

Ubiquiti UniFi

Beginners Guide

Inhalt:

Was ist UniFi und warum sollte mich das interessieren?.....	3
Das UniFi System:.....	3
Der UniFi Controller:.....	3
Der Software Controller:.....	4
CloudKey- dein Freund und Helfer.....	4
Die UniFi App:.....	5
Die UniFi Access Points.....	6
UAP Legacy Modelle:.....	6
UAP AC Modelle:.....	8
Indoor AC.....	8
Outdoor AC.....	10
Special Team:.....	12
Funktionen:.....	16
Router, Firewall und Switche.....	19
UniFi Security Gateway (USG).....	19
UniFi Switch:.....	20
Wissenswertes:.....	25
PoE - Was ist das?.....	25
WLAN Basics.....	26
Konfiguration.....	31
Erste Verbindung auf den CloudKey.....	31
Der UniFi Wizard.....	33
Adoptieren von Geräten.....	36
LED Farbcodes.....	37
Das Gäste WLAN.....	38
Das Portal.....	39
Der Hotspot Manager.....	40
VLAN.....	42
Tipps und Tricks.....	46
Fehlerbehebung:.....	48

Was ist UniFi und warum sollte mich das interessieren?

Bei UniFi von Ubiquiti handelt es sich um ein zentral verwaltetes Netzwerksystem. Im Gegensatz zu traditionellen Netzwerksystemen werden alle Komponenten über einen Controller visualisiert, administriert und überwacht. Daher ist es nicht nötig jedes Gerät, egal ob Netzwerkswitch, WLAN Access Point oder Router/ Firewall, einzeln und für sich isoliert zu konfigurieren. Vereinfacht gesagt ist es nur nötig zu wissen wie sie ihren UniFi Controller erreichen können um ihr gesamtes Netzwerk zu verwalten. Da dem Controller alle seine Netzwerkgeräte bekannt sind ist es zudem möglich komplexere Aufgaben, wie z.B. ein Gästeportal für ihr WLAN, der Aufbau von VLANs und vieles mehr, netzwerkübergreifend komfortabel und intuitiv zu lösen. Das spart ihnen Zeit, Geld und Nerven.

Das UniFi System:

Das UniFi System ist modular auf ihre Bedürfnisse anpassbar und kann jederzeit problemlos erweitert werden. Nachfolgend möchte ich ihnen die derzeitige Produktpalette etwas näher erläutern. Da Ubiquiti ständig an dem UniFi System feilt und es verbessert, ist es möglich das bereits weitere Lösungen für das UniFi System erschienen sind während sie das hier lesen. Besuchen sie doch einfach unsere Web Seite www.netzwerk2000.de oder gehen sie direkt auf www.ubnt.com um Neues zu erfahren.

Der UniFi Controller:

Der Controller ist das Gehirn des UniFi Systems und Anlaufstelle für alle UniFi Geräte. Bei traditionellen Umgebungen in denen alle Geräte lokal über z.B. ein Web-Interface konfiguriert werden bildet sich das Netzwerk nach und nach auf Basis der aktiven Geräte und Konfigurationen. Bei UniFi ist das anders, der Controller bringt Ordnung in das vermeintliche Chaos. Sie designen ihr Netzwerk von Anfang an über den Controller und alle für das jeweilige Gerät erforderlichen Informationen werden auf das Gerät repliziert. Somit ist es bis zu einem gewissen Grad sogar möglich, dass sie ihr komplettes Netzwerk konfigurieren noch bevor sie die Verpackung des ersten Gerätes überhaupt in die Hand nehmen. Der Basisbetrieb kann bei einem Ausfall des Controllers natürlich aufrecht erhalten werden, es ist aber dennoch davon abzuraten das WLAN so zu Planen das der Controller nur für die Inbetriebnahme verwendet wird und danach nicht mehr zur Verfügung steht. Stellen sie sich die UniFi Geräte als Schüler und den Controller als Lehrer vor. Lässt der Lehrer die Klasse unbeaufsichtigt, wissen wir vermutlich alle dass der normal Betrieb für längere Zeit nur bedingt funktioniert. Wenn sie ungeachtet dessen dennoch entschlossen sind ihren Access Point ohne Controller zu betreiben, finden sie in dem Ansatz „Die UniFi APP“ eine Beschreibung für den „Standalone Mode“. Davon ungeachtet empfehle ich ihnen dennoch wenn irgend möglich einen Controller zu betreiben da sie nur so den Funktionsumfang des UniFi Systems auch wirklich nutzen können. Ist von Beginn an eine reine App Lösung gewünscht sollten sie vielleicht einmal einen Blick auf die AmpliFi Serie von UBNT (www.amplifi.com) werfen, da diese für einen reinen App Betrieb ausgelegt ist.

Der Software Controller:

Sie können den UniFi Controller kostenlos für zahlreiche Plattformen von der Ubiquiti Website www.ubnt.com herunterladen. Der Software Controller eignet sich besonders bei größeren UniFi Umgebungen ab 30 UniFi Geräten und/oder wenn auf eine redundante Server Umgebung zurückgegriffen werden kann. Nach Möglichkeit sollte der Controller auf einer eigenständigen z.B. Virtuellen Maschine betrieben werden. Sie sollten tunlichst vermeiden einen produktiven Software Controller auf einer Workstation die auch für alltägliche Arbeiten benutzt wird zu betreiben, da andere Programme unter Umständen mit dem Controller in Konflikt geraten können. Wenn sie eine UniFi Umgebung aufbauen wollen, ohne eine Server oder VM Lösung aus dem Ärmel schütteln zu können, sollten sie sich den nachfolgenden Absatz besonders gut ansehen.



CloudKey- dein Freund und Helfer

Der CloudKey ist die All-in-Wonder Lösung für ihre UniFi Umgebung, er beinhaltet den vollständigen UniFi Software Controller in einem kleinen schnittigen Gehäuse. Der CloudKey sollte schon bei Umgebungen ab einem Access Point die erste Wahl sein. Da in Umgebungen mit weniger als 30 UniFi Geräten in der Regel keine gesonderte Hardware oder virtuelle Maschine zur Verfügung steht, führte das früher meist dazu, das die Software auf einem Notebook oder PC des Kunden bzw. Technikers installiert wurde. Das funktioniert bei der Einrichtung noch problemlos, die Erfahrung zeigt aber das meist schon bei der ersten Anpassung der UniFi Umgebung Probleme auftreten weil es z.B. die alte Hardware nicht mehr gibt, das Betriebssystem schon so Probleme macht das der Controller nicht mehr gestartet werden kann oder einfach ein anderer Techniker vorort ist. Wenn dann teils Stunden mit der Fehlersuche und in vielen Fällen die Neukonfiguration anfallen ist nicht nur der Kunde sauer, sondern auch die vermeintlichen Kosten für den CloudKey wären mit Leichtigkeit abgedeckt gewesen.



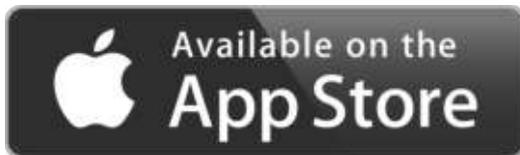
Grundsätzlich unterliegt der CloudKey mit 256+ UniFi Geräten der selbe "Beschränkung¹" wie der Software Controller. Je nach Umgebung sollten sie sich allerdings ab einer Größe von 30-40 UniFi Geräten überlegen ob sie anstelle des CloudKey nicht eine redundante Hardware mit Software Controller einsetzen möchten. Hartnäckig hält sich bei so manchem das Gerücht das der CloudKey nur ein Internet Gerät sei das alle Controlleraufgaben an einen Server irgendwo auf der Welt schickt. Das könnte nicht weiter von der Wahrheit entfernt sein. Alle Operationen werden vollständig von dem Winzling selbst erledigt. Seinen Namen verdankt der CloudKey einer Remote Management Lösung die mit dem Software Controller² nicht genutzt werden kann. Nach einer Registrierung unter <https://unifi.ubnt.com> können sie den CloudKey mit ihrem Account koppeln. Dadurch ist es möglich seine UniFi Umgebungen weltweit sicher, schnell und einfach zu administrieren. Dazu fungiert der gesicherte UniFi Server als gemeinsamer Treffpunkt für den CloudKey und ihrem PC/Notebook oder Smartphone. Der CloudKey meldet, wie er erreicht werden kann an den Server, der die Information für ihren Account hinterlegt. Wenn sie nun über die gesicherte Webseite auf den CloudKey zugreifen wird ein SSH Tunnel zwischen ihrem Gerät und dem CloudKey aufgebaut. Dieser ist verschlüsselt und sorgt dadurch für eine sichere Verbindung die nicht einmal von UBNT selbst eingesehen werden kann.

¹ Mit wachsendem Feature set und neuen Produkten ist es möglich, dass es in Zukunft eine Gerätebeschränkung für den CloudKey gibt.

² Als dieser Guide entstanden ist war die Cloud Funktion in dem Controller vorhanden konnte aber nicht aktiviert werden. Möglicherweise wird die Funktion in Zukunft auch mit dem Software Controller zur Verfügung stehen.

Die UniFi App:

Die UniFi App ist sowohl für iOS als auch Android Betriebssysteme verfügbar und kann kostenlos aus dem App- bzw. Play Store heruntergeladen werden. In erster Linie ist die APP für eine optimierte Administration ihres UniFi Controllers über das Smartphone oder Tablet konzipiert. Für kleinste Umgebungen oder für Tests ist es mit der App aber auch möglich einen Access Point in einem „Standalone Mode“ zu betreiben.



Standalone Mode:

Über die App können einzelne UniFi Access Points mit einem reduzierten Funktionsumfang auch als Access Point ohne Controllerverbindung konfiguriert werden. Ist der Standalone Mode aktiv, tritt der UAP als reiner Access Point mit WAP2 Verschlüsselung auf. Diese Funktion eignet sich besonders um z.B. die Reichweite eines Access Points Vorort zu bestimmen da kein CloudKey oder Notebook mit UniFi Software Controller erforderlich ist. Wenn Zugang zu dem Objekt oder der Baustelle möglich ist kann so die Planung der nötigen Access Points teils erheblich erleichtert werden da je nach Umgebung echte Verbindungstests durchgeführt werden können. Der UniFi Access Point kann natürlich jederzeit zurückgesetzt und in einen UniFi Controller eingebunden werden.



Die UniFi Access Points

Ubiquiti hat ein breites Sortiment an Access Points für den In- und Outdoor Betrieb. Nachfolgend möchten ich ihnen die derzeit verfügbaren Modelle etwas näherbringen. Die Ubiquiti Access Points (kurz UAPs) können in zwei Hauptgruppen unterteilt werden, die Modelle der **"AC"** Serie und der **"Legacy"** Serie.

UAP Legacy Modelle:

Bei der Legacy Serie handelt es sich um Modelle die zwar eigentlich bereits durch Modelle der neueren AC Serie ersetzt worden sind, aufgrund ihrer ungebrochene Beliebtheit aber weiterhin produziert und vertrieben werden. Die Legacy Modelle (UAP, UAP-LR und UAP-Outdoor+) werden meist in bestehenden Umgebungen eingesetzt um die Optik zu wahren. Außerdem verfügen nur die Modelle der Legacy Serie über das proprietäre Protokoll "Zero HandOff Roaming" das nachfolgend noch etwas genauer behandelt wird.

UAP

Den UAP könnte man als Urvater der UniFi Access Points bezeichnen. Er ist zwar mittlerweile durch den UAP-AC-LITE abgelöst worden, wird allerdings gerne weiterhin in bestehenden Umgebungen eingesetzt. Die Stromversorgung erfolgt mittels 24V Passiv PoE und er eignet sich besonders für Umgebungen mit kleinerem Verbindungsaufkommen. Neben dem sehr günstigen Preis ist in manchen Umgebungen auch die Optik ein entscheidender Faktor, denn nur die Access Points UAP und UAP-LR verfügen über einen Grüne LED Status Ring. Wird also lediglich das 2,4Ghz Band benötigt, könnten die Legacy UAP Modelle eine interessante Alternative zu den AC Modellen sein.



UAP-LR

Der UAP Long Range wurde durch den UAP-AC-LR abgelöst und wird wie sein kleiner Bruder gerne in bestehenden Umgebungen, bei denen die Optik gewahrt werden soll oder ZeroHandoff Roaming verwendet wird, eingesetzt. Er operiert im 2,4Ghz Bereich und eignet sich mit seiner Reichweite von bis zu 188m besonders um weitläufigere Umgebungen mit kleinerem Verbindungsaufkommen abzudecken (z.B. Warenlager)



UAP-OUTDOOR+

Der UAP Outdoor Plus ist wie der Name schon vermuten lässt für den Betrieb im Außenbereich konzipiert. Mit einer Reichweite von bis zu 183m kann schon die Standard Konfiguration ein recht weitläufiges Areal versorgen. Anders als die beiden Indoor Modelle verfügt der UAP Outdoor+ über zwei Externe RP-SMA Antennen. So können optional auch andere Antennen mit dem Access Point betrieben werden. Wie auch die beiden anderen Legacy Modelle operiert der UAP Outdoor+ ausschließlich im 2,4Ghz Frequenzband.



Modell Übersicht:



	UAP	UAP-LR	UAP-OUTDOOR+
Frequenzen	2,4GHz	2,4GHz	2,4GHz
Durchsatz LAN	10/100 Mbps	10/100 Mbps	10/100 Mbps
WLAN Standards	802.11b/g/n	802.11b/g/n	802.11b/g/n
Strom Versorgung	Passiv PoE	Passiv PoE	Aktiv PoE 802.3 af
Verbrauch max.	6W (24V/0,5A)	6W (24V/0,5A)	8W (48V/0,5A)
Injektor Inkl.	Single ✓ 3Pack ✓	Single ✓ 3Pack ✓	Single ✓
Netzwerkports	1Stk	1Stk	1Stk
Reichweite³	122m	188m	183m
Clients	100+ 30 (ohne QoS)	100+ 30 (ohne QoS)	100+ 30 (ohne QoS)
802.1q (VLAN)	✓	✓	✓
Zero HandOff Roaming	✓	✓	✓
Fast Roaming 802.11r	✗	✗	✗
Wireless Uplink	✓	✓	✓
MESH	✗	✗	✗
MiMo	2x2 (2,4GHz bis 300Mbps)	2x2 (2,4GHz bis 300Mbps)	2x2 (2,4GHz bis 300Mbps)
Montage	Indoor	Indoor	Outdoor
Lautsprecher	✗	✗	✗

³ Reichweiten Angabe bei Laborbedingungen und frei Sicht

UAP AC Modelle:

Die UAP-AC Modelle stellen die aktuelle Generation der UniFi Access Points da. Mit ihnen wurden die Legacy Modelle abgelöst und die Produkt Palette weiter ausgebaut. Neben den drei Standard Modellen UAP-AC-LITE, UAP-AC-LR und UAP-AC-PRO wurden mit der AC Serie weitere spezialisierte APs eingeführt. Die Serie verdankt ihrem Namen der Einführung des IEEE 802.11ac Standards, mit dem zu dem 2,4GHz auch das 5,4GHz Frequenz Band Einzug gehalten hat. Die Verwendung von zwei Frequenzbändern ermöglicht eine erheblich flexiblere Steuerung der Endgerätdichte und liefert auch einen höheren Gesamtdurchsatz.

Indoor AC

UAP-AC-LITE:

Der UAP-AC-LITE ist der kompakteste der drei Standard Modelle und für Umgebungen mit kleinerem Verbindungsaufkommen (z.B. Privat Haus oder Wohnung) ausgerichtet. Der UAP-AC-LITE wird mit 24V Passiv PoE oder 802.3af Aktiv PoE betrieben. Er besitzt zwar den geringsten Datendurchsatz (2,4GHz bis 300Mbps | 5,4GHz bis 867Mbps), mit seiner Ausrichtung für kleinere Umgebungen wirkt sich das im Realbetrieb allerdings in der Regel nicht aus.



UAP-AC-LR:

Der UAP Long Range, wird bevorzugt in Umgebungen eingesetzt in denen möglichst große Bereiche (bei kleiner bis mittlerer Verbindungsdichte) mit möglichst wenigen Access Points abgedeckt werden soll (z.B. Warenlager, Großraum Büro etc.). Wie sein kleiner Bruder kann er sowohl mit 24V Passiv PoE oder 802.3af Aktiv PoE betrieben werden. Mit seinem Datendurchsatz (2,4GHz bis 450Mbps | 5,4GHz bis 867Mbps) liegt er schon deutlich über dem des UAP-AC-LITE. Da er allerdings auch eine erheblich größere Fläche abdeckt, sollten sie hier das Verbindungsaufkommen nicht aus den Augen verlieren und gegebenenfalls auf mehrere kleinere Access Points anstelle eines großen zurückgreifen.



UAP-AC-PRO

Der UAP-AC-PRO ist sowohl vom Gehäuse als auch der Ausstattung der größte der drei Standard UAP-AC Modelle. Er wird ausschließlich mit 802.3af Aktiv PoE betrieben und verfügt im Gegensatz zu seinen kleineren Geschwistern über eine zusätzliche RJ45 Buchse. Diese ist traditionsbedingt weiterhin ausgeführt und war ursprünglich für die Anbindung an eine Richtfunkstrecke gedacht. Grundsätzlich wäre auch ein DaisyChain Betrieb möglich, empfehlen würde ich es ihnen allerdings nicht da sie sich so selbst eine „Stolperfalle“ bauen. Er verfügt über den höchsten Datendurchsatz der drei (2,4GHz bis 450Mbps | 5,4GHz bis 1300Mbps) und ist für den Einsatz in Umgebungen mit dichtem Verbindungsaufkommen (z.B. Hotel Lobby, Besprechungszimmer, Restaurant etc.) ausgelegt. Der Verpackung liegt zudem eine Silikonabdeckung bei, die den AC-PRO für die Feuchtraummontage tauglich macht.



