Enterprise Wireless LAN & Mobility Lösungen

WHITE PAPER

IdentiFi™ Wireless LAN

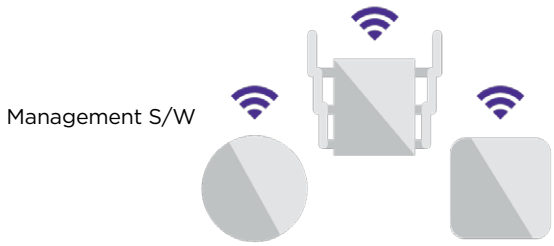
Wireless LAN ermöglicht Unternehmen erhöhte Flexibilitat (zum Beispiel mobile Büros, schnelle Anbindung neuer Bereiche), aber auch Kostensenkung durch Prozessintegration (z. B. Scanner im Logistikbereich, direkte Dokumentation auf digitaler Ebene, mobile Visite im Bereich Gesundheitswesen, Lokation-Tracking zum Auffinden von mobilen Gütern und Personen). Oft wird auch die Bereitstellung von Gastzugängen über Wireless LAN realisiert. Insbesondere die Trends in Unternehmen, zum einen bestehende DECT Systeme durch VoIP over Wireless LAN (WLAN) zu ersetzen, als auch zum anderen die Anforderung neuer Multifunktionssysteme (insbesondere Smartphones, Tablets) mit GSM/GPRS, UMTS, Bluetooth und WLAN Schnittstellen gerecht zu werden und ein kostenoptimiertes Roaming anzubieten (ein Mitarbeiter, der heute mit dem GSM Handy im eigenen Unternehmen telefoniert, wird in Zukunft direkt ins WLAN seines Unternehmens eingebucht und telefoniert dann über VoIP - „kostenlos“) sind hier die wesentlichen Faktoren.

Viele der oben genannten Technologien und Mehrwerte wurden erst durch die WLAN Switching Architektur vollwertig und praktikabel umsetzbar. Hierbei wird die bei der „Thick-AP“-Architektur vorhandene, verteilte Intelligenz je Access Point in eine zusätzliche Komponente, dem so genannten WLAN Controller zentralisiert. Die Access Points selbst werden in so genannte „Thin-APs“ umgewandelt und fungieren nur noch als „intelligente Antennen“. Dadurch wird eine skalierbare, flexible und zukunftssichere WLAN Umgebung geschaffen, die Hunderte von WLAN Switchen und Tausende von APs umfassen kann. Als oberste Hierarchieebene wird meist auch noch ein WLAN Management System eingesetzt, das zentral über WLAN Grenzen hinweg Planungs-, Konfigurations-, Monitoring- und Alarmierungsdienste zur Verfügung stellt.

Typische Funktionen einer WLAN Switching Lösung sind z. B.:

- Automatische Kanalwahl
- Automatische Regelung der Sendeleistung
- Loadbalancing zwischen den APs
- Verarbeiten von Gebäude/ Geländeplanen, um die Funkausbreitung/ Clients/ RFID-Tags/ Fremd-APs visuell darzustellen
- Verkürztes, subnetübergreifendes Roaming
- Automatisiertes Erkennen, Lokalisieren und Bekampfen von Fremd-APs und Clients
- Zentralisierte Planung, Deployment, Reporting & Alarmierung

Durch die IdentiFi Fit AP Architektur bleibt ein grosser Anteil der Intelligenz in den APs erhalten. Dies ermöglicht dezentrales Traffic-Forwarding direkt am AP mit allen nötigen Paramentern wie z. B QoS, Ratelimit, ACLs us.w. und eliminiert dadurch das Nadelöhr am Controller. Weiterhin kann der AP auch ohne Controller den Service in der Luft bereitstellen. Diese Architektur verbindet die Vorteile einer Thick AP Architektur mit denen einer Thin AP Archtektur und eliminiert gleichzeitig die Nachteile der jeweiligen Architekturen.

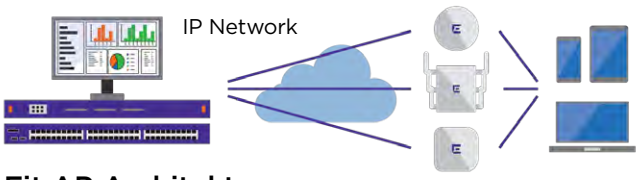


Fat AP Architektur

- Inteligenz und Management direkt auf den APs

Split MAC/Thin AP Architektur

- Splittet MAC Funktionen zwischen AP und Controller (Encryption, QoS, RF Management)
- Skaliert nicht in großen Umgebungen



Fit AP Architektur

- Dezentrales olicy Enforcement (Encryption, QoS, RF Management)
- Zentralisiertes Management und Kontrolle

