# Europejski projekt *eduroam* jako szansa na usprawnienie dostępu do Internetu

*raport dla Miedzyuniwersyteckiego Centrum Informatyzacji*
Tomasz Wolniewicz
Uczelniane Centrum Informatyczne UMK

## *Wstęp*

Celem niniejszego raportu jest podkreślenie celowości budowania sieci bezprzewodowych w oparciu o założenia projektu ***eduroam***. Skorzystanie z doświadczeń tego projektu pozwoli na stworzenie sieci bezpiecznych, wygodnych i skalowanych. Przy okazji można uruchomić mechanizmy zapewniające naszym użytkownikom dostęp do Internetu w wielu uczelniach na świecie. Raport bazuje na doświadczeniach pozyskanych przy wdrażaniu ***eduroam*** w skali krajowej i uczelnianej (na UMK w Toruniu).

## *Uczelniane sieci bezprzewodowe*

Potrzeba wdrażania sieci bezprzewodowych na uczelniach nie wymaga obecnie większego uzasadnienia. Jednym z najważniejszych argumentów jest rola Internetu w procesie nauczania. Studenci coraz częściej kupują komputery przenośne i przychodzą z nimi na uczelnię, w szczególności do biblioteki. Możliwość podłączenia do Internetu własnego komputera jest ogromnym ułatwieniem i jednocześnie zmniejsza nacisk na uczelnię, aby utrzymywała dużą liczbę powszechnie dostępnych stanowisk komputerowych.

### Powody stosowania zabezpieczeń sieci bezprzewodowych

Sieć uczelniana musi służyć dużej grupie uprawnionych osób. Niewątpliwie najprostszym rozwiązaniem zapewniającym dostęp im wszystkim jest stworzenie sieci całkowicie otwartej. Takie sieci były od dawna budowane na wielu uniwersytetach amerykańskich i nadal można się tam z nimi spotkać. Wydaje się jednak, że tendencja w kierunku zabezpieczenia przed niepowołanym dostępem do sieci jest coraz silniejsza. Tam gdzie sieci otwarte już działają, równolegle wprowadza się sieci zabezpieczone, najprawdopodobniej z myślą o tym, by docelowo przejść w całości na rozwiązanie bezpieczne. Jest kilka powodów, które przemawiają za stosowaniem ograniczeń dostępu:

1. ochrona uczelni przed zarzutami o dokonywanie przestępstw i wykroczeń za pośrednictwem jej sieci (spamy, włamania na komputery, dostęp do treści zakazanych, przestępczość komputerowa),
2. ochrona sieci uczelni przed złośliwymi zachowaniami użytkowników (masowe pobieranie adresów internetowych prowadzące do wyczerpania całej dostępnej puli, uruchamianie programów generujących nadmierny ruch w sieci),
3. udostępnianie w sieci aplikacji przeznaczonych dla ograniczonej grupy użytkowników (np. czasopisma elektroniczne chronione tylko adresami IP),
4. ochrona przed nadużywaniem dostępu do Internetu (przepustowości nowoczesnych sieci bezprzewodowych są już tak duże, że za pośrednictwem kilku punktów dostępowych można z łatwością wygenerować ruch liczony w setkach megabitów na sekundę)

Oddzielnym zagadnieniem jest ochrona treści przesyłanych przez sieć bezprzewodową. Sama sieć jest z natury bardzo łatwa do podsłuchania, nawet z bardzo dużych odległości. Można przyjąć podejście, że użytkownik powinien działać w sposób świadomy i nie polegać na tym, że sieć jest chroniona. Nie wszystko jednak można prosto zabezpieczać, użytkownik zazwyczaj nie chce by wszyscy znali adresy stron WWW, z którymi się łączy. Jeżeli sama sieć nie jest dostateczne dobrze zabezpieczona, to użytkownik może być zmuszony do stosowania mechanizmów typu wirtualna siec prywatna (VPN).

Typowe mechanizmy kontroli dostępu stosowane w sieciach bezprzewodowych

1. dostęp na podstawie adresu MAC („sprzętowego” adresu karty)
   a) niepraktyczny na szeroką skalę z powodu trudności w administrowaniu;
   b) nadzwyczaj łatwy do przełamania (adresy uprawnionych kart są „widoczne” dla każdego);

2. dostęp na podstawie znajomości klucza WEP lub WPA-PSK
   a) wymaga powszechnej dystrybucji klucza, który powinien być tajny – z tego powodu nie do zastosowania na szeroką skalę;
3. dostęp poprzez stronę WWW
   a) pozwala obsłużyć dużą grupę użytkowników;
   b) w środowiskach uczelnianych stosunkowo łatwo można uruchomić fałszywe stacje, które będą zbierały identyfikatory i hasła użytkowników (zabezpieczenie strony logowania podpisem uczelni jest zabezpieczeniem pozornym, ponieważ użytkownicy zazwyczaj ignorują komunikaty przeglądarek);
4. dostęp przez wirtualną sieć prywatną (VPN)
   a) podobny do logowania przez WWW, ale pozbawiony wad w postaci zagrożenia bezpieczeństwa danych uwierzytelniających;
   b) wymaga dystrybucji indywidualnych certyfikatów, których obecne zastosowanie będzie ograniczone do udostępniania sieci (wady takiego rozwiązania są opisane poniżej);
5. WPA+802.1x (tzw. WPA-Enterprise)
   a) standardowy (oparty o standardy IEEE 802.1x i 802.11i) system kontroli dostępu gwarantujący bezpieczeństwo danych identyfikacyjnych użytkownika, a jednocześnie bardzo dobrą ochronę całej transmisji;
   b) idealnie nadaje się do wdrożenia na dużą skalę;
   c) może uniemożliwiać zmianę adresu IP przez użytkownika i dzięki temu gwarantować identyfikowanie winnych ew. naruszeń prawa;
   d) ma dodatkowe funkcje, np. przydział użytkowników do wirtualnych podsieci (możliwość nadania innych uprawnień studentom, pracownikom, gościom itp.) lub zbieranie informacji o stopniu wykorzystania sieci przez poszczególnych użytkowników.

