Projekt nr. POIG.02 03. 00-00-028/08-01

www.platon.pionier.net.pl

PLATFORMA OBSŁUGI NAUKI PLATON

KOORDYNATOR: INSTYTUT CHEMII BIOORGANICZNEJ PAN
POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE
ul. Noskowskiego 12/14, 61-704 Poznań, (+48 61) 858 20 00, fax: (+48 61) 852 59 54, e-mail: office@man.poznan.pl, www: http://www.man.poznan.pl

Opis testu i instalacji na potrzeby usługi eduroam

LANCOM WLC-4006

LANCOM

Systems

Tomasz Piontek (Tomasz.Piontek@umk.pl)

Łukasz Cichocki (Lukasz.Cichocki@umk.pl)

dokument przygotowany w ramach projektu PLATON

maj 2012

INNOWACYJNA GOSPODARKA
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ ROZWOJU REGIONALNEGO

DOTACJE NA INNOWACJE Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Rozwoju Regionalnego

Spis treści

Wstęp

Usługa eduroam jest skierowana do społeczności akademickiej na całym świecie. Obejmuje swoim zasięgiem między innymi 32 kraje Europy, 6 krajów Azjatyckich leżących nad Pacyfikiem. Jej głównym celem jest zapewnienie społeczności akademickiej szybkiego i bezpiecznego dostępu do Internetu bez konieczności kontaktowania się z lokalnym administratorem. Uwierzytelnianie stosowane w eduroam umożliwia zabezpieczenie przed dostępem nieupoważnionych osób oraz w przypadku ewentualnych nadużyć umożliwia identyfikację konkretnego użytkownika.

W Polsce z eduroam korzysta obecnie kilkanaście uczelni wyższych, użytkowników sieci PIONIER. Prace nad wprowadzeniem eduroam jako pełnej usługi sieci PIONIER obejmują również rozpoznanie dostępnego sprzętu WiFi i przeprowadzenie testów kompatybilności z założeniami eduroam.

Założenia

Testy skupiają się na tych cechach sprzętu, które są szczególnie istotne w sieci uczelnianej bezprzewodowej włączanej w strukturę eduroam. Z założenia są to zatem testy częściowe.

SSID

W ramach eduroam rozgłaszamy dwie sieci. Podstawowa sieć nazwana jest zawsze „eduroam”, oraz dodatkowa sieć konferencyjna w naszym modelu nazwana „Konferencja”.

Szyfrowanie

- SSID eduroam musi być zabezpieczone WPA2/AES, a opcjonalnie WPA1/TKIP. Teoretycznie nie ma przeciwwskazań, aby na tym samym SSID stosować oba standardy. W praktyce, może to prowadzić do pewnych niekompatybilności z sieciami w innych instytucjach, a nawet utrudnień z wykonaniem połączenia. W czasie testów laboratoryjnych zastosowano metodę mieszaną (WPA2/WPA1)

- SSID „Konferencja” jest traktowane jako sieć do krótkoterminowego użytkowania przez osoby niezwiązane z uczelnią, która jest rozgłaszana tylko na obszarze konkretnej konferencji w czasie jej trwania. Użytkownicy tej sieci nie kontaktują się z administratorami eduroam. Informacje dotyczące sposobu i zasad korzystania z tej sieci otrzymują od organizatora. Sieć ta jest rozgłaszana bez szyfrowania i zabezpieczana portalem dostępowym. Testowana jest jedynie możliwość skonfigurowania takiego SSID i związania go z wydzielonym VLAN-em.

Uwierzytelnienie

Użytkownicy korzystający z SSID „eduroam” są podłączani na podstawie przesyłanych przez nich danych do serwera Radius. Po autoryzacji użytkownik zostaje przypisany do VLANu wskazanego przez serwer Radius. W modelu testowym rozróżniamy 3 grupy użytkowników umownie nazwaliśmy je : pracownicy, studenci oraz goście (użytkownicy uwierzytelniani przez instytucje pracujące w ramach eduroam, posiadające własny serwer Radius) . Uwierzytelnianie jest oparte o 3 typy EAP: TLS, TTLS/PAP, PEAP/MSCHAPv2.

VLAN

Numeracja i opis VLAN-ów stosowanych w testach

- 30 – Pracownicy
- 31 – Studenci
- 32 – Goście
- 33 – Zarządzający dla kontrolera, AP, serwerów DHCP oraz RADIUS
- 35 – Konferencyjny

Infrastruktura stała niezależna od zestawu testowego konieczna do stworzenia modelu

Urządzenia użytkowane w ramach projektu muszą spełniać minimalnie kilka podstawowych funkcji. Podstawowym wymaganiem jest obsługa VLAN 802.1q. W ramach modelu korzystamy z następujących urządzeń:

- Server FreeRadius v. 2.1.12
- Serwer DHCP
- Router
- Przełączniki Ethernet

Przełącznik 1 :

Port 3	– vlan 30,31,32,35	– Tagged
Port 4	– vlan 33	– Untagged
Port 12	– vlan 33	– Untagged,
Port 15	– vlan 30,31,32,33,35	– Tagged

Przełącznik 2 :

Port 4	– vlan 30,31,32,33,35	– Tagged,
Port 12	– vlan 33	– Untagged
Port 13	– vlan 33	– Untagged
Port 15	– vlan 30,31,32,33,35	– Tagged

Opis testowanego zestawu:

Kontroler: LANCOM WLC 4006

L.P.	Rodzaj testów	Wynik
1	Model	WLC 4006
2	Wersja oprogramowania	8.50.0142 / 12.07.2011
3	Ilość portów LAN	5
4	Konfiguracja portu serwisowego	Prędkość: 115200 Bity danych: 8 Parzystość: brak Bity stopu: 1
5	Programowe wyłączanie kontrolera	TAK (nie badano)
6	Obsługa VLANów	TAK
7	Dynamiczne VLANy	TAK
8	Ilość rozgłaszanych SSID	brak danych
9	Accounting	TAK
10	Wbudowany serwer DHCP	TAK
11	Tunelowanie ruchu z AP do kontrolera	TAK
12	Statyczne przekierowanie ruchu z AP do lokalnego VLANu	TAK
13	Dynamiczne przekierowanie ruchu z AP do lokalnego VLANu na podstawie RADIUSa	TAK
14	Wbudowany serwer RADIUS	TAK
15	Wyszukiwanie intruzów	TAK (nie badano)
16	Zwalczanie intruzów	TAK (nie badano)
17	Zewnętrzne oprogramowanie do zarządzania	LANconfig
18	Zewnętrzne oprogramowanie do monitoringu	LANmonitor WLANmonitor
19	QOS	TAK (nie badano)
20	Ilość zarządzanych AP	od 6 do12
21	Obsługa SNMP	TAK

