Michel Smidt
Blog, IT in Schulen
Keine Kommentare

Dass das Thema WLAN für Schulträger nach wie vor drängend ist, zeigte im September einmal wieder eine neue Studie der Bertelsmann Stiftung zur „Digitalisierung an Schulen: Der Geist ist willig, das WLAN schwach“. In dieser gab nur jede dritte Lehrerkraft an, dass sie mit der WLAN-Qualität zufrieden sei. Jede Fünfte gab sogar an, dass es an ihrer Schule gar kein WLAN gibt.

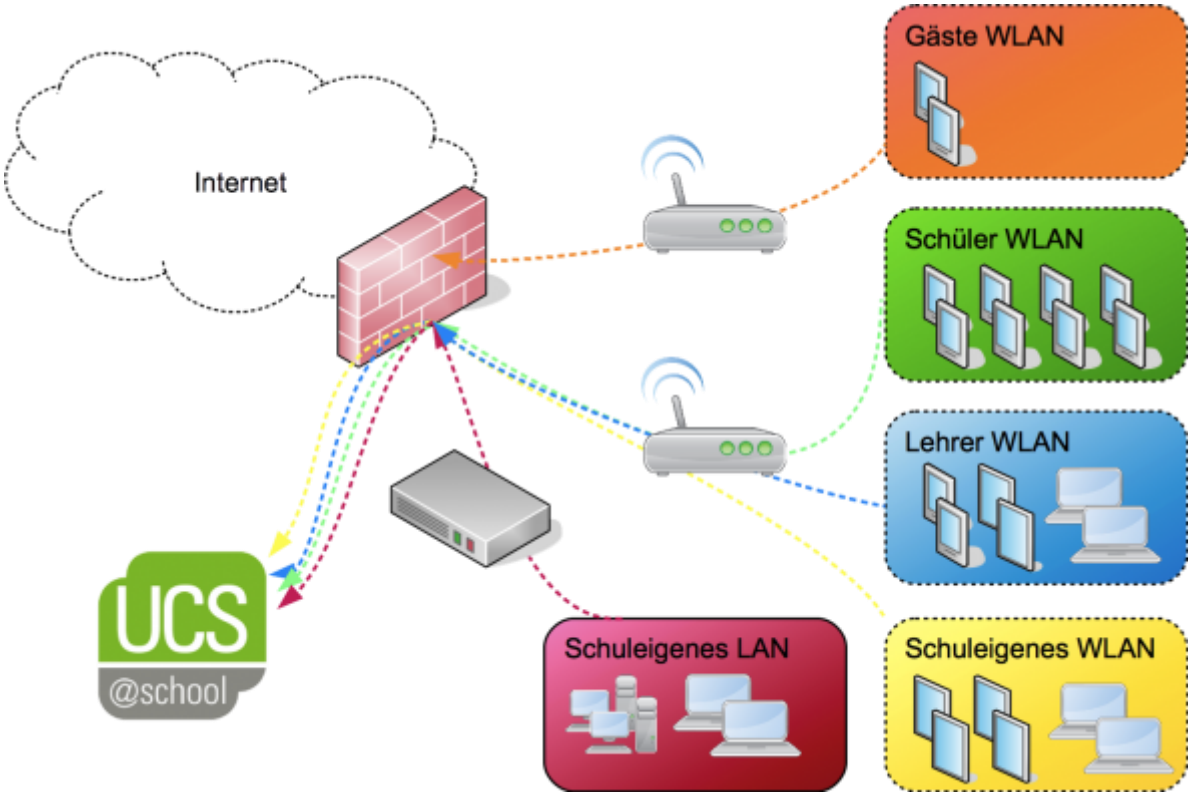
Das Professional Service Team von Univention arbeitet nun schon seit Jahren am flächendeckenden Ausrollen von WLAN-Umgebungen. Nicht nur an Einzelschulen sondern auch schul- und sogar stadtübergreifend, wie zum Beispiel in kommunalen Bibliotheken. Eine Vision, die sich mittelfristig verwirklichen ließe, wäre für Schulträger die automatische Teilnahme an Education Roaming kurz eduroam, einer Initiative für einen freien Internetzugang an Bildungseinrichtungen.
Ein umfangreicher Breitbandausbau wäre dafür natürlich förderlich, aber man kann auch ohne Glasfaser schon viel erreichen. Wesentliche Fragen zur Konzeption und dem technischen Betrieb von WLAN in Schulen haben meine Kollegen Jan Christoph Ebersbach und Tobias Birkefeld in den Beiträgen Kurz erklärt: Bring Your Own Device (BYOD) und Kurz Erklärt: RADIUS bereits beantwortet. Dabei ging es um die konzeptionellen Herausforderungen und den Einsatz der RADIUS-App bei der Einführung von WLAN-Umgebungen. Ich möchte heute nun etwas praktischer auf die konkrete Einführung und Konfiguration von WLAN bei Schulträgern eingehen.
Ziel für Schulträger aus technischer Sicht ist es, den Lehrkräften, Schülern und Schülerinnen der einzelnen Schulen möglichst unkompliziert Zugang zum Internet zu ermöglichen. Leicht administrierbar, sicher und rechtlich abgesichert. Hierfür wird in aller Regel der Term BYOD (Bring Your Own Device) verwandt. Jeder Anwender kann sein eigenes persönliches, internetfähiges Gerät mitbringen und bekommt damit Zugang zum Internet.

In UCS@school (für die paedML gilt das selbstverständlich auch) lösen wir dies zu wesentlichen Teilen mit dem RADIUS-Server FreeRADIUS. Aus diesem Grund

konzentriert sich dieser Artikel auf die Konfiguration des RADIUS-Servers speziell für die Anforderungen von Schulträgern.
Schulträger haben in diesem Zusammenhang meist folgende Anforderungen:

1. Schuleigene Geräte (iPads, Windows Rechner etc.) sollen ein eigenes WLAN-Netz erhalten.
2. Die privaten mobilen Geräte der Lehrerschaft sollen ein separates WLAN-Netz erhalten.
3. Die mobilen Geräte der Schülerschaft sollen ebenfalls ein eigenes WLAN-Netz erhalten.
4. Es soll ein Gäste-Zugang ins WLAN via Voucher-System geben.
5. Die Lehrkräfte sollen in die Lage versetzt werden, (temporär) ihrer Klasse das Internet abzuschalten.

