FreeRADIUS podrobněji

aneb „K této síti se nelze připojit 2“

Pavel Valach

7. října 2017

RADIUS?

- AAA protokol
  - Authentication, Authorization, Accounting
  - Autentizace, Autorizace, Účtování (evidence)

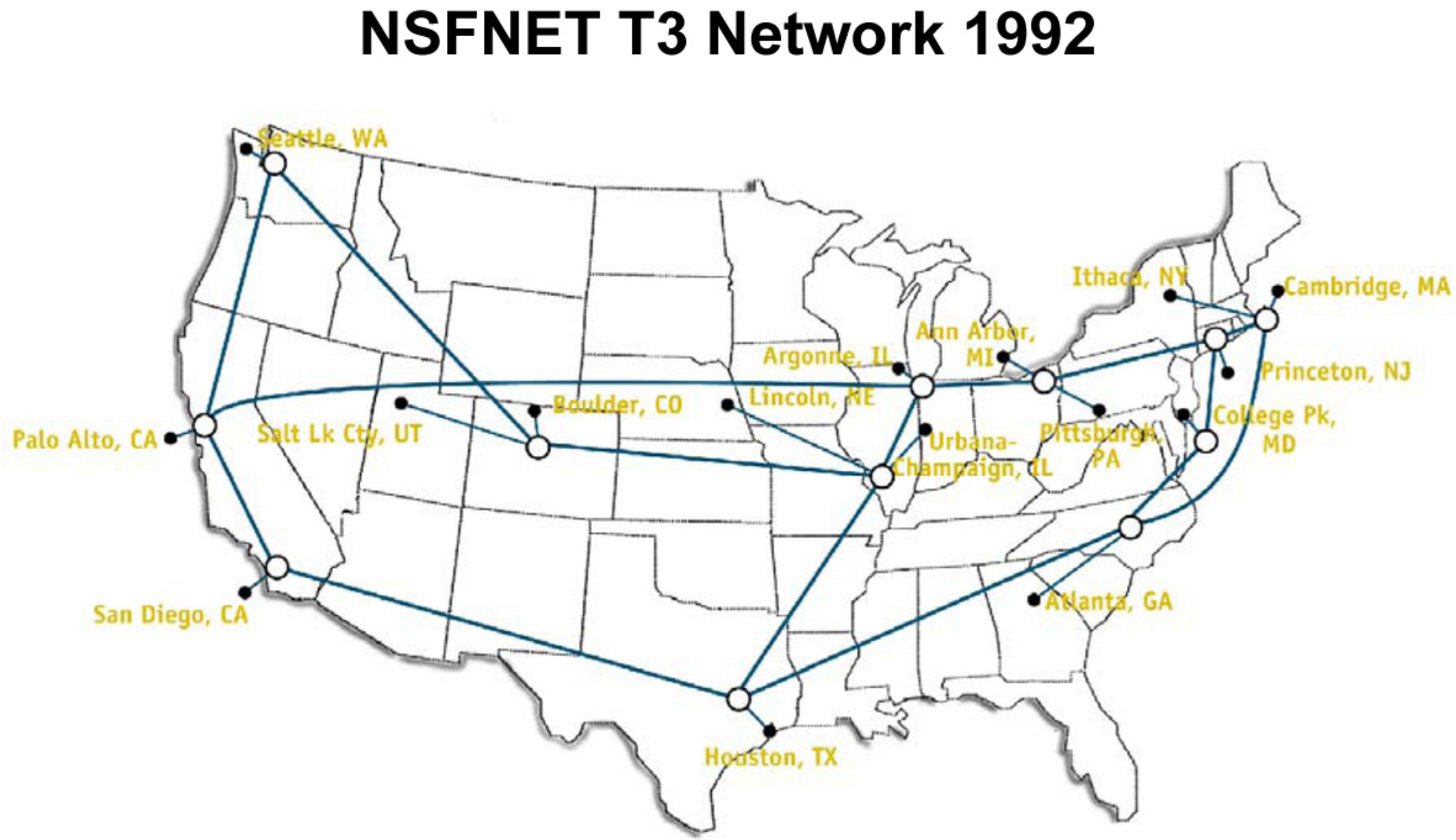
Historie protokolu

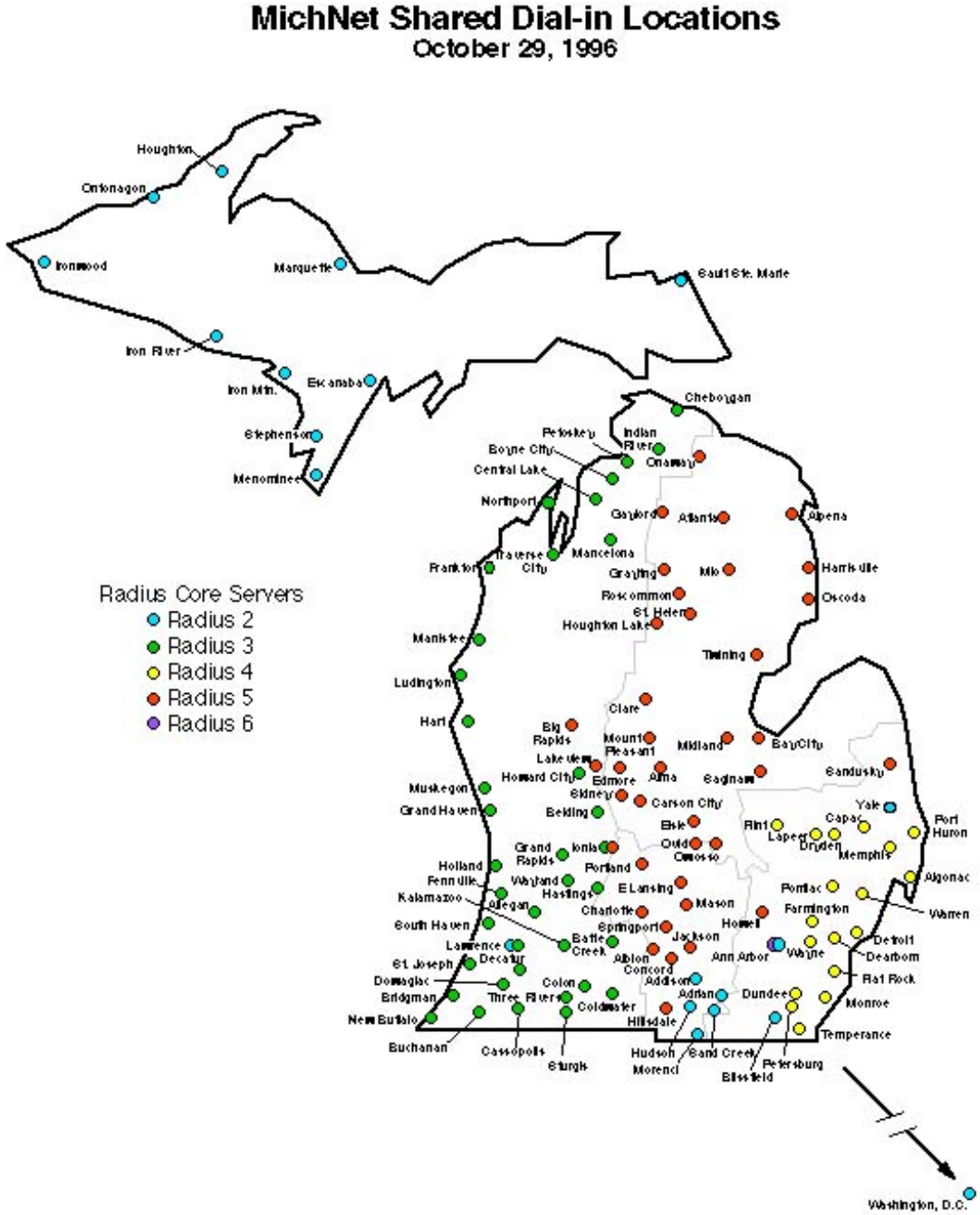
- První uživatelé - počátkem 90. let univerzity v Michiganu
- **Incentiva pro vznik:** přechod z proprietární sítě na protokol TCP/IP a zachování tehdejšího distribuovaného přihlašování napříč univerzitami
- Klíčová slova: ARPAnet, distributed dial-in
- RADIUS zprvu komerčně nabízený protokol v rámci řešení Livingston Portmasters
- 1992 working group pro přípravu standardu
- 1994 Internet Draft, 1997 RFC 2039, 2000 RFC 2865