Access Point: ***LANCOM L-321agn Wireless***

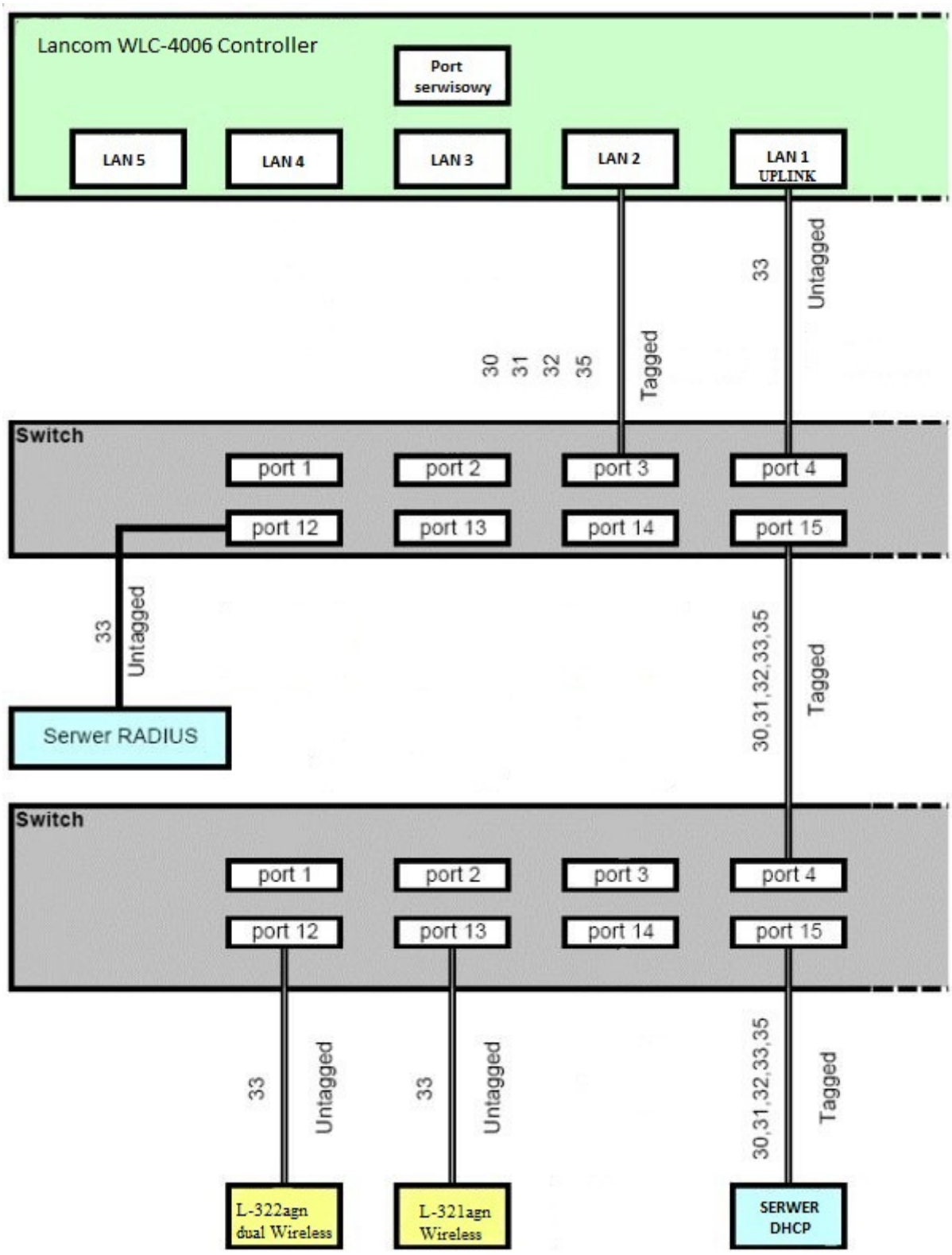
L.P.	Rodzaj testów	Wynik
1	Model	L-321agn
2	Wersja oprogramowania	8.00.0255 / 18.02.2011
3	Ilość portów LAN	2
4	Praca w standardzie 802.11a	TAK
5	Praca w standardzie 802.11n	TAK
6	Praca w standardzie 802.11b	TAK
7	Praca w standardzie 802.11g	TAK
8	Praca samodzielna	TAK
9	Praca pod kontrola kontrolera	TAK
10	Zarządzanie urządzeniem poprzez TELNET	TAK (nie badano)
11	Zarządzanie urządzeniem poprzez SSH	TAK
12	Zarządzanie urządzeniem poprzez CLI	TAK (nie badano)
13	Zarządzanie urządzeniem poprzez WWW	TAK (nie badano)
14	Zasilanie poprzez Ethernet	TAK
15	Praca w standardzie IEEE 802.3af	TAK

DOTACJE NA INNOWACJE Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Rozwoju Regionalnego

Access Point: ***LANCOM L-322agn dual Wireless***

L.P.	Rodzaj testów	Wynik
1	Model	L-322agn dual
2	Wersja oprogramowania	8.00.0255 / 18.02.2011
3	Ilość portów LAN	2
4	Praca w standardzie 802.11a	TAK
5	Praca w standardzie 802.11n	TAK
6	Praca w standardzie 802.11b	TAK
7	Praca w standardzie 802.11g	TAK
8	Praca samodzielna	TAK
9	Praca pod kontrola kontrolera	TAK
10	Zarządzanie urządzeniem poprzez TELNET	TAK (nie badano)
11	Zarządzanie urządzeniem poprzez SSH	TAK
12	Zarządzanie urządzeniem poprzez CLI	TAK (nie badano)
13	Zarządzanie urządzeniem poprzez WWW	TAK (nie badano)
14	Zasilanie poprzez Ethernet	TAK
15	Praca w standardzie IEEE 802.3af	TAK

Schemat modelu



Metodologa testów

Testy laboratoryjne

- **Opis:** Polegają na sprawdzeniu funkcjonalności urządzeń oraz uzyskaniu dostępu zespołu testującego do usług wymaganych w projekcie (2 użytkowników). Czas trwania - od 7 do 10 dni roboczych. A następnie małej grupy użytkowników końcowych (10 użytkowników)
- **Cel:** opis podstawowych cech sprzętu, sprawdzenie możliwości urządzeń pod kątem wymagań eduroam.
- **Wykorzystano:**
  - komputer PC z systemem Windows 7 Professional
  - komputer PC z systemem Windows Vista Business
  - komputer PC z systemem Windows XP Professional
  - aparat telefoniczny z systemem Android 2.3.4
  - aparat telefoniczny z systemem Symbian S60
- **Testowane zagadnienia**

1. Kontrola poprawności połączeń we współpracy z różnymi typami EAP
   - TLS
   - TTLS
   - PEAP
2. Kontrola poprawności przydzielania użytkowników do określonych VLAN-ów
3. Kontrola poprawności współpracy z serwerem DHCP
4. Analiza jakości połączenia. Test ciągłości połączenia, czas przejścia między testowanymi AP oraz czas autentykacji przełączana między AP jest oparty o obserwację pakietów ICMP Ping wysyłanych przy pomocy programu fping z częstotliwością 100ms i czasem oczekiwania 100 ms.

5. Wyniki

L.P.	Nazwa	Opis testu	Karta	System	Wynik
1	Uwierzytelnienie	TLS	Sony Ericsson Neo V	Android	OK
2			Intel 5100 AGN	Windows 7	OK
3			Realtek RTL8187SE	Windows XP	OK
4			Intel 3945	Vista	OK
5			Nokia 5530	Symbian	OK
6		TTLS	Sony Ericsson Neo V	Android	OK
7			Intel 5100 AGN	Windows 7	OK
8			Realtek RTL8187SE	Windows XP	OK
9			Intel 3945	Vista	OK
10			Nokia 5530	Symbian	OK
11		PEAP	Sony Ericsson Neo V	Android	OK
12			Intel 5100 AGN	Windows 7	OK
13			Realtek RTL8187SE	Windows XP	OK
14			Intel 3945	Vista	OK
15			Nokia 5530	Symbian	OK
16	Obsługa VLAN	Przydzielanie do VLANów na podstawie autoryzacji z serwera RADIUS	Sony Ericsson Neo V	Android	OK
17			Intel 5100 AGN	Windows 7	OK
18			Realtek RTL8187SE	Windows XP	OK
19			Intel 3945	Vista	OK
20			Nokia 5530	Symbian	OK
21	Współpraca z serwerem DHCP	Współpraca z zewnętrznym serwerem DHCP	Sony Ericsson Neo V	Android	OK
22			Intel 5100 AGN	Windows 7	OK
23			Realtek RTL8187SE	Windows XP	OK
24			Intel 3945	Vista	OK
25			Nokia 5530	Symbian	OK

Analiza jakości połączenia:

W czasie testów w środowisku testowym WPA2 oraz WPA1 podczas przechodzenia pomiędzy urządzeniami nie zauważono zerwań połączenia.

Obciążenie systemów:

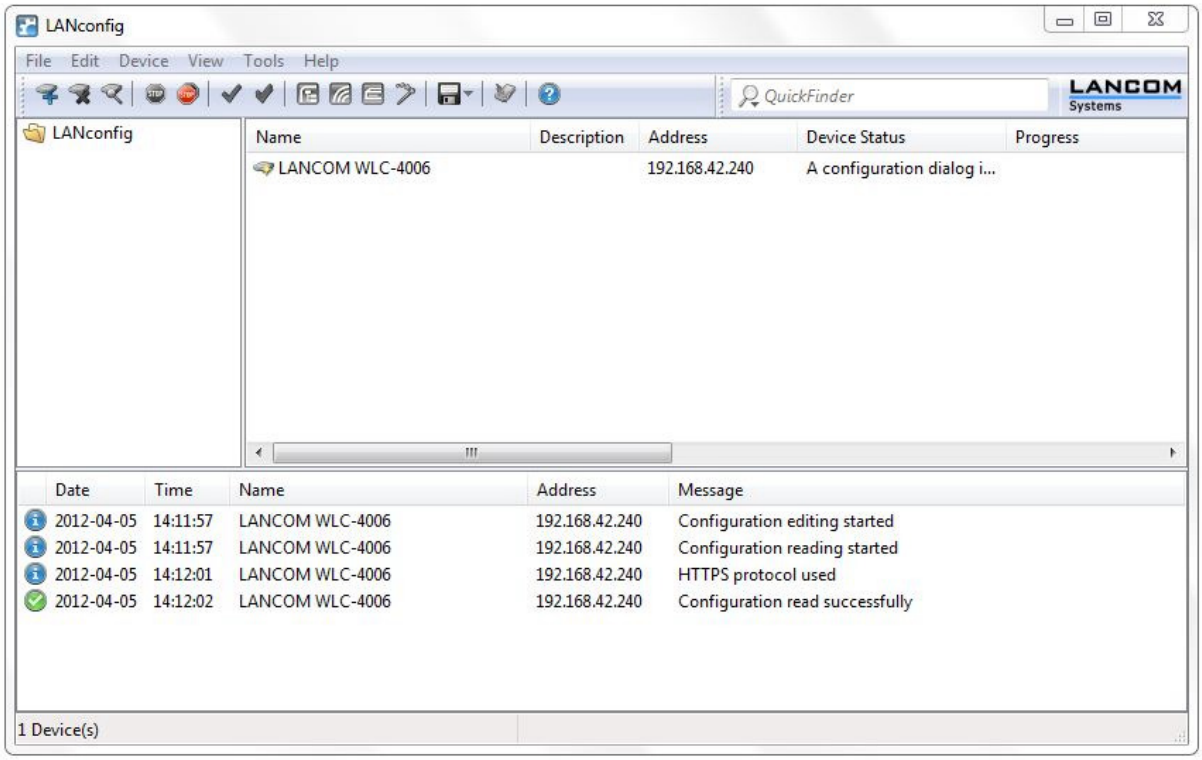
Podczas testów nie zaobserwowano problemów wydajnościowych.