Schematisch könnte ein solches Szenario an einer BYOD-Demo-Schule etwa folgendermaßen aussehen:



Schemagrafik: Szenario an einer BYOD-Demo-Schule

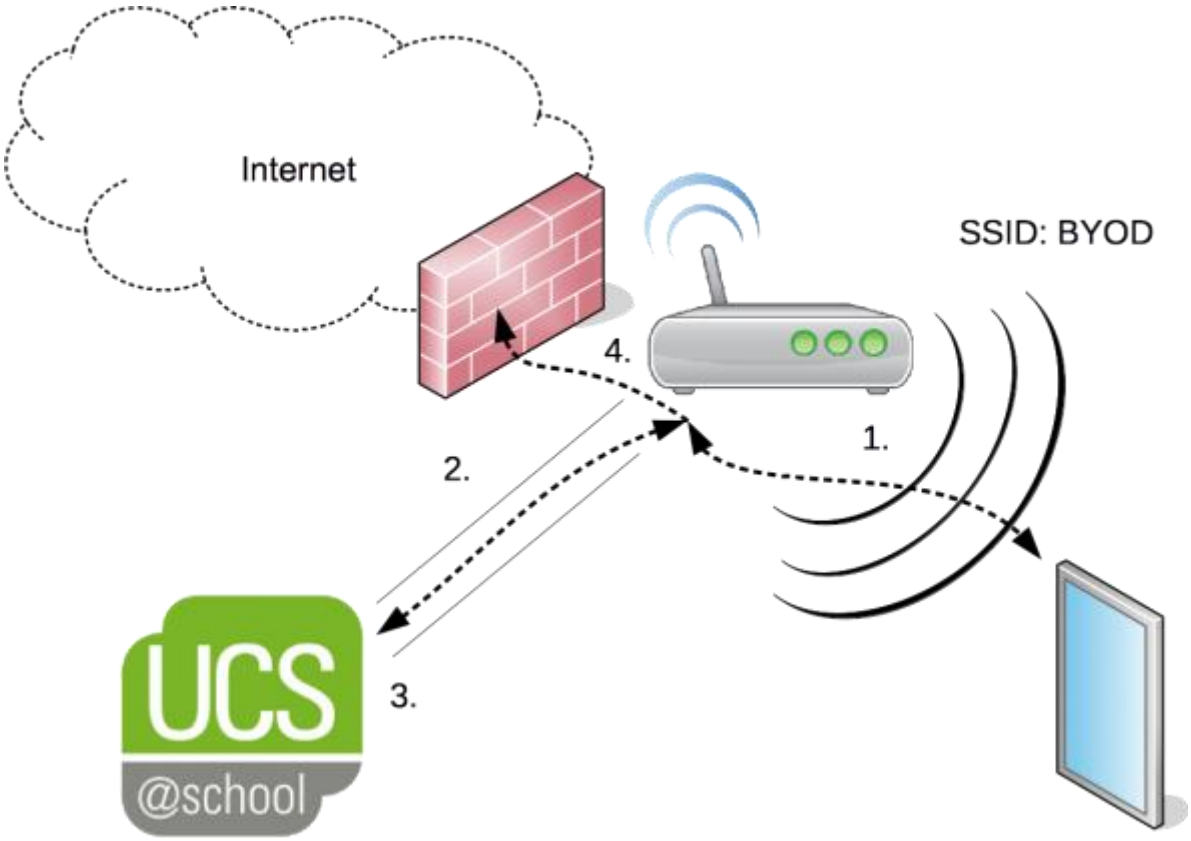
Großer Vorteil dieses Setups ist, dass alle Schüler/innen und Lehrkräfte sich mit den gewohnten persönlichen Anmeldedaten (Windows, Dateiablage, Raumplanung) am WLAN anmelden können. Ein weiterer Vorteil ist, dass schulübergreifende Benutzerkonten voll unterstützt werden und somit beispielsweise Lehrkräfte auch an den weiteren Schulen, an denen sie unterrichten, automatisch WLAN-Zugang erhalten. Technisch wird dieses Setup über VLANs geregelt. Dabei handelt es sich um einen Industriestandard, in dem die Geräte in die einzelnen Netze (schuleigene (gelb), Lehrer- (blau) und Schülergeräte (grün)) separiert werden. Das Gäste-Netz wird über ein Captive-Portal mit Voucher-System betrieben. UCS@school übernimmt für alle anderen Netze die Authentifizierung und VLAN-Zuweisung der Anfragen, die über die Access Points ankommen. Für die Authentifizierung wird dabei noch einmal zwischen Benutzerzugängen (Lehrkräfte und Schüler/innen) und Gerätezugängen (geteilte schuleigene Geräte) unterschieden . Im UCS@school-Verzeichnisdienst befinden sich

typischerweise nicht nur die Benutzer, sondern auch die Geräte, die an den Schulen in Betrieb sind. Diese Geräte – man spricht hier auch von Rechnerkonten – haben genauso wie die Benutzer einen Namen und ein Passwort, mit dem sie zum Beispiel in die Windows-Domäne gejoint sind und welches sie für die Anmeldung am WLAN verwenden können.
Diese Art der Konfiguration ist übrigens sehr ähnlich zu Konfigurationen im Enterprise-Umfeld. In dem Fall handelt es sich natürlich nicht um „Lehrer- und Schülergeräte“ sondern „Marketing-“, „Entwicklungs-“ und „Admin-Notebooks“.

Authentifizierung mit RADIUS

Wie schon erwähnt wird der Zugang zum WLAN über das RADIUS-Protokoll geregelt. Das RADIUS-Protokoll selbst ist eigentlich nur eine zusätzliche Hülle um die Protokolle für die Authentifizierung (PEAP, MSCHAPv2) und Verschlüsselung (WPA, TKIP).

Schematisch stellt sich eine Authentifizierung mit RADIUS folgendermaßen dar:



Schemagrafik: Authentifizierung mit RADIUS

1. Der Client (hier iPad) versucht sich in das WLAN mit der SSID „BYOD“ einzuwählen.
2. Der Access Point empfängt das Signal und leitet es weiter an den UCS@school RADIUS-Server. Dazu wird ein verschlüsselter Tunnel zwischen dem RADIUS-Server und dem Access Point aufgebaut. Durch diesen Tunnel werden alle folgenden Nachrichten zwischen dem Client und dem RADIUS-Server geleitet.
3. Der RADIUS-Server verifiziert die Anmeldedaten im Verzeichnisdienst und schreibt die der Rolle entsprechende VLAN-ID in die Antwort. Prinzipiell könnte man hier auch weitere

Attribute mitgeben, um beispielsweise „Quality of Service“ (QoS) rollenbasiert zu machen. Meiner Erfahrung nach reicht es aber in der Regel aus, „Quality of Service“ einfach VLAN-basiert durchzuführen und damit sicherzustellen, dass der Datenverkehr von schuleigenen Geräten Vorrang vor BYOD-Datenverkehr hat.