Indoor Modelle Übersicht:



	UAP-AC-LITE	UAP-AC-LR	UAP-AC-PRO
Frequenzen	2,4GHZ und 5,4GHz	2,4GHZ und 5,4GHz	2,4GHZ und 5,4GHz
Durchsatz LAN	10/100/1000 Mbps	10/100/1000 Mbps	10/100/1000 Mbps
WLAN Standards	802.11a/b/g/n/ac	802.11a/b/g/n/ac	802.11a/b/g/n/ac
Strom Versorgung	Passiv PoE oder Aktiv PoE 802.3af	Passiv PoE oder Aktiv PoE 802.3af	Aktiv PoE 802.3af
Verbrauch max.	6,5W (24V/0,5A)	6,5W (24V/0,5A)	9W (48V/0,5A)
Injektor Inkl.	Single ✓ 5Pack ✗	Single ✓ 5Pack ✗	Single ✓ 5Pack ✗
Netzwerkports	1 Stk	1 Stk	2Stk 1x LAN IN 1x GBit Passthrough
Reichweite⁴	122m	188m	122m
Clients	200+ 60 (ohne QoS)	200+ 60 (ohne QoS)	200+ 60 (ohne QoS)
802.1q VLAN	✓	✓	✓
Zero HandOff Roaming	✗	✗	✗
Fast Roaming 802.11r	✓	✓	✓
Wireless Uplink	✓	✓	✓
MESH	✗	✗	✗
MiMo	2x2 (2,4GHz bis 300Mbps) 2x2 (5,4GHz bis 867Mbps)	3x3 (2,4GHz bis 450Mbps) 3x3 (5,4GHz bis 867Mbps)	3x3 (2,4GHz bis 450Mbps) 3x3 (5,4GHz bis 1300Mbps)
MU MiMo AC Wave 2	✗	✗	✗
SSR (Spectral Security Radio)	✗	✗	✗
Montage	Indoor	Indoor	Indoor/Outdoor ⁵
Lautsprecher	✗	✗	✗

4 Reichweiten Angabe bei Laborbedingungen und frei Sicht.

5 Feuchtraum geeignet.

Outdoor AC

Die Outdoor Modelle der UAP-AC sind für den Einsatz in rauer Umgebung von bis zu -40°C und $+70^{\circ}\text{C}$ ausgelegt. Sie können sowohl direkt an einen Mast oder an die Wand montiert werden. Als Besonderheit können der UAP-AC-M und UAP-AC-M-PRO ein MESH Netzwerk aufbauen. Weiter unten finden sie hierzu eine genauere Beschreibung.

UAP-AC-M

Der UAP-AC-M ist der kompaktere der beiden MESH Outdoor APs und kann wahlweise mit 24V Passiv PoE oder 802.3af Aktiv PoE betrieben werden. Er ist mit zwei RP-SMA Antennen ausgestattet die bei Bedarf einfach gegen andere Antennen getauscht werden können (z.B. Sektorantenne). Der Access Point widersteht selbst harschen Bedingungen von -30°C bis $+70^{\circ}\text{C}$ und ist Out-of-the-Box für die Mast- oder Wandmontage ausgestattet. Mit seinem Datendurchsatz (2,4GHz bis 300Mbps | 5,4GHZ bis 867Mbps) eignet er sich primär für Umgebungen mit mittelstarkem Verbindungsaufkommen (z.B. Garten, Wohnstraße, Lager, etc.).



UAP-AC-M-PRO

Der UAP-AC-M-PRO verfügt über 3x3 MiMo und wird über 802.3af Aktiv PoE mit Strom versorgt. Anders als sein kleinerer Bruder verfügt er über keine externen Antennen, und kann in extremen Umgebungen von -40°C bis $+70^{\circ}\text{C}$ betrieben werden. Eine Montage an der Wand oder Masten ist durch die modulare Aufhängung problemlos möglich. Mit seinem Datendurchsatz (2,4GHz bis 450Mbps | 5,4GHZ bis 1300Mbps) eignet er sich für Umgebungen mit hohem Verbindungsaufkommen und kann durch die höhere Kapazität besonders gut als netzgebundener AP oder Relay AP in Multi Hop Umgebungen eingesetzt werden.



Outdoor Modelle Übersicht:



	UAP-AC-M	UAP-AC-M-PRO
Frequenzen	2,4GHZ und 5,4GHZ	2,4GHZ und 5,4GHZ
Durchsatz LAN	10/100/1000Mbps	10/100/1000Mbps
WLAN Standards	802.11a/b/g/n/ac	802.11a/b/g/n/ac
Strom Versorgung	Passiv PoE oder Aktiv PoE 802.3af	Aktiv PoE 802.3 of
Verbrauch max.	8,5W (24V/0,5A)	9W (48V/0,5A)
Injektor Inkl.	Single ✓ 5Pack ✗	Single ✓ 5Pack ✗
Netzwerkports	1 S1k	2 S1k 1x LAN IN 1x GBit Passthrough
Reichweite⁶	183m	183m
Clients	250+ 60 (ohne QoS)	250+ 60 (ohne QoS)
802.1q VLAN	✓	✓
Zero HandOff Roaming	✗	✗
Fast Roaming 802.11r	✓	✓
Wireless Uplink	✓	✓
MESH	✓	✓
MiMo	2x2 (2,4GHz bis 300Mbps) 2x2 (5,4GHz bis 867Mbps)	3x3 (2,4GHz bis 450Mbps) 3x3 (5,4GHz bis 1300Mbps)
MU MiMo AC Wave 2	✗	✗
SSR (Spectral Security Radio)	✗	✗
Montage	Outdoor	Outdoor
Lautsprecher	✗	✗

⁶ Reichweiten Angabe bei Laborbedingungen und frei Sicht.

Special Team:

Neben den bereits Vorgestellten UAPs gibt es auch noch Access Points in der UniFi Familie die für Spezielle Anwendungen optimiert worden sind.

UAP-AC-IW und UAP-AC-IW-PRO

Der UAP-AC-IW ist speziell für kleine Umgebungen entwickelt worden, bei denen der Fokus auf die Abdeckung eines speziellen Bereichs liegt und eine zu große Ausbreitung verhindert werden soll. Klassische Anwendungsfälle sind hier Hotelzimmer. Nicht in allen Hotel Szenarios ist es gewünscht, möglichst viele Zimmer mit möglichst wenig Access Points "irgend-wie" abzudecken. Ein dedizierter AP pro Zimmer ermöglicht weitreichende Steuerungsmöglichkeiten die anders nicht umgesetzt werden können. So gibt es einen wachsenden Trend bei Hotelgäste nach Möglichkeit die WLAN Strahlung während des Schlafes zu vermeiden. In einer Umgebung mit UAP-AC-IW ist es ein leichtes den Access Point punktgenau für dieses eine Zimmer zu deaktivieren ohne andere Zimmer in Mitleidenschaft zu ziehen. Durch die Reichweite von max. 80m auf freie Sicht bleibt der betreffende Gast auch von den Funksignalen des Nachbarn verschont während dieser weiterhin sein WLAN nutzen kann. Die Access Points verfügen zudem noch über einen PoE Passthrough und LAN Port. Der UAP-AC-IW-PRO entspricht in Aussehen und Funktion dem UAP-AC-IW erreicht aber einen höheren Durchsatz.



UAP-AC-HD

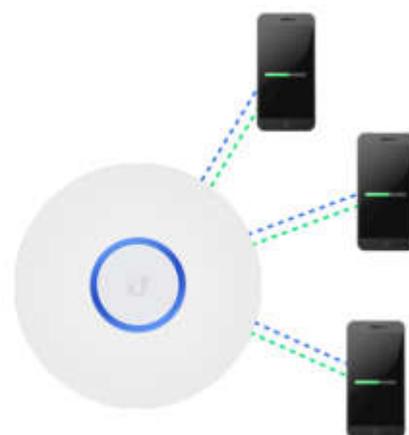
Der UAP-AC-HD verfügt als erster UAP über den neuen 802.11ac Wave2 Standard mit MU MiMo Unterstützung. Mithilfe des neuen AC Standards kann die Kommunikation mit den Endgeräten zielgerichteter erfolgen was dem UAP-AC-HD erlaubt bis zu 500 Verbindungen simultan aufzunehmen. So eignet er sich besonders gut für Umgebungen mit sehr dichtem Verbindungsaufkommen (z.B. Stadion, Aula, Konzerthallen, Schulen etc.). Der höheren Leistung geschuldet, wird der Access Point über den stärkeren 802.3at Aktiv PoE Standard mit Strom versorgt.



Mu MiMO Aus

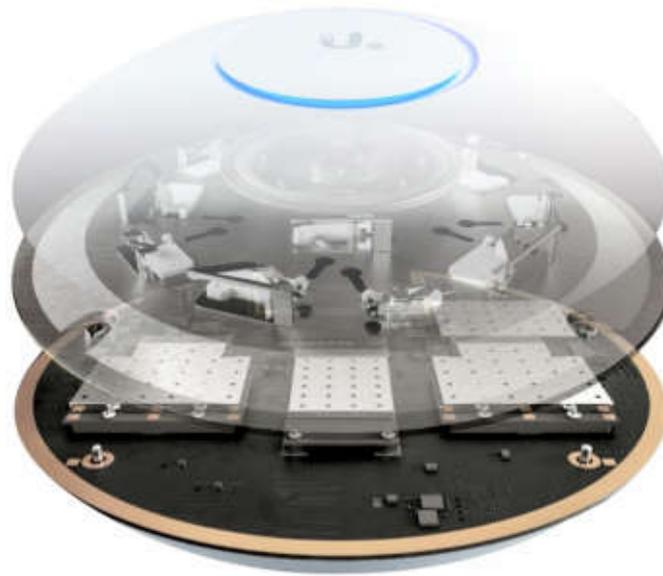


Mu MiMO Ein



UAP-AC-SHD

Der UAP-AC-SHD ist wie der UAP-AC-HD mit dem neuen AC Wave2 Protokoll und MU MiMo ausgestattet. Er verfügt aber zusätzlich über ein dediziertes Security Radio welches kontinuierlich das Spektrum im 2,4GHz und 5,4GHz Band überwacht. So kann nicht nur die eigene Kommunikation optimiert, sondern auch Störquellen gezielt aufgespürt werden. Interessant ist diese Funktion primär für Umgebungen in denen aus Sicherheitsgründen die Kommunikation über alternative Access Points wie z.B. einem persönlichen Hotspot via Smartphone unterbunden oder Angriffe über z.B. Man-in-the-Middle Attacken vorgebeugt werden muss. Klassische Anwendungsgebiete sind hier z.B. Banken, Krankenhäuser oder Universitäten.



UAP-AC-EDU

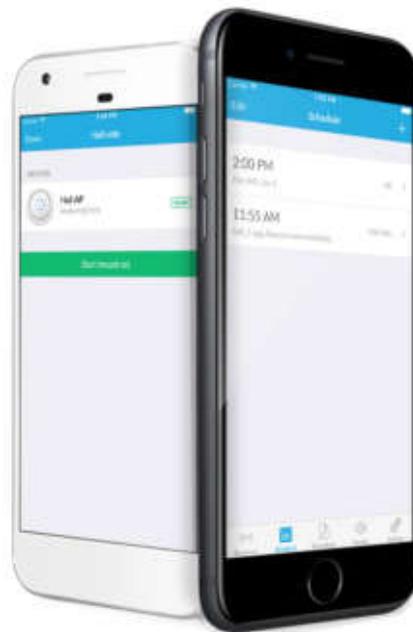
Der UAP-AC-EDU wurde speziell für Schulen, Universitäten, Bildungszentren und ähnliches entwickelt. Der eigentliche Access Point trägt hier noch einen leistungsstarken 60W Lautsprecher huckepack. Über den Lautsprecher können via App Durchsagen oder Audio Dateien⁷ ausgegeben werden. Das kann auch zeitgesteuert passieren um z.B. das Pausenklingeln abzuspielen. Der Access Point selbst entspricht dem UAP-AC-PRO benötigt aber aufgrund des Lautsprechers den stärkeren 802.3at Aktiv PoE Standard. Mit seiner Datenrate (2,4Ghz bis 450Mbps | 5,4GHz bis 1300Mbps) ist er auch für große Verbindungsaufkommen bestens gerüstet. Die Montage erfolgt, bedingt durch die Bautiefe aufgrund des Lautsprechers grundsätzlich nur in abgehängten Decken oder Rigips Wänden.



UniFi EDU App

Die UniFi EDU App ist sowohl für iOS als auch Android verfügbar. Über die App werden alle für den Lautsprecher relevanten Aktionen ausgeführt.

Neben Durchsagen können sie auch Audio Files, wahlweise manuell oder zeitgesteuert, aus der App wiedergegeben.



⁷ Musik Streaming ist nicht möglich

Special Team Modelle Übersicht:



	UAP-AC-IW	UAP-AC-HD	UAP-AC-SHD	UAP-AC-EDU
Frequenzen	2,4GHZ und 5,4GHZ	2,4GHZ und 5,4GHZ	2,4GHZ und 5,4GHZ	2,4GHZ und 5,4GHZ
Durchsatz LAN	10/100/1000 Mbps	10/100/1000 Mbps	10/100/1000 Mbps	10/100/1000 Mbps
WLAN Standards	802.11a/b/g/n/ac	802.11a/b/g/n/ac/ ac-wave 2	802.11a/b/g/n/ac/ ac-wave 2	802.11a/b/g/n/ac
Strom Versorgung	Aktiv PoE+ 802.3 at	Aktiv PoE+ 802.3 at	Aktiv PoE+ 802.3 at	Aktiv PoE+ 802.3 at
Verbrauch max.	6W (48V/0,5A)	17W (48V/0,5A)	17W (48V/0,5A)	20W (48V/0,5A)
Injektor Inkl.	Single ✗ 5Pack ✗	Single ✓ 5Pack ✗	Single ✓ 5Pack ✗	Single ✓ 5Pack ✗
Netzwerkports	3Stk 1xLAN IN 1xPOE Passthrough 1x1GBit Passth.	2Stk 1x LAN IN 1x GBit Passthrough	2Stk 1xLAN IN 1xGBit Passthrough	1Stk
Reichweite⁸	100m	122m	122m	122m
Clients	100+ 30 (ohne QoS)	500+ 120 (ohne QoS)	500+ 120 (ohne QoS)	200+ 60 (ohne QoS)
802.1q VLAN	✓	✓	✓	✓
Zero HandOff Roaming	✗	✗	✗	✗
Fast Roaming 802.11r	✓	✓	✓	✓
Wireless Uplink	✓	✓	✓	✓
MESH	✗	✗	✗	✗
MiMo	UAP-AC-IW 3x3 (2,4GHz bis 300Mbps) 3x3 (5,4GHz bis 867Mbps) UAP-AC-IW-PRO 3x3 (5,4GHz bis 450Mbps) 3x3 (5,4GHz bis 1300Mbps)	4x4 (2,4GHz bis 800Mbps) 4x4 (5,4GHz bis 1733Mbps)	4x4 (2,4GHz bis 800Mbps) 4x4 (5,4GHz bis 1733Mbps)	3x3 (2,4GHz bis 450Mbps) 3x3 (5,4GHz bis 1300Mbps)
MU MiMo AC Wave 2	✗	✓	✓	✗
SSR (Spectral Security Radio)	✗	✗	✓	✗
Montage	Indoor	Indoor/Outdoor ⁹	Indoor	Indoor
Lautsprecher	✗	✗	✗	✓

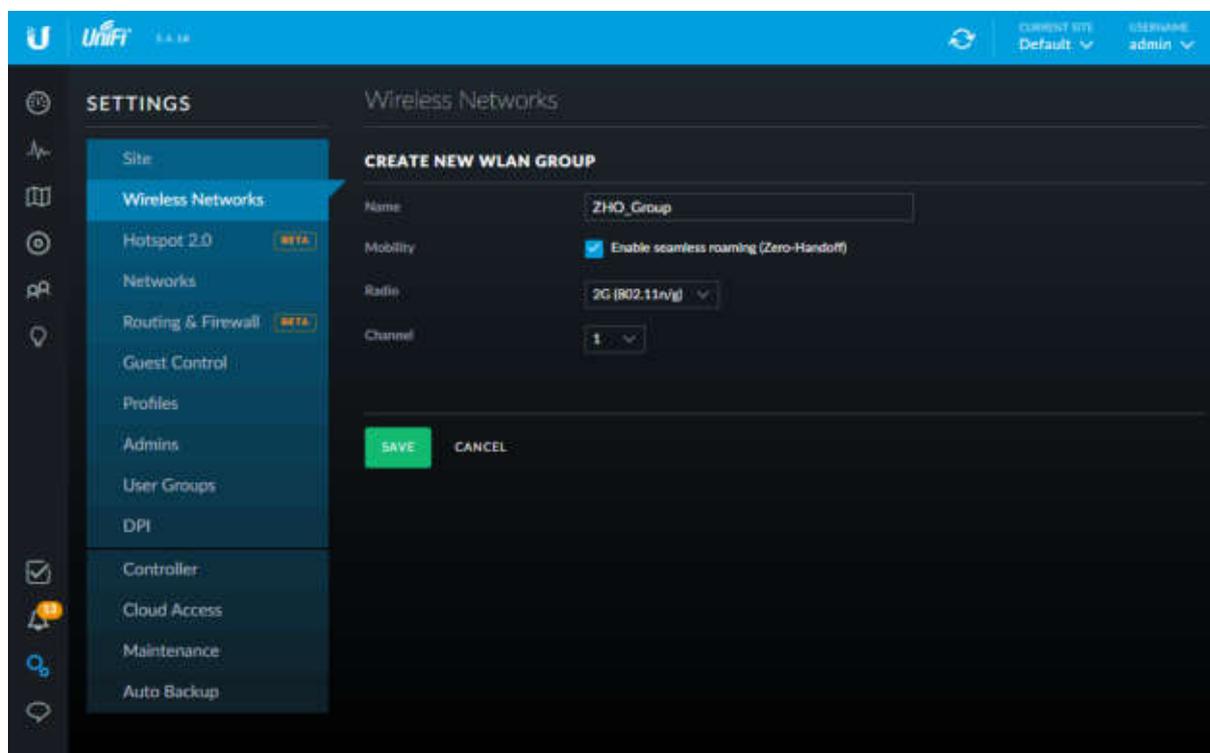
⁸ Reichweiten Angabe bei Laborbedingungen und frei Sicht.

⁹ Feuchtraum geeignet.

