eduroam zbavený tajomstiev

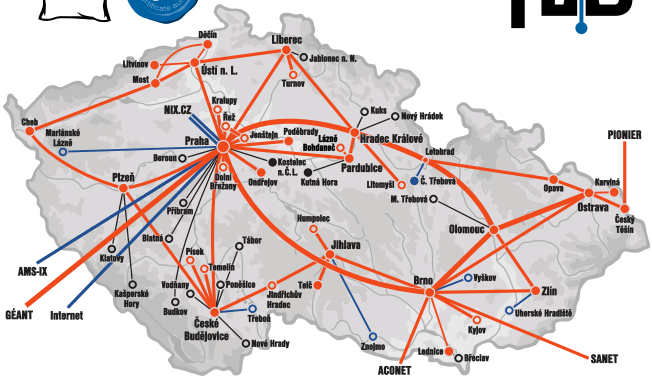
Ondřej Caletka

cesnet

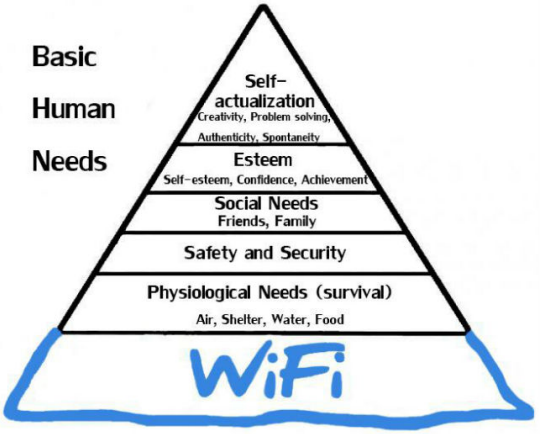
21. apríla 2018

Uvedené dílo podléhá licenci Creative Commons Uveďte autora 3.0 Česko.

O združení CESNET



Internet ako ľudská potreba



cesnet

(Takmer) všetci chceme Wi-Fi

- rýchle a spoľahlivé
- zadarmo
- bez zložitej konfigurácie
- bezpečné
- aj v časoch LTE (špecifický trh)
- hlavne v železobetónových budovách

cesnet

Druhy Wi-Fi sietí

- nešifrovaná sieť, priamy prístup
  - ľahko prevádzkovateľné
  - ľahko použiteľné
  - velmi nebezpečné pre používateľa aj prevádzkovateľa
- nešifrovaná sieť, captive portál
  - ľahko prevádzkovateľné
  - zle použiteľné
  - veľmi nebezpečné pre používateľa
- sieť zabezpečená zdielaným WPA heslem
  - ľahko prevádzkovateľné a použiteľné
  - veľmi bezpečné pre používateľa
- sieť zabezpečená pomocou 802.1X
  - ťažko prevádzkovateľné i použiteľné
  - veľmi bezpečné

cesnet

Keď zaklope polícia…

- anonymné Wi-Fi siete fungujú dobre, než sú zneužité k páchániu kyberkriminality
- prevádzkovateľa majú (aspoň niekde) zodpovednosť za správanie používateľov vo svojej sieti
- prinajmenšom je to nepríjemnosť
- prevádzkovanie anonymnej siete ako alibi pre svoju vlastnú ilegálnu činnosť nefunguje

cesnet

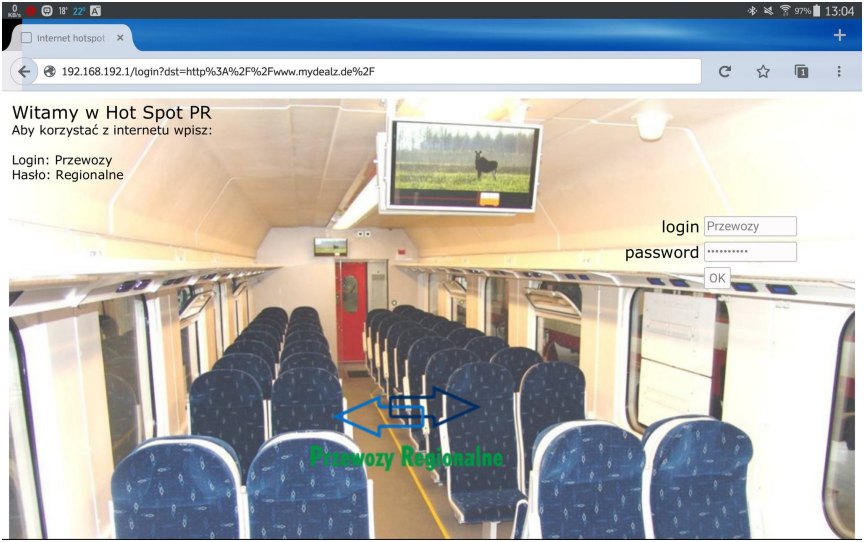
Captive portály

- klient sa pripojí k nešifrovanej sieti
- jeho komunikácia je blokována a HTTP prevádzka odklonená (!) smerom k autentizačnému portálu
- po overení mena a hesla je komunikácia pre danú MAC adresu povolená