Historie protokolu

- První uživatelé - počátkem 90. let univerzity v Michiganu
- **Incentiva pro vznik:** přechod z proprietární sítě na protokol TCP/IP a zachování tehdejšího distribuovaného přihlašování napříč univerzitami
- Klíčová slova: ARPAnet, distributed dial-in
- RADIUS zprvu komerčně nabízený protokol v rámci řešení Livingston Portmasters
- 1992 working group pro přípravu standardu
- 1994 Internet Draft, 1997 RFC 2039, 2000 RFC 2865

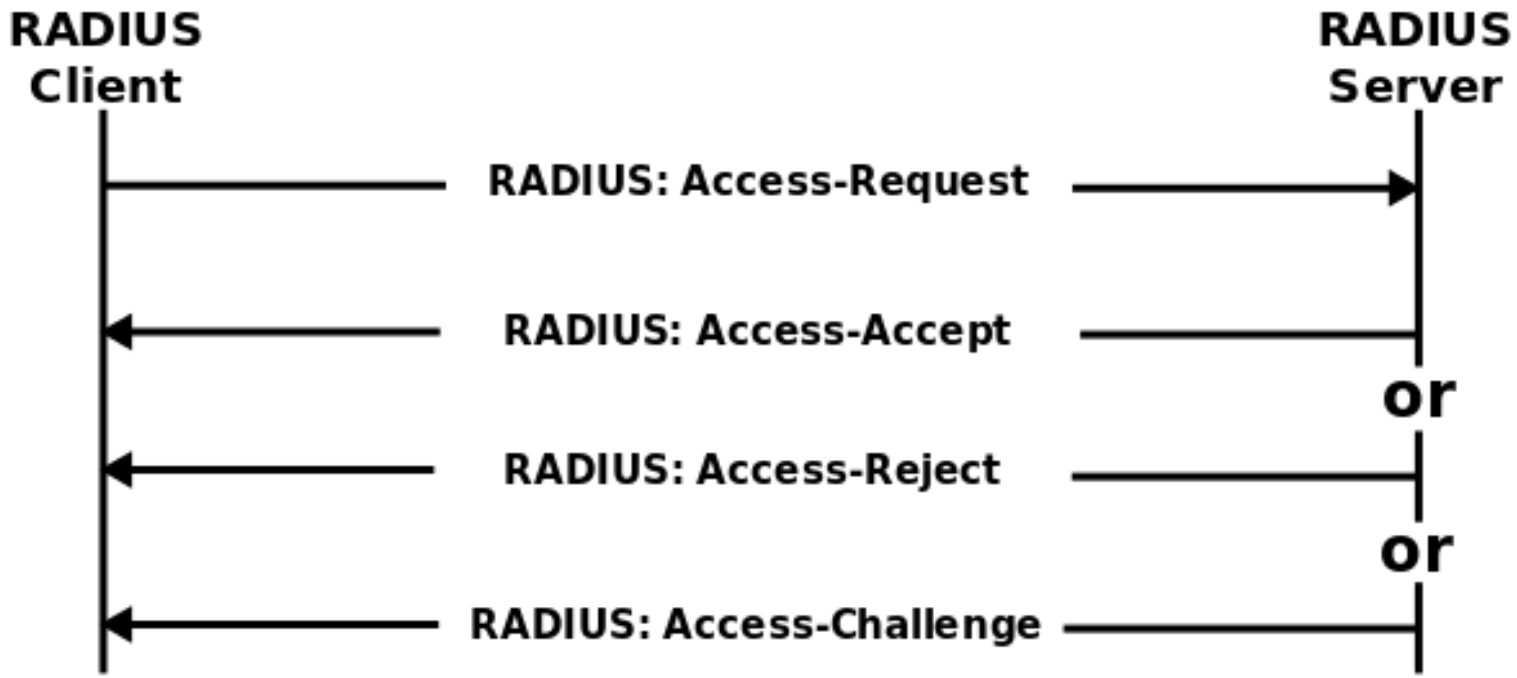
NSFnet v roce 1993




MichNet Shared Dial-in Locations
October 29, 1996
Houghton
Ontonagon
Ironwood
Marquette
Sault Ste. Marie
Iron River
Iron Mtn.
Escanaba
Stephenson
Menominee
Cheboygan
Petoskey
Indian River
Boyne City
Central Lake
Northport
Gaylord
Atlanta
Alpena
Traverse City
Manistee
Frankfort
Mancelona
Grayling
Mio
Harrisville
Roscommon
Oscoda
St Helen
Houghton Lake
Manistee
Ludington
Hart
Clare
Big Rapids
Mount Pleasant
Midland
Bay City
Lake City
Howard City
Edmore
Alma
Saginaw
Sandusky
Muskegon
Grand Haven
Sidney
Carson City
Yale
Belding
Flint
Capac
Port Huron
Grand Rapids
Ionia
Portland
Holland
Fennville
Wayland
Hastings
E Lansing
Pontiac
Algonac
Kalamazoo
Otsego
Charlotte
Mason
Farmington
Warren
South Haven
Springport
Jackson
Howell
Detroit
Lawrence
Battle Creek
Albion
Ann Arbor
Wayne
Dearborn
St Joseph
Decatur
Concord
Addison
Flat Rock
Dowagiac
Colon
Adrian
Dundee
Bridgman
Three Rivers
Coldwater
Monroe
New Buffalo
Hillsdale
Buchanan
Cassopolis
Sturgis
Hudson
Sand Creek
Morenci
Blissfield
Petersburg
Temperance
Washington, D.C.
Radius Core Servers
Radius 2
Radius 3
Radius 4
Radius 5
Radius 6

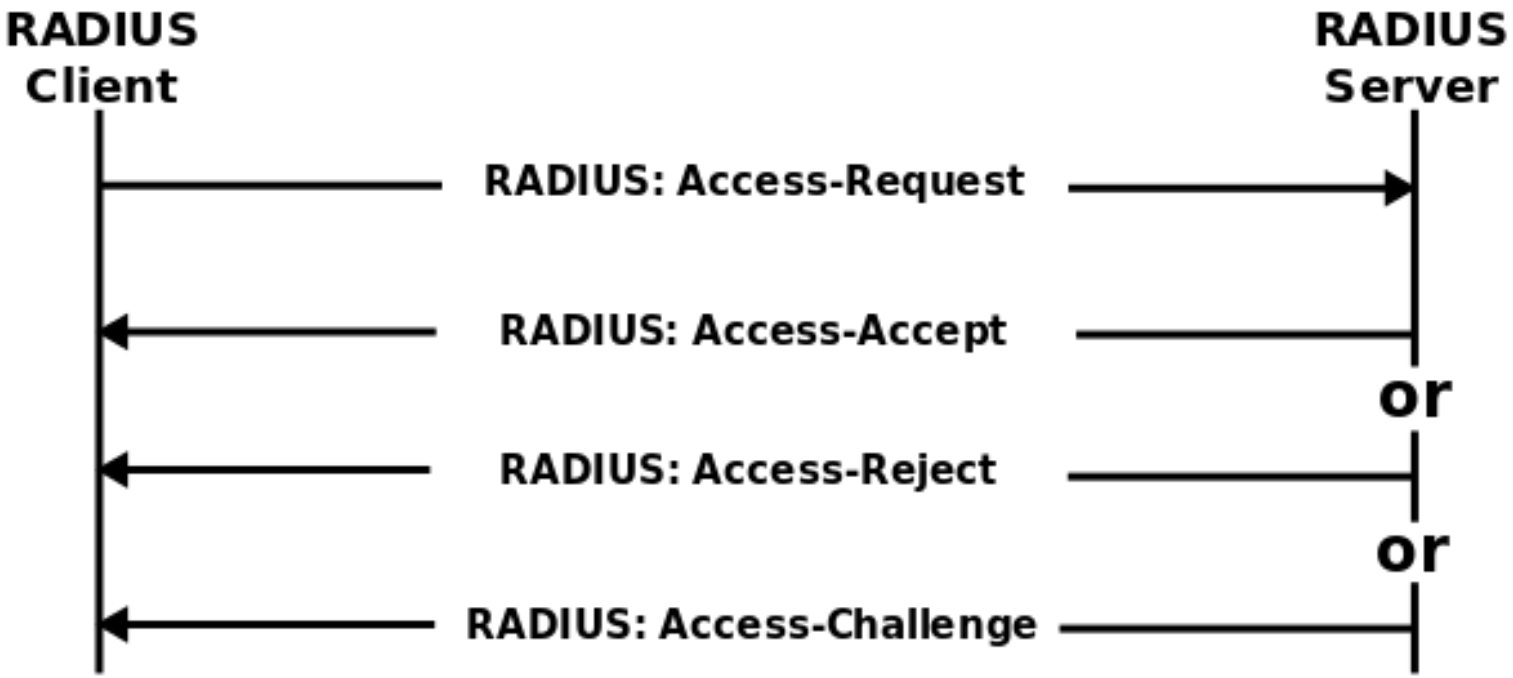
RADIUS

- Základní vlastnosti:
  - Rozšiřitelný protokol
  - Komunikace pomocí UDP, default porty 1812, 1813
  - Sady atributů ve stylu *key-value*
- Podobné protokoly: kupř. TACACS+
- Nástupce: DIAMETER



