Radius-Server mit MAC-Authentication an den Switchen einrichten

Inhaltsverzeichnis

Dieser Beitrag konzentriert sich den Bereich Netzwerk.

Folgende Sachen sind an diesem Wiki Beitrag noch zu überarbeiten:

1. Konsolidierung mit dem WLAN Beitrag, bspw. das Anlegen eines Radius Profils und von Radius Usern in einen eigenen Beitrag auslagern und dann von hier darauf verweisen
2. Herausfinden ob und beschreiben wie MACauth am Uplink Port funktioniert
3. Fallback VLAN besser beschreiben
4. Gebt gern Feedback unten in der Kommentarfunktion. Was fehlt euch, was ist unverständlich beschrieben, etc.?

Was wollen wir?

Radius in der Unifi Network Application (Controller) konfigurieren, damit wir dies als Basis für MAC Authentication an unseren Switchen verwenden können.

Warum wollen wir das?

Wir wollen, dass sich Geräte per MAC-Adresse am Switchport authentifizieren, um diese dynamisch in unterschiedliche VLANs zu führen. Außerdem wollen wir ein Fallback VLAN konfigurieren, damit nicht jeder, der ein Ethernetkabel in einen evtl. physikalisch ungeschützten Switch (unverschlossener Raum oder Verteilerschrank) steckt, Zugriff auf schützenswerte Komponenten, Applikationen oder Daten erhalten kann.

Hinweis: Eine reine MAC-Authentication ist nicht als sicher einzustufen, da MAC-Adressen leicht gespoofed (mitgeschnitten) und an der Schnittstelle eines PCs konfiguriert werden können. Die Konfiguration ist aber besser als nichts und bietet zudem den bereits erwähnten Vorteil der automatischen VLAN Zuweisung auf Basis der MAC-Adresse. Wir müssen also nur einen Radius User mit einer VLAN ID anlegen und anschließend wird das Endgerät bei entsprechender Konfiguration der Switchports automatisch in das richtige VLAN gebracht.

Was ist MAC-Authentication?

Auf Basis der MAC-Adresse entscheidet der Radius Server, ob sich ein Gerät mit dem Netzwerk verbinden darf. Ist die MAC-Adresse nicht bekannt, wird der Verbindungsaufbau abgelehnt oder das Gerät in ein Fallback VLAN geschoben.

Und wie geht das genau?

1 Radius Profil anlegen

Menü (v6.5.55): "Settings - Advanced Features - Radius" -> Einstellungen des Default Profiles wie folgt anpassen:

Wenn sich Endgeräte mit Ethernet-Schnittstelle per MAC-Adresse am Switchport per Radius authentifizieren sollen, ist die Einstellung "Enable Wired" im "Default" Radius Profil zu aktivieren. Wenn dieses Profil zusätzlich auch für Wireless Endgeräte verwendet werden soll, ist zusätzlich die Option "Enable Wireless" zu aktivieren, mehr dazu: >>> hier klicken <<<

Datei nicht gefunden oder type unknown
?thumbnail=1

2 Radius User anlegen

Menü (v6.5.55): "Settings - Advanced Features - Radius" -> "Default Profile - Radius Users" auswählen und Schaltfläche "Create New Radius User" betätigen:

Image not found or type unknown
?thumbnail=1

Hier wird kein herkömmlicher User mit Passwort angelegt, sondern die MAC-Adresse eures Gerätes als "User" und "Password" eingegeben.

Achtung! Es funktioniert ausschließlich folgendes Format (Im Bereich WLAN können auch andere Formate ausgewählt werden. Diese funktionieren hier aber nicht!):

AABBCCDDEEFF

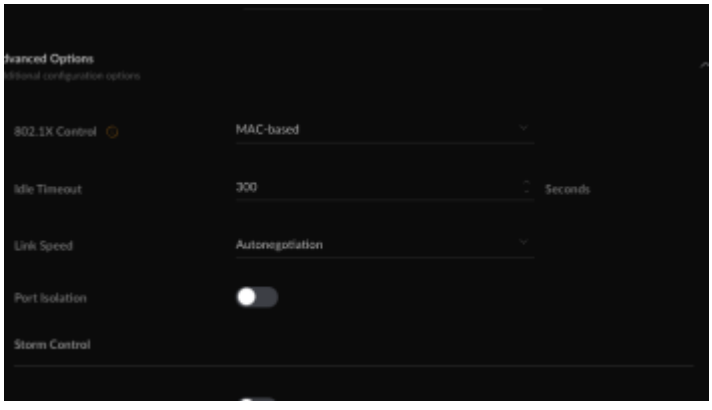
- Username: <mac-address>
- Password: <mac-address>
- VLAN ID: <vlan_id>
- Tunnel Type: 13 - Virtual LANs (VLAN)
- Tunnel Medium Type: 6 - 802 (includes all 802 media plus Ethernet "canonical format")

Bei der VLAN ID tragt ihr einfach die ID eures VLANs ein, wie der Name schon sagt. Soll das entsprechende Gerät bzw. der User in das Default LAN lasst ihr das Feld einfach leer.

Wenn man die MAC-Adresse nicht kennt, kann die Konfiguration eines Fallback VLANs hilfreich sein.

