



**Medienberatung
NRW**

WLAN AN SCHULEN

Eine Orientierungshilfe
für Schulträger, Schulleitungen und
Entscheidungsgremien



HERAUSGEBER

Medienberatung NRW
 Bertha-von-Suttner-Platz 1
 D-40227 Düsseldorf
 www.medienberatung.nrw.de

AUTOREN

Achim Harhoff, Philip Rehorst

BERATUNG

krzn | **regio it** | Geschäftsstellen Gigabit.NRW

REDAKTION

Birgit Giering

VERANTWORTLICH

Stefan Drewes, Markus Köster

GESTALTUNG

Bosbach Kommunikation & Design GmbH, Köln

DRUCK

msh marketingservice köln GmbH

1. Auflage 2020



Dieses Dokument steht unter CC BY ND 4.0 Lizenz.

BILDNACHWEISE

Titelbild: Alexander Supertramp/shutterstock.com,
 S. 8, 14, 15, 16, 18, 20, 21 Medienberatung NRW, S.9 Nico-
 ElNino/shutterstock.com, S. 10 Farknot Architect/shutter-
 stock.com, S. 13 Matej Kastelic/shutterstock.com, Rawpi-
 xel.com/shutterstock.com, S. 19 Natali_Mis/shutterstock.
 com, S. 22 TierneyMJ/shutterstock.com, S. 27 alice-photo/
 shutterstock.com

INHALT

Einleitung	4
Teil 1: Planungsaspekte	5
1.1 Prozessdauer	5
1.2 Förderprogramme	5
1.3 Wichtige Dinge vorab	6
1.4 Vorbereitungen zu Prozessbeginn	6
1.5 Empfehlungen zur Prozessgestaltung	9
Teil 2: Technische Aspekte	10
2.1 Die professionelle Ausleuchtung	10
2.2 Das 2,4-GHz-Frequenzband im Vergleich zum 5-GHz-Frequenzband	11
2.3 Stromversorgung der Accesspoints	12
2.4 Netzwerkadministration Teil 1: WLAN-Controlling	13
2.5 Netzwerkadministration Teil 2: Device-Management und Benutzerverwaltung	16
2.6 Lösungen für besondere bauliche Anforderungen	20
Glossar	23
Weitere Publikationen	26

EINLEITUNG

Diese Publikation richtet sich an Schulträger des Landes NRW in der Anfangsphase der kommunalen Medienentwicklungsplanung sowie an die beteiligten Schulleitungen und Entscheidungsgremien. Vorausgesetzt wird, dass die Schulen bereits über einen Breitbandanschluss verfügen oder eine Breitbandanbindung auf den Weg gebracht ist.

Ziel der schulischen IT-Infrastruktur ist der gesicherte und performante Zugang zum schulischen Netzwerk und Internet für jede Schülerin und jeden Schüler an jedem schulischen Lern- und Unterrichtsort. Diese Aufgabe umfasst nicht nur die Verkabelung, die Verteilungshardware wie Switches und die Accesspoints, sondern auch die Administration aller im Netz verbundenen Geräte sowie die Administration der Benutzerrechte. Bei aller Komplexität der Netzwerkkonfiguration muss das System störungsfrei, reibungslos und entsprechend den aktuellen Anforderungen an die Geschwindigkeit und Sicherheit funktionieren. Umsetzungsempfehlungen für den Aufbau von sicheren Netzen und deren Erweiterung um ein WLAN gibt das Bundesamt für Sicherheit in der Informationstechnik (BSI) durch den IT-Grundschutz.

Der erste Teil dieser Publikation formuliert Orientierungshilfen für die Prozessgestaltung des Projektes WLAN an Schulen. Im zweiten Teil werden Orientierungshilfen in Bezug auf die hard- und softwaretechnischen Aspekte aufgezeigt, um den Vertreterinnen und Vertretern von Schulen und Schulträgern einen Überblick sowie ein systemisches Verständnis aktueller Netzwerktechnik zu bieten.

Bei der Verarbeitung personenbezogener Daten, die mit der Nutzung der bereitgestellten Komponenten einhergeht, spielen auch datenschutzrechtliche Aspekte eine Rolle. Diese werden hier aber nicht vertiefend dargestellt. Die behördlichen Datenschutzbeauftragten für die Schulen stehen bei datenschutzrechtlichen Fragen beratend zur Seite. Orientierungshilfen und Unterstützung bietet zudem die Medienberatung NRW.

Weiterführende Informationen

Weiterführende Informationen und Unterstützungsangebote zu den Themen IT-Sicherheit und Datenschutz bieten die folgenden Quellen:



BSI: IT-Grundschutz



Schulministerium NRW:
Datenschutz im Schulbereich



Medienberatung NRW:
Datenschutz und Datensicherheit



TEIL 1: PLANUNGSASPEKTE

1.1 PROZESSDAUER

Die Planung und Umsetzung einer schulischen IT-Grundstruktur bis hin zum Aufbau und zur Inbetriebnahme zentraler IT- und Netzwerkdienste ist ein Prozess, der sich über einen längeren Zeitraum erstreckt. So veranschlagen Experten für die Umsetzung einer **Campus-Lösung** für alle Schulen eines Schulträgers circa ein Jahr, wobei die Zeit für Ausschreibungen nicht mit eingerechnet ist.

Pilotprojekte, bei denen einzelne Gebäude oder Gebäudeteile im Voraus ausgestattet werden, können zwar in kürzerer Zeit realisiert werden, sollten aber in ein Gesamtsystem der schulischen IT-Administration integrierbar sein.

Falls Sie als Schulträger den Anschluss an bestehende Strukturen (z.B. kommunale Rechenzentren; *siehe www.kdn.de/mitglieder*) anstreben, wird die Anpassung der Administrationsstrukturen an die medienkonzeptionelle Ausrichtung der Schulen ebenfalls eine gewisse Zeit in Anspruch nehmen.

Aufgrund der Komplexität eines Projektes »Schulnetz und Administration« sollten Planung und Realisation in die Hände eines professionellen IT-Dienstleisters gelegt werden.

1.2 Förderprogramme

Für die digitale Ausstattung der Schulen mit IT-Infrastruktur stellen Bund und Land vielfältige Förderprogramme zur Verfügung.

Mit dem DigitalPakt Schule haben der Bund und die Länder einen großen Schritt in die Richtung der flächendeckenden Digitalisierung der Schulen in Nordrhein-Westfalen gemacht. Mit dem DigitalPakt wird der Ausbau der IT-Infrastruktur an Schulen gefördert. Förderbar sind daher die Bereiche IT-Grundstruktur, digitale Arbeitsgeräte, schulgebundene mobile Endgeräte sowie regionale Maßnahmen, soweit diese von den Schulen unmittelbar genutzt werden können.

Darüber hinaus stehen den Schulträgern weitere Mittel aus den Förderprogrammen Gute Schule 2020 sowie dem Kommunalinvestitionsförderungsgesetz für die Errichtung von IT-Infrastruktur an Schulen zur Verfügung.

Die Förderung von professioneller IT-Administration für Schulen im Rahmen einer Zusatzvereinbarung zum DigitalPakt Schule ist derzeit zwischen Bund und Ländern in Planung und wird in Kürze zur Verfügung stehen.

1.3 WICHTIGE DINGE VORAB

- Sämtliche Hardwarekomponenten sollten Business-Komponenten sein. Maßstab für den Grad der Professionalität des Systems Schul-IT ist nicht das häusliche WLAN, sondern die Konfiguration eines größeren mittelständischen Betriebes. Fachleute empfehlen, alle Hardwarekomponenten von einem Hersteller zu beziehen, um eine reibungslose Kommunikation der Komponenten untereinander zu gewährleisten. Zudem muss sichergestellt sein, dass der Hersteller für die eingesetzten Netzwerkkomponenten eine langfristige Versorgung mit Firmware- und Sicherheitsupdates garantiert.
- Eine strukturierte Gebäudeverkabelung hat immer Vorrang gegenüber drahtlosen Überbrückungshilfen (z.B. **WLAN-Bridges**, **WLAN-Meshes**). Sofern sie noch nicht vorhanden ist, sollte sie den modernen Datenraten entsprechend (gigabitfähig) realisiert werden. Bereits vorhandene Gebäudeverkabelungen sollten modernisiert werden, wenn sie den Ansprüchen an aktuell übliche Datenübertragungsraten nicht genügen. Alle Kosten für Neueinrichtung, Ausbau oder Modernisierung einer strukturierten Gebäudeverkabelung sind förderfähig.
- Bei der Planung und Umsetzung der **Backbone-Verkabelung** sollte direkt auch die Platzierung von Accesspoints durch professionelle Ausleuchtung festgelegt werden. Zudem müssen zwingend Brandschutzvorschriften und gegebenenfalls auch Denkmalschutzaufgaben berücksichtigt werden. Die entsprechenden Fachabteilungen müssen in den Prozess eingebunden werden. Technische Lösungen für den Fall, dass Gebäudeteilbereiche aus oben genannten Gründen nicht verkabelt werden können, werden im zweiten Teil dieser Publikation vorgestellt (siehe S. 20).
- Jeder Unterrichtsraum sollte mindestens vier LAN-Zugänge für pädagogische Zwecke (Präsentationssysteme, Standgeräte wie PC, o.Ä.) erhalten. Für eine Direktversorgung der Unterrichtsräume mit eigenem Accesspoint ist eine weitere Zuleitung notwendig. Auch Leitungen für smarte Gebäudesteuerung (Heizung, Rollos o. Ä.) oder Telefone müssen gesondert berücksichtigt werden.
- Die Leistungsfähigkeit des IT-Systems sollte für die maximale Menge der zu versorgenden Endgeräte je Schule ausreichend veranschlagt sein.
- Für professionelle Netzwerke, insbesondere WLANs mit einer Vielzahl von zusätzlichen Endgeräten, ist es dringend zu empfehlen, ein **IP Address Management (IPAM)** zu nutzen.

