Konfiguracja ustawień sieci w systemie Windows XP z użyciem oprogramowania Odyssey Client

Jako że oprogramowanie Odyssey Client zapewnia pełną kontrolę nad interfejsem bezprzewodowym, zlecane jest wyłącznie opcji „Użyj systemu Windows do konfiguracji ustawień sieci bezprzewodowej” w zakładce „Sieci bezprzewodowe” we właściwościach interfejsu bezprzewodowego.

Wstępna konfiguracja klienta

Aby zastosować klienta tego sieci bezprzewodowej zintegrowanego z suplikantem protokołu 802.1x, należy najpierw wstępnie go skonfigurować:

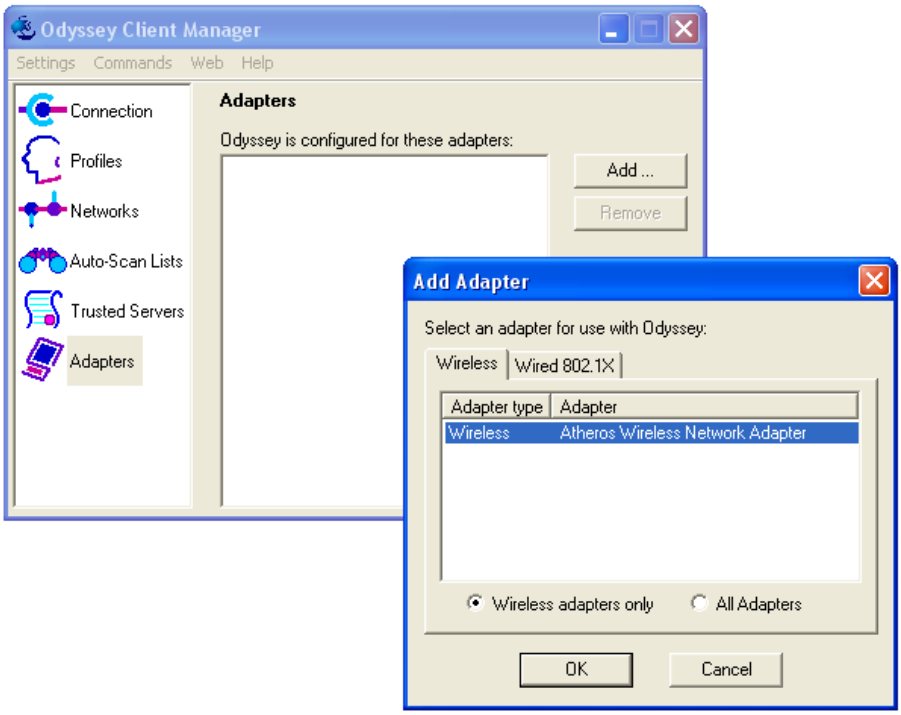
1. Dodać interfejs sieciowy do lisy obsługiwanych przez klienta.
2. Stworzyć profil uwierzytelniania, który opisuje protokoły oraz metody uwierzytelnienia użytkownika, a także zawiera konkretne informacje uwierzytelniające, jak np. nazwę użytkownika.
3. Dodać nową sieć bezprzewodową z którą będziemy się łączyć.

Po dokonaniu powyższej konfiguracji, klient Odyssey przejmuje pełną kontrolę nad interfejsem bezprzewodowym, pozwalając na:

- podłączenie się do sieci bezprzewodowej,
- dokonanie uwierzytelnienia,
- automatyczne uzyskanie kluczy szyfrujących,
- monitoring aktualnego sygnału sieci bezprzewodowej, a także stanu uwierzytelnienia klienta oraz stosowanego szyfrowania danych.

