

Ráno Eduroamisto, večer takisto

David Antoš, Martin Osovský, Marek Saitl, Václav Lorenc, ÚVT MU

1 Úvod

Od doby, kdy se notebooky a další mobilní zařízení vybavená Wi-Fi (PDA, pokročilé mobilní telefony, ...) staly běžnou výbavou jak vědeckých pracovníků, tak i studentů, a kdy bez připojení k síti téměř nelze pracovat, narážíme na častý problém: jak na cestách připojit zařízení k síti.

Pomineme-li komerční možnosti, jako (nezřídka placené) připojení v hotelích nebo obvykle v zahraničí velmi drahé připojení mobilním telefonem, zbývají kavárny nebo podobné podniky, kde často mívají pro hosty otevřené bezdrátové připojení. Jak se ale připojit k síti v místech, kde pracovat skutečně potřebujeme, na univerzitách a vědeckých ústavech? Jejich sítě bývají často zabezpečené, získávání účtu zdržuje a zatěžuje uživatele i správce a je docela nesystémové. Proto v rámci aktivit sdružení TERENA (přesněji skupiny TF-Mobility and Network Middleware [5]) vznikl projekt Eduroam [1]. TERENA koordinuje projekt celosvětově, národní infrastrukturu ČR spravuje sdružení CESNET. Ústav výpočetní techniky MU zajišťuje provoz poskytovatele identit uživatelů z MU, ve spolupráci s lokálními správci sítí koordinuje zavádění Eduroamu na univerzitě a značné části sítě Eduroam na MU samo spravuje.

Základním účelem Eduroamu je umožnit studentům a zaměstnancům akademických institucí bezplatný přístup k síti, kdekoli je Eduroam dostupný, bezpečně a co možná jednotným způsobem bez nutnosti změny konfigurace jejich počítačů.

Síť Eduroam je dostupná v rostoucím počtu budov MU. Eduroamem postupně nahrazujeme starší bezdrátové připojení, tzv. MUNI-VPN. Oproti MUNI-VPN přináší Eduroam většinou vyšší rychlost připojení a zejména výhodu mobility. MUNI-VPN je čistě lokální přístupový mechanismus MU a ve střednědobém horizontu přestane být podporován.

Tento článek se zaměří spíše na uživatele, jehož technické detaily příliš nezajímají, a také na



Obrázek 1: Logo Eduroamu

zcela praktické rady v prostředí MU. V sekci 6 se zmíníme také o novince: do Eduroam sítě MU je možno dovolit přístup hostům, kteří nemají ve své domovské organizaci správce identit pro síť Eduroam. Pro ty, kteří by se rádi dozvěděli více o technických principech implementace Eduroamu, můžeme odkázat na starší přehledový článek ve Zpravodaji [6], případně na webové stránky projektu [1, 3], které obsahují podrobný technický popis. Pro uživatele z MU je hlavním zdrojem informací o Eduroamu a jeho nastavení portál [2].

2 Jak použít Eduroam

Pro připojování k síti Eduroam je třeba mít nainstalován program pro autentizaci, tzv. suplikant. Ve většině moderních operačních systémů je přímo součástí systémové instalace (zejména uživatelé Windows od verze XP výše nebudou mít problém). Aktuální návody pro řadu operačních systémů naleznete na univerzitních stránkách [4].

Jak proběhne připojení k bezdrátové síti, to si ukážeme na příkladu. Předpokládejme, že uživatel z MU je zrovna v budově ČVUT v Praze. Na svém notebooku, jako jednu z dostupných bezdrátových sítí, vybere síť „eduroam“. Pro jednoduchost hovoříme o notebooku, ale principy se týkají většiny zařízení s Wi-Fi. V konfiguraci suplikantu má zadáno uživatelské jméno ve tvaru uco@eduroam.muni.cz a sekundární heslo z ISu¹. Není třeba se obávat, že uživatel zadává tyto údaje v cizí síti – jméno a heslo se zadává pouze do konfigurace uživatelova stroje. Je to daleko bezpečnější, než třeba přes webový formulář. Heslo se ověří vůči serverům MU. Tyto autentizační servery (říká se jim také poskytovatelé