### Problem przydziału identyfikatorów i haseł

Przydzielanie kont wyłącznie na użytek dostępu do sieci bezprzewodowej jest uzasadnione w sytuacjach, kiedy korzystanie z łączności jest odpłatne. W takim przypadku użytkownicy nie udostępniają swojego konta osobom trzecim, a z całą pewnością nie dopuszczają, by ich dane stały się powszechnie znane. W przypadku obsługi studentów jedyną motywacją dla ochrony danych może być fakt, że za pomocą tych samych danych uzyskuje się dostęp do zasobów, które student chce chronić (poczta elektroniczna, konto w systemie obsługi studiów). Posiadanie jednego kompletu danych identyfikacyjnych do wszystkich usług na uczelni jest zgodne z coraz powszechniejszą praktyką systemów Single-Sign-On. Jeden komplet danych jest wygodniejszy, a w przypadku ujawnienia zdecydowanie łatwiejszy do zmiany. Stosowanie jednego kompletu danych nakłada jednak na uczelnię obowiązek, by przy budowaniu sieci bezprzewodowej stworzyła środowisko, w którym przejęcie tych danych będzie praktycznie niemożliwe. W chwili obecnej jedynym systemem, który może to zagwarantować jest WPA+802.1x.

## *Projekt eduroam*

***eduroam*** (www.eduroam.org) jest projektem zapoczątkowanym przez europejskie akademickie sieci komputerowe stowarzyszone w organizacji TERENA (www.terena.nl), a obecnie współpracującym również z sieciami pozaeuropejskimi (Australia, Tajwan, USA).

Wyjściowym założeniem ***eduroam*** było stworzenie systemu, w którym pracownicy i studenci uczelni mogliby uzyskiwać dostęp do sieci na terenie innych uczelni – bezpłatnie i powszechnie. System miał gwarantować zwolnienie uczelni z konieczności zakładania kont gościnnych dając jednocześnie pewność, że w przypadku problemów, możliwe będzie zlokalizowanie osoby odpowiedzialnej za konkretny incydent.

***eduroam*** opiera się na infrastrukturze zaufania, w której osoba starająca się o gościnny dostęp może skorzystać z tych samych danych uwierzytelniających, których używa w swojej macierzystej uczelni. Dane są przekazywane do serwera uczelni macierzystej, a przesłane stamtąd potwierdzenie tożsamości musi być traktowane jako wiążące. Docelowo system będzie się opierał o porozumienia zawierane między uczelniami a krajowym koordynatorem ***eduroam***, co ma gwarantować poprawność działania systemu reagowania na incydenty.

W ***eduroam*** rozważano początkowo trzy sposoby uwierzytelnienia: logowanie przez WWW, VPN oraz 802.1x. Po przeanalizowaniu aspektów bezpieczeństwa oraz złożoności implementacji uznano, że ***eduroam*** ograniczy się do 802.1x.

Jeżeli zgodzić się prezentowaną wyżej tezą, że 802.1x jest najlepszym rozwiązaniem do budowy uczelnianej sieci bezprzewodowej, to włączenie się w strukturę ***eduroam*** nie nakłada na uczelnię praktycznie żadnych dodatkowych obciążeń.

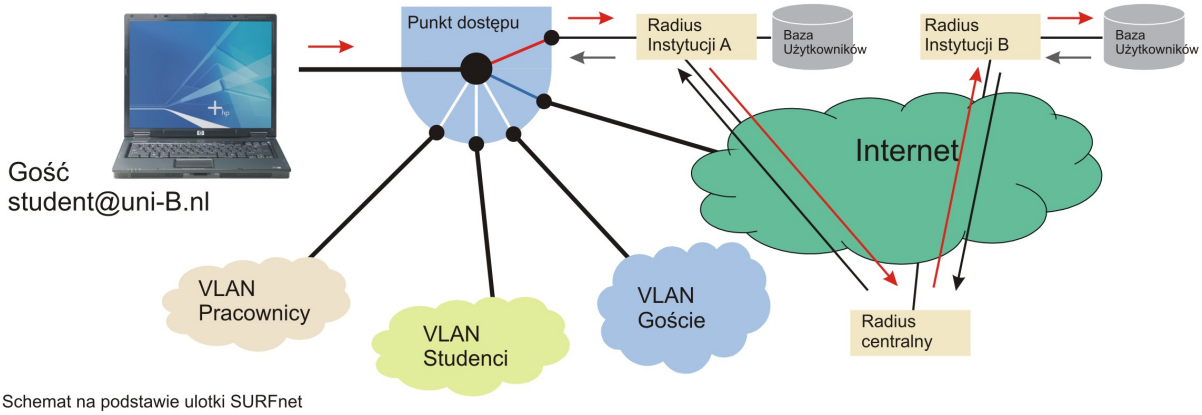
## 802.1x w *eduroam*

Standard IEEE 802.1x, w zastosowaniu do sieci bezprzewodowych umożliwia precyzyjną kontrolę dostępu do sieci. Radiowe urządzenie dostępowe (access-point – AP) sygnalizuje potencjalnym klientom, że oczekuje uwierzytelnienia. Klienckie oprogramowanie 802.1x, zainstalowane na komputerze użytkownika, za pośrednictwem AP, nawiązuje dialog z uwierzytelniającym serwerem Radius. Jeżeli dane uwierzytelniające użytkownika zostaną przez serwer zaakceptowane, to przesyła on do AP zgodę na otworzenie dostępu do sieci. W tym momencie komputer użytkownika może pobrać adres sieciowy i rozpocząć normalną pracę w sieci.

Opisany schemat należy rozszerzyć o kilka szczegółów:

1. do momentu zakończenia uwierzytelnienia komputer użytkownika może wysyłać tylko dane uwierzytelniające, wszelki inny ruch jest blokowany przez AP;
2. dane uwierzytelniające wymieniane są między komputerem użytkownika a serwerem Radius i wszelkie dane wrażliwe (np. hasło) są przesyłane w postaci zaszyfrowanej i są nie do odczytania nawet przez AP;
3. komputer użytkownika sprawdza certyfikat, którym przedstawia się serwer Radius, jeżeli użytkownik nie zna serwera, to nie wyśle żadnych danych wrażliwych (jest to zabezpieczenie przed fałszywymi sieciami bezprzewodowymi);
4. na zakończenie sesji uwierzytelniającej serwer Radius wysyła klucze szyfrujące do komputera użytkownika i do AP, te indywidualne klucze będą służyły do zabezpieczenia transmisji bezprzewodowej (istnienie tych indywidualnych kluczy ma jeszcze dwie istotne konsekwencje, po pierwsze użytkownik ma pewność, że łączy się z AP będącym częścią oficjalnej sieci, po drugie użytkownik nie może zmienić adresu sprzętowego karty sieciowej i zachować połączenia);
5. razem z decyzją o dopuszczeniu do sieci serwer Radius może przekazać informacje o tym do jakiej sieci wirtualnej należy przydzielić komputer użytkownika;
6. AP „ufa" tylko jednemu lub dwóm serwerom Radius, ale serwer Radius może przekazać zlecenie uwierzytelniające innemu serwerowi i wówczas pełni rolę przekaźnika, nie mając dostępu do danych wrażliwych, musi jednak ufać uzyskanej odpowiedzi uwierzytelniającej i przekazać ją do AP,
7. AP może regularnie wysyłać informacje o ruchu generowanym przez każdego z użytkowników, co zdecydowanie ułatwia wykrywanie problemów w sieci.