1.4 VORBEREITUNGEN ZU PROZESSBEGINN

Bevor IT-Unternehmen mit der Planung und Einrichtung des LAN/WLAN beauftragt werden, sollten seitens der Schulen und des Schulträgers wichtige vorbereitende Schritte zur Planung erfolgen.

AUFGABEN DER SCHULEN

Falls Schulträger für notwendige Investitionen Fördermittel aus dem DigitalPakt Schule beantragen wollen, muss den Anträgen ein technisch-pädagogisches Einsatzkonzept der Schulen mit Berücksichtigung medienpädagogischer, didaktischer und technischer Aspekte beiliegen.

Für eine sinnvolle und schulgerechte Strukturplanung können folgende Fragen hilfreich sein:

- Welche Vorstellungen oder Zielperspektiven hat die Schule bezüglich der digital gestützten Unterrichts- und Schulentwicklung?

- Wo und zu welchem Zweck soll das WLAN über die Lern- und Unterrichtsräume hinausgehend verfügbar sein (Verwaltung, Lehrerzimmer, Aula, Turnhalle, Außenbereiche usw.)?
- Welche **Netzsegmente** (logisch getrennte Netzwerke) sind erforderlich (Schülernetz, Lehrernetz, Verwaltungsnetz, Gastnetz usw.)?
- Für welche Netzwerke sollen drahtlose Zugangsmöglichkeiten eingerichtet werden?
- Welche Nutzungs- und Zugangsrechte für geplante Netzwerke sollen vergeben werden? Also kurz: Wer darf was in welchem Netzwerk?
- Welche Nutzungsregeln für digitale Endgeräte, schulisch gemanagt oder rein private, sollen gelten? Wie wird beispielsweise sichergestellt, dass keine Endgeräte ohne aktuelle Systemupdates das Netzwerk gefährden? Wie sieht gegebenenfalls das schulische BYOD-Konzept aus?
- Welche Qualifizierungsbedarfe bestehen im Kollegium und von wem können diese gedeckt werden?
- Wie können schulische Mitwirkungsgruppen eingebunden werden?

ERSTE PLANUNGSSCHRITTE DES SCHULTRÄGERS

Parallel zu den vorbereitenden Maßnahmen der Schulen kann der Schulträger bereits folgende Schritte einleiten:

- Ermittlung des Ist-Zustands der Netzwerke und des gesamten IT-Inventars der zu versorgenden Schulen. Dieser Service kann auch von einem IT-Dienstleister erbracht werden, falls eine aktuelle Inventarisierung oder auch das Fachpersonal zur Erhebung einer solchen fehlt.
- Bei der Planung der Netze sollten die Empfehlungen des **BSI-IT-Grundschutzes** berücksichtigt werden, um Vertraulichkeit, Integrität und Verfügbarkeit der Netze zu gewährleisten.
- Sofern die Unterstützung eines professionellen IT-Dienstleisters in Anspruch genommen wird, sollte dieser Erfahrung mit der Einrichtung vergleichbarer Systeme haben.
- Klärung, inwieweit aufgrund des Projektumfangs Ausschreibungsverfahren durchzuführen sind und es bestehende offene Rahmenverträge bzw. Einkaufsgemeinschaften gibt. Im Beschaffungsverfahren sollten auch datenschutzrechtliche Aspekte wie z.B. Auftragsdatenverarbeitung sowie gegebenenfalls Aspekte der Informationssicherheit berücksichtigt sein.
- Klärung der Möglichkeit, sich mit anderen Schulträgern zu vernetzen oder sich einem kommunalen Rechenzentrum anzuschließen. Eine Übersicht über bereits bestehende Zweckverbände finden Sie auf der Webseite des Dachverbandes kommunaler IT-Dienstleister KDN – www.kdn.de.
- Unabhängig von der Performanz der vorhandenen Internetanbindung sollte die IT-Grundstruktur allen denkbaren zukünftigen Anforderungen gewachsen sein. Auch Anwendungen im Intranet setzen ein performantes Netzwerk innerhalb der Schule voraus.
- In modernen Netzwerk- und Administrationsszenarien sind Schulen und Unternehmen nicht mehr auf räumliche Nähe zu einem Dienstleister angewiesen.

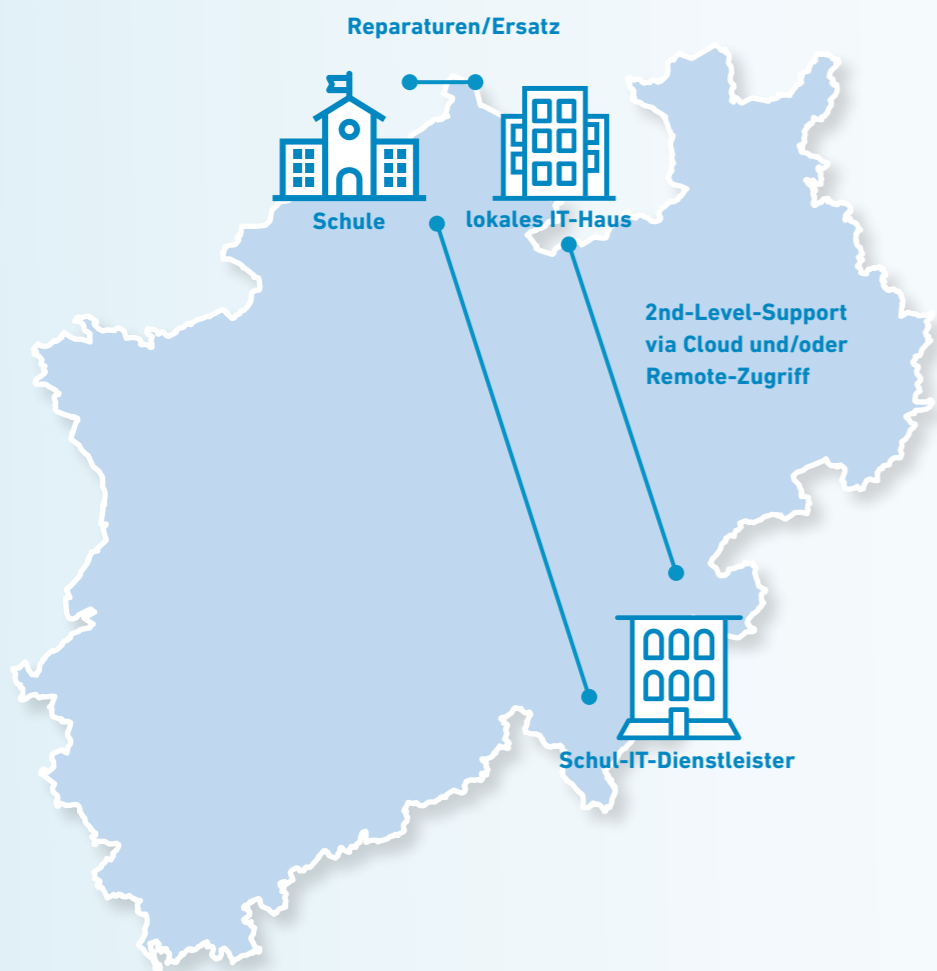


Abb. 1: Dezentrale Administration via Cloud

1.5 EMPFEHLUNGEN ZUR PROZESSGESTALTUNG

Mit den vorbereitenden Maßnahmen hat das Projekt die entscheidenden Impulse erhalten. Sukzessiv können nun die Ausstattungswünsche und die Systemkonfiguration nach den Vorstellungen und den konkretisierten Bedürfnissen der Schulen ihren Feinschliff erhalten. Folgende Aspekte können helfen, das Projekt erfolgreich durchzuführen:

