

UBIQUITI ENTERPRISE NETZWERKE

Gateways, Switches und Access Points planen, umsetzen und betreiben

Ein praktisches Fachhandbuch für Architekten, Integratoren und Betriebsverantwortliche

Ausgabe 2026 · Birdnetworks KG | Stephan Vogel · Keine offizielle Publikation von Ubiquiti Inc.

Impressum und Hinweise

Titel: [Ubiquiti](#) Enterprise Netzwerke – [Gateways](#), [Switches](#) und [Access Points](#) planen, umsetzen und betreiben.

Stand der technischen Recherche: September 2026. Produktbezeichnungen, Durchsatzwerte, Portlayouts und Softwarefunktionen ändern sich schneller, als man ein Inhaltsverzeichnis aktualisieren kann. Vor Beschaffung und Inbetriebnahme gelten die aktuellen Datenblätter auf techspecs.ui.com sowie die Release Notes der [UniFi](#) Network Application und von [UniFi OS](#) – nicht dieses Buch allein.

Dieses Buch ist ein Fachhandbuch von Birdnetworks KG | Stephan Vogel. Es steht in keiner offiziellen Verbindung zu [Ubiquiti](#) Inc. [UniFi](#), [Ubiquiti](#), [Dream Machine](#), [UniFi OS](#), Etherlighting, PRISM, [Site Magic](#) und weitere genannten Namen sind Marken ihrer jeweiligen Inhaber. Die Verwendung erfolgt ausschließlich zur sachlichen Beschreibung.

Die Inhalte dienen der beruflichen Weiterbildung. Sie ersetzen weder projektspezifische Planung noch Herstellerdokumentation, Normung oder eine Sicherheitsfreigabe. Falsche Firewall-, Routing- oder [WLAN](#)-Einstellungen können Verfügbarkeit und Vertraulichkeit beeinträchtigen – und tun das erfahrungsgemäß gern ab Freitagabend. Änderungen an Produktionsnetzen gehören deshalb hinter Freigabe, Backup und Wartungsfenster.

Leistungsangaben wie IDS/IPS-Durchsatz, Clientzahlen oder [PoE](#)-Budgets sind herstellerseitig oft Best-Case- oder Plattformwerte. Im Feld entscheiden Kabelqualität, [Optik](#), Temperatur, Firmware, aktivierte Sicherheitsdienste und das tatsächliche Verkehrsmuster.

Methodik

Die Darstellung folgt öffentlich verfügbaren Produktdaten, Hilfeartikeln und bewährter Betriebspraxis großer [UniFi](#)-Installationen. Wo Angaben zwischen Quellen schwanken, benennt der Text die Unsicherheit statt eine Scheingenauigkeit vorzutäuschen.

Inhaltsverzeichnis

Inhaltsverzeichnis beim Öffnen in Word aktualisieren (F9).

Word und die meisten kompatiblen Programme aktualisieren das Feldverzeichnis mit F9. Bis dahin dient die folgende Gliederung als Lesekarte. Der zweite Buchblock nach Kapitel 22 – Produktatlas, Vertiefungen, Praxisteile, Arbeitsbücher, Standortmappen, Verfahren, Übungen, Merkblätter und FAQ – gehört ebenfalls ins Verzeichnis.

Vorwort

Wie dieses Buch zu lesen ist

Teil I • Grundlagen

1 Das [UniFi](#)-Ökosystem im Enterprise-Kontext

2 Architekturprinzipien

3 Control Plane und Betriebsmodelle

4 Adressierung, [Switching](#) und Routing

Teil II • Hardware

5 [Gateways](#)

6 [Switches](#)

7 [Access Points](#)

8 Strom, [PoE](#), [Optik](#) und Peripherie

Teil III • Planung

9 Anforderungsanalyse

10 Standorttechnik und Verkabelung

11 [VLAN](#)- und Zonenkonzept

12 [WLAN](#)-Funkplanung

13 Sicherheit by Design

14 Hochverfügbarkeit und Kapazität

Teil IV • Umsetzung

15 Labor, Adoption, Erstkonfiguration

16 Netze, DHCP und DNS

17 Zone-Based Firewall

18 Routing, Multi-WAN und dynamisches Routing

19 VPN, SD-WAN und Identität

20 [Switching](#) im Betrieb

21 [WLAN](#) im Betrieb

22 Qualität, Sprache und Medien

Produktatlas in Prosa

Vertiefungen A–J

Praxisteile und Entwurfsmuster

Essays zur Entwurfshaltung

Arbeitsbücher [Gateway](#) bis Multi-Site

Störungskatalog und Abnahme

Standortmappen und Lehrbriefe

Verfahrenskatalog

Übungen und Lösungen

Merkblätter

Häufige Fragen

Teil V • Betrieb

23 Beobachtbarkeit

24 Lifecycle, Firmware und Change

25 Störungssuche

26 Multi-Site und Organisation

27 Referenzszenarien

Anhang A Checklisten

Anhang B Referenztabellen

Anhang C Glossar

Schlagwortverzeichnis

Vorwort

Enterprise-Netze werden selten an einem Nachmittag entworfen und fast nie durch ein einzelnes Gerät definiert. Sie entstehen aus Anforderungen an Verfügbarkeit, Segmentierung, Funkversorgung, Identität und Betrieb – und aus der Einsicht, dass all das gleichzeitig wichtig wird, sobald die erste Störung kommt.

Wer [UniFi](#) nur als „einfachen Controller plus [Access Points](#)“ kennt, unterschätzt die heutige Plattform. 2026 reicht die [Gateway](#)-Linie vom kompakten [Cloud Gateway](#) bis zum Enterprise Firewall Core mit 100-Gigabit-Anbindung. [Switching](#) reicht vom Flex-Mini bis zum Campus-Access mit 10 GbE und [PoE+++](#) sowie einem Core mit mehreren Terabit. [Access Points](#) decken [Wi-Fi 6E](#) und [Wi-Fi 7](#) ab, inklusive Enterprise-Modellen mit 10-Gigabit-Uplink und redundanter Zweitbuchse. Die Software hat mit Policy Engine, Zone-Based Firewall, [Site Magic](#), [Shadow Mode](#) und dynamischem Routing einen Reifegrad erreicht, der professionelle Entwürfe trägt – sofern man die Grenzen kennt. Genau darum geht es hier: die Grenzen kennen, bevor sie einen kennen.

Dieses Buch behandelt die drei Geräteklassen – [Gateway](#), [Switch](#), [Access Point](#) – als System. Es erklärt, was die Plattform kann, wie man ein belastbares Sollkonzept schreibt, wie man es umsetzt, ohne später in Ausnahmen zu ertrinken, und wie man den Betrieb so organisiert, dass Firmware, Backup und Störungssuche nicht dem Zufall überlassen bleiben.

Der Ton ist praxisnah und skeptisch gegenüber Marketingzahlen. Ein [Gateway](#), das „12,5 Gbit/s IDS/IPS“ ausweist, leistet das nicht automatisch auf jedem Regelwerk, mit SSL-Inspection und gleichzeitigem VPN – Datenblätter lügen nicht, aber sie schweigen gern über die Umstände. Ein [Access Point](#) mit zehn räumlichen Streams versorgt keine Aula, wenn der Uplink nur 1 Gbit/s hat oder der Kanalplan überlappende 80-MHz-Zellen erzeugt. Gute [UniFi](#)-Netze sind deshalb vor allem eines: gut geplant.

Wie dieses Buch zu lesen ist

Teil I schafft die gemeinsame Sprache – auch dann lesen, wenn Sie schon [UniFi](#) betreiben. Viele Produktionsprobleme entstehen nicht aus fehlenden Klicks, sondern aus einem unklaren Betriebsmodell: [Cloud Gateway](#) gegen unabhängiges [UXG](#), lokale Konsole gegen zentrales Hosting, Layer-2-Zugang gegen Layer-3-Grenze.

Teil II ist der Produktatlas, absichtlich vergleichend geschrieben. Modellnamen wechseln schneller als Firmware-Versionen; die Entscheidungsmuster bleiben: Durchsatz mit Sicherheit an, Managementgrenzen, Portgeschwindigkeit, [PoE](#)-Klasse, Netzteile, Steuerungsort.

Teil III ist die Planungslehre: [VLAN](#)-Matrizen, Funkkonzepte, [PoE](#)-Bilanzen und Ausfalldomänen – bevor das erste Gerät adoptiert wird, nicht danach. Teil IV übersetzt das Konzept in die Network Application. Teil V beschreibt den Alltag nach dem Go-live, also den Teil, über den Prospekte schweigen.

Kästen markieren Warnungen, Entwurfsregeln und typische Fehler. Tabellen verdichten Vergleiche. Die Fallstudien in Kapitel 27 sind synthetisch, aber an reale Projektgrößen angelehnt: Mittelstandscampus, Filialnetz, Lager/Produktion, Veranstaltungshaus.

- Leserouten: Erstes größeres Netz: Kapitel 2, 3, 9, 11, 12, 15, 17. Bestehende Installation härten: 11, 13, 14, 17, 23, 24. Hardware wählen: 5-8, Produktatlas, Anhang. Störungen jagen: 20, 21, 25 – und sonst von vorn.
-
-
-

Teil I – Grundlagen

Ein [UniFi](#)-Netzwerk ist kein Stapel isolierter Boxen, sondern zwei Ebenen in einem Haus: die Steuerungsebene und die Datenebene. Wer beide im Kopf trennt, plant besser. Die Steuerungsebene umfasst [UniFi OS](#), die Network Application, Identitäten, Backups und den Site Manager. Die Datenebene umfasst Routing, [Switching](#), Funk und die physischen Pfade. Viele Funktionen – Firewall, DHCP, VPN – sitzen auf dem [Gateway](#) und gehören damit zu beiden Ebenen. Das ist der Hauptgrund, warum man dieses Gerät nicht am Portpreis kauft.

1 Das [UniFi](#)-Ökosystem im Enterprise-Kontext

1.1 Was „Enterprise“ bei [Ubiquiti](#) bedeutet

[Ubiquiti](#) verwendet den Begriff Enterprise sowohl als Produktfamilie als auch als Anspruch. In der Hardware erkennt man ihn an 10- und 25-Gigabit-Anschlüssen, redundanten Netzteilen, hohen [PoE](#)-Budgets, [Shadow Mode](#), Stacking und Campus-Access-Points. In der Software erkennt man ihn an zentralen Richtlinien, dynamischem Routing, SD-WAN-Fabric und einer Firewall, die Zonen statt isolierter Einzelregeln denkt.

Enterprise heißt hier nicht automatisch „Carrier-Core“ oder „hochreguliertes Rechenzentrum“. Die Plattform zielt auf Organisationen, die viele Standorte, viele [Access Points](#) und eine einheitliche Bedienoberfläche wollen, ohne pro Feature zu lizenzieren. Das ist eine Stärke und eine Grenze zugleich. Wer Mikrosegmentierung auf Workload-Ebene, hochkomplexe NAT-Ketten oder zertifizierte Appliances nach Common Criteria braucht, muss die Passung prüfen statt sie vorauszusetzen.

Für die Mehrheit der Campus-, Büro-, Lager- und Filialnetze reicht die Plattform weit, wenn Architektur und Betrieb professionell sind. Genau dieses „wenn“ ist der Gegenstand des Buches.

1.2 Produktfamilien und Abgrenzungen

[UniFi](#) ist die Linie für einheitlich gesteuerte LAN-/[WLAN](#)-Netze. UISP bedient Provider und Weitverkehrsstrecken mit anderer Software und anderen Erwartungen an Routing und Abrechnung. AmpliFi und ältere Consumer-Produkte gehören nicht in ein Enterprise-Sollkonzept. EdgeRouter und [EdgeSwitch](#) existieren weiter in manchen Beständen, werden in neuen Entwürfen aber nicht mehr als Standardpfad empfohlen, wenn das Ziel ein einheitliches [UniFi](#)-Netz ist.

Innerhalb von [UniFi](#) trennt man sinnvoll zwischen Network, Protect, Access, Talk und Connect. Dieses Buch behandelt Network – also [Gateway](#), [Switch](#) und [Access Point](#). Protect taucht auf, weil Kameras [PoE](#), [VLAN](#) und Recorder-Kapazität auf denselben [Switches](#) und [Gateways](#) verbrauchen. Wer Protect dicht neben Network betreibt, muss die Konsole nach CPU, Speicher und Platten dimensionieren, nicht nur nach Routing.

Linie	Rolle	Steuerung	Typischer Einsatz
-------	-------	-----------	-------------------

UniFi Network	LAN, WLAN , Firewall, VPN	UniFi OS / Network Application	Campus, Büro, Filiale, Lager
UniFi Protect	Video	gleiche oder eigene Konsole	Objektschutz, Produktion
UISP	WAN, Funkstrecken, ISP	UISP Application	Provider, Campus-Backbone-Funk
EdgeMAX	klassische Router/ Switches	eigene Web-UI/CLI	Bestand, Spezialrouting

Tabelle 1.1: Einordnung der relevanten [Ubiquiti](#)-Linien

1.3 Die drei Geräteklassen

Das [Gateway](#) ist der Policy- und Routingpunkt: WAN, NAT, Firewall, VPN, IDS/IPS, oft DHCP und DNS. [Cloud Gateways](#) bringen zusätzlich die Network Application mit. Unabhängige [UXG](#)-Modelle routen vor Ort, lassen die Steuerung aber auf Cloud Key, [UniFi](#) OS Server oder Official Hosting.

Der [Switch](#) ist die skalierende Datenebene. Access-[Switches](#) speisen Endgeräte und [Access Points](#) mit Daten und oft mit Strom. Aggregations- und Core-[Switches](#) bündeln Uplinks, bieten höhere Portraten und Redundanzmechanismen wie [MC-LAG](#) oder Stacking. Layer-3-Funktionen auf dem [Switch](#) entlasten das [Gateway](#), wenn Ost-West-Verkehr zwischen Netzen nicht durch die Firewall muss – was eine bewusste Sicherheitsentscheidung ist, keine bloße Komfortfrage.

Der [Access Point](#) ist die kontrollierte Funkzelle. Enterprise-Modelle unterscheiden sich durch Stream-Zahl, 6-GHz-Fähigkeit, spektrale Analyse, Antennenform, Uplinkgeschwindigkeit und Montageort. [WLAN](#) scheitert selten am fehlenden Logo auf dem Gehäuse, sondern an Dichte, Kanalbreite, Leistung und Roaming-Schwellen.

1.4 Lizenzmodell und TCO

[UniFi](#) verkauft Hardware und optionales Hosting, nicht den klassischen Feature-Schlüssel für IPS, VPN-Benutzer oder AP-Anzahl. Das verändert die TCO-Rechnung: Capex für Geräte und Verkabelung dominiert, Opex entsteht durch Planung, Monitoring, Ersatzteilkhaltung und Arbeitszeit. Official [UniFi](#) Hosting ist ein Abonnement für die Steuerungsebene, nicht für Durchsatz.

Trotzdem ist „lizenzfrei“ kein Synonym für „kostenlos im Betrieb“. Ein unterdimensioniertes [Gateway](#) mit aktivierter Inspektion wird zum Flaschenhals. Ein [Switch](#) ohne Reserve-[PoE](#) zwingt zum Tausch der ganzen Etage. Ein AP-Raster ohne 6-GHz-Plan verschwendet die teuerste Hardwaregeneration. TCO gehört deshalb in die Planung, nicht in die Nachkalkulation.

1.5 Typische Einsatzfelder

Mittelständische Zentralen nutzen häufig [UDM-Pro-Max](#) oder [UDM-Beast](#) plus Pro-Max- oder Enterprise-[Switches](#) und U7-/E7-Access-Points. Größere Campusse gehen in Richtung [EFG](#) oder [EF-Core](#), [ECS-Core](#)

und Enterprise-Campus-Access. Filialnetze kombinieren kompakte [Gateways](#) mit wenigen [Switches](#) und standardisiertem [WLAN](#)-Profil, gesteuert über Site Manager und SD-WAN.

Bildung, Hotellerie und Healthcare bringen zusätzlich Dichte, Gastzugang und oft regulatorische Trennung. Produktion und Logistik bringen Roaming für Scanner, schwierige Funkräume und OT-Netze, die nicht im selben Broadcast wie Büro-PCs liegen dürfen. Jedes dieser Felder nutzt dieselbe Plattform, aber nicht dasselbe Design.

1.6 Was [UniFi](#) nicht ersetzen soll

[UniFi](#) ersetzt kein Identity- und Endpoint-Programm. RADIUS, Zertifikate und Gerätehaltung bleiben Voraussetzung für ernsthafte Netzzugangskontrolle. [UniFi](#) ersetzt auch keine Gebäudeverkabelung nach Norm, keine USV-Planung und keine dokumentierte Notfallorganisation. Wer diese Schichten überspringt, erzeugt ein nett aussehendes Dashboard über einem fragilen Unterbau.

2 Architekturprinzipien

2.1 Schichten statt Gerätehaufen

Ein belastbares Netz hat eine Kern-/Edge-Schicht für WAN und inter-[VLAN](#)-Policy, eine Aggregationsschicht für Gebäude- oder Etagenbündelung und eine Access-Schicht für Endgeräte und Funk. Kleine Standorte dürfen Schichten in einem Gehäuse zusammenlegen. Große Standorte dürfen das nicht, nur weil die Oberfläche dieselben Menüs zeigt.

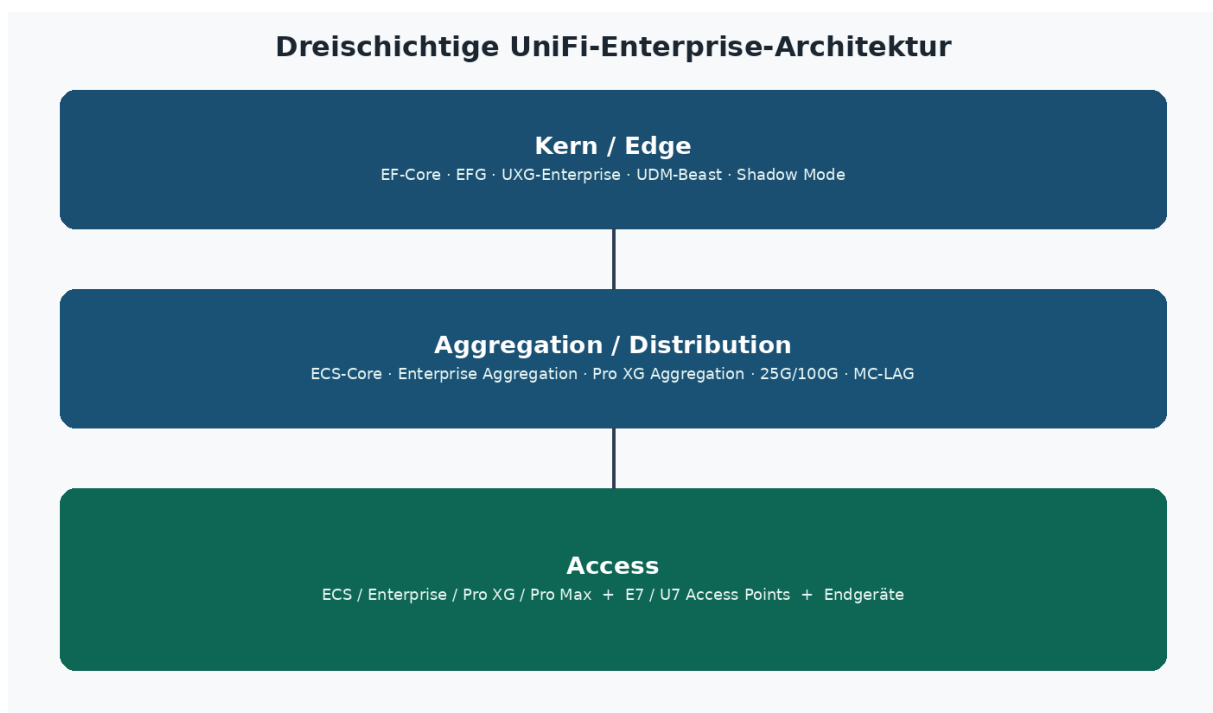


Abbildung 2.1: Dreischichtige [UniFi](#)-Architektur

Die Pfeile zwischen den Schichten sind physische und logische Verträge: Geschwindigkeit, Redundanz, [VLAN](#)-Satz, MTU, Storm Control, Management-VRF oder zumindest Management-[VLAN](#). Wer einen

Access-[Switch](#) mit einem einzigen 1-Gigabit-Uplink an zehn [Wi-Fi-7](#)-APs hängt, hat die Schichtgrenze zwar gezeichnet, aber nicht dimensioniert.

2.2 Ausfalldomänen

Eine Ausfalldomäne ist alles, was bei einem Ereignis gemeinsam stirbt: ein Netzteil, ein ToR-[Switch](#), ein Etagenstrang, ein [Gateway](#) ohne Shadow, ein [WLAN](#)-Kanalcluster, ein DHCP-Scope. Gute Entwürfe machen Domänen klein und ihre Abhängigkeiten sichtbar. Schlechte Entwürfe verstecken sie hinter einem grünen Statuspunkt.

Praktisch heißt das: Zwei Uplinks auf zwei Aggregationsglieder, getrennte Stromkreise für redundante Netzteile, [Gateway](#)-Paar mit State-Sync wo die Plattform es anbietet, überlappende AP-Zellen ohne identische Kanäle, und ein Managementpfad, der nicht ausschließlich über das Produktions-[WLAN](#) läuft.

2.3 Ost-West und Nord-Süd

Nord-Süd ist Verkehr zwischen Innen und Außen oder zwischen Standort und Zentrale. Ost-West ist Verkehr zwischen Servern, Clients und [VLANs](#) am selben Standort. [Gateways](#) mit starker Inspektion sind für Nord-Süd gebaut. Wenn jeder Druckauftrag und jeder Dateikopie zwischen [VLAN](#) 20 und [VLAN](#) 30 durch dasselbe [Gateway](#) muss, wird dessen CPU zur gemeinsamen Bremse.

Die Gegenmaßnahme ist nicht „alles auf einem Flat Network“. Sie ist eine bewusste Platzierung der Layer-3-Grenze: kritisches Ost-West mit Policy auf dem [Gateway](#) oder einer Inspektionsstrecke, unkritisches Ost-West auf dem L3-[Switch](#), und dokumentierte Ausnahmen statt stiller Shortcuts.

2.4 Steuerungs- und Datenebene trennen denken

Fällt die Network Application aus, soll die Datenebene weiterarbeiten. Adoptierte Geräte behalten ihre Konfiguration. Neue Geräte lassen sich jedoch schlecht aufnehmen, und zentrale Änderungen stehen still. Deshalb gehört die Konsole auf eine überwachte Instanz mit Backup, und deshalb ist ein reines Cloud-Login ohne lokale Wiederherstellungsfähigkeit ein Risiko.

Umgekehrt darf die Steuerung nicht zum Datenpfad werden. Management-[VLAN](#), Out-of-Band-Port wo vorhanden und ein Notfallzugang per Konsole oder lokalem Konto sind Teil der Architektur, nicht der Nacharbeit.

2.5 Standardisieren, dann spezialisieren

Filialen, Etagen und AP-Gruppen folgen einem Profil: [VLAN](#)-IDs, SSID-Namen, NTP, Syslog, SNMP oder API-Zugriff, Firmware-Kanal. Abweichungen werden als Ausnahme mit Owner und Ablaufdatum geführt. [UniFi](#) macht Standardisierung leicht, weil Vorlagen und Site-Replikation existieren. Es macht Abweichungen aber auch leicht, weil jeder Admin schnell „nur schnell diese eine SSID“ anlegt. Disziplin ist hier ein Architekturelement.

3 Control Plane und Betriebsmodelle

3.1 Die zwei Gateway-Familien

Cloud Gateways (UCG, UDR, UDM, EFG, EF-Core in der Konsolenrolle) betreiben UniFi OS und die Network Application selbst. Sie sind Standortgehirn und Router in einem. Unabhängige Gateways der UXG-Linie werden von einer externen Network Application adoptiert. Hardware kann dabei sehr ähnlich sein – EFG und UXG-Enterprise sind das bekannteste Zwillingspaar – die Betriebsfrage ist eine andere.

Wählen Sie Cloud Gateway, wenn der Standort autonom laufen soll, Schutzanwendungen lokal bleiben und das Team keine zentrale Controllerfarm betreiben will. Wählen Sie UXG, wenn viele Standorte an einer Steuerung hängen, unterschiedliche Teams dieselben Policies rollen oder die Konsole in einem Rechenzentrum bzw. Official Hosting liegen soll.

Harte Grenze

Ein Cloud Gateway lässt sich nicht nachträglich als reines UXG an einen fremden Controller hängen. Die Entscheidung über das Betriebsmodell fällt vor dem Kauf, nicht nach dem Auspacken.

3.2 Konsolenoptionen

Neben dem Cloud Gateway selbst stehen Cloud Key, UniFi OS Server auf eigener Hardware und Official UniFi Hosting. Cloud Key eignet sich für mittlere lokale Steuerungen ohne Routerfunktion. UniFi OS Server passt, wenn bereits Virtualisierung und Backupstrategien existieren. Hosting passt, wenn das Team keine lokale Steuerungsplattform betreiben will und die WAN-Anbindung der Standorte stabil genug für Adoption und Telemetrie ist.

Die Konsole muss zur Gerätezahl und zu den mitlaufenden Apps dimensioniert sein. Angaben wie „200+ UniFi-Geräte“ oder „500+“ sind Plattformrichtwerte. Viele Kameras, viele Clients und aggressive Statistikintervalle reduzieren den Wohlfühlbereich. In der Praxis plant man Reserve statt exakt an der Kante.

3.3 Site Manager, Sites und Multi-Tenant

Der UniFi Site Manager bündelt Standorte, Status und oft den Einstieg in SD-WAN-Fabrics. Eine Site ist die administrative und meist auch die routingtechnische Einheit. Zu viele logische Netze in einer Site machen Richtlinien unlesbar. Zu viele Mini-Sites ohne Vorlage machen den Betrieb unnötig teuer.