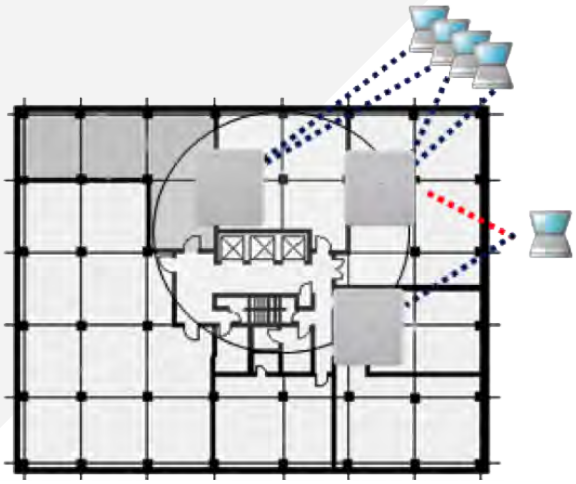
WLAN High-Density & Performance Best Practise

Um den gestiegenen Anforderungen hinsichtlich Client-Dichte und Leistung in heutigen modernen WLAN-Netzen Rechnung zu tragen, beinhaltet unsere Lösung eine Vielzahl von Funktionen, um diese Herausforderungen effizient und einfach zu lösen:

LOAD BALANCING & BANDSTEERING

Load Balancing verteilt Clients über eine definierte Anzahl von Radios um sicherzustellen, dass ein einziger Radio oder Kanal nicht überlastet wird, während andere ungenutzt bleiben. Voraussetzung ist, dass sich die APs gegenseitig in der Luft sehen. Typischerweise wird dieses Feature in grossen Besprechungsräumen, Bibliotheken oder Hörsälen eingesetzt.

Band-Steering erkennt, ob ein Client das 5 Ghz-Band unterstützt und steuert diesen dann gezielt auf dieses Radio. Voraussetzung hierfür ist, dass die WLAN Ausleuchtung auch für das 5 Ghz-Band sichergestellt ist, da es sonst für diese Clients zu Verbindungsabbrüchen kommen kann. Beide Funktionen kombiniert maximieren die Effizienz und den Durchsatz des Gesamtsystems.



SINGLE SSID DESIGN

Die Vielzahl an Applikationen und Endsystemen in heutigen WLAN-Netzen kann nicht mehr durch zusätzliche SSIDs Domänen umgesetzt werden. Durch die Möglichkeit, userbezogene Policies mit allen nötigen Parametern (VLAN, ACL, Topoligie, Ratelimit,QoS) zu vergeben, wird dies beim Single SSID Design innerhalb der SSID gelöst. Dadurch ergeben sich folgende Vorteile:

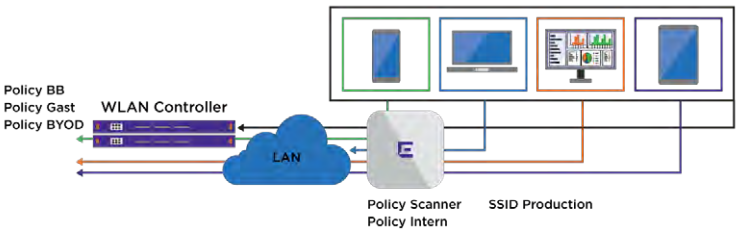
- Per User Topologie,QoS, Ratelimit und ACL
- weniger SSIDs nötig – einfachere Konfiguration der Clients
- einfacheres Durchsetzen von Security-Policies, da weniger SSIDs zu schützen sind
- Bessere Performance in der Luft – da weniger Beacons

Besonders durch das Minimieren der Beacons steigt die Performance in der Luft erheblich:

BEISPIEL MIT SSID PER AP – 3 APS IM GLEICHEN BEREICH	
Beacon Datenrate	**Channel Bandbreitennutzung**
1 Mbps	**25.92%**
2 Mbps	**12.96%**
5.5 Mbps	4.71%
11 Mbps	2.36%
6 Mbps (802.11a/g)	4.32%
12 Mbps (802.11a/g)	2.16%

GLEICHES NETZWERK MIT NUR 3 SSIDS PER AP	
Beacon Datenrate	**Channel Bandbreitennutzung**
1 Mbps	**12.96%**
2 Mbps	**6.48%**
5.5 Mbps	2.36%
11 Mbps	1.18%
6 Mbps (802.11a/g)	2.16%
12 Mbps (802.11a/g)	1.08

Prinzipschaubild:



AIRTIME FAIRNESS

Obwohl die Anzahl der installierten 11n-APs stetig steigt, findet man auf der Client-Seite fast ausschließlich Umgebungen, in denen 11n- und 11a/b/g-Clients auf die gleiche Infrastruktur zugreifen. Durch den bestehenden Zugangsmechnanismus wird jedem Client, unabhängig von der Geschwindigkeit, mit der er verbunden ist, erlaubt, die gleiche Anzahl an Paketen zu versenden. Bei gemischten Clientzugangstechnologien (11n vs .11a/b/g) führt dies dazu, dass z. B. ein 11b Client den Kanal erheblich länger belegt als ein 11n Client. In der Summe wird dadurch der Gesamtdurchsatz der Funkzelle stark vermindert. Dieses Verhalten wird als Packet Fairness bezeichnet.

Durch Ändern dieses Verhaltens von Packet Fairness auf Airtime Fairness, bei dem jedem Client die gleiche Sendezeit eingeräumt wird, wird der Gesamtdurchsatz der Funkzelle gesteigert.