Funktionen:

Zero HandOff Roaming:

Da der UniFi Controller alle seine Access Points zentral verwaltet wird auch die SSID, wenn nicht anders konfiguriert, auf alle APs ausgestrahlt. Haben sie nun z.B. 5Stk UAPs mit ihrem UniFi Controller gepaart, melden sich alle 5Stk mit derselben SSID. Um sich nicht durch endlose Listen mit SSIDs scrollen zu müssen, nur um sein Smartphone oder Notebook mit dem WLAN zu verbinden, wird in der Regel am Client Gerät die SSID nur einmal angezeigt. Verbinden sie sich nun mit der SSID, sucht ihr Client den AP mit dem besten Signal und baut die Verbindung auf. Setzt sich der Client innerhalb des Wirkungsbereichs in Bewegung so verändert sich auch das Signal zwischen beiden Geräten zum Besseren oder Schlechteren. Wird ein vordefinierter Signalpegel unterschritten so trennt der Client die Verbindung und wechselt auf einen anderen bekannten Access Point um die Verbindung mit dem Netzwerk sicherzustellen. Bei diesem Verbindungswechsel gehen immer ein paar Datenpakete verloren. Für die meisten Anwendungen ist das auch kein Problem weil die entsprechenden Pakete neu angefordert werden und der User davon nichts mit bekommt. Allerdings gibt es auch spezielle Anwendungen bei denen Pakete nicht einfach erneut angefordert werden können. Bei Zero HandOff Roaming verhält es sich etwas anders, hier wird dem Client vorgespielt das alle UAPs (in unserm Beispiel 5Stk) in Wirklichkeit nur EIN Access Point ist. So kümmert sich der Controller dann um den Wechsel zwischen den APs, dadurch kann für den Client eine wesentlich kürze Latenzzeit erreicht werden. Das kann für spezielle Anforderungen wie z.B. selbstfahrende Stapler Systeme erforderlich sein, für den normalen Betrieb in Büros, Schulen, Hotels, Haushalten etc. ist diese Funktion aber in der Regel weder nötig noch empfehlenswert.



INFO: Das Zero HandOff Roaming ist nicht für die Modelle der AC Serie verfügbar. Bei den AC Modellen (mit Ausnahme des UAP-AC Gen1) wird eine generelle Verbesserung des Roaming durch den IEEE Standard 802.3r erreicht. Dadurch ist das ZHO Roaming bei den AC Modellen auch nicht mehr relevant.

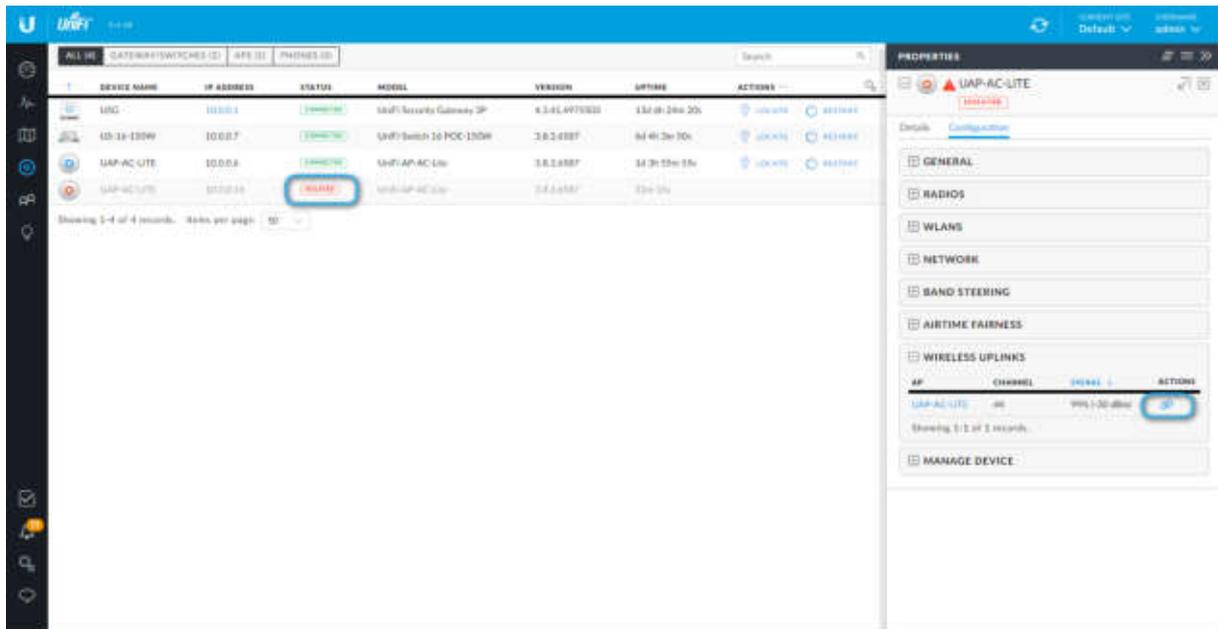
Fast Roaming

Die Modelle der AC Serie verfügen über das sogenannte Fast Roaming das in dem IEEE Standard 802.3r definiert ist und das Zero HandOff Roaming der Legacy Modelle abgelöst hat. Durch das einbringen in einen Industriestandard kann zudem die Kompatibilität unter den verschiedenen Herstellern verbessert werden.

Wireless Uplink:

Mit der Funktion Wireless Uplink können sie eine Funkbrücke zwischen zwei UAPs aufbauen.

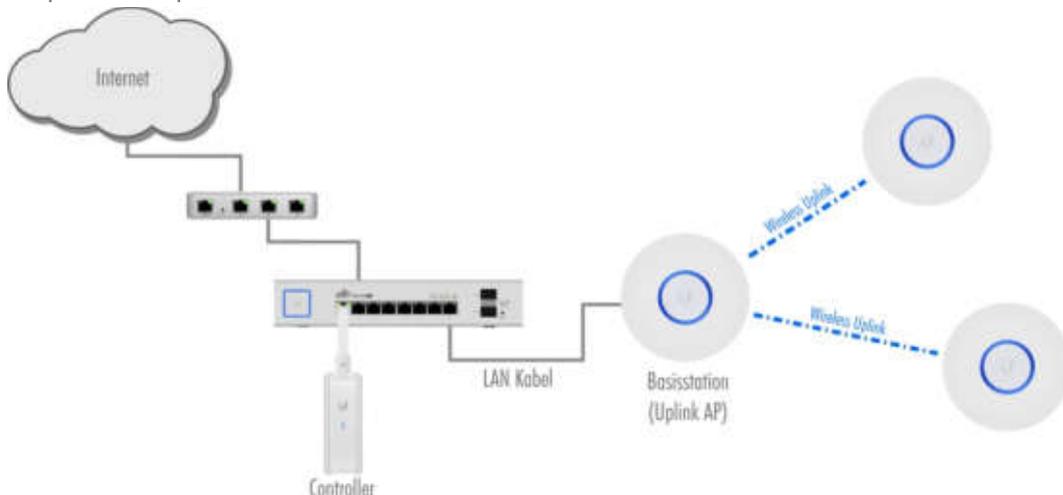
Einer ist dabei über Kabel mit ihrem Netzwerk verbunden und der zweite wird via Funk gekoppelt. Diese Funktion ist z.B. bei Installationen im Außenbereich wie in Gärten, Parks etc. praktisch da in solchen Umgebungen meist leichter eine Stromquelle als eine Netzwerkverkabelung zur Verfügung steht. Erkennt ein adoptierter UAP einen UAP ohne Kabelverbindung in seiner Reichweite, wird dieser als "Isoliert" angezeigt und kann über Wireless Uplink gekoppelt werden. Wurde der UAP noch nicht mit dem Controller gekoppelt müssen sie lediglich wie gewohnt auf "Adopt" klicken um den UAP hinzuzufügen, die Verbindung über Wireless Uplink wird dann im Hintergrund automatisch durchgeführt. Haben sie den UAP bereits mit einer Kabelverbindung im Controller adoptiert müssen sie diesen erst auf Wireless Uplink umstellen. Wählen sie dazu den als „Isoliert“ angezeigten UAP aus und klicken sie unter „Configuration\Wireless Uplink“ auf das „Link“ Symbol  das neben dem gewünschten kabelgebundenen UAP angezeigt wird.



The screenshot shows the UniFi Controller interface. On the left, a table lists devices with columns for Device Name, IP Address, Status, Model, Version, and Uptime. The 'UAP-AC-LITE' device is highlighted with a red box around its status 'Isolated'. On the right, the 'PROPERTIES' panel for 'UAP-AC-LITE' is shown, with the 'WIRELESS UPLINKS' section expanded and a 'Link' button circled in red.

DEVICE NAME	IP ADDRESS	STATUS	MODEL	VERSION	UPTIME	ACTIONS
LDG	10.0.0.1	CONNECTED	SWT-Security Gateway 3P	4.3.0.4977803	13:01:26w 25s	UNLINK RECONNECT
LD-16-120W	10.0.0.7	CONNECTED	SWT-Switch 16-POE-120W	3.0.3.438P	04:46:3w 10s	UNLINK RECONNECT
UAP-AC-LITE	10.0.0.8	ISOLATED	SWT-UAP-AC-Lite	3.0.2.658P	14:3h 15w 15s	UNLINK RECONNECT
UAP-AC-LITE	10.0.0.9	ISOLATED	SWT-UAP-AC-Lite	3.0.2.658P	13w 13s	UNLINK RECONNECT

Wireless Uplink Konzept:

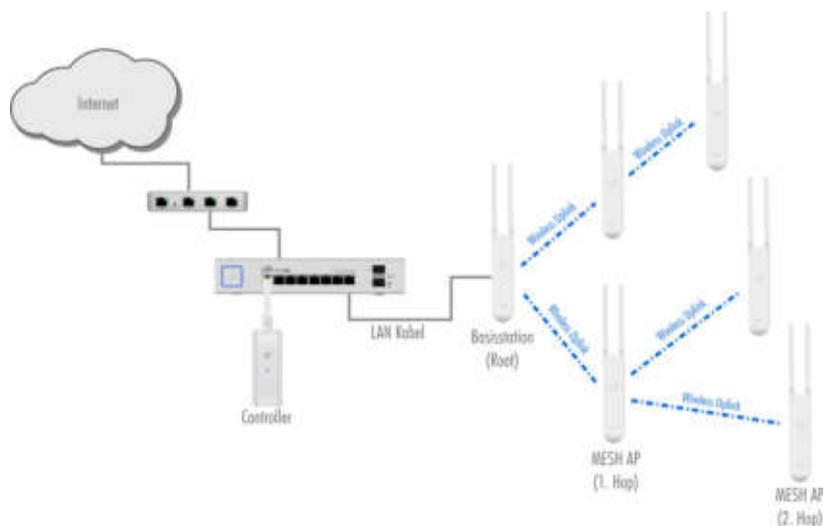


Info: Wireless Uplink ist zwar sowohl für die Legacy und AC Serie verfügbar, ein Mischen der Serien über Wireless Uplink ist aber nicht möglich.

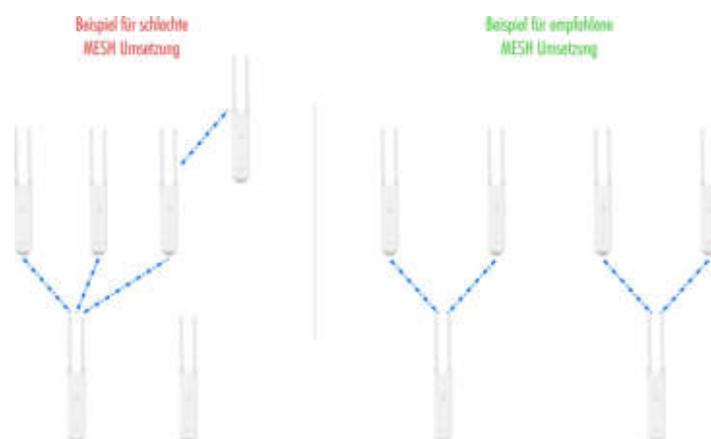
MESH Netzwerk:

Die UniFi MESH Modelle UAP-AC-M und UAP-AC-M-PRO können zusätzlich zu Wireless Uplink auch ein MESH Netzwerk aufbauen. Bei einem Wireless Uplink ist es nur möglich einen einzelnen Hop aufzubauen, also einen UAP der über ein Kabel an das Netzwerk verbunden ist, mit einem oder mehrere UAPs über Funk zu koppeln. Bei einem MESH Netzwerk ist es hingegen auch möglich Multi-Hops aufzubauen, es können also auch UAPs mit einem Access

Point verbunden werden der selbst über Funk mit einem UAP verbunden ist. So kann auch mit einer kleinen Anzahl von Netzwerkanschlüssen eine große Fläche mit WLAN versorgt werden. Bevor sie jetzt aber losstürmen und all ihre Netzkabel aus der Wand reißen weil sie zukünftig alles via MESH anbinden wollen, sollten sie bedenken dass es natürlich auch eine Kehrseite gibt. Dadurch, dass neben der Clients auch alle MESH angebundene APs über Funk miteinander kommunizieren erhöht sich entsprechend das Verbindungsaufkommen was den Datendurchsatz reduziert. Natürlich ist die tatsächliche Reduktion von vielen Faktoren abhängig aber für ein „worst case“ Szenario sollten wir pro Hop eine Reduktion von bis zu 50% annehmen. Somit hätte der zweite Hop nur mehr 25% der ursprünglichen Bandbreite. Im Realbetrieb sollten die Werte durchaus besser aussehen aber für die Planung zeigt das Beispiel worauf bei einem MESH Netzwerk zu achten ist. Zusammengefasst ist MESH ein extrem mächtiges Werkzeug um WLAN auch an Orten verbreiten zu können in denen es ansonsten gar nicht oder nur mit großem Aufwand möglich wäre. Allerdings sollte für ein bestmögliches Ergebnis eine sorgfältige Planung durchgeführt werden.



Da MESH ein intelligentes System ist, verfügt es über mehr Steuermöglichkeiten als ein "einfacher" Wireless Uplink. So ist möglich die via Funk angebundene APs zu gruppieren und gezielt einem bzw. mehreren "Relay" APs (Kabel oder Funkgebunden) zuzuweisen. So ist sichergestellt das nicht ein einzelner AP unter der Last aller angebundene APs zusammenbricht, während andere APs unterfordert sind. Zudem ist es möglich ein Fallback zu definieren. Fällt ein APs aus, egal ob "Relay" AP oder direkt an das Netzwerk angeschlossen, so können die MESH APs selbstständig auf ihren Ausweichaccesspoint umschalten. Dadurch kann das WLAN (vielleicht etwas langsamer aber stabil) weiter genutzt werden bis der Fehler behoben werden kann.



Router, Firewall und Switche

UniFi Security Gateway (USG)

Das USG ist die Router/Firewall für ihr UniFi System. Wenn wir den Controller als Regierung des UniFi Netzwerks sehen, dann ist das USG so etwas wie die Netzwerkpolizei. Als Firewall kümmert sie sich darum wer mit wem, wohin, wie, wann, was kommunizieren darf und als Router um den Verkehr in und aus dem lokalen Netzwerk z.B. in andere Netzwerke wie das Internet. Das USG ist dabei voll in den Controller integriert was zu Beginn eventuell etwas Umdenken bedarf, dafür sind viele Funktionen bereits aber auch ohne eingebundenes USG im Controller sichtbar und werden lediglich mit einem kleinen Hinweis versehen das die Funktion ein USG erfordert. So ist es möglich sich schon nach dem ersten Anmelden an den Controller einen Überblick zu verschaffen ohne alle Geräte gekauft bzw. eingebunden zu haben.

USG

Das USG ist das kleinere der beiden und eignet sich besonders für bis mittelgroße Umgebungen. Mit seiner kompakten Bauform und dem abgesetzten Netzteil kann es einfach verstaubt oder über die „+“ Langlöcher montiert werden. Das USG verfügt über einen LAN, WAN und VoIP Port wobei letzterer als zweiter WAN Port konfiguriert werden kann. Das USG wird auch gerne zur Entkopplung des WLANs in bestehenden Netzwerkumgebungen verwendet, wenn dieses z.B. von einem anderen Anbieter verwaltet wird. Dadurch gibt es lediglich eine WAN Schnittstelle als Berührungspunkt was die Fehlersuche erheblich vereinfacht.



USG-PRO-4

Das USG-PRO-4 ist für die Montage in einen 19" Schrank vorgesehen und hat ein integriertes Netzteil. Neben den beiden LAN Ports verfügt es über zwei WAN Anschlüsse die wahlweise als RJ45 oder SFP Ports konfiguriert werden können. Außerdem verfügt es über einen doppelt so starken Prozessor und 4x so viel RAM im Vergleich zu dem kleineren USG. Um Überhitzung zu verhindern, verfügt das USG-PRO außerdem über eine aktive Kühlung durch zwei Lüfter.



	USG	USG-PRO-4
Anzahl Ports	3Stk	50Stk
LAN Ports	1Stk	2Stk
SFP (1Gbit)	✗	2Stk✓ (Shared)
WAN	2Stk ¹⁰ ✓	2Stk✓
Prozessor	Dual-Core 500Mhz	Dual-Core 1Ghz
RAM	512MB DDR2	2GB DDR3
Speicher	2GB	4GB
Stromversorgung	Extern (12V/1A) 	Intern 
Layer 3 Forwarding	1Mpps (64Byte Packet) 3Gbps (Line Rate/ >512byte Packet)	2,4Mpps (64Byte Packet) 4Gbps (Line Rate/ >512byte Packet)
Lüfter	✓	✓
19" Montage	✗	✓
Wandmontage	✓	✗

¹⁰ Über den Controller kann der VoIP Port auf WAN2 geändert werden.

UniFi Switch:

Die UniFi Switches kurz „US“ sind in einer Vielzahl von Modellen verfügbar um eine möglichst modulare Lösung anbieten zu können. Je nach Modell verfügen die Switches über 24V Passiv PoE und 802.3af/at Aktiv PoE welches über den Controller verwaltet wird.

US-8

Der US-8 ist der kleinste der Serie und verfügt über ein paar Besonderheiten gegenüber seiner größeren Verwandten. Als einziger UniFi Switch kann der US-8 alternativ zu dem mitgelieferten Netzteil auch über PoE (Aktiv PoE 802.3af/at oder 24V Passiv PoE) mit Strom versorgt werden. Somit ist er höchst flexibel z.B. als Zwischenverteiler einsetzbar. Wird der Switch über das Netzteil oder Aktiv PoE betrieben kann Port 8 auch als Passthrough¹¹ Port verwendet werden um z.B. einen UAP-AC-PRO mit Strom zu versorgen. Die Passthrough Ausgangsspannung ist von der verwendeten Eingangsquelle abhängig.



US-8-60W

Der US-8-60W ist wie der US-8 in ein sehr kompaktes Blechkleid gehüllt, verfügt aber über 4 Ports die Aktiv PoE (802.3af) ausgeben können. Er eignet sich besonders gut für kleine Umgebungen mit z.B. drei UAP-AC-PRO und einen CloudKey.