Uwagi:

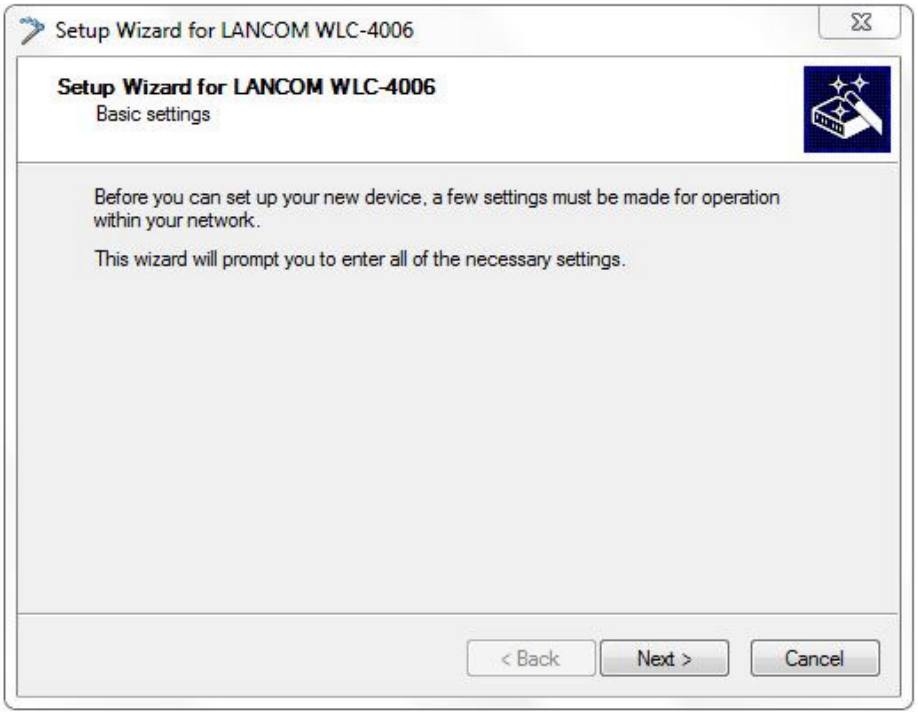
1. Podczas konfiguracji należy zwrócić szczególną uwagę na poprawne ustawienie serwera NTP na kontrolerze. Access Point bez synchronizacji czasowej nie podłączy się do kontrolera.
2. Access Point może pracować w różnych trybach. Sprawdzamy w konfiguracji Access Pointa czy wybrany tryb pracy to *Managed*. W tym celu logujemy się na Access Point poprzez oprogramowanie LANconfig i zaznaczamy w Physical WLAN settings – WLAN interface: *WLAN operation mode: Managed (Access point)*

Konfiguracja eduroam krok po kroku

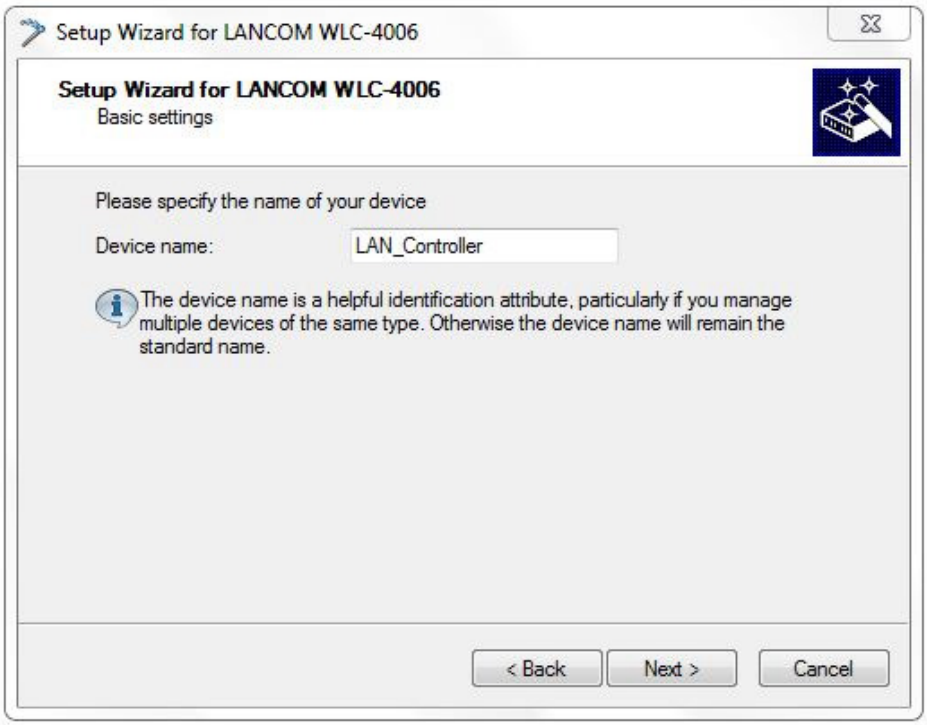
W pierwszej kolejności uruchamiamy kontroler i podłączamy do niego stację roboczą (np. laptop) oraz Access Point. Następnie instalujemy oprogramowanie dołączone przez producenta – LANconfig.



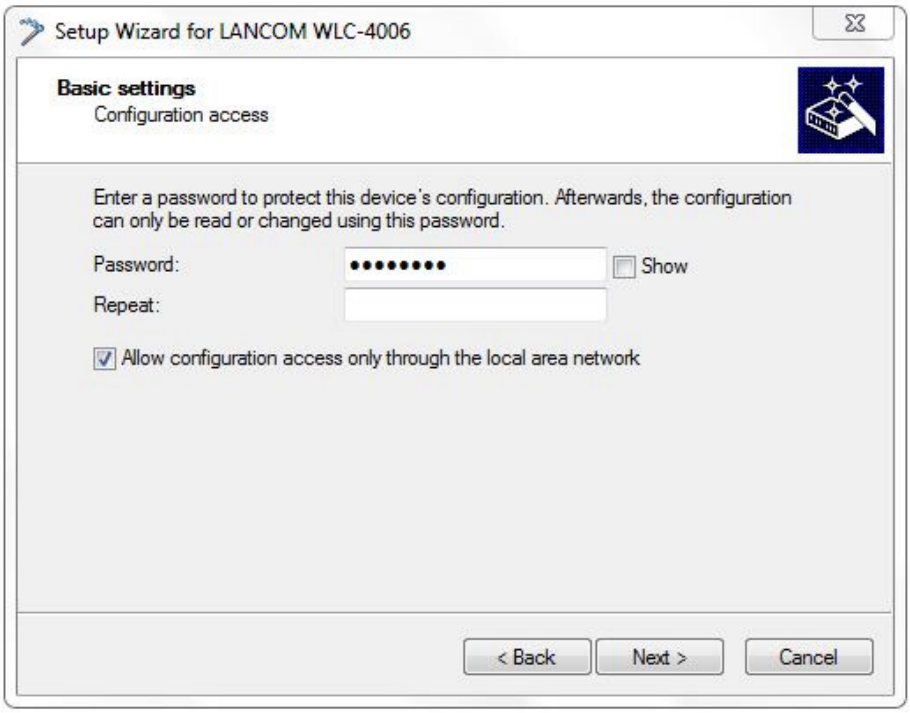
Program automatycznie wykryje kontroler i uruchomi kreator konfiguracji.



