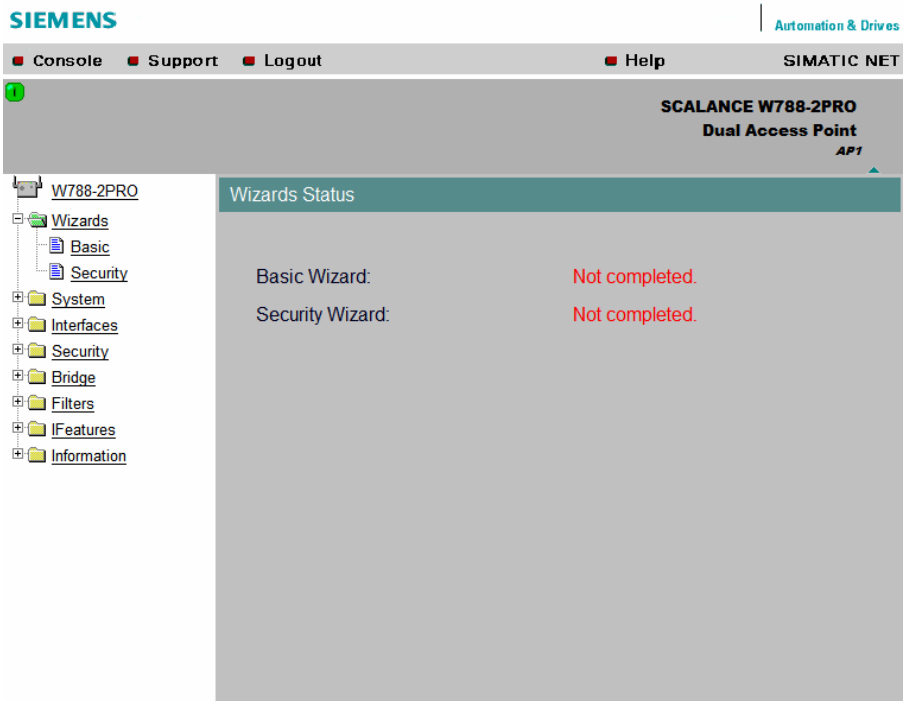
Moduł SCALANCE W788-xPRO – opis możliwości konfiguracyjnych.

Połączenie z modułem oraz podstawową parametryzację i zabezpieczenia za pomocą dostępnych w interfejsie urządzenia kreatorów opisano w dokumencie „SCALANCE W788-xPRO – konfiguracja podstawowa”.

Niniejszy dokument przedstawia szczegółowo wszystkie dostępne opcje ustawień SCALANCE W788-1PRO oraz SCALANCE W788-2PRO oraz tłumaczy ich działanie.

1. Zakłada „Wizards”.

Producent zadbał w swoim oprogramowaniu o specjalnie przegotowane kreatory podstawowych ustawień modułu.

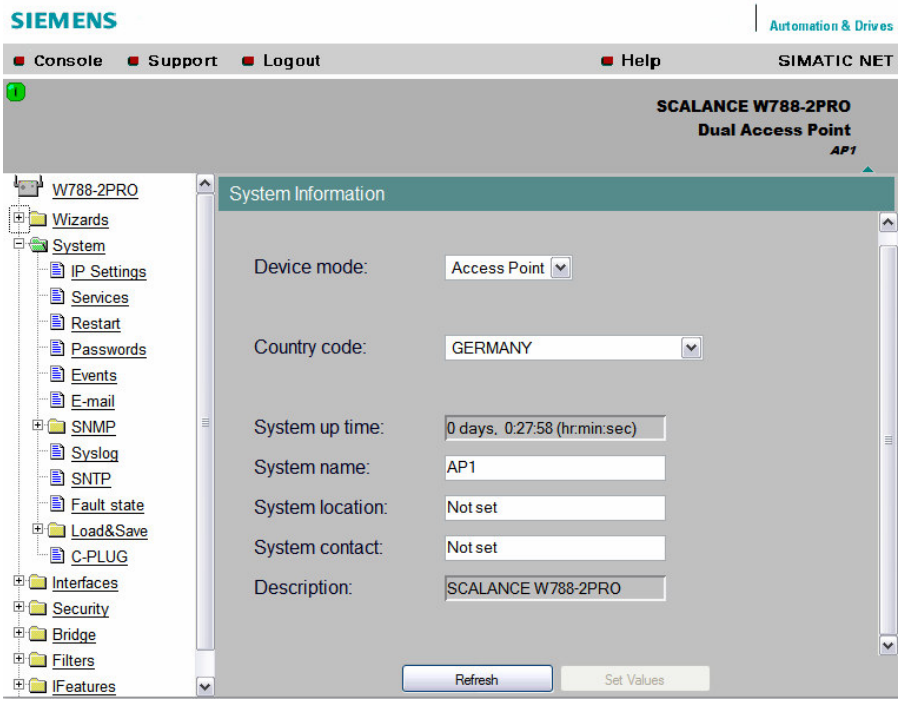


Opcja „Basic” pozwala na przeprowadzenie niezbędnej parametryzacji urządzenia do pracy w sieci.
Opcja „Security” pomaga nam w zabezpieczeniu dostępu do modułu oraz transmisji.

„Przejście” tych kreatorów powinno być pierwszym krokiem pełnej konfiguracji urządzenia.
Szczegółowy ich opis został przedstawiony w dokumencie „SCALANCE W788-xPRO – konfiguracja podstawowa”.

2. Zakładka „System”.

W zakładce „System” zawarte są opcje dotyczące działania oraz wykorzystywanych funkcji urządzenia.



System information

Do tego zestawu opcji przechodzimy bezpośrednio po kliknięciu w kartę „System”.

„Device mode”
pozwala nam ustawić tryb pracy urządzenia na „Access Point” lub „Client”.

W trybie „Access Point” nasz moduł będzie pracował jako stacja bazowa dla stacji klienckich, za pośrednictwem której będą one się łączyły ze sobą w ramach lokalnej sieci bezprzewodowej oraz ze stacjami sieci lokalnej podłączonej do interfejsu Ethernet’owego modułu. Punkt dostępowy jest widoczny „na zewnątrz” dla wszystkich urządzeń bezprzewodowych.

Tryb „Client” pozwala nam łączyć się za pośrednictwem modułu z sieciami przez punkty dostępowe, czyli urządzenia pracujące jako „Access Point”.
W tym trybie nasza stacja jest widoczna tylko z poziomu sieci, z którą jest połączona.

„Country code”
ustawia parametry systemowe urządzenia oraz interfejsów bezprzewodowych zgodnie z wymogami obowiązującymi w wybranym kraju.

„System up time”
informuje o czasie pracy naszego modułu, liczonym od jego włączenia.

„System name”
to pole nazwy naszego urządzenia. Pozwala ono na identyfikację urządzenia w sieci lokalnej na podstawie nazwy.
Maksymalnie 255 znaków.

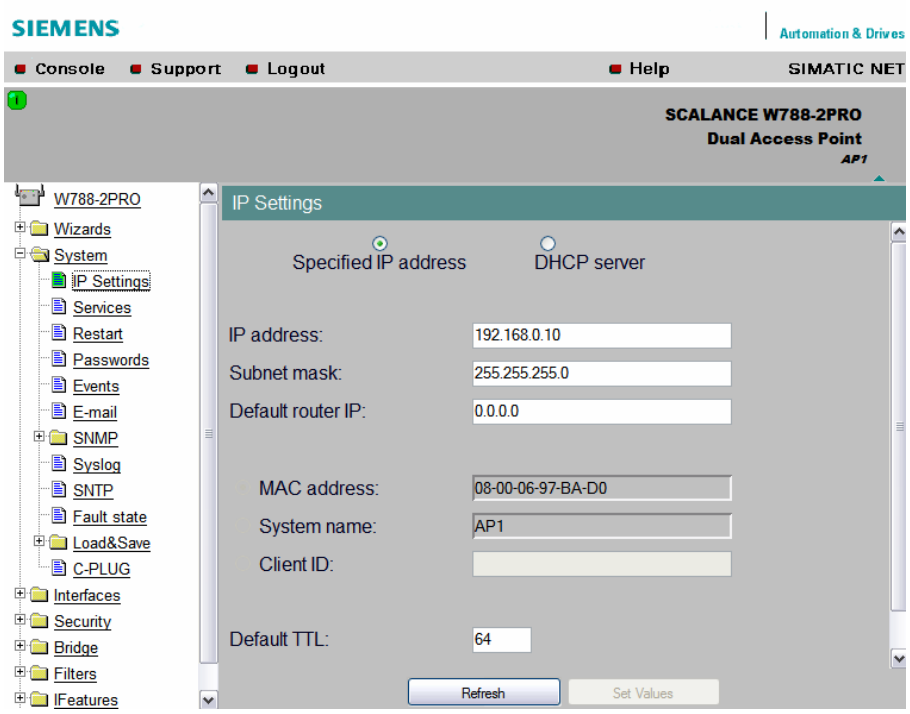
„System location”
określa lokalizację naszego systemu i jest polem czysto informacyjnym.
Maksymalnie 255 znaków.

„System contact”
Może zawierać informacje kontaktowe osoby zarządzającej modułem.
Maksymalnie 255 znaków.

„Description”
przedstawia typ danego urządzenia.

IP Settings

Tutaj ustawiamy opcje adresu IP naszej stacji.



Jeżeli posiadamy w naszej sieci serwer DHCP, który automatycznie przydziela adresy urządzeniom w sieci, wybieramy opcję „*DHCP server*” oraz zaznaczmy i wpisujemy w odpowiednie pole adres MAC, nazwę urządzenia lub identyfikator klienta w zależności od ustawień serwera.

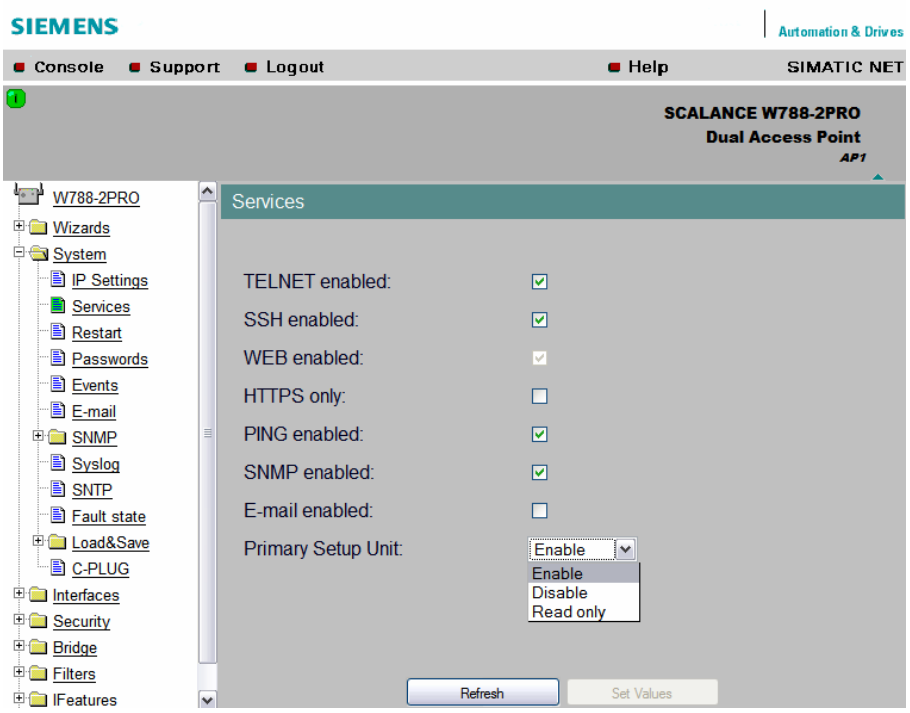
W przeciwnym przypadku musimy sami nadać adres IP naszemu modułowi. Zaznaczamy opcję „*Specified IP address*” i wprowadzamy w odpowiednie pola adres IP, maskę podsieci oraz adres IP routera, jeżeli takowy znajduje się w naszej sieci.

Wpis 0.0.0.0 oznacza brak urządzenia w sieci.

Pole „*Default TTL*” określa wartość „Time To Live” w generowanych ramkach. Jest to liczba przeskoków ramki pomiędzy kolejnymi routerami. Każdy router zmniejsza tą wartość, a po odebraniu ramki z TTL=1 odrzuca ją i usuwa z sieci. Zabezpiecza to sieć przed zapychaniem łącza krążącymi ramki w razie błędnej konfiguracji, powodującej zapętlenia ruchu.

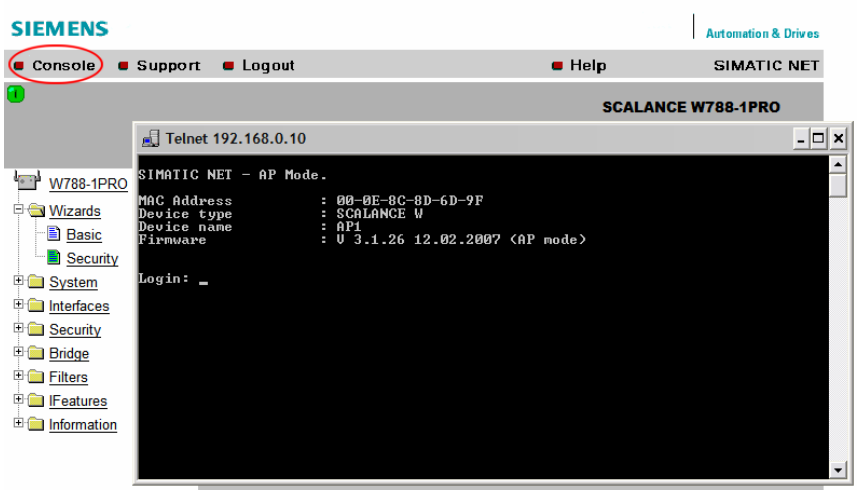
Services

W oknie tym wybieramy obsługiwane przez moduł serwisy komunikacyjne. Ze względu na bezpieczeństwo, należy korzystać z szyfrowanych protokołów oraz aktywować tylko te, z których będziemy korzystać, zgodnie z zasadą minimalnej liczby dróg dostępu.



„Telnet enabled”
włącza komunikację z modułem za pomocą nieszyforwanego protokołu Telnet.

Możemy w ten sposób konfigurować oraz diagnozować urządzenie za pomocą tekstowych komend linii poleceń CLI, wykorzystując klienta Telnet wbudowanego w większość systemów operacyjnych
(Windows – polecenie: telnet „adres IP / nazwa urządzenia”).
Konsola telnet’owa jest także dostępna w menadżerze WEB.



Za pomocą komend CLI możemy dokonać wszystkich możliwych ustawień modułu. W wielu przypadkach jest to narzędzie, wbrew pozorom, wygodniejsze i szybsze.

Zestaw komend CLI można znaleźć w załączniku „CLI – komendy.pdf".

Niestety informacje przekazywane tą drogą są całkowicie widoczne dla podsłuchującego transmisję intruza, jeżeli nie stosujemy dodatkowych zabezpieczeń.

„SSH enabled"
włącza komunikację z modułem za pomocą szyfrowanego protokołu SSH.

Opcję ta daje nam te same możliwości co komunikacja przez Telnet i dodatkowo jest znacznie bezpieczniejsza. Do komunikacji za jej pośrednictwem potrzebujemy klienta SSH. W systemie Linux możemy wykorzystać polecenie: *ssh „adres IP"*,
a w systemie Windows musimy skorzystać z dodatkowej aplikacji, np.: „Putty".
Przed pierwszym połączeniem musimy zaakceptować certyfikat urządzenia.

„WEB enabled"
daje nam możliwość połączenia się z modułem za pomocą przeglądarki internetowej wykorzystującej protokół HTTP. Opcja ta może być modyfikowana tylko, jeżeli komunikujemy się z modułem poza przeglądarką.

„HTTPS only"
włącza komunikację WEB z wykorzystaniem szyfrowanego protokołu HTTPS.
W przeglądarce wpisujemy wtedy adres w postaci „https://adres_IP".
Przed pierwszym połączeniem musimy zaakceptować certyfikat urządzenia.

„PING enabled"
powoduje, że urządzenie odpowiada na ramki ICMP typu „Response Request", wykorzystywane do sprawdzania obecności urządzenia w sieci oraz jakości połączenia. Aby wykorzystać mechanizm „PING" korzystamy z polecenia:

„ping *adres_IP*”, dostępnego w większości systemów operacyjnych.

Uwaga!
Włączenie tej opcji zalecane jest tylko podczas konfiguracji oraz testowania sieci, jako że może zostać wykorzystane przez włamywaczy do odczytania struktury naszej sieci.

„SNMP enabled”
(Simple Network Management Protocol) pozwala na odczyt i zapis ustawień urządzenia sieciowego w postaci strukturalnego obiektu MIB (Management Information Base).

Protokół ten wykorzystywany jest do konfiguracji i diagnostyki urządzeń sieciowych w narzędziach takich, jak Simatic STEP 7, WinCC, PST (Primary Setup Tool) – dostępny wraz z modułem, MIB Browser, OPC Scout.

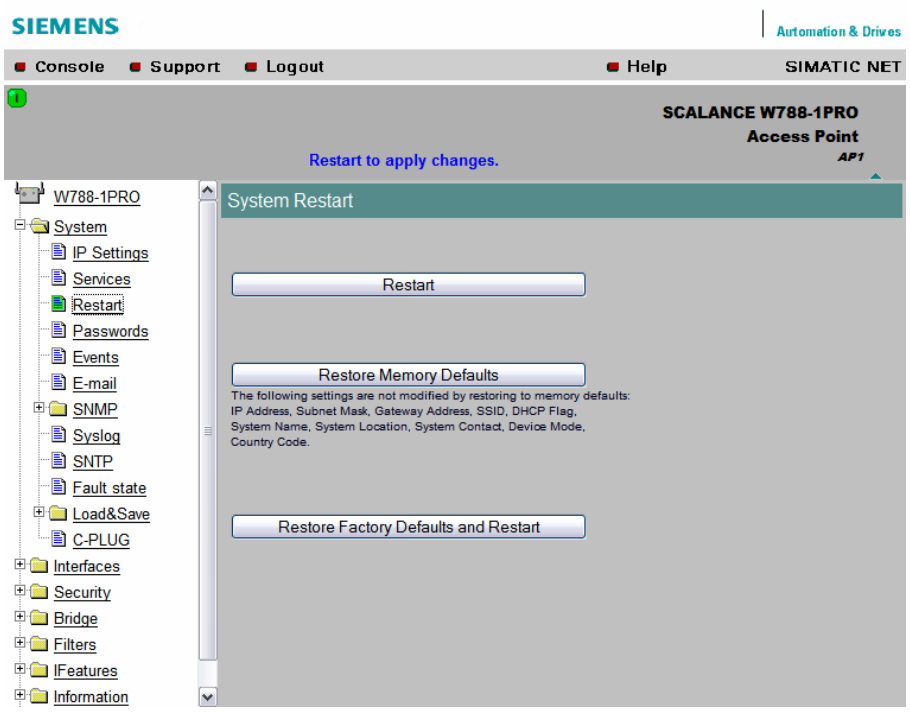
Jeżeli zamierzamy konfigurować lub diagnozować nasz moduł poprzez te narzędzia, należy włączyć opcję SNMP.

Więcej o SNMP oraz narzędziach wykorzystujących ten protokół w załączniku „IWLAN_Diag_SNMP.pdf”.

„E-mail enabled”
umożliwia wysyłanie przez urządzenie widomości e-mail, generowanych na podstawie zdarzeń zachodzących w module.

„Primary Setup Unit”
ustawia obsługę urządzenia za pomocą zewnętrznego narzędzia PST (Primary Setup Tool), dostępnego na płycie CD dostarczanej razem z modułem.
Mamy do dyspozycji opcje:
- „Enable” – włączony zapis i odczyt konfiguracji;
- „Disable” – wyłączona obsługa narzędzia;
- „Read only” – włączony tylko odczyt konfiguracji.

Restart



Do dyspozycji mamy 3 opcje restartu:

1) „Restart” – zwykły restart z zachowaniem zapisanych ustawień.
2) „Restore Memory Defaults” – restart z przywróceniem ustawień fabrycznych za wyjątkiem: adresu IP, maski podsieci, adresu bramy sieciowej, SSID, flagi DHCP, nazwy systemu, lokalizacji systemu, kontaktów systemowych, trybu pracy, kodu kraju.
3) „Restore Factory Defaults and Restart” – restart z przywróceniem wszystkich ustawień fabrycznych.

Oprócz restartu programowego możemy wykorzystać restart poprzez chwilowe odłączenie zasilania modułu (z zachowaniem konfiguracji) lub restart za pomocą przycisku „Factory Reset” z tyłu urządzenia.

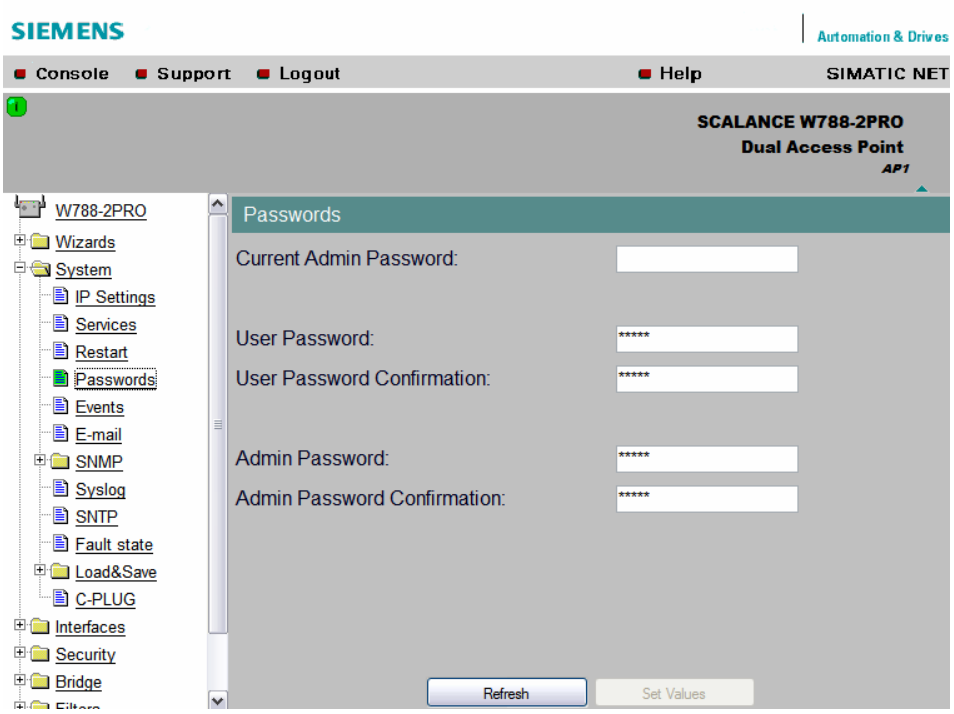
Passwords

W oknie tym mamy możliwość zmiany haseł wbudowanych kont użytkowników.
Do dyspozycji mamy dwa konta:

1) Admin – administrator, który może dokonywać wszelkich możliwych ustawień;
2) User – użytkownik, który może tylko podglądać ustawienia, informacje diagnostyczne oraz zmieniać ustawienia zapisu plików logu.

Domyślnie do konta Admin przypisano hasło *„admin”*, a do konta User hasło *„user”*.

Uwaga!
Hasła te należy ze względów bezpieczeństwa jak najszybciej zmienić!



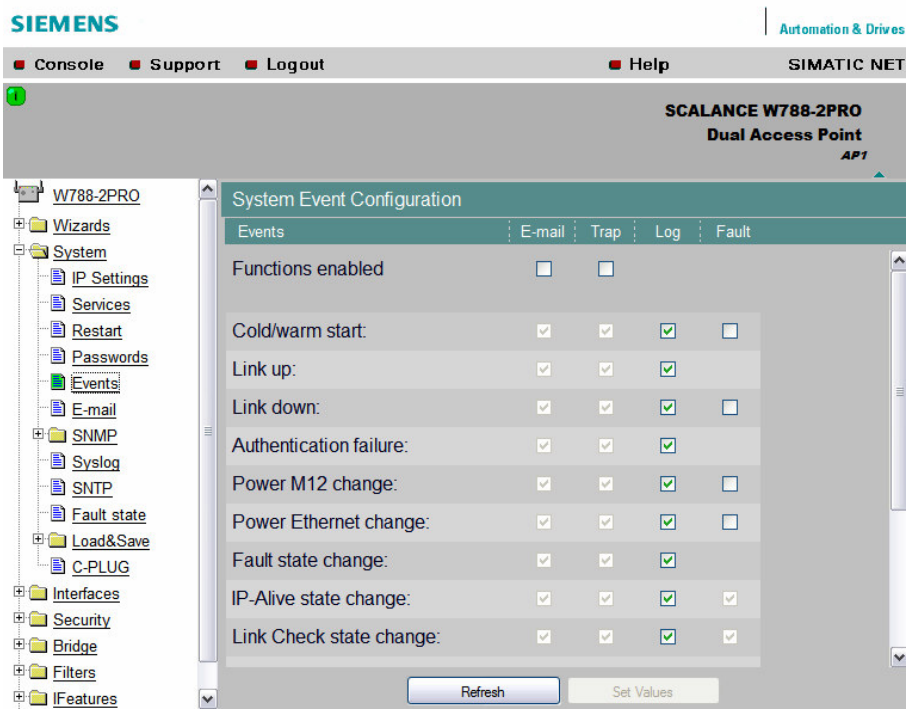
Aby zmienić hasła dostępu do systemu modułu w polu *„Current Admin Password”*, podajemy aktualne hasło administratora.

W polach *„User/Admin Password”* wpisujemy nowe hasła dla wybranego konta oraz potwierdzamy je ponownym wpisem w polach *„User/Admin Password Confiramtion”*.

Uwaga!
Należy pamiętać o „mocy” hasła, tzn. nie powinno ono być wyrazem, który możemy znaleźć w słowniku; najlepiej, aby był to losowy zlepek liter i cyfr.

Events

Zakładka ta pozwala na wybór rejestrowanych zdarzeń systemowych oraz sposobu powiadamiania o ich zajściu.



Wiersz „Functions enabled” zawiera możliwe sposoby komunikowania użytkownika o zdarzeniach, czyli:

- wysłanie informacji pocztą elektroniczną (E-mail);
- generowanie ramki „Trap”, wychwytywanej przez narzędzia obsługujące protokół SNMP;
- zapis informacji do pliku logu (Log);
- sygnalizacja zdarzenia przez diodę „F” na panelu urządzenia (Fault - problem).

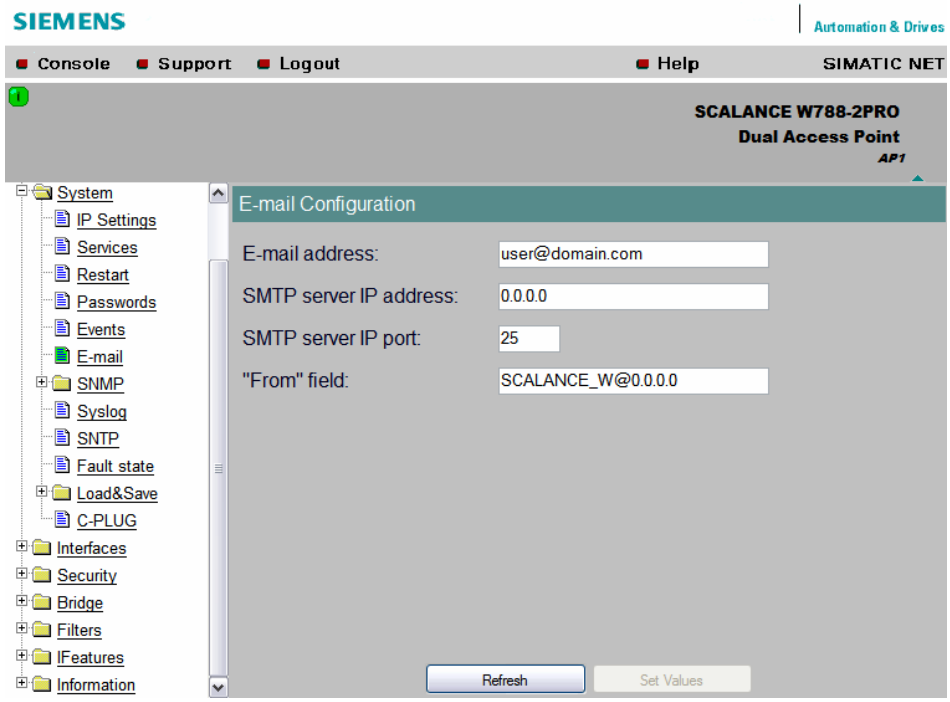
Kolejne wiersze zawierają obsługiwane zdarzenia oraz umożliwiają wybór sposobu obsługi (zawartość jest uzależniona od trybu Access Point / Client).

- *„Cold/warm start”* – start urządzenia po włączeniu zasilania lub po restarcie.
- *„Link up”* – nawiązanie połączenia Ethernet’owego.
- *„Link down”* – zerwanie połączenia Ethernet’owego.
- *„Authentification failure”* – błąd autentyfikacji użytkownika.
- *„Power M12 change”* – zmiana zasilania na łączu M12.
- *„Power Ethernet change”* – zmiana zasilania na przyłączu zasilająco-sygnałowym
- Power-On-Lan.
- *„Fault state change”* – wystąpienie lub zanik zdarzenia oznaczonego jako „Fault”.
- *„IP-Alive state change”* – zerwanie lub nawiązanie połączenia monitorowanego na poziomie aplikacji.

- *„Link Check state change”* – zerwanie lub nawiązanie połączenia monitorowanego na poziomie łącza.
- *„iQoS events”* – wystąpienie zdarzenia związanego z rezerwacją przepustowości połączenia bezprzewodowego przez mechanizm „i Quality of Sernice”.
- *„Redundancy event”* – zdarzenie generowane w czasie zmian na łączach redundantnych.
- *„Overlap AP detection”* – informacja o pojawieniu się w zasięgu naszej stacji obcego urządzenia AP zakłócającego transmisję, czyli pracującego na tym samym kanale lub na kanale nakładającym się z naszym.
- *„Forced Roaming on IP down”* – wyłączenie interfejsu, który nie jest w stanie zapewnić komunikacji z danym adresem IP i wymuszenie przełączenia się klientów na inny AP, do czasu przywrócenia poprawnego połączenia.
- *„(R)STP events”* – zdarzenia generowane przez mechanizm Spanning Tree, np. automatyczna zmiana konfiguracji połączeń redundantnych, odłączenie/przyłączenie węzła sieci.
- *„WDS events”* – zdarzenia generowane przez mechanizm Wireless Distributed System, zarządzającym współpracą wielu urządzeń AP, jako elementów jednej logicznej sieci bezprzewodowej.

