Koncepcja wdrożenia usługi eduroam w sieci PIONIER

Tomasz Wolniewicz, UCI UMK (twoln@umk.pl)
Maja Górecka-Wolniewicz, UCI UMK (mgw@umk.pl)
Zbigniew Ołtuszyk, PCSS (zbigniew.oltuszyk@man.poznan.pl)
dokument przygotowany w ramach projektu B-R eduroam-PIONIER
wersja 1.0

Spis treści

1. Wstęp

Organizacja usługi eduroam w Polsce powinna brać pod uwagę specyfikę sieci PIONIER. W Polsce, inaczej niż w innych sieciach naukowych Europy, zdecydowana większość instytucji korzysta z sieci poprzez przyłącze do sieci miejskich członków Konsorcjum PIONIER, a nie bezpośrednio do samego szkieletu PIONIER.

Polskie instytucje naukowe zazwyczaj podpisują umowy o korzystaniu z sieci PIONIER z jednostkami wiodącymi sieci miejskich. Z tego powodu bezpośrednim partnerem i reprezentantem Konsorcjum PIONIER jest jednostka wiodąca, a nie Operator sieci PIONIER. Uwzględniając tę strukturę organizacyjną dodatkowo określamy Regionalnych Operatorów eduroam, którymi są jednostki wiodące – członkowie sieci PIONIER.

Planując wdrożenie eduroam należy od razu wziąć pod uwagę rozwiązania oparte o protokół RadSec, ponieważ to one będą dominowały w przyszłości.

Usługa eduroam umożliwia zainteresowanym instytucjom uruchomienie uwierzytelnianego gościnnego dostępu na swoim terenie, a dodatkowo pracownicy i studenci instytucji korzystającej z usługi eduroam uzyskują możliwość korzystania z gościnnego dostępu we wszystkich sieciach eduroam na świecie.

Każda instytucja korzystająca z usługi eduroam musi prowadzić własny serwer RADIUS, za pośrednictwem którego realizowane są uwierzytelnienia zarówno użytkowników własnych jak i gości.

Identyfikator użytkownika jest skonstruowany zgodnie z RFC 4282 w postaci (id@domena), co umożliwia odnalezienie serwera RADIUS instytucji odpowiedzialnej za uwierzytelnienie użytkownika. Uwierzytelnianie gości wymaga połączenia między serwerem instytucji udostępniającej sieć i serwerem instytucji macierzystej gościa. Te połączenia są realizowane za pośrednictwem infrastruktury eduroam.

2. Ustalenia formalne

Podstawowym dokumentem ustalającym zasady działania polskiej usługi eduroam jest *Polska Polityka eduroam* dostępna pod adresem http://www.eduroam.pl/polityka/.[1] W niniejszym dokumencie nie będziemy powtarzać ustaleń zapisanych w Polityce.

Instytucje – członkowie Konsorcjum PIONIER – pełnią rolę Regionalnych Operatorów eduroam w oparciu o umowy [2].

Aby rozpocząć korzystanie z eduroam instytucja musi podpisać deklarację [3] , w której zobowiązuje się do przestrzegania zasad Polityki. Deklarację przyjmuje właściwy operator (na ogół regionalny). Po potwierdzeniu spełnienia przez przystępującego wymogów formalnych oraz włączenia serwera instytucji do struktury eduroam, operator przyjmujący deklarację wystawia dokument potwierdzający uruchomienie usługi oraz zobowiązania Operatora i Koordynatora wynikające z Polityki [4]. Operator zgłasza Koordynatorowi fakt dołączenia kolejnego użytkownika i wprowadza do bazy eduroam odpowiednie informacje.

3. Faza I – rozwój hierarchicznej struktury serwerów RADIUS

3.1. Struktura serwerów

Zaprojektowana struktura przewiduje trzy poziomy hierarchii:

- poziom I – serwery krajowe,
- poziom II – serwery regionalne,
- poziom III – serwery instytucji.

Zgodnie z aktualnym modelem europejskiej usługi eduroam, jeżeli serwer otrzymuje zlecenie uwierzytelnienia zawierające domenę, której nie obsługuje, to musi je przekazać do nadrzędnego serwera w hierarchii. W przypadku polskich instytucji korzystających z usługi eduroam, serwerem nadrzędnym jest serwer regionalny, lub, w specyficznych przypadkach, jeden z serwerów krajowych.

