Protocols

Application Note

Configuring IEEE 802.1x

Table of Contents

1 Introduction

1.1 Purpose

This document describes how to configure IEEE 802.1x port-based authentication in METEL devices to prevent unauthorized devices (clients) from gaining access to the network and basic information about IEEE 802.1x protocol.

1.2 Scope

This document describes

- Understanding 802.1X Authentication
- How to configure METEL s.r.o. switches

2 Understanding 802.1x Authentication

METEL s.r.o. implemented according to:

IEEE Std 802.1X™- 2004

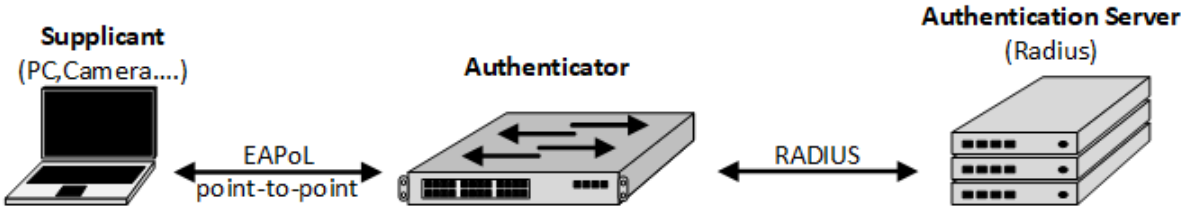
(Revision of IEEE Std 802.1X-2001)

The IEEE 802.1x standard defines a client and server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. The authentication server authenticates each client connected to a switch port and assigns the port to a VLAN before making available any services offered by the switch or the LAN.

During the authentication process, 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

2.1 Topology

802.1x defines the following three required components:



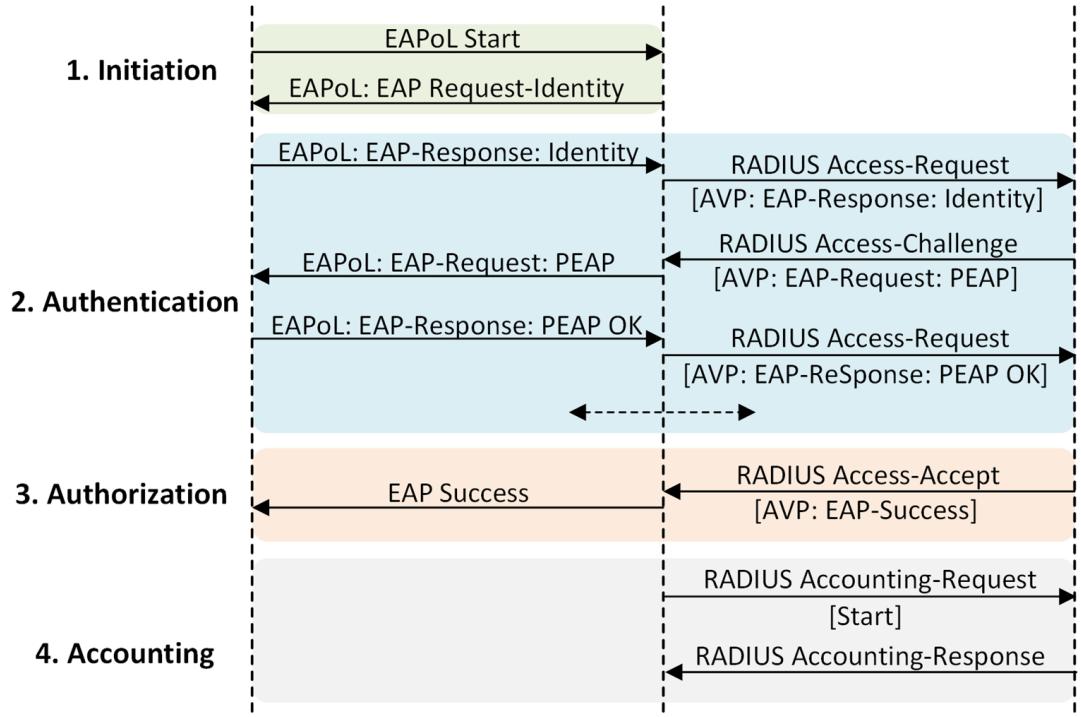
Supplicant: An entity at one end of a point-to-point LAN segment that seeks to be authenticated by an Authenticator attached to the other end of that link.

