

Whitepaper

MAC Authentifizierung mit Microsoft IAS

Integration von Legacy-Geräten in eine 802.1X Infrastruktur

November 2006

Zusammenfassung

Die Integration von nicht-802.1X-fähigen Geräten in einer 802.1X Infrastruktur lässt sich mit der sog. MAC Authentifizierung, im Cisco-Jargon auch „MAC Authentication Bypass“ genannt, elegant realisieren. Allerdings bietet der häufig als RADIUS Server zum Einsatz kommende Microsoft IAS nur unzureichende Unterstützung zur Nutzung der MAC Authentifizierung. Selbst der Cisco-eigene RADIUS Server ACS hat hier Defizite aufzuweisen.

Der im Rahmen dieses Dokumentes betrachtete Lösungsweg zeigt auf, wie mit Hilfe einer von rt-solutions.de entwickelten IAS Erweiterung die MAC Authentifizierung trotzdem erfolgreich und an die jeweilige Infrastruktur angepasst nutzen lässt.

Inhalt

1	Das Problem.....	1
2	Die Lösung.....	3
	Referenzen	4

1 Das Problem

Zur Absicherung der internen Netzwerkzugänge (LAN, WLAN) eignet sich der Standard IEEE 802.1X [1] hervorragend. Ein Endgerät oder ein Benutzer erhält nur dann Netzwerkzugang, wenn zuvor eine Authentifizierung stattgefunden hat. Darüber hinaus erlaubt es IEEE 802.1X, Anschlüssen von authentifizierten Endgeräten zusätzliche Attribute zuzuweisen, insbesondere auch VLAN-IDs. Damit wird es möglich, ein Netzwerk dynamisch zu strukturieren und es automatisch an flexible Produktionsprozesse, z.B. in einem Industriepark [2], anzupassen.

Dies alles setzt natürlich voraus, dass die Infrastruktur IEEE 802.1X-fähig ist. Für aktuelle Switches und APs gehört diese Funktionalität inzwischen zum Standardumfang. In einer Microsoft-Umgebung hat zudem der Windows Server 2003 bereits den passenden RADIUS Server (IAS) integriert und auch die Microsoft Client-Betriebssysteme Windows 2000/XP/Vista haben die benötigten Software-Komponenten (sog. Supplicants) integriert.

Ist eine Microsoft-Umgebung mit Server 2003 bereits vorhanden, fällt die Wahl des RADIUS Server für eine 802.1X Installation in der Regel auf den Microsoft IAS, denn dieser lässt sich ohne Zusatzkosten nutzen, ist eng mit dem Active Directory integriert und bietet mit den beiden Authentifizierungsprotokollen PEAP und EAP-TLS auch eine hinreichende Flexibilität.

Jedoch tritt zwangsläufig die Frage auf, was mit Endgeräten zu tun ist, die gar kein 802.1X unterstützen. Diese Problematik ergibt sich typischerweise im LAN. Klassisches Beispiel hierfür sind Netzwerkdrucker, für die bis auf wenige Ausnahmen bis dato 802.1X ein Fremdwort ist. Aber auch Spezial- oder Altgeräte (legacy devices) sind von dieser Fragestellung betroffen. Auf den ersten Blick gibt es drei Lösungen:

a) Betroffene Geräte aktualisieren (Upgrades)

Die betroffenen Geräte könnten prinzipiell auch 802.1X-fähig gemacht werden. Dabei steht man jedoch vor dem Problem, dass häufig gar keine Möglichkeit vom Hersteller hierfür angeboten wird – und falls doch, die Upgrades recht kostenintensiv sind.

b) Für die entsprechenden LAN Ports wird kein 802.1X aktiviert

Das selektive Abschalten von 802.1X für bestimmte LAN Ports schwächt die Sicherheit deutlich ab. Es hindert niemanden daran, ein fremdes Gerät an die jeweilige Netzwerkdose zu klemmen und diese missbräuchlich zu nutzen.

c) Für die entsprechenden LAN Ports wird sog. Port Security benutzt

Es besteht bei vielen Switches die Möglichkeit, für LAN Ports bestimmte MAC Adressen vorzukonfigurieren, d.h. ein LAN Port für einen Drucker würde dessen MAC Adresse fest zugeordnet werden. Dieses Verfahren ist jedoch sehr umständlich und mit viel Verwaltungsaufwand verbunden, vor allem dann, wenn die Anzahl der betroffenen Geräte hoch ist und wenn häufig Umzüge (Geräte, Personen, Abteilungen) stattfinden.

