Protokoły

Nota Aplikacyjna

Konfiguracja IEEE 802.1x

Spis treści

1 Wstęp

1.1 Cel

W tym dokumencie opisano, jak skonfigurować uwierzytelnianie oparte na portach IEEE 802.1x w urządzeniach METEL, aby uniemożliwić nieautoryzowanym urządzeniom (klientom) dostęp do sieci oraz podstawowe informacje o protokole IEEE 802.1x.

1.2 Zakres

Ten dokument opisuje

- Zasady uwierzytelniania 802.1X
- Konfigurację przełączników METEL s.r.o.

2 Zasady uwierzytelniania 802.1X

Implementacja METEL s.r.o. jest zgodna z:

IEEE Std 802.1X™- 2004

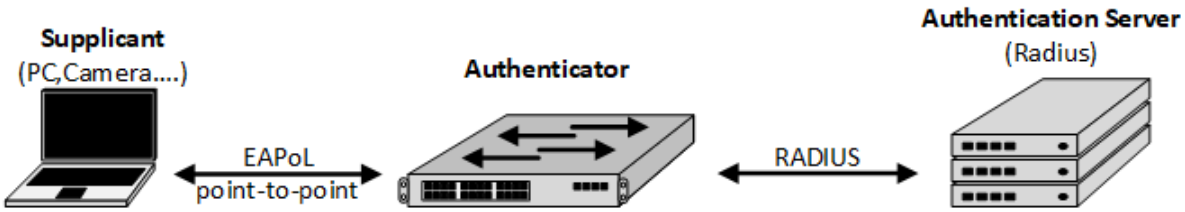
(Revision of IEEE Std 802.1X-2001)

Standard IEEE 802.1x definiuje w oparciu o technologię klient – serwer kontrolę dostępu i protokół uwierzytelniania, który ogranicza nieautoryzowanym klientom łączenie się z siecią LAN za pośrednictwem publicznie dostępnych portów. Serwer uwierzytelniający autoryzuje każdego klienta podłączonego do portu przełącznika i przypisuje port do sieci VLAN przed udostępnieniem jakichkolwiek usług oferowanych przez przełącznik lub sieć LAN.

Podczas procesu uwierzytelniania, kontrola dostępu 802.1X zezwala jedynie na ruch danych w porcie do którego jest podłączony klient w ramach protokołu Extensible Authentication Protocol over LAN (EAPOL). Po uzyskaniu autoryzacji, normalny ruch poprzez port jest dostępny.

2.1 Topologia

802.1x definiuje poniższe trzy wymagane komponenty:



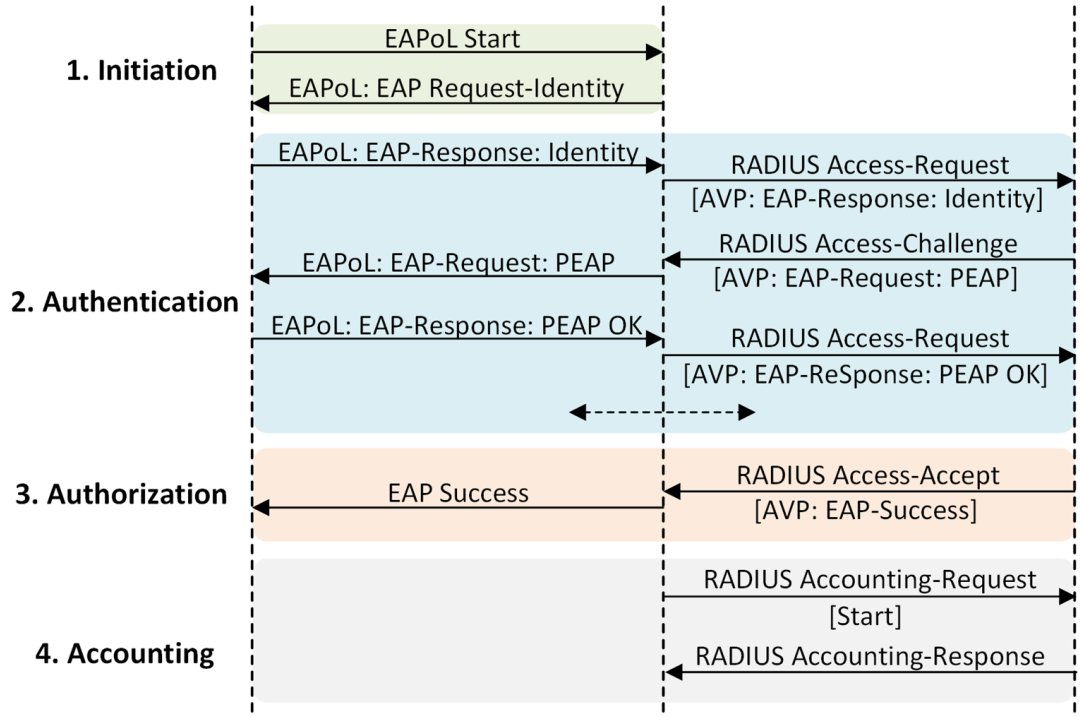
Supplicant: Jednostka na jednym końcu segmentu typu punkt – punkt sieci LAN, która chce zostać uwierzytelniona przez Authenticator dołączony do drugiego końca tego łącza.