Podobně pro **accounting**

- `Accounting-Request` →
- ← `Accounting-Response`



Podobně pro **accounting**

- `Accounting-Request` →
- ← `Accounting-Response`

Základní pojmy

- RADIUS server
  - „poskytovatel dat“, autentizační server (koncový bod TLS spojení)
- RADIUS proxy
  - „middle-man“, zprostředkuje autentizaci a autorizaci jinam
- NAS - Network Access Server
  - „prostředník“ k spojení s RADIUS serverem (switch, AP), poskytuje přístup do sítě / ke službě
- Supplicant
  - „klient“ žádající o přístup (wpa_supplicant, Windows EAP klient)

Základní pojmy

- RADIUS server
  - „poskytovatel dat“, autentizační server (koncový bod TLS spojení)
- RADIUS proxy
  - „middle-man“, zprostředkuje autentizaci a autorizaci jinam
- NAS - Network Access Server
  - „prostředník“ k spojení s RADIUS serverem (switch, AP), poskytuje přístup do sítě / ke službě
- Supplicant
  - „klient“ žádající o přístup (wpa_supplicant, Windows EAP klient)

Základní pojmy

- RADIUS server
  - „poskytovatel dat“, autentizační server (koncový bod TLS spojení)
- RADIUS proxy
  - „middle-man“, zprostředkuje autentizaci a autorizaci jinam
- NAS - Network Access Server
  - „prostředník“ k spojení s RADIUS serverem (switch, AP), poskytuje přístup do sítě / ke službě
- Supplicant
  - „klient“ žádající o přístup (wpa_supplicant, Windows EAP klient)

Základní pojmy

- RADIUS server
  - „poskytovatel dat“, autentizační server (koncový bod TLS spojení)
- RADIUS proxy
  - „middle-man“, zprostředkuje autentizaci a autorizaci jinam
- NAS - Network Access Server
  - „prostředník“ k spojení s RADIUS serverem (switch, AP), poskytuje přístup do sítě / ke službě
- Supplicant
  - „klient“ žádající o přístup (wpa_supplicant, Windows EAP klient)

Implementace RADIUSu

- **FreeRADIUS** je nejznámější svobodnou implementací (GPLv2)

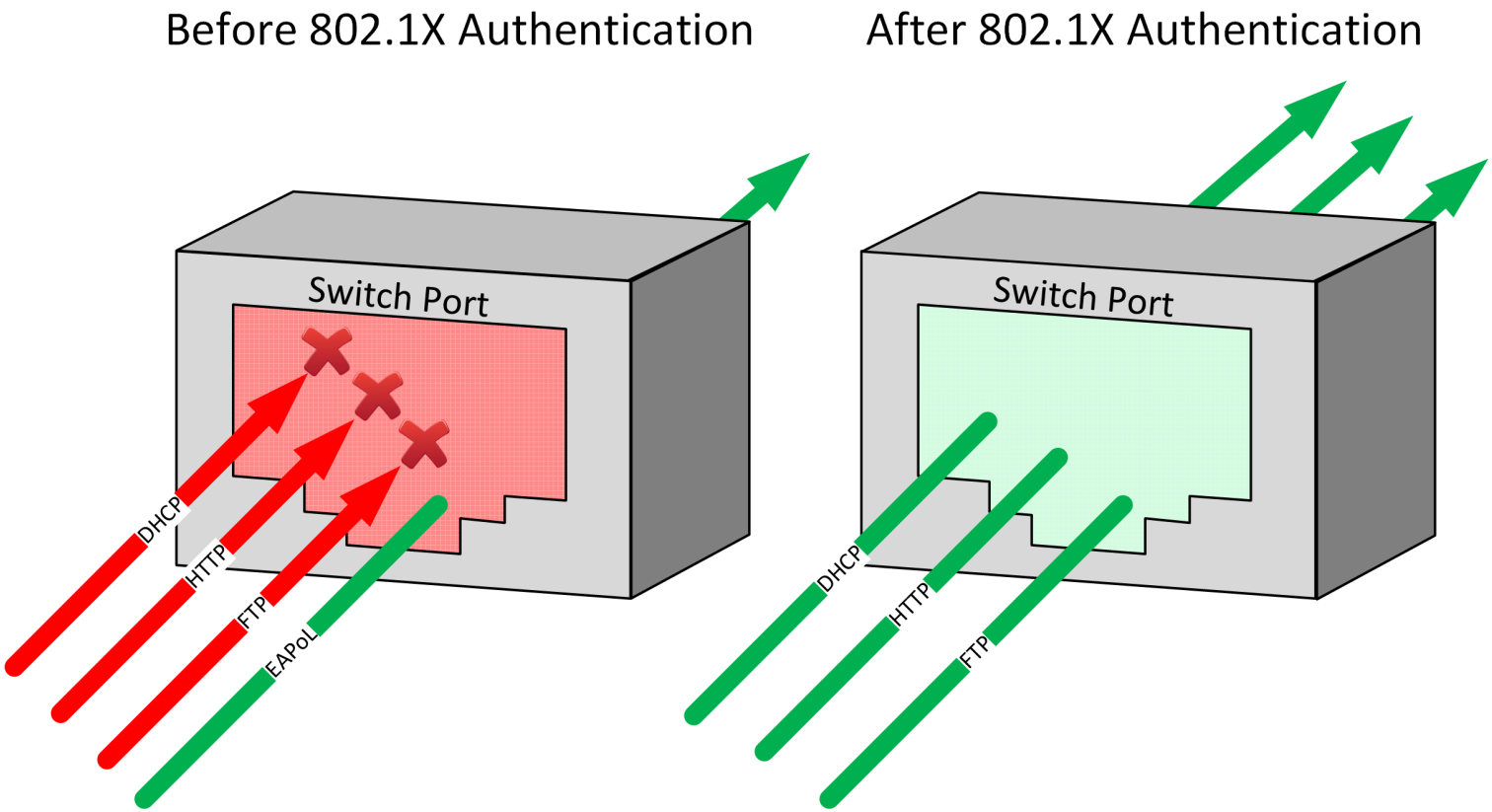
- Komerční alternativa je např. **Radiator**

Implementace RADIUSu

- **FreeRADIUS** je nejznámější svobodnou implementací (GPLv2)