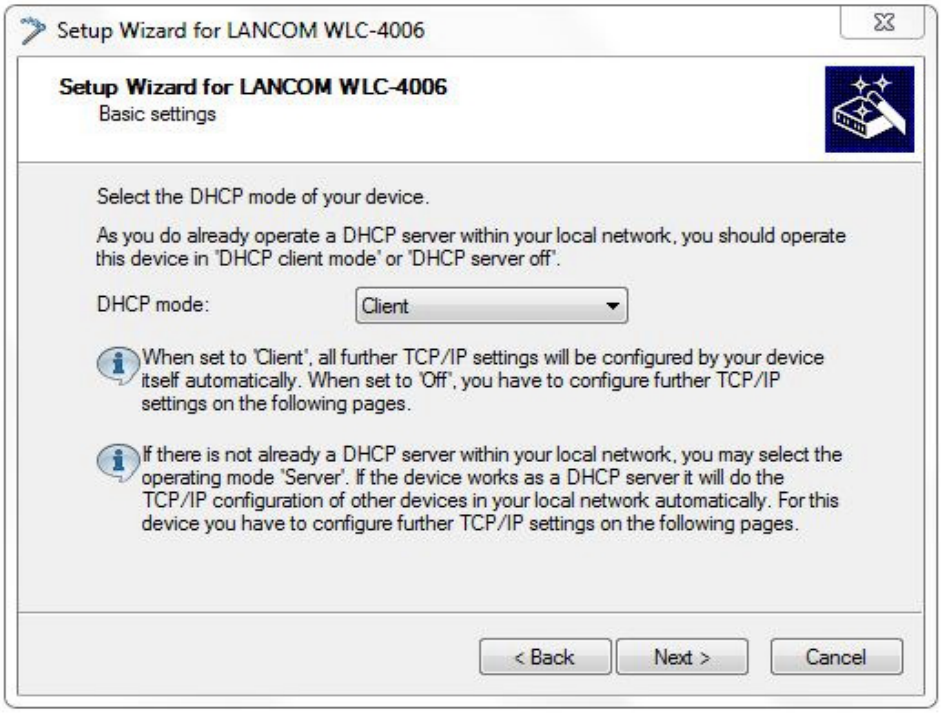
1. Wprowadzamy nazwę urządzenia (np. *LAN_Controller*).



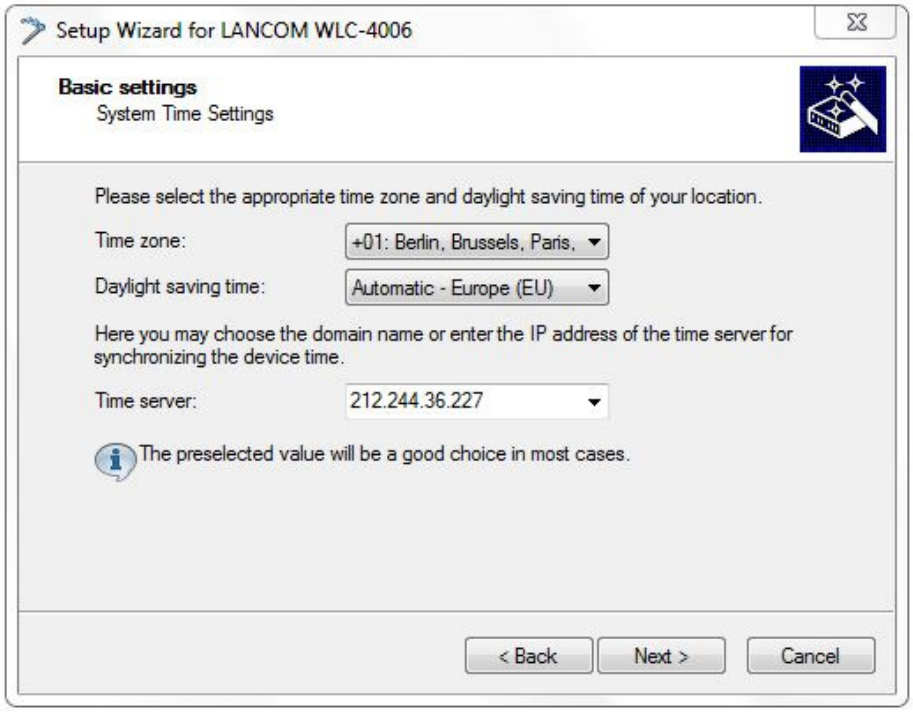
2. Następnie wprowadzamy hasło



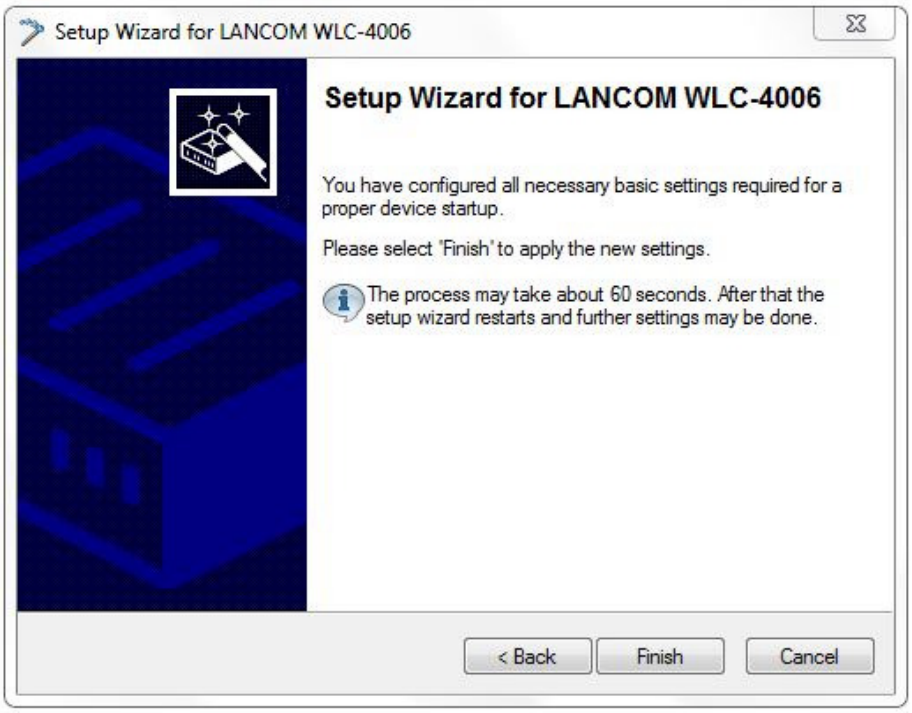
3. Wybieramy tryb pracy DHCP. (w tym przypadku wykorzystany jest zewnętrzny serwer DHCP, więc należy wybrać ***DHCP mode***: *Client*)



4. Następnie wybieramy strefę czasową oraz wprowadzamy adres serwera NTP do synchronizacji czasu



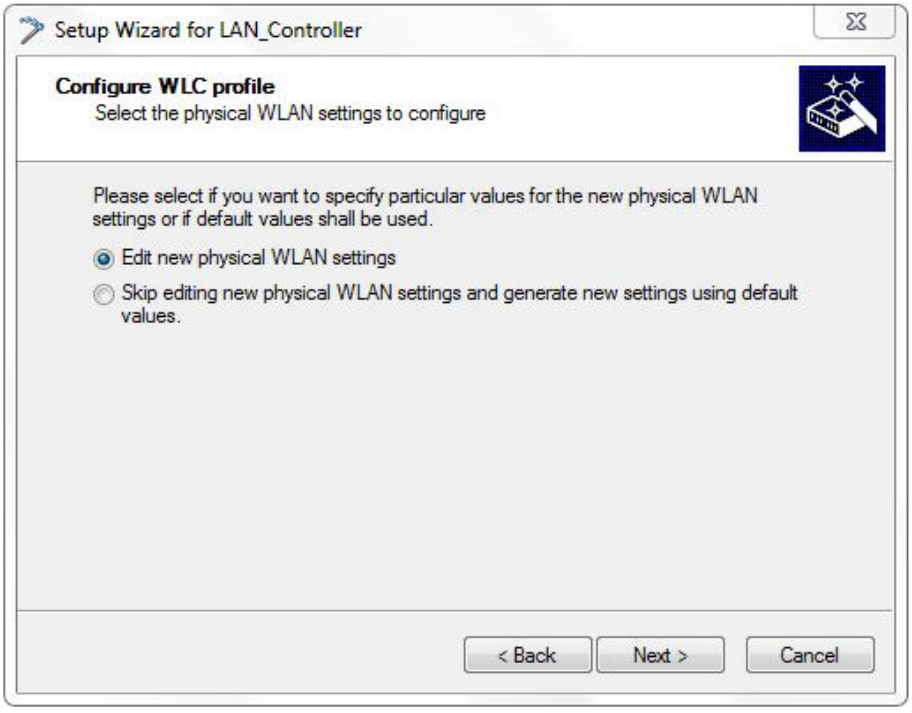
5. Koniec działania kreatora, aby zakończyć wybieramy *Finish*.



