LEITFADEN

NETZWERKINFRASTRUKTUR IN SCHULEN

Wie zeitgemäße LAN- und WLAN-Infrastruktur die Digitalisierung im Bildungswesen ermöglicht

aruba
a Hewlett Packard Enterprise company

INHALT

VORWORT

„Die Digitalisierung hat die Gesellschaften verändert – und wird sie weiter rasant verändern. Weltweit prägen digitale Medien und Werkzeuge den Alltag vieler Menschen. Dieser Wandel macht auch vor den Klassenzimmern nicht Halt: damit Schulen im digitalen Zeitalter ihren Bildungs- und Erziehungsauftrag erfüllen und Schülerinnen und Schüler auf das Leben gut vorbereiten können, brauchen Schulen gut ausgebildete Lehrkräfte, geeignete pädagogische Konzepte, sowie eine leistungsfähige digitale Infrastruktur. Das ist das gemeinsame Verständnis von Bund und Ländern.[1]“

Die von dem Bundesministerum für Bildung und Forschung hervorgehobene digitale Infrastruktur ist die essentielle Grundlage für digitale Schule. Erst durch eine leistungsfähige, belastbare und skalierende Infrastruktur können sowohl Lernprogramme, als auch Lehrer- und Schülerendgeräte reibungslos, stabil und sicher genutzt werden. Dabei wird unter dem Begriff Infrastruktur sowohl Schulserver und Speichersysteme, als auch die Netzwerkinfrastruktur zusammengefasst.

Dieser Leitfaden soll zum Verständnis der Netzwerkinfrastruktur im Detail beitragen und den Entscheidungsträgern in Schulen dabei helfen, im komplexen IT-Umfeld fundierte Entscheidungen treffen zu können.

ZUSAMMENFASSUNG – WAS IST DAS ZIEL DIESES LEITFADENS?

Der Leitfaden „Netzwerkinfrastruktur in Schulen“ dient als Referenzdokument für sämtliche Akteure im Bildungsumfeld. Nach dem Studium des Leitfadens sollen die Herausforderungen und Lösungen im Netzwerkumfeld auch für Laien verständlich sein. Er schafft eine Entscheidungsgrundlage für den verantwortungsvollen Umgang mit Budget und Ressourcen. Damit wird das Ziel des Bundesministeriums für Bildung und Forschung erreicht: den Zugang zu digitaler Bildung für jeden einzelnen Schüler zu ermöglichen.

Die Empfehlungen und Produktvorschläge sind konkret auf das Umfeld von Schulen und Bildungseinrichtungen abgestimmt und wurden aus den Erkenntnissen einer großen Anzahl bereits umgesetzter Schulprojekte gesammelt.

Aruba, ein Unternehmen der Hewlett Packard Enterprise, bietet als führendes Technologieunternehmen qualitativ hochwertige LAN-, WLAN- und Netzwerksicherheitslösungen für Schulen. Darüber hinaus stellen wir auf die Anforderungen von Schulen abgestimmte Lösungen zu Schulkonditionen bereit.

HERAUSFORDERUNGEN IM UMFELD DER DIGITALISIERUNG VON SCHULEN

Während die Mehrheit der Lehrer sich darüber einig ist, dass Digitalisierung den Unterricht bereichert, stehen viele Akteure vor der Herausforderung, wie eine Umsetzung dieser gelingt. Dabei spielen viele Themen eine Rolle:

- Welche Endgeräte für Lehrer und Schüler (Tablets, Notebooks, Smartphones, ...)?
- Verwendung eigener Geräte durch Personal und Schüler (BYOD – Bring Your Own Device)?
- Wie steht es um die Sicherheit im Netzwerk und Sicherheit der Daten vor Angreifern?
- Wie gestaltet sich die Umsetzung und Einhaltung der Datenschutzgrundverordnung (DSGVO) und anderer relevanter Richtlinien?
- Wie werden elektronische Tafeln, Beamer, Drucker, IP-Telefone, Schließsysteme, Hausautomationssysteme, etc. ... (IoT – Internet of Things) eingebunden?
- Ist die Bandbreite in das Internet ausreichend?
- Wie lösen sich die Begrenzung zeitlicher Ressourcen und das Know-How in Zukunft?
- Wie hoch muss das Budget für die Umsetzung sein?

Aruba unterstützt Schulen und Lehrer mit ihren Produkten und Lösungen dabei, diese Hindernisse zu überwinden.

Das Netzwerk, und damit letzlich auch WLAN, ist eine Grundversorgung für die digitale Schule wie Strom und Wasser.

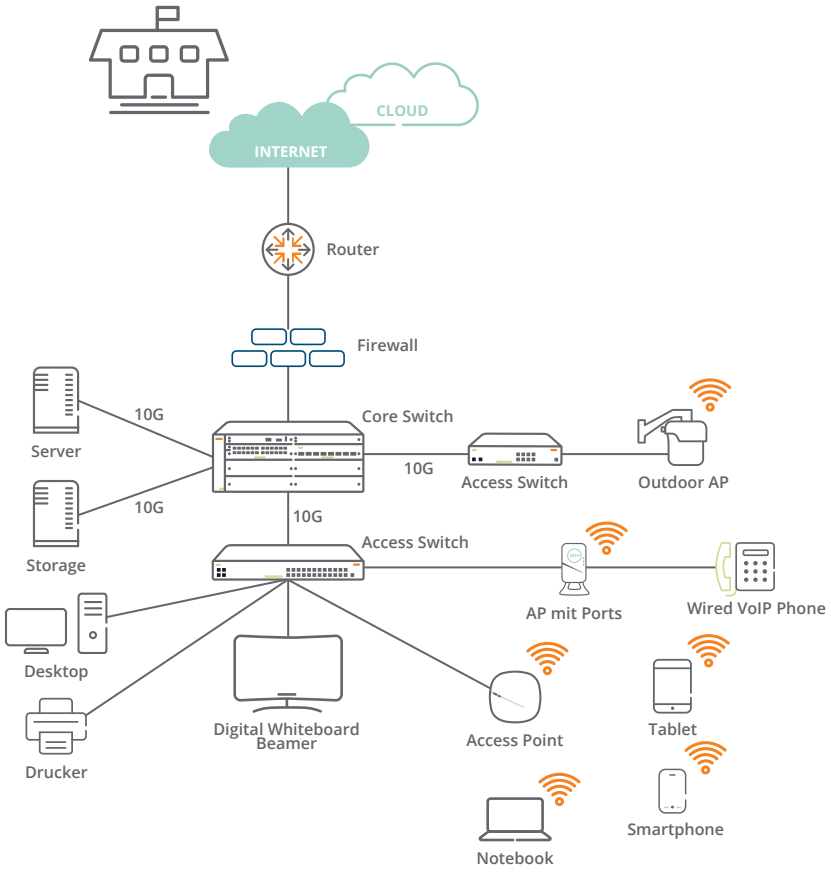
Wenn es um die Digitalisierung der Schulen und deren Herausforderungen geht, dann gibt es Bereiche, die stärker durch pädagogische Konzepte und Herangehensweisen beeinflusst werden, und welche, die davon quasi unberührt bleiben.

So ist etwa die Strom- und Wasserversorgung in jedem Fall essentiell, dass Unterricht stattfinden kann, unabhängig davon, für welche Didaktik und welches Konzept sich der einzelne Lehrer entscheidet. Sie stellen eine Grundvoraussetzung dar.

Anders verhält es sich etwa bei den eingesetzten Lehrmitteln und Medien: Ist es beispielsweise durch den Lehrer gewünscht, dass Schüler selbständig Videos drehen können, müssen Endgeräte angeschafft werden, die entsprechend mobil sind und über eine vernünftige Kamera verfügen.

Die Netzwerkausstattung einer Schule zählt zu den Grundvoraussetzungen für die digitale Schule. Ähnlich wie bei Strom und Wasser kommt es darauf an, dass das Netzwerk in der richtigen Qualität und mit der richtigen Leistung aufgebaut wird. Es ermöglicht die Kommunikation der (neu eingeführten) Medien untereinander, die Nutzung von Internetdiensten, sowie von zentral bereitgestellten Lernprogrammen (die etwa in der Cloud oder auf einem Schul-

[1] https://www.bmbf.de/de/mit-dem-digitalpakt-schulen-zukunftsfaehig-machen-4272.html Stand 15.10.2019



server laufen). Die Gestaltung des Netzwerkes wird jedoch nicht immer durch die neuen Medienkonzepte und pädagogischen Ansätze beeinflusst.

Damit kann das Netzwerk als erste Maßnahme für die Digitalisierung angegangen werden. Alle anderen Bereiche bauen dann darauf auf und werden in Abhängigkeit vom erarbeiteten Medienkonzept entwickelt und umgesetzt, z.B. welche Anzeigegeräte oder Endgeräte zukünftig eingesetzt werden.