Opisana w punkcie 6. możliwość przekazywana zleceń uwierzytelnienia stała się podstawą stworzenia ***eduroam***. Każdy użytkownik przedstawia się nazwą skonstruowaną jak adres e-mail – **uzytkownik@nazwa.domenowa.kraj**. Na podstawie nazwy domenowej serwer Radius, do którego przekazano zlecenie, podejmuje decyzję, czy jest właściwy dla jego obsłużenia, czy powinien przekazać je dalej. W drugim przypadku zlecenie jest przekazywane do serwera krajowego, który albo przesyła je do właściwej instytucji w kraju, albo do centralnego serwera ***eduroam***. Serwer centralny kieruje zlecenie do odpowiedniego serwera krajowego, a ten do odpowiedniej instytucji. Zlecenia uwierzytelniające trafiają w ten sposób do macierzystego serwera uwierzytelniającego danego użytkownika. Tożsamość serwera macierzystego jest potwierdzana odpowiednim certyfikatem, który powinien być zainstalowany na komputerze użytkownika. Z tego certyfikatu korzysta się również w celu stworzenia szyfrowanego kanału między komputerem użytkownika a serwerem uwierzytelniającym i tym kanałem przekazuje się wszelkie dane wrażliwe. Serwer Radius w instytucji udostępniającej sieć nie może wprawdzie ingerować w decyzję macierzystego serwera uwierzytelniającego, ale może przydzielić użytkownika do odpowiedniej sieci wirtualnej. Dzięki temu goście mogą być odseparowani od użytkowników lokalnych, a również na poziome lokalnym można oddzielać np. studentów od pracowników.




Schemat na podstawie ulotki SURFnet

Powyżej opisany proces nie działa prawidłowo w przypadku domen nie kończących się symbolem kraju, a ponadto drzewiasta struktura serwerów jest stosunkowo mało odporna na awarie; prowadzone są jednak prace nad rozwiązaniami, które usuną te wady.

Zastosowanie 802.1x wymaga urządzeń, które ten standard wspierają, ale obecnie dotyczy to już zdecydowanej większości sprzedawanego sprzętu. Przypisywanie użytkowników do odrębnych sieci wirtualnych jest na razie opcją nie występującą w tańszych urządzeniach, trzeba zatem podjąć decyzję, czy rozdział użytkowników jest niezbędny, ewentualnie stosować rozwiązania mieszane. Drugim wymogiem jest odpowiednie oprogramowanie po stronie użytkownika. Również w tym zakresie 802.1x jest już bardzo dobrze wspierane.

## Warunki przystąpienia do *eduroam*

Jeżeli uczelnia chce uruchomić nowoczesną sieć bezprzewodową, to albo skorzysta z jednego z nietypowych rozwiązań komercyjnych, albo użyje 802.1x. Ponieważ rozwiązania oparte o standardy na dłuższą metę zawsze sprawdzają się lepiej od zamkniętych, to decyzja o zastosowaniu 802.1x jest zupełnie naturalna. Uruchomienie systemu 802.1x wymaga zainstalowania uwierzytelniającego serwera Radius. Aby zapewnić kompatybilność z ***eduroam*** identyfikatory użytkowników powinny być budowane w postaci uzytkownik@nazwa.domenowa.kraj.

Uczelnia posiadająca sieć bezprzewodową opartą o standard 802.1x, w celu przystąpienia do ***eduroam*** musi:

- zaakceptować zasady działania ***eduroam*** (politykę krajową i europejską);
- uzgodnić dane uwierzytelniające dla swojego serwera Radius z krajowym administratorem ***eduroam*** i otworzyć odpowiednie porty komunikacyjne do kontaktu z serwerami krajowymi;
- skonfigurować swój serwer Radius tak, by przekazywał zlecenia o nieznanej części domenowej do serwera krajowego;
- jeżeli zachodzi taka potrzeba, skonfigurować sieci wirtualne, urządzenia bezprzewodowe i serwer Radius do obsługi dynamicznego przydziału do sieci wirtualnych.

Jeżeli uczelnia decyduje się na przystąpienie do ***eduroam***, to musi przyjąć zasadę, że na swoim terenie będzie do sieci bezprzewodowej dopuszczała gości związanych z innymi instytucjami biorącymi udział w ***eduroam***. W zamian, studenci i pracownicy tej uczelni będą mogli korzystać z sieci we wszystkich innych instytucjach partycypujących w ***eduroam***. Uczelnia powinna również przyjąć nazwę ***eduroam*** jako nazwę swojej sieci bezprzewodowej, ewentualnie wspierać tę nazwą jako dodatkową. Uczelnia powinna również uruchomić stronę informacyjną dla gości, a także zapewnić wsparcie techniczne dla własnych użytkowników. Nie oczekuje się, aby uczelnia udzielała jakiegokolwiek indywidualnego wsparcia technicznego gościom.

Uczelnia musi przechowywać informacje o osobach, które uwierzytelnia. W razie stwierdzenia, że osoba uwierzytelniona przez uczelnię dopuściła się wykroczenia w czasie korzystania z gościnnego dostępu do sieci w innej instytucji, uczelnia, we współpracy z administratorem krajowym, powinna być w stanie wskazać uprawnionym organom ścigania osobę, której dotyczyło dane uwierzytelnienie. Dane związane z uwierzytelnieniem należy uważać za dane osobowe i w związku z tym muszą podlegać odpowiedniej ochronie.

W przypadku odwrotnym, a zatem gdy do sieci uczelni dostęp uzyska gość korzystający z mechanizmów ***eduroam*** i następnie dopuści się wykroczenia, to uczelnia, korzystając z umowy z