Für Multi-Tenant-Gebäude gilt: Isolation zuerst, gemeinsame SSIDs nur mit sauberer VLAN-Abbildung oder dynamischer Zuweisung. Ein SSID-Wald hilft dem Funk nicht und der Verwaltung nur scheinbar.

3.4 Identitäten und Zugänge zur Steuerung

UI-Accounts, lokale Admins, SSO wo verfügbar und API-Tokens sind Teil der Sicherheitsarchitektur. Gemeinsame Passwörter in einem Teamchat sind ein typischer Auditfund. Jede steuernde Identität braucht ein Rollenmodell: nur Lesen für Leitstand, Change für Betrieb, voller Admin für wenige Personen. Wiederherstellungskonten gehören in den Tresor, nicht in dieselbe Cloud-Mailbox wie der Alltag.

4 Adressierung, Switching und Routing

4.1 Adressplan

Ein Adressplan ist vor der ersten GUI-Sitzung fertig. Er nennt RFC 1918-Bereiche je Standort, VLAN-IDs, DHCP-Bereiche, Reservierungen für Infrastruktur, VPN-Pools und die Regel, dass sich Standorte nicht überlappen, wenn Spoke-to-Spoke oder zentrales Monitoring ohne NAT geplant ist.

Bewährt ist ein Muster aus Standortkennung plus Funktion. Beispiel: 10.S.V.0/24 mit S als Standort und V als VLAN-Funktion. /24 bleibt für Clients übersichtlich. Server- und Managementnetze dürfen kleiner sein. Gäste und BYOD dürfen größer sein, wenn die Tabelle und der Broadcast es tragen – oft ist /23 genug, /16 fast immer zu grob.

<u>VLAN</u>	Name	Beispielnetz	<u>Gateway</u>	DHCP
10	Mgmt	10.10.10.0/24	.1	nur Infrastruktur-Reservierungen
20	Mitarbeiter	10.10.20.0/23	.1	dynamisch, Lease 8 h
30	Server	10.10.30.0/24	.1	Reservierung
40	Drucker/IoT	10.10.40.0/24	.1	dynamisch, kurzer Lease
50	Kamera	10.10.50.0/24	.1	Reservierung
60	Sprache	10.10.60.0/24	.1	Reservierung
70	Gast	10.10.70.0/23	.1	dynamisch, Isolation

Tabelle 4.1: Beispielhafter VLAN- und IPv4-Plan eines Bürocampus

4.2 Layer 2 – das unsichtbare Fundament

VLAN, Trunk, Native VLAN, Spanning Tree und Storm Control klingen nach gestern und entscheiden trotzdem über gestern Nacht. UniFi-Switches bringen RSTP, Portprofile und oft LACP. Loop-Gefahr entsteht durch unsaubere Patchfelder, durch Bridges an Arbeitsplätzen und durch falsch als Access konfigurierte Trunks.

Das Native [VLAN](#) auf Trunks gehört bewusst gesetzt und sollte nicht das Produktions-Clientnetz sein. Management und User-Daten trennen. Unbenutzte Ports liegen in einem Park-[VLAN](#) ohne DHCP oder sind administrativ down.

4.3 Layer 3 – wo das Netz Entscheidungen trifft

Inter-[VLAN](#)-Routing kann auf dem [Gateway](#) oder auf einem L3-[Switch](#) liegen. Auf dem [Gateway](#) gewinnen Sie Sichtbarkeit und Policy. Auf dem [Switch](#) gewinnen Sie Durchsatz und Latenz. Mischformen sind üblich: Default-[Gateway](#) der Clients zeigt auf das [Gateway](#), ausgewählte Netze routen lokal, oder umgekehrt mit gezielten Firewall-Redirects.

BGP und OSPF sind auf den großen [UniFi-Gateways](#) angekommen und machen die Plattform anschlussfähig an bestehende WAN-Netze. Sie ersetzen nicht die Notwendigkeit, AS-Nummern, Route-Policy und Redistribution zu verstehen. Dynamisches Routing ohne Filter ist ein verteilter Fehlerverstärker.

4.4 DHCP, DNS, NTP

DHCP gehört in jedes Segment, das Clients aufnimmt, mit klaren Optionen für [Gateway](#), DNS und wenn nötig PXE oder VoIP. DNS sollte intern kontrollierte Namen auflösen und nach außen weiterleiten. Das [Gateway](#) als Resolver ist bequem und erzeugt eine Abhängigkeit; getrennte Resolver auf den Servernetzen sind robuster, müssen aber in der Firewall erreichbar sein.

NTP ist in Funk- und Zertifikatswelten keine Kleinigkeit. Falsche Zeit zerlegt Logging, Zertifikatsprüfung und später die Forensik. Alle Infrastrukturgeräte beziehen Zeit aus derselben Quelle.

Teil II – Hardware

Hardwarewahl ist Architektur in Einkaufssprache. Wer zuerst den Warenkorb füllt und danach das Sollkonzept schreibt, kauft Reserveports in der falschen Geschwindigkeit – und bezahlt anschließend doppelt: einmal falsch und einmal richtig. Dieser Teil beschreibt [Gateways](#), [Switches](#) und [Access Points](#) so, dass Entscheidungen begründbar bleiben, auch wenn einzelne SKUs auslaufen. Denn sie laufen aus. Immer.

5 [Gateways](#)

5.1 Aufgaben des [Gateways](#)

Das [Gateway](#) ist der Türsteher des Netzes: Es terminiert WAN, erzwingt Policy, übersetzt Adressen, baut VPN, verteilt oft DHCP – und ist in [UniFi](#) zusätzlich Sensor für IDS/IPS und Anwendungserkennung. Es ist selten der Durchsatzkönig des Campus (das sind die [Switches](#)), aber es ist der Ort, an dem das Netz Ja oder Nein sagt. Ein guter Türsteher ist nicht der Größte im Raum – er ist der, der die Liste kennt.

Deshalb dimensioniert man [Gateways](#) nach gleichzeitig inspiziertem Verkehr, Session-Zahl, VPN-Spitzen, WAN-Vielfalt und Managementgrenzen – nicht nach dem schönsten Frontdisplay. Das Display hilft im Rackgang. Es ersetzt keine Lastannahme.

5.2 [Cloud Gateways](#) der Kompaktklasse

[UCG-Ultra](#), [UCG-Max](#) und [UCG-Fiber](#) sind Desktop- oder Kleinrack-Lösungen für Filialen, Projektbüros und Labornetze. Ultra deckt Gigabit-Szenarien mit überschaubarer Gerätezahl. Max erhöht Routing- und Speicherkapazität und eignet sich, wenn Protect klein mitlaufen soll. Fiber bringt 10-Gigabit-Anschlüsse in diese Klasse und ist der sinnvolle Einstieg, sobald der WAN- oder LAN-Kern schneller als 2,5 Gbit/s wird.

Diese Klasse hat begrenzte Redundanz. Es gibt kein echtes Gerätepaar wie bei den Enterprise-[Gateways](#). Verfügbarkeit erreicht man über kaltes Ersatzgerät, gute Konfigurationssicherung und allenfalls WAN-Failover, nicht über nahtloses Umschalten. Wer 99,9 Prozent am selben Standort braucht, steigt eine Klasse auf.

5.3 [Dream Machine](#) als Standortzentrale

[UDM-Pro](#), [UDM-SE](#) und [UDM-Pro-Max](#) sind die Arbeitspferde vieler Mittelstandsnetze: 1-HE-Gehäuse, integrierter Acht-Port-[Switch](#), 10G-[SFP+](#), lokale Platte für Protect, volle [UniFi](#)-App-Palette. Die SE ergänzt [PoE](#) und schnelleres Kupfer-WAN. Die Pro Max erhöht CPU, RAM, Client- und Gerätegrenzen und bietet ein zweites Laufwerk.

Der integrierte [Switch](#) ist ein Zugang für Labor, Kameras in Racknähe oder Management, nicht der Etagen-Access eines Gebäudes. Wer 24 [PoE](#)-APs an die UDM hängt, weil „Ports ja da sind“, vermischt Kern und Access und verliert die Austauschbarkeit.

[UDM-Beast](#) verschiebt die Klasse nach oben: 25G-Anschlüsse, deutlich höherer IDS/IPS-Durchsatz, höhere Geräte- und Benutzer Grenzen, Shadow-Fähigkeit. Sie ist die Antwort auf Standorte, denen Pro Max an CPU und WAN davonläuft, ohne gleich in die Firewall-Core-Welt zu wechseln.

5.4 Enterprise-Firewalls und unabhängige UXG

[EFG](#) und [UXG-Enterprise](#) bilden das 25-Gigabit-Paar der Enterprise-Kante: hoher inspizierter Durchsatz, große Session-Tabellen, Dual-PSU, [Shadow Mode](#), SSL-Inspection und fortgeschrittenes Routing. Der Unterschied ist die Control Plane. [EFG](#) trägt [UniFi](#) Network selbst und bleibt bei den übrigen Apps zurückhaltend. [UXG-Enterprise](#) will adoptiert werden.

[EF-Core](#) erweitert das nach oben in den 100-Gigabit-Bereich mit sehr hohen Geräte- und Benutzer Grenzen sowie IDS/IPS-Werten, die nur Sinn ergeben, wenn auch der Rest des Netzes diese Breitbandwelt tragen kann. Ein Core-Firewall ohne 25/100G-Aggregation dahinter ist ein teurer Anschauungsgegenstand.

[UXG-Lite](#), [UXG-Max](#), [UXG-Fiber](#) und [UXG-Pro](#) füllen die unabhängige Linie nach unten. Sie sind die richtige Wahl für zentral gesteuerte Filialen. [UCG-Industrial](#) adressiert DIN-Schiene und raue Umgebung – hier siegt das Gehäuse über die Portpoesie.

5.5 Leistungsklassen im Vergleich

Modellklasse	Typische WAN-Welt	IDS/IPS-Größenordnung	Steuerung	Redundanz
UCG Ultra / Max	1 / Multi-Gig	ca. 1–2,5 Gbit/s	lokal (Cloud GW)	kalt
UCG Fiber / UXG Fiber	10G	ca. 2,5–5 Gbit/s (Datenblatt prüfen)	lokal bzw. extern	kalt
UDM-Pro / SE	10G	ca. 3,5 Gbit/s	lokal, volle Apps	WAN-Failover
UDM-Pro-Max	10G	ca. 5 Gbit/s	lokal, volle Apps	WAN-Failover
UDM-Beast	25G	bis in den 25-G-Bereich	lokal, volle Apps	Shadow-fähig
EFG / UXG-Enterprise	25G	ca. 12,5 Gbit/s inspiziert	lokal bzw. extern	Shadow, Dual-PSU
EF-Core	100G	sehr hoher insp. Durchsatz	Enterprise-Konsole	Shadow, Dual-PSU

Tabelle 5.1: Orientierungswerte der Gateway-Klassen, Stand öffentliche Angaben 2026

Lesen von Datenblättern

Unterscheiden Sie Routing ohne Inspektion, Routing mit IDS/IPS und Routing mit SSL-Inspection. Die drei Zahlen sind keine Synonyme. VPN-Durchsatz ist eine vierte, oft kleinere Zahl.

5.6 WAN, Multi-WAN und Overlay

Enterprise-Gateways können mehrere WAN-Ports nutzen: aktive Lastverteilung, Failover, policybasiertes Routing. Gute Entwürfe trennen Leitungsarten physisch und logisch: Glas der Zentrale, Backup-Ethernet eines zweiten Providers, optional LTE/5G. Health-Checks müssen die Anwendung sehen, nicht nur das nächste Gateway des ISPs.

SD-WAN und Site Magic sitzen als Overlay obenauf. Sie ersetzen nicht den physikalischen WAN-Vertrag, sondern machen ihn orchestrierbar. Überlappende Filialsubnetze zwingen zu NAT-Spokes und verhindern echte Initiierung aus der Zentrale. Das gehört in den Adressplan, bevor der erste Tunnel grün wird.

5.7 Sicherheitsservices auf dem Gateway

IDS/IPS, Regionenfilter, Content- und URL-Filter und Anwendungskontrolle sind wirksam, wenn das Team sie pflegt. Ungepflegte Signaturen plus pauschales Allow sind Theater. Tiefere Inspektion verschlüsselter Sitzungen ohne interne PKI und ohne Ausnahmeliste für zertifikatsempfindliche Fachverfahren erzeugt Helpdesk-Ticketberge.

Cyber-Sicherheit auf dem Gateway ergänzt Endpoint-Schutz, ersetzt ihn aber nicht. Ein kompromittierter Client im Internal-Zonennetz ist zuerst ein Identitäts- und Segmentierungsproblem.

5.8 Auswahlregeln

- Messen Sie den geplanten inspizierten Peak, nicht den Marketing-Download des Anschlusses.
- Zählen Sie UniFi-Geräte plus Kameras plus künftige Etagen, nicht nur die Geräte von Woche eins.
- Wenn zwei Gebäude oder zwei Provider überleben müssen: Dual-PSU und Shadow Mode in die Pflicht nehmen.
- Wenn Protect, Talk oder Access lokal laufen sollen: Cloud Gateway mit App-Unterstützung, nicht blind EFG.
- Wenn 20 Filialen eine Policy teilen: UXG plus zentrale Steuerung.
- Wenn der Kern 25/100G spricht: Gateway derselben Welt, sonst wandert der Engpass nur um einen Hop.

6 Switches

6.1 Rollen im Switching-Satz

Access-Switches stehen nahe am Endgerät. Sie brauchen passende Portgeschwindigkeit, PoE-Klasse und einen Uplink, der die Summe der realen Last trägt. Aggregations-Switches sammeln Access-Uplinks auf 10/25G. Core-Switches verbinden Aggregationen, Gateways und Serverfarmen auf 25/100G und halten große MAC- und Route-Tabellen.

UniFi hat diese Rollen über Jahre mit Pro, Pro Max, Enterprise, Pro XG, Enterprise Campus und schließlich ECS-Core ausgebaut. Die Namenslogik ist nicht immer selbsterklärend. Entscheiden Sie entlang Portgeschwindigkeit, PoE, Uplink und Redundanz, nicht entlang des schönsten Beinamens.

6.2 Zugangsklassen

Flex und Flex Mini sind Werkzeuge für Arbeitsplätze, Vitrinen, kleine Techniknischen. Sie werden gespeist statt zu speisen. Pro und Pro Max sind die Standard-Etage: Gigabit plus ausgewählte Multi-Gig-Ports, solide PoE-Budgets, Layer-3-Fähigkeit in den größeren Modellen, 10G-Uplinks.

Enterprise-Access mit 2,5 GbE auf jedem Kupferport ist die rationale Antwort auf Wi-Fi-6/7-APs, die mehr als 1 Gbit/s nachhaltig liefern können. Pro XG und Enterprise Campus heben ausgewählte oder alle Ports auf 10 GbE und PoE++/PoE+++. Das ist Pflicht, sobald E7-Klasse-APs, PTZ-Kameras oder Arbeitsplätze mit 10G-NICs die Etage bevölkern.

Die zweite Generation der Campus-Access-Switches ergänzt hohe PoE-Leistungen, MACsec in Hardware und ein dediziertes 100G-Stacking. Stacking verkleinert die Verwaltungseinheit und kann die Ausfalldomäne vergrößern – beides muss man wollen.

6.3 Aggregation und Core

Enterprise Aggregation und Pro XG Aggregation leben von vielen schnellen Lichtwellenleitern. Neuere Firmware der Enterprise Aggregation hat MC-LAG, RSTP-Konvergenz und MAC-Lernkapazität spürbar in Richtung Campus-Kern geschoben. ECS-Core stellt 3,2 Tbit/s nichtblockierend und eine sehr große MAC-Welt in den Mittelpunkt – sinnvoll, wenn viele Aggregationen und 100G-Links zusammenlaufen.

Stacking und – auf neueren Plattformen, sofern das Datenblatt es ausweist – MC-LAG erlauben, dass Access- oder Distributionsglieder nicht an einem einzelnen Chassis kleben. Das setzt identische Planung der Portkanäle, saubere Faserwege und getestetes Failover voraus. Ein ungeprüftes Bündel ist ein Gerücht.

6.4 PoE als Entwurfsgröße

PoE ist nicht „der AP geht an“. Es ist eine Energiebilanz: Klasse pro Port, Budget des Netzteils, Reservefaktor, Kabelverlust, Startstrom, Temperatur. PoE+ (Klasse 4) trägt viele U6/U7-APs. PoE++ (Klasse 6) und PoE+++ (Klasse 8) werden bei E7, manchen Outdoor-APs, PTZ und Displays Pflicht.

Budgets von 180 W bis in den hohen dreistelligen oder – je nach Campus-Modell – noch höheren Watt-Bereich klingen nach unendlich, bis Winter, alle Kameras und eine Etage voller APs gleichzeitig booten. Planen Sie den Worst Case des gleichzeitigen Starts, nicht den Idle-Schnitt eines Datenblatts. Redundante Netzteile in Shared- oder Redundant-Mode ändern die verfügbare Leistung – das Datenblatt dazu lesen, nicht raten.

6.5 Layer-3-Switching

SVIs, statische Routen und teilweise dynamisches Routing auf [UniFi-Switches](#) entlasten das [Gateway](#). Schalten Sie L3 nur mit Adressplan, Rückrouten und einer Antwort auf die Frage „Wer loggt und filtert diesen Pfad?“. Ein L3-Shortcut um die Firewall herum ist schnell gebaut und jahrelang unsichtbar, bis er der Incident-Pfad ist.

6.6 Vergleichende Orientierung

Klasse	Downlink	Uplink-Welt	PoE-Idee	Rolle
Flex / Mini	1 / 2,5G	Uplink oft PoE -in	wird gespeist	Nische, Desk
Pro / Pro Max	1G plus Multi-Gig	10G SFP+	PoE+ / ++	Standard-Etage
Enterprise	2,5G flächig	10G SFP+	PoE+	AP-dichte Etage
Pro XG / HD	2,5 / 10G Mix	10 / 25G	PoE++ / +++	hochbitige Access
Enterprise Campus / ECS-S	10G-lastig	25G, 100G-Stack	PoE+++ , Dual-PSU	Campus-Access
Aggregation / ECS-Core	10 / 25 / 100G	25 / 100G	meist ohne Endgeräte- PoE	Distribution / Kern

Tabelle 6.1: [Switch](#)-Klassen nach Entwurfsrolle

6.7 Portprofile, Etherlighting, Diagnostik

Portprofile sind das Gedächtnis des Access-Layers: Data, Voice, AP, Kamera, Trunk, Disable. Wer Profile pflegt, kann eine Etage in Minuten tauschen. Wer jeden Port einzeln bemalt, erzeugt Kunst statt Betrieb.

Etherlighting und Front-Displays verkürzen die Zeit im Rackgang, wenn das Team die Farb- und Anzeigecodes kennt. Sie ersetzen keine Kabeldokumentation. Ein beleuchtetes [Patchkabel](#) ohne Buchungsnummer bleibt ein Rätsel mit LED.

7 Access Points

7.1 Vom U6-Enterprise zum E7

U6-Enterprise und In-Wall-Enterprise haben 6 GHz in dichte Innenräume gebracht. Die U7-Familie macht [Wi-Fi 7](#) alltagstauglich: Multi-Link, breitere Kanäle, bessere Spektrumnutzung. E7, E7 Campus und E7 Audience sind die explizite Enterprise-Stufe: mehr Streams, 10 GbE, zweite Kupferbuchse für Hochverfügbarkeit, bei Campus gerichtete Antennen und aktives RF-Filtering.

U7 Pro XG/XGS verbinden die Stärken der U7-Reihe mit 10-Gigabit-Uplink und spektralem Scan. Outdoor-Modelle brauchen IP-Schutz, korrekten Temperaturbereich und eine Antennenwahl, die Fläche statt Nachbarschaft beleuchtet.

7.2 Radios, Streams und Bänder

2,4 GHz bleibt das Band der Reichweite und der alten Scanner, zugleich das Band der Interferenzen. 5 GHz ist das Arbeitstier. 6 GHz ist das saubere Hochleistungsspektrum, solange Clients und regulatorische Leistungsgrenzen mitspielen. Ein AP ohne 6-GHz-Clients ist kein Fehleinkauf, wenn der Rest stimmt – aber dann muss man 6 GHz nicht mit 160 MHz in jede Zelle zwingen.

Räumliche Streams erhöhen Kapazität in der Zelle, nicht magisch die Reichweite durch Beton. Zehn Streams auf E7 wollen Clients, die MU-MIMO und die Kanalbreite ausnutzen, und einen Uplink, der das Ergebnis abführt.

7.3 Montageformen

Decke ist der Default für offene Büros. Wand und In-Wall bedienen Zimmerflure, Hotel und Klassenzimmer, erzeugen aber andere Keulen. Outdoor und Mesh überbrücken Höfe, dürfen aber nicht zum Ersatz für fehlende Glasfaser werden. Gerichtete Campus-Antennen sind Werkzeuge gegen Interferenz zwischen Gebäuden, nicht Dekoration.

Die zweite Ethernetbuchse der E-Serie erlaubt Link-Redundanz oder eine definierte Fallbacksituation. Sie nützt nur, wenn zwei Pfade bis in unterschiedliche [Switches](#) existieren.

7.4 Dichte und Zellplanung

Abdeckung ist die Frage „hört das Gerät noch?“. Kapazität ist die Frage „kommen 80 Laptops durch eine Prüfung?“. Enterprise-[WLAN](#) stirbt häufiger an Kapazität. Deshalb plant man Zonen: Aula, Klassenzimmer, Open Space, Lagerregal, Parkhaus. Jede Zone bekommt eine Clientannahme, eine Bandstrategie und eine AP-Zahl, nicht ein Gefühl.

Überlappung von 15 bis 25 Prozent auf 5/6 GHz ist ein gängiger Startwert für Roaming. Zu viel Überlappung plus zu hohe Sendeleistung erzeugt klebrige Clients und Co-Channel-Interferenz. Zu wenig Überlappung erzeugt Funklöcher genau dort, wo Leute telefonieren.

7.5 AP-Klassen im Überblick

Modellfamilie	Standard	Uplink	Charakter
U6 Enterprise / IW	Wi-Fi 6E	2,5G	dichte Innenräume, In-Wall mit Mini- Switch
U7 Pro / Mesh / Outdoor	Wi-Fi 7	2,5G-Klasse	Breite der Fläche, Preis-Leistung
U7 Pro XG / XGS	Wi-Fi 7	10G	höhere Zellenlast, Scan-Radio
E7	Wi-Fi 7 , 10 Streams	10G + Redundanzport	Enterprise-Innenraum
E7 Campus	Wi-Fi 7 , PRISM, gerichtet	10G + Redundanzport	Campus, Höfe, Hallen
E7 Audience	Wi-Fi 7 , sehr hohe Stream-Zahl	10G + Redundanzport	Auditorium, Event

Tabelle 7.1: Access-Point-Familien für Enterprise-Entwürfe

8 Strom, [PoE](#), [Optik](#) und Peripherie

8.1 Stromkette

Vom Hausanschluss über USV und PDU zum redundanten Netzteil des [Switches](#) reicht die Kette, die niemand sieht, bis sie fehlt. Enterprise-Racks bekommen zwei unabhängige Einspeisungen, soweit der Bau es hergibt, und eine USV-Autonomie, die einem kontrollierten Failover oder einer geordneten Abschaltung entspricht, nicht einem Hoffnungswert von „ein paar Minuten“.

USP-RPS und hot-swap-fähige Netzteile sind unterschiedliche Dinge. Nicht jedes [Gateway](#) akzeptiert dasselbe Reservestromprodukt. Die Kompatibilitätsliste gilt vor dem Warenkorb.

8.2 [Optik](#) und [DAC](#)

[SFP+](#), [SFP28](#) und [QSFP28](#) verzeihen keine Mischmasch-Romantik. [Optik](#), Distanzklasse, [BiDi](#) oder Duplex, Temperatur und Firmware gehören dokumentiert. [DAC](#) ist kurz und effizient im Rack. [AOC](#) und LR-Module tragen Gebäude und Campus. Ein billiger Dritthersteller-Stick, der nach dem nächsten Firmwarezug aussteigt, ist teurer als das Markenmodul.

[LWL](#)-Dokumentation nennt Faser, Stecker, Dämpfung, Patchfeldport. Ohne sie wird jedes [MC-LAG](#) zum Ratespiel.

8.3 Uhren, Konsole, Out-of-Band

Management-Netz, lokales Notkonto und – wo das Gerät einen Konsolen- oder dedizierten Mgmt-Port mitbringt – dieser Pfad sind der Weg, wenn die GUI nicht mehr antwortet. Ein Laptop-Image und ein dokumentiertes lokales Konto gehören in den Notfallkoffer. Out-of-Band über ein kleines separates Netz oder eine LTE-Strecke rettet Standorte, deren Produktions-WAN und -LAN gleichzeitig krank sind.

Teil III – Planung

Planung ist die preiswerteste Fehlerkorrektur, die es im Netzbau gibt. Eine Stunde an der [VLAN](#)-Matrix spart einen Samstag an der Firewall – und den Samstag wollen Sie vermutlich anders verbringen. Dieser Teil übersetzt Geschäft in Topologie: aus Anforderungen werden Netze, aus Zonen werden [VLANs](#), aus Erwartungen werden Zahlen.

9 Anforderungsanalyse

9.1 Stakeholder und Nutzungszonen

Sprechen Sie nicht zuerst über Modellnummern. Sprechen Sie über Schichten: Wer arbeitet wo, mit welchen Endgeräten, welchen Anwendungen, welcher Toleranz für Ausfall? Der Facility-Leiter kennt Kabeltrassen. Der Sicherheitsbeauftragte kennt Zonen. Der Betriebsrat kennt Gast-[WLAN](#)-Debatten. Der Produktionsleiter kennt Scanner, die nicht kleben dürfen.