Email

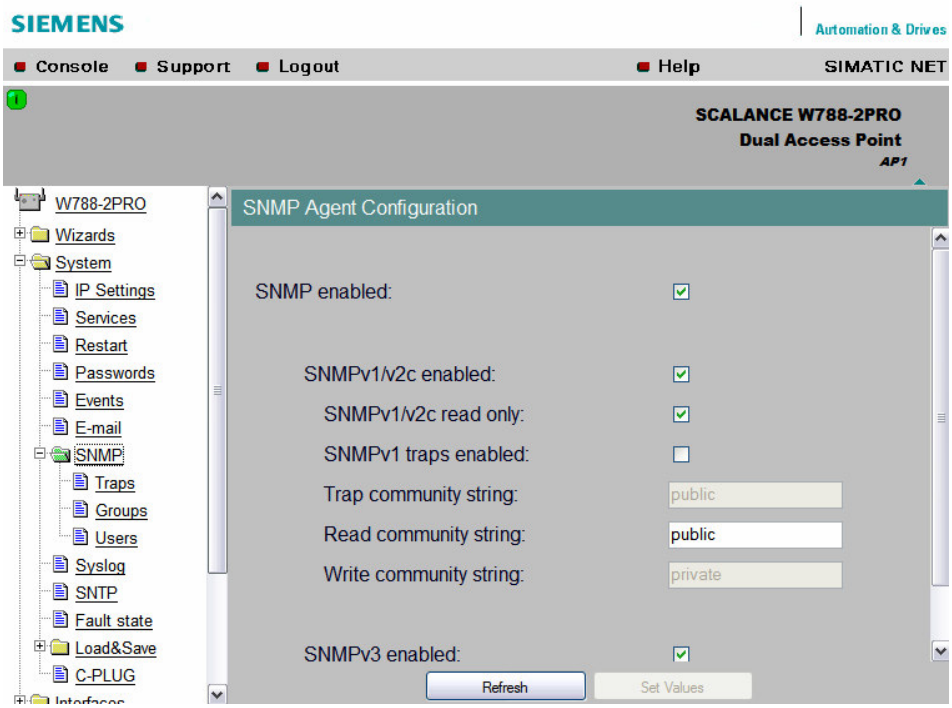
Opcja pozwala na konfigurację połączenia z serwerem poczty elektronicznej SMTP.



W polu „E-mail address” wpisujemy adres e-mail, na który moduł będzie wysyłać widomości.
W polach „SMTP Server IP address” oraz „SMTP Server IP port” podajemy adres IP serwera oraz port usługi pocztowej.
Pole „From” zawiera informację o nadawcy wiadomości widoczną dla odbiorcy w polu informacyjnym „From / Od”.

SNMP

Zakładka ta pozwala na ustawienie wersji oraz własności protokołu SNMP.
(Zasada działania SNMP została opisana w punkcie „Services").



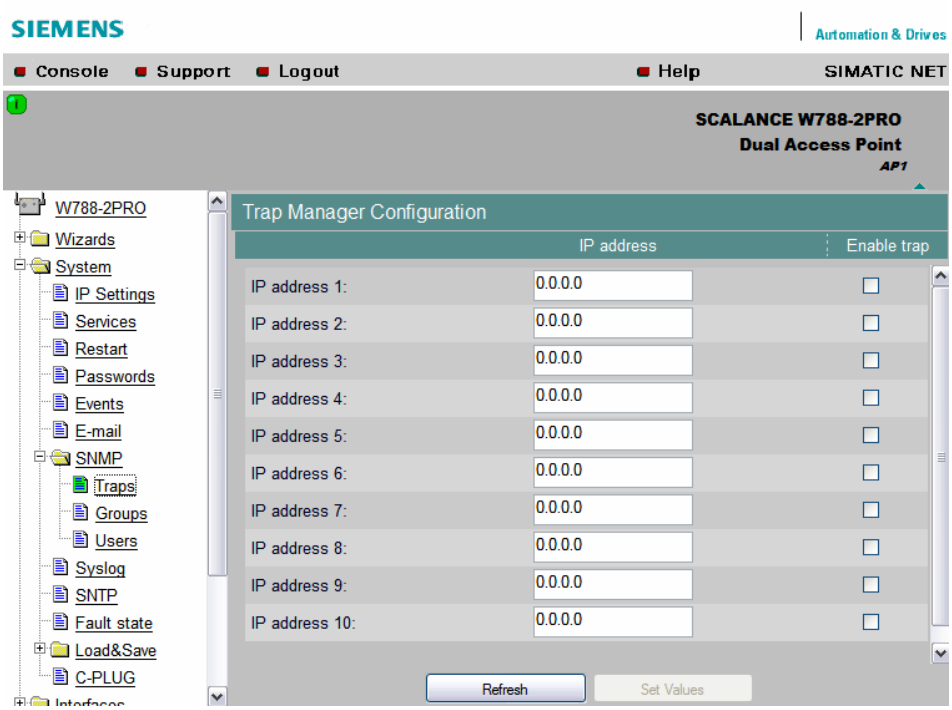
W głównej karcie dokonujemy aktywacji obsługi protokołu („*SNMP enabled*") oraz wyboru jego wersji („*SNMPv1/v2c enabled*", „*SNMPv3 enabled*").
Opcje te nie powinny być aktywowane równocześnie, ponieważ zabezpieczenia SNMPv3, mogą zostać ominięte przez użycie SNMPv1/v2c.

SNMPv1/v2c jest zabezpieczone przez klucz globalny (tzw. community string), który ustawiamy w polach „*Trap/Read/Write communiy string*", w zależności od praw dostępu poprzez protokół (otrzymywanie wiadomości o zdarzeniach – „*traps*", odczyt, zapis). Klucz ten niestety jest wysyłany poprzez sieć w postaci niezaszyfrowanej i może być łatwo „podsłuchany".
Opcje dostępu poprzez SNMPv1/v2c możemy wybierać poprzez pola *„SNMPv1/v2c read only" i „SNMPv1 traps enabled"*.

SNMPv3 aktywujemy w polu „*SNMPv3 enabled*".
Wersja ta posiada lepsze zabezpieczenia wykorzystujące grupy i użytkowników, którymi zarządzamy poprzez karty „Groups" oraz „Users".

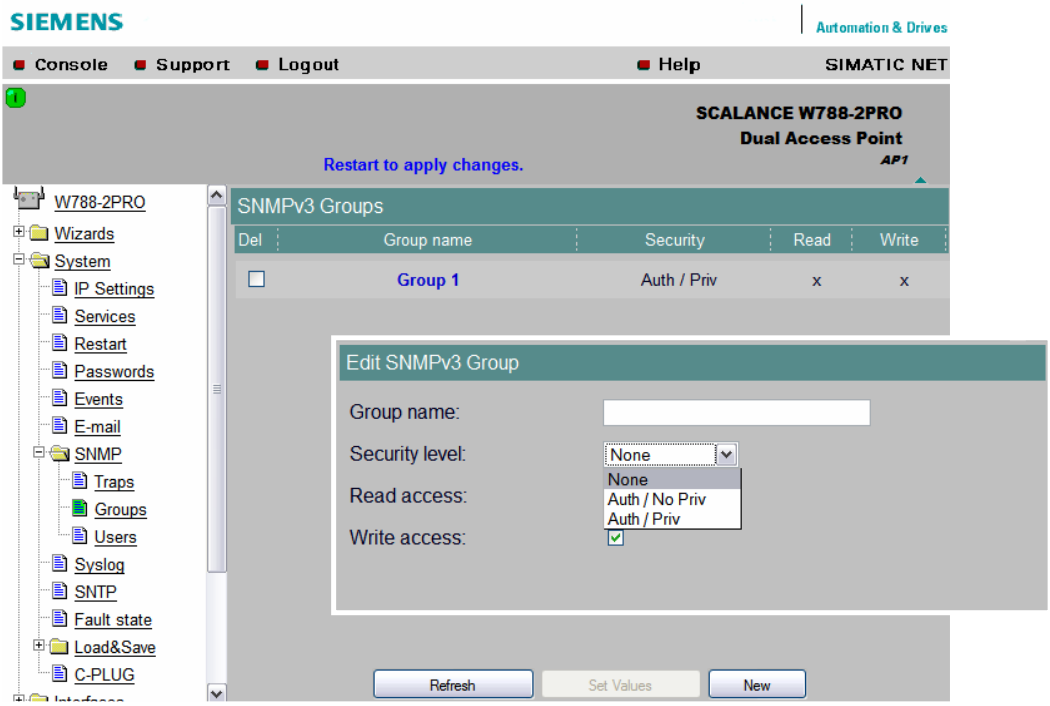
SNMP – Traps

W karcie tej możemy wpisać adresy IP dziesięciu stacji, do których będą wysyłane komunikaty zdarzeń „Trap". Komunikaty będą wysyłane do danej stacji, tylko jeśli dodatkowo aktywujemy odpowiednie pole w kolumnie „*Enable trap*".



SNMP - Groups

W karcie tej zarządzamy grupami użytkowników protokołu SNMPv3.



Po kliknięciu „*New*” pojawia się przed nami okno edycyjne grupy.

W pole „*Gruop name*” wprowadzamy nazwę grupy.

„*Security level*” pozwala na wybór poziomu zabezpieczeń i posiada trzy opcje:

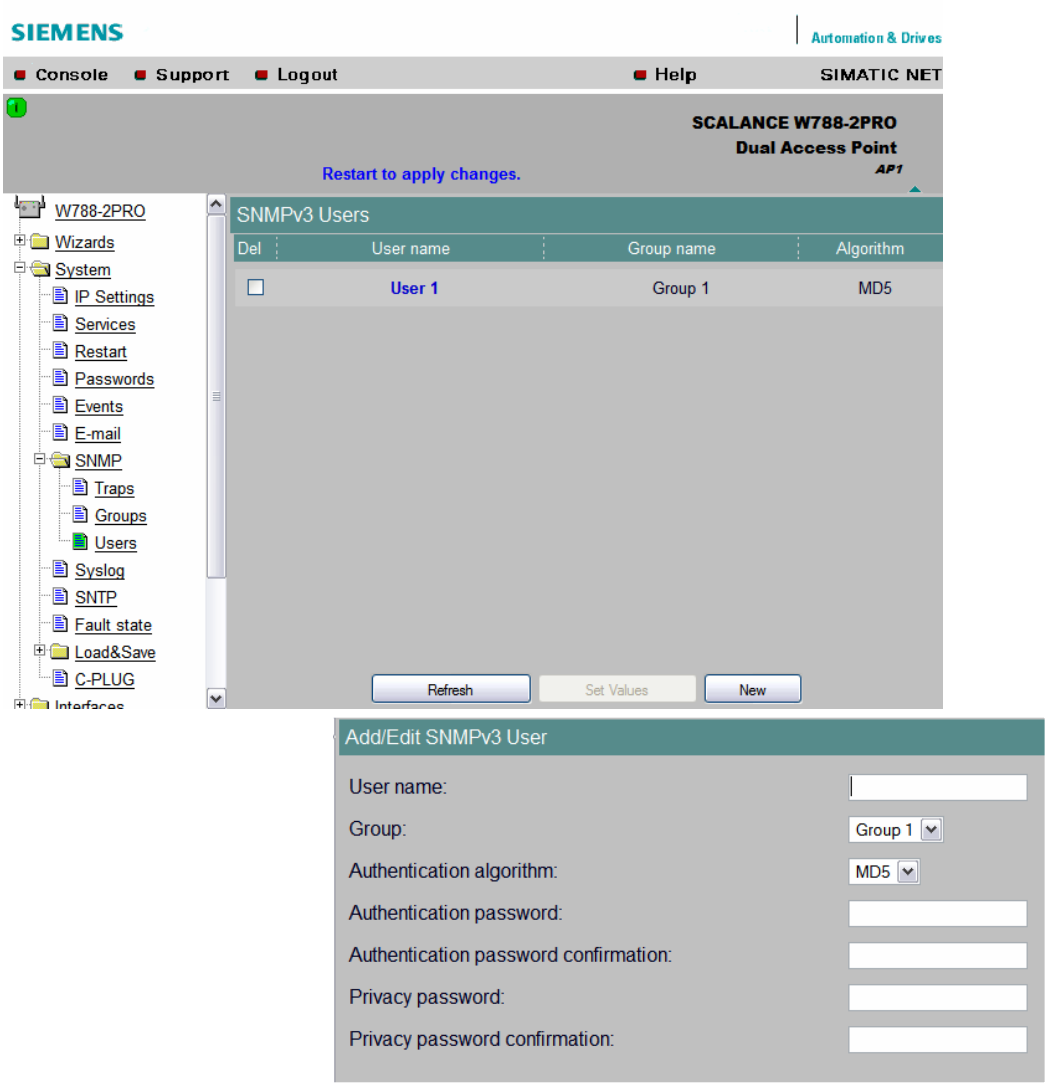
- „*None*” – brak jakichkolwiek zabezpieczeń;
- „*Auth / No Priv*” – autoryzacja użytkownika przed dostępem do danych grupy, brak szyfrowania przesyłanych danych;
- „*Auth / Priv*” – autoryzacja użytkownika przed dostępem do danych grupy, szyfrowanie danych.

Pola „*Read access*” oraz „*Write access*” pozwalają na dobór praw odczytu i zapisu dla użytkowników grupy.

W oknie karcie głównej „*Groups*” widzimy dodane grupy.
Zaznaczenie pola w kolumnie „*Del*” oraz potwierdzenie wyboru klawiszem „*Set Values*” spowoduje usunięcie odpowiedniej grupy.

SNMP – Users

Karta odpowiada za zarządzanie użytkownikami protokołu SNMPv3.



Kliknięcie klawisza „New” pozwala na edycję nowego użytkownika.
Pole „User name” zawiera nazwę użytkownika.
W „Group” mamy do wyboru dostępne grupy, do których możemy przypisać użytkownika.

Uwaga!
Jeżeli nie istnieje żadna grupa nie możemy stworzyć nowego użytkownika.

„Authentification algorithm” odpowiada za dobór algorytmu autentyfikacji; do wyboru mamy algorytmy MD5 oraz SHA.

Wskazówka
Oba algorytmy generują kod na podstawie wprowadzonego klucza
(zamiast jawnych danych, w systemie przechowywane są odpowiadające im kody).
MD5 tworzy kod 128-bitowy, natomiast SHA 160-bitowy.
Algorytmy nie są całkowicie bezpieczne, istnieją sposoby ich „złamania”.

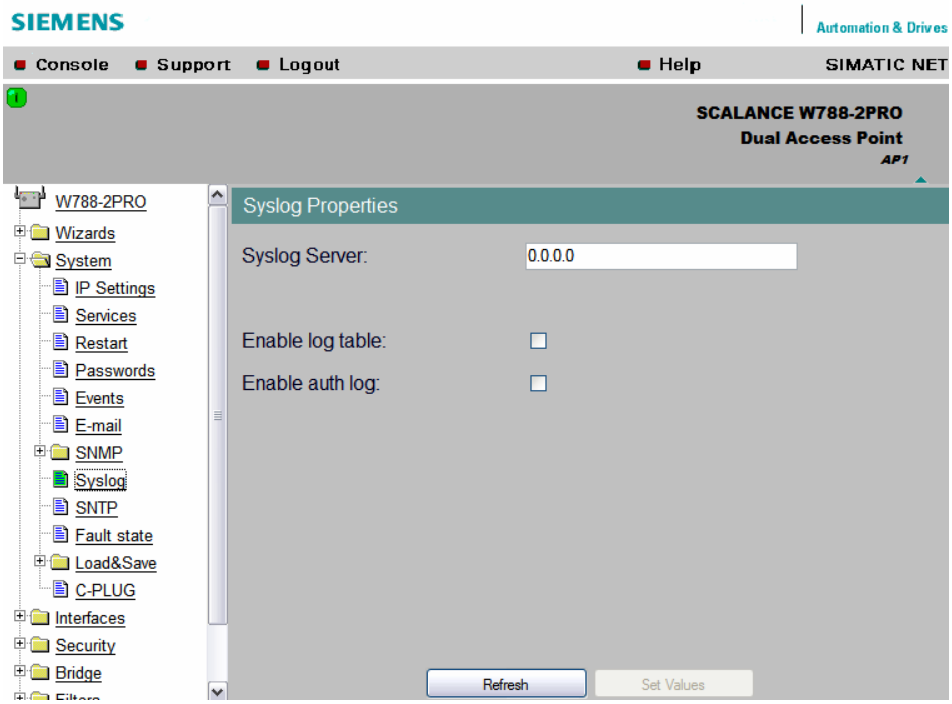
W polu „Autentification password” wprowadzamy hasło użytkownika
(max. 63 znaki), a w kolejnym potwiedzamy je powtarzając wpis.

Pole „Privacy password”, to klucz szyfrujący przesyłane dane (max. 63 znaki), który wymaga także potwierdzenia w następnym polu.

W oknie karcie głównej „*Users*” widzimy dodanych użytkowników.
Zaznaczenie pola w kolumnie „*Del*” oraz potwierdzenie wyboru klawiszem „*Set Values*” spowoduje usunięcie odpowiedniego użytkownika.

Syslog

Tutaj wprowadzamy ustawienia protokołu „Syslog”, odpowiedzialnego za wysyłanie informacji o działaniu oraz zdarzeniach występujących w systemie.



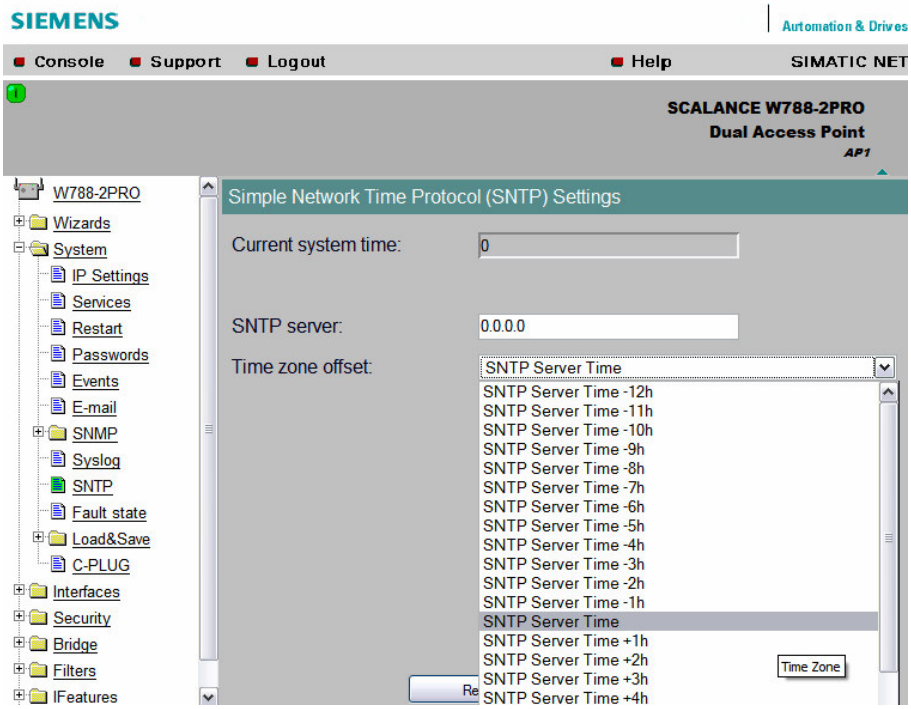
W polu „*Syslog Server*” wprowadzamy adres IP serwera syslog w rejestrującego informacje systemowe.
Adres 0.0.0.0 powoduje wyłączenie wysyłanie informacji syslog przez nasz moduł.

Aktywacja opcji „*Enable log table*” powoduje wysyłanie informacji „*Log*” wybranych w karcie „*Events*”.

Aktywacja opcji „*Enable auth log*” włącza przekazywanie logów dotyczących procesów autentyfikacji.

SNTP

Karta pozwala na skonfigurowanie połączenia z serwerem czasu poprzez mechanizm Simple Network Time Protocol.
Dzięki serwerowi SNTP nasz moduł może być zsynchronizowany czasowo z innymi urządzeniami w sieci.



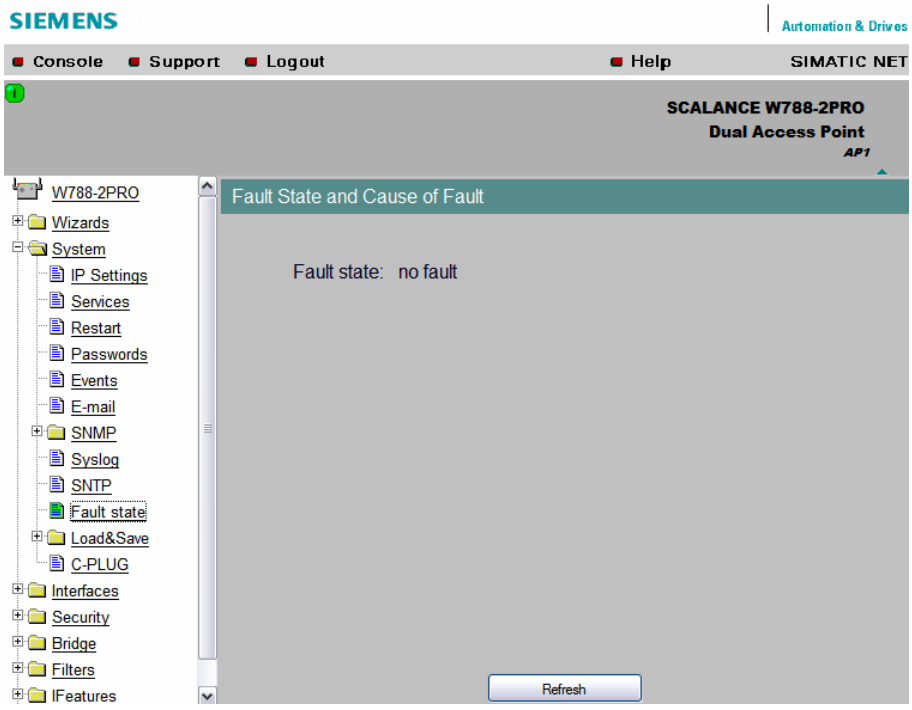
Pole „Current system time” wyświetla aktualny czas, otrzymywany z serwera.

„SNTP server” zawiera adres IP serwera czasu SNTP.

„Time zone offset” wprowadza przesunięcie czasowe między naszą lokalizacją a strefą czasową serwera.

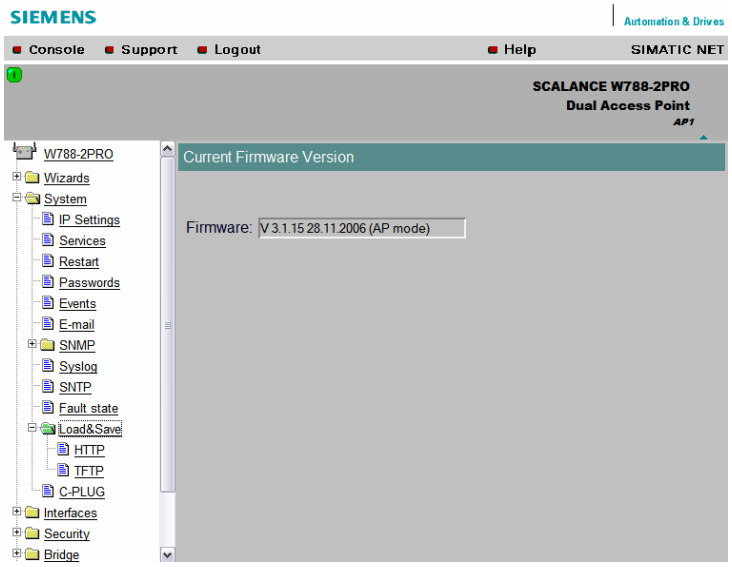
Fault state

W tym miejscu możemy poglądać opis zdarzenia „*Fault*” sygnalizowanego przez diodę „*F*” na panelu modułu oraz aktywowanego w karcie „*Events*”.



Load&Save

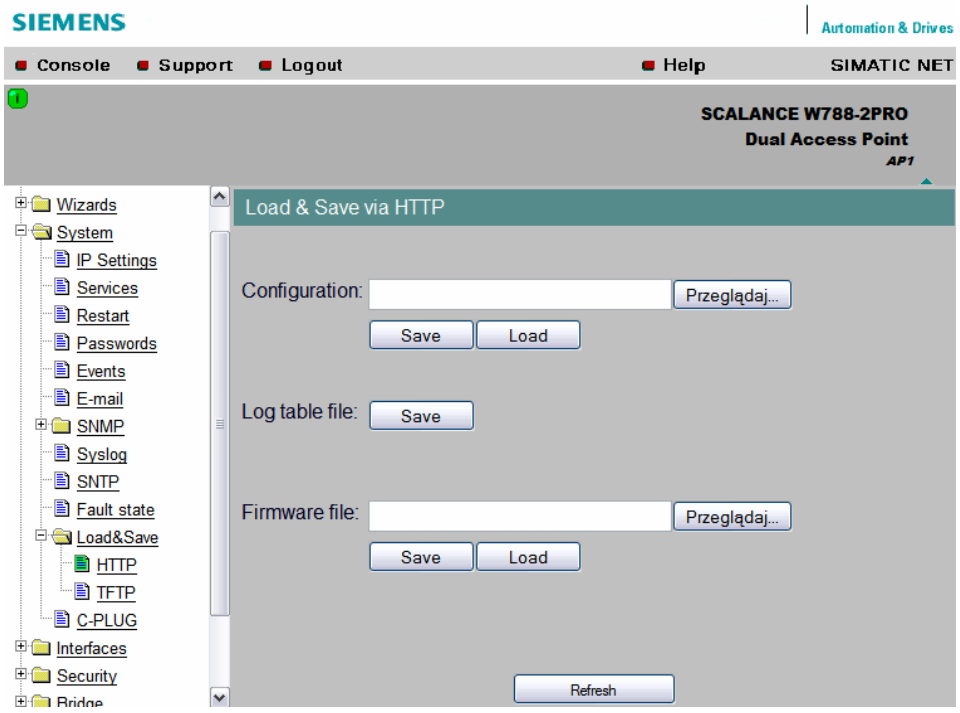
Ten zestaw opcji pozwala nam na wgrywanie i zapisywanie oprogramowania systemowego modułu oraz danych konfiguracyjnych.



W oknie głównym widzimy numer aktualnej wersji firmware’u.

HTTP

Zakładka ta pozwala na odczyt i zapis firmware'u, konfiguracji oraz logów systemowych z poziomu przeglądarki WEB za pomocą mechanizmów protokołu HTTP.



„*Configuration*" pozwala na zachowanie („*Save*") lub załadowanie („*Load*") pliku konfiguracji modułu, którego lokalizację wprowadzamy bezpośrednio lub z wykorzystaniem przycisku „*Przeglądaj…*". Domyślnie jest to plik *cfgFile.cfg*.

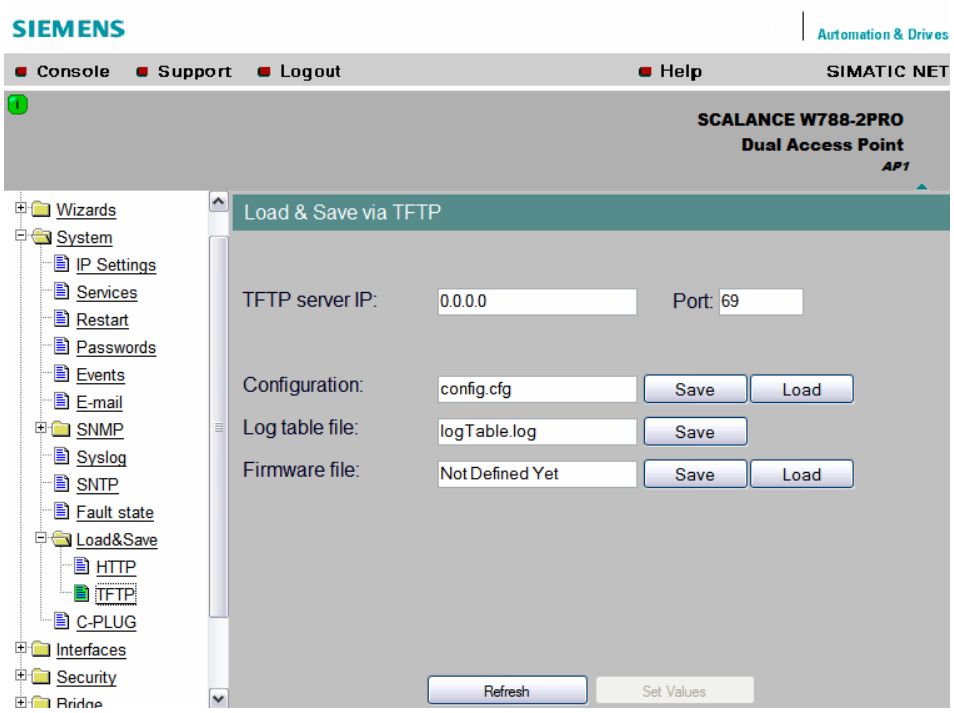
Za pomocą „*Log table file*" możem zapisać do pliku tekstowego logi zdarzeń wybranych w tabeli „*Events -> Log*". Domyślnie plik *logTable.log*.

„*Firmware file*" daje nam możliwość wygodnej aktualizacji oprogramowania systemowego modułu.
Przed każdorazową aktualizacją firmware'u należy dla bezpieczeństwa zapisać aktualną wersję za pomocą „*Save*".
Plik z nową wersją firmware'u wczytujemy za pomocą „*Load*" uprzednio wprowadzając jego lokalizcję lub korzystając z przycisku „*Przeglądaj…*".
Proces aktualizacji jest zautomatyzowany i następuję po nim restart urządzenia.