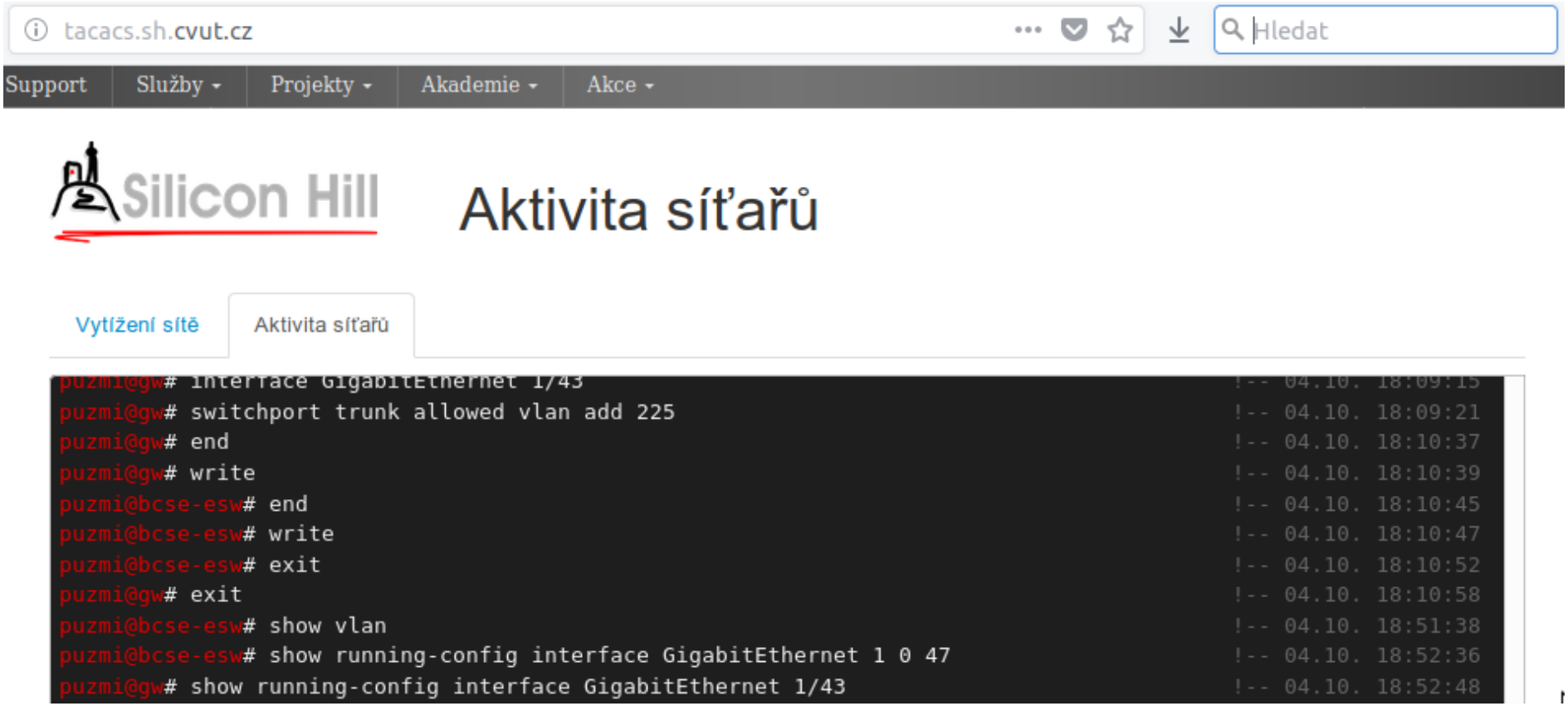
- Komerční alternativa je např. **Radiator**

K čemu AAA protokol na switchi?



https://networklessons.com/wp-content/uploads/2014/10/8021x-port-control.png

K čemu AAA protokol na switchi?



https://tacacs.sh.cvut.cz

K čemu RADIUS na Wi-Fi?

K čemu RADIUS na Wi-Fi?

K čemu WPA2-Enterprise (802.1x) a RADIUS?

- WPA2 s předsdíleným heslem není moc bezpečné
  - heslo jde často velmi snadno zjistit
  - spousta systémů heslo posílá *do cloudu*
  - když zachytíte výměnu klíčů a znáte heslo, **rozšifrujete komunikaci**
- Při použití WPA2-Enterprise se generují unikátní šifrovací klíče
- správně nastavené je ~~poměrně bezpečné~~ o něco málo bezpečnější
- WPA2-Enterprise potřebuje *zdroj autentizačních dat*
  - tím bývá většinou RADIUS server

K čemu WPA2-Enterprise (802.1x) a RADIUS?

- WPA2 s předsdíleným heslem není moc bezpečné
  - heslo jde často velmi snadno zjistit
  - spousta systémů heslo posílá *do cloudu*
  - když zachytíte výměnu klíčů a znáte heslo, **rozšifrujete komunikaci**
- Při použití WPA2-Enterprise se generují unikátní šifrovací klíče
- správně nastavené je ~~poměrně bezpečné~~ o něco málo bezpečnější
- WPA2-Enterprise potřebuje *zdroj autentizačních dat*
  - tím bývá většinou RADIUS server

K čemu WPA2-Enterprise (802.1x) a RADIUS?

- WPA2 s předsdíleným heslem není moc bezpečné
  - heslo jde často velmi snadno zjistit
  - spousta systémů heslo posílá *do cloudu*
  - když zachytíte výměnu klíčů a znáte heslo, **rozšifrujete komunikaci**
- Při použití WPA2-Enterprise se generují unikátní šifrovací klíče
- správně nastavené je ~~poměrně bezpečné~~ o něco málo bezpečnější
- WPA2-Enterprise potřebuje *zdroj autentizačních dat*
  - tím bývá většinou RADIUS server

K čemu WPA2-Enterprise (802.1x) a RADIUS?

- WPA2 s předsdíleným heslem není moc bezpečné
  - heslo jde často velmi snadno zjistit
  - spousta systémů heslo posílá *do cloudu*
  - když zachytíte výměnu klíčů a znáte heslo, **rozšifrujete komunikaci**
- Při použití WPA2-Enterprise se generují unikátní šifrovací klíče
- správně nastavené je ~~poměrně bezpečné~~ o něco málo bezpečnější
- WPA2-Enterprise potřebuje *zdroj autentizačních dat*
  - tím bývá většinou RADIUS server

Instalujeme FreeRADIUS

Gentoo

```
# emerge -v freeradius
```

Debian/Ubuntu

```
# apt-get install freeradius
```

Arch Linux

```
# pacman -S freeradius
```

Fedora

```
# dnf install freeradius
```

Instalujeme FreeRADIUS

Gentoo

```
# emerge -v freeradius
```

Debian/Ubuntu

```
# apt-get install freeradius
```

Arch Linux

```
# pacman -S freeradius
```

Fedora

```
# dnf install freeradius
```

Instalujeme FreeRADIUS

Gentoo

```
# emerge -v freeradius
```

Debian/Ubuntu

```
# apt-get install freeradius
```

Arch Linux

```
# pacman -S freeradius
```

Fedora

```
# dnf install freeradius
```

Instalujeme FreeRADIUS

Gentoo

```
# emerge -v freeradius
```

Debian/Ubuntu

```
# apt-get install freeradius
```

Arch Linux

```
# pacman -S freeradius
```

Fedora

```
# dnf install freeradius
```

Základy konfigurace

- Konfigurační soubory v `/etc/raddb`, popř. `/etc/freeradius/3.0`
- Výchozí nastavení v `/etc/raddb.default`

- Není těžké konfiguraci totálně zvorat! Dělejte malé změny!
- Používejte příkaz `radiusd -X` a zkoušejte

Základy konfigurace

- Konfigurační soubory v `/etc/raddb`, popř. `/etc/freeradius/3.0`
- Výchozí nastavení v `/etc/raddb.default`

- **Není těžké konfiguraci totálně zvorat! Dělejte malé změny!**
- Používejte příkaz `radiusd -X` a zkoušejte

Certifikáty - Na co si dát pozor?

- výchozí self-signed certy jsou dobré na testy
- pro autentizaci přes jméno/heslo použít **EAP-TTLS/PEAP-MSCHAPv2** a certifikát s důvěryhodnou CA
- pro autentizaci klientským certifikátem (EAP-TLS/EAP-TTLS) **vlastní autoritu**
  - Lepší kontrola nad certifikáty a revokacemi

Certifikáty - Na co si dát pozor?

- výchozí self-signed certy jsou dobré na testy
- pro autentizaci přes jméno/heslo použít **EAP-TTLS/PEAP-MSCHAPv2** a certifikát s důvěryhodnou CA
- pro autentizaci klientským certifikátem (EAP-TLS/EAP-TTLS) **vlastní autoritu**
  - Lepší kontrola nad certifikáty a revokacemi

Certifikáty

- složka `certs` - výchozí certifikáty, CA
  - `./bootstrap`
    vygenerujete `server.pem` podepsaný self-signed CA
  - `openssl dhparam -out ./dh 2048`
    vygenerujete DH soubor
  - další info v `README`
- konfigurace v `mods-available/eap`

EAP

- **EAP = Extensible Authentication Protocol**
- data se přenáší ve zprávách `Access-Request` a `Access-Challenge` v atributu `EAP-Message`
- pro účely přihlašování na Wi-Fi se dnes nejčastěji používají
  - EAP-PEAP, MSCHAPv2
  - EAP-TTLS
  - EAP-TLS
  - EAP-SIM *(z nějakého důvodu to občas bývá default)*
- PEAP, TLS i TTLS vytvářejí mezi supplicantem a koncovým RADIUS serverem TLS tunel
  - ověřuje se zde důvěryhodnost CA a hostname, příp. i platnost předloženého klientského certifikátu
  - poté zde probíhají další fáze EAPu (PAP, CHAP, GTC, MSCHAPv2 etc.)