BESTANDTEILE EINES MODERNEN NETZWERKS

Ein zeitgemäßes Netzwerk besteht üblicherweise aus folgenden Komponenten:

Router

Der Router ist ein Koppelelement für unterschiedliche Netzbereiche, in unserem Beispiel zwischen dem Schulnetz und dem Zugang nach außen (Internet und Cloudlösungen), und wird zumeist vom jeweiligen Internet-Provider zur Verfügung gestellt. Bestimmte Router bieten neben der kabelgebundenen Leitung alternativ auch eine Internetanbindung über UMTS oder LTE an, um im Fehlerfall eine Ersatzroute ins Internet aufbauen zu können.

Firewall

Die Firewall stellt eine wichtige Komponente dar, um die Sicherheit im Netzwerk zu gewährleisten. Sie kann als Filter betrachtet werden, der von ein- und ausgehendem Datenverkehr passiert werden muss. Unzulässige Inhalte können entsprechend blockiert werden, sodass das interne Netz geschützt bleibt. Aus der Grafik ist aber auch ersichtlich, dass Inhalte, die innerhalb des Netzwerkes ausgetauscht werden (also ohne den Weg zum Router zu passieren), diesen Beschränkungen nicht unterliegen. Daher stellt eine Firewall nur einen Teil der relevanten Maßnahmen zur Netzwerksicherheit dar.

Core-Switch

Sogenannte Core-Switches sind Verteiler, die meist in lokalen Rechnernetzen eingesetzt werden. Diese erlauben den angeschlossenen Geräten, Daten in Form von Paketen an einen Empfänger zu senden und zu kommunizieren. Sie besitzen mehrere Ports (Anschlüsse), an die weitere Switches und Endgeräte und WLAN-Access-Points angeschlossen werden. Ganz vereinfacht können sie wie eine Steckdosenleiste, aber für das Netzwerk, betrachtet werden.

Der Core-Switch stellt den Kern des Netzwerks dar, in dem alle Verbindungen zusammengeführt werden. Man spricht bei der Verbindung vom Core-Switch zum Router vom sogenannten „Uplink“, während die Verbindungen zu den Verteilerswitches (Access-Switches) als „Downlinks“ bezeichnet werden.

Eine weitere Aufgabe des Core-Switches ist die zentrale Anbindung lokaler Ressourcen wie Server und Netzwerkspeicher (Storage). Meist befinden sich diese gemeinsam mit dem Core-Switch in einem Serverraum.

Für eine zukunftssichere Installation sollten die Verbindungen zwischen Core-Switch und Access-Switches Bandbreiten von 10 Gigabit/Sekunde unterstützen. Im Idealfall werden diese Verbindungen mit Glasfaserleitungen ausgeführt, da diese auch für zukünftige Technologien noch viel Spielraum betreffend der Bandbreite haben. Es wird zwischen Multimode-Leitungen für kürzere Verbindungslängen und Singlemode-Leitungen für längere Strecken unterschieden. Üblicherweise sind für Schulen Multimode-Verkabelungen nach dem OM3- oder OM4-Standard eine gute Wahl, wobei auch hier Singlemode mehr Kapazitäten für spätere Entwicklungen hat. Bei der Verbindung von unterschiedlichen Gebäuden bieten Glasfaserleitungen auch den Vorteil einer elektrischen Potentialtrennung (Schutz bei Blitzschlägen, unterschiedliches Erdungspotential, ...).

Für sehr kurze Strecken innerhalb eines Raumes (<7 m) können alternativ zur Glasfaser auch günstigere so genannte DAC (Direct Attach Cable) aus Kupfer eingesetzt werden. Eine weitere Möglichkeit bieten 10Gigabit-Kupferverbindungen (10GBASE-T), bei denen jedoch die maximale Länge, sowie die Verfügbarkeit von unterstützten Produkten, eingeschränkt ist. Derartige Lösungen können vor allem zur Anbindung der Server und Storagesysteme Kosteneinsparungen bringen.

Bei kleineren Installationen mit limitierter Anzahl an Endgeräten und maximal 100 m Leitungslänge kann eventuell auf den Core-Switch verzichtet werden. Typischerweise trifft dies auf kleinere und zumeist Grundschulen zu.

Access-Switch

Access-Switches sind sehr ähnlich zu Core-Switches, werden aber aufgrund ihrer Position im Netzwerk anders bezeichnet. Sie stehen in dem Bereich, wo ein Endgerät Zugang („Access“) zum Netz erhält. Über die Access-Switches werden daher alle Endgeräte (PCs, Drucker, Beamer, elektronische Tafeln, IoT-Geräte, ...) sowie Access-Points angeschlossen. Üblicherweise gibt es Access-Switches in Ausführungen von 8 Ports bis maximal 48 Ports. Werden mehr als 48 Ports an einem Standort benötigt, besteht die Möglichkeit des „Stackings“, bei dem mehrere Switches untereinander verbunden werden und nach außen hin wie ein einziger Switch wirken. In einigen Fällen lassen sich auch modulare Switches einsetzen, bei denen mehrere Einschübe mit jeweils bis zu 48 Ports die Gesamtzahl der Anschlüsse abdecken.

LC Duplex Stecker Multimode

SFP+ Transceiver für 10G Glasfaserverbindungen

Um den heutigen Anforderungen gerecht zu werden, sollten die Ports alle eine Bandbreite von 1 Gigabit/Sekunde bieten (1000BASE-T). Allein aus der Summe der dadurch möglichen Datenraten ergibt sich die Sinnhaftigkeit der 10-Gigabit-Leitungen für den Uplink zum Core-Switch. Diese sollten je Switch zumindest mit 2 Stück 10G-Ports, im Idealfall mit 4 Ports ausgeführt sein. Die 10G-Ports sind mit SFP+-Steckmöglichkeiten ausgestattet, in die dann entweder Multimode- oder Singlemode-Transceiver oder ein DAC Kabel eingesteckt werden. Der Transceiver (für 10G auch SFP+ genannt) stellt die Verbindung zu den Glasfaser-Kabeln her, die mit optischen LC-Duplex-Steckern ausgestattet sind.

Power-over-Ethernet (PoE) 802.3af/at/bt hat sich als Technologie durchgesetzt, um Netzwerkgeräte über den Switch über das LAN Kabel gleich mit Strom zu versorgen. So spart man sich die zusätzliche Installation und Verkabelung einer Steckdose in unmittelbarer Nähe von Geräten wie z.B. Access-Points, VoIP -Telefonen oder Sicherheitskameras.

Bei der Verwendung von PoE gibt es mehrere Leistungsklassen der Endgeräte, die bei der Wahl der Switches berücksichtigt werden müssen. Heute ist PoE Plus (802.3at, maximal 30 Watt, auch PoE+) üblich und reicht für die meisten Geräte aus. 802.3bt ermöglicht sogar bis zu 60 Watt per Port, was den Betrieb von sehr leistungsstarken Access-Points und sogar LED-Beleuchtung erlaubt.

Jeder Switch stellt dafür eine maximale Gesamtleistung zur Verfügung, die die Summe der Leistungen der versorgten Geräte nicht überschreiten kann. So muss die Leistung eines Access-Points mit der Anzahl der am Switch angeschlossenen Access-Points multipliziert werden, um den Gesamtbedarf abzuklären.

Bei Planungen der Netzwerkinfrastruktur, am besten durch ein Fachunternehmen, ist zu beachten, dass:

- größere Switches durch ihren Lüfter Geräusche erzeugen
- Abwärme abgeführt werden muss (Überhitzung)
- ausreichend Stromkreise vorgehalten werden
- die zu erstellende Verkabelung PoE-tauglich ist (bis zu 60W pro Leitung)

Sollte die Bereitstellung einer PoE-Infrastruktur (z.B. in älteren Gebäuden) nicht möglich sein, stellt die Verwendung

von PoE-Injektoren oder lokalen externen Netzgeräten eine Alternative dar. Dazu sollten gegebenenfalls in unmittelbarer Nähe der Access-Points Steckdosen vorgesehen werden.

Lüfterlose Switches sollten vor allem dann in Betracht gezogen werden, wenn diese in einem Raum eingesetzt werden, in dem sich Personen länger aufhalten. Die stetige Geräuschbelastung durch Lüfter kann sonst als störend empfunden werden.

Bei allen Geräten muss eine ausreichende Wärmeabfuhr gewährleistet sein – entweder durch klimatisierte Bereiche oder ausreichende Luftzufuhr. Es sollte berücksichtigt werden, dass es in Netzwerkschränken zu keinem „Lüftungskurzschluss" kommt – wenn die Ventilatoren der Geräte in gegengleiche Richtungen blasen und so die warme Abluft der anderen Geräte ansaugen.