Utrzymywanie serwerów regionalnych jest uzasadnione z kilku powodów:

- przemieszczanie się użytkowników będzie się odbywało w przeważającej części w obrębie jednego regionu (a nawet jednego miasta);
- na etapie uruchamiania usługi eduroam w kolejnych instytucjach, dużo wygodniejszy jest kontakt z partnerem lokalnym;
- w obecnym modelu, świadczenie usługi eduroam musi być powiązane z prowadzeniem serwera pośredniczącego, a zatem oba zadania powinny być prowadzone przez ten sam podmiot.

Ustawienia serwera niższego poziomu powinny preferować jeden serwer nadrzędny, serwer dodatkowy powinien być używany wyłącznie w czasie awarii serwera preferowanego. Preferowanym serwerem nadrzędnym dla regionalnych serwerów pośredniczących powinien być topologicznie bliższy serwer krajowy. Warszawa, w której działają dwie jednostki będące członkami Konsorcjum PIONER, może być potraktowana w szczególny sposób, tzn. na jej terenie mogą działać dwa niezależne serwery regionalne, między którymi mogą być stworzone bezpośrednie połączenia dla domen przez nie obsługiwanych.

Serwery ogólnopolskie powinny pełnić symetryczną rolę – pracować na identycznym oprogramowaniu i w identycznych konfiguracjach. Wyjątkiem od tej reguły mogą być konfiguracje testowe.

3.2. Zabezpieczenie serwerów regionalnych

Przygotowując koncepcję uruchomienia usługi eduroam w Polsce rozważono dwie możliwości zabezpieczenia regionalnych serwerów pośredniczących. Pierwsze rozwiązanie, to uruchamianie pojedynczych serwerów i korzystanie z serwera krajowego jako serwera zapasowego, w drugim, zdublowane serwery regionalne.

Technicznie, pierwszy model można uznać za wystarczający – awaria serwera regionalnego jest mało prawdopodobna, w wyjątkowych sytuacjach serwer krajowy powinien być odpowiednim zabezpieczeniem. Takie rozwiązanie wprowadza jednak szereg komplikacji organizacyjnych:

- niezbędne jest konfigurowanie tablicy wszystkich serwerów instytucjonalnych nie tylko na poziomie regionalnym, ale również krajowym, co oznacza, że w sprawie każdej instytucji potrzebny jest kontakt z dwoma grupami administratorów;
- niezbędne jest dużo dokładniejsze synchronizowanie planowych wyłączeń serwerów regionalnych i serwerów krajowych;
- utrudnione jest zbieranie statystyk roamingowych poziomu regionalnego.

W związku z tym, przyjęto że prostszy w implementacji i bardziej niezawodny w działaniu jest model drugi, a więc zdublowane serwery regionalne. Główny serwer regionalny powinien być utrzymywany na odpowiednio wydajnym komputerze dedykowanym do tego zadania. Serwer zapasowy będzie stosowany tylko w wyjątkowych sytuacjach, z tego powodu nie ma konieczności, aby w tym przypadku stosować dedykowany komputer.

3.3. Warunki techniczne działania serwerów pośredniczących

Z uwagi na ograniczoną funkcjonalność serwerów pośredniczących oraz na planowane wdrożenie protokołu RadSec najwłaściwsze jest wdrożenie oprogramowania radsecproxy. Wstępną konfigurację tego pakietu przygotuje Koordynator [5] . W okresie przejściowym dopuszcza się pracę regionalnych serwerów pośredniczących na oprogramowaniu FreeRADIUS.

Serwery krajowe będą korzystały z oprogramowania komercyjnego Radiator lub radsecproxy. Ostateczna decyzja w tej sprawie zależy od tego jak szybko do radsecproxy zostaną dodane funkcji zbierania statystyk.

Serwery pośredniczące powinny być skonfigurowane w taki sposób, aby w przypadku nieotrzymania w ustalonym czasie odpowiedzi z kolejnego punktu hierarchii, przekazywały odpowiedź Access-Reject[1].

Serwery pośredniczące muszą rejestrować wszystkie pakiety Access-Accept i utrzymywać zapisy przez 6 miesięcy.

Serwery pośredniczące muszą prowadzić statystyki pozwalające na określenie liczby pakietów Access-Accept oraz liczby poprawnie uwierzytelnionych adresów MAC. Administratorzy serwerów pośredniczących muszą współpracować z Koordynatorem w sprawie zbierania statystyk wymaganych przez eduroam Service Activity.