4. Der Access Point liest die VLAN-ID aus und weist den Client in das VLAN.
5. Der Client ist erfolgreich im WLAN und kann nun in das Internet.

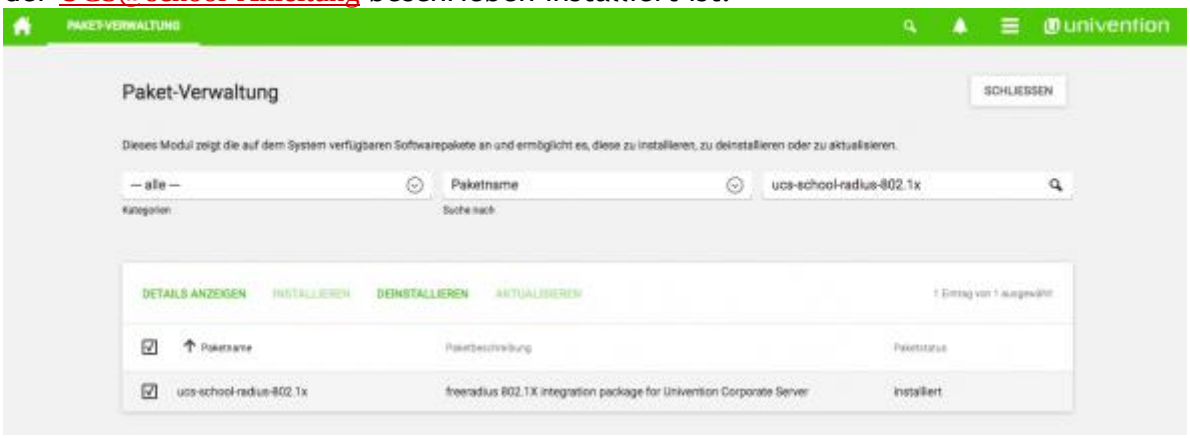
RADIUS-Server Installation

In UCS@school gibt es zur Zeit zwei Varianten, einen RADIUS-Server umzusetzen.

1. Die Installation der RADIUS-App aus dem Univention App Center
2. Die Installation des Pakets „ucs-school-radius-802.1x“

Die erste Variante empfehlen wir bei rein zentralen UCS-Systemen und einer Administration ausschließlich von Domänen-Administratoren. Neben der Authentifizierung findet hier Autorisierung über LDAP-Attribute an den Nutzer-Objekten statt.

Die zweite Variante empfehlen wir in Schulumgebungen, da es über Internetregeln möglich ist, den Zugang für bestimmte Benutzer und Klassen einzuschränken. Diese Möglichkeiten zur Autorisierung können außerdem an die Lehrerschaft und Schuladmins delegiert werden. Schulübergreifende Benutzer haben selbstverständlich an allen für sie freigeschalteten Schulen weiterhin WLAN-Zugang. In den folgenden Abschnitten setzen wir deshalb voraus, dass das Paket „ucs-school-radius-802.1x“ wie in der UCS@school-Anleitung beschrieben installiert ist.