- Vertreterinnen und Vertreter der Lehrerkollegien und des Schulträgers sollten zusammen eine Fachgruppe bilden, die im Dialog und Austausch mit Vertreterinnen und Vertretern des IT-Dienstleisters die schulischen Anforderungen an die Netzwerkstruktur konkretisiert (vgl. auch Medienberatung NRW (2019). Medienentwicklungsplanung in NRW, S. 12 ff.). Die Vertreterinnen und Vertreter der Schulen und des Schulträgers sollten fachlich und thematisch so weit vorbereitet sein, dass sie den Vorschlägen eines IT-Dienstleisters folgen bzw. diesem ihre Bedürfnisse konkretisiert und verständlich vermitteln können.
- Um teure **Rollbacks** zu vermeiden, sollten alle Entscheidungsschritte den späteren Nutzerinnen und Nutzern zeitnah vermittelt werden, sodass auch deren Einwände und Verbesserungsvorschläge berücksichtigt werden können. Allerdings sollte im Vorfeld geklärt sein, dass die technische Expertise bei dem beauftragten IT-Dienstleister liegt.
- Schulen und Schulträger treffen Vereinbarungen hinsichtlich der Umsetzung des First- und Second-Level-Supports, um den reibungslosen Betrieb der IT-Infrastruktur sicherzustellen.



Medienentwicklung in NRW

Es bietet sich eine Orientierung an den Prozessschritten zur Medienentwicklungsplanung an (vgl. Medienberatung NRW, 2019. Medienentwicklungsplanung in NRW, S. 5).



TEIL 2: TECHNISCHE ASPEKTE

2.1 DIE PROFESSIONELLE AUSLEUCHTUNG

Nachdem die Strukturplanung abgenommen wurde, kann das WLAN eingerichtet werden. Mit der entsprechenden Simulationssoftware sollte zunächst eine virtuelle Ausleuchtung erfolgen. Zeit- und kostensparend ist dabei die Bereitstellung folgender Informationen:

- **Gebäudeplan mit Maßstab:** Ein »Scan« wird in die Software eingefügt und bildet die Basis für die virtuelle Ausleuchtung.
- **Baumaterial von Wänden, Türen etc.:** Je nach Material dämpfen diese die Funksignale unterschiedlich stark. Die Informationen werden in den Gebäudeplan der Simulationssoftware eingegeben. Entsprechende Dämpfungswerte sind hier bereits vorgegeben.
- **Besondere bauliche Aspekte** wie z.B. Aufzugschächte, Metallregale, Stahlträger: Auch diese können lokal Einfluss auf die Signalstärke ausüben.
- **Brandschutzbestimmungen:** Beispielsweise kann es problematisch sein, Accesspoints auf Fluren anzubringen, da hierfür häufig Brandschutzeinrichtungen durchbrochen werden müssten.

Auf der Basis aller oben genannten Informationen kann mithilfe der Software sehr genau simuliert werden, welche Standorte und welche Funkkanäle sich für die Accesspoints am besten für die gewünschte Flächendeckung eignen. Sind die Accesspoints der virtuellen Ausleuchtung folgend angebracht und eingerichtet worden, erfolgt eine reale Ausleuchtung, um die tatsächliche Signalqualität zu prüfen, und gegebenenfalls ein Feintuning. Dabei ist zu beachten, dass all diese Schritte im laufenden Schulbetrieb und nicht unter Laborbedingungen in den Ferien stattfinden.



Abb. 2: Beispielansicht einer (groben) Ausleuchtung, hier mit einer kostenlosen »Homeuser«-Software: je tiefer das Blau, desto stärker das Signal; je stärker das Rot, desto schwächer das Signal. Die Accesspoints in Reichweite werden mit Informationen zu Funkstandard, Sendekanal und maximaler Datenrate aufgelistet.

2.2 DAS 2,4-GHZ-FREQUENZBAND IM VERGLEICH ZUM 5-GHZ-FREQUENZBAND

Die Frage, ob das WLAN im 2,4-GHz- oder im 5-GHz-Frequenzband eingerichtet werden soll, ist sowohl für die Ausleuchtung als auch für die Wahl der Accesspoint-Modelle und die pädagogisch-technischen Aspekte relevant. Zunächst einmal ein kurzer Vergleich der Techniken:

2,4 GHz	5 GHz
Größere Signalreichweite bei gleicher Sendeleistung	Geringere Signalreichweite; sie kann durch Erhöhung der Sendeleistung zum Teil kompensiert werden.
Stärkere Durchdringung von Wänden	Stärkere Signaldämpfung durch Wände etc.; sie kann durch Erhöhung der Sendeleistung zum Teil kompensiert werden.
Nur drei überlappungsfreie Kanäle; es besteht ein höheres Risiko für Störeinstreuungen, zumal z. B. auch Bluetooth auf dieser Frequenz arbeitet.	Frequenzband mit bis zu 19 überlappungsfreien Kanälen; es ist deutlich weniger anfällig für Störeinstreuungen.
Viele ältere Endgeräte können nur auf dieser Frequenz senden.	Neue Endgeräte arbeiten sowohl mit 2,4 GHz als auch mit 5 GHz.

Viele Accesspoints können parallel in beiden Frequenzbereichen funken und Endgeräte bedienen. Für Außenbereiche bestehen jedoch Nutzungseinschränkungen im 5-GHz-Bereich, da auch Radarsysteme und Satellitensignale einige Kanäle dieses Frequenzbereiches nutzen. Daher müssen Outdoor-Accesspoints einen fremden Sender erkennen und gegebenenfalls den Kanal wechseln können. Dieses Ausstattungsmerkmal ist Pflicht für die Nutzung eines bestimmten Kanalbereiches im 5-GHz-Bereich.

Hier wird deutlich, wie sehr die Strukturplanung der Schulen die Komplexität des Ausstattungsprozesses beeinflusst. Die vorausgehenden Überlegungen können noch weiter gehen:

- Sollen beide Netzfrequenzen zur Verfügung stehen? Bei **Bring-Your-Own-Device**-Konzepten ist zu bedenken, dass kostengünstigere oder ältere Endgeräte zurzeit nur die 2,4-GHz-Technik unterstützen. Zusätzlich ist zu beachten, dass das Netzwerk die Datenübertragungsrate, also das Tempo, an das langsamste Endgerät anpasst. Oder kurz gesagt: Das langsamste Gerät im Netzwerk bestimmt das Tempo für alle! Daher ist es sinnvoll, dass neuere Geräte auf das 5-GHz-Frequenzband ausweichen können, um ihre schnellere Konnektivität auszuspielen zu können, während die ohnehin langsameren Altgeräte im 2,4-GHz-Bereich verbleiben. Die meisten Accesspoint-Modelle lassen sich wahlweise konfigurieren (nur 2,4 GHz, 2,4 GHz + 5 GHz, nur 5 GHz), sodass bei einer später zu erwartenden Gesamtausstattung mit 5-GHz-fähigen Geräten der 2,4-GHz-Modus deaktiviert werden kann.

- Will die Schule von vornherein nur ein leistungsstärkeres 5-GHz-Netz betreiben, muss über entsprechende Ausstattungskonzepte eine einheitliche Verfügbarkeit dieser Technologie auf allen eingesetzten Endgeräten gewährleistet sein. Das betrifft auch Peripheriegeräte, die unter Umständen ebenfalls über WLAN in das Netzwerk integriert werden sollen. Dies sollte jedoch nur in Ausnahmefällen geschehen, da die Ideallösung für stationäre Geräte die Einbindung mit LAN-Kabeln ist.

