https://www.elektronik-kompendium.de/sites/net/1409281.htm

IEEE 802.1x / RADIUS

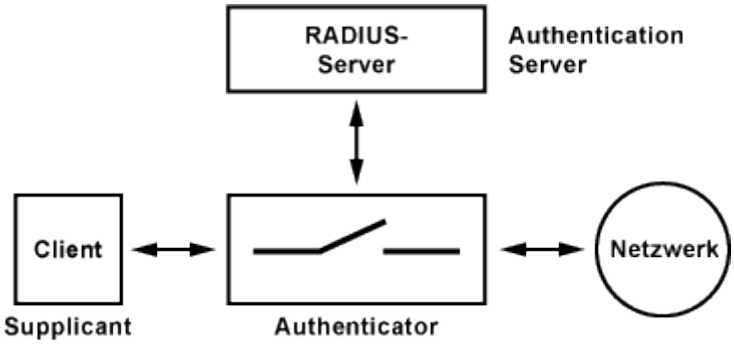
IEEE 802.1x ist ein sicheres Authentifizierungsverfahren für Zugangskontrollen in lokalen Netzwerken (LAN). Im Zusammenhang mit IEEE 802.1x werden auch häufig EAP und RADIUS genannt.
Das Protokoll EAP (Extensible Authentication Protocol), das ursprünglich als Erweiterung für PPP-Verbindungen entwickelt wurde, ist der Kern von IEEE 802.1x. IEEE 802.1x beschreibt die Einbettung von EAP-Datagrammen in Ethernet-Frames. Das ermöglicht den Austausch von Authentifizierungsnachrichten auf der Schicht 2 des OSI-Schichtenmodells.
EAP beschreibt ein einfaches Frage-Antwort-Verfahren, bei dem die Authentifizierungsdaten vom Benutzer zum Authentifizierungs-Server und dessen Antworten ausgetauscht werden.
RADIUS kann bei der Anbindung einer zentralen Benutzerverwaltung eine wichtige Rolle spielen. Aber, IEEE 802.1x schreibt keinen RADIUS-Server vor. Doch in der Regel wird beim Einsatz einer Zugangskontrolle mit IEEE 802.1x auch ein RADIUS-Server eingesetzt.

Im Zusammenhang mit WLAN wird die Authentifizierungsmethode IEEE 802.1x auch als WPA2-Enterprise, WPA2-1x oder WPA2/802.1x bezeichnet.

Funktionen von IEEE 802.1x

- Zugangskontrolle
- Authentifizierung, Autorisierung und Accounting (AAA) [1)]
- Bandbreitenzuweisung (QoS)
- Single Sign-on (SSO)

Wie funktioniert IEEE 802.1x?



Bestandteil eines Authentifizierungsverfahrens wie IEEE 802.1x ist der Supplicant (Antragsteller), der Authenticator (Beglaubigter) und ein Authentication Server, der den Antrag des Supplicant überprüft und seine Entscheidung dem Authenticator mitteilt. Der Authenticator schaltet den Zugang zum Netzwerk für den Supplicant frei oder verweigert ihn.

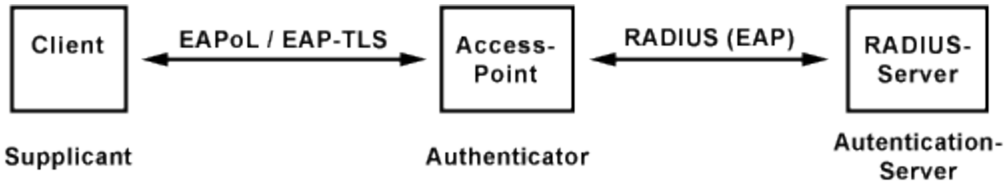
- Authenticator (Beglaubigter/Unterhändler): WLAN-Access-Point oder Switch mit IEEE 802.1x
- Authentication Server: RADIUS-Server, LDAP-Gateway/-Server, WLAN-Access-Point
- Supplicant (Antragsteller): WLAN-Client, LAN-Station

Anmeldungen vom Supplicant (Client) werden vom Authenticator zuerst an den Authentication Server weitergeleitet. Der entscheidet, ob der Supplicant Zugang bekommt. In Abhängigkeit einer erfolgreichen Authentifizierung wird der Zugang zum Netzwerk über einen bestimmten Port freigeschaltet. Wegen dem Bezug auf einen Port wird IEEE 802.1x auch als "Port-Based Network Access Control" bezeichnet.
Für IEEE 802.1x kann ein Port eine Buchse an einem Switch oder eine logische Assoziation sein. Denkbar ist hier die Zugangsmöglichkeit zum Netzwerk für einen WLAN-Client an einem WLAN-Access-Point. Mit IEEE 802.1x/EAP wird dem WLAN-Client zu Beginn einer Sitzung die dafür gültigen WPA2-Schlüssel mitgeteilt.

