



# Služby e-Infrastruktury CESNET

*Internet v Telči 2016*

*11. 8. 2016*



EVROPSKÁ UNIE  
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ  
INVESTICE DO VAŠÍ BUDOUCNOSTI



Tomáš Košňar

CESNET z. s. p. o.

- 1996 – založeno veřejnými VŠ a AV ČR
  - od ČVUT převzalo provoz sítě CESNET
  - začátky pan-evropského budování sítí pro výzkum, vývoj, vzdělávání → CESNET buduje oddělenou síť pro tento účel → provozuje 2 sítě (prodej komerční sítě 2000)
- několik generací sítí pro VVV, vždy v souvislosti s vývojem v evropském kontextu (TEN-34, Quantum, GÉANT..)
- 2011 – systematická podpora infrastruktur pro VV
  - cestovní mapa (vláda ČR) → Velká Infrastruktura CESNET
- 2016 → e-Infrastruktura CESNET

- Členství



PLANETLAB

An open platform for developing, deploying, and accessing planetary-scale services

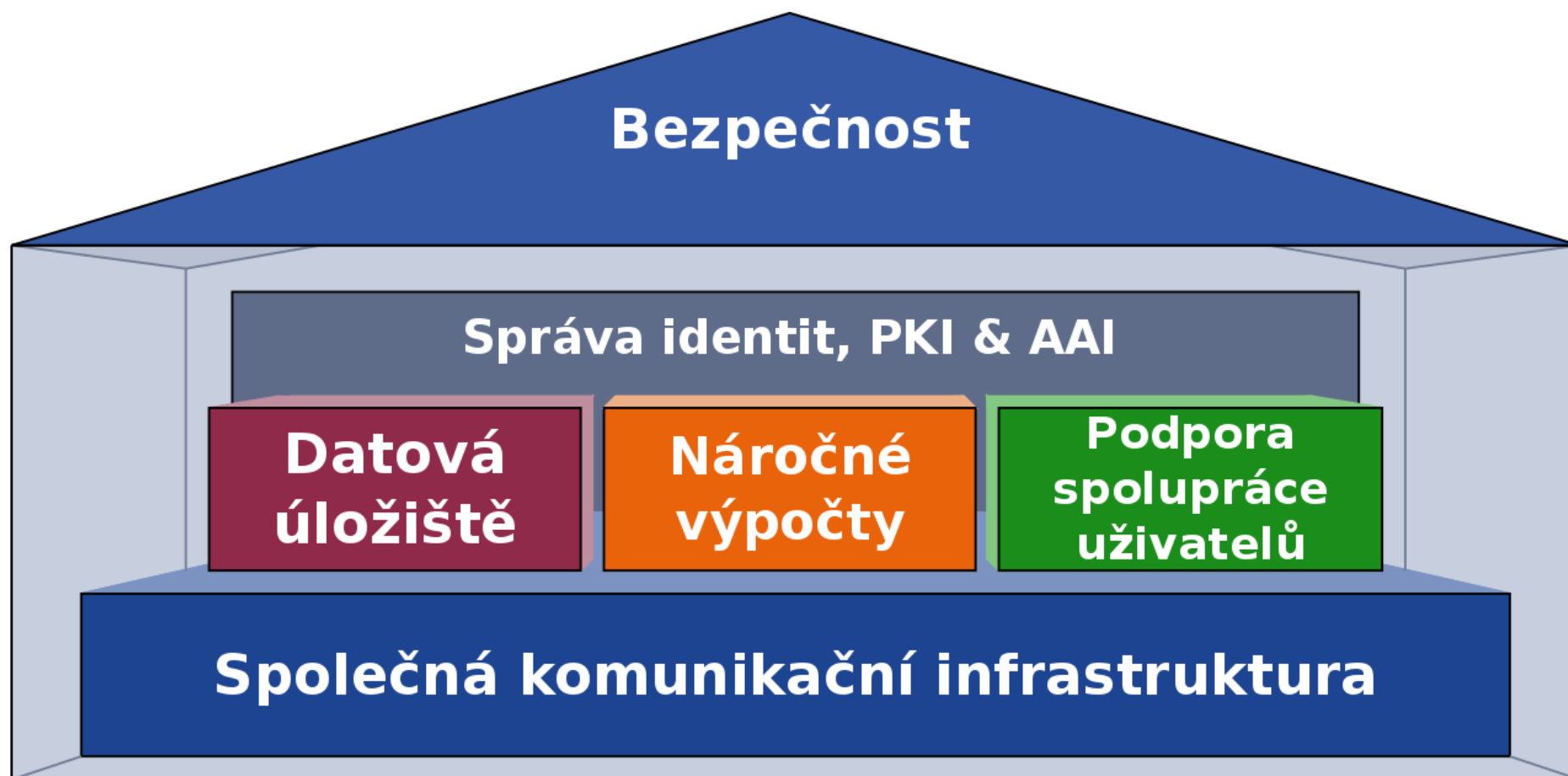


NIX.CZ



- Budování komplexního prostředí pro potřeby VVV
- Uživatelé
  - Více než 300 organizací
  - Členové (Veřejné VŠ - 24, Státní VŠ – 2, AV ČR – 57 ústavů)
  - Veřejné a soukromé VŠ, nemocnice, výzkumné organizace, knihovny, muzea, galerie, ZŠ, SŠ, VOŠ, veřejná správa, samospráva, ..
  - *~ 450 tisíc individuálních uživatelů*
  - Přístup ke službám e-Infrastruktury vymezen „Access Policy“

- Symbolická architektura, základní komponenty



## Podpůrná Infrastruktura

- Správa adresových zdrojů v4, v6, údajů v RIPE, asistence při zakládání LIR
- **DNS** – primární, sekundární, záložní, DNSSEC
- **Mail-relay** – záložní
- **AntiSpam Gateway**
- **Monitoring** infrastruktury, **IP provozu**
- **24x7 dohled**

## IP/MPLS páteřní infrastruktura

- Multi-Protocol Label Switching, IP,
- Platforma pro vytváření **logických sítí** nebo **okruhů** pomocí služeb optické přenosové infrastruktury