Offensichtlich sind die o.g. „Lösungen“ nicht praktikabel. Da kommt als Ausweg ein von Cisco seit Anfang des Jahres eingeführtes Features sehr gelegen: „MAC Authentication Bypass“ (im Folgenden auch MAC Authentifizierung genannt) [3]. Das ganze funktioniert wie folgt: die LAN Ports für Endgeräte verhalten sich zunächst wie 802.1X Ports, d.h. sie erfordern eine Authentifizierung, bevor Netzwerkzugang erlaubt wird. Reagiert das angeschlossene Gerät offensichtlich nicht auf die entsprechenden Protokollanforderungen und ist für diese Ports zusätzlich die Option MAC Authentifizierung aktiviert, so führt der Switch dann alternativ im Namen des Endgerätes eine 802.1X-Authentifizierung durch. Als Identität wird dabei die MAC Adresse des Endgerätes benutzt.

Dieses Verfahren hat den Vorteil, dass keinerlei Konfigurationsunterschiede für LAN Ports der Endgeräte gemacht werden müssen. Es spielt keine Rolle, ob ein Gerät 802.1X unterstützt oder nicht. Wenn ein Endgerät 802.1X unterstützt, wird eine 802.1X Authentifizierung durchgeführt. Wenn keine 802.1X Unterstützung vorliegt, wird das Endgerät anhand seiner MAC Adresse authentifiziert. Der administrative Aufwand beim Umzug von Geräten entfällt. Natürlich bedeutet auch dieses Verfahren eine nicht unerhebliche Abschwächung der erreichten Netzwerksicherheit, denn nach wie vor gilt: mit hinreichender krimineller Energie ist es prinzipiell einfach, eine bekannte MAC-Adresse vorzutäuschen und sich auf diese Weise Netzwerkzugang zu verschaffen. Langfristig ist auf jeden Fall eine vollständige Implementierung der vollständigen 802.1X Authentifizierung anzustreben. Da die MAC-Authentifizierung aber zz. den einzig gangbaren Migrationspfad für ein größeres Netzwerk mit Legacy-Komponenten darstellt und immer noch eine erhebliche Verbesserung gegenüber dem völlig ungesicherten LAN bedeutet, ergibt sich mit diesem Verfahren eine vertretbare Lösung, um Altgeräte in eine 802.1X Infrastruktur zu integrieren.

Für die MAC Authentifizierung muss allerdings der RADIUS Server nun zusätzlich Zugriff auf eine MAC Adressdatenbank haben, deren Pflege in die sonstigen Managementprozesse eingebettet ist. Im Falle vom Microsoft IAS dient das Active Directory als entsprechende Datenbank. Damit der IAS eine MAC Authentifizierung vornehmen kann, müssen im Active Directory User-Objekte angelegt werden, für die gilt: Name der Users = MAC Adresse des Endgerätes = Passwort.

Und genau hier offenbart sich ein weiteres zu lösendes Problem: die Standard-Policies für Passwörter eines User-Objekts verweigern aus guten Gründen das Anlegen eines AD-Objektes, dessen Namen gleich dessen Passworts ist. Zwar kann diese Einstellung verändert werden, aus Sicherheitsgründen kann davon aber nur dringend abgeraten werden. Hinzu kommt, dass der IAS auf das Active Directory angewiesen ist, eine Datenhaltung der MAC Adressen in einer Datei oder einer anderen Datenbank wird nicht unterstützt.

