachung ermöglicht, sowie die Unterstützung für SNMP (Simple Network Management Protocol), CLI (Command Line Interface) und Remote Management über Netzwerkmanagement-Software.
- Der Switch unterstützt SSH und Telnet ist deaktivierbar.

Auswahlkriterien

Stacking-Funktion

- Bei einigen Modellen des Managed Switch besteht die Möglichkeit des Stacking, d. h. mehrere Switches können zu einer logischen Einheit zusammengeschlossen werden. Dadurch wird die Skalierbarkeit erhöht, die Verwaltung vereinfacht und eine hohe Verfügbarkeit gewährleistet.

Redundanz und Ausfallsicherheit

- Der Managed Switch unterstützt verschiedene Mechanismen zur Verbesserung der Netzwerkverfügbarkeit, darunter Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP) und Link Aggregation (EtherChannel).

Schnittstellen

Mindestanforderungen

Port-Kapazität

- Der Managed Switch ist nach aktuellem Stand der Technik mit mindestens Gigabitfähigen Ports ausgestattet.
- Der Switch bietet ausreichend Ports.

PoE-Unterstützung

- Der Switch verfügt über Power over Ethernet (PoE) gem. IEE 802.3at.

Auswahlkriterien

- 10-Gigabit Ethernet Ports / MultiGB-Ports
- API-Schnittstellen bieten die Möglichkeit durch flexibles Management auch auf Geräte anderer Hersteller zuzugreifen um diese zu konfigurieren.

Sicherheit

Mindestanforderungen

- Der Switch bietet fortschrittliche Sicherheitsfunktionen wie Zugriffskontrolllisten (ACLs), MAC-Authentifizierung, Port-Sicherheit und 802.1X-Authentifizierung.
- Der Switch unterstützt EAP, PEAP, EAP-TLS, EAP-TTLS, EAP-TEAP.

Auswahlkriterien

- Zusätzliche Authentifizierungsmethoden wie das Einbinden von Zertifikaten oder MAC-Filterung sollte unterstützt werden.



Hinweis

Das Netzwerkmanagement an einer Schule bildet eine funktionale Einheit. Es ist daher ratsam, Herstellerabhängigkeiten zu reduzieren. Schnittstellen (z. B. API-Schnittstellen), die die Kommunikation zwischen Geräten unterschiedlicher Hersteller ermöglichen, können die Abhängigkeit von einem Hersteller verringern.

Quality of Service & Support

Mindestanforderungen

- Der Managed Switch bietet fortschrittliche QoS-Funktionen, mit denen der Netzwerkverkehr priorisiert und verwaltet werden kann.
- Der Switch ermöglicht die Zuweisung von Bandbreitenprioritäten für bestimmte Anwendungen oder Dienste, um eine optimale Leistung zu gewährleisten.
- Gewährleistung mind. 60 Monate
- Gerät muss für die Dauer der Nutzung Herstellersupport (Softwarepflege) erhalten
- Hersteller verfügt über deutschsprachigen Service

Access Point (AP)

Ein Access Point (AP) ist ein Gerät in einem Netzwerk, das als zentrale Schnittstelle dient, um drahtlose Geräte wie Computer, Smartphones, Tablets oder andere Endgeräte mit dem Netzwerk zu verbinden. Der Access Point fungiert als Drahtloszugriffspunkt und ermöglicht es diesen Geräten, Daten über WiFi (drahtloses Netzwerk) mit dem verdrahteten Netzwerk, normalerweise über ein Gateway (Router, Switch oder WLAN-Controller), zu kommunizieren. Access Points werden oft in Umgebungen eingesetzt, in denen drahtlose Konnektivität benötigt wird, wie Büros, Schulen, Hotels, Flughäfen und öffentliche Plätze. Sie erweitern das verdrahtete Netzwerk, indem sie drahtlose Abdeckung bieten und ermöglichen es Nutzenden, ihre Geräte ohne physische Kabel mit dem Internet und anderen Netzwerkressourcen zu verbinden.

Die Access Points einiger Hersteller sind inzwischen so konstruiert, dass sie ohne einen separaten WLAN-Controller konfiguriert und administriert werden können. Hier gilt es für die jeweilige Situation an der Schule eine zugeschnittene individuelle Lösung zu finden, die in das Ausstattungskonzept der Schule passt.

Grundlagen

Mindestanforderungen

WLAN-Standard

- Der Access Point unterstützt den neuesten WLAN-Standard 802.11ac (Wi-Fi 5) oder 802.11ax (Wi-Fi 6).

Dual-Band-Unterstützung

- Der Access Point arbeitet mit Dual-Band-Technologie und unterstützt sowohl das 2,4-GHz- als auch das 5-GHz-Frequenzband, ggf. auch das 6 GHz-Band.