Zeichnen Sie Nutzungszonen in den Grundriss: Empfang, Open Space, Meeting, Lager, Produktion, Technik, Outdoor, Parken. Jede Zone erhält Dichte, Mobilität, Sicherheitsstufe und Verfügbarkeitsklasse.

9.2 Last- und Wachstumsmodell

Ein seriöses Lastmodell nennt gleichzeitige Clients, typische Anwendung (Office, Video, Lagerbuchung, Bildgebung), Speicherspitzen und die Wachstumsrate über drei Jahre. Addieren Sie 30 Prozent Reserve auf Ports, [PoE](#) und AP-Kapazität, wenn das Gebäude nicht am Ende seiner Nutzung steht.

WAN-Last und LAN-Last sind entkoppelt. Ein Standort kann intern 40 Gbit/s zwischen Storage und Schnittstelle bewegen und trotzdem nur 2 Gbit/s ins Internet brauchen. Das [Gateway](#) nach WAN zu kaufen und den Core zu vergessen ist ein Klassiker.

9.3 Rahmenbedingungen

Normen der Verkabelung, Brandschutz in Steigschächten, Denkmalschutz bei AP-Montage, Datenschutz bei Logs, NIS2 oder branchenspezifische Auflagen verändern das Netz mehr als ein zusätzlicher [SFP](#)-Port. Schreiben Sie sie in die Präambel des Konzepts. Was dort fehlt, wird später zum Änderungsantrag.

9.4 Sollkonzept als Liefergegenstand

Ein Sollkonzept enthält: Topologie, Adress- und [VLAN](#)-Plan, [WLAN](#)-Kanalstrategie, [PoE](#)-Bilanz, HA-Skizze, Betriebsmodell der Steuerung, Backup, Monitoring, Schnittstellen zu Identität und Telefonie, Stückliste mit Reserven, offene Punkte. Ohne diesen Satz ist „wir nehmen [UniFi](#)“ keine Planung.

10 Standorttechnik und Verkabelung

10.1 Räume und Wege

Der Netzraum braucht Fläche, Kälte, zwei Strompfade, saubere Potentialgleichheit, Platz für Reserverollen und eine Tür, die nicht gleichzeitig Lager für Weihnachtsdekoration ist. Etagenverteiler folgen derselben Logik in klein. APs brauchen eine dokumentierte Position, nicht „ungefähr über der dritten Leuchte“.

Kupferlängen bleiben im Limit der Klasse. [10GBase-T](#) auf schlechter Kat. 5e ist ein Laborwitz. Für [Wi-Fi-7](#)-APs mit 10G-Uplink gehört die Strecke zur AP-Dose in die Qualitätsprüfung, nicht nur der [Switch](#)port.

10.2 Design Center und digitale Zwillinge

Das [UniFi](#) Design Center erlaubt Grundrisse, automatisierte Wandauswertung, AP-Vorschläge und erste Kanalideen. Es ist ein Kommunikationswerkzeug gegenüber Bauherren und ein Startpunkt, kein Ersatz für Messung. Wände aus Blechregalen, Personenmengen und Mikrowellen erscheinen dort nicht in ihrer echten Bosheit.

Nutzen Sie den digitalen Zwilling für Varianten: drei AP-Raster, zwei [Switch](#)-Standorte, eine Outdoor-Ergänzung. Entscheiden Sie anhand von Kosten, Montage und erwarteter Dichte, nicht anhand der buntesten Heatmap.

10.3 Zählung der Ports

Jeder AP, jede Kamera, jedes Telefon, jeder Arbeitsplatz, jedes Reserve-Patch. Plus 20 Prozent. Plus die Ports, die nach dem ersten Jahr „plötzlich“ für Digital Signage gebraucht werden. Unterportierte Etagen erzeugen Mini-[Switches](#) in Schränken – die berühmte Flex-Kaskade – und damit neue Ausfalldomänen.

11 [VLAN](#)- und Zonenkonzept

11.1 Segmentierung mit Zweck

Ein [VLAN](#) ohne Policy ist Beschriftung. Ein [VLAN](#) mit Zone und Default-Deny zwischen Vertrauensstufen ist Segmentierung. [UniFi](#) legt neue Netze gern in die Internal-Zone, in der Verkehr untereinander erlaubt ist. Wer das nicht ändert, hat farbige Subnetze in einem großen Vertrauensraum.

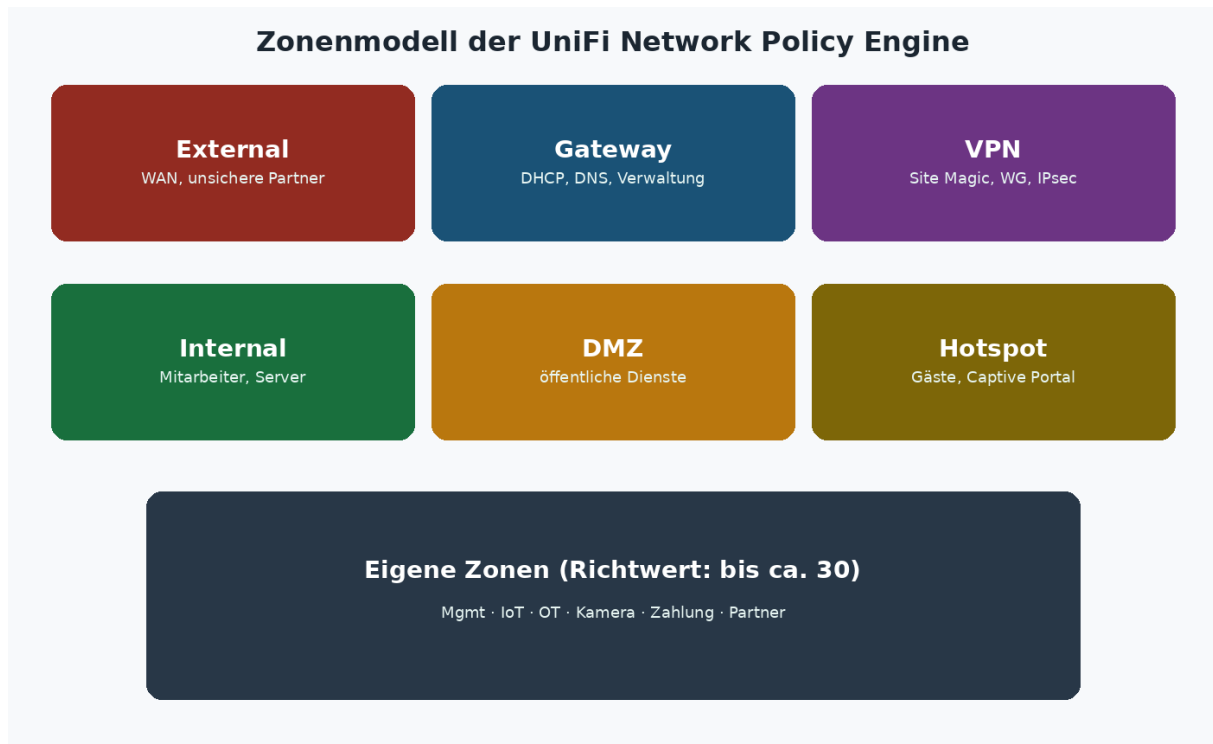


Abbildung 11.1: Built-in-Zonen und eigene Zonen

11.2 Ein belastbares Zonenbild

Built-in-Zonen decken External, Internal, [Gateway](#), VPN, Hotspot und DMZ ab. Eigene Zonen lohnen für Management, IoT, OT, Kamera, Zahlung und Partner. Die Zahl sollte klein bleiben. Eine zweistellige Zonenzahl ist selten nötig und selten wartbar.

Zwischen Management und allem anderen gilt Default-Deny, erlaubt sind Verwaltungshosts und Monitoring. Zwischen IoT und Mitarbeiter gilt Deny, plus wenige gezielte Freigaben zu Steuerungskernen. Gäste bleiben in Hotspot mit Client-Isolation. VPN startet nicht als Allerweltszutritt; die Default-Lage „VPN darf viel“ muss bewusst verengt werden.

11.3 Zuweisung

Statisch: SSID auf [VLAN](#), Portprofil auf [VLAN](#). Dynamisch: RADIUS, PPSK, Gerätetyp. Dynamik reduziert SSID-Zahl und erhöht Abhängigkeiten zur Identität. Für Gäste reicht oft Hotspot plus Voucher. Für Mitarbeiter in regulierten Netzen gehört 802.1X auf Kupfer und Funk.

11.4 IPv6

IPv6 nicht zu planen heißt, es später als Überraschung zu betreiben. Entweder bewusst abschalten, wo es keinen Nutzen hat, oder Präfixe, Firewall und DNS gleichwertig zu IPv4 führen. Halbe Aktivierung erzeugt Schattenpfade an der IPv4-Policy vorbei.

12 WLAN-Funkplanung

12.1 Survey statt Hoffnung

Predictive Survey auf dem Grundriss liefert die erste Stückliste. Pre-Design-Messung bestehender Interferenzen rettet vor Nachbar-WLANs und Industriequellen. Post-Install-Survey bestätigt, dass die gebaute Welt der geplanten gleicht. Ohne die dritte Stufe bleibt das Netz eine Behauptung.

Messgrößen: RSSI am Client, SNR, Channel Utilization, Retry-Rate, Roaming-Schwellen, reale Durchsätze je Band. Schönwetter-Speedtests am Empfangstresen sind kein Survey.

12.2 Kanal, Breite, Leistung

2,4 GHz: 20 MHz, wenig APs, niedrige Leistung, oft nur für Legacy. 5 GHz: 40 MHz als Campus-Default, 80 MHz nur bei nachgewiesenem Spektrum. 6 GHz: 80 MHz als sinnvoller Start, 160 MHz als gezielte Hochleistungszelle, nicht als Fläche. Sendeleistung so niedrig wie mit Überlappung vereinbar. Der AP soll nicht drei Etagen durchleuchten.

Auto-RF ist ein Assistent. In dichten Häusern gewinnt ein dokumentierter Plan plus periodische Revision. Spektrale Scan-Radios der XGS- und E-Klasse helfen, aber nur wenn jemand die Plots liest.

12.3 Roaming und Echtzeit

Sprache und Scanner brauchen schnelles, vorhersehbares Roaming. Das bedeutet ausreichende Überlappung, 802.11k/v/r nur nach Test mit der echten Clientflotte, und keine aggressiven Band-Steering-Experimente am Stichtag. Fast Roaming, das ein Drittel der Handhelds aus dem Netz wirft, ist kein Fortschritt.

12.4 SSID-Disziplin

Jede SSID kostet Airtime. Drei bis fünf sind ein gesundes Maximum je Funkzelle: Mitarbeiter, IoT, Gast, optional Sprache oder gebäudeinterner Scan. PPSK oder 802.1X verhindern den Wald aus Abteilungs-SSIDs. Versteckte SSIDs sind kein Sicherheitskonzept.

13 Sicherheit by Design

13.1 Fläche verkleinern

Nicht jeder Client muss jeden Server sehen. Nicht jedes VLAN braucht Internet. Nicht jedes administrative Protokoll gehört auf das Mitarbeiternetz. Die Fläche, die ein kompromittiertes Gerät ablaufen kann, ist die eigentliche Sicherheitsmetrik des LAN.

13.2 Zugang

WPA3-Enterprise wo Clients es tragen, WPA2-Enterprise als Übergang, PPSK für leichtgewichtige Trennung, Portsicherheit und 802.1X am Kupfer für regulierte Bereiche. MAC-Listen sind Hygiene gegen versehentliches Anstöpseln, keine Abwehr gegen Absicht.

13.3 Managementhärtung

GUI nur aus Managementnetz oder über VPN. SSH aus und nur bei Bedarf an. Standardpasswörter der Adoptionphase ersetzen. Firmware-Quellen vertrauen, aber Releases staffeln. API-Tokens rotieren. Logs verlassen das Gerät in ein System, das nicht dasselbe Schicksal hat wie das [Gateway](#).

14 Hochverfügbarkeit und Kapazität

14.1 [Shadow Mode](#)

[Shadow Mode](#) koppelt zwei kompatible Enterprise-[Gateways](#) mit Zustandsabgleich. Der Schatten übernimmt Adresse und Sessions, wenn das Primärgerät stirbt. Die Verkabelung ist Teil des Features: definierte Interlink-Ports, gespiegelte WAN- und LAN-Anbindungen, getesteter Failover, Monitoring auf beide Chassis.

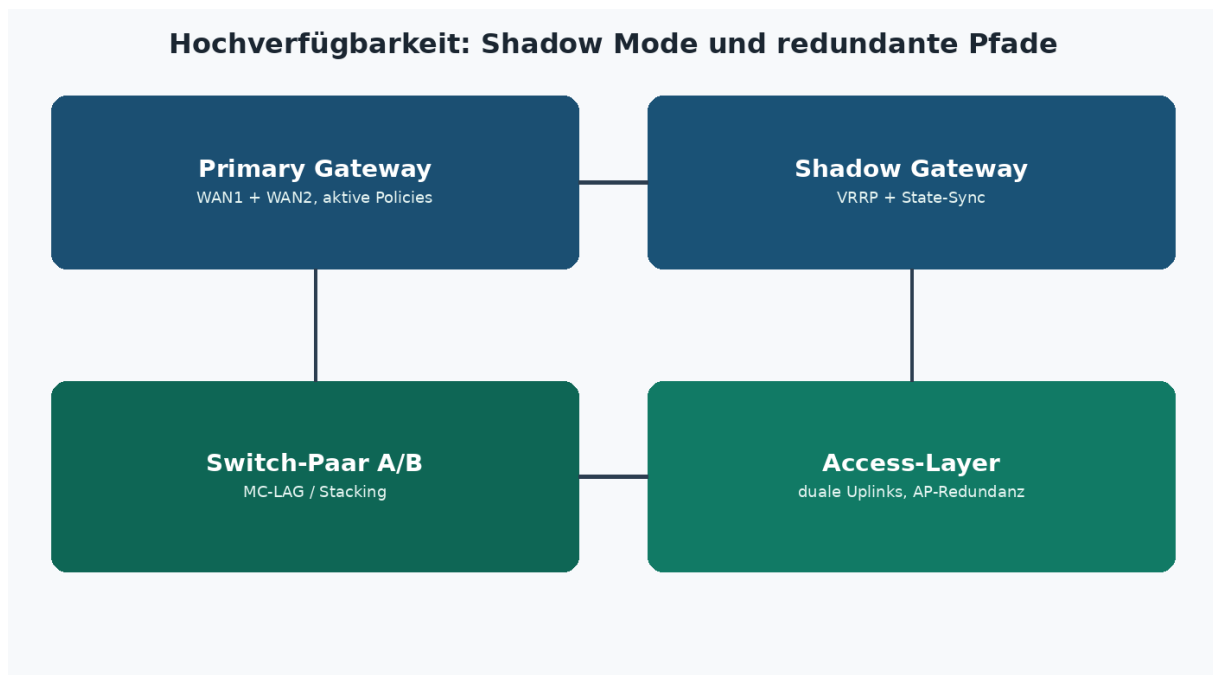


Abbildung 14.1: Redundanz aus [Gateway](#)-Paar und [Switch](#)-Pfaden

[Shadow Mode](#) rettet das [Gateway](#), nicht den einzigen [Switch](#) darunter und nicht den einzigen WAN-Provider. HA ist ein Stapel.

14.2 Switching-HA

Zwei Netzteile, zwei Uplinks, Stacking oder – wo nachgewiesen – MC-LAG nach bewusster Wahl, getrennte Trassen. Stacking vereinfacht und koppelt Schicksale. Ein Multi-Chassis-Bündel erhält unabhängiger Control Planes und verlangt mehr Disziplin. Beide Modelle wollen Probeumschaltung vor dem Go-live.

14.3 WLAN-HA

Überlappende Zellen, APs an unterschiedlichen Access-Switches, bei E-Serie duale Uplinks. Controllerausfall darf bestehende Funkzellen nicht löschen. Neue SSIDs in genau diesem Moment auszurollen ist trotzdem keine Strategie.

14.4 Kapazität als Zeitreihe

Kapazität plant man nicht nur in Gbit/s, sondern in „was passiert dienstags um zehn“. Prüfung, Schichtwechsel, Backupfenster, Livestream. Messpunkte im Ist-Netz schlagen Schätzungen. Nach dem Go-live gehören dieselben Messpunkte in das Monitoring, sonst war die Planung eine einmalige Schauspielszene.

Teil IV – Umsetzung

Umsetzung ist das Sollkonzept in Klicks, Kabeln und Tests. Die Reihenfolge ist nicht Geschmackssache: Labor und Templates zuerst, dann Kern, dann Access, dann Funk, dann Feinpolicy, dann Last- und Ausfalltest. Wer mit der Gäste-SSID beginnt, weil sie sichtbar ist, baut das Haus vom Dachfirst.

15 Labor, Adoption, Erstkonfiguration

15.1 Laboraufbau

Ein Tisch mit dem geplanten [Gateway](#), einem repräsentativen [Switch](#), einem AP, einem Clientlaptop und einem Messgerät verhindert Produktionsüberraschungen. Dort entstehen Controllerversion, Basisimage, Portprofile, [VLAN](#)-Satz und die erste Policy-Matrix. Das Laborgerät darf nicht dasselbe Backupziel und nicht dieselbe Cloud-Zwei-Faktor-Nummer haben wie später das Produktionshirn, sonst werden Tests zu Incidents.

Dokumentieren Sie Firmwarestände. Ein Labor auf Early Access und eine Produktion auf Official mischen Verhaltensweisen, die niemand mehr erklären kann.

15.2 Auspacken und Basis

Inventar: Seriennummer, MAC, Standort, Rolle, Bestellreferenz. Montage nach Drehmoment und Herstelleranleitung, nicht nach Gefühl am Trockenbaudübel. Erdung und Potentialausgleich bei Outdoor und Metalldecken. Erste Speisung über das geplante [PoE](#)-Profil, nicht über ein zufälliges Steckernetzteil aus der Schublade, wenn das Gerät [PoE](#) erwartet.

Werkseinstellung ist der ehrliche Start. Altgeräte aus einem anderen Site-Konto müssen sauber vergessen und zurückgesetzt werden. Halb adoptierte Geister erzeugen die notorische „Pending Adoption“-Schleife.

15.3 Adoption in der richtigen Reihenfolge

Zuerst die Konsole bzw. das [Cloud Gateway](#), dann der unabhängige Router falls getrennt, dann Core und Aggregation, dann Access-[Switches](#), dann APs. Jede Stufe bekommt Management-Adresse, NTP, Syslog und einen Namen nach Konvention: standort-rolle-nummer. „[Switch](#)-neu-2“ ist keine Konvention.

Informieren Sie das Team, dass Adoption das Gerät unter zentrale Herrschaft bringt. Ein [Switch](#), den jemand parallel über die Alt-IP pflegt, wird zum Split-Brain.

15.4 Templates

Bevor der zweite Standort entsteht, gibt es ein Template: Netze, SSIDs ohne standortlokale Geheimnisse, Portprofile, Syslog-Ziel, Firmware-Kanal. Standortlokales – Adressen, WAN, PSK-Ableitungen – bleibt Parameter. Wer das nicht trennt, kopiert die IP des ersten Standorts zwanzigmal.

16 Netze, DHCP und DNS

16.1 Netze anlegen

In [UniFi](#) Network entstehen virtuelle Netze mit [VLAN-ID](#), [Gateway](#)adresse, DHCP und Zone. Schalten Sie Auto-Scale aus, sobald ein Adressplan existiert. Automatisch wachsende Netze sind bequem und in VPN-Welten giftig.

Jedes Netz erhält einen Satz: Zweck, Owner, Zone, Internet ja/nein, DHCP-Pool, Reservierungen, DNS, NTP. Dieser Satz steht im Konzept und in der GUI, nicht nur in einem von beiden.

16.2 DHCP-Details

Lease-Zeiten nach Mobilität: kurz für Gäste, mittel für Laptops, lang oder Reservierung für Drucker, APs, Kameras. Option 43 oder gesonderte Controller-Discovery nur dort, wo wirklich [UniFi](#)-Geräte per DHCP finden müssen. Reservierungen dokumentieren, sonst entsteht ein Schatten-Excel.

DHCP-Guard auf Access-Ports verhindert, dass ein falsch angeschlossener SOHO-Router das Netz umerzieht. Das Feature ist langweilig und verhindert genau die Incidents, die samstags um halb vier beginnen.

16.3 DNS-Strategie

Interne Namen für Infrastruktur, getrennte Zonen für das, was Clients brauchen. Filterprofile auf dem [Gateway](#) helfen gegen Kategorien, ersetzen aber keine Resolving-Architektur. Split-Horizon nur mit Dokumentation, sonst debuggen zwei Teams zwei Wahrheiten.

17 Zone-Based Firewall

17.1 Von Listen zu Matrizen

Die Firewall denkt heute in Zonen. Interfaces – [VLAN](#), WAN, VPN – gehören zu einer Zone. Policies beschreiben erlaubten oder verbotenen Verkehr zwischen Zonen, optional verengt auf Netze, Adressen, Apps und Zeit. Die alte Welt aus LAN-In, LAN-Out und LAN-Local bleibt als mentale Last nur bei nicht migrierten Altinstallationen.

Die Matrix in der Oberfläche ist das eigentliche Arbeitsblatt. Lesen Sie zuerst Defaults: Internal zu Internal oft erlaubt, VPN zu Internal oft erlaubt, Hotspot nach innen gesperrt. Dann schreiben Sie die Abweichungen, nicht ein Paralleluniversum aus hundert Mikroregeln ohne Default.

17.2 Policy-Handwerk

Reihenfolge zählt. Spezifische Allows vor breiten Denys, wo die Engine so arbeitet; unnötige Duplikate vermeiden. Jede Policy hat einen Namen, der den Zweck trägt: „IoT-zu-Broker-8883“, nicht „Regel 12“. Jede Policy hat einen Owner.

Gateway-Zone betrifft Verkehr zum Gerät selbst: Administration, DNS, DHCP. Wer die Gateway-Zone aufmacht wie ein Wohnzimmer, öffnet die Steuerungsebene. Wer sie zumacht ohne DHCP und DNS, erstickt das Netz.

17.3 Migrationspfad

Die Umstellung auf die Policy Engine erzeugt ein Backup und übersetzt so gut wie möglich. Danach folgt ein Lesen der Matrix, kein Vertrauen auf Vollständigkeit aller Alt-Sonderfälle. Testplan: interne Kommunikation, Drucken, Telefonie, VPN-User, Gast, eine explizite Deny-Prüfung.

Häufiger Fehler

Neue VLANs bleiben in Internal und dürfen damit seitlich alles. Segmentierung beginnt mit der Zone, nicht mit der Farbe im Topologiebild.

17.4 Beispielmatrix

Quelle \ Ziel	Mgmt	Mitarbeiter	IoT	Kamera	Gast	External
Mgmt	erlaubt	admin nur	admin nur	admin nur	deny	aktualisieren
Mitarbeiter	deny	erlaubt	broker/druck	deny	deny	erlaubt gefiltert
IoT	deny	deny	begrenzt	deny	deny	vendor begrenzt
Kamera	deny	deny	deny	recorder	deny	deny
Gast	deny	deny	deny	deny	isoliert	erlaubt begrenzt
VPN	begrenzt	nach Rolle	deny	deny	deny	policy

Tabelle 17.1: Beispiel einer Zonenmatrix, die erst durch konkrete Ports lebendig wird

18 Routing, Multi-WAN und dynamisches Routing

18.1 Statische Welt

Die meisten Standorte leben mit Default-Route plus wenigen statischen Pfaden in VPN-Netze. Das ist ehrenwert. Statische Routen müssen auf beiden Seiten und in der Firewall zusammenpassen. Ein Tunnel, der steht, aber keine Route hat, ist ein Tunnel für die Galerie.

18.2 Multi-WAN

Failover braucht Tests mit gezogenem Kabel und mit totgesagtem DNS des Providers. Load-Balancing braucht Verständnis für Session-Haftung. Ein Online-Banking, das die WAN-Seite wechselt, ist kein Beweis für gute Verteilung. Policy-Routing schickt Gäste über die billige Leitung und Sprache über die gute, sofern die Messung das bestätigt.

18.3 OSPF und BGP

OSPF erscheint in SD-WAN-Fabrics zwischen [UniFi-Gateways](#), um ausgewählte Netze zu verkünden. Wenn OSPF-Hellos in der Policy sterben, bleibt der Tunnel optisch leben und die Routen fehlen. BGP bindet das [Gateway](#) an bestehende Autonome Systeme. Route-Maps, Prefix-Listen und das Verbot, Full-Table aus dem Internet in ein Filialgateway zu saugen, sind Pflichtlektüre vor dem ersten Peering.

Labortest mit zwei [Gateways](#) und einer Route-Injection sagt mehr als jedes Whitepaper. Redistribution aus statisch nach dynamisch ohne Filter ist ein Klassiker mit Folgeerscheinung in allen Standorten gleichzeitig.

19 VPN, SD-WAN und Identität

19.1 Site-to-Site

IPsec bleibt das Esperanto zu Fremdherstellern. Route-based ist der [UniFi-Default](#) und spielt mit statischen Routen oder OSPF. Policy-based verlangt identische Interessensnetze auf beiden Seiten. OpenVPN und WireGuard haben ihre Nischen. Überlappende Netze entweder auflösen oder bewusst NAT-en.

19.2 Site Magic und Fabric

SD-WAN über Site Manager orchestriert Hubs und Spokes, wirbt Netze an, setzt optional Spoke-Isolation und WAN-Failover. Ein Hub zu viel ohne Kapazitätsplanung erzeugt eine teure Sternspitze. Spoke-Isolation ist ein Sicherheitsgewinn und ein Fluch, wenn Filialen Dateien untereinander brauchen. Beides steht im Konzept.