CLIENT MIX	EFFECTIVE BANDWIDTH (MBPS)	
	PACKET FAIRNESS	AIRTIME FAIRNESS
11a @ 6 Mbps	4.5	1.5
11a @ 6 Mbps	4.5	6
11a @ 6 Mbps	4.5	26
11a @ 6 Mbps	4.5	60
Total Throughput	18.0	93.5

RATELIMIT & QOS

Da sich die in einer Funkzelle eingeloggten Clients die Bandbreite und Sendezeit dieser Zelle teilen, ist es höchst effizient, mit Ratelimits & QoS den Zugriff auf die Zelle je nach Nutzer (z. B. Gäste vs. internen Clients) zu steuern. Dadurch ist es möglich, die limitierte Kapazität nutzer- & applikationsbezogen effizient zu verteilen.

ERHÖHEN DER MINIMUM-BASIC-RATE:

Management- sowie Multicast-Frames werden mit der geringstmöglichen Geschwindigkeit übertragen, damit sichergestellt wird, dass der Traffic auch von allen Clients erreicht wird. Bei entsprechender Ausleuchtung kann diese erhöht werden und so die Gesamtleistung des Systems verbessert werden.

PERFORMANCE-TUNING FÜR MULTICAST-VERKEHR:

Die gestiegene Nutzung von Video-over-WLAN & Zero-Config-Protokollen wie Bonjour, UpnP und LLMNR führt zu einem erheblich größeren Anteil an Multicast-Traffic innerhalb eines WLANs. Da Multicast-Traffic immer mit der Minimum-Basic-Rate versendet wird, kann dies zu Performance-Engpässen führen. Daher wird folgender Umgang mit Multicast-Traffic empfohlen:

- Multicast-Filterung @ AP
- Multicast zu Unicast Umwandlung
- Proxy ARP @ AP
- Anpassbare Multicast Senderate

Sicherung von WLAN Netzen

Zur Sicherung der Luftschnittstelle wurde ursprünglich der Sicherheitsstandard Wired Equivalent Privacy (WEP) eingeführt. Dieser erwies sich jedoch schon nach kurzer Zeit als lückenhaft, denn durch das Aufzeichnen und Analysieren der Kommunikation ist es möglich, den Netzwerkschlüssel zu ermitteln und somit die „Privacy“ zu kompromittieren. Der eigentliche Standard (IEEE 802.11i) zur Sicherung von WLANs war zu diesem Zeitpunkt noch in Arbeit, daher etablierte sich WPA als Zwischenlösung. Hier wurden durch diverse Hilfsmittel wie dynamische Schlüssel und bessere Authentifizierung - insbesondere durch Berücksichtigung von RADIUS Authentifizierung - eine höhere Sicherheit gewährleistet, welche noch nicht kompromittiert wurde.

Das Thema Sicherheit im Wireless LAN ist nach langer Diskussion nun final gelöst: Der Standard 802.11i (auch WPA2 genannt) ist verabschiedet und bietet für alle existierenden Sicherheitslücken innerhalb der 802.11 Familie eine adäquate Lösung. Die Authentifizierung via 802.1x (Port Based Authentication) und dessen gängige Methoden EAP-TLS, PEAP und EAPTTLS (zertifikats- und passwortbasiert) stellen neben der eigentlichen Authentifizierung die Basis für das Key Management dar.
Die Verschlüsselung ist 128-Bit AES (Advanced Encryption Standard) -basiert. Die Integrität von Daten und Header wird durch CCM (CCM = Counter Mode Encryption mit CBC-MAC) gewährleistet. Replay Attacks werden durch ein IV (Initialization Vector) Sequencing mit 48 Bit IV verhindert. Ein weiterer Punkt zur Sicherung von WLAN Netzen ist der Umgang mit Fremd-APs/Clients sowie 802.11-fremden Störungen, wie z. B. defekten Mikrowellen oder DECT-Stationen, die das gesamte RF-Spektrum stören können. Hierzu scannen die APs automatisch nach anderen Geräten, die im selben RF-Band arbeiten. Dadurch werden fremde Sender sowie natürlich die APs, die zum eigenen System gehören, erkannt. Alle fremden Sender stellen potentielle Rogues dar. Hierbei ist eine automatische Unterscheidung zwischen „Interfering AP“, „Rogues“ und „Ad-hoc Clients“ wichtig.

Ein Interfering AP wird auf der RF-Schnittstelle von den APs gesehen. Dieser hat jedoch keine Verbindung über die LAN Schnittstelle ins eigene Netz und stellt daher nur eine Störung auf der Funkseite dar. Meist sind dies Netze in benachbarten Gebäuden oder interne, unabhängige WLANs. Ein Rogue hingegen hat auch eine Verbindung über die LAN Schnittstelle ins eigene Netz und stellt damit ein erhöhtes Sicherheitsrisiko dar, da sich über diesen AP auch fremde Clients in das interne Netz einloggen können. Ad-hoc Clients kommunizieren direkt miteinander ohne Verbindung zum eigentlichen Netzwerk.
Dies stellt ähnlich wie die Interfering APs kein direktes Sicherheitsrisiko dar, allerdings werden sie als Störung auf der Funkseite erkannt.