WLAN-Access Points

Wenn es um WLAN geht, müssen zwei Komponenten klar voneinander abgegrenzt werden, nämlich der WLAN-Router und der WLAN-Access-Point. Der allseits bekannte WLAN-Router des privaten Internetzugangs besteht aus drei Funktionseinheiten: dem WLAN-Access-Point, einem Switch für kabelgebundene Geräte und einem Router zur Internetanbindung. Ein dedizierter WLAN-Access-Point stellt den Zugangspunkt für das WLAN zur Verfügung. Entgegen den bereits erwähnten WLAN-Routern, werden Access-Points nicht direkt mit dem Internet verbunden, sondern verwenden das lokale Netz. Dieses Netz verfügt selbst über einen zentralen Übergang zum Internet. Dieses Konzept ist so gewählt, weil die Versorgung mehrerer oder aller Bereiche in einer Schule für einen reibungslosen digitalen Unterricht auch mehrere Zugangspunkte erfordert. Um eine flächendeckend breitbandige Abdeckung mit WLAN, bzw. die gewünschte Abdeckung mit WLAN, zu gewährleisten, empfiehlt sich eine professionelle Begutachtung der baulichen Situation, im Idealfall mit entsprechenden Testaufbauten und Messgeräten. Man spricht von einer „WLAN-Ausleuchtung" des Gebäudes, diese wird von Fachunternehmen angeboten.

Grundsätzlich hat sich als Daumenregel ergeben, dass je Klassenraum ein Access-Point installiert wird. Eine Ausleuchtung ist jedoch immer vorzuziehen, allein, um die gewünschte Kapazität zu erzielen und zu vielen Accesspoints vorzubeugen, die sich aus Anwendung der Daumenregel oft ergeben. Für Lehrerzimmer und Büros gibt es eigene Modelle, die neben der Ausstrahlung des WLAN-Signals zusätzliche Netzwerk-Ports aufweisen, die eine PoE-Weiterleitung und somit den Anschluss von zusätzlichen Geräten wie VoIP-Telefonen oder Verwaltungsrechner erlauben. Für Veranstaltungsräume (Aula, Turnsaal, Festsaal, ...) empfiehlt es sich, leistungsstarke Access-Points einzusetzen, da hier gegebenenfalls die Dichte der Endgeräte (z.B. Smartphones bei Veranstaltungen) sehr hoch sein kann. Zur besseren Anpassung der Abdeckung können auch Modelle mit verstellbaren externen Antennen im Einzelfall von Vorteil sein.

Wenn auch im Außenbereich (Schulhof, Sportplatz, ...) WLAN angeboten werden soll, gibt es spezielle Outdoor-Access-Points. Qualitativ hochwertige Modelle können ohne zusätzlichen Schutz den tiefsten Temperaturen im Winter, sowie der prallen Sonne im Sommer, ausgesetzt werden, ohne Leistungseinbußen aufzuweisen. Eine professionelle Möglichkeit eines eventuell notwendigen Blitzschutzes (von Montagesituation und Leitungslängen abhängig) muss gegeben sein.

Bei der Wahl der Access-Points sollte die Montagemöglichkeit mit beachtet werden. Abhängig vom Ort der Installation kann dies als Deckenmontage (eventuell mit Montagekit für abgehängte Decken), Wandmontage oder Mastmontage erfolgen. Die verschiedenen AP-Modelle sind in ihrem Funkverhalten und der daraus resultierenden Signalausbreitung auf je eine dieser Optionen abgestimmt. Sind die Access-Points für Personen physisch zugänglich, ist auf eine sichere Anbringung zu achten, die eine Demontage nur mit Spezialwerkzeug oder Schlüssel ermöglicht.

WLAN-STANDARDS

Seit 1997 ist WLAN in der IEEE-Arbeitsgruppe 802.11 in aufeinanderfolgenden Entwicklungsstufen standardisiert. Da die Nomenklatur mit 802.11 a/b/g/n/ac/ax usw. nicht nur für Laien sehr kryptisch ist, wurde im Oktober 2018 von der Wi-Fi-Allianz eine vereinfachte Benennung beschlossen. Die neue Bezeichnung zu dem aktuellen Standard 802.11ax lautet Wi-Fi 6 und die älteren WLAN-Standards werden rückwärts durchnummeriert. Die Wi-Fi-Allianz ist die Organisation, die WLAN-Produkte für die Einhaltung der WLAN-Standards zertifiziert.

Ein entscheidender Vorteil von WLAN besteht darin, dass der neuere Standard immer abwärtskompatibel zu älteren Standards ist, das bedeutet, dass ein WLAN neuester Generation Endgeräte mit älteren Standards unterstützt, ganz im Gegensatz zu 5G im Mobilfunk.

Wi-Fi 5 - 802.11ac

Dieser seit 2014 veröffentlichte Standard hat viele Vorteile und Leistungsverbesserungen gebracht und sollte den Mindeststandard bei WLAN-Netzen darstellen. Die Einführung des Standards erfolgte in zwei Wellen, wobei in Schulen eingesetzte Access-Points zumindest „ac Wave 2" unterstützen sollten. Frühere Standards (Wi-Fi 1-4, 802.11a/b/g/n/ac Wave 1) sollten für Installationen nicht mehr in Betracht gezogen werden, da sie, sowohl betreffend der Übertragungsbandbreite als auch bezüglich Sicherheit, veraltet sind.

Wi-Fi 6 – 802.11ax

Dieser zuletzt vorgestellte Standard bringt viele weitere technologische Verbesserungen und Vorteile gegenüber Wi-Fi 5, die neben höheren Bandbreiten vor allem eine größere Nutzerdichte ermöglichen. Um alle Vorteile nutzen zu können, ist es essentiell, dass die Access-Points die aktuellsten Chipsätze verbaut haben. Einige Hersteller haben vor der Ratifizierung des Standards erste Produkte auf den Markt gebracht, die nicht alle Funktionen unterstützen. Derzeit sind bereits einige Endgeräte (Handys, Tablets, Notebooks) erhältlich, die Wi-Fi 6 implementiert haben, noch mehr werden folgen. Für eine zukuntssichere Infrastruktur und einen langen Investitionsschutz sollte daher Wi-Fi 6 als Standard für Schulen gewählt werden. Die mit digitalen Bildungsinhalten verbundenen benötigten Bandbreiten summieren sich sowohl über die Anzahl der gleichzeitigen Nutzer, als auch über die Medien-Inhalte selbst, wie Videoströme, Grafiken und Fotos und Video-basierte Zusammenarbeit mit anderen Schulen, Einrichtungen oder an anderen Orten. Da auch bereits 802.11ac Wave 2 Bandbreiten von weit über 1 Gigabit unterstützt, liegt derzeit der Flaschenhals meist nicht im WLAN, sondern in der Anbindung der Access-Points. Eine Variante ist, moderne Access-Switches für Access-Points einzusetzen, deren Ports mehr als 1 Gigabit/s anbieten können. Um eine zukunftsorientierte Installation zu gewährleisten, empfiehlt es sich, dass der gewählte WLAN-Hersteller alle bisher angeführten Technologien und die entsprechenden Wi-Fi-6-Access-Point-Modelle auch im Mischbetrieb unterstützt. So ist später ein schrittweises Upgrade möglich, und es muss nicht das gesamte Netz auf einmal getauscht werden, wenn ein Technologiewechsel ansteht.

Antennenanzahl in Access-Points

Neben dem implementierten WLAN-Standard spielt die Anzahl der Antennen, sowie der gleichzeitigen parallelen Funkverbindungen, eine wichtige Rolle bei der Performance der Access-Points. Je nach Anforderung und Budget stehen Modelle mit einer unterschiedlichen Anzahl von Antennen und gleichzeitigen Datenströmen zur Verfügung. Damit können je nach zu erwartender Nutzung sowohl Klassenräume, als auch Bereiche mit höherer Nutzerdichte, ausreichend ausgestattet werden. Die Auswahl reicht von Modellen mit je zwei Sende- und Empfangsantennen und zwei räumlichen Datenströmen bis hin zu Modellen mit je vier Antennen und bis zu acht Datenströmen. In der Fachterminologie spricht man von Multiuser-Multiple In / Multiple Out, kurz MU-MIMO und kürzt die Antennenanordnung und Datenübertragung ab, analog zum oben genannten Bereich mit 2x2:2 bis 4x4:8. Daraus ergeben sich pro einzelnem Access-Point Nutzerzahlen zwischen ca. 50 bis hin zu etwa 1000 Nutzern bzw. Endgeräten.

An dieser Stelle sollte für eine nachhaltige Ausstattung die zukünftige Entwicklung abgeschätzt werden. Als Daumenregel kann man die Anzahl Personen in einem Bereich eines Access-Points mit dem Faktor 3 bis 4 multiplizieren, um eine Endgeräteanzahl pro Accesspoint zu erhalten. Das liegt daran, dass zum einen jeder Nutzer bereits heute im Schnitt mehr als ein WLAN-fähiges Endgerät benutzt und die Schulen selber eine steigende Anzahl funkfähiger Endgeräte einsetzt, wie z.B. digitale Whiteboards, Klassensätze an Endgeräten und Geräte der Gebäudetechnik.