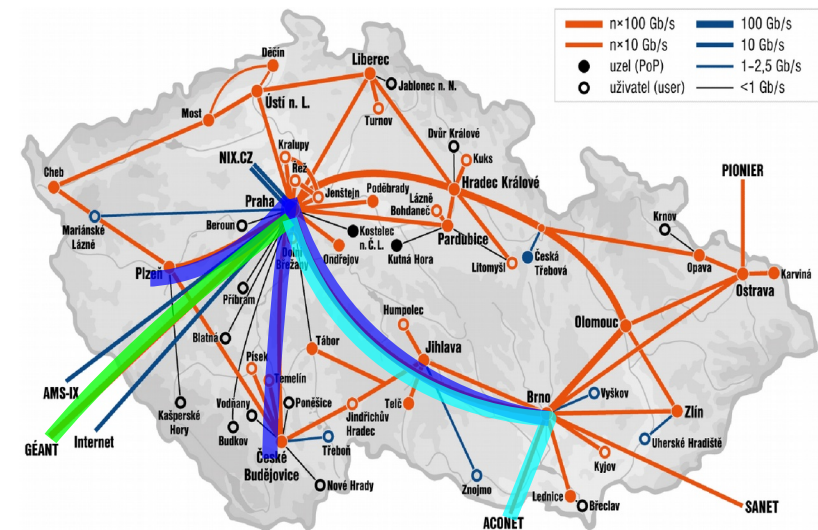
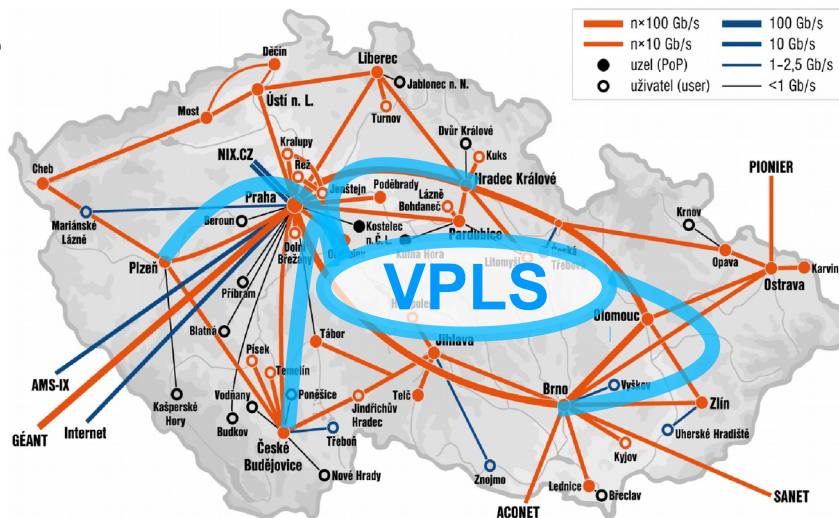
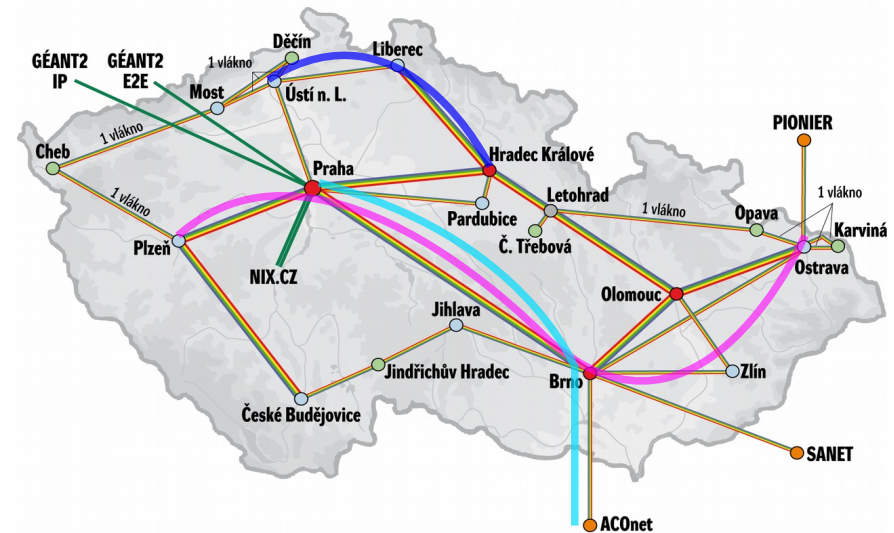
## Optická přenosová infrastruktura

- Vlnový multiplex – WDM technologie, 2 systémy
  - Cisco 15454, až 80 kanálů 1-100Gps – jádro
  - Open DWDM, 1-100Gps, připojování k páteři
- Platforma pro vytváření **nezávislých propojů bod-bod**

## Fyzická infrastruktura (temná vlákna)

- Optická vlákna, duální připojení páteřních uzlů
- cca 6000 km (1800 jednovláknové)

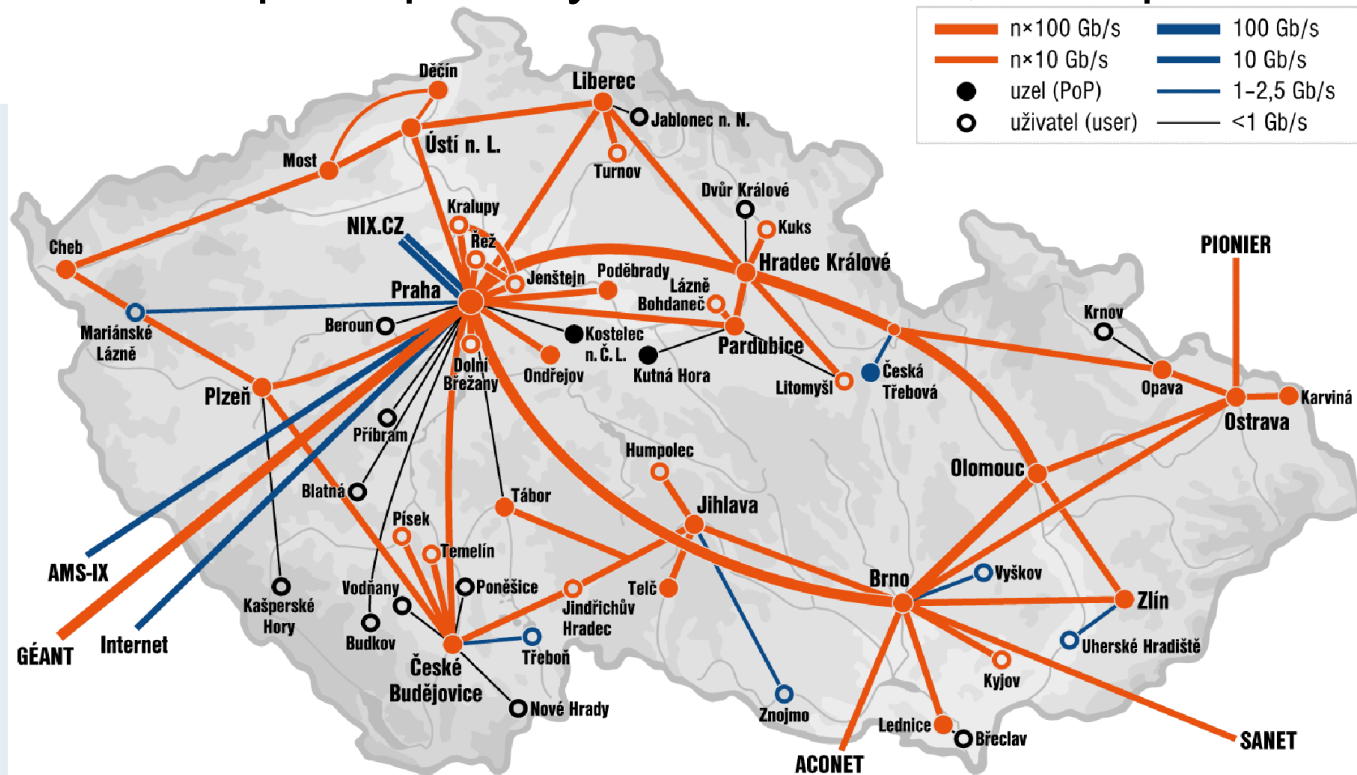
- Vyhrazené okruhy a sítě
- Fotonické služby – nezávislé „čistě“ optické propoje
  - Speciální náročné aplikace
- Lambda služby – optické propoje s OEO konverzí
- Vyhrazené okruhy a sítě
  - EoMPLS
  - VPLS





