elektrorevue
ISSN 1213 - 1539

Rok / Year:	Svazek / Volume:	Číslo / Number:
2010	12	5

Aktuální stav projektu eduroam v ČR

The Contemporary state of the Eduroam Project in the Czech Republic

Zbyněk Kocur, Lubomír Vacula, Vladimír Machula

zokl@fel.cvut.cz, vacullub@fel.cvut.cz, machuvla@fel.cvut.cz

Fakulta elektrotechnická ČVUT v Praze

Abstrakt: Tento článek popisuje základní rysy celosvětového akademického projektu eduroam. Čtenář je obeznámen nejen s jeho historií, ale i se současným stavem a jeho dalším vývojem na území ČR.

Abstract: This article describes the basic lines of the worldwide academic project called Eduroam. The reader is apprised either with the whole history, or the contemporary phase and its further development at the area of the Czech republic.

elektrorevue
ISSN 1213 - 1539

Aktuální stav projektu eduroam v ČR

Zbyněk Kocur, Lubomír Vacula, Vladimír Machula

České vysoké učení technické v Praze, Fakulta elektrotechnická
Email: zokl@fel.cvut.cz, vacullub@fel.cvut.cz, machuvla@fel.cvut.cz

Abstrakt *– Tento článek popisuje základní rysy celosvětového akademického projektu eduroam. Čtenář je obeznámen nejen s jeho historií, ale i se současným stavem a jeho dalším vývojem na území ČR.*

1 Úvod

EDUROAM (EDUcation ROAMing) [1] je mezinárodní projekt umožňující snadný roaming mezi zúčastněnými výzkumnými a akademickými organizacemi. Projekt byl založen v roce 2003 pod záštitou asociace TERENA (Trans - European Research and Education Networking Association) [2] a její pracovní skupiny TF - MOBILITY (Task Force on Mobility). Cílem projektu je umožnit snadnou vzájemnou mobilitu uživatelů všech participujících organizací.

2 Současný stav projekt eduroam

2.1 Historie projektu

Počátky spadají do roku 2003, kdy v rámci TF - MOBILITY začal vznikat projekt zaměřený na mobilitu uživatelů. Cílem projektu bylo umožnit volný pohyb mezi jednotlivými akademickými sítěmi vzdělávacích a výzkumných organizací v Evropě. Tento projekt byl později přejmenován na eduroam. Logo projektu je dílem známého českého autora knih Pavla Satrapy a je zobrazeno na obr. 1.

Obrázek 1: Logo projektu eduroam

Jako první se do programu zapojily instituce z Holandska, Finska, Portugalska, Chorvatska a Velké Británie. Později se začaly připojovat další organizace.

V České republice veškeré záležitosti s provozováním eduroamu zajišťuje sdružení CESNET, z.s.p.o. [3]. Toto sdružení bylo založeno vysokými školami a Akademií věd České republiky v roce 1996 za účelem provozu a rozvoje páteřní akademické počítačové sítě. Jednou z participujících univerzit a zároveň velkým přispěvatelem do projektu je rovněž ČVUT (České vysoké učení technické v Praze).

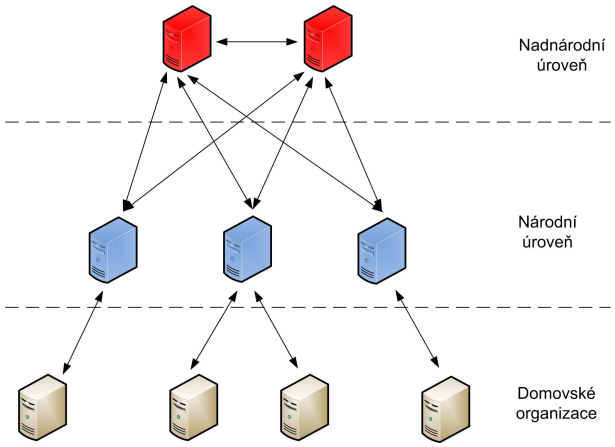
2.2 Principy ověřování

Technologie eduroamu je založena na standardu IEEE 802.1x a hierarchické struktuře RADIUS (Remote Authentication Dial In User Service) proxy serverů. Důvodem hierarchické skladby serverů je princip předávání přihlašovacích údajů uživatele až k jeho domovské organizaci. Každá instituce zapojená do projektu eduroam musí mít vlastní ověřovací server. V rámci jedné země jsou pak všechny ověřovací servery připojených organizací připojeny do národního ověřovacího serveru, který je vždy jeden pro danou zemi. Národní servery, nebo-li NTLR (National Top-Level RADIUS) jsou ve většině případů provozovány národní vzdělávací a výzkumnou organizací dané země. Tyto servery obsahují kompletní seznamy všech institucí zapojených do projektu eduroam v rámci jedné země. Pokud se ale bude snažit přihlásit uživatel z jiné země, je potřeba předat žádost o ověření až na jeho domovskou organizaci. S použitím NTLR to není možné, proto vznikla ještě vyšší vrstva, která zajišťuje předávání informací mezi jednotlivými NTRL. A právě zde se nacházejí tzv. nadnárodní servery. V současné době je eduroam ve světě rozdělen na tři části, Evropskou, Asijsko – Pacifickou a Kanadskou. V Evropě se nacházejí dva nadnárodní servery, tzv. ETLR (European Top-Level RADIUS). Jeden je umístěn v Holandsku a druhý v Dánsku. Pro Asijsko – Pacifickou oblast zajišťují směrování servery v Austrálii a na universitě v Hong Kongu. Kanada má server pouze jeden a ten je umístěn ve Vancouveru. Struktura propojení jednotlivých úrovní ověřovacích serverů je principiálně znázorněna na obr. 2.

