LANCOM SYSTEMS

Whitepaper

Switch Security mit IEEE 802.1X

Switches sind eine wichtige Sicherheitskomponente in Netzwerken, immerhin regeln sie den Verkehr für jegliche interne Datenkommunikation. Das Netzwerk wird nach außen von Firewalls und VPN Gateways geschützt, allerdings wird die interne Sicherheit des Netzwerkes oft vernachlässigt. Diese Vernachlässigung erlaubt Angriffe aus dem internen Netzwerk. Professionelle managed Switches sind mit umfangreichen Sicherheitsfunktionen ausgestattet und unterstützen dabei, die Sicherheitsanforderungen an das Netzwerk einzuhalten. Dieses Whitepaper gibt einen Einblick, wie Switches mit Hilfe des Standards IEEE 802.1X zur Sicherheit im LAN beitragen können.

Dieses Paper ist Teil der **Themenreihe „Switching-Lösungen“**.
Erfahren Sie mit Klick auf die Icons, welche weiteren Informationen es von LANCOM dazu gibt:

1	2	3	4	5	6
Grundlagen Two-Tier- & Three-Tier-Switch-Architekturen	**Grundlagen** Switch Security mit IEEE 802.1X	**Design Guide** Redundanz-konzepte für Switch-Netzwerke	**Setup Guide** VPC-Konfiguration mit LANCOM Switches	**Setup Guide** Stacking mit LANCOM Switches	**Setup Guide** Konfigurations-optionen LANCOM XS-6128QF

Die sichere Zugriffskontrolle

Der Standard IEEE 802.1X wurde entwickelt, um Zugangsrechte für Netzwerke zu verwalten. Er leistet die Vorarbeit für die eigentliche Authentifizierung am Netzwerk. Die grundlegenden Voraussetzungen sind das Vorhandensein eines managebaren „intelligenten“ Netzwerk-Switches sowie eines RADIUS-Servers zur Authentifizierung.

IEEE 802.1X – Vier Methoden der Zugriffskontrolle

Für eine sichere Zugriffskontrolle ergeben sich mehrere Möglichkeiten, IEEE 802.1X effektiv zu nutzen, um bestmögliche Sicherheit zu erreichen. Im Folgenden werden die vier Verfahren (Port-based, Single, Multi und MAC-based) erklärt und ihre jeweiligen Einsatzszenarien aufgezeigt.

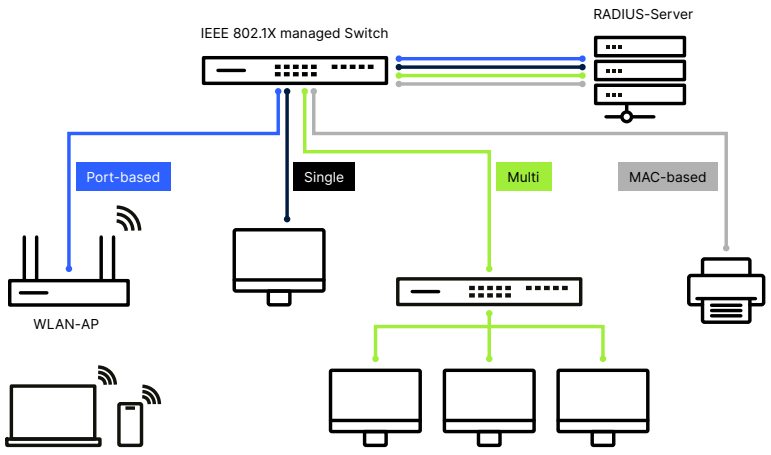

Abbildung 1:
IEEE 802.1X – Vier Methoden der Zugriffskontrolle im Überblick

1) Port-based IEEE 802.1X

Port-based IEEE 802.1X reguliert die Authentifizierung der Clients am Port des Switches durch das Verifizieren von Zertifikaten oder Zugangsdaten zu einem RADIUS-Server. Nach erfolgreicher Authentifizierung bleibt der Port permanent geöffnet für den Netzwerkzugriff. Der Vorteil ist, dass nach der erfolgreichen Authentifizierung, der Port für den Netzwerkzugriff des authentifizierten Geräts ständig zugänglich bleibt und auch weitere, am authentifizierten Gerät angeschlossene Clients, Netzwerkzugriff erhalten.