- **Sdílená IP síť – připojení IP protokolem**
- **100 Gbps jádro; uzly Nx10 Gbps, 40-100 Gbps**
- Dostatečná kapacita, dostatečné přístupové rychlosti ~ Nx10, 40Gbps

- **Externí propojení**
- **220 Gbps**
- 100 Gbps GÉANT
- 120 Gbps IX, partneři
  - 40 Gbps NIX.CZ
  - 20 Gbps ACONET (VIX)
  - 20 Gbps SANET (SIX)
  - 10 Gbps PIONIER
  - 10 Gbps AMS-IX
  - 10 Gbps Google
  - 10 Gbps Tier-1
- **E2E**
  - 4x10 Gbps GÉANT
  - Nx10 CBF (AT, SK, PL)
  - 10 Gbps GLIF



- IPv4, IPv6 – dual stack, unicast, multicast
- Duální fyzické připojení uzlů
- Duální páteřní uzly
- Redundance, flexibilita

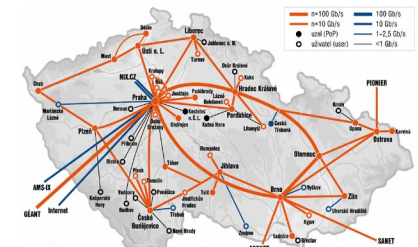


- **Sdílená IP síť – připojení IP protokolem**
- Symetrické připojení bez regulace provozu (legitimního), možnost redundantního připojení do dalšího uzlu
- Dohled a monitoring funkcí a bezpečnosti sítě 24/7/365
- Správa a přidělování adresových zdrojů IPv4, IPv6, správa údajů v RIPE, asistence při zakládání LIR
- DNS – primární, sekundární, záložní, DNSSEC
- Mail-relay – záložní
- AntiSpam Gateway

- **Sdílená IP síť – připojení IP protokolem**
- BCP38, RPF check + další mechanismy eliminace podvržených zdrojových adres na vstupu do páteře
- Semi-automatická obrana páteře proti DDoS útokům na bázi amplifikace
- RTBH jako služba (BGP připojené sítě)
- Permanentní monitoring stavu a využití celé páteře
- Permanentní monitoring IP provozu (flow-based) na perimetru sítě a v celé páteři + detekce typických útoků
- ...perspektivy ~ *BGP FlowSpec* ?
- CESNET - zakládající člen projektu FENIX v rámci NIX.CZ
- ...uživatelé a *FENIX*, podmínky projektů ?



Důvěryhodný  
operátor



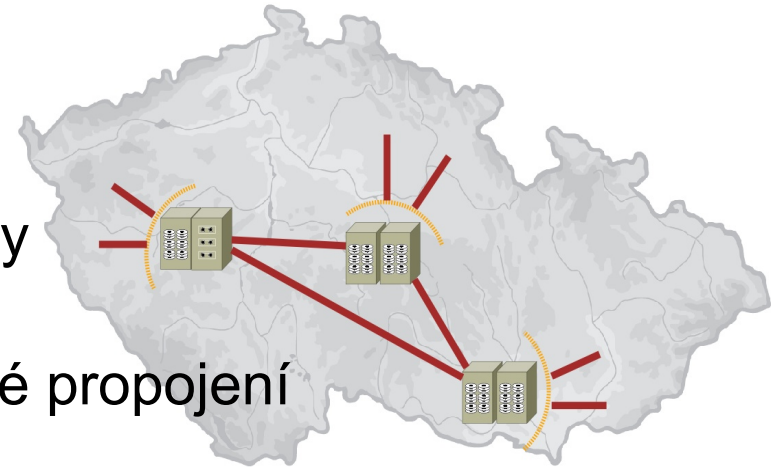
- **MetaCentrum zajišťuje a koordinuje provoz NGI** (Národní Gridové Infrastruktury) – národní součást **EGI** (Evropské GI)

*„Sdružení výpočetních a datových zdrojů pro řešení velmi náročných úloh, které jsou za hranicemi výpočetních možností samostatného pracoviště“*

- Aktuálně ~ 12k jader, 2PB storage (EGI 3.8PB)
- **Grid+Cloud+MapReduce výpočty**
  - Konvenční i specifický HW
- **Aplikační SW**
  - Koordinace pořizování a správy programového vybavení
  - <https://wiki.metacentrum.cz/wiki/Kategorie:Aplikace>
- **Uživatelská podpora**
  - Konkrétních problémy, optimalizace algoritmů, ...
- **Integrace výpočetních kapacit do NGI**
- **Příprava specifického prostředí**
  - Úprava stávajícího nebo nové platformy (Galaxy, Chipster)
  - Specifické velké skupiny uživatelů (EGI, ELIXIR)



- Distribuovaná architektura HSM úložišť
- Plzeň, Jihlava, Brno → 21+PB fyzické kapacity
- Dedikovaná síťová infrastruktura pro vzájemné propojení
- Dedikovaná infrastruktura pro připojení do páteřní sítě
- Dlouhodobé ukládání primárně vědeckých dat (úroveň binárních dat)
- **Zálohy, archivace, sdílení dat, speciální aplikace**
  - Souborově orientovaný přístup - NFSv4, FTP, rsync, SCP, ...
  - Speciální aplikace - Grid storage element, DCache
  - FileSender
  - ownCloud



- **Webkonference** – základní kvalita obrazu
- **Videokonference** – H.323/SIP, MCU (Limit Full HD)
  - Začlenění zařízení uživatelů do VC infrastruktury, ClearSea, rezervační portál **meetings.cesnet.cz**
- **IP telefonie** – propojení IP-telefonních sítí v rámci e-infrastruktury a s partnery
- **Streaming** – distribuční platforma pro multimediální vysílání do Internetu (Windows Media, MPEG-4 Flash/HTML5)
- **Videoarchiv** – platforma pro uložení obsahu a jeho vystavení pomocí streamovacích serverů
- **Speciální obrazové přenosy a vizualizace**
  - Vysoké rozlišení, nízká latence, lékařské zákroky, vědecké vizualizace (SAGE, CAVE), vzdálená spolupráce při zpracování obrazových dat HD+ (2K, 4K, 8K) apod.
  - Vlastní vyvíjené systémy (UltraGrid, 4K Gateway)

