802.1X

Inhaltsverzeichnis

802.1X authentifiziert Geräte oder Nutzer am Netzwerkport bzw. WLAN, bevor voller Zugang gewährt wird. RADIUS prüft Identitäten; Switches und APs setzen das Ergebnis um.

1 Funktionsweise

Supplicant (Client), Authenticator (Switch/AP) und Authentication Server (meist RADIUS) verhandeln den Zugang. Erst nach Erfolg kommt der Port in das vorgesehene VLAN.

- **EAP-Methoden:** z. B. EAP-TLS, PEAP
- **Dynamic VLAN:** Zuweisung nach Identität/Gerät
- **MAB:** MAC-Ausnahmen für Drucker o. Ä. (schwächer)

2 Typische Einsatzbereiche

- Unternehmens-WLAN und kabelgebundene Ports
- BYOD- und Gäste-Szenarien mit Steuerung
- Zero-Trust-nahe Netzwerkzugänge

3 Wichtige Hinweise

- Zertifikats- und Geräteverwaltung sind der Betriebsaufwand.
- Fallback-Ports und Exceptions eng halten.
- Monitoring fehlgeschlagener Auths einplanen.

4 Fazit

802.1X bringt Identität an den Netzwerkrand – deutlich sicherer als offene Ports, mit spürbarem IAM- und Zertifikatsaufwand.