Protokol

Application Note

Konfigurace IEEE 802.1x

Obsah

1 Úvod

1.1 Účel

Tento dokument popisuje, způsob konfigurace IEEE 802.1x v zařízeních METEL, aby se zabránilo neoprávněným zařízením (klientům) v získání přístupu k síti a základní informace o protokolu IEEE 802.1x.

1.2 Rozsah

Tento dokument popisuje:

- porozumění 802.1X autentizaci
- jak nastavit METEL s.r.o. switche

2 Porozumění 802.1x autentizaci

METEL s.r.o. implementace podle:

IEEE Std 802.1X™- 2004

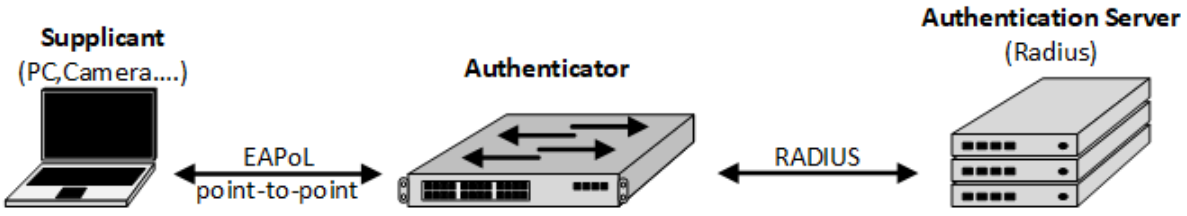
(Revize IEEE Std 802.1X-2001)

Standard IEEE 802.1x definuje protokol pro řízení přístupu a ověřování na základě klienta (Supplicant) a serveru (Authentication server), který omezuje přístup neoprávněných klientů k LAN prostřednictvím veřejně přístupných portů. Authentication server ověřuje každého klienta připojeného k portu switche a přiřazuje port do VLAN předtím než zpřístupní všechny služby nabízené switchem nebo sítí LAN.

Během procesu autentizace umožňuje řízení přístupu 802.1X pouze přenos přes Extensible Authentication Protocol over LAN (EAPOL) skrze port, ke kterému je klient připojen. Po úspěšném ověření může port přejít do běžného provozu.

2.1 Topologie

802.1x definuje následující tři požadované komponenty:



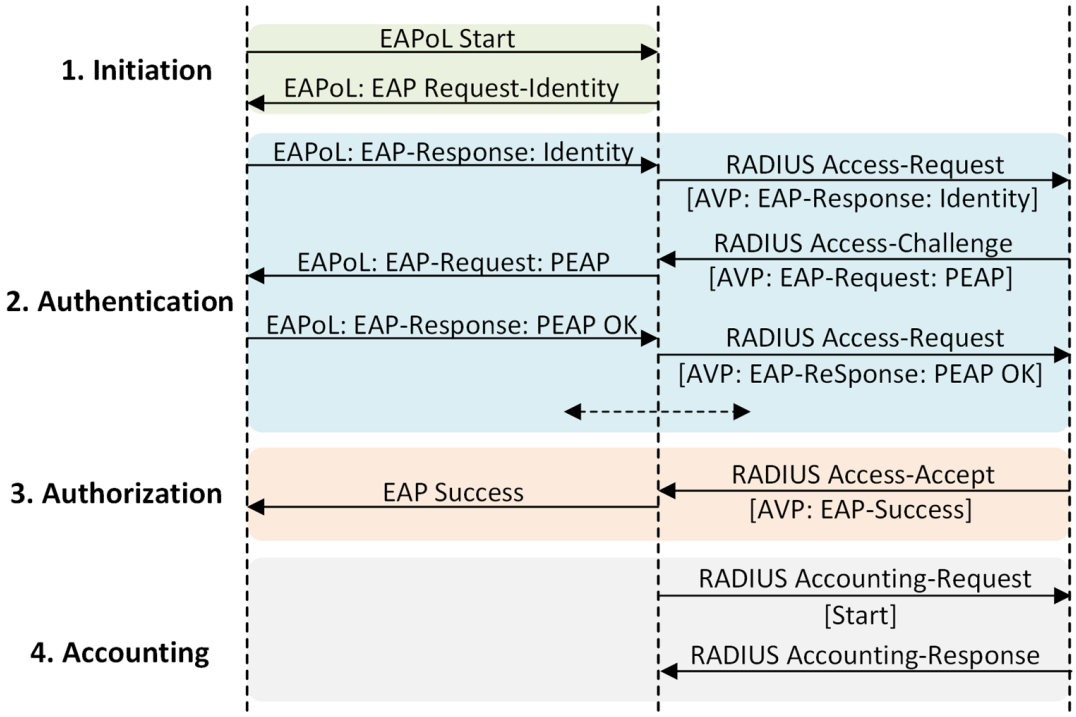
Supplicant: Subjekt na jednom konci segmentu LAN typu point-to-point, který se snaží být ověřen subjektem Authenticator připojeným k druhému konci tohoto spojení.

