Raport
“Wdrożenie usługi eduroam w sieci PIONIER”

Maja Górecka-Wolniewicz, Tomasz Wolniewicz

Projekt eduroam – wprowadzenie

Projekt eduroam został zainicjowany przez Surfnet i był rozwijany w ramach grupy roboczej TERENY TF-Mobility. Podstawowym założeniem było zbudowanie infrastruktury pozwalającej na swobodne uzyskiwanie dostępu do sieci przez studentów oraz pracowników instytucji akademickich, z jednoczesnym zachowaniem bezpieczeństwa i identyfikowalności użytkowników. Pierwsza szersza prezentacja tego rozwiązania opartego na protokole 802.1x, odbyła się w trakcie konferencji TNC 2003 w Zagrzebiu. W czasie kolejnej konferencji TNC 2004 na Rodos, projekt eduroam był już jednym z ważniejszych tematów wystąpień. Podobnie było rok później w Poznaniu, z tym, że sieć eduroam była już dostępna i używana przecz uczestników konferencji.

W niniejszym raporcie przedstawiamy założenia projektu eduroam i prace, które zostały wykonane w celu podłączenia sieci PIONIER do struktury europejskiej. Poza opisem spraw formalnych, zastosowanego oprogramowania i przygotowań do uruchomiania serwerów centralnych, załączono wskazówki pomagające skonfigurować serwery instytucji, zwracając uwagę na mniej oczywiste aspekty, zwłaszcza dotyczące bezpieczeństwa. Takie wskazówki powinny być w przyszłości rozwinięte do postaci pełnej instrukcji konfiguracyjnej.

Założenia organizacyjne eduroam

W pierwotnym zamierzeniu infrastruktura systemu eduroam zakładała trzy możliwe rozwiązania w celu realizacji zadania uwierzytelnienia i autoryzacji użytkowników:

1. użycie VPN (Virtual Private Network),
2. zastosowanie mechanizmu przekierowania WWW,
3. wykorzystanie protokołu 802.1x.

Dwa pierwsze podejścia opierają się na sieci dokującej, która z założenia jest niezabezpieczona – użytkownik domyślnie uzyskuje do niej dostęp i sieć ta służy następnie do realizacji uwierzytelnienia w macierzystej instytucji. Trzeci typ, uwierzytelnienie bazujące na protokole 802.1x wymaga stosowania szyfrowanych kanałów, opiera się na serwerach uwierzytelniania – Radius (*Remote Authentication Dial In User Service*, RFC 2865).

Analiza bezpieczeństwa dostępu do sieci spowodowała, że rozwiązanie 2 jest obecnie uważane za niepożądane i po pewnym czasie zostanie uznane jako niedopuszczalne. Rozwiązanie 1, jest złożone organizacyjnie i nie zostało wdrożone na skalę europejską i ostatecznie zarzucone. Wariant 3, oparty na uwierzytelnianiu 802.1x jest obecnie dominujący i uważany za jedyny, który będzie rozwijany.

Równolegle do rozwiązań technicznych tworzona jest konfederacyjna struktura zaufania. Podstawowymi elementami tej struktury są krajowe, akademickie sieci komputerowe (NREN) łączone przez punkt centralny, którym jest TERENA. Sieci krajowe nawiązują bezpośredni kontakt z instytucjami akademickimi w swoim kraju i stanowią gwarancję ich odpowiedzialności względem innych instytucji skonfederowanych w eduroam.

Zgodnie z przyjętym nazewnictwem, struktury krajowe są federacjami, a struktura europejska - konfederacją. Z uwagi na rosnąca popularność eduroam, zakłada się możliwość istnienia wielu konfederacji, które będą nawiązywały stosunki partnerskie.