Diese Unterscheidung wird automatisch von den Systemen vorgenommen und kategorisiert. Weiterhin stellen die Systeme Möglichkeiten zur Verfügung, um Gegenmaßnahmen zu ergreifen, die verhindern, dass sich WLAN Clients mit einem Rogue AP verbinden. Hierbei gibt sich das WLAN Switching System als Rogue AP aus und sendet sogenannte Disassociation Frames zu den am eigentlichen Rogue AP eingeloggten Clients. Diese verlieren dadurch die Verbindung und es kann keine saubere Kommunikation mehr aufgebaut werden. Zusätzlich können alle Arten von Fremd-APs/Clients mit Hilfe von Gebäudeplanen lokalisiert werden.

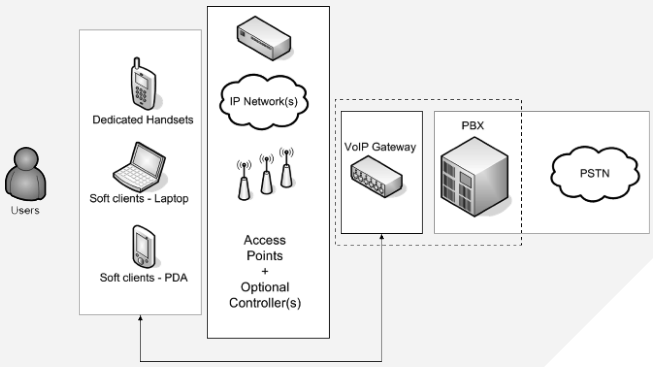
Voice over WLAN – QoS & Security

Die Zugriffsmethode für WLANs basiert derzeit meist noch auf CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Damit können keine QoS Merkmale geliefert werden.

Der IEEE 802.11e Standard beschreibt einige Erweiterungen, um diese Merkmale in einer WLAN Umgebung zu ermöglichen. Einige Unterfunktionen dieses Wireless Standards werden als WiFi Multimedia (WMM) vermarktet.

WMM eignet sich vor allem für Video- und Sprachübertragungen. Für den Kanalzugriff (Medium Access Control - MAC) sind in IEEE 802.11 zwei Verfahren spezifiziert worden: Die Distributed Coordination Function (DCF) ist ein verteilter, zufallsgesteuerter Zugriffsmechanismus (Carrier Sense Multiple Access with Collision Avoidance, kurz: CSMA/CA), der einen Best-Effort-Dienst liefert. Die Point Coordination Function (PCF) ist ein zentral gesteuerter Mechanismus, bei dem die beteiligten Stationen in regelmäßigen Abständen durch einen Master (typischerweise ein Access Point) per Polling ein Senderecht erhalten. Auf diese Weise kann für die beteiligten Stationen eine gewisse Bandbreite zugesichert werden.

Die Implementierung der DCF ist in IEEE 802.11 zwingend vorgeschrieben, die Realisierung der PCF ist jedoch nur als optional klassifiziert. Daher ist es nicht verwunderlich, dass in allen bekannten Implementierungen lediglich die DCF umgesetzt wurde. Da DCF zufallsgesteuert in einem Shared Medium wie Wireless LAN arbeitet, ist bei dieser Technik jedoch keine Bandbreitengarantie möglich – die Latenzzeit kann stark schwanken (Jitter), was für VoIP sehr negative Auswirkungen auf die Sprachqualität hat.



KOMPONENTEN EINER VoWLAN-LÖSUNG

Aus den oben genannten Gründen verwenden die meisten VoWLAN-Phone Hersteller eine Kombination aus standardbasierten und propritären Mechanismen, um ein schnelles Hand-Over von AP zu AP zu ermöglichen. Das Ziel dieses Roamingvorganges ist es, ein für den Anwender nicht merkbares Wechseln der Funkzelle zu ermöglichen. Bei den heute am meisten verwendeten Codecs G.711 und G.729 beträgt die maximal zu akzeptierende Roamingzeit ca. 50ms.

Als Roaming-Vorbereitung eines VoWLAN-Clients ist es nötig, dass dieser die APs in seinem Sendebereich kennt. Um dies umzusetzen senden die Clients Probe-Requests. Manche VoWLAN-Clients können so konfiguriert werden, dass nur bestimmte Kanäle (1,6,11) gescannt werden. Oder es werden spezielle Elemente in den AP Becons verwendet, um die Scangeschwindigkeit zu verbessern. Ebenso können manche Endgeräte so eingestellt werden, dass sie das Scannen erst bei Erreichen eines bestimmten Schwellenwerts beginnen. Dieser liegt meist bei -65 bis -70dBm. Diese Funktionen verbessern die Akkulaufzeiten und sorgen für ein schnelleres Roaming. Eine der größten Hürden in Bezug auf schnelles Roaming beim Ausrollen von VoWLAN-Lösungen sind die Verschlüsselungstechniken. Das beste Roamingverhalten wird bei unverschlüsseltem Verkehr oder mit WEP mit unter 8ms erreicht. Dieser Wert umfasst die Zeitspanne vom letzten erfolgreich gesendeten Paket auf dem alten AP bis zu dem ersten erfolgreich gesendeten Paket auf dem neuen AP.