Wichtig bei WLAN, der WLAN-Access-Point muss auf WPA2-Enterprise eingestellt sein. Dabei hinterlegt man die IP-Adresse des RADIUS-Servers und ein Passwort, mit dem der RADIUS-Server und der WLAN-Access-Point ihre Kommunikation verschlüsseln und sichern.

Prinzipiell kann ein RADIUS-Server auch zur Verwaltung von Zugangsdaten dienen. Es gibt Architekturen bei denen der RADIUS-Server die Benutzer-Zugangsdaten nicht verwaltet, sondern zum Beispiel ein LDAP-Server (Verzeichnisdienst). In diesem Fall leitet der RADIUS-Server die Authentifizierung an den LDAP-Server weiter.

EAP - Extensible Authentication Protocol

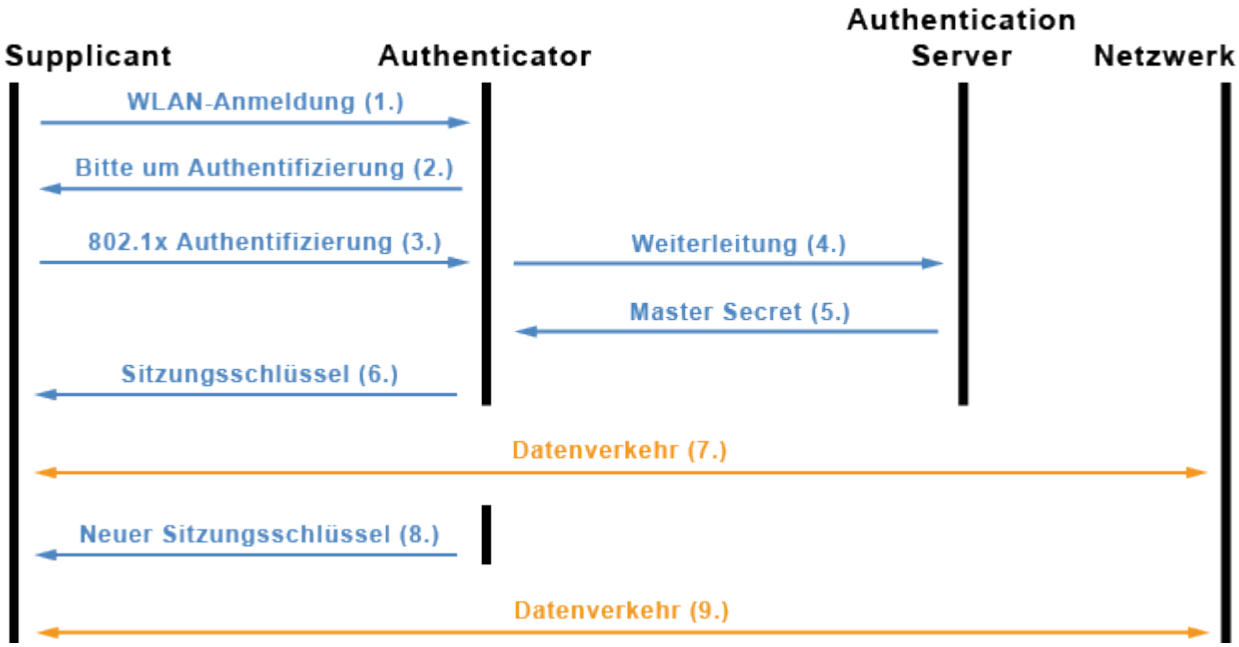


Die Kommunikation zwischen Supplicant und Authenticator erfolgt über das Extensible Authentication Protocol over LAN (EAPoL). Die Kommunikation zwischen Authenticator und Authentication Server erfolgt über in RADIUS-Paketen gekapselte EAP-Pakete.

