

Reference: NEW_802.1x_C
onfiguration_CZ
.docx

Issue: 1.1

Date: 03.04.2025

Aplikační poznámky
Konfigurace IEEE 802.1X



Protokol

Application Note

Konfigurace IEEE 802.1x

Obsah

1	Úvod.....	3
1.1	Účel.....	3
1.2	Rozsah.....	3
2	Porozumění 802.1x autentizaci	4
2.1	Topologie	4
2.2	802.1x Sekvence	5
2.2.1	Zahájení relace (Initiation).....	5
2.2.2	Ověření relace (Authentication).....	5
2.2.3	Oprávnění k relaci (Authorization).....	6
2.2.4	Relace účtu (Accounting).....	6
3	Konfigurace.....	7
3.1	SIMULand.v4	7
3.1.1	System (Globální povolení 802.1x)	8
3.1.2	Pae (Port mód)	9
3.1.3	Radius (Konfigurace autorizačního serveru)	10
3.1.4	Authenticator.....	12
3.1.5	Supplicant.....	14
3.2	Příkazový řádek.....	15
3.2.1	Globální povolení/zákaz 802.1x	15
3.2.2	Nastavení radius serveru na zařízení.....	16
3.2.3	Nastavení port mode (PAE) – Supplicant/Authenticator	17
3.2.4	Port Authenticator	17
3.2.5	Port Supplicant.....	18
3.2.6	Ukázka základní konfigurace 802.1x.....	18

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 switchu 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:



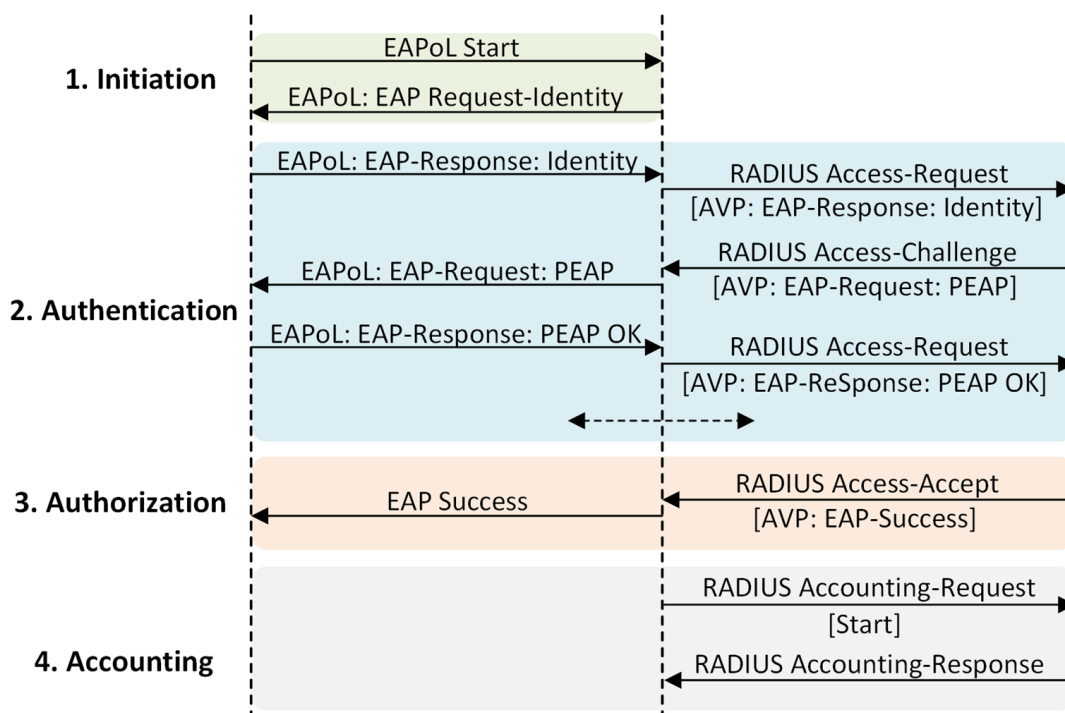
Supplicant: Subjekt na jednom konci segmentu LAN typu point-to-point, který se snaží být ověřen subjektem Authenticator připojeným k druhému konci tohoto spojení.