Durch die Einführung von 802.11i wurde die Sicherheit in WLAN-Netzen drastisch erhöht, speziell auf 802.1x-basierende Implementierungen, allerdings auf Kosten eines schnellen Roamingvorgangs. Durch die Einbeziehung eines RADIUS Servers bei diesem Standard innerhalb jedes Authentifizierungsvorgangs werden die Roamingzeiten auf 50-200ms erhöht.

Selbst unter besten Voraussetzungen mit einem lokalen, nicht unter Last stehenden RADIUS Server, werden sehr schnell die gewünschten 50ms überschritten. Dies wird durch den Einsatz von WPA-PSK umgangen. Beide dazugehörigen Standards, WPA-PSK und WPA2-PSK, erreichen fast ein ähnliches Sicherheitsniveau wie die 802.1x-Implementierung, jedoch ohne Einbeziehung einer RADIUS Abfrage. Zusätzlich zu den einfachen Verfahren ohne Verschlüsselung oder WEP wird jedoch bei jedem Roamingvorgang die Erzeugung von Keys vorgenommen. Dieser Vorgang führt zu einer Verzögerung von weniger als 7ms bei WPA-PAS und 5ms bei WPA2-PSK. Dies führt in der Summe zu Gesamtroamingzeiten von 13-15ms. Das ist eine erhebliche Verbesserung gegenüber Verfahren die einen RADIUS Server ansprechen.

Allerdings ergeben sich durch den Einsatz von WPA-PSK auch einige Nachteile. So ist diese Technologie, wie alle Preshared-Key-Technologien, anfällig gegenüber Wörterbuchattacken, sobald ein einfacher Verschlüsselungskey gewählt wurde. Weiterhin ist das Ändern des Keys auf den Endgeräten meist mit einem Konfigurationsaufwand auf jedem Endgerät verbunden.

CLASS	APPLICATIONS	TRAFFIC	LATENCY DELAY	PACKET LOSS SENSITIVITY
Background	FTP Email	Bidirectional/Asymetric Variable Pkts	Unbounded <5-10s	Low
Interactive	Web Telnet	Bidirectional/Asymetric Variable Pkts	Tolerable <1s	Low
Fast Interactive	Video Gaming	Bidirectional/Asymetric Variable Pkts	Tolerable <100ms	High
Non-RT Streaming	VOD Cable TV	Unidirectional Large Pkts / Multicast	Bounded <5s	Low
RT Streaming	IP TV	Unidirectional Large Pkts / Multicast	Bounded <1s	High
Conversational	VoIP Video Phone Internet Game	Birdirectional Small Pkts (VoIP, Gaming) Large Pkts	Strict & Low <50ms	High

Diese Punkte treffen für eine auf RADIUS Abfrage basierende Technologie nicht zu. Um die zusätzlich benötigten schnellen Roamingvorgänge umsetzen zu können, die bei VoWLAN benötigt werden, wurden zwei neue Technologien entwickelt: OKC und Pre-Authentication.

Opportunistic Key Caching (OKC) verteilt den Key, den ein WLAN-Phone bei der ersten RADIUS Abfrage (für gewöhnlich beim Einschalten) erhält, auf alle APs, die den Service beinhalten. Bei einem Roamingvorgang ist es nun nicht mehr nötig, den RADIUS Server abzufragen, da sich der passende PMK bereits auf den APs befindet. Dadurch ergeben sich Roamingzeiten wie bei der PSK-Variante mit den Security-Vorteilen einer RADIUS Infrastruktur. Allerdings wird das Sicherheitsniveau einer vollen 802.11i Implementierung nicht erreicht, da der gleiche PMK auf alle APs verteilt und für die Authentifizierung und Verschlüsselung benutzt wird. 802.11i fordert jeweils einen neuen PMK per Session pro AP. Zur Zeit gibt es noch wenige Endgeräte, die OKC unterstützen.

Pre-Authentication ist eine Lösung, die eine volle RADIUS Abfrage an jedem AP benutzt. Dieser Vorgang, der mithilfe des Roamings stattfindet, ist erheblich zeitsparender. Mit Pre-Authentication führt das Endgerät eine vollwertige RADIUS basierende Authentifizierung beim erstmaligen Verbinden mit einem AP durch. Danach scannt das Endgerät nach jedem AP in der Umgebung mit der selben ESSID (aber anderen BSSID) und nutzt seine existierende Verbindung zur Infrastruktur, um eine vollwertige RADIUS Authentifizierung an den umgebenden APs durchzuführen, bevor der Roamingvorgang stattfindet. Der PMK wird sowohl von dem AP als auch Endgerät für eine spätere Benutzung vorgehalten. Bei einem Roamingvorgang wird über diesen Key ein Sessionkey je AP generiert. Der Zeitaufwand hierfür ist vergleichbar mit dem bei WPA-PAK. Pre-Authentication ist anfällig gegenüber Infrastrukturen mit hoher AP-Dichte und sehr mobilen Endgeräten. Dies kann zu Situationen führen, bei denen ein Roamingvorgang stattfindet bevor die Pre-Authentication durchgeführt wurde. Die Technologie gilt als sicherer als OKC, ist aber erst auf wenigen Endgeräten verfügbar.

