

# macmon 802.1X-Integration

## 1 Probleme bei der Einführung von 802.1X

Nach dem 802.1X Standard arbeitende Netze bieten die Möglichkeit, schon am Netzwerkzugangsport eine Geräteidentifizierung vornehmen zu können, um ein regelbasiertes Zugangskontrollsystem zu errichten. Die meisten an einem Netzwerk angeschlossenen Geräte (Drucker, Telefone, Thin Clients,...) verfügen aber über keinen 802.1X-Supplikanten und können sich deshalb nicht anmelden. Viele Hersteller bieten darum spezielle Switchtypen an, die über die *MAC Authentication Bypass* -Funktion verfügen, was eine ersatzweise Anmeldung über die MAC-Adresse erlaubt. Bei vielen im Einsatz befindlichen Switch-Modellen fehlt diese Funktion allerdings.

Die Implementierung der *MAC Authentication Bypass* -Funktion ist bei einigen Switches allerdings auch mangelhaft. So warten Cisco-Switches, die über ein IOS vor 12.2(50) verfügen, immer zuerst auf eine 802.1x-Authentifizierung und fallen erst nach Ablauf eines Timeouts (Default: 3 Minuten) auf *MAC Authentication Bypass* zurück. Dies dauert unter Umständen für eine erfolgreiche DHCP-Zuweisung zu lange. Die DHCP-Anfrage erhält zwischenzeitlich ein Timeout und der IP-Protokollstack wird nicht ordnungsgemäß aufgebaut. Der Client kann so nicht auf das Netzwerk zugreifen.

Eine weitere Herausforderung bei der Einführung ist, dass eine portweise manuelle Konfiguration des 802.1x-Status für *MAC Authentication Bypass* durchgeführt werden muss, was administrativ in großen Netzen nicht zu leisten ist.

## 2 Switchport-Steuerung mit macmon

macmon kann in seiner Referenztabelle über Gruppenzugehörigkeit oder Attribute 802.1X-fähige von nicht 802.1X-fähigen Geräte unterscheiden. Auch die Leistungsmerkmale der Switches, ob sie *MAC Authentication Bypass*, 802.1X oder keines dieser beiden Sicherheitsfunktionen unterstützen, kann in macmon gepflegt, bzw. von macmon erkannt werden.

macmon übernimmt nun die Steuerung des 802.1X-Status der Switch-Ports.

Ein Port wird in den 802.1X-Modus geschaltet, wenn der Client auch 802.1X-fähig ist, andernfalls bleibt der Port im Standard-Mode, bzw. wird von macmon in diesen zurückgeschaltet. Dies erfolgt unabhängig vom jeweiligen Port, so dass 802.1X-fähige Geräte beliebig mit nicht 802.1X-fähigen Geräten getauscht werden können. Die bereits implementierten Steuerungsmöglichkeiten über 802.1X und RADIUS bleiben erhalten und können unabhängig von den macmon-Richtlinien genutzt werden. Per RADIUS oder macmon

können den Endgeräten entsprechende VLANs zugewiesen werden. Sichere 802.1X-Clients können so von anderen Devices getrennt werden.