Authenticator: Jednostka na jednym końcu segmentu typu punkt – punkt sieci LAN, która pomaga w uwierzytelnianiu jednostki podłączonej do drugiego końca tego łącza.

Authentication Server: Podmiot zapewniający usługę uwierzytelniania dla Authenticatora. Usługa ta określa, na podstawie poświadczeń podanych przez Dostawcę, czy jest on uprawniony do dostępu do usług świadczonych przez system, w którym znajduje się Authenticator.

2.2 802.1x Sekwencja

Przykład sekwencji 802.1x:



2.2.1 Inicjacja sesji

Uwierzytelnianie 802.1X może być inicjowane przez przełącznik lub suplikanta. Z perspektywy przełącznika sesja uwierzytelniania rozpoczyna się, gdy przełącznik wykryje łącze w porcie. Przełącznik inicjuje uwierzytelnianie, wysyłając komunikat **EAP-Request-Identity** do suplikanta. Jeśli przełącznik nie otrzyma odpowiedzi, retransmituje to żądanie w stałych odstępach czasu.
Suplikant może zainicjować uwierzytelnienie, wysyłając ramkę **EAPoL-Start**. Komunikat **EAPoL-Start** umożliwia suplikantom przyśpieszenie procesu uwierzytelniania bez oczekiwania na następny okresowy **EAP-Request-Identity** z przełącznika. Komunikaty **EAPoL-Start** są wymagane w sytuacjach, gdy suplikant nie jest gotowy do przetworzenia **EAP-Request** z przełącznika (na przykład, gdy system operacyjny wciąż się uruchamia); lub gdy nie ma fizycznej zmiany stanu łącza na przełączniku (na przykład, gdy suplikant jest połączony pośrednio przez telefon IP lub hub).

2.2.2 Uwierzytelnienie Sesji

Podczas tego etapu przełącznik przekazuje komunikaty EAP między suplikantem a serwerem uwierzytelniającym, kopiując komunikat EAP w ramce EAPoL do pary AV w pakiecie RADIUS i odwrotnie. W przykładowej części wymiany suplikant i serwer uwierzytelniający zgadzają się na metodę EAP (PEAP).

Resztę wymiany określa wybrana metoda EAP. Metoda EAP określa typ referencji, która ma być używana do sprawdzania tożsamości suplikanta oraz sposób, w jaki referencja jest przesyłana. W zależności od metody suplikant może przesłać hasło, certyfikat, token lub inne dane uwierzytelniające. Poświadczenie to może być następnie przekazane do szyfrowanego tunelu TLS, jako wynik działania funkcji skrótu lub w innej chronionej formie.

2.2.3 Autoryzacja Sesji

Jeśli suplikant prześle prawidłowe poświadczenie, serwer uwierzytelniający zwróci komunikat **RADIUS Access-Accept** zamknięty w komunikacie **EAP-Success**. Wskazuje to przełącznikowi, że suplikant powinien mieć dostęp do portu. Opcjonalnie serwer uwierzytelniania może dołączać instrukcje dynamicznej polityki dostępu do sieci (na przykład dynamiczną sieć VLAN lub ACL) w komunikacie **Access-Accept**. W przypadku braku instrukcji dynamicznych zasad przełącznik po prostu otwiera port.

Jeśli suplikant prześle nieprawidłowe dane uwierzytelniające lub ze względu na zasady uwierzytelniania nie może uzyskać dostępu do sieci, serwer uwierzytelnienia zwraca komunikat **RADIUS Access-Reject** zawierający komunikat **EAP-Failure**. Wskazuje to przełącznikowi, że suplikant nie powinien mieć dostępu do portu. W zależności od konfiguracji przełącznika może on ponowić uwierzytelnianie, ustawić port w tryb Auth-Fail VLAN lub wypróbować alternatywną metodę uwierzytelniania.