Überblick US Kompakt

	 US-8	 US-8-60
Anzahl Ports	8Stk	8Stk
RJ45 Ports (10/100/1000Mbps)	8Stk	8Stk
SFP (1Gbit)	✗	✗
SFP+ (10Gbit)	✗	✗
PoE Out	1Stk	4Stk
PoE Standards	Passthrough 48V	IEEE802.3af ✓ Passiv PoE 24V ✗
19" Montage	✗	✗
Wandmontage	✓	✓
Stromversorgung	Extern (48V/0,5A)  Aktiv PoE 802.3af/at oder 24V Passiv POE ¹² 	Extern (48V/1,25A) 
Durchsatz (Non-Blocking)	8Gbps	8Gbps
Switching Capacity	16Gbps	16Gbps
Forwarding Rate	11,9Mpps	11,9Mpps
Strom bedarf max.	24W	60W
Strombedarf (ohne PoE Out)	12W	12W
Lüfter	✗	✗
Lautstärke Lüfter¹³	0dBa	0dBa
Kensington Lock	✓	✓

¹¹ Beachten sie bitte dass der PoE Input groß genug gewählt ist damit der Switch und das Angeschlossene Gerät versorgt werden können.

¹² Kein Passthrough bei 24V Passive PoE Input möglich.

¹³ Bei Modellen mit Lüfter sind diese in der Regel nicht aktiv und schalten sich nur bei Bedarf mit einer von 4 Stufen zu.

US-8-150W

Der US-8-150W kann sowohl in 10" Schränke als auch an die Wand montiert werden und verfügt bereits über die vollständige Ausstattung der "großen" UniFi Switches. Er kann auf allen LAN Ports wahlweise Aktiv PoE 802.3af/at oder 24V Passiv PoE ausgeben. Zusätzlich verfügt er über zwei eigenständige SFP Ports in denen sowohl LWL als auch RJ45 SFP Module verwendet werden können, was ihn zu einem vollwertigen 10Port Switch macht.



US-16-150W

Der 16Port Switch verfügt über dieselbe Ausstattung wie das 8Port Modell, kann aber neben der Wandmontage alternativ auch in einen 19" Schrank eingebaut werden.



Überblick Modelle 8Port und 16Port

	US-8-150W	US-16-150W
Anzahl Ports	10Stk	18Stk
RJ45 Ports (10/100/1000Mbps)	8Stk	16Stk
SFP (1Gbit)	2Stk ✓	2Stk ✓
SFP+ (10Gbit)	✗	✗
PoE Out	8Stk	16Stk
PoE Standards	IEEE802.3af/at ✓ Passiv PoE 24V ✓	IEEE802.3af/at ✓ Passiv PoE 24V ✓
19" Montage	✗	✓
Wandmontage	✓	✓
Stromversorgung	Intern 	Intern 
Durchsatz (Non-Blocking)	10Gbps	18Gbps
Switching Capacity	20Gbps	36Gbps
Forwarding Rate	14,88Mpps	26,78Mpps
Strombedarf max.	150W	150W
Strombedarf (ohne PoE Out)	20	28W
Lüfter	✗	✓
Lautstärke Lüfter¹⁴	0dBa	max. 37dBa
Kensington Lock	✗	✗

14 Bei Modellen mit Lüfter sind diese in der Regel nicht aktiv und schalten sich nur bei Bedarf mit einer von 4 Stufen zu.

US-24 Serie

Alle UniFi Switche mit 24Port sind für die Montage in 19" Schränken vorgesehen. Die beiden eigenständigen SFP Slots können wahlweise mit LWL oder RJ45 Modulen bestückt werden und erweitern den Switch auf 26Ports. Neben der beiden PoE Modelle die Aktive PoE nach 802.3af/at Standard oder 24V Passiv PoE ausgeben können gibt es hier aber auch noch ein Model ohne PoE.



Überblick Modelle 24Port

	US-24	US-24-250W	US-24-500W
Anzahl Ports	26Stk	26Stk	26Stk
RJ45 Ports (10/100/1000Mbps)	24Stk	24Stk	24Stk
SFP (1Gbit)	2Skt ✓	2Skt ✓	2Skt ✓
SFP+ (10Gbit)	✗	✗	✗
PoE Out	✗	24Stk	24Stk
PoE Standards	✗	IEEE802.3af/at ✓ Passiv PoE 24V ✓	IEEE802.3af/at ✓ Passiv PoE 24V ✓
19" Montage	✓	✓	✓
Wandmontage	✗	✗	✗
Stromversorgung	Intern 	Intern 	Intern 
Durchsatz (Non-Blocking)	26Gbps	26Gbps	26Gbps
Switching Capacity	52Gpbs	52Gpbs	52Gpbs
Forwarding Rate	38,69Mpps	38,69Mpps	38,69Mpps
Strombedarf max.	25W	250W	500W
Strombedraf (ohne PoE Out)	25W	25W	25W
Lüfter	✓	✓	✓
Lautstärke Lüfter¹⁵	max. 37dBa	max. 47dBa	max. 53dBa
Kensington Lock	✗	✗	✗

¹⁵ Bei Modellen mit Lüfter sind diese in der Regel nicht aktiv und schalten sich nur bei Bedarf mit einer von 4 Stufen zu.

US-48 Serie

Wie die Modelle der US-24 Serie gibt es auch bei den 48Port Switchen neben den beiden PoE Modellen mit der Ausgabe von Aktiv PoE 802.3af/at oder Passiv PoE, ein Modell ohne PoE. Zusätzlich zu den beiden SFP Slots wie sie auch in den kleineren US Switchen verbaut werden sind die 48Port Modelle mit 2 SFP+ Slots ausgestattet, die eine Übertragung von bis zu 10Gbit ermöglichen. Die Switche eignen sie speziell für große Umgebungen bei denen sehr viele Anschlüsse zentral zusammen laufen.



Überblick Modelle 48Port

	US-48	US-48-500W	US-48-750W
Anzahl Ports	52Stk	52Stk	52Stk
RJ45 Ports (10/100/1000Mbps)	48Stk	48Stk	48Stk
SFP (1Gbit)	2Skt ✓	2Skt ✓	2Skt ✓
SFP+ (10Gbit)	2Skt ✓	2Skt ✓	2Skt ✓
PoE Out	✗	48Stk	48Stk
PoE Standards	✗	IEEE802.3af/at ✓ Passiv PoE 24V ✓	IEEE802.3af/at ✓ Passiv PoE 24V ✓
19" Montage	✓	✓	✓
Wandmontage	✗	✗	✗
Stromversorgung			
Durchsatz (Non-Blocking)	70Gbps	70Gbps	70Gbps
Switching Capacity	140Gbps	140Gbps	140Gbps
Forwarding Rate¹⁶	104,16Mpps	104,16Mpps	104,16Mpps
Strombedarf max.	56W	64W	64W
Strombedarf (ohne PoE Out)	56W	500W	750W
Lüfter	✓	✓	✓
Lautstärke Lüfter¹⁷	max. 37 dBa	max. 47 dBa	max. 48 dBa
Kensington Lock	✗	✗	✗

¹⁶ Angabe in Mpps (Million packets per second)

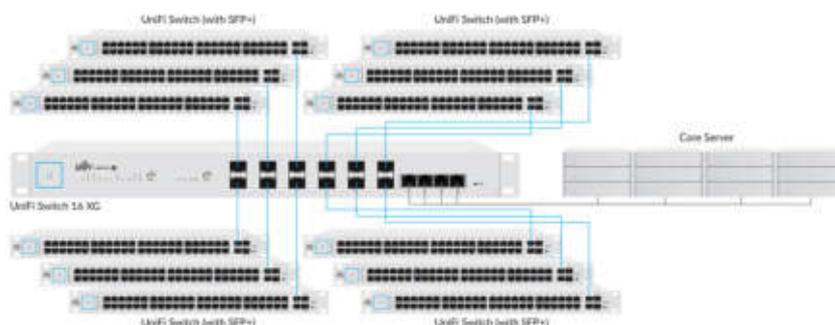
¹⁷ Bei Modellen mit Lüfter sind diese in der Regel nicht aktiv und schalten sich nur bei Bedarf mit einer von 4 Stufen zu.

US-16-XG

Der US-16-XG eignet sich mit seinen 12Stk SFP+ und 4Stk RJ45 10Gbit Ports besonders als zentraler Knotenpunkt um z.B. mehrere Gebäude an einen Hauptserverraum anzubinden. Als einziges Modell der UniFi Switch Serie verfügt der US-16-XG über die Möglichkeit eine redundante Stromversorgung über ein optionales externes Netzteil aufzubauen.



10Gbps Anbindungsbeispiel:



	US-16-XG	
Anzahl Ports	16Stk	
RJ45 Ports (10/100/1000Mbps)	4Stk	
SFP (1Gbit)	✗	
SFP+ (10Gbit)	2Stk ✓	
PoE Out	✗	
PoE Standards	✗	
19" Montage	✓	
Wandmontage	✗	
Stromversorgung	Intern 	Extern ¹⁸ 25VDC  (Optional)
Durchsatz (Non-Blocking)	160Gbps	
Switching Capacity	320Gbps	
Forwarding Rate¹⁹	238,10Mbps	
Strombedarf max.	56W	
Strombedarf (ohne PoE Out)	56W	
Lüfter	✗	
Lautstärke Lüfter²⁰	0dBa	
Kensington Lock	✗	

¹⁸ Netzteil für redundanten Betrieb nicht im Lieferumfang enthalten.

¹⁹ Angabe in Mpps (Million packets per second)

²⁰ Bei Modellen mit Lüfter sind diese in der Regel nicht aktiv und schalten sich nur bei Bedarf mit einer von 4 Stufen zu.

Wissenswertes:

PoE - Was ist das?

Bei PoE kurz für "Power over Ethernet" wird wie der Name schon sagt Strom in das Netzkabel eingespeist. So kann man die Stromquelle (z.B. Switch oder Injektor) zentral belassen und muss das Gerät nur mit einem LAN Kabel anbinden. Grundsätzlich gibt es Aktiv und Passiv PoE, die allerdings zueinander nicht kompatibel sind.

Aktiv und Passiv PoE- Wo ist er Unterschied?

Aktiv PoE

Wird von Aktiv PoE gesprochen dann sind die beiden Netzwerkstandards IEEE802.3af oder IEEE802.3at gemeint. Diese prüfen aktiv ob es sich bei dem angeschlossenen Gerät um ein kompatibles PoE Gerät handelt. Ist das der Fall wird der entsprechende Standard ausgehandelt und erst dann der Strom aufgeschaltet. Schließen sie nun z.B. einen Access Point und ein Notebook an einen Switch an, dann wird erkannt, dass es sich bei dem Notebook um kein PoE Gerät handelt und nur für den AP der Strom eingeschaltet. Die beiden IEEE Standards verwenden eine Spannung von 48V und unterscheiden sich durch die angebotene Leistung (802.3af /15,4W | 802.3at / 25,5W)

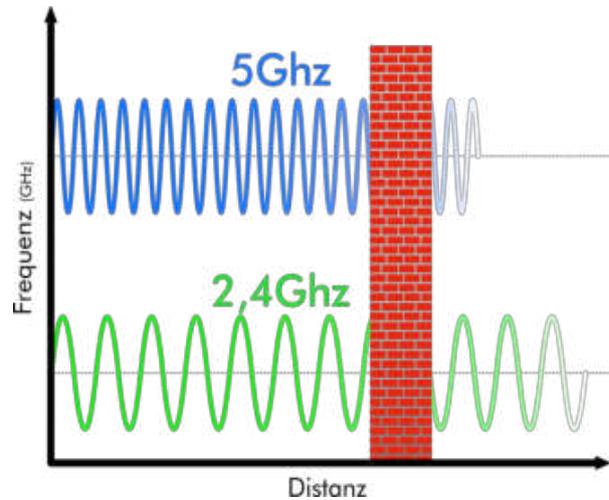
Passiv PoE

Im Gegensatz zu Aktiv PoE gibt es bei Passiv PoE keinen festgeschriebenen Standard, vielmehr hat sich Passiv PoE aus dem Industriebereich gebildet. Auch wenn an sich fast jede beliebige Spannung verwendet werden kann hat sich im Laufe der Zeit doch 24V als die geläufigste Spannung etabliert. Im Gegensatz zu Aktiv PoE wird bei Passiv PoE nicht geprüft ob das angeschlossene Gerät für den Betrieb mit PoE geeignet ist. Der Netzwerk Port bei Passiv PoE verhält sich im wesentlichen wie eine Stromsteckdose, bei der wenn aktiv immer Strom anliegt. Sie sollten daher bei Passiv PoE besonders darauf achten kein Gerät anzuschließen das nicht für die Stromaufnahme über die Netzwerk Schnittstelle geeignet ist. Ansonsten könnte das Gerät irreparabel beschädigt werden.

WLAN Basics

Wie der Name schon sagt wird bei WLAN (Wireless Local Area Network) anstelle einer Kabelverbindung, Funk für die Datenübermittlung verwendet. Dadurch ergibt sich ein grundlegend anders Verhalten was sowohl Vor- als auch Nachteile mit sich bringt. Da die Funktechnik ein sehr umfangreicher Bereich ist, der den Rahmen hier bei weitem sprengen würde, wollen wir uns nur das grundlegende Prinzip etwas ansehen ohne dabei tiefer in die Materie einzutauchen.

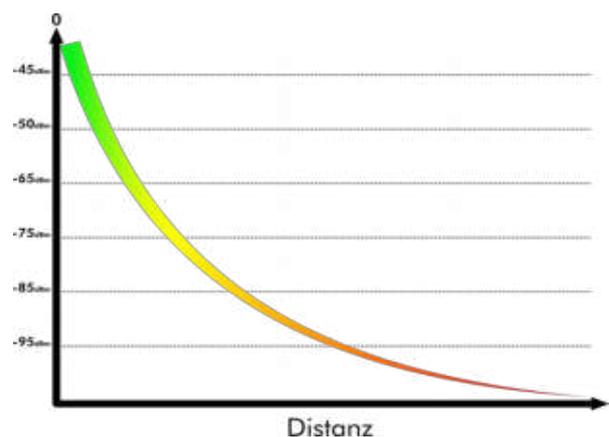
Vereinfacht gesagt handelt es sich bei Funk um elektromagnetische Wellen die sich mit einer Schwingung, der Frequenz, ausbreiten. Ein bewährtes Sinnbild ist ein Stein der in einen See geworfen wird. Die Wellen breiten sich kreisförmig aus und werden mit zunehmender Distanz zum Zentrum im Durchmesser immer Größer, dafür aber immer flacher bis sie nicht mehr sichtbar sind. Das Medium Funk kann in einem sehr breiten Spektrum operieren. Da verschiedene Frequenzen auch verschiedene Charakteristika haben und nicht jede Frequenz einfach für jede Anwendung geeignet ist mussten die Frequenzbereiche schon sehr früh reglementiert werden um gegenseitige Störungen zu vermeiden. Es stehen daher nur ein paar „Freie“ Frequenzen für die Benutzung ohne spezieller Lizenz zur Verfügung. Access Points operieren in der Regel in dem Frequenzband 2.4GHz (2400-2472Mhz | IEEE802.11b,g,n,ac) bzw. 5GHz (5150-5725MHz | IEEE802.11a,n,ac). Mit dem kommenden IEEE802.11ad²¹ Standard wird es wohl auch Anwendungen in dem 60GHz Frequenzbereich geben. Aufgrund der sehr hohen Frequenz wird der 802.11ad Standard aber wohl ausschließlich für Übertragungen mit hoher Bandbreite auf sehr kurze Distanz zum Einsatz kommen, weswegen wir hier nicht weiter darauf eingehen werden. Je nach dem welches Medium die Funkwellen passieren wird mehr oder weniger der Energie absorbiert, reflektiert, abgelenkt oder gestreut, wodurch sich die Reichweite des Signals stark verändert. Die beiden Frequenzen haben also durchaus unterschiedliche Anwendungen. Das 5GHz Frequenzband kann im Vergleich zu 2,4GHz durch die höhere Frequenz (mehr Schwingungen in der Sekunde) mehr Daten in der selben Zeit übertragen. Das 2,4GHz Band hat durch die niedrigere Frequenz hingegen den Vorteil eine größere Distanz abzudecken bzw. verfügt es über ein besseres Durchdringverhalten von Materie.



Für die Planung bzw. den Aufbau eines WLANs ist es daher wichtig sich der Tatsache bewusst zu sein, dass verschiedene Frequenzen Vor- und Nachteile aufweisen und der / die Access Point/s entsprechend platziert werden müssen um ein bestmögliches Ergebnis zu erhalten.

Das Signal

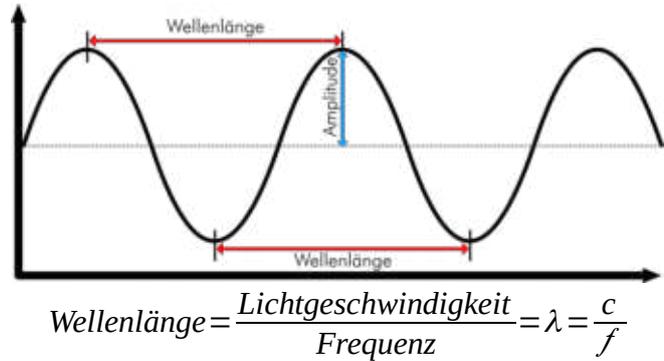
In den Umgebungen in denen wir uns mit WLAN bewegen wird die Signalstärke in der Regel in „dBm“ also „Dezibel/Milliwatt“ angegeben. Da das Signal unmittelbar nach Erzeugung durch Umwelteinflüsse an Stärke verliert wird das Ausgangssignal mit „0“ definiert wodurch sich bei dem Empfangenen Signal ein „- Wert“ ergibt. Wie auch bei einem Bankkonto gilt, wenn schon kein „+“ dann ist ein „kleines“ Minus immer noch besser als ein „großes“ Minus. In unserem Fall besteht also bei einem möglichst keinen „-Wert“ die best mögliche Verbindung.