Konfigurace EAP

- v `mods-available/eap`
- PEAP, TLS a TTLS komunikace probíhá přes tzv. `inner-tunnel`, což je ve FreeRADIUSu samostatný server - proto je nutné vlastní přihlášení hodit i tam!

Jak otestovat EAP

```
echo "User-Name=bob@marus.ex,User-Password=loveH4te123,Calling-
    Station-Id=7c:d1:c3:db:fd:f3"
| radclient 127.0.0.1 auth testing123 -x -s
```

Klienti RADIUS serveru (NAS)

- clients.conf
  - client iftest {
  - type = auth | acct | auth+acct
  - ipaddr | ipv4addr | ipv6addr = hostname | localhost
  - secret = TakCca16ZnakuANicSlovnikoveho
  - nas_type = viz /usr/share/freeradius/dictionary.* / other
  - }

Přihlašování uživatelů

Způsoby autentizace se definují v jednotlivých virtuálních hostech

- sites-enabled/ např. default

v sekci `authorize`

- `files` (soubor `users`)
- `unix`
- `ldap`
- `sql`
- `perl`

Pro PEAP, TTLS je třeba je uvést i ve virtual hostu `inner-tunnel`.

Ukládání hesel

- Pro nejběžnější metody přihlašování (PEAPv0, ověření MSCHAPv2) platí:
  Hesla uživatelů je třeba poskytnout v **plaintextu** nebo **NT/LM**!

Ukládání hesel

- Pro nejběžnější metody přihlašování (PEAPv0, ověření MSCHAPv2) platí:
  Hesla uživatelů je třeba poskytnout v **plaintextu** nebo **NT/LM**!

NTLM Decrypter - Over 312.072 billion cracked NTLM hashes. NTLM ...
https://hashkiller.co.uk/ntlm-decrypter.aspx ▾ Přeložit tuto stránku
Your free online **LM** / **NTLM** decryption and encryption website - **NTLM** ... Please note the **password** is after the : character, and the **NTLM** hash is before it.

Roaming

Podpora uživatelů z různých realmů

- naprosto zásadní pro provoz *eduroamu* a dalších rozlehlých sítí
- definovaná v souboru `proxy.conf`
- lze definovat
  - skupiny serverů pro realm, i pro více realmů
  - load-balancing, fail-over
- lze nastavit jiné chování pro domovský realm a externí realmy, třeba přímo v definici virtuálního serveru

Roaming

Podpora uživatelů z různých realmů

- naprosto zásadní pro provoz *eduroamu* a dalších rozlehlých sítí
- definovaná v souboru `proxy.conf`
- lze definovat
  - skupiny serverů pro realm, i pro více realmů
  - load-balancing, fail-over
- lze nastavit jiné chování pro domovský realm a externí realmy, třeba přímo v definici virtuálního serveru

Roaming

Podpora uživatelů z různých realmů

- naprosto zásadní pro provoz *eduroamu* a dalších rozlehlých sítí
- definovaná v souboru `proxy.conf`
- lze definovat
  - skupiny serverů pro realm, i pro více realmů
  - load-balancing, fail-over
- lze nastavit jiné chování pro domovský realm a externí realmy, třeba přímo v definici virtuálního serveru

Roaming

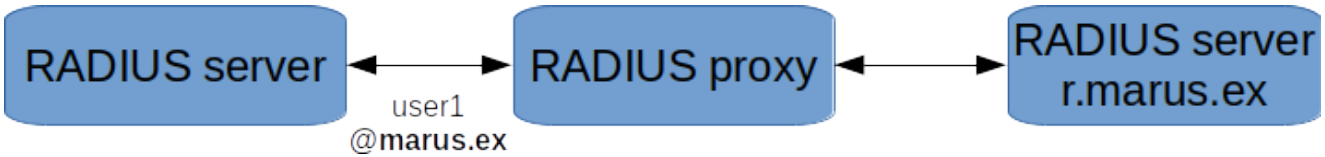
Podpora uživatelů z různých realmů

- naprosto zásadní pro provoz *eduroamu* a dalších rozlehlých sítí
- definovaná v souboru `proxy.conf`
- lze definovat
  - skupiny serverů pro realm, i pro více realmů
  - load-balancing, fail-over
- lze nastavit jiné chování pro domovský realm a externí realmy, třeba přímo v definici virtuálního serveru

Roaming

Podpora uživatelů z různých realmů

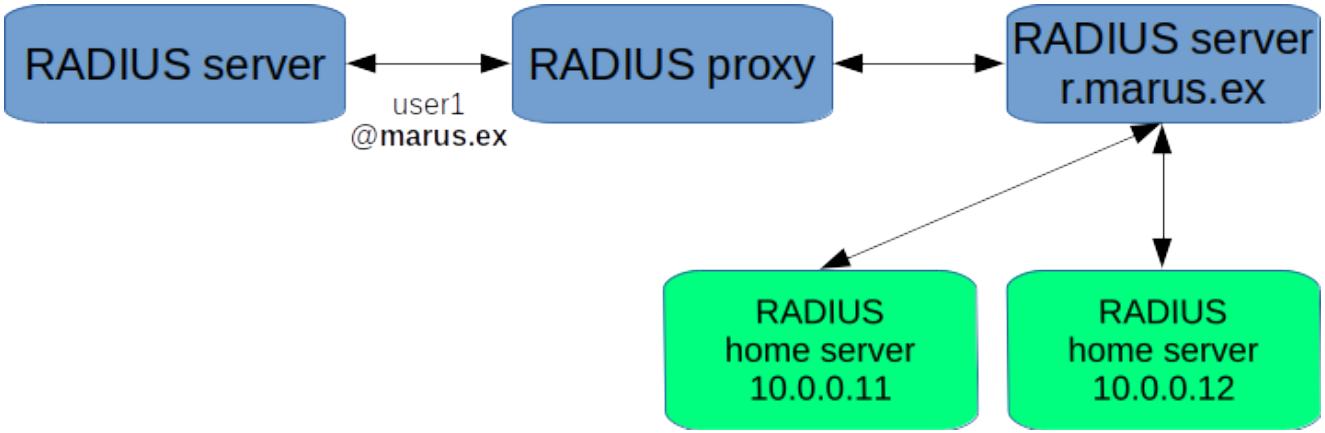
- naprosto zásadní pro provoz *eduroamu* a dalších rozlehlých sítí
- definovaná v souboru `proxy.conf`
- lze definovat
  - skupiny serverů pro realm, i pro více realmů
  - load-balancing, fail-over
- lze nastavit jiné chování pro domovský realm a externí realmy, třeba přímo v definici virtuálního serveru



Roaming

Podpora uživatelů z různých realmů

- naprosto zásadní pro provoz *eduroamu* a dalších rozlehlých sítí
- definovaná v souboru `proxy.conf`
- lze definovat
  - skupiny serverů pro realm, i pro více realmů
  - load-balancing, fail-over
- lze nastavit jiné chování pro domovský realm a externí realmy, třeba přímo v definici virtuálního serveru