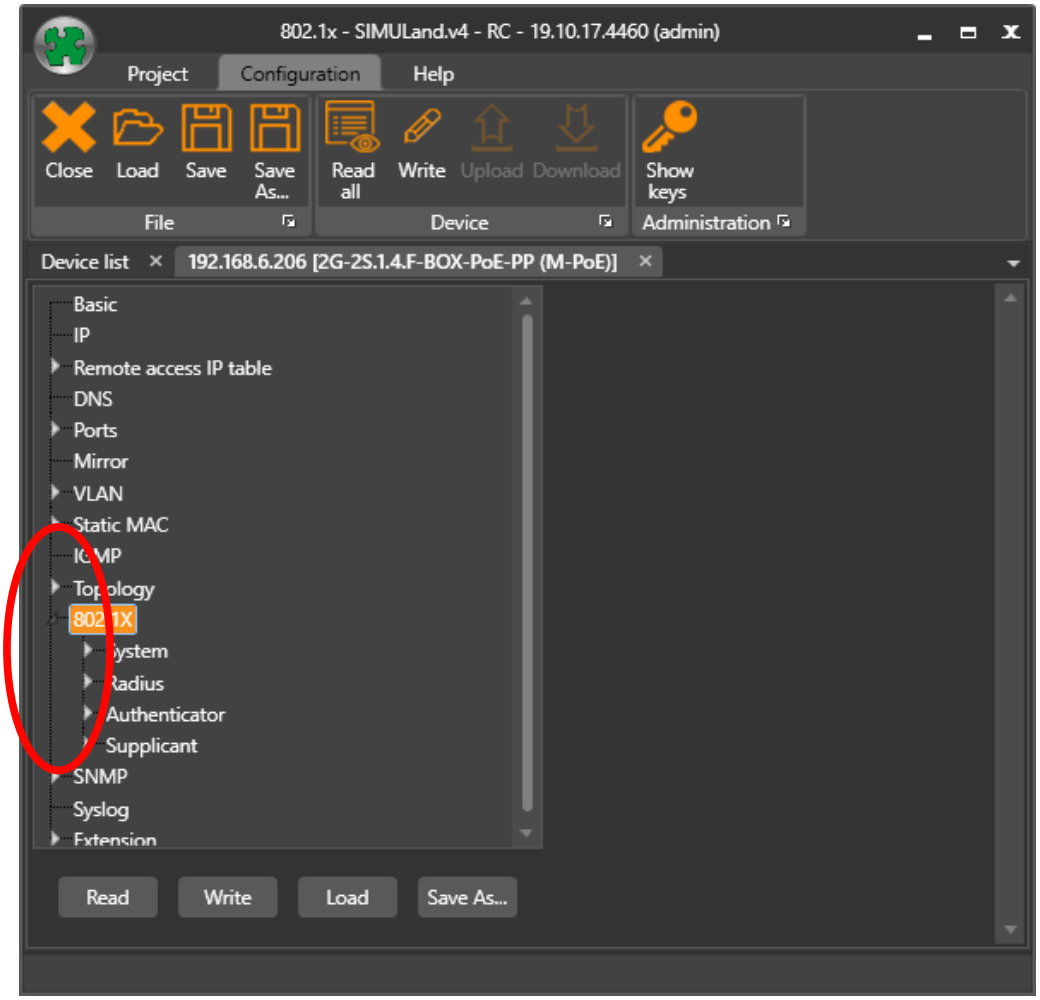
2.2.4 Dokumentowanie Sesji

Jeśli przełącznik może pomyślnie zastosować zasady autoryzacji, może wysłać do serwera uwierzytelniającego komunikat RADIUS Accounting-Request ze szczegółowymi informacjami na temat autoryzowanej sesji. Komunikaty Accounting-Request są wysyłane zarówno dla sesji dynamicznie autoryzowanych, jak i sesji autoryzowanych lokalnie; na przykład Guest VLAN i Auth-Fail VLAN.

3 Konfiguracja

Ten rozdział opisuje podstawową konfigurację IEEE 802.1x.

- **System** – Globalne zezwolenie na uwierzytelnianie 802.1x
- **Radius** – Konfiguracja parametrów serwera Radius
- **Pae** – Tryb pracy portu (None, Authenticator, Supplicant)
- **Authenticator** – Konfiguracja zachowania Authenticatora
- **Supplicant** – Konfiguracja zachowania suplikanta