WLAN-FUNKTIONEN

Den größten Unterschied im reibungslosen Betrieb von WLAN-Netzen machen die von den Herstellern implementierten Funktionen.

Dual Radio

Durch die sehr begrenzt verfügbaren Funkkanäle im 2,4-GHz-Frequenzbereich (von den 13 Kanälen können nur 3 überlappungsfrei verwendet werden), sowie der Störanfälligkeit durch z.B. Mikrowellenherde etc., sollte simultan das 5-GHz-Funkmodul genutzt werden können. Dieses ermöglicht größere Bandbreiten und eine bessere Verteilung der Endgeräte.

Kanal- und Sendeleistungseinstellung

Erfahrene WLAN-Planer können bei der ersten Inbetriebnahme die Kanäle und Sendeleistungen der Access Points vergeben, um eine gegenseitige Interferenz zu vermeiden. Damit kann aber nicht auf sich verändernde Umstände eingegangen werden. Noch praktischer ist daher eine dynamische, automatisch koordinierte Anpassung dieser Parameter durch die Intelligenz in der Steuerung des Netzwerks. Es ist wichtig zu verstehen, dass es kontraproduktiv ist, die Leistung aller Access-Points auf das Maximum einzustellen. Dies führt dazu, dass sich die Access-Points gegenseitig stören und Frequenzen unnötig belegt werden. Daher ist die oft gestellte Frage nach der maximalen Sendeleistung der Access-Points zumeist nicht relevant (diese ist gesetzlich begrenzt), sondern die Möglichkeiten zur Optimierung der Sendeleistung in Abstimmung des gesamten Netzwerks. Aruba bietet diese Funktion in Form des „Green-AP“ Modus, der bei geringer Auslastung redundante Access-Points in einen Stromsparmodus versetzt.

Roaming zwischen Access-Points

Aus dem Mobilfunk sind wir gewohnt, dass unsere Telefonate automatisch an die nächste Basisstation weitergegeben werden, wenn wir uns fortbewegen. Im WLAN trifft das Endgerät die Entscheidung zu roamen und das kann dazu führen, dass ein Nutzer so lange mit dem ersten Access-Point verbunden bleibt, bis sich die Signalstärke so weit senkt, dass ein neuer Access-Point gesucht wird. Dies führt nicht nur bei diesem Nutzer zu schlechter Performance, sondern beeinflusst auch alle anderen Nutzer, die mit

diesem Access Point verbunden sind. Diese so genannte „Sticky Client"-Problematik kann in vielen Netzwerken gut beobachtet werden, da die meisten Nutzer mit dem ersten Access-Point verbunden bleiben, der sich z.B. im Eingangsbereich des Gebäudes befindet.

Da das Endgerät die Entscheidung trifft den Accesspoint zu wechseln, hat Aruba, um dieses Verhalten zu ändern, aufbauend auf der zentralisierten Abstimmung der Access-Points untereinander die patentierte ClientMatch-Funktionalität im Einsatz. Das Netzwerk beobachtet und bewertet die möglichen Verbindungen zu anderen Access-Points und steuert von sich aus eine Übergabe des Nutzers. Bei dieser intelligenten Funktionalität wird nicht nur die Funkleistung in Betracht gezogen, sondern auch die Auslastung der Access-Points und der verfügbare WLAN-Standard am Endgerät mit einbezogen. Somit erzielt ClientMatch die bestmögliche Netzwerkperformance für alle Teilnehmer. Es ist keine Installation von Software auf den Endgeräten erforderlich.

Erkennung und Klassifizierung von Inhalten

Während Firewalls vor schädlichen Inhalten schützen können, die von extern (aus dem Internet) kommen, benötigt es innerhalb des Netzwerkes andere Mechanismen. Durch Technologien wie „Deep Packet Inspection", mit denen der Datenverkehr analysiert werden kann, kann Aruba AppRF den Datenverkehr von über 2800 Programmen bzw. Apps erkennen. Diese Zahl erhöht sich laufend. Sind bestimmte Apps in Verwendung, die noch nicht automatisch erkannt werden, können diese manuell hinzugefügt werden. Die leistungsstarken Prozessoren in den Access-Points ermöglichen somit

- Priorisierung von Apps (z.B. Kommunikation via Skype, Unterrichtsapps, ...)
- Limitierung der Bandbreiten oder Sperre für Apps (z.B. Spotify, Facebook, Netflix ...)
- unterschiedliche Einstellungen für Schüler vs. Lehrer möglich
- optionale Firewall-Funktionalität mit Applikationserkennung und Inhaltsklassifizierung
- Blockieren bzw. Filtern von Verkehr z.B. zum Einhalten von Jugendschutz

Einfache Installation

Durch den Mangel an qualifizierten IT-Fachkräften in Schulen sind eine einfache Installation und Wartung sehr wertvoll. Daher ist es wünschenswert, dass Netzwerkelemente „Zero Touch Provisioning" unterstützen. Das bedeutet, dass neue Access-Points dem Netzwerk einfach hinzugefügt werden können bzw. im Fall eines Tausches dieser ohne aufwändige Installationsroutinen erfolgen kann.

Vermaschung und Serienschaltung von Access Points

Ist eine Anbindung eines Access-Points mittels Ethernet-Kabel nicht möglich, besteht die Möglichkeit der Vermaschung, das sogenannte „Meshing". Dabei werden Access-Points untereinander über das 5-GHz-Funkmodul miteinander verbunden, um den Datenverkehr der Nutzer so ins Netzwerk zu übertragen.

Sollte aus besonderen Gründen eine „Serienschaltung" von Access-Points erwünscht sein (ein Ethernet-Kabel geht zum ersten Access-Point, von dort geht ein Kabel weiter zum nächsten), hat Aruba auch Sondermodelle. Dies spart Ports am Switch und Verkabelung.

Wann immer möglich, sollte eine eigene Leitung zu jedem Access-Point verlegt werden. Auf ein kluges Design ist zu achten, da Meshing und Serienschaltung die gesamte zur Verfügung stehende Bandbreite für User deutlich reduziert und Frequenzen für das Meshing belegt werden. Diese können dann nicht für den WLAN Zugriff zur Verfügung gestellt werden.

Für die besondere Herausforderung, geographisch abgesetzte Gebäude mit dem Schulnetz zu verbinden, ermöglichen spezielle Funkbrücken, wie der Aruba AP-387, Distanzen von bis zu 400 Metern, mit einer Übertragungsrate von bis zu 3,37 Gigabit pro Sekunde, zu überbrücken. Die automatische Ausrichtung der Antennen ermöglicht es, diese Richtfunkstrecke sehr einfach in Betrieb zu nehmen. Als Bestandteil des WLAN-Konzepts fügt sich diese Lösung – anders als herkömmliche Richtfunk-Strecken - nahtlos in das Gesamtportfolio ein.

Zusatzfunktionen

Moderne Access Points beschränken sich nicht nur auf WLAN, sondern unterstützen in vielen Fällen auch Bluetooth, ZigBee und zukünftig weitere Standards, die in der Steuerung von Lichtsystemen (Stichwort Smart Buildings) etc. eingesetzt werden. Auch wenn diese derzeit vielleicht nicht genutzt werden, sollte, im Sinne der Zukunftssicherheit, in die Überlegungen einbezogen werden, dass damit z.B. Asset-Tracking (Auffinden von Gegenständen wie mobilen Beamern im Gebäude, Warnung beim Verlassen des Gebäudes, ...), Indoor-Navigation, Steuerung von Schließsystemen, digitale Raumbeschilderung etc. realisiert werden können.

Qualität - Limited Lifetime Warranty

Ein wichtiger Faktor in der Differenzierung von Netzwerkausrüstung ist die Qualität der Hardware und Software. Namhafte Hersteller bieten daher eine „Limited Lifetime Warranty" an. Das bedeutet, dass ein Austausch der Hardware bei unverschuldetem Defekt kostenlos stattfindet, nicht nur während des Gewährleistungszeitraumes von 12 Monaten im B2B-Bereich. Dies entspricht einer Investitionssicherung, die besonders für Schulen wichtig ist, da die Investitionszyklen meist länger sind als in anderen Branchen.

Die Limitierung der lebenslangen Garantie bezieht sich vorrangig darauf, dass diese für den ersten Endkunden gilt – daher ist es wichtig, bei autorisierten Partnern zu kaufen, welche die Schule dem Hersteller gegenüber als Endkunden anführen.

Unterstützung bei Fragen - Support

Auch in diesem Punkt trennt sich die Spreu vom Weizen. Eine Schule sollte eine Supportorganisation des Herstellers im eigenen Land erwarten, zusätzlich leisten Foren und das Know-How des installierenden Unternehmens einen wichtigen Beitrag.

