WLAN-Authentifizierung

IEEE 802.1X

> 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.

Der Standard definiert drei grundlegende Funktionskomponenten. Diese sind:

1. der Antragsteller (Supplicant): zum Beispiel ein Rechner in einem LAN oder WLAN
2. der Unterhändler (Authenticator): zum Beispiel ein LAN-Switch oder WLAN-Accesspoint
3. der Authentifizierungsserver (Authentication Server): zum Beispiel ein RADIUS-Server

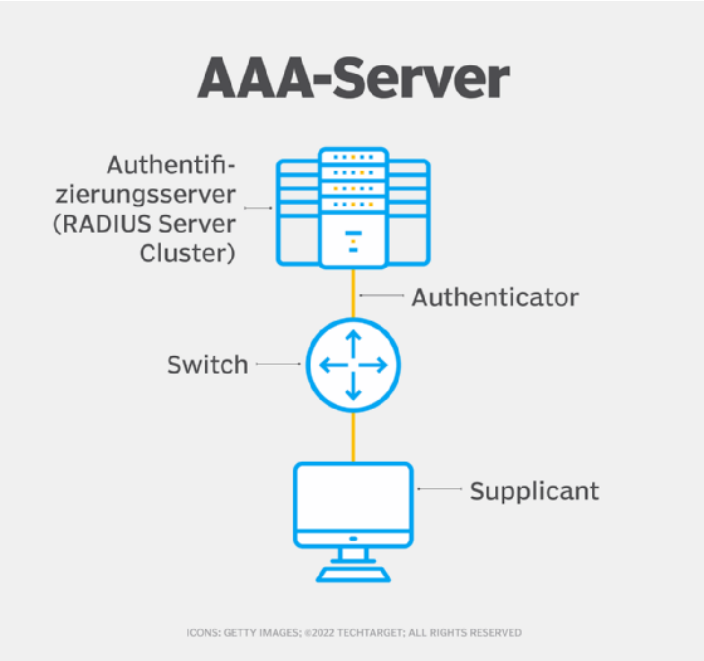
Ein Client, der Zugang zu einem LAN oder WLAN benötigt, wendet sich zunächst an den Unterhändler. Er sendet seine Anmeldedaten an einen Authenticator (zum Beispiel Switch oder WLAN-Accesspoint). Der Informationsaustausch findet per Extensible Authentication Protocol (**EAP**) statt. Der Authenticator nimmt die Anfrage entgegen und leitet die Anmeldeinformationen an den Authentication Server (zum Beispiel einen separaten **RADIUS**-Server) weiter. Der Authentication Server ist für die Benutzerverwaltung und -authentifizierung zuständig. Er prüft die erhaltenen Anmeldeinformationen und teilt das Ergebnis dem Authenticator mit. Dieser schaltet abhängig von der Prüfung der Anmeldedaten den logischen oder physischen Zugang zum lokalen Netzwerk (zum Beispiel einen Switch-Port) frei oder verweigert den Zugang.

Funktionen von .1x

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

AAA-Server (Authentifizierung, Autorisierung und Accounting)

> „Authentication Authorization Accounting“, kurz AAA, steht für ein Sicherheitskonzept in dem die drei Hauptaufgaben Authentifizierung, Autorisierung und Accounting zusammengefasst sind. Mit AAA kann man die Zugangskontrolle in einem Netzwerk organisieren.



Created 2022-11-03 17:09:29 UTC by Joshua Lieder
Updated 2022-11-04 07:57:30 UTC by Joshua Lieder