Implementacja formalnej struktury zaufania jest obecnie realizowana poprzez hierarchiczny system serwerów Radius i identyfikatorów użytkowników. Identyfikator użytkownika musi być zgodny z RFC 2486 (Network Identifier Specification), a zatem postaci id@realm, gdzie realm jest nazwą domenową. Uwierzytelnienie użytkownika eduroam jest realizowane poprzez jego serwer macierzysty, wyszukiwany na podstawie realm. Ścieżka do serwera macierzystego jest budowana od serwera instytucji udostępniającej sieć, poprzez serwer krajowy, serwer centralny, kolejny serwer krajowy, do serwera instytucji macierzystej, zgodnie z mechanizmami radius-proxy (opisanymi w RFC 2865). Pierwszym krokiem we wdrożeniu eduroam w Polsce musiało zatem być uruchomienie serwera krajowego, a następnie krajowego serwera zapasowego.

Dalszy rozwój eduroam

Początkowo głównym motorem rozwoju sieci była działalność grupy TF-Mobility. Obecnie nacisk jest przeniesiony na projekt JRA5, w ramach GEANT2. W ramach JRA5 prace skupiają się na przebudowaniu projektu pilotowego, jakim obecnie jest eduroam, w oficjalną usługę. Jednocześnie coraz bardziej zauważalne staję się to, że na bazie struktury zaufania stworzonej w eduroam oraz środków technicznych, jakimi są serwery Radius, można budować usługi inne, niż tylko gościnny dostęp do sieci. Z rozszerzania się eduroam wynikają też nowe wyzwania, na przykład różnice legislacyjne w różnych krajach mogą wymuszać przesyłanie dodatkowych informacji o użytkowniku (np. wieku, a przynajmniej potwierdzenie przekroczenia pewnej granicy wieku). Oznacza to, że proste początkowe założenie, że fakt uwierzytelnienia jest tożsamy z przyznaniem praw dostępu, będzie musiało ulec modyfikacji.

Polityka bezpieczeństwa

Podstawowymi dokumentami eduroam są polityki bezpieczeństwa – europejska i krajowe. Zaawansowanie prac nad ich tworzeniem jest bardzo różne. Polityka europejska jest jednym z zadań projektu JRA5. Polityki krajowe są zazwyczaj tworzone indywidualnie, chociaż widoczna jest współpraca sieci krajowych, w celu możliwie maksymalnego ich ujednorodnienia.

Podstawowe różnice w podejściu do polityki bezpieczeństwa można podzielić na następujące grupy:

1. określenie instytucji uprawnionych do korzystania z eduroam – zasadniczo przyjmowano, że eduroam jest projektem dla szkolnictwa wyższego i świata nauki, w niektórych sieciach pojawiają się jednak głosy, że to ograniczenie jest zbyt restrykcyjne, inne z kolei stoją bardzo wyraźnie przy wyjściowym stanowisku, ostatecznie decyzje w sprawie zakresu eduroam będą prawdopodobnie w gestii sieci krajowych;
2. informacje o przebiegu sesji użytkownika – w tym zakresie widoczne są dwa stanowiska:
   a) informacja rozliczeniowa jest wyłącznie sprawą instytucji udostępniającej sieć i wysyłanie jej dalej naruszałoby prywatność użytkownika,
   b) informacja rozliczeniowa jest użyteczna, a nawet niezbędna do poprawnego administrowania użytkownikami, więc powinna być wysyłana do instytucjami macierzystej;
3. sposób dostępu do sieci
   a) dopuszczalność uwierzytelniania przez WWW,

b) rodzaj stosowanych metod uwierzytelniania 802.1x i szyfrów w sieci bezprzewodowej,
c) używane SSID.

Analiza zasadności wdrażania sieci bezprzewodowych opartych o standard 802.1x

Dynamiczny rozwój technologii bezprzewodowej, opartej o standardy 802.11 był nacechowany wszystkimi wadami zachłyśnięcia się nowym rozwiązaniem, bez analizy potencjalnych zagrożeń. Tworzenie sieci bezprzewodowych stało się powszechne. Bardzo często takie sieci nie były w żaden sposób zabezpieczane.