Load Balancing in VoWLAN-Umgebungen wird durch eine von mehreren Call Admission Control (CAC) Funktionen erreicht. Extreme Networks WLAN benutzt hierzu TSPEC, wobei ein Endgerät eine Traffic-SPECification (TSPEC) erstellt und diese an den AP sendet. Dieser reserviert die angekündigte Menge an Up- und Down-Stream Bandbreite. Die Implementierung erlaubt es, Limits für neue und bestehende Roaming-Verbindungen zu setzen. Weiterhin können Bandbreitenreservierungen in unabhängigen Klassen gemacht werden, in denen z. B. Voice eine höhere Priorität bekommt als Video. Die Implementierung beim Extreme Networks WLAN geht sogar soweit, dass spezielle Aktionen definiert werden können, sobald die angekündigte Up- und Down-Stream Bandbreite überschritten wird, was auf einer per SSID-Basis geschieht.

Location-Tracking in WLAN Netzen

Eine weitere Technologie, die erst durch WLAN Switching ermöglicht wurde, sind Location Based Services. Mit Hilfe dieser Technologie können Geräte geortet werden, die eine WLAN Karte besitzen (Notebooks, VoIP WLAN Phones) sowie dedizierte Location Tags, in denen z. B. Panic-Buttons und Bewegungssensoren integriert sind. Diese können an wichtigen Gütern, z. B. mobilen Infusionspumpen im Krankenhausbereich oder an Staplern in der Logistik, befestigt werden. Durch die lokationsbezogenen Daten kann sehr einfach eine Prozessoptimierung durchgeführt werden, wie z. B. standortabhängige Disponierung von Staplern im Logistikbereich.

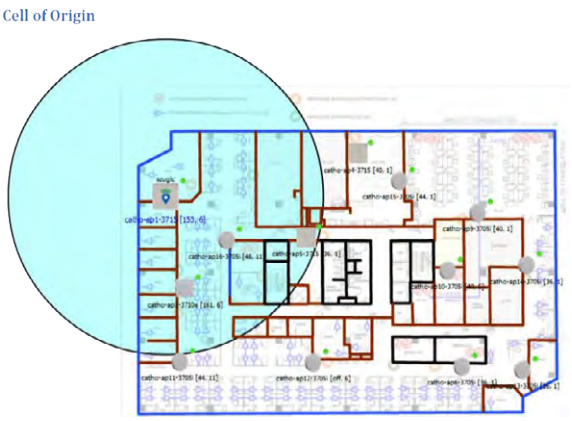
Für die Ortung selbst werden verschiedene Technologien eingesetzt:

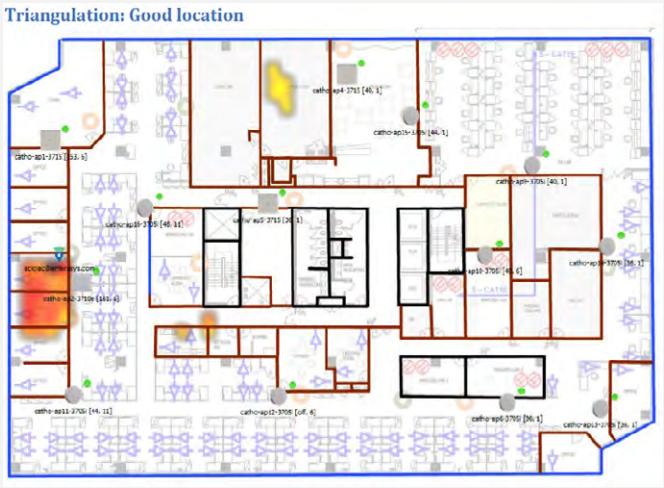
- **Anwesenheit** – Ein Tag sendet z. B. alle 2 Minuten oder sobald er bewegt wird ein Signal. So wird sichergestellt, dass immer die aktuelle Lokation angezeigt wird.
- **Echtzeit** – Ein Client/Tag wird gezielt vom User/System abgefragt und die aktuelle Lokation zurückgemeldet.
- **Lokationsbezogen** – Ein Tag wird bei Passieren einer bestimmten Lokation über einen so genannten Exiter gezwungen, seine Lokation an das System zu melden.

Weiterhin gibt es verschiedene Ortungsmethoden:

AP CONNECTION UND RSSI-WERT

- Die bekannte AP Lokation sowie der RSSI-Wert des Client ergibt eine Abstandsabschätzung
- Der Client befindet sich auf der RSSI-Kontour
- RF-Hindernisse haben Einfluss auf die RSSI-Kontour
- Zur Lokationsbestimmung wird die Client Sendestärke verwendet
- Triangulation
- Bekannte AP Lokationen und Client RSSI-Werte ermöglichen Distanzangaben
- Ab einer Anzahl von 3 Distanzwerten (APs) kann die Lokation sauber bestimmt werden
- RF-Hindernisse können die Qualität der Werte beeinflussen
- Folgende Faktoren können die Werte verbessern
- Anzahl der Aps, die den Client sehen
- Geometrie der APs
- Qualität des RF-Models des Gebäudeplans





SERVERBASIERENDES PATTERN MATCHING

- Der von mehreren APs gesehene RSSI-Pattern eines Clients kreiert einen eindeutigen „Fingerabdruck“
- Hat ein weiterer Client den selben RSSI-Pattern, ist er an der gleichen Lokation
- Client Sendestärke ist nicht relevant
- kein RF-Model des Gebäudes notwendig

Die identiFi WLAN-Lösung ermöglicht Location Tracking über die o. g. Methoden. Als Frontend-Applikation kann Netsight-ADV eingesetzt werden. Weiterhin ist ab der Version 9.15 ein zyklisches Abfragen von Clientlokationen via XML/PHP-Script möglich, um damit weitere Applikationen zu befüllen.