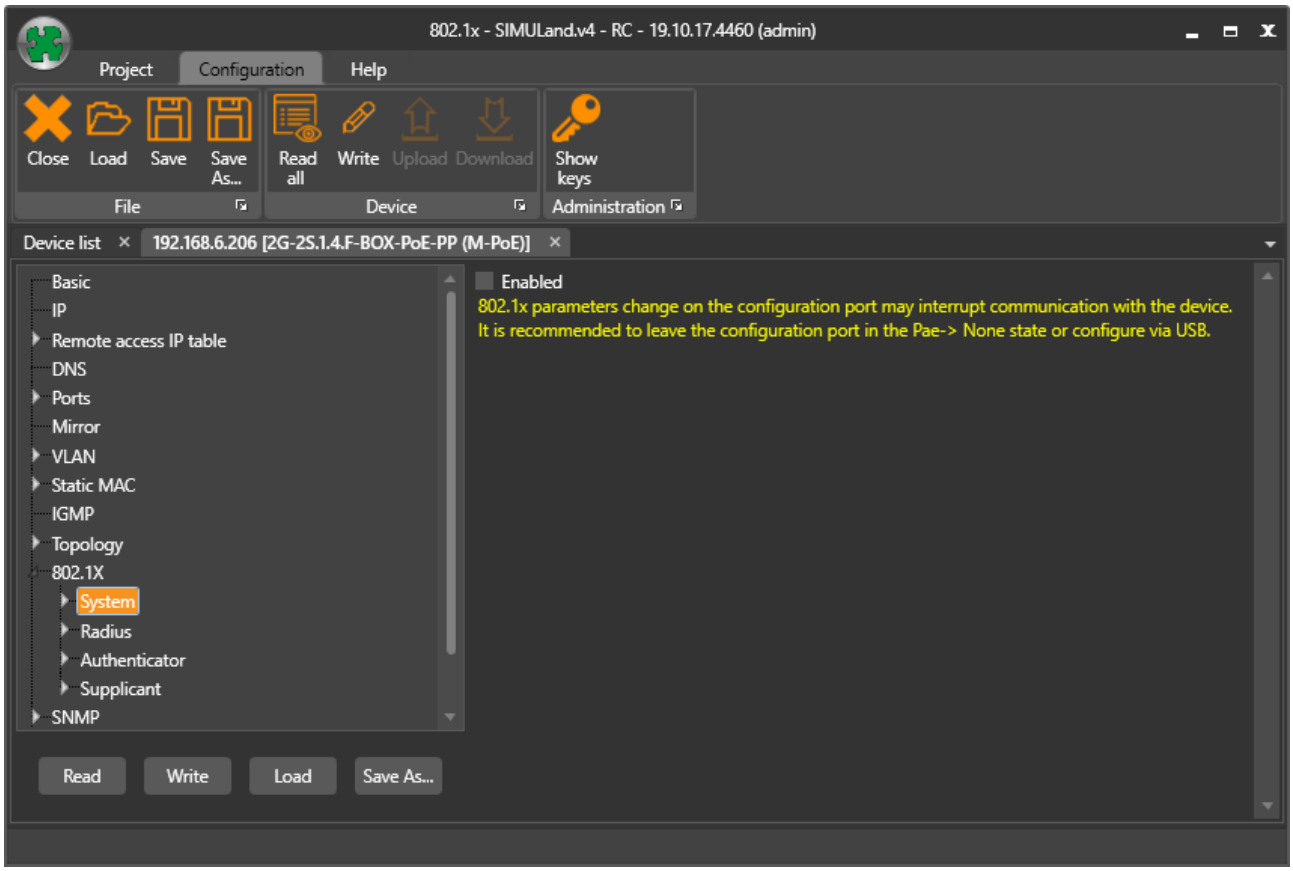


3.1 System (Globalne zezwolenie 802.1x)

Pole wyboru “**Enable”** w sekcji **802.1x -> System** globalnie zezwala lub zabrania stosowania 802.1x dla wszystkich urządzeń.

Zaznaczone - wszystkie parametry konfiguracyjne menu 802.1x (System, Radius, Pea, Authenticator, Supplicant) są aktywowane i ustawiane do użycia do uwierzytelniania nowo podłączanych klientów (suplikantów) do sieci LAN.

Odznaczone - 802.1x jest zabronione na wszystkich portach.



3.2 Pae (Tryb pracy portu)

Dla każdego portu przełącznika możliwe jest ustawienie różnego trybu pracy. Przełącznik wspiera tryby: **None, Authenticator, Supplicant**.

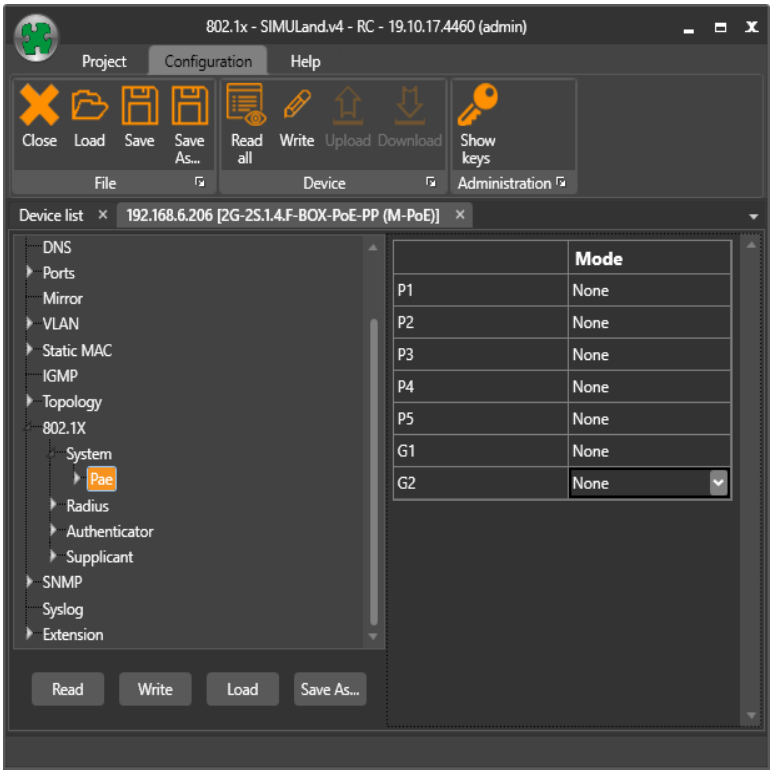
None - Port jest wyłączany z uwierzytelniania 802.1x i zachowuje się jak standardowy port przełącznika.