- **eduID.cz - Česká akademická federace identit**

- **Jedno uživatelské jméno a heslo pro přístup k řadě síťových služeb** (*v multi-institucionálním prostoru*)
- Poskytovatelé služeb z národní komunity i mezinárodní
- Součást mezinárodní interfederace eduGAIN



- **Certifikáty pro uživatele a servery**

- Důvěryhodný server
- Důvěryhodná identita uživatele

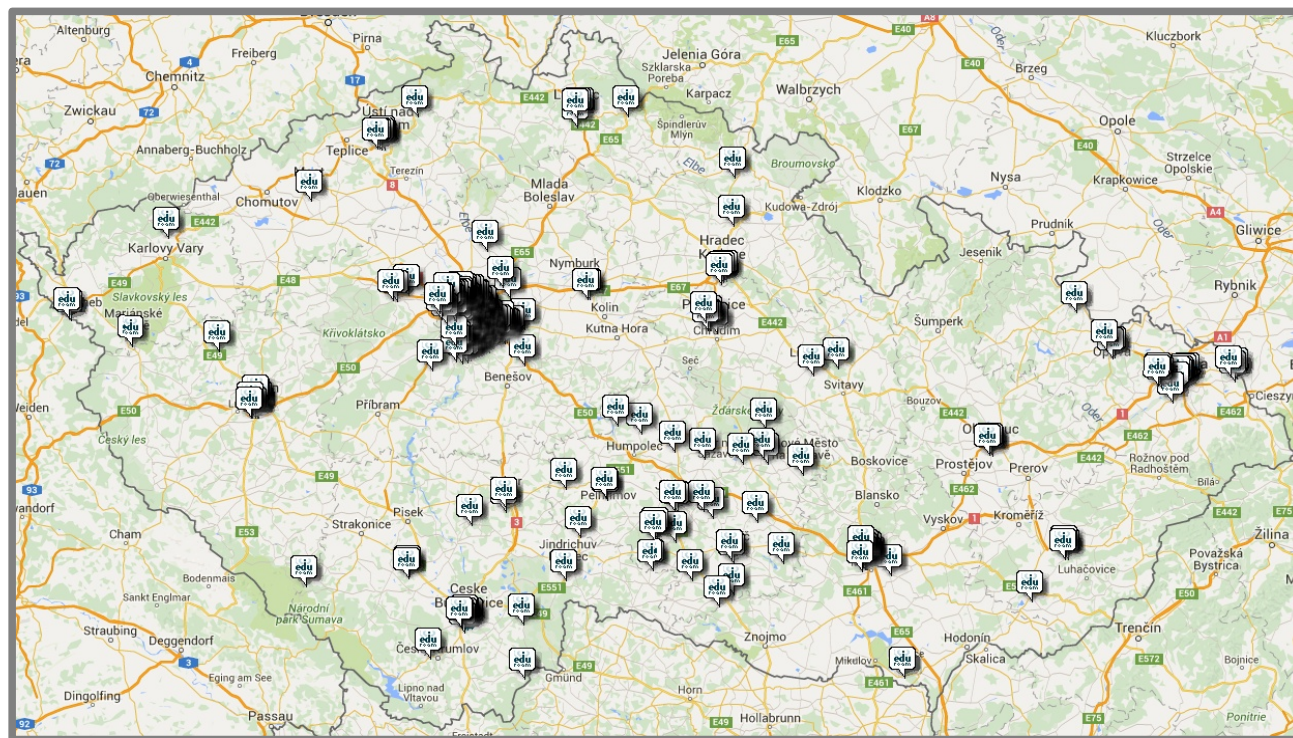
- **Jednotný systém správy účtů v e-Infrastruktuře**

- Některé služby odebírané na individuální bázi
- Strukturování uživatelské komunity
- Řízený přístup ke zdrojům





- **eduroam** - „služba na pomezí“: služba z oblasti ověření uživatelů, z pohledu koncového uživatele síťová služba - **roaming uživatelů v hostitelské síti**
  - Síťovou infrastrukturu zajišťuje hostitelská síť; síťová infrastruktura je opřena o autentizační infrastrukturu (technicky RADIUS server hostitelské organizace zapojený do národní hierarchie)
  - ...*podmínky projektů* ?



- **Řešení bezpečnostních incidentů (CSIRT)**
  - Bezpečnostní tým CESNET-CERTS
    - <https://csirt.cesnet.cz/>
  - Platforma (technická, organizační) pro řešení a asistenci při řešení bezpečnostních incidentů v e-infrastruktuře CESNET a administrativní doméně komunity



The screenshot shows the CESNET-CERTS website. The top navigation bar includes links for e-Infrastruktura, Sít, Výpočty, Uložení, Spolupráce, Multimédia, Bezpečnost, and Identita. The main content area features the CESNET-CERTS logo, a search bar, and a sidebar with navigation links: O NÁS, HLÁŠENÍ INCIDENTU, SLUŽBY, PROJEKTY, SPOLUPRÁCE, ČASTÉ DOTAZY, ODKAZY, DOKUMENTY, AKCE, and KONTAKT. The main text area is titled 'O nás' and 'Pole působnosti', providing information about the team and their scope of work. It also includes 'Základní informace' (Basic information) with contact details and a 'Jak nás můžete kontaktovat' (How you can contact us) section. At the bottom, there is a 'Naše cíle' (Our goals) section and an 'Ohlášení incidentu' (Incident reporting) section. The website is accredited by the Trusted Introducer (TI).

e-Infrastruktura  
CESNET

Sít Výpočty Uložení Spolupráce Multimédia Bezpečnost Identita Přihlášení

**CESNET CERTS**

Hledat

- ▶ O NÁS
- ▶ HLÁŠENÍ INCIDENTU
- ▶ SLUŽBY
- ▶ PROJEKTY
- ▶ SPOLUPRÁCE
- ▶ ČASTÉ DOTAZY
- ▶ ODKAZY
- ▶ DOKUMENTY
- ▶ AKCE
- ▶ KONTAKT

### O nás

CESNET-CERTS je oficiální jméno bezpečnostního týmu sdružení [CESNET, z.s.p.o.](#), od ledna roku 2004. Tým tvoří zaměstnanci sdružení se sídlem v Žitkově 4, Praha, Česká republika.

### Pole působnosti

Naším polem působnosti je síť [CESNET2](#), tj. všechny IP adresy autonomního systému AS2852. CESNET-CERTS přímo zodpovídá za řešení bezpečnostních incidentů strojů a služeb v doménách [cesnet.cz](#), [cesnet2.cz](#), [ces.net](#), [liberouter.org](#), [liberouter.net](#), [ipv6.cz](#), [acad.cz](#), [eduroam.cz](#) a v IP adresách interní infrastruktury sítě CESNET2, jež jsou v databázi [RIPE](#) označeny jako INFRA-AW.

