STANDARD: 802.1X

IEEE 802.1x is a standard for port-based network access control. It provides the capability to permit or deny network access based on the identity and credentials of the user or device attempting to connect to the network.
802.1x is commonly used in wireless networks to prevent unwanted users from connecting to it. .

802.1x has its own terminology for some of the required devices. The three primary components are

- **Supplicant** = any device that is requesting network access when connected to a switch port. Supplicants must have software that runs 802.1x to be able to request access.
- **Authenticator** = device that acts as a translator between the supplicant and authentication server. It takes the EAP frames from the supplicant and encapsulates them in RADIUS packets to forward to the authentication server. Authenticators must support 802.1x and have ports enabled for Confidential 8 802.1x operation
- **Authentication server** = The authentication server is the device that decides whether the supplicant is granted access. The authenticator forwards all requests to the authentication server and expects a reply

EAP

- The Extensible Authentication Protocol (EAP) is an authentication framework that supports multiple authentication methods.
- On wired implementations, EAP is also referred to as EAP over LAN (EAPOL). EAP is used by the supplicant and authenticator to communicate.
- EAP does not require IP to operate, as it is a Layer-2 protocol.
- L'utilizzo di EAP all'interno di una rete wireless, ad esempio, prevede che non sia l'access point ad autenticare il client: esso redirige la richiesta di autenticazione avanzata dal client ad uno specifico server, configurato per questo scopo come un RADIUS.

RADIUS

- RADIUS (Remote Authentication Dial-In Service) is an authentication and accounting network protocol. In 802.1x deployments, the RADIUS protocol is used to communicate authentication information between the authenticator and the authentication server.
- The RADIUS protocol uses the client-server model = CLIENT: Authenticator, SERVER: Server that runs RADIUS (Usually AAA servers)
- As For the EAP, RADIUS has his own terms:
    - **User / Device** = Requests access to the network. This is the 802.1x supplicant.
    - **Network Access Server (NAS)** = Provides access to the network. This is the 802.1x authenticator.
    - **Authentication Server** = Authenticates requests from the NAS. This is the 802.1x authentication server.
    - **Data Store** = An optional database with user information.

802.1X Communication

1) The supplicant communicates to the authenticator using EAP frames.
2) The authenticator places the EAP message into an AVP (Attribute Value Pairs) in a RADIUS packet to send to the authentication server.
3) The authentication server responds with an EAP message inside a RADIUS packet.
4) The authenticator removes the EAP message from the RADIUS packet to send back to the supplicant as an EAP frame

- Initiation

Either the MFP or switch can start the 802.1X authentication process:

1) **SWITCH INIT =** the switch will periodically send EAP-Request-Identity frames out of each 802.1X enabled port. If the MFP has 802.1x enabled, it will respond with its identity and the authentication process can begin
2) **HOST INIT =** The Host will also transmit EAPOL-Start frames when It is connected to a switch port. The switch will see the EAPOL-Start frame and know an 802.1X device is connected. This will start the 802.1X authentication process without having to wait for the switch to initiate.

- AUTHENTICATION AND AUTHORIZATION

After receiving the EAP-Request-Identity frame, the MFP will respond with an EAP-Response that contains the identity (username).
During this stage, the switch sends EAP messages between the MFP and the authentication server: The switch will take the EAP message, place it into an AV-pair within a RADIUS packet, and send it to the server.
The server's response will be an EAP message inside a RADIUS packet with the switch as the destination
Authentication happens in two stages:

1) They decide what kind of EAP they are going to use
2) Authentication takes place with the decided EAP method

- ACCOUNTING

If configured, the switch can start and accounting procedure in the server

- TERMINATION

An 802.1 x session can be terminated in a few ways. LINK DOWN, INACTIVITY TIMEOUT OR OTHER METHODS.

EAP METHODS

There are four available EAP methods for TA Triumph-Adler/UTAX devices:

- **EAP-TLS:** is a widely supported, deployed, and secure EAP method. While it offers excellent security, it also requires a more complicated installation due to the requirement for mutual authentication. The supplicant and the authentication server both require a certificate. This is a more labor- intensive installation since the certificates need to be deployed on all devices that will authenticate to the server. Due to the requirement for client certificates, a working PKI (public key infrastructure) is needed to deploy EAP-TLS. Authentication is performed over a TLS tunnel using the client and server certificates.
- **EAP-PEAP:** is a widely supported EAP method. It is similar to EAP-TLS but does not have the requirement for client certificates. Authentication is performed over a TLS tunnel using a username and password
- **EAP-TTLS:** It is similar to EAP-TLS but does not have the requirement for client certificates. Authentication is performed over a TLS tunnel using a username and password
- **EAP-FAST:** EAP-FAST is generally used when the authentication server is a Cisco ACS device. Authentication is performed over a TLS tunnel created using a PAC (Protected Access Credentials) as opposed to a client certificate
- **EAP-MD5:** It offers minimal security due to the vulnerability of md5. EAP-MD5 differs from other EAP methods in that it only provides authentication of the EAP peer to the EAP server but not mutual authentication. By not providing EAP server authentication, this EAP method is vulnerable to man-in-the-middle attacks.