

# **Sicherheit in Enterprise-Netzen durch den Einsatz von 802.1X**

**von**

**Cornelius Höchel-Winter**

## 4 Produkte und Methoden: Kriterien zur Auswahl

### 4.1 Auswahl der Authentifizierungsmethoden

Bei der Wahl der EAP-Methode(n) sind im Wesentlichen die folgenden Punkte zu beachten:

- Welche Clients sollen unterstützt werden?
  - Geräte- oder Benutzerauthentifizierung?
- In welche Betriebssystem-Landschaft soll die Lösung integriert werden?
- Steht eine PKI zur Verfügung oder soll eine aufgebaut werden?
  - Falls Ja, sollen/können die Clients mit Zertifikaten ausgestattet werden oder nur die Authentifizierungsserver?
  - Falls alle oder auch nur einige Clients keine Zertifikate erhalten, gegen welche Datenbasis soll dann authentifiziert werden?
- Soll die Anbindung von Clients über Wireless LAN unterstützt werden?

#### 4.1.1 Geräte- oder Benutzerauthentifizierung

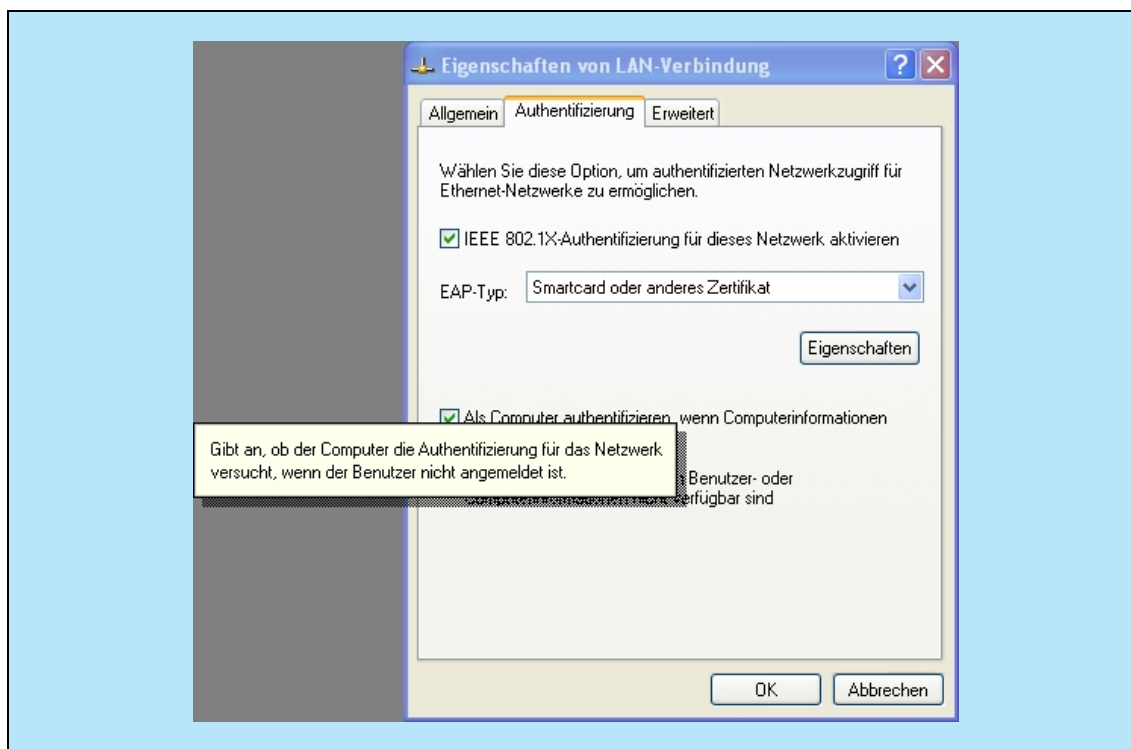


Abbildung 4.1: Aktivierung der Geräteauthentifizierung unter Windows XP

Die in Kapitel 3 vorgestellten Standards unterscheiden nicht zwischen Geräte- und Benutzerauthentifizierung. Tatsächlich ist diese Unterscheidung auch etwas akademisch, die beiden Begriffe stammen ursprünglich aus der Windows-

Welt, wo im Active Directory Benutzerkonten und Computerkonten geführt werden. Eine Authentifizierung kann hier folglich gegen ein Benutzerkonto (= Benutzerauthentifizierung) oder gegen ein Computerkonto (= Geräteauthentifizierung) erfolgen.