Wie nun aber trotzdem die MAC Authentifizierung erfolgreich mit dem Microsoft IAS eingesetzt werden kann, zeigt das nächste Kapitel.

2 Die Lösung

Microsoft hat explizit vorgesehen, den IAS mit Hilfe von sog. „IAS Extension“ um weitere Funktionalität zu bereichern [4]. Und genau hier kann angesetzt werden, um das Problem der MAC Authentifizierung in den Griff zu bekommen. Eine von rt-solutions.de entwickelte Erweiterung [5] erlaubt es, die MAC Authentifizierung unter Nutzung beliebiger Datenquellen zu realisieren.

Technisch passiert folgendes: die als DLL implementierte IAS Erweiterung klinkt sich in den Authentifizierungsprozess ein, d.h. jedes RADIUS Paket wird durch die Erweiterung durchgeschleust. Wenn eine MAC Authentifizierung erkannt wird, ergreift die IAS Erweiterung die Initiative und führt die Authentifizierung des Gerätes anhand einer Datenquelle (kundenspezifisch, z.B. Textdatei) durch. Das Ergebnis der Authentifizierung wird dann dem IAS mitgeteilt. Bei Bedarf kann die IAS Erweiterung sich zusätzlich um Autorisierungsaspekte kümmern und so beispielsweise VLAN-Attribute zur Zuweisung des Gerätes in ein bestimmtes VLAN setzen.

Liegt jedoch eine „echte“ 802.1X Authentifizierung (z.B. EAP-TLS) vor, so verhält sich die IAS Erweiterung völlig transparent und greift nicht in den Authentifizierungsvorgang ein.

Etwas komplizierter wird es, wenn eine 802.1X Netzwerkinfrastruktur gemeinsam von mehreren unabhängigen Organisationen und Firmen genutzt wird. Üblicherweise kommen in diesem Fall RADIUS Proxy Server zum Einsatz, die eine Authentifizierungsanfrage anhand der Benutzer- oder Computernamens einer Organisation zuordnen und anschließend an das entsprechende Authentifizierungsserver weiterleiten. Nach erfolgreicher Authentifizierung ist es dann auch typischerweise die Aufgabe eines Proxy Servers, das richtige VLAN dem Gerät oder Benutzer zuzuweisen. Der bei einer MAC Authentifizierung gelieferte Benutzername ist jedoch die MAC Adresse eines Gerätes – allein anhand dieser Information ist eine Zuordnung zu einer Organisation nicht möglich. Aber auch dieser Fall kann mit der genannten IAS Erweiterung gelöst werden. Die IAS Erweiterung kommt einfach auf den IAS Proxy Servern zum Einsatz, d.h. die MAC Authentifizierung wird bereits auf den Proxy Servern terminiert. Dabei muss die IAS Erweiterung auf die MAC Adressdaten der jeweiligen Organisationen zurückgreifen können. Wird die zu authentifizierende MAC Adresse in einer der Adressdatenbanken gefunden, so wird dem Gerät Zugang gewährt und das der Organisation zugehörige VLAN gesetzt.

Mit Hilfe der von rt-solutions.de realisierten IAS Erweiterung lassen sich also auch Altgeräte ohne 802.1X-Unterstützung elegant in eine 802.1X Infrastruktur integrieren, ohne dabei auf die Vorzüge des Microsoft IAS zu verzichten.

Referenzen

- [1] IEEE 802.1X - Port Based Network Access Control
<http://www.ieee802.org/1/pages/802.1x.html>
- [2] IEEE 802.1x für Henkel Industriepark-LAN
http://www.rt-solutions.de/upload/Story_rt_Henkel_Final.pdf
- [3] Cisco MAC Authentication Bypass Feature
<http://tools.cisco.com/ITDIT/CFN/Dispatch?act=featdesc&task=display&featureId=6901>
- [4] Microsoft MSDN - Internet Authentication Service Extensions
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ias/ias/ias_start_page.asp
- [5] <http://www.rt-solutions.de/>