2.3 Způsoby ověřování uživatelů

V době vzniku projektu eduroam existovaly celkem tři typy ověřování.

- Webový formulář.
- Přístup pomocí virtuální privátní sítě.
- Protokol IEEE 8021.x.

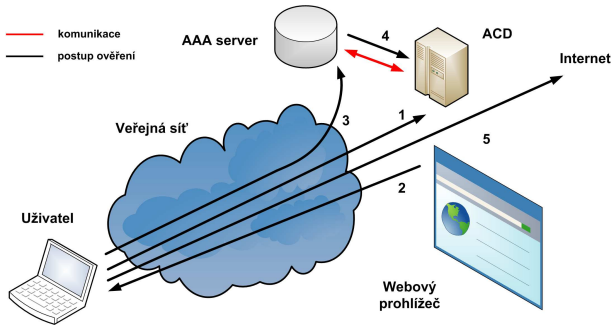


Obrázek 2: Hierarchická struktura ověřovacích serverů

2.3.1 Webový formulář

Architektura ověřování pomocí webu je velice jednoduchá. Ze strany uživatele je potřeba pouze webový prohlížeč schopný zobrazit přihlašovací stránku. Zde uživatel vyplní své přihlašovací údaje. Funkce ověřování jsou umístěny na okraji sítě. Zde se nachází ACD (Access Control Device), které blokuje veškerý síťový provoz, který pochází od neautorizovaných uživatelů.

Když se uživatel pokusí přihlásit do takovéto sítě, obdrží nejprve od DHCP (Dynamic Host Configuration Protocol) serveru IP (Internet Protocol) adresu, ale není schopen odesílat ani přijímat žádná data mimo tuto síť. Proto se musí nejprve ověřit pomocí webového formuláře. Uživatel tedy otevře webový prohlížeč a zadá libovolnou adresu. ACD rozpozná HTTP (HyperText Transfer Protocol) připojení a přesměruje uživatelův prohlížeč na ověřovací stránku. Zde uživatel zadá ověřovací údaje, které ACD ověří. Pokud je ověření úspěšné, tak ACD změní nastavení firewallu a umožní uživateli přístup do Internetu. Pokud proběhne ověření neúspěšně, zobrazí se znovu ověřovací stránka. Pro lepší bezpečnost se doporučuje používat HTTPS (HyperText Transfer Protocol Secure). Princip funkce je znázorněn na obr. 3.

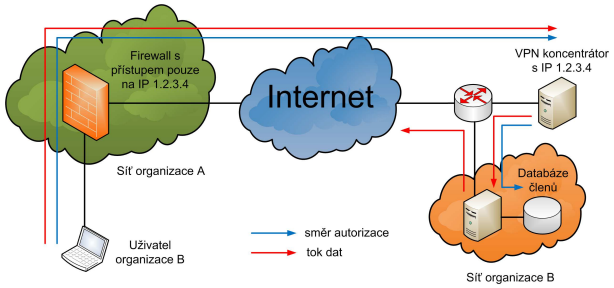


Obrázek 3: Ověření uživatele pomocí webového formuláře

2.3.2 Přístup pomocí virtuální privátní sítě

Princip virtuální privátní sítě, dále jen VPN (Virtual Private Network), je založen na vytvoření virtuální sítě mezi jednotlivými počítači, bez ohledu na to, kde se ve skutečnosti fyzicky nacházejí. Ve výsledku se tedy chovají přesně tak, jako by byly umístěny v jedné společné síti. Uživatel si zažádá server o vytvoření tunelu, ten příjme jeho žádost a ověří jej pomocí přístupového jména a hesla. Pokud je ověření úspěšné, vytvoří se mezi serverem a uživatelem šifrovaný tunel pro přenos dat. Server slouží jako přístupový bod k Internetu a navenek se připojený uživatel tváří, jako by byl připojen přímo k tomuto serveru. Více počítačů připojených k jednomu serveru pak vytváří samotnou virtuální síť.

Jedna z možností implementace ověřovaní uživatele pomocí VPN může vypadat následovně. Síť, ze které se chce cizí uživatel připojit na Internet je oddělena od běžné místní sítě a obsahuje firewall. Ten má předem definovanou určitou množinu VPN bran, ke kterým povolí připojení. V praxi je pro každou spolupracující organizaci přiřazena jedna brána. Uživatel tedy naváže spojení se serverem své domovské organizace, kde se ověří vůči domovské databázi a vytvoří se tak mezi nimi šifrovaný tunel. Komunikace mezi serverem a uživateli probíhá pouze v tomto tunelu. Veškerá komunikace jdoucí ven z tunelu vychází ze serveru. Princip je zobrazen na obr. 4.