Screenshot: Paket-Verwaltung in UCS@School

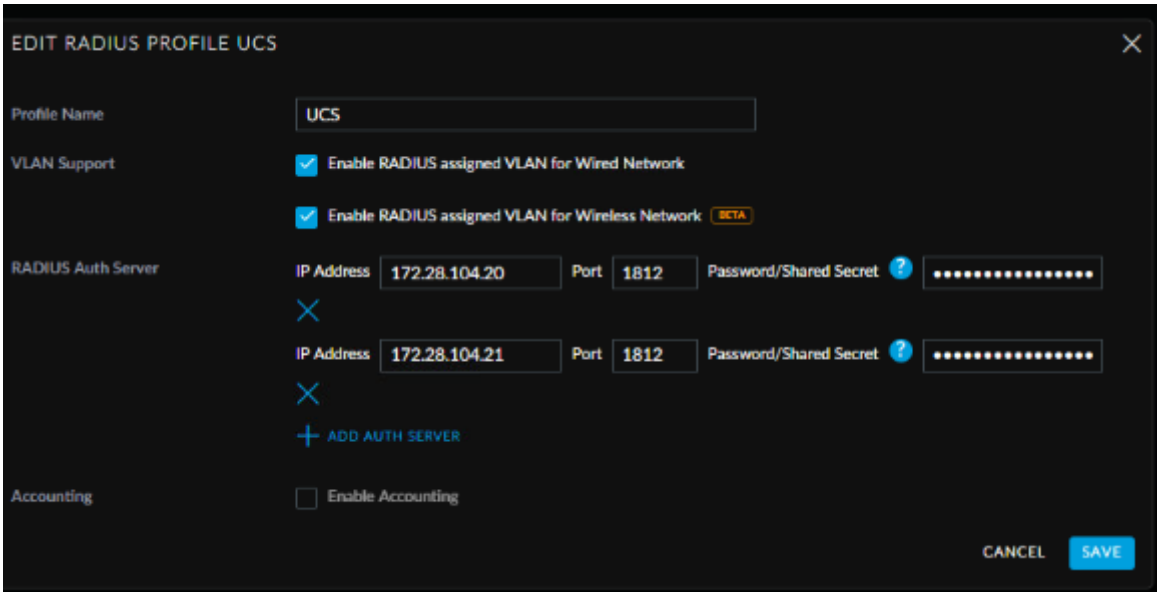
RADIUS-Server Shared Secret

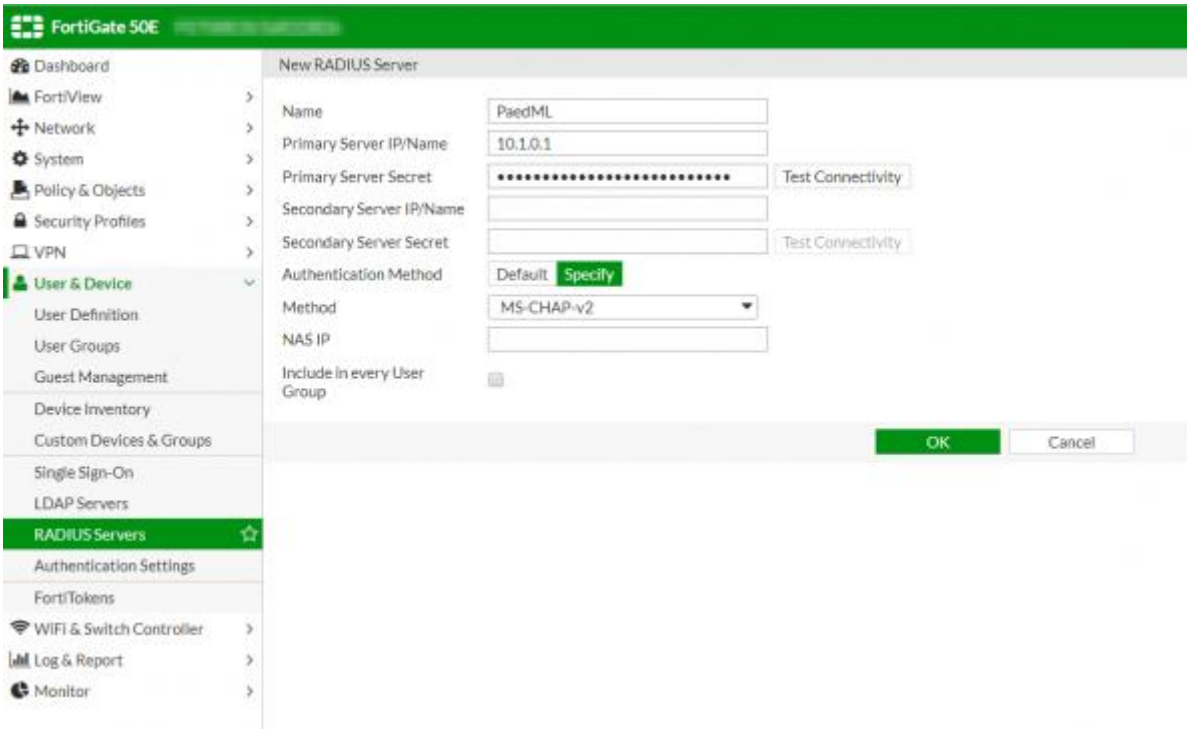
Für den Aufbau des Tunnels in Abbildung 2 „Schemagrafik: Authentifizierung mit RADIUS“ in Schritt 2 wird ein Secret (Pre-Shared-Key) zwischen dem RADIUS-Server und Access Points ausgetauscht. In UCS@school wird dazu in der Datei clients.conf (/etc/freeradius/clients.conf) das Secret eingetragen:

```
client 10.200.22.0/24 {

 secret = geheimgeheim
```

```
}
```

Im Access Point Controller sieht dies beispielsweise folgendermaßen aus:





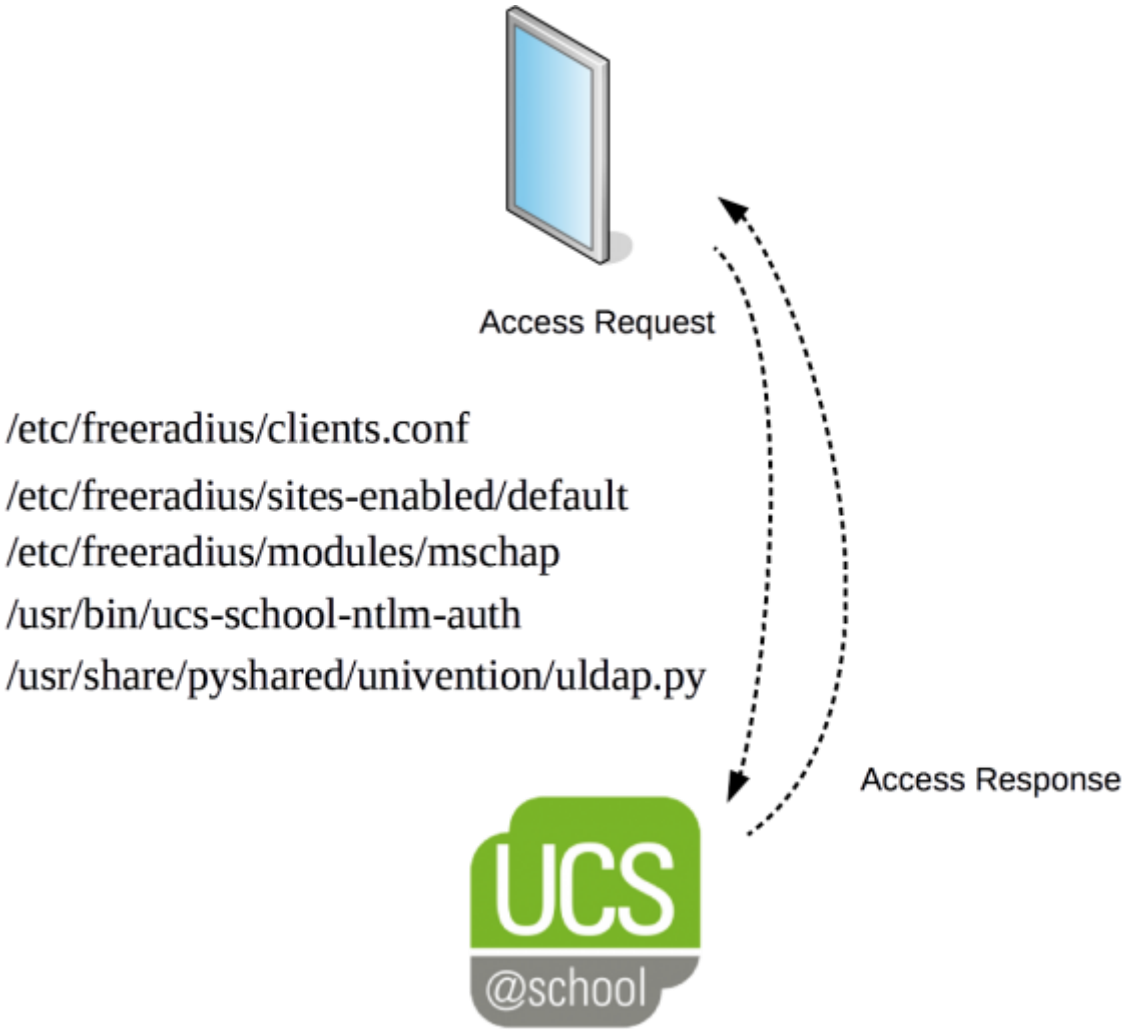
RADIUS-Server - Authentifizierungs-Anfrage, der interne Prozess und Konfiguration

Eine Authentifizierungs-Anfrage sieht typischerweise folgendermaßen aus:

```
Sending Access-Request of id 13 to 127.0.0.1 port 1812

 User-Name = "testlehrer"
```

```
NAS-IP-Address = 10.200.44.41

NAS-Port = 0

Message-Authenticator = 0x00000000000000000000000000000000

MS-CHAP-Challenge = 0x25c553d097a145a5

MS-CHAP-Response = 0x000100000000000000000000000000000000000000000000000000c06
```

