ExtremeCloud™ IQ

Lösungsübersicht

Stand : 11. August 2020

alexander.eichholz@extremenetworks.com
ralf.klockewitz@extremenetworks.com

Bitte beachten Sie:

Dieses Dokument enthält unter anderem auch Informationen über künftige Lösungen und Funktionen. An dieser Stelle weisen wir darauf hin dass für Art und Zeitpunkt der Bereitstellung dieser Leistungsmerkmale nicht gehaftet werden kann. Ergänzend finden Sie hier den entsprechenden Disclaimer:

This product information represents Extreme Networks® current product direction.

All product releases will be on a when-and-if available basis.

Actual feature development and timing of releases will be at the sole discretion of Extreme Networks.

Not all features are supported on all platforms.

Presentation of the product strategy does not create a commitment by Extreme Networks to deliver a specific feature.

Contents of this Document are subject to change without notice.

Vorwort

Der weitgefächerte Blick auf die IT Landschaft zeigt sehr deutlich den allgemeinen Trend zu Software as a Service (SaaS). Von der Officeanwendung über Kommunikationssysteme bis hin zu sensiblen CRM Lösungen – viele essentielle Dienste sind heute schon an Serviceprovider ausgelagert.

Warum ist das so? Die Bereitstellung von IT Ressourcen im eigenen Rechenzentrum wird mit steigender Komplexität zunehmend aufwändiger. Dabei geht es nicht nur um Hardware, Energiebedarf und Klimatisierung. Die unbedingte Verfügbarkeit von Diensten ist ein unternehmenskritischer Faktor. Ausfälle führen in kürzester Zeit zum Zusammenbruch der Wertschöpfungskette mit allen daraus entstehenden Konsequenzen.

Aber auch schwer kalkulierbare Wachstumsfaktoren und damit verbundene Kosten stellen die IT Abteilung mittelständischer Unternehmen unter ungeheuren Planungsdruck.

Software as a Service bedeutet nicht nur, IT Prozesse ganz oder teilweise auszulagern. Die Möglichkeit, Rechen- und Speicherkapazitäten dynamisch und nach Bedarf kostengünstig zu buchen bietet eine reizvolle Alternative zur Beschaffung und Bereitstellung von Ressourcen auf dem eigenen Campus.

Diese – grundsätzlich elegante - Lösung verdient jedoch einen kritischen Blick. Wie abhängig mache ich mich von meinem Serviceprovider? Welche Konsequenzen hat ein Ausfall der WAN Anbindung? Und inwieweit habe ich die Kontrolle über Bewegung und Speicherung meiner Unternehmensdaten?

Genau betrachtet stehen wir nicht mehr vor der Entscheidung für oder gegen die Cloud. Denn die täglich genutzte Officeanwendung bietet heute schon flexible Kollaboration an – die Dokumente werden dabei außerhalb des Unternehmens bearbeitet. CRM Software läuft auf weltweit verteilten Servern. Und Storage ist – außerhalb der lokalen IT - so leicht und bequem nutzbar, dass sich Unternehmen berechtigte Sorgen über die Sicherheit ihrer kritischen Daten machen.

Wir sind bereits im Cloudzeitalter angekommen. Wichtig ist, die nächsten Schritte bewusst zu unternehmen und bei der Einführung von SaaS die richtigen Fragen zu stellen.

Mit diesem Dokument geben wir Ihnen einen Überblick über die Architektur unseres cloudbasierten Managementsystems. Wir sprechen über Funktionen und Mehrwerte, aber auch über die Maßnahmen, die wir zur Absicherung unserer Lösung getroffen haben.

XIQ - Die Lösung

Motivation

Was bewegt uns, die bewährte Strategie des controllerbasierten Wireless LAN durch etwas neues und bahnbrechend Anderes zu ersetzen?

Nun, vor 20 Jahren war WLAN in der Regel das Anhängsel eines LAN Redesigns. Ein Accesspoint im Besprechungsraum, einer im Foyer für Gäste. Und nur wenige, privilegierte Nutzer mit einer WLAN Karte im Notebook konnten diesen Dienst – mit einer Übertragungsrate von anfänglich 2Mbps überhaupt nutzen.
Aber nur wenige Technologien haben unsere Arbeitswelt – und unseren Lebensstil – so radikal auf den Kopf gestellt wie das mittlerweile omnipräsente WLAN. Und die Erwartungshaltung ist enorm. Wasser aus dem Hahn, Strom aus der Steckdose, Internet aus der Luft.

Das enorme Wachstum WLAN-fähiger Endgeräte stellt uns als Hersteller vor große Herausforderungen. Mit immer ausgefeilterer Technologie versorgen wir eine rapide steigende Zahl mobiler Systeme. Das ist tatsächlich kompliziert. Der Trick ist, den Umgang für Betreiber und Konsumenten trotz steigender Komplexität einfach zu machen.

WLAN für alle – Immer – Überall – Sicher!

Zielsetzung

ExtremeCloud IQ (XIQ) ist ein branchenführender und visionärer Ansatz für Cloud-managed Netzwerke, um die Funktionalität der End-to-End-Netzwerklösungen von Extreme voll auszunutzen. ExtremeCloud IQ bietet eine einheitliche Verwaltung von Access Points, Switches und Routern.

Das beinhaltet alle Elemente des Lebenszyklus eines WLAN: Onboarding, die Konfiguration, Überwachung, Fehlerbehebung, Reporting und vieles mehr. Innovative Technologien für maschinelles Lernen (ML) und künstliche Intelligenz (KI / AI) analysieren und interpretieren Millionen von Netzwerk- und Benutzerdatenpunkten vom Edge bis zum Data Center.

XIQ bedient alle aktuellen Anforderungen von Nutzern an WLAN, deckt den aktuellen Wirelessbedarf und skaliert nahezu unbegrenzt, um den Wachstumsanforderungen in Wireless, Switching sowie zukünftigen Technologiebereichen im Cloud-Management, gerecht zu werden.

Erste Schritte

Was bedeutet das im Klartext?

Ihr erstes WLAN Projekt besteht vielleicht aus einer Handvoll Access Points (AP) die Sie in Ihr LAN einbinden. Sie registrieren die Seriennummern im Cloud Management und können zusehen wie die neuen APs in kurzer Zeit automatisch Verbindung mit der Cloud aufnehmen. Ihre erste Network Policy umfasst einen einfachen WLAN

Zugang mit einem Preshared Key (PSK). Damit ist Ihr Job bereits getan. Konfiguration und Feintuning – die sogenannte Orchestrierung des WLAN übernimmt XIQ.

Natürlich leistet XIQ weitaus mehr. Aber jede große Reise beginnt mit dem ersten Schritt – und der sollte einfach sein!

XIQ – Die Architektur

Management der 4. Generation?

XIQ ist eine Cloud Management Plattform der vierten Generation. Die Vorstufen reichen von der einfachen Auslagerung eines Controllers über die Schaffung von Redundanzen, dem Aufbau einer Microservicestruktur bis hin zur Integration von ML und AI zur automatisierten Analyse und Konfiguration.

Microservices

Monolithisch programmierte Anwendungen sind vergleichsweise grobschlächtig. Jede Änderung im Code erfordert einen Compilerlauf. Die Einbringung ins Produktivsystem ist oft nicht ohne Wartungsfenster möglich. Daher müssen Änderungen und Bugfixes zeitlich dem Updatezyklus angepasst werden. Stellen Sie sich nun ein Konstrukt vor, in welchem einzelne Funktionsgruppen in Container gepackt werden. Diese Microservices kommunizieren untereinander über definierte Softwareschnittstellen – und sie lassen sich einfach und flexibel austauschen ohne dass die Funktion des Gesamtsystems beeinträchtigt wird. Auf diese Weise wurden im Jahr 2019 rund 130 Updates integriert – ohne Wartungsfenster.

Auch die Skalierung des Systems wird von Microservices unterstützt. Lastschwellwerte aktivieren einen automatischen Dispatcher, der zusätzliche Ressourcen reserviert und mit den nötigen Containern bestückt, um die Leistung des Gesamtsystems dynamisch zu erhöhen.

Cloud – oder doch On Premise Betrieb?

Natürlich ist der XIQ Betrieb in der Public Cloud die einfachste und kostengünstigste Variante. Alternativ gibt es jedoch auch die Möglichkeit, dedizierte Ressourcen in einer sogenannten Private Cloud bereitzustellen.

Die Local Cloud dagegen bildet die komplette XIQ Architektur auf separater Hardware bzw. einem VM Host in Ihrem eigenen Rechenzentrum ab. Diese Lösung erfordert natürlich eigene Ressourcen und ist damit etwas aufwändiger, bietet jedoch nahezu den gleichen Funktionsumfang – mit der gleichen Architektur und Verwendung derselben AP- und Switchmodelle. Lediglich auf Location und Presence Tracking muss verzichtet werden. Daran arbeiten wir.

Gerne beraten wir Sie bei der Auswahl des für Sie passenden Betriebsmodelles.

Cloud? Aber sicher!

Und wie steht es um die Sicherheit? Jeder Anbieter von Cloudlösungen nimmt für sich in Anspruch, eine ISO27001 Zertifizierung zu besitzen. In zahlreichen Fällen beruft man sich gerne auf die Sicherheit des jeweiligen Cloud Rechenzentrums. Das genügt uns nicht.

Nach dem heutigen Stand ist Extreme Networks der einzige Anbieter cloudbasierter Managementsysteme der für seine Informationssicherheits-Managementsysteme (ISMS) nach **ISO 27001** zertifiziert ist. Und da diese Systeme permanent weiterentwickelt werden, unterziehen wir sie einer zyklischen Rezertifizierung.. Das jeweils aktuelle ISO 27001 Zertifikat kann direkt in XIQ eingesehen werden. Es garantiert einen sicheren Umgang mit den Daten unserer Kunden. Mehr Informationen finden Sie unter:

www.extremenetworks.com/company/legal/extremecloud-iq-privacy-policy/

Alle Daten werden verschlüsselt, unabhängig davon, ob sie gespeichert oder übertragen werden. Der Zugriff auf die Daten unterliegt vollständig der Kontrolle des Endbenutzers.

XIQ differenziert zwischen Control-, Management- und Dataplane. Das bedeutet, dass der Austausch zwischen Switches, APs und der Cloudinstanz ausschließlich Steuerungs- und Monitordaten umfasst. Die eigentlichen Nutzdaten verbleiben zu jedem Zeitpunkt im lokalen Unternehmensnetz.

XIQ verwendet geo-redundante, verteilte Rechenzentren, um Latenzen und die Verfügbarkeit der Dienste zu optimieren. Die Einrichtungen befinden sich in Nordamerika, Südamerika, Europa, Asien und Australien.

Das regionale Rechenzentrum für Deutschland wird in Frankfurt gehostet. Ein weiteres liegt in der Schweiz.

Amazon AWS war unsere erste Providerplattform. Mittlerweile haben wir uns emanzipiert und betreiben XIQ auch bei Google GCP und Microsoft Azure. Alle diese Anbieter bieten öffentliche Erklärungen zu SOC 1, 2, 3, PCI, ISO und anderen Konformitäten, die an folgenden Stellen überprüft werden können:

- https://aws.amazon.com/compliance/programs/
- https://cloud.google.com/security/compliance/offerings/
- https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-home

XIQ erfüllt die europäischen Datenschutzbestimmungen durch Einhaltung der Richtlinien für geografische Daten. Das in Europa ansässige

Rechenzentrum führt eine datenübergreifende Replikation ausschließlich innerhalb der Europäischen Region durch, um die EU-Datenschutzbestimmungen und die DSGVO / GDPR zu erfüllen.

Das Lizenzmodell

Kosten-Nutzenanalyse

Das innovative, flexible Architekturmodell erlaubt es uns die effiziente Cloudnutzung in Form einer reduzierten TCO (total cost of ownership) an unsere Kunden weiterzugeben. XIQ bietet eine OPEX-Einsparung von 30% im Vergleich zu anderen Lösungen.

Extreme bietet eine wertbasierte, abgestufte Lizenzierungsstruktur. Einfach und portabel bietet diese unseren Kunden die Flexibilität, Lizenzen basierend auf Budget und IT-Anforderungen zu beziehen. Ein Upgrade auf höhere Funktionsebenen kann einfach implementiert werden. Alle Lizenzen sind unabhängig von Gerätetyp und Modell.

Subscription - SaaS

Der Wandel ist – sogar über die Grenzen der IT hinaus – zu beobachten. An die Stelle eines einmaligen Kaufpreises treten Subscription Modelle, die für einen definierten Zeitraum die Nutzung einer Lösung erlauben. Was im KFZ-Leasing mittlerweile Gang und Gäbe ist, erscheint bei Software auf den ersten Blick vielleicht befremdlich.

Szenarien, in welchen ein monolithisches Softwarepaket über Jahre ohne Update betrieben wird, treten mehr und mehr in den Hintergrund. Schon die konsequente Aufrechterhaltung eines hohen Sicherheitsstandards bedeutet aufwändige Arbeitszyklen, in welchen immer wieder geprüft und korrigiert wird. Komplexe Software entwickelt sich mehr und mehr zu einem quasi-organischen Konstrukt, das einer permanenten Aufmerksamkeit bedarf. Innovationen erweitern das Leistungsspektrum und die Effizienz eines Systems.

Mit einem wertorientierten SaaS-Lizenzmodell macht es Extreme noch einfacher, die technischen und kommerziellen Anforderungen abzudecken.

Wichtig ist, dass sich das XIQ-Modell transparent, portabel und für alle Produkte geräteunabhängig [Einzelkostenlizenz pro Gerät] darstellt.

Dies erleichtert Planung und Bestellung und gewährleistet vollständige Flexibilität nach dem Kauf. Die Laufzeit lässt sich in Jahren wählen, wobei Rabatte auf Mehrjahresabonnements gewährt werden.