Authenticator: An entity at one end of a point-to-point LAN segment that facilitates authentication of the entity attached to the other end of that link.

Authentication Server: An entity that provides an authentication service to an Authenticator. This service determines, from the credentials provided by the Supplicant, whether the Supplicant is authorized to access the services provided by the system in which the Authenticator resides.

2.2 802.1x Sequence

Example of 802.1x sequence:



2.2.1 Session Initiation

An 802.1X authentication can be initiated by either the switch or the supplicant. From the perspective of the switch, the authentication session begins when the switch detects a link up on a port. The switch initiates authentication by sending an **EAP-Request-Identity** message to the supplicant. If the switch does not receive a response, the switch re-transmits the request at periodic intervals.
The supplicant can initiate authentication by sending an **EAPoL-Start frame**. The EAPoL-Start message enables supplicants to speed up the authenticate process without waiting for the next periodic **EAP-Request-Identity** from the switch. EAPoL-Start messages are required in situations where the supplicant is not ready to process an EAP-Request from the switch (for example, because the operating system is still booting); or where there is no physical link state change on the switch (for example, because the supplicant is indirectly connected via an IP phone or hub).

2.2.2 Session Authentication

During this stage, the switch relays EAP messages between the supplicant and the authentication server, copying the EAP message in the EAPoL frame to an AV-pair inside a RADIUS packet and vice versa. In the example part of the exchange, the supplicant and the authentication server agree on an EAP method (PEAP).

The rest of the exchange is defined by the specific EAP method. The EAP method defines the type of credential to be used to validate the identity of the supplicant and how the credential is submitted. Depending on the method, the supplicant may submit a password, certificate, token, or other credential. That credential can then be passed inside a TLS-encrypted tunnel, as a hash or in some other protected form.

2.2.3 Session Authorization

If the supplicant submits a valid credential, the authentication server returns a **RADIUS Access-Accept** message with an encapsulated **EAP-Success** message. This indicates to the switch that the supplicant should be allowed access to the port. Optionally, the authentication server may include dynamic network access policy instructions (for example, a dynamic VLAN or ACL) in the Access-Accept message. In the absence of dynamic policy instructions, the switch simply opens the port.

If the supplicant submits an invalid credential or is not allowed to access the network for policy reasons, the authentication server returns a **RADIUS Access-Reject** message with an encapsulated **EAP-Failure** message. This indicates to the switch that the supplicant should not be allowed access to the port. Depending on how the switch is configured, it may retry authentication, deploy the port into the Auth-Fail VLAN, or try an alternative authentication method.