### Základní informace

- Telefonní číslo: +420 2 2435 2994
- Časová zóna: CET (GMT+0100 v zimě, GMT+0200 v létě)
- E-mailová adresa: [certs@cesnet.cz](mailto:certs@cesnet.cz)
- Twitter účet: [@CESNET\\_CERTS](#)
- Naš PGP klíč:
  - User ID: CESNET-CERTS <[certs@cesnet.cz](mailto:certs@cesnet.cz)>
  - Key ID: 0x9CAA8579
  - Key type: DH/DSS
  - Key size: 1024 bits
  - Expiration: never
  - Fingerprint: 341D 3EB0 0160 941F 6A06 4401 F9BF C741 9CAA 8579

### Jak nás můžete kontaktovat

Preferujeme kontakt elektronickou poštou na adresu [certs@cesnet.cz](mailto:certs@cesnet.cz). V urgentním případě, nebo v případě, že nemůžete poslat zprávu, použijte výše uvedené telefonní číslo. Pokud nám potřebujete poslat citlivá data, zašifrujte je naším veřejným PGP klíčem.

### Ohlášení incidentu

Přejete-li si poslat nám hlášení o bezpečnostním incidentu, postupujte prosím podle uvedeného [návodu](#).

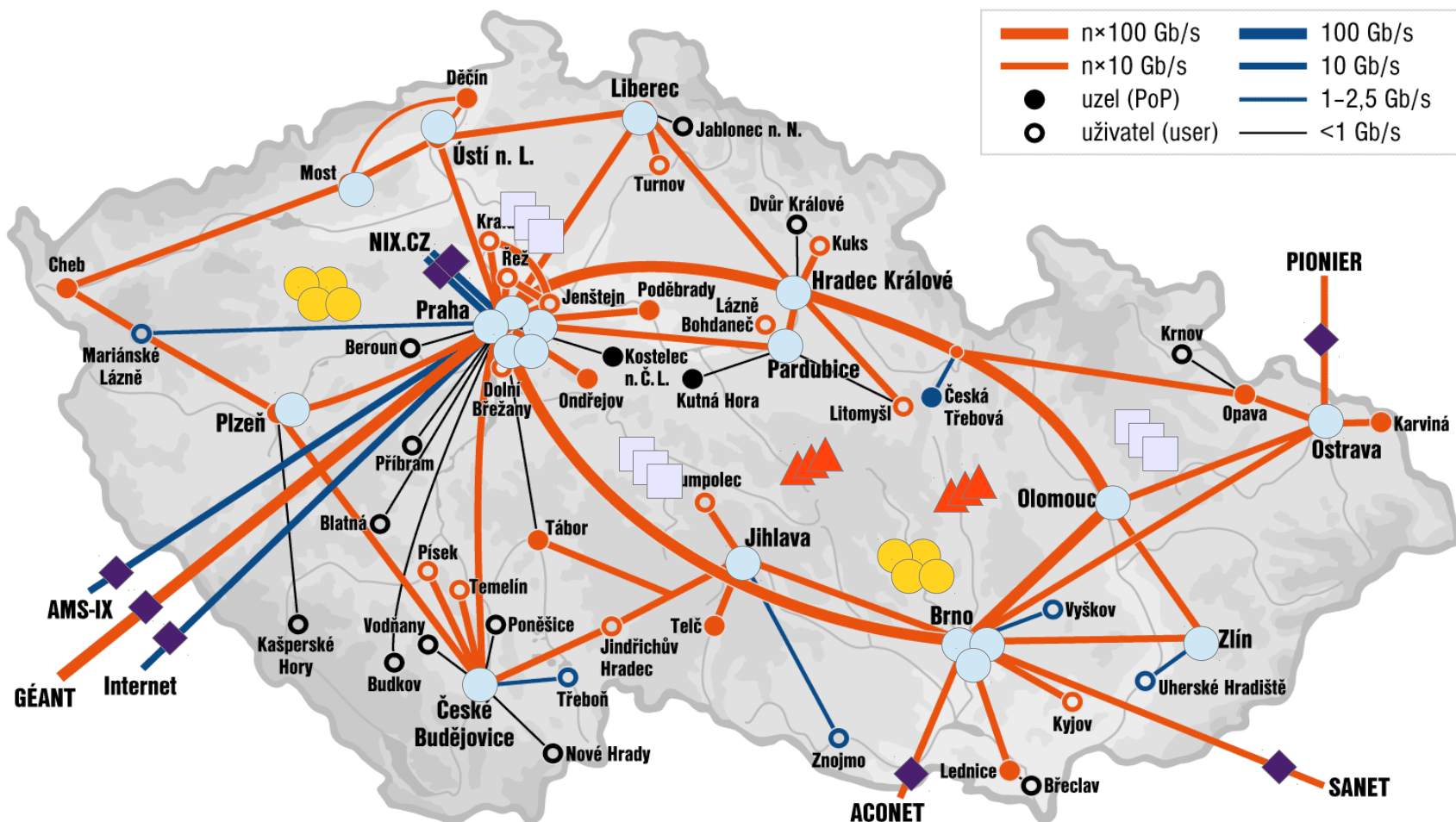
### Naše cíle

- Zajišťujeme jednoduchý a důvěryhodný kontakt pro celou síť CESNET2.
- Koordinujeme řešení a prevenci bezpečnostních incidentů v síti CESNET2.
- Pomáháme institucím připojeným k síti CESNET2 vyvíjet jejich bezpečnostní strategie týkající se provozu sítě a služeb.