19.3 Remote-Benutzer

Identity One-Click, WireGuard, OpenVPN, Restbestände L2TP: Jeder Client-VPN-Weg mündet in der VPN-Zone. Default-Allow nach Internal ist bequem für den ersten Test und falsch für den Dauerbetrieb. Rollen: Vollzugriff für Admins auf Mgmt, eingeschränktes Büronetz für Mitarbeitende, kein IoT, kein Kamera-[VLAN](#).

19.4 RADIUS, PPSK, Portale

802.1X gegen einen gepflegten RADIUS, ideal mit Zertifikaten, ist der Enterprise-Weg. PPSK verteilt [VLANs](#) über Passwortvarianten und passt zu Wohnheimen, Gästen mit Gruppen und leichten Mandanten. Captive Portals sind Onboarding, keine Authentisierung im Sinne eines Audits.

Zertifikatsrollen, Sperrlisten und die Frage „was passiert, wenn RADIUS tot ist“ gehören zum Entwurf. Fail-closed am Managementport kann das eigene Rettungsteam aussperren. Fail-open am Zahlungsnetz ist keine Alternative.

20 [Switching](#) im Betrieb

20.1 Portprofile anwenden

AP-Ports: tagged [VLANs](#) der SSIDs, Management untagged oder nach Standard des Entwurfs, [PoE](#) an, Storm Control maßvoll. Kamera-Ports: ein [VLAN](#), [PoE](#) der richtigen Klasse, oft Isolation zum Recorder. User-Ports: Access-[VLAN](#), optional Voice als tagged, Portsicherheit. Uplinks: Trunk mit explizitem [VLAN](#)-Satz, LACP wenn zwei oder mehr Glieder, beide Seiten identisch.

20.2 LACP, [MC-LAG](#), Stack

LACP ohne gleiche Geschwindigkeit und ohne beidseitige Konfiguration ist ein teurer Single-Link mit Extra-Schritten. [MC-LAG](#) testet man durch Abschalten eines Chassis, nicht durch Theorie. Stacks bekommen eigene Firmwaredisziplin, weil ein schlechtes Image alle Mitglieder gleichzeitig kennt.

20.3 Storms, Loops, Broadcast

Storm Control, RSTP und die Disziplin, keine unmanaged Mini-[Switches](#) in Schleifen zu setzen, halten Layer 2 erwachsen. Ein Loop zeigt sich als plötzliche Last auf allen Ports und als GUI, die nicht mehr atmet. Die Antwort ist Trennen nach Plan, nicht wildes Ziehen aller Kabel gleichzeitig ohne Markierung.

20.4 L3 auf dem [Switch](#)

SVI-Adressen aus dem Plan, keine freien Erfindungen im Rackgang. Hilfsrouten zurück zum [Gateway](#). Monitoring auf CPU des [Switch](#)-L3, nicht nur auf Portgrün. Wenn Inter-[VLAN](#) plötzlich das [Gateway](#) umgeht, muss die Firewallmatrix das wissen.

21 WLAN im Betrieb

21.1 SSID-Parameter

WPA3 wo möglich, gemischte Modi nur als Brücke. Bandsteuerung nach Test. Mindest-RSSI, ab dem ein Client nicht mehr gehalten wird, konservativ beginnen. Fast Roaming gezielt. DTIM und Datenraten so setzen, dass alte alten 1-Mbit-Ballast-Raten nicht die Zelle fressen, ohne Scanner auszusperrern.

21.2 RF-Betrieb

Nachtläufe für Kanalwechsel ankündigen. Nach Umzügen von Wänden neu messen. High-Density-Zellen bekommen mehr APs bei kleinerer Keule, nicht mehr Sendeleistung. 6-GHz-Zellen brauchen Clients; sonst bleibt das Band eine leere Versprechung mit schönem Graph.

21.3 Mesh nur mit Absicht

Mesh ist eine Überbrückung, kein Campus-Backbone. Jeder Mesh-Hop frisst Airtime und macht Diagnose schwerer. Wenn ein Graben für Glas drei Wochen dauert, darf Mesh drei Wochen leben – mit Kalenderdatum.

22 Qualität, Sprache und Medien

22.1 QoS ohne Mythos

Quality of Service rettet knappe Links und Echtzeit, nicht kaputte Funkplanung. Markierungen (DSCP) müssen vom Endgerät oder vom Netz gesetzt und auf WAN-Engpässen eingehalten werden. Eine Queue auf dem Gateway nützt nichts, wenn der AP-Uplink schon voll ist.

22.2 Sprache

VoIP-VLANs, korrekte Optionen, jitterarme Pfade, gemessenes Roaming. Talk als UniFi-App kann Teil der Konsole sein und teilt sich CPU mit Protect und Network. Auf großen Standorten gehört Sprache in eine bewusste Kapazitätsrechnung.

22.3 AV über IP

Die Enterprise-Audio/Video-Switches adressieren deterministische Medienwelten mit hohen PoE-Klassen und schnellen Uplinks. Wer Medien und Büro auf demselben Access-Switch mischt, muss Multicast, IGMP und Last trennen können. Andernfalls bekommt die Präsentation Ruckler und das ERP Timeouts.

Produktatlas in Prosa

Der Atlas wiederholt keine Marketingfolie. Er nennt Entscheidungssätze je Klasse. Modellnummern ändern sich; die Sätze bleiben als Prüffragen tauglich.

Gateways in einem Satz plus einem Nebensatz

UCG-Ultra

Filiale oder Labor mit Gigabit-WAN, wenige Dutzend Geräte, lokale Konsole, kein HA-Anspruch. Gut als Standardfiliale, schlecht als einziger Kern eines 400-Personen-Hauses.

UCG-Max

Wie Ultra, aber mit mehr Atem für Apps und Clients. Sinnvoll, wenn Protect klein mitlaufen soll und 2,5G-Welt reicht.

UCG-Fiber / UXG-Fiber

Einstieg in 10G an der Kante ohne 1-HE-Politik. Fiber-Cloud-Gateway, wenn der Standort sein Hirn behalten soll; UXG-Fiber, wenn das Hirn zentral liegt.

UDM-Pro

Klassischer Mittelstandskern mit Platte und acht Ports. Heute oft durch Pro Max ersetzt, wenn die Clientzahl wächst. Immer noch gültig, wo 3,5 Gbit/s Inspektion und moderate Gerätezahl reichen.

UDM-SE

Pro plus PoE und schnelleres Kupfer-WAN. Verlockend für Rack mit ein paar Kameras. Die Verlockung endet, wenn die acht PoE-Ports zum Gebäudeaccess werden.

UDM-Pro-Max

Default-Empfehlung vieler Zentralen unterhalb der 25G-Welt: mehr CPU, mehr Clients, zweite Platte, 5 Gbit/s-Klasse Inspektion.

UDM-Beast

Wenn 25G, viele Geräte und volle App-Palette zusammenkommen. Shadow-fähig, damit ernsthaft kernfähig.

EFG

Network-fokussierte Festung, 25G, Inspektion und große Tabellen, lokale Konsole ohne App-Vollsortiment. Für reine Netzkerne.

UXG-Enterprise

Dieselbe Datenebene wie EFG, Hirn extern. Pflichtkandidat zentral gesteuerter Enterprise-Kanten.

EF-Core

100G-Kante. Nur mit ebenbürtiger Aggregation sinnvoll. Geräte- und Benutzer Grenzen in einer anderen Liga.

UXG-Pro / Max / Lite

Unabhängige Linie nach unten. Lite für sehr kleine autonome Routerrollen, Max für Multi-Gig-Filiale, Pro für 10G ohne lokale Konsole.

UCG-Industrial

DIN-Schiene, Klima, Staub. Die Frage ist die Umgebung, nicht der Benchmark.

UDR7 / UX7

All-in-one mit Funk. In diesem Buch als Projektbüro, Showroom oder Notfallkoffer, nicht als Campus-Kern.

Switches in Entscheidungssätzen

Flex Mini / Flex

Letzter Meter, gespeist, nie der Ersatz für eine geplante Etage.

Pro 24/48 PoE

Solides Gigabit-Access, wenn APs nicht dauerhaft über 1 Gbit/s liegen.

Pro Max

Allround-Etage mit Multi-Gig-Inseln und brauchbarem Budget. Häufig die richtige Langeweile.

Enterprise 24/48 PoE

Flächig 2,5G – die rationale AP-Etage der Wi-Fi-6/7-Generation ohne 10G an jedem Platz.

Pro XG / Pro HD

10G dorthin, wo Endgeräte oder APs sie holen. PoE-Klassen lesen.

Enterprise Campus / ECS Access

Campus-Access mit hoher Leistung, Dual-PSU, Stacking-Backplane, MACsec. Für Häuser, nicht für das einzelne Sekretariat.

Aggregation / Hi-Capacity / Pro XG Aggregation

Sammelt Uplinks. Hier leben MC-LAG und 25G.

ECS-Core

Terabit-Kern. Nur mit ehrlichem Bedarf an Ports und MAC-Welt.

AV-XG

Medienwelten. Nicht stillschweigend als Büroaccess zweckentfremden, ohne Multicastkonzept.

Access Points in Entscheidungssätzen

U6-Enterprise

6E-Bestand, 2,5G, in dichten Innenräumen weiter gültig, solange Clients und Uplink passen.

U6-Enterprise-IW

Zimmerwand, Mini-[Switch](#), Hotel und Klassenzimmer. Keine Hallenlösung.

U7 Pro / Mesh / Outdoor

Fläche und Preis-Leistung. Outdoor nur mit ehrlicher Antenne und Wetter.

U7 Pro XG/XGS

Wenn die Zelle mehr als Gigabit nachhaltig zur Etage schieben soll.

E7

Enterprise-Innenraum, 10 Streams, 10G, Zweitport. Default teurer Flächen mit Anspruch.

E7 Campus

Gerichtete Energie, PRISM, Campus und Hof. Falsch in der kleinen Teeküche.

E7 Audience

Dichte auf der Tribüne und in der Aula. Überdimensioniert für 12-Personen-Teams.

Vertiefung A – Vom Lastmodell zur Stückliste

Dieses Kapitel übersetzt Zahlen in Geräte, ohne die Illusion, es gäbe die eine richtige Stückliste. Es zeigt Rechenwege, die ein Review überlebt.

A.1 Beispielrechnung Büroetage

Annahme: 48 Arbeitsplätze, 8 Meetingräume, 6 APs vom Typ U7 Pro XGS, 8 Kameras [PoE+](#), 12 Telefone [PoE](#), 4 Shared Printer. Jeder Arbeitsplatz erhält eine Dose, auch wenn heute [WLAN](#) dominiert.

Begründung: Dockingstations, Störungen, Gäste mit Adapter, morgige Umorganisation.

Ports: $48 + 8 \text{ Raumdosen} + 6 \text{ APs} + 8 \text{ Kameras} + 12 \text{ Telefone} + 4 \text{ Drucker} + 6 \text{ Reserve} = 92$. Zwei 48-Port-[Switches](#) sind ehrlicher als ein 48-Port plus Mini-Kaskaden. Uplink: sechs XGS-APs können in der Spitze mehr als 1 Gbit/s je Zelle verlangen. Ein 10G-Uplink je [Switch](#) ist Pflicht, zwei 10G als LACP sind klug, sobald die Etage Dateiserver lokal nutzt.

[PoE](#) grob: $6 \times 25 \text{ W} + 8 \times 15 \text{ W} + 12 \times 8 \text{ W} = 150 + 120 + 96 = 366 \text{ W}$ plus Reserve 30 Prozent ergibt rund 480 W. Ein [Switch](#) mit 400 W Budget reicht knapp nicht, zwei [Switches](#) mit je 400 W reichen bequem und verteilen die Ausfalldomäne. Genau so entstehen Stücklisten: nicht aus dem Bauch, aus Summen.

A.2 Beispielrechnung Funkdichte

Open Space 600 m², 80 gleichzeitige Laptops, Videokonferenz als Normalfall. 5-GHz-Zelle mit 40 MHz trägt in der Praxis oft 25 bis 40 aktive Videoclients, bevor Retries steigen – abhängig von Bau und Nachbarschaft. Vier APs sind die Untergrenze, sechs die planerische Komfortlinie inklusive Meetingräume an den Rändern.

Deckenhöhe 3 m, leichte Trennwände: Deckenmontage. Betonkern in der Mitte: AP nicht in den Kernschatten. 6 GHz zusätzlich aktiv, aber nicht als einzige Hoffnung, weil ein Teil der Flotte 6 GHz noch nicht spricht.

A.3 Beispielrechnung WAN und Inspektion

Anschluss 2 Gbit/s symmetrisch. Inspiziert werden soll der Internetverkehr plus VPN zusätzlich: Spitze mittags 1,2 Gbit/s Internet plus 300 Mbit/s VPN, also rund 1,5 Gbit/s inspiziert – mit Wachstum und späterer SSL-Inspektion auf ausgewählten Zonen eher 2 bis 2,5. Ein [Gateway](#) mit 1-Gbit/s-IDS/IPS-Zahl wäre die falsche Sparsamkeit. [UCG-Fiber](#) oder [UDM-Pro-Max](#) sind die Diskussion, [UDM-Pro](#) nur, wenn die Inspektion selektiv bleibt. Die Zahl 12,5 Gbit/s der Enterprise-Klasse wäre hier Komfort ohne Not – Geld, das in zweite Fasern zwischen den Häusern besser liegt.

Vertiefung B – Verkabelung und Aufnahme

B.1 Kupfer

Kat. 6A ist die rationale Default-Spezifikation neuer Etagen, die 2,5/5/[10GBase-T](#) sehen werden. Kat. 6 trägt 2,5 und 5 Gbit/s auf üblichen Bürolängen oft, ist aber die schlechtere Zukunft. Geschirmte Strecken brauchen durchgängig geschirmte [Patchkabel](#) und korrekte Erdung, sonst wird der Schirm zur Antenne.

Aufnahme: Drahtfolge, Länge, Map, NEXT/RL wenn das Messgerät es kann. AP-Strecken nicht vergessen – sie sind Produktionsstrecken. Farbkonvention am Patchfeld: Management, Access, AP, Kamera, Uplink. Farbe ohne Legende ist Dekoration.

B.2 Faser

OS2 für Campus und Hausstrecken, OM4 nur wo schon da und die Distanz es erlaubt. LC im Rack ist Alltag, MPO/MTP erscheint an 100G. Jede Faser hat ein Ende A und ein Ende B in der Dokumentation, nicht „irgendwo im Keller links“.

Dämpfungswerte nach dem Spleißen messen und ablegen. Ein [MC-LAG](#), dessen einer Zweig 8 dB zu viel frisst, faillt erst bei Hitze oder bei der nächsten [Optik](#)generation.

B.3 Montage von [Access Points](#)

Abstand zu Metalllampen, Sprinkler, Kabeltrassen. Nicht in die Ecke des Aufzugschachts. Nicht über das einzige Blechregal des Lagers. Outdoor: Tülle nach unten, Dichtung nicht vergessen, Erdung nach Anleitung, Surge wo die Norm und der Hersteller es verlangen.

Beschriftung am AP und in der GUI identisch. Ein AP „default-17“ über Raum 3.04 ist die Ursache für 40 Minuten Suchzeit.

Vertiefung C – Identity und Zertifikate

Netzwerkzugang ohne Identität ist ein Hotel-[WLAN](#) mit besserem Gehäuse. 802.1X mit EAP-TLS skaliert, wenn eine PKI existiert und Geräte eingeschrieben werden. PEAP-MSCHAPv2 ist der Kompromiss mit Passwort und den bekannten Schwächen. MAC-Bypass für Drucker bleibt eine Ausnahme mit Inventar.

RADIUS hochverfügbar: zwei Server, Timeouts, die den Client nicht in die Hölle schicken, und ein definiertes Verhalten bei Totalausfall. Auf Mitarbeiterfunk fail-closed nach kurzer Schonzeit ist vertretbar, wenn das Team erreichbar ist. Auf dem einzigen Management-SSID am Bauwochenende ist es unfreundlich.

Interne GUI-Zertifikate der Konsole ersetzen das Default-Zertifikat. Browserwarnungen trainieren Menschen darauf, Warnungen zu ignorieren. Genau das will man an der Verwaltungsoberfläche nicht.

Vertiefung D – Protect neben Network

Kameras sind Endgeräte mit [PoE](#), [VLAN](#) und Speicherhungers. Sie gehören nicht ins Mitarbeiternetz, nicht ins Management und nicht ins Gastnetz. Recorder-Pfade sind Ost-West mit Bitrate. 40 × 4K auf einer [UDM-SE](#)-Platte ist ein anderes Gerät als 8 mal HD zur Türkontrolle.

Die Konsole, die Network, Protect und Talk gleichzeitig stemmt, muss nach der schwersten App dimensioniert sein. [EFG](#) als reines Network-Gerät sagt implizit: Video liegt woanders. Das ist keine Schwäche, das ist eine Ansage, sie zu hören.

Vertiefung E – Änderungs- und Notfallrunbooks

E.1 Firmware eines Access-Stacks

Ankündigung, Backup, Release Notes, Labor, Fenster, ein [Switch](#) oder ein Stack zuerst, Ping auf SVI und ein AP-Client, 24 Stunden beobachten, Rest rollen. Bei [PoE](#)-Ausfall während des Zuges Batterie-Telefone und Kameras einplanen. Rollbackentscheidung vor dem Fenster treffen, nicht in Minute 70.

E.2 Gateway-Wechsel

Image der Konfiguration, Adressgleichheit, WAN-Credentials, Shadow auflösen bevor Hardware wechselt, physische Ports spiegeln, DHCP-Down-Time kommunizieren, ARP-Cache der Server im Blick, nachher Policy-Stichprobe. Ein Wechsel „wir stecken um und schauen“ ist ein Projekt, kein Runbook.

E.3 Kompromittierter Client

Port oder [WLAN](#)-Client sperren, Zonenlogs, Endpoint-Team, Kopie der Sessiondaten, nicht das ganze Internal-Netz in Panik-Deny setzen, wenn die Zone ihre Arbeit schon tut. Nacharbeit: warum war Lateral Movement möglich, welche Policy fehlte, welcher Port war zu weit.

Vertiefung F – Messprotokolle

Ein Messprotokoll nach Inbetriebnahme enthält Datum, Firmware, Messgerät, Grundriss mit Punkten, RSSI/SNR je Band, Durchsatz an festen Punkten, Roamingpfad eines Referenzclients, Uplinkauslastung bei Lasttest, [PoE](#)-Ist gegen Soll, Temperatur der [Switches](#) nach einer Stunde, Ergebnis des WAN-Ziehtests.

Ohne Protokoll gibt es kein Vorher-Nachher. Jede spätere Klage über „früher war besser“ bleibt unbeantwortbar.

Vertiefung G – Typische Anti-Patterns

- Ein großes flaches Netz, weil Firewall „kompliziert“ sei.
- Management über dasselbe [WLAN](#) wie Gäste.

- APs alle auf Kanal 36 und 80 MHz, Auto-RF aus Bequemlichkeit aus.
- [PoE](#)-Budget gleich Summe der Datenblatt-Idle-Werte.
- Ein Uplink für eine Etage voller [Wi-Fi-7](#)-Zellen.
- Early-Access-Firmware auf dem einzigen [Gateway](#).
- Site-to-Site mit identischen 192.168.1.0/24 an jedem Ort.
- VPN-Admins mit Default-Allow in alle Zonen.
- Undokumentierte L3-Shortcuts auf dem Core.
- Mesh als Dauerzustand über den Parkplatz.
- Kameras im DHCP-Pool der Mitarbeiter.
- Backup nur auf der internen SSD desselben Geräts.

Jedes dieser Muster entsteht aus Zeitdruck. Genau deshalb stehen sie auf einer Liste, die man vor dem Go-live vorliest.

Vertiefung H – Einkauf und Lebensdauer

Kaufen Sie analog zur Firmwarepolitik: aktuelle Generation für neue Flächen, eine Generation Toleranz im Bestand, keine Museumsstücke für neue Sicherheitszonen. Ersatzkauf derselben SKU, solange sie lebt, ist Betrieb. Zwangsmigration aller APs alle achtzehn Monate ist Unruhe.

Achten Sie auf regionale Frequenzvarianten der APs, auf Netzteiltypen, auf Racktiefe der großen [Gateways](#) und auf die Frage, ob das Gerät NDAA-relevante Lieferkettenanforderungen Ihres Auftraggebers erfüllen muss. Das ist keine Technikromantik, das ist Vertrag.

Vertiefung I – Zusammenarbeit mit anderen Gewerken

Elektro plant Trassen und USV, Trockenbau die Decken, Sicherheit die Kamerastandorte, IT die Policy. Wer als Netzplaner nicht in deren Terminen sitzt, findet APs über Metallsegeln und [Switches](#) ohne Kälte. Übergabepunkte schriftlich: Dose, Faser, Strom, Montagehöhe, Brandschott.

Nachunternehmer, die „mal schnell einen [Switch](#) dazwischen setzen“, sind ein Änderungsantrag, kein Handgriff. Das steht im Vertrag besser als im Nachhinein in der Störung.

Vertiefung J – Schulung des Betriebsteams

Drei Ebenen: Sehen (Dashboard, Ampeln), Handeln (Portprofil, Client blocken, AP neu starten), Verändern (Policy, Routing, Firmware). Nicht jeder Nachtbetrieb braucht die dritte Ebene. Runbooks mit Screenshots der eigenen Version schlagen allgemeine YouTube-Videos, die eine Generation zurückliegen.

Eine jährliche Notfallübung: [Gateway](#) aus, Uplink aus, RADIUS aus. Zeit stoppen. Danach die Dokumentation aktualisieren, nicht die Übung als bestanden feiern, wenn nur das Protokoll fehlt.

Praxisteil – Arbeitsweisen in der Network Application

Oberflächen ändern Menünamen zwischen Versionen. Die Arbeitsweise bleibt. Dieses Kapitel beschreibt Aufgaben so, dass sie sich in Network 9.x und Nachfolgern wiederfinden: über Einstellungen, Geräte, Policy-Tabelle, Portmanager und [WLAN](#).

Gerät benennen und verorten

Nach der Adoption erhält jedes Gerät einen Namen nach Konvention und eine Karte oder einen Raum. Die Kartenansicht ist kein Spielzeug, sie ist die Grundlage für „AP in 3.04 blinkt“. Alias, Skizze, Foto der Montage – alles, was Suchzeit frisst, gehört hierher. Wer zwanzig APs „U7-Pro“ nennt, hat Inventar, kein Netz.

Portmanager denken, nicht Port einzeln

Der Portmanager zeigt Profile und [VLAN](#)-Zugehörigkeit. Arbeiten Sie von Profilen aus. Ein neues Telefonmodell bekommt ein Profil „voice-access“, nicht 40 Einzelklicks. Wenn ein Profil falsch ist, sind alle seine Ports falsch – das ist der Preis und der Gewinn von Konsistenz.

[WLAN](#)-Gruppen

Nicht jeder AP muss jede SSID strahlen. IoT-SSID in der Produktionshalle ja, im Vorstandszimmer unnötig. Gast im Foyer ja, in der OT-Zone nein. [WLAN](#)-Gruppen und AP-Gruppen halten die Funklast und die Angriffsfläche klein.

Traffic Identification nutzen und misstrauen

Anwendungserkennung hilft bei der Frage „was füllt den WAN-Link“. Sie ist ein Hinweis, kein Gerichtsgutachten. Encrypted Client Hello, VPNs und interne Apps erscheinen als Kategorien, die nicht immer die Fachabteilung spiegeln. Policy auf App-Erkennung stützen Sie nur dort, wo Fehlklassifikation verkraftbar ist. Gehaltsabrechnung gehört auf Fünf-Tupel und Identität, nicht auf einen Anzeigenamen.

Clienthistorie

Die Clientansicht zeigt Roaming, Signal, Spektrum, Erfahrungswerte. Nutzen Sie sie zusammen mit dem goldenen Laptop. Ein einzelner schlechter Client mit veralteter Treiberversion darf nicht das Raster von dreißig APs umbauen. Umgekehrt ist eine Etage voller schlechter Erfahrung ein Rasterproblem, kein Treiberproblem.

Praxisteil – Gebäudeüberführungen

Zwei Häuser auf einem Grundstück sind der häufigste Mini-Campus. Die richtige Lösung ist [LWL](#), zwei Fasern, zwei Aggregationen oder ein [MC-LAG](#)-Paar, Management und Produktion getrennt gedacht. Die falsche Lösung ist ein Outdoor-AP im Mesh und die Hoffnung, dass der Regen höflich bleibt.

Wenn Vermieter keine neue Faser erlauben, dokumentieren Sie die Einschränkung als Risiko mit Name und Datum. Funkbrücken aus dem UISP-Portfolio können tragen, gehören aber in eine andere Betriebssoftware-Welt oder zumindest in eine ehrliche Kapazitätzahl. Eine 500-Mbit-Brücke ist kein 25G-Aggregationsersatz.

Praxisteil – Gäste und Veranstaltungen

Dauerhafte Gäste: Hotspot-Zone, Isolation, Rate-Limit, Content-Filter nach Politik, getrenntes DHCP, kurzer Lease, keine interne Namensauflösung. Veranstaltungsgäste: zusätzliche APs oder temporäre XGS/E7, festes Kanalraster, Portal-Brand, Personal am Empfang, das Voucher wirklich ausgeben kann.

Sponsoren-[WLAN](#) auf derselben Fläche braucht entweder PPSK-Gruppen oder 802.1X. Eine vierte SSID „Partner-Messe“ für drei Tage ist akzeptabel, wenn sie ein Ablaufdatum in der GUI und im Kalender hat.

Praxisteil – Drucken, Scannen, Freigaben

Drucker sind IoT mit Papier. Sie gehören in ein eigenes Netz mit Freigaben zu den Druckservern, nicht zu jedem Client. Scan-to-Folder braucht einen Zielservers, nicht das ganze Mitarbeiternetz. AirPrint und mDNS sind bequem und überschreiten [VLAN](#)-Grenzen nur mit Reflektoren, die man bewusst einschaltet. Ein globaler mDNS-Reflektor ist ein Broadcastgeschenk an alle.