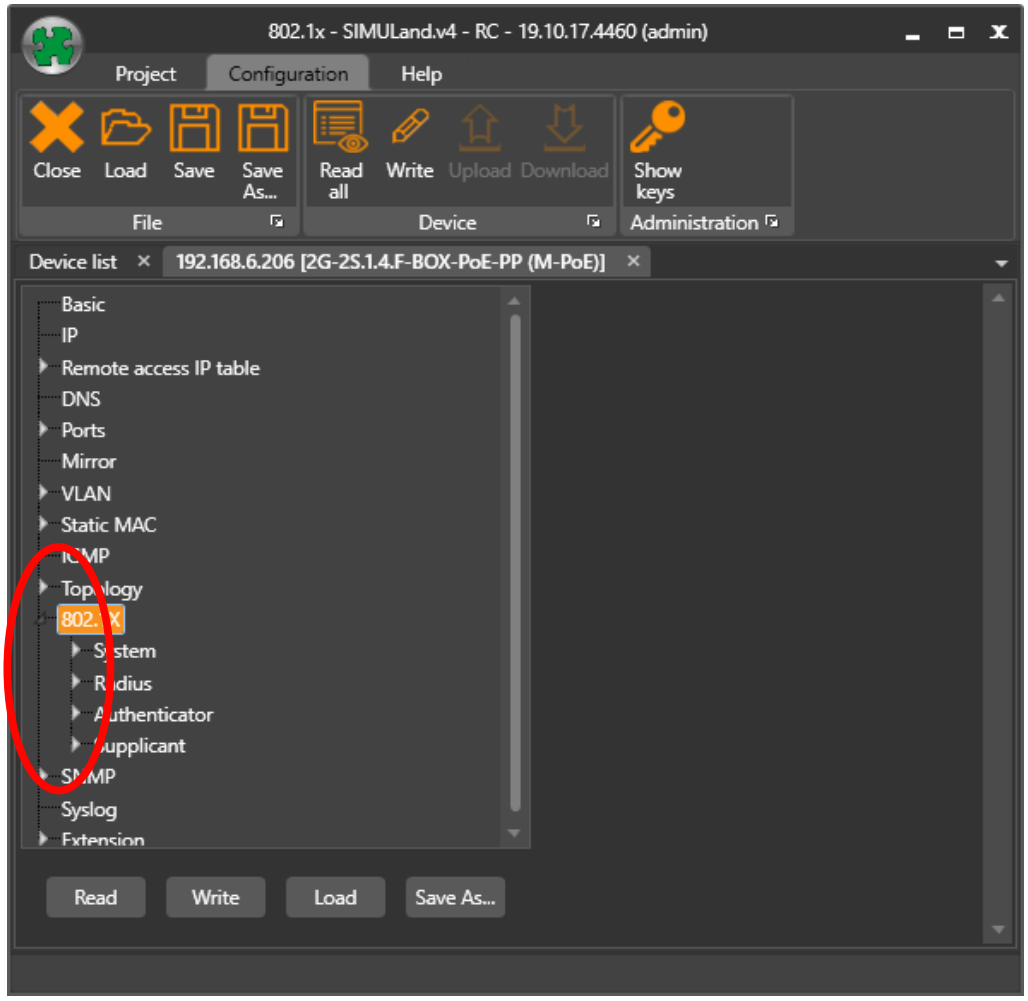
2.2.4 Session Accounting

If the switch is able to successfully apply the authorization policy, the switch can send a RADIUS Accounting-Request message to the authentication server with details about the authorized session. Accounting-Request messages are sent for both dynamically authorized sessions as well as locally authorized sessions; for example, Guest VLAN and Auth-Fail VLAN.

3 Configuration

This section describes basic configuration of IEEE 802.1x.

- **System** – Global enabling 802.1x authentication. Port control mode (None, Authenticator, Supplicant)
- **Radius** – Radius server configuration parameters
- **Authenticator** – Configuration of Authenticator behavior
- **Supplicant** – Configuration of Supplicant behavior