Übertragungsgeschwindigkeit

- Der Access Point bietet mind. eine Übertragungsgeschwindigkeit von 1 Gbit/s.

Multiple SSIDs

- Der Access Point ist Multi-SSID-fähig.

Zentrales Management

- Der Access Point kann in ein zentrales Verwaltungssystem integriert werden, um eine einfache und effiziente Konfiguration, Überwachung und Verwaltung zu gewährleisten.

Auswahlkriterien

- Einige Hersteller bieten Lösungen zum Einrichten eines WLAN mit nur einer SSID. Anhand der Authentifizierung werden dem Gerät dann die entsprechenden Rechte zugewiesen.

Schnittstellen

Mindestanforderungen

LAN mit Power over Ethernet (PoE)

- Die Access Points unterstützen Power over Ethernet (PoE) nach IEE 802.3af, IEE 802.3at.

Auswahlkriterien

LAN-Schnittstelle

- Sie bietet die Möglichkeit, ein weiteres Netzwerkfähiges Gerät mit einzubinden, ohne eine weitere physische Netzwerkdose installieren zu müssen. Das LAN-Signal wird im AP „durchgeschleift“.

**Hinweis**

Sofern der Access Point (AP) kein PoE unterstützt, muss jeder Access Point am Installationsort mit Strom versorgt werden. Sofern der Switch oder WLAN-Controller, an dem die APs angeschlossen sind, kein oder unzureichend PoE liefert, können die APs mit sogenannten PoE-Injektoren mit Strom über die LAN-Anbindung versorgt werden.

Hierbei ist es ratsam, darauf zu achten, dass die Access Points auch bei Ausfall des Controllers ihren Betrieb fortführen können.

Sicherheit**Mindestanforderungen**

- Der Access Point bietet umfassende Sicherheitsfunktionen, um Ihr drahtloses Netzwerk zu schützen. Dies umfasst die Unterstützung von Verschlüsselungsprotokollen wie WPA2 oder WPA3, MAC-Adressfilterung, Zugriffskontrolllisten (ACLs) und Intrusion Detection/Prevention Systeme (IDS/IPS).

Quality of Service & Support**Mindestanforderungen**

- Gewährleistung mind. 60 Monate
- Gerät muss für die Dauer der Nutzung Herstellersupport (Softwarepflege) erhalten
- Hersteller verfügt über deutschsprachigen Service

WLAN-Controller (Gateway)

Ein WLAN-Controller, auch bekannt als Wireless LAN Controller oder WLC, ist ein zentrales Netzwerkgerät, das entwickelt wurde, um die Verwaltung und Steuerung von drahtlosen Netzwerken zu erleichtern. Er spielt eine wichtige Rolle bei der Bereitstellung, Überwachung und Optimierung von drahtlosen Kommunikationsinfrastrukturen, insbesondere in größeren Unternehmensumgebungen. Es ist wichtig anzumerken, dass WLAN-Controller nicht in jedem Netzwerk erforderlich sind. In kleineren Umgebungen können Access Points unabhängig voneinander verwaltet werden.

WLAN-Controller sind jedoch besonders nützlich in größeren Netzwerken, in denen eine zentrale Verwaltung, Überwachung und Optimierung der drahtlosen Kommunikation notwendig ist. Inzwischen bieten einige Hersteller intelligente Access Points an, die über eine integrierte Logik verfügen und nicht über einen separaten WLAN-Controller administriert werden müssen. Dennoch können diese intelligenten APs über eine entsprechende Software zentral administriert und überwacht werden.

Grundlagen

Mindestanforderungen

Konfiguration und Bereitstellung

- Der WLAN-Controller ermöglicht die zentrale Konfiguration und Bereitstellung von drahtlosen Netzwerkeinstellungen. Dies umfasst die Festlegung von mehreren SSIDs (Service Set Identifiers), Sicherheitsrichtlinien, Zugriffskontrollen und anderen drahtlosen Netzwerkparametern.
- Controller muss managebar sein und muss mit anderen Controllern kommunizieren können (zentrales Management).

Roaming-Optimierung

- Der WLAN-Controller ermöglicht das nahtlose Roaming von drahtlosen Geräten innerhalb des Netzwerks. Er überwacht die Signalstärke und andere Faktoren und steuert den Übergang eines Geräts von einem Access Point zum anderen, um eine stabile Verbindung aufrechtzuerhalten.

Leistungsüberwachung und Fehlerbehebung

- Der WLAN-Controller bietet umfangreiche Überwachungs- und Fehlerbehebungsfunktionen für das drahtlose Netzwerk. Er kann die Leistung der Access Points überwachen, Signalstörungen erkennen, Verbindungsprobleme diagnostizieren und Alarime bei Netzwerkstörungen oder Sicherheitsvorfällen generieren.