¹Sekundární heslo v ISu lze nastavit na stránce <https://is.muni.cz/auth/system/heslo.pl>

identit) příslušné vzdálené síti potvrdí, že uživatel skutečně pochází z MU, a tudíž je oprávněn síť použít. Uživatel pak dostane do sítě přístup a může ji využívat v souladu s její lokální politikou. Bezdrátové spojení notebooku uživatele s příslušným přípojným místem je navíc kompletně šifrováno, takže nehrozí odposlech samotného bezdrátového provozu v blízkosti uživatelova notebooku.

Z pohledu uživatele proběhne připojení zcela shodně, ať je uživatel kdekoli v dosahu nějaké sítě Eduroam. Třebaže síť Eduroam nejčastěji používá jméno (SSID) „eduroam“, není tomu tak vždy. Bývá nicméně zvykem, že toto slovo v názvu alespoň obsahuje, často se používá forma „eduroam-xyz“, kde „xyz“ je zkratka poskytující instituce (například eduroam-fi na Fakultě informatiky MU).

Jméno sítě by nemělo být skryté (tj. má být přístupovým bodem oznamováno, konfigurační program jej pak umí vypsat), nicméně pokud ve výpisu dostupných sítí uživatel žádné nadějně jméno nenalezne, lze alespoň zkusit připojení k síti „eduroam“. Národní politika Eduroamu dovoluje, že toto jméno oznamováno být nemusí. K síti, jejíž jméno není oznamováno, se lze připojit, pokud toto jméno a další potřebné údaje známe předem a do konfigurace je zadáme.

Je vhodné si uvědomit, že připojení není anonymní. Vzdálená síť uchovává o uživateli uživatelské jméno, přidělenou adresu a dobu, kdy byl uživatel připojen. Pokud se uživatel dopustí nějakého bezpečnostního incidentu, správci sítě musí incident řešit. Protože ale o uživateli mají jen velmi strohé údaje, budou kontaktovat správce domovské organizace uživatele (které organizaci uživatel patří se pozná z uživatelského jména), kterému sdělí uživatelské jméno a popis incidentu. Správce domovské organizace je politikou Eduroamu zavázán ke spolupráci a zodpovídá za vyřešení incidentu včetně odpovědi správci vzdálené sítě.

Přestože celý princip fungování sítě Eduroam vypadá triviálně, za uživatelskou jednoduchostí a transparentností se skrývá košatá struktura autentizačních serverů, které si šifrované autentizační údaje předávají podle dosti složitých pravidel.

3 Používám Eduroam na MU

Všichni, kdo jsou oprávněni používat Eduroam, jej mohou používat i na MU. To se samozřejmě týká i vlastních zaměstnanců a studentů univerzity. Provoz v této síti není omezen firewallem a platí v ní stejná pravidla použití jako v dalších sítích MU.

Aktuální seznam míst pokrytých sítí Eduroam v prostorách MU najdete na webu ÚVT [2]. Na tomto webu také najdete formulář pro hlášení problémů. Kromě kontaktování správců elektronickou cestou je možné osobně navštívit Celouniverzitní počítačovou studovnu, jejíž operátoři také umí pomoci s konfigurací mobilního zařízení a nastavení lze přímo ve studovně otestovat.

4 Časté problémy

Než se uživatel obrátí na správce s žádostí o řešení problému, je vhodné, aby si zkontroloval základní nastavení. Často se chybuje v zadání uživatelského jména, to je pro uživatele z MU ve formátu „učo@eduroam.muni.cz“, kde „učo“ je identifikační číslo osoby, které najdete například v ISu. Uživatelé často zapomínají na ono „@eduroam.muni.cz“, to je ale nezbytné, aby autentizační servery poznaly, kterou instituci kontaktovat pro ověření identity uživatele.