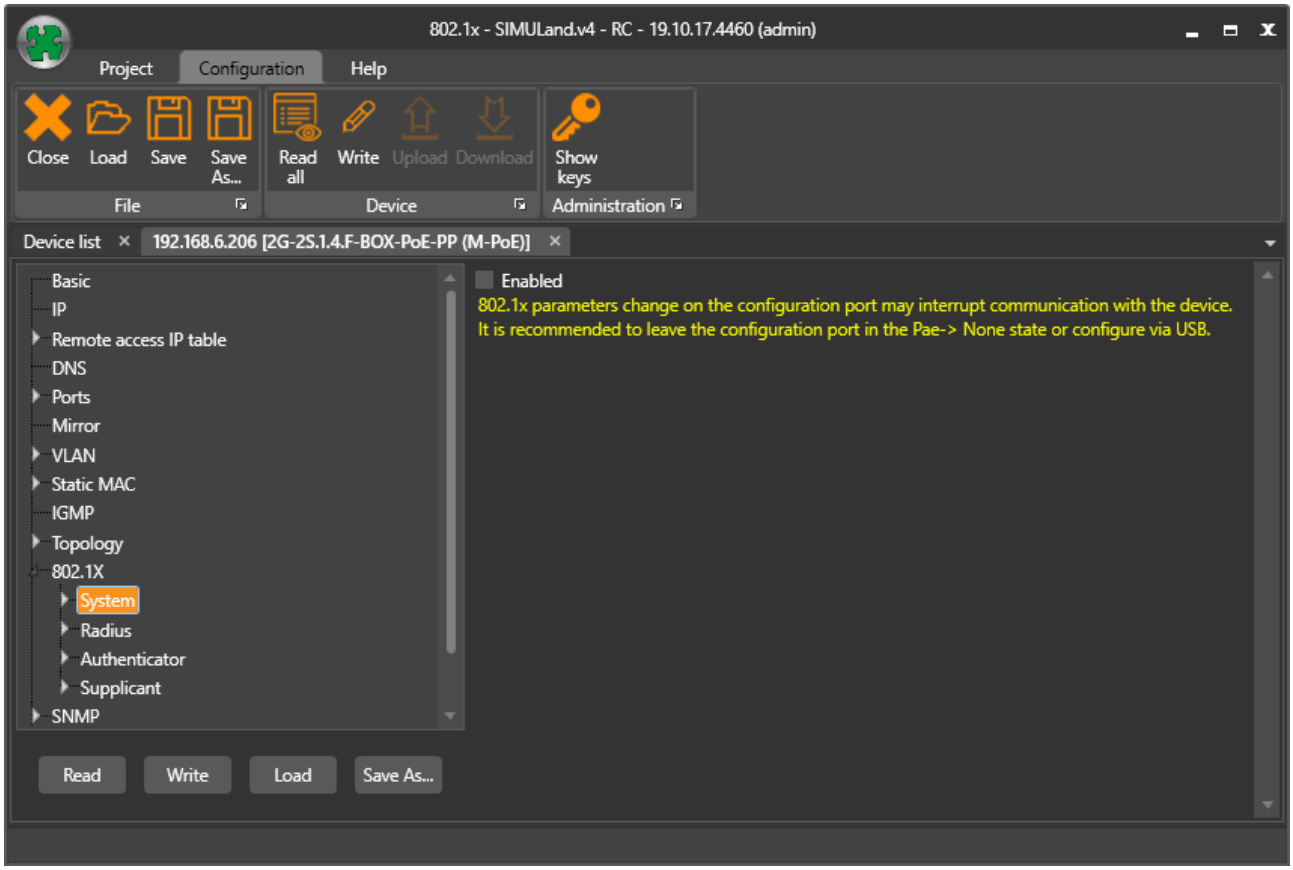
3.1 System (Global enabling 802.1x)

The checkbox "**Enable"** of the section **802.1x -> System** globaly enable or disable 802.1x for whole device.

Checked - All configuration parameters of the menu 802.1x (System, Radius,

Pea, Authenticator, Supplicant) are activated and setted parameters will be used for authentication a new connected clients (supplicants) in to the LAN.

Unchecked - 802.1x is disabled at all ports.



3.1.1 Pae (Port Control Mode)

For each port of the switch it is possible to set to a different mode. Switch supports mode **None, Authenticator, Supplicant**.

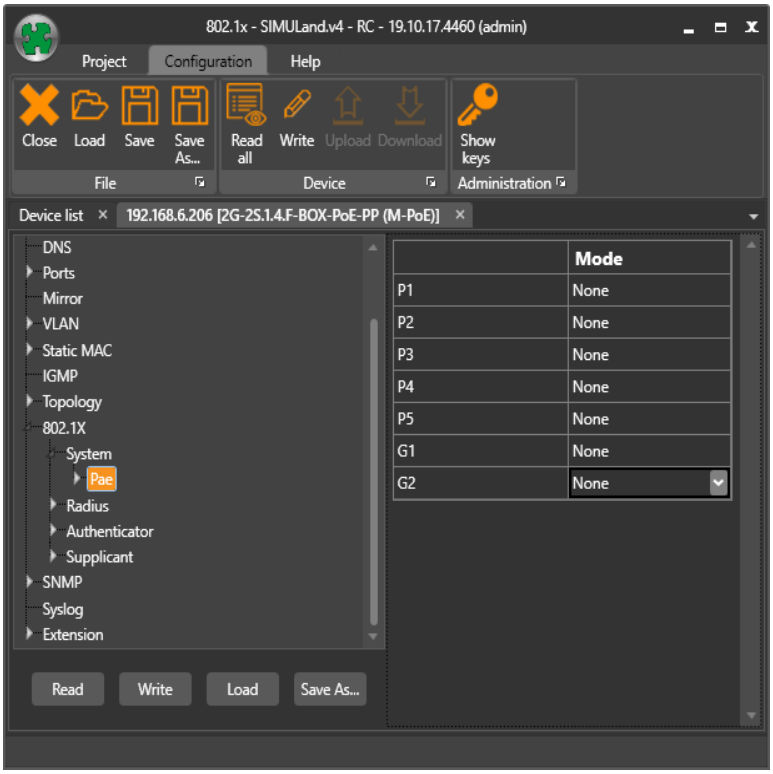
None - Port is discarded of 802.1x and its actions are as a standard switch port.

