PLATFORMA OBSŁUGI NAUKI

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



zie MAN

INNOWACYJNA

GOSPODARKA

maj 2012

Insci







SHINTERN

1NZ3

90

PLATFORMA OBSŁUGI NAUKI PLATON

Spis treści

Wstęp
Założenia3
SSID
Szyfrowanie
Uwierzytelnienie
VLAN
Infrastruktura stała niezależna od zestawu testowego konieczna do stworzenia modelu 5
Opis testowanego zestawu
Kontroler6
AP7
Schemat modelu9
Metodologa testów10
Testy laboratoryjne10
Testowane zagadnienia10
Wyniki testów11
Opis konfiguracji testowanego zestawu13





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







PLATFORMA OBSŁUGI NAUKI PLATON

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	llość 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	ТАК
7	Dynamiczne VLANy	ТАК
8	Ilość rozgłaszanych SSID	brak danych
9	Accounting	ТАК
10	Wbudowany serwer DHCP	ТАК
11	Tunelowanie ruchu z AP do kontrolera	ТАК
12	Statyczne przekierowanie ruchu z AP do	ТАК
	lokalnego VLANu	
13	Dynamiczne przekierowanie ruchu z AP do	ТАК
	lokalnego VLANu na podstawie RADIUSa	
14	Wbudowany serwer RADIUS	ТАК
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	llość zarządzanych AP	od 6 do12
21	Obsługa SNMP	ТАК







PLATFORMA OBSŁUGI NAUKI PLATON

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	llość portów LAN	2
4	Praca w standardzie 802.11a	ТАК
5	Praca w standardzie 802.11n	ТАК
6	Praca w standardzie 802.11b	ТАК
7	Praca w standardzie 802.11g	ТАК
8	Praca samodzielna	ТАК
9	Praca pod kontrola kontrolera	ТАК
10	Zarządzanie urządzeniem poprzez TELNET	TAK (nie badano)
11	Zarządzanie urządzeniem poprzez SSH	ТАК
12	Zarządzanie urządzeniem poprzez CLI	TAK (nie badano)
13	Zarządzanie urządzeniem poprzez WWW	TAK (nie badano)
14	Zasilanie poprzez Ethernet	ТАК
15	Praca w standardzie IEEE 802.3af	ТАК







PLATFORMA OBSŁUGI NAUKI PLATON

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	llość portów LAN	2
4	Praca w standardzie 802.11a	ТАК
5	Praca w standardzie 802.11n	ТАК
6	Praca w standardzie 802.11b	ТАК
7	Praca w standardzie 802.11g	ТАК
8	Praca samodzielna	ТАК
9	Praca pod kontrola kontrolera	ТАК
10	Zarządzanie urządzeniem poprzez TELNET	TAK (nie badano)
11	Zarządzanie urządzeniem poprzez SSH	ТАК
12	Zarządzanie urządzeniem poprzez CLI	TAK (nie badano)
13	Zarządzanie urządzeniem poprzez WWW	TAK (nie badano)
14	Zasilanie poprzez Ethernet	ТАК
15	Praca w standardzie IEEE 802.3af	ТАК







PLATFORMA OBSŁUGI NAUKI PLATON

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			Sony Ericsson Neo V	Android	ОК
2			Intel 5100 AGN	Windows 7	ОК
3		TLS	Realtek RTL8187SE	Windows XP	ОК
4			Intel 3945	Vista	ОК
5			Nokia 5530	Symbian	ОК
6	C		Sony Ericsson Neo V	Android	ОК
7	wier		Intel 5100 AGN	Windows 7	ОК
8	zyte	TTLS	Realtek RTL8187SE	Windows XP	ОК
9	Inier		Intel 3945	Vista	ОК
10	nie		Nokia 5530	Symbian	ОК
11			Sony Ericsson Neo V	Android	ОК
12			Intel 5100 AGN	Windows 7	ОК
13		PEAP	Realtek RTL8187SE	Windows XP	ОК
14			Intel 3945	Vista	ОК
15			Nokia 5530	Symbian	ОК
16			Sony Ericsson Neo V	Android	ОК
17	Obsł	VLANów na	Intel 5100 AGN	Windows 7	ОК
18	uga	podstawie	Realtek RTL8187SE	Windows XP	ОК
19	VLAN	autoryzacji z serwera RADIUS	Intel 3945	Vista	ОК
20	2		Nokia 5530	Symbian	ОК
21	S		Sony Ericsson Neo V	Android	ОК
22	Wsp erwe	Współpraca z	Intel 5100 AGN	Windows 7	ОК
23	oółpr grem	zewnętrznym D ca serwerem DHCP	Realtek RTL8187SE	Windows XP	ОК
24	aca z DHC		Intel 3945	Vista	ОК
25	P		Nokia 5530	Symbian	ОК