Wskazówka.
Najnowszą wersję firmware'u możemy pobrać ze strony producenta.
Jest on bezpłatny.
Aktualizacja oprogramowania systemowego poprawia działanie urządzenia oraz często dostarcza nowe funkcjonalności i opcje.
Należy uważać, aby firmware był zgodny z naszą wersją sprzętu oraz rekomendowany przez producenta.
Wraz z nową wersją oprogramowania, warto pobrać, zazwyczaj również aktualizowaną, wersję instrukcji obsługi oraz opis wprowadzonych zmian.

TFTP

Trival File Transfer Protocol pozwala na prosty zapis i odczyt plików na zdalnym komputerze.



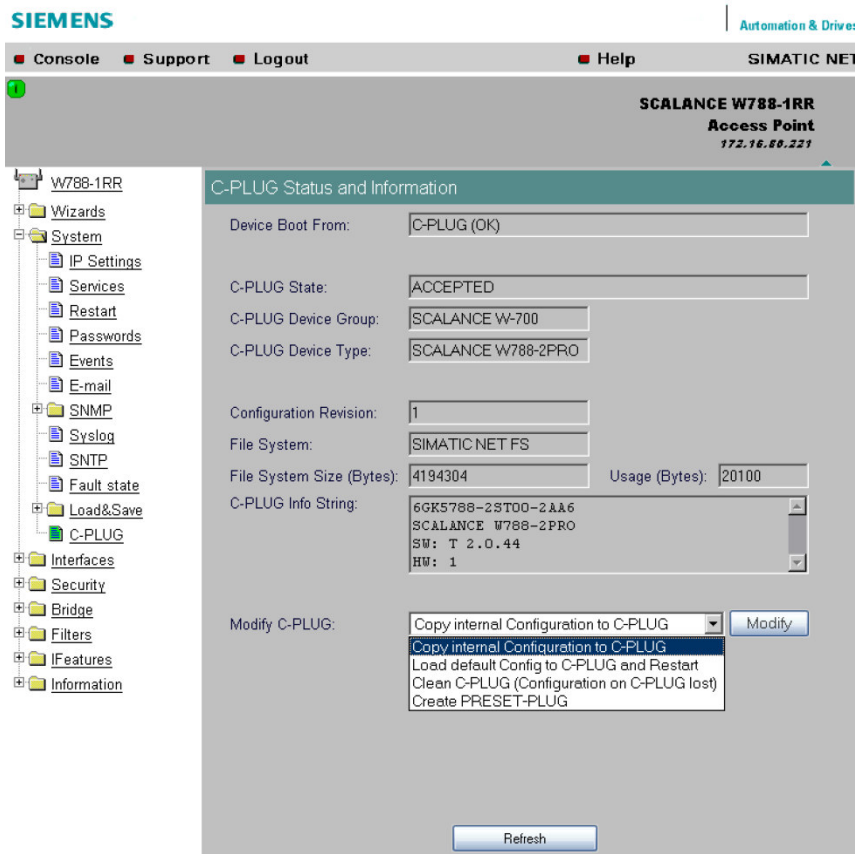
W polu „TFTP Server IP" wprowadzamy adres IP serwera, a w polu "Port" numer portu, na którym uruchomiona jest obsługa TFPT.

Pola „Configuration", „Log table file" oraz „Firmware file" są odpowiednikami funkcji opisywanych w poprzednim punkcie, z tą różnicą, że pliki te są zapisywane lub odczytywane ze zdalnej lokalizacji.

Jeżeli nie ma połączenia z serwerem TFTP, próba zapisu/odczytu jest odrzucana wraz z komunikatem o braku serwera.

C – PLUG

C-PLUG to rodzaj karty pamięci, którą możemy zainstalować w naszym urządzeniu, korzystając ze złącza z tyłu obudowy modułu.
Po zainstalowaniu C-PLUG'a i restarcie urządzenia, odłączana jest pamięć wewnętrzna modułu, który od tej chwili pobiera wszelkie dane konfiguracyjne z zewnętrznej karty pamięci.
Zawartość C-PLUG'a możemy również modyfikować, co pozwala na szybkie wprowadzenie takiej samej konfiguracji dla większej liczby modułów.



Pole „Device Boot From" informuje o źródle konfiguracji urządzenia. Może w nim zobaczyć komunikat „C-PLUG (OK)/(FAULT)", w przypadku uruchomienia z kartą C-PLUG, lub „INTERNAL (no C-PLUG)", w przypadku braku tej karty.

„C-PLUG state" wyświetla stan karty C-PLUG:

- - „ACCEPTED" – karta jest sprawna i posiada poprawną zawartość;
- - „NOT ACCEPTED" – karta uszkodzona, nie zawiera poprawnych danych lub jest sformatowana;
- - „NOT ACCEPTED, HEADER CRC ERROR" – błędna zawartośc karty;
- - „NOT PRESENT" – brak zainstalowanej karty.

Pola „C-PLUG Device Group / Type" zawierają informacje o rodzinie oraz modelu urządzenia.

„Configuration Revision” wyświetla aktualną wersję konfiguracji struktury urządzenia, powiązaną z funkcjami oferowanymi przez firmware.

„File System” wyświetla informację o systemie plików (formacie) karty C-PLUG.

„File System Size (Bytes)” to pojemność karty.

„Usage (Bytes)” informuje o ilości wykorzystanego miejsca na karcie.

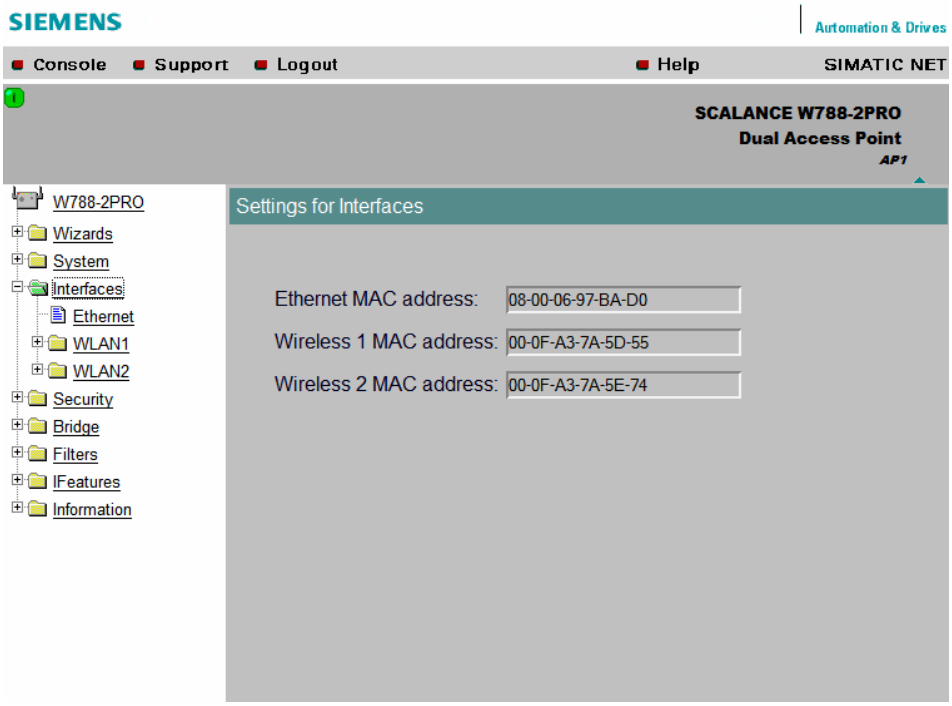
„C-PLUG Info String” zawiera informacje na temat urządzenia, które utworzyło konfigurację zapisaną na C-PLUG’u.

„Modify C-PLUG” powala nam na modyfikację zawartości karty. Do dyspozycji mamy opcje:

- - „Copy internal Configuration to C-PLUG” – kopiuje konfigurację zapisaną w pamięci wewnętrznej modułu na kartę C-PLUG i restartuje urządzenie;
- - „Load default Config to C-PLUG and Restart” – zapisuje na karcie ustawienia fabryczne danego urządzenia i wykonuje restart;
- - „Clean C-PLUG” – wykonuje niskopoziomowe formatowanie karty, powoduje usunięcie wszystkich danych;
- - „Create PRESET PLUG” – tworzy kartę konfiguracji dla wybranego modelu urządzenia. W odróżnieniu od C-PLUG’a, nie modyfikuje on jednak ustawień adresów IP, aby nie wywołać konfliktów w sieci.

3. Zakładka „Interfaces”.

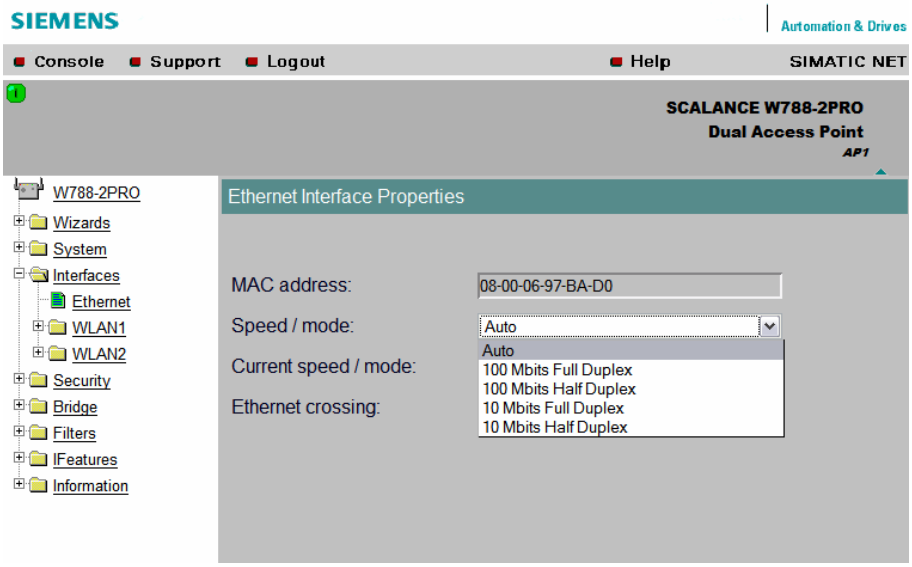
Ten zestaw opcji umożliwia zaawansowaną konfigurację wszystkich interfejsów sieciowych modułu SCALANCE W.



W oknie głównym widzimy dostępne interfejsy oraz ich unikatowe adresy MAC.

Ethernet

Okno pozwala na konfigurację interfejsu sieci przewodowej Ethernet.



„MAC address” wyświetla adres MAC interfejsu Ethernet’owego.

„Speer / mode” pozwala na ustawienie trybu oraz szybkości przesyłania danych.

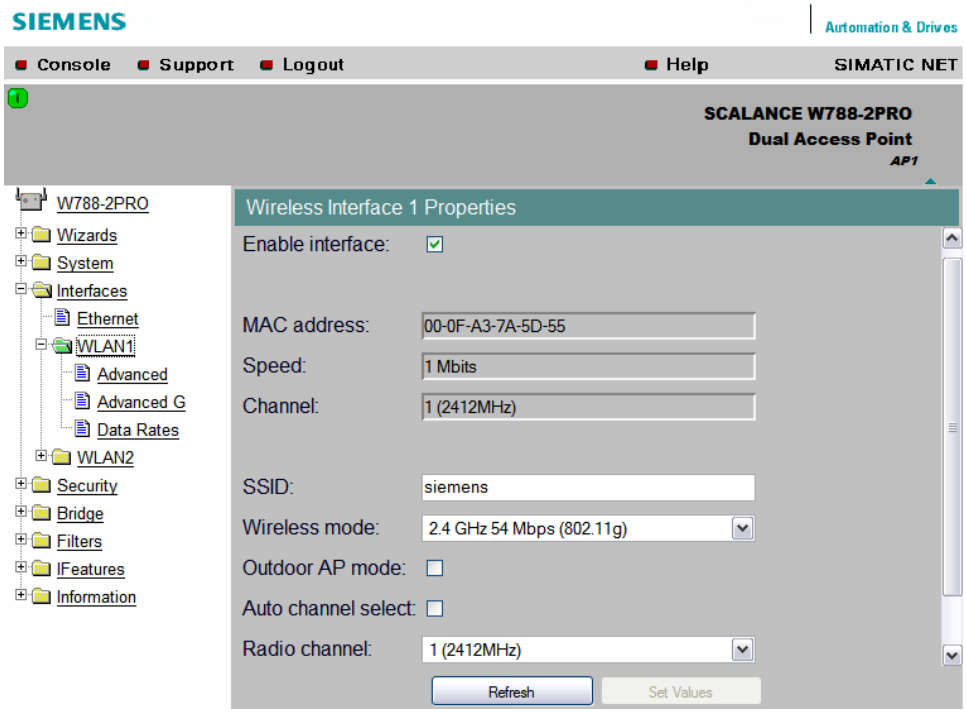
Opcja „Auto” dobiera odpowiednie parametry na podstawie struktury i połączeń sieci. Reszta opcji będzie przydatna, jeżeli urządzenia, z którymi się łączymy wymagają specyficznej komunikacji: mniejszej prędkości (10 Mbits) lub nie obsługują jednoczesnego wysyłania i odbierania danych (Half Duplex).

Jeżeli wybierzemy opcję inną niż „Auto”, musimy także ustawić opcję „Ethernet crossing”, w przypadku używania połączenia cross-over, przy bezpośrednim połączeniu dwóch stacji (bez pośrednictwa switch’a).

Pole „Current speed / mode” wyświetla aktualnie ustawiony tryb i prędkość połączenia.

WLAN1/2

W oknie głównym tego menu dokonujemy podstawowych ustawień interfejsu bezprzewodowego WLAN.



Zaznaczone pole „*Enable interface*” aktywuje interfejs.

Pole „*MAC address*” wyświetla adres MAC danego interfejsu bezprzewodowego.

„*Speed*” informuje o aktualnej prędkości połączenia radiowego.

W polu „*Channel*” widzimy numer kanału, na którym aktualnie jest ustanowione połączenie oraz częstotliwość kanału.

W polu „*SSID*” mamy możliwość nadania nazwy Service Set IDentifier, która będzie rozgłaszana na zewnątrz jako identyfikator naszej sieci bezprzewodowej.
Nazwa ta musi być unikalna, a ze względów bezpieczeństwa nie powinna zawierać informacji o charakterze sieci czy też jej zasobach.
Maksymalna długość 32 znaki, bez polskich znaków.

W polu „*Wireless mode*” wybieramy tryb, w którym będzie pracowała nasza sieć bezprzewodowa, w zależności od pożądanego pasma, prędkości transmisji czy mocy sygnału.
Charakterystykę trybów pracy sieci bezprzewodowej przedstawia poniższa tabelka.

Standard	**802.11b**	**802.11g**	**802.11a/h**	**802.11a/h**	**802.11a/h**	**802.11a/h ***
Zakres	2,4 GHz	2,4 GHz	5,15-5,25 GHz	5,25-5,35 GHz	5,4-5,7 GHz	5,7-5,8 GHz
Maks. prędkość transmisji	11 Mbps	54 Mbps , 108 Mbps – tryb Turbo	54 Mbps	54 Mbps	54 Mbps	54 Mbps
Liczba nienakładających się kanałów	3	3	4	4	10/11	5/4
Transmitowana moc	100 mW EIRP (ETSI), 1 W (FCC)	100 mW EIRP (ETSI), 1 W (FCC)	200 mW EIRP (ETSI), 50 mW (FCC)	200 mW EIRP (ETSI), 250 mW (FCC)	1 W EIRP (ETSI)	1 W (FCC)
Modulacja	DSSS, HR-DSSS	DSSS, HR-DSSS, OFDM	OFDM	OFDM	OFDM	OFDM
Przenikanie przez ściany	Średnie	Średnie	Słabe	Słabe	Słabe	Słabe
Odbicia od przeszkód	Mocne	Mocne	Mocne	Mocne	Mocne	Mocne
Ryzyko interferencji z innymi urządzeniami	Średnie	Średnie	Małe	Małe	Bardzo małe	Bardzo małe

* - pasmo niedozwolone w Polsce.

Uwagi:

Standard 802.11h jest rozwinięciem 802.11a o mechanizmy kontroli mocy transmisji (TPC) oraz dynamicznego doboru częstotliwości (DFS), w celu uniknięcia zakłócania częstotliwości radarowych. Urządzenia posiadające te mechanizmy mogą pracować z wykorzystaniem większych mocy.

Podana maksymalna prędkość transmisji odnosi się do prędkości transmisji radiowej. Narzut protokołu powoduje, że efektywność transmisji wymiany danych pomiędzy użytkownikami wynosi ok. 50%.
Na prędkość transmisji ma wpływ wiele czynników zewnętrznych, tj.: odległość pomiędzy stacjami, moc zastosowanych anten, przeszkody pomiędzy stacjami czy interferencja kanałów z innymi urządzeniami.

W standardzie 802.11g niektóre urządzenia posiadają tryb Turbo (Super G). Pozwala on osiągnąć prędkość transmisji radiowej do 108 Mbps, dzięki wykorzystaniu kilku kanałów dostępnego pasma. Oczywiście chcąc wykorzystać ten mechanizm,

musimy posiadać na naszym terenie dodatkowe wolne kanały, co staje się trudne do osiągnięcia, jeżeli mamy do czynienia z wieloma sieciami na jednym obszarze.

Standard 802.11g jest zgodny „w dół" ze standardem 802.11b, co oznacza, że urządzenia pracujące w tych trybach mogą się komunikować. Trzeba jednak zaznaczyć, że w takim przypadku maksymalna prędkość transmisji wynosi 11 Mbps.

Wszelkie ustawienia mocy transmisji oraz pasm częstotliwości konfigurowane są automatycznie, po wyborze odpowiedniego trybu.

Opcja „*Outdoor AP mode*" wybierana jest, jeżeli nasz moduł pracuje na zewnątrz i pozwala na automatyczny dobór mocy sygnału, ze względu na restrykcje obowiązujące w danym kraju.
(W praktyce powoduje ona zawsze zwiększenie mocy sygnału).

Uwaga!
Jeżeli nasz SCALANCE W pracuje na zewnątrz, należy zabezpieczyć go przed deszczem oraz bezpośrednim działaniem słońca.

Zaznaczenie pola „*Auto channel select*" powoduje automatyczny i optymalny wybór kanału.
Jeżeli chcemy sami ustawić kanał transmisji, pole to musi być odznaczone.

Aktywne pole „*Radio channel*" pozwala na indywidualny wybór kanału.
Jest to opcja szczególnie przydatna, gdy mamy do czynienia z wieloma stacjami w naszej sieci, kiedy to ważny jest dobór kanałów w taki sposób, aby ich pasma „nie nachodziły" na siebie wzajemnie.

Warto w tym miejscu nadmienić, iż szerokość pasma jednego kanału wynosi 22 MHz, zatem w różnych trybach mamy do dyspozycji, różną liczbę „czystych" kanałów.

Wskazówki:
W trybie 802.11b/g, mamy do dyspozycji 3 nienakładające się kanały spośród 13 możliwych.
Jeżeli nasze stacje znajdują się na obszarze płaszczyzny, wybieramy kanały:
1, 6, 11.
Jeżeli stacje są rozmieszczone na różnych poziomach względem siebie, używamy 4 kanałów (rezygnujemy z szerokiego pasma na rzecz niepowtarzalności kanałów w sąsiedztwie): 1, 4, 8, 11 lub 1, 5, 9, 13.

W trybie 802.11a/h mamy do dyspozycji szersze pasma:

Zakres częstotliwości	Szerokość pasma	Nienakładające się kanały
5,15 – 5,25	100 MHz	4
5,25 – 5,35	100 MHz	4
5,47 – 5,725	200 MHz	10
5,725 – 5,825	100 MHz	4

W tych trybach kreator na podstawie wcześniejszych ustawień lokalizacji, selekcjonuje dla nas odpowiednie kanały automatycznie.

W trybie 802.11g Turbo nie mamy możliwości wyboru kanałów, ze względu na wbudowany mechanizm tego trybu.

W Polsce dozwolone są następujące moce transmisji w zależność od trybu pracy:

Tryb pracy	Kanał	Częstotliwość	PWR(EIRP)	Miejsce pracy
11b, 11g, g-Turbo				
	1-13	2412-2472 MHz	100 mW	w budynku/na zewnątrz
11a				
TPC	36	5180	60 mw	w budynku
TPC	40	5200	60 mw	w budynku
TPC	44	5220	60 mw	w budynku
TPC	48	5240	60 mw	w budynku
11h				
DFS+TPC	36	5180	200mW	w budynku
DFS+TPC	40	5200	200mW	w budynku
DFS+TPC	44	5220	200mW	w budynku
DFS+TPC	48	5240	200mW	w budynku
DFS+TPC	52	5260	200mW	w budynku
DFS+TPC	56	5280	200mW	w budynku
DFS+TPC	60	5300	200mW	w budynku
DFS+TPC	64	5320	200mW	w budynku
DFS+TPC	100	5500	1000mW	w budynku/na zewnątrz
DFS+TPC	104	5520	1000mW	w budynku/na zewnątrz
DFS+TPC	108	5540	1000mW	w budynku/na zewnątrz
DFS+TPC	112	5560	1000mW	w budynku/na zewnątrz
DFS+TPC	116	5580	1000mW	w budynku/na zewnątrz
DFS+TPC	120	5600	1000mW	w budynku/na zewnątrz
DFS+TPC	124	5620	1000mW	w budynku/na zewnątrz
DFS+TPC	128	5640	1000mW	w budynku/na zewnątrz
DFS+TPC	132	5660	1000mW	w budynku/na zewnątrz
DFS+TPC	136	5680	1000mW	w budynku/na zewnątrz

Wireless Settings (w trybie klienta)

W trybie klienta, w polu „SSID" podajemy identyfikator istniejącej sieci WLAN oraz wybieramy tryb, w którym dana sieć pracuje.
Kanał transmisji dobierany jest automatycznie.

Opcja „Connect to ANY SSID" powoduje, że nasz klient połączy się z dowolną siecią, która odpowiada jego konfiguracji zabezpieczeń.
Jeżeli jest więcej takich sieci, czynnikiem decydującym jest jakość sygnału konkretnego AP.

MAC Address of the Client (w trybie klienta)

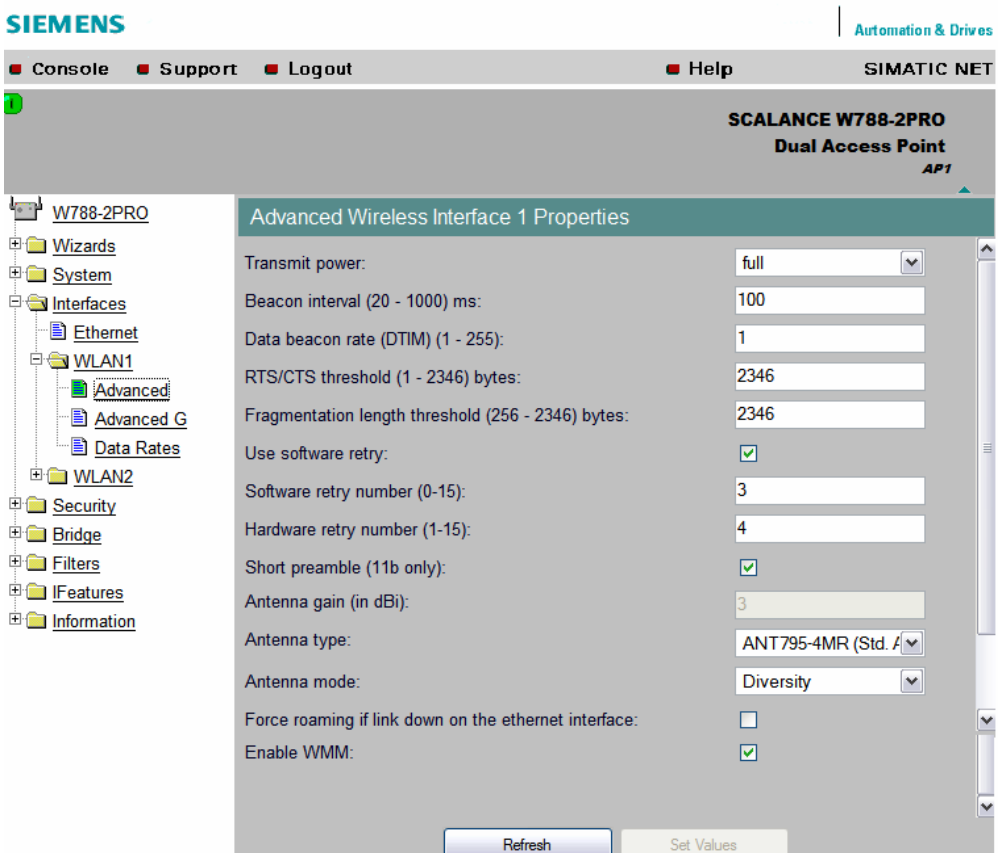
Moduł klienta posiada opcję przypisania adresu MAC do jego interfejsu bezprzewodowego WLAN. Innymi słowy, mamy tutaj możliwość wyboru, urządzenia lub urządzeń, które będą widoczne dla nas od strony sieci bezprzewodowej.

W polu wyboru *"MAC mode"* mamy opcje:

- *„Auto find 'Adopt MAC' „* – do interfejsu WLAN przypisany zostaje adres źródłowy pierwszej ramki, która pojawiła się w module od strony interfejsu Ethernet'owego, czyli adres stacji, za pomocą której jesteśmy połączeni z modułem klienta przez kabel. W ten sposób w sieci bezprzewodowej widoczny jest jeden adres MAC;
- *„ Set 'Adopt MAC' manually"* – podajemy adres MAC, który ma być widoczny z poziomy sieci bezprzewodowej;
- *„Adopt own MAC"* – do interfejsu WLAN modułu jest przypisywany adres MAC jego interfejsu Ethernet;
- *„Layer 2 Tunnel"* – do interfejsu WLAN przypisywany jest adres MAC interfejsu Ethernet'owego, natomiast w sieci bezprzewodowej widocznych jest do 8 adresów MAC urządzeń podłączonych do modułu klienta (np. za pomocą Switch'a).
  Opcja ta jest wykorzystywana w aplikacjach przemysłowych, które wymagają komunikacji na poziomie adresów MAC z kilkoma urządzeniami.
  Uwaga!
  Połączenia rezelizowane w ten sposób możliwe są tylko z urządzeniami *SCALANCE W* z firmwarem powyżej wersji 3.0 lub kompatybilnymi.

Advanced

Okno to pozwala nam na modyfikację parametrów warstwy fizycznej oraz łącza interfejsów bezprzewodowych.
Domyślne wartości są dobrane optymalnie dla większości aplikacji i powinni je modyfikować w razie potrzeby tylko zaawansowani użytkownicy.



„*Transmit power*" pozwala nam na dobór mocy wyjściowej interfejsu WLAN.

Do wyboru mamy: „full" – pełna moc (zależy od trybu połączenia), „half" (-3 dB), „quater" (-6 dB), „eighth" (-9 dB), „min" (ok. 1 dBm).

Wskazówka.
Zależność mocy wyjściowej modułu od trybu i prędkości połączenia przedstawia poniższa tabela.

Prędkość transmisji [Mbps]	P_0 [dBm]
802.11b (2,4 GHz)	
1	18
2	18
5,5	18
11	18

802.11g (2,4 GHz)	
6	17
9	17
12	17
18	17
24	17
36	13
48	11
54	10
802.11a/h (5 GHz)	
6	17
9	17
12	17
18	17
24	17
36	13
48	11
54	10

„*Beacon interval*" – określa *interval* rozsyłania pakietów „beacon", które informują o istnieniu danej sieci.

„*Beacon Rate*" – (występuje w trybie klienta) ustawia prędkość transmisji pakietów „beacon". Im ta prędkość jest wyższa, tym mniejszy zasięg sieci.

„*Data beacon rate (DTIM)*" – (Delivery Traffic Indication Map) odpowiada za częstotliwość rozsyłania do wszystkich stacji danej podsieci pakietów rozgłoszeniowych broadcast oraz pakietów multicast, odpowiedzialnych za identyfikację stacji oraz optymalizację ruchu.
Wartość w tym polu określa, co ile pakietów beacon będą rozsyłane pakiety broadcast i multicast. Większa liczba pozwala na większą oszczędność energii w stacjach podsieci, ale też powoduje większe opóźnienia w transmisji.

„*RTS/CTS threshold*" – wartość odpowiada rozmiarowi pakietu, po którego przekroczeniu jest aktywowany mechanizm RTS/CTS.

Wskazówka.
Mechanizm ten przeciwdziała tzw. problemowi „ niewidzialnej stacji", występującemu wtedy, gdy dwie lub więcej stacji w zasięgu jednego AP „nie widzą się" wzajemnie i próbują wysłać pakiety do niego w tym samym czasie. Następuje kolizja, której możemy uniknąć zapewniając dodatkowe sygnały, informujące o potrzebie transmisji „Request To Send" oraz niezajętości łącza „Clear To Send" pomiędzy klientem i stacją bazową. Mechanizm ten wprowadza dodatkowy ruch, ale zabezpiecza przed problemem wielokrotnych kolizji.

„*Fragmentation length threshold*" – określa maksymalny rozmiar pakietu na łączu radiowym. Jeśli pakiet przekracza ten rozmiar, następuje jego fragmentacja, czyli podział na mniejsze pakiety, w celu uniknięcie przekłamań dużych ilości danych, gdy jakość łącza jest słaba.

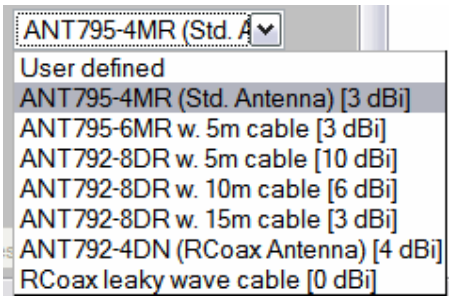
„*Use software retry*" – opcja aktywuje funkcję programowego ponawiania prób wysyłania niepotwierdzonych pakietów, w przypadku gdy mechanizm repetycji sprzętowej nie uzyskuje odpowiedzi.

Ilość powtórzeń mechanizmu programowego oraz sprzętowego ustawiamy w polach „*Software retry number*" i „*Hardware retry number*".

