www.italnet.pl

ul.Zwoleńska 16A
04-761 Warszawa
nip 547-146-12-81
info@italnet.pl
tel. 22.100.57.85

# KONFIGURACJA TERMINALA

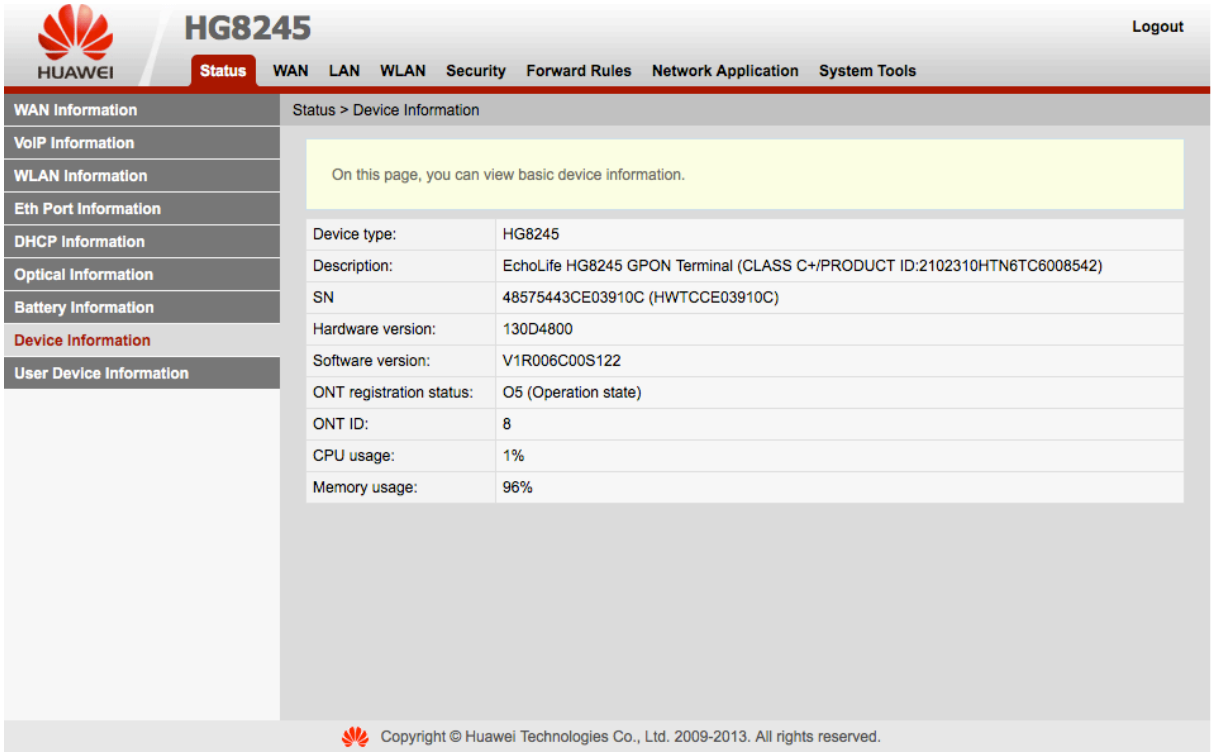
# GPON ONT HG8245

## 1. Konfiguracja WiFi

W domyślnej konfiguracji terminal ONT posiada zdefiniowane 4 port ethernet z dostępem do internetu (w trybie NAT – oznacza to że urządzenie klienta otrzymuje wewnętrzny adres IP, natomiast adres zewnętrzny przypisany jest do terminala ONT), oraz z włączoną funkcją sieci WiFi w trybie domyślnym SSID: Italnet.eu oraz hasło: iiiiiii (8x i).
Aby skonfigurować sieć WiFi należy uruchomić przeglądarkę internetową i w polu adresu wpisać http://192.168.100.1 (domyślny adres terminala ONT HG8245). Wyświetli się stroną umożliwiająca zalogowanie się do terminala ONT, tak jak na rysunku nr 1.