21 IEEE802.11ad befindet nach derzeit (04/2018) noch in Vorbereitung

Wellenlänge:

Es kommt durchaus vor das für Funkübertragungen ein Metrischer Wert z.B. im Millimeter Bereich angegeben wird. Dabei handelt es sich um die Wellenlänge. Elektromagnetische Wellen breiten sich in einem Vakuum mit Lichtgeschwindigkeit aus, die uns als Konstante dient ($c \sim 300.000.000 \text{m/s}$). Die Wellenlänge gibt dabei die Distanz zwischen den Scheitelpunkte an. Somit kann aus der Frequenz die Wellenlänge und umgekehrt berechnet werden.



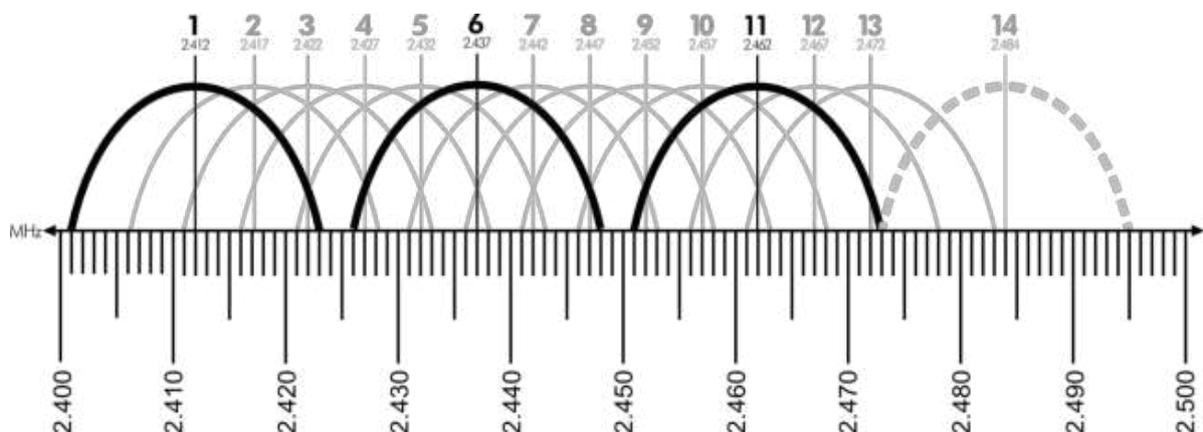
Die Kanäle:

Wie schon erwähnt operiert WLAN in den beiden Freien Funkbändern 2,4GHz und 5GHz. Da die beiden Frequenzbänder sehr schmal sind muss es hier natürlich auch eine weitere Unterteilung geben damit sich nicht alle gegenseitig stören und schlussendlich niemand eine Verbindung aufbauen kann. Bei WLAN sind dafür mehrere Kanäle (Channels) festgelegt worden. In der Regel reicht es aus wenn eine AccessPoint die Umgebung während des Starts prüft und sich selbst einen freien Kanal sucht. Allerdings ist es dennoch gut zu wissen wie diese Kanäle aufgebaut sind das es notwendig sein kann in Dichten (sogenannten „Lauten“ Umgebungen) den Kanal selbst zu wählen.

Zunächst sei erst einmal erwähnt das Channels nicht soweit von einander getrennt sind das die Verwendung von zwei unterschiedlichen Kanälen in einer WLAN Umgebung automatisch sicherstellt das keine Störungen auftreten. Vielmehr werden Channels dazu verwendet um nicht mit der sperrigen vollständigen Frequenz hantieren zu müssen. So ist z.B. „Ch.1“ einfacher zu kommunizieren als „2412MHz“, von „2.412.000Hz“ ganz zu schweigen.

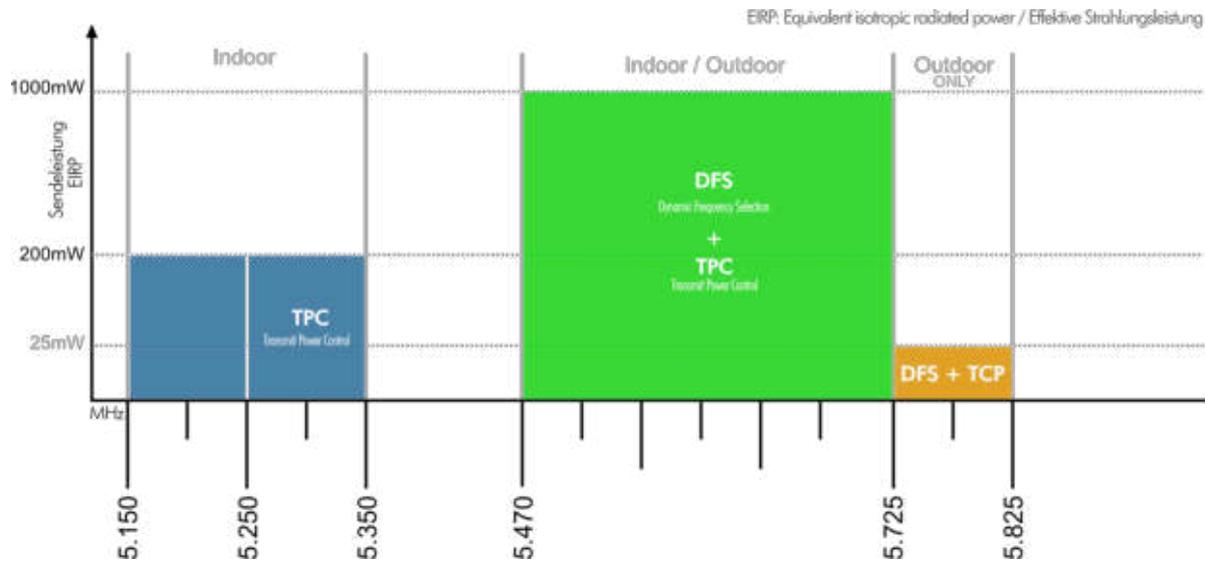
2,4GHz:

Bei 2,4GHz wird in der Regel mit 20MHz oder 40MHz breiten Kanäle gearbeitet. Bei Verwendung von 20MHz Kanälen ergeben sich so nur 3 überlappungsfreie Kanäle. Die Channel 1,6 und 11 verfügen über genügend Abstand um sich nicht gegenseitig zu beeinträchtigen. Der Channel 14 hätte zwar auch genügend Abstand liegt aber bereits Außerhalb des in der EU erlaubten Bereich.

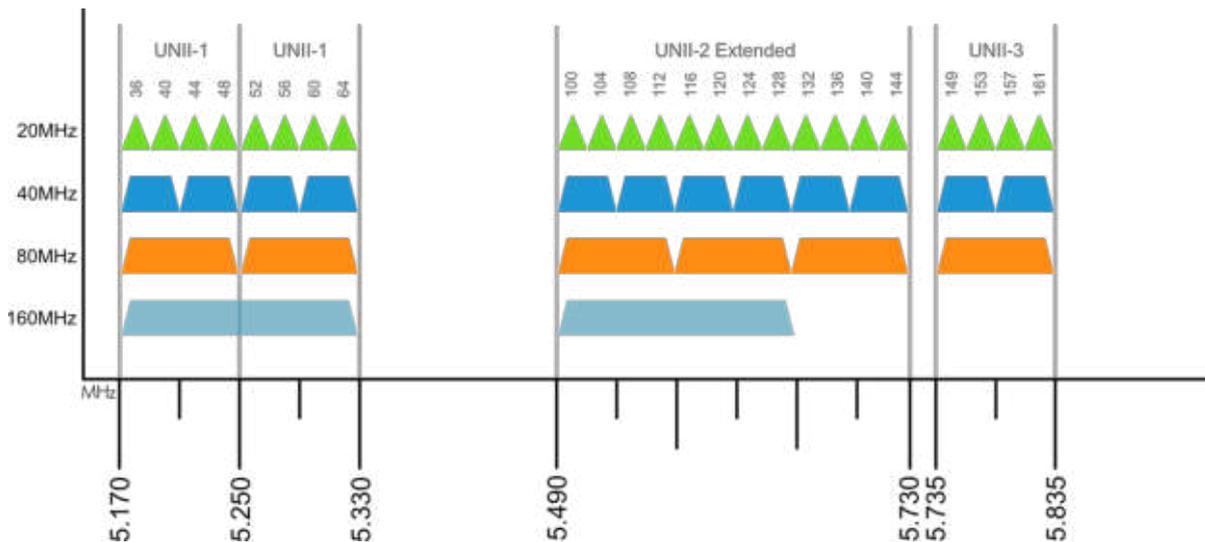


5GHz:

Wenn im Zusammenhang mit WLAN von 5GHz die Rede ist dann sind die lizenzfreien Bereiche 5.150-5.350MHz, 5.470-5.725MHz und 5.725-5.825MHz gemeint. Diese Parzellen unterliegen unterschiedlichen Einschränkungen wie nachfolgend zu sehen ist.



Wie auch bei 2,4GHz werden 20MHz Kanalbreiten verwendet die zu 40, 80 oder 160MHz Kanalbreiten „gebündelt“ werden können. Durch das verwenden von größeren Blöcken kann die effektive Bandbreite stark gesteigert werden. Allerdings ist dabei zu beachten das dazu genügend „Platz“ vorhanden sein muss und kein anderes Signal oder Störungen die Verwendung einer Breiteren Kanalbreite verhindert.



Radar Detection – Was ist DFS und TPC

Wie wir gesehen haben gibt es bei 5GHz Bereiche in denen TPC bzw. DFS für den Betrieb vorgeschrieben sind. Umgangssprachlich wird hier in der Regel von „Radar Detection“ gesprochen. Wie anfangs schon erwähnt ist 5GHz zu einem großen Teil ein lizenzfreier Bereich, er wird aber teilweise von lizenzierten Anwendern mitverwendet die gesetzlich Vorrang haben und nicht gestört werden dürfen. In dem Gesetzestext steht stark vereinfacht ausgedrückt, das als Betreiber von unlizenzierten Anwendungen sichergestellt werden muss das die Lizenzierten Anwendungen (z.B. Flugradar, Militär, Weterradar, Rettungsdienste etc.) keinesfalls gestört werden und sie mit diesen Beeinträchtigung klarkommen müssen, respektive unter Umständen Pech haben und keinen freien Bereich finden in dem sie operieren können. Das ist derzeit zwar Primär ein Problem bei Richtfunkanwendungen, kommt aber dort durchaus häufiger vor und wird mit zunehmender Auslastung des 5GHz Bandes wohl eher zunehmen.

DFS: Dynamic Frequency Selection

DFS umgangssprachlich auch „Radar Detection“ genannt, sorgt dafür das die Frequenz sofort gewechselt wird sobald ein anders Signal erkannt wird. Das ist erforderlich um den Schutz von lizenzierten Anwendungen wie z.B. Weterradar zu gewährleisten und muss für den Betrieb in Österreich bzw. der EU aktiv sein.

TPC: Transmit power controll

Der Standard IEEE802.11h hat TPC zusammen mit DFS eingeführt. Über TPC kann die Sendeleistung automatisch angepasst werden, um die länderspezifischen Vorgaben zu erfüllen. Wenn sie bei der ersten Inbetriebnahme des UniFi Controllers das Land auswählen wird so die für Österreich erlaubten Sendeleistungen eingestellt.

Konfiguration

Die Konfiguration der UniFi Geräte erfolgt wie wir ja schon wissen ausschließlich über den UniFi Controller. Nachfolgend wollen wir uns die erste Inbetriebnahme anhand eines CloudKey einmal genauer ansehen.

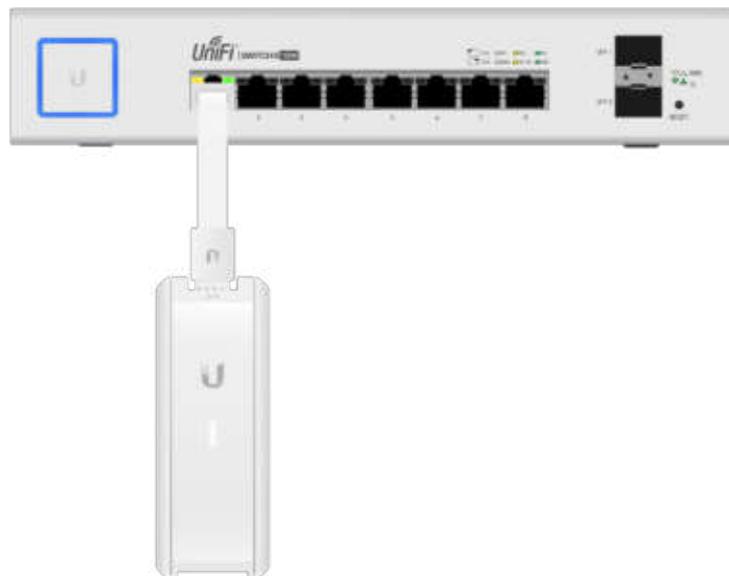
Info:

Der Zugriff auf den UniFi Controller kann grundsätzlich von jedem beliebigen Webbrowser aus erfolgen. Wir empfehlen allerdings Google Chrome für die Konfiguration und Administration des UniFi Controllers zu verwenden da UBNT derzeit primär auf dieser Browser Plattform entwickelt. Zudem kann der Controller vollständig in deutscher Sprache betrieben werden. Als Amerikanische Firma ist die primär Sprache bei Beschreibungen, Support und innerhalb der Community wie zu erwarten Englisch, weswegen wird auch in dieser Beschreibung die Englische Spracheinstellung verwendet um ihnen das zuordnen bei weiteren Recherchen zu vereinfachen. Wie sie die Sprache ändern finden sie weiter hinten in diesem Guide auf Seite 43.

Erste Verbindung auf den CloudKey

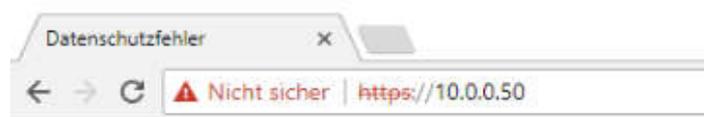
Der CloudKey kann sowohl über 802.3af Aktiv PoE als auch über USB mit Strom versorgt werden. Da in den meisten Umgebungen ohnehin ein PoE Switch für die Access Points eingesetzt wird, konzentrieren wir uns in dieser Anleitung auf die Verwendung von PoE als Stromquelle.

Nach dem der CloudKey das erste Mal angeschlossen worden ist, dauert es eine Weile bis er für die



Einrichtung bereit ist. Hat er den ersten Bootvorgang abgeschlossen, leuchtet die LED statisch weiß. Wie in der Schnellstartanleitung beschrieben besteht auch die Möglichkeit den CloudKey über ein Chrome Pulg-in mittels UBNT CloudAccess einzurichten. Wir möchten uns hier aber speziell den „traditionellen“ Weg ansehen. Der CloudKey bezieht standardmäßig die IP Adresse von einem DHCP Server, hat mit 192.168.1.30 aber auch eine Fallback Adresse wenn keiner zur Verfügung steht.

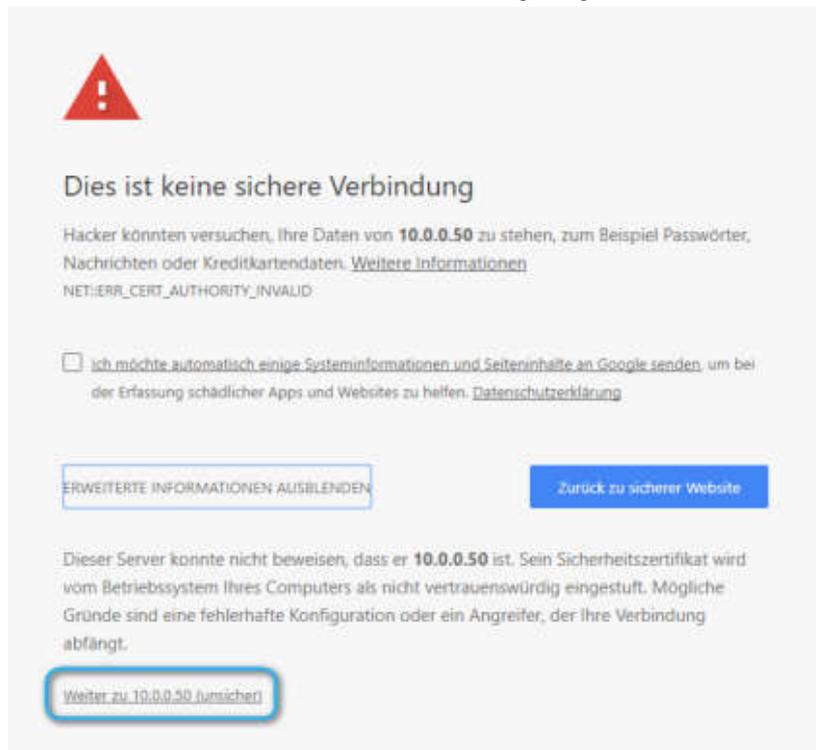
Öffnen sie ihren Browser (Chrome empfohlen) und verbinden sie sich auf den CloudKey. In unserem Beispiel hat der CloudKey die DHCP Adresse 10.0.0.50 bezogen. Wenn sie den CloudKey direkt an ihre Netzwerkkarte angeschlossen haben verwenden sie die Fallback Adresse um sich auf den CloudKey zu verbinden.



Fallback Adresse: 192.168.1.30

Hinweis: Um über die Fallback Adresse auf den CloudKey zugreifen zu können muss ihre Netzwerkkarte entsprechend konfiguriert werden.

Es ist sehr wahrscheinlich das Chrome ihnen eine Fehlermeldung ausgibt das die Verbindung nicht sicher sei.



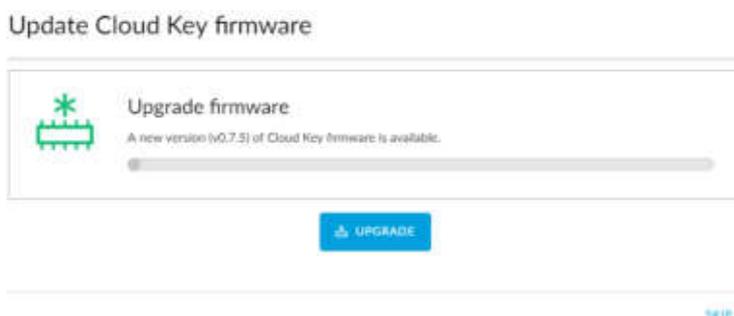
Keine Sorge, das liegt lediglich daran das der CloudKey ein selbst signiertes Zertifikat für die https Verschlüsselung verwendet. Leider reagieren moderne Browser recht „hysterisch“ auf selbst ausgestellte Zertifikate da sie primär für Web Seiten optimiert sind. In unserem Fall dient das Zertifikat aber lediglich der technischen Sicherung und nicht der Identitätssicherung. Klicken sie auf [Erweiter] und anschließend auf [Weiter...].