PLATFORMA OBSŁUGI NAUKI PLATON

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:

- Podczas konfiguracji należy zwrócić szczególną uwagę na poprawne ustawienie serwera NTP na kontrolerze. Access Point bez synchronizacji czasowej nie podłączy się do kontrolera.
- 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)*







PLATFORMA OBSŁUGI NAUKI PLATON



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.

CANconfig						
File Edit Dev	vice View	Tools Help				
777 (🛛 🥥 🔻	/ ✔ @ @ @ ≫ 	0	P. Qu	ickFinder	Systems
🔄 LANconfig		Name	Description	Address	Device Status	Progress
		LANCOM WLC-4006		192.168.42.240	A configuration dialog i	
Date	Time 14:11:57	✓	Address	Message 0 Configuration	editing started	•
2012-04-05	14:11:57	LANCOM WLC-4006	192.168.42.24	0 Configuration	reading started	
2012-04-05	14:12:01	LANCOM WLC-4006	192.168.42.24	0 HTTPS protoco	ol used	
2012-04-05	14:12:02	LANCOM WLC-4006	192.168.42.24	0 Configuration	read successfully	
1 Device(s)						









Program automatycznie wykryje kontroler i uruchomi kreator konfiguracji.

Setup Wizard for LANCOM	WLC-4006
Basic settings	
Before you can set up your within your network.	new device, a few settings must be made for operation
This wizard will prompt you t	o enter all of the necessary settings.

1. Wprowadzamy nazwę urządzenia (np. LAN_Controller).









PLATFORMA OBSŁUGI NAUKI PLATON

2. Następnie wprowadzamy hasło

Basic settings		
Configuration access		
Enter a password to p can only be read or c	protect this device's configuration hanged using this password.	on. Afterwards, the configuration
Password:	•••••	Show
Desert		
Repeat:		
Repeat:	n access only through the local	area network
Repeat:	n access only through the local	area network
Repeat:	n access only through the local	area network
Repeat:	n access only through the local	area network
Nepeat:	n access only through the local	area network
Repeat:	n access only through the local	area network

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





nści





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

Basic settings		*
System Time Settings		
Please select the appropr	riate time zone and daylight saving time of your locati	on.
Time zone:	+01: Berlin, Brussels, Paris, 🔻	
Daylight saving time:	Automatic - Europe (EU)	
Here you may choose the synchronizing the device	e domain name or enter <mark>the IP address of the time se</mark> time.	rverfor
Time server:	212.244.36.227 👻	
	lue will be a good choice in most cases	
The preselected val		

5. Koniec działania kreatora, aby zakończyć wybieramy Finish.











Po zakończeniu, uruchomi się kolejny kreator.

1. Kreator 2 Wybieramy Configure WLC profile

Setup Wizard for LAN_Con	troller	X
	Setup Wizard for LAN_Controller	
	This wizard lets you configure your device for specific applications quickly and easily.	
	What do you want to do?	
0	Manually edit the configuration	
	Configure WLC profile	
	 Set up Internet access Provide remote access (RAS, VPN) 	E
	Connect two local area networks (VPN) Remove remote site or access	
	Check security settings	*
	< Back Next > C	ancel

2. Następnie wybieramy Edit New physical WLAN settings

Co	nfigure WLC profile
	Select the physical WLAN settings to configure
	Please select if you want to specify particular values for the new physical WLAN settings or if default values shall be used.
	edit new physical WLAN settings
	Skip editing new physical WLAN settings and generate new settings using default values.
	< Back Next > Can