Authenticator - Włącza uwierzytelnianie 802.1x w interfejsie. Maszyny stanów PAE

Authenticatora komunikują się z jednostką wyższej warstwy, która zarządza funkcjami EAP i AAA. W Authenticatorze rola PAE polega na transporcie ramek EAP między suplikantem a jednostką Authenticatora wyższego poziomu oraz kontrolowaniem dostępu do portu na podstawie wyniku uwierzytelnienia. Maszyny stanu Authenticatora robią to bez sprawdzania nagłówka EAP w ramce.

Supplicant - Konfiguruje interfejs jako suplikant jednostki dostępu do portu (PAE). Maszyny stanu PAE suplikanta komunikują się z pojedynczą jednostką wyższej warstwy: EAP. W przypadku suplikanta rola PAE polega na transporcie ramek EAP między siecią a wyższą warstwą oraz opcjonalnym kontrolowaniem dostępu do portu na podstawie wyniku uwierzytelnienia. Maszyny stanów suplikanta robią to bez sprawdzania nagłówka EAP w ramce.

Sekcja **Pae** jest nadrzędna w stosunku do sekcji **Authenticator** i **Supplicant**!



3.3 Radius (Konfiguracja serwera)

Serwer Radius (Authentication) sprawdza i potwierdza tożsamość podłączonych klientów (suplikantów) i powiadamia przełącznik, czy klient może zostać upoważniony do dostępu do sieci LAN lub usług przełączników.

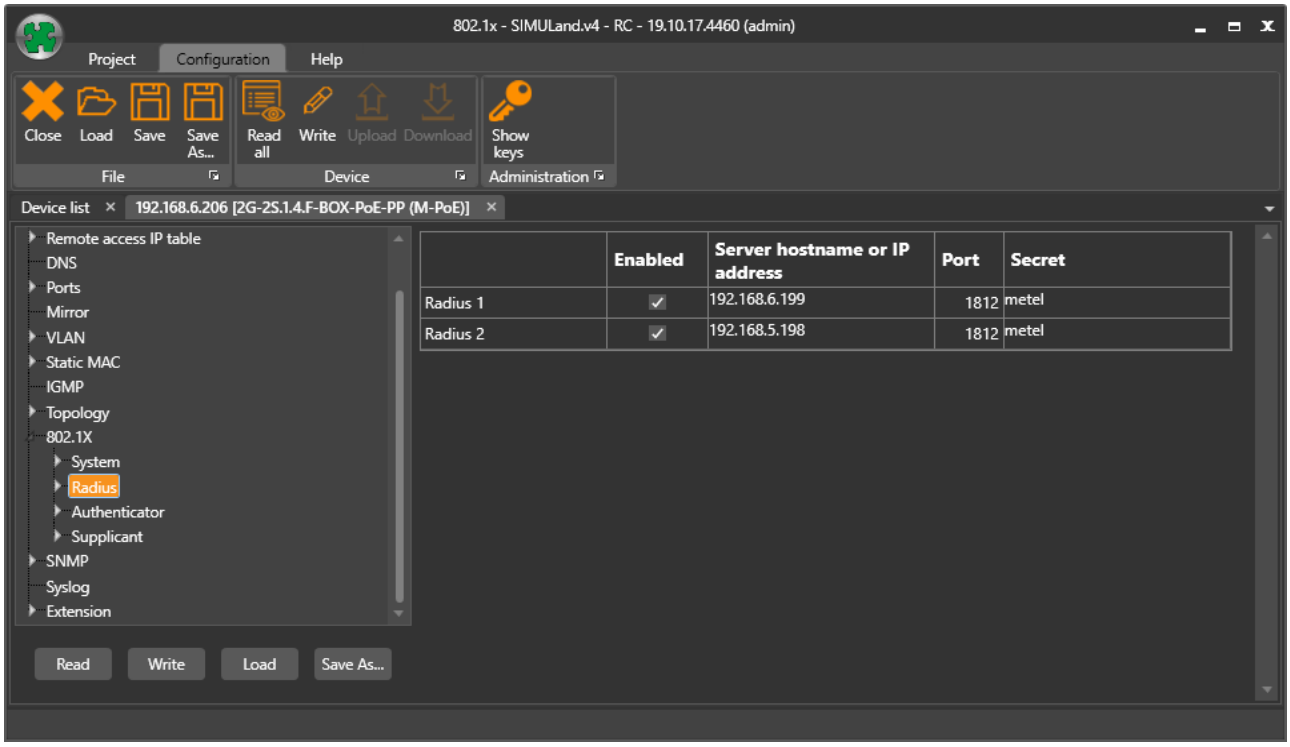
W przypadku, gdy port jest skonfigurowany jako **Authenticator**, do pomyślnego skonfigurowania uwierzytelniającego serwera radius potrzebne są:

Enabled - Zaznaczone – Włącza serwer Radius.
Odznaczone – Wyłącza serwer Radius.