Praxisteil – IPv4-Engpässe

Ein /24 mit 254 nutzbaren Adressen stirbt in Gastnetzen und in BYOD-Prüfungen. Lieber /23 für Gäste als NAT-Kunst. VPN-Pools nicht aus demselben /24 wie interne Clients. Reservierungen nicht den dynamischen Pool auffressen lassen. DHCP-Erschöpfung ist eine der wenigen Störungen, die sich Stunden vorher in Grafiken zeigt, wenn jemand hinsieht.

Praxisteil – Temperatur und Lautstärke

Enterprise-[Switches](#) mit hohen [PoE](#)-Budgets sind Heizgeräte mit Ethernet. Der Netzraum, der im Winter charmant ist, erstickt im August. Temperaturwerte in der GUI sind Frühwarnung. Lautstarke Lüfter nach Firmware sind ein Change-Review wert, bevor der Serverraum zur Klage der Nachbarabteilung wird.

Praxisteil – Recht und Log

Voucher-Daten, Clientlisten, Kameras neben APs, Deep Inspection: alles kann personenbezogen sein. Aufbewahrung, Auskunft, Löschung gehören zur Betriebsbeschreibung. Technische Möglichkeit ist keine Erlaubnis. Dieses Buch liefert keine Rechtsberatung, aber die Aufforderung, die Frage vor dem Go-live an die richtige Stelle zu geben.

Nachtfenster und Nutzerkommunikation

Ein Wartungsfenster, das nur im Netzteam bekannt ist, ist eine Störung. Kurze, ehrliche Ankündigung: was, wann, wie lange, welcher Dienst, wer ansprechbar ist. Nacharbeiten dieselbe Gruppe. Stille Firmware an APs kann harmlos sein oder alle Telefone neu verbinden. Das entscheidet nicht der Optimismus.

Wechsel der SSID-Namen

SSID-Umbenennungen sind politische Projekte. Drucker, Scanner, TV, Gebäudesteuerung und das eine Fachverfahren mit hart kodiertem Namen fallen um. Parallelbetrieb alt/neu, Frist, Inventar der nicht verwalteten Clients. Ein Buchstabe Unterschied in der SSID erzeugt zwei Funknetze und eine Woche Hotline.

Umzug einer Etage

Zuerst Dosen und Trassen, dann [Switches](#), dann APs, dann Policy-gleiche Portprofile, dann Survey. Nicht zuerst APs an provisorische [PoE](#)-Injektornester. Provisorien haben die Halbwertszeit von Jahren.

Integration einer Fremd-Firewall

[UniFi](#) darf nur Access und Funk liefern, während eine bestehende Perimeter-Firewall bleibt. Dann ist das [UniFi-Gateway](#) überflüssig oder nur WAN-unabhängig für Filialen. Klare NAT-Grenze, keine doppelten DHCP, keine zwei Default-Routes im selben Segment. Zwei Sheriffss in einem Subnetz sind ein Western.

Labornetz im Produktionscontroller

Separate Site oder separates Gerät. Labor-[VLANs](#) in der Produktionsmatrix erzeugen Laborunfälle in der Buchhaltung. Isolation gilt auch für Neugier.

Praxisteil – Qualitätssicherung vor Übergabe

Übergabe ist ein Zustand mit Unterschrift, kein Gefühl. Mindestumfang: Sollkonzept gegen Ist, Abweichungsliste, Messprotokoll, Backup-Restore-Nachweis, Benutzerrollen, Ersatzteilliste, Runbooks der fünf häufigsten Störungen, Kontakte, Firmwarestand. Der Auftraggeber bestätigt, dass Gäste, Sprache, ERP und VPN mit echten Konten geprüft wurden.

Was nicht geprüft wurde, steht explizit als offen da. Offene Punkte ohne Owner sind geschlossene Fallen.

Entwurfsmuster

Stern mit klugem Hub

Viele Filialen, zwei Hubs, identische Templates, keine überlappenden Netze, Spoke-Isolation an, zentrales Logging. Der Hub ist ein Paar, nicht ein einzelner [UDM-Pro](#) aus 2021.

Campus mit L3-Grenze am [Gateway](#)

Sicherheitsgeführt, Ost-West überschaubar, Inspektion gewollt. [Switches](#) bleiben überwiegend L2. Skaliert bis die CPU protestiert, dann ausgewählte Servernetze lokal routen.

Campus mit L3 in der Aggregation

Große Ost-West-Last, Firewall nur an Zonengrenzen nach außen und zu OT. Braucht reife Dokumentation, sonst entstehen unsichtbare Pfade.

Gebäude ohne eigenen Router

Reines L2-Gebäude an den Campus-Kern, APs und [Switches](#) adoptiert, Policy zentral. Gut für Nachbargebäude, schlecht für WAN-Autonomie.

Industriezelle

OT-[Switching](#) physisch oder zumindest L2-getrennt, keine wilden L3-Shortcuts, Sprunghost, keine direkte Internetkante aus der Steuerung.

Frequenz der Revision

Netze altern durch neue Wände, neue Nachbarn im Spektrum, neue Clientgenerationen und neue Apps. Ein jährlicher Review des Funkrasters und ein halbjährlicher Review der Zonenmatrix sind vernünftige Default-Kalender. Nach jedem größeren Umbau außer der Reihe.

Revision heißt messen und lesen, nicht nur Firmware klicken. Wer nur aktualisiert, pflegt Geräte, nicht das Netz.

Essays zur Entwurfshaltung

Die folgenden Texte verdichten Haltung. Sie wiederholen absichtlich Prinzipien aus den Hauptteilen, weil Haltung erst durch Wiederholung in Entscheidungen einsickert.

Warum Durchsatzzahlen lügen dürfen

Datenblätter nennen Zahlen, die unter Laborbedingungen, mit bestimmten Paketgrößen, oft ohne die teuerste Sicherheitsfunktion und gern auf dem schnellsten Port entstehen. Das ist kein Betrug, es ist eine Messvorschrift, die selten Ihrem Dienstag entspricht. Ihr Dienstag besteht aus gemischten Flows, Wiederholungen im Funk, TLS, Backupfenstern und einem IDS, das tiefer schaut, als es dem Durchsatz guttut.

Lesen Sie deshalb jede Zahl als Klasse, nicht als Garantie. 3,5 gegen 5 gegen 12,5 gegen 25 Gbit/s IDS/IPS sagt: Kompakt, Mittel, großes Haus, Hyperscale-Kante. Es sagt nicht, dass 12,5 Gbit/s bei eingeschalteter SSL-Inspection, tausend Policies und zwei Site-to-Site-Tunneln ankommen. Wer die Klasse ignoriert, kauft zweimal. Wer die Klasse vergöttert, kauft zu teuer.

Dieselbe Skepsis gilt bei [WLAN](#): kombinierte PHY-Raten aller Radios sind keine Clientrate. Ein Smartphone mit zwei Streams auf 80 MHz in 6 GHz erlebt eine andere Welt als das Datenblatt mit zehn Streams. Planen Sie die Welt des Smartphones und des Scanners, nicht die Welt des Datenblatts.

Control Plane als Produktionsfaktor

Die Network Application ist Produktionssoftware. Sie verdient Backup, Überwachung, Zugriffssteuerung und einen Updateprozess. Teams behandeln sie oft wie ein Heimgerät, weil die Oberfläche freundlich ist. Freundlichkeit ändert die Kritikalität nicht: ohne sie kein neuer AP, keine Policyänderung, keine forensische Sicht.

Platzieren Sie die Steuerung so, dass ein WAN-Ausfall des Internets nicht gleichzeitig die lokale Änderungsfähigkeit tötet, wenn der Standort autonom bleiben muss. [Cloud Gateways](#) glänzen genau dort. Zentrale Steuerung glänzt, wenn zwanzig Standorte dasselbe tun sollen. Mischformen brauchen explizite Aussagen, welcher Standort welches Hirn hat.

Zugriffsrechte auf die Steuerung sind privilegiert wie Domain-Admin. Geteilte Passwörter, ewige API-Tokens und fehlende Protokolle der Admin-Handlungen sind typische Auditfunde. Sie sind billiger zu vermeiden als zu erklären.

Das Management-[VLAN](#) ist kein Ersatz-[VLAN](#)

Infrastrukturgeräte brauchen ein Netz, das nicht dieselben Clients, nicht dasselbe DHCP-Chaos und nicht dieselbe Angriffsfläche hat wie das Büro. Dieses Netz ist klein, adressiert fest, administrativ eng und nur aus Sprunghost oder VPN-Rolle erreichbar.

Ein häufiger Fehler ist, das Management-[VLAN](#) zugleich als Native [VLAN](#) aller Trunks und als Default aller unkonfigurierten Ports zu verwenden. Dann landet jedes fremde Gerät genau dort, wo es nichts zu suchen hat. Park-[VLAN](#) und Management-[VLAN](#) sind Geschwister, keine Zwillinge.

APs müssen das Management erreichen, aber Clients auf dem AP dürfen es nicht. Das ist eine Frage von tagged [VLANs](#) und Firewall, nicht von Hoffnung. Prüfen Sie mit einem Client auf der Mitarbeiter-SSID, ob die GUI des [Switch](#) antwortet. Wenn ja, ist das Konzept unfertig.

Sendeleistung ist kein Reichweitenknopf

Mehr Leistung treibt den AP weiter in Nachbarzellen und hält Clients fest, die längst wechseln sollten. Weniger Leistung erzeugt Löcher, wenn das Raster nicht nachzieht. Deshalb gehört Leistung zur Zellgröße, nicht zum Impuls, „der Empfang ist schlecht“ mit einem Schieberegler zu beantworten.

Clientgeräte senden schwächer als APs. Eine Zelle, die der AP noch hörbar beleuchtet, hört den Client vielleicht nicht mehr. Asymmetrie ist eine typische Ursache für „voller Balken, keine Daten“. Survey mit echtem Client statt nur mit AP-Messung.

2,4 GHz braucht fast immer weniger Leistung als 5 und 6 GHz, weil es weiter kriecht. Gleiche Leistung auf allen Bändern ist ein Anfängerfehler mit professionellem Gehäuse.

NAT ist kein Design

NAT rettet überlappende Filialen und knappe Adressen. Es zerstört Initiierung aus der Zentrale, erschwert Logs und macht Fehlersuche zu einem Übersetzungsspiel. Wer NAT als Default jedes Spokes setzt, weil [Site Magic](#) es kann, handelt sich Einbahnstraßen ein.

Der bessere Weg bleibt der Adressplan. NAT ist die Ausnahme mit dokumentiertem Grund: Altnetz, Merger, ein Gerät, das 192.168.1.1 hart kodiert hat und das niemand anfasst, bevor das Budget stirbt.

Wenn NAT, dann zentral sichtbar, mit eindeutigen Übersetzungsbereichen je Spoke und mit der klaren Aussage, welche Seite Sitzungen beginnen darf.

Kabeltest ist Teil der Funkabnahme

[Wi-Fi-7](#)-APs mit 10G-Uplink entlarven Strecken, die Jahre lang „irgendwie Gigabit“ waren. Ein AP, der auf 1 Gbit/s verhandelt, obwohl 2,5 oder 10 geplant waren, ist oft das Kabel, der Stecker oder das Profil, nicht das Funkmodul.

Nehmen Sie die Strecke wie eine Serverstrecke auf. Markieren Sie Ports, die nicht die Sollrate halten. Tauschen Sie nicht zuerst den AP. Tauschen Sie zuerst die offensichtliche Physik.

Dasselbe gilt für [PoE](#): ein AP der bootet und in Last stirbt, spricht oft über Spannungsfall auf zu dünnen oder zu langen Strecken. Messen schlägt Raten.

Dokumentation, die man im Incident findet

Dokumentation, die in einem persönlichen Ordner liegt, existiert betrieblich nicht. Dokumentation, die nach dem letzten Praktikanten nie wieder angefasst wurde, lügt aktiv. Gute Dokumentation ist kurz, versioniert, am selben Ort wie die Tickets und nennt die lebendigen Abweichungen zuerst.

Im Incident zählt: Wo ist der Plan der Zonen, wer ist der Owner des VPN, welches Kabel ist Uplink A, welches Backup liegt wo, welches lokale Konto öffnet die Konsole, wenn die Cloud nicht antwortet. Romane über die Geschichte des Projekts helfen dann nicht.

Eine Seite „Notzugang“ plus aktuelle Matrix plus Portbelegung der Etage schlägt ein 80-Seiten-Pflichtenheft ohne Anhang der Ist-Werte.

Menschen als Teil der Datenebene

Das beste Raster stirbt an einem ungemeldeten Mini-[Switch](#) mit Loop, an einem abgezogenen Uplink zugunsten eines Beamers und an einem AP, den die Reinigung als Staubfänger neu positioniert. Betrieb enthält deshalb Begehung, nicht nur Telemetrie.

Beschriftung, verriegelte Schränke, kurze Unterweisung der Hausverwaltung und ein Foto nach der Montage reduzieren genau diese Klasse von Störungen. Sie sind unspektakulär und hochwirksam.

Das Netzteam, das nie im Gebäude war, plant an Grundrissen vorbei. Mindestens eine Begehung vor dem Sollkonzept und eine nach dem Ist gehört zum Handwerk.

Arbeitsbuch Gateway

Dieses Arbeitsbuch beschreibt die Inbetriebnahme eines standorttragenden Gateways so, wie sie in Projekten tatsächlich abläuft: nicht als Klickpfad einer einzelnen Firmware, sondern als Folge von Entscheidungen, Prüfungen und dokumentierten Abweichungen.

Vorbereitung außerhalb der GUI

Bevor das Gerät Strom sieht, existieren der Adressplan, die WAN-Parameter des Providers, die Liste der zu übernehmenden Altnetze, die Admin-Identitäten und das Backupziel. Wer diese Dinge in der GUI „nebenbei“ erfindet, erzeugt den Adressplan aus Zufall und verteidigt ihn später als Standard.

Prüfen Sie Racktiefe, Luftstrom, zweite Einspeisung und die Frage, ob das Gerät Dual-PSU oder nur kalt redundanzfähig ist. Ein Enterprise-Gateway auf einer einzelnen Steckdose unter dem Tisch ist ein logischer Widerspruch.

Beschriften Sie WAN1, WAN2, Interlink für Shadow und den ersten LAN-Uplink physisch. Die GUI-Namen helfen nicht, wenn um 3 Uhr ein Patchkabel in der Hand liegt.

Erstes Netz und nicht das letzte

Das erste IPv4-Netz ist das Management- oder das temporäre Installationsnetz. Es ist klein. Es hat feste Adressen für Gateway, Switch-SVIs und Konsole. DHCP dort nur für Installationslaptops, nicht für die Flotte.

Viele Installationen lassen das Default-Netz 192.168.1.0/24 leben, weil es bootet. Genau dieses Netz kollidiert mit jedem Heimrouter, jedem VPN-Laien und jeder Filiale ohne Plan. Ersetzen Sie es am ersten Tag, nicht nach der Migration von 200 Reservierungen.

IPv6 entweder jetzt mit Präfix und Policy oder aus. Ein stilles SLAAC auf dem WAN, das intern weitergereicht wird, erzeugt Pfade an der IPv4-Matrix vorbei.

WAN sauber terminieren

Ethernet-WAN mit oder ohne VLAN-Tag des Providers, PPPoE, statische Adresse, Dual-WAN. Jede Variante hat ein Health-Ziel, das nicht nur das Nexthop-ICMP des ISPs ist. Ein Provider-Gateway, das antwortet, während der Upstream tot ist, hält ein totes WAN künstlich am Leben.

Dokumentieren Sie die Sekundenzahl, ab der Failover greift. Zu aggressiv zerlegt Sessions bei kurzen Glitches. Zu träge lässt Sprache Minuten ins Leere laufen. Test mit gezogenem Kabel und mit geblocktem Health-Ziel, beide Male.

NAT-Ausnahmen für Server, die nach außen eindeutig erscheinen sollen, gehören in dieselbe Dokumentation wie Portfreigaben. Eine vergessene 1:1-NAT ist ein späterer Security-Finding.

Policy Engine nach dem ersten Tag

Nach dem Anlegen der Produktionsnetze wandern diese in Zonen. Internal ist der Warteraum, nicht das Ziel. Mgmt, Mitarbeiter, Server, IoT, Kamera, Gast, OT wenn nötig.

Schreiben Sie zuerst die Denys zwischen Vertrauensstufen, dann die wenigen Allows. Der umgekehrte Weg erzeugt Regelorgien, die niemand mehr erklären kann. Jedes Allow nennt Port, Ziel und fachlichen Grund.

VPN-Zone verengen, bevor der erste Reisende das Profil erhält. Der Default, der Remote-Nutzer wie interne Hosts behandelt, ist historisch verständlich und aktuell falsch.

Dienste auf dem Gateway dosieren

IDS/IPS auf den WAN-Kanten und auf ausgewählten internen Übergängen, nicht blind auf jedem Ost-West-Paket einer Backupnacht. SSL-Inspection nur mit PKI, Ausnahmen und einem Team, das Zertifikatstickets bearbeitet.

Content-Filter politisch klären. Technische Sperren ohne Kommunikationslinie erzeugen Schatten-VPNs der Fachabteilungen. Schatten-VPNs sind die Ironie jedes Filters.

Flow-Logging so einstellen, dass Platte und CPU überleben. Unendliches Detail auf der internen SSD ist kein SIEM.

Arbeitsbuch Switching

Switches verzeihen Unordnung länger als Gateways, weil Ports grün bleiben. Die Rechnung kommt als Broadcaststurm, als falsches VLAN am AP oder als PoE, das am Montagmorgen nicht reicht.

Profil vor Port

Legen Sie Profile an, bevor das Patchfeld lebendig wird: disable, park, mgmt-access, user-access, user-phone, ap-trunk, camera, uplink-trunk, server. Jedes Profil trägt VLAN-Satz, PoE, Storm Control, LLDP und die Frage, ob der Port in den Zustand „disabled“ fällt.

Uplink-Profile explizit. Ein Uplink, der das Default-User-VLAN untagged führt, mischt zwei Welten. Native VLAN der Trunks ist dokumentiert und möglichst nicht Client-Production.

Wenn ein Gerät eine Ausnahme braucht, bekommt es ein eigenes Profil mit Namen der Ausnahme, nicht einen unkommentierten Einzelzustand.

PoE im Alltag

Überwachen Sie Budget und Portfehler, nicht nur Spannung an/aus. Geräte, die zyklisch booten, erzählen von zu wenig Reserve, von schlechten Strecken oder von defekter Speisung.

Nach Firmware an PoE-Switches rechnen Sie mit einem gemeinsamen Wiedereinschalten der Speisung. USV-Telefone und medizinische Kleingeräte mögen das nicht unangekündigt.

PoE-Passthrough-Kompakt-Switches unter Schreibtischen speisen weiter, was der Etagen-Switch schon gezählt hat – oder eben nicht, wenn die Kette zu lang wird. Kettenlänge begrenzen und in der Stückliste führen.

Uplinks und Bündel

Ein Uplink ist eine Kapazitäts- und eine Ausfallfrage. Zwei Glieder auf dasselbe Chassis sind Kabelredundanz. Zwei Glieder auf zwei Chassis sind Geräteredundanz. Nur das zweite verdient den Namen HA.

LACP-Hash und Serverteams abstimmen, sonst liegen große Flows auf einem Glied und das zweite verliert sich im Leerlauf. Test durch Abziehen je eines Glieds, nicht durch Theorie des Hash.

Geschwindigkeit beidseitig gleich. 10G gegen 1G „zum Testen“ bleibt gern kleben.

Layer-3-Disziplin

SVI-Adressen aus dem Plan, OSPF oder statische Rückwege dokumentiert, Monitoring auf die Control-Plane-CPU. Eine L3-Entscheidung im Rackgang ohne Änderung am Gateway-Routing erzeugt schwarze Löcher, die nur ein Teil der Clients sieht.

Inter-VLAN am Switch bedeutet: die Firewall sieht diesen Verkehr nicht mehr. Schreiben Sie das in die Sicherheitsbeschreibung. Wenn niemand es unterschreibt, findet das Routing am Gateway statt.

Arbeitsbuch WLAN

Vom Raster zur Zelle

Das Raster entsteht auf dem Grundriss, die Zelle in der Messung. Ein AP pro 150 m² in offenen Büros ist eine Daumenregel, keine Abnahme. Wände, Höhe, Menschendichte und Material ändern alles.

Platzieren Sie APs für Clients, nicht für symmetrische Deckenbilder. Ein schönes Raster über einem Blechkanal ist ein schönes Problem.

Höhe: zu nah an Menschenköpfen in niedrigen Räumen erzeugt harte Pegel. Zu hoch in Hallen ohne gerichtete Antenne erzeugt glänzende Hallen und taube Gassen.

Kanalplan schreiben

Zeichnen Sie 2,4, 5 und 6 GHz getrennt. Wiederverwenden Sie Kanäle erst, wenn der Abstand der Zellen und die Leistung es erlauben. 80 MHz auf 5 GHz in der Stadt ist oft die Entscheidung, Nachbarn und sich selbst zu stören.

DFS-Kanäle tragen in manchen Ländern gut und überraschen mit Radar-Ausflügen. In der Nähe von Wetterradar und Häfen testen, bevor Sprache darauf lebt.

Nach dem Go-live den Plan gegen Ist-Kanäle halten. Auto-RF, der den Plan nach drei Nächten zerlegt, braucht entweder Vertrauen mit Monitoring oder eine Leine.

Clientflotte als Teil des Entwurfs

Scanner von 2016, Windows-Docks, iPhones, Android-Besucher, TV-Bars: die langsamste relevante Klasse bestimmt Mindestraten und Bandpflicht. Eine aggressive 6-GHz-only-SSID ist mutig und lässt den Scanner in der Gasse stehen.

Treiberstände der Firmenlaptops gehören ins Runbook der Arbeitsplatzverwaltung. Funkprobleme sind oft Clientprobleme mit Netzsymptomen.

BYOD in Prüfungen und Messen: eigene SSID oder PPSK, Rate-Limit, kein Zugriff auf interne Namen, kapazitiv geplant.

Roaming üben

Gehen Sie den Weg, den Menschen gehen: Flur, Tür, Treppe, Aufzugvorplatz. Messen Sie, wann der Client wechselt, nicht wann der AP noch hörbar ist.

k/v/r-Kombinationen je Hersteller der Clientchips testen. Was dem einen Laptop nützt, wirft den anderen aus der PMK-Verhandlung.

Sprache zusätzlich mit realem Gespräch. Ein Speedtest mit 400 Mbit/s sagt nichts über 20 parallele Calls.

Arbeitsbuch Sicherheit

Fläche und Identität

Segmentierung ohne Identität schützt Netze, nicht Benutzer. Identität ohne Segmentierung schützt Anmeldeversuche, nicht laterale Bewegung. Beides zusammen ist der Mindestanspruch eines Enterprise-LAN.

Servicekonten für Drucker und Scanner nicht als persönliche Konten. Zertifikate mit Laufzeit und Inventar. Widerruf, der länger dauert als das Offboarding, ist ein Offboarding ohne Netzbezug.

Gastidentität darf anonym sein, wenn die Politik das will. Sie darf nicht unbegrenzt und nicht intern berechtigt sein.

Härtung der Oberfläche

Admin-Zugänge per SSO oder zumindest MFA am UI-Konto. Lokale Notkonten im Tresor. API nur mit minimaler Rolle. SSH aus, bis er gebraucht wird.

Benachrichtigungen auf neue Admins, neue Portfreigaben, neue VPN-Peers. Die billigste Intrusion Detection ist eine Mail, die niemand erwartet.

Firmwarequelle und Zeitfenster festlegen. Ein Gerät, das sich selbstständig auf Early Access zieht, ist kein Labor, es ist Produktion ohne Einwilligung.

Protokoll und Beweis

Logs, die nur auf dem [Gateway](#) liegen, sterben mit dem [Gateway](#). Externe Ziele, Uhrensynchronisation, Aufbewahrung nach Vorgabe.

Nach Incidents zählt die Zeitreihe. Ohne sie bleibt die Erzählung. Mit ihr wird aus einem Verdacht an der Gäste-SSID ein belegbarer Pfad oder ein entlasteter AP.

Arbeitsbuch Multi-Site

Template-Disziplin

Ein Template enthält Struktur, keine standortlokalen Geheimnisse im Klartext, wo es vermeidbar ist. PSK-Ableitungen je Standort, wenn Politik das verlangt, mit einem Verfahren, das Offboarding überlebt.

Neue Filiale: Adresse aus dem Plan, WAN-Profil, Template ziehen, zwei APs, ein [Switch](#), Abnahmeliste. Keine Sonder-SSID „weil der Filialleiter das so kennt“, außer als Zeitverfall-Ausnahme.

Version des Templates führen. Sonst weiß niemand, warum Filiale 7 ein anderes Gastportal hat.

Overlay und Underlay

Underlay ist die Leitung, Overlay der Tunnel. Störungen zuerst im Underlay suchen: Licht, [VLAN](#), NAT beim Provider, MTU. Ein Overlay, das fragmentiert, trägt ERP-Tage und stirbt an einem großen Paket.

MTU und MSS bewusst. 1500 Ende-zu-Ende durch IPsec ist ein Wunsch. Klemmen oder clampen, messen mit großen Pings und echten Sessions.

Hub-Kapazität: Summe der Spokes in der Spitze, nicht im Idle. Zwei Hubs in zwei Räumen, beide können die Last allein tragen, sonst ist es kein Hub-Paar.

Störungskatalog

Kein DHCP in einem Segment

Scope voll, Relay falsch, Guard zu scharf, [Gateway](#)-Zone blockt, [Switch](#)port im Park-[VLAN](#), AP mappt SSID auf das falsche Netz. Reihenfolge: Portprofil, Client-[VLAN](#), [Gateway](#)interface, Pool, Firewall zum [Gateway](#).

