IEEE 802.1X:
Jeder will es, keiner nutzt es?!

Im Juni 2001 wurde von der IEEE der Standard 802.1X verabschiedet. Dieser wird auch als "Port based Network Access Control" bezeichnet. Grundlage bilden das Extensible Authentication Protocol (EAP) nach RFC 3748 und der Remote Authentication Dial-in User Service (RADIUS) gemäß RFC 2865 (2868/3575). Über IEEE 802.1X ist eine Authentifizierung eines Geräts bzw. Nutzers direkt am Netzzugang möglich. Die Idee ist, dass erst nach einer erfolgreichen Authentifizierung die Verbindung auf Layer 2 freigeschaltet wird und andernfalls die Kommunikation blockiert wird.

Das Modell von 802.1X sieht dabei verschiedene Rollen der beteiligten Netzelemente vor:

- Der **Supplicant** ist eine Software-Komponente im Client-System, welche einen Netzwerkzugang anfordert.

- Der **Authenticator** ist das Gerät, welches den Netzwerkzugang sperrt oder frei gibt und eine Schnittstelle für die Authentifizierung anbietet. Normalerweise wird die Rolle des Authenticators von einem Access Point oder Access Switch übernommen.

- Der **Authentication Server** ist das Gerät, welches den eigentlichen Authentifizierungsdienst bereitstellt. Der Authentication Server ist typischerweise ein RADIUS-Server.

IEEE 802.1X wird von nahezu jedem Hersteller von Switches und RADIUS-Servern unterstützt. Auf Client-Seite sind die meisten modernen Betriebssysteme von Windows XP bis zu Linux kompatibel. Inzwischen wird sogar eine Palette von Mehrwert-Diensten, die auf IEEE 802.1X basieren, von den Herstellern von Sicherheitslösungen angeboten.

Im WLAN nach IEEE 802.11 kommt man inzwischen an IEEE 802.1X nicht mehr vorbei. IEEE 802.1X wird in den relevanten Spezifikationen zur WLAN-Sicherheit (WPA, WPA2 bzw. IEEE 802.11i) für die Authentifizierung der WLAN-Clients und für das Schlüsselmanagement genutzt.

Leider führt IEEE 802.1X im Bereich der kabelbasierten LAN ein Schattendasein und ist in der Praxis (zumindest für größere LAN) noch kaum zu finden. Dies ist umso erstaunlicher, da die Anforderung eines sicheren Zugangs genauso für das kabelbasierte LAN gilt und es derzeit keine Alternative zu IEEE 802.1X gibt.

Der Grund für die Zurückhaltung der LAN-Gemeinde liegt unter anderem in folgenden Problemen:

- Für die noch weit verbreiteten Versionen Windows 2000, Windows NT und andere ältere Betriebsysteme gibt es massive technische Probleme bei der Unterstützung von IEEE 802.1X. Für diverse Systeme ist gar kein Supplicant verfügbar (z.B. DOS PCs und diverse Kleingeräte, wie Drucker, Kameras und Barcode Scanner oder auch die Controller in der Industrieautomatisierung). Diese Situation besteht nicht nur für ältere Systeme, wie die (fast immer) fehlende Unterstützung von IEEE 802.1X bei VoIP-Telefonen zeigt.

- Die Implementierung des in Windows XP integrierten Supplicants weist Schwächen für das kabelbasierte LAN auf. Eine Verteilung der Konfiguration (speziell der Parameter für die Authentifizierungsmethode) per Group Policy Object (GPO) ist im Gegensatz zu WLAN nicht ohne weiteres möglich. Eine manuelle Konfiguration kommt ab einer gewissen Anzahl von Clients jedoch nicht in Frage.

- Der Standard geht für kabelbasierte LAN von einem Client pro Netzwerk-Port aus. Werden an einem Port eines Authenticators per Hub oder Switch, der IEEE 802.1X nicht unterstützt, mehrere Clients angebunden, fühlt sich der Standard IEEE 802.1X nicht mehr zuständig. Diese Situation tritt auch beim Einsatz von VoIP-Telefonen auf, die über einen integrierten Switch den Anschluss eines Endgeräts am Telefon gestatten. In Konsequenz muss zurzeit jeder Hersteller an dieser Stelle eine eigene Lösung suchen. Die Palette rangiert dabei von der simultanen Authentifizierung mehrerer Supplicants an einem Port bis hin zu fragwürdigen Lösungen, bei denen einem Stellvertreterprinzip folgend ein Client sich per IEEE 802.1X authentifiziert und über den so freigeschalteten Port jeder andere Client kommunizieren kann.