Die folgenden XIQ-Lizenzstufen sind verfügbar:

XIQ Connect

Mit Connect steht allen Kunden eine kostenfreie Basisstufe zur Verfügung steht. Positioniert in der Public Cloud, steht hier ein solides Featureset fürs cloudbasierte Management bereit.

Zu den wichtigsten Connect-Funktionen gehören:

- Device Onboarding
- Geführte Konfiguration (Wizards)
- Zentrales Management
- Wi-Fi Planner
- Basic Monitoring Tools
- Essential Security (PSK, 802.1x, RADIUS)
- XIQ Connect Community Support

XIQ Pilot

Mit der nächsten – und populärsten – Leistungsstufe steigt die Flexibilität der Einsatzszenarien (Public Cloud, Private Cloud und Local Cloud) Infrastrukturverwaltung, Reporting und Remediation Tools bringen das Management auf eine profesionelle Ebene.

Und das sind – in Kurzform - die Funktionen, die mit der Pilot Lizenz freigeschaltet werden:

Dashboard/Scoreboard

Der schnelle Überblick für den Operator. Vom intuitiv erfassbaren Health-Index über Betriebsstatistiken bis hin zu - über kontextbasierte Filter aufbereiteten - granularere Darstellungen.

SD-WAN Router Support

Managen Sie SD-WAN-Router, mit denen Sie Zweigstellen und Remote- oder Home-Offices effizient mit Ihrem Unternehmensnetz verbinden können

Datenvorhaltung

Die bisher 30-tägige Vorhaltung von Messergebnissen, Events und Log-Informationen wurde nahezu unbegrenzt ausgeweitet. Das gibt Ihnen die Möglichkeit Trends und Entwicklungen Ihres Netzwerkes auch über sehr lange Zeiträume zu nachzuvollziehen.

ML Insights / Analytics

Erkennen Sie Herausforderungen, bevor diese sich auf Benutzer auswirken. Machine Learning unterstützt Sie bei der Fehlererkennung und -behebung.

Client 360 Data

Die vollständige Ansicht aller gesammelten Meta-Daten des Clientverhaltens. Dies vereinfacht die Beantwortung von Supportanfragen und verkürzt die Suche nach Fehlerquellen dramatisch.

Private Client Groups & Private PSK

Private-Pre-Shared-Keys (PPSK) ist eleganter als PSK und stellt eine einfache Alternative zu komplexen Identity Management Lösungen dar.

Private Client-Gruppen verwenden PPSK, um eine identitätsbasierte Mikrosegmentierung bereitzustellen

Network Policy

Wird benötigt, um Ihre verwalteten Geräte zu konfigurieren. Enthält alle wichtigen Konfigurationsobjekte wie drahtlose Netzwerke, Gerätevorlagen und viele zusätzliche Einstellungen

BLE Device Monitoring:

Ermöglicht verschiedene Analysen von Besuchern, deren Lokation und Anbindungen

Comparative Analytics

Der Vergleich Ihrer Installation mit anderen, ähnlichen Szenarien gibt Ihnen ein Gefühl der Dienstqualität Ihres WLAN. Informationen hinsichtlich der durchschnittlichen Bandbreite und der Clients pro AP sowie der Anzahl der Clients mit schlechter WLAN Anbindung werden hier anonym korrelliert.

Application Visibility & Control

Überwachen Sie die Nutzung von Applikationen insgesamt und pro Client mit Hilfe verschiedener Filter und Ansichten. So können Sie besser verstehen, wie Ihre Benutzer Ihr Netzwerk verwenden. Verbessern Sie Ihr Netzwerkdesign, indem Sie Aplikationsanforderungen mit einbeziehen.

Reporting

Das Reporting erstellt für Sie bei Bedarf Berichte bezüglich PCI 3.2, WIPS-Events und Nutzungsstatistiken. Diese hilfreichen Informationen lassen sich über einen Zeitplan automatisieren und weiter exportieren.

Troubleshooting

Verschiedene professionelle Tools unterstützen die Fehlersuche und -behebung. Zu den Tools gehören beispielsweise: Spektrumanalyse, Packet-Capture, Client-Monitoring, RADIUS-Testtool, VLAN-Test und vieles mehr.

Application Programming Interface

Voller Zugriff auf die RESTful-API. Mit dieser können Sie Aufgaben automatisieren und in Applikationen von Drittanbietern integrieren. Beispiele hierfür sind: Automatisches Generieren von PPSKs (Beispiel: Selbstregistrierung für Gäste), Weiterleiten von Standort- und Präsenzdaten an Analysetools von Drittanbietern. Informationen über verwaltete Komponenten und Clients lassen scih ebenfalls automatisch exportieren..

Die XIQ Pilot Subscription bietet eine RTU-Lizenz (Right to Use) für alle XIQ-Anwendung, einschließlich Funktions- und Wartungsversionen, sowie die Unterstützung des hauseigenen Global Technical Assistance Centers (GTAC) von Extreme Networks. Mehrwertdienst- und Supportoptionen für die verwalteten Geräte (d. H. AP, Switch) sind verfügbar und umfassen eine TAC / OS-Supportoption sowie eine Option zum erweiterten Hardwareaustausch, die in verschiedenen Service Leveln verfügbar ist.

Erstellen Sie Ihren Wartungsplan à la carte – so wie es Ihren Geschäftsanforderungen am besten entspricht.

Die ExtremeCloud IQ Pilot Public Cloud Subscription (Service #: XCIQ-PIL-S-C-EW) beinhaltet ein einjähriges Pilot Saas-Abonnement und ExtremeWorks SaaS-Unterstützung für ein (1) Gerät.

Und was geschieht, wenn die Subscription ausläuft? Keine Sorge, der LAN/WLAN Betrieb läuft in jedem Fall weiter. Lediglich Änderungen der Konfiguration sind nicht mehr möglich.

XIQ Co-Pilot

In Zukunft erhält der Administrator Unterstützung durch den Co-Pilot. Diese weiterentwickelte Stufe unterstützt künftig sowohl Public- als auch Private Cloud-Installationen und liefert zusätzliche Tools für maschinelles Lernen, Unterstützung für mehrere Clouds, automatisierte Korrekturen, Konfigurationen und Softwareverwaltung.

Beispielsweise reduziert die Funktion "Instant Context " die für Supportanrufe erforderlichen Aktivitäten auf ein Minimum. Ein ML-induziertes, intelligentes Support-Chat-Fenster ermöglicht das Zusammenstellen von Echtzeit- und Verlaufsinformationen zu einem Device oder Client durch Eingabe oder via Drag & Drop-Funktionalität.

Zu den wichtigsten Funktionen von Co-Pilot gehören:

- Supervised ML Insights and Tuning
- Automated Bug Fixes
- ML Issue Remediation
- Automated RMA
- Advanced NAC Integration
- Multi-Cloud Support

Auto-Pilot – Die KI übernimmt

Mit dem Projekt Auto-Pilot arbeiten wir momentan an der fortschrittlichsten und funktionsreichsten Lizenzstufe von XIQ.

Als Unterstützung in Public- und Private-Cloud Szenarien setzt Auto-Pilot modernste KI-Technologie ein, um die Netzwerkperformance weiter zu optimieren. So ist Ihr Unternehmen auch für die zunehmend komplexen Anforderungen durch IoT gerüstet.

Der Auto-Pilot trifft selbständig Entscheidungen. Er initiiert den Austausch eindeutig defekter Komponenten (Auto-RMA), betreibt eigenständig

Feintuning der Konfiguration (z.B. Auto-DFS) oder behebt bekannt gewordene Fehlfunktionen (Auto-BugFix).

Funktionale Erweiterungen liefern künftig Situationsbewertungen und Trendbeobachtungen zur Unterstützung in Administration und Qualitätssicherung.

Zu den wichtigsten, kommenden Auto-Pilot-Funktionen gehören:

- AI Configuration
- AI DFS Optimization
- AI-Driven Quarantine
- AI Segmentation
- AI Anomaly Detection
- AI WIPS

Das klingt zunächst nach dem klassischen Horrorszenario, das Science-Fiction Autoren gerne bemühen. Nein, wir streben nicht nach der Weltherrschaft! Bleiben wir ernst: Wer schon einmal eine WLAN Infrastruktur zwischen Flurfördersystemen, beweglichen Hochregalen und jeder Menge mehr oder weniger hochwertigen Clients austariert hat, der weiß, wie zeitaufwändig sich Troubleshooting und Feintuning gestalten.

Machine Learning arbeitet mit komplexen Vektormodellen und Technologien die aus der Spracherkennung entlehnt sind. Diese, vergleichsweise winzigen, Datenpunkte werden in Relation zueinander gesetzt, um Verhaltensmuster zu erkennen. Vollständig anonymisiert, können diese Muster aus allen Cloudinstanzen heraus korreliert werden. Wie hilfreich wäre so eine Meldung: „Hallo Admin, in Halle 19, Nordostecke nimmt die Verbindungsqualität zu mobilen Geräten immer wieder signifikant ab. Interferenzen weisen auf eine Störquelle hin. Liebe Grüße, Deine K.I.“

Nun, ganz so weit sind wir noch nicht, aber wir arbeiten daran.

Das Look and Feel

Eine Lösungsübersicht ist stets ein Balanceakt. Sinnfrei ist, das Benutzerhandbuch mit allen Features und Funktionen nochmal zu schreiben. Ein Zweiseiter bietet dagegen zu wenig Tiefe. Trotzdem sollen einige essentielle Funktionen von XIQ an dieser Stelle beschrieben werden:

Kontextbasierte Visualisierung

360° ist das Synonym für den uneingeschränkten Rundumblick; daher taucht diese Zahl in den Menüs des Machine Learning immer wieder auf.

Mit der kontextbasierten Darstellung des Netzwerks, einschließlich aller verbundenen Benutzer, Geräte und Anwendungen bietet XIQ ein vollständiges Bild von Leistung, Zustand und Sicherheit aller Benutzer und Geräte in ihrer Infrastruktur.

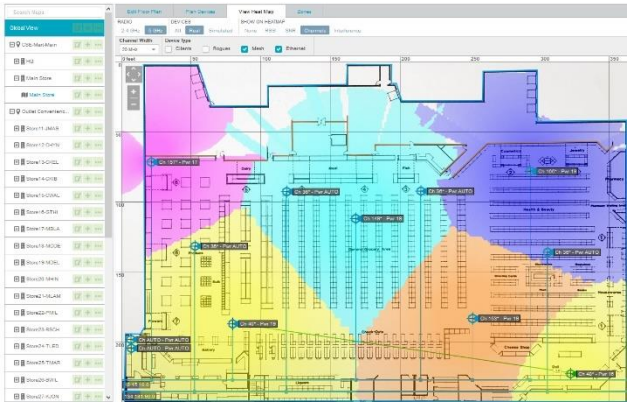
Schon heute fassen die Lernalgorithmen Informationen und Betriebsdaten in Qualitätsindices zusammen. Um eine solche Scorecard zu lesen, ist kein Informatikstudium erforderlich. Ein Verfügbarkeitsgrad von z.B. 72% sollte zumindest Anlass geben, die Ursache genauer zu untersuchen um das Problem zu lösen. Und zwar bevor sich Unmut bei den Nutzern des Netzes breit macht.

Network 360 PLAN

„Network 360 PLAN“ visualisiert Gebäudepläne. Heatmaps (RSSI, SNR, Interferenz) und Kanalpläne stehen für echte oder simulierte AP‘S (z.B. Planung eines Standorts) zur Verfügung, um die tatsächliche Ausleuchtung mit möglichst realistischen Umgebungsparametern zu simulieren oder zu überprüfen.

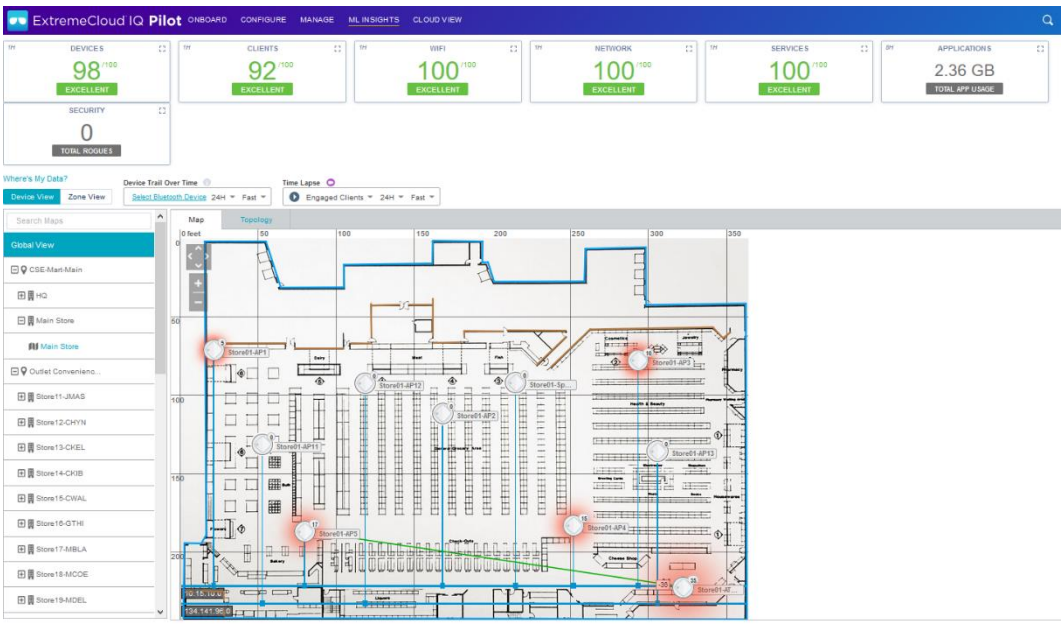
Network 360

„Network 360“ verarbeitet und analysiert schnell große Datenmengen, um den qualitativen Zustand des Netzwerks sowohl als Momentaufnahme als auch in der Vergangenheit darzustellen.