"*Short preamble*" – opcja włącza redukcję długości ramki sieciowej przez skrócenie długości tzw. preambuły, czyli ciągu bitów na początku ramki, które służą do synchronizacji urządzeń. W naszym module opcja ta działa tylko w trybie 802.11b. Należy pamiętać, że funkcja ta musi być obsługiwana przez wszystkie urządzenia sieciowe, z którymi chcemy się łączyć.

„*Antenna gain*" – tu wprowadzamy wartość wzmocnienia anteny dołączonej do modułu, w przypadku, gdy nie jest to urządzenie standardowe, wymienione w kolejnym polu.

„*Antenna type*" – pozwala na wybór typu anteny zewnętrznej producenta lub podanie parametrów innej.
W oknie wyboru widzimy dostępne modele wraz z rekomendowanymi długościami przewodów antenowych oraz uzyskiwanymi wzmocnieniami.



Wskazówka.
Definiując własny model anteny, należy pamiętać, że od wzmocnienia anteny odejmujemy staraty wnoszone przez przewód.
Standardowe kable antenowe wnoszą straty na poziomie 0,5 dBi/m, najlepsze ok. 0,2 dBi/m.
Trzeba zwrócić także uwagę na maksymalną moc emisji nadajnika w danym kraju, dla danego typu sygnału, która ogranicza z prawnego punktu widzenia, wzmocnienie stosowanych anten.

Przykład.
Maksymalna moc nadawcza w Polsce wynosi 100 mW.
Znaczy to, że sumaryczna moc wyjściowa, na którą składają się z moc nadajnika, zysk anten oraz straty wnoszone przez przewody nie może przekroczyć 20 dBm.

$$P\,[dBm] = 10 * \log (P\,[mW] / 1\ mW)$$

0.5 mW ≈ -3 dBm
1 mW = 0 dBm
2 mW ≈ 3 dBm
4 mW ≈ 6 dBm
10 mW ≈ 10 dBm
100 mW ≈ 20 dBm
200 mW ≈ 23 dBm
1 W ≈ 30 dBm

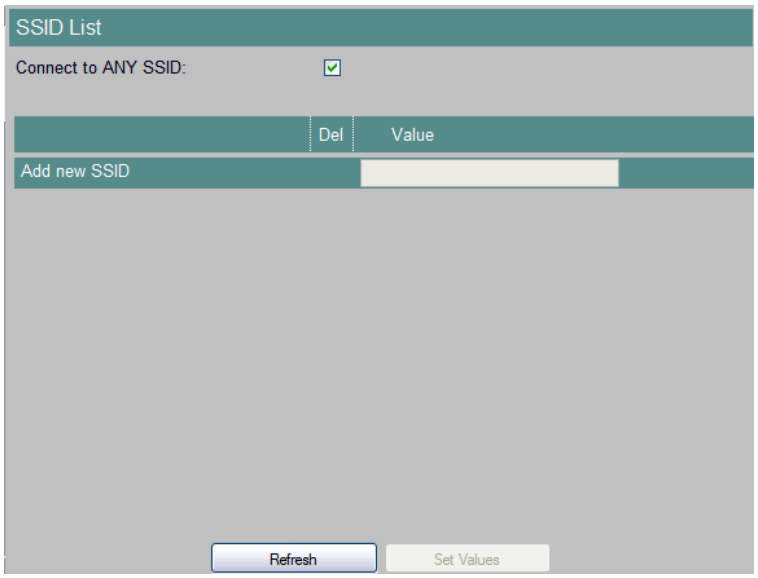
„Antena mode” – tryb wykorzystania anten. Do dyspozycji mamy opcje:
- „Diversity” - wykorzystuje dwie anteny w celu uzyskania jak najlepszego poziomu sygnału;
- „Antenna A” - wykorzystywane jest jedno złącze antenowe, oznaczone na obudowie jako „A„; na drugim złączu („B”), należy zainstalować terminator 50 Ohm;
- „Antenna B” - wykorzystywane jest jedno złącze antenowe, oznaczone na obudowie jako „B„; na drugim złączu („A”), należy zainstalować terminator 50 Ohm;
- „Tx on A, Rx on B” - włącza nadawanie na złączu „A„ odbiór na złączu „B”;
- „Tx on B, Rx on A” - nadawanie na złączu „B„ odbiór na złączu „A”;

„Roaming when there is no Ethernet Interface” - aktywacja tej opcji powoduje, że jeżeli Access Point wykryje, iż jego połączenie Ethernet'owe zostało przerwane, odłącza także interfejs WLAN, aby jego klienci przełączyli się na inny AP, który może posiadać dane połączenie Ethernet'owe. Po odzyskaniu połączenia Ethernet'owego następuje ponowna aktywacja interfejsu bezprzewodowego.

„Enable WMM” - opcja włącza priorytetową wymianę danych zgodną z rozszerzeniem Wireless Multimedia.
Do ramek transmitujących dane dołączane są znaczniki, określające priorytet wg poniższego podziału.

Kategoria WMM	Opis	Znaczniki
WMM Voice priority	Najwyższy priorytet. Pozwala na prowadzenie kilku równoległych rozmów głosowych VIP z dobrą jakością.	7, 6
WMM Video priority	Strumienie wideo transmitowane ponad innymi danymi. Na jednym kanale (802.11g / 802.11a) przesyłane są 3-4 strumienie SDTV lub 1 HDTV.	5, 4
WMM best effort priority	Przeznaczona dla ruchu z urządzeń lub aplikacji niskowydajnych, które są wrażliwe na duże opóźnienia.	0, 3
WMM backgorund priority	Aplikacje i urządzenia, które nie mają wymogów związanych z przepustowością czy opóźnieniami.	2, 1

SSID List (w trybie klienta)

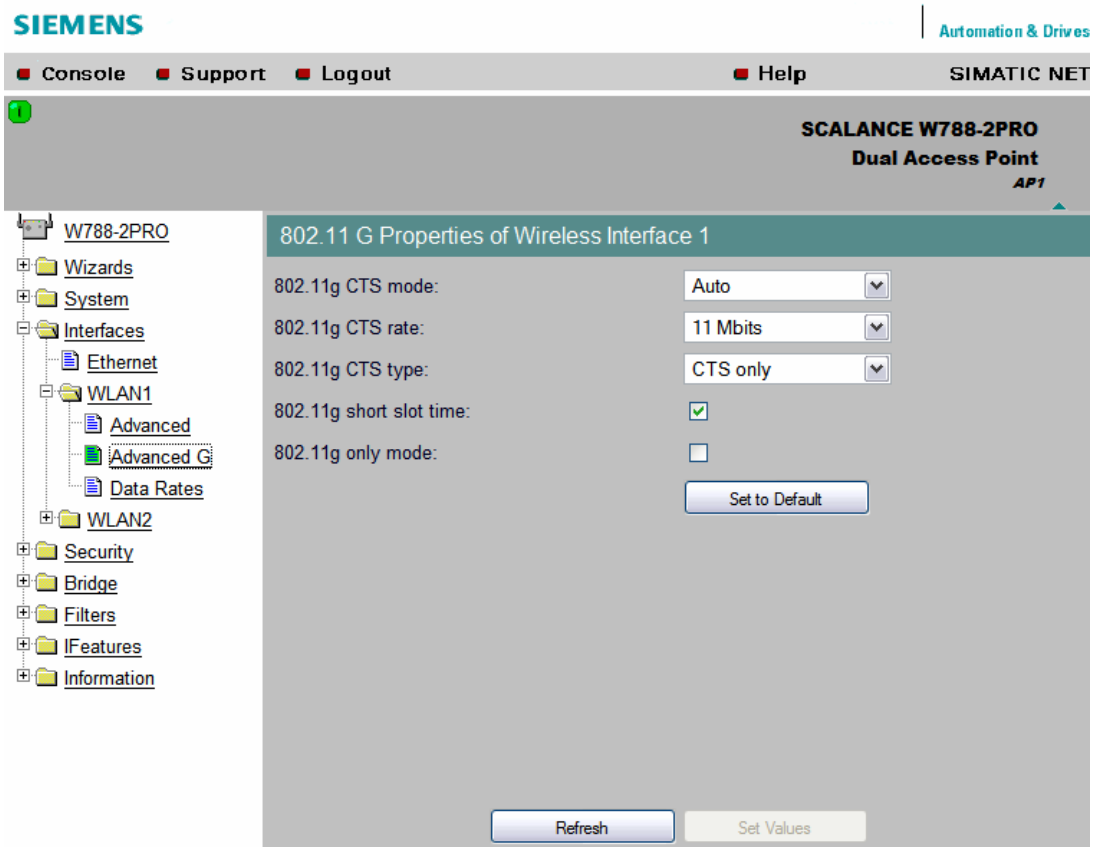


„Connect to ANY SSID" - wybranie tej opcji spowoduje, że nasz moduł klienta będzie starał się połączyć z AP o najlepszej jakości sygnału oraz odpowiadającymi zabezpieczeniami. Nie ma w tym wypadku możliwości połączenia ze stacją bazową, która nie rozsyła jawnie SSID (opcja „Suppress SSID broadcasting„).

Jeżeli powyższa opcja nie jest wybrana, moduł stara się połączyć z AP o najlepszych parametrach transmisji, którego SSID znajduje się na liście.
Lista może zawierać maksymalnie 32 wpisy.

Advenced G

Opcje tej karty dotyczą bezkolizyjnej transmisji w trybie 802.11g ze stacjami pracującymi w trybie 802.11b.



„802.11g CTS Mode” - pozwala na wybór trybu działania mechanizmu RTS/CTS.

Dostępne opcje:
- „0 do not use RTS/CTS” - wyłącza mechanizm;
- „1 always use RTS/CTS with 802.11g packets” - w trybie 802.11g włączony zawsze;
- „2 only use RTS/CTS when there are 802.11b clients in environment” - używa mechanizmu, tylko jeżeli w otoczeniu znajdują się klienci pracujący w trybie 802.11b.

„802.11g CTS Rate” - pozwala na wybór prędkości transmisji ramek RTS/CTS.

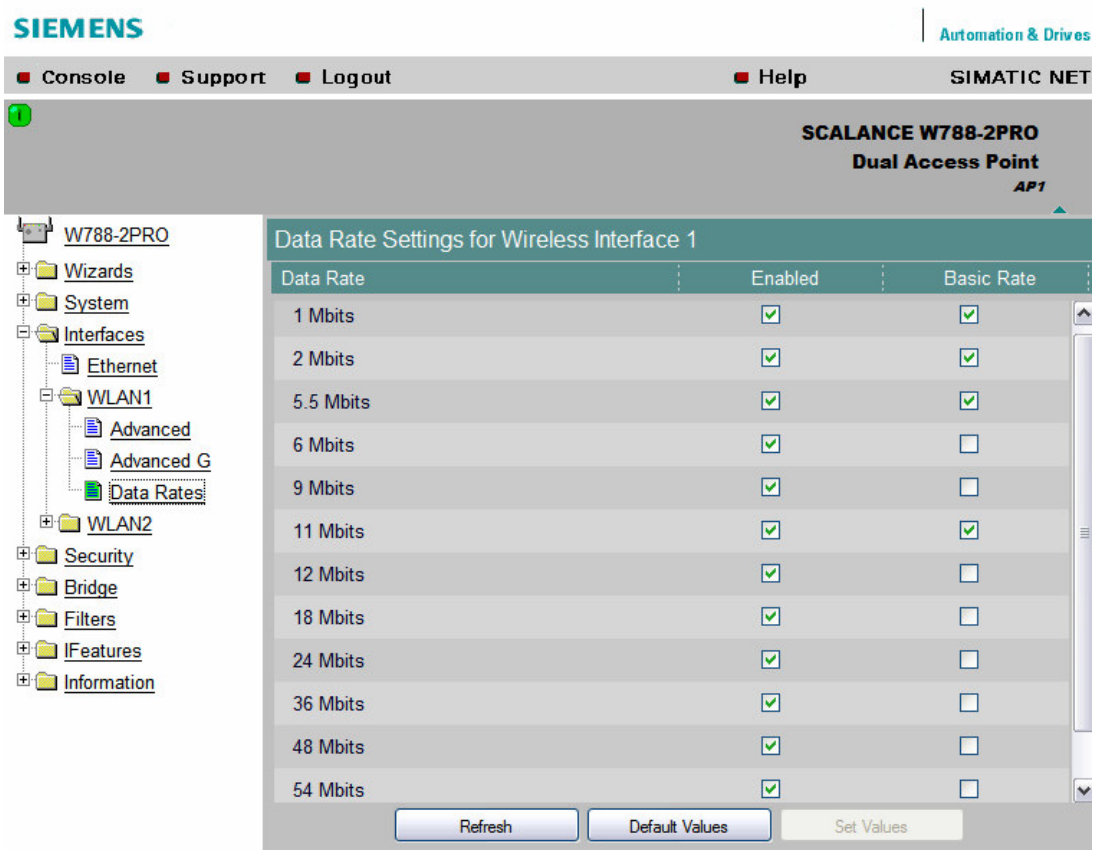
„802.11g CTS Type” - określa typ sygnałów mechanizmu. Możemy wysyłać tylko ramki CTS, rozsyłane przez AP lub oba typy RTS - żądanie klienta i CTS - odpowiedź AP.

„802.11g Short Slot Time” - włącza wykorzystywanie tzw. „krótkiego czasu szczeliny” (czas oczekiwania na zgłoszenia stacji), mającego na celu przyśpieszenie transmisji.
Wszystkie urządzenia muszą obsługiwać tą opcję.

„*802.11g Only Mode”* - wybranie tej opcji pozwala na połączenie tylko z klientami pracującymi w trybie 802.11g, nie dopuszcza do połączenia ze stacjami pracującymi w trybie 802.11b.

Data Rates

W tym oknie dokonujemy wyboru obsługiwanych prędkości transmisji.

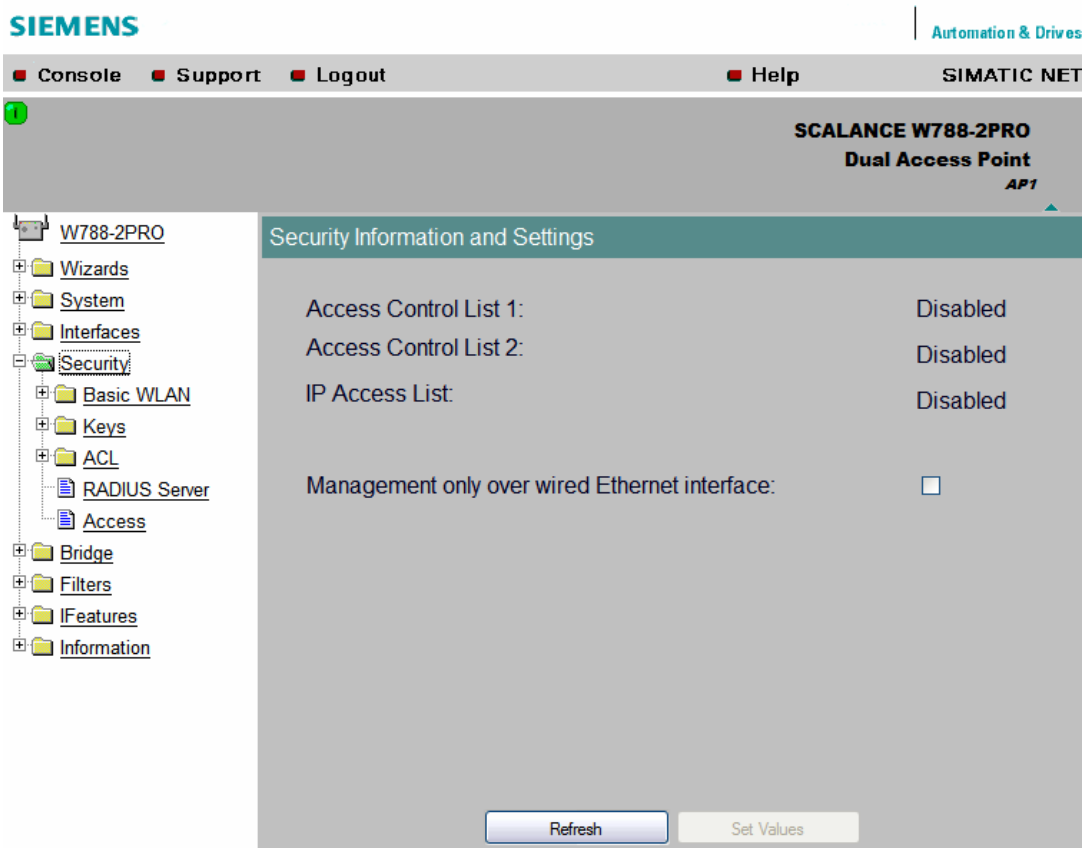


W kolumnie „*Data Rate*” wybieramy prędkości transmisji, jakie będzie obsługiwała nasza stacja.

Prędkości transmisji wybrane w kolumnie „*Basic Rates*” muszą być obsługiwane przez klientów, którzy chcą się połączyć z naszym AP.

4. Zakładka „Security”

W tym punkcie zostanie omówiony zestaw opcji związanych z zabezpieczeniami dostępu do modułu oraz bezpieczeństwem transmisji bezprzewodowej.



W oknie głównym widzimy stan dostępnym opcji zabezpieczeń „*Access Control List*” dla interfejsów WLAN oraz „*IP Access List*”.

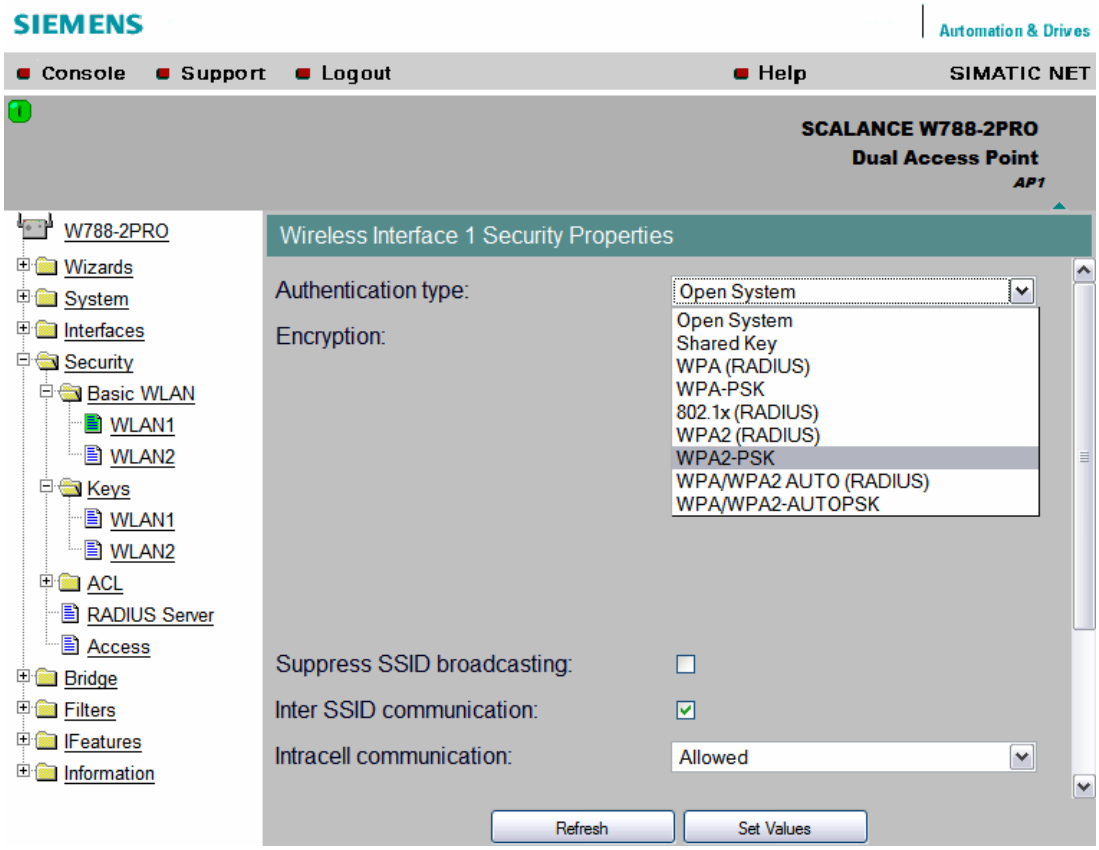
„*Access Control List*” pozwala na kontrolę dostępu na poziomie adresów MAC. Z danym interfejsem mogą połączyć się tylko stacje, o adresach MAC zawartych na liście.

„*IP Access List*” pozwala na dostęp klientom, którzy posiadają przypisany adres IP znajdujący się na liście.

Opcja „*Management only over wired Ethernet interface*” ogranicza dostęp do ustawień oraz informacji systemowych modułu do użytkowników połączonych z urządzeniem przez interfejs Ethernet’owy.
Umożliwia to fizyczne zabezpieczenie modułu przed intruzami.

Basic WLAN

W oknie tym dokonujemy ustawień zabezpieczeń transmisji bezprzewodowej.



„*Authentification type*" pozwala na wybór metodu autentyfikacji użytkowników sieci. Do wyboru mamy następujące poziomy zabezpieczeń:

1) Open System

   W tej opcji wyłączone są wszelkie zabezpieczenia, z naszym modułem może połączyć się każdy, kto jest w zasięgu sieci bezprzewodowej.
   Poziom ten jest ustawiony domyślnie i zaleca się jego zmianę.
   W trybie tym możemy uzyskać pośrednio szyfrowanie danych, bez autentyfikacji, przez dodatkowe ustawienie klucza aktywując opcję „Encryption".

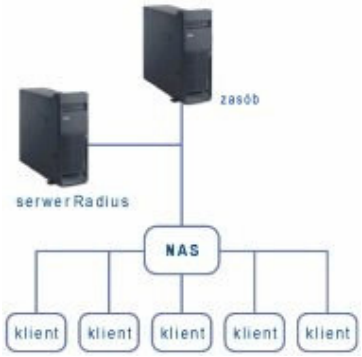
2) Shared key

   Zabezpieczenie na poziomie współdzielonego klucza. Zestaw kluczy zabezpieczających dostęp i transmisję danych podajemy w karcie „*Keys*", natomiast aktualnie aktywny klucz wybieramy w polu „*Default WEP key*".

   Skuteczność tych zabezpieczeń jest niska, aczkolwiek daje małe obciążenie transmisji.

3) WPA (RADIUS)

W przypadku dużej liczby klientów, proces uwierzytelniania, autoryzacji oraz rejestracji dostępu do zasobów przejmuje w sieci dodatkowy serwer RADIUS (Remote Authentication Dial In User Service). Ideę przedstawia rysunek obok. NAS (Network Access Server) to w naszym przypadku Access Point.
Jeżeli nasza sieć posiada taki serwer, mamy możliwość jego wykorzystania poprzez konfigurację naszego modułu, różniącą się w zależności od tego w jakim trybie pracuje.



Do szyfrowania możemy wykorzystać metody (pole „*Cipher*”):
TKIP (Temporal Key Integrity Protocol) i AES (Advenced Encryption Standard).
TKIP wykorzystuje algorytm RC4, a jego główna siła to zmieniające się w czasie wartości kluczy, automatycznie wyprowadzane od klucza głównego. TKIP przeprowadza również korekcję uszkodzonych pakietów.
AES implementuje lepszy algorytm Rijndael'a i rozwija możliwości TKIP.

Klucz początkowy generowany jest przez serwer RADIUS.

Ustawień połączenia z serwerem zabezpieczeń dokonujemy w karcie „RADIUS Serwer”.

4) 802.1x RADIUS

Opcja ta również korzysta z zewnętrznego serwera RADIUS, którego właściwości opisano wcześniej.
W odróżnieniu jednak od WPA szyfrowanie danych realizowane jest za pomocą słabego klucza WEP generowanego przez serwer zewnętrzny.

Ustawień połączenia z serwerem zabezpieczeń dokonujemy w karcie „RADIUS Serwer”.

5) WPA-PSK

WPA-PSK, w odróżnieniu od WPA, nie wykorzystuje serwera RADIUS, a jedynie klucz (*pass phrase*), który jest przechowywany na wszystkich stacjach należących do sieci.

Ten właśnie klucz wprowadzamy do ustawień naszego modułu (min. 8 znaków) w polach „*Pass phrase*” i „*Pass phrase conformation*”.

6) WPA2 (RADIUS)

   Rozwiązanie bazuje na standardzie WPA2 (Wi-Fi Protected Access 2) i implementuje funkcje 802.11i. WPA2 posiada dodatkowy protokół szyfrowania CCMP oraz umożliwia szybkie przełączanie się pomiędzy stacjami oraz logowanie na kilku punktach dostępowych bez standardowych procedur identyfikacji.

   Ustawiamy rodzaj metody szyfrowania (TKIP lub AES) w polu „*Cipher*" oraz wprowadzamy ustawienia połączenia z serwerem RADIUS w karcie „RADIUS Server" (tak jak opisano to we wcześniejszych punktach).

7) WPA2-PSK

   Ta opcja zapewnia zabezpieczenia oferowane przez standard WPA2, jednak zamiast zewnętrznego serwera do uwierzytelniania wykorzystujemy klucz dostępu, który wprowadzamy do naszego modułu oraz urządzeń, z którymi ma on się łączyć.
   Klucz dostępu (min. 8 znaków) wprowadzamy w polach „*Pass phrase*" i „*Pass phrase conformation*".

8) WPA/WPA2 AUTO (RADIUS)

   Opcja pozwala na współpracę naszej stacji z klientami, którzy wykorzystują zabezpieczenia WPA lub WPA2 oraz autentyfikację poprzez serwer RADIUS, automatycznie przełączając się w odpowiedni tryb.
   Metoda szyfrowania musi jednak być ustawiona taka sama na wszystkich stacjach.

9) WPA/WPA2 AUTO PSK

   Opcja pozwala na współpracę naszej stacji z klientami, którzy wykorzystują zabezpieczenia WPA lub WPA2 oraz autentyfikację za pomocą wspólnego klucza PSK, automatycznie przełączając się w odpowiedni tryb.
   Metoda szyfrowania musi jednak być ustawiona taka sama na wszystkich stacjach.

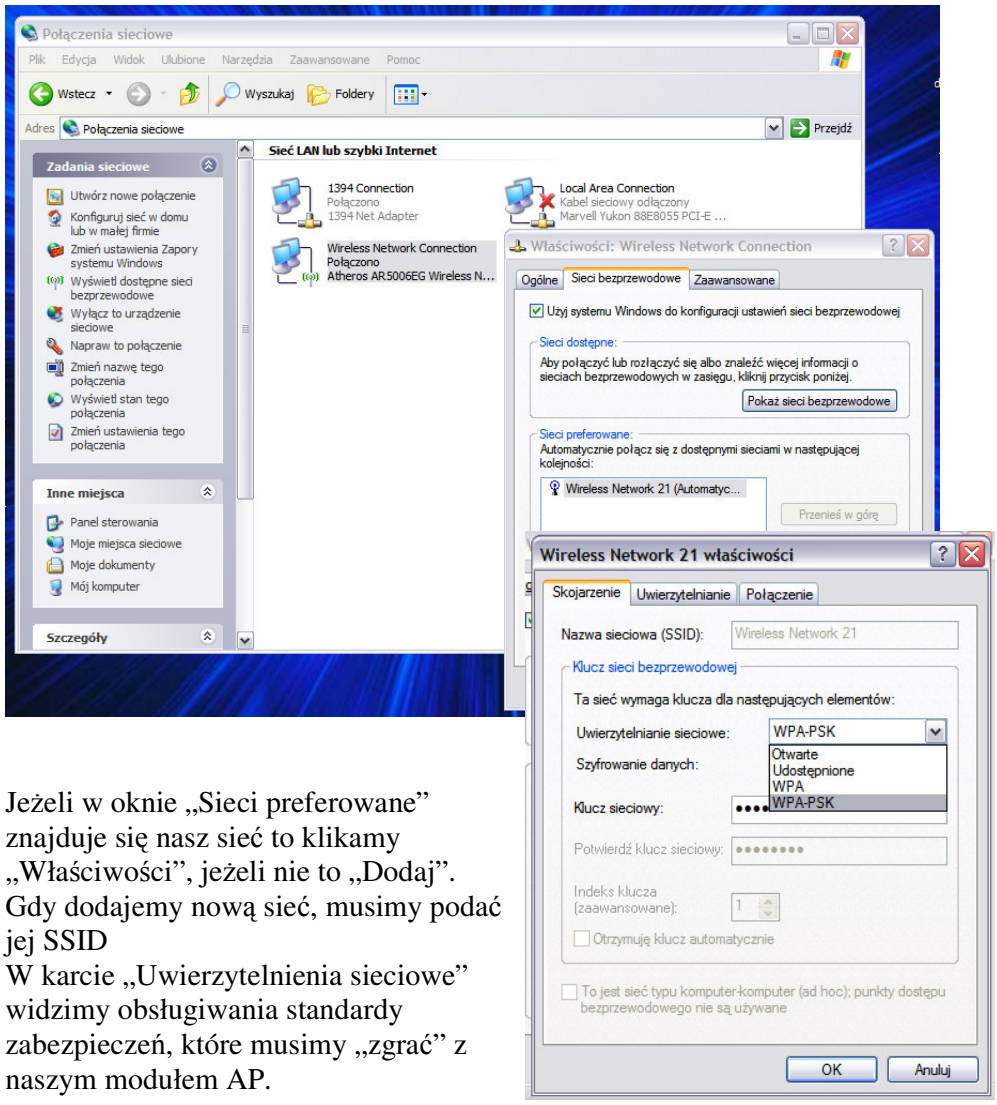
Uwaga!

Należy pamiętać, że stacja kliencka musi obsługiwać tryby zabezpieczeń, które ustawimy w naszym module.
O ile w przypadku współpracy modułów SCALANCE W nie ma tutaj żadnych problemów, o tyle sytuacja może ulec zmianie, jeżeli nasza stacja jest innego producenta lub zarządzana przez inny system operacyjny.

Warto przytoczyć przypadek stacji z systemem Windows.
Do systemu stacji klienckiej musimy wprowadzić odpowiedni dla danej sieci uwierzytelnienia.

System domyślnie przyjmuje zabezpieczenia na poziomie WEP i przy próbie połączenia z siecią zabezpieczoną prosi o podanie takowego klucza. Jeżeli mamy inne zabezpieczenia, musi skonfigurować je sami.

