

# Projekt sieci UMK-EduRoam swobodnego dostępu do Internetu na Uniwersytecie Mikołaja Kopernika w Toruniu

(wersja wstępna, niedokończona)

Tomasz Wolniewicz  
Maja Górecka-Wolniewicz

28 grudnia 2004 roku

## 1 Wstęp

Sieć UMK-EduRoam będzie fragmentem europejskiej sieci EduRoam. Będzie pozwalała ma połączenie się z Internetem pracownikom i studentom UMK, uprawnionym gościom z innych uczelni oraz pewnym dodatkowym grupom, np. stałym czytelnikom Biblioteki Uniwersyteckiej.

## 2 Poziomy dostęp do sieci

W sieci UMK-EduRoam zostaną zaimplementowane różne poziomy dostęp i związane z nimi uprawnienia. Podstawowymi założeniami systemu poziomów dostępu są: umożliwienie pracownikom każdej jednostki nieskrępowanego dostępu do usług lokalnych (np. drukarek) oraz pozwolenie wszystkim pozostałym uprawnionym osobom na nieskrępowany dostęp do Internetu i usług UMK. Pierwsze założenie jest nadzwyczaj istotne jeżeli chce się uniknąć potrzeby tworzenia dodatkowych, lokalnych sieci WLAN.

1. lokalny — dotyczy osób, które są związane z budynkiem, w którym łączą się do sieci (osoby są przypisywane do VLAN-u 1),
2. uczelniany — dotyczy osób (pracowników i studentów UMK), które łączą się do sieci w miejscu, z którym nie są związane, np. na obcym wydziale, lub na terenie ogólnodostępnym (pracownicy są przypisywani do ogólnouczelnianego VLAN-u `staffumk`, a studenci do `studumk`),
3. gościnny — dotyczy wszystkich osób, które się autoryzują za pośrednictwem serwerów radius umieszczonych poza UMK (te osoby są przypisywane do ogólnouczelnianego VLAN-u `guest`),

4. specjalny — dotyczy osób uprawnionych do dostępu do Internetu tylko na specjalnie wydzielonym obszarze, przede wszystkim chodzi o czytelników BU, którzy nie mają innych uprawnień na dostęp do sieci (VLAN *special*),
5. tymczasowy — dotyczy osób, które nie mogą korzystać z protokołu 802.1x albo z powodu braku odpowiedniego konta, albo z powodu braku oprogramowania (osoby są przypisywane do ogólnouczelnianego VLAN-u *temporary*).

### 3 Realizacja

Dostęp do UMK-EduRoam jest możliwy za pośrednictwem urządzeń bezprzewodowych oraz z dedykowanych gniazd ethernetowych.

#### 3.1 Sieć bezprzewodowa

Sieć bezprzewodowa rozgłasza SSID „eduroam”.

Z wyjątkiem dostępu a poziomie „tymczasowym”, wszystkie osoby uprawnione do korzystania z UMK-EduRoam muszą być w niej uwierzytelnione albo za pomocą uczelnianej bazy LDAP, albo za pośrednictwem serwerów EduRoam.

Właściwe uwierzytelnianie odbywa się poprzez protokół 802.1x.

Bez skonfigurowanego 802.1x do sieci można się dołączyć poprzez podanie ogólnie znanego klucza WEP (np. *Torun*). Takie połączenie daje dostęp wyłącznie do dedykowanego serwera WWW, gdzie można przeczytać instrukcje, pobrać oprogramowanie, sterowniki itp.

Rozdział pomiędzy poziomy dostęp do sieci jest realizowany poprzez przydział do odpowiednich VLAN-ów.

Wszelkie przypisania do VLAN-ów są realizowane poprzez przypisanie użytkownika do odpowiednich grup w bazie LDAP. Na podstawie tych grup oraz lokalizacji ustawiany jest odpowiedni VLAN. Każdy pracownik jest przypisany do grupy *staff* oraz do co najmniej jednej grupy lokalnej, każdy student jest przypisany do grupy *stud* i może być dodatkowo przypisany do grup lokalnych, jeżeli zachodzi taka potrzeba.

AP są podzielone na podgrupy odpowiadające sieciom lokalnym. W typowych przypadkach podgrupa składa się z jednego budynku. Połączenie AP z siecią lokalną musi być zrealizowane w taki sposób, że ustawienie VLAN-u o numerze 1 przypisze użytkownika do sieci lokalnej. Na użytek tego tekstu założymy, że zdefiniowane są grupy AP: *ap-law*, *ap-bu*, *ap-uci*, *ap-econ* itd.