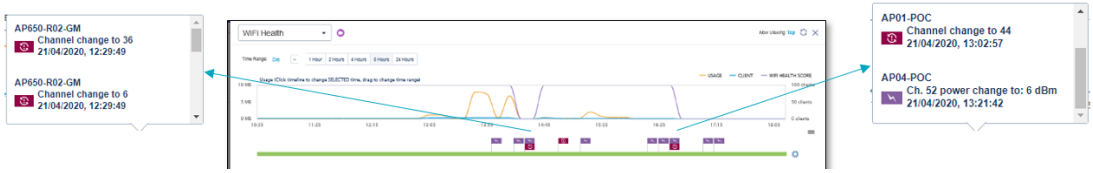


Verfolgen Sie beispielsweise die Last des AP-Clients über einen Zeitraum oder überwachen Sie den allgemeinen Gesundheitszustand Ihres Netzwerks. Bei Bedarf können Sie schnell agieren und auf detailliertere Informationen zugreifen.

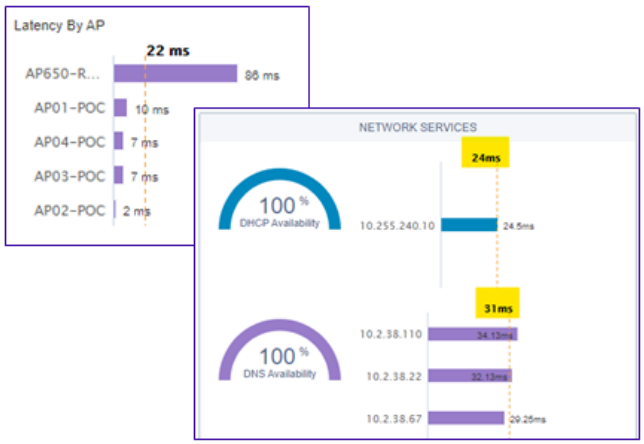
Network 360 bietet außerdem detaillierte Informationen zum automatischen Wechsel von Kanälen oder zur Sendeleistung der Wireless Infrastruktur.



In sehr dynamischen RF-Umgebungen werden Änderungen über die einen Zeitstrahl erfolgt; das vereinfacht die Erkennung von Änderungsmustern und hilft dabei, Verhaltensanomalien zu verstehen.

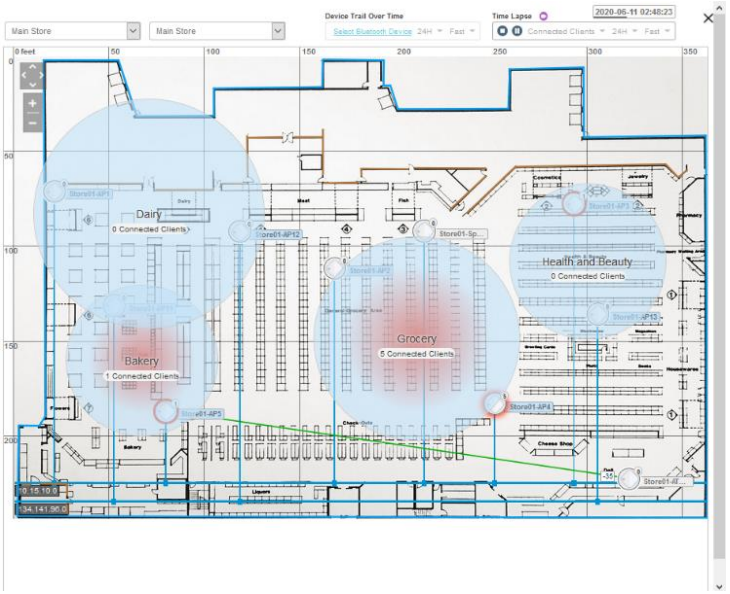


Network 360 liefert Berichte zu wichtigsten Netzwerkdiensten [DNS, DHCP, RADIUS]. Informationen über Latenzen im Netz stellen einen nicht zu unterschätzenden Wert bei der Ermittlung und Behebung von Qualitäts- und Performance-verlusten dar.

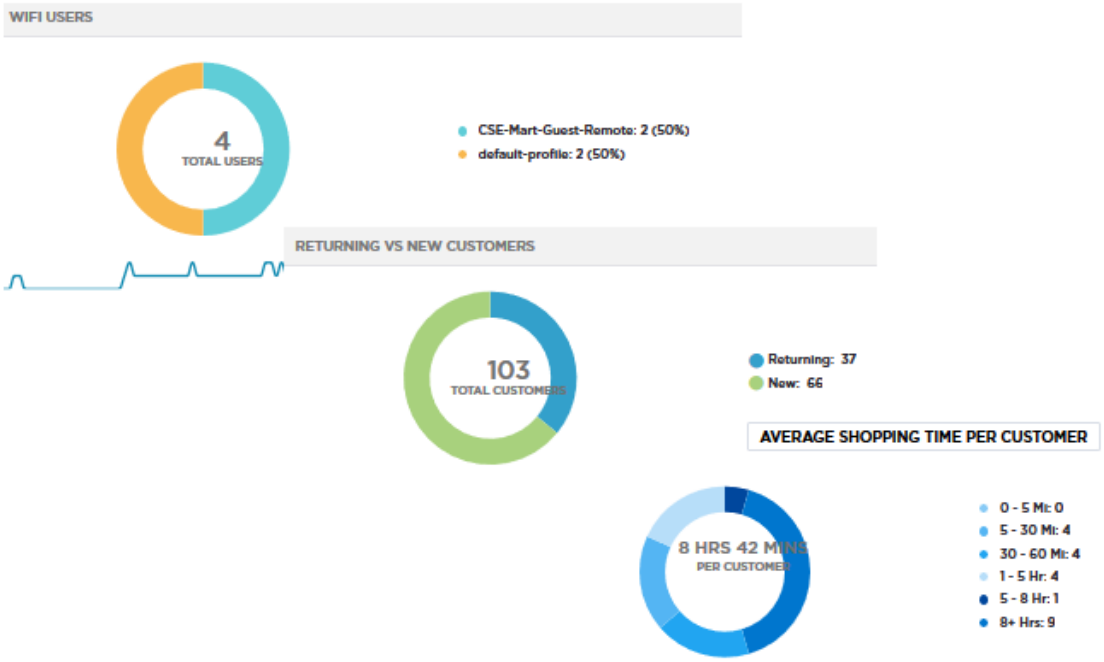


Retail Dashboard

Dieses sehr spezifische Dashboard dient an Veranstaltungsorten oder in Shops zur Ermittlung der Besucherdichte in verschiedenen Zonen. So kann die Konzentration von Personen kombiniert mit der durchschnittlichen Verweildauer in diesen Bereichen abgelesen werden. Diese Information stellt gerade für die Marketingabteilung einer Organisation einen erheblichen Mehrwert dar.

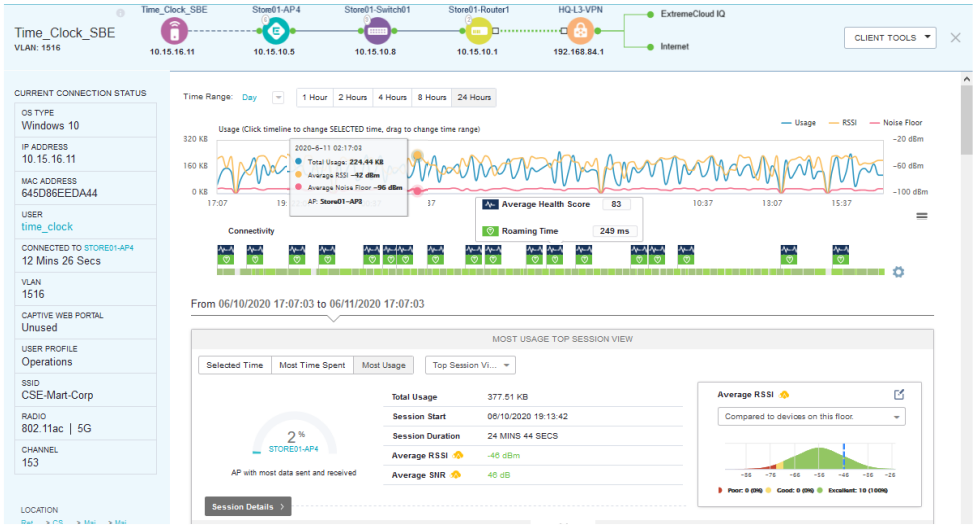


Während z.B. eines Events liefert ein solches Dashboard eine Fülle von Informationen über die Anzahl der Kunden, ihre durchschnittliche Verweilzeit sowie die Zonen, in denen sie die meiste Zeit verbracht haben.



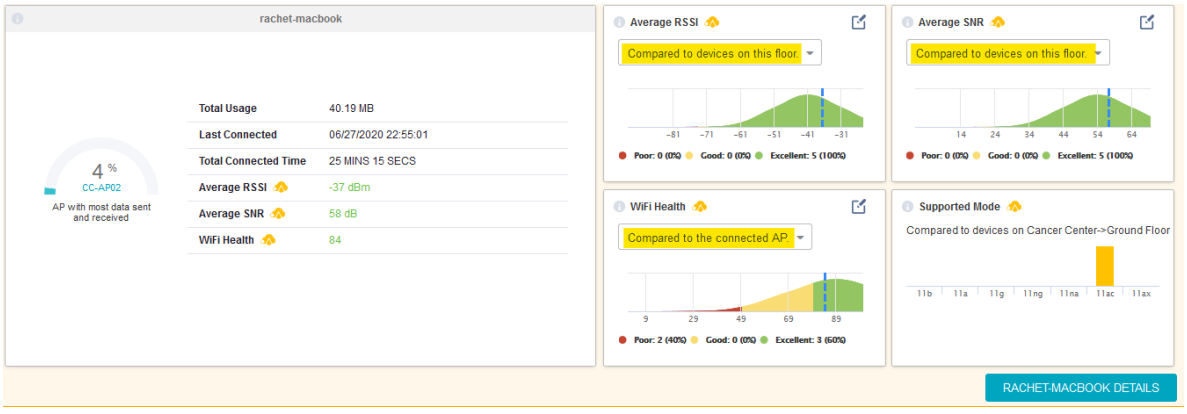
Client 360

Die Analyse des Fußabdrucks von Endgeräte resultiert in der “Total Client Experience”, beschreibt also die Dienstqualität in Echtzeit wie auch in historischer Darstellung. Informationen zum Bewegungsprofil, Top-10-Anwendungen oder Clientfunktionen ermöglichen die schnelle Behebung eines – möglicherweise subjektiv noch gar nicht wahrgenommenen - Qualitätsverlusts im WLAN.



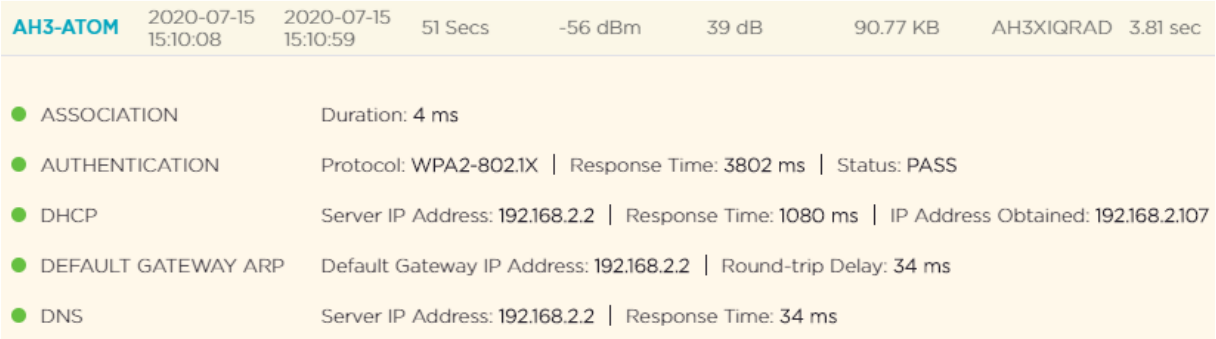
Die sogenannten Client Health Metrics visualisieren Vergleichswerte zu koexistierenden Endsystemen am selben AP oder in derselben Zone. Mit dieser Intepretation lässt sich differenzieren, ob Symptome von der Infrastruktur bzw. dem räumliche Umfeld hervorgebracht werden, oder ob das Problem beim Client selbst liegt.

Dieser hilfreiche Referenzbericht wird bereits heute vom Machine Learning bereitgestellt.



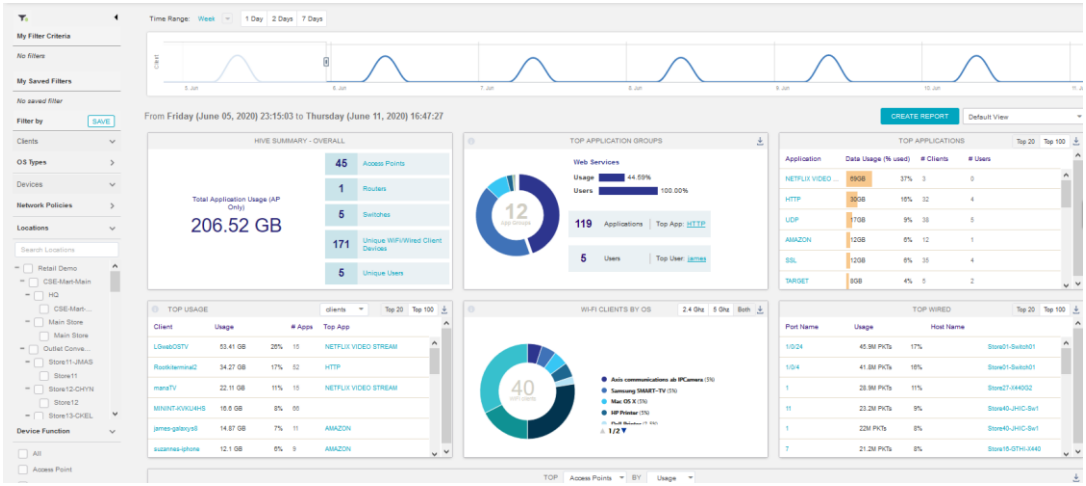
Client Trail

Diese Trackingfunktion protokolliert alle relevanten Events eines Endgerätes. Von der Assoziierung über Authentisierungsabläufe, DHCP/DNS, Roaming und Signalqualität (SNR/RSSI) bis hin zu Datennutzungsparametern lässt sich hier das Kommunikationsverhalten eines Clients im WLAN verfolgen.