Authenticator - Enables 802.1x authentication on the interface. The PAE Authenticator state machines communicate with a higher layer entity, that manages EAP and AAA functionality. On the Authenticator, the PAE's role is to transport EAP

frames between the Supplicant and the Authenticator's higher-layer entity and to control port access based on the result of the authentication exchange. The Authenticator state machines do this without examining the EAP header in the frame.

Supplicant - Configures the interface as a port access entity (PAE) supplicant. The PAE Supplicant state machines communicate with a single higher layer entity: EAP. On the Supplicant, PAE's role is to transport EAP frames between the network and the higher layer and to optionally control port access based on the result of the authentication exchange. The Supplicant state machines do this without examining the EAP header in the frame.

The **Pae** section is superordinate to sections **Authenticator** and **Supplicant**!



3.2 Radius (Server Configuration)

The Radius (Authentication) server validates and checks the identity of the connected clients (Supplicants) and notifies the switch whether or not the client can be authorized to access to the LAN or switch services.

In the event, the port is configured as a **Authenticator** so for the successful authentication radius server configuration needs:

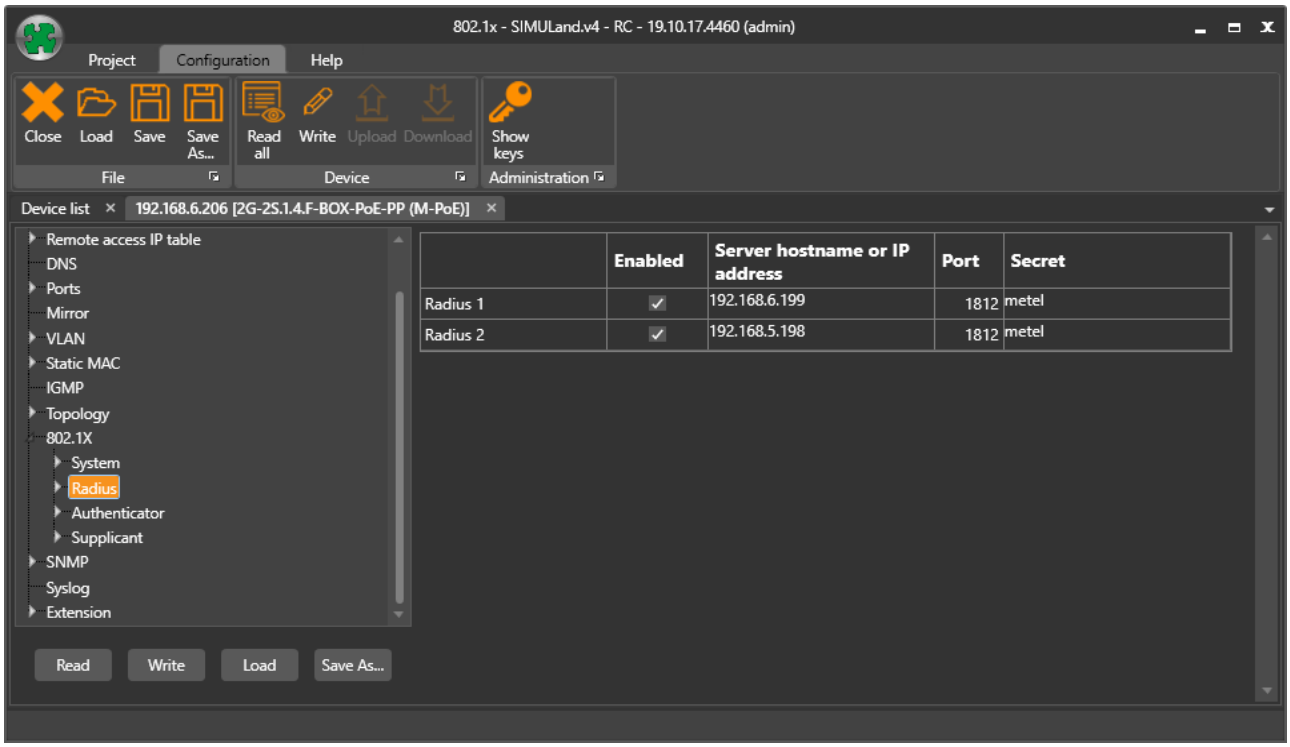
Enabled - Checked - Enable Radius server parameters using.
Unchecked – Disable Radius server parameters.