Langsames WLAN bei vollem Balken

Airtime an 2,4 GHz, Co-Channel, Client hängt am schwachen Uplink, 1-Gbit-Verhandlung am XGS-AP, DFS-Ausflug, Interferer. Messen Utilization und Retries, nicht nur RSSI.

VPN steht, Dienste nicht

Route fehlt, NAT-Spoke einseitig, Firewall VPN→Internal zu eng oder zu weit und in einer anderen Ausnahme gefangen, DNS liefert interne Namen nicht, MTU. Trennen: Phase1/2 grün gegen Paketfluss.

Switch-CPU hoch

Loop, Broadcast, L3-Last, Monitoring-Polling zu dicht, defekter Port mit Errors. Erst Errors und Storm, dann Routing.

PoE-Gerät verschwindet nachts

Budgetgrenze, Temperatur, USV-Umschaltung, Zeitplan in der GUI, defektes Netzteil. Historie der Leistung, nicht nur Ist-Grün.

GUI unerreichbar, Datennetz lebt

Genau der Fall der getrennten Ebenen. Managementpfad, lokale Konto, Konsole, Out-of-Band. Nicht das Produktions-VLAN umbauen, um die GUI zu retten, bevor der Pfad klar ist.

Ein Standort driftet

Template nicht nachgezogen, lokaler Admin, alte Firmware, überlappende Netze nach einem Router-Reset. Vergleich gegen Gold-Image der Site.

Abnahmeprotokolle in Prosa

Ein Abnahmeprotokoll ist eine Erzählung mit Messwerten. Es nennt den Gegenstand, die Methode, das Soll, das Ist, die Abweichung und die Entscheidung. Die folgenden Absätze sind Vorlagen, keine heiligen Formulare.

Funkabnahme

Im Gebäude G wurden an den Punkten P1 bis P24 auf 5 GHz RSSI-Werte zwischen -58 und -67 dBm bei geschlossenen Türen gemessen. 2,4 GHz bleibt auf 20 MHz und niedriger Leistung, Utilization unter 25 Prozent außerhalb der Nachbar-SSIDs. Roaming eines Referenzlaptops vom Empfang zur Cafeteria wechselte bei -72 dBm ohne Gesprächsabbruch der Test-App.

Abweichung: Raum 1.12 unter Soll wegen Metalldecke. Maßnahme: zusätzlicher AP, Nachmessung in 14 Tagen. Unterschrift Planung und Betrieb.

Firewallabnahme

Aus Mitarbeiter-[VLAN](#) ist ERP auf tcp/443 erreichbar, Drucker-[VLAN](#) nur auf den Druckserver, Gast nicht auf interne Netze, Management nur vom Sprunghost. Expliziter Deny-Test: Client im IoT erreicht File-Share nicht. VPN-Rolle Buchhaltung erreicht DATEV-Pfad und nicht Kamera-[VLAN](#).

Abweichung: mDNS-Reflektor für zwei Meeting-Apple-TVs aktiv, befristet drei Monate. Owner Fachbereich IT-Arbeitsplatz.

WAN- und HA-Abnahme

WAN1 gezogen: Failover auf WAN2 in x Sekunden, bestehende Dateiübertragung bricht, neue Sessions stehen. WAN1 zurück: Failback nach Hold-Down ohne Dauerschwingung. Shadow-Test nur wo verbaut: Primary aus, Secondary übernimmt Default-[Gateway](#), Client behält DHCP-Lease, Verwaltungs-GUI folgt dem aktiven Gerät nach Plan.

Ohne Zahl keine Abnahme. „Hat irgendwie geklappt“ ist ein Laborkommentar.

Betreiberorganisation

Rollen

Owner Architektur entscheidet Zonen und HA. Owner Betrieb entscheidet Fenster und Firmwarekanal. Owner Sicherheit entscheidet Allows zwischen Zonen. Owner Gebäude entscheidet Montage und Zutritt. Eine Person darf mehrere Rollen tragen, nicht aber unbenannt.

Eskalation: Leitstand sieht Ampel, Betrieb handelt nach Runbook, Architektur ändert das Runbook. Wenn Leitstand die Matrix ändert, endet die Nachtschicht als neues Soll ohne Review.

Lieferanten

Provider, Elektro, Integrator, Softwarehersteller der Fachverfahren. Jeder hat eine Grenze. Der Integrator, der „das [WLAN](#) schon richten wird“, ohne Survey, liefert Hoffnung. Der Provider, dessen [VLAN](#)-Tag undokumentiert bleibt, liefert den nächsten WAN-Incident.

Verträge nennen Reaktionszeiten und was nicht enthalten ist: etwa Hebebühne, Brandschott-Nacharbeit, Ersatz nach Diebstahl. Netze scheitern an diesen Lücken häufiger als an fehlenden Streams im AP.

Weiterführende Arbeit

Nach der Lektüre folgen drei konkrete Arbeiten, die aus einem Buch ein Netz machen.

Erste Arbeit: schreiben Sie auf einer Seite das Betriebsmodell. [Cloud Gateway](#) oder [UXG](#), wo das Hirn lebt, wer Admin ist, wo das Backup liegt. Wenn die Seite nicht gelingt, ist das Projekt nicht bereit für Hardware.

Zweite Arbeit: zeichnen Sie die Zonenmatrix für den realen Standort, mit den Netzen, die es schon gibt. Legen Sie sie neben die Ist-Firewall. Die Differenz ist Ihr nächstes Fenster.

Dritte Arbeit: gehen Sie mit einem Laptop den Weg der Nutzer und notieren Sie, wo das Netz zögert. Diese Liste schlägt jede Heatmap, die nur auf dem Papier existiert.

Die Plattform wird neue Namen bekommen. Wer diese drei Arbeiten kann, bleibt unabhängig vom nächsten Beinamen einer Switch-Generation.

Standortmappe Nordwerk GmbH

Die Nordwerk GmbH beschäftigt 380 Personen in zwei Häusern mit Verbindungsbau. ERP zentral, 40 Kameras, Gäste im Empfang, Lager mit Scannern, Hybridarbeit. Diese Mappe zeigt ein Soll, kein Kundenprojekt.

Lastannahmen

Gleichzeitige Clients werktags 320, Spitze 11 Uhr 380 inklusive Gäste. Internet 1 Gbit/s mit 500 Mbit/s Backup. Interner File-Verkehr zwischen Häusern bis 4 Gbit/s in Backupfenstern. Sprache 60 parallele Sessions. Kameras 40 mal 4 Mbit/s dauerhaft gegen Recorder.

Wachstum 15 Prozent Clients in drei Jahren, ein drittes Haus angedacht. Reserve in Aggregation und Adressplan: Haus-ID 3 bleibt frei im Schema 10.3.0.0/16.

Betriebsmodell

Cloud Gateway der Beast- oder EFG-Klasse im Rechenraum Haus A, Shadow im Rechenraum Haus B. Network lokal, Protect auf eigenem Recorder, weil die Kamerazahl und Aufbewahrung die Gatewayplatte sprengen. Admins: zwei Personen Architektur, drei Betrieb, Sicherheit liest mit.

Begründung gegen reines UXG: der Standort soll bei Ausfall der Zentrale Holding weiter administrierbar bleiben. Die Holding bekommt lesenden Site-Manager-Zugang, keine Policy-Hoheit.

Adress- und VLAN-Plan Haus A/B

<u>VLAN</u>	Zweck	Haus A	Haus B	Zone
10	Mgmt	10.1.10.0/24	10.2.10.0/24	Mgmt
20	Mitarbeiter	10.1.20.0/23	10.2.20.0/23	Internal-Staff
30	Server	10.1.30.0/24	10.2.30.0/24	Internal-Server
40	IoT/Druck	10.1.40.0/24	10.2.40.0/24	IoT
50	Kamera	10.1.50.0/24	10.2.50.0/24	Kamera
60	Sprache	10.1.60.0/24	10.2.60.0/24	Internal-Staff
70	Gast	10.1.70.0/23	10.2.70.0/23	Hotspot
80	Scanner	10.1.80.0/24	10.2.80.0/24	IoT

Nordwerk: getrennte Netze je Haus gegen Loop und für klare Routen

Inter-Haus-Routing auf der Aggregation, Firewall am [Gateway](#) für Zonenübergänge nach außen, zu Gast, zu Kamera und zu IoT. Mitarbeiter A zu Server A darf die Aggregation lokal routen, sobald die CPU des [Gateways](#) in der Messung der Pilotwoche über 50 Prozent in der Lastspitze liegt. Bis dahin bleibt der strengere Pfad.

Stückliste verdichtet

Zwei Enterprise-fähige [Gateways](#) als Paar. Zwei Aggregationsglieder 25G mit [MC-LAG](#). Sechs Access-[Switches](#) 48 Port, davon vier mit flächigem 2,5G für AP-Etagen, zwei Pro Max im Lager. 28 APs: 20 U7 Pro XGS Büro, 4 E7 Cafeteria/Versammlung, 4 Outdoor/Lager gerichtet. Recorder plus 40 Kameras außerhalb dieses Buchs detailliert, aber auf denselben [PoE-Switches](#) gerechnet.

[Optik](#): 10G-SR innerhalb der Häuser, 25G zwischen Aggregationen und Kern, zwei getrennte Gräben im Verbindungsbau. USV 20 Minuten bei halber [PoE](#)-Last plus Zeit für Dieselstart, den es am Standort nicht gibt – also 20 Minuten geordnetes Herunterfahren der Recorder.

[WLAN-Raster](#)

Bürodeckenraster 12 bis 14 Meter, 5 GHz 40 MHz, 6 GHz 80 MHz, 2,4 GHz nur Scanner-SSID im Lager und ein schwaches Füllnetz im Keller. Cafeteria E7 mit reduzierter Leistung gegen die Bürofront. Lager Gassenmessung Pflicht, nicht nur Deckenfoto.

SSID: NW-Intern (802.1X), NW-IoT (PPSK), NW-Gast (Portal), NW-Scan (WPA3-Personal, nur Lager-APs). Kein Management im Funk außer einem Not-SSID-Profil, das default aus ist.

Risiken

Der Verbindungsbau gehört dem Vermieter. Eine Faser ist zugesagt, die zweite nur „wenn möglich“. Solange die zweite fehlt, bleibt [MC-LAG](#) ein Wunsch und das Shadow-[Gateway](#) in Haus B ein kaltes Hirn hinter einem Single-Path. Das steht im Risikoregister, nicht in der Hochglanzfolie.

Standortmappe Filialkette Quellgold

Quellgold betreibt 22 Verkaufsstellen und ein kleines Lager. Jede Filiale hat acht bis zwölf Clients, zwei Kassen, vier Kameras, ein Gast-[WLAN](#) mit Zeitlimit, LTE-Backup an acht Autobahnstandorten.

Standardfiliale

[UXG](#)-Max oder [UCG](#)-Fiber je nach Anschluss, gesteuert zentral. [Switch](#) Pro Max 16 [PoE](#), zwei U7 Pro, eine Outdoor-Einheit an Filialen mit Parkplatz-Gast. [VLAN](#)-Satz identisch, Adressen 10.F.0.0/24 je Funktion mit F als Filialnummer wäre zu grob – besser 10.60.F.0/24 Mitarbeiter, 10.61.F.0/24 Kasse, 10.62.F.0/24 Kamera, 10.63.F.0/24 Gast.

Kasse darf nicht ins Gastnetz, Gast nicht zur Kasse, Kamera nur zum zentralen Recorder über Overlay. Internet der Kasse über den Hub, nicht direkt, sobald das Kassensystem das hergibt. Wo es das nicht hergibt, dokumentierte Ausnahme mit Anbieterbestätigung.

Hub

Zwei Hubs in zwei Rechenräumen der Zentrale, [UXG-Enterprise](#) oder Beast-Klasse je nach Inspektion. [Site Magic](#), Spoke-Isolation an, NAT-Spoke aus, weil der Adressplan nicht überlappt. Wer eine Altfiliale mit 192.168.1.0/24 noch schleppt, bekommt NAT und einen Migrationstermin.

Betrieb

Filialleitung darf den AP nicht versetzen. Integrator hat ein 24-Stunden-Ersatz-AP-Depot in drei Regionen. Firmware zentral, Freeze in Aktionswochen. Typische Störung: der Mini-[Switch](#) der Kasseninsel, den ein Dienstleister setzte. Vertraglich untersagt, im Runbook trotzdem als erste Frage.

Standortmappe Forum am Strom

Veranstaltungshaus mit 1.200 Plätzen, Presse, Ticketing, getrennte Medienproduktion. Drei Betriebszustände: dunkel, Probe, Show.

Zwei Netze in einem Haus

Bürobetrieb 40 Personen ganzjährig: Pro-Max-Etage, U7 Pro, [Cloud Gateway](#) mittel. Showbetrieb: zusätzliche E7-Audience- oder dichte E7-Zellen, 10G bis in die Halle, AV-[Switching](#) separat, Gast-SSID nur in Showzustand aktiv mit Rate-Limit.

Der Fehler ist, Showlast auf Büro-Uplinks zu legen. Deshalb physisch oder zumindest portseitig getrennte Aggregationen für Medien und für Office/Gast. Multicast der Medien bleibt in der AV-Welt.

Show-Runbook

T minus einem Tag: Kanalplan einfrieren, Auto-RF aus, Firmware-Freeze, Portal testen, WAN-Failover testen, [PoE](#)-Budget gegen alle Show-APs. T minus einer Stunde: Scan der Nachbarschaft, störende eigene Test-SSIDs aus. T plus einer Stunde: Utilisation sichern als Beweis für das nächste Design.

Presse-[WLAN](#) ist nicht Gast und nicht intern. PPSK oder 802.1X der akkreditierten Geräte, Ablauf nach Veranstaltung.

Standortmappe Klinik-Ambula (nicht-kritische Flächen)

Dieses Beispiel behandelt explizit keine medizinproduktkritische Echtzeit an Beatmung oder Saal. Es behandelt Verwaltung, Ambulanzwarte, Gäste und ein getrenntes Techniknetz. Medizinische Netze bleiben außerhalb von [UniFi](#)-Default-Annahmen, solange der Betreiber keine eigene Freigabe hat.

Segmentierung ist hier nicht Komfort. Verwaltung, Patienten-[WLAN](#), Gebäudetechnik, Kamera an öffentlichen Gängen. Keine laterale Bewegung. 802.1X an Verwaltungsdosen. Gäste-Portal mit starkem Filter. Techniknetz ohne Internet, Sprunghost mit Aufzeichnung.

Verfügbarkeit: Shadow an der Kante der Verwaltung, USV nach Hausstandard, APs nicht über Patientendurchgängen ohne Abstimmung Hygiene und Brandschutz. Dokumentation der Abweichungen für den Informationssicherheitsbeauftragten.

Wer dieses Muster auf Saal- oder Diagnosenetze überträgt, ohne die zuständigen Gruppen, handelt fahrlässig. Das Buch verweigert an dieser Stelle bewusst Stücklisten.

Lehrbriefe an das Betriebsteam

Montag: Lesen statt Klicken

Beginnen Sie die Woche mit Alarmen, Backupalter, WAN-Health, [PoE](#)-Headroom und der Frage, welche Änderung letzte Woche ohne Ticket blieb. Erst danach neue Wünsche der Fachbereiche. Ein Netz, das nur noch Wünsche erfüllt und nie liest, driftet.

Dienstag: Eine Abweichung töten

Suchen Sie eine Ausnahme ohne Datum: eine SSID, ein Allow Any, ein Mini-[Switch](#), ein Early-Access-Gerät. Entweder befristen und ownern oder entfernen. Eine pro Woche reicht, um in einem Jahr ein anderes Netz zu haben.

Mittwoch: Messen

Ein Punkt im Gebäude, denselben Client, denselben Test. Werte in die Zeitreihe. Ohne Zeitreihe ist jede Beschwerde wahr.

Donnerstag: Wiederherstellung anfassen

Restore im Labor, Konto im Tresor prüfen, Shadow-Dokument lesen. Nicht den Produktionskern stürzen, aber die Handgriffe nicht zum ersten Mal im Incident üben.

Freitag: Freeze ehrlich machen

Was nächste Woche Aktions-, Prüfungs- oder Abrechnungszeit ist, bekommt Freeze. Was trotzdem muss, bekommt zwei Personen und ein Rollback.

Kommentar zur Namensflut

Zwischen 2024 und 2026 hat [UniFi Gateways](#) und [Switches](#) in einer Dichte umbenannt und ergänzt, die Inventarlisten älterer Bücher entwertet. Deshalb betont dieses Handbuch Klassen und Prüffragen. Wenn Sie 2028 einen ECS-Nachfolger kaufen, bleiben die Fragen: Welchen inspizierten Durchsatz brauche ich wirklich, welche [PoE](#)-Klasse, welche Ausfalldomäne, wo liegt das Hirn?

Schreiben Sie interne Aliase. „Etagen-Access 2,5G [PoE+](#) 48“ überlebt SKU-Wechsel. „Der blaue 48er“ überlebt sie nicht.

Verfahrenskatalog

Jedes Verfahren ist absichtlich kurz. Es eignet sich als Karteikarte im Betrieb und als Prüfung, ob das Sollkonzept tragfähig ist. Wo ein Verfahren nicht ausführbar ist, fehlt meist Inventar, Recht oder ein Werkzeug – nicht ein weiterer Menüpunkt.

Verfahren 1: Gerät zurücksetzen ohne Inventarverlust

Notieren Sie Seriennummer, Rolle, Portprofil und die Site. Reset nach Hersteller, neu adoptieren, Namen sofort setzen. Ein Reset ohne Zettel erzeugt Geister.

Verfahren 2: Pending Adoption auflösen

Gerät wirklich im Layer-2- oder inform-Pfad? Altes Konto gelöscht? Inform-URL korrekt? Nicht drei Konsolen gleichzeitig füttern.

Verfahren 3: Native VLAN an Trunks prüfen

Beide Seiten lesen, nicht eine. Testdose mit untagged Frame und schauen, in welchem Netz der Client landet. Überraschungen dort sind Produktionsstörungen morgen.

Verfahren 4: Park-VLAN einführen

Unbenutzte Ports dorthin oder administrativ down. DHCP aus. Beschreibung „park“. Nach Umzug der Dose zurück ins Profil.

Verfahren 5: AP-Uplinkrate kontrollieren

GUI-Portgeschwindigkeit gegen Soll. Bei 1G statt 2,5/10G Kabel, Profil, Autoneg, Patchfeld. Erst dann den AP tauschen.

Verfahren 6: PoE-Klasse am Port begrenzen

Nicht jeder Port braucht Klasse 8. Begrenzen reduziert Schaden durch Fehlstecken und macht Budgets planbar.

Verfahren 7: Storm Control staffeln

Access strenger als Uplink. Zu streng zerlegt legitime Bursts. Werte dokumentieren, nicht copy-paste von Foren.

Verfahren 8: RSTP-Root festlegen

Aggregation oder Core als Root, nicht ein Access im Keller. Prioritäten setzen, nach Änderung Topologie prüfen.

Verfahren 9: LACP beidseitig

Erst Kabel, dann Bündel konfigurieren oder bewusst Single-Aktiv lassen bis beide Seiten stehen. Vermeidet Teilzustände.

Verfahren 10: MC-LAG üben

Ein Chassis aus, Zeit messen, Client-Sessions beobachten, Logs sichern. Ohne Übung ist MC-LAG Folklore.

Verfahren 11: DHCP-Guard aktivieren

Auf Access-Ports an, auf bekannten Relays und Gateways nicht. Test mit einem SOHO-Router, der nicht gewinnen darf.

Verfahren 12: Lease-Zeiten anpassen

Gäste kurz, Drucker lang. Nach Events Pools prüfen. Erschöpfung ist sichtbar, wenn jemand die Grafik öffnet.

Verfahren 13: Reservierungen exportieren

Nicht nur in der GUI. Monatlicher Export ins Dokumentationssystem. GUI-Restore allein ist zu wenig, wenn Menschen suchen.

Verfahren 14: DNS-Filter ausnehmen

Fachverfahren mit hartem Allow. Sonst entstehen Schattenresolver auf den Clients und die Policy lügt.

Verfahren 15: NTP prüfen

Zeit auf Gateway, Switch, AP, Recorder, RADIUS. Abweichung über Sekunden ist ein Incident der Zertifikate.

Verfahren 16: Gateway-Zone schließen

Admin nur aus Mgmt und VPN-Admin-Rolle. DHCP/DNS der eigenen Netze erlauben. Rest deny.

Verfahren 17: VPN-Default verengen

Neue Policy VPN zu internen Zonen auf das Nötige. Test mit einem Nicht-Admin-Konto.

Verfahren 18: Site-to-Site-MTU

Große Pings, DF-Bit, MSS-Clamp. Datei größer als 10 MB durch den Tunnel. Erst dann „VPN fertig“.

Verfahren 19: Overlapping Subnets finden

Alle Sites in eine Tabelle. Duplikate markieren. NAT nur mit Termin zur Auflösung.

Verfahren 20: Health-Check-Ziele

Nicht ausschließlich öffentliche Resolver. Mindestens ein geschäftskritischer Endpunkt. Timeout und Schwelle notieren.

Verfahren 21: WAN-Failover kommunizieren

Kurze Mail an Betrieb: wir ziehen WAN1 um 21:10. Danach Messergebnis. Stille Tests erzeugen stille Legenden.

Verfahren 22: IDS in den Monitor

Erst beobachten, dann blocken. False Positives der ersten Woche sind Unterricht, nicht Beweis für nutzlose Systeme.

Verfahren 23: SSL-Inspection-Ausnahmen

Banking, Gesundheitskarten-Software, Update-Kanäle der Hersteller. Liste ownern.

Verfahren 24: Admin-MFA erzwingen

UI-Konto ohne zweiten Faktor ist ein geteiltes Geheimnis in Wartestellung.

Verfahren 25: Lokales Notkonto testen

Vierteljährlich an der Konsole. Passwortrotation nach Test. Nicht dasselbe Passwort wie das Cloud-Konto.

Verfahren 26: API-Token rotieren

Inventar der Automationen. Alte Token löschen. Rechte minimal.

Verfahren 27: Syslog-Ziel prüfen

Logger empfängt noch? Zertifikat? Füllstand? Ein Ziel, das seit dem Umzug tot ist, ist Selbsttäuschung.

Verfahren 28: SNMP nur intern

Community oder User nicht aus dem Internet. Read-only außer dort, wo Werkzeuge schreiben müssen – meist nirgends.

Verfahren 29: Karte und Blinken

Neue Techniker üben Locate. Ein AP, den niemand blinken lassen kann, ist nicht inventarisiert.

Verfahren 30: SSID-Gruppe pflegen

IoT aus den Vorstandsbüros, Gast aus der OT, Scan aus dem Empfang. Gruppen sind Policy.

Verfahren 31: Mindest-RSSI vorsichtig

Zu hoch wirft Clients in Löcher. Zu niedrig klebt. In 3-dB-Schritten und mit Gehprobe.

Verfahren 32: 2,4-GHz-Zellen reduzieren

Lieber wenige starke Zwecke als flächige Brühe. Scanner-SSID gezielt.

Verfahren 33: 6-GHz-Pflicht nur mit Flotte

Inventar der Clients. Sonst bleibt das Band leer und die Enttäuschung groß.

Verfahren 34: Mesh befristen

Ticket mit Enddatum. Woche vor Ablauf Glas oder Verlängerung mit neuer Begründung.

Verfahren 35: Outdoor-Erdung

Nach Montage Foto der Erdung. Surge nach Spezifikation. Nicht „machen wir später“.

Verfahren 36: In-Wall nicht in Hallen

IW ist Zimmer. Halle braucht Decke oder gerichtet. Falsche Bauform erzeugt Tickets, keine Deckung.

Verfahren 37: Zweitport des E7 nutzen oder absichern

Wenn ungenutzt: dokumentiert unbeschaltet. Wenn genutzt: zweiter [Switch](#), sonst ist es nur ein Kabel mehr am selben Schicksal.

Verfahren 38: Kameras nicht per WLAN ohne Grund

[PoE](#)-Kabel ist der Default. [WLAN](#)-Kameras sind Ausnahmen mit eigener Dichteplanung.

Verfahren 39: Recorder-Pfad messen

Bitrate-Summe gegen Uplink. Nacht mit allen Streams. Nicht die Hochglanzzahl einer Kamera mal Wunschdenken.

Verfahren 40: USV-Autonomie nachrechnen

PoE ist Heizlast und Watt. Batterieangaben ohne PoE-Last sind Märchen.

Verfahren 41: Temperaturtrend

Alert bei Anstieg, nicht erst bei Abschaltung. Filter wechseln ist Netzbetrieb.

Verfahren 42: Optik inventarisieren

Typ, Reichweite, Slot, Gegenstelle. Ersatz im selben Fach, nicht „irgendwo im Karton 10G“.

Verfahren 43: DAC nicht über Türen

Kurze Twinax bleiben im Rack. Türen und DAC erzeugen Wartungsrituale und Ausfälle.

Verfahren 44: Patchfeldfoto nach Änderung

Ein Foto mit Datum schlägt ein halbes Memory. Ablage im Ticket.

Verfahren 45: Farbcode erklären

Legende am Schrank. Neue Farbe nur mit Update der Legende.

Verfahren 46: Hebebühne vorplanen

AP-Tausch in 8 m Höhe ist kein Ticket für zwischen zwei Meetings.

Verfahren 47: Brandschott nicht brechen

Neue Faser durch Schott nur mit zugelassenem System. Sonst stoppt der Brandschutz das Netzprojekt.

Verfahren 48: Abnahme mit echtem Konto

Nicht nur Admin-Laptop. Ein Lehrer-, Kassen-, Gast- und Scannerkonto.

Verfahren 49: Freeze-Kalender

Prüfungen, Inventur, Weihnachtsgeschäft, Abschlüsse. Sichtbar für alle, die Firmware wollen.

Verfahren 50: Änderungsfenster klein

Ein Systemtyp je Fenster. Gateway und alle APs gleichzeitig ist Mut, kein Prozess.