High-Impact Dashboards

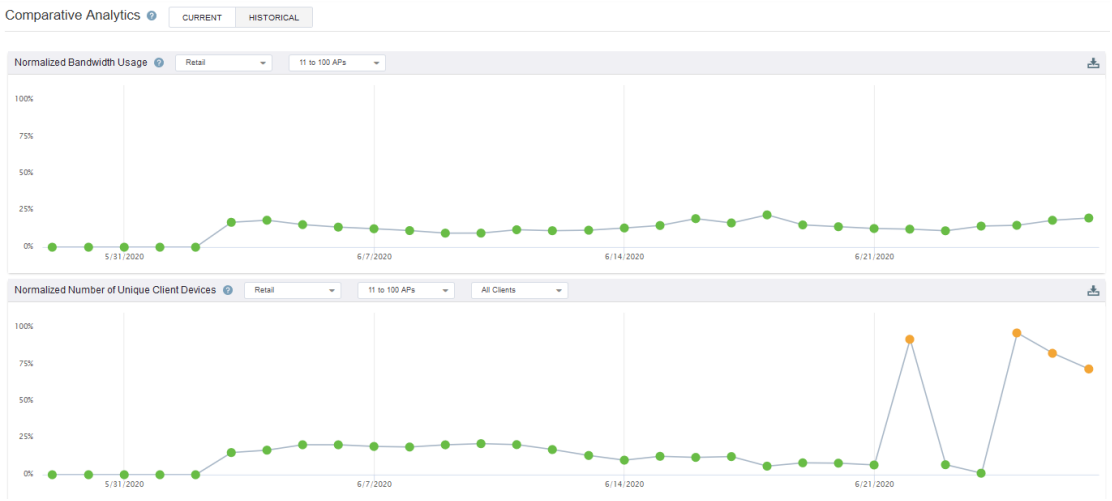
Konsolidierte Dashboards bieten sich, übersichtlich und mit detaillierten Filterfunktionen versehen, als Analysewerkzeug an. Das Spektrum umfasst unter anderem die App-Nutzung, den Client-Betriebssystem-Mix, Top-Nutzer, Top-Clients, Gerätetypen und -nummern. Der Datenhorizont liegt dabei bei 90 Tagen.



Comparative Analytics

Die Qualität eines Netzwerkes hängt nicht nur von der Infrastruktur, sondern natürlich auch vom Verhalten der Clients und nicht zuletzt von zahlreichen Umgebungsfaktoren ab. Aber wie gut ist das WLAN eigentlich? „Comparative Analytics“ bietet vergleichende Einblicke in die Qualität des eigenen Netzwerks in Relation zu ähnlichen Installationen anderer Kunden von Extreme Networks innerhalb desselben Branchentyps oder auch anderer Branchen. Auch diese Form der Analyse wird ausschließlich auf Basis von anonymisierten Metadaten durchgeführt. Bei Bedarf lässt sich die Vergleichsfunktion vollständig deaktivieren.

Erkennt der Administrator anhand dieser Analyse beispielsweise signifikant hohe Endsystemdichten pro Access Point, so kann gezieltes Hinzufügen oder ein Upgrade auf leistungsfähigere AP Modelle in diesem Bereich die Qualität bei optimalem Kosten-Nutzenverhältnis verbessern.



Cloud View

Das Dashboard „Cloud View“ zeigt Größe & Umfang der kollektiven Intelligenz für XIQ. Auf dieser Ansicht wird die Größe und globale Leistungsfähigkeit von XIQ dargestellt. Dabei werden die Anzahl der aktiven virtuellen Instanzen, verwalteten Geräte, cloudbasierten Private Pre-Shared Keys und aktiven Clients sowie die Karte der größten Gerätepools angezeigt.

WLAN - Ein Blick unter die Haube

WLAN muss sich einfach anfühlen. Finden, Anmelden, Loslegen. Dabei vergessen wir gerne, wie komplex es unter der hübsch lackierten Motorhaube aussehen muss, damit diese Technologie nicht nur einfach zu handhaben, sondern auch absolut zuverlässig und sicher ist.

Ohne Anspruch auf Vollständigkeit betrachten wir an dieser Stelle einige neue Techniken, welche den Spagat zwischen einfach und anspruchsvoll ermöglichen.

Private Pre-Shared Key (PPSK)

Das Preshared Key Modell ist als einfache Authentisierungs- und Verschlüsselungsmethode hinreichend bekannt. Für den privaten Gebrauch gut geeignet, ist PSK im professionellen Umfeld eher umständlich zu handhaben.
Vor allem wenn das Geheimnis des Schlüssels kompromittiert wurde, muß dieser auf allen betroffenen Geräten neu konfiguriert werden.
Es gibt sicher sinnvollere Aufgaben für das IT Team.

Mit PPSK lassen sich alle Geräte (ob unternehmenseigen oder im Besitz von Mitarbeitern / Besuchern) schnell, einfach und sicher mit dem WLAN verbinden und administrieren. Dabei wird eine gemeinsame Authentifizierungstechnologie verwendet,

für die auf Clientseite keine Software erforderlich ist. Vor allem die schlichteren Gemüter unter den mikrocontrollerbasierten IoT-Geräten, deren Sicherheitslevel oft recht niedrig liegt, lassen sich so leichter und sicherer handhaben. Die PPSK-Technologie von Extreme Networks ist also mit jedem Wi-Fi-Client kompatibel, der Pre-Shared Key (PSK) unterstützt.

Sie ermöglicht es der IT, Sicherheit auf 802.1X-Level mit weniger Komplexität und ohne den sonst notwendigen Overhead zu replizieren.

- Alle Benutzer und Geräte verfügen über eindeutige Anmeldeschlüssel
- Mehrere Benutzerprofile können mit unterschiedlichen Schlüsseln mit einer einzigen SSID verknüpft werden
- PPSK-Benutzergruppen können genutzt werden, um unterschiedliche Benutzergruppen oder Geräte unterschiedlichen Regelwerken zuzuweisen
- PPSK kann damit auch die Funktion eines einfachen Gastzuganges erfüllen. Wobei ein Gästeportal natürlich einige komfortable Mehrwerte mit sich bringt – und so etwas aufzubauen und zu pflegen ist heutzutage ja auch kein Hexenwerk mehr.

IOT – Device Management mit PPSK in einer einzigen SSID

XIQ bietet zwei Arten von PPSK-Anwendungen zur Auswahl:

Local PPSK

- Lokale PPSK-Clients werden über die zentrale Oberfläche administriert, aber lokal auf jedem XIQ AP gespeichert. Die Tabellen sind auf 10000 Einträge ausgelegt.

Cloud PPSK

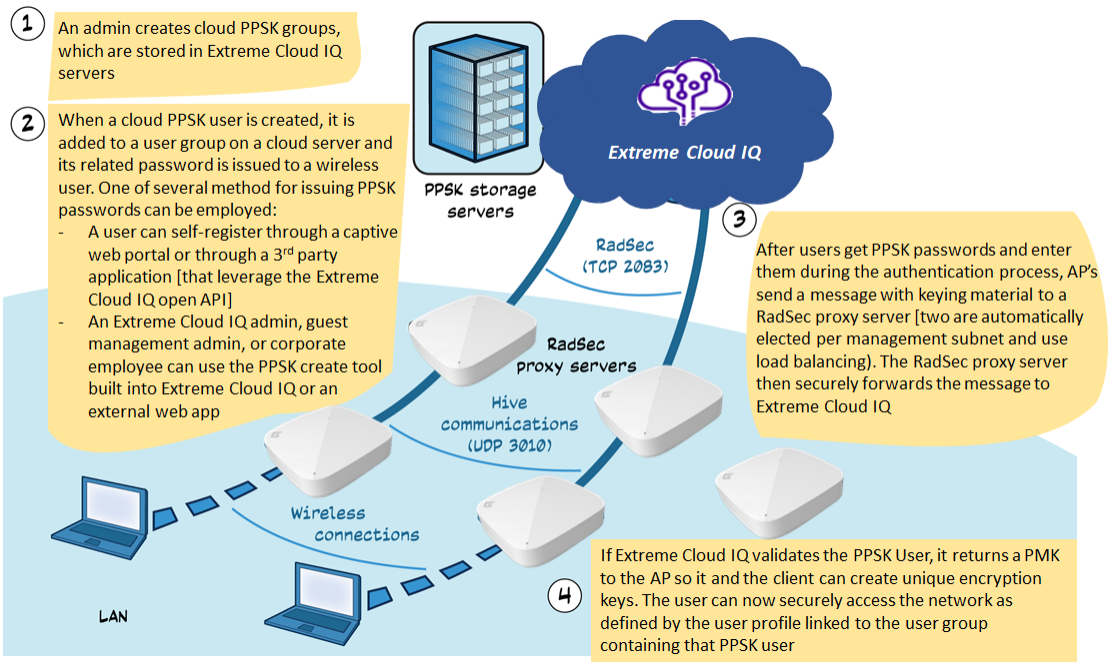
- Cloud PPSK-Benutzer werden in ExtremeCloud IQ verwaltet und gespeichert.
- Ein XIQ-Administrator erstellt PPSK-Benutzergruppen, die in der Cloud gespeichert sind;

- Anschließend erstellen XIQ-Administratoren, Empfangsmitarbeiter, Unternehmens-Mitarbeiter oder sogar Netzwerkbenutzer selbst PPSK-Benutzer. XIQ fügt diese den Gruppen hinzu und verwaltet sie in PPSK-zu-MAC-Adress-Zuordnungs-Tabellen.
- Jede XIQ-Umgebung kann weitaus mehr als die 10.000 lokal gespeicherten PPSK verwalten. Mögliche Grenzen werden lediglich durch die Datenbankarchitektur gesetzt – in der Praxis wurde hier noch keine Limitierung erreicht und beobachtet.

Während die Authentisierung bei Local PPSK direkt auf dem jeweiligen AP abläuft, erfordert die Cloud PPSK Variante eine sichere Kommunikation zwischen AP und Cloud. Dazu wird das Standardprotokoll RADSec (RADIUS-Datagramme über TCP und TLS) verwendet.

RADSec etabliert eine sichere RADIUS-Kommunikation zwischen den Access Points einer Site und der XIQ Management Instanz. Als RADSec-Proxyserver fungiert ein AP, der ausgewählt wird, um PPSK-bezogene RADIUS-Kommunikation für lokale ExtremeCloud-APs im selben Management Subnet über RADSec auf TCP-Port 2083 an das XIQ-Management weiterzuleiten.

Jedes Management Subnet verfügt über zwei RADSec-Proxyserver, welche mittels Load Balancing die Arbeit untereinander verteilen.



Cloud PPSK Architecture

Das Speichern von PPSK-Benutzern in einem zentralen Repository in der Cloud anstelle von APs selbst bietet zahlreiche Vorteile:

- Die XIQ Services-Plattform unterstützt weitaus mehr PPSK-Benutzer als ein einzelner Access Point.
- Benutzer können PPSKs an mehreren Standorten mit identischer SSID verwenden. Da Cloud-PPSK-Benutzer an einem zentralen Ort gespeichert sind und von überall aus auf sie zugegriffen werden kann,

können sie von jedem Ort verwendet werden, der seine SSID mit derselben PPSK-Benutzergruppe verknüpft. Diese Methode skaliert ausgezeichnet mit Cloud PPSK, bei Local PPSK werden die Tabellenlimits naturgemäss früher erreicht.

- Benutzer können sich über ein firmeneigenes Webportal oder eine Drittanbieteranwendung [mithilfe der offenen XIQ-API] selbst registrieren. Captive-Webportale und die Guest Management-Webanwendung können zusätzlich die Zustimmung von Mitarbeitern oder Managern einfordern, bevor ExtremeCloud IQ PPSK-Kennwörter an selbst registrierte Benutzer sendet.
- Für das Erstellen, Ändern und Löschen von Cloud-PPSK-Benutzern und Benutzergruppen sind keine AP-Update Prozesse erforderlich.

Ersetzt PPSK das 802.1x-Modell?

Nein, die standardbasierte Authentisierung nach IEEE ist eine seit Jahren bewährte und für den professionellen Einsatz im Unternehmen in jedem Fall vorzuziehende Lösung. Alleine schon die Tatsache, dass PPSK eine, auf die WLAN Infrastruktur beschränkte Lösung ist, während sich 802.1x in LAN und WLAN nahtlos eingliedert ist der lebende Beweis dafür.

PPSK ist die Lösung für alle Endsysteme die sich mit einer „richtigen“ Authentisierung im WLAN einfach schwer tun. Oder in Szenarien die den Aufwand für entsprechende Authentisierungsinstanzen nicht gestatten.
Die Entscheidung für eine Authentisierungsmethode hängt immer von den Rahmenbedingungen ab. Auch hier beraten wir Sie gerne.

Application Programmable Interface (API)

XIQ bietet eine vollständige Suite von Cloud-optimierten, offenen APIs, die es ermöglichen Anwendungen anzupassen und Integrationen mit anderen Systemen ermöglichen.

Der kontinuierliche Integrationsprozess umfasst auch existierende Lösungen aus dem Portfolio von Extreme Networks wie WLAN Controller, das Extreme Management Center und Extreme Control.