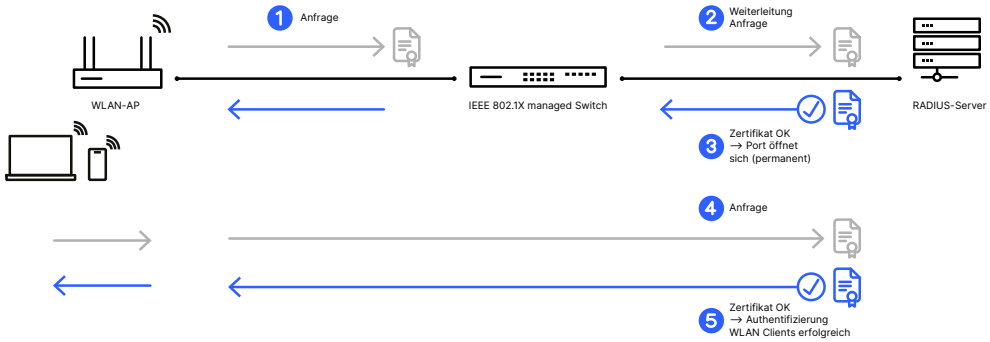

Abbildung 2:
Port-based IEEE 802.1X

Beispielszenario

Ein Access Point ist mit einem Switch-Port verbunden und benutzt Zertifikate und/oder Zugangsdaten zu einem RADIUS-Server und erhält Netzwerkzugriff. Ist der Access Point einmal authentifiziert, wird der entsprechende Switch-Port freigeschaltet und alle WLAN-Geräte, die sich mit dem Access Point verbinden (Laptops, Smartphones, Tablets), erhalten darüber auch Netzwerkzugriff.

2) Single IEEE 802.1X

Durch die Nutzung von Single IEEE 802.1X authentifiziert sich ein bestimmter Client an einem Switch-Port durch die Validierung eines Zertifikates und/oder Zugangsdaten an einem RADIUS-Server. Dieses Verfahren stellt sicher, dass ausschließlich das authentifizierte Gerät einen Netzwerkzugriff durch den Switch erhält.

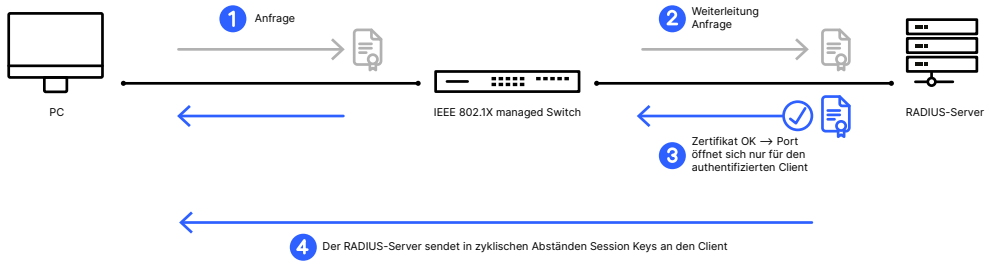

Abbildung 3:
Single IEEE 802.1X

Beispielszenario

Ein Computer wird mit einem Switch-Port verbunden und benutzt ein Zertifikat und/oder Zugangsdaten für die Authentifizierung an einem RADIUS-Server. Ist der Computer einmal erfolgreich angemeldet, sendet der RADIUS-Server regelmäßig geheime Schlüssel, um dieses bestimmte Gerät immer wieder zu authentifizieren.

3) Multi IEEE 802.1X

Wurde bei der Single-Variante nur ein bestimmter Client mit dem Netzwerk verbunden, so geht es nun um die Authentifizierung mehrerer Geräte an einem Switch-Port. Haben sich die Computer erfolgreich authentifiziert, erhalten sie wieder einen geheimen Schlüssel durch den RADIUS-Server für die erneute Authentifizierung. Dies garantiert, dass allein die Geräte Zugang erhalten, welche sich zunächst durch den Switch-Port authentifiziert haben.