2.3 STROMVERSORGUNG DER ACCESSPOINTS

Mit der **PoE**-Technologie (**Power over Ethernet**) können Netzwerkkomponenten wie Switches, Accesspoints etc. über die Netzwerkverkabelung mit Strom versorgt werden. Es ist somit nicht notwendig, das Stromnetz entsprechend zu erweitern. Dennoch gibt es einige technische Aspekte, die bedacht werden sollten:

- Bei PoE transportieren die Ethernet-Kabel nicht nur Daten, sondern zusätzlich auch Strom. Durch den spezifischen Widerstand der Leitungen erhöht sich deshalb auch die Wärmeentwicklung der Kabel. Das wiederum wirkt dämpfend auf die Datenübertragungsraten, sodass durch den Betrieb der Netzwerkkomponenten die tatsächliche Rate von der zuvor aufgrund der Kabelspezifikationen veranschlagten Stärke stark abweichen kann. Hier kann die Wahl der Kabelqualität (bezüglich Durchmesser und Schirmung) entscheidend sein. Ein höherer Durchmesser bewirkt eine geringere Erwärmung, eine gute Schirmung erleichtert den Abfluss der im Kabel entstehenden Wärme nach außen und wirkt dadurch einem Wärmeanstieg entgegen.
- Die über PoE zu versorgenden Geräte müssen also genau auf ihre Leistungsaufnahme hin geprüft werden, damit die Gesamtlast der Kabelstrecken und deren Auswirkung auf Temperatur und Verlust der Datenrate kalkuliert und eventuell notwendige Korrekturen an der Backbone-Verkabelung vorgenommen werden können.
- Aufgrund der Wärmeentwicklung in den für PoE genutzten Kabeln müssen die Werte auf brandschutztechnische Relevanz geprüft werden. Eventuell sind Maßnahmen zur Verbesserung des Brandschutzes notwendig, etwa bei veralteter Verkabelung. Eine Neuverkabelung, die der zu erwartenden Last entspricht und brandschutztechnisch unbedenklich ist, sollte ressourcenintensiven Schritten zur nachträglichen Verbesserung des Brandschutzes vorgezogen werden. Zudem erhöht eine Modernisierung die Datengeschwindigkeit im Netzwerk.
- Zur Einspeisung von Strom in das Datennetz sind entsprechende stromversorgende Geräte nötig. So genannte **Power Switches** versorgen über die von ihnen abgehenden Leitungen die angeschlossenen Accesspoints mit Strom.

Anhand der Wechselwirkungen zwischen kabelgebundener und drahtloser Netzwerkinstallation wird erneut deutlich, wie wichtig eine Betreuung des Projektes durch einen professionellen Dienstleister ist. Zudem ist es aufgrund der Energielast des Systems sinnvoll, alle Komponenten genau auszubalancieren: hin zu maximalem Datenfluss bei minimalem Energieverbrauch.

2.4 NETZWERKADMINISTRATION TEIL 1: WLAN-CONTROLLING

HARDWARELÖSUNG VS. VIRTUELLE CLOUD-LÖSUNG

WLAN-Controller sind Hardwarekomponenten, die die zentrale Administration der angeschlossenen Accesspoints ermöglichen und für die Netzwerkverwaltung in der Regel folgende Funktionen bieten:

- Sie übertragen vorgefertigte Netzwerkkonfigurationen auf Accesspoints, sowohl bei der Ersteinrichtung als auch bei der Erweiterung oder dem Austausch defekter Komponenten.
- **Band Steering:** Sie ermitteln durch Abgleich das passende Frequenzband (2,4 GHz oder 5 GHz) für ein angemeldetes Endgerät und optimieren dadurch den Datenfluss.
- **Access Point Steering:** Ein mobiles Endgerät wird automatisch mit dem situativ besten Accesspoint verbunden. Dadurch wird abbruchfreies **Roaming** ermöglicht, sodass keine Signalunterbrechung im Übergangsbereich von einem Accesspoint zum nächsten auftritt.
- **Self-Healing Network:** Falls ein Accesspoint im Netzwerk ausfällt, wird automatisch die Leistung der umliegenden Accesspoints erhöht, um keine Deckungslücke aufkommen zu lassen.

Die geräteeigene Konfigurationssoftware kann von Administratorinnen und Administratoren über jeden Webbrowser aufgerufen werden. Dort können der Netzwerkstatus und eventuelle Störungen oder Ausfälle in einer Übersicht angezeigt werden, was die Störungssuche und -behebung erleichtert.

Darüber hinaus bieten **Enterprise-Modelle** oft die Möglichkeit, unterschiedliche Netzwerkprofile abzuspeichern und diese im Bedarfsfall aufzurufen, eventuell sogar via Timer-Funktion automatisch zu schalten. So könnte beispielsweise tagsüber bis 17:00 Uhr eine Schulnetzkonfiguration aktiv sein und in einem speziellen Gebäudebereich ab 18:30 Uhr eine Konfiguration für städtische Veranstaltungen.



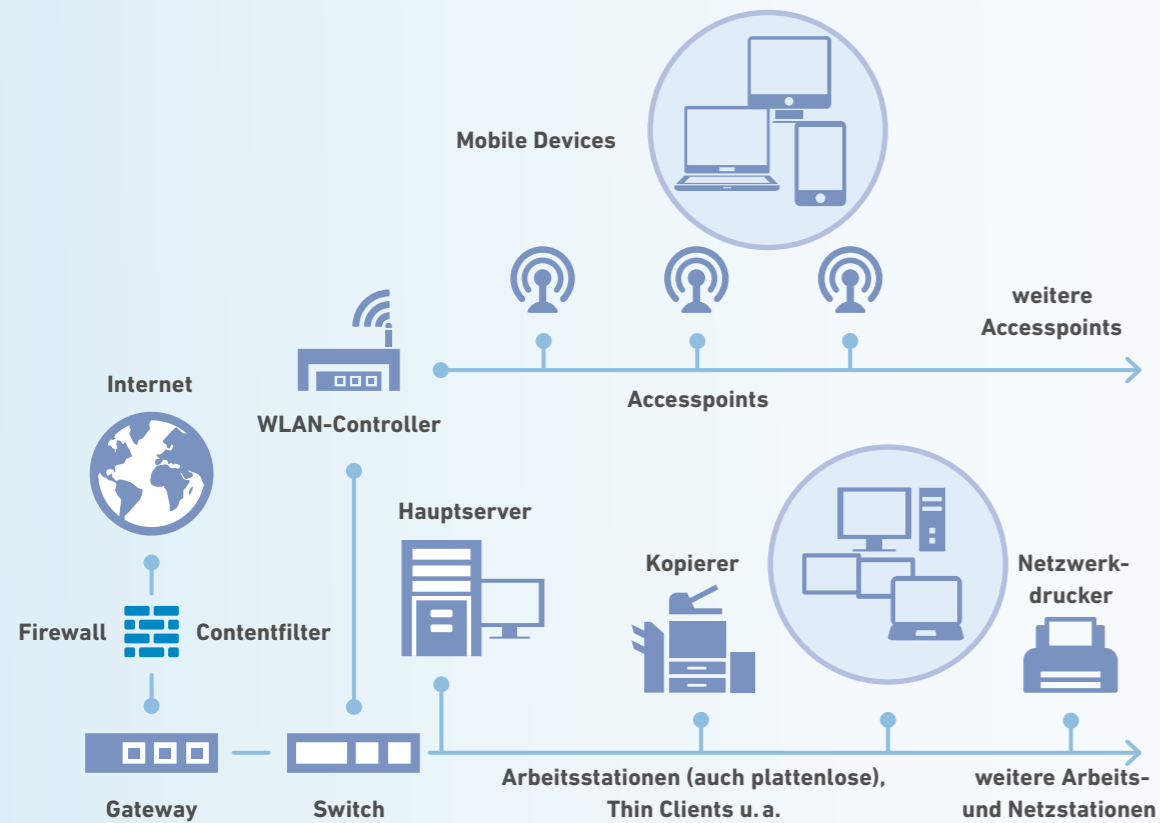


Abb. 3: Typisches Netzwerk (schematisch vereinfacht)

Eine noch junge Entwicklung in der Controlling-Technologie ist die **Virtualisierung** ehemals hardware-basierter Netzwerkkomponenten mithilfe von Cloud-Anwendungen: **Software-Defined WLAN (SD-WLAN)**, allgemeiner auch Software-Defined Networking (**SD-WLAN + LAN**). Die oben aufgeführten Funktionen eines Controllers werden – in Verbindung mit für ein solches System passenden Accesspoints – nicht von einem hardwaregestützten lokalen Controller bereitgestellt, sondern sind in einer Cloud-Anwendung virtualisiert. Von jedem Onlinezugang aus ist es möglich, über einen sicheren Log-in das gesamte Netzwerk zu administrieren.

Auf der einen Seite fallen Kosten für die Anschaffung von WLAN-Controllern an, auf der anderen Seite sind wiederkehrende Lizenzgebühren für die Nutzung einer SD-Lösung zu tragen.

Welche Lösung – SD-WLAN oder stationäre hardwarebasierte WLAN-Controller – für eine Schule besser geeignet ist, wird ein professioneller IT-Dienstleister mit Erfahrungen in beiden Ausstattungskonzepten darlegen können. Wichtig ist, dass ein über WLAN-Controlling administriertes System problemlos skalierbar ist und sukzessiv erweitert werden kann.