Dodanie interfejsu sieciowego do listy obsługiwanych przez program

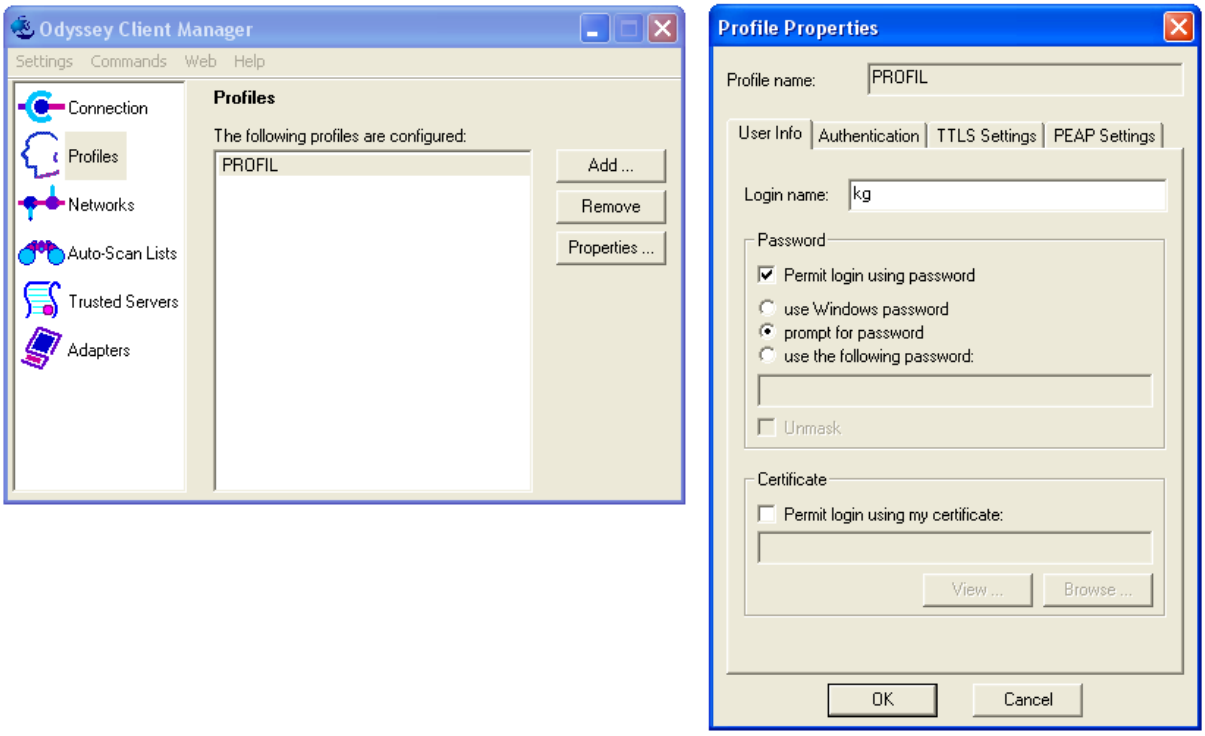
Z listy po lewej stronie należy wybrać pozycję „Adapters”.



Jeśli na pojawiającej się liście nie występuje interesująca nas karta sieciowa, używamy przycisku „Add”. Spowoduje to pojawienie się okna dialogowego zawierającego 2 zakładki „Wireless” (interfejsy bezprzewodowe) oraz „Wired 802.1X” (interfejsy przewodowe).
Wybieramy interesujący nas interfejs i potwierdzamy wybór przyciskiem OK.
Wybrany interfejs sieciowy został dodany do listy obsługiwanych i jest widoczny na liście. Można go stamtąd usunąć przyciskiem REMOVE.

Dodanie nowego profilu uwierzytelnienia

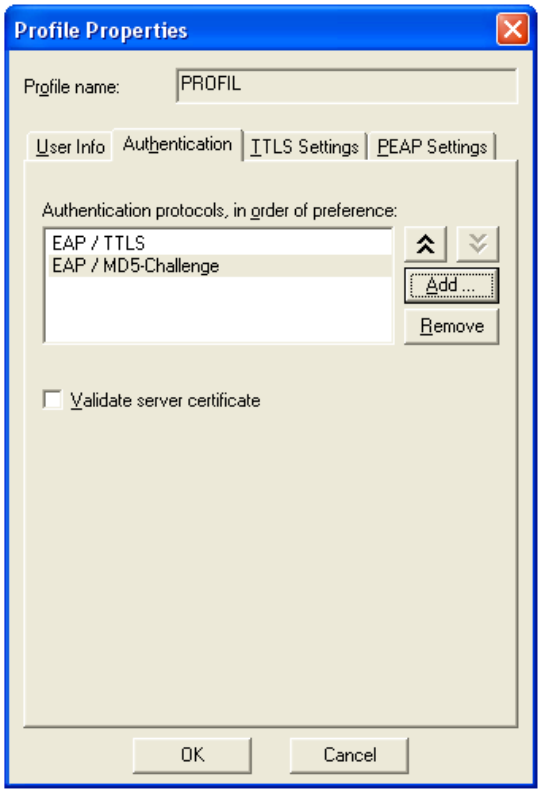
Z listy po lewej stronie należy wybrać pozycję „Profiles”.