Obrázek 4: Přístup pomocí virtuální privátní sítě

2.3.3 Protokol IEEE 802.1x

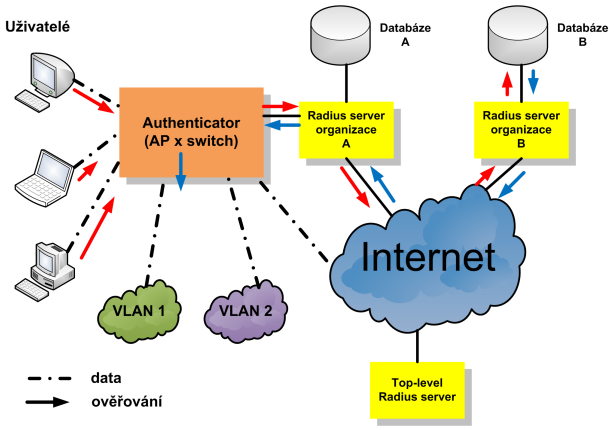
IEEE 802.1x je standard pro autorizaci mezi uživatelem a ACD. Protokol pracuje na druhé vrstvě modelu OSI (Open Systems Interconnection). Ověřování pomocí tohoto protokolu lze použít nejen pro pevné sítě (LAN - Local Area Network), ale i pro bezdrátové sítě (WLAN - Wireless Local Area Network). Veškerá komunikace mezi klientem a ověřovacím serverem je zabezpečena pomocí šifrování.

Struktura ověřování pomocí protokolu 802.1x se skládá ze tří částí. Základním prvkem je RADIUS server. Pokusí-li se uživatel přihlásit na síť, skončí jeho žádost právě na RADIUS serveru. Ten na základě připojené databáze rozhodne, zda uživateli přístup umožní (domácí uživatel), nebo jeho žádost přepošle dál (cizí uživatel).

Uprostřed celého řetězce se nachází ACD, nebo-li Autenticator. Toto zařízení je schopné pracovat s druhou vrst-

vou OSI modelu. V závislosti na druhu přenosového média lze použít přepínač technologie Ethernet, nebo bezdrátový přístupový bod technologie IEEE 802.11 (Wi-Fi). Každý připojený uživatel má přidělen svůj vlastní port. Základní funkcí zařízení je právě ovládání jednotlivých portů, v závislosti na výsledku ověření. V případě úspěšného ověření odešle RADIUS server informaci o povolení přístupu na síť. ACD následně přepne daný port do pozice otevřeno. V opačném případě je port přepnut do pozice zavřeno.

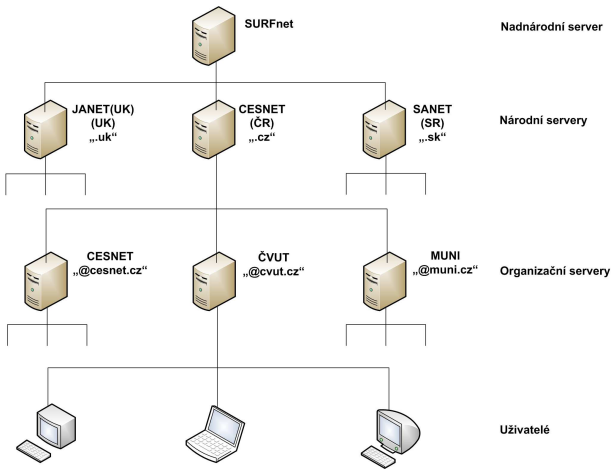
Na úplném konci se nachází připojované zařízení. Aby mohl být proces autentizace umožněn musí být koncové zařízení, většinou síťová karta, kompatibilní s protokolem 802.1x. Princip ověřování pomocí 802.1x je znázorněn na obr. 5.



Obrázek 5: Ověření uživatele pomocí protokolu IEEE 802.1x

Remote Authentication Dial In User Service, známější však pod zkratkou RADIUS je síťový protokol, který umožňuje centralizovaný přístup, autorizaci a správu uživatelských účtů. Po ověření je protokol také schopen jednotlivým uživatelům přidělovat různá práva, podle toho do které kategorie jsou zařazeni. Tato schopnost se nazývá AAA (Athentication, Authorization and Accounting).

Právě hierarchická struktura RADIUS serverů hraje klíčovou roli při ověřování uživatelů. Každá organizace zapojená do projektu eduroam musí mít svůj vlastní RADIUS server, který je schopný ověřit domácí uživatele. Tyto uživatelské účty mohou být uloženy přímo na serveru nebo na jiném zařízení a server využívat pouze jako rozhraní. Všechny RADIUS servery organizací v rámci jedné země musí být připojeny k národnímu RADIUS serveru. Ten slouží jako rozcestník a předává žádosti o ověření mezi jednotlivými organizacemi. Uživatelské údaje jsou složeny ze jména ve tvaru *„username@realm“* a hesla. Jako realm se volí doména domácí organizace, tedy například pro ČVUT je to *„cvut.cz“* Český národní RADIUS server dokáže přesměrovat veškeré požadavky na ověření v rámci domény *„*.cz“*. Stejně jako v rámci jedné země, tak i všechny národní RADIUS servery jsou připojeny k tzv. top-level RADIUS serveru, ten přesměrovává informace mezi jednotlivými zeměmi. V rámci Evropy je top-level RADIUS server provozován společností SURFnet v Holandsku. Celé schéma je znázorněno na obr. 6.