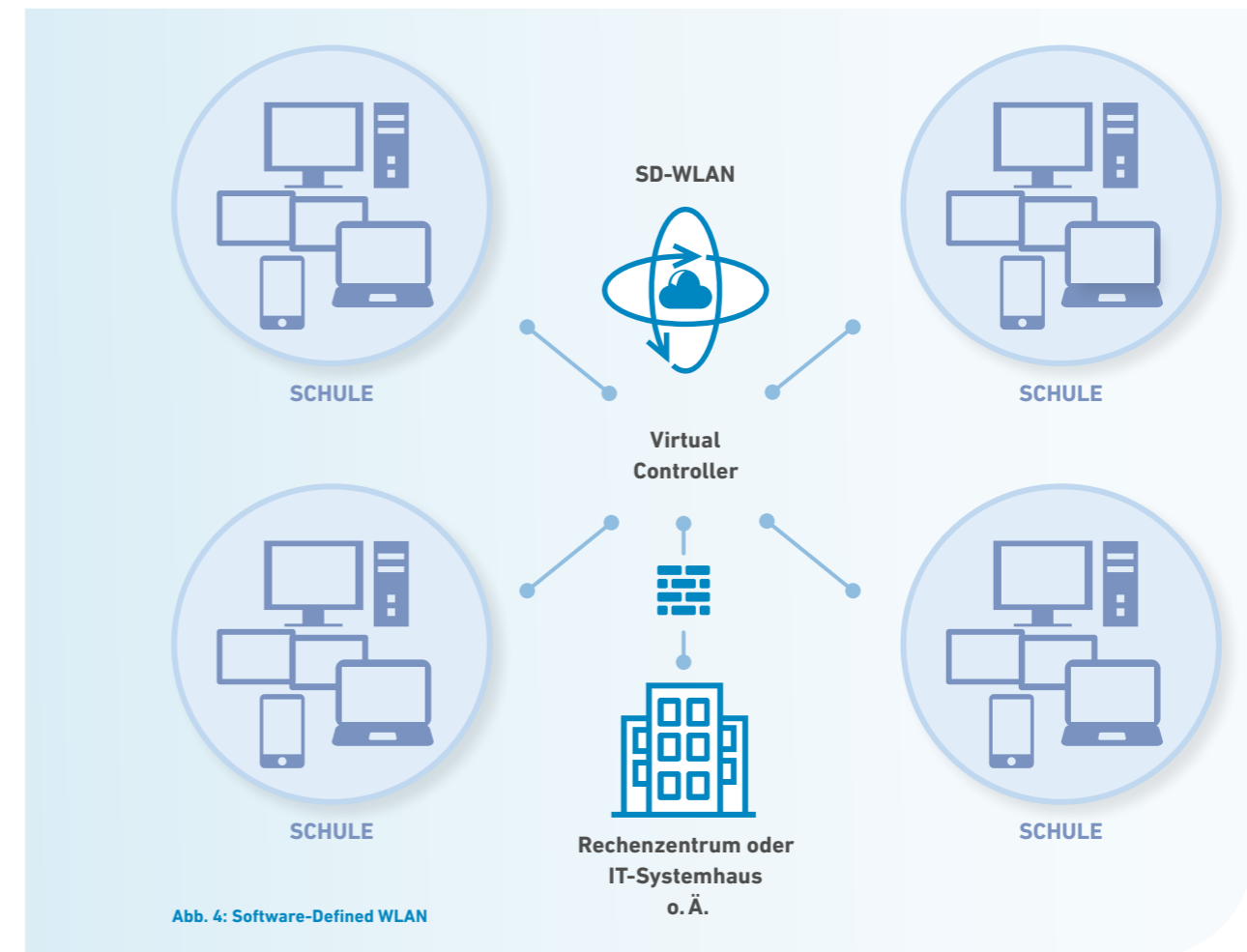


Abb. 4: Software-Defined WLAN

Datenschutz bei Cloud-Lösungen



Beim Einsatz von Cloud-Lösungen stellen sich unter Umständen besondere Anforderungen an den Datenschutz und die Datensicherheit, da dabei zumeist externe Dienstleister zum Einsatz kommen und Daten physisch die Schule verlassen. Der Schulträger, sofern er selbst die Datenverarbeitung für seine Schulen tätigt, aber auch externe Dienstleister haben die eingesetzte IT-Infrastruktur so zu betreiben, dass die Sicherheit der Datenverarbeitung in Verantwortung der Schulleiterin oder des Schulleiters gewährleistet ist. Der externe Dienstleister, zu denen bei Datenverarbeitungen auch der Schulträger zählen kann, muss dazu auf Basis einer schriftlichen Vereinbarung zur sogenannten Auftragsdatenverarbeitung, die er mit dem Verantwortlichen, also der Schulleiterin oder dem Schulleiter, abschließt, die ergriffenen technischen und organisatorischen Maßnahmen zur Datensicherheit benennen und deren Umsetzung und Einhaltung zusichern.

2.5 NETZWERKADMINISTRATION TEIL 2: DEVICE-MANAGEMENT UND BENUTZERVERWALTUNG

Mit der technisch reibungslosen Konfiguration aller Netzwerkkomponenten ist der administrative Aufgabenbereich noch nicht abgedeckt. Entscheidend für den reibungslosen, datenschutz- und gesetzeskonformen Betrieb des Systems sind das Gerätemanagement und die Benutzer-/Rechteverwaltung. Zu beachten sind insbesondere die Vorgaben zur Informationspflicht zum Zeitpunkt der Erhebung von personenbezogenen Daten gem. Art. 13, 14 DSGVO, zur Ausgestaltung wirksamer Einwilligungserklärungen sowie zur Löschung von Daten nach Wegfall der Verarbeitungsgrundlage.

DEVICE-MANAGEMENT

Mobile-Device-Management ist ein weitläufig bekannter Begriff, der jedoch die Anforderungen an die Geräteverwaltung in Schulen nur eingeschränkt widerspiegelt. Auch wenn eine Schule vorrangig mobile Endgeräte einsetzt, ist zu beachten, dass Peripheriegeräte wie z. B. Drucker oder LAN-fähige Präsentationssysteme ebenfalls administriert werden müssen. Zudem wird im Verwaltungsbereich weiterhin mit stationären Rechnern gearbeitet werden.

SOFTWAREVERTEILUNG UND -AKTUALISIERUNGEN

Ein weiterer Aspekt moderner IT-Administrationskonzepte (via lokalen Controller oder Cloud) ist das **Software Deployment** bzw. **App Deployment**. Es bietet die Möglichkeit, Software- bzw. App-Installationen und Software-/Firmware-/Treiberupdates zu gesetzten Zeitpunkten über das Netzwerk auf allen angeschlossenen Geräten durchzuführen. Ist ein Gerät zum festgesetzten Zeitpunkt offline, wird die entsprechende Routine nachgeholt, sobald sich das Gerät wieder im Netzwerk anmeldet.

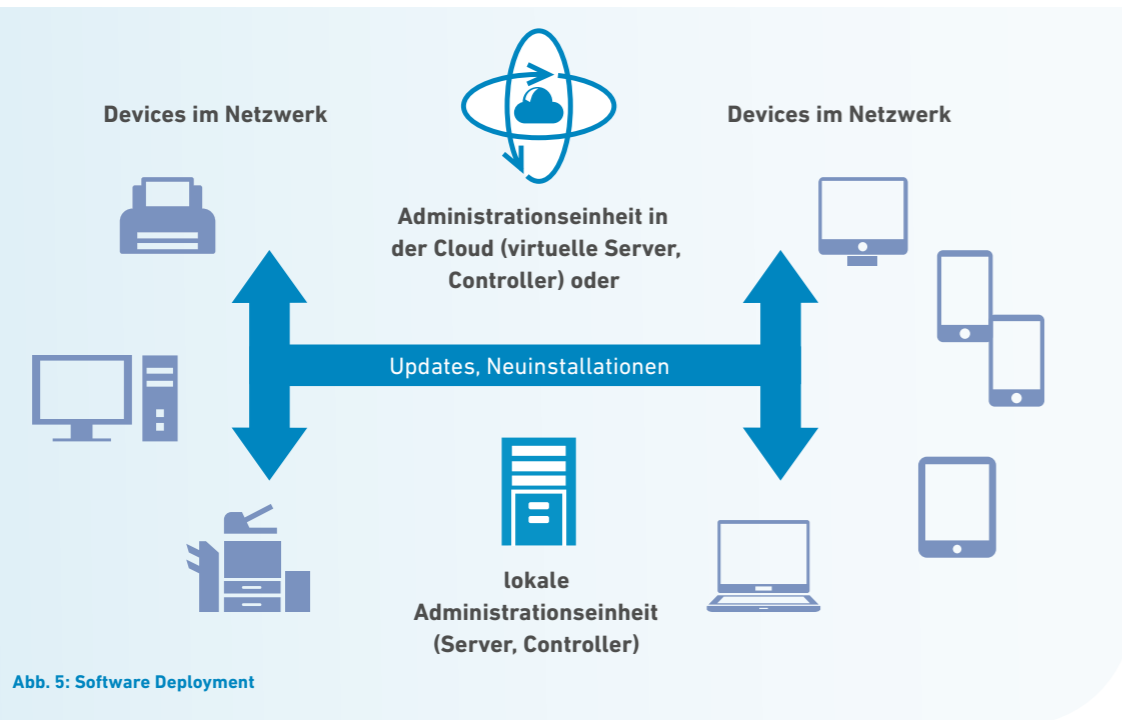


Abb. 5: Software Deployment

Bei der Entscheidung für ein Administrationskonzept ist zu beachten, dass die gewählte Lösung alle in der Schule eingesetzten Betriebssysteme bedienen kann.

