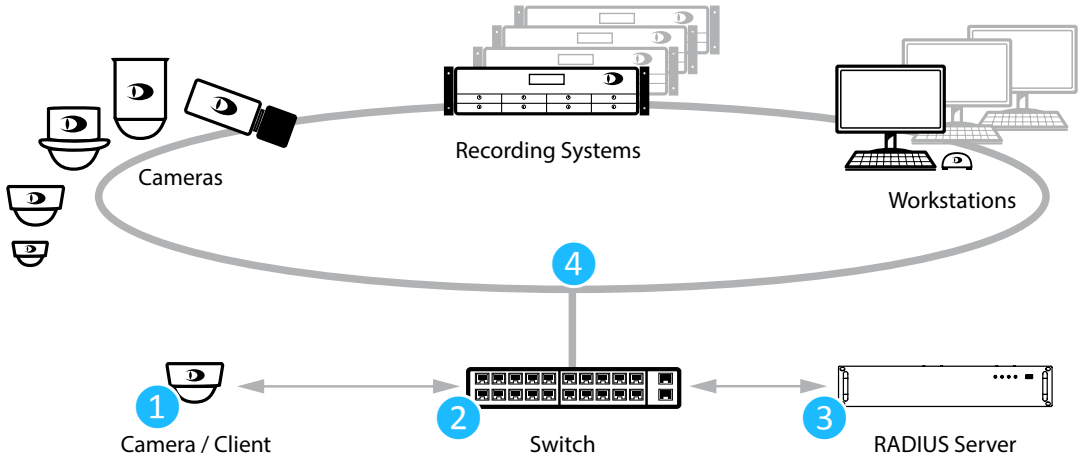
Secure Network Authentication

Protection of the video network by network authentication according to IEEE 802.1X

Designed with a focus on **system security,** the **5000 series cameras** support **secure network authentication** (IEEE 802.1X) along with **encrypted data and video transmission** (TLS/AES-256). Other security measures include user management, password protection, deactivation of unneeded or insecure ports, regular provision of firmware updates as well as the prevention of third-party software execution.

Operators of video systems for the security of public places, airports, casinos or businesses are usually confronted with the problem that **cameras are mounted on the physical edge of the network**. Since these cameras are accessible to third parties, the **risk of unwanted access to the network** increases. An attacker could connect his own device instead of the camera to gain access to the network or read out the data traffic (man-in-the-middle attack).

In addition to tamper-proof installation of the cameras, this risk can be mitigated by a **network setup with authentication according to the IEEE 802.1X standard**. The **use of the 5000 series cameras** is recommended, as all models support authentication using certificates (EAP-TLS) in accordance with IEEE 802.1X.



1 Camera

The camera is equipped with an individual certificate (ID card) before it is connected to the network.

When the camera is connected to the network, it establishes a connection via a network port (door). This connection is restricted (door flap) and only allows sending a request with the certificate to an access switch (doorman).

Any client (attacker) could pass any certificate here. But access to the network would be limited to communication with the switch.

2 Switch

The switch checks the basic legitimacy of the request (ID photo) and forwards the certificate to the RADIUS server (club owner).

An attacker with a badly falsified certificate would already be rejected here. The corresponding port could be blocked automatically.

3 RADIUS Server

The RADIUS server performs a thorough check of the certificate. This can be done by comparing with deposited certificates (customer register) or by comparing the data with an LDAP server (regulatory authority).

All certificates are multilevel signed with HASH codes. A successful falsification by an attacker can be ruled out.

4 Access

If the RADIUS Server determines the validity of the certificate and the owner's (camera) authorization for network access, it sends an appropriate confirmation (entry) to the switch.

An attacker with a valid certificate but without authorization for network access would be finally rejected.

In this case, the switch completely opens the network port (door) and the camera can establish an unrestricted network connection (entrance).

If appropriate roles are defined, the switch can limit network access to certain VLAN subareas (dance area, bar).

After successful authentication, the camera can perform a regular network startup.

General

- If a camera's network connection is interrupted, the Dallmeier recording system automatically detects and reports a failure.
- If authentication is missing, no network access or reading of data traffic is possible.
- Ports with failed authentication attempts can be locked automatically (no more requests possible).

This handout describes IEEE 802.1X in a simplified way. Detailed technical information can be found at https://en.wikipedia.org/wiki/IEEE_802.1X.