Authenticator: Subjekt na jednom konci segmentu LAN typu point-to-point, který umožňuje autentizaci subjektu připojeného na druhý konec tohoto spojení.

Authentication Server: Subjekt, který poskytuje autentizační službu pro Authenticator. Tato služba určuje z pověření poskytnutých žadatelem, zda je žadatel oprávněn k přístupu ke službám poskytovaným systémem, ve kterém je Authenticator umístěn.

2.2 802.1x Sekvence

Ukázka 802.1x sekvence:



2.2.1 Zahájení relace (Initiation)

Ověřování 802.1X může být zahájeno buď switchem nebo supplicantem. Z pohledu switche začíná ověřovací relace, jakmile switch detekuje spojení na portu. Switch zahajuje autentizaci zasláním zprávy **EAP-Request-Identity** supplicantovi. Pokud switch neobdrží odpověď, posílá opakovaně požadavek v pravidelných intervalech.

Žadatel může zahájit autentizaci zasláním rámce **EAPoL-Start**. Zpráva EAPoL-Start umožňuje supplicantům urychlit proces autentizace bez čekání na periodickou zprávu **EAP-Request-Identity** od switche. Zprávy typu EAPoL-Start jsou vyžadovány v situacích, kdy supplicant není připraven zpracovat požadavek EAP od switche (například z důvodu, že operační systém stále bootuje) nebo pokud nedochází ke změně stavu fyzického spojení na switchi (například proto, že supplicant je nepřímo připojen prostřednictvím IP telefonu nebo rozbočovače (hub)).

2.2.2 Ověření relace (Authentication)

Během této fáze switch přeposílá zprávy EAP mezi supplicantem a autorizačním serverem, kopíruje zprávu EAP v rámci EAPoL do AV-pair uvnitř paketu RADIUS a naopak. V příkladové části výměny se supplicant a autorizační server dohodnou na metodě EAP (PEAP).

Zbytek výměny je definován specifickou metodou EAP. Metoda EAP definuje typ pověření, které se má použít k ověření totožnosti supplicanta a podloženost. V závislosti na metodě

může žadatel předložit heslo, certifikát, token nebo jiné pověření. Toto pověření lze poté předat uvnitř tunelu šifrovaného TLS jako hash nebo v jiné chráněné podobě.

2.2.3 Oprávnění k relaci (Authorization)

Pokud supplicant předloží platné pověření, autorizační server vrátí zprávu **RADIUS Access-Accept** se zapouzdřenou zprávou **EAP-Success**. Tím indikuje switchi, že by supplicantovi měl být povolen přístup k portu. Autorizační server může ve zprávě Access-Accept případně připojit pokyny pro zásady dynamického přístupu k síti (například dynamická VLAN nebo ACL). Pokud neexistují pokyny pro dynamické zásady, switch jednoduše otevře port.

Pokud supplicant předloží neplatné pověření nebo není z bezpečnostních důvodů oprávněn k přístupu do sítě, autorizační server vrátí zprávu **RADIUS Access-Reject** se zapouzdřenou zprávou **EAP-Failure**. Tím indikuje switchi, že by supplicantovi neměl být povolen přístup k portu. V závislosti na tom, jak je switch nakonfigurován, může opakovat autentizaci, zařadit port do Auth-Fail VLAN pro selhání ověření nebo zkusit alternativní metodu ověření.