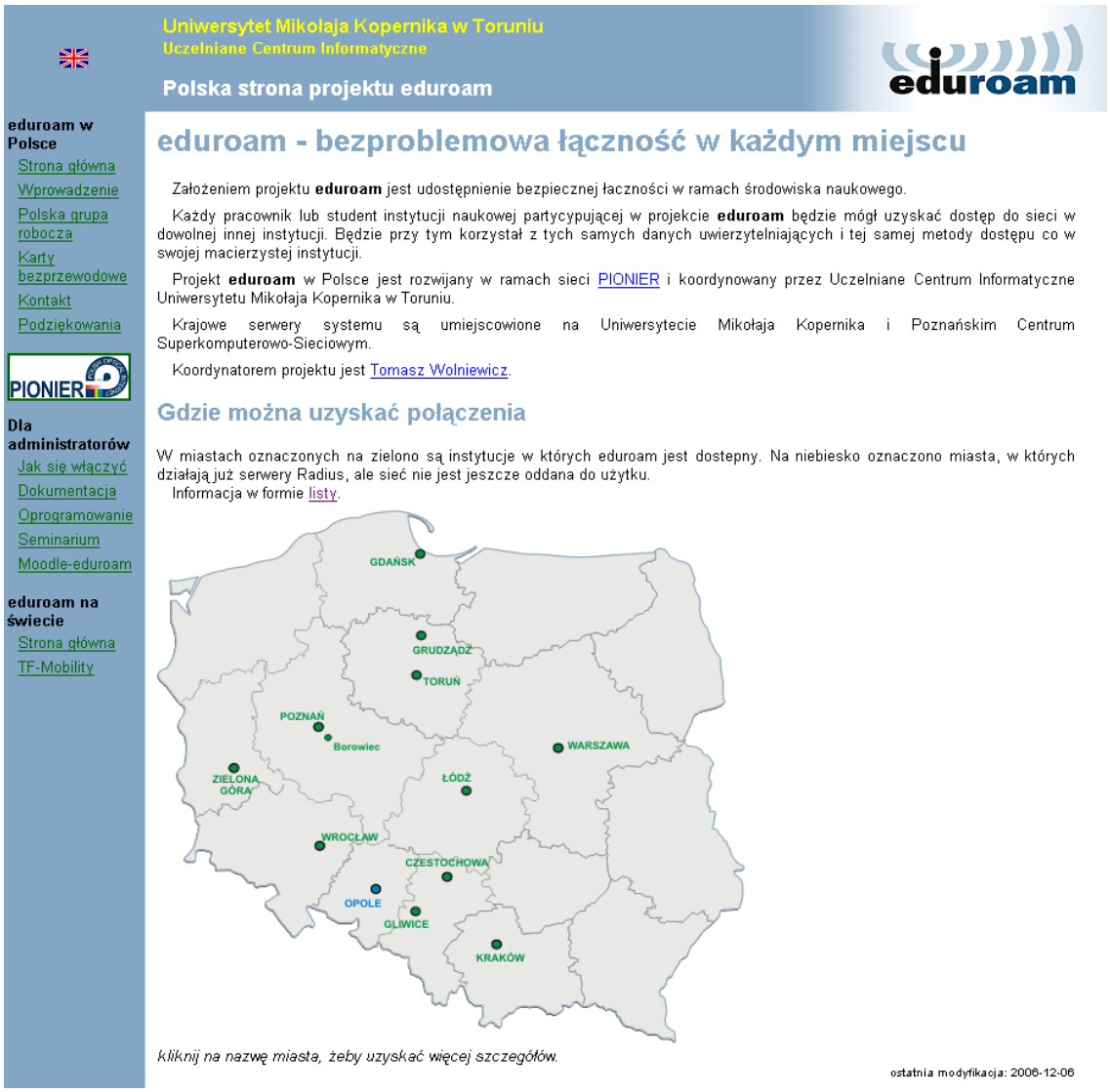
operatorem krajowym, będzie mogła przesunąć odpowiedzialność za ujawnienie danych gościa na jego instytucję macierzystą. Uczelnia musi jednak zadbać o zastosowanie odpowiednich mechanizmów ochrony sieci, tak by móc jednoznacznie związać konkretny adres internetowy z sesją uwierzytelnienia. W mniej poważnych przypadkach, tzn. kiedy użytkownik dopuszcza się działań niezgodnych z regulaminem sieci, z której korzysta, administrator tej sieci ma prawo zablokować dostęp wszystkim gościom przedstawiającym się daną nazwą domenową i przekazać sprawę do wyjaśnienia koordynatorowi krajowemu.

## Stan zaawansowania wdrożenia *eduroam* w Polsce

W Polsce ***eduroam*** jest rozwijany jako projekt komplementarny programu PIONIER. Obecnie projekt jest w nieznacznym stopniu finansowany ze środków na utrzymanie sieci PIONIER oraz ze środków UMK.

Zgodnie z założeniami, instytucją odpowiedzialną za umowy miedzy partnerami projektu będzie operator sieci PIONIER – PCSS. Uczelniane Centrum Informatyczne UMK koordynuje projekt, utrzymuje główny, krajowy serwer Radius i serwis WWW pod adresem http://www.eduroam.pl. Pracownicy UCI UMK pomagają we wdrożeniach, przede wszystkim w konfigurowaniu serwerów Radius. Zapasowy krajowy serwer Radius działa w PCSS w Poznaniu.

W marcu 2006 na UMK odbyło się seminarium sponsorowane przez HP Polska, poświęcone technicznym aspektom ***eduroam***. W seminarium wzięło udział ponad 60 osób z 17 miast. Reprezentowane było 13 polskich Uniwersytetów. Praktycznie wszyscy uczestnicy seminarium zadeklarowali wolę przystąpienia do ***eduroam*** i uruchomienia pierwszego etapu sieci w roku 2006.