Obrázek 6: Topologie sítě eduroam na ČVUT

2.3.4 Současný způsob ověřování

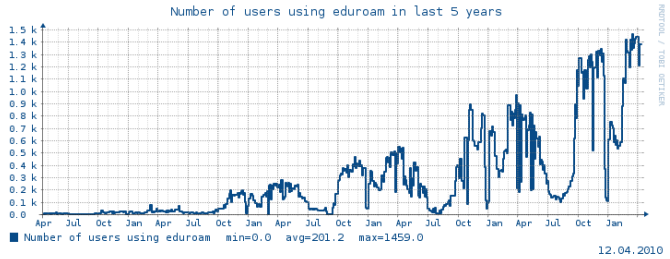
Dnes již VPN ani webový formulář nepatří mezi podporované způsoby ověřování v rámci projektu eduroam. Tyto dvě metody ověřování byly definovány společně s protokolem 802.1x při samotném vzniku projektu. Už tehdy se ale počítalo s jejich postupným odstraněním, a to hlavně z důvodu menšího zabezpečení a horší škálovatelnosti oproti protokolu 802.1x. V době vzniku projektu nebyl ještě protokol 802.1x dostatečně rozšířen a chyběla také jeho podpora. Jak ze strany uživatelů, tak ze strany výrobců síťových zařízení. Z tohoto důvodu bylo nutné definovat jiné způsoby ověření a tak umožnit rychlejší rozšíření projektu na jednotlivé organizace. Dnes již ale doba pokročila, a proto se usoudilo, že toto dočasné řešení není potřeba a bylo oficiálně vyřazeno z roamingové politiky (European Eduroam Confederation Policy). Jako jediný podporovaný způsob ověřování nadále zůstává protokol 802.1x. Na všech připojených organizacích tedy postupně dochází k ukončování sítě eduroam-simple. Na některých organizacích však došlo k přeměně stávajícího eduroam-simple na samostatné místní bezdrátové sítě. Musí však být splněny dvě podmínky. SSID (Service Set Identifier) sítě nesmí obsahovat slovo eduroam a databáze uživatelů musí být vedena odděleně od databáze eduroamu.

3 Aktuální stav projektu eduroam v ČR

Jak již bylo napsáno v úvodu, je projekt eduroam zastoupen v České republice sdružením CESNET. Toto sdružení se primárně stará o provoz páteřní akademické sítě. Poslední generace této sítě nese název CESNET2. Mezi další projekty patří také projekt eduroam. CESNET provozuje národní RADIUS server a umožňuje tak roaming na národní úrovni. Připojit do projektu se může jakákoliv

vzdělávací, či vědecká organizace, která je připojena do sítě CESNET2. To je ovšem pouze jedna z mnoha podmínek. Podmínky nutné pro připojení jsou podrobněji popsány v tzv. roamingové politice [4]. Každá připojená organizace je povinna dodržovat aktuální verzi této politiky, v opačném případě jí hrozí vyloučení z programu. Konečné rozhodnutí o připojení však záleží vždy na správci federace, pro Českou republiku tedy společnosti CESNET.

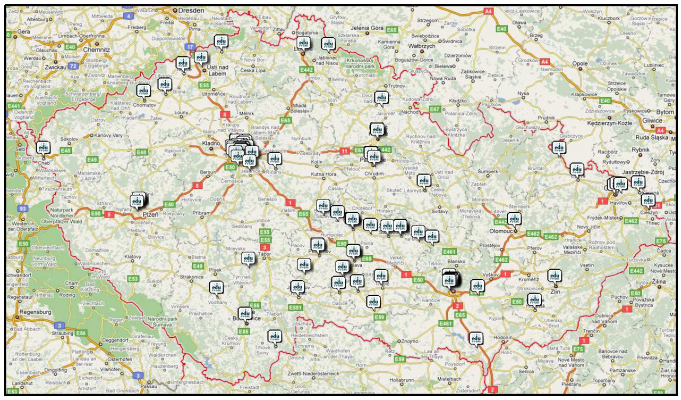
Česká republika se do projektu eduroam zapojila v roce 2004, kdy byl spuštěn pilotní provoz. Rok od roku se do projektu zapojovalo čím dál tím více organizací a zároveň s tím také rostl počet jeho uživatelů. Na obr. 7 lze vidět počty roamujících uživatelů v rámci ČR za období pěti let.



Obrázek 7: Počty roamujících uživatelů v ČR za pět let

3.1 Ústavy zapojené do projektu

V současné době je do projektu na území České republiky zapojeno celkem 34 organizací, které lze vidět na obr. 8. Úplný seznam participujících organizací lze nalézt na stránkách projektu eduroam [5].