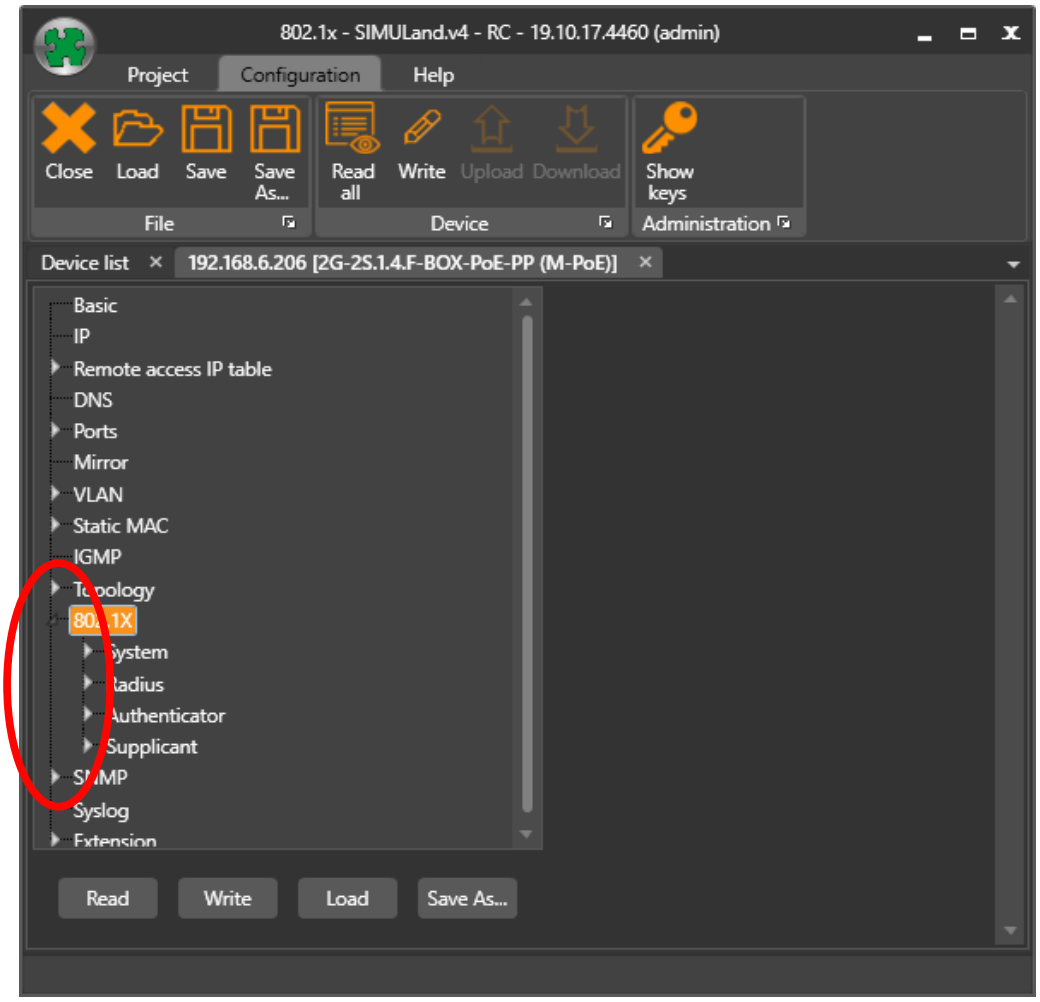
2.2.4 Relace účtu (Accounting)

Pokud je switch schopen úspěšně aplikovat autorizační politiku, switch může odeslat autorizačnímu serveru zprávu **RADIUS Accounting-Request** s podrobnostmi o autorizované relaci. Zprávy s požadavkem na účet jsou zasílány jak pro dynamicky autorizované relace, tak pro lokálně autorizované relace; například Guest VLAN a Auth-Fail VLAN.

3 Konfigurace

Tato sekce popisuje základní konfigurační menu IEEE 802.1x.

- **System** – Globální povolení 802.1x autorizace. Port mód (None, Authenticator, Supplicant).
- **Radius** – Konfigurace navázání spojení s autorizačním serverem.
- **Authenticator** – Konfigurace chování switche jako Authenticator.
- **Supplicant** – Konfigurace chování switche jako Supplicant.