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 nepřímou 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.

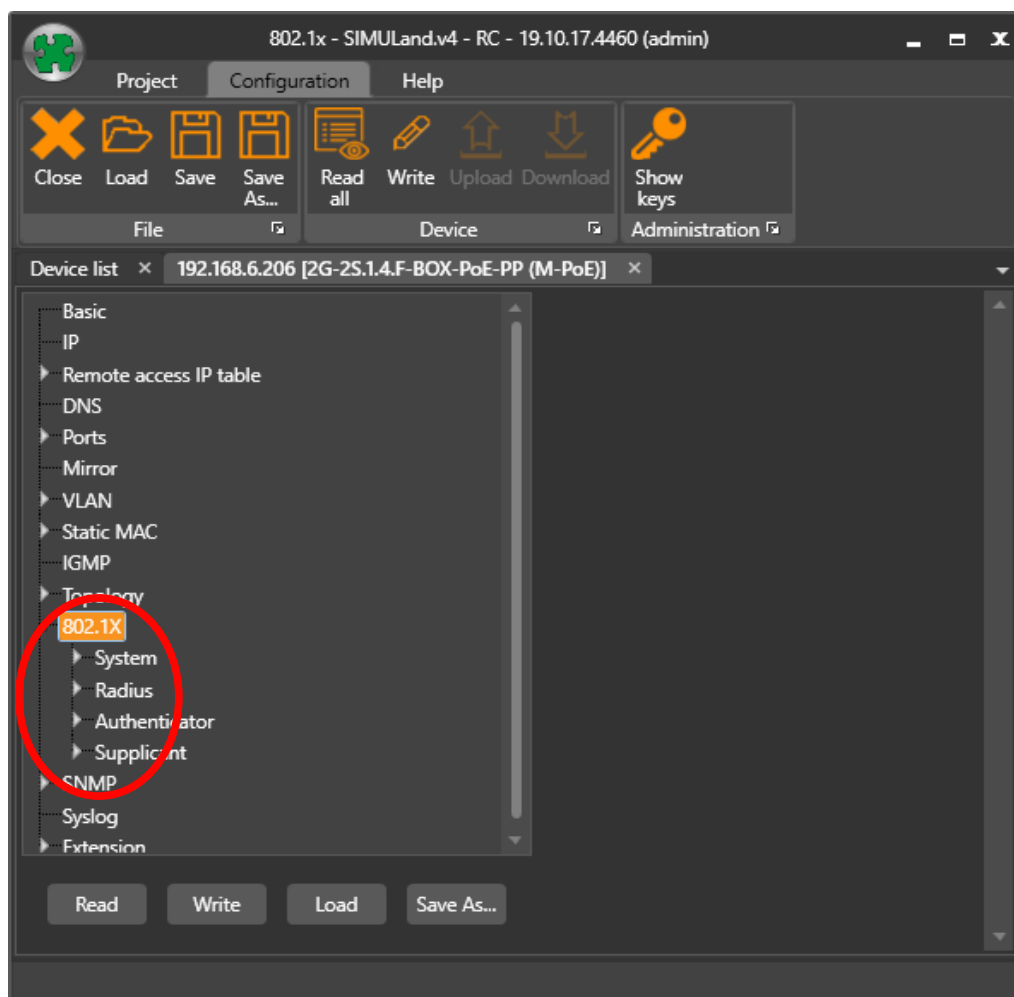
2.2.4 Relace účtu (Accounting)

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 konfiguraci IEEE 802.1x.