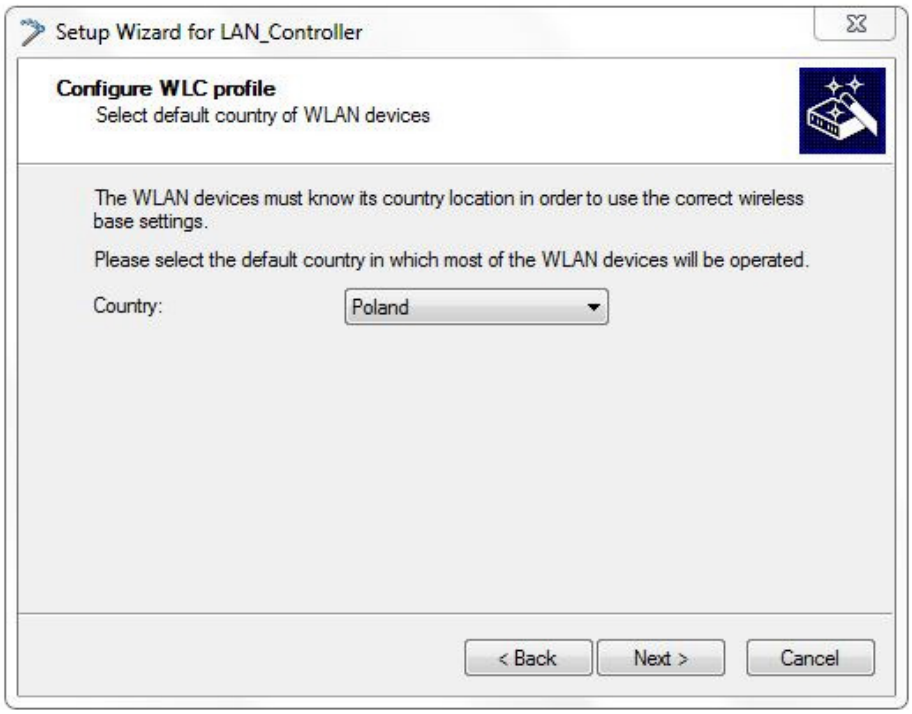
Po zakończeniu, uruchomi się kolejny kreator.

1. Kreator 2 Wybieramy *Configure WLC profile*

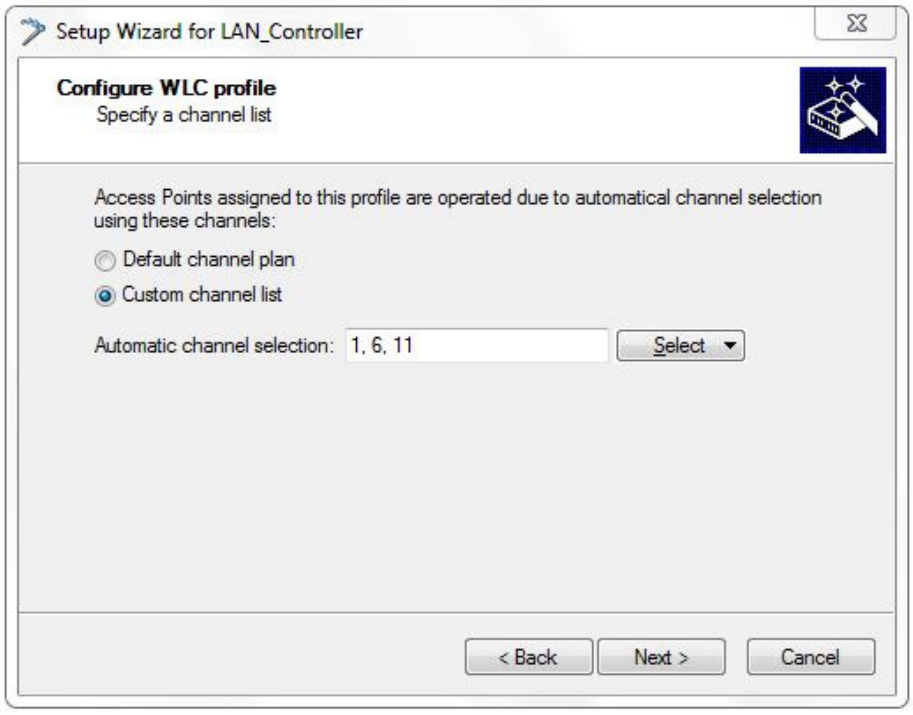
2. Następnie wybieramy *Edit New physical WLAN settings*



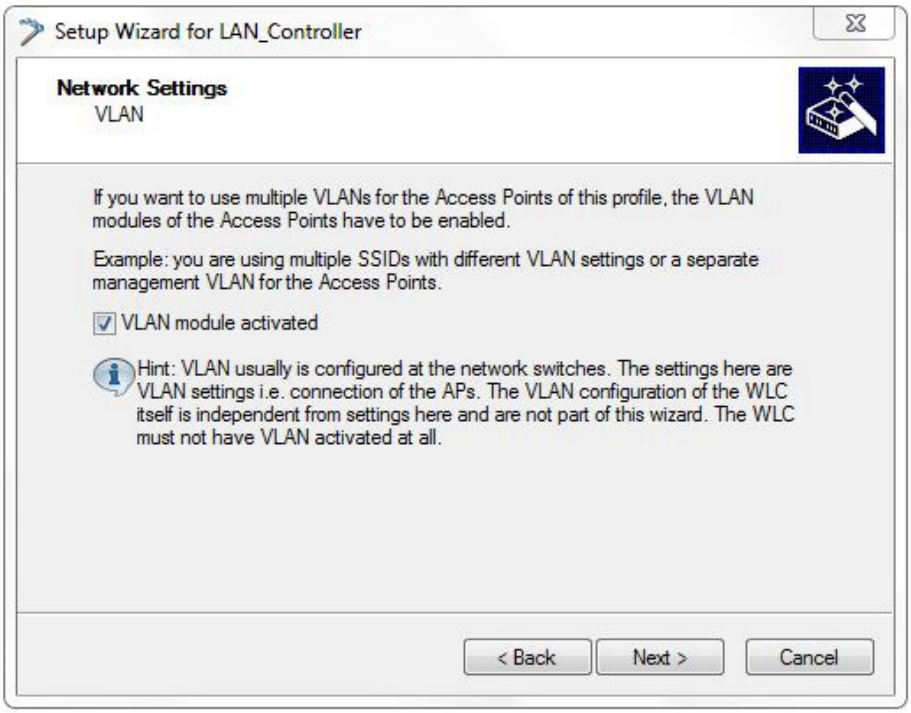
3. Następnie z listy należy wybieramy lokalizację (kraj): *Poland*



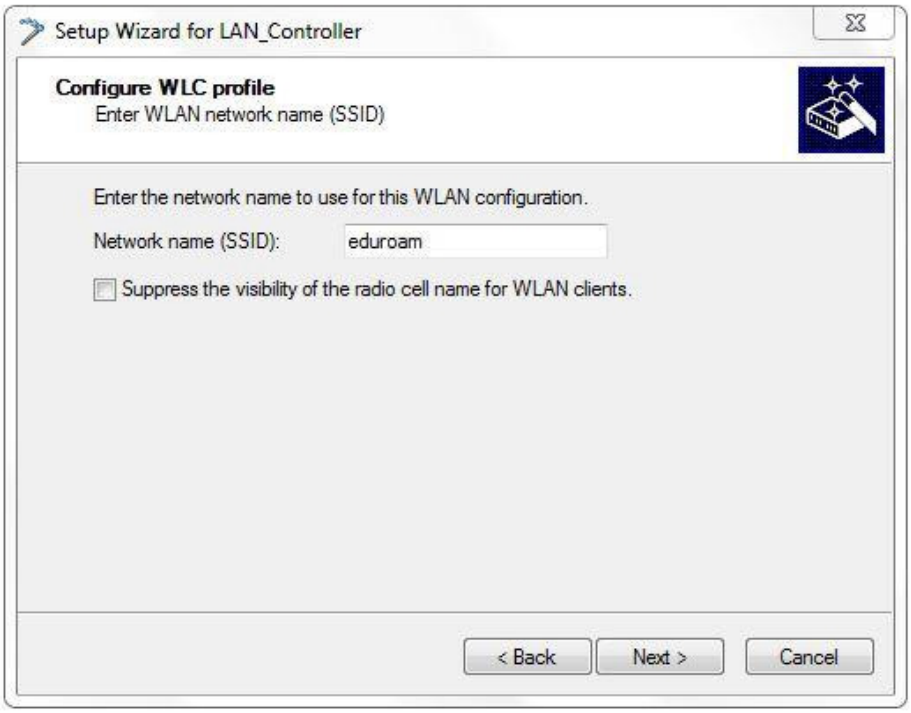
4. Następnie wybieramy kanały w tym przypadku *1, 6, 11*. Wybieramy z rozwijalnej listy *(Select*)