Obrázek 8: Topografické zobrazení připojených organizací do projektu eduroam na území ČR

3.2 Služby provozované v rámci projektu

Díky velmi kvalitní páteřní síti CESNET je konektivita do sítě Internet velmi rychlá a stabilní. Připojení uživatelé obdrží rovněž veřejnou IP adresu. Tyto vlastnosti vedou k nasazení dalších služeb, které mohou uživatelé využít. Kromě běžného přístupu do akademické sítě a skrze ní do Internetu lze přes síť eduroam provozovat IP telefonii známou pod označením VoIP (Voice over IP) [6, 7]. Uživatel vybavený mobilním hlasovým terminálem v podobě VoIP Wi-Fi telefonu se může během hovoru pohybovat a to bez výpadku spojení. Nutným předpokladem pro tento druh mobility je vhodně nastavená bezdrátová síť.

Služby projektu eduroam jsou využitelné i v klasických sítích založených na metalických a optických vedeních, jak již bylo napsáno výše. Jedninou nutnou podmínkou je kompatibilita s protokolem 802.1x. Mnoho univerzit a výzkumných organizací využívá autentizační možnosti eduroamu a na pevných sítích v učebnách a to nejen na běžném metalickém Ethernetu, ale i na jeho optické variantě [8, 9].

4 Připojení do sítě eduroam

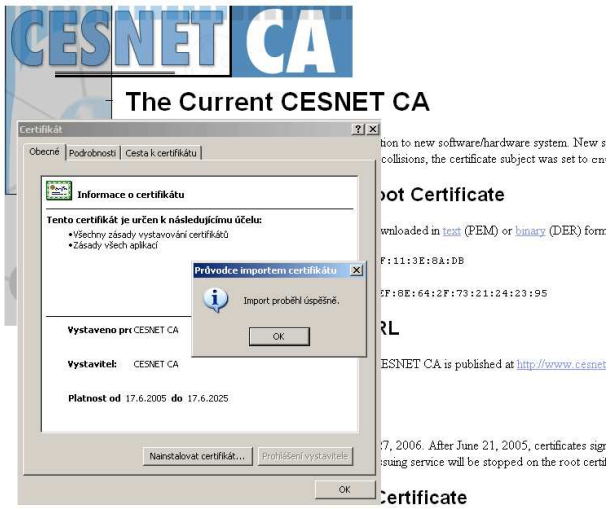
Samotné používání sítě eduroam uživatelem je komfortní a jednoduché. Uživatel po provedení počáteční konfigurace nepotřebuje provádět jakékoliv další zásahy. Konfigurace spočívá jednak v nastavení základních parametrů spojení a zejména potom v nastavení bezpečnostních prvků. Konfigurace konkrétních síťových adaptérů a jejich obslužného software se může značně lišit, proto uvádíme popis konfigurace v operačních systémech Microsoft Windows pomocí interních systémových nástrojů a v systému GNU Linux pomocí univerzálních konfiguračních postupů. K úspěšnému připojení do sítě eduroam je zapotřebí vhodný hardwarový prostředek. Výčet ověřených zařízení a další informace o jejich kompatibilitě jsou uvedeny na webové stránce [10]. Obecně je od použitelného adaptéru vyžadována podpora protokolu 802.1x, dynamických WEP (Wired Equivalent Privacy) klíčů a 128 bitová délka WEP klíče. Konkrétní způsob instalace hardwarového vybavení by měl být uveden v příslušné dokumentaci k zařízení.

4.1 Konfigurace v operačním systému Microsoft Windows

Pro jednotlivé verze operačního systému Microsoft Windows se konfigurace liší pouze ve vzhledu jednotlivých dialogů a mírně odlišnému rozložení ovládacích prvků. Problém s připojením do sítě eduroam se může objevit u verze Windows 98 a starší, které ještě neobsahují kvalitní podporu zabezpečených protokolů pro síťovou komunikaci. Úspěch zde závisí na software a ovladačích dodávaných s hardwarem. V případě verze XP je vhodné mít nainstalovaný servisní balíček verze 3. U novějších systémů jsou veškeré potřebné komponenty již v systému implementovány.

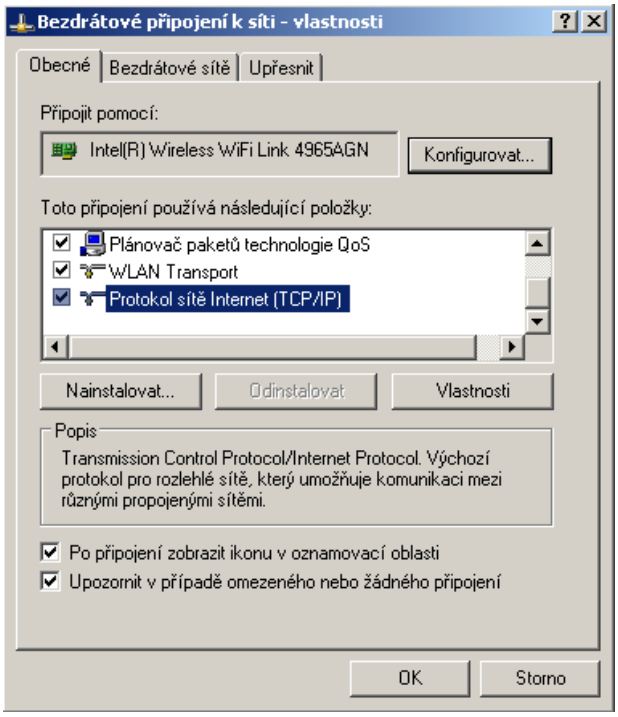
Před samotnou konfigurací je nejprve nutno získat certifikáty ověřovacích serverů. Potřebné certifikáty lze získat z implementační dokumentace dané instituce, která síť eduroam provozuje, případně od její uživatelské podpory. Pro příslušné RADIUS servery v rámci Českého vysokého učení technického je certifikační autoritou CESNET CA [11]. Z jejich webových stránek lze příslušné kořenové certifikáty