Port - Specifies the UDP/TCPport for authenticating (1812 is a default).

Secret - Specifies the authentication and encryption key used between the

switch and the RADIUS daemon running on the Radius server. Both, the switch (authentificator) and the Radius server must be configured to use the same shared secret.

Server Hostname or IP Address – Radius server name or IP address.



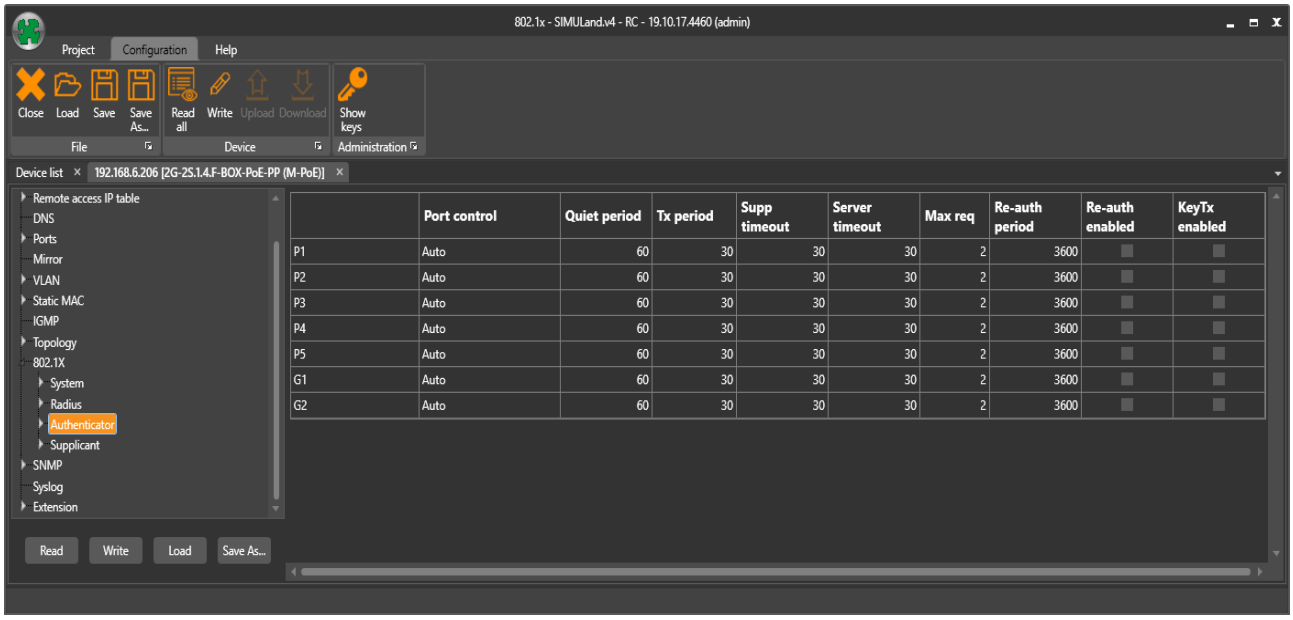
Radius Server Sequence

Radius server configuration of the first row (Radius 1) is used as the main Radius server. Every time when the new authentication process starts the switch tries to send authentication data to the new one. If the first server does not respond after three times (the delay depends on Auhentificator and Server Timeout configuration) then the switch tries to send packets in to the second one (Radius 2).