ACCREDITED BY  
TRUSTED INTRODUCER

Poslední úprava: 27.01.2016 12:59

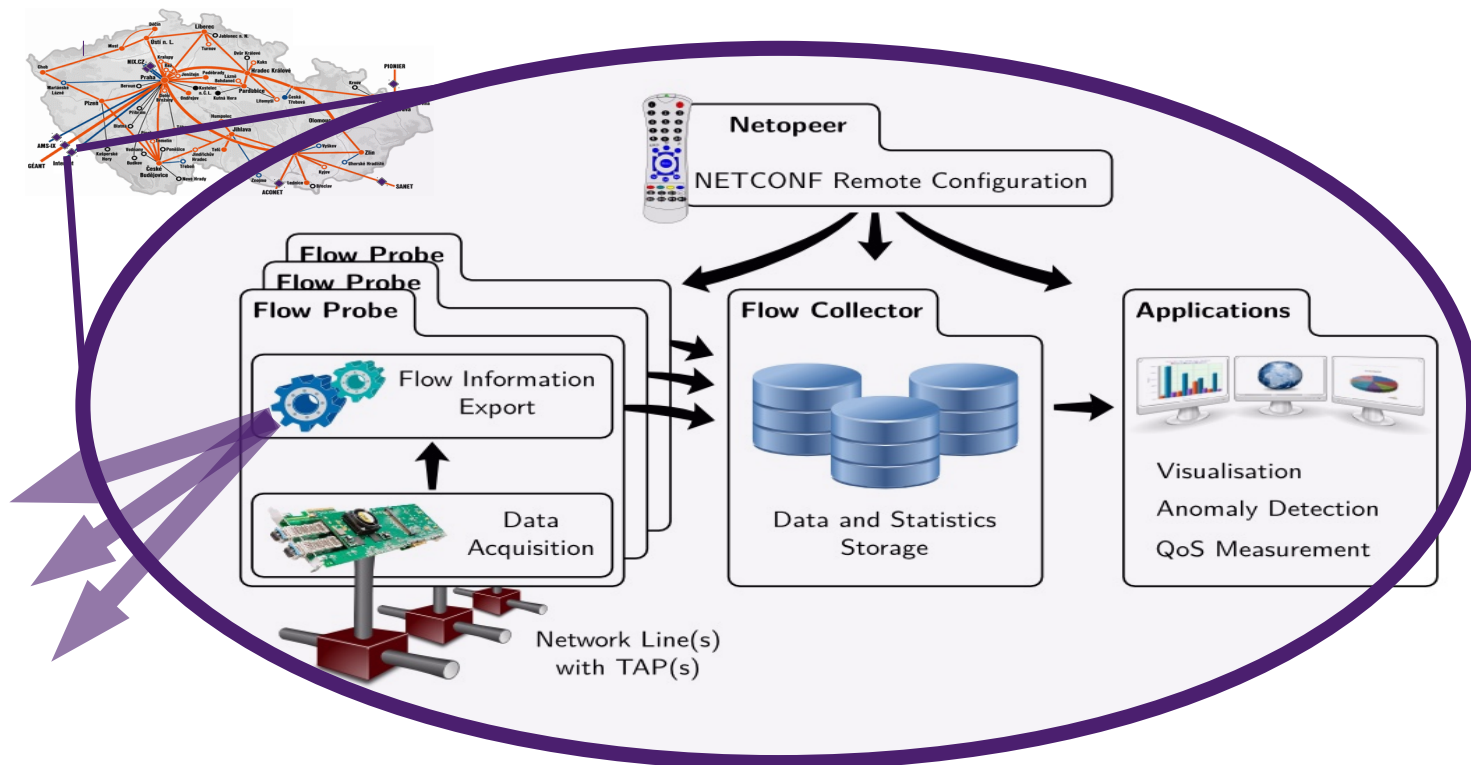
- Infrastruktura a služby v oblasti bezpečnosti



- ◆ - HW akcelerované sondy
- - plošný monitoring IP provozu na bázi toků (zdroje provozních informací)
- - Honey Pots
- - IDS a IPS systémy apod.
- ▲ - monitoring infrastruktury na bázi SNMP

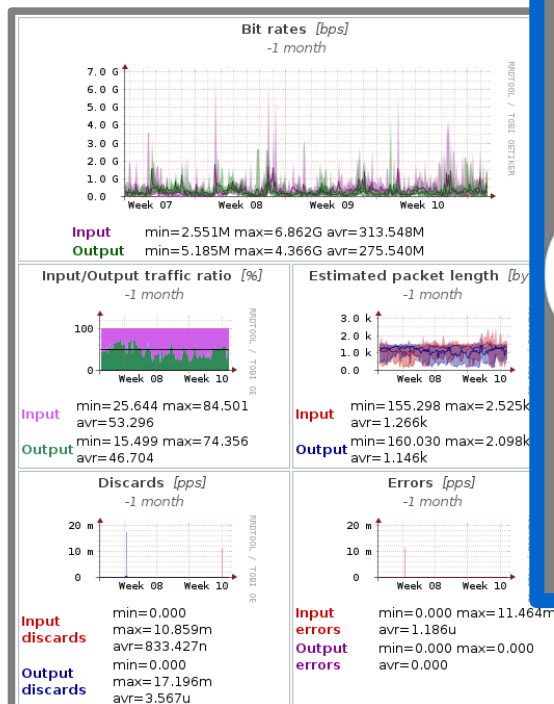
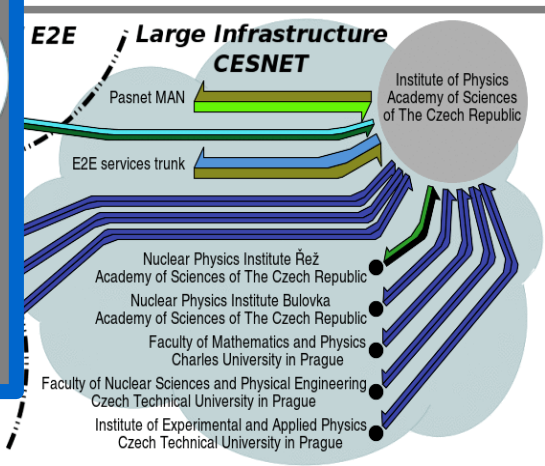
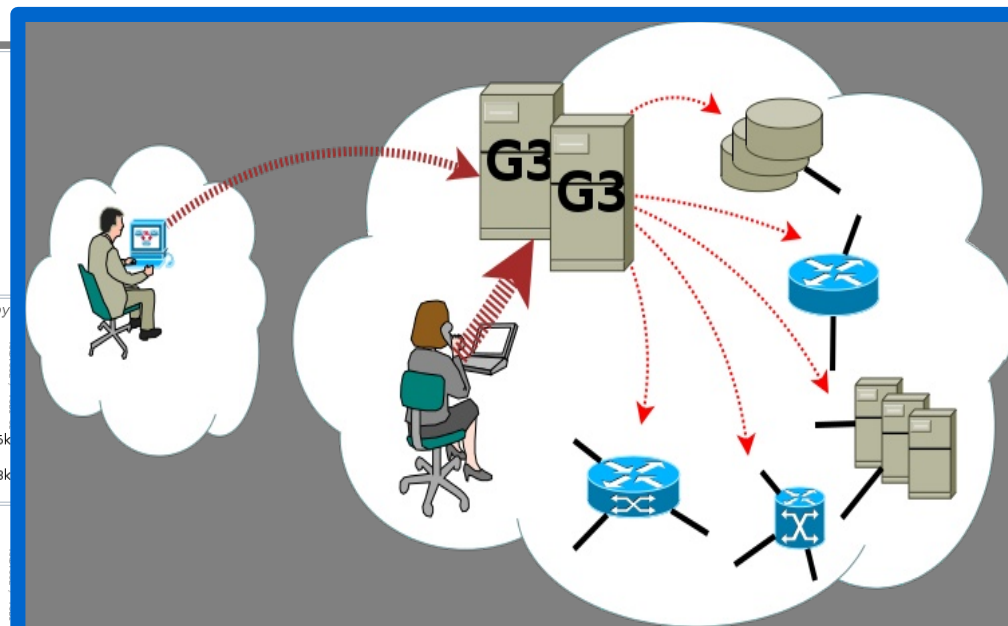
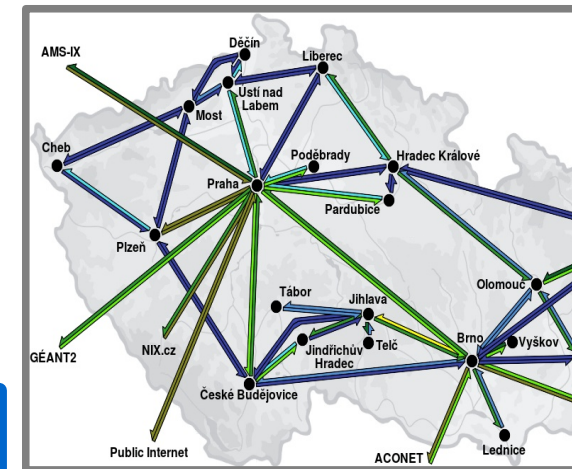