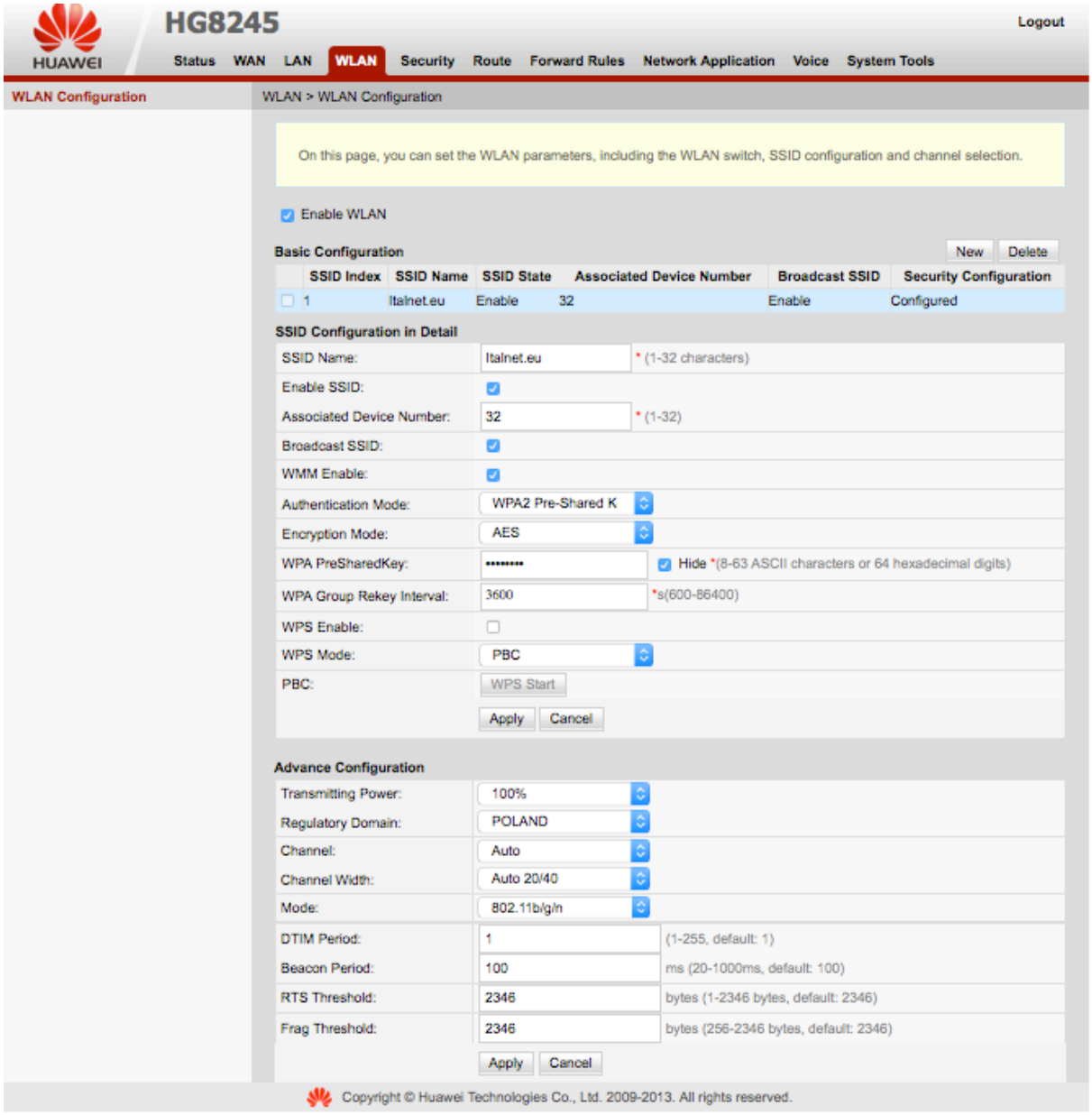

Rysunek nr 1 (logowanie do terminala ONT HG8245)

Domyślnie w polu „Account” należy wpisać user, natomiast w polu „Password” wpisać user, a następnie kliknąć na przycisk „Login”. Po uwierzytelnieniu otworzy nam się główne okno konfiguracyjne terminala, które przedstawia rysunek nr 2.