3.1 SIMULand.v4



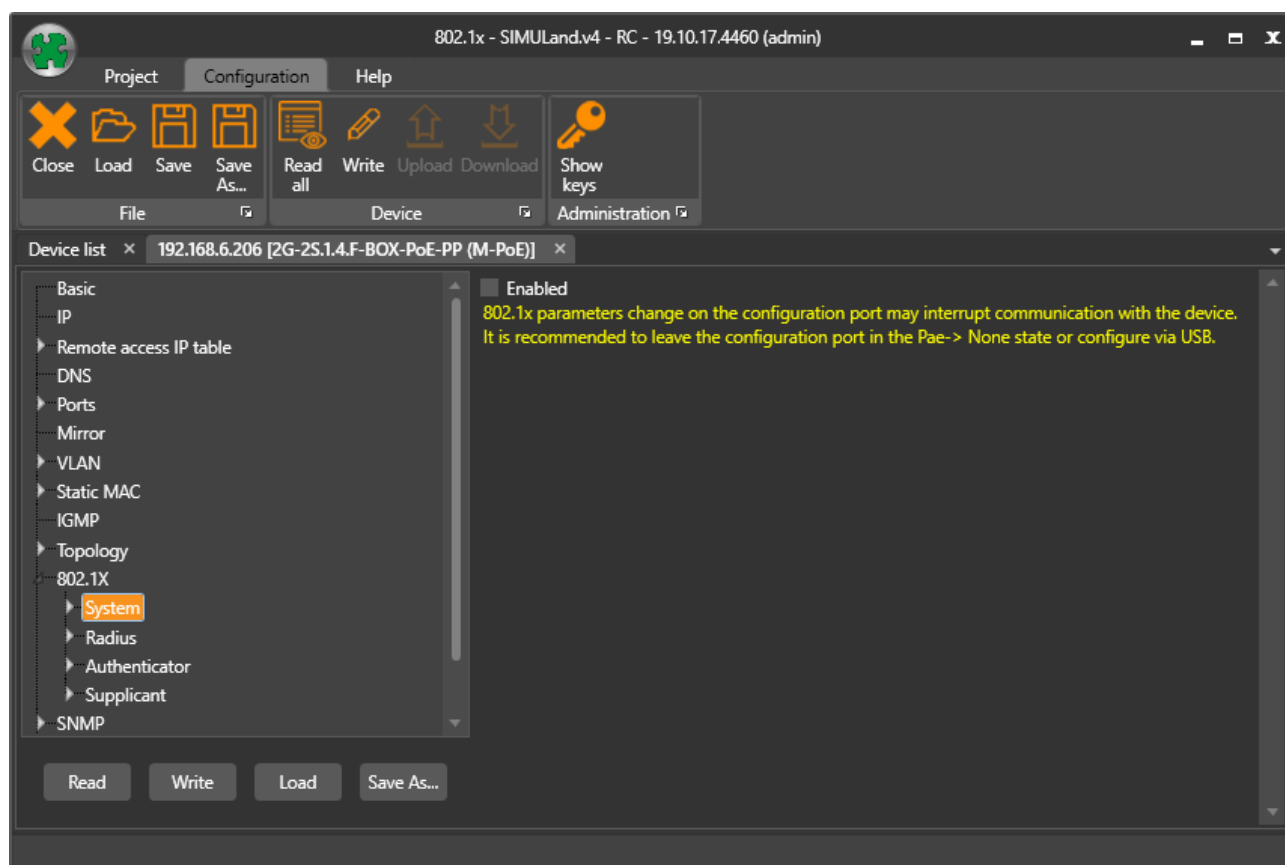
- **System** – Globální povolení 802.1x autorizace. Port mód (None, Authenticator, Supplicant).
- **Radius** – Konfigurace navázání spojení s autorizačním serverem.
- **Authenticator** – Konfigurace chování switche jako Authenticator.
- **Supplicant** – Konfigurace chování switche jako Supplicant.

3.1.1 System (Globální povolení 802.1x)

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

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.

Nezaškrtnuto - 802.1x je zakázáno na všech portech.