Wenn eine Authentifizierungs-Anfrage an den RADIUS-Server gestellt wird, passieren grob folgende Schritte:



Schemagrafik: Ablauf einer Authentifizierungs-Anfrage an den RADIUS-Server

1. Der RADIUS-Server schaut in der clients.conf-Datei nach, ob er zuständig ist. Das heißt, ob es einen Eintrag gibt (IP-Addresse oder Netzbereich), der auf die anfragende IP-Addresse passt. Wird die Anfrage also von einem Access Point mit der IP 10.200.22.31 gestellt, muss in der clients.conf mindestens ein Eintrag vorhanden sein, der diese IP einschließt. Beispielsweise:

```
client 10.200.22.0/24 {

 secret = geheimgeheim
```

```
 virtual_server = custom

 }
```

2. Findet sich ein Eintrag, wird ein verschlüsselter Tunnel zwischen dem Access Point und dem RADIUS-Server aufgebaut. Außerdem wird eine RADIUS-Konfiguration geladen. Standardmäßig ist dies die default-Datei in /etc/freeradius/sites-enabled/. Für ein Szenario ohne VLAN-Zuweisung mit ausschließlicher Authentifizierung reicht diese default-Datei vollkommen aus.

3. Wenn diese Standardkonfiguration jedoch nicht ausreichen sollte, kann in FreeRADIUS ein ähnlicher Mechanismus wie bei Apache mit dem Verzeichnissen sites-available und sites-enabled (/etc/freeradius/sites-{available,enabled}/) genutzt werden. Man kann hier weitere RADIUS-Konfiguration erstellen und mit dem Schlüsselwort „virtual_server“ in der clients.conf auswählen. Ich kopiere meist die default-Datei und umfasse den Inhalt der gesamten Datei mit einem „server custom { … }“-Block (unten am Artikel steht Ihnen so eine Beispieldatei zum Download zur Verfügung).

```
 $ cp /etc/freeradius/sites-available/default /etc/freeradius/sites-
available/custom

 $ ln -s /etc/freeradius/sites-available/custom /etc/freeradius/sites-enabled/

 $ vim /etc/freeradius/sites-available/custom
```

4. Jede RADIUS-Konfiguration enthält verschiedene Abschnitte, die während des Authentifizierungsprozesses durchlaufen werden. Das kann man auch immer sehr schön sehen, wenn man FreeRADIUS im Debug-Modus startet.

```
 $ service freeradius stop

 $ freeradius -X
```

5. Wichtigste Abschnitte im UCS@school Anwendungsfall sind:

- authorize (Module zur Authentifizierung.)
- authenticate (Welche Möglichkeiten zur Authentifizierung werden angeboten.)
- post-auth (Wird nach erfolgreicher Authentifzierung aufgerufen.

6. Der Abschnitt *authorize* definiert alle Module, die zur Authentifizierung sequentiell abgearbeitet werden. Die Module selbst befinden sich im Verzeichnis /etc/freeradius/modules/. Das entscheidende Modul für UCS@school ist das Modul mschap. Neben einer Reihe von Konfigurationsparametern enthält es ganz am Ende eine entscheidende Zeile:

```
 ntlm_auth = "/usr/bin/ucs-school-ntlm-auth-suidwrapper --request-nt-key --
username=%{%{Stripped-User-Name}:-%{%{User-Name}:-None}} --
challenge=%{%{mschap:Challenge}:-00} --nt-response=%{%{mschap:NT-Response}:-00} --
station-id=%{outer.request:Calling-Station-Id}"
```

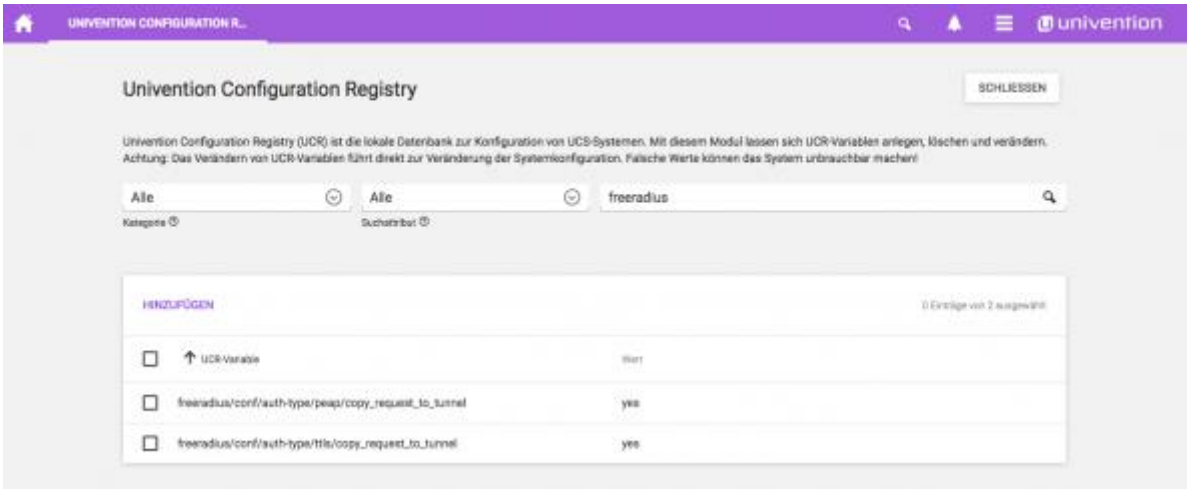
Diese Zeile ruft ein von UCS@school implementiertes Skript auf, das den Benutzer oder Rechner anhand seiner Anmeldedaten im LDAP verifiziert. Aber nicht nur das. Zusätzlich wird hier außerdem geprüft, ob dem Benutzer oder Rechner eine Internetregel zugewiesen wurde, die den WLAN-Zugang erlaubt. Hier finden Sie

weitere Informationen zu Internetregeln. Mit Internetregeln würde man beispielsweise die Anforderung 5. „Die Lehrer sollen in die Lage versetzt werden, (temporär) ihrer Klasse das Internet abzuschalten.“ umsetzen. Man kann dies hier sehr flexibel konfigurieren.