Další častou chybou je použití jiného než sekundárního hesla z ISu (např. primárního). Primárním heslem se uživatel přihlašuje k ISu a dalším základním systémům MU, jako například k systému Inet. Sekundární heslo slouží pro stahování pošty, přístup k Eduroamu, přístup k federovaným webům atd.

Pokud se připojení k síti systematicky nedaří, je dobré ověřit celé nastavení podle návodu na [2], problém někdy bývá v nastavení jiného šifrovacího protokolu. Typickým projevem chyby v nastavení šifrování v systémech rodiny Windows je, že se Eduroam v seznamu sítí ukáže, ale s červeným křížkem jako nedostupná síť.

Uživatelé si občas stěžují na sníženou rychlost nebo výpadky připojení. Celá infrastruktura přístupových bodů je nepřetržitě monitorována a výpadky jsou řešeny, jak je to jen nejdříve možné. Přesto propustnost přípojných míst není neomezená. Pokud se do posluchárny nahrne sto

studentů s notebooky, všichni se připojí (a často někteří z nich začnou stahovat větší data, jak už to studenti dělávají), už jen samotné principy bezdrátového připojení nedovolí, aby pak připojení bylo stejně rychlé, jako když přístupové body sítě nejsou tak zatíženy. Otázka přidání více přípojných míst se samozřejmě převádí na zcela konkrétní částky požadované z univerzitního rozpočtu.

Občas také od uživatelů slýcháme stížnosti typu, že připojení se obnovuje a zase rozpadá, případně že se přenosy dat zasekávají. Obvyklou příčinou je opět bezdrátová technologie. Radiové vlny jsou v budovách pohlcovány a odráženy zejména železobetonovými konstrukcemi. Bezdrátové sítě musí odpovídat průmyslovým standardům a hygienickým normám, proto zvyšování výkonu přípojných míst nepřichází v úvahu. Často postačí se v místnosti přesunout s notebookem o kousek jinam. Autoři tohoto článku mají bohaté zkušenosti s kanceláři ÚVT na Botanické, kde – jako důsledek konstrukce budovy – vznikají desítky centimetrů široká pásma s nevalným signálem těsně vedle míst s velmi dobrým připojením. Tyto problémy vznikají prakticky ve všech v současnosti používaných sítích. Na výraznější zlepšení si budeme nejspíš muset počkat na další generaci těchto technologií. Rozhodně ale s problémy se signálem bezdrátových sítí není od věci kontaktovat lokálního správce, může pomoci i přemístění přípojného bodu.

5 Používám Eduroam na MU a chystám se na cesty

Pokud se uživatel z MU chystá na cesty, může se předem podívat, zda je cíl cesty pokryt sítí Eduroam. Portál [3] hned na první stránce obsahuje mapu pokrytí pro ČR. Eduroam je dostupný na mnoha univerzitách nejen v Evropě, ale také v USA, Kanadě, Austrálii a Japonsku. Na portálu [1] je k dispozici mapa pokrytí pro všechny tyto regiony, stačí kliknout na správný region a pak potřebný stát, a postupně se na mapě proklikat až k příslušnému místu – cílové instituci.

Na webových stránkách cílové instituce jsou zveřejněny podrobné instrukce pro uživatele, obsahující informace o použitých jménech (SSID) sítí,

popis prostoru pokrytého bezdrátovým signálem a další informace nezbytné pro úspěšné použití sítě. Stránky také obsahují kontakt na lokální technickou podporu.