Skalierbarkeit und Flexibilität

- Durch die zentrale Verwaltung ermöglicht der WLAN-Controller eine einfache Skalierung des drahtlosen Netzwerks. Neue Access Points können leicht hinzugefügt werden, ohne dass eine separate Konfiguration erforderlich ist. Der Controller bietet auch Flexibilität bei der Umsetzung verschiedener drahtloser Netzwerktopologien, wie z. B. Unified oder Distributed WLAN-Architekturen.

Multi-SSID

- Der Controller ist in der Lage, mehrere SSID zu verwalten, um eine (mindestens) logische Trennung von Netzwerken in der Schule (Verwaltung, pädagogisches Netzwerk, BYOD ...) zu ermöglichen.

Auswahlkriterien

- Nutzbar für Standortvernetzung (Gateway) mit Schulen oder RZ
- Lokal-Breakout zur Nutzung einer direkten Internetanbindung,
- Traffic-Erkennung und -Priorisierung zur effizienten Auslastung des Netzwerks
- Alternativ zu einem physischen Gerät als WLAN-Controller kann oft auch ein virtueller Controller als SaaS genutzt werden.
- Bei Ausfall des Controllers sollte auf ein redundantes System zugegriffen werden können.

**Hinweis**

Mit Hilfe des WLAN-Controllers kann das WLAN zentral eingerichtet und überwacht werden. Um die Abhängigkeit von einem Hersteller zu verringern, kann die Anschaffung von intelligenten Access Points in Betracht gezogen werden. Diese verfügen über eine Schnittstelle, mit deren Hilfe die APs über eine separate Software gemanaged werden können.

Weiterhin ist es ratsam, dass die Access Points auch bei Ausfall des Controllers ihren Betrieb fortführen können.

Schnittstellen**Mindestanforderungen**

- Physische Konfigurationsschnittstelle
- Netzwerkschnittstelle mit mind. 1 Gbit

Sicherheit**Mindestanforderungen**

- Automatische Optimierung (ARM: Adaptive Radio Management)

Quality of Service & Support**Mindestanforderungen**

- Gewährleistung mind. 60 Monate
- Gerät muss für die Dauer der Nutzung Herstellersupport (Softwarepflege) erhalten
- Hersteller verfügt über deutschsprachigen Service