Serwery pośredniczące powinny odnotowywać pojawienie się atrybutów służących do ustawiania VLAN-ów (Tunnel-Medium-Type, Tunnel-Type, Tunnel-Private-Group-Id), ponieważ zazwyczaj jest to oznaka źle skonfigurowanego serwera RADIUS i może prowadzić do trudności w uzyskaniu dostępu do sieci.

3.4. Tablice domen

Domeny miejskie miast, w których istnieją sieci miejskie członków Konsorcjum PIONIER (np. `lodz.pl`, `wroc.pl`), będą w całości delegowane do regionalnych serwerów pośredniczących. W przypadku instytucji korzystających z domen zarejestrowanych w jednej z domen ogólnopolskich (np. `amu.edu.pl`, `umk.pl`) niezbędne będą indywidualne wpisy w tablicach serwerów krajowych, delegujące obsługę do właściwych serwerów regionalnych.

Przypadek Warszawy będzie obsługiwany indywidualnie.

1 Kwestia czy należy odsyłać Access-Reject, czy po prostu nie odpowiadać, była szeroko dyskutowana na liście TF-Mobility, bez osiągnięcia jednoznacznej decyzji. Obydwa rozwiązania mają i wady i zalety. W naszym przekonaniu odsyłanie Access-Reject jest bardziej uzasadnione.

3.5. Serwery instytucji

Zakłada się, że zdecydowana większość instytucji będzie korzystała z oprogramowania FreeRADIUS lub Microsoft IAS. Sposób konfigurowania tych serwerów został opisany w dokumentach: [6], [7], [8]

4. Faza II – bezpośrednie połączenia serwerów RADIUS przy zastosowaniu protokołu RadSec

Protokół RadSec ma szereg przewag nad zwykłym protokołem RADIUS, z których najważniejszymi są zapewnienie bezpieczeństwa transmisji poprzez zastosowanie tunelu SSL oraz umożliwienie wzajemnej weryfikacji tożsamości serwerów RADIUS poprzez wymianę certyfikatów X.509.

W tradycyjnej strukturze eduroam, serwer ufa wyłącznie tym, z którymi ustanowiono partnerstwo, a weryfikacja drugiej strony opiera się na dopasowaniu adresu IP i wspólnego klucza.

RadSec pozwala na odstąpienie od hierarchicznej struktury serwerów eduroam, ponieważ fakt, że inny serwer jest uprawniony do przekazywania komunikatów eduroam jest gwarantowany posiadaniem przez niego certyfikatu wystawionego przez upoważniony urząd certyfikacyjny oraz zawierającego odpowiednio skonstruowany URN w atrybucie alternativeSubjectName. Dzięki temu odszukanie odpowiedniego serwera RADIUS jest realizowane poprzez DNS, a połączenie nawiązuje się bezpośrednio (patrz [9]).

4.1. Program wdrożenia fazy II

Dojście do docelowego modelu, w którym większość polskich instytucji korzysta z protokołu RadSec i dynamicznego wyboru partnera zostanie rozłożone na kilka kroków pośrednich:

1. zastąpienie standardowych połączeń RADIUS między serwerami regionalnymi a serwerami centralnymi statycznymi połączeniami RadSec;
2. wdrożenie obsługi dynamicznego wyboru partnera na serwerach regionalnych;
3. stopniowe wprowadzanie dynamicznego wyboru partnera dla polskich instytucji korzystających z usługi eduroam.

4.1.1. Wdrożenie statycznych połączeń RadSec między serwerami regionalnymi

Głównymi powodami uruchomienia statycznych połączeń RadSec między serwerami regionalnymi jest podniesienie niezawodności działania tego elementu polskiej struktury eduroam i przygotowanie do wdrożenia obsługi dynamicznego wyboru partnera.

Certyfikaty wystawione na potrzeby połączeń statycznych będą później używane również w fazie dynamicznej i dlatego od razu powinny mieć postać akceptowaną w europejskiej usłudze eduroam.

Po wystawieniu certyfikatów dla serwerów regionalnych pracujących na oprogramowaniu radsecproxy, zmiana połączeń na RadSec będzie wymagała bardzo prostej modyfikacji konfiguracji. Najtrudniejszym elementem tej fazy będzie zorganizowanie procedury wystawienia certyfikatów. Certyfikacja będzie realizowana za pośrednictwem Koordynatora.

W przypadku serwerów korzystających z oprogramowania FreeRADIUS konieczna będzie zmiana oprogramowania. Nawet jeżeli do tego czasu oprogramowanie FreeRADIUS będzie wspierało protokół RadSec, to dla serwerów regionalnych będzie zalecane oprogramowanie radsecproxy.