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

Contigure WLC proti	e		4
Select default count	ry of WLAN devices		
The WLAN devices base settings.	must know its country loc	ation in order to use	the correct wireless
Please select the de	fault country in which mo	st of the WLAN dev	ices will be operated.
Country:	Poland	•	

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

Configure WLC profile				*
Specify a channel list				
Access Points assigned to this using these channels:	s profile are operated	l due to automa	tical channel se	election
🔘 Default channel plan				
Oustom channel list				
Automatic channel selection:	1, 6, 11		Select -	









5. Wybieramy obsługę VLAN (VLAN module activated)



6. Następnie wprowadzamy SSID sieci (eduroam)

			1200
Configure WLC profile			*
Enter WLAN network nam	e (SSID)		
Enter the network name to	use for this WLAN configuration.		
Network name (SSID):	eduroam		
Suppress the visibility o	f the radio cell name for WLAN clients	s.	











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*

Network Settings				*
Intra station traffic				
Here you can define if single V with each other.	VLAN clients in a	radio cell sha	l be able to com	municate
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)

Confi	gure WLC profile
S	elect encryption method to use
Se	elect the encryption method to use for this logical WLAN:
0	802.11i Enhanced Security with Advanced Encryption Standard (WPA2/AES or TKIP) (recommended)
C	Enhanced Security (WPA1/TKIP)
C) Wired Equivalent Privacy with 104 bit key (WEP128)
C	Wired Equivalent Privacy with 40 bit key (WEP64)
(Hint: At the current state of technical development only WPA2/802.11i can be proposed for security reasons.

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.

network Settings				*
VLAN				
Here you can assig	n a VLAN to the SSID.			
VLAN mode:				
Ontagged - The	frames of this SSID are no	t supplied with	a VLAN ID.	
Tagged - The f	rames of this SSID are sup	plied with the	configured VL/	N ID.
VLAN ID:	2			
The valid range for	VLAN ID is 2 till 4094.			









13. Logical WLAN settings (LOGICAL_SET)

consigned in the provide		*
Create new logical WLAN s	ettings	
Enter a name for the new lo	gical WLAN settings.	
New log. WLAN settings:	LOGICAL_SET	

14. Kończymy działanie kreatora dla logical WLAN settings

Þ	Setup Wizard for LAN_Controller
	Configure WLC profile
	Select the logical WLAW settings to configure
	○ Create another new logical WLAN settings
	Inish editing logical WLAN settings
	< Back Next > Cancel









15. Physical WLAN settings (PHY_LAN)

Configure WLC profile		**
Create new physical WLAN	settings	
Enter a name for the new ph	vsical WLAN settings.	
New phy. WLAN settings:	PHY_LAN	

16. Nazwa profilu (EDU_TEST)

Contigure WLC profile Create new profile	B	and the second s
Enter a name for the	new profile	
New profile:	EDU_TEST	







PLATFORMA OBSŁUGI NAUKI PLATON

17. Koniec działania kreatora



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







PLATFORMA OBSŁUGI NAUKI PLATON

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.







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

www.platon.pionier.net.pl

PLATFORMA OBSŁUGI NAUKI PLATON

Ustawienia serwerów RADIUS

3 🕤 🔻 🔎 QuickFinder		Data traffic between the wireless LAN and your local network can
 Profiles AP Config. AP Update 	*	be restricted as required by enabling the MAC address check for individual logical WLAN networks and specifying all stations in the following table you want to grant access to those restricted logical WLAN networks.
Stations		Stations
 Options Interfaces Date & Time General 		To make station filtering work you have to switch on the RADIUS server of this device or make corresponding settings at 'RADIUS Server\Forwarding'.
 Synchronization Time Server Public Holidays Log & Trace Communication TCP/IP 		By default, the WLAN controller will forward requests to the RADIUS. To enable direct communication between AP and RADIUS server a few additional settings must be configured here. RADIUS server
 IP Router Firewall/QoS VPN Certificates COM Ports NetBIOS 	ш	
 Public-Spot RADIUS Server General Forwarding EAP 		
Solutions	-	

Туре	IP address	Port	Secret	OK
Account	158.75	1813	*	Cancel
Access	158.75	1812	*	Cancer
Backup account	158.75	1813	*	
Backup access	158.75	1812	*	