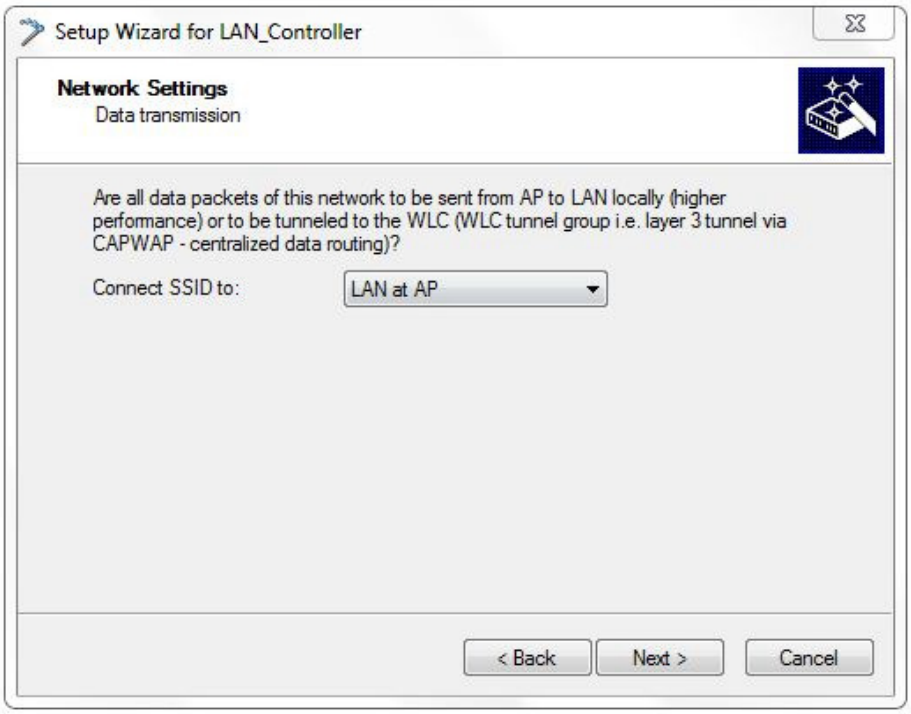
5. Wybieramy obsługę VLAN *(VLAN module activated*)



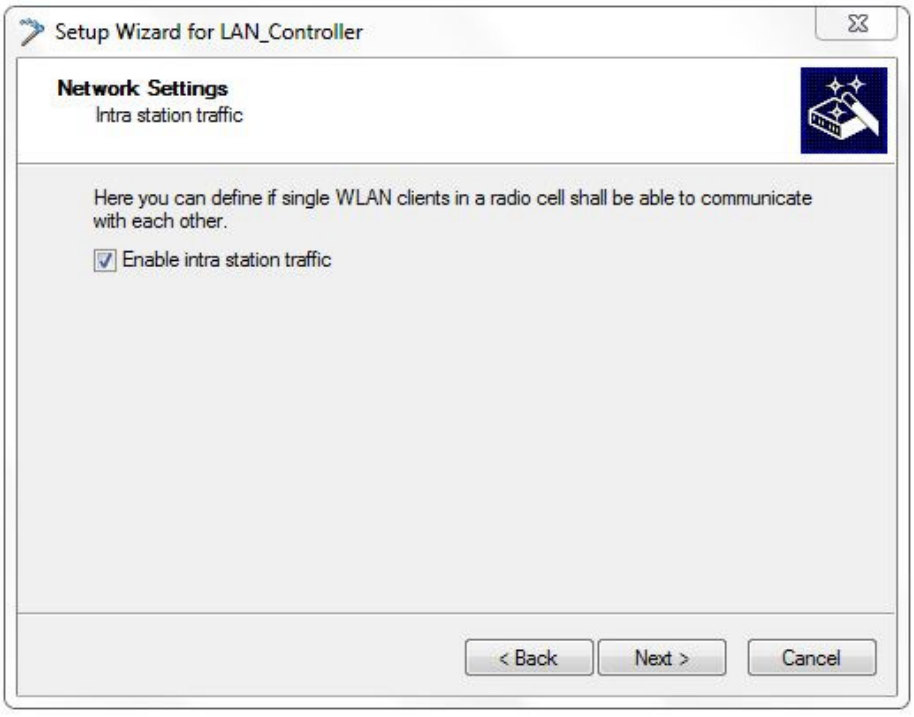
6. Następnie wprowadzamy SSID sieci (*eduroam*)



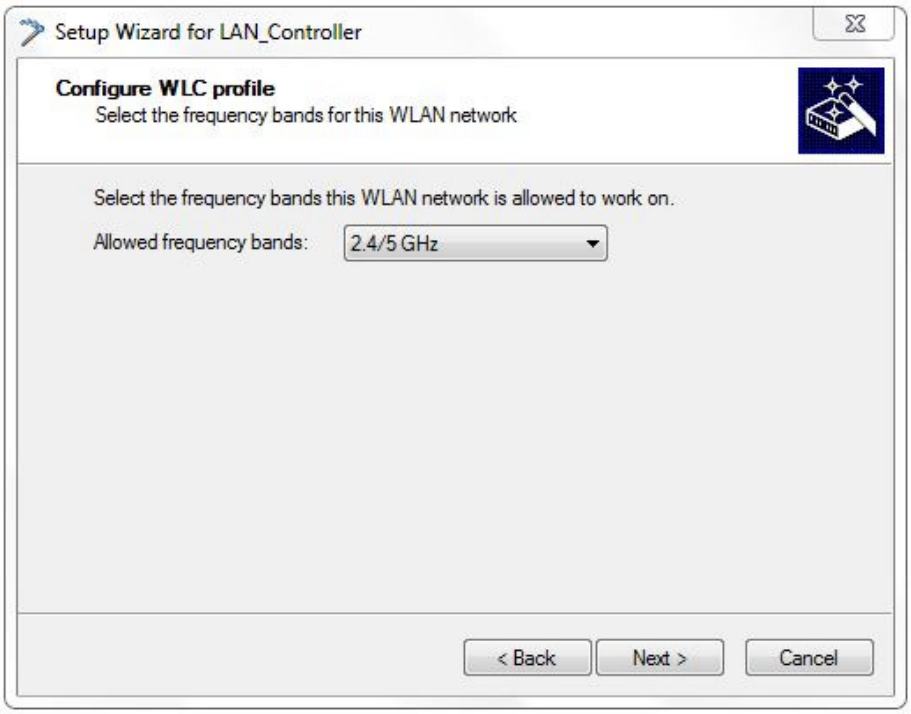
7. Wybieramy przesyłanie pakietów z AP do LAN



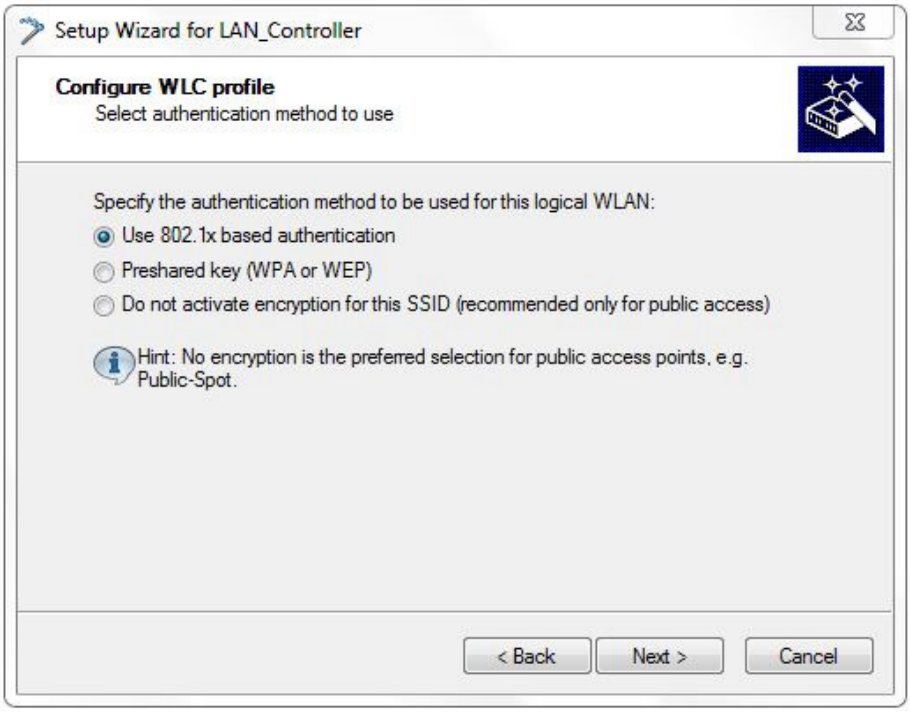
8. Możliwość komunikacji między użytkownikami w sieci bezprzewodowej. W tym przypadku wyrażamy na to zgodę i zaznaczamy *Enable intra station traffic*