Sieci otwarte

Do dzisiaj normalnym zjawiskiem są sieci otwarte, do których podłączyć może się każdy, całkowicie anonimowo. Niezależnie od potencjalnych szkód polegających na nadużywaniu łączności sieciowej przez nieuprawnione osoby, jako coraz większy problem postrzegana jest kwestia odpowiedzialności za naruszające prawo działania użytkowników sieci. Żywiołowe uruchamianie punktów dostępowych, często bez uzgodnienia z administratorami sieci, stało się bardzo istotnym zagrożeniem bezpieczeństwa wewnętrznych sieci instytucji. Korzystanie z sieci bezprzewodowej jest nadzwyczaj wygodne, ale medium transmisyjne jest łatwe do podsłuchu i przejęcia. Wraz z rozwojem oprogramowania obsługującego sieci bezprzewodowe, pojawiło się nowe zagrożenie polegające na uruchamianiu fałszywych punktów dostępowych. Użytkownik tradycyjnej sieci bezprzewodowej nie ma żadnej metody na stwierdzenie, czy łączy się z „legalnym" punktem dostępu. W efekcie jest narażony na to, że jego transmisja będzie przechwytywana, strony, z którymi się łączy mogą okazać się fałszywe itp.

WEP

Pierwszym krokiem w kierunku podniesienia bezpieczeństwa sieci było wprowadzenie WEP (wired equivalent privacy). Rozwiązanie polegało na użyciu symetrycznego klucza szyfrującego transmisję. Klucz nie tylko zabezpieczał transmisję, ale i stanowił element ograniczający dostęp do sieci. Takie rozwiązanie było całkowicie nieprzydatne we większych sieciach, z uwagi na konieczność powszechnej dystrybucji i jednoczesnej jego ochrony przed niepowołanymi. Na dodatek, w implementacji WEP odkryto lukę, pozwalającą na zdeszyfrowanie klucza po przechwyceniu pewnej porcji ruchu, co całkowicie zdyskredytowało tę metodę zabezpieczeń.

Portale dostępowe

Instytucje, których zadaniem było obsługiwanie dużej liczby użytkowników sieci bezprzewodowej, zaczęły stosować metodę portalu dostępowego. W tym rozwiązaniu, korzysta się z sieci niezabezpieczonej i uzyskuje dostęp do strony logowania się. Na stronie logowania użytkownik wprowadza swoje dane, które są weryfikowane i na tej podstawie otwierany jest dostęp do sieci. Takie podejście zakłada, że użytkownik jest świadomy, że jego transmisja jest łatwa do przechwycenia, a zatem musi stosować zabezpieczenia w wyższych warstwach sieciowych. Stosowanie portali dostępowych można uznać za stosunkowo bezpieczne, jeżeli użytkownik jest obsługiwany przez jedną, znaną sobie firmę i ma możliwość zweryfikowania poprawności certyfikatu zabezpieczającego stronę. W praktyce, to

bezpieczeństwo jest jedynie pozorne – użytkownicy nie zwracają uwagi na poprawność certyfikatów, nawet jeżeli przeglądarka wysyła ostrzeżenie; ponadto przedstawienie użytkownikowi ekranu powitalnego z poprawnym (chociaż innym niż zwykle) certyfikatem, spowoduje, że z całą pewnością nie zauważy takiej podmiany i wprowadzi na taką stronę swoje dane uwierzytelniające. System WWW nie posiada skutecznych metod na blokowanie dostępu do stron podpisanych nieznanymi certyfikatami, gdyż takie ograniczenie uniemożliwiałoby de facto korzystanie z Internetu.