802.11n – Technologieübersicht

Mit der Einführung des 11n-Standards, der 2008 verabschiedet wurde, haben einige signifikante Änderungen und Verbesserungen in der WLAN Technologie Einzug gehalten. Aus technischer Sicht sind dies 3 Hauptkomponenten:

- **Multiple Input Multiple Output (MIMO) Technologie** – Bei 11a/b/g wurde bisher die gesamte Datenmenge über eine Antenne gesendet und empfangen. Mit der MIMO Technologie wird der Datenstrom über einen Splitter auf mehrere Sende-/Empfangsantennen (2 oder mehr Stück je nach Produkt) aufgeteilt. Die Anordnung der Antennen auf den WLAN Karten ist so gestaltet, dass die Ausbreitung des Funksignals räumlich versetzt erfolgt und es so zu keinen gegenseitigen Störungen bei der Übertragung kommt. Während die bisherigen Technologien teilweise Probleme mit Reflexionen hatten, nutzt MIMO diese bewusst und erreicht dadurch einen erhöhten Durchsatz, sowie auch eine robustere Kommunikation.
- **Kanalbündelung** – Der einfachste Weg, um den Durchsatz in einem WLAN Netz zu erhöhen, ist die Verdopplung des genutzten Frequenzbandes. 11n nutzt dies, um 2 benachbarte 20 Mhz-Kanäle zusammen zu fassen. Diese Technologie ist am effektivsten im 5 Ghz Bandbereich in dem 19, überlappungsfrei 20 Mhz-Kanäle zur Verfügung stehen. Im 2,4 Ghz-Bereich ist diese Technik weniger effektiv, da bereits mit der alten Technologie nur 3 überlappungsfreie Kanäle verfügbar sind. Durch Kanalbündelung wird dies auf einen Kanal vermindert, was einen praktikablen Einsatz ausschließt.
- **Packet Aggregierung** – Bei konventionellen WLAN Techniken ist der Overhead, um ein Datenpaket zu übermitteln fix, egal wie groß das Paket selbst ist. Bei 11n werden mehrere Nutzdatenpakete zu einem einzigen Sende-Frame zusammengefügt. Dadurch können mehrere Pakete mit den Overhead-Kosten eines einzigen Pakets gesendet werden. Die Effektivität dieser Technologie ist je nach Anwendung verschieden. Besonders groß ist der Vorteil z. B. bei großen Filetransfers, wobei aber Echtzeitanwendungen wie Voice oder Video davon nicht profitieren.

802.11N - MEHRWERTE

- **Erhöhte Kapazität** – Bei 11n wird die Kapazität einer WLAN Zelle von 14-22 Mbps bei 11a/g auf 100-200 Mbps erhöht. Verteilt auf mehrere User pro Zelle sind damit Geschwindigkeiten von bis zu 100 Mbps pro User möglich, was sich in der Praxis in einer größeren Bandbreite für mehr User zeigen wird.
- **Erhöhte Reichweite** – Durch die MIMO Technologie und das bewusste Arbeiten mit Reflexionen durch die räumlich versetzte Funkausbreitung der Funkwellen wird die Reichweite je AP erhöht. Dies wird auch dazu führen, dass die Datenrate mit steigendem Abstand vom AP zum Client langsamer fällt als bei den bisherigen Technologien und somit eine größere Abdeckung mit weniger APs erreicht wird.
- **Höhere Verfügbarkeit / Robustheit** – Bei den bisherigen Technologien kann die Performance eines WLAN Clients schon bei kleinsten Bewegungen oder Änderungen an der Umgebung (Schließen einer Tür, geänderter Einrichtung) stark beeinträchtigt werden. Dieses Problem wird durch Einsatz von unterschiedlichen Antennen entschärft. Fast jedes WLAN Gerät hat 2 Antennen, wobei immer nur die aktiv ist, die das beste Signal bekommt. Durch die MIMO Technologie sind bei 11n immer 2-3 Antennen gleichzeitig aktiv, die dadurch die Robustheit und Verfügbarkeit erhöhen.