4.1.2. Wdrożenie pilotowego programu dynamicznego wyboru partnera na serwerach regionalnych

Celem tego kroku jest wypróbowanie poprawności działania systemu dynamicznego wyboru partnera oraz skrócenie ścieżki uwierzytelnienia.

W tym modelu instytucja udostępniająca sieć nie musi implementować protokołu RadSec, aby pośrednio z niego korzystać. Zapytanie uwierzytelniające jest kierowane do regionalnego serwera pośredniczącego, a on może nawiązać bezpośrednie połączenie z właściwym serwerem RADIUS (o ile

ten serwer obsługuje dynamiczne połączenia RadSec). W ten sposób liczba serwerów pośredniczących może być ograniczona do jednego.

Ponieważ serwery regionalne będą już miały właściwe certyfikaty, to konieczne będzie jedynie przełączenie ich konfiguracji. Gdyby pojawiły się problemy, to w każdej chwili można będzie wrócić do wcześniejszego modelu.

Oczywiście dodatkowo niezbędne będzie wdrożenie protokołu RadSec w pewnej liczbie instytucji uwierzytelniających. Obsługa RadSec będzie realizowana poprzez dodanie serwera radsecproxy oraz dodanie odpowiednich wpisów do DNS. Szczegóły uruchomienia protokołu RadSec są opisane w opracowaniu [5].

4.1.3. Wdrożenie produkcyjnego systemu dynamicznego wyboru partnera

Doświadczenia zdobyte przy wdrażaniu poprzedniego kroku pozwolą na szybkie uruchamianie połączeń dynamicznych. Podobnie, jak w poprzednim kroku, główną trudnością będzie organizacja wystawiania certyfikatów dla serwerów.

Można również oczekiwać pewnego oporu administratorów przed otwieraniem portu serwera RADIUS – przy połączeniach dynamicznych port musi być otwarty bez żadnych ograniczeń. Zastosowanie dodatkowego serwera radsecproxy, o bardzo ograniczonej funkcjonalności, może być tu bardzo pomocne.

5. Analiza możliwych zagrożeń powodzenia projektu

Na podstawie dotychczasowych doświadczeń polskich i zagranicznych oraz rozmów z administratorami sieci uczelnianych można wyspecyfikować kilka obszarów, w których będą występowały trudności techniczne lub organizacyjne oraz określić możliwe zastrzeżenia administratorów.

5.1. Poprawność obsługi incydentów sieciowych

Korzystanie z usługi eduroam opiera się w dużym stopniu na zaufaniu, że procedury odszukiwania osób odpowiedzialnych za incydenty sieciowe są rzeczywiście tak skuteczne, jak to jest opisane w dokumentach eduroam. Podważenie tego zaufania byłoby bardzo dużym zagrożeniem dla całej usługi i dlatego musi być traktowane bardzo poważnie.

Podstawowym warunkiem działania procedur reagowania na incydenty jest zapewnienie właściwej obsługi logów w instytucjach uwierzytelniających. W tym zakresie niezbędna jest współpraca między operatorami eduroam i administratorami w instytucjach oraz przeprowadzanie okresowych testów.

Niezbędne jest, aby administratorzy eduroam w instytucjach udostępniających sieć zdawali sobie sprawę, że poprawne działanie mechanizmów zaprojektowanych w eduroam jest możliwe tylko pod warunkiem, że instytucje same stosują odpowiednie narzędzia zabezpieczające. W typowej sytuacji incydent sieciowy jest identyfikowany jako zdarzenie w określonym czasie i powiązane z dostępem z pewnego adresu IP. Instytucja udostępniająca sieć musi być w stanie powiązać użycie konkretnego adresu IP w danym czasie z konkretnym adresem MAC. Na tej podstawie możliwe będzie skojarzenie incydentu z odpowiednią sesją uwierzytelnienia i, w konsekwencji, wskazanie instytucji odpowiedzialnej za użytkownika. Kluczowe jest zatem prawidłowe powiązanie adresu IP z adresem MAC, a zatem instytucja udostępniająca sieć nie powinna stosować technologii NAT, a dodatkowo powinna stosować mechanizmy trwałego związania adresu MAC z adresem IP.

Polska Polityka eduroam nie zabrania stosowania NAT, jednak wyraźnie sugeruje, aby tego unikać, właśnie z powodów wymienionych powyżej.