### 3 Beispiel Szenario

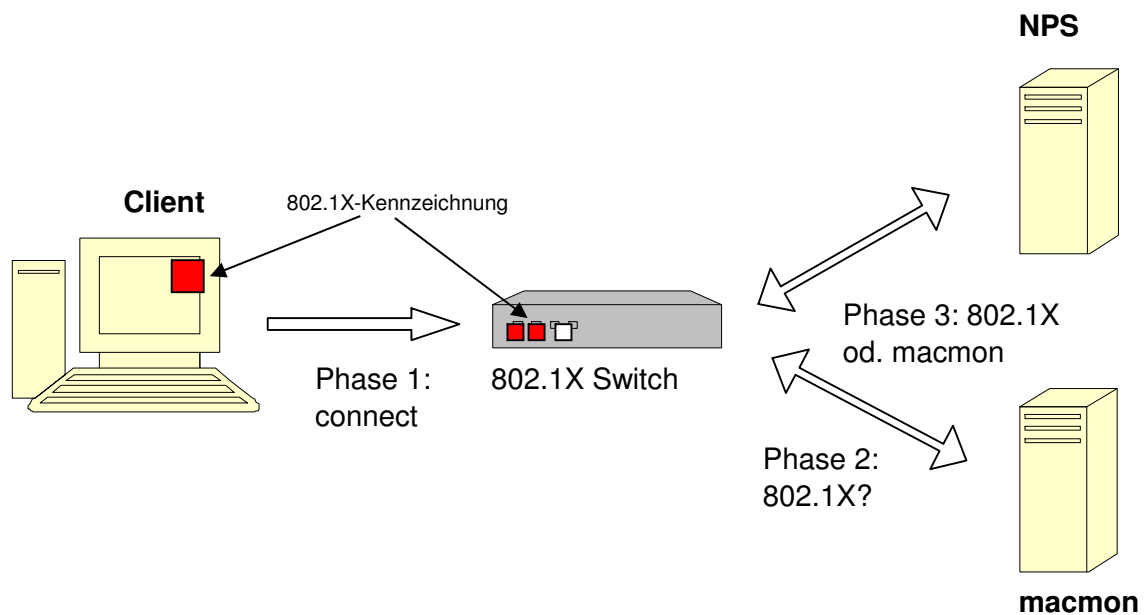
In einem Unternehmen werden 802.1X-fähige Switches (z.B. Cisco 2950) betrieben. An ihnen sind neben den PCs, Notebooks und Servern auch Drucker und Multifunktionsgeräte angeschlossen, welche nicht 802.1X fähig sind. Zur Absicherung des Systems wird auf 802.1X Authentifizierung gesetzt. Auf den Switches wird 802.1X aktiviert, die Switchports werden allerdings so konfiguriert, dass standardmäßig keine 802.1X-Authentifizierung durchgeführt wird.

Es befindet sich ein Server mit macmon incl. VLAN-Management zur Kontrolle der Switches im Netz. Das Netz wird in zwei VLANs unterteilt. Die Netze sind getrennt, das Routing zwischen den Netzen wird über eine Firewall kontrolliert. VLAN 1 ist das Entry-VLAN, mit geringen Zugriffsmöglichkeiten. Es wird für unautorisierte Clients verwendet und steht auch Gästen zur Verfügung. VLAN 2 ist das Intranet mit allen Zugriffsmöglichkeiten. VLAN 2 wird allen autorisierten Clients zugewiesen. Dies sind Clients, die sich per 802.1X authentifiziert haben und Clients, die von macmon über die MAC autorisiert wurden. Weitere Regeln zur Autorisierung von MAC-Adressen mit macmon werden hier nicht betrachtet.

Die 802.1X-Authentifizierung ist im System etabliert. In diesem Beispiel wurde mit einer Microsoft-Umgebung getestet, andere Umgebungen werden gleichermaßen unterstützt und unterscheiden sich in der macmon-Konfiguration nicht.

Für eine Microsoft-Umgebung muss eine Active Directory Domäne mit einem Domänencontroller (DC) bereit stehen. Die 802.1X-Authentifizierung über PEAP (EAP-TLS) erfordert Zertifikate. Dazu muss eine Certification Authority (CA) in der Domäne eingerichtet werden, welche die notwendigen Computerzertifikate ausstellt. Außerdem muss ein NPS-Server in der RADIUS-Rolle eingerichtet werden, der die Authentifizierung vornimmt. Die Clients müssen in die Domäne aufgenommen werden und über Windows XP SP3, Vista SP1 oder Windows 7 verfügen. Auf allen Clients ist die Netzwerkauthentifizierung zu aktivieren und einzurichten. Dazu muss der Client über ein gültiges Computerzertifikat verfügen, das von der CA ausgestellt wurde. Außerdem müssen alle Switches so konfiguriert werden, dass sie 802.1X Authentifizierung durchführen können.