- Andere Themen, wie Wake-on-LAN oder die Anbindung über Medienkonverter, werden ebenfalls nicht oder nur ungenügend im Standard IEEE 802.1X berücksichtigt. Hier greifen im Moment nur herstellerspezifische Lösungen.

Trotz dieser Probleme empfehlen wir, den ersten Schritt in Richtung eines sicheren LAN-Zugangs jetzt zu tun und nicht auf den nächsten internen Sicherheitsvorfall zu warten. Die langfristige Strategie zur Absicherung des lokalen Netzzugangs geht in Richtung IEEE 802.1X. Die ausschließliche Authentifizierung über MAC-Adressen bietet hier jedenfalls keine Alternative.

Statt einen flächendeckenden Einsatz von IEEE 802.1X auf die lange Bank zu schieben, sollte darüber nachgedacht werden kurzfristig zumindest einen punktuellen Einsatz von IEEE 802.1X zu realisieren. Der Schwerpunkt sollte dabei auf die Schaffung der Infrastruktur für die Authentifizierung gelegt werden (d.h. Aufbau und Betrieb der RADIUS-Server sowie - je nach Authentifizierungsmethode - einer Public Key Infrastructure, PKI). Weiterhin ist die Integration der Authentifizierungsfunktion in das übergeordnete Netzmanagement für Konfiguration und Fehlersuche zwingend erforderlich.

Kernelement der Migration für einen flächendeckenden Einsatz von IEEE 802.1X ist die Unterstützung eines Mischbetriebs zwischen Geräten, die IEEE 802.1X unter-

stützen und solchen, die dazu (noch) nicht in der Lage sind. Im Netz müssen damit zwei Nutzergruppen mit einem unterschiedlichen Sicherheitsniveau voneinander getrennt werden, damit ein Gewinn an Sicherheit des Gesamtsystems entsteht. Diese Trennung kann physikalisch durch Aufschalten der Nutzergruppen an verschiedenen Switches geschehen. Alternativ kann eine logische Trennung am Switch Port durch eine dynamische VLAN-Zuordnung im Rahmen der Authentifizierung per IEEE 802.1X über ein spezielles RADIUS-Attribut durchgeführt werden.

Glaubt man den Ausrüstern geht der Trend zu IEEE-802.1X-basierenden Mehrwertdiensten, die es beispielsweise gestatten, dem Client in Abhängigkeit der Rechnerkonfiguration einen Zugang zum Netz zu gewähren und sogar ein nutzerspezifisches Regelwerk auf einen Netzwerk-Port zu laden. Die sinnvolle Nutzung derartiger Dienste setzt jedoch eine flächendeckende und stabile Implementierung von IEEE 802.1X voraus. Die Umsetzung solcher Mehrwertdienste sollte daher schrittweise angegangen werden. Wichtig ist es zunächst die notwendigen Grundlagen zu schaffen und vor allem auch die nicht 802.1X-fähigen Endgeräte in geeigneter Weise zu unterstützen.

Um die Vision von einer breiten Interoperabilität dieser flexiblen und sicheren Authentifizierungsmethode in unseren Netzwerken wahr werden zu lassen, ist natürlich auch der Anwender gefragt. Durch die mit IEEE 802.1X verfügbaren standardisierten Technologien kann bereits heute die Sicherheit im LAN signifikant erhöht werden. Der Nutzer muss sich nur trauen, sie auch produktiv einzusetzen. Nichts ist hier besser geeignet, realen "Leidensdruck" für die Hersteller der diversen Endgeräte und Netzelemente zu erzeugen, als die in der Praxis existierende Anwendung.

Glossar:

IEEE	Institute of Electrical and Electronics Engineers (www.ieee.org)
LAN	Local Area Network
MAC	Media Access Control
RFC	Request for Comments
VoIP	Voice over IP
VLAN	Virtual LAN
WiFI	Wireless Fidelity (www.wi-fi.org)
WLAN	Wireless LAN
WPA	WiFI Protected Access

Autoren: Arbeitskreis IT-Security der BGNW