3.1.2 Pae (Port mód)

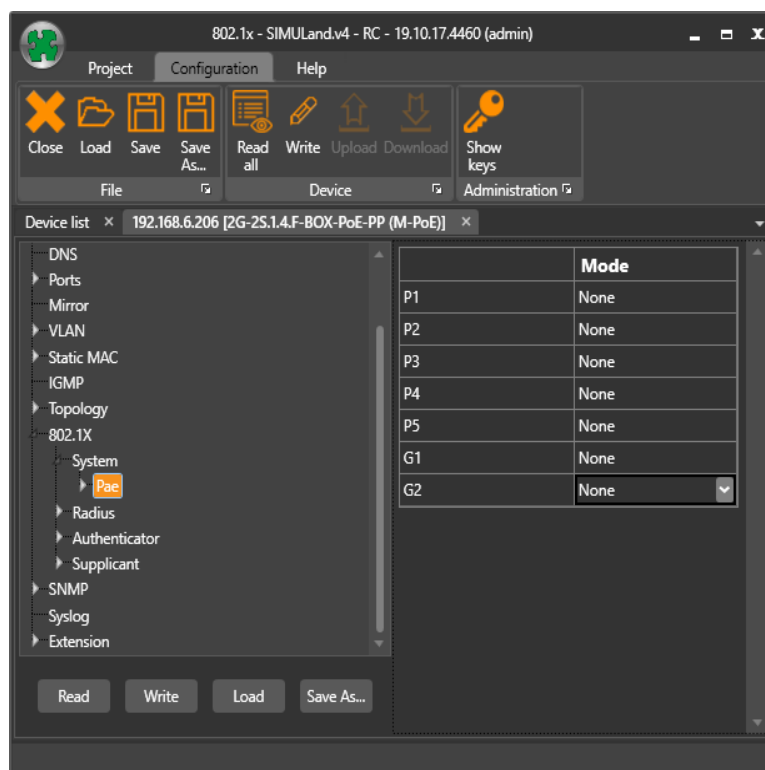
Každému portu switchu je možné nastavit rozdílný mód. Switch podporuje následující módy: **None**, **Authenticator**, **Supplicant**.

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

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 dělají, aniž by prozkoumaly záhlaví EAP v rámci.

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



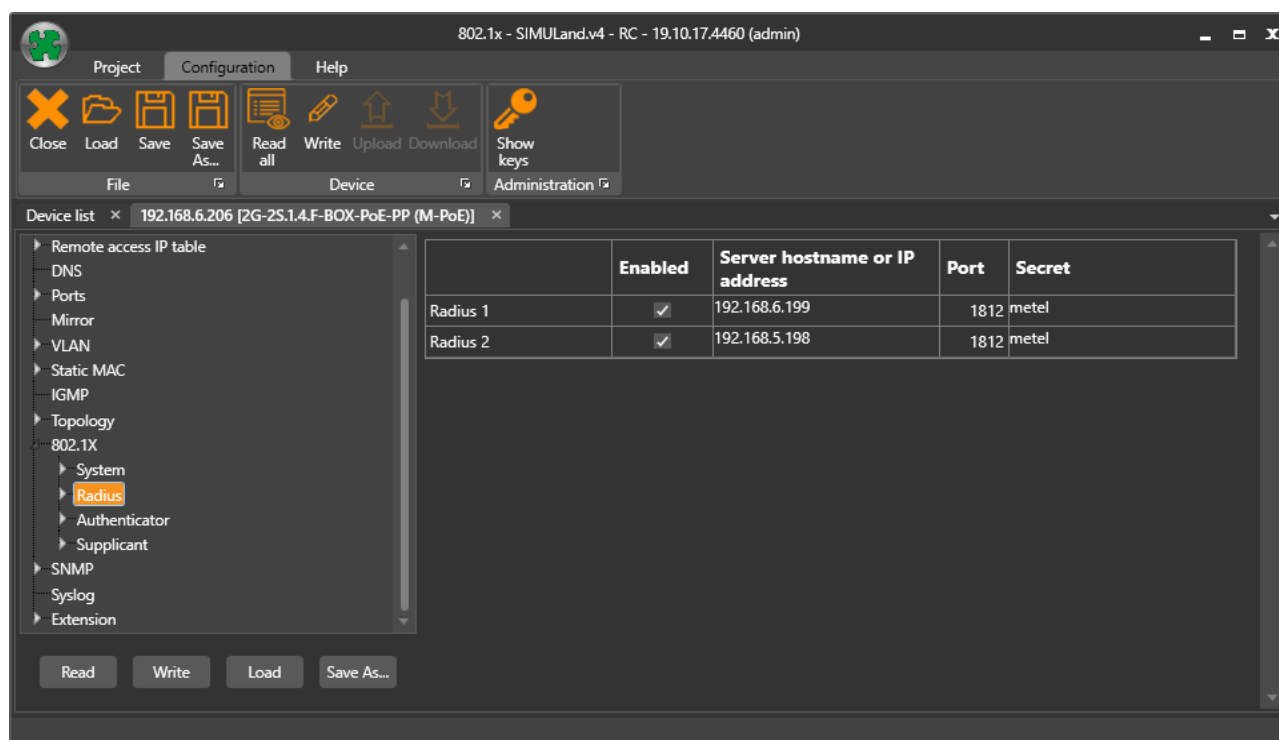
3.1.3 Radius (Konfigurace autorizačního serveru)