Der Ablauf sieht nun wie folgt aus. Ein Client verbindet sich mit dem Switch (Phase 1). macmon registriert den Verbindungsversuch und prüft, ob der Client und der Switch 802.1X-fähig sind (Phase 2). Ist dies der Fall, wird die 802.1X-Authentifizierung am Switch aktiviert und der Client muss die 802.1X-Authentifizierung durchführen, um Netzzugang zu erhalten (Phase 3). Ist der Client nicht 802.1X-fähig, so führt macmon die MAC-Authentifizierung anhand seiner Regeln durch (Phase 3).



## 4 Beispiel-Konfiguration

### 4.1 Kennzeichnung für 802.1X

Um die Regelausführung zu steuern, müssen die Endgeräte und die Switches, oder bei Bedarf auch einzelne Interfaces, in macmon entsprechend ihrer 802.1X-Fähigkeit gekennzeichnet werden. Zur Kennzeichnung werden in unserem Beispiel Benutzerattribute verwendet. Diese müssen unter `Einstellungen -> Benutzeroberfläche` eingerichtet werden. Durch die Vergabe von Namen für die Felder `[MACGROUPS_USER1]`, `[IF_USER1]` und `[DEVICE_USER1]` werden die Attribute aktiviert. Vergeben sie eine verständliche Bezeichnung, Bsp. „DOT1X“, da diese als Spaltenüberschrift in den jeweiligen Dialogen angezeigt wird.

Alle macmon-Gruppen, die ausschließlich 802.1X fähige Geräte enthalten, werden über den Menüpunkt „Gruppeneditor“ durch den Eintrag des Wertes „802.1X“ in der Spalte „DOT1X“ gekennzeichnet.

Die Switches, bzw. im Bedarfsfall die einzelnen Interfaces müssen als 802.1X-fähig gekennzeichnet werden, um zu entscheiden, auf welchen Ports dieses Protokoll benutzt werden kann. Gehen sie auf `Netz -> Devices verwalten`, wählen Sie den entsprechenden Switch aus und tragen Sie in die Spalte „DOT1X“ „802.1X“ ein, oder, falls Sie nur einzelne Interfaces über 802.1X steuern wollen, wählen Sie `Interfaces verwalten` und tragen Sie hier bei allen relevanten Switch-Ports in die Spalte „DOT1X“ „802.1X“ ein.

Im Device Type für die Switches, welche über 802.1X gesteuert werden sollen, muss die Scan-Kategorie DOT1X aktiviert sein, damit die Ereignisvariable [IFDOT1XIFCONFIG] verfügbar ist.

Die zu steuernden Geräte sind nun klassifiziert. Zur Steuerung müssen jetzt Bedingungen, Regeln und Kommandos angelegt werden, welche die Steuerung der Ports beschreiben.

## 4.2 Bedingungen

Es wird eine Bedingung benötigt um zu entscheiden, ob die Portkontrolle auf 802.1X umgeschaltet werden soll. Dies geschieht, wenn das Endgerät in der richtigen Gruppe ist, und der Switchport 802.1X-fähig..

Bedingung für Umschaltung auf 802.1X-Steuerung

```
[MACGROUPS_USER1] ~ "802.1X" //is managed device
and
[IF_USER1] ~ "802.1X" //is a managed interface
```

## 4.3 Kommandos

Zur Steuerung der Switches sind Kommandos notwendig, die zuvor angelegt werden müssen.

Es werden drei Kommandos definiert, um 802.1X am Port ein-, auszuschalten oder um das VLAN zu setzen.

Für das Einschalten der 802.1X Kontrolle am Switch wird SNMP verwendet.