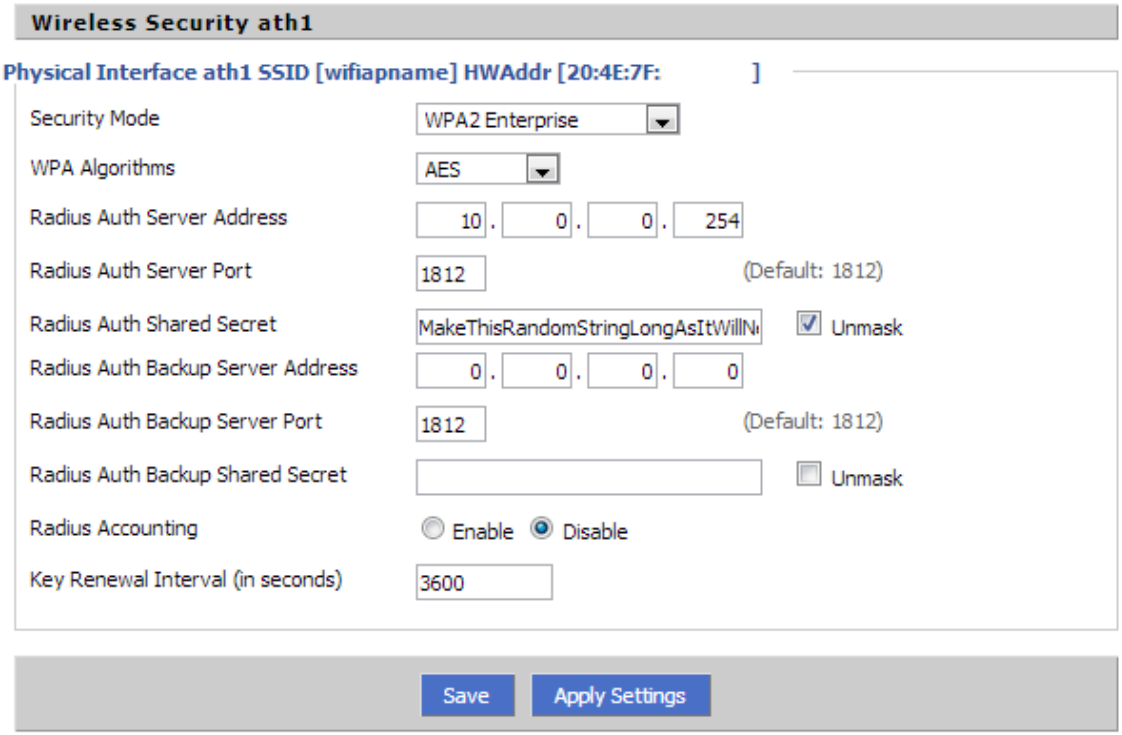


Řešení pro propojení vzdálených RADIUS serverů

- IPSec
- RadSec
  `https://www.eduroam.cz/cs/spravce/pripojovani/radsec/uvod`

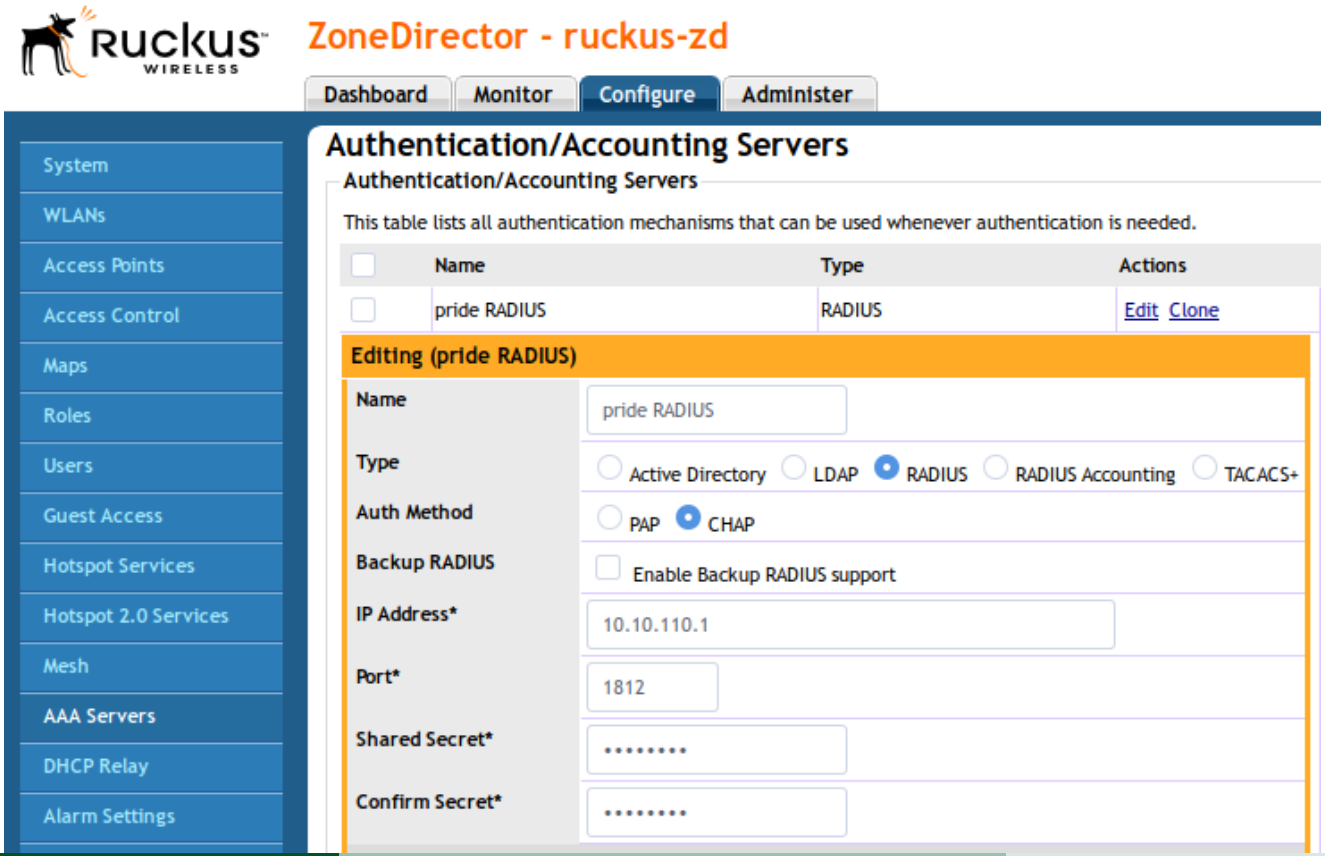
Nastavení Wi-Fi AP / kontroleru

- Každý systém to má jinak
- **WPA2-Enterprise / WPA2-EAP**
- **AES**
- IP adresa RADIUS serveru, auth port (1812), `secret`



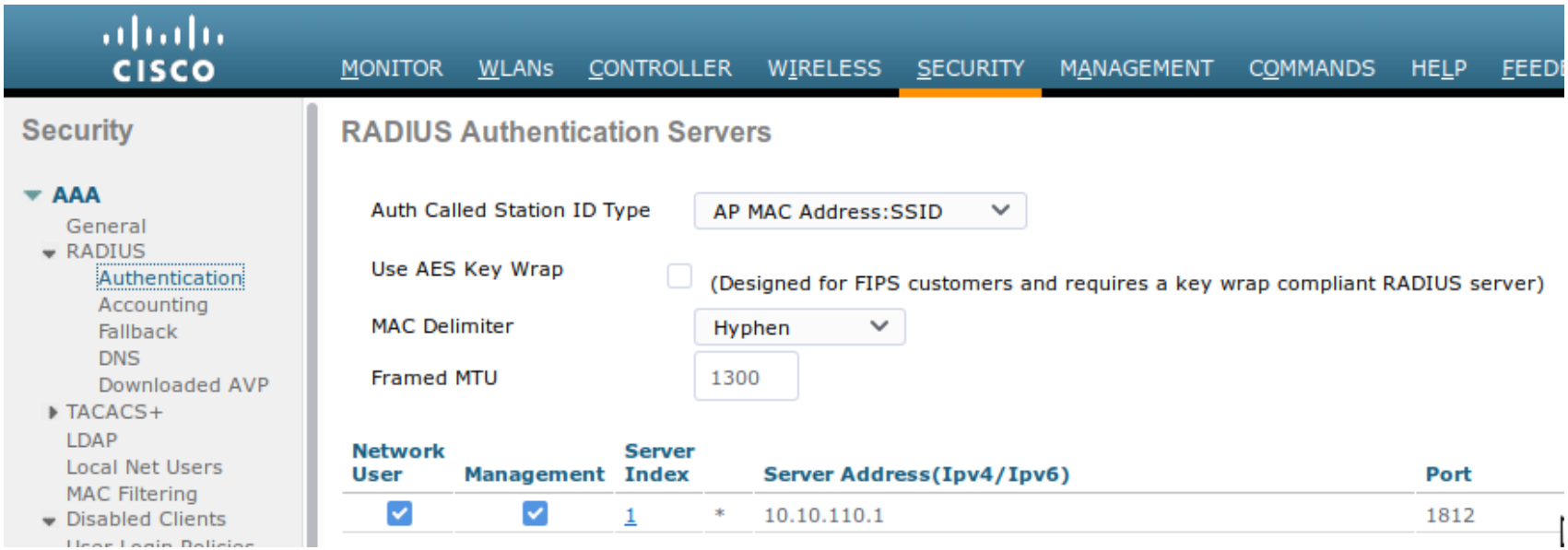
Nastavení Wi-Fi AP / kontroleru

- Každý systém to má jinak
- **WPA2-Enterprise / WPA2-EAP**
- **AES**
- IP adresa RADIUS serveru, auth port (1812), `secret`