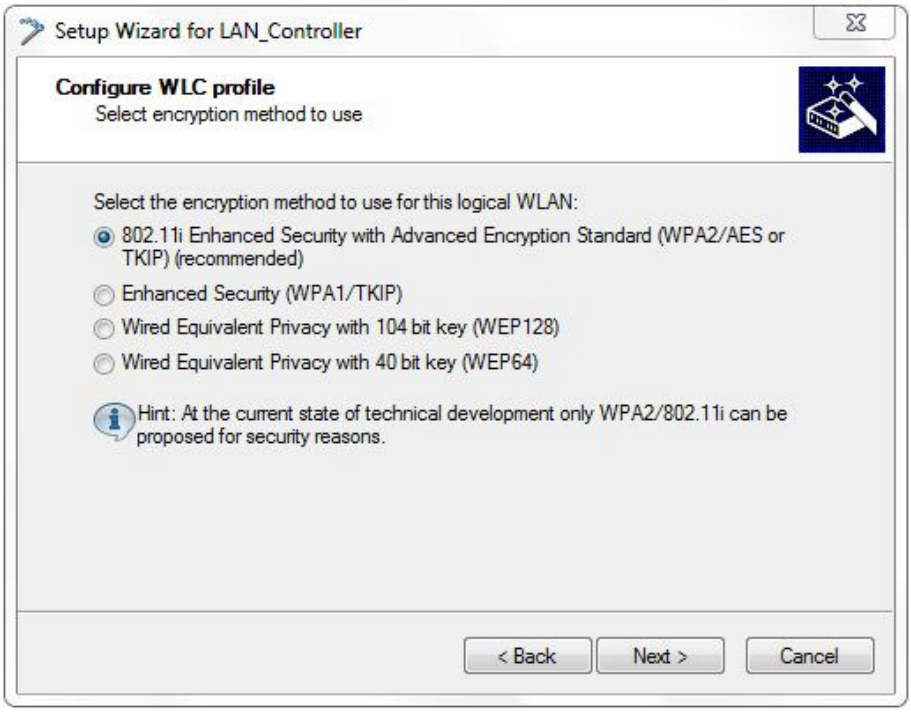
9. Wybieramy dozwolone częstotliwości nadawania (*Allowed frequency bands: 2.4/5GHz*)



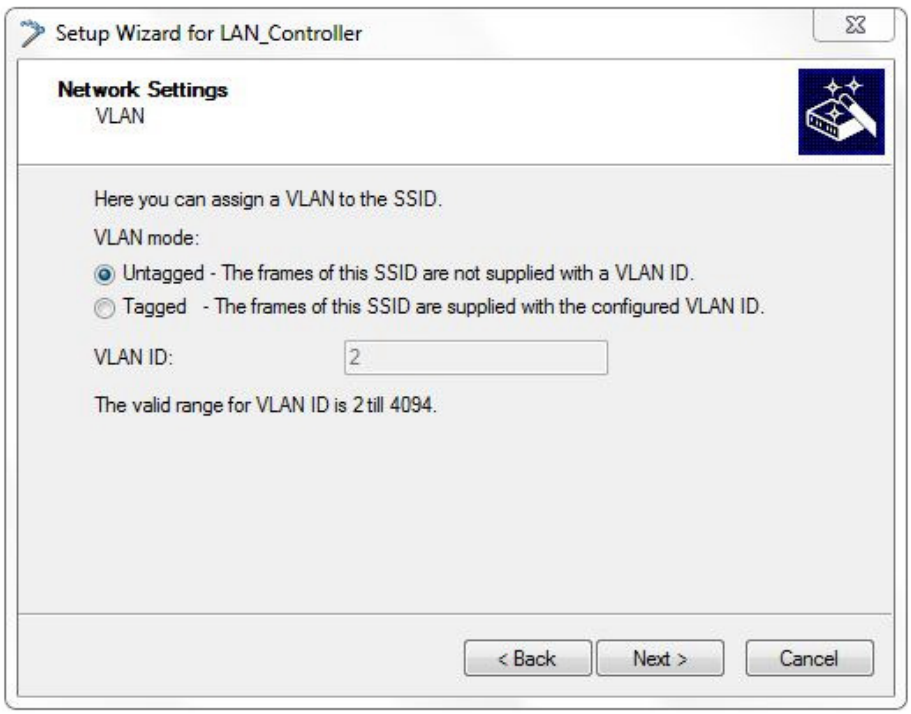
10. Wybieramy metodę uwierzytelniania. Authentication metod (*802.1x*)



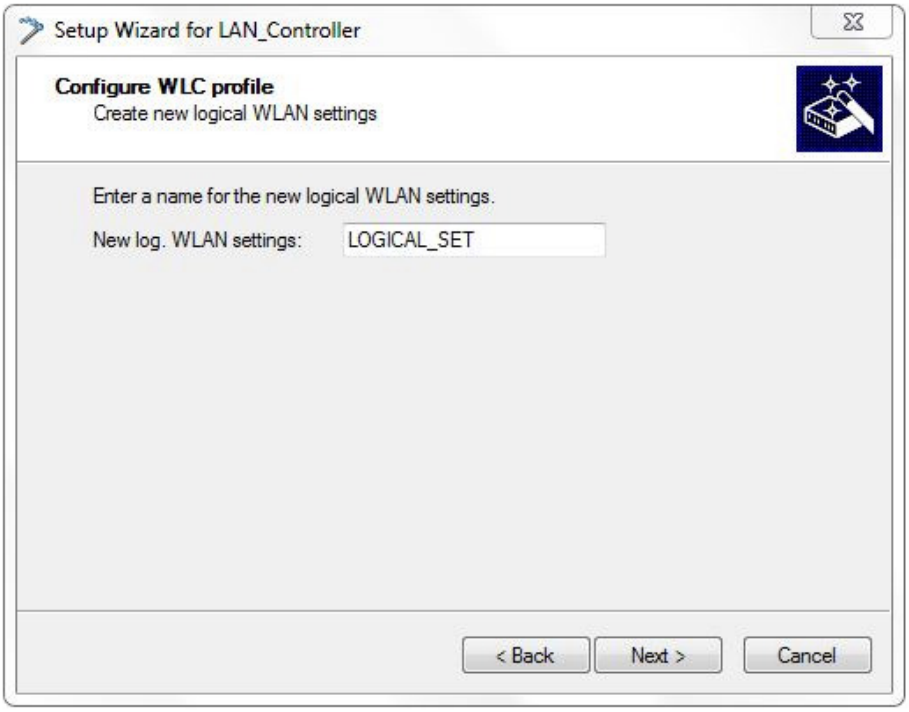
11. Metoda szyfrowania. Encryption metod (*802.11i WPA2*)



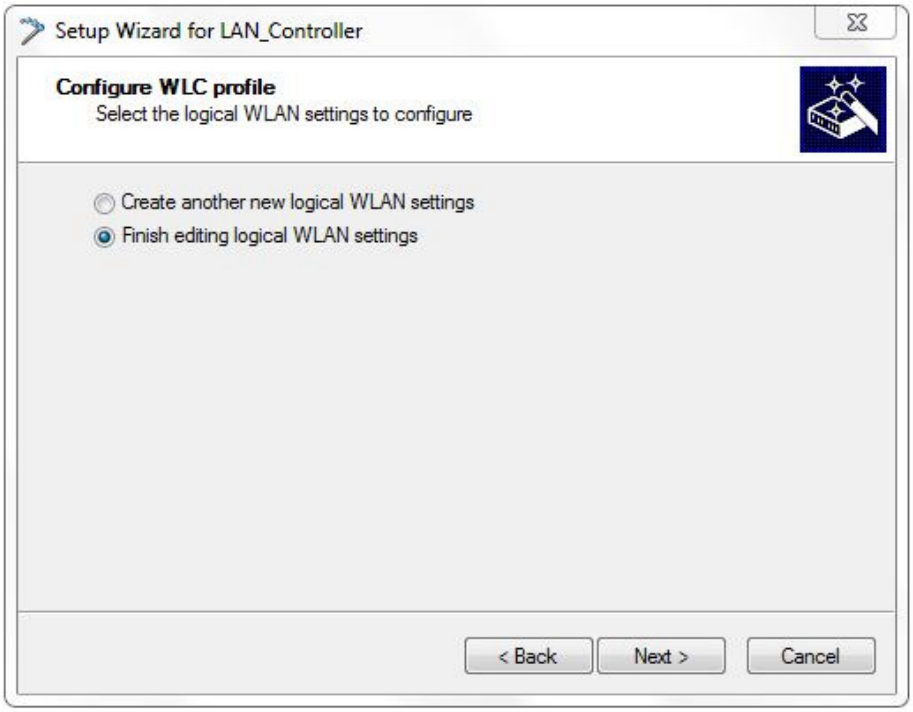
12. VLAN unntaged. Komunikacja AP z serwerem Radius następuje po nietagowanym VLANie. Po poprawnej autoryzacji użytkownik zostanie przypisany do tagowanego VLANu wskazanego przez serwer Radius.