802.11N – DESIGN

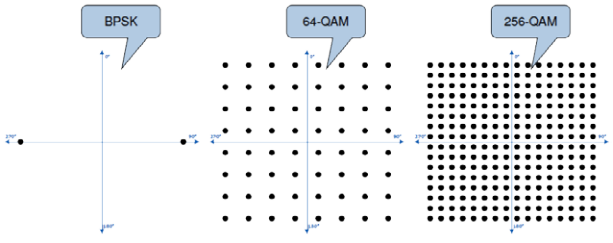
Durch die Abwärtskompatibilität von 802.11n mit a/b/g wird auch die Performance in einer 11n-Funkzelle auf die Geschwindigkeit der bisherigen Technologien verringert. Der größte Teil der bisherigen WLAN Clients arbeitet im 2,4 Ghz-Bereich. Durch die Einschränkung bei der Kanalbündelung in diesem Frequenzband und einer oft geforderten Unterstützung der bisherigen WLAN Clients wird im 2,4 Ghz-Bereich zukünftig 11n sehr oft in einem Kompatibilitätsmodus betrieben werden. Im 5 Ghz-Bereich hingegen wird der Vorteil durch Kanalbündlung voll ausgespielt und die neue Technik in einem 11n-only Modus gesetzt werden, wodurch die oben genannten Vorzüge voll zum Zuge kommen. Abwandlungen dieses Designs können je nach Anforderungen und Randbedingungen auftreten, so z. B. wenn man komplett neue WLAN Netze (Access Points & Clients unterstützen 11n) aufgebaut (Greenfield) oder wenn ein komplett unabhängiges 11n-Netz zu einem bestehenden 802.11a/b/g Netz aufgebaut wird (Overlay).

TECHNOLOGY	20 MHz	40 MHz	80 MHz	160 MHz
802.11b	11 Mbps			
802.11a/g	54 Mbps			
802.11n (1 SS)	72 Mbps	150 Mbps		
802.11ac (1 SS)	87 Mbps	200 Mbps	433 Mbps	867 Mbps
802.11n (2 SS)	144 Mbps	300 Mbps		
802.11ac (2 SS)	173 Mbps	400 Mbps	867 Mbps	1.7 Gbps
802.11n (3 SS)	216 Mbps	450 Mbps		
802.11ac (3 SS)	289 Mbps	600 Mbps	1.3 Gbps	2.3 Gbps
802.11n (4 SS)	289 Mbps	600 Mbps		
802.11ac (4 SS)	347 Mbps	800 Mbps	1.7 Gbps	3.5 Gbps
802.11ac (8 SS)	693 Mbps	1.6 Gbps	3.4 Gbps	6.9 Gbps

802.11ac – Next Generation Gigabit WLAN

Mit 802.11ac ist das nächste Enterprise WLAN Protokoll seit Anfang 2014 bereits verabschiedet. Mit 802.11ac halten neue Technologien Einzug, die bei 11n noch nicht berücksichtigt wurden:

- **Höhere Datenraten** – Potential für Gigabit-und Multi-Gigabit-Geschwindigkeiten - im Vergleich zu maximal 450Mbps mit 11n (per Funk)
- **Breitere Kanäle** – bis 80MHz und 160MHz - im Vergleich zu 20MHz und 40MHz bei 11n. Dies führt dazu, dass 11ac effektiv nur im 5Ghz Band beutzt werden kann, da im 2,4 Ghz Bereich nicht genügend überlappungsfreie Kanäle zur Verfügung stehen.
- **Zusätzliche Spatial Streams** – Bis zu 8 insgesamt (theoretisch) - bei 11n bis 4 insgesamt (kein Anbieter hat mehr als 3 Spatial Streams in Produkten umgesetzt)
- **Multi-User MIMO** – Fähigkeit, mehrere Stationen tx / rx auf dem gleichen Kanal zur gleichen Zeit zu bedienen - im Vergleich zu max. einer Station unterstützt bei 11n. Dies ist eine der vielversprechensten Technologieneuerungen innerhalb von 11ac, bringt allerdings auch eine erhebliche Komplexität in der technischen Umsetzung mit sich, so dass die erste Generation von 11ac Produkten diese Funktion noch nicht unterstützt.
- **Höhere Modulationsverfahren** – 256-QAM – im Vergleich max 64-QAM mit 11n



Ein weitere Hauptvorteil wird durch den bis zu 40% gesunkenen Energieverbrauch erwartet. Dies ermöglicht längere Batterielaufzeiten, für allem im Smartphone Bereich, mit gleichzeitig steigender Geschwindigkeit.

AUSBLICK & EMPFEHLUNG

WLAN Client-Karten mit 11ac werden bereits seit Anfang 2013 geliefert. Extreme Networks hat bereits heute ein vollständiges Portfolio von verschiedensten 11ac APs, um alle Anforderungen optimal abzudecken. Weiterhin können alle WLAN-Controller durch die Möglichkeit des flexiblen Handlings des Client-Traffics die gestiegenen Bandbreitenanforderungen von 11ac abdecken. Bei heutigen Planungen empfehlen wir das 5 Ghz Band mit zu berücksichtigen, um zukünftig einfach und ohne weitere Planungsschritte auf 11ac migrieren zu können. Die neuen 11ac WLAN-Clients werden abwärtskompatibel zu 11n sein, so dass ein sanfter Übergang sichergestellt ist. In Summe kann bereits heute bei Neuinvestitionen ein Umstieg auf 11ac empfohlen werden, da der Aufpreis zu älteren 11n-Produkten nur minimal ist und so eine langfristige Investitionssicherheit sicher gestellt ist.

Extreme networks

http://www.extremenetworks.com/contact / Phone +1-408-579-2800