- **HW akcelerované sondy → kompletní provoz na lince**
  - Bezeztrátové a detailní měření síťových dat na volitelné úrovni detailu, tunelovaný provoz, detailně HTTP, DNS, SIP; užitečné pro ruční analýzu, možnost vyčlenit provoz; statistiky, zdroj dat a informací pro další výzkum
  - Detekce událostí a anomálií na paketové a IP úrovni
  - Perimetr e-Infrastruktury, STaaS



## • Systém G3 → prvky infrastruktury

- Sběr informací (SNMP a další metody) nejen ze síťových prvků
- Interaktivní UI, periodický reporting
- Detekce, vizualizace a notifikace anomálií
- Síťová část e-Infrastruktury
- **Služba pro uživatele – vlastní instance ...kde ?**



**alignment errors** min=0.000 max=0.000 avr=0.000  
**checksum errors** min=0.000 max=12.558m avr=1.267u  
**frames too long** min=0.000 max=2.977k avr=89.183

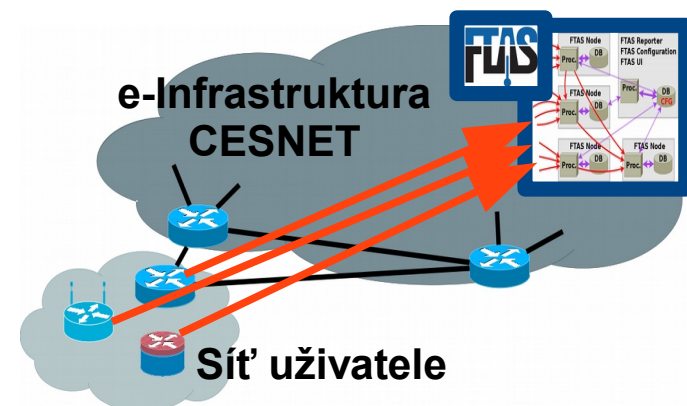
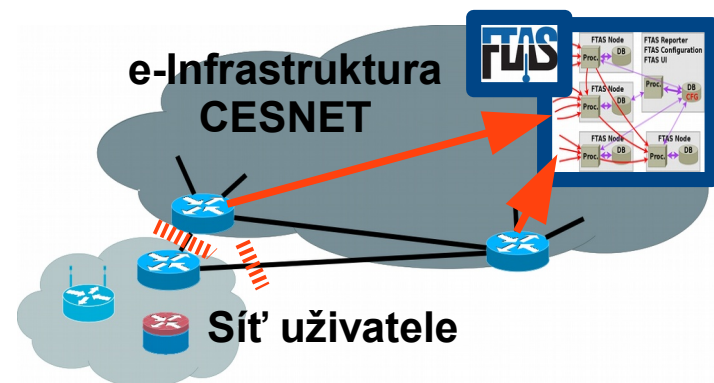
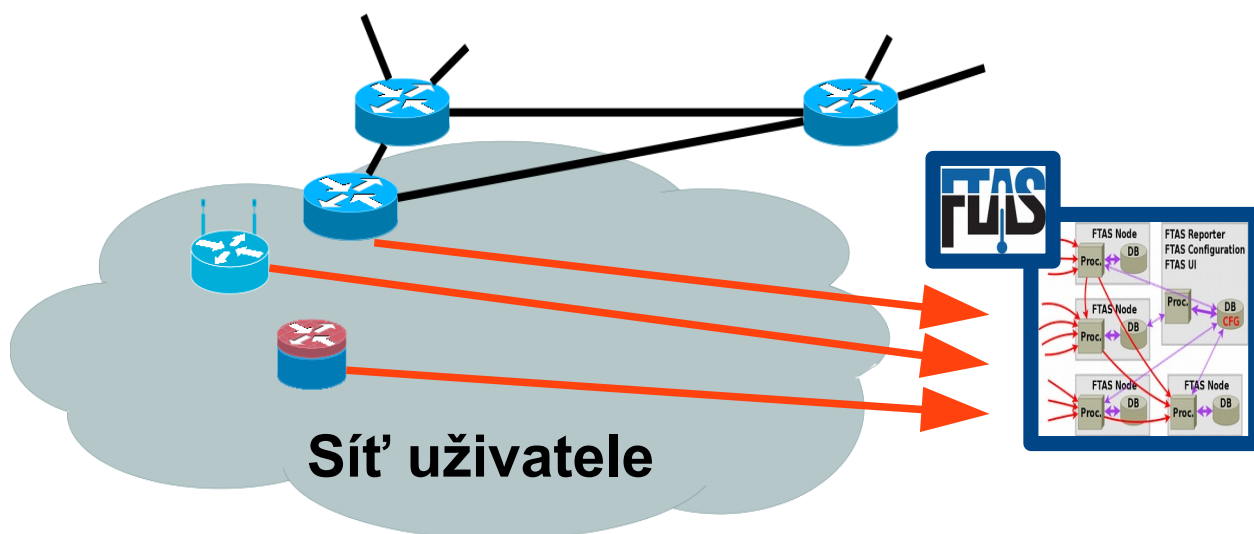
**Admin: up** max=1  
**Operating** max=1

Grid Computing  
Taipei TAIWAN

- **System FTAS → IP provoz na bázi toků**



- Zpracování Informací o IP provozu na bázi toků (tzv. NetFlow)
- Interaktivní UI, periodický reporting
- Detekce a notifikace událostí/anomálií na úrovni IP toků
- Síťová část e-Infrastruktury
- **Služba pro uživatele ...jak, kde ?**



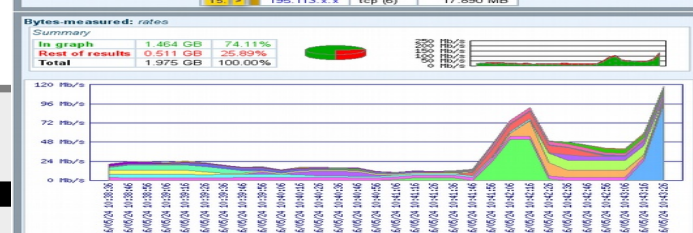




- **Systém FTAS → IP provoz na bázi toků**
- V závislosti na možnostech exportu zařízení
  - ~ běžné provozní záznamy (v1-v9, IPFIX, FNF, sflow)
  - Kompletní překladové provozní záznamy
  - Kompletní překladové logy (NSEL)
  - MAC adresy
- Plně konfigurovatelné detektory anomálií
- Fce UI → komplexní analýza provozu
- ...podmínky projektů ? ZKB ?