Zero Touch Provisioning

Wie anfangs bereits erwähnt, bietet XIQ ein Zero-Touch Deployment Modell welches nicht nur die ersten Schritte stark vereinfacht; auch umfangreiche Roll Out Aktionen lassen sich mit minimalem Aufwand realisieren.

Ohne jede Vorkonfiguration kann ein Switch oder AP mit dem Netz verbunden werden. Einzige Voraussetzung ist selbstredend ein Internetzugang. Vordefinierte und adaptierbare Device Templates sorgen für eine automatische Grundkonfiguration.

Initiale Firmwareupdates und Konfigurationsangleichungen erfolgen automatisch. Individuelle Einstellungen lassen sich an Einzelgeräten, aber auch auf Basis von Gerätegruppen und Standorten vornehmen.

Updates und Upgrades

Die XIQ Wireless Infrastructure Management Plane ist in der Lage, während des Betriebes Funktionen und Merkmale hinzuzufügen, ohne dass ein Wartungsfenster vorgesehen werden muss.

Die Microservice Architektur etabliert neue Features, Funktionen und Verbesserungen, ohne dass ein Eingreifen auf Betreiberseite notwendig wird.

Der Neustart eines Accesspoints oder Switches nach einem Firmwareupdate ist nach wie vor unumgänglich. Es liegt jedoch in der Entscheidung des Administrators, ob ein Update flächendeckend, standortweise oder in Gruppen erfolgt. Bei ausreichender AP Dichte lassen sich auf diese Weise unterbrechungsfreie Updates erzielen.

Die Rolle des Clients ist für den reibungslosen Betrieb nicht unerheblich. Um beispielsweise auftretende Treiberprobleme spezieller Clients zu umgehen, kann auch die Firmwareversion durch den Administrator bei Bedarf frei gewählt werden.

Cooperative Control Architecture

Die Orchestrierung macht aus einem Haufen Accesspoints eine gutgeölte Maschine deren Komponenten reibungslos zusammenarbeiten – die Grundlage für eine perfekte User Experience.

XIQ Access Points arbeiten mit kooperativen Steuerprotokollen und -funktionen, welche alle Vorteile einer controllerbasierten WLAN-Lösung bieten, ohne dass ein Controller oder ein Overlay-Netzwerk erforderlich ist.

Dieser Umstand vereinfacht die Strukturen vor Ort, senkt die Kosten und ist vor allem für Voice-over-Wireless-LAN besser geeignet als gängige, controllerbasierte Architekturen.

Die kooperative Steuerung gruppiert mehrere XIQ APs in sogenannten „Hives“. Die lokale Koordination optimiert das schnelle Roaming, koordiniertes RF-Management, Sicherheit und Quality of Service (QoS) wie auch Mesh-Vernetzung.

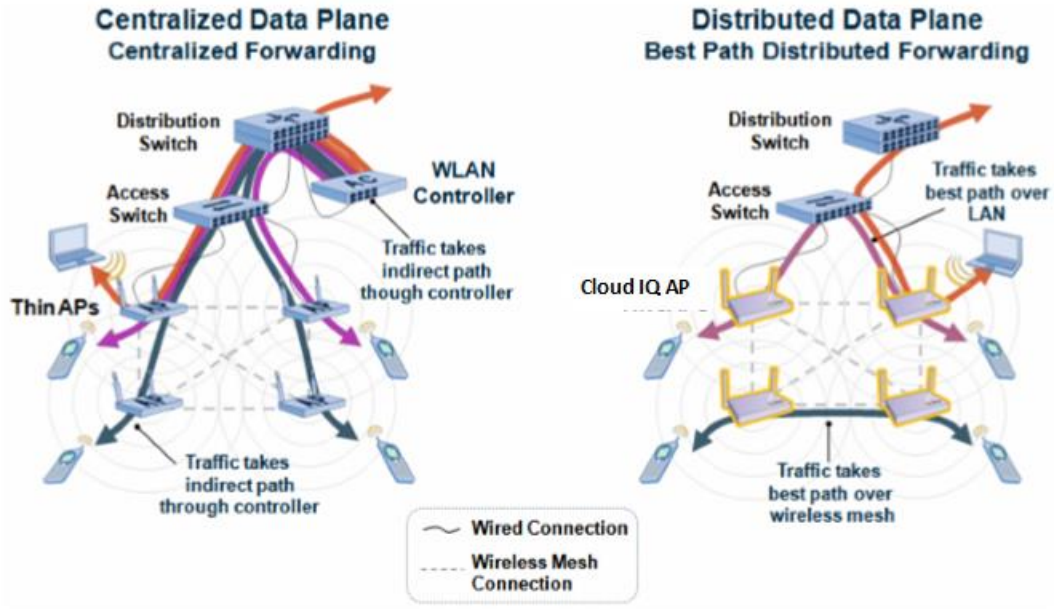
Die kooperative Steuerungsarchitektur wird mit den folgenden selbstorganisierenden kooperativen Steuerungsprotokollen ermöglicht:

AMRP (Aerohive Mobility Routing Protocol)

Dezentrale Kooperation ist der Schlüssel zu einer dynamischen und situationsangepassten Wegeführung in lokalen Segmenten. Zusammengefasst im Aerohive Mobility Routing Protocol AMRP, nutzen Routingalgorithmen den jeweils optimalen Pfad auf Layer 2 und 3. Basierend auf der Anzahl notwendiger Hops und Pfadkosten werden Wege über LAN, aber auch über Meshing Links dynamisch berechnet und im Netz propagiert.

Dabei übt AMRP eine bewusste Selbstkontrolle aus: Um den Broadcast Traffic wie auch die Routingtabellen in einem überschaubaren Maß zu halten, strukturiert sich das WLAN innerhalb großer Installationen in sogenannte Self-Contained-Areas.

Die folgende Grafik veranschaulicht elementare Unterschiede zwischen klassisch zentralisierter und verteilter Architektur.



Betriebskonzepte mit einheitlicher Control und Data Plane leiten den Traffic stets durch die zentralen Controllerkomponenten. Dies hat natürlich den Vorteil eines sehr klar definierten Gefahrenüberganges.
Berücksichtigen wir jedoch steigende Komplexität und Nutzungsintensität der WLAN Infrastruktur, so führt diese Form der Konzentration unweigerlich zu einem potentiellen Flaschenhals. Lässt sich Durchsatz mit dem ensprechenden Aufwand kompensieren, kann eine Erhöhung der Latenz durch die Nutzung zahlreicher Hops nicht einfach wegdiskutiert werden.

Extreme Cloud IQ operiert mit einer zentralen Management Plane, Control und Data Plane bleiben jedoch da, wo sie hingehören. Das optimiert nicht nur die Wegeführung; mit dieser Maßnahme stellen wir auch sicher, dass Nutzdaten das lokale Netzwerk nicht verlassen – ein signifikanter Sicherheitsfaktor.

Jede WLAN Komponente trägt also aktiv zur Steuerung und Kontrolle der Infrastruktur bei. Ähnlich wie im Gridcomputing wächst die Gesamtleistung kontinuierlich mit der Größe. Das sorgt für eine nahezu grenzenlose Skalierung, hohe Verfügbarkeit und die effiziente Nutzung des IT Budgets.

WLAN Clients können nahtlos zwischen Cloud-IQ-APs wechseln, während der Session State, die Firewall-Zugriffsrechte und die QoS-Durchsetzungseinstellungen beibehalten werden.
AMRP ermöglicht schnelle Roaming-Funktionen, mit denen Clientstatus- und Verschlüsselungsschlüsselinformationen vorausschauend und sicher verteilt werden. So können wireless Clients nahtlos zwischen Cloud IQ-APs wechseln und gleichzeitig den Authentifizierungsstatus, die Firewall-Zugriffsrechte und die QoS-Einstellungen beibehalten, ohne die Session zu verlieren.

DNXP (Dynamic Network Extension Protocol)

Bietet ein Mobilitätsframework, um die Erweiterung von Layer-2-Netzwerken über Layer-3-Routing-Domänen zu ermöglichen. Dies ermöglicht Funktionen wie nahtloses Layer-3-Roaming und dynamisches Tunneln zu Remote-Netzwerken basierend auf der Identität eines Clients oder des Service-Set- Identifier (SSID). Innerhalb eines Subnetzes kann DNXP Cloud IQ-APs automatisch auswählen, die für die dynamische Erstellung von Tunnelpfaden zwischen Cloud IQ-APs in verschiedenen Subnetzen verantwortlich sind. Im Wesentlichen bietet DNXP Tunnelerweiterungen zwischen Netzwerken, die in Verbindung mit AMRP zum Austausch von Identität und Schlüsselinformationen arbeiten. Auf diese Weise können Clients nahtlos zwischen Subnetzen wechseln und dabei die IP-Adresseinstellungen, den Client-Sessionstatus, die Firewall-Zugriffsrechte und die QoS-Einstellungen beibehalten.

Identity-Based Dynamic Network Extension (DNX)

Mobilität in einem IP-Netzwerk ist eine Herausforderung, da sich die IP-Einstellungen ändern, sobald Sie von Subnetz zu Subnetz wechseln. Extreme Networks hat das Dynamic Network Extension Protocol (DNXP) entwickelt, damit Benutzer ihre IP-Einstellungen und Netzwerkverbindungen beim Roaming über Subnetze in einem WLAN beibehalten können.

Die gleiche Technologie, welche XIQ zum Layer3 Roaming befähigt, kann auch genutzt werden um WLAN Clients – basierend auf ihrer Identität - zu einem AP in einem anderen Netzwerk zu tunneln.

Nach erfolgreicher Authentisierung wird dem Client per RADIUS Attribut ein Userprofil zugewiesen. Dieses definiert nicht nur Firewall-, VLAN- und QoS Regeln, es kann auch die DNX Funktion steuern.

Auf diese Weise wird dem authentisierten Client – bei Bedarf - zusätzlich ein GRE-Tunnel zu einem Remote AP in einem völlig anderen Netzwerk zugewiesen.

Sicherheits- und QoS Policies greifen bereits lokal; dies ist besonders wichtig für Clients, die z.B. VoWLAN-Anwendungen (Voice over WLAN) verwenden. Der Datenverkehr selbst wird jedoch zu einer Remote Site umgeleitet. Ein probates Mittel um virtuelle Teams bei Bedarf auch auf Netzwerkebene zusammenzubringen.

Die Layer3-Funktionalität optimiert die Performance nach dem Roaming. Wechselt der Client mit aktiven Sitzungen zu einem CloudIQ AP in einem anderen Subnetz, behält er seine IP-Adresse solange bei, wie Sitzungen seine Sessions noch aktiv sind. Sind die Sessions abgeschlossen, kann der Client optional veranlasst werden, im neuen Netz eine lokale IP anzufordern. Dieses individualisierte Timing gestaltet den Netzwechsel elegant und unterbrechungsfrei.

ACSP (Aerohive Channel Selection Protocol)

Wird von Cloud IQ-APs verwendet, um die Funkwellen zu analysieren und gemeinsam die besten Funkkanaleinstellungen für den Wireless Access und Wireless Mesh zu ermitteln. Um eine optimierte WLAN-Leistung zu

erzielen, vermeidet ACSP durch überlappende Funkkanäle entstehende Störungen.

Cloud IQ AP Auto Discovery & Self Organization

CloudIQ APs finden sich gegenseitig und erkennen, ob sie über ein wired oder wireless Netzwerk miteinander verbunden sind. Nachbarn mit gleichen Anmeldeinformationen für den selben VIQ oder mit gleichen Mobility-Credentials, können sich über LAN per AES und über WLAN per WPA mit AES-CCMP sicher miteinander verbinden.
Sind die Nachbarschaftsbeziehungen zwischen Cloud IQ-APs hergestellt greifen die schon beschriebenen kooperativen Steuerungsprotokolle, um nahtlose Mobilität, automatische RF-Steuerung und Ausfallsicherheit bereitzustellen. Liegen Nachbarn in unterschiedlichen Subnetzen oder sind sie anderen VIQs konfiguriert, werden IP Informationen ausgetauscht und eine Kommunikation über Layer3 Grenzen hinaus etabliert. Natürlich nur, wenn die CloudIQ APs mit denselben globalen Mobility Security Settings konfiguriert sind.

Zusammenfassend lässt sich sagen: Die kooperative Steuerung leistet einen essentiellen Beitrag zum sicheren und nahtlosen Wechsel von Clients, ohne die Datenübertragung oder Sprachverbindungen zu beeinträchtigen.

Cooperative RF control – Hochfrequente Flugsicherung

Viel hilft nicht immer viel! Mit steigender Dichte eskaliert der gegenseitige Einfluss direkt und indirekt benachbarter Access Points – vor allem wenn die die manuelle Kanalwahl eher unglücklich ausgefallen ist. Cloud IQ APs nutzen das Aerohive Channel Selection Protocol (ACSP)um die Kanalwahl in Kooperation auszutarieren. Informationen über erkannte WLAN Systeme werden dabei ebenso ausgetauscht wie Störquelleninformationen – als Ergebnis entstehen konsistente Kanalpläne. Auch in komplexen Meshing Szenarien sorgt ACSP für zuverlässige Uplinkverbindungen bei geringen Reibungsverlusten.

Die Orchestrierung der verfügbaren Kanäle ist ein kontinuierlicher Prozess. Ob spontan auftauchende Interferenzen die Kommunikation gefährden, oder ein leer geräumtes Lagerregal für veränderte Rahmenbedingungen in der Umgebung sorgt, ACSP ist in der Lage, die Infrastruktur dynamisch auf das neu entstandene Szenario abzustimmen.

Praktiker wissen: Diese Eigendynamik ist nicht immer gewünscht. In Umfeldern mit sehr sensiblen Clients kann die Kanaloptimierung auf den Moment getriggert werden, in welchem keine Clients eingebucht sind.