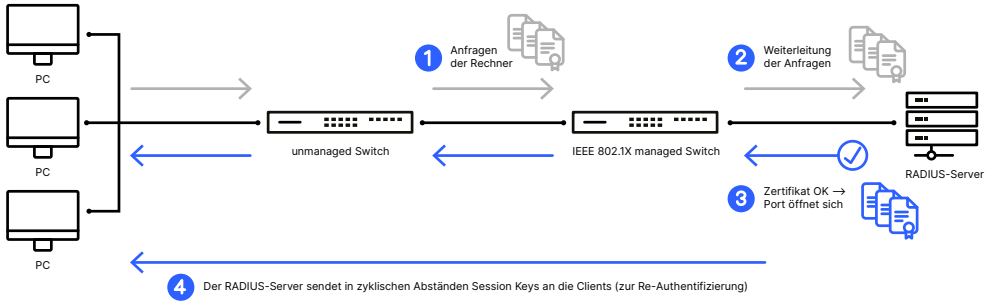

Abbildung 4:
Multi IEEE 802.1X

Beispielszenario

Wie bei der Single-Variante wird wieder ein Switch-Port zur Authentifizierung vorkonfiguriert. Der Unterschied besteht darin, dass nun ein nicht gemanagter Switch zwischen den Switch-Port und die potentiellen Clients geknüpft wird. Diese Clients können sich nun alle mit demselben Zertifikat und/oder Zugangsdaten an einem RADIUS-Server authentifizieren.

4) MAC-based Authentifizierung

Ein weiteres Verfahren zur Authentifizierung von Clients am Switch-Port ist das Abgleichen der MAC-Adresse des Clients über einen RADIUS-Server. Der Switch-Port wird nur für Clients mit ihrer eigenen spezifischen MAC-Adresse geöffnet; anderen Clients wird der Zugang durch diesen Port verweigert. Diese Lösung ist ideal für eine Netzwerkauthentifizierung nicht-intelligenter Clients oder solcher, die IEEE 802.1X nicht beherrschen, z. B. Drucker.

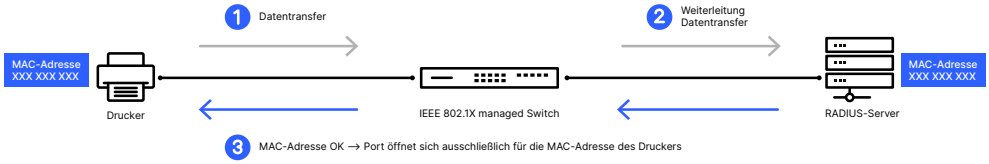

Abbildung 5:
MAC-based IEEE 802.1X

Beispielszenario

Ist ein Drucker mit einem Switch-Port verbunden, so wird die MAC-Adresse des Druckers benutzt, um sich am RADIUS-Server für Netzwerkzugang zu authentifizieren. Der Switch-Port wird dann ausschließlich für die MAC-Adresse des Druckers konfiguriert und freigegeben. Anderen Clients, mit einer abweichenden MAC-Adresse, wird der Switch den Zugriff verweigern.

Infrastrukturelle Voraussetzungen

Zum Einsatz von IEEE 802.1X zur Sicherung des internen Netzwerkes wird ein RADIUS-Server als zusätzliche Komponente benötigt, welcher für die Authentifizierung der Clients zuständig ist. Soll die Authentifizierung über Zertifikate erfolgen, wird zusätzlich eine Certificate Authority (CA) benötigt, welche die Zertifikate für die Clients und den RADIUS-Server ausstellt. Eine CA ist in modernen Routern bereits integriert. Clients ohne IEEE 802.1X-Unterstützung können mit Hilfe der vorgestellten MAC-based Authentifizierung eingebunden werden.

Fazit

Die verschiedenen Methoden, die in diesem Paper vorgestellt wurden, um das Netzwerk auch von innen zu schützen, haben eins gemeinsam: Es werden intelligente Fully Managed Switches benötigt, welche über die notwendigen IEEE 802.1X-Funktionen zur Überwachung und Kontrolle des Zugangs zum Netzwerk verfügen. Die Wahl eines nicht gemanagten Switches hingegen stellt in komplexen Unternehmensnetzwerken ein Sicherheitsrisiko dar, da dessen Ports nicht über entsprechende Zugriffskontrollen verfügen. Einen genaueren Blick auf die Datenblätter und Spezifikationen zu werfen, ist also eine lohnende Aufgabe.

LANCOM Systems GmbH
A Rohde & Schwarz Company
Adenauerstr. 20/B2
52146 Würselen | Deutschland
info@lancom.de | lancom-systems.de