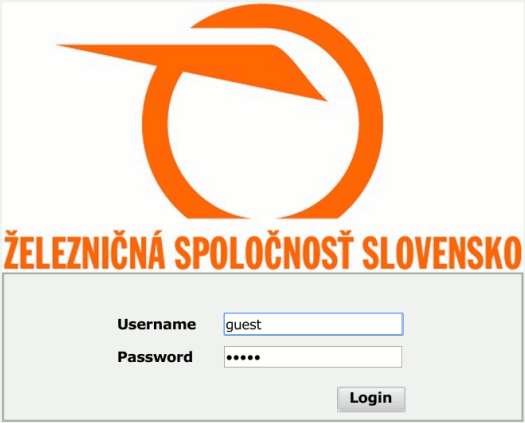
Broken by design

- miešanie autentizovaných a neautentizovaných používateľov v jednej sieti
- nekompatibilita s HTTPS (a IPv6, DNSSEC, atď.)
- nepríjemný používateľský zážitok

cesnet


13:04
internet hotspot
192.168.192.1/login?dst=http%3A%2F%2Fwww.mydealz.de%2F
Witamy w Hot Spot PR
Aby korzystać z internetu wpisz:
Login: Przewozy
Hasło: Regionalne
login
Przewozy
password
OK
Przewozy Regionalne

cesnet


ŽELEZNIČNÁ SPOLOČNOSŤ SLOVENSKO
Username
guest
Password
Login
Copyright © 2015 DrayTek Corp. All Rights Reserved.
2

cesnet

K videniu i na LTE

cesnet

Zapamätané nešifrované siete

- väčšina zariadení si pripojenie k nešifrovanej sieti pamätá
- následne sa snaží aktívne objavovať takú sieť
- útočník triviálne zachytí výzvy a vytvorí požadovanú sieť na mieru
- dostupná riešenie – napr. Wi-Fi Pineapple

Nikdy nenechávejte nešifrované siete v zoznamu obľúbených!

cesnet

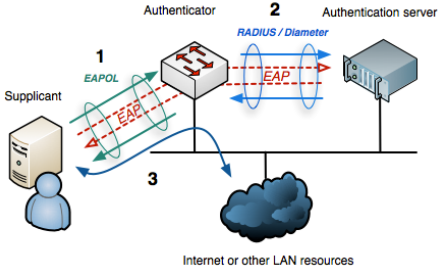
Projekt eduroam

- vznikl v roce 2002 v Holandsku, do ČR dorazil v roce 2004
- problém pro akademiky, migrující mezi univerzitami
  - bylo potreba nahlásiť MAC adresy
  - prípadne si požičať správnú sieťovú kartu
- myšlenka kooperace mezi akademickými prevádzkovateli (bezdrôtových) sietí
  - recipročný princip – kto chce účet, musí poskytovať službu
- pôvodne podpora 802.1x, VPN i captive portálov
  - od 1. 10. 2007 zákaz captive portálov
  - použitie VPN nikedy poriadne nefungovalo
- reší autentizáciu, nie konektivitu (tu dodává hostiteľ)