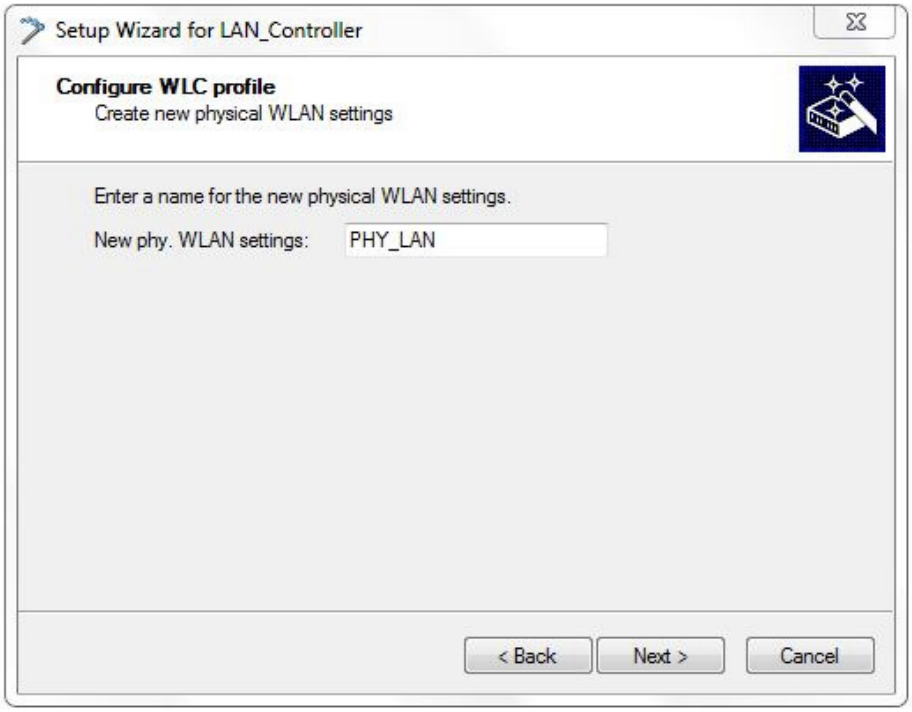
13. Logical WLAN settings (*LOGICAL_SET*)



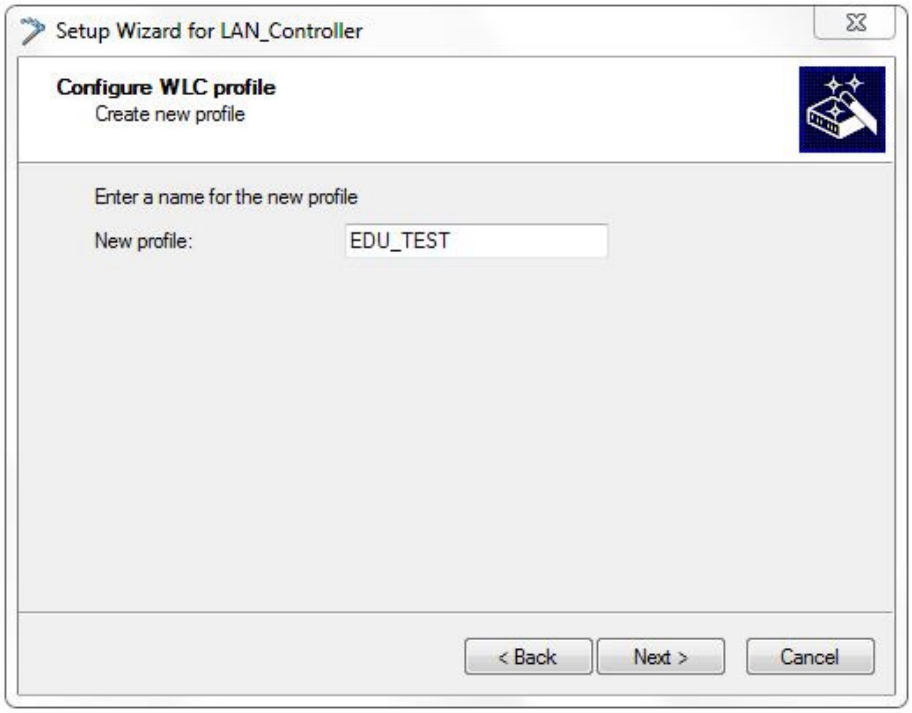
14. Kończymy działanie kreatora dla logical WLAN settings



15. Physical WLAN settings (*PHY_LAN*)

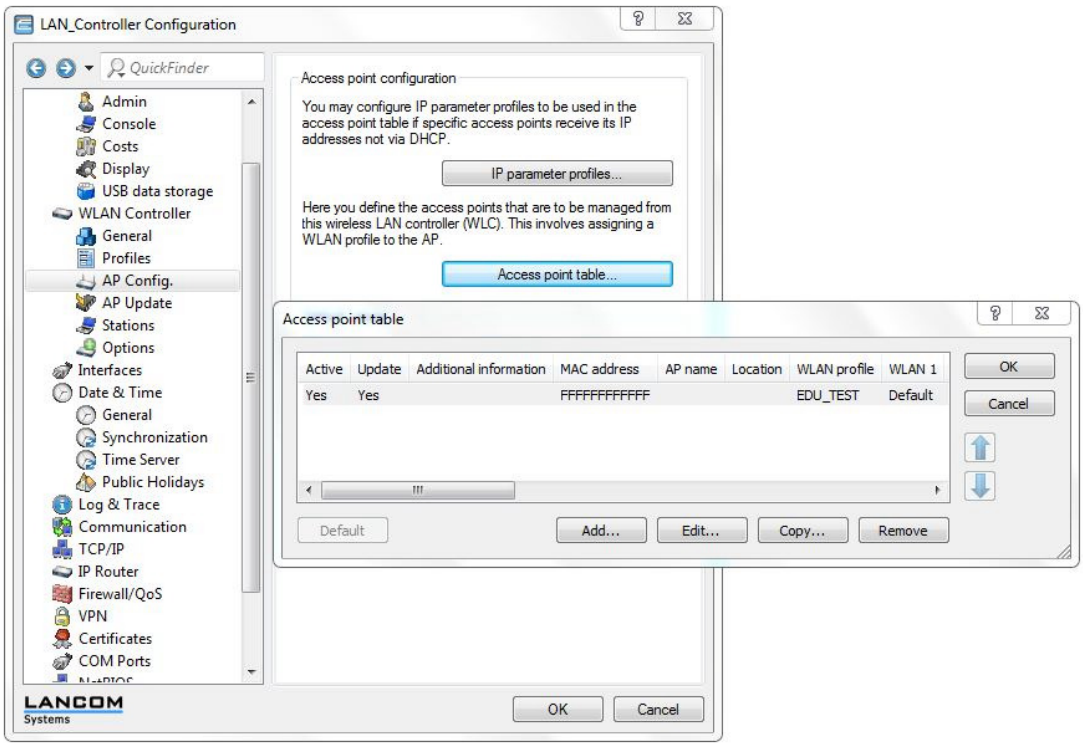


16. Nazwa profilu *(EDU_TEST)*



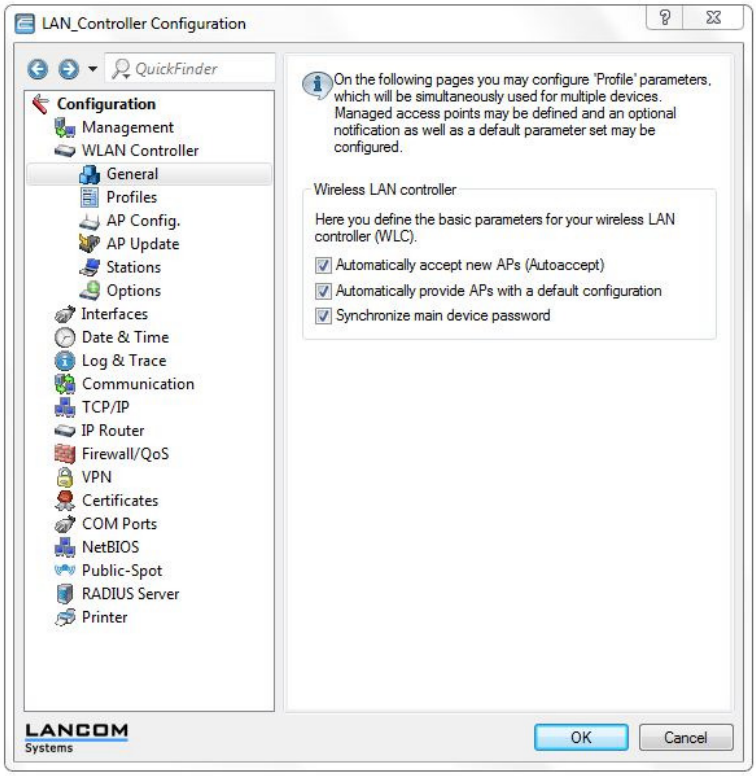
17. Koniec działania kreatora

Po zakończeniu działania kreatora należy poprzez program LANConfig ustawiamy domyślny wpis dla wszystkich Access Point'ów.



Zaznaczamy również pola w sekcji Wireless LAN controller:

1. Automaticaly akcept New APs
2. Automatically provide APs with a default configuration
3. Synchronize main device password



Po tym zabiegu każdy nowy AP otrzyma po podłączeniu profil EDU_TEST.

Ustawienia serwerów RADIUS