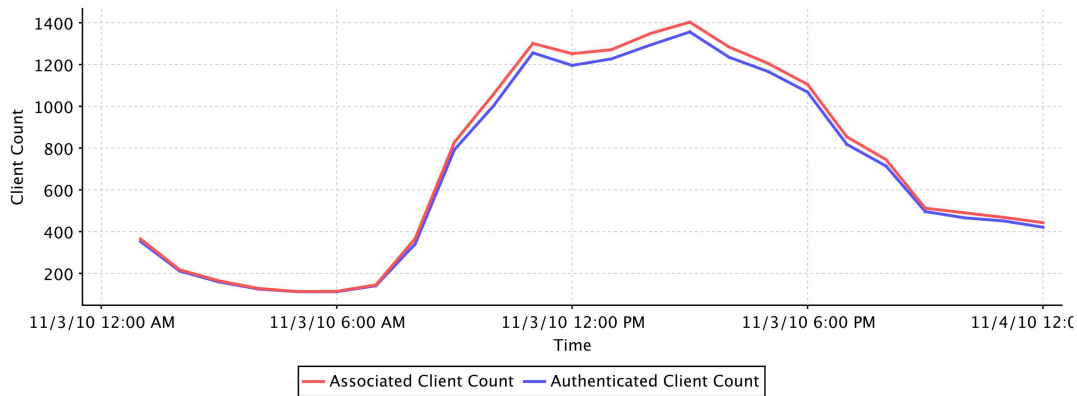
Není od věci si zjistit tyto údaje dříve, než se vypravíme na cestu. Pokud se připojení nezdaří, narazíme na nejslabší místo Eduroamu – velmi složité hledání problému. O postupu při řešení situace, kdy se uživateli nezdaří připojit, vede mezinárodní komunita kolem Eduroamu již několik let vášnivě diskuse, tak vášnivě, že obvykle ani weby s návody neobsahují žádné doporučení pro tento případ. Jak jsme ověřili dotazem u národních koordinátorů sítě Eduroam ze sdružení CESNET, doporučeným postupem pro tyto případy je kontaktovat nejdříve správce z domovské organizace uživatele. Často je nezbytné k tomu použít telefon. Domácí správce ověří, zda přišel ze vzdálené sítě autentizační požadavek a zda byl serverem (poskytovatelem identit) domovské instituce správně zpracován. Pokud je na této straně vše v pořádku, problém bude ve vzdálené síti nebo ve stroji uživatele. Správce z domovské organizace uživatele bude také většinou schopen pomoci i s případnou změnou konfigurace uživatelského stroje, případně alespoň poskytnout kontakt na správce vzdálené sítě (ten je sice na příslušných webových stránkách, ale problémem uživatele je přesně to, že se k síti nemůže dostat).

Místa pokrytá signálem Eduroamu jsou také často označena logem projektu (obr. 1).

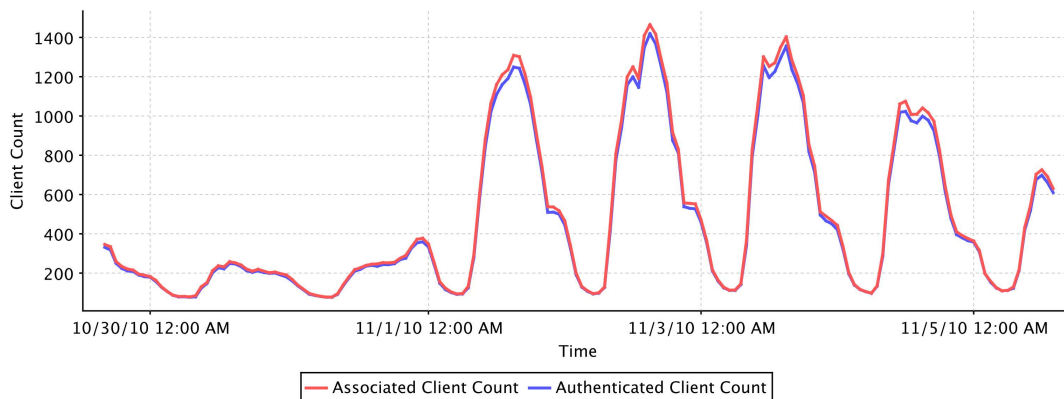
Pokud na cestách narazíte na problém s připojením k Eduroamu, kontaktujte dohledové centrum datových sítí ÚVT na telefonním čísle +420 54949 4241.