cesnet

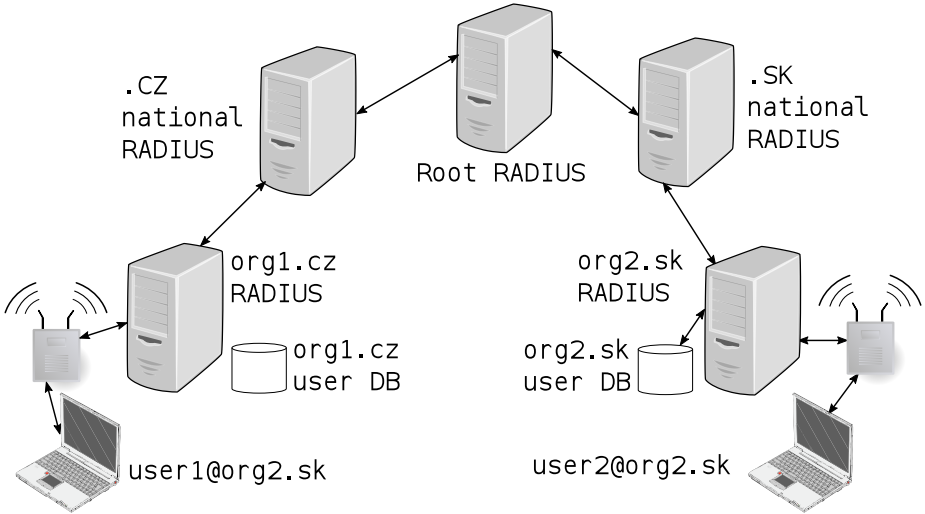
Autentizácia podľa 802.1x

- klient sa fyzicky pripojí k sieti, veškerá prevádzka je blokovaná
- autentikátor vyzve klienta protokolom EAP-over-LAN
- zprávy EAPOL jsou *autentikátorem* (typicky switch nebo AP) predávány autentizačnému serveru
- *supplicant* (súčasť klienta) komunikuje s autentizačným serverom
- pri pozitívnej odpovedi je klient vpustený do siete



Arran Cudbard-Bell, Wikimedia, FDL

Federácia eduroam



cesnet

Federácia eduroam

- lokální používatelia sú odbaveni lokálne
- ostatní sú smerováni pomocou realmu v uživatelskom mene
- EAP sedenie je vždy nadviazano od supplicanta k autentizačnému serveru domovské organizácie (IdP)
- pro používateľe nie je židen rozdiel mezi domovskou a cudzí organizácií
- používané autentizačné metódy:

  EAP-TTLS/EAP-PEAP
  - vonjakjší TLS tunel s autentizacií serverového certifikátu
  - vnútorný EAP overenie klienta (MSCHAPv2, PAP)

  EAP-TLS
  - vzájomná autentizácia certifikáty

cesnet

Vonkajšia a vnútorná identita

vonkajšia (anonymná) identita

- putuje v otvorené podobe
- slúží ke smerovaniu k IdP v rámci federácie
- identita používatelia môže byť anonymizovaná (napr. `anonymous@example.org`)

vnútorná identita

- putuje vnútri TLS tunelu k IdP
- slúží k autentizácii
- vidí ju len IdP

cesnet

Prepojenie RADIUS serverov

- RADIUS protokol používa UDP, šifruje iba heslo zdieľaným tajomstvom
- pre vyššiu ochranu transportován v IPSec
  - zložitá konfigurácia
  - nekompatibilné s preklady adres
  - nutnosť udržovať tunel naživu
- prechod na protokol RadSec
  - RADIUS protokol tunelovaný v TLS/TCP
  - vzájomná autentizácia pomocou TLS certifikátov
  - ľahká konfigurácia

cesnet

eduroam v praxi

cesnet

Problémy SP

Dohľadání majiteľa danej adresy

- 802.1x rieší len prístup k sieti – zná iba MAC adresu
- len niektorá L2 zariadenia registrujú klientské IP(v4/v6) adresy v účtovaciach datoch
- pokiaľ je použit NAT, je treba uchovávať informácie o prekladoch

Zablokování konkrétného používateľa

- je k dispozici iba MAC adresa (tu môže meniť) a vonkajšia identita (ta môže byť spoločná pre všetky používateľa danej organizácie)
- spoľahlivé zablokovanie vyžaduje manuálnú komunikáciu s IdP
- riešením je nový IdP atribut `Chargeable-User-Identity`

Problémy IdP

Způsob autentizácie, voľba EAP protokolu

- najčasťajšie heslom a EAP-MSCHAPv2
- samostatné heslo – bude uložené nechránené v zariadenioch
- generovat alebo nechať používateľe zvoliť?
- podporovať/tolerovať anonymné vonkajšie identity?