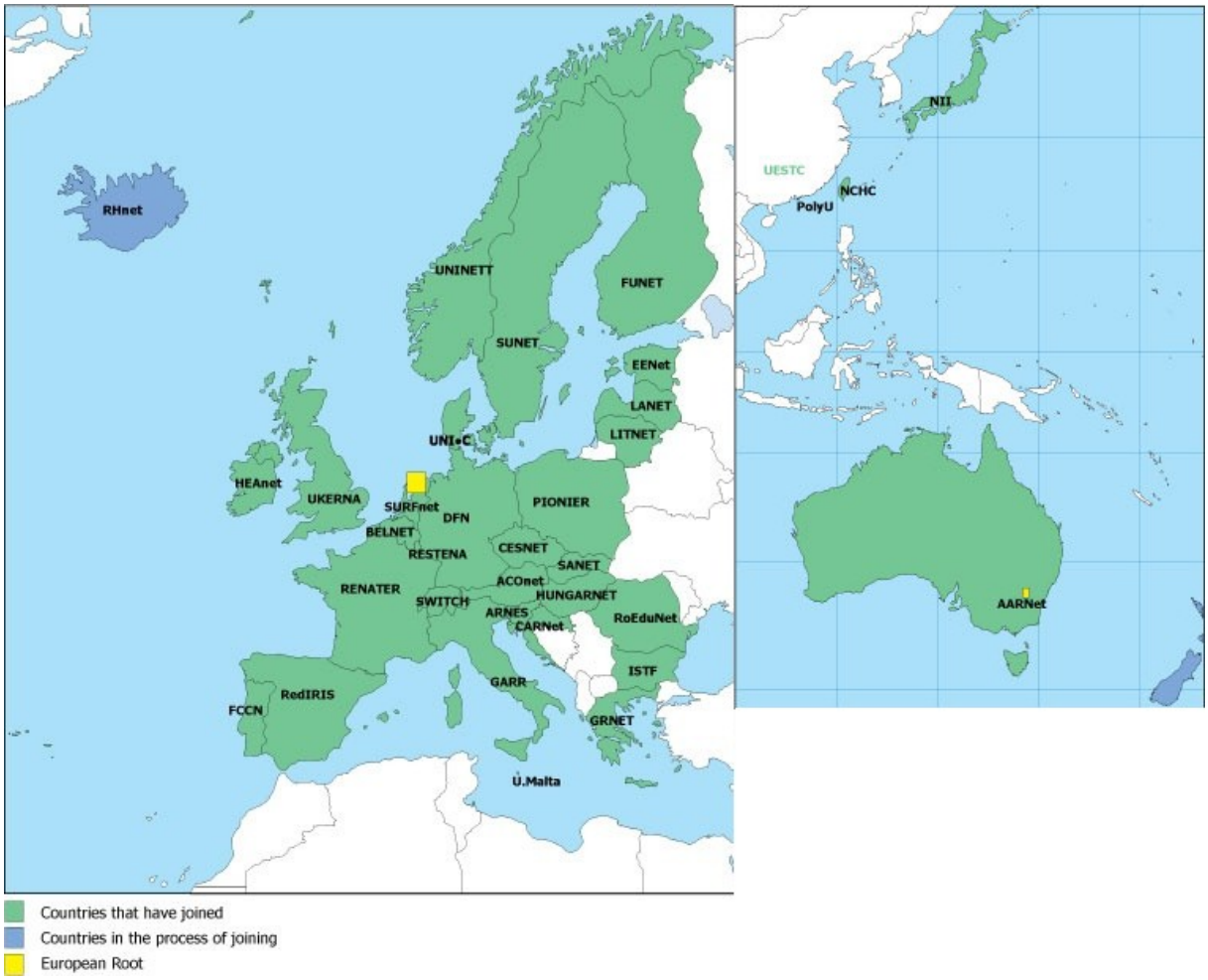

*Polska strona eduroam (www.eduroam.pl)*

Według stanu z 31 stycznia 2006 dostęp do ***eduroam*** został uruchomiony w następujących instytucjach:

1. Obserwatorium astronomiczne w Borowcu
2. Politechnika Częstochowska
3. Politechnika Gdańska
4. Politechnika Gliwicka
5. Politechnika Łódzka
6. Politechnika Krakowska
7. Politechnika Wrocławska (WCSS)
8. Poznańskie Centrum Superkomputerowo-Sieciowe
9. Uniwersytet Adama Mickiewicza
10. Uniwersytet Łódzki
11. Uniwersytet Mikołaja Kopernika (Toruń i Grudziądz)
12. Uniwersytet Warszawski
13. Uniwersytet Zielonogórski

Testowy serwer Radius podłączony do struktury ***eduroam*** działa też w Uniwersytecie Opolskim

## *eduroam* globalnie




*Mapa eduroam (źródło www.eduroam.org)*

Krajowe serwery ***eduroam*** są uruchomione w praktycznie wszystkich krajach Europy (patrz mapa), w Australii, Chinach, Japonii i na Tajwanie. W zależności od kraju, w ***eduroam*** bierze udział od kilku do kilkudziesięciu instytucji.

Nowe rozwiązania dla ***eduroam*** są przygotowywane w ramach podprojektu JRA5, projektu Geant 2. Techniczne działania w skali europejskiej są na razie koordynowane przez grupę roboczą TF-Mobility przy TERENA, a w skali ogólnoświatowej przez eduroam Global Working Group. W najbliższym czasie zarządzanie w skali europejskiej zostanie jednak sformalizowane.

W niektórych krajach Europy ***eduroam*** uzyskuje silne wsparcie formalne. Na przykład w Hiszpanii uruchomiono rządowy program wspierania rozwoju uczelnianych sieci bezprzewodowych; dofinansowanie jest jednak warunkowane deklaracją przystąpienia uczelni do ***eduroam***. Podobny program jest przygotowywany w Republice Czeskiej. Duże zainteresowanie projektem przejawiają też rządy Holandii i Danii.

## *Aspekty techniczne*

### Oprogramowanie

Jak wcześniej wspomniano, praktycznie wszystkie obecnie kupowane radiowe urządzenia dostępowe i wszystkie karty radiowe, mają wystarczające wsparcie standardu 802.1x, aby móc je włączyć w strukturę ***eduroam***.

Serwer uwierzytelniający nie wymaga dużej mocy obliczeniowej i może pracować jako jeden z procesów na typowym serwerze aplikacyjnym. Zalecanym oprogramowaniem jest FreeRadius – bezpłatne oprogramowanie udostępniane w wersji źródłowej. Konfiguracja serwera jest stosunkowo trudna, ale pracownicy UCI UMK służą pomocą. Na serwerze http://www.eduroam.pl dostępne są również przykładowe pliki konfiguracyjne. Serwer może współpracować z dowolną bazą użytkowników, np. LDAP, ActiveDirectory, MySQL, zwykłym plikiem tekstowym.

Uwierzytelnianie użytkowników może być realizowane na wiele sposobów.

- Obecnie najbardziej powszechne jest korzystanie z nazwy użytkownika i hasła, co wymaga jednak zainstalowania dodatkowego (bezpłatnego) modułu w systemie MS Windows. Instalacja tego modułu jest prosta, co zostało potwierdzone w UMK, gdzie studenci pobierają plik, wstępnie skonfigurowany pod potrzeby UMK i samodzielnie dokonują instalacji.
- Inna, powszechna metoda uwierzytelniana jest oparta o indywidualne certyfikaty. Ten system jest na UMK stosowany w odniesieniu do pracowników. Jego zasadniczą zaletą jest to, że po zainstalowaniu certyfikatu (co wymaga kilku kliknięć myszą i wpisaniu jednego hasła) połączenie z ***eduroam*** uzyskuje się automatycznie, bez żadnej konfiguracji. Certyfikaty nie są na UMK stosowane w przypadku studentów, bo zachodzi obawa, że certyfikat, którego jedynym zastosowaniem jest udostępnienie sieci, nie byłby przez studentów traktowany jako wymagający odpowiedniej ochrony.
- Jeżeli uczelnia posiada centralną bazę Active Directory, to możliwe jest uwierzytelnianie użytkowników w oparciu o dane zawarte w tej bazie i standardowe oprogramowanie wbudowane w system Windows.