Aruba bietet all das, mit einer über 90.000 Teilnehmer umfassenden Airheads-Community, die neben Online-Veranstaltungen auch regelmäßige Airheads-Treffen in Deutschland durchführt.

WLAN-ARCHITEKTUR

Netzwerktechnik-Hersteller bieten unterschiedliche Konzepte für die Architektur und Verwaltung der Access-Points an. Jedes der Konzepte hat Vorteile und Nachteile – daher ist es wichtig, dass alle Access-Points des Herstellers flexibel eingesetzt werden können und die verschiedenen Konzepte unterstützen. Sonst führt eine spätere Anpassung bei Änderung der Anforderungen dazu, dass die gesamte Hardware getauscht werden muss – das wäre nicht nachhaltig.

Aruba Instant

Für kleinere Installationen bis 128 Access-Points und maximal 2048 Endgeräte eignet sich Aruba Instant. Bei dieser Architekturvariante übernimmt der erste in Betrieb genommene Access-Point die Rolle eines virtuellen Masters. Er koordiniert die Leistungs- und Kanalanpassung, steuert das automatische Roaming und ermöglicht die reibungslose Installation. Ist dieser Access-Point mit den gewünschten Einstellungen in Betrieb genommen, fügen sich die weiteren Access-Points, die an das gleiche Netzwerk angeschlossen werden, automatisch in den gleichen Cluster hinzu und übernehmen alle Einstellungen. Sollte der Master ausfallen, übernimmt einer der verbleibenden Access-Points diese Rolle.

Controllerbasierende Lösung

Für größere Netzwerke oder bei besonderen Anforderungen empfiehlt sich der Einsatz eines Hardware-Controllers. Dieser wird an den Core-Switch angeschlossen und kommuniziert mit allen Access-Points, um die optimale Performance im Netzwerk zu gewährleisten. Zusätzlich ermöglicht der Einsatz eines Controllers auch die Verwendung von „Remote Access Points“. Diese können an einem beliebigen Ort mit Internetanbindung in Betrieb genommen werden (Home-Office, Hotel, ...), bauen einen Tunnel zum Controller auf und stellen dann vor Ort exakt das gleiche Netzwerk mit allen Zugängen zu Verfügung, wie wenn man sich in der Schule befinden würde.

Eine Alternative zum Hardware-Controller bietet der virtuelle Controller, der als virtuelle Maschine installiert werden kann.

Die Nachhaltigkeit dieser Architektur besteht darin, dass die Access-Points in beiden Varianten die gleichen Modelle sind und somit bei Wechsel von einer Instant- zu einer Controllerlösung an ihrem Installationsort verbleiben können, das spart Zeit, finanzielle Mittel und sichert einen reibungslosen Unterricht, auch wenn Anforderungen sich ändern sollten.

Netzwerkverwaltung und Überwachung

Die Verwaltung (Management) von Netzwerken kann aufwändig sein und viel Zeit in Anspruch nehmen. Daher ist es für Netzwerkadministratoren wünschenswert, wenn damit möglichst wenig Aufwand verbunden ist und Änderungen so selten wie möglich vorgenommen werden müssen. Außerdem hilft ein gemeinsames Management von LAN und WLAN bei der raschen Aufdeckung von Problemen und einem raschen Überblick zur Status des Netzwerkes. Bei der Auswahl der Managementplattform ist zu berücksichtigen, ggf. auch Dritthersteller zu integrieren, um bestehende Infrastrukturen mit einbinden zu können, eine Migration durchzuführen und für die Zukunft offen zu sein.

Aruba bietet hier wieder Alternativen, um den individuellen Bedürfnissen von Schulen gerecht werden zu können.

Vor-Ort Management (On Premises)

Sowohl beim Einsatz von Instant, als auch bei Controllern hat sich für Schulen die Aruba AirWave-Plattform bewährt. Diese unterstützt neben den Aruba-Switches und -Access-Points auch Produkte anderer Hersteller und ermöglicht so einen Gesamtüberblick des Netzwerks in Echtzeit. Die grafische Aufbereitung der Ergebnisse der Überwachung (Monitoring), sowie die Option, auch Details aufzurufen, ermöglichen eine einfache und rasche Ermittlung von Ursachen für Problemen der Nutzer und oder Endgeräten.

Weitere Funktionalitäten sind das Erkennen und Auffinden von unerwünschten, externen Access-Points, die Erkennung von diversen Angriffsmethoden auf WLANs sowie die Darstellung der aufgebauten Infrastruktur und deren Abdeckung in einem Gebäudeplan.

Neben individuell konfigurierbarer, automatischer Alarmierung bei Bedrohungen oder Fehlern im Netzwerk beinhaltet AirWave eine Vielzahl verschiedener vordefinierter Berichte (Reports), wie zum Beispiel: Netzwerkauslastung, Applikationsnutzung, Verkehrsanalyse oder Funkauslastung und Kapazitätsengpässe. Diese Berichte können angepasst und kombiniert werden, um in regelmäßigen Abständen über Netzwerkdetails zu informieren.

Aruba AirWave kann dabei lokal bei der Schule vor Ort installiert werden oder aber auch beim Netzwerkbetreiber (z.B. Schulaufwandsträger) für ein zentrales Management mehrerer Schulen. Für letzteren Anwendungsfall ist es notwendig, dass sich alle Schulen und der Netzwerkbetreiber im gleichen Netz befinden.

Cloud-Management

Für verteilte Netzwerke oder schulübergreifendes Management bietet sich Aruba Central an. Hier sitzt das Management in der Cloud und kann von überall aus über einen Browser bedient werden. So kann ein Systembetreuer mehrere Standorte oder Schulen verwalten, ohne physisch vor Ort sein zu müssen. Es werden nur die Managementdaten an ein hochsicheres Rechenzentrum innerhalb der EU übertragen, weshalb diese Lösung auch DSGVO-konform ist. Der Zugang zu den verwalteten Schulen lässt sich granular zuweisen. Änderungen können pro Access-Point, pro Standort oder für mehrere Standorte gleichzeitig vorgenommen werden.

Zusätzlich zur Konfiguration von Switches und Access-Points ist auch eine Überwachung (Monitoring) mit vergleichbaren Funktionen und Berichten (Reports) wie bei Aruba AirWave vorhanden.

Auf Aruba Central als cloudbasierte Managementlösung wird über einen Internetbrowser zugegriffen.

Die Nutzungsmöglichkeit über den Browser wird durch Apps für Android und iOS ergänzt, die auch am Smartphone oder Tablet den sofortigen Überblick bieten.

ÜBERWACHUNG DER SCHULANWENDUNGEN UND DER INFRASTRUKTUR AUS SICHT DER NUTZER

Zukünftig ist es Hauptaufgabe der Schule, Bildung in einem digitalisierten Umfeld zu vermitteln. Hierbei ist essentiell, dass der Unterrichtsfluss nicht durch Fehler in der Infrastruktur oder nicht verfügbare Programme behindert wird. Daher sollte die Fehlerbehebung vor dem Unterricht erfolgen und auch die Anwendungsverfügbarkeit sollte zu Unterrichtsbeginn sichergestellt sein. Dies kann mittels einfach bereitzustellenden Sensoren erreicht werden. Sie simulieren einen Endanwender im Netz und führen dafür kontinuierlich benutzerorientierte Anwendungstests durch.

In einer einfachen Anzeige auf der Aruba User-Experience-Insight-Plattform, die über einen Browser aufgerufen wird, werden mittels eindeutigen Symbolen und Ampelfarben die Ergebnisse dieser Tests dargestellt. Dadurch kann im Falle eines Falles schnell Abhilfe geschaffen werden, ohne dass der normale schulische Tagesablauf beeinträchtigt wird.

Die Schule erhält damit wie SchülerInnen und LehrerInnen das Netz erleben Einblicke in das, was SchülerInnen und LehrerInnen erleben, um WLAN- und Anwendungszugriffsprobleme proaktiv zu ermitteln. Dieser zeitgemäße Überblick hilft dem Betreiber der schulischen Infrastruktur, da Probleme zusammenhängend sichtbar werden.

SICHERHEIT IM NETZWERK

Die Sicherheit in Netzwerken lässt sich unter mehreren Aspekten betrachten.

Zugangskontrolle (Network Access Control)

Ein zentrales Thema bei der Sicherheit ist das Zugriffsrecht: wer darf in das Netz und wer nicht? Und: wer darf was im Netz tun? War es früher üblich, die unterschiedlichen Zugriffsrechte über verschiedene WLAN-Netze oder unterschiedliche Anschlüsse (Ports) am Switch zu vergeben, wird heute eine rollenbasierende Rechteverwaltung präferiert. Dadurch wird jedem Nutzer dynamisch seine individuelle Rolle zugeordnet und dann die entsprechenden Ressourcen freigegeben. Möchte ein Nutzer sich mit der Infrastruktur verbinden, dann entscheidet seine Rolle als Lehrer oder als Schüler, welche Zugriffsprivilegien zugewiesen bzw. gesperrt werden. Durch dieses dynamische Verfahren kann wesentlich granularer entschieden werden, wer welche Rechte im Netz bekommt, ohne dass ein erhöhter Aufwand für die Verwaltung des Netzes entsteht. Dies liegt in der Automation dieses Verfahrens, die viel manuelle Arbeit ablöst.