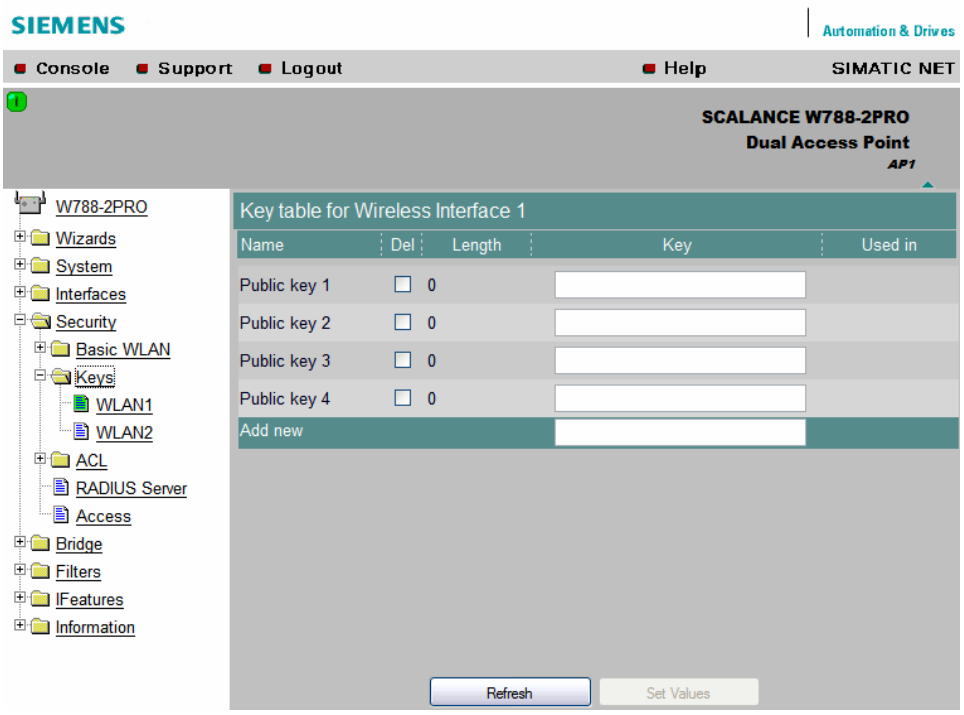
W tym celu przechodzimy do „Start -> Ustawienia -> Panel sterowania -> Połączenia sieciowe”, wybieram interfejs połączenia bezprzewodowego (zazwyczaj „Wireless Network Connection”), otwieramy „Właściwości” i przechodzimy do zakładki „Sieci bezprzewodowe”.



Jeżeli w oknie „Sieci preferowane” znajduje się nasz sieć to klikamy „Właściwości”, jeżeli nie to „Dodaj”.
Gdy dodajemy nową sieć, musimy podać jej SSID
W karcie „Uwierzytelnienia sieciowe” widzimy obsługiwania standardy zabezpieczeń, które musimy „zgrać” z naszym modułem AP.

Keys

Karta służy do wpisywania kluczy WEP, wykorzystywanych w zabezpieczeniach typu Shared Key.



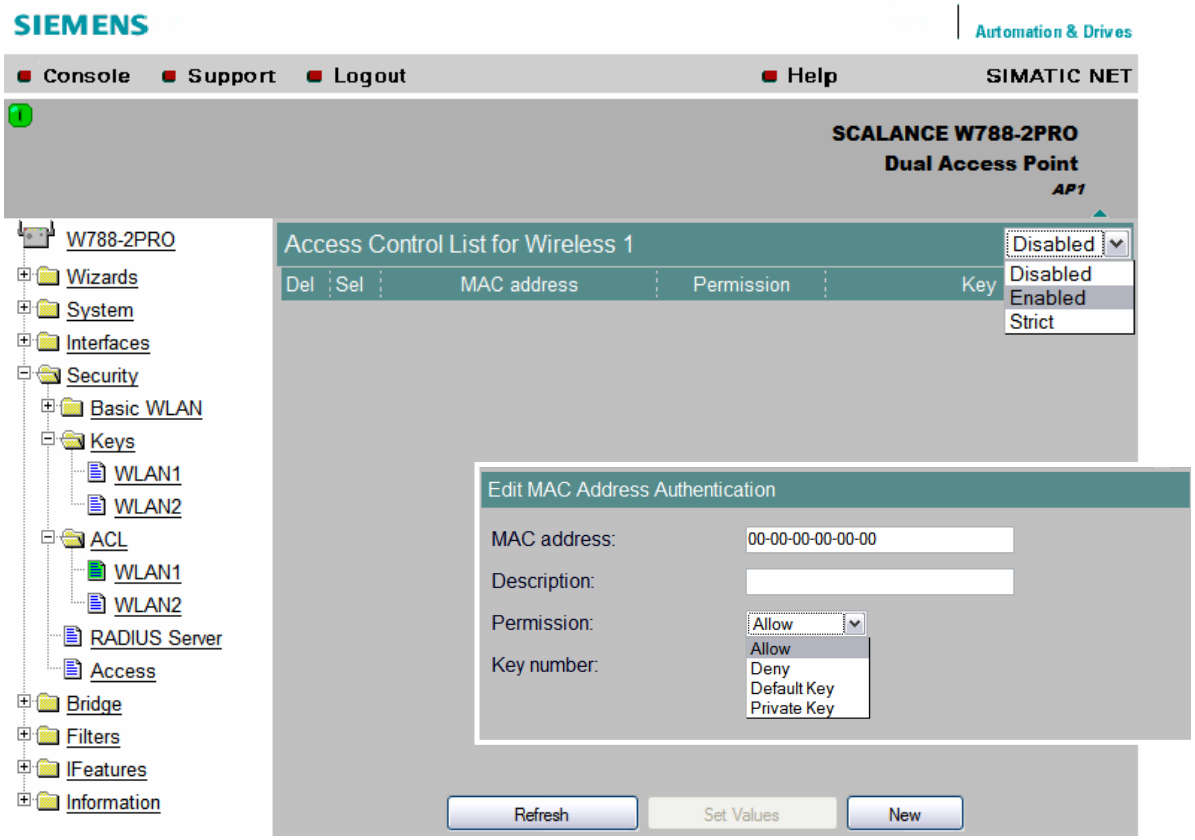
Wartość klucza może być podana w kodzie ASCII (znaki klawiatury) lub jako liczba szesnastkowa (cyfry 0-F).
Jego długość może wynosić 40, 104 lub 128 bitów (5, 13 i 16 znaków ASCII lub 10, 26 i 32 cyfry szesnastkowe).
Im dłuższy klucz tym lepsze zabezpieczenie, ale i większe obciążenie transmisji.

Możemy wiele różnych kluczy, natomiast w danym momencie używany będzie ten wybrany jako „*Default key*”.

Używany klucz powinien być jak najczęściej zmieniany, ponieważ podsłuchanie ok. 2GB zaszyfrowanych danych pozwala na rozkodowanie klucza!

ACL

Okno „*Access Control List*” pozwala na kontrolę klientów na poziomie adresów MAC interfejsów bezprzewodowych.



W głównym oknie mamy do wyboru opcje:

- - „*Disabled*” – ACL nieaktywne;
- - „*Enabled*” – klienci umieszczeni na liście, traktowani są zgodnie z wpisem w polu „*Permission*”, natomiast pozostali klienci mają dostęp do AP.
  Opcja wygodna, jeśli chcemy wykluczyć pewnych klientów.
- - „*Strict*” - klienci umieszczeni na liście, traktowani są zgodnie z wpisem w polu „*Permission*”, klienci, których nie ma na liście nie mają dostępu.
  Opcja wygodna, gdy chcemy nadać dostęp pewnej grupie klientów.

Po kliknięciu w „*New*”, pojawia się przed nami okno edycji nowego klienta.
„*MAC address*” zawiera adres MAC interfejsu klienta.
W pole „*Description*” możemy wprowadzić opis ułatwiający identyfikację stacji.
Pole wyboru „Permission” określa prawa dostępu:

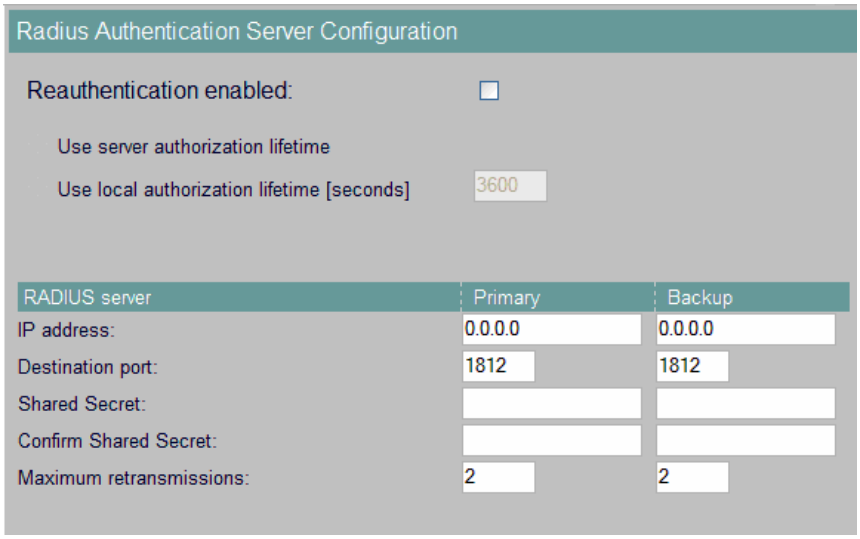
- - „*Allow*” – klienta ma dostęp do AP;
- - „*Deny*” – brak dostępu;
- - „*Default Key*” – dostęp, jeżeli klient używa klucza ustawionego w AP, jako „*Default Key*”;
- - „*Private Key*” – dostęp, jeżeli klient ma ustawiony „*Private Key*” (tryb klienta, Security -> Basic WLAN) zgodny z jednym w kluczy w AP, wybranym w polu „*Key number*”.

RADIUS Server

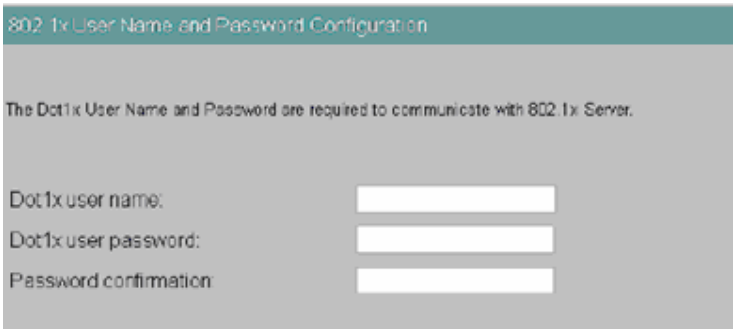
W trybie „*Access Point*”
podajemy adres IP oraz port serwera RADIUS. Dodatkowo musimy wpisać i potwierdzić hasło dostępu do serwera (*Shared Secret* – max. 128 znaków).

W polu „*Maximum retransmission*” podajemy liczbę prób połączenia (0-5). Oprócz podstawowej konfiguracji „*Primary*”, możemy wprowadzić ustawienia awaryjne „*Backup*”, które będą wykorzystanie w przypadku niepowodzenia w pierwszym przypadku.

Zaznaczenie opcji „*Reauthentification enabled*” powoduje wymuszenie ponownej autentyfikacji klienta po upływie określonego czasu.
Jeżeli wybierzemy „*Use server authorization lifetime*”, to czasem tym zarządza serwer RADIUS, natomiast wybór „*Use local authorization lifetime*” umożliwia wprowadzenie tego czasu w sekundach
(min. 60, domyślnie 3600, max. 43200 – 12 godzin).

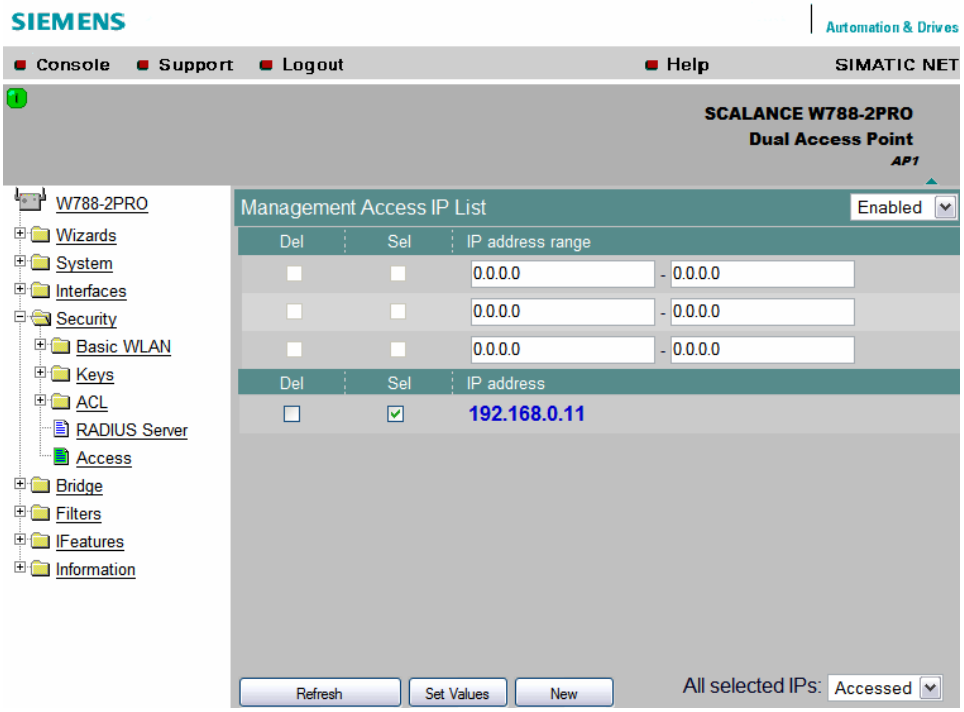


W trybie „*Client*”
wprowadzamy nazwę użytkownika oraz hasło autentyfikacji w systemie 802.1x.



Access

Karta pozwala na ustawienie dostępu do ustawień systemowych według adresów IP.



Aby aktywować ACL, musimy w oknie głównym karty ustawić „*Enabled*”; domyślnie jest wyłączona („*Disabled*”).

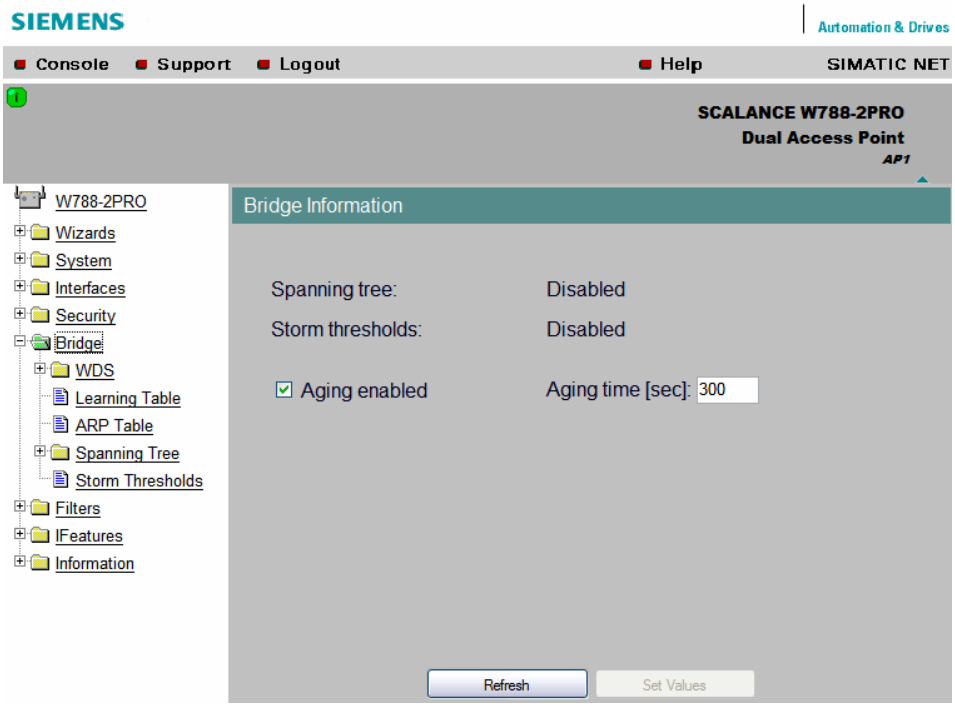
Może wprowadzić trzy zakresy adresów IP w polach „*IP address range*” oraz pojedyncze adresy poprzez przycisk „*New*”.
Kolumna „*Sel*” służy do wyboru stacji, dla których stosowane będą prawa dostępu ustawione w polu „*All selected IPs*”:
- „*Accessed*” – zezwolenie na dostęp do ustawień systemowych;
-„*Denied*” – brak dostępu.

Kolumna „*Del*” pozwala na wybór wpisów, które chcemy usunąć.

Wszelkie zmiany zatwierdzamy przez „*Set Values*”.

5. Zakładka „Bridge”.

Ten zestaw opcji pozwala na ustawiania modułu dotyczące jego współpracy z innymi stacjami bazowymi.

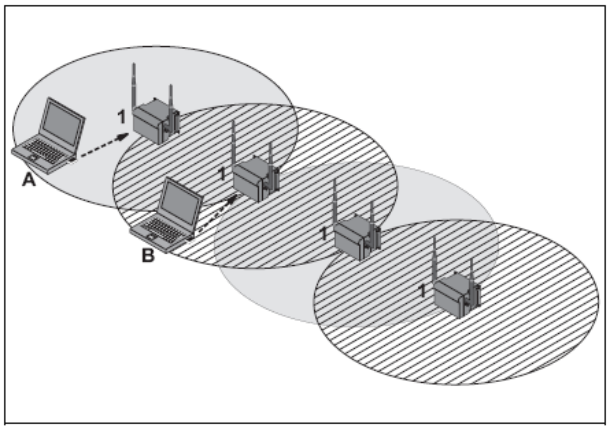


W oknie głównym widzimy stan mechanizmów optymalizacji ruchu sieciowego „*Spanning tree*” oraz „*Storm threshold*”, które zostaną opisane poniżej.

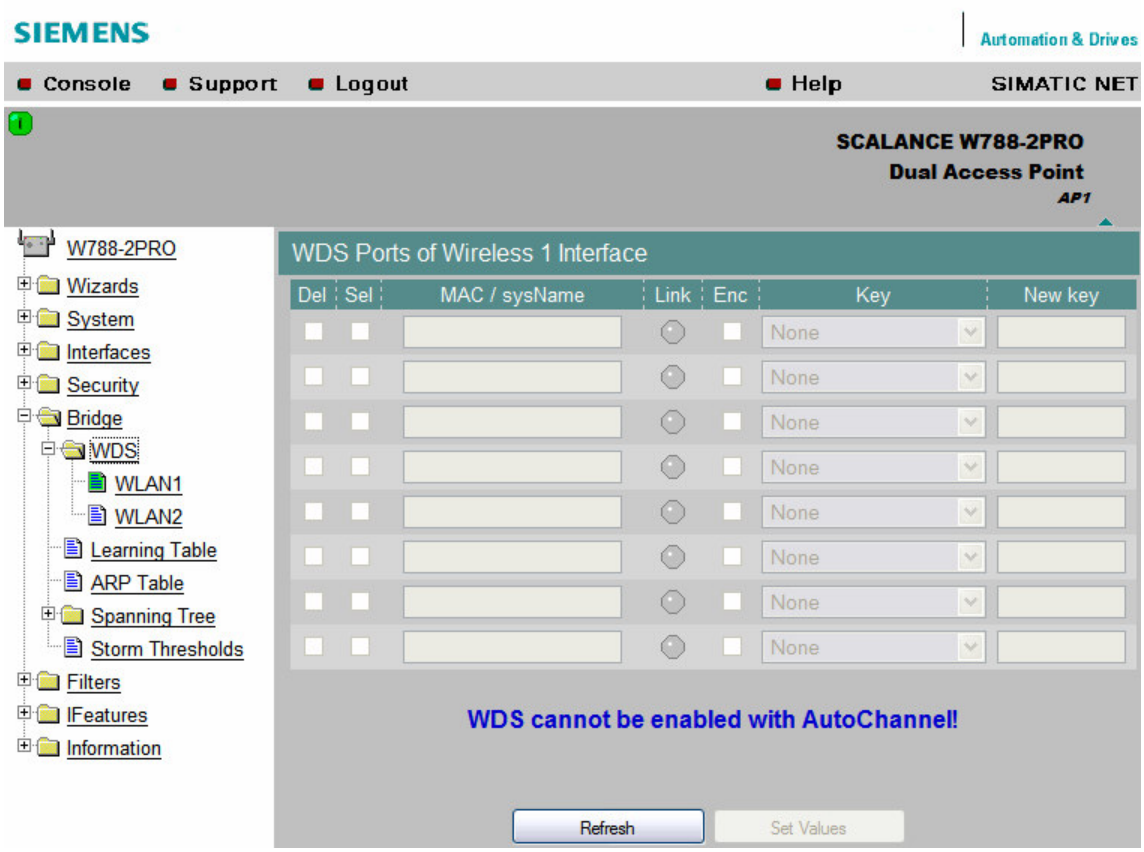
Włączenie opcji „*Aging enabled*” powoduje usuwanie z pamięci modułu informacji o nieaktywnych urządzeniach sieciowych.
Pole „*Aging time*” zawiera czas (w sekundach), po którym następuje usunięcie „przestarzałego” wpisu.

WDS

Mechanizm „*Wireless Distributed System*” umożliwia połączenie wielu zgodnych stacji AP w rozproszony system zapewniający dostęp do jednej sieci bezprzewodowej na zwiększonym obszarze.



Urządzenia w tym systemie pracują na jednym kanale nie zakłócając się, a rozszerzając zasięg danej sieci.



Chcąc aktywować WDS nie możemy korzystać z opcji „*AutoChannel*”.
Kanał musi być przypisany na „sztywno”, taki sam na wszystkich stacjach mających pracować w tym systemie.

W kolumnie „*MAC/sysName*” wprowadzamy adres MAC lub nazwę systemową stacji, z którymi mamy się połączyć w ramach WDS.

Zaznaczenie opcji „*Enc*” powoduje włączenie szyfrowania. Może ono być przeprowadzane z użyciem mechanizmu WEP lub AES (opisane w punkcie „*Security*”).

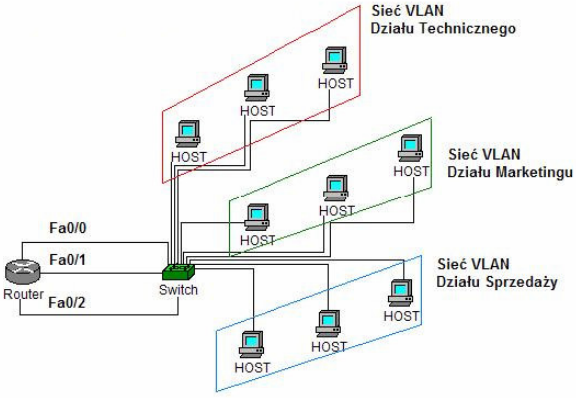
Wymagane klucze wprowadzamy w polu „*New Key*”, natomiast aktywny klucz wybieramy w polu „*Key*”.

Aktywne połączenia muszą być wybrane w kolumnie „*Sel*”, a ich stan jest sygnalizowany w polu „*Link*”.

Uwaga!

Nie zaleca się stosowania tego mechanizmu w trybie 802.11h, ponieważ ze względu na wbudowane w ten standard narzędzie DFS, stacja bazowa po wykryciu uprzywilejowanego urządzenia pracującego na tym samym kanale, automatycznie przełącza się na inny kanał, burząc tym samym strukturę WDS.

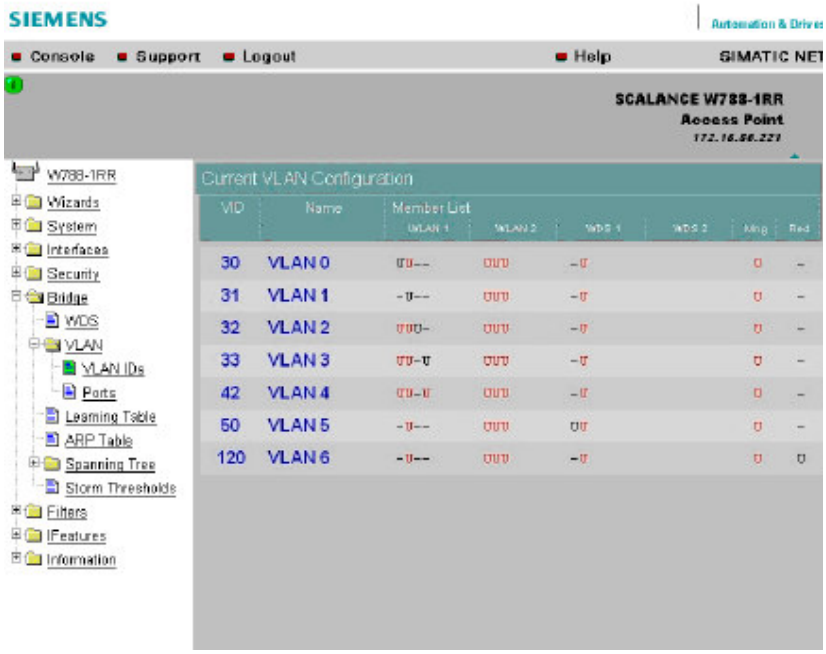
VLAN



Wirtualna sieć lokalna Virtual LAN pozwala na tworzenie logicznych domen rozgłoszeniowych (czyli podsieci urządzeń objętych adresami IP z puli jednej maski) niezależnie od fizycznej struktury sieci.
Jest to możliwe dzięki urządzeniom przełączającym typu Switch, które mają możliwość przypisania swoich portów komunikacyjnych do logicznych struktur sieciowych.
Na przykładowym rysunku widzimy jedną sieć fizyczną rozdzieloną na trzy sieci logiczne. Oczywiści połączenia wirtualne mogą być realizowane za pomocą większej ilości przełączników.
Informacja o przynależności danego urządzenia do określonej sieci wirtualnej umieszczona jest w dodatkowym polu ramki sieciowej. Jeżeli ramka pochodzi od urządzenia, które nie jest przypiasne do żadnego VLAN, pole to jest puste. Stąd termin tagged/untagged (oznaczona/nieoznaczona).

Moduły SCALANCE W umożliwiają szczegółową konfigurację sieci VLAN, która jednak wymaga pewnej znajomości tematu oraz analizy ruchu sieciowego.

W pierwszym oknie widzimy wykaz skonfigurowanych sieci VLAN.



„*VID*" zawiera numer identyfikacyjny danej sieci wirtualnej.
„*Name*" to nazwa służąca do identyfikacji sieci w naszym systemie.
Pole „*Member List*" zawiera listę interfejsów naszego modułu. Każda pozycja w polu danej kolumny odpowiada portowi, którego pozycja zależy od jego ID (np. WLAN 1, WLAN 1 VAP 1, WLAN 2 VAP 2… or WLAN 1 WDS 1, WLAN 1 WDS 2...).
Dodatkowo zamieszczone są kolumny odpowiadające portowi zarządzania systemem "*Mng*" oraz redundancji "*Rnd*".

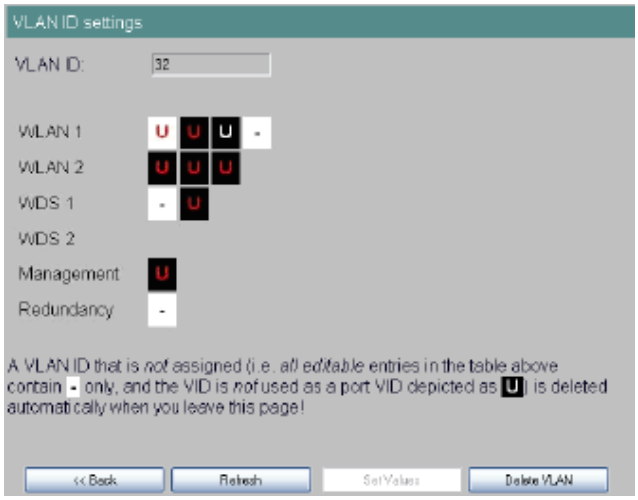
Uwaga.
Interfejs Ethernet'owy nie usuwa tagów z wychodzących ramek, jeżeli używamy VLAN, natomiast interfejsy WLAN usuwają.

Oznaczenia:

- „U"
  - VID tego portu nadawany jest nieoznaczonym ramkom WLAN.
  - oznaczone ramki Ethernet'owe są przekazywane przez ten port.
- „ – „
  - wszystkie ramki Ethernet'owe (za wyjątkiem tych, które mają VID tego portu) oraz pozostałe ramki nieoznaczone lub nieskonfiguroVID są blokowane.

Kolor czerwony odpowiada portom w tabeli, czarny portom przypisanym do danego VID.

Klikając na dowolny wiersz w pole zaznaczone na niebiesko, przechodzimy do karty konfiguracyjnej danego VLAN.



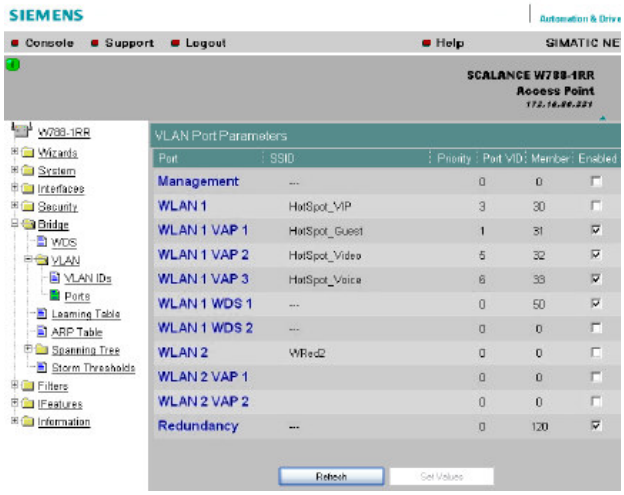
Pola na karcie odpowiadają polom w tablicy głównej.

Oznaczenia:

-	Pole edytowalne (zmiana na „U”). Jeżeli wszystkie pola oznaczone są w taki sposób dany VID jest usuwany.
U	Pole edytowalne (zmiana na „-„)
-	Pole nieedytowalne. Wszystkie wejścia dla danego VLAN zostały wykorzystane.
U	Pole nieedytowalne. VID jest przypisane do portu.
U	Pole nieedytowalne. Port jest przypisany do wszystkich VID.