Port - Ustawia port UDP/TCP dla uwierzytelniania (domyślnie 1812).

Secret - Określa klucz uwierzytelniania i szyfrowania używany między przełącznikiem a demonem RADIUS działającym na serwerze Radius. Zarówno przełącznik (urządzenie uwierzytelniające), jak i serwer Radius muszą być skonfigurowane do korzystania z tego samego wspólnego hasła.

Server Hostname or IP Address – Nazwa serwera Radius lub adres IP.



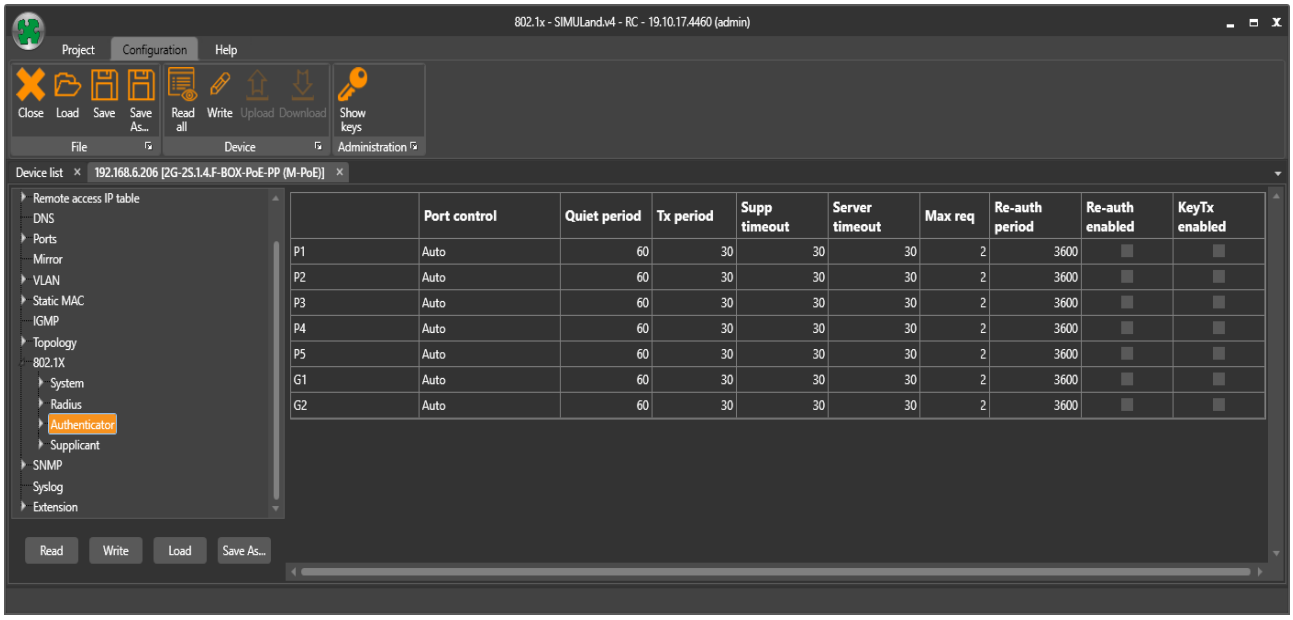
Sekwencja serwera Radius

Konfiguracja serwera Radius w pierwszym wierszu (Radius 1) jest używana jako główny serwer Radius. Za każdym razem, gdy rozpoczyna się nowy proces uwierzytelniania, przełącznik próbuje wysłać dane uwierzytelniające do niego. Jeśli pierwszy serwer nie odpowie trzy razy (przerwa zależy od konfiguracji limitu czasu Authenticatora i serwera), przełącznik próbuje wysłać pakiety to drugiego (Radius 2).

Drugi jest zazwyczaj używany jako zapasowy dla pierwszego i podłączony lokalnie (nie poprzez sieć WAN).

3.4 Authenticator

Część konfiguracji Authenticatora bardziej szczegółowo określa parametry portu w trybie **Pae Authenticator**. Dla każdego portu można ustawić różne właściwości.



Port Control

Force authorized - Wyłącza proces uwierzytelniania 802.1x i powoduje przejście portu do stanu autoryzacji bez konieczności wymiany uwierzytelnienia. Port przesyła i odbiera normalny ruch bez uwierzytelniania klientów w standardzie 802.1x.

Force unauthorized - Powoduje, że port pozostaje w stanie nieautoryzowanym, ignorując wszystkie próby uwierzytelnienia klienta. Przełącznik nie może świadczyć usług uwierzytelniania dla klienta za pośrednictwem interfejsu. Port jest w stanie blokowania.

Auto - Włącza uwierzytelnianie 802.1x i powoduje, że port rozpoczyna pracę w stanie nieautoryzowanym, umożliwiając wysyłanie i odbieranie tylko ramek **EAPOL** przez port. Proces uwierzytelniania rozpoczyna się, gdy stan łącza portu przechodzi z dołu do góry lub po odebraniu ramki **EAPOL-start**. Przełącznik żąda tożsamości klienta i rozpoczyna przekazywanie komunikatów uwierzytelniających między klientem a serwerem uwierzytelniającym. Każdy klient próbujący uzyskać dostęp do sieci jest jednoznacznie identyfikowany przez przełącznik za pomocą adresu MAC klienta.