Der entscheidende Unterschied zwischen beiden Authentifizierungstypen ist also nicht die Frage, welcher Kontentyp genutzt wird, sondern: Erfolgt die Authentifizierung mit oder ohne Interaktion mit einem Benutzer?

Unter Geräteauthentifizierung versteht man also einen Authentifizierungsvorgang, der ohne Eingaben von Benutzerseite automatisiert abläuft. In diesem Fall müssen die benötigten Authentifizierungsdaten (Credentials) folglich auf dem System lokal vorliegen.

Hiermit stellt sich unmittelbar die Frage nach der Sicherheit

1. für die hinterlegten Credentials auf dem Gerät und
2. für das zu schützende Netzwerk.

Bei Benutzerauthentifizierungen setzt man meist auf die Komponente „Wissen“ (in der Regel ein Passwort) oder auf eine Kombination aus den Komponenten „Wissen“ und „Besitz“ (z.B. Smartcard plus PIN), an Hand derer der Benutzer identifiziert wird. Beides geht bei der Geräteauthentifizierung natürlich nicht, das Gerät identifiziert sich eben allein, Passwort oder Zertifikat sind direkt auf dem Gerät hinterlegt. Daher muss sichergestellt werden, dass diese Daten (Credentials) nicht entwendet und von anderen Systemen für einen unberechtigten Netzzugang missbraucht werden können.

Von den in Kapitel 3 vorgestellten EAP-Methoden nutzen die meisten ein Passwort zur Clientauthentifizierung und benötigen daher die Interaktion mit einem Benutzer – zumindest wenn man das Passwort nicht im Klartext auf dem Client hinterlegen möchte. Doch selbst wenn man sich dafür entscheiden würde, müssen für diese Verfahren gerätespezifische „Benutzer“-Konten mit eigenen Passwörtern angelegt und gepflegt werden.

Ausnahmen und daher besser zur Geräteauthentifizierung geeignet sind:

- EAP-TLS, hierbei werden Clientzertifikate überprüft;
- EAP-FAST, hierbei wird ein Pre-Shared Key genutzt;
- EAP-SIM und EAP-AKA, hierbei werden Daten von SIM-Karten genutzt – dies setzt jedoch voraus, dass die SIM-Karten ohne PIN aktiviert werden können.

Zur Geräteauthentifizierung ist es also (selbstverständlich) erforderlich, dass der Authentication Server das Gerät über die gewählte EAP-Methode überhaupt authentifizieren kann! Das heißt, er muss je nach EAP-Methode auch über eine geeignete Datenbasis der Systeme verfügen.

Entscheidend, ob man sich für die Benutzer- oder Geräteauthentifizierung entscheidet, ist aber zunächst die Frage, wann das einzelne System Netzwerkzugriff benötigt: Bevor oder erst nachdem sich ein Benutzer angemeldet hat. Beispiele für einen Netzwerkzugriff ohne angemeldeten Benutzer sind:

- Wake-on-LAN,
- Softwareverteilungsroutinen,
- computerbasierte Richtlinien im Windowsnetz,
- lokale Ressourcen (wie z.B. Drucker), die im Netz freigegeben sind,
- zentrale Datensicherung lokaler Ressourcen,
- Serverdienste für das Netzwerk,
- öffentliche Angebote zur anonymen Nutzung wie beispielsweise ein Besucherinformationssystem an öffentlich zugänglichen PCs.