- EAP - Extensible Authentication Protocol

Beispiel für die Anwendung von IEEE 802.1x, EAP und RADIUS

Beim Zugriff auf ein lokales Netzwerk eines Unternehmens über WLAN reicht die einfache Authentifizierung über ein gemeinsames Passwort (WPA2-PSK) nicht aus. Wenn das Passwort die Runde macht, dann ist das WLAN praktisch offen.
Mit RADIUS werden serverseitig Passwörter zugeteilt, was dem Administrator Arbeit erspart und für die Nutzer vergleichsweise einfach ist. In dieser Konstellation kommt WPA2-Enterprise zum Einsatz, bei dem die WLAN-Basisstation die Zugriffe der WLAN-Clients über das Protokoll IEEE 802.1x mit einem RADIUS-Server aushandeln.
Ein RADIUS-Server ist nicht immer zwingend erforderlich. Manche WLAN-Router enthalten bereits einen RADIUS-Server, der für kleine Netzwerke eine Alternative ist.



1. Zuerst meldet sich der WLAN-Client (Supplicant) am WLAN-Access-Point (Authenticator) an. Beide Geräte sind entsprechend auf WPA2-Enterprise konfiguriert.
2. Der Access-Point (Authenticator) fordert den Client (Supplicant) zur Authentifizierung auf. In der Regel folgt hier die Eingabe von Benutzername und Passwort durch den Nutzer.
3. Der Client (Supplicant) authentisiert sich nach IEEE 802.1x.
4. Der Access-Point (Authenticator) leitet die Authentifizierung an den RADIUS-Server (Authentication Server) weiter.
5. Bei erfolgreicher Authentifizierung gibt der RADIUS-Server das Master Secret zurück.
6. Der Access-Point generiert den Sitzungsschlüssel und teilt diesen dem Client mit.
7. Durch den Sitzungsschlüssel bekommt der Client Zugriff auf das Netzwerk.
8. In regelmäßigen Abständen bekommt der Client einen neuen Sitzungsschlüssel mitgeteilt.
9. Damit ist weiterhin der Zugriff auf das Netzwerk durch den Client möglich.

RADIUS - Remote Authentication Dial In User Service

Innerhalb eines großen Netzwerks findet die Verwaltung und Speicherung von Benutzerdaten an einer zentralen Stelle statt. Diese Daten dienen auch zur Authentifizierung von Benutzern, die sich am Netzwerk anmelden.
Kommt es zu einem Zugriff von außen auf das Netzwerk wird eine RAS- oder VPN-Verbindung hergestellt. Über diese Verbindung muss der Benutzer authentifiziert werden, bevor er Zugriff auf das Netzwerk bekommt.
Das Bindeglied zwischen der zentralen Benutzerverwaltung und dem RAS ist der RADIUS. Obwohl IEEE 802.1x keinen RADIUS-Server vorschreibt, sind die meisten Authenticatoren in der Praxis RADIUS-Clients. Das RADIUS-Protokoll übernimmt die Authentifizierung und Verschlüsselung, sowie das Accounting. Vom RADIUS-Server wird der Anfang und das Ende der Benutzung einer Leistung protokolliert und kann zu Abrechnungszwecken herangezogen werden.

Radius kennt drei Pakettypen, deren Namen so lauten, wie ihre Funktion:

- Access-Request (Bitte um Freigabe des Zugriffs)
- Access-Accept (Annahme für die Freigabe des Zugriffs)
- Access-Reject (Ablehnung der Freigabe)

Die RADIUS-Nachrichten werden auf IP-Ebene mit UDP-Paketen versendet. Die Informationen stecken in Attribute-Value Pairs (AVP).

Konfiguration: Switch und Access Point

Beim Switch und Access Point beschränkt sich die Konfiguration auf den Eintrag der IP-Adresse des RADIUS-Servers, sowie ein gemeinsames Passwort (Key) mit dem Switch bzw. Access Point und Server die Kommunikation verschlüsseln. Anschließend müssen im Switch nur noch die betreffenden Ports gekennzeichnet werden, für die die Authentifizierung gilt.
Wenn ein Netzwerk auf diese Weise gesichert ist, muss man dafür sorgen, dass eventuell ungeschützte Ports unzugänglich gemacht sind. Zum Beispiel sollte der Netzwerkschrank oder Netzwerkraum abgeschlossen sein.

Hinweis: IEEE 802.1x geht von einem Host bzw. einem User pro Port aus. Es kann sich also immer nur ein User authentfizieren. Andere User bleiben ausgesperrt. Ausnahme, wenn Multi-802.1x konfigurierbar ist.