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

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.



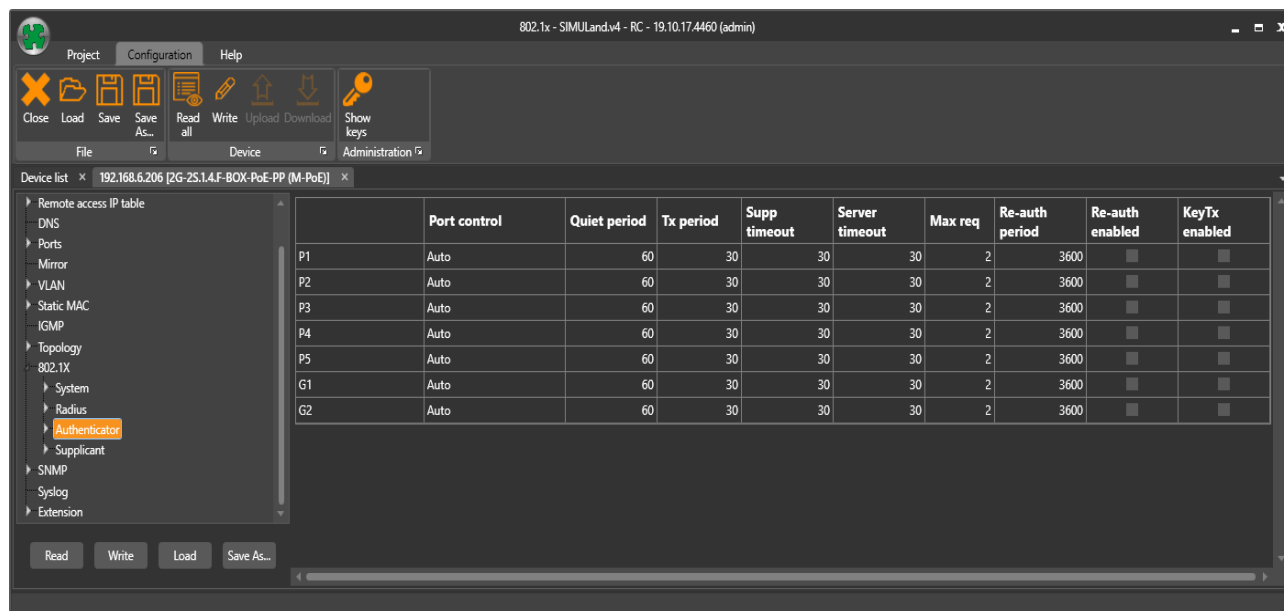
Radius server sekvence

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.

3.1.4 Authenticator

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



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 přijímá 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.