Szersza analiza tych problemów związanych z obsługą incydentów sieciowych jest przedstawiona w opracowaniach: ([10],[11],[12]).

5.2. Nakładanie się zasięgów sieci bezprzewodowych

W przypadku, kiedy dwie instytucje korzystające z eduroam znajdują się bardzo blisko siebie (np. współdzielą jeden budynek) ich sieci bezprzewodowe mogą się nakładać. Jeżeli obie sieci stosują tę

samą nazwę (SSID), to użytkownik będzie losowo przełączany pomiędzy punktami dostępu różnych sieci. Przełączenie do innej sieci będzie wymagało ustawienia nowego adresu IP, co nie dzieje się automatycznie przy każdym uwierzytelnieniu. W efekcie użytkownik będzie tracił łączność na dłuższy czas, a dodatkowo może tracić dostęp do pewnych usług lokalnych (będąc traktowany jako użytkownik lokalny własnej sieci, a za chwilę jako gość w sieci sąsiedniej instytucji).

Opisany problem można rozwiązać na dwa sposoby. Można zastosować różne SSID (tak jak to jest przewidziane w założeniach eduroam, czyli np. `eduroam-ins1`, `eduroam-inst2`) lub uzgodnić wspólną politykę propagacji i ustawiania VLAN-ów, tak by użytkownicy każdej z instytucji oraz goście zawsze trafiali do takiego samego VLAN-u i jednej klasy adresowej. Uzgodnienie takiej wspólnej polityki będzie wymagało współpracy z operatorem regionalnym, ponieważ będzie on musiał zapewnić propagację VLAN-ów oraz wyłączyć alarmy związane z przesyłaniem atrybutów VLAN-owych poprzez serwer regionalny.

5.3. Różne typy szyfrowania

Obecnie coraz powszechniejsze jest ustawianie równolegle dwóch systemów szyfrowania – WPA/TKIP i WPA2/AES. Ten drugi system ma wiele przewag, ale jest dużo słabiej wspierany w sprzęcie. Pozostawia się zatem również WPA/TKIP, aby obsługiwać starsze systemy. Niestety ustawienie obu typów szyfrowania powoduje, że przy automatycznej konfiguracji sieci ustawiane jest szyfrowanie lepsze (a więc WPA2/AES). Użytkownik z tak skonfigurowanym komputerem będzie miał problemy w skorzystaniu z sieci, w której WPA2 nie jest wspierane. Niekiedy będzie musiał dokonać ręcznej korekty ustawień sieci, co dla wielu użytkowników jest zbyt trudne. Dodatkowo, niektóre urządzenia (np. palmtopy pracujące w systemie WM 5.0) w ogóle nie są w stanie korzystać z sieci mającej dwa typy szyfrowania. Ten problem na razie nie ma dobrego rozwiązania, a będzie coraz bardziej narastał, gdyż administratorzy będą chcieli uruchamiać sieci, w których można korzystać ze wszystkich zalet WPA2.

5.4. Anonimowość użytkowników i nadużywanie połączenia gościnnego

Przy tworzeniu eduroam zakładano, że gościnny dostęp oznacza okresowe i stosunkowo sporadyczne korzystanie z sieci na terenie obcej instytucji. Tymczasem, korzystając z anten kierunkowych możliwe jest podłączanie się użytkowników np. z domu i zestawianie de facto stałego radio-łącza. Jeżeli instytucja udostępniająca sieć nie życzy sobie takich zachowań, to należy to wyraźnie zaznaczyć w lokalnym regulaminie eduroam.

Sytuację, w której klient nadużywa łącza trudno jest odróżnić od zwykłego dostępu gościnnego, zwłaszcza gdy klient często zmienia adres MAC i korzysta z uwierzytelniania TTLS z anonimowym identyfikatorem zewnętrznym. Wówczas klient pozostaje faktycznie nierozpoznawalny dla sieci, z której korzysta. Przy częstej zmianie adresu MAC połączenia jednego użytkownika będą wyglądały jak pochodzące od wielu gości. Aby zapobiec takim sytuacjom, w polskim eduroam należy wdrożyć stosowanie atrybutu Chargeable-User-Identity. To rozwiązanie pozwala na przypisanie użytkownikowi identyfikatora, który będzie przekazywany w pakietach Access-Accept. Nikt, poza instytucją macierzystą, nie ma możliwości by poznać tożsamość użytkownika na podstawie tego identyfikatora, ale instytucja udostępniająca sieć ma możliwość, aby wiązać ze sobą połączenia nawiązywane przez tego samego użytkownika. Dzięki temu istnieje możliwość zliczania ruchu generowanego przez jednego użytkownika i reagowania np. gdy przekracza przyjęte wielkości transferu danych. Znajomość identyfikatora przypisanego przez instytucję macierzystą bardzo ułatwi rozwiązywanie problemów z łącznością oraz ew. incydentów.