stáhnout a následně nainstalovat, tak jak je uvedeno na obrázku 9.



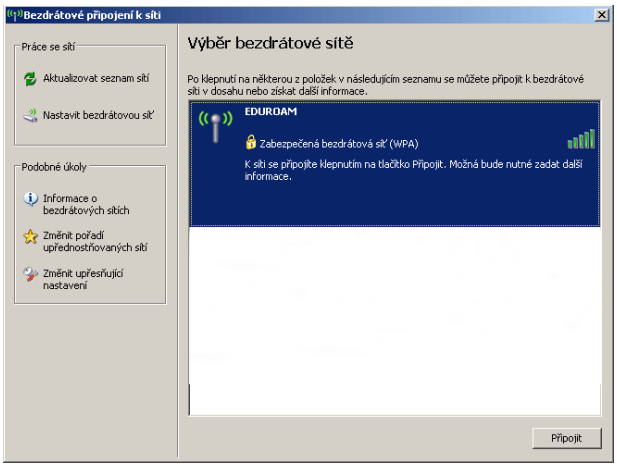
Obrázek 9: Dialog instalace kořenového certifikátu

Následuje konfigurace samotného připojení. Důležitým předpokladem je plně funkční hardwarové rozhraní. Nejprve si otevřeme dialog konfigurace příslušného síťového rozhraní (okno *Bezdrátové připojení k síti*). V tomto okně musí být přítomná a aktivní položka *Protokol sítě Internet (TCP/IP)* jako na obrázku 10.



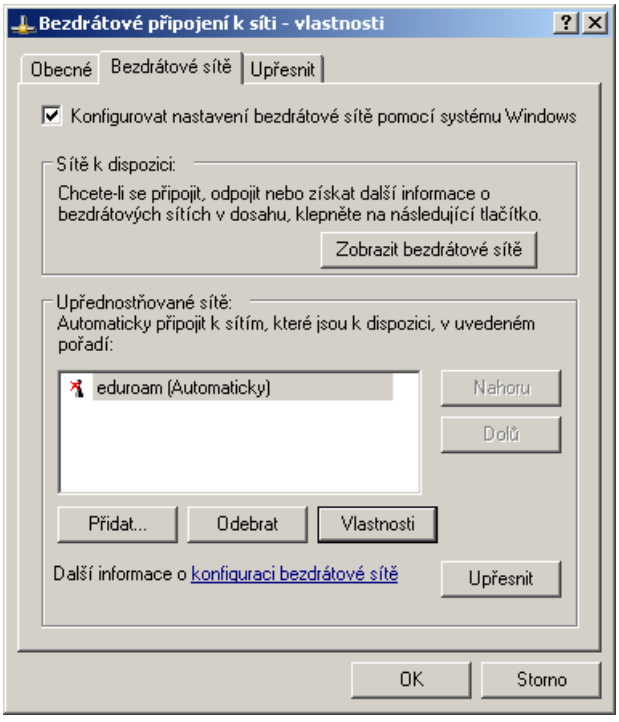
Obrázek 10: Protokoly používané systémem pro připojení

Pokud zde tato položka není, je třeba jí nainstalovat. V tuto chvíli můžeme začít nastavovat samotný přístup do sítě. V dialogu *Bezdrátové připojení k síti* vybereme síť s názvem ***eduroam*** jak je znázorněno na obrázku 11.



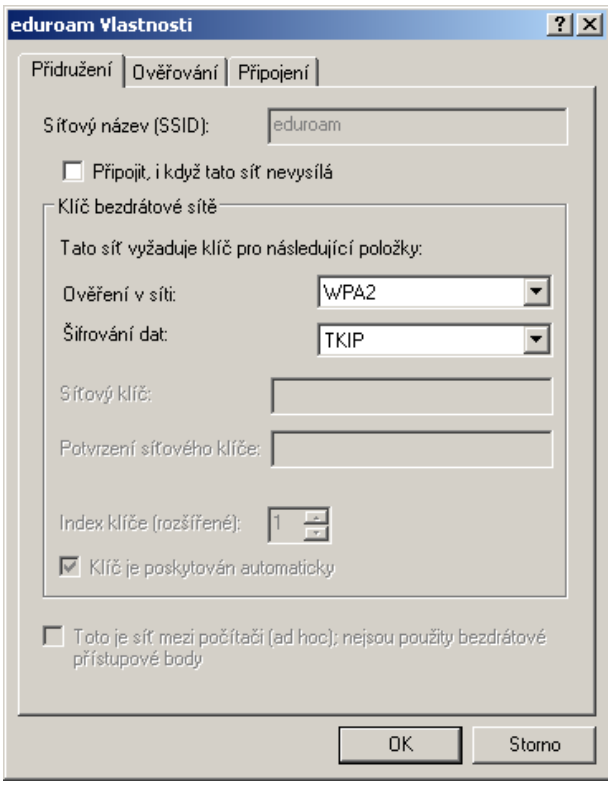
Obrázek 11: Výběr bezdrátové sítě pro přípojení