Nastavení Wi-Fi AP / kontroleru

- Každý systém to má jinak
- **WPA2-Enterprise / WPA2-EAP**
- **AES**
- IP adresa RADIUS serveru, auth port (1812), `secret`



Nastavení Cisco 2960 pro 802.1x s RADIUSem 1/2

Přihlášení do sítě pomocí 802.1x

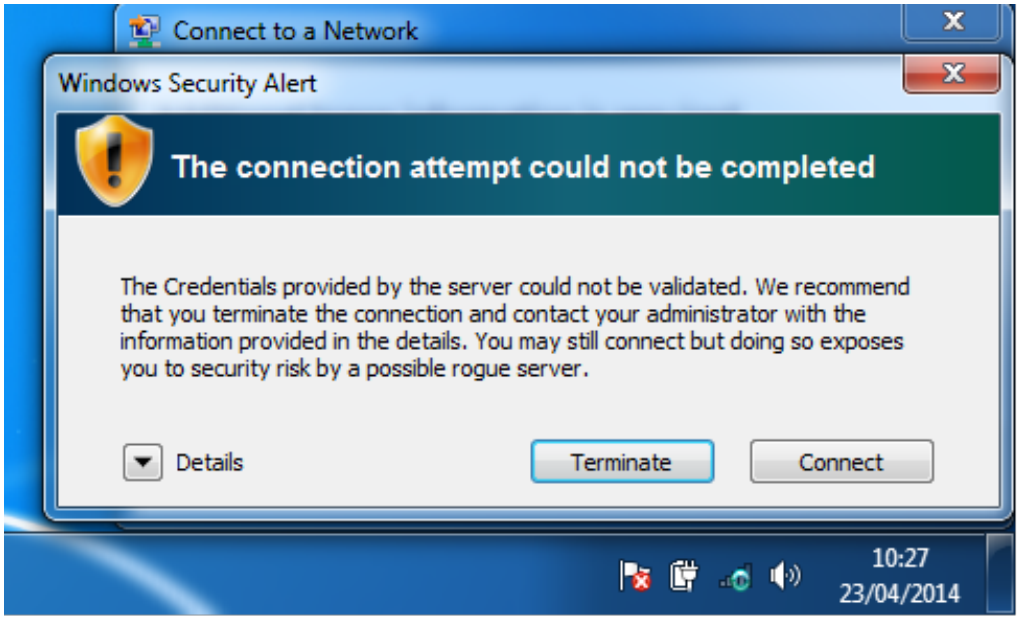
```
!
aaa new-model
!
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
aaa accounting network default start-stop group radius
!
authentication mac-move permit
!
dot1x system-auth-control
!
interface FastEthernet0/14
authentication port-control auto
dot1x pae authenticator
!
```

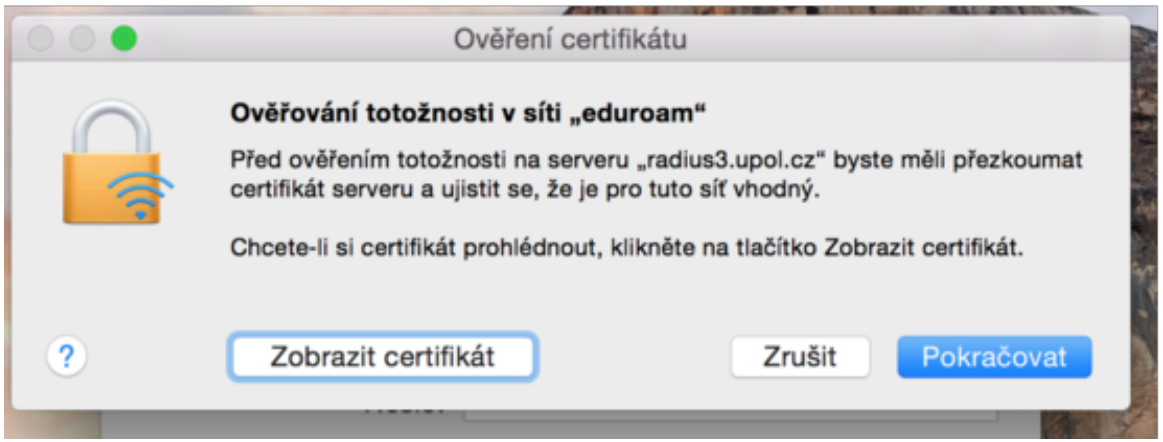
Nastavení Cisco 2960 pro 802.1x s RADIUSem 2/2

```
!
! nasledujici prikaz vyzaduje reload!
radius-server unique-ident 1
!
radius server pride
address ipv4 10.10.110.1 auth-port 1822 acct-port 1823
automate-tester username ciscotest ignore-acct-port idle-time 5
key theKeyThatIsSetOnR4DIUSserver5
!
```