802.1x

Standard 802.1x i związane z nim standardy Radius i EAP, zostały stworzone na potrzeby modemowych sieci dostępowych, ale później zostały zaadaptowane na potrzeby sieci bezprzewodowych. Wprowadzenie 802.1x stanowi przełom w podejściu do bezpieczeństwa sieci dzięki następującym cechom:

1. przed uzyskaniem dostępu do sieci użytkownik jest uwierzytelniany,
2. sieć, z którą użytkownik się łączy, prezentuje mu certyfikat, dzięki czemu użytkownik może mieć absolutną pewność, że nie korzysta z fałszywego punktu dostępowego (przy prawidłowej implementacji i konfiguracji, użytkownik nigdy nie zaakceptuje fałszywego połączenia),
3. użytkownik automatycznie uzyskuje indywidualny klucz WEP, który może być wymieniany dostatecznie często, by uniemożliwić jego złamanie (przy bardziej zaawansowanych metodach, klucz jest wymieniany w każdym pakiecie),
4. istnieje możliwość rozdziału użytkowników na różne VLAN-y i w ten sposób określenia ich dodatkowych uprawnień lub ograniczeń.

Sieci stosujące uwierzytelnianie 802.1x stają się coraz bardziej powszechne i ewidentnie będą wypierały stosowanie portali dostępowych. Obecnie wszystkie punkty dostępowe i wszystkie karty bezprzewodowe posiadają podstawową implementację 802.1x pozwalającą na obsługę cech 1-3. Istnieje bezpłatne oprogramowanie serwera Radius pozwalające na obsługę wielu systemów uwierzytelniania użytkowników (LDAP, Active Directory, relacyjne bazy danych). Wdrożenie sieci opartej o 802.1x wymaga pewnego wysiłku organizacyjnego, ale może być uzyskane niemal bezkosztowo. Jedynym warunkiem jest posiadanie (lub utworzenie) bazy użytkowników sieci.

Dodatkowym argumentem za przyjęciem takiego rozwiązania może być łatwość obsługi kont dla gości poprzez projekt eduroam.

Implementacja eduroam w Polsce

Wdrażanie eduroam w Polsce rozpoczęło się od projektu złożonego jako wniosek LAN UMK, w roku 1993 oraz od współpracy między UMK i KPSI, w ramach której KPSI przekazała UMK do prac rozwojowo-badawczych sprzęt sieciowy i urządzenia łączności bezprzewodowej. Po uzgodnieniach między UMK i PCSS, na UMK uruchomiono krajowy serwer Radius i rozpoczęto prace testowe.

Zarejestrowano domenę eduroam.pl i uruchomiono krajowy serwis informacyjny www.eduroam.pl.

W czerwcu 2005 działały już dwa polskie serwery krajowe – na UMK i w PCSS, które zapewniły między innymi łączność eduroam w czasie konferencji TERENA 2005. Była to pierwsza konferencja sieciowa TERENY, na której taka sieć była powszechnie dostępna.

Obecnie trwają prace nad przygotowaniem założeń polskiej polityki bezpieczeństwa. Ważne są również działania marketingowe zmierzające do upowszechnienia eduroam w Polsce.

Standard Radius w polskim projekcie eduroam, wybór oprogramowania

Istnieje wiele implementacji standardu Radius. W projekcie eduroam najczęściej są stosowany pakiet Radiator (http://www.digitalpoint.com/products/radiator, komercyjny) oraz bezpłatne oprogramowanie FreeRADIUS (www.freeradius.org). Częścią Microsoft Windows 2000 (i 2003) Server jest serwer radius, pod nazwą Internet Authentication Service. Inne produkty warte wspomnienia to Steel-Belted Radius z Funk Sofrware - http://www.funk.com/radius/default.asp, czy Radius produkcji Lucent Technologies (stosowany m.in. w eduroam w Chorwacji).