Przydział użytkownika do VLAN-u następuje w oparciu o dwa kryteria:

- grupę do której przyporządkowano użytkownika,
- grupę AP do której się dołączył.

Przydział następuje na radiusie uwierzytelniającym użytkownika tzn. pracownik Wydziału Prawa, który uwierzytelnia się na radiusie obsługującym realm *law.umk.pl*, musi na tym radiusie otrzymać odpowiedni VLAN. Na radiusie

„law” trzeba zatem zdefiniować grupę AP **ap-law**, grupy użytkowników prawa: (**staff-law**, ew. **stud-law**) oraz grupy ogólne: **staff**, **stud**, **guest**. Podobnie, na radiusie „econ” trzeba zdefiniować grupę AP **ap-econ** i grupy użytkowników **staff-econ**, **staff**, **stud**, **guest**, **reject**. Na radiusie ogólnouczelnianych zdefiniowane będą wszystkie grupy AP i wszystkie grupy pracowników.

Pracownik Wydziału Prawa, dołączający się w ramach grupy **ap-law** zostanie uwierzytelniony albo w oparciu o konto na Wydziale Prawa, albo konto na serwerze uczelnianym, w obu przypadkach zostanie rozpoznany jako członek grup **staff-law** i **staff** i na tej podstawie przypisany do VLAN-u 1. Pracownik Wydziału Ekonomii dołączający się w tym samym punkcie (w ramach grupy **ap-law**) będzie uwierzytelniany w oparciu o konto na wydziale lub na serwerze uczelnianym i rozpoznany jako członek grup **staff-econ** i **staff**, ponieważ jednak kombinacja grup (**ap-law**)&(b)staff-econ) nie będzie nigdzie zdefiniowana, to przypisanie do VLAN-u nastąpi na podstawie przynależności do grupy **staff**, zatem pracownik zostanie przypisany do VLAN-u **staffumk**.

W tym schemacie nieistotne jest, czy konkretna lokalizacja jest obsługiwana przez dedykowany serwer radius, czy poprzez serwer wspólny, kontaktujący się z kilkoma serwerami LDAP.

Osoba, która ma prawo dostępu tylko w określonej lokalizacji posiada tylko jedną grupę specjalną (na przykład **user-bu**) oraz grupę **reject**. Grupa **user-bu** występuje tylko w połączeniu z grupą AP **ap-bu** i przypisuje osobę do VLAN-u specjalnego, w każdej innej lokalizacji do głosu dojdzie grupa **reject** powodująca odrzucenie połączenia.

Odpowiednia konfiguracja kolejności grup na serwerach radius powoduje, że przypisania bardziej szczegółowe będą miały pierwszeństwo.

Pewnym problemem może być sytuacja, kiedy AP z sieci jednego budynku są odbierane w budynku sąsiednim. W takim przypadku osoba znajdująca się na terenie budynku macierzystego może być przypisywana do AP z budynku sąsiedniego i w konsekwencji do VLAN-u **staffumk** a nie do VLAN-u 1. Na terenie UMK ta sytuacja nie powinna być jednak częsta i przy tworzeniu grup AP należy zwrócić uwagę, aby ten problem minimalizować przy konstrukcji grup i rozmieszczaniu AP. Przenikanie grup będzie jednak występować głównie na terenach otwartych i tam nie powinno stanowić istotnego problemu.

Jeżeli osobie nie przypisano żadnej grupy, to konfiguracja serwera radius przypisuje mu VLAN **guest**. Ten przypadek występuje zawsze, kiedy ktoś jest uwierzytelniany poza UMK za pośrednictwem EduRoam.

Wszystkie AP będą włączone do portów tagowanych 802.1q na przełączniku ethernetowym. Porty są przypisane do VLAN-ów: 1, **staffumk**, **studumk**, **guest**, **temporary** (domyślny VLAN AP) oraz VLAN-u **special** (jeżeli występuje w danej jednostce).

VLAN-y: **staffumk**, **studumk**, **guest** i **temporary** są zdefiniowane w całej uczelni.

## 4 Obsługa

### 4.1 Poza UCI

VLAN-om ogólnuczelnianym trzeba zapewnić obsługę w zakresie: przydziału adresu IP, routingu, serwera DNS. Firewall UCI rozpoznaje na interfejsie zewnętrznym wszystkie VLAN-y ogólnuczelniane. VLAN-om **staffumk**, **studumk** i **guest** przydziela prywatne adresy internetowe i realizuje maskaradę adresów.