Weiterhin ist darauf zu achten, dass das Management privater Endgeräte die Zustimmung der Besitzerinnen und Besitzer voraussetzt.

NETZWERKKONFIGURATIONEN UND BENUTZERVERWALTUNG

In der modernen Netzwerktechnik gibt es sicherheitszertifizierte Software, die die erforderliche logische Trennung der Netze in unterschiedliche Netzsegmente, sogenannte VLANs (virtuelle Netzwerke), innerhalb eines physikalischen Netzwerkes ermöglicht. Damit ist eine physikalische Trennung von Netzwerken nicht mehr notwendig. In Verbindung mit einem **RADIUS-Server** (Remote Authentication Dial-In User Service) bieten VLANs ein hohes Maß an Datensicherheit.

Darüber hinaus ermöglichen VLAN-fähige Accesspoints, zeitgleich Lehrkräfte mit einem Lehrernetzwerk und Schülerinnen und Schüler mit dem für sie freigeschalteten Netzwerk zu verbinden.

Ein einfacher Zutritt zu einem Schulnetzwerk über sogenannte **Pre-Shared Keys**, einem gemeinsamen Kennwort für alle Benutzer im WLAN, ist für Schulen nicht geeignet. Bei dieser Methode entfällt die Benutzerauthentifizierung, wodurch jeder im Netzwerk angemeldete User die selben Zugriffsrechte hat. Zudem könnte durch Weitergabe des Passwortes an Dritte ein unkontrollierter Zugriff durch Unbefugte auf das Netzwerk erfolgen.

Zu beachten ist, dass sich in **Netzsegmenten**, in denen pädagogische Verwaltungstätigkeiten ausgeführt werden, ein besonderes Schutzniveau ergeben kann. Diesem muss dann durch technisch-organisatorische Maßnahmen entsprochen werden.

Ein abgestimmtes Rollen-/Rechtemanagement ist von zentraler Bedeutung für die Datensicherheit im System, da es sicherstellt, dass nur berechtigte Benutzergruppen mit entsprechend autorisierten Endgeräten Zugriff auf für sie vorgesehene Daten haben. Schülerinnen und Schülern, die sich in dem Netzwerk mit Namen und Kennwort authentifizieren, ist nur der Zugriff auf die für ihre Benutzergruppe freigegebenen Daten möglich. Benötigen Benutzergruppen Zugriff auf mehr als ein Netzwerk, sollten aus Gründen der Benutzerfreundlichkeit unterschiedliche Log-ins vermieden werden.

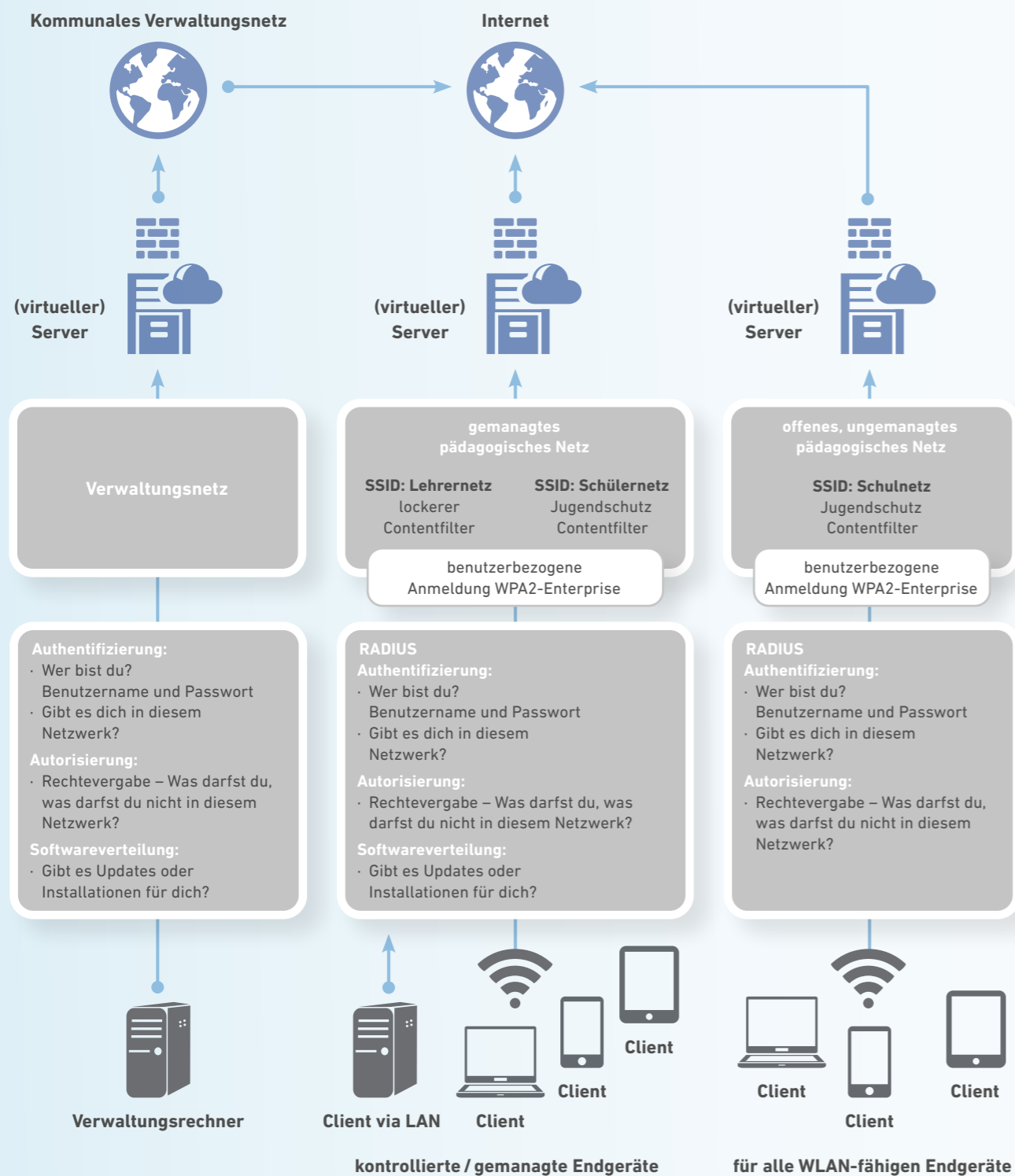


Abb. 6: Beispiel für eine Netzstruktur, bei der zwei Varianten von WLANs im pädagogischen Bereich vorhanden sind

Datenschutz – Verantwortlichkeiten



Bei den hier aufgezeigten Konfigurationsaspekten tritt die Datenschutzrelevanz besonders deutlich zutage. Auch wenn davon auszugehen ist, dass ein professioneller Dienstleister die Software-Infrastruktur eines Systems unter IT-Sicherheitsaspekten technisch konform einrichtet, können bestimmte Anwendungsfehler zu datenschutzkritischen Situationen führen. Da jede Datei physikalische Spuren in einem Speicher hinterlässt, dürfen beispielsweise keine besonders sensiblen Daten (z. B. Förderpläne oder Dokumente im Rahmen der Feststellung eines sonderpädagogischen Förderbedarfs) auf Endgeräten bearbeitet werden, auf die auch Schülerinnen und Schüler zugreifen können. Die Schulleitung ist für den Schutz der Daten und die Einhaltung der datenschutzrechtlichen Bestimmungen im Rahmen des Bildungsauftrags der Schule verantwortlich. Es müssen also nicht nur klare Nutzungsregeln für das Lehrerkollegium aufgestellt werden, sondern auch die unterschiedlichen Zuständigkeiten der Schulleitung (Schutz der schulbezogenen Daten) einerseits und der Schulträger (Ausstattung inklusive Datenspeicher) andererseits berücksichtigt werden.