Rysunek nr 2 (strona startowa terminala ONT HG8245)

Aby zmienić ustawienia sieci WiFi należy kliknąć na zakładkę „WLAN”. Odznaczenie opcji „Enable WLAN” spowoduje wyłączenie modułu WiFi w terminalu, oraz zgaszenie na terminalu kontrolki opisanej jako „WLAN”. Zaznaczenie tej opcji rozwinie nam również menu konfiguracyjne sieci WiFi, tak jak pokazano to na rysunku nr 3.



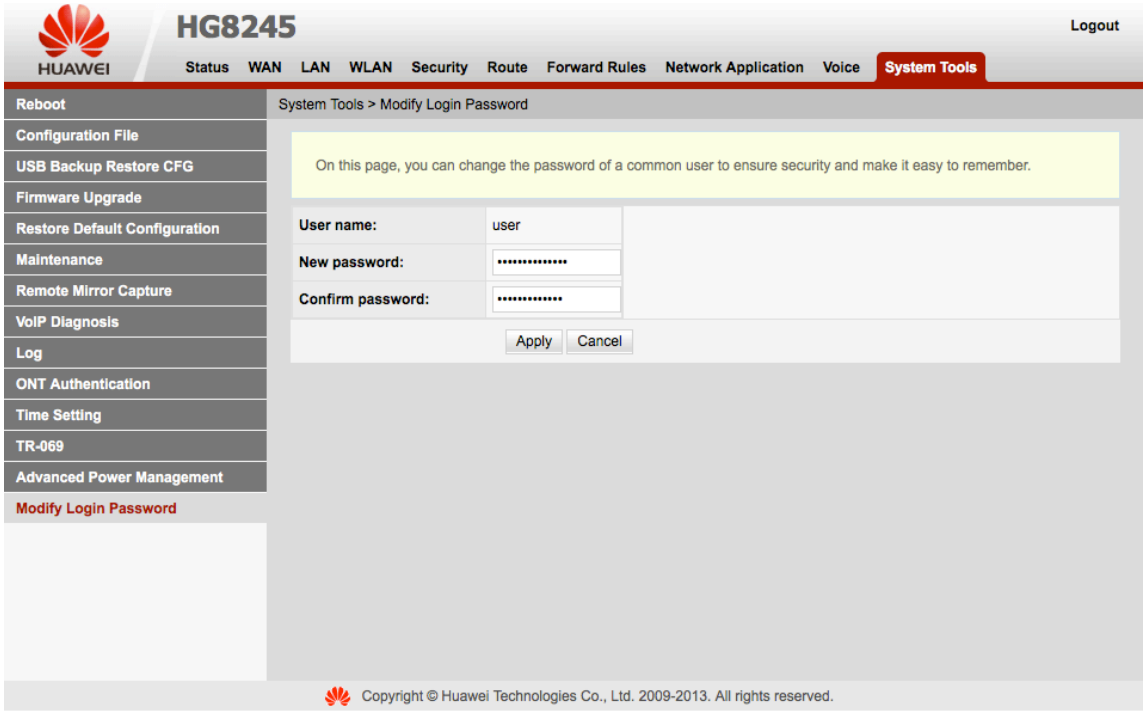
Rysunek nr 3 (parametry konfiguracyjne WiFi)