3 Switch Port Profil einrichten

Im Menü "Settings - Advanced Features - Switch Ports" ist über die Schaltfläche "Add a Port Profile" ein neues Profil anzulegen und wie folgt zu konfigurieren:

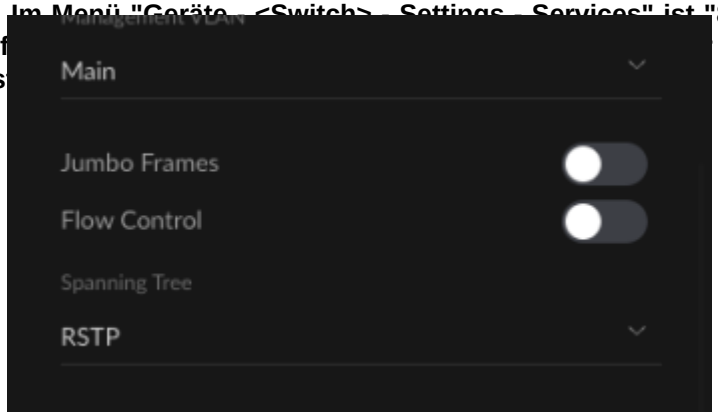


Erläuterungen:

- Unter "Native Network" gebt Ihr euer Management (V)LAN an (in meinem Fall "Main")
- Unter "Tagged Networks" sind alle Netzwerke anzugeben, die später auch über den RADIUS zugewiesen werden können sollen
- Unter "802.1x Control" ist "MAC-based" auszuwählen

4 802.1x am Switch aktivieren

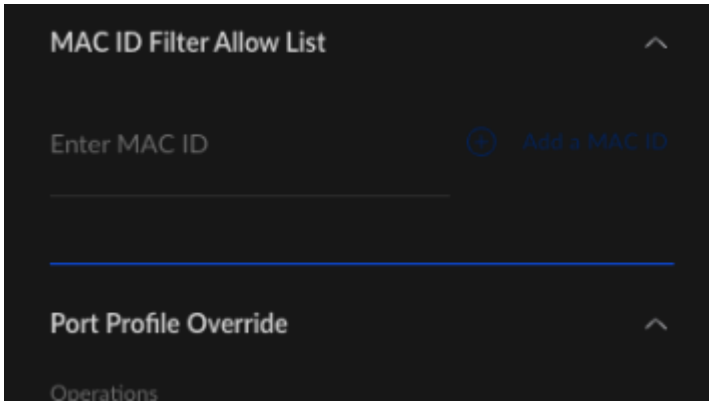
4.1 Im Menü "Geräte - <Switch> - Settings - Services" ist "802.1x Control" zu aktivieren, das Radius Prof bevorzugtes Fallback VLAN (bspw. das Gäs



4.2

5 Switch Port Profile umstellen

5.1 Im Menü "Geräte - <Switch> - Settings - Ports" ist ein Port auszuwählen, wo ihr bspw. einen Windows PC für Testzwecke anschließt, und das Port Profile von "All" auf das zuvor erstellte Profil "MACauth" umstellt. Wir konfigurieren erstmal nur einen Port! Wenn dieser eine Port so läuft wie wir uns das vorstellen, können weitere Radius User angelegt und weitere Switch Ports auf das MACauth Profil umgestellt werden.



1. "MAC ID Filter Allow List" ist für unseren Usecase nicht relevant
2. "Port Profile Override" Einstellungen können bei Bedarf angepasst werden, können aber auch in den Default Einstellungen bleiben

6 Testen anhand eines Windows PCs

1. Öffne ein Kommando Fenster "cmd" und ermittle die derzeitige IP-Adresse mit "ipconfig /all".
2. Anschließend führe ein "ipconfig /release" aus, um das DHCP-Lease des Windows PCs freizugeben
3. Nun führe ein "ipconfig /renew" aus, um eine IP aus dem dem Radius User zugewiesenen VLAN zu erhalten

4. Ändere die VLAN ID am Radius User Um zu testen, ob der User eine IP aus diesem VLAN erhält, führe Schritt 2. und 3. dieses Kapitels erneut aus

7 Tips und Tricks

7.1 MAC-Authentication funktioniert trotz Übernahme des Switch Port Profils nicht

Nach der Übernahme des MACauth Switch Port Profils auf einen spezifischen Switch Port kann es vorkommen, dass die Einstellungen nicht sofort greifen. Heißt, die MAC-Authentication funktioniert am Port nicht. Ich habe zufällig herausgefunden, dass es klappt, wenn man wie folgt vorgeht:

1. Im Menü "Settings - Advanced Features - Switch Ports" das erstellte Profil "MACauth" anklicken und anschließend unter "Advanced Options - 802.1x Control" umstellen auf "Force authorized" -> "Apply Changes"
2. Im Menü "Settings - Advanced Features - Switch Ports" das erstellte Profil "MACauth" anklicken und anschließend unter "Advanced Options - 802.1x Control" umstellen auf "MAC-based" -> "Apply Changes"

8 Upvote des Feature Requests im offiziellen Ubiquiti Forum

Wenn euch Radius, 802.1x, MAC-Authentication und Co gefällt, lasst gerne ein Upvote bei folgendem Feature Request da und diskutiert mit, was euch fehlt:

https://community.ui.com/questions/Radius-Users-and-Radius-Profile-improvement-suggestions/41760fec-f6b0-4d09-ae12-bffa14a6a664

Auswählen:

Gültige Software-Version Keine Firmware-Relevanz!