Glossar

ACL	ACL steht für "Access Control List" (Zugriffskontrollliste) und ist eine Sicherheitsmaßnahme in Computernetzwerken. Sie ermöglicht die Definition von Regeln, die bestimmen, welche Nutzende oder Gruppen von Nutzenden auf welche Ressourcen (Dateien, Ordner, Netzwerkressourcen) zugreifen dürfen. ACLs dienen dazu, die Zugriffsrechte zu verwalten und unautorisierte Zugriffe zu verhindern.
ARM	Adaptive Radio Management trägt dazu bei, die drahtlose Netzwerkleistung in sich ändernden Umgebungen zu optimieren und die Benutzererfahrung zu verbessern, indem es auf Echtzeitinformationen reagiert und automatisch Anpassungen vornimmt, um die bestmögliche Kommunikationsqualität zu gewährleisten.
CLI	CLI steht für "Command Line Interface" und ist eine textbasierte Schnittstelle, die es Nutzenden ermöglicht, Befehle direkt in einem Terminal oder einer Eingabeaufforderung auszuführen, um mit einem Computer oder einem Betriebssystem zu interagieren. Statt einer grafischen Benutzeroberfläche verwenden Benutzer Befehle und Optionen, um Aufgaben wie Dateiverwaltung, Softwareinstallation und Systemkonfiguration auszuführen. CLI bietet oft eine schnellere und effizientere Möglichkeit zur Steuerung von Computern, insbesondere für erfahrene Benutzer oder Automatisierungszwecke.
Enterprise-Produkte	Enterprise-Produkte sind spezialisierte Lösungen, die auf die Anforderungen großer Organisationen zugeschnitten sind. Sie bieten leistungsstarke Funktionen und Skalierbarkeit, um komplexe Geschäftsprozesse zu unterstützen. Diese Produkte sind i.d.R. hochgradig anpassbar und bieten Integrationen mit anderen Unternehmenssystemen. Sie konzentrieren sich oft auf Datensicherheit, Compliance und umfassenden Support, um den anspruchsvollen Anforderungen von Unternehmen gerecht zu werden.
IDS	IDS steht für Intrusion Detection System, ein Sicherheitsmechanismus in Computersystemen und Netzwerken, der ungewöhnliche oder verdächtige Aktivitäten überwacht, erkennt und darauf reagiert. Es analysiert den Datenverkehr oder Systemzustand, um potenzielle Eindringversuche, Angriffe oder bösartige Aktivitäten zu identifizieren und Nutzende oder Administratoren zu benachrichtigen. IDS trägt dazu bei, die Sicherheit von IT-Infrastrukturen zu erhöhen, indem es frühzeitig auf potenzielle Bedrohungen hinweist.
IPS	IPS steht für Intrusion Prevention System und ist eine Sicherheitstechnologie, die Netzwerke überwacht, um verdächtigen Datenverkehr zu erkennen und zu blockieren, bevor er Schaden anrichten kann. Es identifiziert potenzielle Angriffe, wie z. B. Malware oder Eindringlingsversuche, durch Analyse von Datenpaketen und Verhaltensmustern, und ergreift automatisch Maßnahmen zum Schutz des Netzwerks. IPS trägt dazu bei, die IT-Infrastruktur vor Bedrohungen zu schützen und Sicherheitsvorfälle frühzeitig zu verhindern.
Link	Aggregation Link Aggregation ist eine Technik in Netzwerken, bei der mehrere physische Netzwerkverbindungen zwischen Geräten gebündelt werden, um die Bandbreite zu erhöhen und die Ausfallsicherheit zu verbessern. Dies geschieht durch die Verwendung eines Aggregationsprotokolls wie LACP (Link Aggregation Control Protocol), das die Verbindungen zu einem logischen Hochgeschwindigkeitslink zusammenfasst. Diese Methode ermöglicht eine effizientere Nutzung der verfügbaren Netzwerkressourcen und eine erhöhte Zuverlässigkeit durch Redundanz.
Managed Switch	Ein Managed Switch ist ein Netzwerkgerät, das erweiterte Funktionen zur Konfiguration und Überwachung von Netzwerkverkehr bietet. Es ermöglicht die Steuerung von Datenfluss, VLAN-Konfiguration und Sicherheitseinstellungen. Ein "Core" bezieht sich auf das zentrale Element in einem Netzwerk, das den Hauptverkehr zwischen verschiedenen Segmenten verarbeitet. Es ist leistungsstark und darauf ausgelegt, hohe Datenmengen schnell und effizient zu übertragen. "Access" bezieht sich auf Netzwerksegmente oder Ports, die normalerweise Endgeräten wie Computern oder Druckern zugewiesen werden. Diese Zugangsebene ermöglicht die Verbindung von Endgeräten zum Netzwerk, wobei der Managed Switch die Kontrolle über den Datenfluss behält.
QoS	Quality of Service bezieht sich auf die Fähigkeit eines Netzwerks, bestimmten Datenverkehr Prioritäten zuzuweisen und sicherzustellen, dass bestimmte Dienste oder Anwendungen eine zuverlässige Leistung und minimale Verzögerungen erhalten, um eine konsistente Nutzererfahrung zu gewährleisten. Dies wird oft durch die Kontrolle von Bandbreite, Latenz und Paketverlust erreicht.
PoE	Power over Ethernet ist eine Technologie, die es ermöglicht, sowohl Daten als auch Strom über ein einziges Ethernet-Kabel zu übertragen. Dadurch entfällt die Notwendigkeit für separate Stromkabel und Steckdosen, was die Installation und den Betrieb von Geräten wie IP-Kameras, VoIP-Telefonen und WLAN-Access-Points vereinfacht.
(R)STP	Rapid Spanning Tree Protocol ist ein Netzwerkprotokoll, das in Ethernet-Netzwerken verwendet wird, um Schleifen zu vermeiden und die Konvergenzzeit bei Ausfällen zu verkürzen. Es identifiziert schnell den besten Pfad für den Datenverkehr und passt sich dynamisch an Veränderungen in der Netzwerktopologie an.

Abbildungsverzeichnis

Abbildung 1: Beispiel für Server in schulischem Netzwerk 4

Autorinnen und Autoren

Mathias Ragnow (PD – Berater der öffentlichen Hand GmbH)

Dr. Michael Krause (PD – Berater der öffentlichen Hand GmbH)

PD – Berater der öffentlichen Hand GmbH Friedrichstr. 149, 10117 Berlin | www.pd-g.de | schuedigital@pd-g.de



Schon gewusst?

Mehr Fachwissen zum Thema Schul-IT
finden Sie auf unserer Webseite:

 www.schul-it-navigator.de

Haben Sie Feedback zu den Umsetzungshilfen für uns? Fehlt Ihnen noch etwas?

Ihre Rückmeldungen sind für uns wichtig, da die Umsetzungshilfen kontinuierlich überarbeitet werden. Wir freuen uns auf Ihre Rückmeldung.

 feedback@schul-it-navigator.de