Sieć WiFi jest domyślnie skonfigurowana tak jak na rysunku nr 3. Jest to jednak konfiguracja predefiniowana na każdym urządzeniu, więc takie elementy jak nazwa sieci SSID oraz hasło są wszędzie takie same, a tym samym znane każdemu użytkownikowi w sieci italnet. Pozostawienie tych ustawień domyślnych jest niewskazane ze względów bezpieczeństwa. Jeżeli każdy zna te ustawienia to oznacza, że każdy może się zalogować do tak zdefiniowanej sieci WiFi. Dlatego w pierwszej kolejności należy bezwzględnie zmienić hasło. Jeżeli z jakiś względów ustawienia (poza SSID i hasłem) różnią się od tych pokazanych na rysunku, sugerujemy ich zmianę tak jak to pokazane. Szczególnie ważne jest szyfrowanie połączenia, które ustawia się w polu „Authentication Mode”. Brak szyfrowania powoduje, że przesyłane dane (również loginy, hasła, czy dane bankowości
elektronicznej) są łatwe do przechwycenia przez osoby trzecie. Brak szyfrowania to również umożliwienie osobom trzecim dostępu do Waszego internetu, w tym swoich danych jak również w celu dokonania przestępstw. Należy pamiętać, że nikt nie jest anonimowy w internecie, na podstawie adresu IP uprawnione organy ścigania mogą w łatwy sposób określić jego właściciela, więc w przypadku osoby, która korzystając z niezabezpieczonej sieci WiFi dokonuje przestępstwa, naraża nas na nieprzyjemności związane z udowodnieniem swojej niewinności. Dlatego należy bezwzględnie upewnić się czy jest włączone szyfrowanie mechanizmem WPA2,

które na dzień dzisiejszy uznawane jest za bezpieczne. Nie należy mylić WPA2 z WPA, które jest mniej bezpieczne.
Niektóre starsze urządzenia klienckie mogą nie wspierać WPA2, wtedy możemy być skazani na zabezpieczenie WEP, które jest bardzo łatwe do złamania. Po upewnieniu się odnośnie szyfrowania, kolejnym krokiem powinna być zmiana domyślnego hasła. Aby je zmienić w polu „WPA PreSharedKey" należy wprowadzić znane tylko sobie hasło dostępu do sieci bezprzewodowej. Hasło jest drugim elementem poza szyfrowaniem, mającym bezpośredni wpływ na poziom bezpieczeństwa
sieci. Dlatego też należy zadbać o jego jakość. Proste hasła, składające się z wyrazów słownikowych, imion, liczb można w prosty sposób złamać stosując metodę „brute force". Polega ona na sprawdzaniu wszystkich haseł ze słownika, aż do skutku. Dlatego lepszym zabezpieczeniem jest stosowanie długich i skomplikowanych haseł. Hasło aby było bezpieczne powinno składać się z minimum 12 znaków oraz zawierać kombinację małych i dużych liter, znaków specjalnych oraz cyfr. Dobrze jest też co jakiś czas je zmieniać.
Pozostałe ustawienia pokazane na rysunku nr 3 są mniej istotne i można pozostawić domyślne.

# 2. Zmiana hasła użytkownika

Również domyślne hasło użytkownika jest ogólnie znane. Dlatego kolejnym krokiem powinna być jego zmiana. Hasło to jest równie ważnym elementem bezpieczeństwa naszej sieci jak hasło dostępu do sieci WiFi, więc i tutaj sugerujemy zastosowanie tych samych reguł co do jego jakości.
W celu zmiany hasła użytkownika należy „kliknąć" na zakładkę „System Tools". Po lewej stronie będzie dostępna jako ostatnia opcja „Modify Login Password". Po wybraniu tej opcji ukaże nam się ekran jak na rysunku nr 4. W celu zmiany hasła należy w polu „Old Password" wpisać aktualnie obowiązujące hasło (jeżeli nie było nigdy zmieniane, będzie to user). Następnie w polu „New Password" należy wprowadzić nowe hasło, pamiętając o tym aby było odpowiedniej jakości i odpowiadało minimalnym wymaganiom systemu. W polu „Confirm Password" należy jeszcze raz wprowadzić nowe hasło, w celu jego weryfikacji, gdyż w polach tych nie są widoczne wprowadzane znaki, lecz zostają one zamieniane na znaki „*". Aby zaakceptować zmiany należy „kliknąć" na przycisk opisany „Apply".