Voľba certifikátu pre autentizáciu vonkajšieho TLS tunelu

- zvolenou CA je velmi obtížné vymeniť
- verejné CA funguje out-of-the-box, ale nebezpečne
- privátná CA vyžaduje zložitejšiu konfiguráciu, ale môže byť bezpečnejšia

Problémy používateľov

- ako službu nakonfigurovať aby fungovala
  - a aby bola bezpečná
  - a aby to zvládol i bežný používateľ
- problematické overovanie vonkajšieho TLS tunelu
  - Windows ve východiskovom stave vyžadujú akýkoľvek platný verejný certifikát
  - Apple používá TOFU prístup, vyvolá dialog pre overení otisku
  - ostatné platformy ve východiskovom stave neoverují nič
- ideálné správné nastavenie
  - dôvera v privátnú CA, ktorá vydává certifikáty iba pre RADIUS
  - dôvera vo verejné PKI a **explicitne konfigurované meno serveru**

cesnet

Prečo je overovanie certifikátu dôležité

- ktokoli môže nastaviť své AP, aby vysílalo ESSID eduroam
  - aj keď tým riskuje žalobu od GÉANT
- autentizácii nezapojí do eduroamu, ale otočí proti svojmu serveru
  - klient nepozná, že nerozpráva s domovskou organizáciou
  - v prípade použitie PAP je heslo ihned odcudzeno
  - MSCHAPv2 je dávno prelomený, získanie hesla je otázkou max. hodin

Ťažké overenie certifikátu

- *supplicant* nezná správné meno serveru
- bez pripojení nelze kontrolovať revokacii

cesnet

Overovanie klientským certifikátom

- eliminuje možnosť odcudziť heslo
- obvykle **velmi** ťažké pre používateľa
- problém s velkými pakety
  - ClientHello s certifikátom je velký
  - niektoré tunely mohou mať menší MTU a vynucovať fragmentácii
  - niektoré firewally blokujú fragmenty
  - autentizačná výzva do domovskej organizácie nedoide
  - v medziach ČR automaticky testované

cesnet

eduroam Configuration Assistant Tool

- nástroj pre ľahkú a bezpečnú konfigurácii
- vychádza z XML profilu, ktorý publikuje IdP
- generuje inštalátor pre konkrétnú inštituciu a platformu
  - Windows Vista+
  - OS X / macOS
  - Linux (funguje takmer všude!)
  - Chrome OS
  - Apple iOS 5+
  - Android 4.3+
- jediný spôsob, ako v Androidu < 7 nastaviť kontrolu mena serveru

cesnet

Ručná konfigurácia – WPA Supplicant

```
network={
        ssid="eduroam"
        key_mgmt=WPA-EAP
        eap=PEAP
        identity="caletka@cesnet.cz"
        password=hash:012c9edfb06b543233745c9aff836490
        ca_cert="/etc/ssl/certs/CESNET_EAP_CA.pem"
        altsubject_match="DNS:rad1.ces.net;DNS:rad2.ces.net"
}
```

Získanie hashe hesla – ochrana pred letmým pohľadom

```
$ python -c 'import getpass,hashlib; print(hashlib.new("md4",
> getpass.getpass().encode("utf-16le")).hexdigest())'
Password: CorrectHorseBatteryStaple
012c9edfb06b543233745c9aff836490
```

Problematická signalizácia

- vyhodnocovanie živosti realmov
  - server konkrétneho realmu prestane odpovedať
  - klient preposílá dotaz cez nadradený server
  - nadradený server nemá ako odpovedať
  - klient vyhodnotí nadrazený server ako nefunkčný
  - prestanú fungovať aj iné realmy
- zlé správanie supplicanta
  - nezobrazujú používateľovi dôvod odmietnutie žiadosti
  - timeout odpovedi vyhodnotí ako zlé heslo
- neexistuje nijaký spôsob komunikácie IdP/SP s používateľom

cesnet

Expirované účty

- pri oputení univerzity používateľia zabúdajú odkonfigurovať uložené účty
- vybíjajú si bateriu, kedykoľvek sú v dosahu eduroamu
- pre autentizačné servery žiadný praktický problém
- situácia sa zhoršila so zálohou Wi-Fi sietí do cloudu

cesnet

Kolízia Wi-Fi sietí

- typický problém v kampusoch
  - jedna budova, 3 rozdielné eduroamy
  - každý poskytuje nezávislú IP konektivitu
  - niektorá zariadenia sa trvale držia nesprávné siete
- nemožnosť vynutiť použítie konkrétnej siete/technológie
  - essid typu `eduroam-5Ghz`, `eduroam-cesnet` rozbíjajú roaming
  - rešením môže byť HotSpot 2.0