Parametry zabezpečení se tímto krokem nastaví na základní hodnoty a je potřeba je doladit. Pomocí *Změnit upřesňující nastavení* získáme podrobnější konfigurační dialog, který je uveden na obrázku 12 a následně upravíme zmiňované parametry.

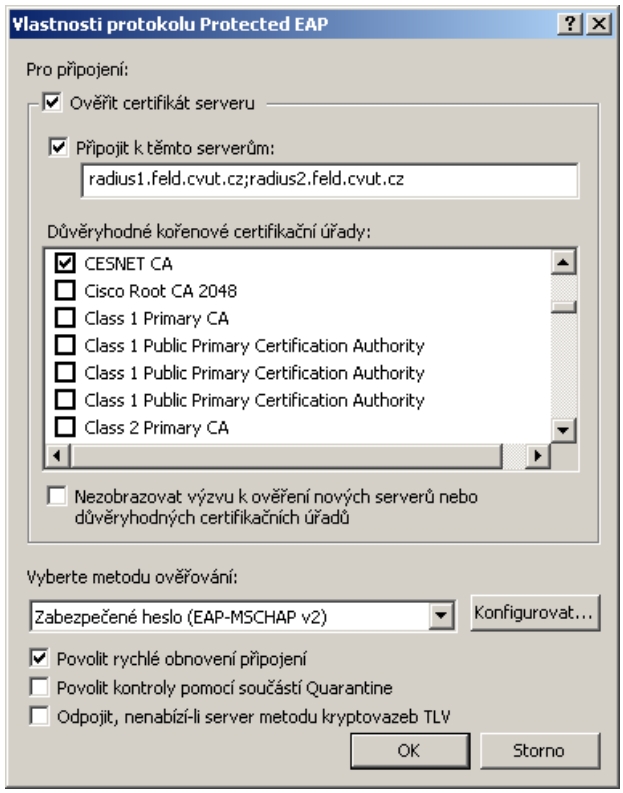


Obrázek 12: Upřesňující nastavení připojení do sítě eduroam

Ověření v síti nastavíme na hodnotu WPA případně WPA2 a šifrování dat na hodnotu TKIP nebo AES pokud to daná síť podporuje viz obrázek 13.



Obrázek 13: Nastavení šifrování spojení se sítí eduroam



Obrázek 14: Výběr kořenového certifikátu a definice adres ověřovacích serverů RADIUS

Na další záložce nastavíme typ protokolu na PEAP (Protected Extensible Authentication Protocol) a vybereme nastavení jeho vlastností jak je znázorněno na obrázku14.

Důležité je zapnout volbu **Ověřit certifikát serveru** a *Připojit k těmto serverům*. Zde uvedeme ověřovací RADIUS servery organizace, která je pro nás zřizovatelem připojení do sítě eduroam. Musíme také vybrat příslušný certifikační úřad, který poskytl kořenový certifikát. Posledním parametrem je *Způsob ověření*, který je třeba nastavit na hodnotu *Zabezpečené heslo (EAP-MSCHAP v2)*. Potvrdíme všechny volby a můžeme zahájit připojení do sítě eduroam. Při připojování se systém zeptá upozorněním v oznamovací oblasti na zadání přihlašovacích údajů. Po klepnutí na toto upozornění se otevře dialog pro uživatelské jméno a heslo. Uživatelské jméno se zadává ve tvaru *„username@realm“*. Po zadání by mělo být navázáno spojení do sítě a proces konfigurace je hotov. Žádné další kroky již nejsou potřeba ani v případě přechodu do jiných organizací.

4.2 Konfigurace v operačním systému GNU Linux

Operačních systémů typu Linux existuje mnoho variant. V našem případě se zaměříme na použití ve variantě Debian a s použitím komponenty WPA_Supplicant. Pro připojení lze využít i dalších nástrojů a k jejich konfiguraci je třeba prostudovat příslušnou dokumentaci. V našem případě se jednotlivé bezdrátové sítě, ke kterým se chceme připojovat definují v konfiguračním souboru /etc/wpa_suplicant.conf. Přesné umístění tohoto souboru se může u jednotlivých typů distribucí lišit. Tento konfigurační soubor má mnoho voleb, které jsou popsány v dokumentaci. Na příkladu uvedeme pouze část týkající se parametrů připojení do sítě eduroam. Definice bude vypadat následovně:

```
network={
    priority=1
    ssid="eduroam"
    scan_ssid=1
    key_mgmt=WPA-EAP
    eap=PEAP
    identity="eduroam_jmeno@realm"
    password="eduroam_heslo"
    ca_cert="/etc/ssl/certs/cesnet-ca.pem"
    altsubject_match="DNS:radius1.feld.cvut
        .cz;DNS:radius2.feld.cvut.cz"
    phase1="peaplabel=0"
    phase2="auth=MSCHAPV2"
}
```