Verfahren 51: Rollbackbedingung vorab

Wenn Fehlerrate x oder Dienst y tot, zurück. In Minute 70 entscheidet Angst, vorher Verstand.

Verfahren 52: Gold-Laptop pflegen

Bekannt guter Client, aktuelles Image, Inventarnummer. Ohne ihn werden Debatten weltanschaulich.

Verfahren 53: Nachbar-SSID-Liste

Jährlich: wer strahlt uns zu. Gespräche mit Nachbarn sind RF-Arbeit.

Verfahren 54: Power-Schedule prüfen

Vergessene Nachtabstaltung an APs in 24/7-Bereichen. Kalender vs. Betrieb.

Verfahren 55: Gastportal-Text rechtlich

AGB und Logging-Hinweis nicht aus einem fremden Hotel kopieren. Fachstelle lesen lassen.

Verfahren 56: Voucher-Kontingent

Wer darf wie viele erzeugen. Missbrauch ist ein Intranet mit Gäste-QoS.

Verfahren 57: PPSK-Inventar

Welches Passwort welches VLAN. Offboarding entfernt das Passwort, nicht nur den Menschen.

Verfahren 58: RADIUS-Timeout

Zu kurz erzeugt Flapping, zu lang langsame Logins. Mit der echten Serverlatenz messen.

Verfahren 59: Zertifikatsablauf kalendern

RADIUS, GUI, Captive, VPN. 30 Tage vorher Ticket, nicht am Montagmorgen der Ablaufs.

Verfahren 60: Schatten-IT-Switch finden

MAC-Tabelle nach unbekannten Chassis durchsuchen. LLDP hilft. Ansprache vor Konfiszierung, außer bei Loops.

Übungen und Lösungen

Die Übungen eignen sich für interne Schulungen. Schreiben Sie die Antwort zuerst selbst. Die Lösung ist eine von mehreren tragfähigen, nicht die einzige.

Übung 1: Adresskollision

Aufgabe. Zwei Filialen nutzen 192.168.1.0/24 und sollen Spoke-to-Spoke ohne NAT. Warum scheitert das, und was ist der kleinste saubere Schritt?

Lösung. Identische Präfixe sind im Overlay nicht unterscheidbar. Der kleinste saubere Schritt ist die Umnummerierung einer Filiale nach Plan, nicht NAT auf beiden Seiten. NAT wäre ein Parallelpfad mit Einbahnstraße.

Übung 2: Shadow oder kalt

Aufgabe. Eine Kanzlei mit 25 Personen, ein Gebäude, ERP in der Cloud. Braucht sie [Shadow Mode](#)?

Lösung. Wirtschaftlich meist nein. Ein gepflegtes Ersatzgerät und ein Wiederanlauf unter einer Stunde tragen das Risiko. Shadow lohnt, wenn jede Viertelstunde Honorare und Fristen zerstört und kein Ausweichbüro existiert.

Übung 3: Uplink rechnen

Aufgabe. Zwölf U7 Pro XGS an einem [Switch](#), ein 1G-Uplink. Welche Zahl fehlt, und welche Entscheidung folgt?

Lösung. Es fehlt die angenommene gleichzeitige Zellenlast. Schon bei 200 Mbit/s je AP in einer Prüfung ist der Uplink die Bremse. Entscheidung: 10G-Uplink, besser zwei, und APs auf zwei [Switches](#) verteilen.

Übung 4: Zone Internal

Aufgabe. Alle [VLANs](#) liegen in Internal und „dürfen alles“. Ist das segmentiert?

Lösung. Nein. Farben ohne Deny zwischen Vertrauensstufen sind Beschriftung. Mindestens Gast, IoT, Kamera und Mgmt aus Internal heraus und Defaults verengen.

Übung 5: 2,4 GHz 40 MHz

Aufgabe. Warum gilt das als Fehler in Etagennetzen?

Lösung. Nur drei nicht überlappende 20-MHz-Kanäle existieren sinnvoll. 40 MHz frisst Nachbarn und sich selbst. Legacy-Geräte und Störer machen das Band ohnehin eng.

Übung 6: EFG plus Protect

Aufgabe. Warum ist das oft die falsche Kombination?

Lösung. EFG ist als Network-Festung gedacht, nicht als App-Vollkonsole. Video gehört auf Recorder oder eine Konsole mit Protect-Kapazität. Sonst kauft man die falsche Stärke.

Übung 7: Mesh über den Hof

Aufgabe. Welche Frage an den Bauherren ist die richtige?

Lösung. Wann liegt die Faser? Mesh ist Überbrückung mit Datum. Ohne Datum wird aus einer Brücke ein unsichtbarer Backbone mit Wetterabhängigkeit.

Übung 8: DHCP im VPN

Aufgabe. Remote-Nutzer bekommen Adressen aus 10.10.20.0/24, dem Mitarbeiter-LAN. Was knirscht?

Lösung. Adressgleichheit erschwert Logs, Policies und mögliche Konflikte mit lokalen Leases. VPN-Pools gehören in eigene Präfixe in der VPN-Zone.

Übung 9: L3-Shortcut

Aufgabe. Der Core routet VLAN 20 zu 30 lokal. Die Matrix am Gateway verbietet 20 zu 30. Wer gewinnt?

Lösung. Der Pfad, den der Client nimmt. Default-Gateway auf dem Core bedeutet, die Matrix sieht den Verkehr nicht. Entweder Routing zurück zum Gateway oder Policy auf dem Core – beides schriftlich.

Übung 10: PoE-Winter

Aufgabe. Im Januar booten Outdoor-APs und PTZ gleichzeitig nach einem Stromausfall. Was kippt?

Lösung. Das Budget und der Startstrom. Worst Case rechnen, nicht Idle. Reservenetzeile im Shared-Mode nicht mit Redundant-Mode verwechseln.

Übung 11: Auto-RF in der Aula

Aufgabe. Warum einfrieren?

Lösung. Kanalwechsel in der Show erzeugen kurze Brüche und unkontrollierte Nachbarschaft. Vorher messen, dann festziehen.

Übung 12: Gäste-DNS

Aufgabe. Gäste nutzen den internen Resolver mit allen Zonen. Risiko?

Lösung. Namensoffenbarung interner Systeme. Gäste bekommen eigene Resolver-Sicht oder nur öffentliche Auflösung.

Übung 13: UXG plus Cloud Key

Aufgabe. Welches Hirn adoptiert das UXG, und was darf nicht parallel passieren?

Lösung. Genau eine Network Application. Zwei Hirne erzeugen Adoptionskriege. Cloud Gateway am selben Standort zusätzlich ist ein zweites, unverträgliches Modell.

Übung 14: SSID-Wald Schule

Aufgabe. Acht SSIDs je AP. Symptom?

Lösung. Airtime-Overhead, schlechte Sichtbarkeit, mehr Fehlverbindungen. Zusammenlegen über 802.1X oder PPSK.

Übung 15: Health 8.8.8.8

Aufgabe. Warum reicht das nicht?

Lösung. Der Weg zu einem öffentlichen Resolver kann leben, während das ERP tot ist. Health muss das Geschäft sehen.

Übung 16: In-Wall in der Halle

Aufgabe. Warum scheitert das Muster?

Lösung. Keule, Höhe, Dichte und Montagewinkel sind für Zimmer gebaut. Die Halle braucht andere Antennen und andere Montage.

Übung 17: Backup nur intern

Aufgabe. Gateway sichert auf die eigene SSD. Welches Ereignis tötet beides?

Lösung. Platten-, Gehäuse-, Brand- oder Ransomware-Ereignis auf genau diesem Gerät. Zweites Ziel offline oder außen.

Übung 18: Early Access Produktion

Aufgabe. Nennen Sie ein Gegenargument, das nicht „Angst“ heißt.

Lösung. Fehlende Rollbackübung, unklare Release Notes zu Policy-Defaults, fehlendes Labor. Risiko ohne Messpunkt.

Übung 19: NAT-Spoke und zentrale Initiative

Aufgabe. Zentrale will Datei in die Filiale schieben. Warum klappt es nicht?

Lösung. Source-NAT am Spoke macht die Filiale nicht eindeutig erreichbar; Sessions startet der Spoke. Anderen Adressplan oder explizite Gegenrichtung bauen.

Übung 20: Gold-Laptop fehlt

Aufgabe. Drei Nutzer schwören, das WLAN sei tot. Was zuerst?

Lösung. Reproduzieren mit bekannt gutem Client am selben Ort. Danach Raster oder Treiber. Ohne Trennung arbeitet man an beiden gleichzeitig und an keinem richtig.

Merkblätter für den Alltag

Die Merkblätter sind bewusst klein. Sie hängen einzeln am Schrank oder im Wiki. Zusammen bilden sie ein Betriebshandbuch, das die großen Kapitel in Handgriffe zerlegt.

Merkblatt 1: Inform-URL und Adoptionpfad

Geräte müssen die Network Application erreichen, bevor sie sinnvoll arbeiten. In Cloud-[Gateway](#)-Welten ist das lokal. In [UXG](#)-Welten ist es die zentrale App über WAN oder Overlay.

Prüfen Sie DNS, Firewall zur Steuerung, Zertifikate und ob ein Alt-Inform auf eine tote Cloud-Key-Adresse zeigt. Ein Gerät mit zwei Hirn-Adressen in der Historie pendelt.

Abnahme: Gerät erscheint in der richtigen Site, Name gesetzt, Firmwarekanal korrekt.

Merkblatt 2: Layer-2-Entdeckung begrenzen

LLDP ist nützlich und gesprächig. In unsicheren Bereichen reicht es, wenn Access-Ports weniger erzählen als Uplinks.

Unbekannte Mini-[Switches](#) erkennt man trotzdem oft über MAC-Tabellen. Abschalten ist keine Unsichtbarkeit gegen Absicht.

Dokumentieren Sie, wo LLDP Pflicht ist: Uplink, AP, Server.

Merkblatt 3: Port-Security leichtgewichtig

Eine MAC-Limite von zwei am User-Port verhindert kleine Hubs und fängt Dockingstations noch ein.

Zu streng zerlegt VoIP plus PC plus Dongle. Zu lasch nützt nichts. Ausnahmeprofile für Labs.

Incident: Port down durch Limit ist ein Erfolg, wenn das Runbook das so nennt und nicht „[WLAN](#) kaputt“.

Merkblatt 4: IGMP in Mediennetzen

Multicast ohne Pflege flutet Access. IGMP-Snooping und ein Querier gehören zum AV-Entwurf.

Büro-[VLANs](#) brauchen das selten flächig. Global an ist oft global falsch.

Test: ein Stream, ein Empfänger, Nachbarport ohne Stream bleibt ruhig.

Merkblatt 5: Jumbo nur Ende-zu-Ende

MTU 9000 auf einem [Switch](#) und 1500 auf dem [Gateway](#) zerlegt oder fragmentiert merkwürdig.

Storage-Netze dürfen Jumbo, wenn alle Mitglieder mitziehen. APs und WAN meist nicht.

Messen mit großen Rahmen, nicht mit Hoffnung.

Merkblatt 6: IPv6-RA kontrollieren

Router Advertisements aus dem falschen Gerät erzeugen doppelte Defaults.

Entweder [UniFi](#) allein oder der bestehende Router allein. Zwei Sheriffss, ein Client.

ipconfig /all auf dem Gold-Laptop nach der Inbetriebnahme lesen.

Merkblatt 7: Captive-Portal-Ausnahmen

Geräte ohne Browser – Drucker, Scanner, manche TVs – sterben am Portal.

Pre-Auth-Allow nur für das Nötige. Weite Ausnahmen machen aus dem Portal Dekoration.

Inventar der portal-unfähigen Geräte führen.

Merkblatt 8: Rate-Limit ehrlich

Gäste-Limits auf dem [Gateway](#) greifen nicht, wenn der AP-Uplink schon voll ist.

Limit als Politik gegen einzelne Nutzer, nicht als Ersatz für fehlende Zellen.

Messung mit zwei Clients, einer begrenzt, einer intern.

Merkblatt 9: Scheduler für SSIDs

Schul-SSIDs nachts aus sparen wenig Energie und erzeugen morgens eine Anmeldewelle.

Nützlich für Event-SSIDs und Prüfungsnetze mit klarem Fenster.

Kalender der Gebäudezeiten, nicht der Wunsch des ersten Tickets.

Merkblatt 10: Band-Steering testen

Steering, das 2,4-GHz-only-Scanner verjagt, ist Sabotage der Logistik.

Gruppenweise aktivieren. Lager-APs anders als Büro-APs.

Gehprobe mit beiden Geräteklassen.

Merkblatt 11: Mindest-Datenraten

Alte 1- und 2-Mbit-Raten fressen Airtime. Ausschalten hilft der Zelle und kann Legacy töten.

Inventar zuerst. Dann Raten anheben. Nicht umgekehrt.

Abnahme mit dem ältesten noch unterstützten Gerät.

Merkblatt 12: Airtime-Fairness nicht als Allheilmittel

Fairness mildert einen langsamen Client, repariert kein überlappendes Raster.

Wenn Utilization hoch und RSSI gut, zuerst Kanäle und Breite.

Feature-Toggle gehört ins Labor, nicht in die Showzeit.

Merkblatt 13: Spektrales Scan-Radio lesen

Plots ohne Interpretation sind Poster. Suchen Sie nicht-WLAN-Störer und dauerhafte Occupancy.

Videobrücken, DECT-Inseln, Maschinen. Dann erst AP-Dichte erhöhen.

Foto oder Export des Plots ins Ticket.

Merkblatt 14: Kanalbreite 160 MHz

Nur wo 6 GHz frei und Clients stark und Zellen klein.

Flächig in der Stadt ist 160 MHz ein Nachbarschaftsproblem.

Default 80 MHz, 160 als bewusste Hochleistungsinsel.

Merkblatt 15: RSSI-Karten lügen ohne Client

AP-seitige Heatmaps kennen den Uplink des Smartphones nicht.

Survey im Sendemodus des Clients oder mit bekanntem Gerät.

Punkte in Fluren und an Arbeitsplätzen, nicht nur in Raummitten.

Merkblatt 16: Deckenmaterial

Metall, Holz, Beton, Raster mit Folie: jedes ändert die Keule.

Montageplatten und Reserveantenne nach Hersteller, keine Eigenkonstruktion aus Blech.

Nachträglich gedämmte Decken erfordern Nachmessung.

Merkblatt 17: Aufzugsschächte

Funk um den Schacht herum, nicht hinein hoffen.

Versorgung im Fahrkorb ist ein eigenes Projekt mit Regeln des Aufzugsbauers.

Nicht im Sollkonzept als „machen die APs schon“ verstecken.

Merkblatt 18: Parkhaus

Beton, Autos als Absorber, niedrige Höhe. Viele kleine Zellen, 2,4 GHz bewusst, 5 GHz für moderne Clients.

Outdoor- oder spezifizierte Modelle, Feuchte, Temperatur.

Roaming entlang der Fahrspur testen, nicht nur am Fußweg.

Merkblatt 19: Denkmalschutz

APs unsichtbar oder an bestehende Leuchten. Das ändert Dichte und Preis.

Früh die Behörde bzw. Bauherrn einbinden. Sonst stirbt das Raster an der letzten Genehmigung.

Foto-Soll vor der Bestellung.

Merkblatt 20: Hotelzimmer IW

In-Wall speist eine Dose im Zimmer. Trunk vom Flur-[Switch](#) muss [VLANs](#) für Gast, Minibar-IoT und Telefon tragen.

Nicht jedes Zimmer ein eigenes [VLAN](#), außer die Politik das erzwingt. PPSK oder Portprofil je Etage.

Prüfen: Gast im Zimmer sieht nicht den Gast nebenan und nicht das PMS-Netz.

Merkblatt 21: POS-Netze

Kassen isolieren, Internet nur zu Zahlungszielen, keine Drucker im selben Trust wie Gäste.

PCI-Fragen sind Vertrags- und Prozessfragen, nicht nur [VLAN](#)-Farben.

Dienstleister-Zugänge befristen.

Merkblatt 22: Gebäudetechnik

OT/GA oft alte [Switches](#). Nicht einfach in Internal hängen.

Firewall default deny, Sprunghost, keine direkte Fernwartung aus dem Internet ohne Brokerschicht.

Inventar der Steuerungen, bevor jemand „kurz Internet“ verlangt.

Merkblatt 23: Drucker-[VLAN](#) und AirPrint

Reflektor gezielt zwischen Mitarbeiter und Drucker, nicht global.

Serverbasiertes Drucken ist langweiliger und robuster.

Wenn Reflektor, dann mit Owner und mit der Option, ihn auszuschalten.

Merkblatt 24: Datei-Server Ost-West

Große Kopien nicht durch IPS-Spitze am [Gateway](#) zwingen, wenn die Sicherheitslage den lokalen Pfad erlaubt.

Messung vor der Entscheidung. Nach der Entscheidung Matrix und Routing anpassen.

Backupfenster getrennt von der Nutzer-QoS.

Merkblatt 25: QoS-Markierung am Rand

Wenn das Telefon nicht markiert, muss der Port es tun.

Vertrauen Sie nicht darauf, dass WAN-Provider DSCP erhalten. Oft tun sie es nicht.

Sprache zuerst im LAN retten, dann über WAN diskutieren.

Merkblatt 26: SIP über NAT

ALG und Timeouts. Lange stille Gespräche sterben an kurzen Sessions.

Eigenes [VLAN](#) hilft der Policy, nicht automatisch dem NAT-Verhalten.

Testgespräch 40 Minuten, nicht 40 Sekunden.

Merkblatt 27: Teleport und One-Click

Bequemlichkeit für Admins ist kein Mitarbeiter-VPN-Konzept.

Rollen trennen. Admin-Teleport nicht dasselbe Profil wie Homeoffice-Buchhaltung.

Nach Offboarding Konto und Gerät prüfen.

Merkblatt 28: L2TP-Restbestände

Abbauen. Moderne Clients und Policies gehören auf WireGuard, IPsec oder Identity-Wege.

Jeder Rest ist eine Dokumentationslüge „wir sind schon um“.

Termin im Lifecycle.

Merkblatt 29: BGP zu einem Transit

Filter inbound und outbound. Keine Default-Originatation aus Versehen. Keine Full Table auf Filial-CPU.

AS-Nummer, Peering-LAN, MD5 oder besser, Prefix-Liste.

Labor mit zwei Peers, bevor Produktion den ersten Prefix sieht.

Merkblatt 30: OSPF-Area-Einfachheit

Eine Area reicht oft. Mehr Areas ohne Grund sind Prestige.

Hellos durch die Policy lassen. Passive an Access-SVIs.

Nach Änderung die Datenbank vergleichen, nicht nur „Nachbar up“.

Merkblatt 31: Redistribution filtern

Statisch nach OSPF ohne Filter verkündet auch das Labornetz.

Explizite Prefix-Listen. Jedes redistribuierte Netz hat einen Owner.

Show auf beiden Enden.

Merkblatt 32: Blackhole-Routen

Für zusammengefasste Netze, die nicht existieren, damit nicht default ins falsche WAN zieht.

Klassiker nach Umnummerierung.

Dokument im Adressplan.

Merkblatt 33: Policy-based Routing

Gäste über billige Leitung, Sprache über gute. Sessions nicht zerreißen.

Zu viele PBR-Regeln werden zur zweiten Firewall, die niemand sieht.

Je Regel ein Geschäftszweck.

Merkblatt 34: Dual-NAT vermeiden

Gateway NAT plus Provider-NAT plus Overlay-NAT ist ein Museum der Ports.

Jede NAT-Schicht braucht ein Bild.

Wenn möglich eine Schicht weniger als gestern.

Merkblatt 35: Portfreigaben inventarisieren

Jede Freigabe Datum, Dienst, Owner, externe Prüfzeit.

Ungenutzte Freigaben sind Einladungen.

Vierteljährliches Lesen der Liste, nicht nur Anlegen.

Merkblatt 36: Geo-Filter

Hilft gegen Lärm, nicht gegen gezielte Angriffe über erlaubte Länder.

Ausnahmen für Reisende und Cloud-Regionen der Fachverfahren.

False-Positive-Prozess definieren.

Merkblatt 37: Botnet- und Threat-Listen

Nützlich, wenn aktuell. Schädlich, wenn sie Fach-IPs listen, die niemand pflegt.

Override mit Begründung.

Nach Update eine Woche beobachten.

Merkblatt 38: Admin-GUI nicht aus WAN

Selbst „nur mit starkem Passwort“ ist ein Scan-Ziel.

VPN oder Out-of-Band. Punkt.

Externer Scan nach Go-live als Beweis.

Merkblatt 39: Default-PSK drehen

Nach Integratorübergabe alle vorläufigen Schlüssel.

Sonst kennt ein ehemaliger Dienstleister das Gäste- und oft das IoT-Netz.

Rotation im Offboarding-Check des Lieferanten.

Merkblatt 40: Site-Passwörter

Nicht dasselbe PSK in 22 Filialen, wenn eine Filiale öffentlich kompromittiert werden kann.

Ableitung oder 802.1X.

PPSK oder Enterprise statt eines Zettels an allen Tresen.

Merkblatt 41: Firmware-Notiz lesen

Breaking: Policy-Defaults, [WLAN](#)-Radio-Verhalten, [Optik](#)-Kompatibilität, Protect-Platten.

Wer nur die Versionsnummer sieht, testet in Produktion.

Labor zuerst, zwei Sätze Notizen im Ticket.

Merkblatt 42: Geräte in Chargen

Nicht 200 APs in einer Minute. Wellen mit Beobachtung.

Erste Welle ein Gebäude, nicht alle Dächer.

Stoppkriterium vorab.

Merkblatt 43: Controller zuerst

Konsole aktualisieren, dann Geräte. Umgekehrt erzeugen Inkompatibilitäten.

Backup vor der Konsole. Immer.

GUI-Login und eine Adoption danach testen.

Merkblatt 44: Config-Version taggen

Nach großen Änderungen Export mit Datum und Ticketnummer.

Sonst ist Restore ein Ratespiel zwischen drei Dateien namens backup.unf.

Ablage außerhalb der Konsole.

Merkblatt 45: Restore üben

Laborgerät, nicht Theorie. Zeit messen. Welche Secrets fehlen (PSK, Tokens)?

Üben macht das Notkonto sichtbar, das niemand mehr kennt.

Protokoll mit Uhrzeit.

Merkblatt 46: Monitoring nicht auf demselben WAN

Wenn der Standort stirbt, soll die Ampel von außen rot werden.

Externer Probe plus lokaler Syslog.

Test durch Ziehen des Management-Pfads.

Merkblatt 47: Kapazitätsalarm

DHCP-Pool 80 Prozent, PoE 80 Prozent, Uplink 70 Prozent in der Spitze, CPU Gateway 60 Prozent inspiziert.

Zahlen justieren, aber Zahlen haben.

Alarm ohne Runbook ist Lärm.

Merkblatt 48: Falsch-positive Alarme töten

Ein Dauerrot trainiert Ignoranz.

Schwelle oder Dienst ändern. Nicht stumm schalten ohne Notiz.

Wöchentliche Alarmhygiene.

Merkblatt 49: Change-Kalender sichtbar

Ein gemeinsames Brett. Doppelte Fenster auf demselben Core sind vermeidbar.

Fachbereiche sehen Freeze.

Nachspiel: was war ungeplant.

Merkblatt 50: Postmortem ohne Schuldshow

Zeitreihe, Wirkung, fehlende Übung, eine Verbesserung.

Zwei Verbesserungen, die niemand umsetzt, sind schlechter als eine umgesetzte.

Termin der Umsetzung im selben Dokument.

Merkblatt 51: Ersatzteil-Lagerort

AP, Optik, kleines Gateway, Netzteil. Nicht im selben Raum wie der Kernbrand.

Liste mit Serien, die noch nicht adoptiert sind.

Vierteljährlich Staub und Datum prüfen.

Merkblatt 52: Leihgerät-Prozess

Integrator lässt ein Laborgerät liegen. Es wird Produktion ohne Inventar.

Ausgangskontrolle am Rack.

MAC gegen Liste.

Merkblatt 53: Namenskonvention

standort-rolle-etage-nummer. Keine Eigennamen von Mitarbeitern am Gerät.

Umbenennen nach Umzug, nicht zusätzlich.

Regex in der Doku, nicht nur Beispiele.

Merkblatt 54: Kartenmaßstab

Falscher Maßstab im Design Center erzeugt falsche AP-Zahlen.

Einen Flur nachmessen und gegen die Karte halten.

Erst dann automatische Vorschläge ernst nehmen.

Merkblatt 55: Wandtypen im Modell

Glas, Beton, Trockenbau nicht dieselbe Dämpfung. Wer alles als „Wand“ zeichnet, malt Kunst.

Stichprobe messen und Modell kalibrieren.

Dokument der angenommenen dB.

Merkblatt 56: Personen als Dämpfung

Volle Mensa ist nicht die leere Mensa des Survey-Samstags.

High-Density-Reserven oder Messung zur Stoßzeit.

Veranstaltungsnetze sowieso unter Lastprobe.

Merkblatt 57: Client-Zahl lügen lassen

200 assoziierte Clients, 20 aktive. Planung auf aktive plus Reserve.

Sleeping Phones sind keine Videokonferenz.

Trotzdem Broadcast und Verwaltungslast der 200 nicht ignorieren.

Merkblatt 58: Broadcast-Domäne

Zu große L2-Netze machen Scans und Chats zu Stürmen.

/22 für Clients nur mit Grund. /24 bleibt Default.

Nach Merger bewusst splitten.

Merkblatt 59: DHCP-Optionen VoIP

Falsche Option legt Telefone ins falsche VLAN oder an den falschen Server.

Labor mit einem Telefon, dann Etage.

Vendor-Dokument, nicht Forum-Snippet allein.

Merkblatt 60: PXE und VLAN

Imaging braucht Relay und oft ein eigenes Fenster, in dem Guard und Policy mitspielen.

Dauerhaft offene PXE-Pfade sind unnötig weit.