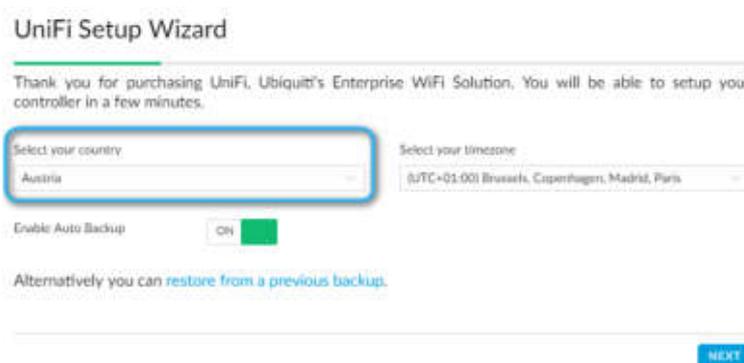
Nun befinden sie sich auf der Hauptseite des CloudKey. Hier können sie den UniFi Controller zur Verwaltung ihrer Geräte aufrufen oder den CloudKey selbst administrieren. Klicken sie für die Erstkonfiguration unter „Manage your Devices by UniFi Controller“ auf [MANAGE] um den Einrichtungsassistenten zu starten.

Der UniFi Wizard

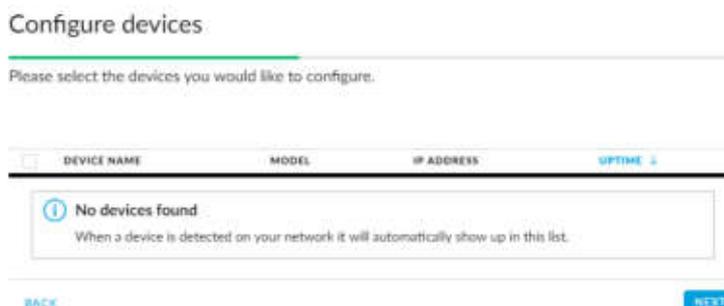
Abhängig von der installierten Firmware und ob der CloudKey eine Verbindung in das Internet hat, wird ihnen in der Regel angezeigt das ein Update zur Installation zur Verfügung steht. Sie können dieses entweder gleich durchführen oder mit Skip überspringen. Generell empfiehlt es sich das Update gleich durchzuführen da nicht nur der CloudKey sondern auch der UniFi Controller auf den neuesten Stand gebracht wird.



Der CloudKey lädt die Firmware vollständig herunter und führt das Update erst nach interner Prüfung durch. Ein Internet oder Stromausfall ist für ein erfolgreiches Update also keine Hürde. Nach Abschluss des Updates wird die Länder und Zeitzonen Auswahl angezeigt. Wählen sie hier „Austria“ als Land aus. Das ist erforderlich weil dadurch auch die länderspezifisch zulässigen WLAN Einstellungen definiert werden. Wählen sie hier kein anderes Land aus, als das in dem sich die Anlage befindet, da sie als Betreiber für die Einhaltung der Richtlinien für den Betrieb gemäß 2014/53/EU²² verantwortlich sind.



Wenn sie den CloudKey zurückgesetzt haben oder einen bestehenden durch diesen ersetzen möchten, können sie über die Funktion „restore from a previous backup“ das Backup ihrer Konfiguration direkt einspielen ohne den kompletten Assistenten durchführen zu müssen. Beachten sie dabei dass für eine erfolgreiche Wiederherstellung dieselbe Controller Version erforderlich ist, da es ansonsten zu Problemen kommen kann. Klicken sie anschließend auf [NEXT] um fortzufahren.



Wenn sie bereits UniFi Geräte an ihr Netzwerk angeschlossen haben die frei zur Adoption sind, können sie diese gleich hier in ihren Controller einbinden. Das ist in erster Linie Geschmackssache, in der Regel ist die Adoption nach der ersten erfolgreichen Konfiguration des Controllers aber die komfortablere Methode.

²² Hilfestellung auf Basis uns vorliegender Informationen, Haftung jeglicher Art ist ausdrücklich ausgeschlossen. Bitte wenden sie sich an einen Juristen für rechtsverbindliche Auskunft.

Wenn sie ihre UniFi Umgebung für Access Points einrichten können sie bereits hier eine SSID samt WPA2 Verschlüsselung für Ihr WLAN hinterlegen bzw. ihr Gast WLAN aktivieren und benennen. Da für die Verwendung des Gast Zuganges aber weitere Einstellungen erforderlich sind empfiehlt es sich die Gast SSID gesondert nach Abschluss des Einrichtungsassistenten zu konfigurieren.

Configure WiFi

You may skip this step if you are not setting up any UniFi access points.

UniFi_TEST *****

Optionally, you may create an open wireless network for your guests:

Enable Guest Access

BACK SKIP NEXT

Sie werden aufgefordert ihre Benutzerinformationen und Passwörter zu hinterlegen. Die Abfrage gliedert sich dabei in drei Teile, dem Controller, dem Cloud Zugriff und dem CloudKey selbst. In dem ersten Bereich legen sie den Administrator für ihren UniFi Controller fest.

Controller Access

Please provide an administrator name and password for UniFi Controller access.

admin unifi@demo.com

***** *****

Password strength: Good

In der Regel wird der Controller Benutzer auch für die Verbindung über den Cloud Access via SSH verwendet. Ist das nicht gewünscht müssen sie nur den Haken bei „Use the same name and password for SSH access“ entfernen um einen eigenen Benutzer und Passwort anzulegen.

Use the same name and password for SSH access.

AdminSSH

***** *****

INFO: Die Kopplung des CloudKey mit ihrem UBNT Account für den Cloud Access über <https://unifi.ubnt.com> findet nach Abschluss der Einrichtung statt.

Wie der Name schon sagt wird hier der Benutzer für den Zugriff auf den CloudKey selbst definiert. Sie sollten hier nach Möglichkeit einen anderen Benutzer bzw. Passwort als den des UniFi Controllers hinterlegen. Wenn sie auf [NEXT] klicken erhalten sie eine Übersicht der hinterlegten Einstellungen. Um Angaben zu ändern klicken sie auf [BACK] bzw. auf [FINISH] um den Einrichtungsassistenten abzuschließen.

Confirm

Please review the settings below. Once finished you will be redirected to the management interface.

Country	Austria
Timezone	Europe/Brussels
Secure SSID	UniFi_TEST
Guest SSID	-
Admin Name	admin
Device Admin Name	admin

BACK FINISH

Nach Abschluss der Einrichtung wird die Anmeldung für den CloudAccess angezeigt. Melden sie sich hier mit ihrem UBNT Account an um den CloudAccess zu aktivieren. Sollten sie noch keinen Account haben, klicken sie auf „No Account? Register now“ um einen zu erstellen oder auf [SKIP] und den Schritt zu überspringen.



CLOUD LOGIN CREDENTIALS

Please enter your UBNT.com account credentials.
Note that this is not the account that you used to sign into this controller.

Email or Username:

Password:

No Account? Register now.

SKIP ENABLE CLOUD ACCESS

Die Ersteinrichtung über den Assistenten ist nun abgeschlossen und sie können sich erstmals an den Controller anmelden.



UniFi
5.5.24

Username:

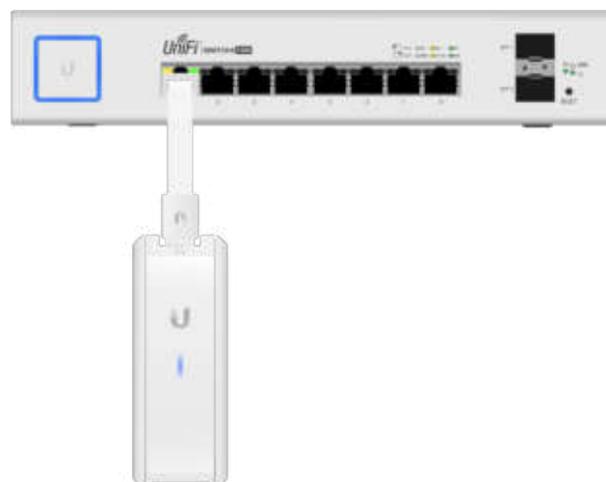
Password:

Remember me

SIGN IN

FORGOT PASSWORD?

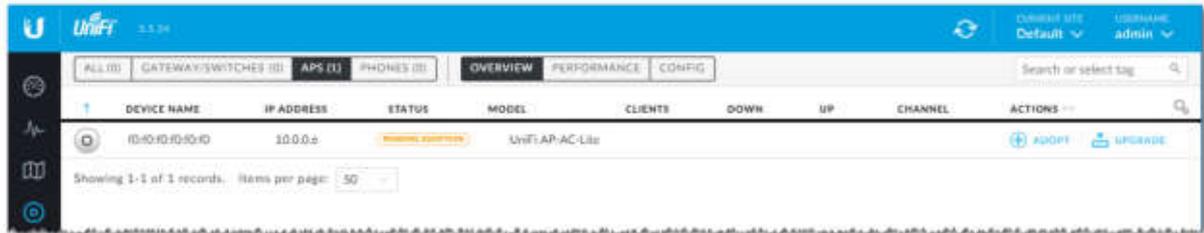
Ist die Einrichtung abgeschlossen leuchtet die LED des CloudKey blau um anzuzeigen dass der CloudKey konfiguriert und betriebsbereit ist.



 **Tipp:** Führen sie nach der ersten Konfiguration und Einbindung der Geräte ein manuelles Backup durch! Mehr dazu finden sie auf Seite 44

Adoptieren von Geräten

Wie wir ja schon wissen werden alle UniFi Geräte über den Controller konfiguriert. Damit das möglich ist müssen die Geräte adoptiert, also mit dem Controller gekoppelt werden. Wenn sie ein UniFi Gerät mit ihrem Netzwerk verbunden haben wird dieses im Controller unter „DEVICES“ als „PENDING ADOPTION“ angezeigt. Das Auffinden der Geräte erfolgt dabei auch Subnet übergreifend. Sollte also ein Gerät mit einer IP Adresse Außerhalb ihres Subnet konfiguriert oder mit der Fallback Adresse gestartet sein, wird ihnen das in der Geräteübersicht inklusive IP angezeigt was die Fehlersuche extrem vereinfacht.

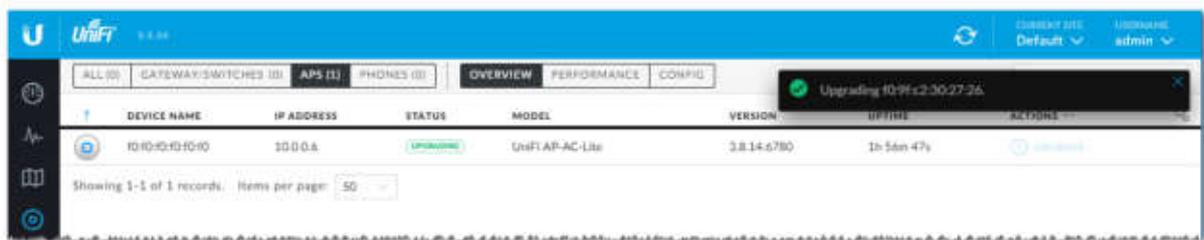


Hinweis:

Es empfiehlt sich vor der ersten Inbetriebnahme alle Geräte auf den neuesten Stand zu aktualisieren um Probleme zu vermeiden.

Firmware Upgrade:

Ist eine neuere Firmware als die auf dem Gerät verfügbar wird ihnen das Upgrade Symbol angezeigt. Das Gerät lädt dabei die Firmware direkt von der UBNT Webseite. Eine Internetverbindung²³ ist somit für das Auto Update erforderlich.



Hinweis:

Es wird immer die neueste Firmware Version geladen, darum ist es erforderlich ist auch den Controller aktuell zu halten um Probleme durch Versions Zerklüftung zu vermeiden.



Tipp: Führen sie nach der ersten Konfiguration und Einbindung der Geräte ein manuelles Backup durch! Mehr dazu finden sie auf Seite 44

²³ Ab Controller Version 5.6.26 ist es möglich die Firmware auch über den Controller für die Geräte zur Verfügung zu stellen.

LED Farbcodes

Eine besonders praktische Funktion der UniFi Geräte ist die verbaute Multistatus-LED. Über diese ist der Zustand des Gerätes jederzeit vorort mit einem Blick ablesbar. Das vermeidet gerade bei der Fehlersuche die ansonsten klassische „Was-machst-du-Ding-gerade“ Situation wenn gerade keinen Zugriff auf den Controller besteht. Nachfolgend eine Auflistung der Standard LED zustände.



Keine LED Anzeige:

Die LED ist in der Standardeinstellung aktiv und zeigt einen der folgenden Zustände an. Sofern das UniFi Gerät also nicht vom Strom getrennt oder die LED in den Einstellungen manuell deaktiviert worden ist gibt es immer einen LED Status.



Weiß oder Orange:

Leuchtet die LED Statisch weiß (orange bei Legacy Geräten) ist das Gerät mit keinem Controller gekoppelt und kann von einem UniFi Controller adoptiert werden.



Blau oder Grün:

Eine konstante blaue LED (grün bei Legacy Geräten) zeigt an das, das Gerät bereits mit einem Controller gekoppelt ist.



Weiß oder Orange Blinken:

Eine weiß blinkende LED (orange bei Legacy Geräten) zeigt an das, das UniFi Gerät gerade bootet. Bei der ersten Inbetriebnahme kann es nach anschließen des Stromes etwas dauern bis die LED aufleuchtet und zu blinken beginnt.



Weiß/Blau oder Orange/Blau Blinken:

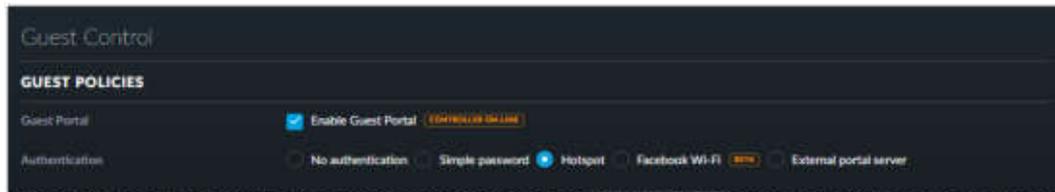
Wenn die LED des UniFi Gerätes zwischen der beiden Zuständen wechselt, gibt das an das gerade Änderungen am Gerät durchgeführt werden, während dessen ein Betrieb nicht möglich ist (z.B. Firmware Update).

Das Gäste WLAN

Das Gäste WLAN ist eines der meist genutzten Funktionen des UniFi Systems. Es glänzt besonders durch die einfache und intuitive Einrichtung und dem großen Funktionsumfang. Nachfolgend wollen wir uns einmal das erstellen der häufigsten Varianten ansehen.

Guest Policies

Die Einrichtung des Gäste Netzwerkes findet zentral unter „Guest Control“ statt und wird anschließend der entsprechenden SSID zugewiesen. In den Standard Einstellungen ist das Gäste Netzwerk ausgeschaltet und muss erst aktiviert werden. Nach dem Aktivieren werden ihnen unter „Authentication“ mehrere Betriebsarten angezeigt von denen die drei ersten (No authentication, Simple password und Hotspot) die am häufigsten verwendeten sind, daher werden wir uns diese etwas genauer ansehen.



No authentication	Diese Funktion wird gerne für Umgebungen verwendet in denen lediglich das akzeptieren von z.B. AGBs gewünscht wird. Über das Menü „Expiration“ definieren sie den Gültigkeitszeitraum für die einzelnen Sitzungen. Dazu können sie die vordefinierten Zeiten nutzen oder unter „User-defined“ frei wählen.
Simple password	Um den Zugang zu dem Netzwerk etwas zu beschränken gibt es die Funktion „Simple Passwort“. Die Handhabung ist gleich wie die der „No authentication“ Funktion, nur das hier zusätzlich ein Passwort eingegeben werden muss. Beachten sie aber bitte dass es sich dabei um <u>keine Verschlüsselung</u> wie z.B. WPA2 sondern wirklich nur um ein Passwort zur Zugangsbeschränkung über die Landing Page handelt. Wenn sie eine Verschlüsselung verwenden möchten, müssen sie das unter Wireless Network für die entsprechende SSID hinterlegen. Wie bei „No authentication“ können sie auch hier unter „Expiration“ eine der vordefinierten Zeiten nutzen oder den Gültigkeitszeitraum für die Sitzungen frei wählen.
Hotspot	Die Funktion „Hotspot“ ist die umfangreichste der drei Funktionen. Hier werden Vouchers, also Gutscheincodes für das Authentifizieren verwendet. Diese können mit unterschiedlichen Bedingungen über die Gültigkeitsdauer, Bandbreite etc. generiert werden. Daher kommt diese Funktion häufig in Hotels zum Einsatz da der Concierge so den entsprechenden Code aus der Schublade zaubern kann ohne Zugriff auf den Controller bzw. Hotspot Manager haben zu müssen. Details dazu finden sie in der Kategorie „Hotspot Manager“.

Landing Page

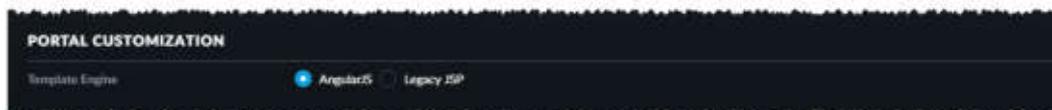
Unter der Option „Landing Page“ können sie festlegen was nach erfolgreicher Authentifizierung passieren soll. Als Standard ist die Option „Redirect to the original URL“ ausgewählt. In diesem Fall wird die Landing Page mit den AGBs etc. erst angezeigt wenn der Client versucht eine Webseite zu öffnen.



