Network Authentication - 802.1x

Secure the Edge of the Network

Table of contents

© Bosch Security Systems B.V. 2023

1 Secure the edge of the network

Security devices are mostly located at the physical edge of the network.
Especially intrusion devices, with network access such as the MAP5000 main panel, are installed at customer's network.
As these devices are connected to the network, this also increases the risk of unwanted access to the network:
people could try to disconnect the security device and connect their own equipment to try to gain access to the network or attach pass-through equipment to try a so-called a man-in-the-middle attack.

Simple usage:

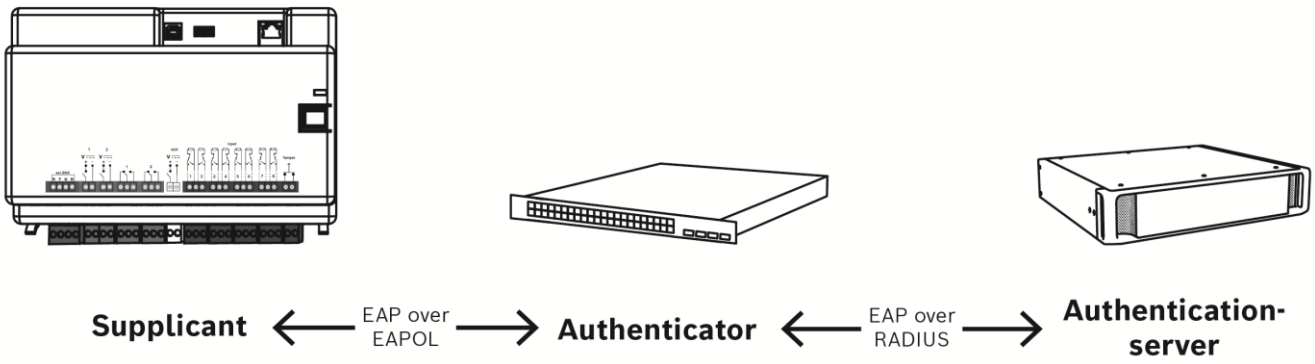

Figure 1 802.1x simple method

- Ensure the device meets the requirements related to physical strength and cabling management:
  Bosch MAP5000 main panel that have an IP30 rating have this network connection point inside their enclosure. This means they need to be physically access to the MAP5000 main panel before the network connection point can be accessed.
  This access is further secured by the tamper of the enclosure.
- Authenticate the device to the network before allowing it to access the network's resources. There are several ways to ensure that only authenticated devices can access the network.
  Bosch MAP5000 main panel support authentication based on username and passcode (802.1x).
  Username: 8 – 64 alphanumeric characters
  Passcode: 8 – 64 alphanumeric characters

1.1 IEEE 802.1x

IEEE 802.1x is a standard published by the **I**nstitute of **E**lectrical and **E**lectronics **E**ngineers Standards Association. This organization within the IEEE develops global standards in a broad range of industries, including power and energy, biomedical and health care, information technology, telecommunication, transportation, nanotechnology, information assurance and many more. This standard is part of the IEEE 802.1 group of networking protocols and provides an authentication mechanism to prevent unauthorized devices to access network resources.

This protocol involves three kinds of main elements:

- The element that wants to be able to access the network resources is named the ***Supplicant***, for example the MAP5000 Main Panel.
- The element that verifies if the supplicant may access the network resources is named the ***Authenticator***.
  Mostly this is a manageable switch, router, or wireless access point.
- The element that steers the authentication process is named the ***Authentication server***.
  The authentication server contains the information that is used to decide if a supplicant may or may not access the network resources. Typically, this is a server that supports the RADIUS protocol, which is a networking protocol that provides centralized authentication, authorization and accounting. The RADIUS protocol is part of the Internet Engineering Task Force (IETF) standards.

© Bosch Security Systems B.V. 2023

1.2 Extensible Authentication Protocol

The Extensible Authentication Protocol is an authentication framework which supports multiple authentication methods. EAP typically runs directly over data link layers such as Point-to-Point Protocol (PPP) or IEEE 802, without requiring IP. EAP provides its own support for duplicate elimination and retransmission but is reliant on lower layer ordering guarantees.

A typical EAP authentication procedure using RADIUS consists of four steps:

1. Initialization:
After the authenticator detects that a device is connected to its port, this port is set to the "unauthorized" state and will only allow 802.1X traffic. Other traffic, such as UDP or TCP is not allowed and dropped.

2. Initiation:
The authenticator will request the identity of the supplicant. When the authenticator receives this information it will forward it to the authentication server by means of the RADIUS protocol.

3. Negotiation:
The authentication server verifies the supplicant identity and sends a challenge back to the supplicant via the authenticator. This challenge also contains the authentication method, which could be based on a username and password.

4. Authentication:
The authentication server and supplicant agree on an authentication method and the supplicant will respond with the appropriate method by providing its configured credentials. If authentication is successful, the authenticator allows the supplicant access to the defined network resources.