W polskim projekcie eduroam, w roli serwerów krajowych jest używane bezpłatne oprogramowanie FreeRADIUS. Podczas prac wstępnych zainstalowano wersję 0.9.3. Oprogramowanie to szybko rozwija się, od września 2005 jest dostępna (i zainstalowana na polskich serwerach) wersja 1.0.5. W fazie rozpoznawania możliwości innych pakietów została zainstalowana próbna, 30 dniowa wersja oprogramowania Radiator. Z powodu trudności w konfiguracji nie starczyło czasu na dokładne przetestowanie produktu.

Oprogramowanie FreeRADIUS pozwala na korzystanie z różnych metod uwierzytelniania. Przyjęto, że w polskim projekcie eduroam będzie możliwy dobór techniki uwierzytelniania na podstawie lokalnej infrastruktury. Zalecane, przetestowane podczas dotychczasowych prac, metody to EAP-TLS, EAP-TTLS, EAP-PEAP.

Organizacja sieci serwerów Radius w polskim projekcie

W celu współpracy z projektem eduroam niezbędne było uruchomienie serwera poziomu krajowego. Taki serwer pracuje od lipca 2004 (radius1.eduroam.pl) w Uczelnianym Centrum Informatycznym UMK, w Toruniu. Serwer krajowy powinien być redundantny, dlatego uruchomiono zastępczy serwer radius2.eduroam.pl, który najpierw działał w sieci UCI UMK, następnie, w kwietniu 2005 został uruchomiony w PCSS, Poznań.

Serwer krajowy pełni wyłącznie funkcję proxy – przyjmuje zlecenia, analizuje domenę użytkownika i na jej podstawie przekazuje zlecenie do właściwego serwera obsługującego daną domenę lub do serwera poziomu głównego. Serwery poziomu głównego (serwery poziomu 1) – European Top Level Radius Servers stanowią korzeń drzewa, obecnie dostępne są dwa serwery:

- etlr1.eduroam.org (prowadzony przez SURFnet, Holandia),
- etlr2.eduroam.org (prowadzony przez UNI-C, Denmark).

Serwer krajowy odrzuca zlecenie w przypadku, gdy domena użytkownika znajduje się w drzewie .pl, ale nie jest dla niej zdefiniowany serwer Radius. Serwery krajowe pełnią funkcję serwerów poziomu 2.

Podstawowym elementem konfiguracji serwera krajowego jest utrzymanie pliku proxy.conf definiującego domeny podlegające technice proxy oraz klucze stosowane do komunikacji pomiędzy serwerami docelowymi. W tym pliku są wpisane wszystkie serwery poziomu jednostek organizacyjnych biorące udział w projekcie eduroam w Polsce.

Serwery krajowe, jeśli pełnią, tak jak w polskim projekcie, wyłącznie funkcję proxy i nie są punktem końcowym protokołu nadrzędnego EAP nie wymagają konfiguracji TLS-a.

Kolejny poziom w hierarchii stanowią serwery poziomu 3, tj. serwery instytucji, np. serwer UMK, serwer PCSS, czy serwer Politechniki Śląskiej. Zazwyczaj to te serwery są wskazywane w konfiguracji punktów dostępowych jako serwery Radius. Serwery instytucji mogą współpracować z serwerami poziomu 4 czy 5, będącymi serwerami jednostek instytucji (np. serwer uczelni może przekazywać zlecenia serwerowi wydziałowemu). Możliwe jest

również rozwiązanie, w którym lokalne punkty dostępowe współpracują z serwerem wydziałowym, a ten w razie potrzeby przekazuje zlecenia serwerowi uniwersyteckiemu itd.

Serwery poziomu powyżej 2 realizują właściwe uwierzytelnienie i ich konfiguracja jest najbardziej skomplikowana. W zależności od preferowanej w danym środowisku metody uwierzytelniania można odpowiednio dostosować sposób działania serwera. Serwery poziomu powyżej 2 wymagają zabezpieczeń, muszą przesyłać dane w ramach szyfrowanych połączeń, korzystają z infrastruktur PKI rodzimych instytucji. Podstawowe funkcje serwerów realizujących zadania autoryzacji i uwierzytelniania są definiowane w ramach sekcji autoryzacji (authorize) oraz sekcji uwierzytelniania (authentication) w pliku radiusd.conf.

