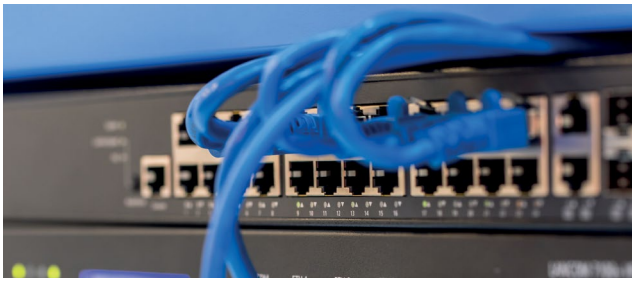
LANCOM White Paper
Switch security with IEEE 802.1X

Switches are a vital security component in networks: After all, they control the traffic for all of your internal data communications. Although the network is protected from the outside by firewalls and VPN gateways, the matter of internal network security is often neglected. This leaves the way open for attack from within the internal network. Professional managed switches are equipped with a comprehensive range of security features, which help networks to comply with security requirements. This white paper provides an insight on how switches operating the IEEE 802.1X standard contribute to security on the LAN.

Secure access control

The IEEE 802.1X standard was developed for managing network access rights. It handles the work leading up to the actual authentication at the network. In the simplest case,



IEEE 802.11X requires the use of a managed "intelligent" network switch and a RADIUS server for authentication.

IEEE 802.1X – four methods of access control

In the interests of secure access control, a number of possibilities are available to make effective use of IEEE 802.1X to achieve the best possible security. In the following we explain the four methods (port-based, single, multi, and MAC-based) and we illustrate the usage scenarios for each one.

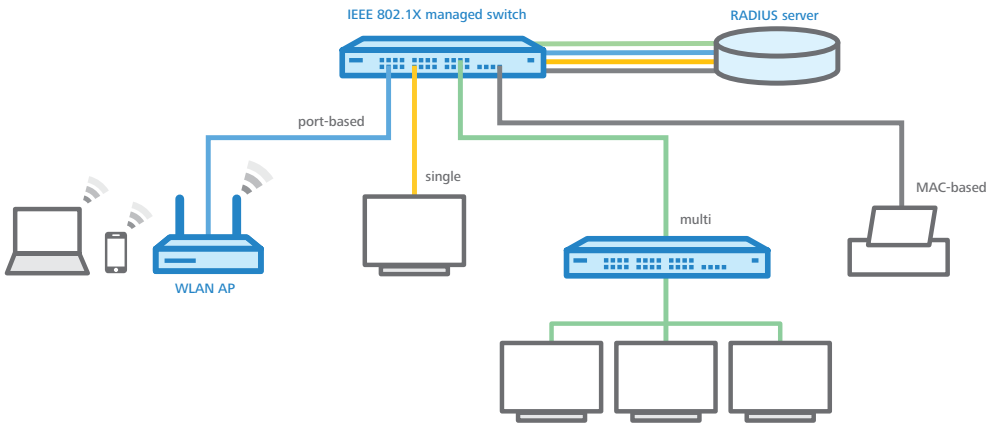


Figure 1: IEEE 802.1X – four methods of access control at a glance

LANCOM Systems

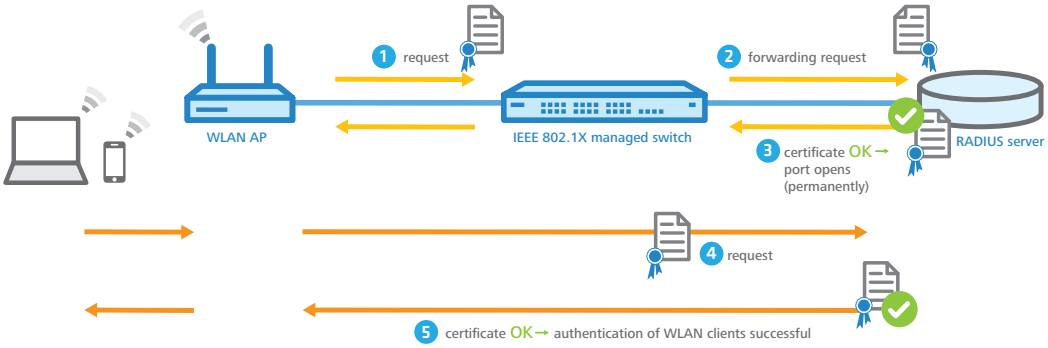


Figure 2: Port-based IEEE 802.1X

1) Port-based IEEE 802.1X

Port-based IEEE 802.1X regulates the authentication of clients at the switch ports by verifying certificates or access credentials against a RADIUS server. After successful authentication, the port remains permanently open for access to the network. The advantage is that, after successful authentication, the port remains permanently open for network access and other clients that connect to the authenticated device also gain network access.

Example scenario

An access point connected to a switch port uses certificates and/or access credentials to authenticate at a RADIUS server and gain network access. Once the access point is authenticated, the corresponding switch port is opened and any Wi-Fi devices that connect to the access point (laptops, smartphones, tablets) are also given network access.