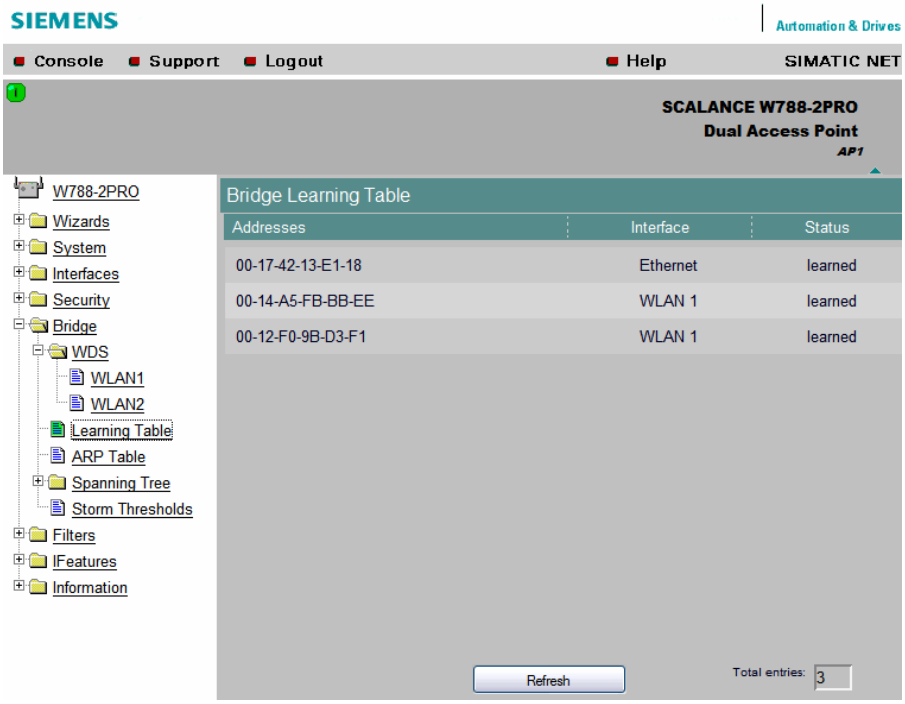
Ports

Okno to przedstawia dostępne porty, ich konfigurację oraz pozawala na ich aktywację lub dezaktywację.



Learning Table

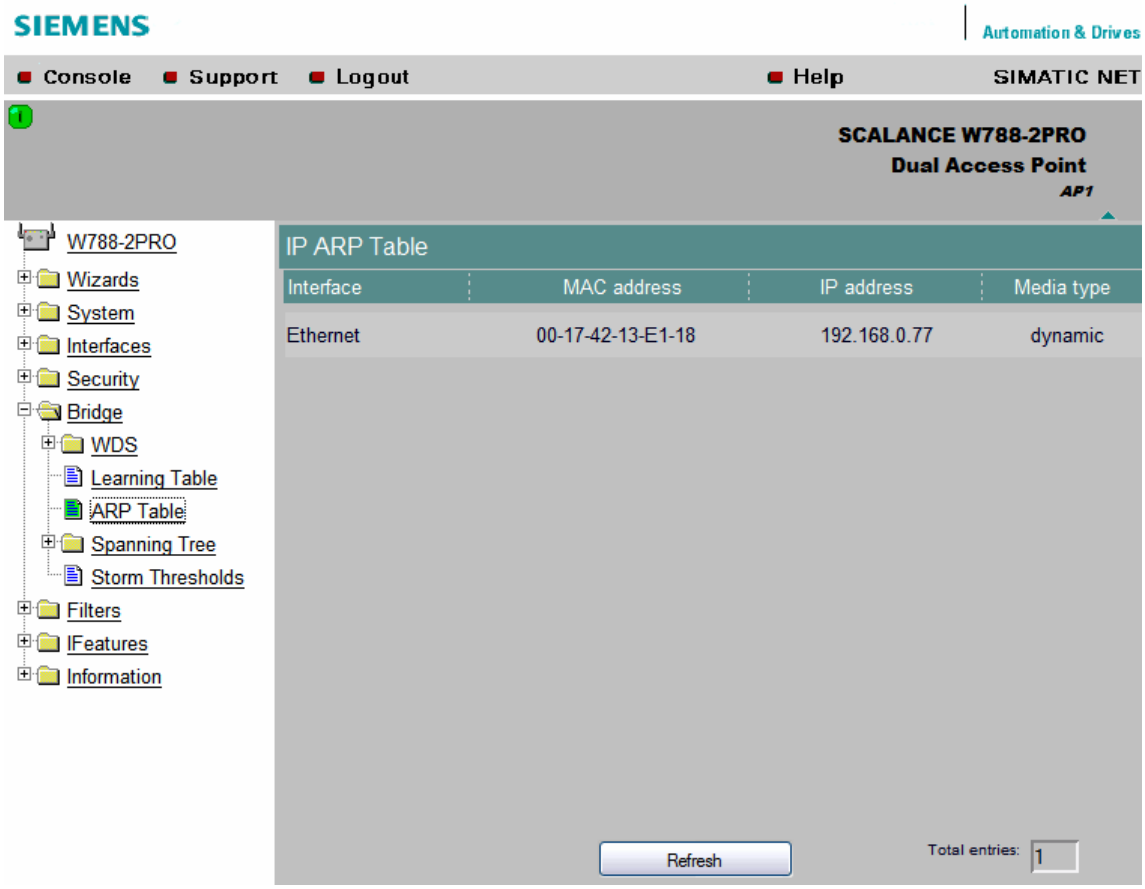
Karta ta wyświetla tablicę urządzeń, z którymi nasz moduł nawiązał połączenie. W przypadku aktywacji opcji „*Aging*”, wpisy z tej tablicy są usuwane po czasie nieaktywności połączenia określonym przez parametr „*Aging time*”.



Kolumna „*Addresses*” zawiera adresy MAC urządzeń, natomiast pola „*Interface*” wskazują przez jaki interfejs uzyskano z nimi połączenia.

ARP Table

Karta zawiera informacje uzyskiwane przez „*Address Resolution Protocol*”, który przypisuje adresy IP, do konkretnych urządzeń identyfikowanych przez adresy MAC.

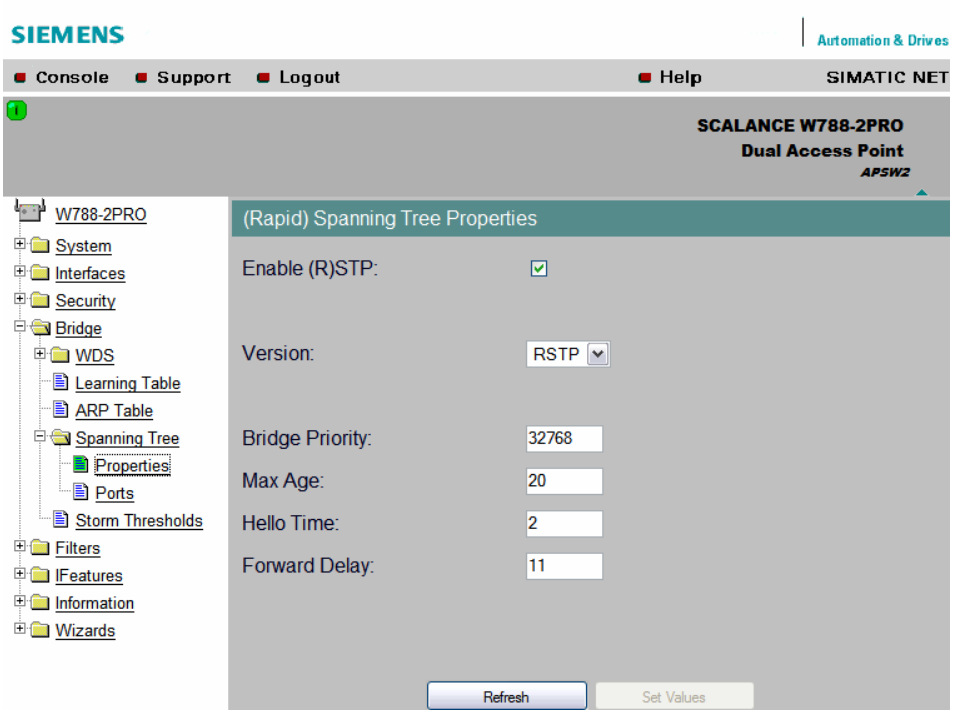


Kolumna „*Interface*” wskazuje przez jaki interfejs uzyskano połączenie.

„*Media type*” może zawierać wpis „*dynamic*”, co oznacza, że informację ARP uzyskano przez połącznie z urządzeniem, lub „*static*”, jeżeli informacja wynika z dokonanego w AP przypisania.

Spanning Tree

Aktywacja mechanizmu Spanning Tree zabezpiecza sieć redundantną przed powstawaniem zapętleń pakietów, które obniżają wydajność sieci, a w końcowym efekcie powodują utratę komunikacji pomiędzy stacjami.



Aby aktywować Spanning Tree, zaznaczamy opcję „*Enable (R)STP*" oraz wybieramy jego ulepszoną, szybszą w rekonfiguracji wersję RSTP, jeżeli inne stacje w sieci są z tym protokołem zgodne.

Pozostałe pola najlepiej pozostawić bez modyfikacji, jako że wymagają zaawansowanej znajomości mechanizmu, a poza tym ich wartości domyślne są dobrane optymalnie dla większości przypadków.

Pole „*Bridge Priority*" ustala priorytet danego urządzenia w procesie wyboru tzw. „root bridge", który odpowiada za zarządzanie strukturą sieci.
Im mniejsza wartość tym większy priorytet.

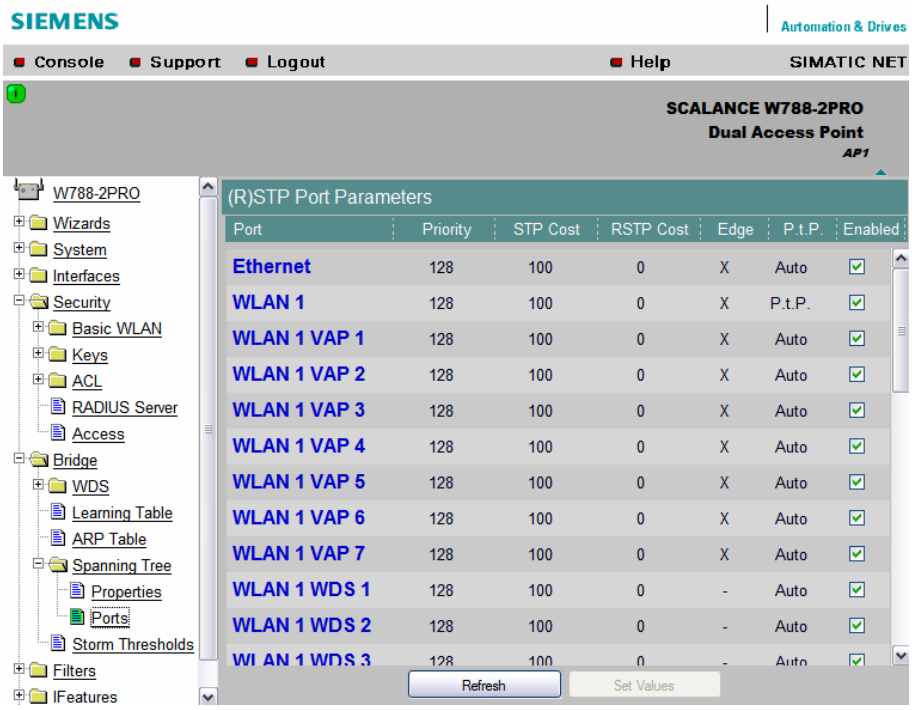
„*Max Age*" określa czas ważności przechowywanej informacji o strukturze sieci.
Po jego upływie następuje ponowne skanowanie sieci.
Wartość musi mieścić się w przedziale 6-40 sekund.

„*Hello Time*" to *interval* rozsyłania informacji o strukturze sieci, potrzebnej do konfigurowania najlepszych dróg komunikacji..
Wartość z przedziału 1-10 sekund.

„*Forward Delay*" ustala czas, po którym bridge stosuje nową konfigurację, tak, aby mieć pewność, że wszystkie urządzenia posiadają już aktualną informację.
Wartość z przedziału 4-30 sekund.

Ports

Karta pozwala na dobór parametrów dostępnych w module portów, które będą brane pod uwagę w czasie obliczania kosztu ścieżki komunikacji przez mechanizm Spanning Tree.



Po kliknięciu w pole odpowiadające danemu portowi możemy edytować widoczne w oknie głównym parametry.

Wartość w polu „*Priority*" określa priorytet danego portu spośród wszystkich dostępnych w urządzeniu przy wyborze ścieżki. Im mniejsza wartość tym większy priorytet.

„*STP Cost" oraz „RSTP Cost*" określają koszt danego portu pod względem prędkości transmisji, w zależności od wybranej wersji protokołu.
Mniejsza wartość powoduje zwiększenie prawdopodobieństwa wyboru danego portu przez mechanizm.

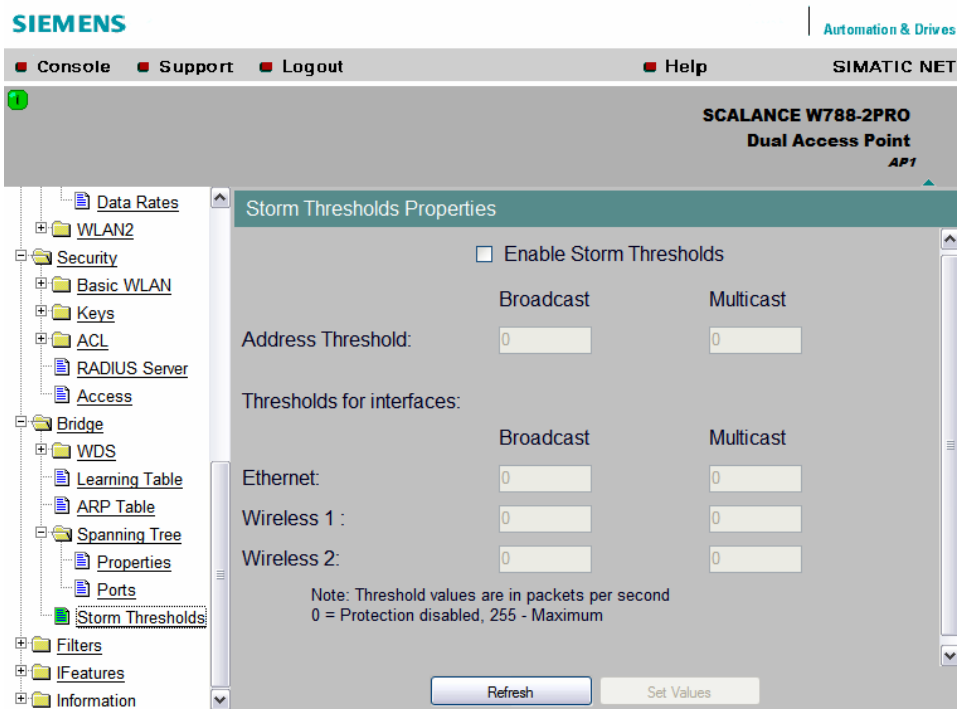
„*Edge*" – oznacza port, do którego jest podłączona stacja końcowa, bez dalszych rozgałęzień. Porty takie nie biorą udziału w wymianie danych protokołu Spanning Tree, a przełączanie się przez nie jest szybsze.
Jeżeli jednak struktura sieci zmieni się i przez port oznaczony jako „*Edge*" przejdą dane konfiguracyjne (R)STP, opcja „*Edge*" jest automatycznie odznaczana.

„*P.t.P.*" – opcja punkt-punkt, odnosi się do portów, przez które są ze sobą połączone urządzenia sieciowe obsługujące mechanizm (R)STP. Możemy im nadać następujące statusy:
- „*ForceTrue*" – niezaleznie od rodzaju połączenia, zakładana jest zawsze połączenie bezposrednie pomiedzy urządzeniami;
- „*ForceFalse*" – w żadnym wypadku nie zakładamy połączenia bezposredniego;
- „*Auto*" – połączenie wykrywane automatycznie (jeżeli włączony jest tryb halfduplex, nie zakłada się istnienia połączenia bezposredniego).

- „*Enabled*” – jeżeli to pole jest zaznaczone, port obsługuje mechanizm Spanning Tree.

Storm Threshold

Opcja ma za zadanie redukcję ruchu sieciowego przez wyłączanie przekazywania ramek rozgloszeniowych broadcast oraz multicast, po przekroczeniu progowej wartości ich natężenia.



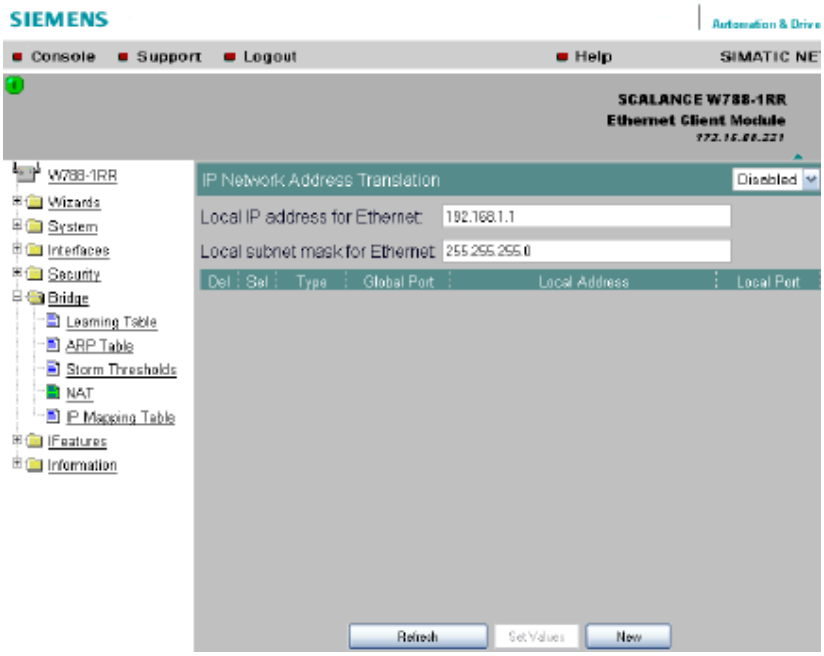
Opcja aktywowana jest w polu „*Enable Storm Threshold*”.

„*Address Threshold*” – określa próg liczby ramek na sekundę wysyłanych ciągle z tego samego adresu.

„*Thresholds for interfaces*” – pozwala na określenie progu natężenia ramek broadcast i multicast dla poszczególnych interfejsów sieciowych modułu.

NAT (tryb klienta)

Network Address Translation to usługa, która umożliwia stacjom sieci lokalnej, niewidocznym na zewnątrz, komunikację z innymi sieciami (np. Internet) za pomocą jednego zewnętrznego adresu IP ustawionym na bramie. NAT tłumaczy adresy lokalne stacji na jeden adres zewnętrzny oraz tworząc tablicę translacji kieruje ruchem odpowiednich danych do odpowiednich stacji.



Usługę aktywujemy w górnym pasku okna, ustawiając „*Enabled*”.

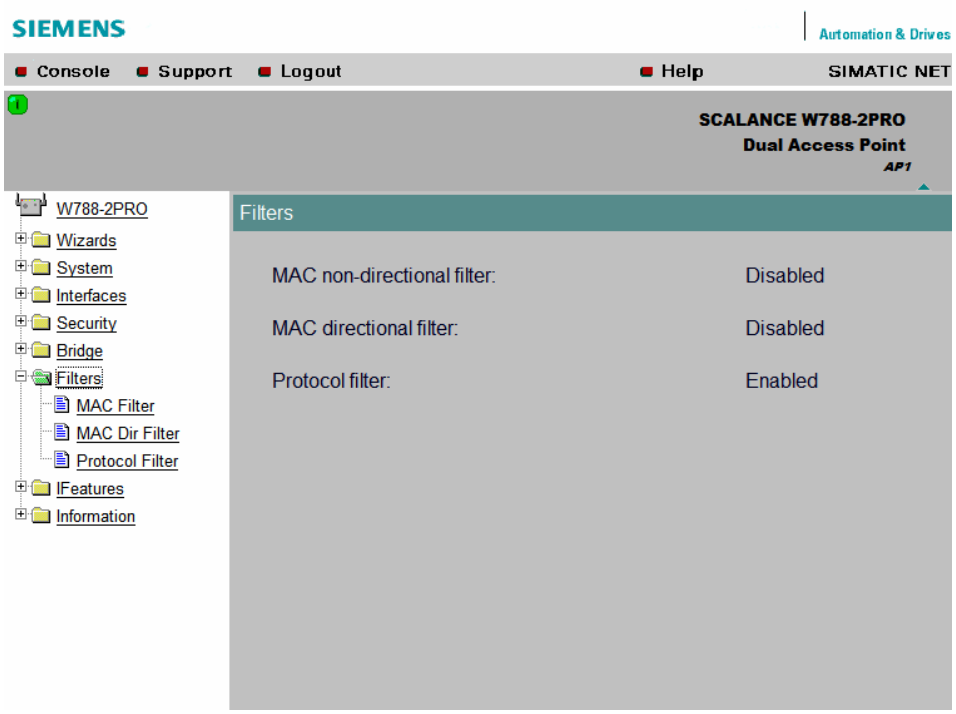
„*Local IP address for Ethernet*” – zawiera adres interfejsu Ethernet’owe klienta (adres zewnętrzny bramy podsieci LAN).
„*Local subnet mask for Ethernet*” – maska lokalnej podsieci.

Poprzez „*New*” przechodzimy do okna, który umożliwia nam za pomocą NAPT, przekierować określone porty na zewnątrz.

W polu „*Type*” wybieramy komunikację poprzez TCP lub UDP.
„*Global port*” zawiera numer portu widoczny na zewnątrz.
W pole „*Local Address*” wprowadzamy adres urządzenia w lokalnej sieci Ethernet.
„*Local Port*” odpowiada za port lokalnego urządzenia.

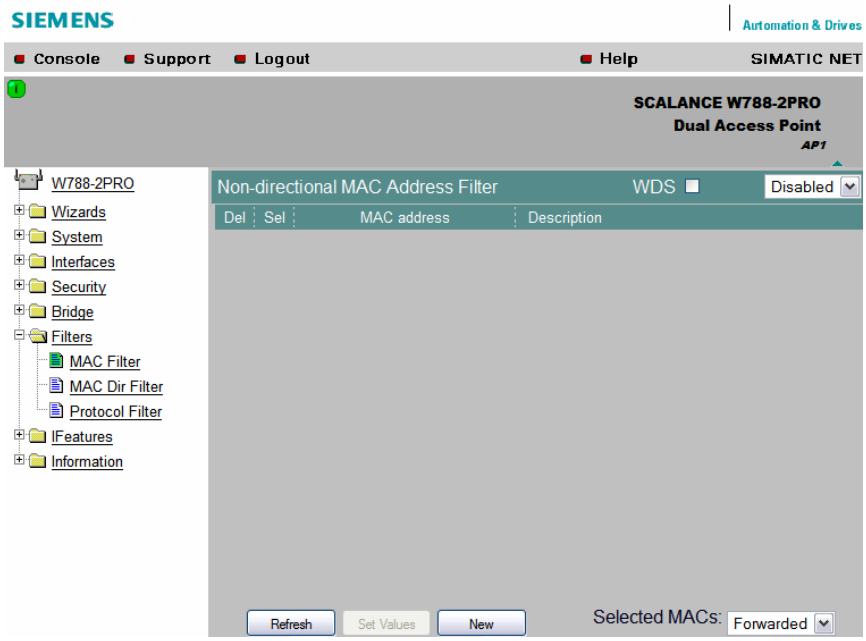
6. Zakładka „Filters”.

Zestaw opcji pozwala na filtrowanie danych na poziomie adresów MAC oraz protokołu w celu zwiększenia bezpieczeństwa lub redukcji ruchu sieciowego.
W oknie głównym zakładki widzimy stan dostępnym mechanizmów filtrowania.



MAC Filter

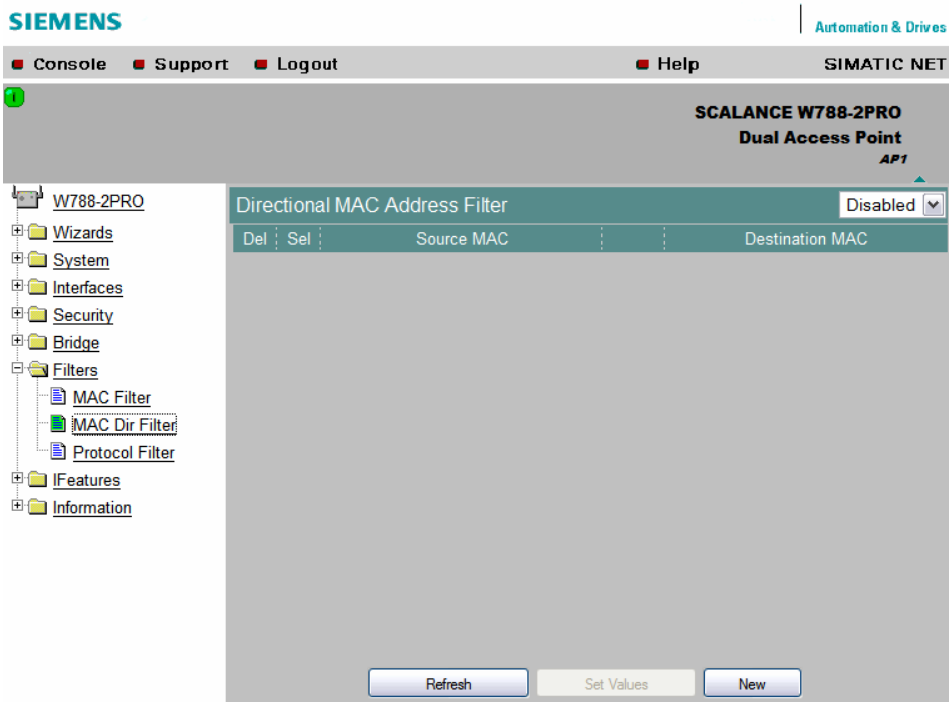
Filtr pozwala na selekcję urządzeń podłączonych do interfejsu Ethernet’owego, z którymi chcemy się komunikować.



Po kliknięciu „*New*” przechodzimy do okna, w którym uzupełniamy pola „*MAC address*” oraz „*Descritpion*”, w którym możemy podać opis identyfikujący dane urządzenie.
Maksymalnie można wprowadzić 50 adresów MAC.
Opcja „*Selected MACs*” pozwala na ustawienie polityki pakietów z wprowadzonych urządzeń na przepuszczanie – „*Forwarded*” lub blokowanie „*Blocked*”.
Aktywacja polityki dla danego adresu MAC wymaga zanaczenia w polu „*Sel*” oraz wybrania „*Set Values*”.
Jeżeli chcemy usunąć wpis zaznaczamy „*Del*” i zatwierdzamy także przez „*Set Values*”.
Zaznaczenie pola „WDS” sprawia, że do ruchu dopuszczone lub wykluczone są wszystkie stacje, które posiadają odpowiedni wpisy, w którymkolwiek z modułów wchodzącym w skład WDS, niezależnie od tego, z którym modułem są fizycznie połączone.

MAC Dir Filter

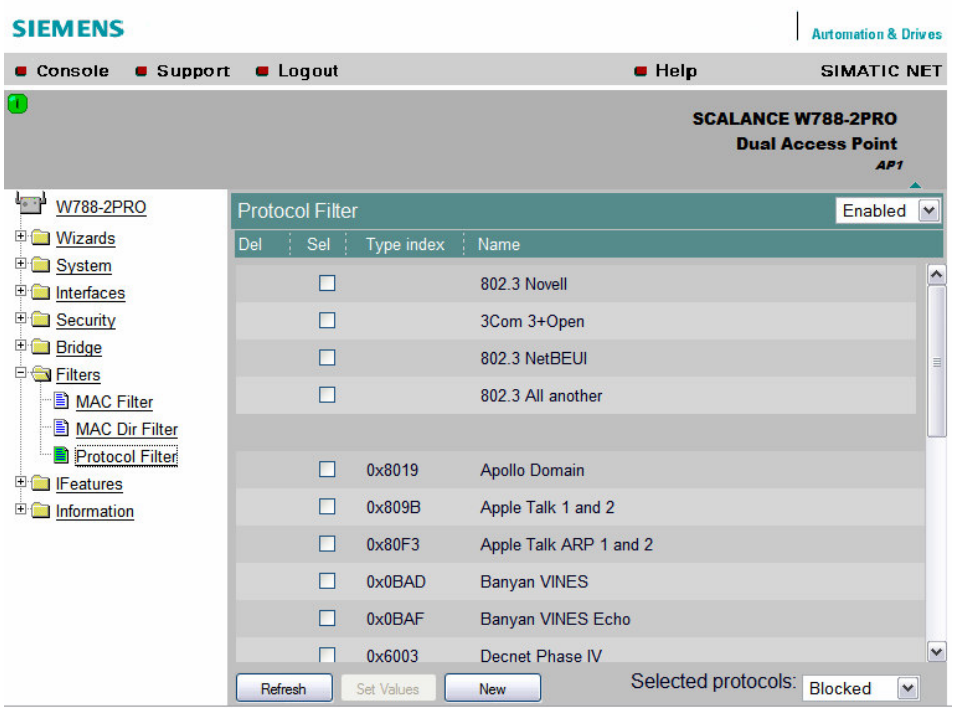
Opcja pozwala na kierunkową filtrację pakietów na podstawie adresów MAC.



Po wybraniu „*New*” wprowadzamy w pole „*Source MAC*” adres źródła pakietów, czyli stacji z których dane pakiety będą wysyłane, natomiast w pole „*Destination MAC*” adresy przeznaczenia pakietów, czyli stacji, do których pakiety będą wysyłane.
W ten sposób możemy kontrolować przepływ informacji pomiędzy wybranymi dwoma stacjami z uwzględnieniem kierunku. Aby aktywować filtrowanie należy ustawić „*Enabled*” w górnym pasku okna.