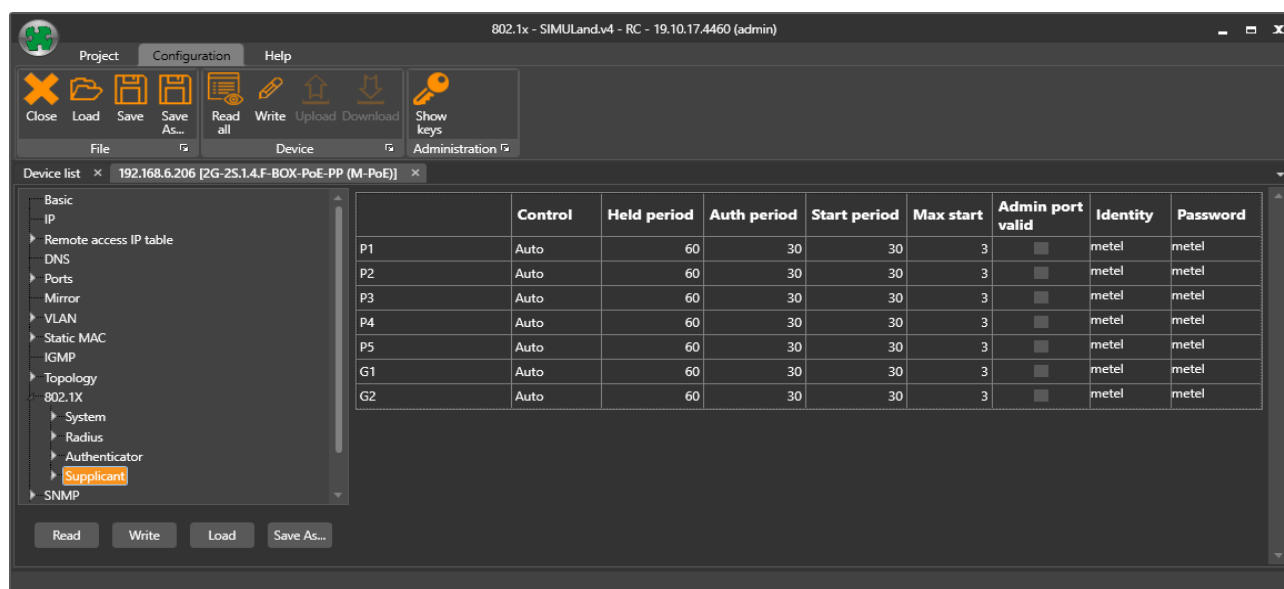
- b) Nastavení portControl je Auto.
- c) Byl povolen přenos klíčů.
- d) K dispozici jsou nové klíčové materiály pro přenos.
- e) Stavový stroj autentizace backendu prohlásil keyRun, aby indikoval, že key machine může být spuštěn.

3.1.5 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 switchu umožňuje ověřovat switch stejně jako kteréhokoliv klienta nebo uživatele v síti.



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 switchu 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 autentifikátoru (switchu) 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 (switchu). 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 předpokládat, 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 authenticatoru 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 authenticatoru 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).

Tato sekce popisuje základní konfiguraci IEEE 802.1x.

3.2 Příkazový řádek

- Vychází ze SIMULand.v4, v kapitole [4.1](#) jsou parametry popsány podrobněji
- Pro nastavení 802.1X uživatel pracuje v konfiguračním módu zařízení

3.2.1 Globální povolení/zákaz 802.1x

- Pro globální povolení funkce 802.1x použijeme příkaz `dot1x enable`
 - Veškerá konfigurace na portech týkající se 802.1X se stane aktivní ()
- V opačném případě `dot1x disable`

- Funkce 802.1x přestane fungovat, konfigurace radius serveru a konfigurace na portech se zachová

3.2.2 Nastavení radius serveru na zařízení

Používáme příkaz **radius**,

Příkaz požaduje vybrat konfiguraci primárního a záložního serveru

- **radius server1** -primární
- **radius server2** -záložní server, užívá se v případě, že komunikace se server1 selhala