Quiet period - Gdy przełącznik nie może uwierzytelnić klienta, pozostaje bezczynny przez określony czas, a następnie próbuje ponownie. Komenda konfiguracji interfejsu **QuietPeriod** kontroluje okres bezczynności. Nieudane uwierzytelnienie klienta, może wynikać z podania nieprawidłowego hasła. Wprowadzając liczbę mniejszą niż domyślna, możesz zapewnić użytkownikowi krótszy czas reakcji.
W rzeczywistości **QuietPeriod** jest wartością inicjalizacyjną używaną dla timera quietWhile (czas, w którym nie będzie próbował dodać suplikanta). Jego domyślna wartość wynosi 60 s; może być ustawiony na dowolną wartość z zakresu od 0 do 65 535 s.

Tx period - Zegar używany przez maszynę stanów PAE Authenticatora do określania, kiedy ma zostać przesłana jednostka PDU EAPOL.

Czas oczekiwania przełącznika na odpowiedź na ramkę **EAP-request-identity** od klienta przed ponownym przesłaniem żądania.

Supp timeout - Ustawia czas oczekiwania przełącznika na odpowiedź suplikanta na żądanie EAP. Jeśli suplikant nie odpowie w skonfigurowanych ramach czasowych, sesja wygasa.

Server timeout - Ustawia czas oczekiwania przełącznika na odpowiedź serwera na żądanie uwierzytelnienia. Jeśli nie ma odpowiedzi w skonfigurowanym przedziale czasowym, przełącznik zakłada, że upłynął limit czasu próby uwierzytelnienia. W zależności od bieżącego ustawienia **max-req** przełącznik wyśle nowe żądanie do serwera lub zakończy sesję uwierzytelniania.

Max-req - Ustawia liczbę prób uwierzytelnienia z przekroczonym limitem czasu, które spowodują niepowodzenie uwierzytelnienia i zakończenie sesji uwierzytelniania.

Re-auth period - Authenticator PAEs może okresowo kończyć uznawanie stanu informacji o uwierzytelnieniu i za pomocą timera maszyny stanu ponowić uwierzytelnienie. Okres dla takich limitów czasu to **Re-auth period** w sekundach od ostatniego potwierdzenia stanu autoryzacji. Włączona zmienna stanu **Re-Auth** kontroluje, czy ma miejsce okresowe uwierzytelnianie.

Ponowne uwierzytelnienie może być włączane i wyłączane, a **Re-auth period** modyfikowane przez zarządzającego. Domyślne ustawienie 3600 s (jedna godzina) i ponowne uwierzytelnienie wyłączone.

Re-auth enabled - **enable / disable** włącza lub wyłącza timer maszyny stanu ponownego uwierzytelnienia.

KeyTx enabled - Ramka EAPOL typu EAPOL-KEY, zawierająca pakiet EAPOL-key, jest przesyłana do suplikanta.

Maszyna stanu Key Transmit Authenticatora przesyła EAPOL-Key PDUs do suplikanta, jeśli poniższe warunki są prawdziwe:

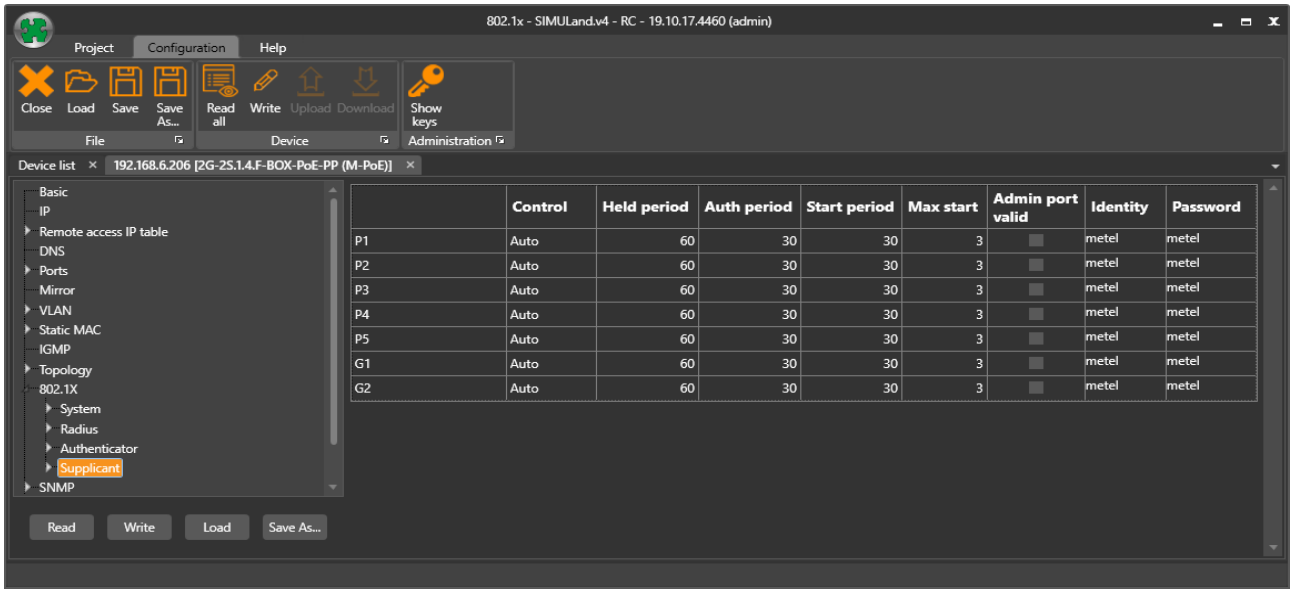
a) Port jest w trakcie inicjalizacji.
b) portControl jest ustawione na Auto.
c) Key transmission jest włączony.
d) Dostępny jest nowy kluczowy materiał do transmisji.
e) Maszyna stanu uwierzytelniania potwierdziła keyRun, aby wskazać, że maszyna klucza może działać.