K úspěšnému připojení je potřeba instalace kořenového certifikátu certifikační autority, která vydala certifikát k RADIUS serveru. V našem případě se jedná opět o CESNET CA, jako je uvedeno v konfiguraci pro operační systémy Microsoft Windows. Certifikát je třeba nainstalovat do příslušného úložiště v závislosti na použité distribuci

Linuxu. Více informací lze získat v příslušné dokumentaci k systému.

Po nastavení parametrů WPA Supplicantu provedeme připojení na rozhraní např. wlan0 generickým příkazem:

#wpa_supplicant −Dwext −iwlan0 −c/etc/wpa_supplicant.conf

Proběhla-li autentifikace korektně, je třeba ještě získat síťovou IP adresu pro rozhraní pomocí DHCP klienta například tímto příkazem:

#dhcpcd wlan0

Pokud distribuce systému Linux podporuje WPA_Supplicant ve svých spouštěcích skriptech není většinou tento krok potřeba. Samozřejmě existují další možné způsoby konfigurace v operačním systému Linux, například pomocí grafických nástrojů a různých průvodců. Popis takových variant však překračuje rámec tohoto článku a je třeba se obrátit na příslušnou dokumentaci k používaným nástrojům.

5 Závěr

Cílem tohoto článku bylo seznámit čtenáře s aktuálním stavem projektu eduroam na území ČR a osvětlit hlavní principy tohoto projektu. Následně pak na dvou jednoduchých příkladech bylo demonstrováno připojení do sítě eduroam z operačních systému Microsoft Windows a GNU Linux.

Projekt eduroam má na české akademické půdě velmi dlouhou tradici. Z počátku, kdy byl tvořen jen několika přístupovými body, se rozrostl do sítě čítající několik tisíc přístupových bodů s několika desítkami tisíc uživatelů.

Projekt se nadále úspěšně rozvíjí a kromě vysokých škol a výzkumných organizací proniká i do středního a základního školství. S projektem eduroam se lze potkat i v řadě institucí jakými jsou knihovny, nemocnice a různá občanská sdružení.

V současné době se pracuje na návrhu integrace projektu eduroam do struktur Studentské unie ČVUT, která je největší studentskou organizací v ČR s přibližně 6 500 členy.

Poděkování

Příspěvek vznikl v rámci specifického výzkumu FEL, ČVUT v Praze.

Literatura

[1] Projekt eduroam [online]. 2010 [cit. 2010-27-04]. Dostupný z WWW: ⟨http://www.eduroam.org/⟩.

[2] TERENA Association [online]. 2010 [cit. 2010-27-04]. Dostupný z WWW: ⟨http://www.terena.org/⟩.

[3] Sdružení CESNET [online]. 2010 [cit. 2010-27-04]. Dostupný z WWW: ⟨http://www.cesnet.cz/sdruzeni/⟩.

[4] Roamingová politika. Roamingová politika projektu eduroam. Praha: CESNET, z.s.p.o., 14.7.2009. 10 s. Dostupné z WWW: ⟨http://eduroam.cz/doku.php?id=cs:roamingova_politika⟩.

[5] Seznam připojených lokalit [online]. 2010 [cit. 2010-27-04]. Dostupný z WWW: ⟨http://www.eduroam.cz/doku.php?id=cs:pripojene_organizace⟩.

[6] Vozňák, M., Řezáč, F. IP telefonie nejen v akademické síti CESNET2. Semináře Moderní technologie počítačových sítí a embedded systémy pro komunikace,Vydavatel: VŠB Ostrava, 30.3.2009.

[7] Vozňák, M. Voice over IP. Vysokoškolská skripta, 176 stran. Vydavatel: VŠB-TU Ostrava, Dotisk prvního vydání, v Ostravě, září 2009, ISBN 978-80-248-1828-3.

[8] Rozhon, J., Babica, V., Vozňák, M., Macura, L. , Vychodil, J. Wireless IP Phone for the visually impaired, In conference proceedings RTT 2010, pp. 172-175 Velké Losiny, September 8-10, 2010, ISBN 978-80-248-2261-7.

[9] Boháč, L., Bezpalec, P. Komunikace v datových sítích. Cvičení 1. vyd. Praha: Vydavatelství ČVUT, 2006. 151 s. ISBN 80-01-03536-0.

[10] Konfigurace a připojení do EDUROAM [online]. 2010 [cit. 2010-27-04]. Dostupný z WWW: ⟨http://www.eduroam.cz/doku.php?id=cs:uzivatel:uvod⟩.

[11] Certifikační autorita CESNET CA [online]. 2010 [cit. 2010-27-04]. Dostupný z WWW: ⟨http://www.cesnet.cz/pki/crt.html⟩.