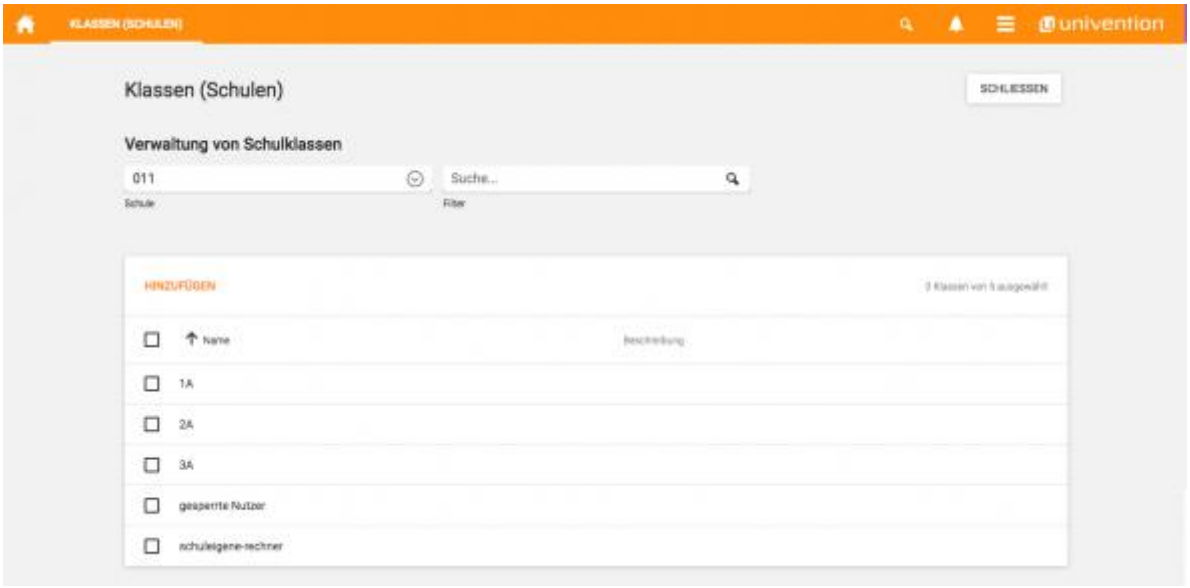
7. Nach erfolgreicher Authentifizierung des Benutzers oder Rechners wird abschließend noch der Abschnitt *post-auth* aufgerufen. Hier fügen wir dann normalerweise die speziellen VLAN-IDs der Antwort (RADIUS-Response) hinzu. Einen beispielhaften Abschnitt der Konfiguration für die custom-Datei (/etc/freeradius/sites-available/custom) finden Sie hier sowie angehängt an den Artikel:

```
# Load module: ldap

 ldap

 if ("%{request:User-Name}" =~ /^host\/(.*).domain$/) {

 update request {

 User-Name := "%{1}$"

 }

 }

 # Gemeinsame SSID



# Anforderung 1. Schuleigene Geräte (iPads, Windows Rechner etc.) sollen ein
eigenes WLAN-Netz erhalten.

 if ("%{ldap:ldap:///dc=ldap,dc=basis ?cn?sub?(&(memberUid=%{User-
Name})(cn=schuleigene-rechner))}") {

 update reply {

 Reply-Message := "DEBUG: Schuleigene Rechner"

 Tunnel-Type := VLAN

 Tunnel-Medium-Type := IEEE-802

 Tunnel-Private-Group-Id := "1032"

 }

 }

 # Anforderung 2. BYOD der Lehrerschaft sollen ein eigenes WLAN-Netz erhalten.

 elsif ("%{ldap:ldap:///dc=ldap,dc=basis?cn?sub?(&(memberUid=%{User-
Name})(cn=lehrer-schuleXXX))}") {

 update reply {

 Reply-Message := "DEBUG: Lehrer Schule BYOD"
```

```
Tunnel-Type := VLAN

Tunnel-Medium-Type := IEEE-802

Tunnel-Private-Group-Id := "1064"

}

# Anforderung 3. BYOD der Schülerschaft sollen ein eigenes WLAN-Netz erhalten.

elsif ("%{ldap:ldap:///dc=ldap,dc=basis ?cn?sub?(&(memberUid=%{User-
Name})(cn=schueler-schuleXXX))}") {

update reply {

Reply-Message := "DEBUG: Schüler Schule BYOD"

Tunnel-Type := VLAN

Tunnel-Medium-Type := IEEE-802

Tunnel-Private-Group-Id := "1064"

}

}

else {

update reply {

Reply-Message := "DEBUG: Not found, reject"

}

reject

}
```



8. Mit dieser Konfiguration kann man die Standardanforderungen erfolgreich umsetzen. Wichtig hinzuzufügen ist, dass schuleigene Geräte standardmäßig der Klasse „schuleigene-rechner“ hinzugefügt wurden.



Screenshot-Verwaltung-von-Schulklassen-in-UCSatSchool

9. Testen kann man die Konfiguration am besten folgendermaßen:

1. Es gibt in der clients.conf (/etc/freeradius/clients.conf) immer ein Beispielkonfiguration für den „client localhost“. Darin setzen sie die zu verwendende Konfiguration auf „custom“:

```
virtual_server = custom
```

2. Anschließend stoppen Sie den Service FreeRADIUS und starten den Debug-Modus:

```
$ service freeradius stop

$ freeradius -X
```

3. Mit folgenden Befehlen auf der Kommandozeile können Sie nun die RADIUS-Konfiguration testen. Achten Sie darauf, dass Sie beim Testrechner immer ein „$“ dem Name hinzufügen. Das ist wichtig, um deutlich zu machen, dass es sich um ein Rechnerkonto handelt.
Reine LDAP-Authentifizierung:

```
$ radtest testbenutzer passwort localhost 10 testing123

$ radtest testrechner$ passwort localhost 10 testing123
```

Als Ausgabe muss eine Access-Accept-Antwort ausgegeben werden:

```
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=246, length=20
```

Sollte es eine Access-Reject-Antwort geben, prüfen Sie bitte Benutzernamen und Passwort erneut:

```
rad_recv: Access-Reject packet from host 127.0.0.1 port 1812, id=129, length=20
```

LDAP-Authentifizierung und Internetregelprüfung:

```
 $ radtest -t mschap testbenutzer passwort localhost 10 testing123

 $ radtest -t mschap testrechner$ passwort localhost 10 testing123
```

Als Ausgabe muss eine Access-Accept-Antwort ausgegeben werden:

```
 rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=198, length=84

 MS-CHAP-MPPE-Keys =
0x00000000000000000d5194e85da278bd6a55144941cbdc1f80000000000000000

 MS-MPPE-Encryption-Policy = 0x00000002

 MS-MPPE-Encryption-Types = 0x00000004
```

Sollte es eine Access-Reject-Antwort geben, könnte folgender Konfigurationsfehler vorliegen:

1. Fehlerhafte VLAN-Zuweisung:

```
 rad_recv: Access-Reject packet from host 127.0.0.1 port 1812, id=225, length=110

 MS-CHAP-MPPE-Keys =
0x00000000000000000d5194e85da278bd6a55144941cbdc1f80000000000000000

 MS-MPPE-Encryption-Policy = 0x00000002

 MS-MPPE-Encryption-Types = 0x00000004

 Reply-Message = "DEBUG: Not found, reject"
```

Keiner der VLAN-Filter matched. Man sollte nochmal im Log nachschauen, warum das der Fall ist. Sollte es einen speziellen LDAP-Filter geben, der erwartet wird, prüfen sie erneut die LDAP-Suche:

```
expand: %{ldap:ldap:///dc=byod,dc=univention,dc=de?cn?sub?(&(memberUid=%{User-
Name})(cn=schueler-011))} ->

 ? Evaluating
("%{ldap:ldap:///dc=byod,dc=univention,dc=de?cn?sub?(&(memberUid=%{User-
Name})(cn=schueler-011))}") -> FALSE
```

2. Internetregelprüfung schlägt fehl:

```
 rad_recv: Access-Reject packet from host 127.0.0.1 port 1812, id=44, length=38

 MS-CHAP-Error = "\000E=691 R=1"
```

Die zugewiesene Internetregel lässt kein WLAN zu (Checkbox WLAN-Aktivierung nicht ausgewählt).

Solltet es dann immer noch nicht möglich sein herauszufinden, warum die Authentifizierung nicht funktioniert, kann folgendes spezielles Login aktiviert werden:

```
ucr set freeradius/conf/auth-type/mschap/authhelper-logfile=/tmp/mschap.log
```

In dem Logfile werden anschließend folgende Dinge geloggt:

1. Die Internetregeln.

2. Status der WLAN Aktivierung in der am höchsten priorisierten Regel.

3. Ob das sambaNTPassword gelesen werden konnte.

4. Ob der Benutzer möglicherweise deaktiviert ist.

5. Ob das eingegebene Passwort falsch ist.

Herzlichen Glückwunsch, Sie haben gerade eine erfolgreiche zukunftsfähige WLAN-Konfiguration flächendeckend für all Ihre Schulen erstellt!

WLAN – Captive Portal

Um Gästen an Schulen einen temporären Zugang in das Internet zu erlauben, wird in der Regel ein Captive Portal aufgesetzt. Meist auf der Firewall installiert, ermöglicht es den Zugang mit einem Voucher-System über eine eigene WLAN-SSID und ein eigenes VLAN.

WLAN – Konfiguration für schuleigene Geräte

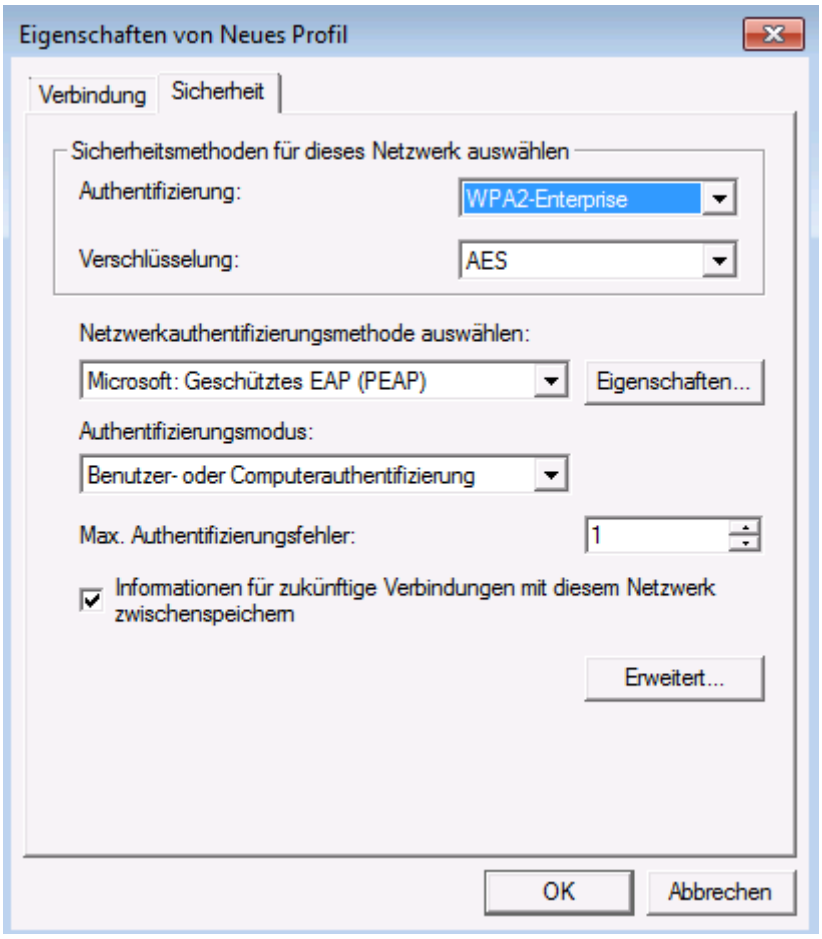
Die Konfiguration von schuleigenen Geräten ist jedes Mal eine Herausforderung. Hilfreich sind hier Management-Systeme, die den Betrieb vereinfachen. Die derzeit am häufigsten verwendeten Geräte sind nach wie vor Windows Clients und iPads. Für beide Systeme soll hier eine kurzer Hinweis gegeben werden wie diese konfiguriert werden können.