Diese rollenbasierende Rechtezuweisung ist besonders durch die immer breitere Verwendung von sogenannten „IoT"-Geräten relevant. Dabei handelt es sich um alle Geräte des Internet of Things (IoT), wie IP-Kameras, und Sprachassistenten, wie Amazon Alexa, Lichtsteuerungen oder sogar Kaffeemaschinen und Kühlschränke. Das intelligente Erkennen eines Satzes von speziellen Eigenschaften, das sogenannte Fingerprinting zur Erkennung derartiger Geräte, und die Zuweisung der richtigen Netzwerkrechte, schützt vor unberechtigten Zugriffen und vor Angriffen von Hackern.

Ein weiterer Vorteil ist, dass nicht für jede Nutzergruppe (Lehrer, Schüler, Administratior) a) ein eigener Netzwerkname ausgestrahlt werden muss und b) jeder Anschluss (Port) genutzt werden kann. Alle können sich mit dem allgemeinen Schul-Netz verbinden und erhalten ihre individuellen Zugangsrechte.

Gästenetzwerk

Die Einrichtung eines Gästenetzwerks kann in Schulen sinnvoll sein, um Vertretungslehrern, Schülern, Eltern, Gästen oder anderen schulexternen Personen die Möglichkeit zu geben, das Internet über WLAN zu nutzen. Die Möglichkeiten der Zugangsgenehmigung reichen von einem Zugang ohne Passwort, einfacher Selbstregistrierung über „gesponsorte" Zugänge (der Zugang wird von einer definier-

ten schulinternen Person freigegeben), bis hin zu zeitlich eingeschränkten Zugängen mit Nutzername und Passwort.

Integrität der Access Points

WLAN-Aruba-Geräte besitzen einen Sicherheitschip, ein sogenanntes "Trusted Platform Modul (TPM)". Dieses TPM ermöglicht es sicherzustellen, dass das entsprechende Gerät weder gefälscht noch geklont wurde. Die Vertrauenswürdigkeit z.B. eines Access-Points wird somit garantiert. Passwörter und Zugangsdaten können aus den Geräten nicht ausgelesen werden, was zusätzliche Sicherheit bietet.

WLAN-Verschlüsselung

Im Laufe der Jahre wurden verschiedene Verschlüsselungs- und Authentifizierungsverfahren wie WEP, WPA, WPA2 und WPS entwickelt, die noch oft im Einsatz sind aber inzwischen als unsicher und veraltet anzusehen sind. Daher sollten Access-Points den aktuellen WPA3-Standard erfüllen, aber trotzdem abwärtskompatibel zu WPA2 sein, um auch ältere Geräte zu unterstützen.

Ausfallssicherheit und Redundanz

Auch wenn in Schulen ein kurzer Netzwerkausfall üblicherweise keine schwerwiegenden Folgen nach sich zieht, sollte in Anbetracht von Prüfungssituationen, insbesondere den Abschlussprüfungen auf Computern, die Ausfallssicherheit betrachtet werden.

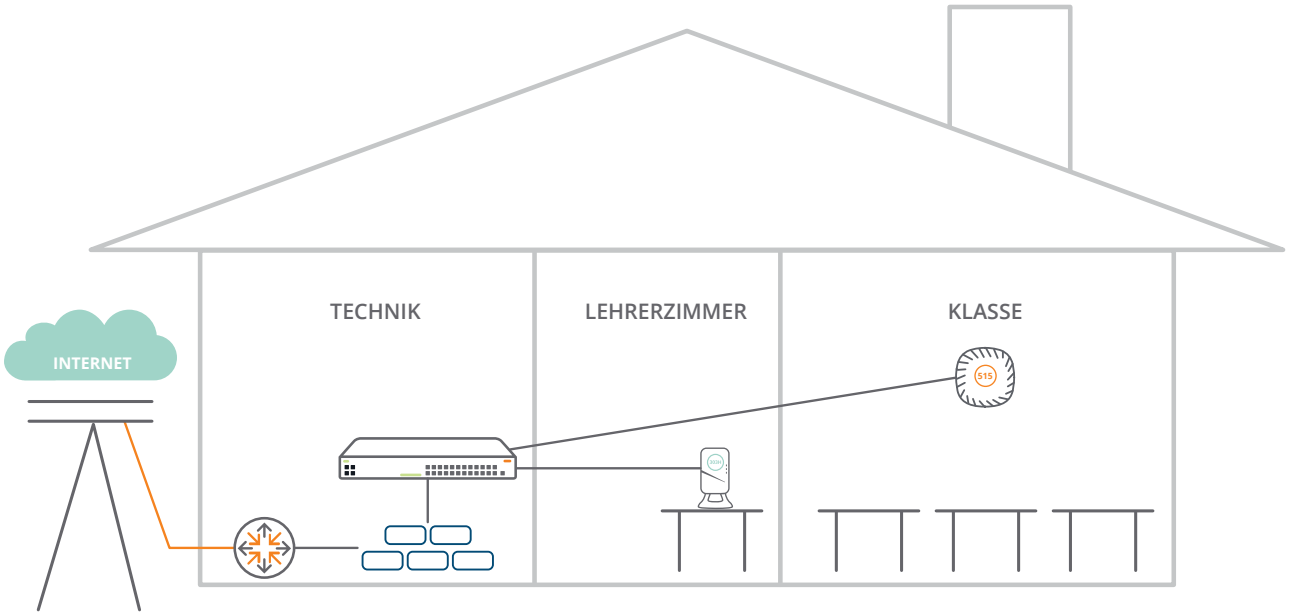
Um eine möglichst hohe Verfügbarkeit des Netzwerks zu gewährleisten, empfiehlt es sich, den Core-Switch doppelt und damit redundant auszuführen. Das bedeutet, dass alle Access-Switches sowie andere Ressourcen wie Server und Storage mit mindestens je einer Leitung an beide Core-Switches angeschlossen werden. Sinnvoll ist – so verfügbar –, die beiden Core-Switches über unabhängige Stromkreise zu versorgen, sowie jeweils mindestens 2 redundante Netzteile pro Switch zu verwenden. Dies erlaubt bei einem Ausfall eines Core-Switches einen ungestörten Netzwerkbetrieb.

Für das WLAN ist eine Überlappung der Abdeckungsbereiche vor allem dann gegeben, wenn die Anordnung der Access-Point anhand einer vorher erfolgten Ausleuchtung ermittelt wurde. Dadurch kann die Infrastruktur der benachbarten Bereiche bis zum Tausch eines defekten Access-Points die Aufgaben übernehmen. Diese Überlappung ermöglicht auch eine erfolgreiche lückenlose Übergabe, das sogenannte Roaming, wenn sich der Nutzer im Gebäude bewegt.

Bei besonderen Anforderungen können detailliertere Redundanzkonzepte erarbeitet werden.

LÖSUNGEN FÜR KLEINE SCHULEN

Im Schnitt beherbergen die ca. 33000 allgemeinbildenden Schulen in Deutschland 10 Klassen. Insbesondere Grundschulen haben, im Gegensatz zu Gymnasien, geringere Schüleranzahlen, damit weniger Klassen und daher oft keinen Bedarf an komplexer Netzwerkinfrastruktur mit Core-Switch und Verteilerswitches. Zudem sind die Anforderungen an diesen Schulen recht statisch und Netzwerke



sollten aufgrund der begrenzten Ressourcen an IT-Fachwissen möglichst ohne regelmäßige Wartung funktionieren. Lange Garantiezeiten sorgen für geringes Investitionsrisiko bei gleichzeitiger Sicherheit.

Wenn die Größe der Schulen und die baulichen Gegebenheiten es erlauben, kann ein einzelner Switch der 2930M-Serie die Schule versorgen. Dieser bieten eine hohe PoE-Leistung, redundante Stromversorgung und je nach Anforderungen bis zu 52 Gigabit-Ports oder schneller.

Alternativ eignet sich als Core-Switch ein Gerät der 3810M-Serie. Diese Serie bietet in einer kompakten Bauform mit redundanter Stromversorgung bis zu 24 schnelle 10G-Ports, an die Access-Switches angeschlossen werden können. Als Access-Switches bietet Aruba mit der 2540-Serie kostengünstige Modelle mit 24 oder 48 Gigabit-Ports an. Wenn kein schallisolierter Technikraum oder -schrank zur Verfügung steht, kann zudem ein lüfterloser, und damit leiser, 8-Port-Switch der 2530-Serie genutzt werden.