Hot Spot 2.0 / Passpoint / 802.11u

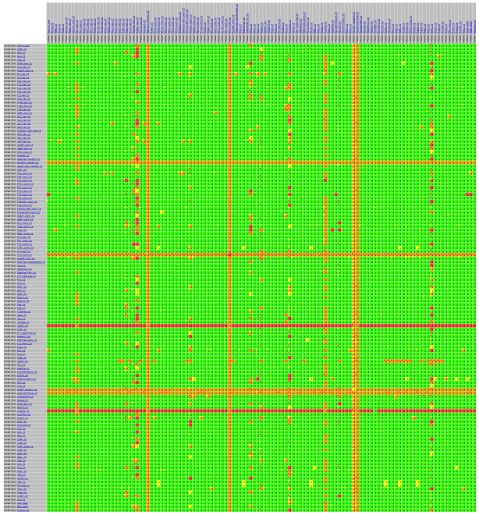
- rozšírení metadát Wi-Fi AP
- možnosť komunikácie s používateľom pred autentizácií
- možnosť identifikovať roamingovú asociácii nezávisle na essid

Priveľa paranoidný SP

- organizácie poskytujúci eduroam môže pripojovať používateľa dynamicky do rôznych sietí
- miestní používateľa mohou byť pripojováni ľubovolne
- hosté by mali byť pripojováni do siete s prístupom alespon k:
  - HTTP/S, FTP
  - SSH
  - OpenVPN/IPSec/PPTP
  - IPv6 in IPv4
  - SMTP/S, POP3/S, IMAP/S
- testovací účty by nemaly mať prístup nikam