W obecnej wersji oprogramowania 3COM, klienci, którzy nie zostali uwierzytelnieni poprzez 802.1x są przypisani do domyślnego VLAN-u access-pointa. Ponieważ chcemy takim klientom dawać ograniczony dostęp do sieci, a jedyną realną metodą aby ich obsłużyć jest wydzielenie dla nich ogólnouniwersyteckiego VLAN-u, to w konsekwencji wszystkie AP muszą być w jednym VLAN-ie.

Oczywiście ten sam VLAN dla AP i dla niewierzytelnionych klientów jest bardzo niebezpiecznym rozwiązaniem, dlatego należy zakładać, że docelowo 3COM rozdzieli te dwa VLAN-y, nie będzie to jednak miało bardzo istotnego wpływu na projekt UMK-EduRoam, pozwoli jedynie złagodzić pewne zabezpieczenia.

W zasadzie należałoby projektować system korzystający z dwóch VLAN-ów — **temporary** — dla niewierzytelnionych użytkowników i **management** dla zarządzania AP i ich kontaktu z serwerami radius. Przedstawione rozwiązanie posługuje się dwoma VLAN-ami, w celu rozdzielenia ich funkcji, należy jednak pamiętać, że w istocie dwie nazwy oznaczają na razie ten sam VLAN.

Ponieważ wszystkie AP są w jednym VLAN-ie, to kontakt AP z serwerami radiusowymi musi się odbywać poprzez jeden punkt (bramkę VLAN-u **management**), chyba że również serwery radius są w tym VLAN-ie. Uwierzytelniający serwer radius jest bardzo wrażliwym punktem, bo włamanie na niego pozwala zmienić konfigurację i przechwytywać hasła. Serwery uwierzytelniające powinny być zatem bardzo dobrze zabezpieczone i włączenie ich w niebezpieczny VLAN należy uznać za niedopuszczalne. Dobrym rozwiązaniem jest serwer proxy, nie posiadający certyfikatu. Włamanie na taki serwer i zmiana jego konfiguracji nie mogą spowodować przejmowania haseł użytkowników. Włączenie takiego serwera w VLAN **temporary** (i jednocześnie **management**) i ustawienie go na Bielanych pozwoli na utrzymywanie dwóch serwerów radiusowych pracujących niezależnie od siebie. W przypadku możliwości rozdzielenia obu VLAN-ów, można by zrezygnować z serwera proxy, nie zmieni to jednak liczby potrzebnych serwerów, a funkcja proxy ułatwia zarządzanie całością, więc w przypadku docelowym można wyposażyć serwer bielański w dodatkową kartę (albo ustawić obsługę VLAN-ów 1q), tak by nadal obsługiwać oba VLAN-y na jednym komputerze.

Firewall UCI będzie posiadał listę wszystkich MAC access-pointów. Tym MAC-om będzie przydzielał adresy, na podstawie statycznej listy. Prawdopodobnie właściwe jest również ustawienie statycznych wpisów ARP. Domyślną bramką dla AP będzie firewall UCI. Firewall powinien odrzucać pakiety od wszystkich innych MAC-ów.

Radius bielański powinien mieć dwa interfejsy fizyczne, jeden z nich będzie

wpięty do VLAN-u **temporary**, drugi do sieci uczelnianej. Na tym serwerze pracować będzie również serwer DHCP na użytek sieci nieuwierzytelnionej. Dobrze by było, aby miał również kopię statycznej tablicy z firewala UCI, w ten sposób podwyższyłoby się niezawodność konfiguracji access-pointów. Uruchomiony tam serwer WWW będzie dawał dostęp do wszystkich informacji, które są niezbędne do skonfigurowania prawidłowego dostępu.

*Opracowania wymaga sposób przekierowania wszystkich zapytań WWW na ten jeden serwer.*

Dzięki takiej konfiguracji, każdy AP będzie mógł się kontaktować zarówno z radiusem uczelnianym w UCI, jak też z radiusem uczelnianym na Bielanach.

Decyzje, które trzeba podjąć: na jakich komputerach postawić serwery, gdzie fizycznie zlokalizować serwery (BU byłaby może najlepszym miejscem)

## 4.2 W UCI

W UCI zdefiniowane są VLAN-y **staffumk** - 32, **studumk** - 33, **guest** - 34 oraz **temporary** - 35. Te VLAN-y są obsługiwane w obrębie segmentu stacji roboczych UCI. Interfejs sieciowy firewala UCI, wpięty do tego segmentu, obsługuje te VLAN-y przydzielając adresy DHCP i realizując przemapowanie adresów. W UCI jest zatem odwzorowana struktura sieci zewnętrznej, ale obsługiwana w sposób niezależny. W UCI pracuje również kopia serwisu WWW dla użytkowników nieautoryzowanych.