The second one is usually used as backup for first one and connected locally (no WAN network).

3.3 Authenticator

The part Authenticator of configuration more specifies parameters for port in **Pae mode Authenticator**. For each port is possible set the specific properties.



Port Control

Force authorized - Disables 802.1x authentication process and causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1x authentication of the clients.

Force unauthorized - Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch can not provide authentication services to the client through the interface. Port is in the state blocking.

Auto - Enables 802.1x authentication and causes the port to begin in the unauthorized state, allowing only **EAPOL** frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up or when an **EAPOL-start** frame is received. The switch requests the identity of the client and begins relaying authentication messages between the client and the authentication server. Each client attempting to access the network is uniquely identified by the switch by using the client's MAC address.

Quiet period - When the switch can not authenticate the client, the switch remains idle for a set period of time and then tries again. The **Quiet period** interface configuration command controls the idle period. A failed authentication of the client might occur because the client provided an invalid password. You can provide a faster response time to the user by entering a number smaller than the default.
In fact, the **QuietPeriod** is a initialization value used for the quietWhile timer (time during which
it will not attempt to acquire a Supplicant.) Its default value is 60 s; it can be set by management to any value in the range from 0 to 65 535 s.

Tx period - A timer used by the Authenticator PAE state machine to determine when an EAPOL PDU is to be transmitted.

Time that the switch waits for a response to an **EAP-request-identity** frame from the client before retransmitting the request.

Supp timeout - Sets the period of time the switch waits for a supplicant response to an **EAP request**. If the supplicant does not respond within the configured time frame, the session times out.

Server timeout - Sets the period of time the switch waits for a server response to an authentication request. If there is no response within the configured time frame, the switch assumes that the authentication attempt has timed out. Depending on the current **max-req** setting, the switch will either send a new request to the server or end the authentication

session

Max-req - Sets the number of authentication attempts that must time-out before authentication fails and the authentication session ends.

Re-auth period - Authenticator PAEs can time out the authorization state information on a periodic basis by means of the Re-authentication Timer State Machine. The time period for such timeouts is **Re-auth period** seconds since the last time that the authorization state was confirmed. The state variable **Re-Auth enabled** controls whether periodic reauthentication takes place.

Reauthentication can be enabled and disabled, and the **Re-auth period** modified, by management. The default settings are 3600 s (one hour) and for reauthentication to be disabled.

Re-auth enabled - The **enable / disable** control used by the Reauthentication Timer state machine.

KeyTx enabled - An EAPOL frame of type EAPOL-KEY, containing an EAPOL-Key packet, is transmitted to the Supplicant.

The Authenticator Key Transmit state machine transmits EAPOL-Key PDUs to the Supplicant, if the following conditions are all true:

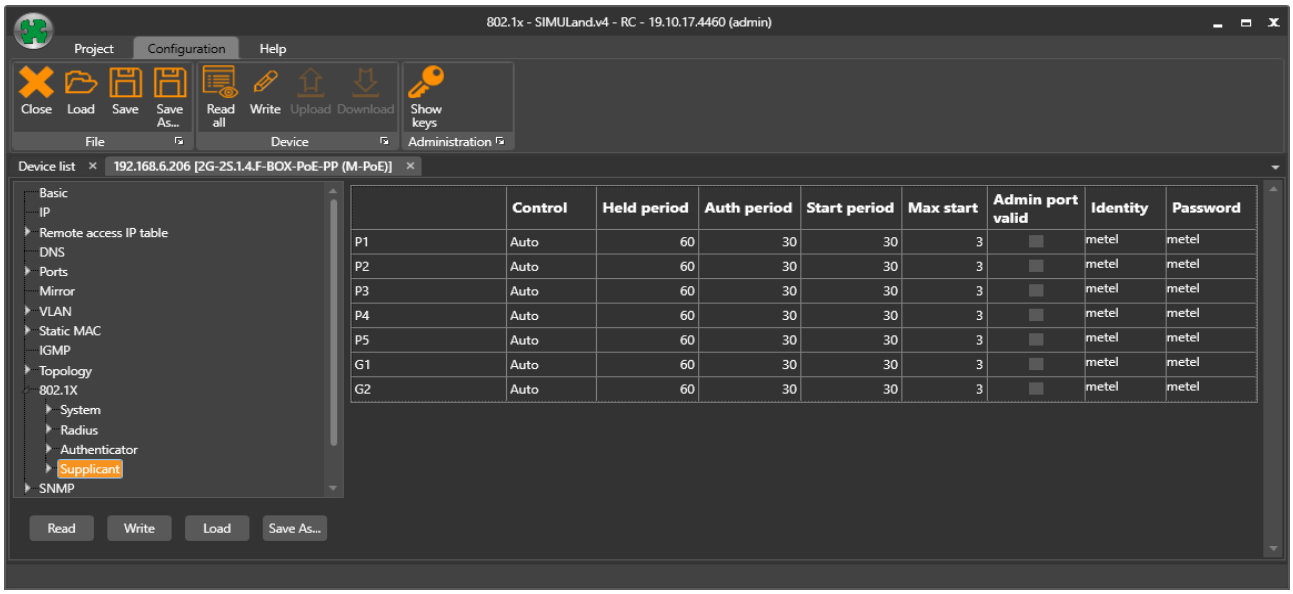
a) The Port is not undergoing initialization.
b) The portControl setting is Auto.
c) Key transmission has been enabled.
d) There is new key material available for transmission.
e) The Backend Authentication state machine has asserted keyRun to indicate that the key machine may run.

3.4 Supplicant

The part Supplicant of configuration uses more specifies parameters for port in **Pae mode Supplicant**. For each port is possible set the different properties.

Supplicant is a user or client (PC, camera, switch…) that wants to be authenticated for access into the LAN.

Supplicant mode implemented in the switch allows authenticate switch just like any client or user.



Port Control
Used in conjunction with to switch between the Auto and non-Auto (ForceAuthorized, ForceUnauthorized) modes of operation of the Supplicant PAE state machine. This variable can take the following values:

Force Unauthorized - The controlled Port is required to be held in the Unauthorized state.In this state, port blocking all packets.

Force Authorized - The controlled Port is required to be held in the Authorized state. In this state, port forwarding all packets.

Auto - The controlled Port is set to the Authorized or Unauthorized state in

accordance with the outcome of an authentication exchange between the Supplicant and the Authentication Server.

Held period – The initialization value used for the held timer. Its default value is 60 s. The held timer starts when the supplicant receive a authentication failure message of the authenticator (switch) or the attempts of authentication is more than **Max start** counter is.

Auth period - The initialization value used for the **Auth period** timer. Its default value is 30 s. A timer used by the Supplicant PAE to determine how long to wait for a request from the Authenticator before timing it out.

Start period - The initialization value used for the **Start period** timer. Its default value is 30s. An EAPOL-Start packet is transmitted by the Supplicant, and the **Start period** timer is started, to cause retransmission if no response is received from the Authenticator. If the **Start period** timer expires, the transmission is repeated up to a maximum of **Max start** transmissions.

Max start - The maximum number of successive EAPOL-Start messages that will be sent before the Supplicant assumes that there is no Authenticator present. Its default value is 3.

Admin port valid – Its deafult value is FALSE. If the value is changed to TRUE and no response of authentificator is received after **Max start** transmissions, the state machine assumes that it is attached to a System that is not EAPOL aware, and transitions to **AUTHENTICATED** state (forwarding).

Username—The supplicant uses this username when responding to requests from an 802.1X authenticator. The username can be 1 to 64 characters long. ASCII-printable characters are allowed, which includes uppercase and lowercase alphabetic letters, numeric digits, and all special characters except quotation marks.

Password—The supplicant uses this MD5 password when responding to requests from an 802.1X authenticator. The password can be 1 to 64 characters in length. ASCII-printable characters are allowed, which includes uppercase and lowercase alphabetic letters, numeric digits, and all special characters except quotation marks

The implemented **EAP Method** algorithm to be used for encrypting authentication user names and passwords is a **MD5** (a hash function defined in RFC 3748 that provides basic security).