Konfigurowanie serwerów poziomu 2

Autoryzacja i uwierzytelnienie

W oprogramowaniu FreeRadius przyjęto niestandardowe podejście do kolejności dokonywania uwierzytelnienia i autoryzacji. W procesie autoryzacji następuje pobranie informacji o użytkowniku w celu sprawdzenia, czy ma on uprawnienia do uwierzytelnienia. Na tym etapie jest również podejmowana decyzja o metodzie uwierzytelnienia (dzięki temu podejściu można np. wykluczyć stosowanie niektórych metod uwierzytelniania w odniesieniu do określonych użytkowników). Uwierzytelnienie to porównanie danych uwierzytelniania podanych przez użytkownika z przechowywanymi w bazie danych i dostępnymi serwerowi Radius.

Przykładowe techniki uwierzytelniania to :

- PAP – klient przekazuje w szyfrowanym tunelu TLS dane uwierzytelniania (nazwa użytkownika i hasło), wspiera wiele typów szyfrowania: clear, crypt, md5, sha1,
- MS-CHAP, MS-CHAPv2 – klient i serwer generują *challenge*, klient przesyła dane do serwera, serwer weryfikuje poprawność danych,
- TLS – pozwala na obustronne uwierzytelnianie klienta i serwera, negocjację sposobu szyfrowania oraz wymianę wspólnego klucza.

Nadrzędnym protokołem wspierającym różne metody uwierzytelniania jest EAP (Extensible Authentication Protocol), działający w warstwie łącza danych (warstwa 2). Wymienione wcześniej rozszerzenia EAP-TLS, EAP-TTLS, EAP-PEAP implementują konkretne techniki uwierzytelniania, i tak:

- EAP-TLS dotyczy uwierzytelniania w oparciu o mechanizm certyfikatów,
- EAP-TTLS służy do szyfrowanego tunelowania danych uwierzytelniania,
- PEAP (Protected EAP) podobnie jak EAP-TTLS umożliwia bezpieczny transport danych uwierzytelniania, jest protokołem zdefiniowanym przez Microsoft, CISCO i RSA Security.

EAP-TLS wymaga zastosowania infrastruktury kluczy publicznych (X.509) – zazwyczaj w instytucjach akademickich takie infrastruktury już istnieją, ale ich rola jest na ogół ograniczona do wystawiania certyfikatów dla serwerów i usług. W tym przypadku należy zbudować mechanizmy generowania danych uwierzytelniania X.509 dla użytkowników sieci oraz bezpiecznej ich dystrybucji. EAP-TTLS pozawala na wykorzystanie istniejącej infrastruktury kont użytkowników. Wadą tego rozwiązania jest konieczność instalowania dodatkowego oprogramowania klienckiego, gdyż system Windows nie wspiera tej metody EAP (istnieje darmowe oprogramowanie SecureW2, które dokłada tę brakującą metodę). W procesach autoryzacji i uwierzytelniania realizowana jest współpraca z bazą użytkowników. Jeśli korzystamy z bazy LDAP to pożyteczne jest rozszerzenie schematu do opisu użytkownika – zaleca sią korzystanie z klasy radiusProfile oraz jej atrybutów, np.

dialupAccess i radiusGroupName. Można przyjąć zasadę, że o dopuszczeniu do fazy uwierzytelniania decyduje obecność atrybutu dialupaccess we wpisie użytkownika (sprawdzenie obecności tego atrybutu następuje na etapie autoryzacji). Z kolei w oparciu o atrybut radiusGroupName, po pozytywnym uwierzytelnieniu, może zostać zrealizowane przypisanie odpowiedniego numeru VLAN.