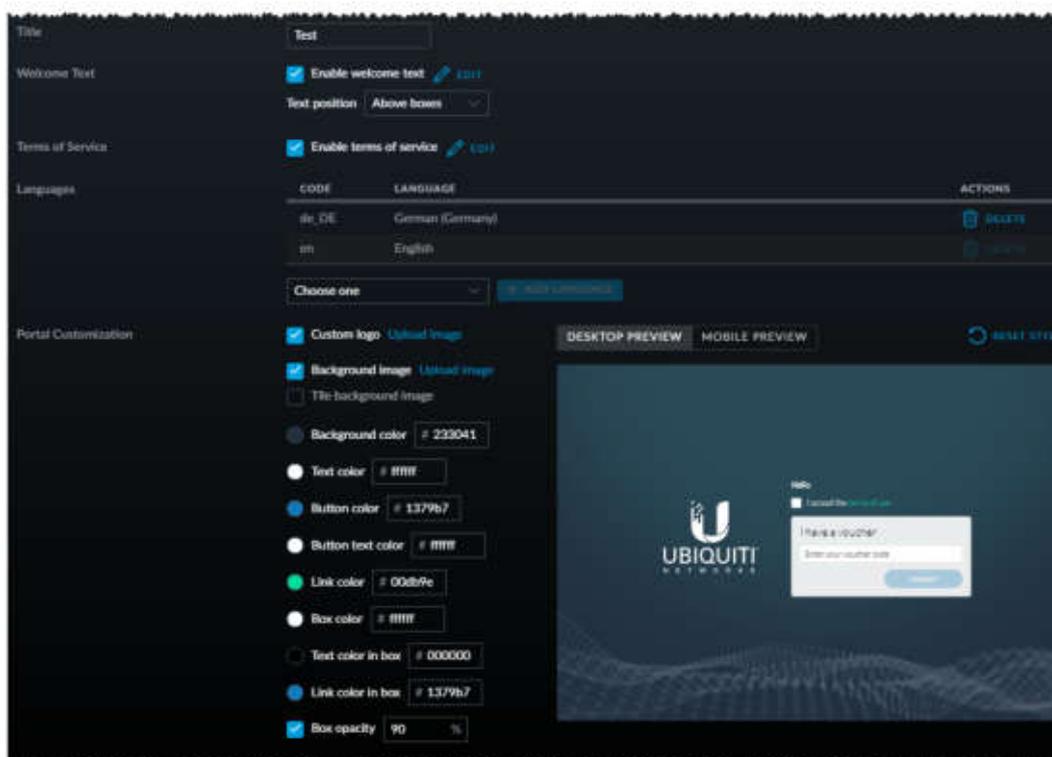
Hat er die Anforderungen der Landing Page erfüllt (z.B. AGBs. zugestimmt) wird er an die angeforderte Seite weiter bzw. zurück gleitet. Dieses Verfahren hat aber je nach verwendeten Client (Smartphone, Notebook etc.) bzw. verwendeten Betriebssystem (iOS, Android, Windows etc.) den Nachteil dass erst versucht werden muss eine Webseite zu öffnen. Versucht der Client z.B. lediglich seine Mails abzurufen erhält er einen Verbindungsfehler, da ja der WLAN Zugang noch nicht gewährt worden ist. In diesem Fall empfiehlt sich die Option „Promotional URL“. Hier wird automatisch versucht eine vordefinierte URL (z.B. die des Betreibers) zu öffnen wodurch die Landing Page sofort aufgerufen wird.

Das Portal

Bevor sie mit der Gestaltung der Landing Page beginnen müssen sie Auswählen welches Template sie verwenden wollen. Zur Auswahl stehen ihnen „AngularJS“ und „Legacy JSP“. Als Standard ist „Angular JS“ ausgewählt was eine Dynamische Erstellung der Seite mittels *Java Script* ermöglicht. Bei der Vorgänger Version „Legacy JSP“ wird *Java Server Pages* verwendet was es erforderlich macht die Landing Page manuell anzupassen.

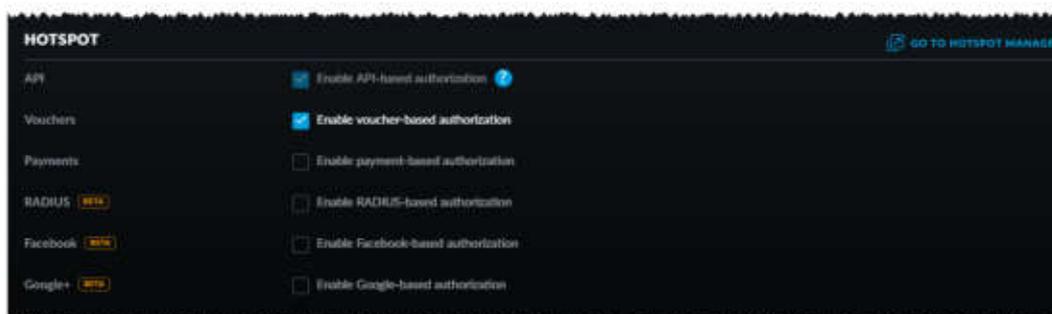


Wie ihnen vermutlich bereits aufgefallen ist passt sich die Landing Page automatisch der ausgewählten Authentifizierung an. In unserem Beispiel verwenden wir die Option „Hotspot“ da hier alle Einstellungen eingeblendet sind. Über die nachfolgenden Punkte können sie nun ihre Landing Page an ihre Vorstellungen anpassen. Alle Änderungen werden dabei dynamisch in dem Vorschauenfenster für Desktop und Mobile Darstellen angezeigt.



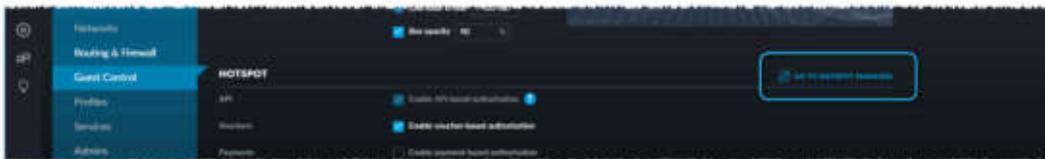
Hotspot

Über den Bereich „Hotspot“ stehen ihnen mehrere Optionen für die Authentifizierung zur Verfügung. Nachfolgend werden wir uns die Voucher basierte Authentifizierung etwas genauer ansehen da diese die häufigste Art der Authentifizierung ist.



Der Hotspot Manager

Klicken sie unter „Guest Control“ in dem Bereich „Hotspot“ auf „GO TO HOTSPOT MANAGER“ um die Hotspot Manager Seite zu öffnen.



Nach öffnen des Hotspot Managers finden sie sich in der Rubrik „Analyse“ wieder. Wie das Dashboard wird ihnen hier eine Übersicht der Aktivitäten angezeigt.



Unter der Kategorie „Guests“ werden ihnen die aktuell verwendeten Gutscheincodes angezeigt. Über die Actions „Extend“ und „Disconnect“ können sie zudem einzelne Verbindungen verlängern oder vorzeitig trennen.

A screenshot of the 'Guests' list table in the Hotspot Manager. The table has columns for 'NAME', 'PACKAGE', 'START TIME', 'STATUS', 'SESSION ID', and 'ACTIONS'. One row is visible with the name 'Phone' and a start time of '12/12/2017 4:38 pm'. The 'ACTIONS' column contains 'Extend' and 'Disconnect' buttons. Below the table, it indicates 'Showing 1 of 1 records'.

In der Kategorie „Voucher“ erstellen und verwalten sie die Gutschein Codes. Diese können neben der Gültigkeitsdauer auch mit weiteren Parametern erstellt werden.

A screenshot of the 'Create Voucher' form in the Hotspot Manager. The form has a title bar 'CREATE VOUCHER' and a search bar. Below the title bar are several input fields: 'CODE', 'START TIME', 'BONUS', 'OFF', 'BYTES QUOTA', 'NOTES', 'DURATION', 'STATUS', and 'ACTIONS'. A message box in the center of the form states: 'No vouchers found. No vouchers have been created.'

Erstellen von Voucher

Über den Button [Create Vouchers] können neue Gutscheincodes erstellt werden, die Anzahl der mit diesen Einstellungen zu erstellenden Codes ist dabei über das Feld „Create“ frei wählbar. Über „Quota“ können sie zusätzlich definieren ob dieser Code nur einmal eingelöst werden kann oder ob sie für mehrere Geräte verwendet werden kann. Abhängig von der Anwendung ist diese Funktion sehr nützlich da so nicht mehrere Codes an z.B. einen Hotelgast ausgegeben werden muss. Über „Expiration Time“ wird die Gültigkeitsdauer ab Beginn der ersten Verbindung eingestellt. Die Zeit kann dabei aus einer Liste von vordefinierten Werten gewählt oder über „User-defined“ frei definiert werden. Neben der Zugangskontrolle bietet die Voucher Authentifizierung zusätzlich die Möglichkeit die Bandbreite und/oder das Datenvolumen zu limitieren. Da Voucher mit den unterschiedlichsten Kombinationen generiert werden können ist so eine breite Palette an maßgeschneiderten Reglementierungen möglich.

ID	Code	Status	IP	Byte Quota	Notes	Expiration	Actions
11922-84622	11922-84622	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11923-85340	11923-85340	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11924-85976	11924-85976	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11925-86612	11925-86612	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11926-87248	11926-87248	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11927-87884	11927-87884	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11928-88520	11928-88520	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11929-89156	11929-89156	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11930-89792	11930-89792	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11931-90428	11931-90428	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11932-91064	11932-91064	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11933-91700	11933-91700	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11934-92336	11934-92336	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11935-92972	11935-92972	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11936-93608	11936-93608	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11937-94244	11937-94244	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11938-94880	11938-94880	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11939-95516	11939-95516	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11940-96152	11940-96152	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11941-96788	11941-96788	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11942-97424	11942-97424	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11943-98060	11943-98060	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11944-98696	11944-98696	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11945-99332	11945-99332	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11946-99968	11946-99968	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11947-100304	11947-100304	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11948-100940	11948-100940	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11949-101576	11949-101576	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11950-102212	11950-102212	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11951-102848	11951-102848	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11952-103484	11952-103484	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11953-104120	11953-104120	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11954-104756	11954-104756	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11955-105392	11955-105392	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11956-106028	11956-106028	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11957-106664	11957-106664	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11958-107300	11958-107300	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11959-107936	11959-107936	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11960-108572	11960-108572	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11961-109208	11961-109208	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11962-109844	11962-109844	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11963-110480	11963-110480	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11964-111116	11964-111116	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11965-111752	11965-111752	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11966-112388	11966-112388	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11967-113024	11967-113024	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11968-113660	11968-113660	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11969-114296	11969-114296	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11970-114932	11970-114932	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11971-115568	11971-115568	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11972-116204	11972-116204	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11973-116840	11973-116840	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11974-117476	11974-117476	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11975-118112	11975-118112	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11976-118748	11976-118748	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11977-119384	11977-119384	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11978-120020	11978-120020	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11979-120656	11979-120656	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11980-121292	11980-121292	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11981-121928	11981-121928	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11982-122564	11982-122564	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11983-123200	11983-123200	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11984-123836	11984-123836	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11985-124472	11985-124472	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11986-125108	11986-125108	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11987-125744	11987-125744	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11988-126380	11988-126380	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11989-127016	11989-127016	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11990-127652	11990-127652	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11991-128288	11991-128288	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11992-128924	11992-128924	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11993-129560	11993-129560	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11994-130196	11994-130196	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11995-130832	11995-130832	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11996-131468	11996-131468	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11997-132104	11997-132104	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11998-132740	11998-132740	OK				Valid for multi-use (unlimited)	Print Refresh Delete
11999-133376	11999-133376	OK				Valid for multi-use (unlimited)	Print Refresh Delete
12000-134012	12000-134012	OK				Valid for multi-use (unlimited)	Print Refresh Delete

Operatoren

In vielen Fällen müssen auch Personen Gutscheincodes erstellen bzw. verwalten können die keinen Zugriff auf den eigentlichen Controller erhalten sollen z.B. in der Rezeption. Für diese Anwendungen ist es möglich „Operatoren“ zu erstellen. Operatoren haben vollen Zugriff auf die Kategorien „Analyse“, „Guests“, „Payment“ und „Vouchers“. Die Kategorie „Operators“ ist allerdings ausgeblendet und ein Anmelden an den Controller oder CloudKey ist nicht möglich.

ID	Name	Notes
	123456	

Showing 2 of 1 records. Order per page: 10

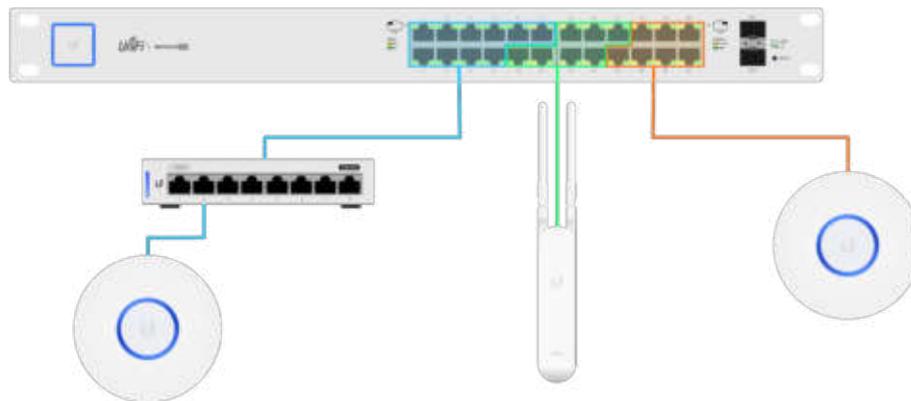
VLAN

VLANs kurz für „Virtual Local Area Network“ werden wie der Name schon vermuten lässt dazu verwendet physikalische Netzwerke in virtuelle Netzwerke zu unterteilen. Dadurch ist es möglich mehrere komplett voneinander getrennte Netzwerke gleichzeitig über ein physikalisches Netzwerk zu betreiben.

Hinweis: Für die Verwendung von VLANs über das UniFi System ist ein USG oder USG-PRO-4 erforderlich.

Portbasiertes VLAN/ Untagged VLAN

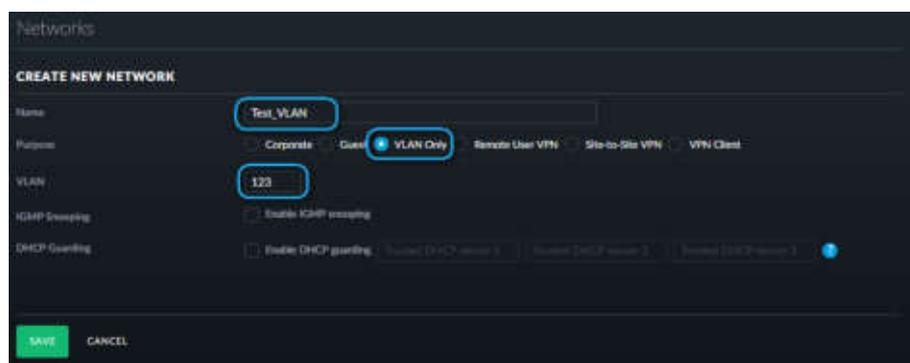
In unserem nachfolgenden Beispiel hätten wir also unseren UniFi 24Port Switch in 3stk logische Switches aufgeteilt. Das Verhalten ist dabei so als hätten sie je einen kleinen Switch für je eines der drei Netzwerke aufgebaut. Auch wenn es einige Szenarien gibt in denen eine portbasierte Aufteilung von Vorteil ist gibt es durchaus auch Nachteile. Da sie nun im wesentlichen drei Switches haben, benötigt auch jedes VLAN einen eigenen Uplink z.B. auf ihre Router/Firewall um eine Verbindung in das Internet aufbauen zu können. Das heißt die Router/Firewall muss auch mit dem Uplink von drei verschiedenen Netzwerken zurechtkommen.



Konfiguration

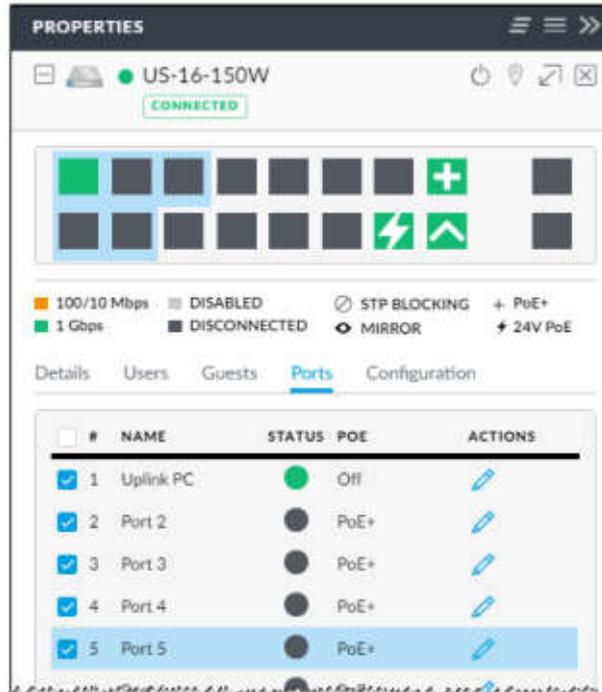
Um die entsprechenden Ports auf dem Switch zu konfigurieren muss dieser von dem Controller adoptiert sein. Gehen sie nun in die Controller Einstellungen, klicken sie unter „NETWORK“ auf [CREATE NEW NETWORK].

Info: Wenn sie für ihr VLAN ein anders Subnet verwenden möchten, wählen sie die Option „Corporate“ unter „Purpose“ aus. Weitere Infos finden sie im Bereich „Tagged VLAN“



Vergeben sie einen Namen für ihr VLAN, wählen sie die Option „VLAN Only“ und vergeben sie eine VLAN ID. Klicken sie auf [SAVE] um die Einstellungen abzuschließen. Jetzt haben wir ein VLAN erstellt und müssen es noch den Ports zuweisen.

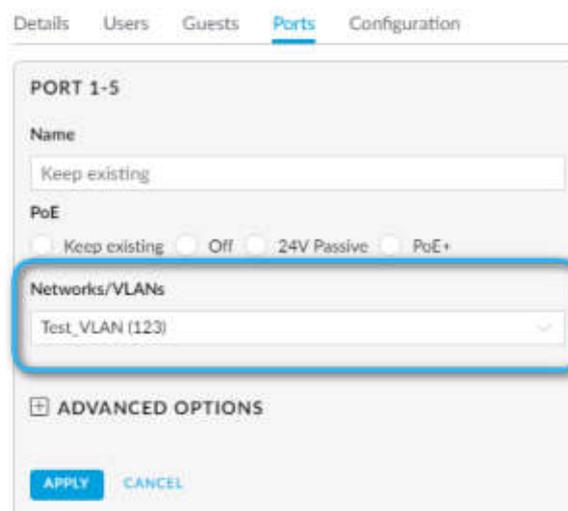
Wählen sie dazu unter „DEVICES“ den entsprechenden Switch aus um die Geräteeinstellungen zu öffnen. Markieren sie in der Portliste alle Ports die sie zu dem VLAN hinzufügen möchten.