6 Mám na MU hosta s notebookem

Jak je z předchozích částí patrné, návštěvníci univerzity přicházející z organizací zapojených do Eduroamu, by s připojením k naší síti neměli mít problém. Co ovšem s těmi, kteří takovou domovskou organizaci nemají, přesto jsou u nás třeba účastníky konference nebo hosty univerzitního hotelu, a potřebujeme jim proto umožnit přístup na síť?



Obrázek 3: Denní průběh počtu klientů na MU



Obrázek 4: Týdenní průběh počtu klientů na MU

Na většině fakult je možné se obrátit na místní laboratoř výpočetní techniky nebo jiné oddělení, které má na starost výpočetní techniku. Pracovníci těchto oddělení jsou oprávněni vytvořit dočasný účet nebo účty s oprávněním přístupu na internet pomocí Eduroamu. Účet platí pouze pro přístup do Eduroam sítě Masarykovy univerzity (tj. nikoli do sítí jiných organizací) a vytváří se na omezenou dobu.

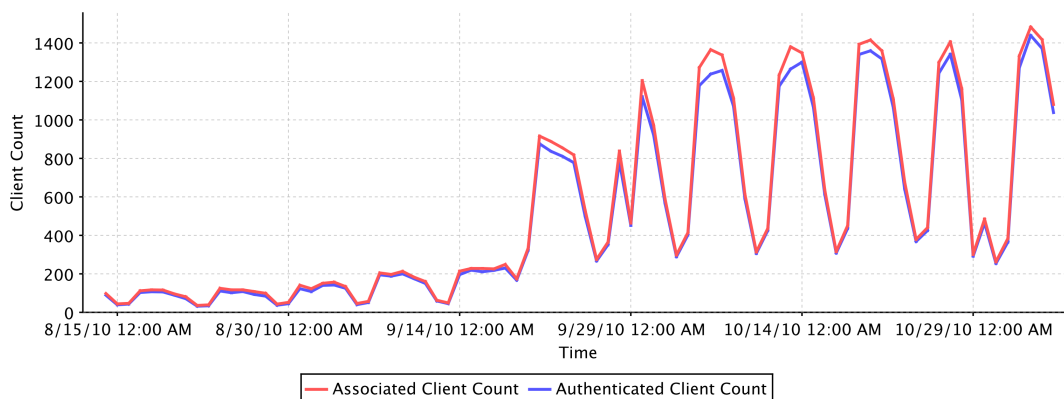
Oprávněné osoby mají za tímto účelem k dispozici aplikaci vyvinutou na ÚVT (obr. 2, která umožňuje

- vytvořit jeden nebo několik účtů ručně (informace o osobě, pro kterou je účet vytvářen, se zadávají do systému),
- vytvořit účty hromadně ze souboru (CSV nebo Excel),
- vytisknout po vytvoření účtu kartičku s vytištěným přihlašovacím jménem, případně jménem a příjmením a heslem,

- přiřadit do nějakého data nebo odebrat účtu jedno nebo více z nabízených oprávnění (obvykle Eduroam nebo VPN),
- změnit heslo existujícího účtu.

Bezpečnostní politika MU vyžaduje, aby hostující uživatelé bezdrátových sítí byli identifikovaní a dohledatelní. Proto je nejvhodnější dočasné účty vytvářet přímo pro konkrétní osoby. Pokud to není možné, lze vytvořit i sadu anonymních účtů, pořadatelé příslušné akce pak ovšem zodpovídají za to, že evidují, které osobě přiřadili příslušné uživatelské jméno. Při pořádání konference nebo workshopu jsou nicméně seznamy účastníků obvykle známy předem, takže příslušné účty lze také předem připravit. Detailní informace a podporu poskytnou pracovníci laboratoří výpočetní techniky.