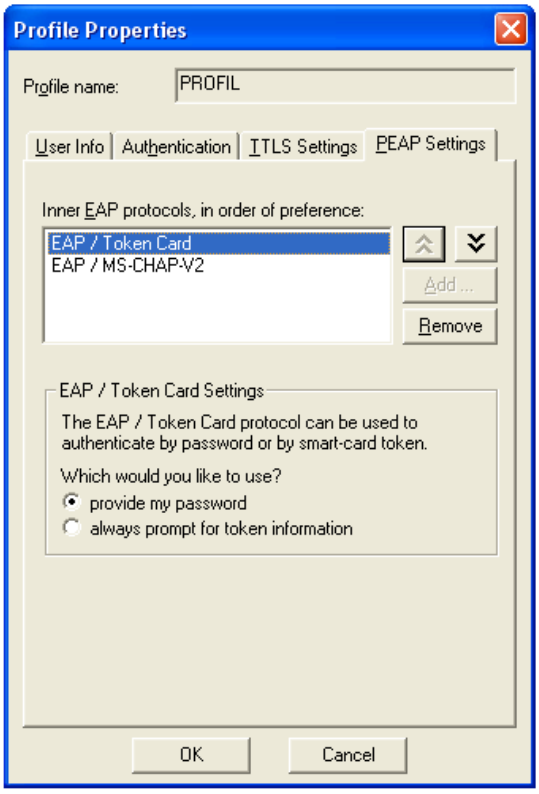


Pojawiające się okno zawiera listę stworzonych profili uwierzytelniania, które zawierają opisy kompletne sposoby i dane pozwalające nam uwierzytelnić się w sieci.
Możemy dodawać nowe profile (Add), usuwać niepotrzebne (Remove) lub edytować istniejące (Properties).

Pierwsza zakładka „User info” zawiera dane użytkownika, które zostaną wykorzystane do uzyskania dostępu do sieci.

- Login name – zawiera nazwę użytkownika,
- Password – pozwala na zalogowanie się z użyciem hasła. Aby użyć tej możliwości należy włączyć „Permit login using password”, a następnie wybrać sposób jego podawania:
  - use Windows password – zostanie automatycznie użyte hasło podane podczas logowania do systemu Windows,
  - prompt for password – użytkownik zostanie poproszony o podanie hasła przy łączeniu się z siecią,
  - use the following password – zostanie użyte hasło wprowadzone poniżej.
- Certificate – pozwala na zalogowanie się z użyciem certyfikatu osobistego.





Zakładka „Authentication” pozwala na określenie protokołów uwierzytelniania, które zostaną użyte do uwierzytelnienia użytkownika w sieci.
Do widocznej listy dodajemy protokoły których chcemy użyć. Jeśli będzie ich kilka, pierwsze zostaną użyte te na górze listy, a następnie dalsze, w kolejności występowania.
Jeśli którykolwiek z protokołów umożliwia użytkownikowi potwierdzenie tożsamości serwera RADIUS, zanim wyśle mu dane uwierzytelniające, aktywna będzie opcja „Validate server certificate”, której włączenie spowoduje sprawdzenie certyfikatu serwera przez zalogowaniem się użytkownika.