2.6 LÖSUNGEN FÜR BESONDERE BAULICHE ANFORDERUNGEN

WENN GEBÄUDETEILE ODER -BEREICHE NICHT ÜBER KABEL IN DAS NETZWERK EINGEBUNDEN WERDEN KÖNNEN

Es kann vorkommen, dass Brandschutz- oder Denkmalschutzaufgaben bzw. andere bauliche Zwänge eine Anbindung bestimmter Gebäudeteile oder weiterer Schulgebäude an die strukturierte Verkabelung unmöglich machen. Für diese Fälle ist **Wireless Bridging** eine mögliche Lösung. Hier wird die Lücke im kabelgebundenen Datentransfer mithilfe zwei spezieller Accesspoints im schnellen 5-GHz-Modus überbrückt. Bei Inbetriebnahme richten sich die Bridging-Accesspoints so gezielt aufeinander aus, dass das Funksignal nicht, wie bei normalen bereichsdeckenden Accesspoints, radial, sondern linear gebündelt abgestrahlt wird. So kann das kurzweilige 5-GHz-Signal tatsächlich auch größere Entfernungen überbrücken, bei »Sichtkontakt« sogar mehrere Kilometer.

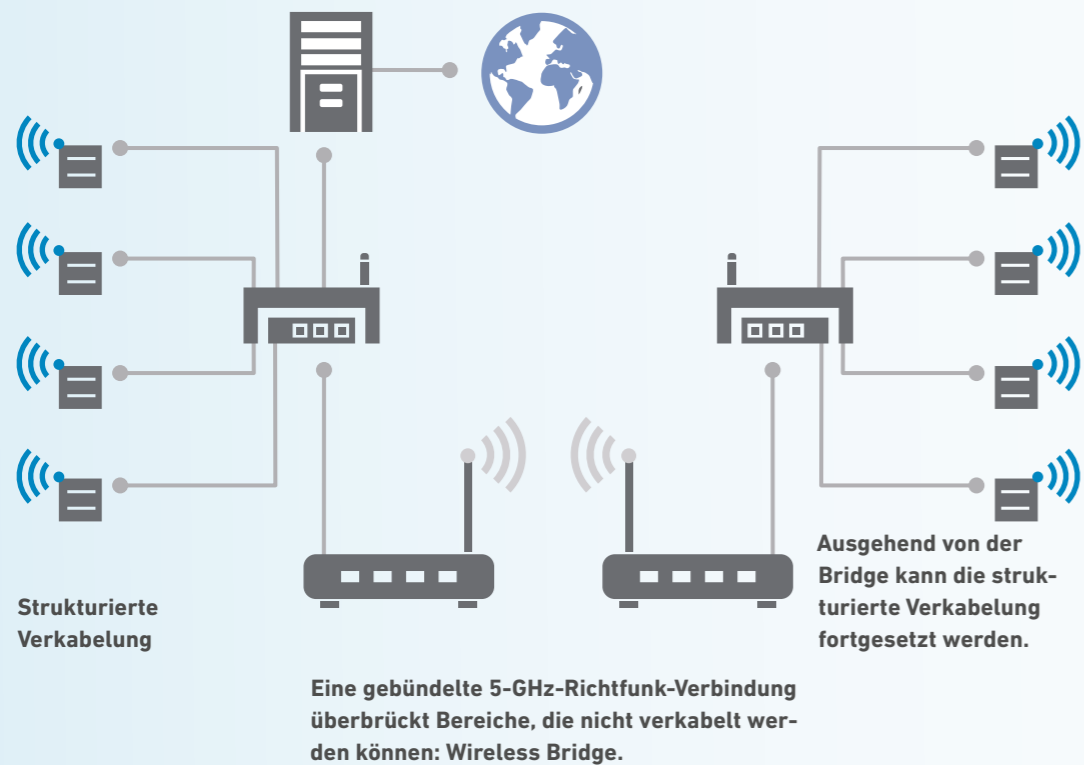


Abb. 7: Schematische Darstellung einer Wireless Bridge

WLAN-MESH ODER AUCH MESH-WLAN – WENN KEINE LAN-VERKABELUNG MÖGLICH IST

Mithilfe der **Mesh**-Technologie kann ein WLAN ohne strukturierte LAN-Verkabelung aufgezogen werden. Über die Funkkommunikation der Accesspoints konfiguriert sich das System quasi selbst:

- Alle Accesspoints senden dieselbe Netzwerkkennung (**SSID**) und erhalten dieselbe Netzwerkkonfiguration; diese ist von der Administratorin bzw. vom Administrator einmal für den Basis-Accesspoint eingestellt worden und wird beim Starten des Mesh automatisch auf alle anderen Accesspoints übertragen.
- Das Mesh agiert sozusagen »self-controlling«. Durch Funkaustausch ermöglicht es, wie auch die WLAN-Controller, **Band Steering**, **Access Point Steering** und **Self-Healing**.

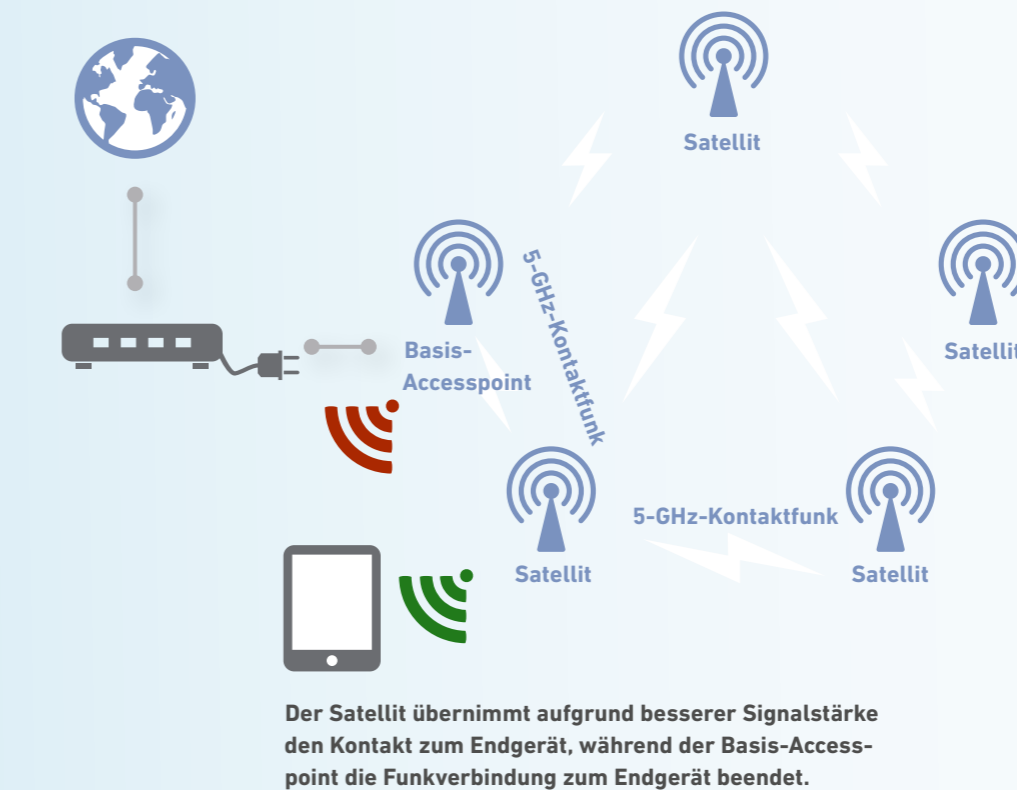


Abb. 8: Vereinfachtes Schaubild eines WLAN-Mesh

Dual-Band-Mesh-Lösungen senden auf 1x 2,4 GHz und 1x 5 GHz. Über das 5-GHz-Frequenzband läuft dann allerdings sowohl der Datenverkehr verbundener Endgeräte als auch die Kommunikation der Accesspoints untereinander, was zu Einschränkungen in der Bandbreite führt.

Die Tri-Band-Lösung sendet 1x 2,4 GHz und 2x 5 GHz, wobei ein 5-GHz-Band ausschließlich der Kommunikation der Systemkomponenten untereinander dient. Damit steht im zweiten 5-GHz-Band die volle Bandbreite für Endgeräte zur Verfügung.

Der Abstand der Accesspoints zueinander darf nicht zu hoch sein, da der 5-GHz-Kontaktfunk eine geringe Reichweite hat. Schon in den Grenzbereichen des Empfangs verringert sich die Bandbreite erheblich und bremst so das ganze System aus. Zudem ist die Anzahl der Accesspoints, die zu einem funktionstüchtigen Mesh zusammengeführt werden können, auf fünf bis sechs begrenzt. Somit scheidet diese Lösung für größere Schulflächen per se aus.