System pro správu identit hostů je vyjma Eduroamu možno použít i pro zpřístupnění dalších služeb, jako jsou webové stránky, přihlašování na počítače a podobně.



Obrázek 5: Dlouhodobý průběh počtu klientů

7 Jak je síť Eduroam na MU využívána

Oddělení datových sítí ÚVT aktuálně spravuje celkem 376 přístupových bodů bezdrátové sítě Eduroam. Počty připojených klientů kolísají v závislosti na tom, zda běží semestr, během týdne i během dne.

Guest Manager

[Nový účet](#)
[Vytvořit více účtů](#)
[Účty](#)
[Hledat](#)
[Tresty](#)
[Můj účet](#)
[Nápověda](#)
[Odhlásit](#)

Account Information

Účet: Guest133182 id: 1401

Atributy

Křestní jméno:

Příjmení:

Adresa:

Datum narození:

Emailová adresa:

Popis:

Typy

VPN

Platnost do:

EduroamInternal

Platnost do:

Obrázek 2: Správce hostujících identit

Grafy na obrázcích zachycují typický vzor počtu uživatelů. Červená čára je počet klientů, kteří se připojí k přístupovým bodům sítě, modrá čára pak zobrazuje ty, kteří se úspěšně autentizují, tj. byli do sítě vpuštěni. Je patrné, že ne všichni připojení klienti se také autentizovali, mezi ně typicky patří zařízení, která nemají Eduroam nakonfigurovaný, nicméně jsou nastavena tak, že se zkusí připojit k nějaké dostupné síti. Obr. 3 zachycuje typický den v semestru, je zjevné, že průběh odpovídá obvyklé pracovní době akademických pracovníků i době, kdy se obvykle koná výuka. Ve špičkách je připojeno kolem 1400 uživatelů. Obr. 4 znázorňuje typický týdenní průběh (graf začíná víkendem). Je patrná tendence studentů (i tvůrců rozvrhu) mít většinu přednášek začátkem pracovního týdne. Na grafu 5 je jasně patrný vliv prázdnin a náběhu semestru.

Množství přenášených dat silně koreluje s počtem klientů. Datové toky ve špičkách dosahují 200 Mbit/s, přitom přibližně dvě třetiny až čtyři pětiny tohoto toku směřují k uživatelům (download). Uživatelé Eduroamu se tedy chovají srovnatelně s uživateli pevně připojených strojů.

8 Shrnutí

Síť Eduroam, oproti jiným způsobům připojování k bezdrátové síti univerzity, přináší zásadní výhodu uniformního přístupu k síti na stále rostoucím množství institucí a míst jak v Evropě, tak i na jiných kontinentech. Od roku 2005, kdy se tato technologie začala na MU zavádět, se neustále zvětšuje počet přípojných bodů i na naší univerzitě. Jsme přesvědčeni, že výhody této technologie výrazně převažují nad poněkud složitější prvotní konfigurací a předpokládáme, že se Eduroam po dlouhou dobu udrží jako dominantní metoda přístupu k síti pro studenty a pracovníky v akademické sféře.



Tento článek byl podpořen projektem „Vzdělávání akademických pracovníků v oblasti e-Infrastruktur“ (CZ.1.07/2.3.00/09.0074). Tento projekt je spolufinancován z Evropského sociálního fondu a státního rozpočtu České republiky.

Literatura

- [1] Eduroam. <http://www.eduroam.org/>.
- [2] Eduroam na MU. <http://eduroam.muni.cz/>.
- [3] Eduroam.cz. <http://www.eduroam.cz/>.
- [4] Návod pro konfiguraci na stránkách Eduroamu MU. <http://eduroam.muni.cz/doku.php?id=navody>.
- [5] TERENA TF-Mobility and Network Middleware. <http://www.terena.org/activities/tf-mobility/>.
- [6] Michal Procházka. Všichni chceme Eduroam! *Zpravodaj ÚVT MU*, XVII(2):4-6, 2006. ISSN 1212-0901. □