Für das WLAN empfiehlt sich eine Architektur ohne Hardware-Controller. Als Access-Points haben sich diese Modelle bewährt:

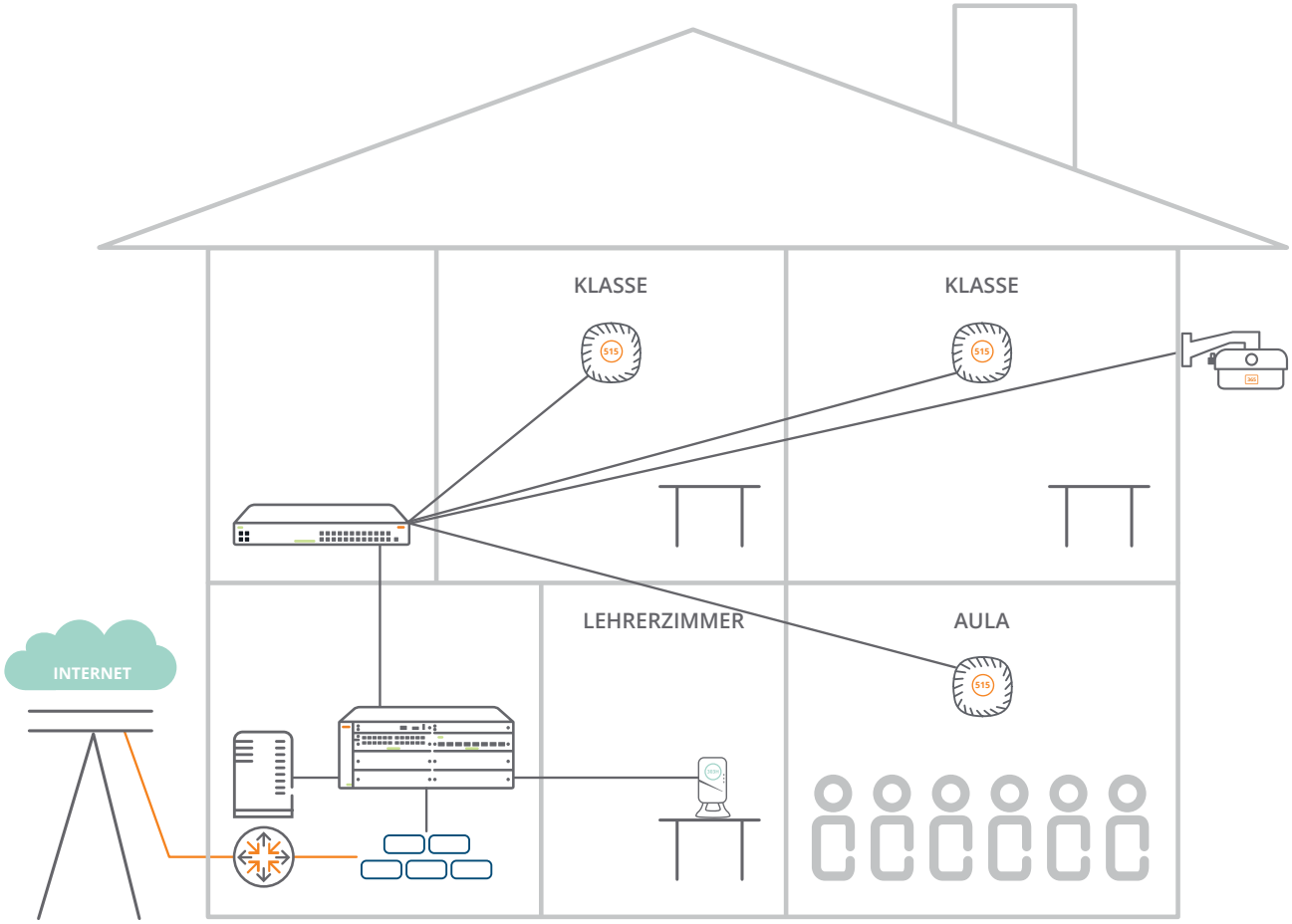
- AP-515 als Standardmodell für Klassenräume
- AP-535 als leistungsstärkeres Modell für Aulen, Musiksäle etc., wenn bei Veranstaltungen mehr als 50 gleichzeitig aktive Nutzer erreicht werden
- Optional AP-303H für Lehrerzimmer. Hier können an drei Ethernet-Ports zusätzlich kabelgebundene Geräte angeschlossen werden

LÖSUNGEN FÜR MITTELGROSSE SCHULEN

In etwas größeren Installationen ist typischerweise ein größerer Core-Switch notwendig, um eine höhere Anzahl Endgeräte und Access-Switches anschließen zu können. Hier bietet sich die flexible und anpassungsfähige 5400-Serie an. Dieses Modell ist modular aufgebaut, in sechs oder zwölf Einschüben können, je nach Anforderungen, verschiedene Module mit unterschiedlichen Ports eingesetzt und nachgerüstet werden. Natürlich bietet auch diese Serie eine redundante Stromversorgung an, darüber hinaus sogar auch die Option auf redundante Management-Module.

Im Access-Bereich kann weiterhin auf die Geräte der 2540-Serie gesetzt werden.

Für das WLAN kann auch bei mittelgroßen Schulen noch eine Architektur ohne dedizierten Controller genutzt werden. Diese Lösung skaliert bis etwa 30-40 Klassenräume (unter Annahme von 30 Personen mit je zwei Geräten pro



Raum). Die Auswahl der Access-Points ist wie oben beschrieben (vgl. Lösungen für kleinere Schulen). Zusätzlich kann für die Abdeckung von Außenbereichen die AP-360-Serie eingesetzt werden. Diese Modelle sind gegen Witterungseinflüsse geschützt.

LÖSUNGEN FÜR GROSSE SCHULEN

Bei über 40 Klassenräumen sollte aus Skalierungsgründen im WLAN auf dedizierte Controller gesetzt werden. Ausschlaggebend für den Architekturwechsel ist, in einer Umgebung wie einer Schule mit einer relativ hohen Dichte an Nutzern, dabei weniger die Anzahl der Access-Points, sondern vielmehr die Anzahl der Endgeräte.

Als WLAN-Controller für große Schulen empfiehlt Aruba das Modell 7205. Damit sind bis 256 Access-Points und 8000 Endgeräte möglich, was für die allermeisten Schulen ausreichend sein sollte. Da die WLAN-Controller in einer controllerbasierten Architektur eine zentrale Rolle im Netz einnehmen und ohne sie das WLAN nicht betrieben werden kann, sollten dringend nicht nur ein einzelner, sondern zwei, sich gegenseitig absichernde, WLAN-Controller eingeplant werden.

Die Access-Point-Modelle sind die gleichen, wie zuvor beschrieben (Vgl. Lösung für kleinere Schulen).

Das kabelgebundene Netz muss natürlich mitwachsen, die für mittelgroße Schulen empfohlenen Komponenten reichen dafür bereits aus. Als Access-Switches können folglich die Geräte der 2540-Serie eingesetzt werden. Im Core kommt weiterhin ein Switch der modularen 5400-Serie zum Einsatz, bei großen Schulen nun aber mit mehr Einschubmodulen.

LÖSUNG CAMPUS MEHRERE SCHULEN (ARUBA CENTRAL)

Für Schulen oder übergeordneten Organisationen mit mehreren räumlich verteilten Standorten stellt sich die besondere Herausforderung, das Netzwerk trotzdem mit wenig Aufwand zu verwalten. Muss bei vielen klassischen Ansätzen der Netzwerkadministrator entweder persönlich vor Ort sein oder sich auf unterschiedliche Arten ins Netz einwählen, gibt es mit Aruba Central eine komfortable und sichere Lösung. Mit der Anmeldung im Browser über die Cloud sieht der Administrator alle Standorte, kann Änderungen bequem für einzelne oder gleichzeitig mehrere Standorte durchführen, und erkennt Situationen, die ein Eingreifen erfordern, auf einen Blick. Und selbst dann noch, wenn die Standorte nicht untereinander vernetzt sind,

Dabei steht der störungsfreie Betrieb wieder an höchster Stelle – selbst bei einem Ausfall der Internetverbindung steht das lokale Netzwerk dem Administrator vollständig zu Verfügung und kann vor Ort verwaltet werden.

FÜR DIE SCHULTRÄGER

Mitunter sehen die Schulträger das IT-Management an den Schulen als wichtigen Bestandteil ihrer Aufgabe. Je nach Bundesland, Region und z.T. Kommune wird die Betreuung der Schulen unterschiedlich umgesetzt. Es hat sich jedoch herausgestellt, dass eine schulübergreifende Betreuung der Netzwerke zu einer Effizienzsteigerung führt. Dafür sind, bzw. werden, daher z.T. Organisationsstrukturen geschaffen, die mehrere Schulen betreuen oder die IT-Verwaltung mehrerer Schulen an einen externen Dienstleister gegeben.