Protocol Filter

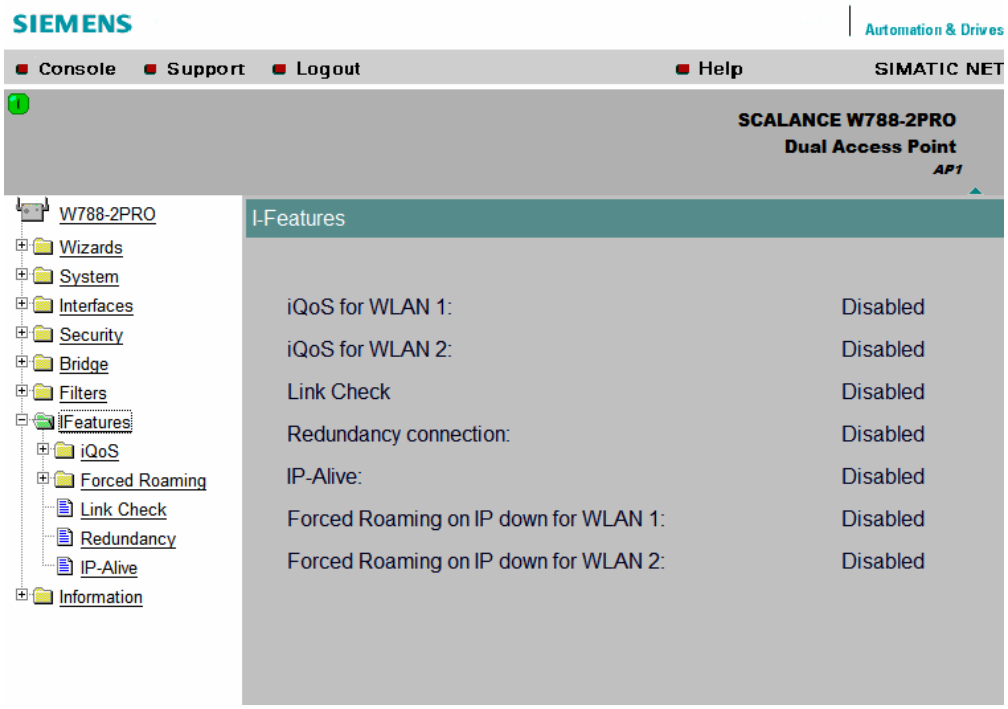
Karta pozwala na filtrowanie informacji przesyłanych w ramach różnych protokołów komunikacyjnych.



Oprócz domyślnych protokołów, możemy wprowadzić do 50 własnych filtrów wybierając „*New*”, a następnie wpisując indeks ramki standardu Ethernet II danego protokołu oraz opcjonalny opis.
Politykę dla wybranych protokołów wybieramy w polu „*Selected protocols*”. Ramki danych protokołów możemy blokować „*Blocked*” lub przekazywać dalej „*Forwarded*”.

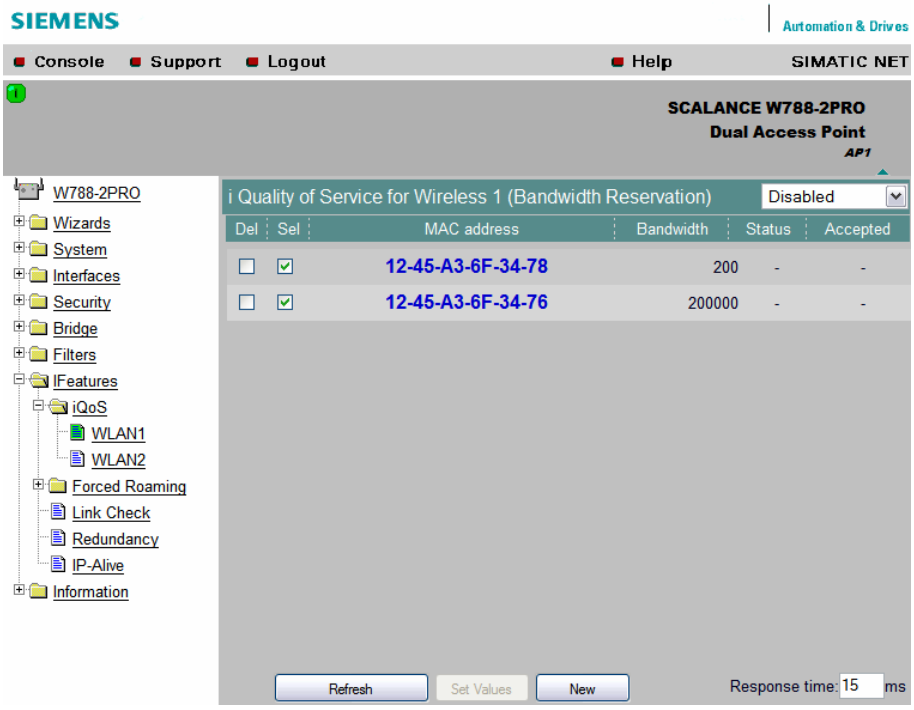
7. Zakładka „IFeatures”.

Zakładka zawiera zestaw narzędzi służących do kontroli i utrzymania połączenia.



iQoS

Opcja pozwala na rezerwację pasma transmisji o danej przepustowości na łączu WLAN.



Możemy dodać maksymalnie czterech klientów, z którymi chcemy zapewnić sobie komunikację na określonym poziomie przepustowości.
Nowe wpisy dodajemy za pomocą „*New*”.
W oknie edycji wprowadzamy adres MAC klienta oraz szybkość transmisji w [kbit/s], z jaką chcemy się z nim komunikować.
Narzędzie pozwala na wprowadzenie dowolnych wartości, jednak możliwość ich osiągnięcia jest weryfikowana podczas połączenia w polach „*Status*” oraz „*Accepted*”.

Pole „*Response time*” zawiera wartość czasu odpowiedzi naszego modułu, jaką chcemy zagwarantować. Minimalna wartość to 15 ms.

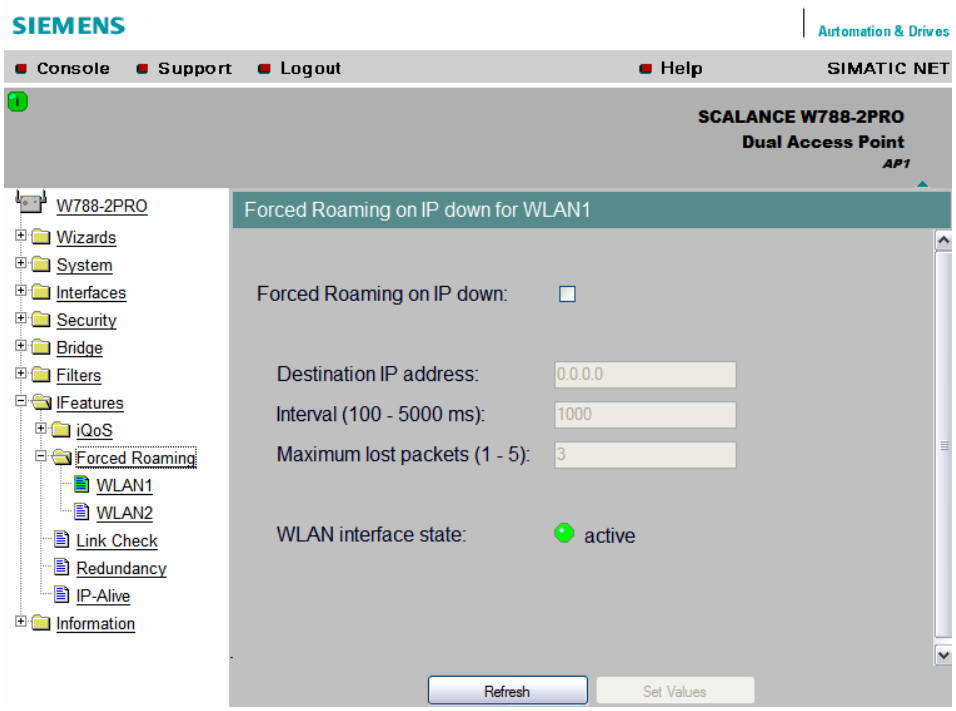
Aktywacja rezerwacji pasma następuje po wyborze w polu „*Sel*” oraz ustawienia „*Enabled*” (aktywacja rezerwacji z automatycznym dopasowaniem do rzeczywistych warunków) lub „*Enabled(Static)*” (aktywacja na sztywno – dezaktywacja, jeżeli nie ma warunków).

Uwaga!

Klienci, których adresy MAC wprowadzimy w to pole, mają zagwarantowane połączenie na danym poziomie kosztem innych stacji. Jeżeli przepustowość łącza jest ograniczona, stacje klienckie spoza listy zostają odłączone w calu zapewnienia wymaganej łączności klientom z listy.

Forced Roaming

Włączenie opcji „*Forced Roaming on IP down*” powoduje rozłączenie stacji klienckiej z interfejsem, na którym pojawiają się problemy w komunikacji z urządzeniem o określonym adresie IP, do czasu przywrócenia poprawnej wymiany informacji.
W naszym przypadku spowoduje to przełączenie stacji klienckiej do poprawnie działającego interfejsu WLAN.



Adres IP monitorowanej stacji wpisujemy w pole „*Destination IP address*”.

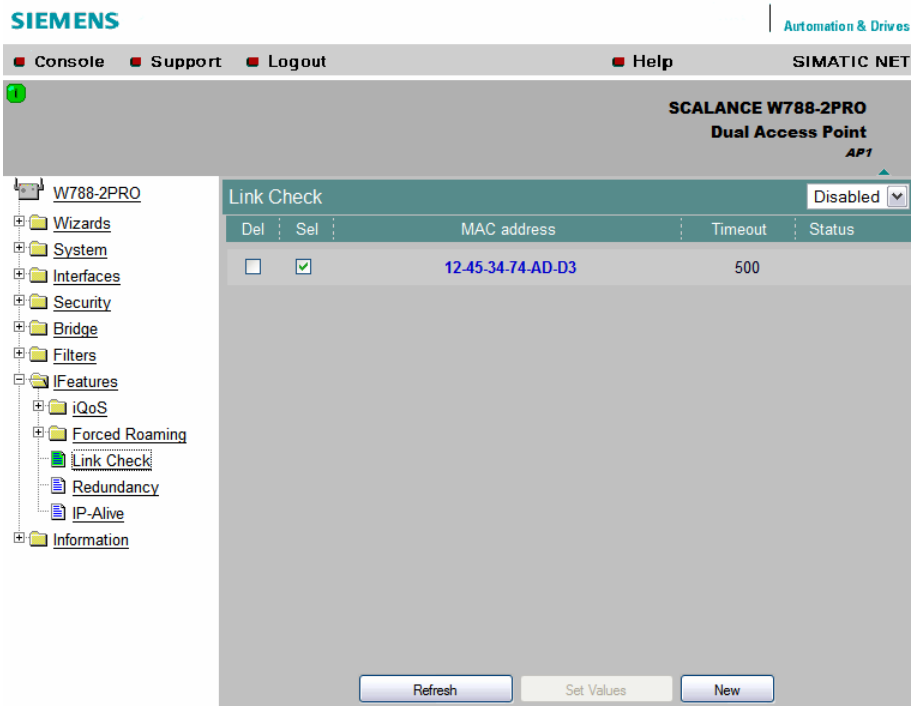
W polu „*Interval (100 – 5000ms)”* wpisujemy wartość interwału testów połączenia z podanego przedziału.

„*Maximum lost packets*” określa liczbę utraconych pakietów, powodująca przełączenie.

Aktywność danego interfejsu WLAN, jest sygnalizowana w polu „*WLAN Interface state*”.

Link Check

Opcja pozwala na kontrolę połączenia z klientem WLAN na poziomie łącza.



Monitorowane stacje dodajemy za pomocą „*New*”.

W oknie edycyjnym wprowadzamy MAC adres oraz „*Timeout*”, czyli czas, po którym w razie braku aktywności danego urządzenia w sieci, wysyłane są pakiety kontrolne.

W polu „*Status*” wyświetlana jest informacja o stanie połączenia z danym klientem.

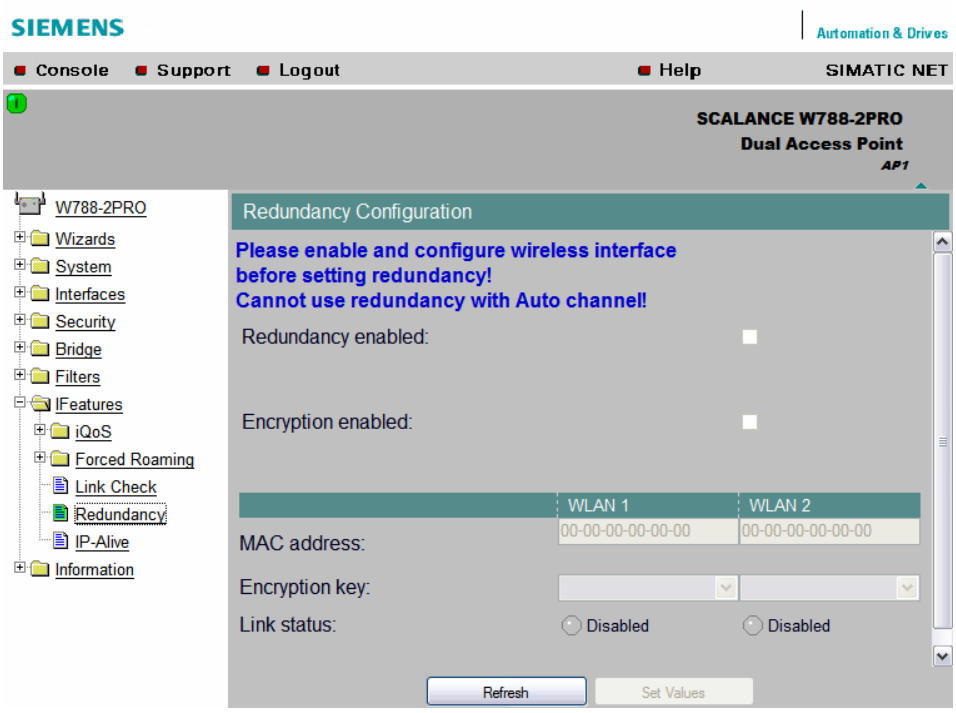
Aktywacja monitoringu następuje po wybraniu klienta w polu „*Sel*” oraz opcji „*Enabled*” w górnym pasku okna.

Uwaga!

Wyświetlane informacje dotyczą obecności urządzenia w sieci; nie pozwalają na stwierdzenie poprawnej komunikacji.

Redundancy

Narzędzie służy do konfiguracji połączeń redundantnych pomiędzy modułami SCALANCE W78x posiadającymi dwa interfejsy WLAN.



Narzędzie wymaga aktywności obu interfejsów WLAN urządzenia oraz ustawienia różnych kanałów komunikacji bezprzewodowej (Nie można stasować opcji „*Auto channel*”.

Aktywacji opcji dokonujemy w polu „*Redundancy enabled*”.

Jeżeli mamy połączenia szyfrowane zaznaczamy „*Encryption enabled*”.

Uwaga!
W tym wypadku możemy korzystać z szyfrowania WEP lub AES.

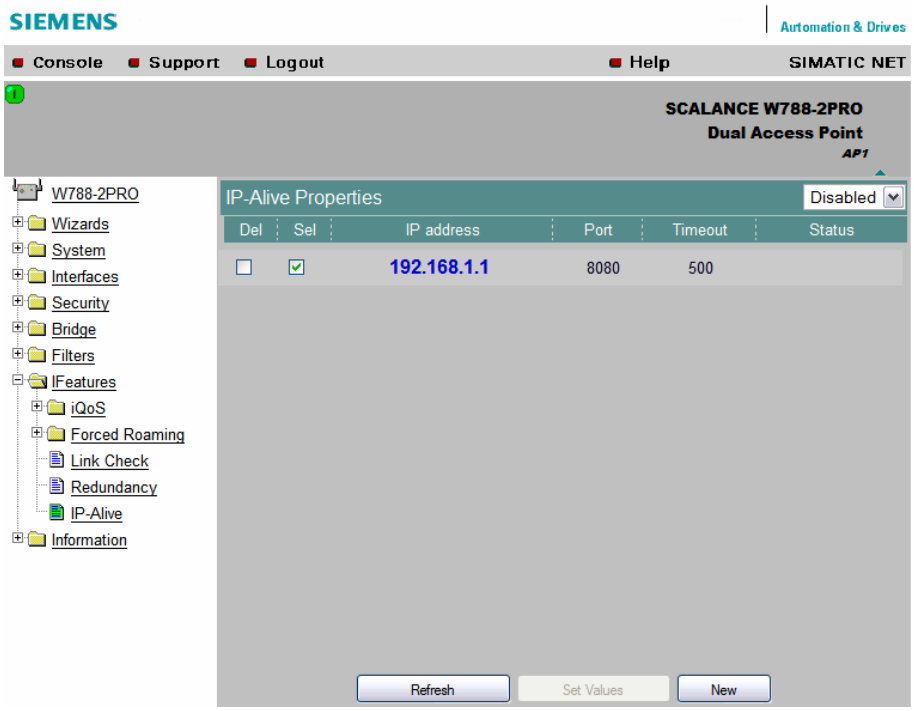
Dla interfejsów WLAN1 oraz WLAN2 wprowadzamy adresy MAC lub nazwy systemowe „*sysName*” redundantnych modułów oraz podajemy uprzednio ustawiony prywatny klucz szyfrujący („*private key*”), jeżeli korzystamy z zabezpieczeń 802.1x lub WPA

Uwaga!
Nie możemy wprowadzać jako redundantnych adresów interfejsów własnych naszego modułu. Redundancję taką możemy jednak pośrednio uzyskać, ustawiając identyczne parametry obu interfejsów WLAN, tzn. SSID, kanał oraz rodzaj połączenia.

Stan łączności z urządzeniami redundantnymi wyświetlany jest w polu „*Link status*”

IP-Alive

Opcja służy do monitorowania połączenia WLAN na poziomie aplikacji.



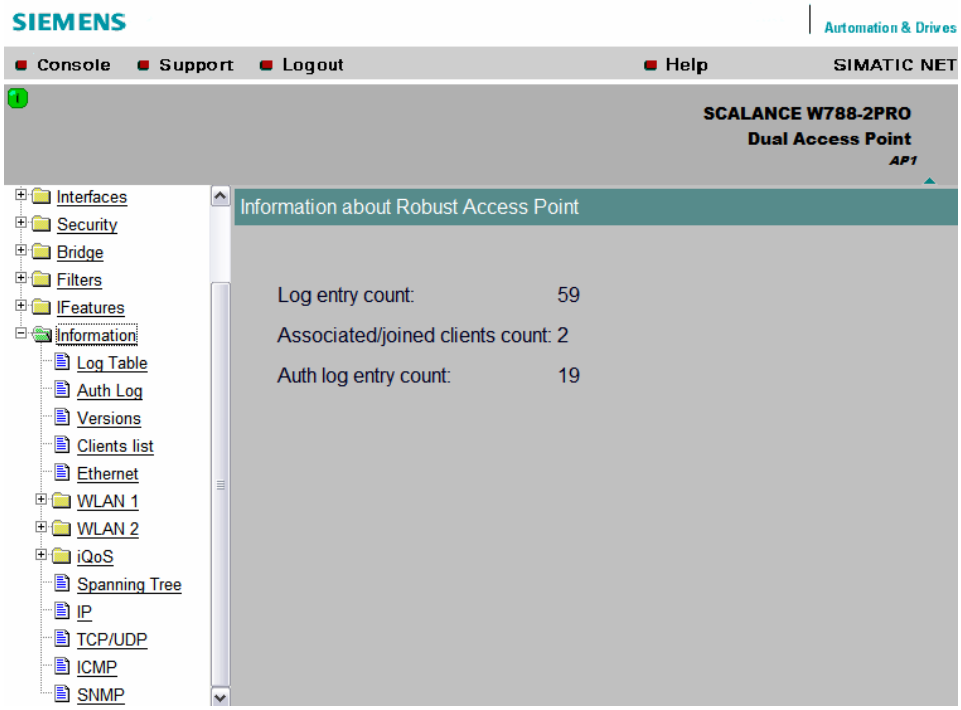
Monitorowanie połączenia dodajemy za pomocą „*New*”.

W pojawiającym się oknie wprowadzamy adres IP stacji, port aplikacji czy usługi (np. port 8080 to serwer http) oraz „*Timeout*”, po którym następuje w razie nieaktywności usługi wysłanie pakietów kontrolnych i odpowiednia modyfikacja informacji o stanie połączenia w polu „*Status*”.

Połączenie jest monitorowane po wybraniu go w polu „*Sel*” i zatwierdzeniu przez „*Set Values*” oraz aktywacji narzędzia przez ustawienie „*Enabled*” w górnym pasku okna.

8. Zakładka „Information”.

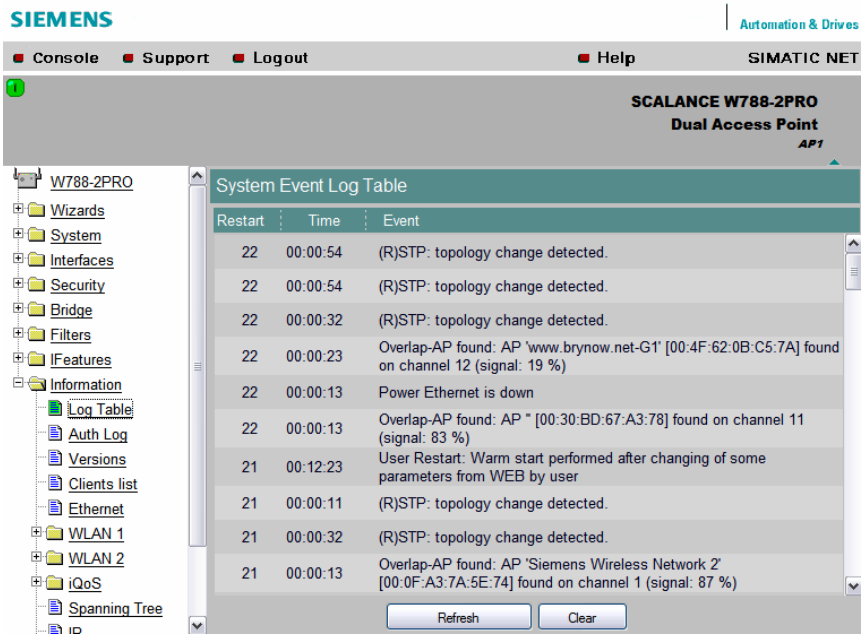
Wbudowany zestaw kart informacyjnych pozwala na wszechstronną diagnostykę pracy modułu SCALANCE W oraz monitorowanie jakości połączeń.



W oknie głównym widzimy informacje dotyczące ilości zarejestrowanych logów „*Log entry count*”, ilości zarejestrowanych lub połączonych klientów „*Associated/joined client count*” oraz ilości logów dotyczących procesu autoryzacji użytkowników „*Auth log entry count*”.

Log Table

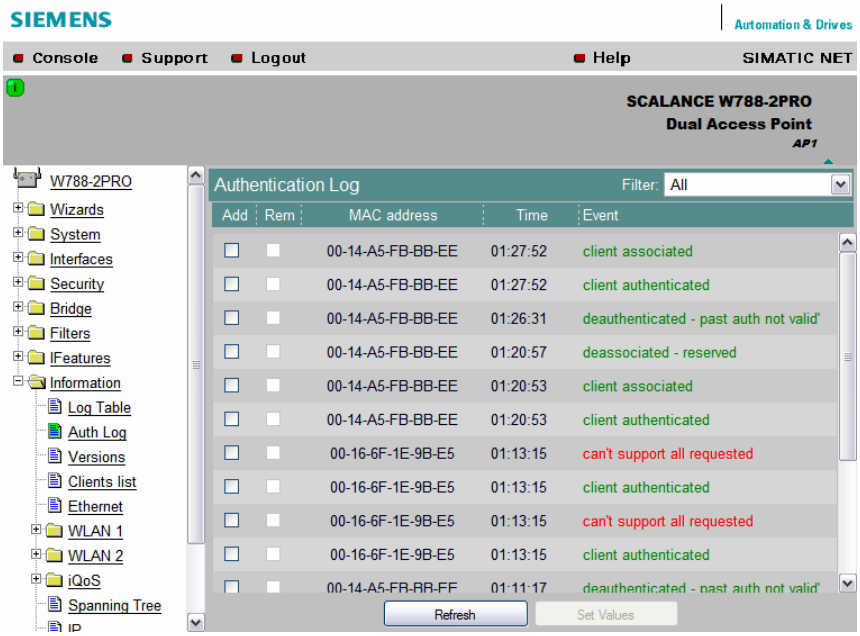
Tablica zawiera logi zdarzeń wybranych w karcie „*System -> Events*”.



Kolumna „*Restart*” zawiera numer sesji po kolejnym restarcie modułu.
Pole „*Time*” wyświetla czas wystąpienia danego zdarzenia od kolejnego restartu.
„*Event*” zawiera opis zdarzeń systemowych.

Auth log

Okna zawiera tablicę logów autentyfikacji.



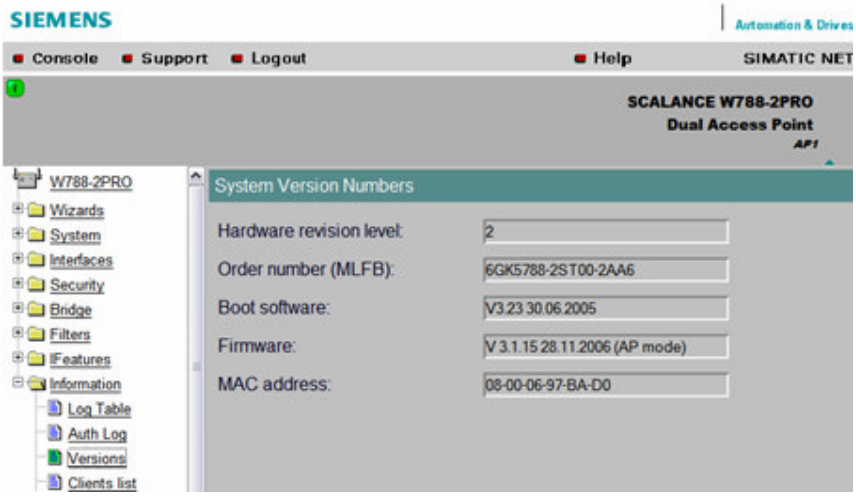
Zaznaczenie pola „*Add*” oraz potwierdzenie wyboru przez „*Set Value*” powoduje dodanie adresu MAC z pola „*MAC address*” do listy kontroli dostępu „*Security -> ACL*”.

Pole „*Rem*” służy do usuwania danych stacji z ACL.

Pole „*Time*” wyświetla czas zdarzenia opisanego w polu „*Event*” od restartu urządzenia.

Version

Karta wyświetla informacje dotyczące wersji urządzenia oraz jego oprogramowania.



„*Hardware revision level*” – numer kolejnej aktualizacji firmware’u.

„*Order number (MLFB)”* – numer katalogowy urządzenia.

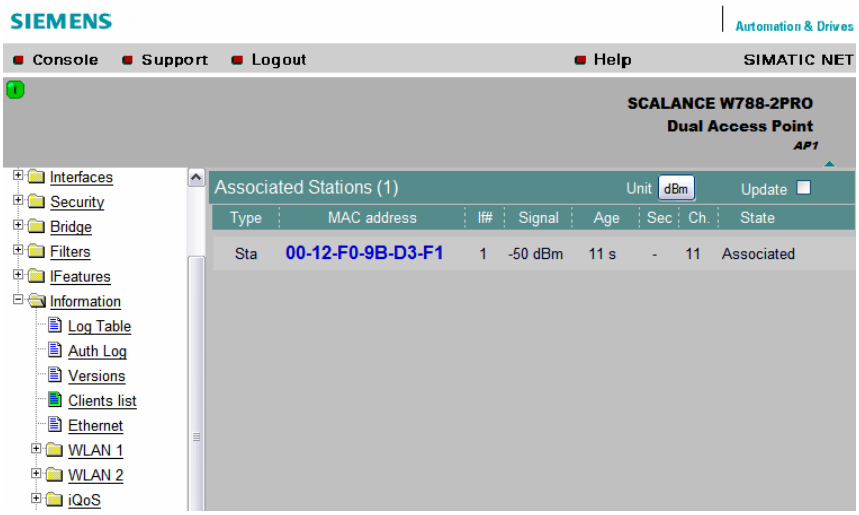
„*Boot software*” – wersja oprogramowania startowego („BIOS” urządzenia).

„*Firmware*” – wersja oprogramowania systemowego oraz tryb pracy.

„*MAC address*” – adres MAC interfejsu Ethernet.

Client list

Okno wyświetla listę klientów połączonych z naszym modułem AP.



W kolumnie „*Type*" zawarta jest informacja o typie połączonego urządzenia o adresie w polu „*MAC address*" („*Sta*" – stacja kliencka, „*WDS*" – AP współpracujące w trybie WDS).

„*If#*" – numer interfejsu WLAN, z którym jest połączona dana stacja.

„*Signal*" – siła sygnału połączenia, do wyboru w polu „Unit" mamy skalę w dBm lub procentach.

„*Age*" – czas od ostatniej aktywności sieciowej urządzenia.

„*Sec*" – typ zabezpieczeń połączenia.

„*Ch.*" - numer kanału połączenia WLAN.

„*State*" – stan połączenia („*Associated*" – stacja zalogowana, „*AP is up*" – aktywny węzeł WDS").