Klicken sie auf „EDIT SELECTED“ um die Gruppe zu konfigurieren.

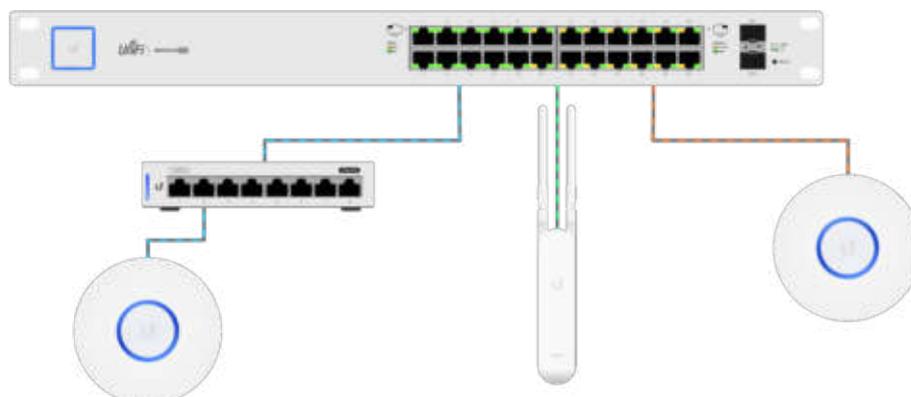


Wählen sie das erstellte VLAN aus und klicken sie auf [APPLY] um die Einstellung zu übernehmen.



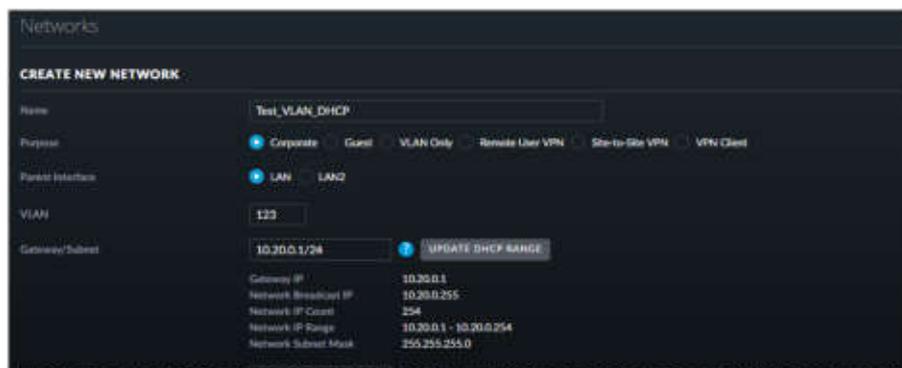
Tagged VLAN (Guest WLANs separieren)

Bei Tagged VLANs findet die Trennung nicht über einzelne Ports, sondern auf Paket Basis statt. Dabei bekommt das Datenpaket quasi ein Etikett (engl. Tag) mit der VLAN Zugehörigkeit mit auf den Weg. Dadurch ist es möglich über einen Port/ Kabel (Trunk) mehrere VLANs zu übertragen. Ein typisches Anwendungsgebiet ist die Trennung von Verwaltungs- und Gästenetzen. So ist es einfach möglich mehrere SSIDs über einen physikalischen Access Point zu verbreiten ohne dabei einen Zugriff untereinander zu befürchten.



Konfiguration

In dem nachfolgenden Beispiel werden wir ein neues VLAN erstellen und einem Gast WLAN zuweisen. Das neue VLAN wird sich zudem in einem anderen Subnet befinden und über einen eigenen DHCP Bereich verfügen. Dadurch wird auch das Zuordnen der Clients vereinfacht. Gehen sie nun in die Controller Einstellungen, klicken sie unter „NETWORK“ auf [CREATE NEW NETWORK]. Belassen sie die Auswahl auf „Corporate“ und hinterlegen sie eine VLAN ID. Geben sie anschließend ihr neues Subnet ein, in unserem Beispiel 10.20.0.1/24. Durch die Angabe „/24“ wird das Subnet mit 24Bit maskiert was der Darstellung von z.B. Windows von „255.255.255.0“ entspricht. Das Subnet ist somit also 10.20.0.x. Klicken sie auf [UPDATE DHCP RANGE] um den IP Bereich für den DHCP automatisch einzutragen.



Passen sie ihren DHCP Bereich unter „DHCP Range“ auf die gewünschte Größe an. Im Bereich „DHCP Lease Time“ wird automatisch „86400 Sekunden“ hinterlegt, das entspricht einer Vorhaltezeit von 24h und kann frei definiert werden. Klicken sie auf [SAVE] um das Netzwerk zu erstellen.



Nach dem wir nun das VLAN erstellt haben muss es nur noch in das Gäste WLAN eingetragen werden. Dazu wechseln wir zu „Wireless Networks“ und klicken bei unserem Gäste WLAN „EDIT“.



Klicken sie auf das [+] bei „ADVANCED OPTIONS“ um die erweiterten Funktionen einzublenden.



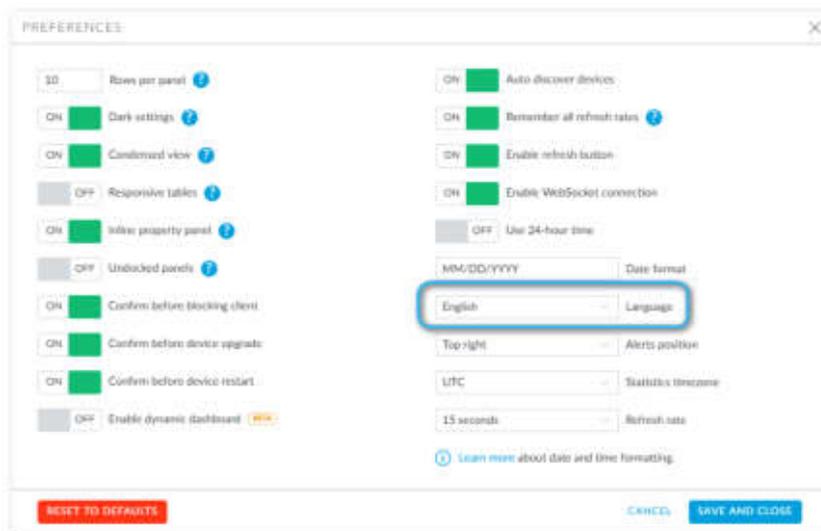
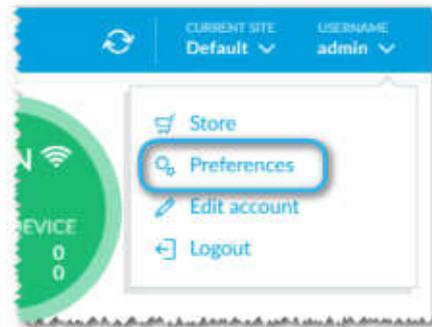
Aktivieren sie anschließend unter „VLAN“ die Option „Use VLAN“ und tragen sie die VLAN ID ein die sie erstellt haben. In unserem Beispiel ist es die VLAN ID 123.

Klicken sie auf [SAVE] um die Einstellungen zu übernehmen.

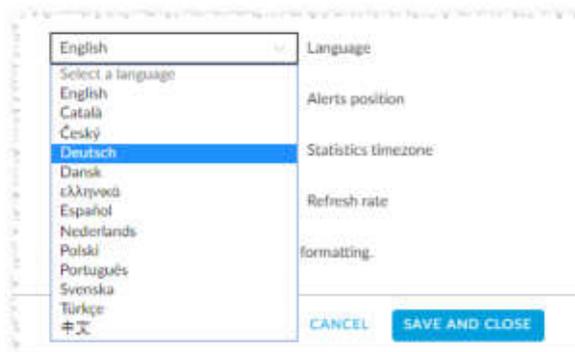
Tipps und Tricks

Ändern der Controller Sprache

Der UniFi Controller wurde bereits auf mehrere Sprachen übersetzt. Die Landessprache wird in der Regel bei der ersten Konfiguration durch die Browsereinstellungen erkannt und entsprechend eingestellt. Sollte das nicht der Fall sein oder möchten sie eine andere Sprache als die Systemsprache nutzen können sie das ganz einfach ändern. Klicken sie dazu im Controller auf den Benutzernamen rechts oben in dem blauen Balken und danach auf die beiden Zahnräder.



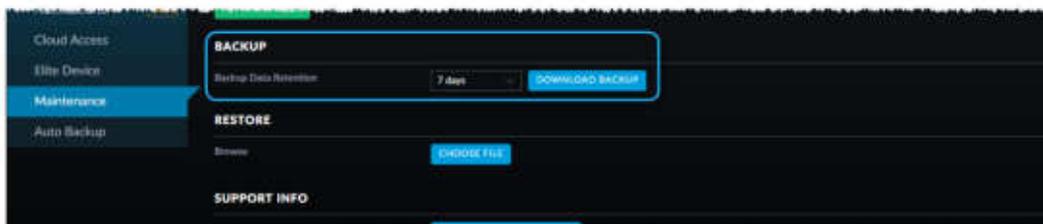
Suchen sie nun nach dem Eintrag „Language“ (die Bezeichnung wird in der aktiven Sprache dargestellt).



Wählen sie die zu verwendende Sprache aus und klicken sie auf [Speichern und Schließen].

Manuelles Backup des Controllers

Nach der ersten erfolgreichen Konfiguration und dem Adoptieren aller Geräte ist es empfehlenswert ein manuelles Backup des Controllers durchzuführen. Neben der Sicherung aller Einstellungen wird auch der generierte Hash des Controllers gespeichert. Dadurch ist es bei einem wechseln des CloudKey bzw. des Computer nicht nötig alle Geräte zurück zu setzen und neue zu adoptieren. Öffnen sie dazu die „Settings“ klicken sie auf „Maintenance“ und suchen sie nach „Backup“.



Über das Dropdown Menü können sie den Zeitraum wählen, wie weit zurück die Einträge (Alerts, Events etc.) gesichert werden sollen. Klicken sie auf [Download Backup] um die Sicherungsdatei zu erstellen.

CloudKey herunterfahren

Wie jeden Computer empfiehlt es sich auch den CloudKey herunter zu fahren bevor man ihn vom Strom trennt. Das können sie entweder über den Web Browser oder die App tun.

Web

- Verbinden sie sich auf den CloudKey und klicken sie unter „Configure your UniFi CloudKey“ auf [Configure]
- Melden sie sich am CloudKey an.
- Klicken sie auf „Maintenance“ und anschließend auf [Power Off]

App

- Melden sie sich an dem CloudKey an und klicken sie auf [Mehr]
- Drücken sie auf „Einstellungen“
- Scrollen sie bis ganz nach unten und drücken sie auf „Wartung“
- Scrollen sie wieder bis ganz nach unten und drücken sie auf „Cloud Key herunterfahren“



Fehlerbehebung:

Mein UniFi Gerät kann nicht oder nur eingeschränkt adoptiert werden.

Scheitert das Adoptieren eines UniFi Gerätes liegt das in der Regel an eine der folgenden Gründe und kann sehr einfach behoben werden.

Firmware Version:

Wenn die auf dem Gerät installierte Firmware Version sehr viel älter oder neuer als der verwendet Controller ist, kann es vorkommen das eine Adoption nicht oder nur eingeschränkt funktioniert. Um das Problem zu beheben führen sie ein Update durch. Eventuell ist es erforderlich das UniFi Gerät noch einmal aus dem Controller zu entfernen und neu einzubinden.

Falsches Subnet (kein DHCP Server):

Da für das Discovery SNMP verwendet wird können auch Geräte über das eigene Subnet hinaus gefunden werden. Für das Adoptieren bzw. für den Betrieb ist es aber erforderlich das sich die Geräte in demselben Subnet wie der Controller befinden. Meist tritt das auf wenn die Geräte in einer Umgebung ohne DHCP Server in Betrieb genommen werden. Alle UniFi Geräte (mit Ausnahme des CloudKey) verwenden dieselbe Fallback Adresse (192.168.1.20) wenn kein DHCP gefunden wird. Wenn sie den CloudKey nun also bereits mit einem andern Subnet konfiguriert haben kann das Gerät nicht hinzugefügt werden. Gehen sie wie folgt vor um die Geräte zu adoptieren:

- Ändern sie die IP Adresse des CloudKey (z.B. 192.168.1.123)damit sie sich in dem Subnet der Fallback Adresse befindet.
- Adoptieren sie ihre UniFi Geräte.
- Nach dem die Geräte erfolgreich adoptiert worden sind, ändern sie die IP Adresse der einzelnen Geräte so dass sie sich in dem Ziel Subnet befinden für das sie den CloudKey zu Beginn konfiguriert haben.
- Die Geräte Übernehmen die Einstellung und werden nach dem Neustart der Geräte als „Heartbeat Missing“ angezeigt.
- Nach dem sie alle Geräte adoptiert und die IP Adresse geändert haben, ändern sie die IP Adresse des CloudKey auf die ursprüngliche IP.
- Nun sollten alle Geräte adoptiert sein und verwendet werden können-

Nicht alle meine UniFi Geräte werden im Controller angezeigt (kein DHCP Server)

UniFi Geräte die noch keinem Controller zugeordnet sind suchen automatisch während des Boot Vorgang nach einem DHCP Server. Wird keiner gefunden oder keine Adresse ausgegeben so fährt das Gerät mit der Fallback Adresse 192.168.1.20 hoch. Da alle UniFi Geräte mit Ausnahme des CloudKey dieselbe Fallback Adresse verwenden kommt es natürlich unweigerlich zu einem IP Adressen Konflikt. Gehen sie wie folgt vor um das Problem zu beseitigen:

- Trennen sie alle angeschlossenen UniFi Geräte von der Stromversorgung.
- Schließen sie ein einzelnes UniFi Gerät wieder an.
- Adoptieren sie das Gerät und ändern sie anschließend die IP Adresse
- Prüfen sie ob das adoptierte Gerät mit der neuen IP Adresse in dem Controller als „Connected“ angezeigt wird.
- Wiederholen sie die vorherigen Punkte bis alle Geräte erfolgreich adoptiert wurden.

Nicht alle meine UniFi Geräte werden im Controller angezeigt (mit DHCP Server)

UniFi Geräte die noch keinem Controller zugeordnet sind suchen automatisch während des Bootvorgang nach einem DHCP Server. Wird keiner gefunden oder keine Adresse ausgegeben so fährt das Gerät mit der fallback Adresse 192.168.1.20 hoch. Das UniFi Gerät das den Bootvorgang abgeschlossen hat wird in dem Controller mit der IP Adresse angezeigt. Alle anderen verursachen einen IP Adressen Konflikt und trennen die Netzwerk Verbindung wieder. Wenn sie einen DHCP Server verwenden gibt dieser die Adresse an die Geräte aus wodurch jedes Gerät seine eigene Adresse erhält und es zu keinem Konflikt kommen kann. Wenn die Geräte nun trotz DHCP Server keine IP Adresse erhalten liegt ein Problem an ihrem DHCP Server vor. Prüfen sie daher folgende Punkte

IP Leases:

Ein DHCP Server vergibt IP Adressen aus einem vordefinierten IP Adressen Bereich (DHCP Pool) die einem Gerät das diese bezogen hat für einen eingestellten Zeitraum (Lease time) zugeordnet bleibt bis sie wieder vergeben werden kann. Befinden sich also alle verfügbaren Adressen in Verwendung können keine weiteren mehr ausgegeben werden und das Gerät verhält sich so als ob kein DHCP vorhanden wäre. Um das Problem zu beseitigen können sie folgende Punkte prüfen:

- **DHCP Pool Größe:** Wenn sie nicht genügend IP Adressen zur Verfügung haben können sie den DHCP Pool vergrößern um mehr IP Adressen ausgeben zu können.
- **Leas time:** Überprüfen sie wie lange die Vorhalzeit (Leas time) eingestellt ist und verkürzen sie diese

Piraten DHCP Server:

In einem Netzwerk gilt die fundamentale Regel das es nur einen DHCP Server pro Subnet geben kann (von eventuellen Spezial Umgebungen abgesehen). Es kann allerdings vorkommen (meist unbeabsichtigt) dass neben dem Server der verwendet werden soll, sich noch weitere DHCP Server in dem Subnet tummeln. Oft passiert dass dann wenn z.B. ein neues Gerät das über eine DHCP Server Funktion verfügt (z.B. Router, Printserver, etc.) an das Netzwerk ohne vollständige oder richtige Konfiguration angeschlossen wird. Fährt ein DHCP Client hoch bezieht dieser die IP von dem Server der als erstes auf die Anfrage antwortet. Um das Problem zu beseitigen müssen sie daher das entsprechende Gerät finden und den DHCP Server deaktivieren.

Der UniFi Switch gibt nach einem Stromausfall kein PoE mehr aus

In vereinzelt Fällen ist es vorgekommen dass der UniFi Switch nach einem Stromausfall kein PoE mehr ausgab, ansonsten aber ohne Probleme funktioniert hat. Der Fehler konnte einfach behoben werden, indem alle angeschlossenen Netzkabel abgeschlossen, der Switch neugestartet und anschließend wieder angeschlossen wurde. In allen Fällen konnte der Fehler nicht reproduziert werden und alle Geräte funktionierten danach ohne Probleme oder Ausfälle auch nach weiteren Stromausfällen.

Info:

Auch wenn der beschriebene Fehler sehr selten auftritt und in der Regel keine Schäden bzw. Folgeschäden/Probleme verursacht empfehlen wir ausdrücklich alle Switche so wie die Kernkomponenten wie USG und CloudKey durch eine USV vor Stromausfällen und Spannungsschwankungen zu schützen.

Der CloudKey blinkt weiß und der Controller kann nicht geöffnet werden

Werden auf Grund eines Stromausfalles oder Spannungsschwankungen Konfigurationsdateien beschädigt kann der Controller nicht mehr richtig starten. In diesem Fall ist es erforderlich den CloudKey zurück zu setzen und die Sicherung einzuspielen.

Info: Wir empfehlen alle UniFi Kern Komponenten wie CloudKey, USG und alle Switche mit einer USV vor Spannungsschwankungen und Stromausfällen zu sichern und den CloudKey vor jedem Trennen vom Stromkreis herunter zu fahren um Probleme zu vermeiden.