Für diese Struktur bildet Aruba Central eine ideale Lösung, um kosteneffizient einen hohen Grad an Dienstleistung erfüllen zu können. Das Management der Netzwerke kann einerseits von den Schulen selbst, andererseits aber zentral von den betreuenden Organisationen durchgeführt werden. Aufgrund des zentralen Managements müssen Netzwerkbetreuer nicht lokal in der Schule anwesend sein, was speziell im Falle kurzfristig benötigter Änderungen von Vorteil ist. Durch die Möglichkeit, Einstellungen gleichzeitig für mehrere Standorte vorzunehmen, kann z.B. sehr rasch ein Gästenetzwerk auf allen Schulen aktiviert werden oder neue Sicherheitsstandards ausgerollt werden.

Die Flexibilität im Einsatz der Aruba-Lösungen ermöglicht alle Szenarien mit einer Hardware – mit der Option, klein anzufangen und später zu wachsen. Somit sind die Investitionen gesichert.

FÜR DEN DIREKTOR

Für den Schulleiter stehen die Sicherheit der Schüler und ein hoher Bildungsstandard an erster Stelle. Aruba unterstützt dabei mit einer sicheren und zuverlässigen IT-Infrastruktur, die eine Umsetzung von Tablet-Klassen und eine Digitalisierung der Pädagogik ermöglicht.

Die Expertise und Erfahrung von Aruba und seinen Partnern kommt der Schule zugute, was bereits in der Auswahl der geeigneten Produkte ersichtlich wird.

Um darüber hinaus die spezielle Situation von Schulen zu berücksichtigen, bietet Aruba spezielle Schulpreise, die über entsprechend zertifizierte Aruba-Partner abgerufen werden können. Zusätzlich können die Produkte als Dienstleistung „as a Service“ bezogen werden, also gegen einen attraktiven regelmäßigen Betrag anstelle eines einmaligen Kaufes. Die Registrierung der Schule als Endkunde beim Hersteller ermöglicht nicht nur attraktive Projektpreise auch bei kleinen Stückzahlen, sondern stellt auch sicher, dass die Schule in den Genuss der Limited Lifetime Warranty kommt.

Die Investition in ein Aruba-Netzwerk garantiert eine zukunftssichere Lösung. Nicht umsonst wird die Vorreiterrolle von Aruba durch große Institutionen wie Gartner, IDC, Forrester und viele andere regelmäßig bestätigt.

FÜR DEN IT-SYSTEMBETREUER

Die Betreuung mehrerer Schulen stellt oft eine Herausforderung an das Zeitmanagement dar. Dabei kann der Einsatz der Aruba-Infrastruktur im Netzwerk eine entscheidende Rolle spielen. Einerseits ist das Management, Reporting und die Problembehandlung einfach und übersichtlich gestaltet, andererseits ermöglichen zentrale Managementlösungen wie Aruba Central eine Betreuung mehrerer Standorte, ohne vor Ort sein zu müssen. Änderungen müssen nur ein Mal durchgeführt werden und können leicht auf mehrere Netze ausgerollt werden.

Immer mehr Sicherheitsanforderungen verlangen größeres Fachwissen von IT-Administratoren. In den meisten Schulen werden die Netzwerke „nebenbei" verwaltet, oft nur unter großem persönlichem Einsatz.

Aruba unterstützt mit hochwertigen und zuverlässigen Komponenten. Beginnend in der Installationsphase mit Plug-and-Play-Funktionalitäten (Zero-Touch-Provisioning) ergibt sich eine enorme Zeitersparnis, die sich im Betrieb durch Ausfallssicherheit und stabile Verbindungen fortsetzt. Weniger Beschwerden über die Netzwerkqualität bringt mehr Zeit für die wirklich relevanten Dinge.

Regelmäßige, automatisierte Reports und Alarmierungsfunktionen zeigen Engpässe auf, bevor Probleme entstehen. Durch die vielfältigen Funktionen der Aruba-Lösungen können die Anforderungen von Schulleitern und dem Lehrpersonal auf höchstem Niveau umgesetzt werden.

SICHERHEIT

Die Sicherheit der Daten im Netzwerk sollte ein Hauptaugenmerk erhalten. Dies beginnt damit, den Zugang zum Netzwerk nur berechtigten Personen zu ermöglichen. Aber auch innerhalb des Netzwerks ist eine Unterteilung bei den Zugangsrechten in Gruppen wie Administration, Lehrer, Schüler und Gäste sinnvoll. Die oft verwendete Variante von einem „geheimen" Zugangspasswort für das WLAN ist leider keine sichere Lösung.

Moderne Zugangslösungen setzen auf einen rollenbasierenden Zugriff. Jedes Gerät im Netzwerk bekommt eine Rolle zugewiesen, mit der dann die jeweiligen Berechtigungen bei der Anmeldung am Netzwerk verknüpft sind. So wird effektiv verhindert, dass Schüler auf Ressourcen zugreifen können, die Lehrern vorbehalten sind. Gleichzeitig unterstützen automatisierte Regeln den Netzwerkbetreuer, so dass dieser nicht jedes Gerät freischalten muss. Nutzer können ihre Geräte selbst administrieren, was besonders in Zeiten, in denen Smartphones, Tablets oder Notebooks häufig getauscht werden, ein wichtiger Faktor ist.

Diese Art von Sicherheit kann mit der Aruba Lösung ClearPass geschaffen werden. Durch deren Einsatz müssen sich Schulen keine Sorge um die Sicherheit der Zugänge machen. Um den Aufwand bei Schulen gering zu halten, besteht die Möglichkeit, ClearPass als Service zu beziehen – es wird keine Sicherheits-Expertise an der Schule vorausgesetzt.

Details zur Einhaltung der Datenschutzgrundverordnung kann folgender Seite entnommen werden:

https://www.arubanetworks.com/gdpr

Für mehr Fragen und einen direkten Austausch wenden Sie sich gerne an: digitale-schule@hpe.com. Wir freuen uns auf Ihre E-Mail!

DER DIGITALISIERUNGSCHECK

Anbindung ans Internet und andere externe Netzwerke

- [ ] Die Bandbreite ist adäquat, um gleichzeitiges Online-Arbeiten zu ermöglichen

Firewall

- [ ] Filterung von gefährdenden Inhalten
- [ ] Berücksichtigung der DSGVO-Vorgaben

Verkabelung

- [ ] Verbindungen zwischen Core-Switch und Access-Switches sind in Glasfaser (mindestens 10G) ausgeführt
- [ ] Verbindungen zu Access-Points erfolgen mit mindestens 1000BASE-T (Gigabit Kupfer, AWG22 Kat.7)
- [ ] Stromversorgung der Verteilerswitches für PoE-Leistung der angeschlossenen Geräte dimensioniert (Alternativ je Access-Point eine Steckdose)

Netzwerk

- [ ] Redundanz des Core-Switches mit unabhängigen Stromkreisen ist gegeben
- [ ] Es stehen ausreichend Ports zu Verfügung
  - Je Klasse 1x Access-Point, 1x Beamer, 1x Lehrer-PC
  - Je Lehrerzimmer/Büro 1x Access-Point, eventuell PoE-Telefonie, Drucker
  - Weitere Anwendungen wie Schließsysteme, elektronische Tafeln etc. berücksichtigt
- [ ] Das Power-over-Ethernet-Budget entspricht den angeschlossenen Geräten

WLAN

- [ ] Access-Points unterstützen automatische Kanal- und Leistungsabstimmung
- [ ] Automatisches Roaming zwischen Access-Points (ClientMatch)
- [ ] Filterung und Priorisierung von Inhalten (AppRF) mittels Deep-Packet-Inspection (DPI)
- [ ] Bandbreitenbegrenzung für Schüler und Lehrer

WLAN-Abdeckung

- [ ] Alle Klassenräume
- [ ] Lehrerzimmer und Büros
- [ ] Aula und Veranstaltungsräume
- [ ] Außenbereiche

Security

- [ ] Rollenbasierende Zugangskontrolle (Network Access Control) für alle Geräte im Netzwerk
- [ ] Trennung zwischen Lehrer- und Schülergeräte
- [ ] Gästenetzwerk getrennt vom Schulnetz (nur Internetzugang für Gäste)

Management

- [ ] Eine einheitliche Plattform zum Management von LAN und WLAN
- [ ] Einfache Installation durch Zero-Touch-Provisioning (Plug&Play)
- [ ] Cloud-basierendes Management zur einfachen Verwaltung mehrerer Schulen

Reporting und Alarmierung

- [ ] Regelmäßige Netzwerk-Health-Reports mit definierbaren Inhalten
- [ ] Konfigurierbare Alarmierung bei kritischen Netzwerkproblemen und Angriffen

aruba
a Hewlett Packard Enterprise company