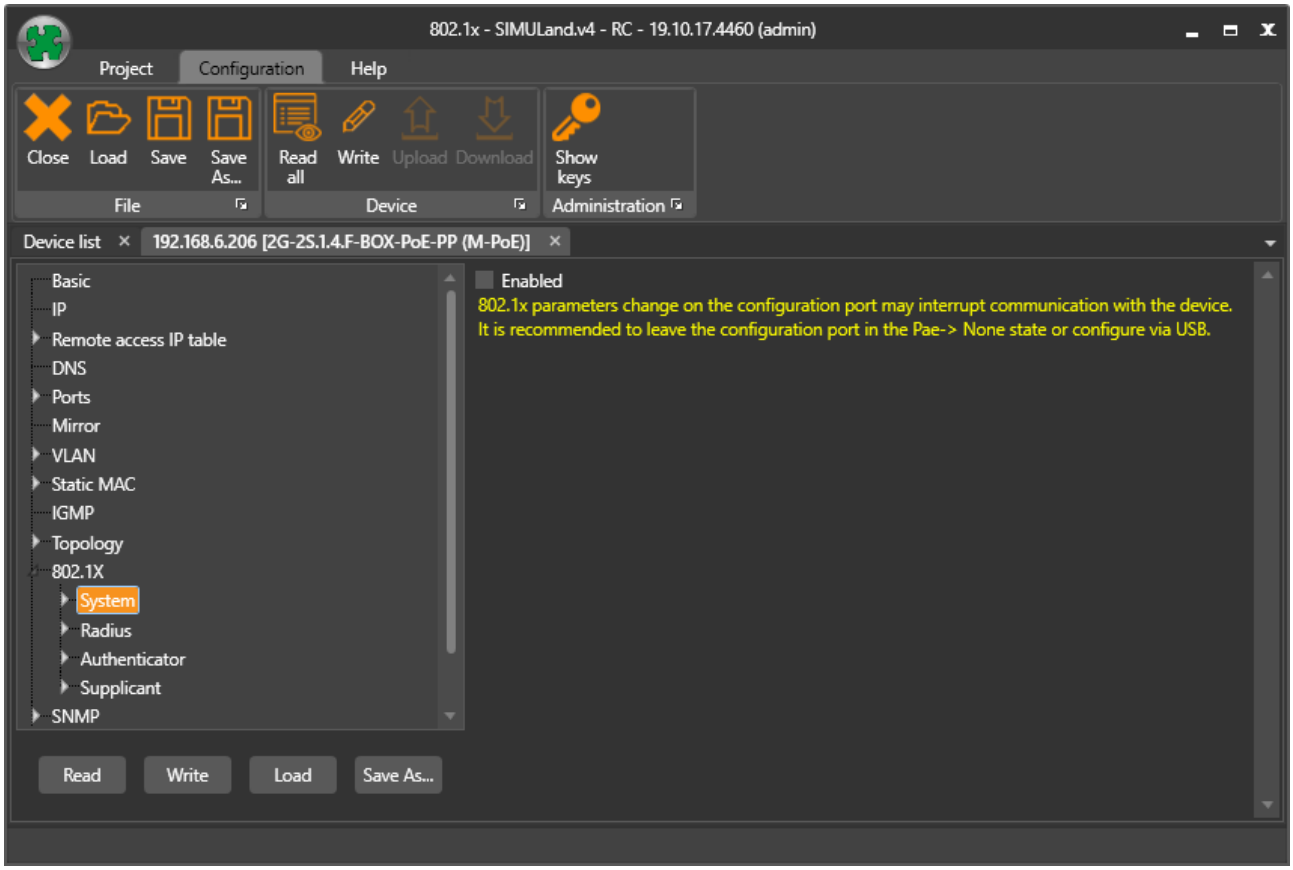


3.1 System (Globální povolení 802.1x)

Checkbox “**Enable”** v sekci **802.1x -> System** globálně povoluje nebo zakazuje 802.1x pro všechny porty.

1 **Zaškrtnuto - Aktivují se všechny konfigurační parametry nabídky 802.1x (System, Radius, Pea, Authenticator, Supplicant) a nastavené parametry budou použity k autentizaci připojených supplicantů (klientů) do LAN.**

2 **Nezaškrtnuto - 802.1x je zakázáno na všech portech.**



3.1.2 Pae (Port mód)

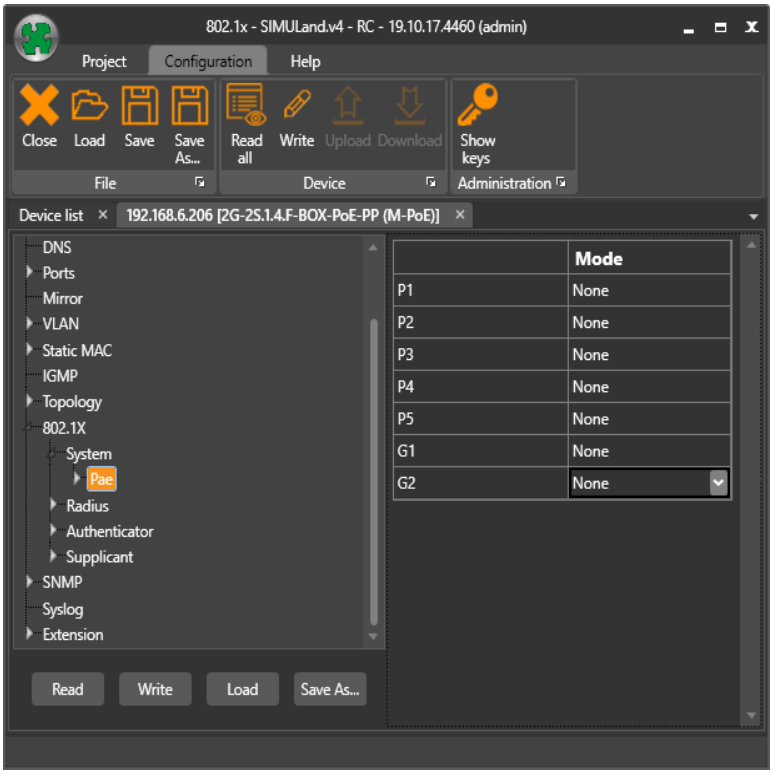
Každému portu switche je možné nastavit rozdílný mód. Switch podporuje následující módy: **None, Authenticator, Supplicant**.

None - Port je vyřazen z 802.1x a jeho chování je jako standardní port switche.