Software Selectable Radios

Alle ExtremeCloud IQ APs, die WiFi6 unterstützen besitzen neben den 5GHz Radios auch solche, deren Transmitter zwischen 2,4 und 5GHz umgeschaltet werden können. Grundlegend erlaubt das, in einer Umgebung mit hoher AP-Dichte die Anzahl aktiver 2,4 Radios bewusst zu reduzieren. Warum, ist einfach erklärt: In Relation zu 5GHz bietet das untere ISM Band eine etwas höhere Reichweite, beinhaltet aber nur drei, überlappungsfreie Kanäle. Eine AP Planung unter dem Gesichtspunkt

flächendeckender 5GHz Ausleuchtung bringt zwangsläufig Störeffekte (ACI/CCI) auf 2,4Ghz mit sich. Ein Dilemma, welches in der Vergangenheit fallweise durch bewusstes Abschalten jedes zweiten 2,4GHz Radios kompensiert werden musste.

ACSP nimmt sich auch dieser Problematik an. Basierend auf aktuellen, aber auch zurückliegenden Messwerten werden die APs automatisch auf den 2,4/5GHz oder den Dual 5GHz Mode eingestellt um die Umgebung optimal und so störungsfrei wie möglich auszuleuchten.

Eine Bemerkung an dieser Stelle: Auch hochrangige Fachleute der WLAN Branche haben oft eine eigene Meinung über den Einsatz von RF-Automatisierung. Ein statischer Abgleich von Kanälen und Sendeleistungen ist zeitaufwändig, kann aber – je nach Szenario – für langfristig stabile Verhältnisse sorgen. Aber – machen Sie das mal für eine Organisation mit zweitausend Standorten. Oder in einem Hochregallager, dessen Umgebungsbedingungen sich alle fünf Minuten dramatisch ändern. Hier hat die Dynamik selbstorganisierender Systeme eindeutig die Nase vorne.
Eine Polarisierung ist also nicht nötig! Alle haben Recht; es kommt eben aufs Szenario an.

Hochverfügbarkeit

Sehen wir es realistisch: Ob ein Netzwerk an irgendeiner Stelle einen Single Point of Failure aufweist, hängt von den Anforderungen und dem betriebenen Aufwand ab. Eine realistische Kosten/Nutzenabschätzung ist empfehlenswert um den Verfügbarkeitsbedarf an den richtigen Positionen optimal zu bedienen.

Extreme Cloud IQ trägt mit seiner verteilten Architektur zum resilienten Regelbetrieb bei.

Fällt ein Access Point aus, wechseln die damit verbundenen Endsysteme automatisch zum nächsten erreichbaren AP – Session und Authentisierungsstatus bleiben ebenso erhalten wie Sicherheit und QoS Priorisierung. Aber auch gestörte Switches, Uplinks oder Meshing Knoten werden über Prozesse wie das beschriebene AMRP kompensiert.

QoS und Security - Policy Enforcement

Policy Enforcement ist ein Schlüsselelement der Extreme Networks Cooperative Control Architektur. Basierend auf der Identität von Endsystem und Nutzer treten Regelwerke in Kraft, um Datenpakete bereits beim Eintritt in die Infrastruktur zu kontrollieren und zu priorisieren. Unerwünschter Datenverkehr wird als solcher klassifiziert und entfernt – lange bevor er über mehrere Hops einen Controller erreicht.

QoS Policy Enforcement im Access

Wireless LAN hat sich aus einem Nischendasein zur primären Form der Netzanbindung im Access entwickelt. Extreme Networks hat hierbei den geläufigen QoS Mechanismus WMM (WiFi Multimedia) mit effektiveren und robusten Funktionen erweitert. Basierend auf dessen zeitkritischer Natur wird der Datenverkehr in vier unterschiedlich priorisierten Warteschlangen klassifiziert. Hochpriorisierte Daten nutzen dabei einen

kleineren Inter-Frame-Space sowie ein kürzeres Random Back-Off Window – (beides Algorithmen zur Kontrolle mehrerer Stationen in einem Shared Medium) um die Latenz kritischer Pakete zu verkürzen.

WMM QoS Settings

Access Category	Contention Window Minimum (1-15)	Contention Window Maximum (1-15)	AIFS (1-15)	TXOP Limit (0-8192)
Voice	2	3	1	1504
Video	3	4	1	3008
Best-effort	4	6	3	0
Background	4	10	7	0

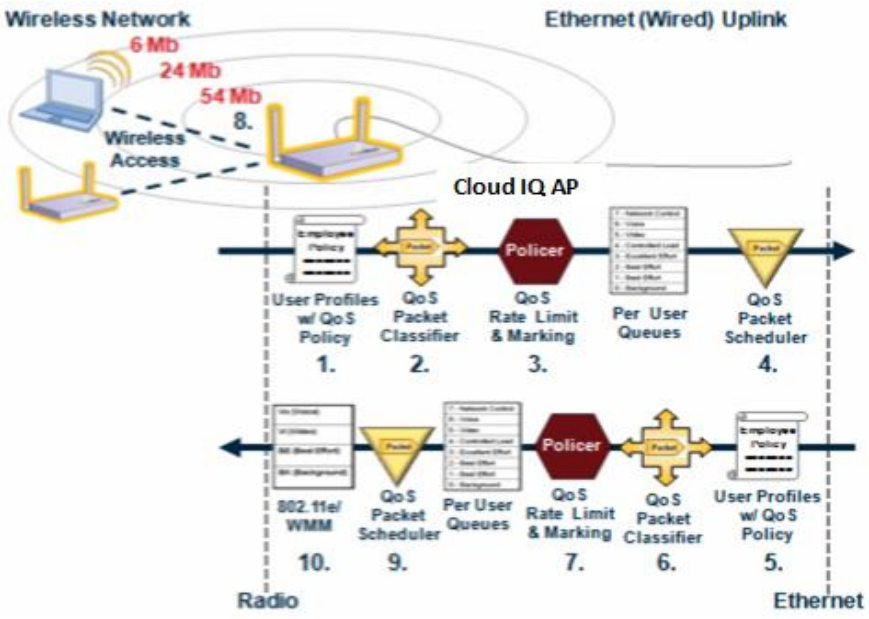
Minimum und Maximum des Contention Window definieren die Wartezeit, die ein Client ausharrt bevor er auf dem freien Kanal zu senden beginnt. Ein verkürztes AIFS (Arbitration inter-frame spacing) definiert die Wartezeit bis zum Senden des nächsten Frames. TXOP definiert das Zeitlimit, in welchem der Client mehrere Pakete senden darf.

Ja, unter der Haube präsentiert sich WLAN als richtig komplex. Nur so ist es möglich, allen Teilnehmern einer Funkzelle einen fairen Anteil der Luftschnittstelle zuzugestehen und darüber hinaus zeitkritische Daten wie Sprache mit besonderer Achtsamkeit zu behandeln.

WMM ist per default eingeschaltet und kann bei Bedarf auf der SSID adaptiert werden.

XIQ bietet darüber hinaus mit ihrer Packet Scheduling Engine zusätzliche Algorithmen, welche die Verfügbarkeit der Warteschlangen überwachen. Damit lassen sich Paketverluste und Jittereffekte vermeiden. Das Ergebnis ist eine fehlerfreie Sprachqualität.

Die folgende Grafik erläutert den QoS-Workflow innerhalb eines Extreme Cloud IQ Access Points.



Hardware – Access Points

Software as a Service, Cloud based Management, alles virtuell. Ganz ohne Hardware geht es aber trotzdem nicht. Werfen wir also einen Blick auf die Accesspoints, die bei näherem Hinsehen doch nicht alle gleich sind:

Extreme bietet ein robustes Portfolio von Cloud-verwalteten Wi-Fi 6-APs der Enterprise-Klasse, um eine nahtlose Netzabdeckung und eine überlegene Benutzererfahrung bei unterschiedlichen Anforderungen an Bereitstellung und Dichte zu gewährleisten. Die Wi-Fi 6-Technologie bringt drahtlose Netzwerke auf ein völlig neues Niveau. Sie adressiert auf einzigartige Weise eine größere Kapazität, unterstützt mehr Geräte gleichzeitig, nutzt das verfügbare Spektrum wesentlich effizienter und passt die Bandbreite für verschiedene Geräte und Anwendungen nach Bedarf dynamisch an. Alle Wi-Fi 6-Access Points von Extreme Networks verfügen über die wesentlichen Funktionen, die in den heutigen Mobile-First-Organisationen zur Unterstützung erforderlich sind:

- Hochleistungsumgebungen für HD-Video-Streaming und -bearbeitung mit vergleichsweise großem Transfervolumen
- Umgebungen mit sehr hoher Clientdichte, in welchen neben dem Nettodurchsatz auch die Koexistenz zahlreicher Endgeräte optimiert werden kann.
- Wi-Fi-basierte VoIP-Umgebungen mit hohen Erwartungen an Resilienz und Sprachqualität
- Internet of Things (IoT) – hier ist das Spektrum sehr weit gefasst. Vom leistungsfähigen Röntgengerät bis zum – technologisch leicht beschränkten - Temperatursensor der Gebäudeklimatisierung. Meist ist hier die schiere Masse an Clients ausschlaggebend – und genau darauf ist WiFi6 ausgelegt.

Alle APs von Extreme Networks sind auf Sicherheit, Zuverlässigkeit und Benutzerfreundlichkeit ausgelegt.

Sie bieten alle Funktionen, um die Verfügbarkeit unternehmenskritischer Anwendungen sicherzustellen, was zu einer außergewöhnlichen Benutzerfreundlichkeit (QoE Quality of Experience) für Mitarbeiter und IT führt.

Das Portfolio von Extreme Networks lässt kaum Wünsche offen. Ob indoor oder outdoor, interne oder externe Antennen, Dual-, Tri- und Sensor-Radios – die Liste ist ziemlich lang geworden.

WiFi6 Indoor Wireless Access Points

Das Indoor AP Portfolio von Extreme Networks deckt alle Anforderungen von Low Budget bis High End ab:

- Der **AP305C** ist ein Indoor-AP der Enterprise Klasse, der auf einem neuen System-on-a-Chip (SoC) Design mit zwei integrierten Dualband-Funksystemen basiert.
- Der **AP410C** ist ein hocheffizienter, leistungsstarker 4x4:4 / 2x2:2 802.11ax Access Point Tri-Radio-AP.

- Der **AP510C** ist ein dualer hocheffizienter 4x4:4 802.11ax Access Point mit hoher Performance und aggregierten Datenraten von 4,8 Gbit/s.

Diese kurze Übersicht dient lediglich Ihrer Orientierung. Technische Einzelheiten finden Sie in den Datenblättern unter https://www.extremenetworks.com/products/extremewireless

AP305C/CX

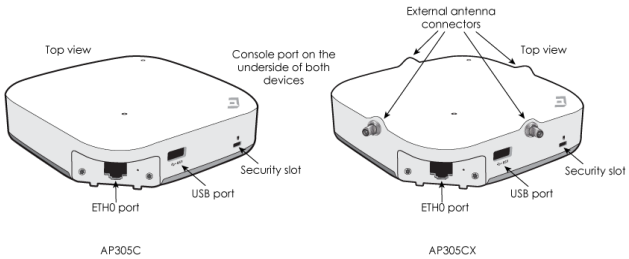
Der AP305C/CX positioniert sich als kostengünstiger Dual-Radio-WiFi6 Access Point für Umgebungen mit mittleren Anforderungen.

Im Design dieses Modells wurden ökologische Aspekte mit berücksichtigt. Gefertigt aus hochwertigem Recyclingkunststoff begnügt sich dieser AP auch beim Energiekonsum typischerweise mit weniger als 10w, kann also auch von älteren PoE Switches nach IEEE 802.3af versorgt werden. Das integrierte Powermanagement der Hardwareplattform wird künftig eingesetzt, um bei geringer Nutzung automatisch Energiesparmassnahmen einzuleiten. Das mag angesichts der ohnehin geringen Leistungsaufnahme belanglos erscheinen. Aber stellen Sie sich mal die Gesamtanzahl der APs in Ihrem Unternehmen vor: 24 Stundenbetrieb, 365 Tage im Jahr. Was wäre, wenn Ihre Accesspoints beispielsweise per Lichtsensor bestimmen können, ob sie im Moment gebraucht werden oder sich ein Stromsparnickerchen erlauben können?

Jedes der beiden Radios arbeitet mit zwei Antennen (2x2 MIMO) und auch der AP305C unterstützt den, oben beschriebenen SSR Modus, welcher zwischen dem 2,4/5GHz bzw 5/5GHz wechseln kann.

Der Indoor AP305C ist in zwei Modellen erhältlich:

Integrated antenna model (Part # AP305C-WR)	External antenna model (Part # AP305CX-WR).
	 (Include 4 RP SMA connectors)

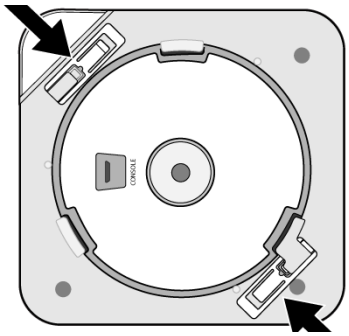


Der AP305CX verfügt über vier RP-SMA-Stecker zum Anschließen von Dualband-Dipolantennen. Beachten Sie dabei: Mit der Bestellnummer AH-ACC-ANT-AX-KT werden 8 Antennen geliefert, ausreichend für jeweils zwei APs. Der Gewinn dieser 2,4 / 5-GHz-Antennen mit liegt bei 3 bzw. 5-dBi.

Die 10/100/1000 Mbit/s LAN Schnittstelle ist durch eine Kunststoffabdeckung geschützt und im Regelbetrieb nicht einsehbar.

Der AP305C / CX verwendet 802.3af PoE für die volle WLAN Funktionalität. Lediglich für die volle Leistung USB-Ports benötigt das System eine PoE+ Versorgung (Siehe Tabelle).