Rysunek nr 4 (zmiana hasła użytkownika)

# 3. W przypadku posiadania usługi telewizyjnej

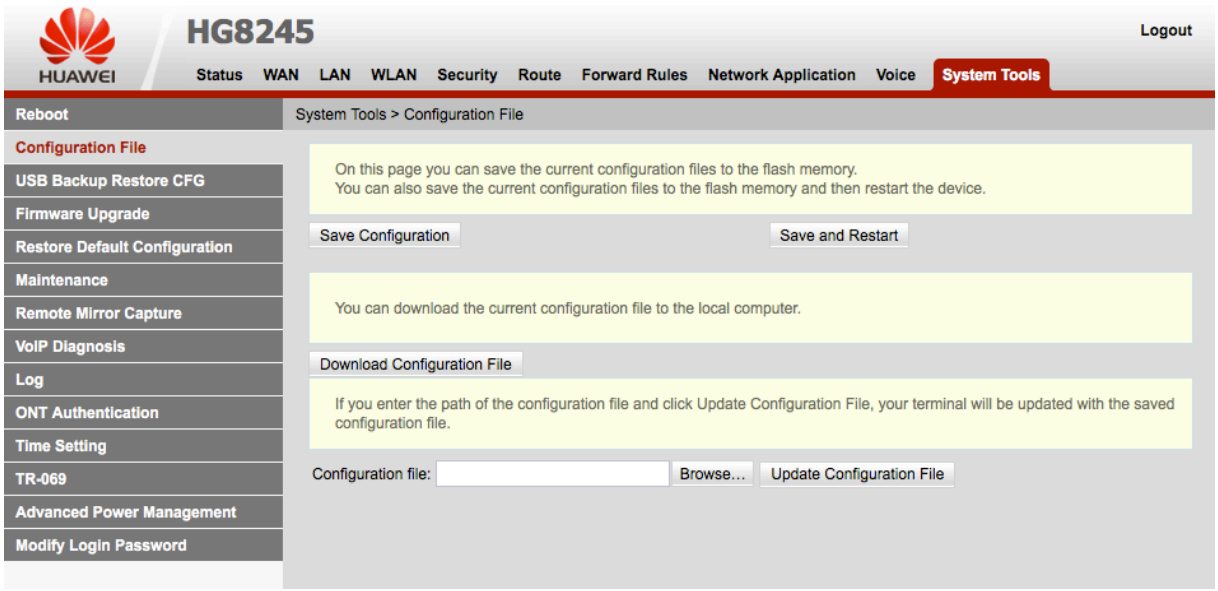
Klienci posiadający wykupioną usługę dostępu do platformy telewizyjnej posiadają inaczej skonfigurowane porty Ethernet w routerze niż w konfiguracji domyślnej.

Dostęp do Internetu zapewniany jest przez porty 1-3 a port 4 służy do podłączenia dekodera telewizyjnego. Inne podłączane urządzenia do tego portu wykryte przez operatora mogą skutkować blokadą sygnału telewizyjnego do czasu restartu urządzenia i usunięcia innego urządzenia podłączonego np. do switcha przez który przechodzi telewizja.

Internet do telewizora Smart TV OBLIGATORYJNIE podłączamy do portów 1-3.

# 4. Zapis ustawień konfiguracyjnych

Ostatnim etapem konfiguracji urządzenia powinno być zapisanie konfiguracji do pamięci trwałej urządzenia, która nie zostanie usunięta nawet po zresetowaniu terminala. Aby zapisać ustawienia należy ponownie kliknąć na zakładkę „System Tools", a następnie wybrać opcję „Configuration File" po lewej stronie ekranu. Ukaże się nam obraz jak na rysunku nr 5. Aby zapisać konfigurację do pamięci stałej, należy „kliknąć" przycisk „Save Configuration".




Rysunek nr 5 (zapis konfiguracji)

italnet – sieć światłowodowa
ul. Zwoleńska 131 lok.8
04-761 Warszawa
tel. 22 4777 777, 22 100 57 85
mail: support@italnet.eu
http://www.italnet.eu
https://www.facebook.com/italnet.internet/