Darüber hinaus wird man schnell feststellen, dass es eine große Menge weiterer Geräte im Netzwerk gibt, die gar keine benutzerbasierte Authentifizierung sinnvoll zulassen. Hierzu gehören

- alle Server,
- Netzwerkdrucker,
- VoIP-Hardphones,
- Erfassungsgeräte wie Scanner, Zeiterfassungsterminals,
- Überwachungsgeräte wie Kameras,
- Steuerungstechnik,
- Produktionsmaschinen
- und viele mehr.

Zusammenfassend kann man über eine Geräteauthentifizierung sagen:

- Für eine flächendeckende Sicherheitslösung kann man in der Regel auf gerätebasierende Authentifizierungsverfahren nicht verzichten.
- Zu prüfen ist dann, wie die Vorteile einer ergänzende Benutzerauthentifizierung integriert werden können (siehe hierzu Kapitel 4.1.3).
- Wünschenswert sind Geräteauthentifizierungen über EAP-TLS.

### 4.1.2 Authentifizierung auf Basis der MAC-Adresse

Falls von bestimmten Clienttypen keine 802.1X-basierende Authentifizierung unterstützt wird, müssen hierfür am Zugangspunkt/Switch Ausnahmeregelungen geschaffen werden, die letztlich Löcher in den aufgebauten Schutzwall reißen.

Als Authentifizierungsverfahren auf niedrigster Stufe bieten für diesen Fall die meisten Produkten an, auf der Basis von MAC-Adressen zu authentifizieren. Auch hierbei unterstützen die meisten Switches und Access Point neben der Definition einer lokalen Accessliste auch die Möglichkeit, die MAC-Adressen über RADIUS von einem zentralen Authentifizierungsserver überprüfen zu lassen. Damit verliert man zumindest den Vorteil der zentralen Datenbasis nicht, das Verfahren kann nahtlos in eine RADIUS-Infrastruktur zur Authentifizierung eingebettet werden und eignet sich daher insbesondere als Einstiegs- oder Übergangsvariante bei der Einführung von 802.1X.