AP305C/CX	802.3af	802.3at
2.4 G 5G Radio	Yes -2x2	Yes -2x2
BLE	Enabled	Enabled
USB	Yes USB power < =500mA	Yes
1 G Ethernet	Yes	Yes



Der AP305C/CX besitzt zwei Halteklammern zur schraubenlosen Befestigung an den Schienen standardisierter, abgehängter 15/16-Zoll-Elementdecken

Verschiedene optionale Montagehalterungen sind ebenfalls erhältlich, um alternative Montagemethoden zu unterstützen, einschließlich Wandmontage und abgehängter Decken unterschiedlichen Stils.
Praktiker empfehlen für die vereinfachte Montage im Feld das optionale Mount Kit AH-ACC-BKT-AX-TB mitzubestellen.

AP410C

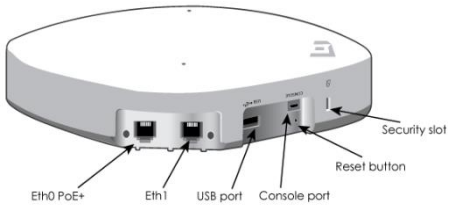
Die nächste Leistungsklasse wird vom Modell AP410C ausgefüllt. Dieser leistungsstarke Tri-Radio Wi-Fi 6-Access Point ist für Umgebungen mit hoher Client-Dichte konzipiert.

Ein dediziertes Vollzeit-Sensormodul ist in der Lage das Risiko von Sicherheitslücken oder Angriffen zu minimieren. Über das gesamte WLAN Spektrum wird hier kontinuierlich nach Störquellen und unerwünschten Geräten gesucht. Die beiden programmierbaren Radios decken damit lückenlos den Produktivbetrieb ab – auch hier wahlweise im 2,4/5- oder 5/5GHz Band, je nach Anforderung.

Neben der 2x2:2 (2,4GHz) bzw 4x4:4 (5GHz) MIMO Charakteristik bietet der AP410C auch ein integriertes BLE Radio.

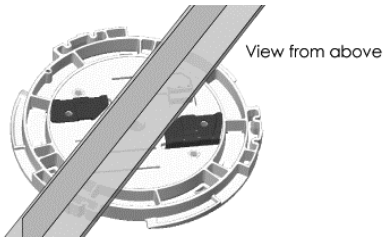
Unter der Haube des AP410C arbeitet ein internes Antennenarray mit omnidirektionaler Ausbreitungscharakteristik. Das unauffällige Design fügt

sich auch in hochwertige Räumlichkeiten ein. In diesen Einsatzszenarien bringen externe Antennen nur selten Vorteile, daher wurde auf eine CX Variante verzichtet.



Mit einer Multispeedschnittstelle bis zu 2,5Gbps sowie einem 10/100/1000BaseTX Interface sind auf den Ausbau der LAN Umgebung angepasste Aggregationsmodelle möglich.
Der AP410C bezieht über PoE+ (IEEE802.3at) ca. 18 Watt. Im Betrieb an älteren PoE Switches (802.3af) geht er automatisch in den Stromsparmodus. Hier stehen dann etwas weniger Ressourcen zur Verfügung (siehe Tabelle), andererseits lassen sich so auch Übergangsszenarien optimal abbilden.

AP410C	802.3af	802.3at
2.4 G Radio	2x2 (14 dBm)	2x2 (18 dbm)
5 G Radio	2x2: (17 dBm)	4x4 (18 dBm)
Sensor Radio	2.4 G and 5 G (15 dBm)	2.4 G and 5 G (18 dBm)
BLE	Enabled	Enabled
USB	No	Yes
2.5 G Ethernet	Yes	Yes
1 G Ethernet	No	Yes



Der AP410C wird mit einer Montagehalterung für 15/16 Zoll bündig montierte Deckenplatten (AH-ACC-BKT-AX-TB) geliefert.

Verschiedene optionale Montagehalterungen sind ebenfalls erhältlich, um alternative Montagemethoden zu unterstützen, einschließlich Wandmontage und abgehängter Decken unterschiedlichen Stils.

AP510C/CX

Die oberste Leistungsklasse des XIQ AP Portfolios erfüllt höchste Leistungsanforderungen in allen Bereichen mit sehr hoher Endgerätedichte. Über alle Bänder hinweg leistet das System eine kumulierte Bandbreite von bis zu 4,8Gbps.

Zwei vollredundante LAN Ports mit 2,5 und 1Gbps sorgen mit verteilter PoE Versorgung für die Abdeckung aller gängigen Hochverfügbarkeitsszenarien.

Für die volle Funktionalität benötigt der AP510C/CX den PoE+ Standard gemäß IEEE 802.3at. Mit einfachem PoE (802.3af) auf einem oder beiden Ports ist der Betrieb, wie bei den anderen Modellen mit reduziertem Feature Set möglich. Beachten Sie dazu die folgende Tabelle.

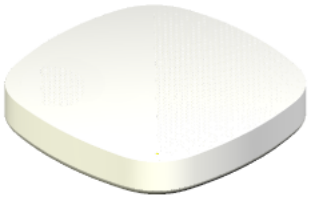
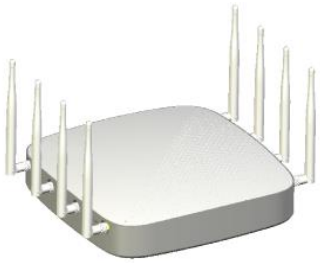
AP510C / CX	802.3af - Eth0	802.3af - Eth1	802.3at
2.4 G Radio	2x2 (12 dBm)	4x4 (10 dbm)	4x4 (20 dbm)
5 G Radio	2x2 (12 dBm) dual 5GHz mode not supported	4x4 (10 dbm) dual 5GHz mode not supported	4x4 (20 dBm)
BLE	Enabled	Enabled	Enabled
USB	No	No	Yes
2.5 G Ethernet	Yes [1G]	No	Yes
1 G Ethernet	No	Yes	Yes

Auch bei diesem Access Point sorgt die programmierbare Radio Architektur für eine optimierte Heatmap mit verteilten 2,4/5GHz bzw. 5/5GHz WLAN APs. Zusätzlich lässt sich eines der Radios optional als WIPS Sensor nutzen.

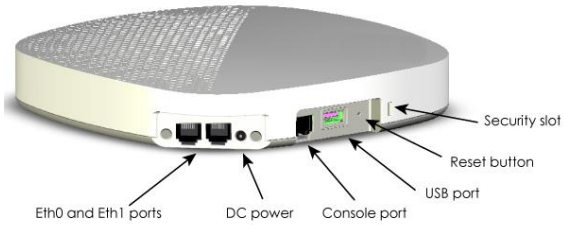
Das omnidirektionale interne Antennenarray des AP510C stellt sich wie folgt auf:

- 4 interne omnidirektionale 2,4 / 5-GHz-Dualbandantennen,
- 4 interne omnidirektionale 5-GHz-Antennen
- 1 interne BLE-Antenne (I-Beacon)

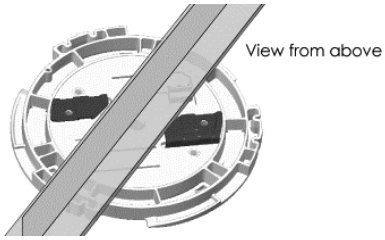
Die -CX Variante ist baugleich, die Anschlüsse für die 8 WLAN Antennen sind jedoch als Reverse SMA Konnektoren von aussen zugänglich.
Und obwohl es sich hierbei nicht um ein Outdoorgerät handelt, ist der erweiterte Temperaturbereich (-20° bis +55°C) in besonderen Szenarien ein echter Erfolgsfaktor.

Integrated antenna model (Part # AP510C-CE)	External antenna model (Part # AP510CX-CE).
	 (Include 8 RP SMA connectors**)**

Der AP510CX verfügt über acht RP-SMA-Stecker zum Anschließen von Dualband-Dipolantennen (AH-ACC-ANT-AX-KT - wird im Bundle zu 8 Stück geliefert - omnidirektionale 2,4 / 5-GHz-Antennen mit einer 3/5-dBi-Verstärkung).



Es werden zwei RJ45-Schnittstellen unterstützt: 1 x 2,5 und 1x 10/100/1000 Mbit/s; Beide Schnittstellen unterstützen Auto-Negotiation.



Der AP410C wird mit einer Montagehalterung für 15/16 Zoll bündig montierte Deckenplatten (AH-ACC-BKT-AX-TB) geliefert.

Verschiedene optionale Montagehalterungen sind ebenfalls erhältlich, um alternative Montagemethoden zu unterstützen, einschließlich Wandmontage und abgehängter Decken unterschiedlichen Stils.

WiFi5 Indoor AccessPoints

Die Chipsätze der folgenden beiden Access Point Modelle unterstützen den Standard 802.11ac, sind also keine WiFi6 Komponenten. Wegen ihrer besonderen Eigenschaften verdienen sie trotzdem Erwähnung.

AP150W – Mit der Extraportion Ports

Ein Access Point fürs Homeoffice? WLAN-Anforderungen da, wo die Verkabelungsressourcen gerade nicht ausreichen?

Der AP150W springt hier in die Bresche. Als intelligenter Ersatz für eine LAN Dose übernimmt er die üblichen zwei Leitungen und leitet eine davon transparent nach vorne weiter (Pass Through Port) die zweite Verbindung versorgt den AP mit Energie (PoE+).

Neben 2x2 MIMO (2,4GHz) und 3x3 MIMO (5GHz) stellt der AP150W drei LAN Ports bereit; einer davon liefert für angeschlossene Clients 12W PoE Leistung.

Eine separate Stromversorgung gibt dem AP150W noch mehr Unabhängigkeit. Als Meshing Access Point stellt er so LAN Anschlüsse an Stellen bereit, die sonst keine Anschlussmöglichkeiten bieten.

AP30 – Mehr als ein Steckernetzteil

Die schnellste Methode einen Accesspoint zu installieren. In die Steckdose stecken – fertig.

Der kompakte AP30 liefert 2x2:2 MIMO sowohl im 2,4 wie auch im 5GHz Band. Ein Gigabit LAN Port dient entweder zur Kopplung ans lokale Netzwerk, oder er macht den meshingtauglichen Accesspoint zur mobilen LAN Dose.
Zusammen mit dem einfachen Onboarding ist der kompakte AP30 wohl die flexibelste Lösung um – eben mal – das Netzwerk dahin zu bringen, wo bisher noch nichts war.

AP122 und AP250

Die rasanten Innovationszyklen in der WLAN Welt sind allenthalben bekannt. Bei der Beschaffung von Infrastruktur agieren Faktoren wie Preis, Leistung und Produktlebenszyklus konträr. Anstatt Glaubenssysteme dogmatisch zu postulieren, ist es sinnvoll, die realen Anforderungen etwas nüchterner zu betrachten. WiFi6 ist heute State of the Art, doch das bedeutet noch lange nicht, dass 802.11ac damit unbrauchbar geworden ist.

Der AP122 ist mit 2x2 MIMO und WiFi5 eher der leichten Kavallerie zuzuordnen, punktet dafür mit einem auffallend günstigen Preis.

Auch der 3x3 MIMO AP250 ist ein bewährtes Element unseres Portfolios und hat es sich verdient, genannt zu werden.

Projekte mit schmalem Budget lassen sich mit diesen Modellen fallweise leichter realisieren. Ein smarter Mix aus High End APs für Zonen mit hoher Aktivität und kleineren Leistungsklassen für periphere Bereiche hat scih in der Praxis schon immer ausgezahlt.

Möchten Sie mehr erfahren? Hier finden Sie unser gesamtes Portfolio:

https://www.extremenetworks.com/products/extremewireless

Key Features – Indoor Access Points

Zu den wichtigsten Funktionen und Vorteilen von Indoor WiFi6 Extreme Networks Cloud IQ Access Points gehören:

 **Security**	Extreme Cloud IQ Indoor Access Points bieten ein Höchstmaß an Sicherheit, beginnend mit der Unterstützung der neuesten WPA3-Sicherheitszertifizierungen der Wi-Fi Alliance. Darüber hinaus unterstützen sie eine Stateful L2-L7 DPI-Firewall für kontextbasierte Zugriffssicherheit, Private Pre-Shared Key (PPSK) und vieles mehr.
 **Wi-Fi 6 Technology**	Die 802.11ax-Technologie verbessert sowohl die Wi-Fi-Effizienz als auch -Geschwindigkeit und bringt Wi-Fi-Netzwerke auf ein völlig neues Niveau. Extreme Networks hat den branchenweit ersten softwaredefinierten 802.11ax-AP auf den Markt gebracht, der nicht nur eine dual 5-GHz-Fähigkeit unterstützt, sondern auch zwei durch Software programmierbare Modi zur optimalen Verwaltung der Funksysteme, um ein Höchstmaß an Clientleistung zu erzielen.
 **Programable Radios**	Mit der intelligenten Überwachung der softwarekonfigurierbaren Funksysteme von Extreme Networks Cloud IQ Indoor Access Points können Netzwerkmanager die Netzwerk-RF-Technologie basierend auf der Benutzerumgebung konfigurieren und die Access Points nach Bedarf in verschiedenen Modi konfigurieren.
 **Management Analytics**	In Verbindung mit XIQ (Cloud basiert oder on-Prem) bieten die Cloud IQ Indoor Access Points sehr umfangreiche Dashboards, die über kontextgesteuerte Widgets angezeigt werden und historische Daten oder eine Kombination aus historischen und aktuellen Daten darstellen. Dies bietet kontextspezifische Granularität mit perspektivischen Ansichten für Standorte, Netzwerk, APs, einzelne Clientgeräte sowie Policies. In jedem Kontext können Administratoren Dashboards anpassen, um eine eigene Widget-Bibliothek zu erstellen.