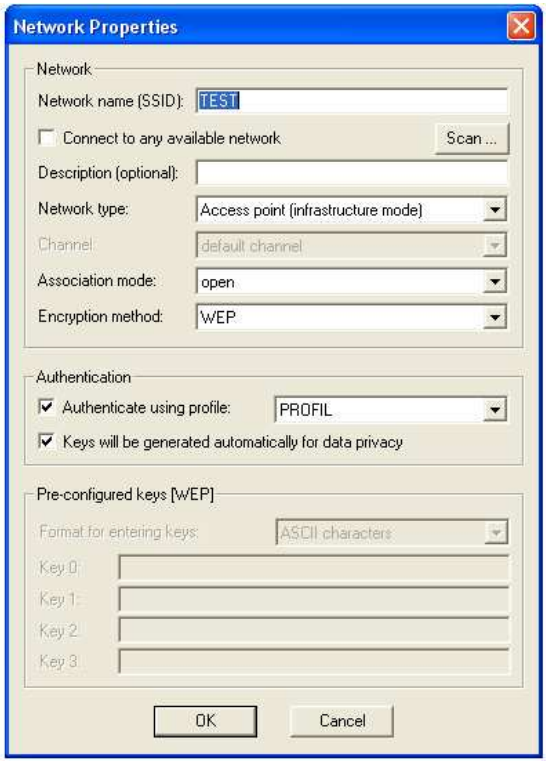
Dalsze zakładki „TTLS” i „PEAP” oferują możliwość szczegółowej konfiguracji tych najbardziej zaawansowanych protokołów uwierzytelniania.
Podczas laboratorium interesuje nas protokół PEAP – jego zakładka zawiera listę możliwych metod uwierzytelniania, które obsługuje ten protokół. Są to:

- EAP / MSCHAP-V2 – metoda wykorzystująca nazwę użytkownika i hasło,
- EAP / TokenCard – metoda wykorzystująca kartę chipową.

Podczas wykonywania zadań laboratoryjnych używana będzie tyko pierwsza z nich i tylko ona powinna być obecna na liście.

Dodanie nowej sieci bezprzewodowej

Z listy po lewej stronie należy wybrać pozycję „Networks”.



Pojawiające się okno zawiera listę skonfigurowanych sieci bezprzewodowych, możemy dodawać nowe sieci (Add), usuwać niepotrzebne (Remove) lub edytować istniejące (Properties).
Po użyciu opcji Add lub Properties, pojawia się okno zawierające szczegółowe opcje pracy danej sieci.

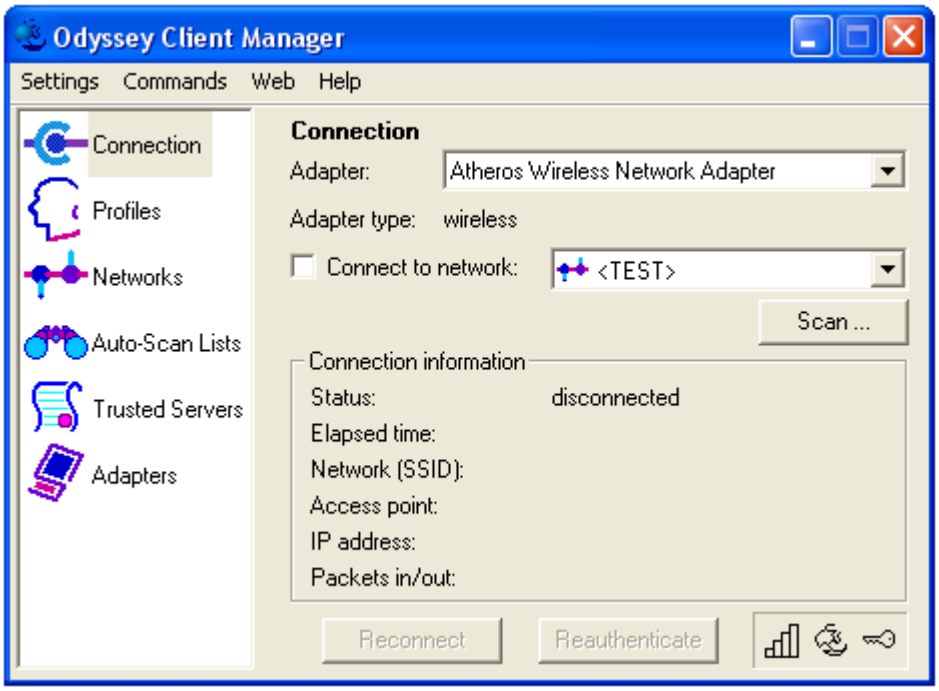
- **Nazwę sieci bezprzewodowej (SSID)** – wypełniamy ręcznie lub korzystając z przycisku SCAN, który da na listę do wyboru.
  Możliwe jest również zaznaczenia opcji „Connect to any …”, która spowoduje, że wprowadzone tu ustawienia zostaną użyte do połączeń ze wszystkimi sieciami bezprzewodowymi, które nie są osobno zdefiniowane w programie.
- **Rodzaj sieci (Network type)** – określa czy dana sieć pracuje w trybie ad-hoc, czy infrastructure.
- **Sposób asocjacji (Association mode)** – wybieramy opcję „OPEN” gdyż nie stosujemy uwierzytelniania ze wspólnym hasłem będącego częścią procedury asocjacji standardu 802.11.
- **Szyfrowanie (Encryption method)** – sposób szyfrowania ruchu sieciowego. Wybieramy w zależności od ustawień sieci do której się podłączamy.