© Bosch Security Systems B.V. 2023

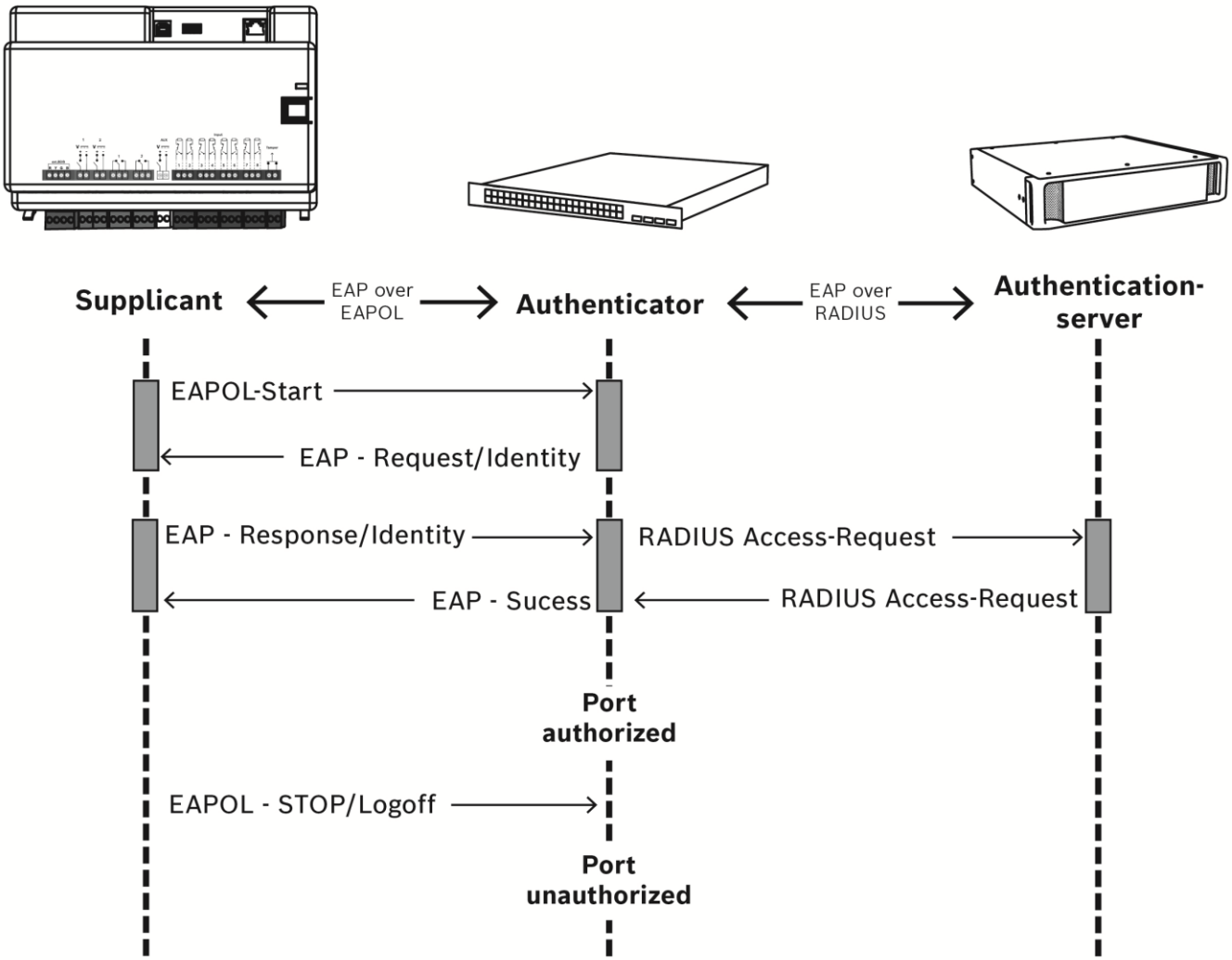

Figure 2 802.1x Authentication Sequence Diagram

1.3 Extensible Authentication Protocol - Transport Layer Security

The Extensible Authentication Protocol (EAP) provides support for multiple authentication methods.
Transport Layer Security (TLS) provides for mutual authentication, integrity-protected cipher suite negotiation, and key exchange between two endpoints. EAP-TLS includes support for certificate-based mutual authentication and key derivation. In other words, EAP-TLS encapsulates the process in which both the server and client send each other a certificate.

1.4 Protected Extensible Authentication Protocol – SSL / TLS

The Protected Extensible Authentication Protocol (PEAP) provides a method to transport securely authentication data, including legacy password-based protocols, via 802.1x networks.
PEAP accomplishes this by using tunneling between PEAP clients and an authentication server. Like the competing standard Tunneled Transport Layer Security (TTLS), PEAP authenticates LAN clients using only server-side certificates, thus simplifying the implementation and administration of a secure LAN. Microsoft, Cisco, and RSA Security developed PEAP.

© Bosch Security Systems B.V. 2023

2 Prerequisites and RPS for MAP

2.1 Prerequisites

- Use minimum the MAP5000 bundle version 1.47.4 with
  - Main panel firmware: 1.4.0231
  - RPS for MAP: 1.22.0.166
- 802.1x secured network with PEAP protocol

2.2 RPS for MAP

The Bosch MAP5000 main panels used the 802.1x PEAP protocol with username and passcode.

1. 802.1x Enable
2. 802.1x Authentication Type / Protocol is PEAP.
3. / 4. User Name / Passcode are given by the Authentication Server → Customers IT department

Figure 3 802.1x settings in RPS for MAP

© Bosch Security Systems B.V. 2023

Bosch Security System B.V. 2023

Torenallee 49
5617 BA Eindhoven
Netherlands

www.boschsecurity.com

© Bosch Security Systems B.V., 2023