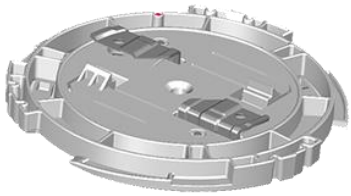
RF Monitoring	Die Extreme Networks Cloud IQ Indoor Access Point-Serie verfügt über ein adaptives HF-Management mit AI / ML-ähnlicher Funktionalität. Dies ermöglicht eine intelligente Auswahl der besten verfügbaren Kanäle und Sendeleistung für einen uneingeschränkten dualen 5-GHz-Betrieb. Lastausgleich, Bandsteuerung und viele andere Attribute des RF können automatisiert werden.
IoT Integrated BLE and Zigbee	Um sowohl IoT- als auch Guest Engagement-Dienste zu unterstützen, nutzt der Extreme Networks Cloud IQ Indoor Access Point Bluetooth. Somit können mittels Thread Wireless IoT-Geräte oder Mitarbeiter, Studenten und Gäste mit Apple iBeacon verbunden werden.

Montageelemente für Indoor Access Points

Es gibt eine ganze Reihe unterschiedlicher Montagesätze für die XIQ Accesspoints. In Einzelheiten finden Sie diese in den Hardware Manuals.

Um die Auswahl für lokale Verhältnisse etwas zu vereinfachen, schauen wir uns zwei Elemente an, mit welchen die meisten Szenarien abgedeckt werden können:

Das Gehäuse jedes Indoor APs weist Klammern auf, die eine Montage an abgehängten Decken erlauben. Zusätzlich bringen die Modelle AP410C und AP510C die Halterung AH-ACC-BKT-AX-TB mit, welche auch eine Dübelverankerung an Wand und Decke zulässt.
Beim AP305C lässt sich diese Montageplatte optional bestellen.



Manche Szenarien erfordern etwas Stauraum für Anschlussleitungen oder der zusätzliche Abstand zur Decke erleichtert einfach die Montage. Das optionale Element AH-ACC-BKT-AX-WI sorgt für die nötige Distanz.

Weitere Varianten empfehlen sich für den Einsatz bei besonders profilierten Deckenkonstrukten, aus Gründen der Einfachheit wird hier der Blick in den Hardware Guide der jeweiligen AP Modelle empfohlen.
Outdoor Wireless Access Points

WiFi 6Outdoor Access Points

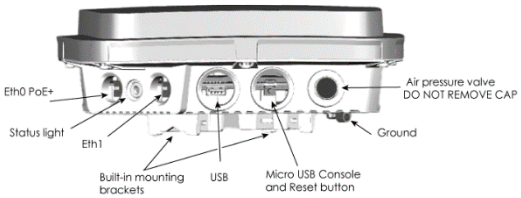
X460C

Um auch in Außenbereichen bzw. in Zonen mit schwierigen Umweltbedingungen für eine optimale WLAN Abdeckung zu sorgen, wurde der AP460C entwickelt. Das Tri-Radio-Design baut auf dem Standard 802.11ax auf. Der 2,4GHz Bereich wird über 2 Antennen (2x2 MIMO) versorgt, für 5GHz steht ein Array aus 5 Antennen (4x4MIMO) bereit. Jedes Modell verfügt darüber hinaus über eine omnidirektionale Antenne für Bluetooth Low Energy.

Auch beim AP460 lassen sich die Radios an Ihre individuellen Aufgaben anpassen. Ob 2,4/5GHZ, 5/5GHz oder 5GHz/Sensor – alle Optionen sind hier frei wählbar.

Interessant für eine an die Umwelt angepasste Ausleuchtung ist die Ausweitung auf drei – optisch identische – AP Modelle mit unterschiedlicher Abstrahlcharakteristik. Das Standardmodell mit omnidirektionalen Eigenschaften wird durch den AP460S6C mit 60°, sowie den AP460S12C mit 120° Sektorantennen ergänzt. Auf diese Weise lassen sich die, im Freien oft eingeschränkten, Montagemöglichkeiten wirkungsvoll ausgleichen. Durch die Integration der Antennen im Gehäuse wirkt der AP unauffälliger und fügt sich somit gut ins Fassadenbild ein.

Zusammen mit einer Schutzklasse IP67 arbeitet der AP460C in einem Temperaturbereich zwischen -40° und +60°C auch in exponierten Positionen.

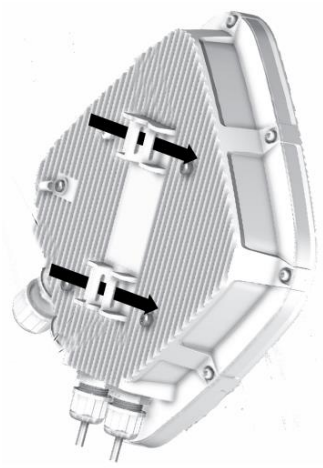


Auf der LAN Seite stehen eine Multispeedschnittstelle (max. 2,5Gbps) sowie ein Gigabit Port zur Verfügung.

Die Stromversorgung des AP460C erfolgt optimal über PoE+ gemäss IEEE802.3at – alternativ begnügt sich der AP auch mit 802.3af, dafür schaltet er das Funktionspektrum in den ECO Mode

AP460C	802.3af	802.3at
2.4 G Radio	2x2 (14 dBm)	2x2 (18 dbm)
5 G Radio	2x2 (17 dBm)	4x4 (18 dBm)
Sensor Radio	2.4 G and 5 G (15 dBm)	2.4 G and 5 G (18 dBm)
BLE	Enabled	Enabled
USB	No	Yes

AP460C	802.3af	802.3at
2.5 G Ethernet	Yes	Yes
1 G Ethernet	No	Yes



Zur direkten Befestigung des AP an einem Mast lassen sich Kunststoff- oder Metallbänder durch die vorbereiteten Gehäuseprofile ziehen.
Für die Wandmontage ist ein Montageset (AH-ACC-BKT-ASM) erhältlich.

Eine komplette Montagegarnitur aus rostfreiem Edelstahl inklusive Schrauben, Montageplatte und Metallbändern wird unter AH-ACC-MRN-KIT angeboten.

Auch extralange Stahlschellen für Masten mit Durchmessern von 7,5-35cm können separat bezogen werden.

Eine genaue Beschreibung der Montage finden Sie hier:

http://docs.aerohive.com/330000/docs/help/english/ng/Content/hardware/ap/ap460.htm#Accessories

Key Features – Outdoor Access Points

Security	Der AP460C bietet ein Höchstmaß an Sicherheit, beginnend mit der Unterstützung der neuesten WPA3-Sicherheitszertifizierungen der Wi-Fi Alliance. Darüber hinaus wird eine stateful L2-L7 DPI-Firewall für kontextbasierten Zugriff, PPSK (Private Pre-Shared Key) und vieles mehr unterstützt.
Wi-Fi 6 Technology	Frühere Generationen von 802.11n, 802.11ac Wave 1 und 2, können als Generationsverbesserungen mit Schwerpunkt auf verbesserte Geschwindigkeit betrachtet werden. Die 802.11ax-Technologie verbessert stattdessen die Wi-Fi-Effizienz und -Geschwindigkeit. Sie bringt Wi-Fi-Netzwerke auf ein völlig neues Niveau.
Programable Radios	Der AP460C ist der erste Tri-Radio 802.11ax Access Point mit zwei Modi, welche per Software programmiert werden. Die Verwaltung von Radios, die Optimierung von Client-Leistung und gleichzeitig eine kontinuierliche HF-Überwachung gegen Sicherheitsbedrohungen werden bereitgestellt. Mit der intelligenten Überwachung der per Software konfigurierbaren Radios können Netzwerkmanager die Netzwerk-RF-Topologie basierend auf der Benutzerumgebung konfigurieren und die Access Points nach Bedarf in verschiedenen Modi konfigurieren.
Management Analytics	In Verbindung mit XIQ (Cloud oder On-Prem) bietet der AP460C sehr umfangreiche Dashboards, die über kontextgesteuerte Widgets angezeigt werden und historische Daten oder eine Kombination aus historischen und aktuellen Daten darstellen. Dies bietet kontextspezifische Granularität mit

	perspektivischen Ansichten für Standorte, Netzwerk, APs, einzelne Clientgeräte sowie Policies. In jedem Kontext können Administratoren Dashboards anpassen, um eine eigene Widget-Bibliothek zu erstellen.
 RF Monitoring	Der AP460 verfügt über ein adaptives HF-Management mit AI / ML-ähnlicher Funktionalität, welches eine intelligente Auswahl der besten Kanäle und Sendeleistung für einen unbeeinträchtigten dualen 5-GHz-Betrieb ermöglicht. Lastausgleich, Bandsteuerung und viele andere Attribute des RF können automatisiert werden.
 Integrated BLE and Zigbee	Um sowohl IoT- als auch Guest Engagement-Dienste zu unterstützen, nutzt der Extreme Networks Cloud IQ Indoor Access Point Bluetooth Low Energy. Somit können mittels Thread Wireless IoT-Geräte oder Mitarbeiter, Studenten und Gäste mit Apple iBeacon verbunden werden.

Hardware – Switches

ExtremeCloudIQ ist mehr als ein in die Cloud aufgestiegener WLAN Controller. Das haben wir zu Beginn schon angedeutet. Die schrittweise Integration des Switchportfolios ist auf einem guten Weg. Ein, in die Firmware integriertes Modul ist in der Lage, nicht nur die lokale Managementinstanz zu kontaktieren (Zero Touch Provisioning Plus) sondern auch den Weg in die Cloud zu finden.

Schon aus der Historie heraus hat ExtremeCloudIQ eine Reihe von Access Switches unterstützt:

SR2208P	8 x 10/100/1000BaseTX, 2 x 1G Uplinks SFP/RJ45, PoE+
SR2224P	24 x 10/100/1000BaseTX, 4 x 1G Uplinks SFP, PoE+
SR2324P	24 x 10/100/1000BaseTX, 4 x 10G Uplinks SFP, PoE+
SR2348P	48 x 10/100/1000BaseTX, 4 x 10G Uplinks SFP, PoE+

Seit Anfang des Jahres integrieren wir Schritt für Schritt das Switchportfolio von Extreme Networks in XIQ. Dies umfasst Stand heute:

X435	Für einfache Szenarien mit bis zu 24 Ports
X440	Das Arbeitspferd für den Access
X450	Für den Access mit erhöhten Leistungsanforderungen
X460/465	Anspruchsvolle Switches für Access und Distribution

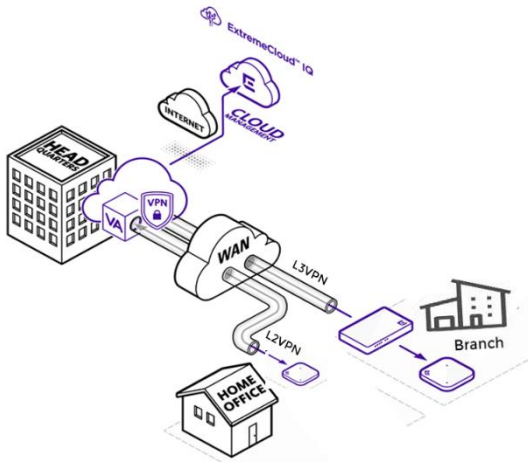
Die vollständige Liste unterstützter Komponenten finden Sie hier:

http://docs.aerohive.com/330000/docs/help/english/ng/Content/learning-whats-new.htm

Und wenn Sie mehr über unser Portfolio erfahren möchten, stöbern Sie in unserem Solution Guide – oder sprechen Sie direkt mit uns.

Router, VPN und SD-WAN

Verteilte Organisationen benötigen sichere WAN Verbindungen. Gerade im Jahr 2020 hat sich gezeigt, wie wichtig es ist, auch komplexe Weitverkehrsstrukturen einfach zu etablieren und zu überwachen.



Das Portfolio von ExtremeCloud IQ enthält voll integrierte SD-WAN Komponenten für den Einsatz in Homeoffices bzw. Geschäftstellen.

Bei der Arbeit zuhause ist nicht mehr als ein Access Point notwendig, welcher automatisch einen gesicherten Tunnel in die Unternehmenszentrale aufbaut. Für die Anbindung von Außenstellen stehen die Hardwarerouter XR200p bzw. XR600p mit VPN Durchsatzraten von 100/250Mbps bereit.

Für die zentrale Anbindung empfiehlt sich der Einsatz der VGVA einer virtuellen Appliance zur Ankopplung von bis zu 1000 VPN Tunneln.

Zusammenfassung

Wir leben in interessanten Zeiten. Die Cloudtechnologie verdient tatsächlich das Attribut disruptiv und hat die Meinungen stark polarisiert.

An dieser Stelle ist eine nüchterne Betrachtung sicher hilfreich. Software as a Service heißt das – garnicht mehr so neue – Paradigma. Viele Lösungen arbeiten nach diesem Prinzip. Die Mehrwerte und Risiken lassen sich klar benennen und darauf abgestimmte Arbeitsprozesse erleichtern Einführung und Betrieb solcher Systeme.

Extreme Cloud IQ bringt die Innovationszyklen auf Touren. Noch nie hat sich eine Plattform so schnell und dynamisch entwickelt ohne dabei die Robustheit zu vernachlässigen. Die Geschwindigkeit mit welcher sich Infrastrukturen etablieren lassen hat sich vor allen im Jahr 2020 als vorteilhaft erwiesen.

Und wer dem Enthusiasmus skeptisch gegenübersteht, nutzt nach wie vor die bewährten OnPremise Szenarien in welchem Management-, Control- und Dataplane nach wie vor im kontrollierten Umfeld des eigenen Unternehmensnetzes verbleiben.

In Zukunft wird die Abgrenzung zwischen dem lokalen Rechenzentrum und in der Cloud gelagerten Ressourcen immer weiter aufgelöst. Hybridarchitekturen werden Dienste und Funktionen dort ausführen wo sie eben am besten aufgehoben sind.

Diese Zukunft hat schon längst begonnen – und wir sind dabei.