Szczególnie interesuje nas grupa ustawień „Authentication” czyli uwierzytelnianie.
Włączenie opcji **„Authenticate using profile: ___”** spowoduje użycie sposobu uwierzytelniania określonego we wcześniej stworzonym profilu uwierzytelniania.
Opcja **„Keys will be generated automatically for data privacy”** pozwala klientowi na skorzystanie z klucza szyfrującego WEP, automatycznie wygenerowanego i przesłanego mu przez serwer RADIUS po udanym uwierzytelnieniu. Jeśli ta opcja jest wyłączona, a wybrano

WEP jako metodę szyfrowania danych w sieci, aktywuje się sekcja „Pre-configured keys” umożliwiająca ręczne wprowadzenie kluczy WEP.

Połączenie z siecią

Z listy po lewej stronie należy wybrać pozycję „Connection”.
Pojawiające się okno zawiera szczegółowe dane dotyczące aktualnego stanu klienta i jego połączenia z siecią.



Pozycja „Adapter” pozwala na wybranie interfejsu sieciowego, którego użyjemy do połączenia z siecią. Aby interfejs sieciowy buł widoczny na tej liście, musi zostać dopisany do listy obsługiwanych interfejsów, w opisany wcześniej sposób.
Po wybraniu interfejsu, jego typ zostanie wyświetlony poniżej (adapter type).
Opcja „Connect to network” pozwala na nakazanie połączenia z wybraną z rozwijanej listy siecią. Lista zawiera sieci zdefiniowane wcześniej w oknie „Networks”. Zaznaczenie opcji powoduje natychmiastowe rozpoczęcie łączenia z wybraną siecią. Odznaczenie opcji przerywa proces łączenia, lub powoduje rozłącznie z siecią.
Przycisk „Scan” powoduje wyświetlenie listy dostępnych sieci, wraz z ich aktualnym poziomem sygnału.

Przycisk „RECONNECT” pozwala na rozłączenie się (dezasocjację) z aktualnie wybraną siecią i rozpoczęcie procesu podłączania (asocjacji) od nowa.
Przycisk „REAUTHENTICATE” powoduje anulowanie aktualnego uwierzytelnienia i rozpoczęcie procesu uwierzytelniania do nowa. Połączenie (asocjacja) z siecią zostaje zachowana.

Sekcja „Connection information” zawiera szczegółowe informacje na temat aktualnego stanu łączności klienta z siecią. Najważniejszą informacją jest **aktualny stan klienta (Status)**:

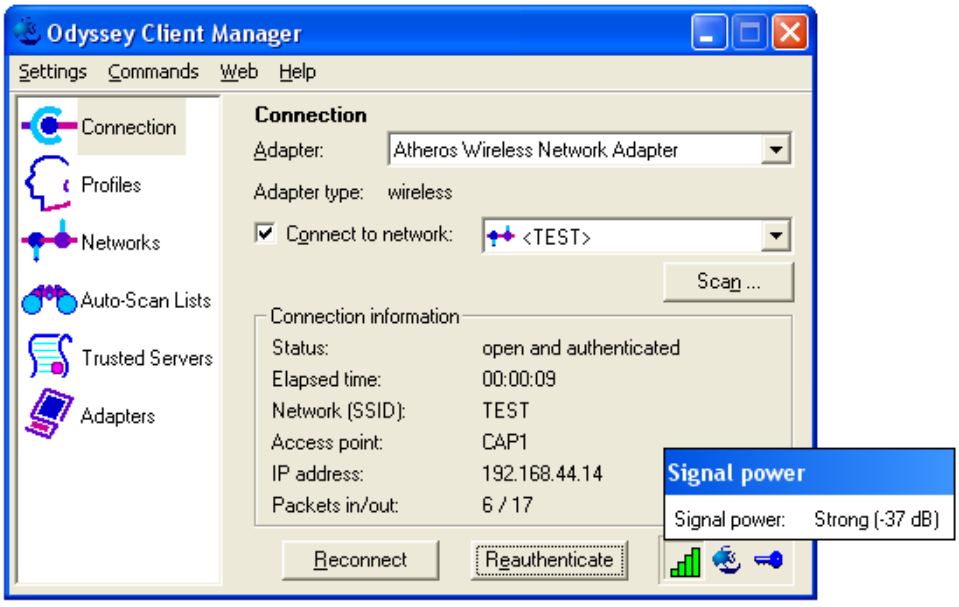
- ***Disconnected*** – klient nie próbuje łączyć się z siecią, gdyż zabronił tego użytkownik odznaczając opcję „Connect to natwork: ____”.
- ***Searching for access point*** – klient sprawdza listę dostępnych sieci bezprzewodowych.
- ***Searching for <SSID>*** - klient szuka podanej sieci bezprzewodowej w celu podłączenia się.
- ***Waiting to authenticate*** – klient jest podłączony do sieci bezprzewodowej, lecz nie rozpoczął uwierzytelniania, gdyż czeka na upływ określonego czasu. Występuje najczęściej po nieudanej próbie uwierzytelnienia. Natychmiastowe rozpoczęcie uwierzytelniania można wymusić używając przycisku „REAUTHENTICATE”.
- ***Requesting authentication*** – klient właśnie rozpoczął proces uwierzytelniania i oczekuje na odpowiedź ze strony sieci.
- ***Authenticating*** – klient jest w trakcie uwierzytelniania i nastąpiła już obustronna wymiana wiadomości pomiędzy klientem a siecią.
- ***Waiting for keys*** – klient uwierzytelnił się i oczekuje na przesłanie przez serwer kluczy szyfrujących.
- ***Open and authenticated*** – klient uwierzytelnił się oraz skonfigurował pomyślnie, i może pracować w danej sieci.
- ***Open / authentication*** – klient uwierzytelnił się już oraz skonfigurował pomyślnie i może pracować w danej sieci, lecz przeprowadzane jest aktualnie ponowne uwierzytelnianie.