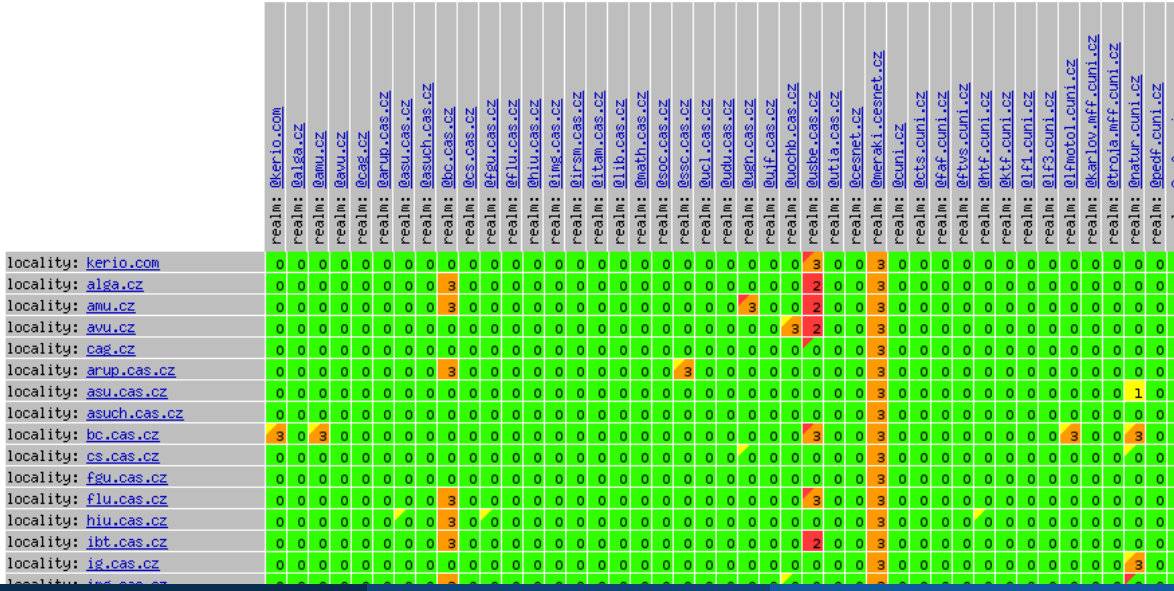
cesnet

Matica dostupnosti

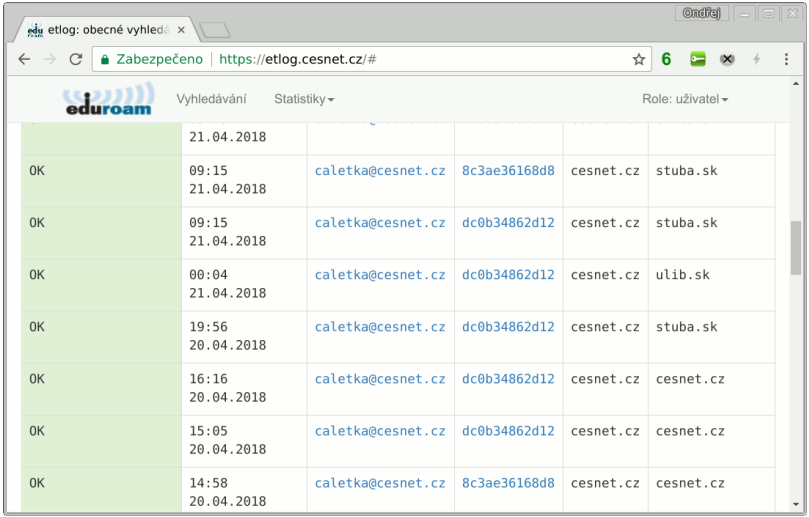


https://ermon.cesnet.cz/matrix/index.html

cesnet


realm: @kerio.com
realm: @alga.cz
realm: @amu.cz
realm: @avu.cz
realm: @cag.cz
realm: @arup.cas.cz
realm: @asu.cas.cz
realm: @asuch.cas.cz
realm: @bc.cas.cz
realm: @cs.cas.cz
realm: @fgu.cas.cz
realm: @flu.cas.cz
realm: @hiu.cas.cz
realm: @img.cas.cz
realm: @irsm.cas.cz
realm: @itam.cas.cz
realm: @lib.cas.cz
realm: @math.cas.cz
realm: @soc.cas.cz
realm: @ssc.cas.cz
realm: @ucl.cas.cz
realm: @udu.cas.cz
realm: @ufch.cas.cz
realm: @ufe.cas.cz
realm: @uochb.cas.cz
realm: @usbe.cas.cz
realm: @utia.cas.cz
realm: @cesnet.cz
realm: @meraki.cesnet.cz
realm: @cuni.cz
realm: @cts.cuni.cz
realm: @faf.cuni.cz
realm: @ftvs.cuni.cz
realm: @htf.cuni.cz
realm: @ktf.cuni.cz
realm: @lf1.cuni.cz
realm: @lf3.cuni.cz
realm: @lfmotol.cuni.cz
realm: @karlov.mff.cuni.cz
realm: @troja.mff.cuni.cz
realm: @natur.cuni.cz
realm: @pedf.cuni.cz
locality: kerio.com
locality: alga.cz
locality: amu.cz
locality: avu.cz
locality: cag.cz
locality: arup.cas.cz
locality: asu.cas.cz
locality: asuch.cas.cz
locality: bc.cas.cz
locality: cs.cas.cz
locality: fgu.cas.cz
locality: flu.cas.cz
locality: hiu.cas.cz
locality: ibt.cas.cz
locality: ig.cas.cz

Spracovanie logov z národného RADIUS serveru



	21.04.2018				
OK	09:15 21.04.2018	caletka@cesnet.cz	8c3ae36168d8	cesnet.cz	stuba.sk
OK	09:15 21.04.2018	caletka@cesnet.cz	dc0b34862d12	cesnet.cz	stuba.sk
OK	00:04 21.04.2018	caletka@cesnet.cz	dc0b34862d12	cesnet.cz	ulib.sk
OK	19:56 20.04.2018	caletka@cesnet.cz	dc0b34862d12	cesnet.cz	stuba.sk
OK	16:16 20.04.2018	caletka@cesnet.cz	dc0b34862d12	cesnet.cz	cesnet.cz
OK	15:05 20.04.2018	caletka@cesnet.cz	dc0b34862d12	cesnet.cz	cesnet.cz
OK	14:58 20.04.2018	caletka@cesnet.cz	8c3ae36168d8	cesnet.cz	cesnet.cz

https://etlog.cesnet.cz/

Zhrnutie

- captive portály sú zlo
- 802.1x má slabá miesta, ale poskytuje vysoký komfort
- nikdy **nenechávajte nešifrované siete** v zoznamu obľúbených
- vždy konfigurujte svoj eduroam účet bezpečne
  - volte silné heslo
  - overujte identitu svojho IdP
- prednostne používajte nástroj `https://cat.eduroam.org`
  - ak vaša inštitucia nie je v ponúke, požádajte správca svojho IdP
- námet na start-up
  - rozšíriť koncept eduroam mimo akademickú obec
  - konkurovať riešením postaveným na captive portáloch
  - užívať národné e-identity

cesnet

Ďakujem za pozornosť

Ondřej Caletka
Ondrej.Caletka@cesnet.cz
https://Ondřej.Caletka.cz