Authenticator - Povoluje 802.1x autorizaci na portu. Stavové mechanismy PAE Authenticator komunikují se subjektem vyšší vrstvy, která řídí funkčnost EAP a AAA. V případě Authenticator je úlohou PAE transportovat rámce EAP mezi supplicantem a subjektem vyšší vrstvy Authenticator a řídit přístup k portu na základě výsledku výměny autentizace. Authenticator stavové mechanismy toto provedou, aniž by prozkoumaly záhlaví EAP v rámci.

Supplicant - Konfiguruje port jako supplicanta s žádostí o přístup (PAE). Mechanismus PAE supplicant komunikuje odděleně se subjektem vyšší vrstvy EAP. Úlohou PAE je transportovat rámce EAP mezi sítí a vyšší vrstvou a volitelně řídit přístup k portu na základě výsledku autentizace. Stavové mechanismy supplicanta to dělají, aniž by prozkoumaly záhlaví EAP v rámci.

Pae sekce je nadřazena sekcím **Authenticator** a **Supplicant**!



3.2 Radius (Konfigurace autorizačního serveru)

Autorizační (RADIUS) server ověřuje a kontroluje identitu připojených supplicantů a upozorňuje switch, zda může být supplicant oprávněn pro přístup k síti LAN nebo službám switche.

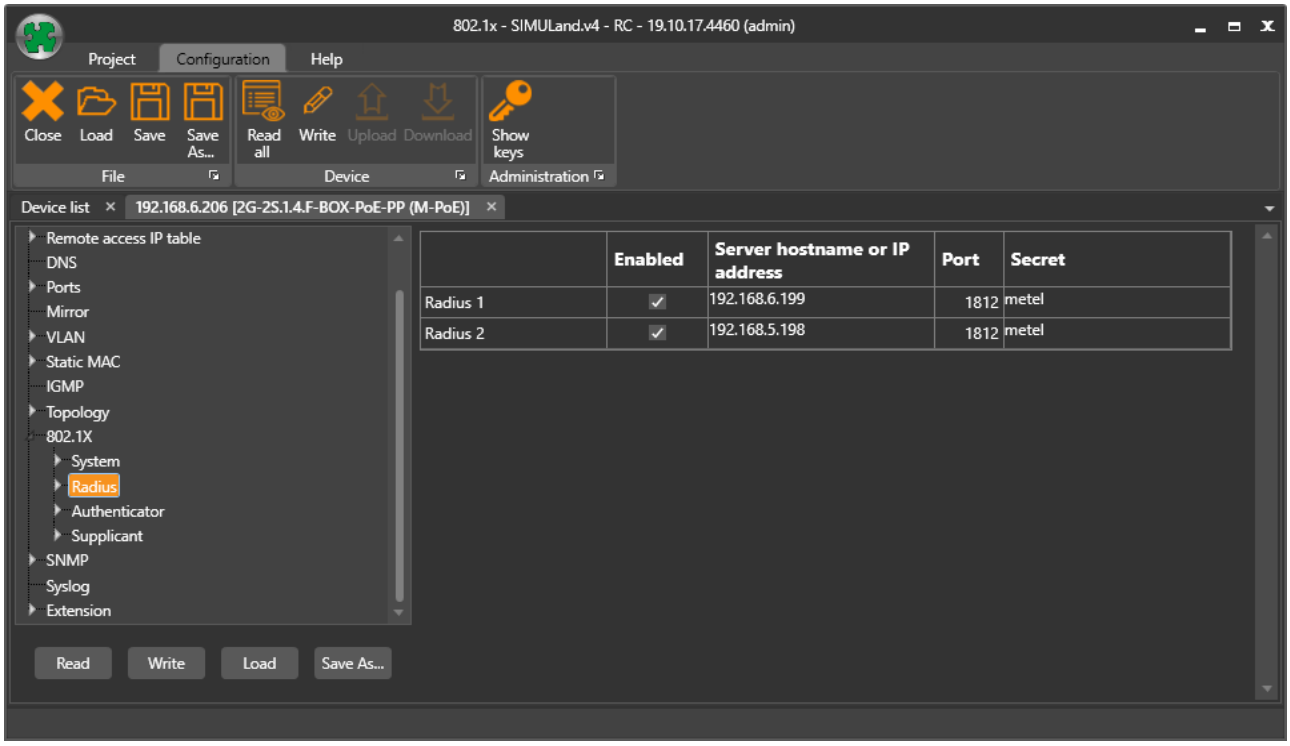
V případě, že je port nakonfigurován jako **Authenticator**, pro úspěšné ověření supplicanta vyžaduje:

Enabled - Zaškrtnuto - Povolení použití nastavených parametrů serveru.
- Nezaškrtnuto - Ignoruje nastavené parametry serveru.

Port - Specifikuje UDP/TCP port k autorizaci (1812 je default).

Secret - Určuje autorizační a šifrovací klíč používaný mezi switchem a službou RADIUS spuštěnou na autorizačním serveru Radius. Switch (authenticator) i server musí být nakonfigurovány tak, aby používaly stejné sdílené heslo.