### Sprzęt

Jak wcześniej wspomniano, praktycznie wszystkie nowoczesne urządzenia bezprzewodowe wspierają standard 802.1x (często kryjący się pod hasłem Enterprise WPA). Przydział do wydzielonych VLAN-ów oraz separacja użytkowników od VLAN-u, poprzez który zarządza się urządzeniami, jest jednak funkcją dostępną tylko w droższych urządzeniach. Kolejną cechą, którą należy brać pod uwagę przy wyborze urządzeń, jest obsługa co najmniej dwóch wirtualnych sieci bezprzewodowych, jednej z uwierzytelnianiem 802.1x, drugiej niezabezpieczonej; bardzo pożądane jest aby obie sieci były rozgłaszane, czyli widoczne dla użytkowników (ta druga nieszyfrowana sieć jest nieoceniona przy obsłudze konferencji).

Obecnie producenci sprzętu bezprzewodowego coraz silniej lansują połączenie urządzeń dostępowych z centralnym kontrolerem. Często dopiero takie rozwiązanie daje pełne możliwości. Wadą takich systemów jest ich cena – zaletą ogromna łatwość panowania nad całą strukturą, duża odporność na błędy, wykrywanie punktów dostępowych uruchamianych bez zezwolenia itp. Z pewnością, przygotowując wystąpienie o środki na budowę dużej sieci bezprzewodowej warto takie rozwiązania brać pod uwagę. Funkcja wykrywania niezarejestrowanych punktów dostępowych bardzo podnosi bezpieczeństwo całej sieci uczelnianej. Często zdarza się, że np. pracownicy uruchamiają tanie urządzenie bezprzewodowe, bez żadnych zabezpieczeń, po to by ułatwić sobie pracę z komputera przenośnego. Nie zdają sobie sprawy, że taka sieć jest dostępna również poza budynkiem i stanowi boczne wejście do sieci wewnętrznej. Regulamin sieci powinien zawierać zakaz samodzielnego uruchamiania punktów dostępowych, a przestrzeganie tego zakazu powinno być kontrolowane przez skanowanie sieci. Kontrolery bezprzewodowe można skonfigurować w taki sposób, by automatycznie wykrywały „intruzów” i wysyłały powiadomienie do administratora sieci.

### Od czego zacząć

Minimalnym wymaganiem warunkującym przestąpienie do eduroam jest uruchomienie jednego urządzenia dostępowego połączonego z lokalnym serwerem Radius. Na stronach http://www.eduroam.pl zamieszczona jest przykładowa konfiguracja, która pozwala na uruchomienie takiego rozwiązania. Oczywiście, bez uruchomienia bazy użytkowników lokalnych nie osiągnie się prawdziwego celu, jakim jest ułatwienie pracownikom i studentom swojej uczelni dostępu do internetu w innych instytucjach.

## *Aspekty formalne*

Podstawowy dokument polskiego ***eduroam*** – ***Polska Polityka eduroam*** – jest jeszcze w trakcie przygotowywania. Będzie on jednak bazował na innych tego typu dokumentach oraz na Europejskiej Polityce eduroam. Polska Polityka musi być powszechnie akceptowalna i dlatego musi powstać w oparciu o dosyć szerokie konsultacje środowiskowe.

Po marcowym seminarium w Toruniu stworzona została nieformalna grupa robocza. Jednym z pierwszych zadań tej grupy powinna być właśnie praca nad Polityką. Grupa powinna się spotkać przed końcem roku 2006, aby podsumować zarówno prace na Polityką jak i nad wdrożeniami eduroam w polskich uczelniach.

Europejska polityka ***eduroam*** została już przyjęta przez władze TERENY i do końca roku 2006 będzie podpisywana przez wszystkie sieci krajowe.

### Ochrona danych osobowych

Technologia 802.1x pozwala na zbieranie bardzo dużej ilości informacji. Osoba mająca dostęp do kompletu danych ma możliwość stwierdzenia kto i w jakim miejscu łączył się do sieci i ile danych przez sieć przesyłał. Takie możliwości mogą budzić uzasadnione obawy o prywatność użytkownika. W tej części przedstawimy analizę działania ***eduroam*** w kontekście ochrony prywatności.

Przyjmijmy, że użytkownik chce skorzystać z sieci poza swoją instytucją macierzystą. W tym celu użytkownik musi przekazać urządzeniom instytucji, w której się znajduje swój identyfikator w postaci id@domena.m.kraj. Tym identyfikatorem będą znakowane wszystkie pakiety, które będą przekazywane do instytucji macierzystej w celu uwierzytelnienia. Pakiety te będą przesyłane przez sieć serwerów ***eduroam*** i będą w nich odnotowywane. Trzeba sobie jednak zdawać sprawę, że powiązanie konkretnej osoby z identyfikatorem jest na ogół niemożliwe poza instytucją macierzystą. Ponadto użytkownik może skorzystać z takiej metody uwierzytelnienia, w której widoczny dla wszystkich identyfikator nie będzie w żaden sposób z nim związany (np. może to być ten sam identyfikator dla wszystkich użytkowników z danej instytucji). Powiązanie konkretnej sesji z rzeczywistą osobą jest możliwe tylko w instytucji macierzystej, ale, z kolei, w tej instytucji nie ma na ogół możliwości stwierdzenia skąd użytkownik się logował, ponieważ adres urządzenia bezprzewodowego na ogół nie daje wystarczającej informacji.

Aby przedstawić tę sytuację we właściwej perspektywie należy ją porównać z innymi sytuacjami, kiedy użytkownik korzysta z sieci. Jeżeli użytkownik wysyła pocztę elektroniczną, to jego list jest przekazywany przez szereg serwerów sieciowych, gdzie jego identyfikator sieciowy, a bardzo często również imię i nazwisko są widoczne. Ponadto, jeżeli korzysta z macierzystego serwera pocztowego, to w logach tego serwera są odnotowywane parametry połączenia, na podstawie których można ustalić gdzie przebywa. To samo ma miejsce, gdy użytkownik korzysta z macierzystego serwera VPN. Połączenia ***eduroam*** nie są w żaden sposób szczególne.

Jednoznaczna określenie zakresu zastosowania przepisów dotyczących ochrony danych osobowych do ***eduroam*** wymagają ekspertyzy prawnej, ale powyższa analiza pokazuje, że jedynym miejscem, gdzie można mówić o przetwarzaniu danych osobowych jest instytucja macierzysta, a to przetwarzanie niczym nie odbiega od rutynowego wsparcia korzystania z lokalnej sieci informatycznej.

Dla zwiększenia zaufania użytkowników należy przyjąć następujące zasady:

- wszystkich administratorów ***eduroam*** obowiązuje zachowanie tajemnicy służbowej, w takim samym zakresie jak przy obsłudze wszystkich innych systemów transmisji danych;
- zapisy systemowe dotyczące uwierzytelniania użytkowników mogą być przekazywane wyłącznie uprawnionym organom ścigania, w szczególności nie mogą być wymieniane między administratorami struktury ***eduroam***;
- strony informacyjne ***eduroam*** muszą zawierać informację, że w czasie korzystania z ***eduroam*** widoczny identyfikator użytkownika będzie zapisywany w logach instytucji udostępniających sieć.