3.5 Suplikant

Część konfiguracji Supplicant bardziej szczegółowo określa parametry portu w trybie **Pae mode Supplicant**. Dla każdego portu można ustawić różne właściwości.

Suplikant jest użytkownikiem lub klientem (PC, kamera, przełącznik…), który chce być uwierzytelniony dla dostępu do LAN.

Tryb Supplicant zastosowany w przełączniku pozwala uwierzytelnić przełącznik tak samo jak klienta lub użytkownika.



	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
Używany w połączeniu z przełączaniem między trybem automatycznym i nieautomatycznym (ForceAuthorized, ForceUnauthorized) maszyny stanu PAE Suplikanta. Ta zmienna może przyjmować następujące wartości:

Force Unauthorized - Kontrolowany port musi być utrzymywany w stanie nieautoryzowanym. W tym stanie port blokuje wszystkie pakiety.

Force Authorized - Kontrolowany port musi być utrzymywany w stanie autoryzacji. W tym stanie port przekazuje wszystkie pakiety.

Auto - Kontrolowany port jest ustawiany w stan Autoryzowany lub Nieautoryzowany zgodnie z wynikiem wymiany uwierzytelnienia między Suplikantem a Serwerem uwierzytelniającym.

Held period – Wartość inicjalizacji używana przez timer oczekiwania. Jego domyślna wartość to 60 s. Timer oczekiwania uruchamia się, gdy suplikant otrzyma komunikat o błędzie uwierzytelnienia Authenticatora (przełącznika) lub gdy prób uwierzytelnienia jest więcej niż licznik **Max start**.

Auth period - Wartość inicjalizacji używana przez timer okresu autoryzacji. Jego domyślna wartość to 30 s. Timer używany przez PAE Suplikanta do określania czasu oczekiwania na żądanie od Authenticatora przed wystąpieniem przekroczenia limitu czasu.

Start period - Wartość inicjalizacji używana przez timer **Start period**. Jego domyślna wartość to 30s. Pakiet EAPOL-Start jest przesyłany przez Suplikanta i uruchamiany jest timer **Start period**, aby spowodować retransmisję w przypadku braku odpowiedzi od Authenticatora. Jeśli upłynie czas zliczania timera **Start period**, transmisja zostanie powtórzona maksymalnie **Max start** razy.

Max start - Maksymalna liczba kolejnych komunikatów EAPOL-Start, które zostaną wysłane, zanim Suplikant założy, że nie ma Authenticatora. Jego wartość domyślna to 3.

Admin port valid – Jego wartość domyślna to FALSE. Jeśli zostanie zmieniona na TRUE, a po otrzymaniu **Max start** transmisji nie zostanie odebrana żadna odpowiedź od authenticatora, maszyna stanów założy, że jest podłączona do systemu, który nie rozpoznaje protokołu EAPOL, i przejdzie do stanu **AUTHENTICATED** (przekazywanie).

Username—Suplikant używa tej nazwy użytkownika podczas odpowiadania na żądania od Authenticatora 802.1X. Nazwa użytkownika może mieć od 1 do 64 znaków. Dozwolone są znaki drukowalne ASCII, w tym wielkie i małe litery, cyfry i wszystkie znaki specjalne z wyjątkiem cudzysłowów.

Password—Suplikant używa tego hasła MD5 podczas odpowiadania na żądania od Authenticatora 802.1X. Hasło może mieć od 1 do 64 znaków. Dozwolone są znaki drukowalne ASCII, w tym wielkie i małe litery, cyfry i wszystkie znaki specjalne z wyjątkiem cudzysłowów.

Zaimplementowanym algorytmem metody **EAP** do szyfrowania nazw użytkowników i haseł uwierzytelniających jest **MD5** (funkcja skrótu zdefiniowana w RFC 3748 zapewniająca podstawowe bezpieczeństwo).