Arbeitsplatzteam als Owner.

Merkblatt 61: Gäste und Drucker

Gäste sollen nicht den Geschäftsdrucker sehen. Auch nicht über AirPrint-Unfall.

Reflektor-Regeln lesen.

Test mit einem Gastkonto nach jedem Reflektor-Change.

Merkblatt 62: BYOD-Prüfung

Eigenes Netz, eigenes DHCP, kein interner DNS, Rate-Limit, Freeze.

Kapazität wie ein Event planen.

Nach der Prüfung Netz wieder eng oder aus.

Merkblatt 63: Lieferant im Netz

Befristeter Zugang, eigene Rolle, kein Mgmt, Logging.

Kein Shared-Admin „für den Techniker am Dienstag“.

Ablaufdatum sichtbar.

Merkblatt 64: Zwei Provider, eine Policy

Failover testen einschließlich DNS der Provider und unterschiedlicher NAT-Adressen.

Fachverfahren mit IP-Allowlists am anderen Ende müssen beide Adressen kennen.

Liste dieser Verfahren führen.

Merkblatt 65: LTE-Backup

Budget, Antenne, Tarif-Drossel nach Volumen. Health nicht nur gegen das Modem-[Gateway](#).

Nicht als heimliches Haupt-WAN in der Filiale ohne Tarif, der das trägt.

Monatliches Testdatum.

Merkblatt 66: Stromkreis-Farben

A- und B-Feed an Dual-PSU wirklich A und B, nicht zwei Stecker einer Leiste.

Begehung mit Elektriker.

Foto der Leisten.

Merkblatt 67: USV-Bypass

Wartung der USV legt ohne Plan das Netz tot.

Bypass-Fenster gleich Change-Fenster.

[PoE](#)-Last während Bypass kennen.

Merkblatt 68: Kälte im Rack

1U-Geräte mit hohen Watt nicht zwischen zwei Blindplatten ohne Luft.

Herstellerangaben zum Abstand.

Temperatur nach einer Stunde Last.

Merkblatt 69: Schranktür und Lichtwellen

Enge Biegeradien an der Tür sind spätere Dämpfungsoffer.

Führung und Reserve-Schlaufe.

Nach dem Schließen der Tür messen, nicht nur bei offener Tür.

Merkblatt 70: [Patchkabelqualität](#)

Cat6-Patch an Cat6A-Strecke kann der schwächste Meter sein.

Lager mit geprüften Längen.

Fehlerzähler am Port als Hinweis, nicht als Charakterzug des [Switches](#).

Merkblatt 71: Fremdoptik

Kann funktionieren und nach Update nicht mehr.

Risiko akzeptieren oder nicht, aber schriftlich.

Labor-Firmware vor Fläche.

Merkblatt 72: [BiDi](#)-Faser

Spart Fasern, verdoppelt Verwechslungen von TX/RX-Farben.

Beschriftung zwingend.

Ersatzpaar im selben Beutel.

Merkblatt 73: Hausübergabe-Protokoll

Dose, Faser, Schott, Messung. Ohne das ist der Integrator der Prüfer seiner selbst.

Stichproben durch Dritte oder Betrieb.

Offene Punkte mit Geldwert, nicht nur mit Smileys.

Merkblatt 74: Schulung 90 Minuten

Leitstand sieht, Betrieb handelt drei Runbooks, Architektur bleibt außen.

Besser 90 Minuten am eigenen Netz als ein Tag Theorie an Screenshots einer anderen Version.

Wiederholung nach Major-Release.

Merkblatt 75: Version der Screenshots

Runbooks mit GUI-Bildern datieren. Network 8-Bilder in einem 9-Policy-Haus erzeugen falsche Klicks.

Nach Major Update Bilder tauschen.

Verantwortlich: Owner Betrieb.

Merkblatt 76: Schatten-SSID der Nachbarn

Gleicher Name, anderes Passwort: Nutzer beschwerten sich über „unser [WLAN](#)“.

Namen eindeutig wählen. Hotel-Lobby-Namen meiden.

Nach Umbenennung Alt-SSID befristet parallel.

Merkblatt 77: QR-Codes am Empfang

Bequem und öffentlich. Rotation und Ablauf.

Nicht das interne PSK als QR in der Eingangshalle.

Foto der Halle nach Go-live als Audit.

Merkblatt 78: Social Engineering gegen Empfang

Voucher-Kontingent und Schulung. Das Netz kann nicht erkennen, ob der Empfang nett war.

Prozess, nicht Feature.

Stichprobe.

Merkblatt 79: Inventur einmal im Jahr

Geräte, die in der GUI leben und in der Decke nicht, oder umgekehrt.

Locate und Begehung.

Differenzliste mit Owner.

Merkblatt 80: Ende eines Standorts

Geräte vergessen, Keys drehen, Overlay-Peer löschen, Adressen freigeben, Doku archivieren.

Sonst verbindet sich nächstes Jahr ein Schatten.

Checkliste Standort-Close.

Merkblatt 81: Lesen gegen die Langeweile

Langeweile im Betrieb ist ein Qualitätsmerkmal. Wer Langeweile mit Early Access bekämpft, kauft Spannung auf Kredit.

Spannung gehört in Labor und Übung.

Ende der Merkblätter heißt nicht Ende der Pflege.

Häufige Fragen

Brauchen wir Shadow Mode?

Wenn der Standort bei Gateway-Ausfall wirtschaftlich oder sicherheitlich nicht stehen darf und kein gleichwertiger Ausweichstandort in Minuten trägt: ja, sofern die Modellreihe es bietet. Sonst gut gepflegtes Kaltreserve plus kurze Wiederanlaufzeit.

Können wir das Gateway überspringen und nur Switches plus APs nutzen?

Ja, wenn ein anderes Gerät NAT, DHCP und Firewall übernimmt. Dann ist UniFi Access-Schicht. Zwei DHCP-Server in einem Broadcast sind trotzdem zwei DHCP-Server zu viel.

Ist Auto-RF genug?

In Einfamilienhäusern oft. In Etagen mit Nachbarn, Prüflingen und Lagerhallen nein. Auto-RF plus jährliche Revision ist der Kompromiss.

Wie viele SSIDs?

So wenige wie die Politik erlaubt. Drei sind ein gutes Ziel, fünf ein Maximum, acht ein Geständnis.

Wann L3 auf dem Switch?

Wenn Ost-West die Gateway-CPU nachweislich belastet und die Sicherheitslage den Shortcut erlaubt. Nicht, weil das Häkchen existiert.

Was tun mit Alt-USG?

Nicht mehr als Standardpfad. Ersatz durch UXG oder Cloud Gateway, bevor die nächste große Policy-Engine-Funktion ausbleibt.

Cloud-Hosting trotz Datenschutzfragen?

Klärung vor dem Warenkorb. Technische Alternative ist lokale Konsole. Halbe Migrationspfade erzeugen doppelte Zuständigkeit.

Wie oft Firmware?

Lesen monatlich, installieren nach Bedarf und nach Labor, nicht nach Langeweile. Sammelfenster schlägt wöchentliche Überraschungen.

Reichen Flex-Switches unter Schreibtischen?

Als bewusste Dose-Verlängerung ja. Als heimliche Etage nein.

Was ist mit IPv6?

Entweder gleichwertig planen oder bewusst aus. Halb ist ein Loch.

Teil V – Betrieb

Der Go-live ist der Beginn der Wahrheit. Betrieb heißt, dass Änderungen reproduzierbar sind, dass Abweichungen auffallen, bevor Nutzer sie fühlen, und dass Wiederherstellung geübt ist. Ein Dashboard ohne Alarmierung ist Innenarchitektur: schön anzusehen, und es alarmiert niemanden.

23 Beobachtbarkeit

23.1 Was UniFi selbst zeigt

Die Network Application kennt Gerätezustand, Clientlisten, Durchsatz, Warnungen, RF-Umgebung, WAN-Gesundheit und viele Flows der Anwendungserkennung. Das reicht für den Alltag kleiner Teams, wenn jemand hinschaut – der Clou liegt im „wenn jemand hinsieht“. Es reicht nicht als alleiniges Langzeitarchiv und nicht als SIEM.

Bauen Sie Views nach Rolle: Der Leitstand sieht WAN, Gateway-CPU, Switch-Uplinks, AP-Utilisation, Clientzahl, USV. Der Betrieb sieht Tickets und Firmware. Die Sicherheit sieht Policy-Hits und VPN-Anomalien. Drei Blickwinkel, ein Netz – jeder sieht, was er verantwortet.

23.2 Export

Syslog, SNMP, wo sinnvoll, API-Abfragen, Netflow-ähnliche Sichten, soweit die Version sie bietet. Externe Ziele liegen nicht auf demselben Gateway, das sie beobachten sollen – der Zeuge wohnt nicht im selben brennenden Haus. Aufbewahrung folgt Datenschutz und Nachweispflicht, nicht der Default-Größe der internen Platte.

23.3 SLIs

Sinnvolle Indikatoren: WAN-Erreichbarkeit kritischer Ziele, DHCP-Erschöpfung, CPU und Temperatur von Gateway und Core, PoE-Budget auf Reserve, AP-Retry-Raten, VPN-SA-Stabilität, Zahl der nicht adoptierten Geräte, Backupalter. Was keinen Schwellenwert hat, ist keine Messung, sondern Dekoration.

24 Lifecycle, Firmware und Change

24.1 Kanäle

Official, Release Candidate, Early Access. Produktion steht auf Official, Labor darf vorauslaufen. Ein Standort, der „mal schnell EA testet“, ist ein Standort ohne Change-Prozess – der Test läuft, nur weiß niemand, dass er einer ist. Lesen Sie Release Notes auf Breaking Changes bei Policy Engine, WLAN-Defaults und Optik-Kompatibilität.

24.2 Rollout

Reihenfolge: Konsole, [Gateway](#), Core, Aggregation, Access, AP. Nie alles gleichzeitig. Je Stufe Beobachtungszeit. Rückfallimage bereithalten. [PoE](#)-APs nach [Switch](#)-Firmware neu starten können – das gehört ins Wartungsfenster, nicht in die Mittagspause der Produktion.

24.3 Backup

Automatische Sicherung der Network Application an zwei Orte: eines offline, eines außer Haus. Verschlüsselung und Wiederherstellungstest vierteljährlich. Ein Backup, das niemand einspielt, ist eine Datei; ein Restore, der nie geübt wurde, ist eine Hoffnung. Exportieren Sie zusätzlich den Adressplan und die Zonenmatrix als lesbares Dokument, falls die Oberfläche nach einem Disaster langsamer zurückkommt als das Team.

24.4 Änderungskalender

Jede produktive Änderung hat Ticket, Fenster, Risiko, Rollback. Notfälle dürfen den Kalender brechen, nicht die Dokumentation danach. [UniFi](#) macht Änderungen leicht – genau deshalb braucht es die Bremse.

25 Störungssuche

25.1 Denkmodell

Zuerst den Scope: ein Client, eine Zelle, eine Etage, ein Standort, alle Standorte. Dann die Schicht: Funk, Access-Port, Uplink, [Gateway](#), WAN, Identität. Dann die Zeit: seit Firmware, seit Umbau, seit Sturm. Wer überall gleichzeitig klickt, erzeugt die zweite Störung – diesmal seine eigene.

25.2 [WLAN](#)-Pfade

Client sieht SSID nicht: Band, versteckte SSID, Mindestrate, geblockte MAC, falsches Profil am AP. Client sieht, verbindet nicht: PSK/802.1X, Systemzeit, RADIUS, DHCP. Client verbindet, arbeitet nicht: [VLAN](#), Firewall, DNS, Routing. Client klebt: Leistung zu hoch, Fast Roaming schief, sticky Steering.

25.3 LAN-Pfade

Port down: Kabel, [PoE](#)-Klasse, Fehlerzähler, andere Seite. [VLAN](#) falsch: Profil, Native [VLAN](#), tagged/untagged-Missverständnis. Slow Path: Duplex, defekter Crimp, voller Uplink, CPU auf L3-[Switch](#), [Gateway](#)-Inspektion. Loop: Last überall, RSTP-Topologie prüfen, Miniswitch suchen.

25.4 [Gateway](#)-Pfade

WAN tot: Layer 1, [VLAN](#) beim ISP, [PPPoE](#), Health-Check-Ziel. Policy zu scharf: letzte Änderung, Matrixzelle, VPN-Zone. CPU hoch: IPS plus SSL-Inspection plus Flow-Logging plus Threat-Listen in der Spitze. Shadow greift nicht: Interlink, Firmware-Paar, Test nie geübt.

25.5 Werkzeuge

Neben der GUI: Kabeltester, Spektrum, iperf zwischen bekannten Endpunkten, Paketspiegel auf dem [Switch](#), Client-Logs, RADIUS-Logs, ein goldener Laptop mit bekannt gutem Profil. Der goldene Laptop beendet religiöse Debatten über „das [WLAN](#) ist schuld“.

26 Multi-Site und Organisation

26.1 Betreibermodell

Ein zentrales Netzteam mit Vorlagen skaliert besser als 40 lokale Helden. Lokale Kräfte brauchen Runbooks für physische Arbeit: tauschen, patchen, AP ausrichten. Änderungen an Policy bleiben zentral, sonst driftet die Matrix.

26.2 Stückliste und Ersatz

Ersatz-APs derselben Generation, ein Access-[Switch](#) je verbreiteter Klasse, [Optik](#)-Satz, ein [Gateway](#) der Filialklasse. Shadow-Paare sind keine Ersatzteile, sie sind Produktion. Ein drittes Gerät im Lager rettet den Tag, an dem beide Netzteile dasselbe Schicksal haben.

26.3 Dokumentation als Produkt

Lebende Dokumente: Adressplan, Zonenmatrix, Portbelegung, Funkraster, WAN-Verträge, Wiederanlauf. Ablage, die das Team findet. Versionierung. Das Buch, das Sie gerade lesen, ersetzt keines dieser Standortdokumente.

27 Referenzszenarien

27.1 Mittelstandscampus, 400 Personen, zwei Häuser

Anforderung: Büro, etwas Lager, 30 Kameras, Gäste, Hybridarbeit, ein Rechenraum. Entwurf: [UDM-Beast](#) oder [EFG](#) je nach WAN und Inspektion, Shadow wenn der Standort geschäftskritisch ohne Ausweichbüro ist. Aggregation 25G zwischen Häusern auf zwei Fasern getrennter Trassen. Etagen als Enterprise- oder Pro-XG-Access je nach AP-Uplink. [WLAN](#): U7 Pro XGS in Büros, E7 in der Cafeteria-Dichte, 5 GHz 40 MHz, 6 GHz 80 MHz, drei SSIDs.

Zonen: Mgmt, Mitarbeiter, Server, IoT, Kamera, Gast. Ost-West Server-Client über [Gateway](#), Backupverkehr im Servernetz lokal. Protect auf der Konsole nur, wenn die Kamerazahl zur Plattform passt; sonst eigener Recorder.

Betrieb: Official-Firmware, monatliches Fenster, Syslog nach außen, vierteljährlicher Failover-Test des WAN, jährlicher [Gateway](#)-Schattentest falls vorhanden. Typische Fallstricke: UDM-interne Ports als Gebäudeaccess, ein einzelner Graben/Gebäudeübergang als [LWL](#)-Trasse, Gäste im Internal.

27.2 Filialnetz, 25 Standorte

Anforderung: gleiche Policy, lokales Drucken, zentraler ERP-Zugriff, kleines Protect, 5G-Backup an der Autobahnfiliale. Entwurf: [UXG](#)-Max oder [UXG](#)-Fiber je nach Anschluss, zentrale Network Application, Site-Template, [Site Magic](#) Stern auf zwei Hubs in getrennten Rechenräumen. [Switch](#) Pro Max 16/24 [PoE](#), zwei U7 Pro, [VLAN](#)-Satz identisch, Adressen nicht überlappend.

WAN-Health gegen das ERP, nicht gegen 8.8.8.8 allein. Spoke-Isolation an, außer für definierte Druck- und Dateipfade über die Zentrale. Lokales Team darf APs tauschen, nicht die Matrix.

27.3 Lager und Leichtindustrie

Anforderung: Scanner-Roaming, Stapler, Metallregale, OT-Steuerung, Kameras an Toren. Entwurf: predictive plus Messsurvey in den Gassen. Mehr APs an den Kreuzungen als über den Regalmitte-Blindstellen. 2,4 GHz bewusst für alte Scanner, 5 GHz für moderne, 6 GHz nur wenn die Flotte es trägt. [Switches](#) mit [PoE](#)-Reserve wegen Kältestart. OT in eigener Zone ohne Internet, Sprungserver aus dem Management.

Mesh über den Hof höchstens als Brücke zur Pforte. Glas unter der Rampe ist billiger als zwei Jahre unlösbare Roamingtickets.

27.4 Auditorium und Event

Anforderung: 800 Clients in einer Halle, BYOD, Ticketing offline-fähig, Medienstrecke getrennt. Entwurf: E7 Audience oder sehr dichte E7-Campus-Zellen mit gerichteter Energie in die Fläche, nicht in die Nachbarwand. 10G bis zum AP, Aggregation mit echter Summe, nicht mit Hoffnung. Gast-SSID mit Portal und Rate-Limit, Mitarbeiter getrennt, Medien auf AV-[Switching](#).

Probe auf voller Last. Ein Test mit zwölf Laptops ist keine Aula. Kanalplan fest, Auto-RF in der Showzeit aus oder eingefroren.

27.5 Schule

Anforderung: Klassendichte, Prüfungsmodus, Lehrerverwaltung, Gast im Foyer, Jugendmedienschutz. Entwurf: viele mittlere Zellen statt weniger Leuchttürme, Content-Filter auf dem [Gateway](#) plus Endgeräteverwaltung, Prüfungs-SSID mit explizitem Allow-Netz, 802.1X für Lehrgeräte wo möglich. [Switches](#) in abschließbaren Schränken, APs gegen Abnahme gesichert.

Ferien sind Firmwarezeit. Schulbeginn ist Freeze.

Anhang A – Checklisten

A.1 Konzept

- Nutzungszonen und Verfügbarkeitsklassen beschrieben
- Adress- und [VLAN](#)-Plan ohne Überlappung zu VPN-Partnern
- Zonenmatrix mit Default und Ausnahmen
- [WLAN](#)-Dichte je Zone, Bandstrategie, SSID-Zahl
- [PoE](#)-Bilanz Worst Case inkl. Start
- Uplinksummen gegen reale Last
- Steuerungsmodell Cloud GW vs. [UXG](#) entschieden
- Backup, Monitoring, Identitätsquellen benannt
- Stückliste mit Reserve und [Optik](#)

A.2 Go-live

- Laborimage entspricht Produktionsschiene
- Adoptionsreihenfolge eingehalten
- DHCP, DNS, NTP in jedem Segment geprüft
- Firewalltests inkl. expliziter Deny
- VPN-Benutzerrolle verengt
- Roaming mit echter Clientflotte
- WAN-Failover gezogen
- Backup erzeugt und Probe-Restore im Labor
- Dokumentation an das Betriebsteam übergeben

A.3 Monatlicher Betrieb

- Alarme ohne Dauerrot
- Backupalter geprüft
- [PoE](#)- und Uplink-Headroom
- Firmware-Kanäle gelesen, nicht unbedingt installiert
- Geistergeräte und pendende Adoptionen
- Zertifikats- und RADIUS-Gesundheit
- Kapazitätszeitreihe angesehen

Anhang B – Referenztabellen

B.1 [PoE](#)-Klassen

Bezeichnung	Standard	Typische Leistung	Typische Last
-------------	----------	-------------------	---------------

PoE	802.3af	bis ca. 15 W	kleine Telefone, einfache Kameras
PoE+	802.3at	bis ca. 30 W	viele U6/U7-APs, Standardkameras
PoE++	802.3bt Typ 3	bis ca. 60 W	stärkere APs, PTZ, Displays
PoE+++	802.3bt Typ 4	bis ca. 90 W	E-Klasse, High-Power, AV

Tabelle B.1: [PoE](#)-Orientierung für die Leistungsbilanz

B.2 Funkbänder

Band	Rolle	Kanalbreite Start	Hinweis
2,4 GHz	Legacy, Fläche, Störung	20 MHz	wenig Zellen, niedrige Leistung
5 GHz	Alltagskapazität	40 MHz	80 MHz nur mit Spektrum
6 GHz	hohe Bitrate, kurze Wege	80 MHz	Clients und Regulation prüfen

Tabelle B.2: Bandstrategie als Startwert, keine Dogmatik

B.3 Steuerungsentscheidung

Frage	Cloud Gateway	UXG + zentrale App
Standort autonom?	ja	eingeschränkt
Viele gleiche Filialen?	möglich, aufwendiger	ja
Protect lokal auf dem Router?	oft ja	nein, extra Recorder
Shadow / Dual-PSU kritisch?	Modellabhängig	Enterprise- UXG ja
Team ohne eigene Server?	stark	Hosting nötig

Tabelle B.3: Control-Plane-Entscheidung

Anhang C – Glossar

Adoption. Aufnahme eines [UniFi](#)-Geräts unter die Network Application.

Cloud Gateway. Router plus lokale [UniFi-OS-Konsole](#).

DAC. Direct Attach Copper, kurzer Twinax-[SFP](#)-Anschluss.

EFG. [Enterprise Fortress Gateway](#).

Etherlighting. Portbeleuchtung zur schnellen Diagnose an ausgewählten [Switches](#).

IDS/IPS. Erkennung bzw. Verhinderung verdächtiger Muster auf dem [Gateway](#).

LACP. Bündelung paralleler Ethernetglieder zu einem logischen Portkanal.

MC-LAG. Portkanal über zwei Chassis gegen Einzelausfall.

Mesh. [WLAN](#)-Rücktransport über Funk statt Kabel.

Native VLAN. Ungetaggtter Verkehr auf einem Trunk.

PPSK. Privater PSK, der Nutzer auf unterschiedliche [VLANs](#) legen kann.

PRISM. Aktive RF-Filtertechnik ausgewählter Campus-APs.

RSTP. Rapid Spanning Tree gegen Schleifen in Layer 2.

Shadow Mode. [Gateway](#)-Paar mit Zustandsabgleich mit Zustandsabgleich.

Site Magic. Orchestrierte Site-to-Site-Overlay-Funktion im [UniFi-Ökosystem](#).

SSID. Angezeigter Name eines Funknetzes.

SVI. Virtuelles Interface einer [VLAN](#)-Schnittstelle am L3-[Switch](#) oder [Gateway](#).

UXG. Unabhängiges [UniFi-Gateway](#) ohne eigene Network-Konsole.

Zone-Based Firewall. Policy zwischen Interface-Gruppen statt isolierter Ketten je Richtung.

Schlagwortverzeichnis

Das Verzeichnis verweist auf Kapitel, nicht auf flüchtige Seitennummern vor der endgültigen Umbruchfassung. In Word kann zusätzlich ein Indexfeld gepflegt werden.

A

- [Access Point](#) 7, 12, 21
- Adoption 15
- Aggregation 6, 14
- API 3, 23

B

- BGP 4, 18
- Broadcast 20
- Backup 24

C

- [Cloud Gateway](#) 3, 5
- Core [Switch](#) 6
- Captive Portal 19

D

- [DAC](#) 8
- DHCP 4, 16
- DNS 4, 16
- DSCP 22

E

- E7 / E7 Campus / E7 Audience 7
- [EF-Core](#) 5
- [EFG](#) 5
- Etherlighting 6

F

- Failover 5, 14, 18
- Firmware 24
- Firewall-Zonen 11, 17

G

- [Gateway](#)-Zone 17
- Glossar Anhang C

H

- Hochverfügbarkeit 14
- Hotspot 11, 17

I

- IDS/IPS 5, 13
- IPsec 19
- IPv6 11
- IoT-Zone 11

L

- LACP 20
- Layer 3 4, 6, 20
- Lizenzmodell 1

M

- Management-[VLAN](#) 4, 13
- [MC-LAG](#) 6, 14
- Mesh 21
- Multi-WAN 5, 18

N

- Native [VLAN](#) 4, 20
- NTP 4
- Network Application 3

O

- OSPF 18, 19
- [Optik](#) 8
- OT-Netz 11, 27

P

- [PoE](#) 6, 8, Anhang B
- PPSK 11, 19
- Portprofil 6, 20
- Protect 1, 5

Q

- QoS 22

R

- RADIUS 19
- Roaming 12, 21
- RSTP 4, 20
- Routing 4, 18

S

- SD-WAN 19
- [Shadow Mode](#) 14
- [Site Magic](#) 19
- SSID 12, 21
- Stacking 6, 14
- Storm Control 20
- Survey 12

T

- Template 15, 26

- TCO 1

U

- [UCG](#) 5
- UDM-Familie 5
- [UXG](#) 3, 5
- USV 8

V

- [VLAN](#) 4, 11
- VPN 17, 19
- VRRP 14

W

- WAN 5, 18
- [Wi-Fi 6E](#) / 7 7, 12
- WireGuard 19

Z

- Zone-Based Firewall 11, 17
- Zonenmatrix 17, Anhang A

Schlussbemerkung

Ein [UniFi](#)-Enterprise-Netz ist dann gut, wenn es langweilig ist: vorhersehbare Zonen, langweilige Firmwarefenster, langweilige Backups, langweilige Failover-Tests. Spannung gehört in das Funkdesign vor dem Bau und in die Störung, die trotz alledem kommt – nicht in den Alltag der Policy-Matrix.

Die Plattform wird weiter neue Cores, neue APs und neue Assistenten bekommen. Die Fragen dieses Buches bleiben: Wo liegt die Layer-3-Grenze? Wie klein ist die Ausfalldomäne? Wer darf wen erreichen? Welcher Uplink trägt die Zelle wirklich? Wer spielt das Backup ein?

Wenn diese Fragen schriftlich beantwortet sind, tragen [Gateways](#), [Switches](#) und [Access Points](#) den Rest mit einer Souveränität, die kein Datenblatt allein erzeugt.