Ważnym aspektem niezawodnościowym jest stosowanie zastępczych serwerów. Po pierwsze większość punktów dostępowych umożliwia określenie drugiego serwera Radius, używanego w przypadku braku dostępu do pierwszego. Dlatego zaleca się dublowanie serwerów Radius, można to połączyć z optymalizacją lokalizacji serwerów – przykładowo mamy dwa uczelniane serwery Radius zlokalizowane w różnych kampusach uczelni. W zależności od lokalizacji punktu dostępowego jako pierwszy wskazujemy bliższy serwer Radius. Jak wcześniej wspomniano, również sposób definiowania proxy pozwala na określenie drugiego (fail-over) serwera Radius. Podobnie w przypadku wskazania bazy LDAP (czy innego źródła danych uwierzytelniania i autoryzacji) można wprowadzić mechanizm dodatkowego zabezpieczenia, poprzez definicję bloku redundant, w którym wymieniamy kolejne, wcześniej zdefiniowane źródła danych o użytkownikach. Dyrektywy takiego bloku są realizowane sekwencyjnie, jeśli pierwszy moduł jest dostępny, kolejne są pomijane, jeśli nie jest dostępny, próbowany jest kolejny itd.

Dynamiczne przypisywanie użytkownikom numeru VLAN

W zależności od lokalnej konfiguracji sieci komputerowej może być niezbędne dynamiczne powiązanie pozytywnie uwierzytelnionego użytkownika z odpowiednim numerem VLAN, który następnie zadecyduje o przydzielonym adresie IP. Służą do tego odpowiednie atrybuty Radius (RFC2868) oraz możliwość, pobierania wartości atrybutów z bazy użytkowników lub ustawiania ich wartości przy spełnieniu określonych warunków. Jedną z metod jest pobranie atrybutu radiusTunnelPrivateGroupId, radiusTunelMediumType, radiusTunnelType z wpisu użytkownika w bazie. Jeśli jakiś z tych atrybutów ma przypisaną wartość we wpisie użytkownika i w pliku zdefiniowanym jako dictionary_mapping dla danego modułu ldap istnieje przemapowanie atrybutu LDAP nazwę atrybutu Radius (jako replyItem), to wartość atrybutu Radius jest wysyłana w odpowiedzi. Bardziej popularną metodą jest podział użytkowników na grupy i przydzielanie numeru VLAN na podstawie przynależności do grupy lub przydzielanie numeru VLAN na podstawie domeny logowania użytkownika. Przykładowo: pracownicy są umieszczani w VLAN-ie 40, studenci w 41, a goście w 42. Do przypisania tych numerów służą dyrektywy w pliku users, np. wiersze:

```
DEFAULT Realm == pracownicy
        Tunnel-Medium-Type = 6,
        Tunnel-Private-Group-Id := 40,
        Tunnel-Type = VLAN
```

oznaczają, że gdy nazwa użytkownika jest dowolna (DEFAULT), a domena logowania to pracownicy, to: (1) jest dodawany atrybut Tunnel-Medium-Type o wartości 6, (2) jeśli istnieje w odpowiedzi atrybut Tunnel-Private-Group-Id, to jego wartość zostanie zastąpiona wartością 6, w przeciwnym razie jest dodawany atrybut Tunnel-Private-Group-Id o wartości 6, (3) jest dodawany atrybut Tunnel-Type o wartości VLAN.

Poniższe rozwiązanie bazuje na grupie użytkownika pobranej z bazy:

```
DEFAULT ldap1-Ldap-Group == "staff"
        Tunnel-Medium-Type = 6,
        Tunnel-Private-Group-Id := 40,
        Tunnel-Type = VLAN
```

W tym przypadku sprawdzanym elementem nie jest domena logowania, lecz grupa LDAP (ldap1 jest zdefiniowany w radiusd.conf jako jeden z modułów ldap). W przypadku dopasowania grupy, ustawienia atrybutów są realizowane analogicznie.