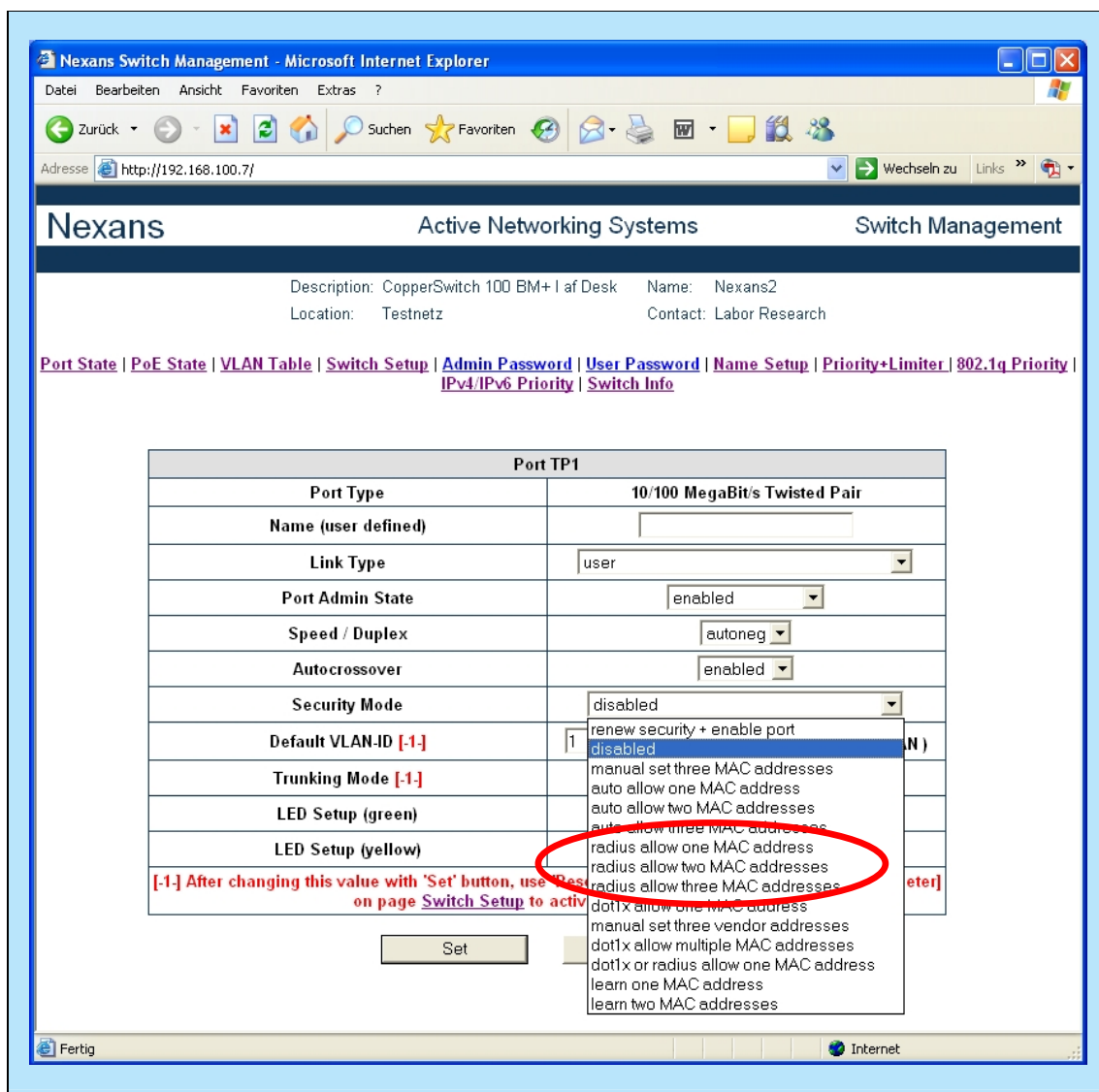


Abbildung 4.2: Authentifizierung auf Basis der MAC-Adresse

Insbesondere alle über RADIUS austauschbaren Informationen (siehe Kapitel 4.3) können vom Switch/Access Point und vom Authentifizierungsserver übermittelt und ausgewertet werden.

Offensichtlich ist jedoch das Authentifizierungskriterium „MAC-Adresse“ kein geheimes Credential und kann daher leicht für Angriffe unter der Identität eines regulären Systems genutzt werden (MAC-Address-Spoofing). Dies ist das größte Problem an einer Authentifizierung via MAC-Adresse.

Zu beachten ist daher: Eine Authentifizierung über MAC-Adressen liefert zwar ein Accounting regulärer Benutzer bzw. Geräte und kann auch zur Trennung von Benutzergruppen verwendet werden, bietet aber für das entsprechende LAN-Segment keinen weiteren Schutz vor aktiven Angriffen!

Einige Produkte unterstützen pro Port eine Art Fall-Back der Authentifizierungsverfahren:

- Als Erstes wird über EAP-Request-Identity eine 802.1X-Authentifizierung gestartet,
- wird dieser Request innerhalb eines Timeout-Intervalls nicht beantwortet, wird (über RADIUS) versucht die MAC-Adresse zu überprüfen.