Server Hostname or IP Address – IP adresa nebo název serveru.



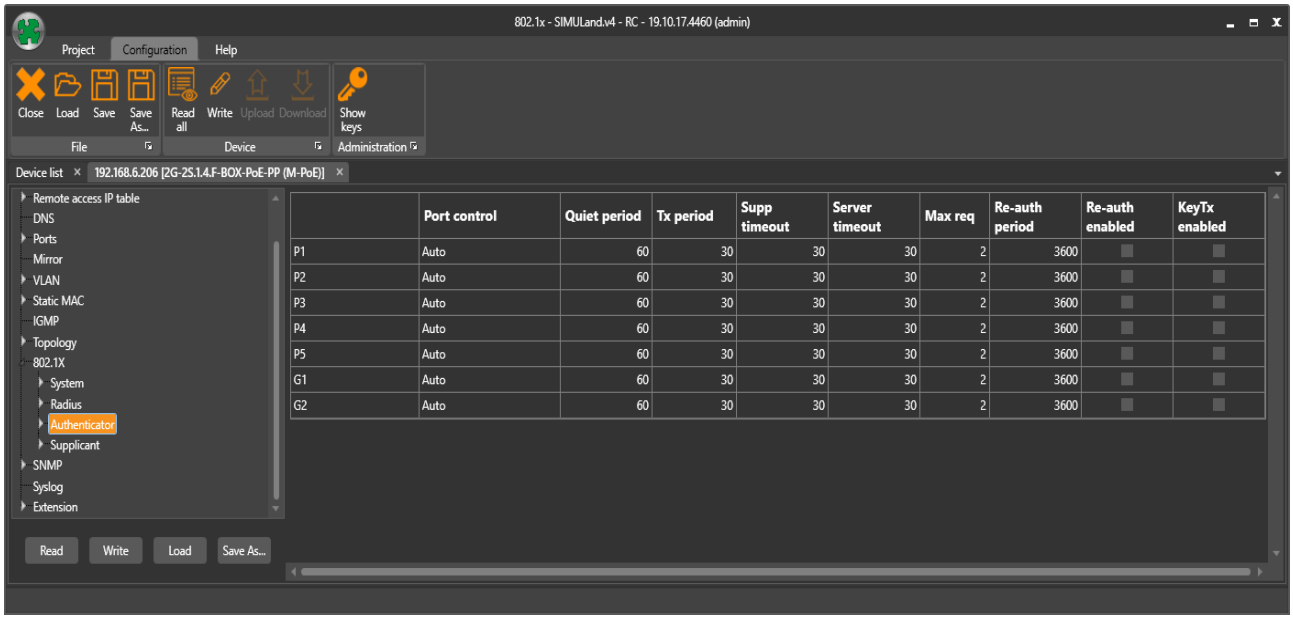
Radius server sekvence

Konfigurace Radius serveru z prvního řádku (Radius 1) se uplatňuje jako výchozí pro komunikaci s Radius serverem (hlavní server). Pokaždé, když se spustí nový proces autentizace, switch se pokouší zaslat autorizační data právě na tento server. Pokud první server třikrát v řadě neodpoví (prodleva závisí na konfiguraci Auhentificator a Server Timeout), switch se pokusí navázat komunikaci s druhým serverem (Radius 2).

Druhý server je obvykle použit jako záložní a doporučuje se jeho lokální připojení v síti LAN.

3.3 Authenticator

Konfigurační část Authenticator blíže specifikuje parametry pro port v režimu **Pae Authenticator**. Pro každý port je možné nastavit různé parametry.



	Port control	Quiet period	Tx period	Supp timeout	Server timeout	Max req	Re-auth period	Re-auth enabled	KeyTx enabled
P1	Auto	60	30	30	30	2	3600		
P2	Auto	60	30	30	30	2	3600		
P3	Auto	60	30	30	30	2	3600		
P4	Auto	60	30	30	30	2	3600		
P5	Auto	60	30	30	30	2	3600		
G1	Auto	60	30	30	30	2	3600		
G2	Auto	60	30	30	30	2	3600		

Port Control

Force authorized - Zakáže proces ověřování 802.1x a způsobí přechod portu do autorizovaného stavu bez nutnosti výměny ověřování. Port vysílá a přijímá normální provoz bez ověřování klientů 802.1x.

Force unauthorized - Způsobí, že port zůstane v neautorizovaném stavu, ignoruje všechny pokusy klienta o ověření. Switch nemůže poskytovat ověřovací služby klientovi prostřednictvím portu. Port je ve stavu blokování.