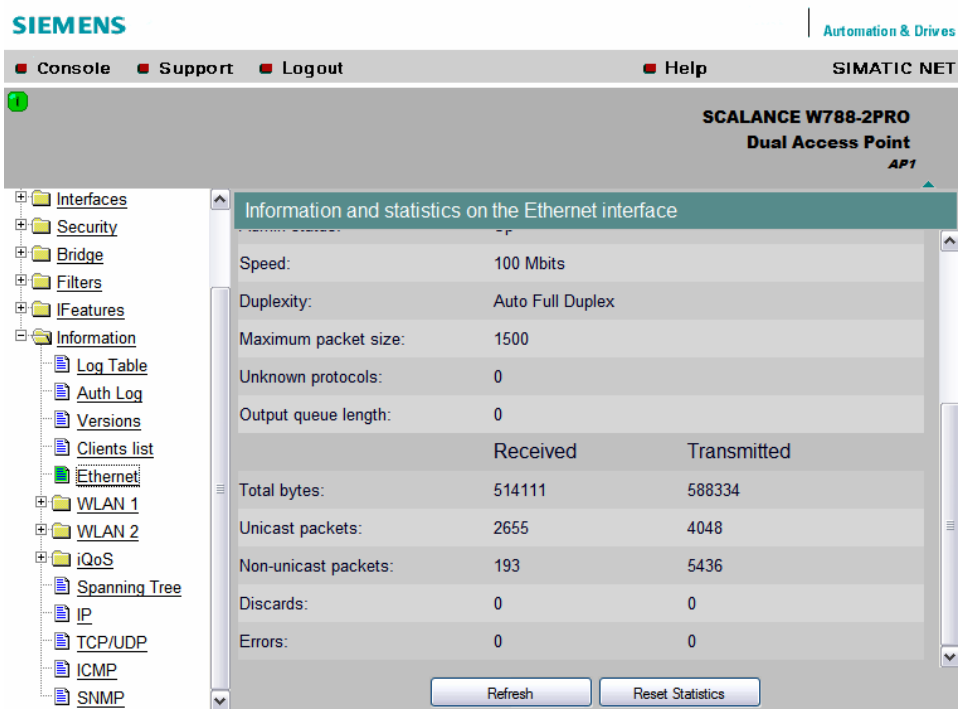
Zaznaczenie opcji „*Update*" powoduje odświeżanie informacji co 2s.

Wskazówka.
Kliknięcie w oznaczony kolorem niebieski adres MAC stacji powoduje, w tej oraz pozostałych kartach, przejście do okna statystyk ruchu oraz informacji połączenia dla danego klienta.

Odpowiednikiem tej karty w trybie „*Client*" jest karta „***Avaliable APs***", która zwiera podobne informacje o dostępnych w otoczeniu stacjach bazowych sieci bezprzewodowych.

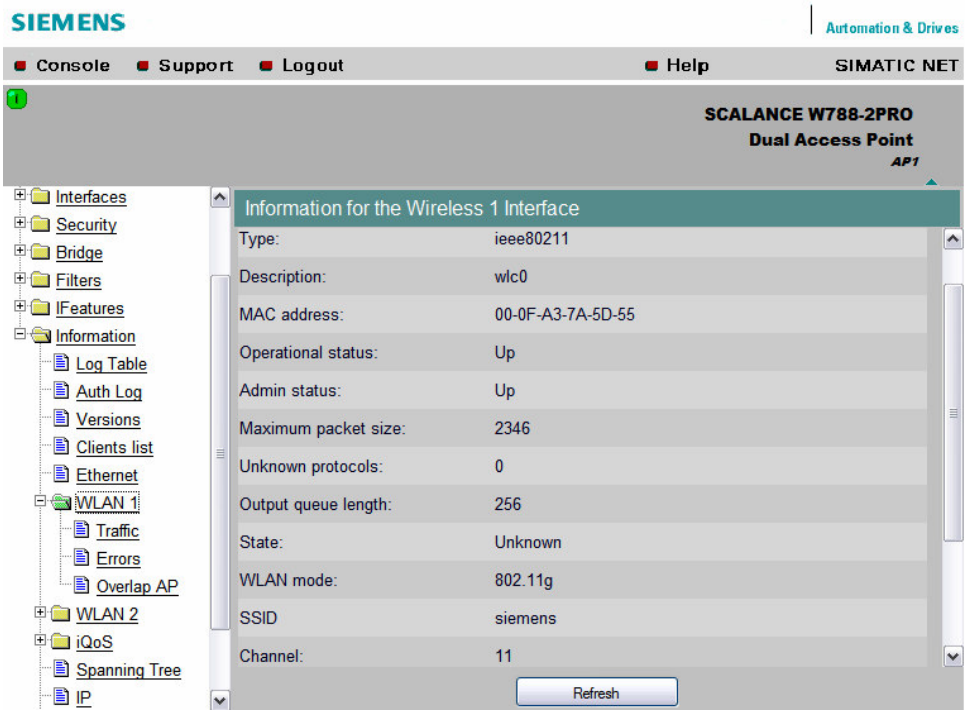
Ethernet

Karta przedstawia informacje dotyczące konfiguracji połączenia sieci Ethernet oraz statystyki ruchu na tym łączu.



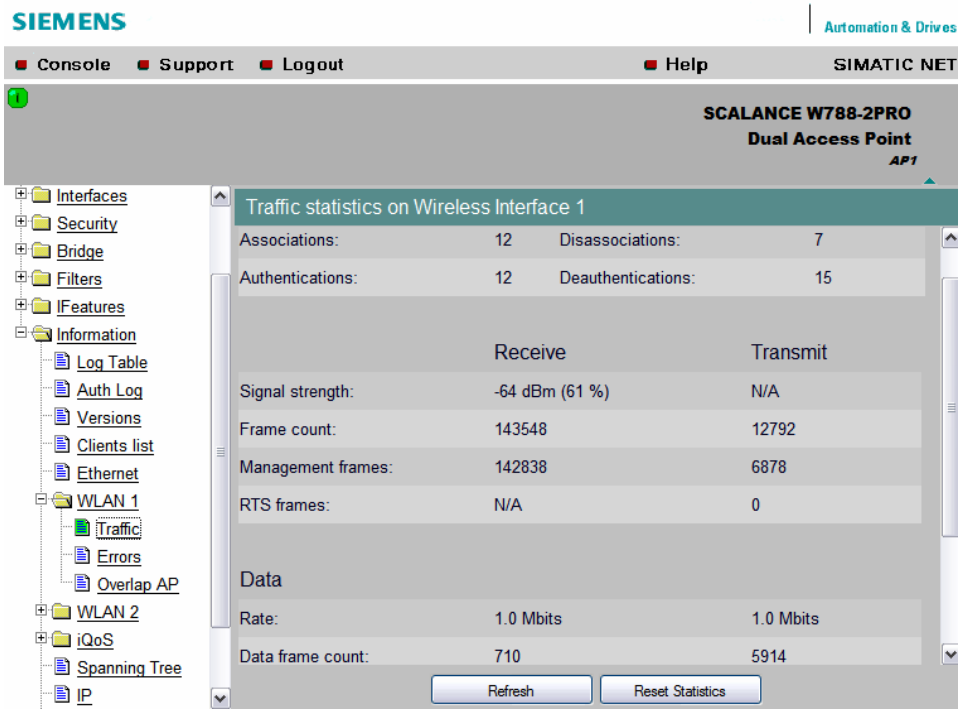
WLAN

Karta zawiera informację na temat połączeń interfejsów WLAN.
W oknie głównym widzimy informacje konfiguracyjne połączenia na wybranym interfejsie.



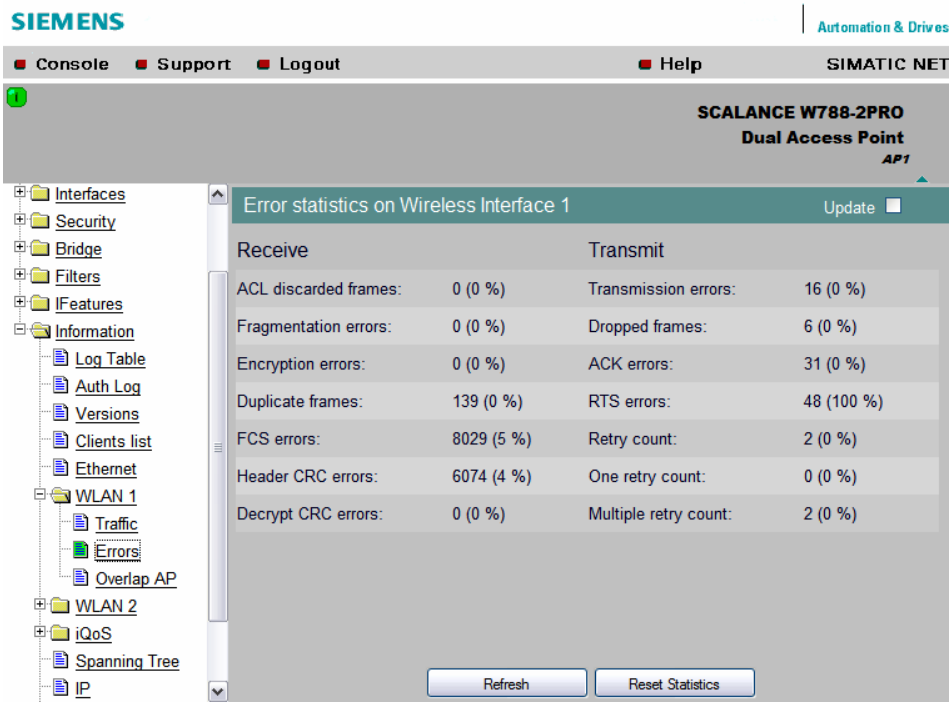
Traffic

Okna zawiera statystyki dotyczące ruchu oraz połączeń na danym interfejsie bezprzewodowym.



Errors

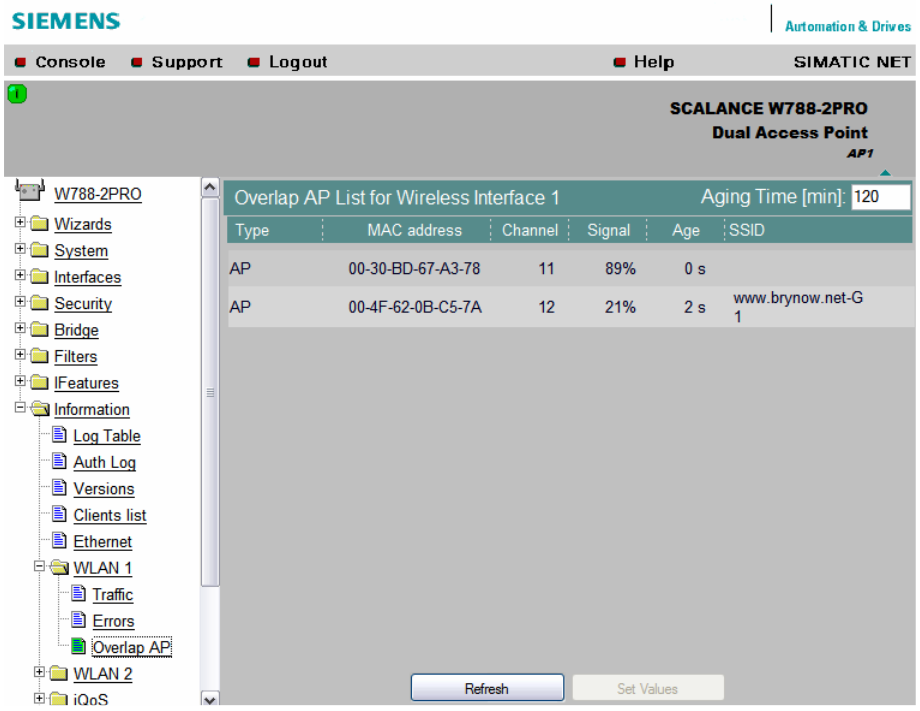
W tym miejscu dostępne są statystyki błędów pojawiających się na łączu WLAN.



Opcja „*Update*” włącza odświeżanie informacji, przycisk „*Refresh*” służy do ręcznego odświeżania, a „*Reset Statistics*” do wyzerowania statystyk.

Overlap AP

Okno zawiera informacje na temat stacji AP, które wykorzystują kanały nachodzące na pasmo transmisji naszego modułu AP, powodując w ten sposób ograniczenie możliwości transmisji.

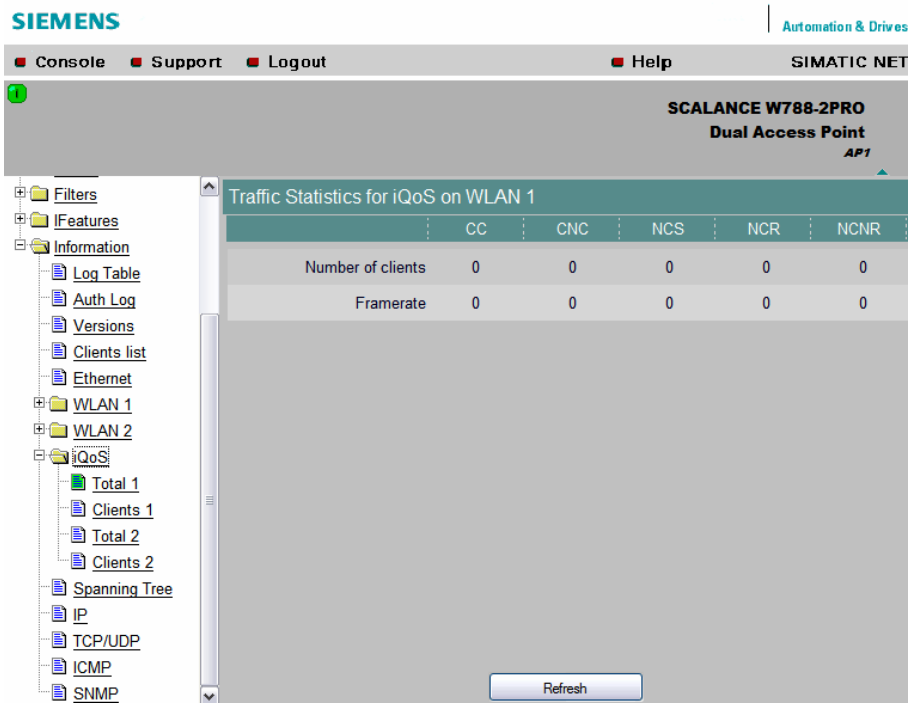


Dostępne informacje dotyczą typu stacji, adresu MAC, numeru kanału, siły sygnału, czasu od ostatniej aktywności oraz identyfikatora SSID.

W polu „*Aging Time*” możemy podać w minutach wartość czasu, przez który informacja o stacji będzie wyświetlana pomimo zaniknięcia problemu.

iQoS - Total

Okno przedstawia statystyki ruchu dla połączeń poszczególnych interfejsów nadzorowanych przez mechanizm kontroli jakości usług konfigurowanych w karcie „*IFeaturesi -> iQoS*”.



Wiersze odpowiadają liczbie klientów „*Number of clients*” oraz prędkości przesyłania ramek „*Framerate*”.

Znaczenie kolumn:

CC (Critical Compliant) – klienci, którzy zostali przypisanie jako krytyczni oraz spełnione są dla nich wymogi dotyczące prędkości transmisji oraz czasu odpowiedzi.

CNC (Critical Non-Compliant) – klienci krytyczni, dla których w danym momencie nie można zapewnić wymganej jakości łącza.

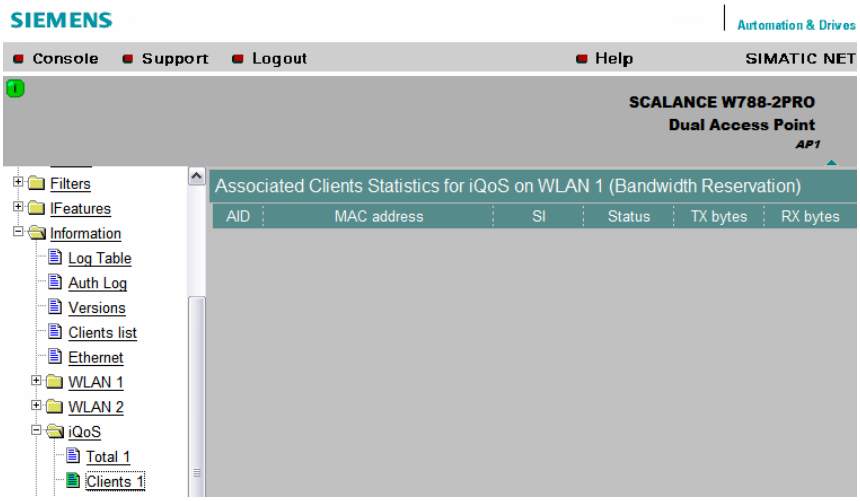
NCS (Non-Critical Satisfied) – klienci niekrytyczni, którzy nie mają żadnych wymogów jakości transmisji oraz nie zostali objęci restrykcjami mechanizmu iQoS.

NCR (Non-Critical Restricted) – klienci niekrytyczni, którzy zostali objęci restrykcjami mechanizmu iQoS na rzecz polepszenia parametrów transmisji dla klientów krytycznych.

NCNR (Non-Critical Non-Responsive) – klienci niekrytyczni, którzy, co więcej, nie wymagają potwierdzeń zdeterminowanych czasowo, np. komunikujący się poprzez protokół bezpołączeniowy UDP, który nie kontroluje transmisji pakietów po ich wysłaniu.

iQoS - Clients

Karta wyświetla statystyki dla połączonych klientów w ramach rezerwacji pasma transmisji przez iQoS.



Pole „*AID*" zawiera numer identyfikacyjny połączenia z klientem o adresie fizycznym w polu „*MAC address*".

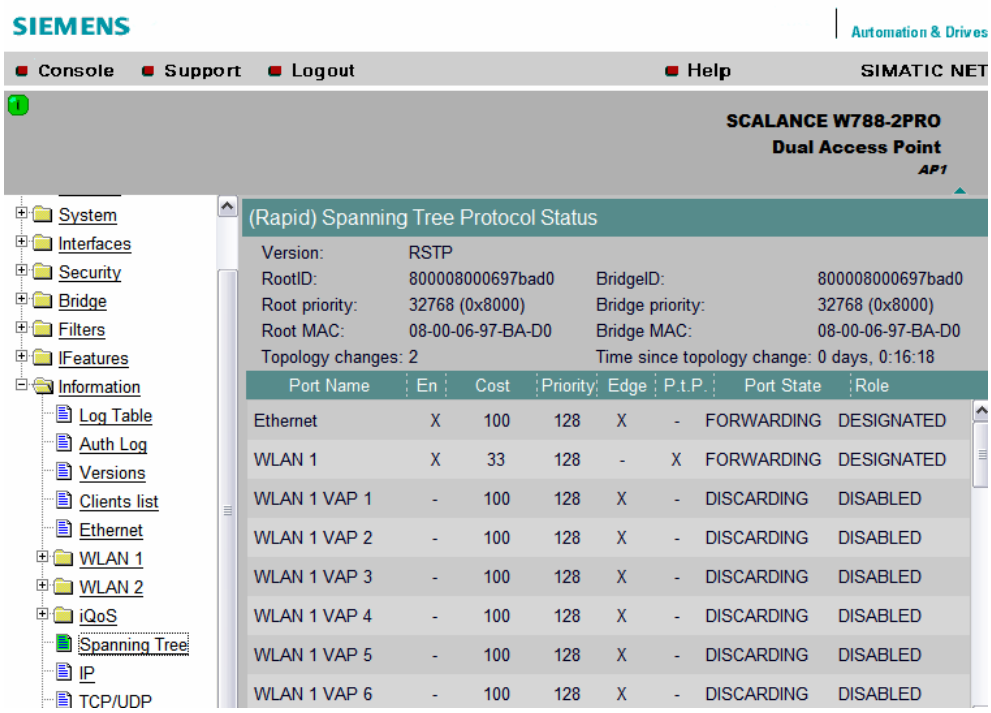
Pole „*SI*" (*Shaper Interval*) określa minimalną przerwę pomiędzy dwoma ramkami ustawianą przez mechanizm iQoS.

„*Status*" przedstawia klasyfikację klienta wg iQoS, opisaną w poprzednim punkcie.

„*Tx/Rx bytes*" zawierają informację o ilości wysłanych i odebranych bajtów danych.

Spanning Tree

Karta zawiera informacje dotyczące zarówno ustawień portów komunikacyjnych naszego urządzenia, jak i aktualnej konfiguracji całego systemu (R)STP.



W górnej części okna widzimy informację o wersji protokołu, dane o węźle zarządzającym strukturą sieci („Root"), dane o naszym module w tej strukturze („Bridge"), a także ilość zmian optymalizacyjnych topologii sieci oraz czas ostatniej takiej zmiany.

Druga część okna dotyczy konfiguracji portów naszego urządzenia.

Wartość w polu „*Priority*" określa priorytet danego portu spośród wszystkich dostępnych w urządzeniu przy wyborze ścieżki. Im mniejsza wartość tym większy priorytet.

„*STP Cost" oraz „RSTP Cost*" określają koszt danego portu pod względem prędkości transmisji, w zależności od wybranej wersji protokołu.
Mniejsza wartość powoduje zwiększenie prawdopodobieństwa wyboru danego portu przez mechanizm.

„*Edge*" – oznacza port, do którego jest podłączona stacja końcowa, bez dalszych rozgałęzień. Porty takie nie biorą udziału w wymianie danych protokołu Spanning Tree, a przełączanie się przez nie jest szybsze.

„*P.t.P.*" – opcja punkt-punkt, odnosi się do portów, przez które są ze sobą połączone urządzenia sieciowe obsługujące mechanizm (R)STP.

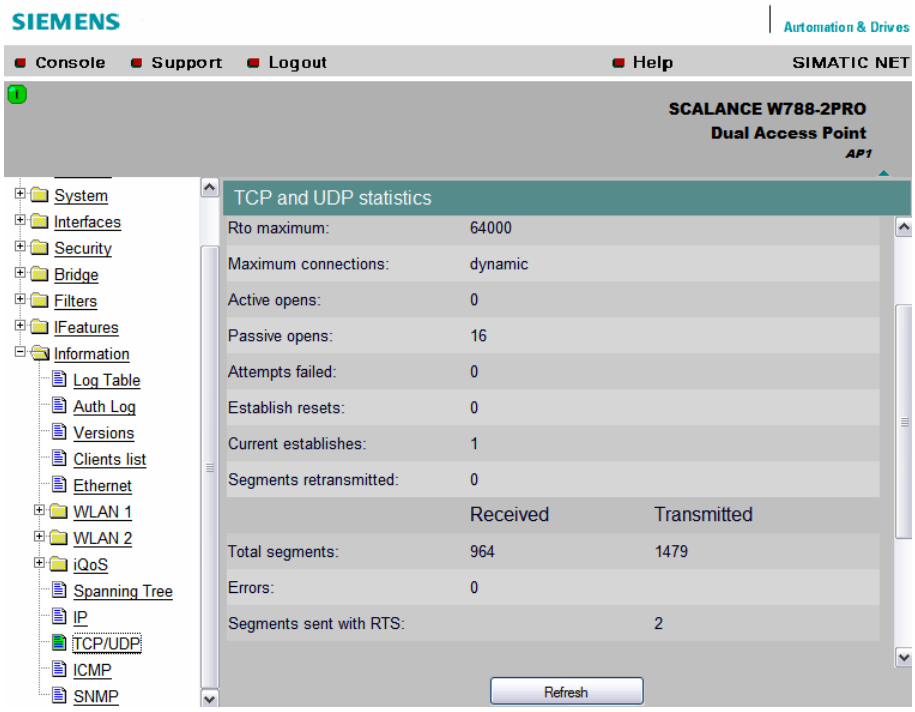
„*Port State*” – stan danego portu. Może przyjmować wartości:

- - „*DISCARDING*” – port nieaktywny, wyłączony przez użytkownika lub protokół.
- - „*LEARNING*” – port nasłuchuje, zapisuje stacje w tablicy adresów „Learning Table”, ale nie przekazuje danych dalej.
- - „*FORWARDING*” – port w pełni aktywny.
- - „*DISABLED*” – port wyłączony.

„*Role*” – określa relację portu do głównego mostu „Root”.
„*ROOT*” oznacza, że port jest bezpośrednio połączony z mostem zarządzającym, „*DESIGNATED*” odpowiada aktywnym portom niepołączonym do Root’a, natomiast „*BLOCKED*” świadczy o blokadzie portu.

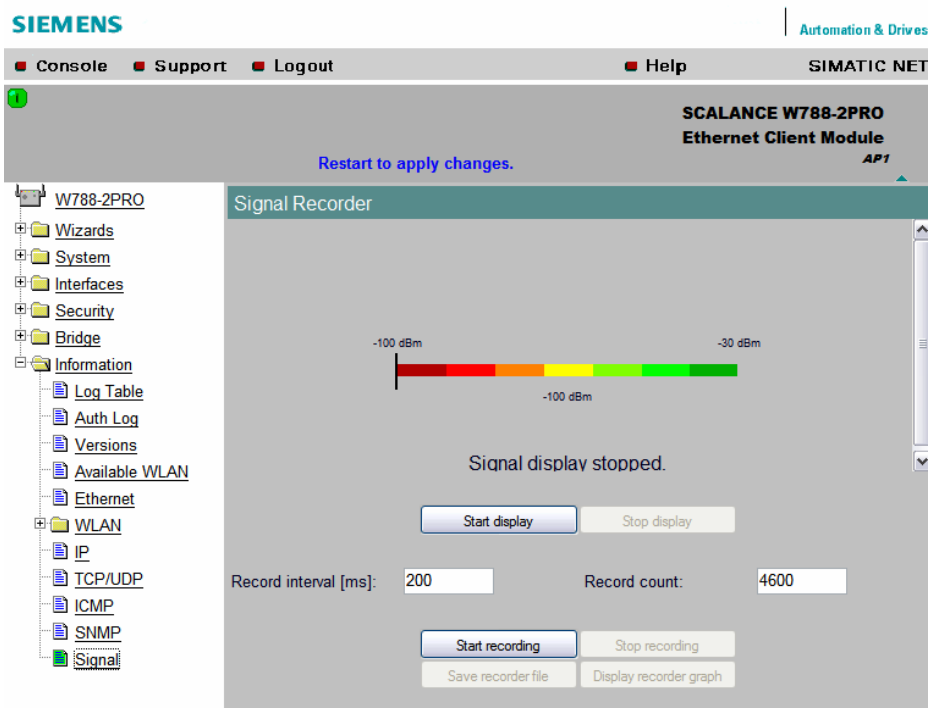
IP, TCP/IP, ICMP, SNMP

Karty te zawierają statstyki oraz informacje na temat ramek protokołów komunikacyjnych:
- IP – protokół połączeniowy, odpowiada za organizację połączeń w sieci;
- TCP/UDP – protokoły wymiany danych;
- ICMP – protokół informacji diagnostycznych, niestety często wykorzystywany do włamań;
- SNMP – protokół odpowiedzialny za konfigurację i diagnostykę urządzeń sieciowych.



Signal (tryb klienta)

Narzędzie to pozwala na podgląd oraz rejestrację poziomu sygnału połączenia bezprzewodowego.



Jeżeli mamy ustanowione połączenie bezprzewodowe, po kliknięciu „*Start display*” zobaczymy przesuwający się po skali wskaźnik oraz zmieniającą się wartość tłumienia sygnały po środku skali.

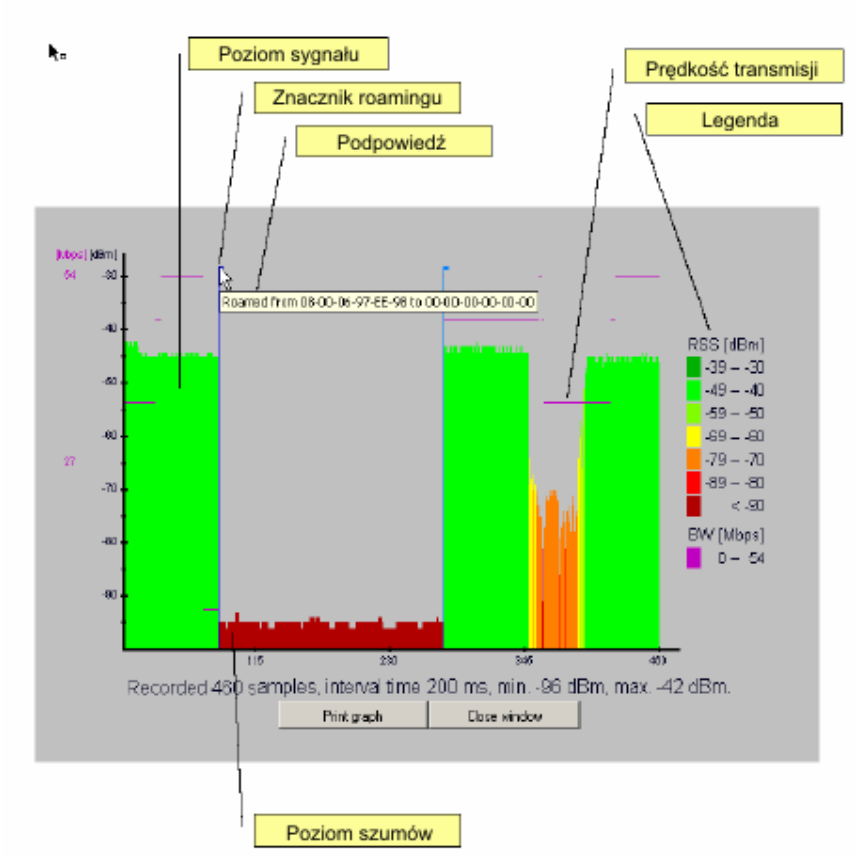
Jeżeli brak ustanowionego połączenia zobaczymy komunikat „DISCONNECTED!”.

W trakcie podglądu możemy włączyć rejestrację wyników, klikając na „*Start recording*”. Możemy ustawić parametry rejestracji: „*Record interval*” – odstęp czasowy pomiędzy rejestrowanymi pomiarami oraz „*Record count*” – ilość rejestrowanych próbek.

Zakończenie pomiarów lub rejestracji możemy przerwać ręcznie używając odpowiednich klawiszy „*Stop*”.

„*Save recorder file*” pozwala na zachowanie wyników pomiarów do pliku w formacie tekstowym.

„*Display recorder graph*” wyświetla graficzną prezentację pomiarów, której przykład zamieszczono na kolejnej stronie.


Poziom sygnału
Znacznik roamingu
Podpowiedź
Prędkość transmisji
Legenda
Roamed from 08-00-06-97-EE-98 to 00-00-00-00-00-00
RSS [dBm]
-39 – -30
-49 – -40
-59 – -50
-69 – -60
-79 – -70
-89 – -80
< -90
BW [Mbps]
0 – 54
Recorded 460 samples, interval time 200 ms, min. -96 dBm, max. -42 dBm.
Print graph
Close window
Poziom szumów