MAC-based Authentication

Wenn man eine IEEE-802.1x-Authentifizierung im Netzwerk betreibt hat man häufig das Problem, dass es Netzwerk-Geräte gibt, die keine IEEE-802.1x-Unterstützung mitbringen. Zum Beispiel Drucker, Webcams oder VoIP-Telefone. In so einem Fall benötigt man eine Alternative für IEEE 802.1x, um auch diese Hosts zu authentifizieren. Dazu nimmt der Switch die MAC-Adresse des Hosts als Benutzername und Passwort in hexadezimaler Schreibweise für die Authentifizierung mit dem RADIUS-Server.
Aber, das hat einen schwerwiegenden Nachteil. Die MAC-Adresse kann ein Angreifer leicht übernehmen. Dazu muss der Angreifer nur die MAC-Adresse eines entsprechenden Druckers, Telefons oder eines anderen Geräts ausfindig machen. Häufig stehen die MAC-Adresse auf Typenschildern.
Ein solcher Angriff ist natürlich mit etwas Aufwand verbunden. MAC-based Authentication schützt also nur vor versehentlichen Verbindungsversuchen und unbedarften Personen.

Multi-802.1x

Normalerweise funktioniert die Authentifizierung mit IEEE 802.1x nur einmal pro Ethernet-Port (Switch). Mit Multi-802.1x kann ein Switch an einem Port auch mehrere Hosts authentifizieren. Beispielsweise, wenn an einem Port ein weiterer Switch hängt, der kein IEEE 802.1x beherrscht.
Hinweis: Damit IEEE 802.1x über mehrere Switche hinweg funktioniert, muss jeder Switch EAPOL-Frames durchlassen. Dieses Leistungsmerkmal ist nicht selbstverständlich.

Troubleshooting

- Die meisten Probleme bei IEEE 802.1x entstehen durch Zertifikatsfehler. Ein typisches Beispiel sind selbstausgestellte Zertifikate für den RADIUS-Server, die nicht alle Clients, insbesondere Smartphones, annehmen. Hier muss man zuerst das passende Root-Zertifikat auf den Clients installieren.
- Bei einer Authentifizierung mit EAP-TLS muss sich nicht nur der RADIUS-Server mit einem Zertifikat ausweisen, sondern auch der Client. Hier muss zuerst das Nutzer-Zertifikat ausgestellt und auf dem Client installiert werden.

Wie sicher ist RADIUS?

Die per RADIUS verwendeten Zugangsdaten (Benutzername und Passwort) sind normalerweise nicht sicherer als zum Beispiel ein WLAN-WPA2-Passwort. Eine höhere Sicherheit erreicht man nur durch den Einsatz zusätzlicher Zertifikate über EAP-TLS. Hierbei identifizieren sich RADIUS-Server und Client gegenseitig. Der dafür notwendige Einrichtungsaufwand sollte nicht unterschätzt werden. Selbst große Unternehmen betreiben diesen Aufwand nicht.

1) AAA

Authentifizierung / Authentication

Authentifizierung bedeutet, die Identität zu überprüfen. Zum Beispiel mit Benutzername und Passwort. Knackpunkt bei jeder Authentifizierung ist die Übertragung von Benutzername und Passwort. Erfolgt sie unverschlüsselt, dann ist es möglich, dass ein Angreifer beides ausspäht und für die eigene Authentifizierung missbraucht.

Autorisierung / Authorization

Bei der Autorisierung stellt man fest, ob ein bestimmter Benutzer einen bestimmten Dienst nutzen darf. Nur weil sich der Benutzer authentifiziert hat bedeutet das nicht, dass er auch berechtigt ist einen bestimmten Dienst zu benutzen. Wenn hinter einer Authentifizierung mehrere Dienste angeboten werden, dann auch die Berechtigungen zu prüfen, wenn nicht alles pauschal freigegeben sein soll.

Accounting

Beim Accounting geht es darum, die Nutzung eines Dienstes durch einen Benutzer festzuhalten und zu dokumentieren. Später kann die Nutzung zum Beispiel abgerechnet werden. Es ist aber auch möglich, für Service-Fälle festzustellen, was der Benutzer gemacht hat, um Fehler aufzuspüren.

Single Sign-on

(SSO, mitunter als „Einmalanmeldung“ übersetzt) bedeutet, dass ein Benutzer nach einer einmaligen Authentifizierung an einem Arbeitsplatz auf alle Rechner und Dienste, für die er lokal berechtigt (autorisiert) ist, am selben Arbeitsplatz zugreifen kann, ohne sich jedes Mal neu anmelden zu müssen. Wechselt der Benutzer den Arbeitsplatz, wird die Authentifizierung, wie auch die lokale Autorisierung, hinfällig.