Jeśli dodatkowo decyzja o przydzielonym numerze VLAN ma być uzależniona od miejsca dostępu, wówczas warto skorzystać z możliwości definiowania grup urządzeń w pliku huntgroups, np.

```
budyneka    NAS-IP-Address == 192.168.2.5
budyneka    NAS-IP-Address == 192.168.2.6
budyneka    NAS-IP-Address == 192.168.2.7
```

i na liście sprawdzanych elementów (w pliku users) dodać kontrolę atrybutu Huntgroup-Name, np.:

```
DEFAULT ldap1-Ldap-Group == "staff",  Huntgroup-Name == “budyneka”
        Tunnel-Medium-Type = 6,
        Tunnel-Private-Group-Id := 44,
        Tunnel-Type = VLAN
```

Zmiana danych w pakietach Radius

Moduł rlm_attr_rewrite w oprogramowaniu FreeRADIUS daje możliwość dynamicznej zmiany danych w pakietach Radius. Jest to przede wszystkim użyteczne w fazie autoryzacji, uwierzytelniania i rozliczania (accounting). Przykładowym zastosowaniem może być zamiana User-Name, czy zmiana formatu wartości atrybutu Calling-Station-Id. Moduł ten przejął większość funkcjonalności modułu rlm_attr_filter (który jest nadal dostępny, lecz traktowany jako „zarzucony”), służącego do filtrowania atrybutów i wartości w pakietach Radius. Moduł rlm_attr_filter jest jednak nadal przydatny w celu filtrowania atrybutów w przypadku, gdy użytkownik loguje się używając domeny spoza rodzimej instytucji. W tej sytuacji po otrzymaniu zwrotnej odpowiedzi, serwer powinien wyciąć wszystkie atrybuty związane z ustawieniem VLAN-u, a następnie ustawić je tak, jak jest to potrzebne w danej instytucji.

Moduł rlm_attr_filter standardowo działa następująco: jeśli jest włączone użycie attr_filter, to dla każdej obsługiwanej domeny należy zdefiniowanać zestaw dyrektyw filtrowania – można to zrealizować np. określając postępowanie w przypadku domeny realm_a, a poniżej podać domyślne zasady (DEFAULT). Trudnością w takim rozwiązaniu jest konieczność panowania nad typem transmitowanych atrybutów. W trakcie prac wdrożeniowych dokonano modyfikacji źródła tego modułu, by odwrócić zasadę – domyślnie przepisywane są wszystkie atrybuty, natomiast te, które występują na liście są zamieniane, kasowane lub dodawane. Po tej zmianie plik attrs definiujący zasady filtrowania może przyjąć następującą postać:

```
####
realm_a
        Tunnel-Private-Group-Id := 42,
        Tunnel-Type := VLAN,
        Tunnel-Medium-Type := 6,
        Tunnel-Private-Group-Id !* ANY,
        Tunnel-Type !* ANY,
        Tunnel-Medium-Type !* ANY
DEFAULT
####
```

W efekcie każdemu użytkownikowi przypisanemu do domeny “realm_a” zostanie przydzielony VLAN 42.

Określenie kosztów i korzyści przystąpienia do projektu eduroam

Zgodnie z powyższą analizą, koszty wdrożenia sieci opartej o standard 802.1x są praktycznie identyczne jak koszty stworzenia jakiejkolwiek sieci bezprzewodowej, dając jednocześnie wymierne korzyści dodatkowe. Te fakty powinny przesądzać o zastosowaniu takiego rozwiązania, niezależnie od decyzji o przystąpienia do eduroam.

Przystępując do eduroam instytucja bierze na siebie zobowiązanie polegające głównie na zbieraniu odpowiednich logów systemowych i współpracy w przypadkach ewentualnych incydentów sieciowych w udziałem użytkowników z danej instytucji. W zamian za to, użytkownicy uzyskują dostęp do sieci we wszystkich instytucjach biorących udział w eduroam.