Každý ze serverů má řadu vlastností, které jsou potřeba nastavit pro správné fungování

- **disable** – Zákaz funkce 802.1x, aby používala mnou vybraný server k autorizaci (ve výchozím nastavení je server disable)
- **enable** – Povolení užívání vybraného serveru k autorizaci 802.1x
- **host** – Nastavení adresy serveru. Lze IP formát, nebo lze užít i doménové jméno při konfiguraci DNS.
- **key** – Nastavení klíče k autorizačnímu serveru
 - **code** – V případě že už máte heslo ve formátu BASE32
 - **base32** – Nejběžnější užití, heslo se zadává v čitelné podobě, na pozadí se převede a uloží ve formátu BASE32
 - **none** – vymazání klíče
- **timeout** – Určuje maximální dobu (v sekundách), po kterou zařízení čeká na odpověď od serveru (výchozí hodnota je 30s)

Konfigurace může vypadat následovně:

```
(config)# radius server1 host 10.55.36.1
(config)# radius server1 key base32 STRONG_PASSWORD
(config)# radius server1 timeout 10
```

3.2.3 Nastavení port mode (PAE) – Supplicant/Authenticator

Tentokrát se nacházíme v konfiguraci konkrétního portu ((`config-port-P2`)#). Všechny porty jsou ve výchozím stavu jako `pae-mode-none` a žádné ověřování zde neprobíhá.

Pro změnu lze vyvolat příkazy

- `pae-mode-supp` – nastavení portu jako supplicant
- `pae-mode-auth` – nastavení portu jako authenticator
- `pae-mode-none` – ověřování bude na portu vypnuto

3.2.4 Port Authenticator

Přesný popis hodnot je u kapitoly [3.1.4](#)

`force-auth` – Port control

`force-auto` – Port control

`force-unauth` – Port control

`reauth-enable` – Povolení funkce re-auth

`reauth-disable` – Zakázání funkce re-auth

`keytx-enable` – Povolení KeyTx

`keytx-disable` – Zakázání KeyTx

`quiet-period` – Nastavení hodnoty Quiet period

`tx-period` – Nastavení hodnoty Tx period

`reauth-period` – Nastavení hodnoty Re-auth period

`supp-timeout` – Nastavení hodnoty Supp timeout

`server-timeout` – Nastavení hodnoty Server timeout

`max-request` – Nastavení maximálního počtu pokusů o ověření

3.2.5 Port Supplicant

Přesný popis hodnot je u kapitoly [3.1.5](#)

force-auth – Port control

force-auto – Port control

force-unauth – Port control

admin-valid – Zapnutí admin portu (ve výchozím stavu je vypnut)

admin-invalid – Vypnutí admin portu

identity – Nastavení identity (username) zařízení pro následné ověření

password – Nastavení hesla pro následné ověřování

code – V případě že už máte heslo ve formátu BASE32

base32 – Nejběžnější užití, heslo se zadává v čitelné podobě, na pozadí se převede a uloží ve formátu BASE32

none – vymazání klíče

held-period – Nastavení hodnoty Held period-

auth-period – Nastavení hodnoty Auth period

start-period – Nastavení hodnoty Start period

max-start – Nastavení hodnoty Max start

3.2.6 Ukázka základní konfigurace 802.1x

Zařízení je supplicant na portu P2:

```
(config)# radius server1 host 10.55.36.1
(config)# radius server1 key base32 STRONG_PASSWORD1
(config)# dot1x enable
(config)# port P1
(config-port-P1)# pae-mode-supp
(config-port-P1)# dot1x-supp identity metel
(config-port-P1)# dot1x-supp password base32 STRONG_PASSWORD2
```

Zařízení je autentifikátor na portu P2:

```
(config)# radius server1 host 10.55.36.1
(config)# radius server1 key base32 STRONG_PASSWORD1
(config)# dot1x enable
(config)# port P1
(config-port-P1)# pae-mode-auth
```