Auto - Povoluje autentizaci 802.1x a způsobuje, že port začíná v neautorizovaném stavu. Odesílá a přijímání pouze rámce EAPOL. Proces autentizace začíná, když se změní stav portu z odpojeno na připojeno nebo když je přijat počáteční startovací rámec EAPOL start od klienta . Switch ověří totožnost klienta a začne předávat autentizační zprávy mezi klientem a ověřovacím serverem. Každý klient, který má přístup k síti, je switchem jedinečně identifikován pomocí MAC adresy.
Quiet period - Pokud switch nemůže ověřit klienta, zůstane nečinný po stanovenou dobu quiet period a poté se znovu pokusí o autentizaci. To se např. Používá, pokud dojde k selhání ověření klienta, protože klient poskytl neplatné heslo. Hodnotu lze měnit a uživateli tím poskytnout kratší dobu pro opětovný pokus autentizace nebo naopak tuto dobu prodloužit.

QuietPeriod je vlastně inicializační hodnota používaná pro časovač quietWhile (čas, během kterého se switch nepokouší ověřit klienta). Výchozí hodnota je 60, může být změněna v rozsahu od 0 do 65 535 s.

Tx period - Časovač používaný stavovým automatem PAE Authenticator k určení, kdy má být vyslán EAPOL PDU.

Je to čas, po který switch čeká na odpověď na rámec **EAP-request-identity** od klienta před opětovným odesláním požadavku.

Server timeout - Nastavuje dobu, po kterou switch čeká na odpověď serveru na požadavek na ověření. Pokud v nakonfigurovaném časovém rámci nepřijde odpověď, switch předpokládá, že pokus o ověření vypršel. V závislosti na aktuálním nastavení **max-req** switch buď odešle nový požadavek na server nebo ukončí ověřovací relaci.

Max-req - Nastavuje počet pokusů o ověření, které musí vypršet před tím, než se relace prohlásí za nepodařenou a autentizační sekvence je ukončena.

Re-auth period - Autentifikátor PAE může periodicky opakovat pokus o ověření bez nutnosti restartu mechanismu nebo připojení/odpojení portu. Čas opakování je dán hodnotou **Re-auth period** v sekundách od poslední úspěšné autorizace. Pokud je autentizace úspěšná, nedochází k výpadku dat.

Stavová proměnná **Re-auth enable** řídí, zda se provádí opakovaná autentizace.

Oprávnění lze povolit, zakázat a změnit dobu **Re-auth period**. Výchozí nastavení je 3600 s (jednu hodinu) a deaktivace opakované autentizace.

Re-auth enabled - Ovládací prvek pro povolení / zakázání (**enable / disable)** stavového automatu **Re-auth period**.

KeyTx enabled - Rámec EAPOL typu EAPOL-KEY, obsahující paket EAPOL-Key, je přenášen na klienta.
Automat Authenticator Key Transmit state machine přenáší EAPOL-Key PDU na klienta, jsou-li splněny všechny následující podmínky:

a) Port nepodléhá inicializaci.
b) Nastavení portControl je Auto.
c) Byl povolen přenos klíčů.
d) K dispozici jsou nové klíčové materiály pro přenos.

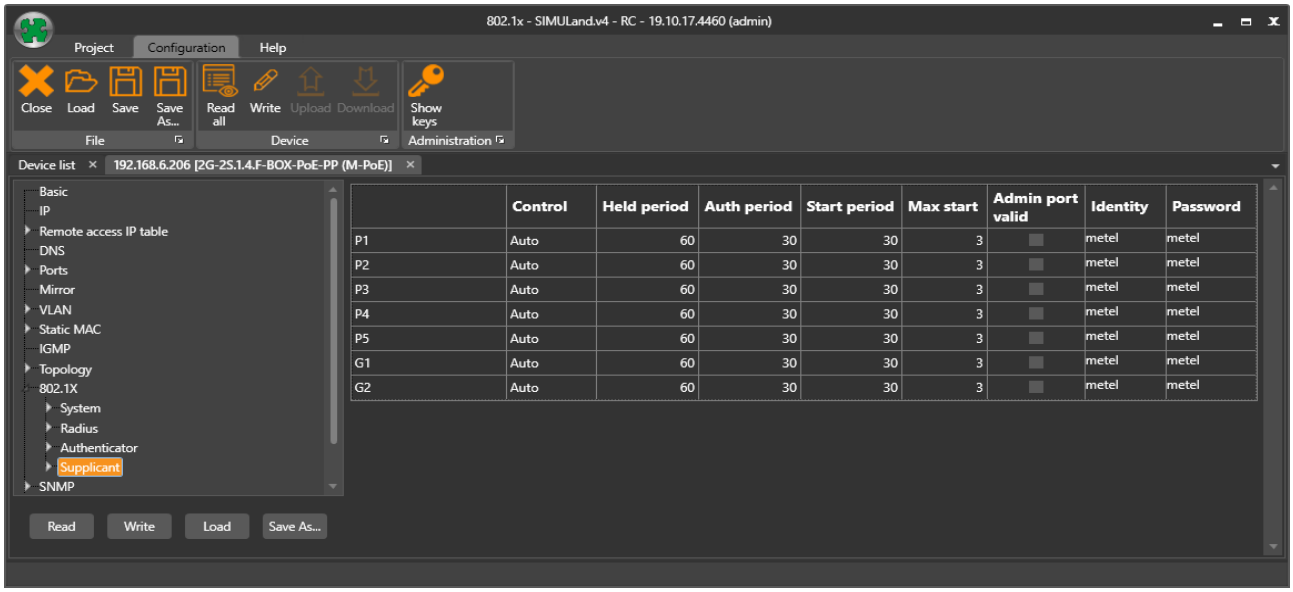
e) Stavový stroj autentizace backendu prohlásil keyRun, aby indikoval, že key machine může být spuštěný.