5.5. Status instytucji udostępniającej sieć

Niektórzy administratorzy sieci uczelnianych wyrażają obawy, że udostępnienie sieci gościnnej nakłada na nich obowiązki rejestracji ruchu wynikające z Prawa Telekomunikacyjnego. Te wątpliwości mogą być rozwiane wyłącznie poprzez ekspertyzę prawną, która powinna być wykonana jako jeden z elementów wdrożenia usługi.

5.6. Brak pełnej informacji o użytkowniku

Pojawiają się obawy, że udostępnienie sieci bez posiadania pełnej informacji o użytkowniku może narazić instytucję na pozwy cywilne lub problemy ze strony organów ścigania. W tej sprawie należy wyraźnie podkreślić, że logi posiadane przez instytucję udostępniającą sieć oraz informacje zapewniane poprzez strukturę eduroam są w stanie dostarczyć dowodów na to, że ew. naruszenie prawa nastąpiło w wyniku działania użytkownika pochodzącego z konkretnej instytucji. Ta instytucja jest, z kolei, zobowiązana do posiadania zapisów pozwalających na wskazanie konkretnej osoby. Fakt, że instytucja udostępniająca sieć nie ma dostępu do informacji które mogą być uważanie za dane osobowe lub dane chronione w myśl przepisów prawa telekomunikacyjnego, należy uznać za zaletę architektury eduroam.

6. Harmonogram wdrożenia struktury regionalnej

Zadanie	data zakończenia
Przygotowanie koncepcji z uwzględnieniem specyfiki sieci miejskich	30.09.2008
Faza I – uruchomienie serwerów regionalnych	31.10.2008
Faza II – wdrożenie RadSec	otwarte
statyczne połączenia między serwerami krajowymi i regionalnymi	31.12.2008
pilotowe wdrożenie połączeń dynamicznych	28.02.2009

Materiały towarzyszące

[1] eduroam-PIONIER; Polska Polityka eduroam (regulamin usługi eduroam), http://www.eduroam.pl/polityka

[2] eduroam-PIONIER; Wzór umowy dotyczącej pełnienia funkcji Regionalnego Operatora eduroam, w przygotowaniu

[3] eduroam-PIONIER; Deklaracja chęci korzystania z usługi eduroam, http://www.eduroam.pl/polityka

[4] eduroam-PIONIER; Deklaracja świadczenia usługi eduroam przez regionalnego Operatora eduroam, http://www.eduroam.pl/polityka

[5] M. Górecka-Wolniewicz; Konfiguracja serwera radsecproxy, http://www.eduroam.pl/Dokumentacja/radsecproxy-1.0.pdf

[6] M. Górecka-Wolniewicz; Instalacja i konfiguracja serwera FreeRADIUS, http://www.eduroam.pl/Dokumentacja/freeradius2-1.0.pdf

[7] M. Górecka-Wolniewicz; Gotowa minimalna konfiguracja serwera FreeRADIUS v. 2 , http://www.eduroam.pl/Dokumentacja/minimum-v2-01.tgz

[8] Konfigurowanie serwera Microsoft IAS,w przygotowaniu

[9] M. Górecka-Wolniewicz; Wykorzystanie technologii RadSec w usłudze eduroam, http://www.eduroam.pl/Dokumentacja/radsec.pdf

[10] M. Górecka-Wolniewicz, Z. Ołtuszyk, T. Wolniewicz; Zasady obsługi incydentów sieciowych w usłudze eduroam, http://www.eduroam.pl/Dokumentacja/incydenty-1.0.pdf

[11] A. Angowski; Zapobieganie samowolnej zmianie IP, http://www.eduroam.pl/Dokumentacja/eduroam_zapobieganie_zmianie_IP.pdf

[12] T. Wolniewicz, M. Górecka-Wolniewicz, Z. Ołtuszyk; Koncepcja sieci uczelnianej włączonej w strukturę eduroam, http://www.eduroam.pl/Dokumentacja/koncepcja_sieci_uczelnianej-1.0.pdf