2) Single IEEE 802.1X

Single IEEE 802.1X enables the authentication of a specific client at a switch port by validating a certificate and/or credentials against a RADIUS server. This method ensures that only the authenticated device has network access through the switch.

Example scenario

A computer is connected to a switch port and uses a certificate and/or credentials to authenticate against a RADIUS server. Once the computer is successfully logged on, the RADIUS server regularly sends secret keys to renew the device authentication.

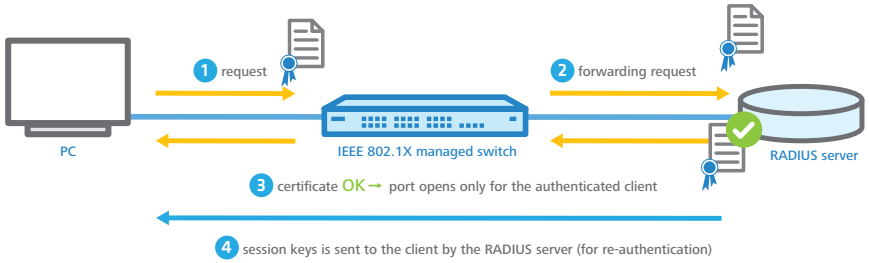


Figure 3: Single IEEE 802.1X

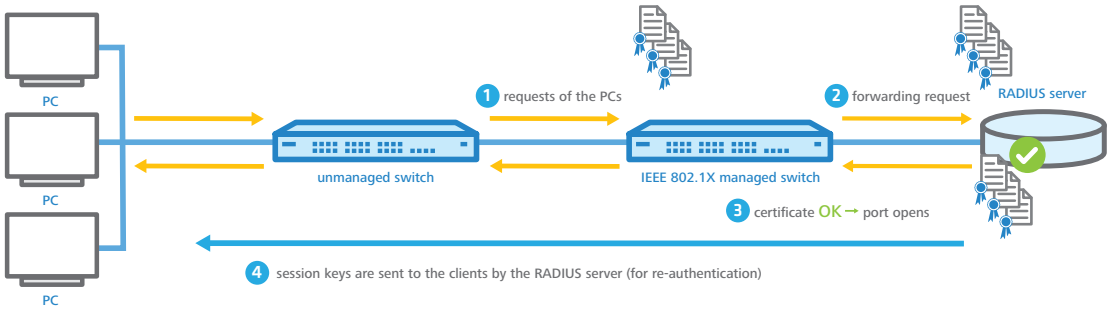


Figure 4: Multi IEEE 802.1X

3) Multi IEEE 802.1X

Whereas the single variant only connects a specific client to the network, the multi variant enables the authentication of multiple devices at a switch port. Once the computers have been successfully authenticated, they receive a secret key from the RADIUS server for re-authentication. This ensures that the only devices to gain access are those that were initially authenticated through the switch port.

Example scenario

As with the single variant, once again a switch port is pre-configured for authentication. The difference now is that a non-managed switch is located between the switch port and the potential clients. All of these clients can use the same certificate and/or access credentials to authenticate against a RADIUS server.

4) MAC-based authentication

Another method of authenticating clients at the switch port is to present a client's MAC address to a RADIUS server. The switch port is opened only for clients that present their own specific MAC address; other clients are denied access to the network through that port. This solution is ideal for the network authentication of unintelligent clients or ones that do not support IEEE 802.1X, such as printers.

Example scenario

In the case where a printer is connected to a switch port, the MAC address of the printer is used to authenticate against the RADIUS server for network access. The switch port is configured exclusively for the MAC address of the printer, which then receives network access. The switch will deny access to other clients with a different MAC address.

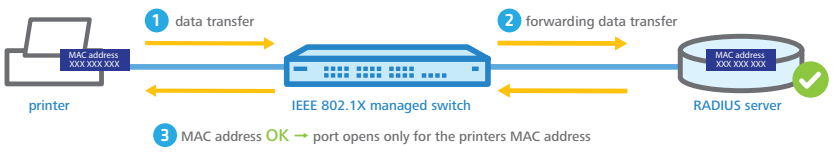


Figure 5: MAC-based IEEE 802.1X

Infrastructure prerequisites

Operating IEEE 802.1X for internal network security requires a RADIUS server as an additional component to handle the authentication of the clients. Certificate-based authentication additionally requires a certificate authority (CA), which issues the certificates for the client and the RADIUS server. Modern routers already feature an integrated CA. Clients that do not support IEEE 802.1X can be networked with the aid of the MAC-based authentication mentioned above.

Summary

The various methods presented in this paper to secure the network from internal attack have one thing in common: They all require intelligent fully managed switches with the necessary IEEE 802.1X functionality for monitoring and control of access to the network. The use of unmanaged switches in complex corporate networks represents a security risk, because their ports do not have the appropriate access controls. To sum up, it is well worth taking a closer look at the data sheets and specifications for your new switches.