3.4 Supplicant

V části konfigurace **Supplicant** se blíže specifikují parametry portu v módu **Pae mode Supplicant** . Pro každý port je možné nastavit různé vlastnosti.

Supplicant je uživatel nebo klient (PC, kamera, switch ...), který chce být autentizován pro přístup do LAN.

Režim Supplicant implementovaný do switche umožňuje ověřovat switch stejně jako kteréhokoliv klienta nebo uživatele v síti.



	Control	Held period	Auth period	Start period	Max start	Admin port valid	Identity	Password
P1	Auto	60	30	30	3		metel	metel
P2	Auto	60	30	30	3		metel	metel
P3	Auto	60	30	30	3		metel	metel
P4	Auto	60	30	30	3		metel	metel
P5	Auto	60	30	30	3		metel	metel
G1	Auto	60	30	30	3		metel	metel
G2	Auto	60	30	30	3		metel	metel

Port Control
Používá se ve spojení s přepínáním mezi Auto a non-Auto (ForceAuthorized, ForceUnauthorized) provozním režimem stavového automatu PAE. Tato proměnná může nabývat následujících hodnot:

> **Force Unauthorized** - Je vyžadováno, aby byl kontrolovaný port držen v neoprávněném stavu. V tomto stavu blokuje port všechny pakety.
>
> **Force Authorized** - Vyžaduje se, aby kontrolovaný port byl držen v autorizovaném stavu. V tomto stavu port přeposílá všechny pakety.
>
> **Auto** - Port je nastaven do stavu Autorizovaný nebo Neoprávněný v souladu s výsledkem výměny autentizace mezi klientem a autentifikačním serverem.

Held period - Inicializační hodnota použitá pro held timer. Výchozí hodnota je 60 s. Held timer se spustí, když klient obdrží zprávu o selhání ověřování od switche nebo pokud je počet pokusů o ověření větší než **Max start** čítač.

Auth period - Inicializační hodnota použitá pro časovač **Auth period**. Výchozí hodnota je 30 s. Časovač používaný PAE mechanismem klienta k určení, jak dlouho má čekat na požadavek od autentifikátora (switche) před vypršením časového limitu.

Start period - Inicializační hodnota použitá pro časovač **Start period**. Výchozí hodnota je 30 s. Paket EAPOL-Start je vyslán klientem a je spuštěn časovač **Start period**, aby způsobil opakovaný přenos, pokud nebyla přijata žádná odpověď z autentifikátoru (switche). Pokud vyprší časovač **Start period**, přenos se opakuje až do maxima **Max start** přenosů.

Max start - Maximální počet po sobě jdoucích zpráv EAPOL-Start, které budou odeslány, než klient začne předpokládá, že není přítomen žádný autentifikátor. Výchozí hodnota je 3.

Admin port valid – Defaultní hodnota je FALSE. Pokud je hodnota změněna na TRUE a po vypršení **Max start** čítače není přijata žádná odpověď od authenticatoru, stavový automat předpokládá, že je připojen k systému, který nepodporuje EAPOL (802.1x), a přechází do stavu **AUTHENTICATED** (forwarding).

Username - Klient používá toto uživatelské jméno, když odpovídá na požadavky authenticatora 802.1X. Uživatelské jméno může být dlouhé 1 až 64 znaků. Jsou povoleny znaky ASCII, které zahrnují velká a malá písmena abecedy, číslice a všechny speciální znaky kromě uvozovek.

Password – Klient používá toto heslo v protokolu MD5, když odpovídá na požadavky authenticatora 802.1X. Heslo může mít délku 1 až 64 znaků. Jsou povoleny znaky ASCII, které zahrnují velká a malá písmena abecedy, číslice a všechny speciální znaky kromě uvozovek.

Implementovaný algoritmus metody EAP, který se má použít pro šifrování uživatelských jmen a hesel ověřování, je MD5 (hash funkce definovaná v RFC 3748, která poskytuje základní zabezpečení).