Folgendes Kommando (802.1X-enable) setzt den Port auf 802.1X-Kontrolle (auto):

```
Kommando: snmpset
Parameter: -v [DEVICE_SNMP_VERS] -c [DEVICE_WCOM]
[DEVICE_IP] 1.0.8802.1.1.1.1.2.1.1.6.[IFINDEX] i 2
```

Folgendes Kommando (802.1X-disable) setzt den Port zurück in *force\_authorized*:

```
Kommando: snmpset
Parameter: -v [DEVICE_SNMP_VERS] -c [DEVICE_WCOM]
[DEVICE_IP] 1.0.8802.1.1.1.1.2.1.1.6.[IFINDEX] i 3
```

Wenn sich das Gerät nicht über 802.1X steuern lässt, dann erfolgt eine Umschaltung in das VLAN 2 mit dem macmon vlan manager.

## 4.4 Regeln

Mit den erstellten Bedingungen und Kommandos ist man nun in der Lage Regeln zu definieren, welche die Ports wie gewünscht steuern. Regeln werden ereignisgesteuert ausgewertet. Es sind die Ereignisse `mac_online` und `interface_down` von Bedeutung.

Das Ereignis `mac_online` wird ausgelöst, wenn ein Client eine Netzwerkverbindung aufbaut.

Regel 802.1X aktivieren: Die Bedingung für die Umschaltung auf 802.1X-Steuerung trifft zu, das Kommando `802.1X enable` wird ausgeführt.

Regel MAC Bypass: Die Bedingung für die Umschaltung auf 802.1X-Steuerung trifft nicht zu, der Switchport wird per `vlan-Modul` in `VLAN 2` umgeschaltet.

Das Ereignis `interface_down` wird ausgelöst, wenn die Verbindung getrennt wird. In diesem Fall müssen die Grundeinstellungen wieder hergestellt werden.

Bei Ereignis `interface_down` und Bedingung `802.1X mit VLAN` wird Kommando `802.1X-disable` ausgeführt. Außerdem muss das `VLAN` wieder hergestellt werden. .

Bitte beachten sie, dass zur Kontrolle der nicht über 802.1X gesteuerten Ports weitere Regeln und Einstellungen notwendig sind, um `VLANs` zuzuweisen, Ports zu sperren oder Benachrichtigungen zu versenden.

## 5 Fazit

Mit Hilfe dieser `macmon`-Konfiguration sind sie in der Lage, `macmon` zur Steuerung der 802.1X-Authentifizierung ihrer Switches einzusetzen. Sie können für Geräte, die 802.1X unterstützen, diese Authentifizierungsmethode verwenden und so ein gehobenes Maß an Sicherheit etablieren. Wenn ein separates `VLAN` für Geräte eingerichtet wird, die sich nur über ihre `MAC-Adresse` authentifiziert haben, kann das Netzwerk zusätzlich gegen `MAC-Spoofing-Attacken` gehärtet werden.

Geräte, die kein 802.1X unterstützen, werden durch `macmon` kontrolliert. Die notwendiger Weise geöffneten Ports für nicht 802.1X-fähige Geräte unterliegen der `MAC-Kontrolle` durch `macmon`. Ein Angreifer hätte somit zumindest Zugriff auf alle nicht-802.1X-fähigen Geräte des Firmennetzes.

## 6 Anhang:

### 6.1 VLAN über RADIUS (Microsoft NPS) einstellen

Sie können das VLAN für 802.1X-authentifizierte Clients per RADIUS festlegen. Dazu sind folgende RADIUS-Attribute festzulegen. Der Tunnel-Typ muss auf VLAN gesetzt werden. Der Tunnel-Medium-Type muss auf 802.1X gesetzt werden und Tunnel-Private-Group-ID muss auf die ID der Ziel-VLANs gesetzt werden. Bei NPS setzen sie diese Werte in der entsprechenden Netzwerkrichtlinie unter Einstellungen.