Die Accesspoints benötigen Stromanschlüsse. Um eine optimale Verteilung der Accesspoints und damit eine maximale Flächendeckung zu erreichen, müssen unter Umständen neue Stromanschlüsse eingerichtet werden. Beschränkt man sich auf gegebene Stromanschlüsse, kann die optimale Flächendeckung eventuell nicht erreicht werden.

Auf keinen Fall sollte man ein WLAN-Mesh in Betracht ziehen, um Investitionen in eine strukturierte Verkabelung zu umgehen, denn die stabilste Anbindung an ein elektronisches System liefert ein Kabel.



GLOSSAR

Abkürzung	Bedeutung
Access Point Steering	Ein mobiles Endgerät wird automatisch mit dem situativ besten Accesspoint verbunden. Dadurch soll abbruchfreies Roaming ermöglicht werden, was bedeutet, dass keine Signalunterbrechung im Übergangsbereich von einem Accesspoint zum nächsten auftritt.
App Deployment	siehe Software Deployment
Backbone-Verkabelung	engl. backbone = Rückgrat, Hauptstrang, Basisnetz bezeichnet den verbindenden Kernbereich eines Telekommunikationsnetzes mit sehr hohen Datenübertragungsraten, der meist aus einem Glasfasernetz sowie satellitengestützten Kommunikationselementen besteht
Band Steering	automatische Zuweisung des am Standort des Endgerätes leistungsfähigsten Frequenzbandes (2,4 GHz oder 5 GHz), wodurch der Datenfluss im System optimal ausgenutzt wird
Bring Your Own Device	Konzepte für die Ausstattung mit Endgeräten. In der ursprünglichen Form meint es den Einsatz von jeweils aktuell zur Verfügung stehenden schüler-eigenen Geräten (Smartphones, Laptops, Tablets).
BSI-IT-Grundschutz	eine vom Bundesamt für Sicherheit in der Informationstechnik (BSI) erstellte Sammlung von Empfehlungen zu Methoden, Prozessen und Verfahren sowie Vorgehensweisen und Maßnahmen zur Gewährleistung eines IT- Grundschutzes in Netzwerken
BYOD	siehe Bring Your Own Device
Campus-Lösung	umschreibt eine IT-Infrastruktur, in der alle Schulen eines Schulträgers bezüglich Softwarebereitstellung, Updates, Benutzer-/Rechteverwaltung usw. von einer zentralen IT gemanagt werden. Alle Lehrenden und Lernenden gelangen über eine Start- und Anmeldeseite im Internet in einen virtuellen Campusbereich, wo z. B. Lernmittel für sie bereitstehen und Arbeitsaufträge einsehbar sind oder erledigte Aufgaben von ihnen abgespeichert und/oder verschickt werden können.
Enterprise-Modell	IT-Infrastruktur, die sich für den Einsatz in professionellen Kontexten eignet, im Gegensatz zu Consumer-Geräten, die für die Nutzung in privaten Haushalten gedacht sind
IP-Adresse	Adresse in Computernetzen, die auf dem Internetprotokoll basieren (z. B. das Internet oder auch firmeninterne lokale Netzwerke). IP-Adressen müssen im Allgemeinen eindeutig sein, das heißt, eine Adresse darf nicht versehentlich mehrfach vergeben werden.

IP Address Management (IPAM)	Software zur Organisation bzw. Verwaltung von IP-Adressen in einem Netzwerk
Mesh-WLAN	siehe WLAN-Mesh
(Mobile-)Device-Management	softwaregestützte Geräteverwaltung in einem Netzwerk; umfasst Software Deployment und IP Address Management
Netzsegment	auch Netzwerksegment; physisch und/oder virtuell (logisch) von anderen Teilen eines größeren Netzwerkes abgetrennter Bereich. Die Segmentierung ermöglicht es, bestimmte Datenbereiche innerhalb des gesamten Netzwerkes nur für definierte Teilgruppen unter allen im Gesamtnetzwerk angemeldeten Nutzern verfügbar zu machen.
Power over Ethernet (PoE)	Stromversorgung von Netzwerkkomponenten (Hardware) über Netzwerkkabel
Power Switch	Ein Switch ist ein Kopplungselement, das mehrere Hosts (Endgeräte) in einem Netzwerk miteinander verbindet, quasi ein Verteiler. Ein Power Switch bietet darüber hinaus die Stromeinspeisung für PoE.
Pre-Shared Key (PSK)	Eine Verschlüsselungsmethode für Kommunikationswege, bei dem der Schlüssel unter den Kommunikationsteilnehmern vorab geteilt werden muss. Ein gängiges Beispiel ist das sogenannte »WLAN-Passwort«.
RADIUS-Server	engl. R emote A uthentication D ial- I n U ser S ervice = Authentifizierungsdienst für sich einwählende Benutzer ein Client-Server-Protokoll, das zur Authentifizierung, zur Autorisierung und zum Accounting (Triple-A-System) von Benutzern bei Einwahlverbindungen in ein Computernetzwerk dient (<i>Quelle: Wikipedia, Stichwort »Remote Authentication Dial-In User Service«, Version vom 5. November 2019, 15:51 Uhr, abrufbar unter https://de.wikipedia.org/w/index.php?title=Remote_Authentication_Dial-In_User_Service&oldid=190333470</i>)
Roaming (WLAN)	engl. roaming = umherwandern Ein Endgerät verbindet sich (im Idealfall) automatisch mit dem empfangs-stärksten Accesspoint (»WLAN-Roaming«).
Rollback	das Zurücksetzen eines EDV-Systems auf einen früheren Zustand
SD-WLAN + LAN	SD = software-defined Netzwerk, das nicht über physische (W)LAN-Controller, sondern über Software-Controller via Cloud administriert wird

Self-Healing Network	engl. self-healing = selbstheilend Fällt im Netzwerk ein Accesspoint aus, wird automatisch die Leistung der umliegenden Accesspoints erhöht, um keine Deckungslücke aufkommen zu lassen.
Software Deployment	bietet die Möglichkeit, Software- bzw. App-Installationen und Software-/ Firmware-/Treiberupdates zu durch die Administration festgesetzten Zeitpunkten auf allen im Netzwerk angeschlossenen Geräten durchzuführen
SSID	Abkürzung für S ervice S et I dentifier allgemein der Name / die Bezeichnung eines WLAN: Ein WLAN-Accesspoint kann mehrere SSIDs bedienen und ermöglicht damit die Nutzung verschiedener (V)LANs.
VLAN	Abkürzung für V irtual L ocal A rea N etwork Verschiedene VLANs verwenden dieselben aktiven Komponenten (Switches), sind aber softwareseitig so voneinander getrennt, dass ein Datenverkehr zwischen den verschiedenen Netzen nicht bzw. nur über definierte Schnittstellen möglich ist.
Virtualisierung	»Nachbau« einer Hardwarekomponente auf Basis von Software
Wireless Bridging	siehe WLAN-Bridge
WLAN-Bridge	Funkbrücke über zwei Accesspoints, die ausschließlich für den dedizierten Datentransfer untereinander genutzt werden, um so eine Verkabelungslücke zu schließen
WLAN-Controller	können Accesspoints lokal und zentral vollautomatisch konfigurieren und steuern; Hardware mit auf dem Gerät installierter Management-Software
WLAN-Mesh	ein drahtloses lokales Netzwerk aus miteinander kommunizierenden Accesspoints, das »sich selbst einrichtet«, indem ein Basis-Accesspoint, in dessen Software die Netzwerkeinstellungen eingegeben wurden, diese Konfiguration via Funk an alle weiteren Accesspoints, die »Satelliten« des Mesh, überträgt. Im Betrieb wird der optimale Datenfluss im System durch die Funkkommunikation der Komponenten untereinander gewährleistet.
WPA2-Enterprise	Abkürzung für Wireless Protected Access Vs.2 Sicherheitsstandard für Funknetzwerke mit sicherer Verschlüsselung durch Advanced Encryption Standard (fortgeschrittener Verschlüsselungsstandard)

WEITERE PUBLIKATIONEN

Medienkompetenzrahmen NRW



In sieben Schritten zum schulischen Medienkonzept



Medienentwicklungsplanung



Lernförderliche IT-Ausstattung für Schulen



Schule und Unterricht in der digitalen Welt



Datenschutz an Schulen in NRW



Weitere Informationen: www.medienberatung.nrw.de



Bestellung Printmaterialien





LWL
Für die Menschen.
Für Westfalen-Lippe.

LVR
Qualität für Menschen

Ministerium für
Schule und Bildung
des Landes Nordrhein-Westfalen