## *Wdrożenie eduroam na UMK*

Sieć UMK powstawała przy założeniu, że będzie włączona do eduroam i, że będzie w niej stosowany rozdział użytkowników między VLAN-y. W przetargu na urządzenia bezprzewodowe zakupiono 53 punkty bezprzewodowe firmy 3COM, typu 7250.

Pierwotnie zakładano bardzo rozbudowaną konfigurację, która uwzględniała rozpoznawanie użytkowników w ich macierzystej lokalizacji (budynku), uważano bowiem, że konieczna będzie np. obsługa wydruków z laptopów pracowników. Ostatecznie odstąpiono od tego rozwiązania z dwóch powodów: po pierwsze nie było nacisku na dodatkowe usługi, a po drugie w sytuacjach, kiedy zasięgi AP z dwóch budynków nachodzą na siebie, zachodziło niebezpieczeństwo przypisywania użytkowników do VLAN-u w niewłaściwym budynku.

Ostatecznie, stworzona konfiguracja rozdziela do oddzielnych VLAN-ów: pracowników UMK, studentów UMK oraz gości (uwierzytelnianych przez eduroam). Możliwość bardziej dokładnego przydziału użytkowników jest jednak nada otwarta.

Korzystając z faktu, że urządzenia 3COM mogą rozgłaszać dwie sieci bezprzewodowe, poza siecią ***eduroam*** uruchamia się w miarę potrzeby niezabezpieczoną sieć ***UMK-conf***. W tej sieci uwierzytelnianie następuje przez interfejs WWW i w oparciu o konta i hasła rozdawane uczestnikom konferencji. Ponieważ identyfikatory są czynne tylko przez krótki czas, służą wyłącznie dostępowi do sieci, więc argumenty przeciw uwierzytelnianiu przez interfejs WWW nie mają w tym przypadku zastosowania.

Jak wcześniej wspomniano, instytucja udostępniająca sieć powinna zadbać, aby wprowadzić mechanizmy uniemożliwiające uwierzytelnionym użytkownikom zmianę przydzielonego im adresu internetowego. Na UMK zaimplementowano taki mechanizm oparty o dedykowany serwer eduroam i oprogramowanie dnsmasq.

Na UMK działa system uwierzytelniających serwerów LDAP. Poza serwerem centralnym wdrożono również dedykowane serwery dla użytkowników korzystających z kont na serwerach wydziałowych.

Na całej uczelni (z wyjątkiem Wydziału Matematyki i Informatyki) zostały zdefiniowane VLAN-y służące do obsługi sieci bezprzewodowej. Te VLAN-y to:

1) zarządzanie – służący do zarządzanie AP i kontaktu między AP a serwerami Radius,
2) pracowniczy – przyporządkowuje się do niego komputery pracowników UMK,
3) studencki – przyporządkowuje się do niego komputery studentów UMK,
4) gościnny – przyporządkowuje się do niego gości uwierzytelnionych przez eduroam,
5) konferencyjny – służy do obsługi uczestników konferencji uwierzytelnianych przez interfejs WWW.

Wszystkie AP struktury uczelnianej wskazują na dwa uczelniane serwery Radius. Uczelniane serwery Radius, na podstawie identyfikatora sieciowego użytkownika, dokonują uwierzytelnienia na jeden z następujących sposobów:

1) weryfikując indywidualny certyfikat pracownika,
2) łącząc się z odpowiednim serwerem LDAP, sprawdzają poprawność podanego hasła,
3) jeżeli jest to gość, przesyłając zlecenie uwierzytelnienia do krajowego serwera eduroam.

Po rozpoznaniu i uwierzytelnieniu użytkownika serwery przesyłają do AP informację o tym, do jakiego VLAN-u użytkownik powinien zostać przypisany.

Przygotowano rozbudowane środowisko informacyjne dostępne pod adresem eduroam.umk.pl. Instrukcje dotyczą instalacji konkretnych, wspieranych przez UCI, kart bezprzewodowych i sposobu konfiguracji uwierzytelniania 802.1x w różnych systemach operacyjnych. Ponieważ na UMK stosowane są dwie metody uwierzytelnienia (inna dla pracowników i inna dla studentów), to instrukcje opracowano w formie dwóch odrębnych ścieżek.

*strona eduroam UMK w Toruniu*


*Strona wyboru instrukcji konfiguracyjnych*


*Instrukcje instalacji karty bezprzewodowej*

Wcześniej zostały przedstawione zalety stosowania indywidualnych certyfikatów oraz powody, dlaczego na UMK nie zastosowano certyfikatów dla studentów. Wprowadzenie tego systemu dla pracowników UMK wymagało zbudowania systemu dystrybucji certyfikatów. W typowych rozwiązaniach, wystawianie certyfikatów wymaga całkowitej pewności co do tożsamości osoby, a

zatem zazwyczaj osobistego kontaktu. Certyfikaty, które , na UMK, są wystawiane na potrzeby eduroam nie mogą być jednak stosowane do innych celów (np. nie można przy ich pomocy podpisywać poczty elektronicznej). Dlatego uznano, że można nieco złagodzić wymogi bezpieczeństwa, zachowując jednak ich rozsądny poziom. W systemie UMK, dla wszystkich pracowników przygotowano komplet klucz prywatny i certyfikat. Każdy taki pakiet jest przechowywany w formacie p12 i jest zaszyfrowany losowym hasłem. Pracownik, który chce pobrać certyfikat musi skorzystać z dedykowanej strony WWW i podać na niej swoje imię, nazwisko i numer PESEL. Po zweryfikowaniu tych danych oraz sprawdzeniu, że pracownik dysponuje uniwersyteckim kontem e-mail, system wyświetla na ekranie hasło, którym zabezpieczony jest plik certyfikatu, a jednocześnie wysyła do pracownika e-mail z odpowiednim, indywidualnym odsyłaczem do pobrania certyfikatu. Po pobraniu certyfikatu włączany jest licznik czasu, który po kilku minutach zablokuje możliwość pobierania ponownego. Na uwagę zasługuje kilka cech tego systemu. Po pierwsze pracownik nie wprowadza na stronę tego systemu swojego identyfikatora i hasła – chodzi o utrudnienie wystawienia strony podszywającej się pod ten system, a służącej zbieraniu haseł pracowników UMK. Po drugie możliwość nieuprawnionego pobrania certyfikatu jest bardzo utrudniona. Osoba, która chciałaby to zrobić musiałaby znać imię, nazwisko i PESEL, a także mieć dostęp do poczty elektronicznej danego pracownika. Samo przejęcie listu z odsyłaczem do certyfikatu nie wystarczy, ponieważ w liście nie ma hasła zabezpieczającego certyfikat. Posiadanie hasła bez dostępu do listu również nic nie daje. System wysyła list na adres zapisany w bazie uczelnianej, nie daje zatem możliwości podstawienia fałszywych danych. System wystawiania certyfikatów działa od dłuższego czasu i nie nastręcza pracownikom UMK trudności.