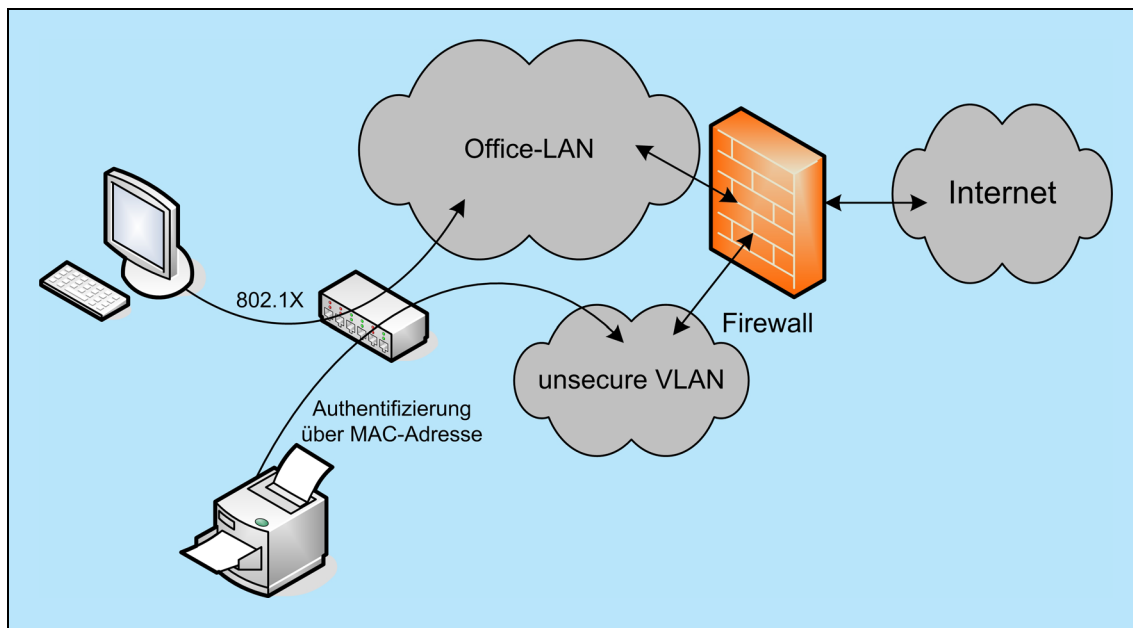
Eine solche sich automatisch zurückstufende Authentifizierung mag während einer Umstellungsphase hilfreich sein, ist aber sicherheitstechnisch zunächst nicht besser als eine MAC-Adressen-basierende Authentifizierung.

Hilfreich ist jedoch das folgende Szenario (siehe auch Abbildung 4.3): Alle über MAC-Adresse authentifizierten Geräte werden dynamisch einem separaten VLAN zugeordnet, welches höheren Sicherheitsbeschränkungen unterworfen ist und durch eine Firewall von restlichen LAN getrennt ist. Aber auch hierbei ist zu bedenken, dass damit alle Systeme in diesem VLAN untereinander nicht geschützt sind und dass es außerdem Angriffsszenarien gibt, die in der Lage sind VLAN-Grenzen zu überschreiten (VLAN-Hopping).

In jedem Fall sollte jedoch für LAN/WLAN-Segmente, in denen Wireless Clients eingesetzt werden müssen, die kein WPA oder 802.11i unterstützen und daher per MAC-Adresse authentifiziert werden, notwendigerweise ein eigenes isoliertes Netzsegment geschaffen werden, welches den gesamten Netzverkehr über eine geeignete Firewall leitet. Zu beachten ist hierbei außerdem, dass ohne WPA/802.11i auch keine sichere Verschlüsselung der übertragenen Daten gewährleistet ist!

Für Wireless LANs nach 802.11i fordert der Standard die Unterstützung dynamischer Schlüsselaustauschverfahren, wobei der PMK (siehe Kapitel 0) jedoch nicht notwendigerweise von einem EAP-Verfahren geliefert werden muss, sondern bei reduziertem Schutzbedarf auch als Pre-Shared Key fest vorgegeben werden kann. Dieses oft als WPA-PSK bezeichnete Verfahren liefert ein akzep-

ables Sicherheitsniveau, falls der Pre-Shared Key genügend komplex gewählt ist (mindestens 20 zufällige Zeichen), und kann durch die zusätzliche Überprüfung der MAC-Adressen ergänzt werden.



**Abbildung 4.3: Trennung von sicher und unsicher authentifizierten Geräten**