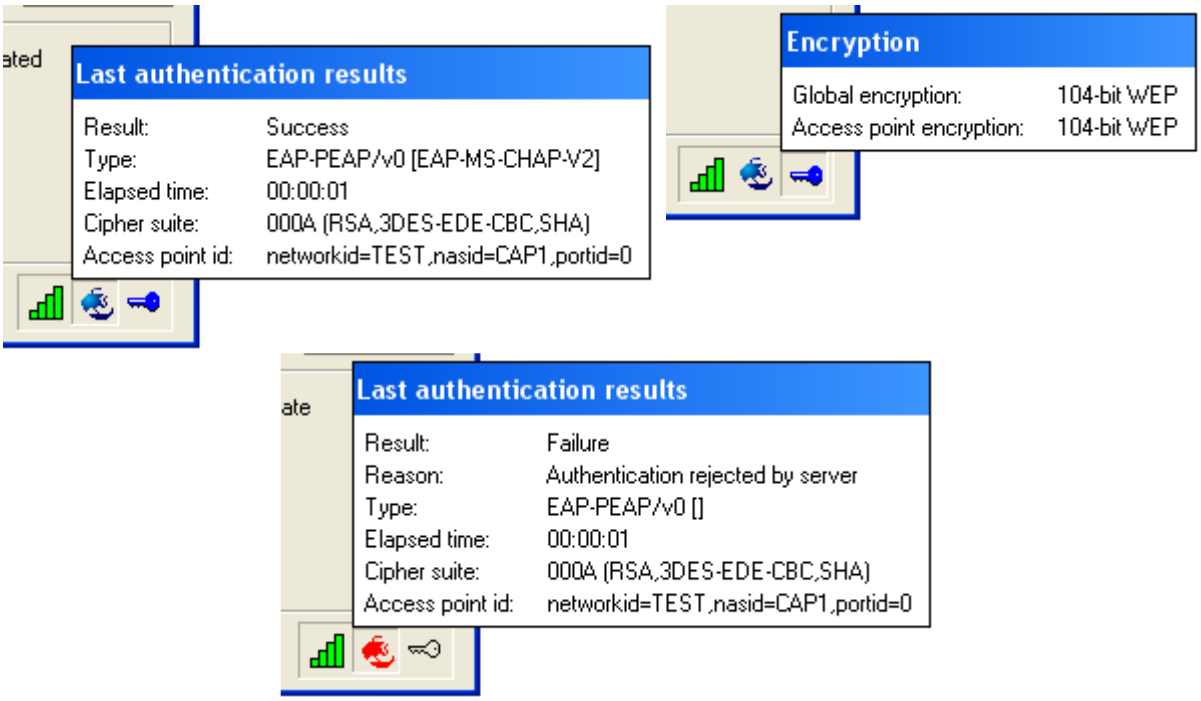
Dalsze informacje dostępne w tej sekcji to: czas połączenia (elapsed time), identyfikator sieci bezprzewodowej (SSID), nazwa punktu dostępowego (access point), adres IP klienta (IP address) i liczba przesłanych pakietów (packets in/out).

Pożyteczne informacje zawierają również 3 ikony w prawym-dolnym rogu okna. Od lewej to: siła sygnału, uwierzytelnienie i szyfrowanie. Kolory ikon mają następujące, ogólne znaczenie:

- szary (przezroczysty) – funkcja nieużywana,
- zielony – funkcja aktywna i działa prawidłowo,
- czerwony – próba realizacji funkcji zakończyła się błędem.

Szczegółowe informacje można odczytać naciskając ikony lewym przyciskiem myszy.





<u>Uwagi do wskaźnika „Status" w sekcji „Connection information"</u>

Opóźnienia na etapie ***„Searching for <SSID>"*** wynikają z problemów ze znalezieniem i podłączeniem się z siecią bezprzewodową i nie mają związku z mechanizmami uwierzytelniania. Pomaga tu najczęściej:

- Odczekanie do około 30 s – 1 min.
- Rozłączanie poprzez wyłączenie opcji „Connect to network" i ponowne jej włączenie.
- Wyłączenie i włączenie interfejsu sieciowego w systemie Windows.

Opóźnienia na etapie ***„Requesting authentication"*** wynikają zwykle z problemów w komunikacji punktu dostępowego z serwerem uwierzytelniania. Powodem jest najczęściej błędna konfiguracja AP lub serwera. Drugim powodem może być użycie przez klienta protokołu/metody uwierzytelniania nieobsługiwanej przez serwer.

Opóźnienia na etapie ***„Waiting for keys"*** wynikają zwykle z wyboru metody uwierzytelnienia, która nie pozwala jednocześnie na przesłanie kluczy szyfrujących klientowi (np. MD5). Należy zrezygnować z szyfrowania w sieci (definicja sieci->Encryption method) lub wybrać metodę uwierzytelniania która na to pozwala (np. PEAP, EAP-TLS, EAP-TTLS).

<u>Uwaga dotycząca hasła wprowadzanego ręcznie</u>

Jeśli korzystamy z opcji „prompt for password", czyli z hasła podawanego ręcznie przy próbie połączenia się z siecią, to po poprawnym uwierzytelnieniu hasło to zostanie zapamiętane i program przestanie o nie pytać.

Jeśli chcemy ponownie uzyskać okno dialogowe pozwalające na ręczne podanie hasła, należy użyć opcji „Forget Password" z menu „Commands" programu.