## *Dodatkowe źródła informacji*


1. http://www.eduroam.pl – polski portal informacyjny eduroam
2. http://www.eduroam.org – główna strona eduroam
3. http://eduroam.umk.pl – wejście do stron informacyjnych UMK na temat eduroam
4. http://www.terena.nl/activities/tf-mobility – strona grupy roboczej TF-Mobility
5. http://www.geant2.net/server/show/nav.758 – strona JRA5
6. http://www.it.utah.edu/services/connected/wireless/index.html – serwis przygotowany przez uniwersytet w UTAH (sieć tego uniwersytetu była jedną z pierwszych sieci uczelnianych zbudowanych w standardzie 802.1x)
7. http://www.ieee802.org/1/pages/802.1x.html – strona główna standardu 802.1x
8. RFC2865 – Remote Authentication Dial In User Service (RADIUS)
9. RFC2866 – RADIUS Accounting
10. RFC2716 – PPP EAP TLS Authentication Protocol
11. RFC3579 – RADIUS Support For Extensible Authentication Protocol
12. RFC3580 – IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines
13. RFC3748 – Extensible Authentication Protocol (EAP) (EAP)
14. EAP TTLS – EAP Tunneled TLS Authentication Protocol (EAP-TTLS)


## *Spis pojęć*

| | |
|---|---|
| 802.1q | standard pozwalający na tworzenie wirtualnych sieci lokalnych (zob. VLAN) |
| 802.1x | standard opisujący zasady dopuszczania użytkownika do sieci po uprzednim uwierzytelnieniu, typowo we współpracy z serwerem Radius |
| 802.1i | synonim WPA2 (zob.) |
| AP | zob. access-point |
| access-point | radiowy punkt dostępowy – urządzenie sieciowe zawierające nadajnik radiowy i pozwalające na przyłączenie do sieci komputerów wyposażonych w karty radiowe; access-point powinien obsługiwać różne standardy szyfrowania transmisji oraz zabezpieczeń przed nieuprawnionym dostępem do sieci |
| autoryzacja | (ang. authorization) proces nadania użytkownikowi uprawnień do pewnych zasobów (pojęcie autoryzacji jest dość często mylone z uwierzytelnieniem) |
| GEANT2 | projekt finansowany głównie przez Komisją Europejską, którego celem jest utrzymanie europejskiej sieci na użytek nauki oraz rozwój nowych technologii sieciowych |

| | |
|---|---|
| IEEE | stowarzyszenie, którego działalność polega między innymi na tworzeniu standardów dla urządzeń elektronicznych, w tym komputerowych |
| JRA5 | Joint Research Activity 5 – Roaming and Authorisation – projekt rozwojowy finansowany w ramach GEANT2, którego celem jest opracowanie standardów współpracy między sieciami europejskimi |
| LDAP | Lightweight Directory Protocol – nazwa oznaczająca zarówno protokół komunikacyjny jak i usługę katalogową, która z niego korzysta. Obecnie bazy LDAP są powszechnie stosowane do zarządzania systemami informatycznymi |
| MAC | adres „sprzętowy" karty sieciowej, w założeniu przydzielany karcie przez producenta i niezmienny, w rzeczywistości bardzo prosty do zmiany przez użytkownika |
| PCSS | Poznańskie Centrum Superkomputerowo-Sieciowe – operator polskiej sieci naukowej PIONIER |
| PIONIER | program rozwoju infrastruktury informatycznej dla polskiego środowiska naukowego, ale nazwą tą obejmuje się również samą ogólnopolską sieć zbudowaną w ramach tego programu |
| Radius | protokół komunikacyjny służący kontroli dostępu do sieci, tą nazwą określa się również oprogramowanie pełniące rolę serwera uwierzytelniającego bazującego na protokole Radius |
| Single-Sign-On | potoczna nazwa systemów stanowiących nadbudową nad wieloma systemami informatycznymi wymagającymi uwierzytelnienia użytkownika, single-sign-on pozwala na jednokrotne uwierzytelnienie i późniejszy dostęp do wszystkich aplikacji objętych tym systemem, już bez ponownego, jawnego procesu logowania się |
| TERENA | Trans European Research and Education Networking Association – organizacja zrzeszająca europejskie krajowe akademickie sieci komputerowe, koordynująca również działania o charakterze badawczo-rozwojowe w ramach tzw. grup roboczych |
| uwierzytelnianie | (ang. authentication) proces pozwalający na potwierdzenie tożsamości użytkownika, będący zazwyczaj fazą wstępną do nadania użytkownikowi praw dostępu do jakiegoś zasobu |
| VLAN | wirtualna sieć lokalna – pojęcie to zazwyczaj odnosi się do zastosowania protokołu 802.1q, umożliwiającego logiczny rozdział pakietów Ethernet w sposób zbliżony do sytuacji eksploatowania kilku, fizycznie rozłącznych sieci komputerowych |
| VPN | wirtualna sieć prywatna – system pozwalający na traktowanie komputera podłączonego w dowolnym miejscu sieci Internet tak jak komputera włączonego do sieci wewnętrznej, budowany w oparciu o oprogramowanie szyfrujące i certyfikaty potwierdzające tożsamość, stosowane np. w przypadku konieczności dostępu do chronionych danych przez modem lub za pośrednictwem niezaufanej sieci |
| WEP | system zabezpieczenia sieci bezprzewodowych oparty o jeden klucz szyfrujący, obecnie uważany za zbyt prosty do przełamania, aby gwarantować bezpieczeństwo sieci |
| WPA | system zabezpieczenia sieci bezprzewodowych oparty na znacznie lepszych zasadach szyfrowania i indywidualnych kluczach szyfrujących dla każdej sesji |
| WPA2 | synonim standardu 802.1i – rozszerzenie i sformalizowanie WPA |
| WPA-Enterprise | połączenie WPA/WPA2 z uwierzytelnianiem 802.1x |
| WPA-PSK | WPA/WPA2 na użytek niewielkiej grupy użytkowników (mała firma lub dom), zamiast uwierzytelniania 802.1x stosuje klucz, który musi być znany wszystkim użytkownikom sieci |