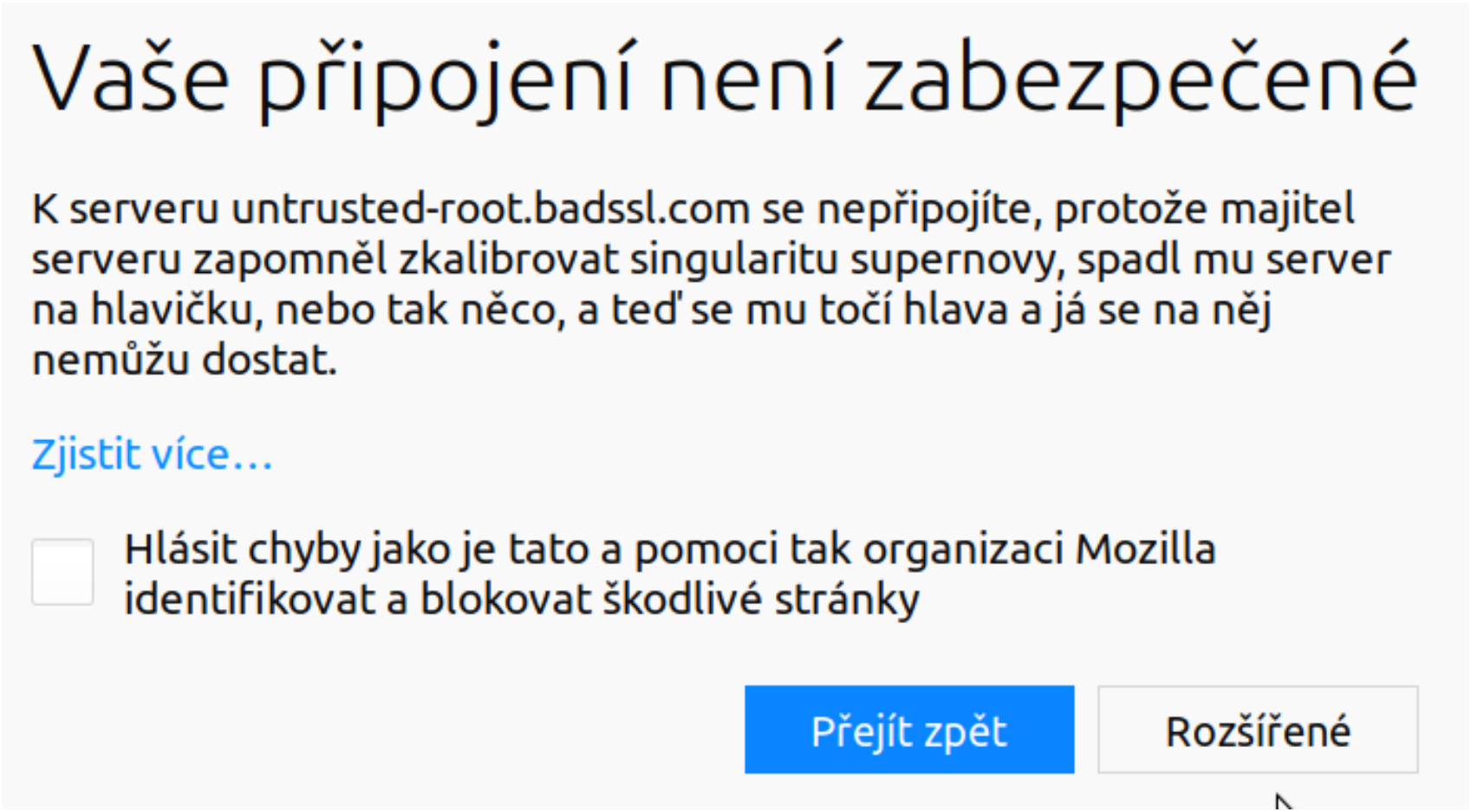
Klient není váš přítel

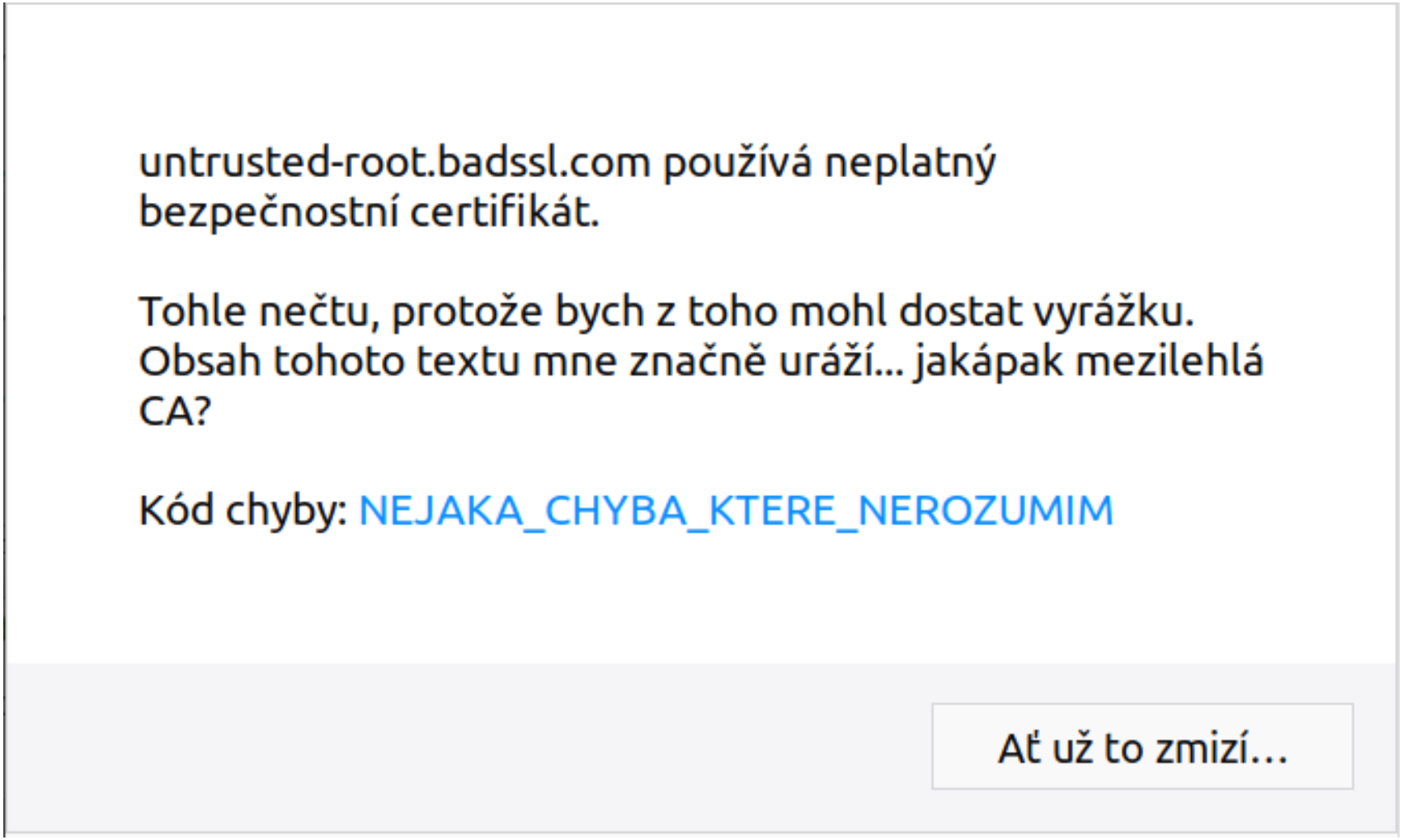
Klient není váš přítel





Ani uživatel není váš přítel!


Vaše připojení není zabezpečené
K serveru untrusted-root.badssl.com se nepřipojíte, protože majitel serveru zapomněl zkalibrovat singularitu supernovy, spadl mu server na hlavičku, nebo tak něco, a teď se mu točí hlava a já se na něj nemůžu dostat.
Zjistit více…
Hlásit chyby jako je tato a pomoci tak organizaci Mozilla identifikovat a blokovat škodlivé stránky
Přejít zpět
Rozšířené


untrusted-root.badssl.com používá neplatný bezpečnostní certifikát.
Tohle nečtu, protože bych z toho mohl dostat vyrážku. Obsah tohoto textu mne značně uráží... jakápak mezilehlá CA?
Kód chyby: NEJAKA_CHYBA_KTERE_NEROZUMIM
Ať už to zmizí...

DIAMETER

- *V podstatě RADIUS v2*
- Na L4 používá SCTP nebo TCP, nikdy UDP
- Pokročilejší ve všech ohledech - autokonfigurace, agenti, P2P režim...
- Začal se vyvíjet brzy po RADIUSu, ale nikdy se tolik nerozšířil
- Hlavní použití v IMS (mobilní operátoři)

Druhy agentů

- **Relay agent**
  - „prostředník“, který předává požadavky dále
  - může je sdružovat
- **Proxy agent**
  - „prostředník“, který může požadavky upravovat, např. podle realmu
- **Redirect agent**
  - centrální konfigurační repozitář pro ostatní nody
  - udržuje směrovací tabulku a na vyžádání zašle adresu pro poptávaný realm
- **Translation agent**
  - „překladatel“ z cizího protokolu (RADIUS, TACACS+) na DIAMETER

OSS DIAMETER servery

- **freeDiameter**
  - BSD-like licence
  - `http://www.freediameter.net`
- **RestComm JDiameter** - TeleStax, Inc.
  - GNU Affero GPL v3.0 i komerční licence
  - `https://github.com/RestComm/jdiameter`
- zbytek je tak nějak polomrtvý
- Open Diameter
  - poslední verze z r. 2004
  - `http://diameter.sourceforge.net/`

OSS DIAMETER servery

- **freeDiameter**
  - BSD-like licence
  - `http://www.freediameter.net`
- **RestComm JDiameter** - TeleStax, Inc.
  - GNU Affero GPL v3.0 i komerční licence
  - `https://github.com/RestComm/jdiameter`
- zbytek je tak nějak polomrtvý
- **Open Diameter**
  - poslední verze z r. 2004
  - `http://diameter.sourceforge.net/`

Ryze komerční DIAMETER servery

- **Radiator**
  - `https://www.open.com.au/radiator/`
- *a určitě ještě kupa dalších*

Závěr a další zdroje

- http://wiki.freeradius.org/guide/HOWTO
- https://www.linuxexpres.cz/praxe/freeradius-server-uvod-a-instalace
- FreeRADIUS Beginner's Guide, Dirk van der Walt, PACKT Publishing
- https://www.interlinknetworks.com/app_notes/History%20of%20RADIUS.pdf
- https://www.ibm.com/developerworks/library/wi-diameter/index.html

Pavel Valach
ja@paulos.cz

Díky za pozornost!

https://paulos.cz/slides/
LinuxDays-2017-FreeRadius.pdf