Windows Clients

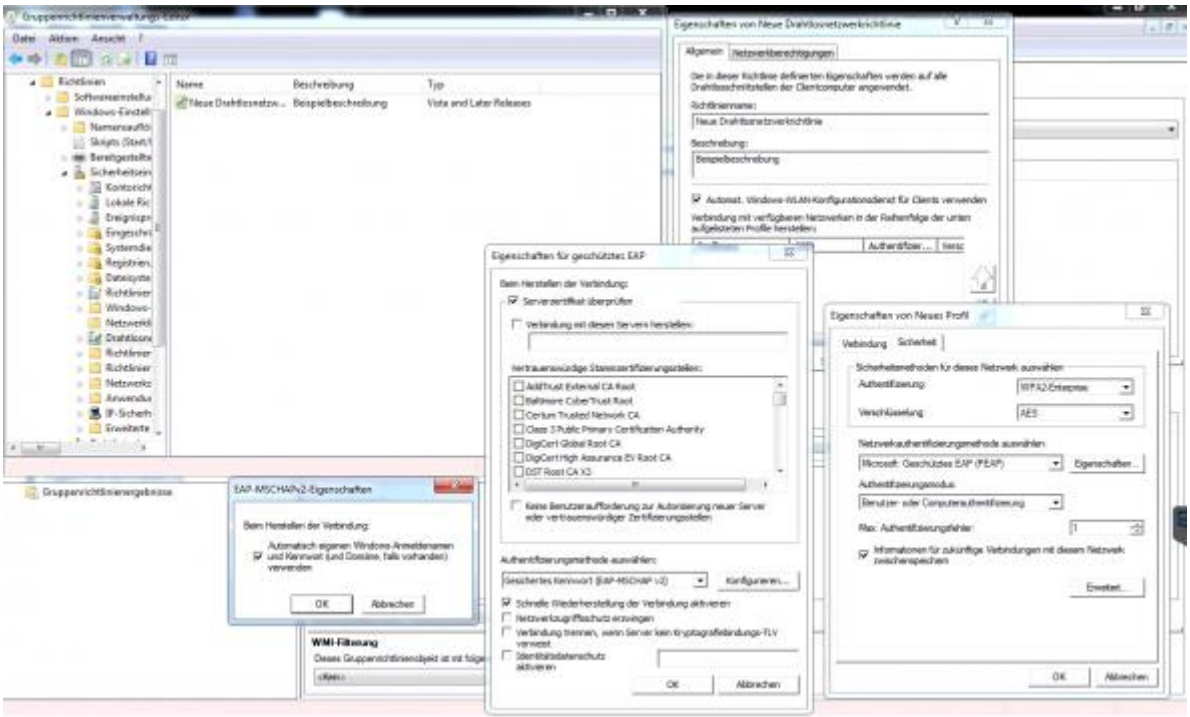
Die Erklärung für die exemplarische Einrichtung des WLAN-Zugriffs über RADIUS finden Sie im Univention Wiki:

- für Windows 7 Clients
- für Windows 10 Clients

Größere Anzahlen von Windows Clients werden im wesentlichen per Gruppenrichtlinien (GPO) verwaltet. Die WLAN-Konfiguration ebenfalls. In der Gruppenrichtlinienverwaltung erstellen Sie eine neue Gruppenrichtlinie oder bearbeiten eine bestehende . Unter Computerkonfiguration → Richtlinien → Windows-Einstellungen → Sicherheitseinstellungen → Drahtlosnetzwerkrichtlinien „Erstellen Sie eine neue Drahtlosnetzwerkverbindung für Windows Vista und neuere Versionen“. Konfigurieren Sie ein neues Profil durch „Hinzufügen…“ → Infrastruktur für alle Clients der Schulen des Schulträgers.



Screenshot: Konfigurationsfenster neues Profil



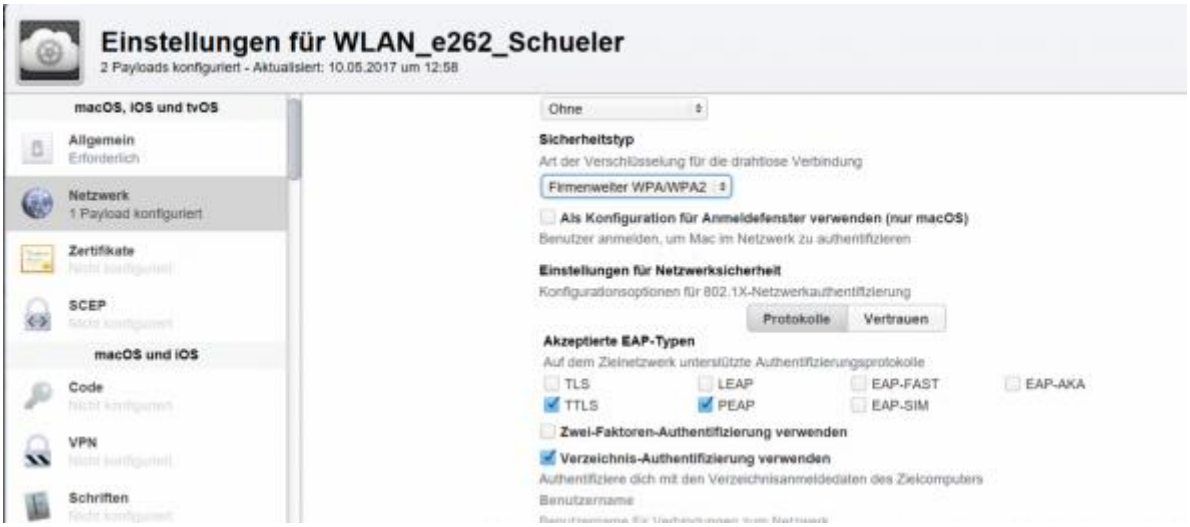
Screenshot: Windows Clients per Gruppenrichtlinien (GPO) verwaltet

Mobile-Device-Management

Mittlerweile gibt es drei Mobile-Device-Management-Systeme im Appcenter: auralis, FileWave und ZuluDesk. FileWave und ZuluDesk haben außerdem eine Verbindung zum Apple School Manager. Spätestens ab 300 iOS Geräten sollten man sich diese Mobile-Device-Management-Systeme unbedingt anschauen. Bis dahin reicht eventuell auch der Apple Profile Manager.

Apple Profile Manager

Der Apple Profile Manager ist eigentlich nur für kleinere Umgebungen gedacht. Insbesondere aber zum Start kann man durchaus darauf zurückgreifen. Eine Beispielkonfiguration:



Screenshot: Beispielkonfiguration mit Apple Profile Manager

Fazit

Das Thema WLAN und damit auch BYOD ist nach wie vor im edukativen Bereich ein großes Thema und sicherlich ein entscheidender Eckpfeiler für #digitaleBildung. Persönlich erlebe ich, dass viele Akteure gar nicht so genau wissen, wo sie anfangen sollen. Es gibt zwar einige wenige gute Leuchturmprojekte in dem Bereich. Die lassen sich aber meiner Erfahrung nach nur bedingt in der Fläche ausrollen. Außerdem sind die Anforderungen von Schulen eben doch anders als von Unternehmen.
In den Projekten bei uns im Professional Service denken wir natürlich jeweils für viele Schulen gleichzeitig und sind außerdem häufig Ansprechpartner für sachverwandte Themen aus der Netzwerktechnik. Hier greifen wir auf die Erfahrung aus verschiedensten Schulträgerprojekten zurück.

Beispieldatei „default-Datei mit „server custom { … }“-Block“ zum Download


Beispieldatei

default-Datei mit „server custom { … }“-Block

Datei-Download