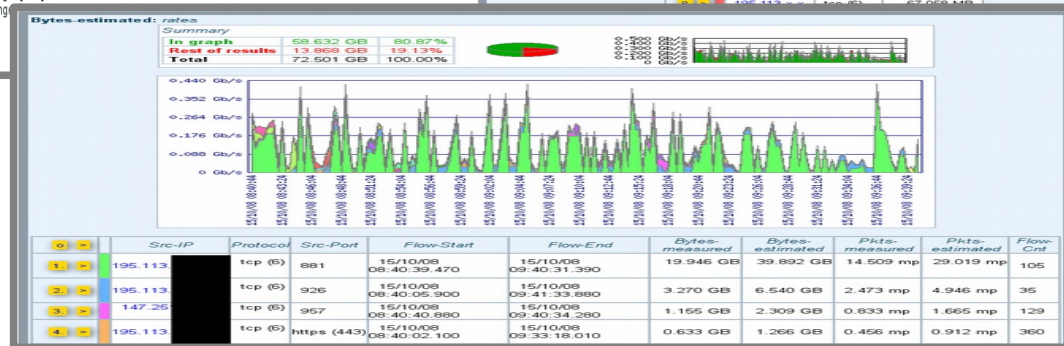
Q	Src-IP	Protocol	Bytes-measured
1	195.113.x.x	tcp (6)	172.809 MB
2	93.184.x.x	tcp (6)	0.209 GB
3	80.188.x.x	tcp (6)	166.831 MB
4	64.182.x.x	tcp (6)	117.781 MB
5	61.95.x.x	tcp (6)	93.136 MB
6	195.113.x.x	udp (17)	203.780 MB
7	195.113.x.x	tcp (6)	88.072 MB
8	195.113.x.x	tcp (6)	67.058 MB
9	57.240.x.x	tcp (6)	64.101 MB
10	31.13.x.x	tcp (6)	69.427 MB
11	31.13.x.x	tcp (6)	54.862 MB
12	195.113.x.x	udp (17)	50.665 MB
13	213.165.x.x	tcp (6)	52.543 MB
14	213.165.x.x	tcp (6)	66.397 MB
15	195.113.x.x	tcp (6)	17.890 MB



Q	Src-IP	Protocol	Bytes-measured
1	195.113.x.x	tcp (6)	172.809 MB
2	93.184.x.x	tcp (6)	0.209 GB
3	80.188.x.x	tcp (6)	166.831 MB
4	64.182.x.x	tcp (6)	117.781 MB
5	61.95.x.x	tcp (6)	93.136 MB
6	195.113.x.x	udp (17)	203.780 MB
7	195.113.x.x	tcp (6)	88.072 MB

From: nobody<nobody@ftas.uhk.cz>  
To: [redacted]@uhk.cz  
Cc: [redacted]  
Subject: FTAS security notification 'Flow burst - UHK destination IP' - 2001:718:1202:45  
Date: Wed, 17 Feb 2016 14:04:40+0100

Notification Detected : Flow burst - UHK destination IP - DETECTED traffic anomaly  
: 2001:718:1202:45: [redacted] (dest. IP) - found 448 (limit 30)  
Flow time range [GMT] : 16/02/17 13:03:45-16/02/17 13:03:45  
Flow time range observed at : 15/10/08  
Events total : 15/10/08  
Next message : 15/10/08



Q	Src-IP	Protocol	Src-Port	Flow-Start	Flow-End	Bytes-measured	Bytes-estimated	Pkts-measured	Pkts-estimated	Flow-Cnt
1	195.113	tcp (6)	881	15/10/08 08:40:39.470	15/10/08 09:40:31.390	19.946 GB	39.892 GB	14.609 mp	29.019 mp	105
2	195.113	tcp (6)	926	15/10/08 08:40:05.900	15/10/08 09:40:34.280	3.270 GB	6.540 GB	2.473 mp	4.946 mp	35
3	147.25	tcp (6)	957	15/10/08 08:40:02.100	15/10/08 09:40:34.280	1.165 GB	2.309 GB	0.833 mp	1.665 mp	129
4	195.113	tcp (6)	https (443)	15/10/08 08:40:02.100	15/10/08 09:40:34.280	0.633 GB	1.266 GB	0.456 mp	0.912 mp	360

**FTAS Query** Development installation at CESNET

Objects Selection ?

Use → ASR testing - NAT Events (NSEL) Flexible Netflow testing Cisco (FNI) testing Uthava PoP, testing flow-stream copy

Selected Objects Information

Object: Jihlava PoP, testing flow-stream copy type: Flow Data Source

Query Parameters ?

Fields to store in results ?

Fields Query Condition - Simple Form ?

Source: www.cesnet.cz, Destination: www.cesnet.cz

Accounted Organization: CESNET

Accounted Group: CESNET

Query Condition Management

Time Parameters ?

Aggregation →

Query Processing ?

Run Now Query →

Query Results ?

Show Results → COMPLETE QUERY, found 18 records total, 18 in last step (in 0 seconds).

- **IDS, IPS systémy Honeypoty**
- **Systémy pro sdílení informací, SIEM**
  - Sběr a „normalizace“ informací o anomáliích a detekovaných událostech



- **Forenzní laboratoř**

- Penetrační testy
- Zátěžové testy
- Analýzy událostí
- <https://flab.cesnet.cz/>



- **Bezpečnostní školení**
  - Na míru pro typové skupiny
    - Zaměstnanci
    - Studenti
  - Na míru tématicky
  - Technické a legislativní aspekty
  - Prevence, odpovědnost za svoje chování v síti, gramotné užívání výpočetní techniky
  - Diskuze o konkrétních problémech (v dané síti/místě/instituci)

- **eduID.cz - Česká akademická federace identit**

- **Jedno uživatelské jméno a heslo pro přístup k řadě síťových služeb** (*v multi-institucionálním prostoru*)
- Poskytovatelé služeb z národní komunity i mezinárodní
- Součást mezinárodní interfederace eduGAIN



- **Certifikáty pro uživatele a servery**

- Důvěryhodný server
- Důvěryhodná identita uživatele

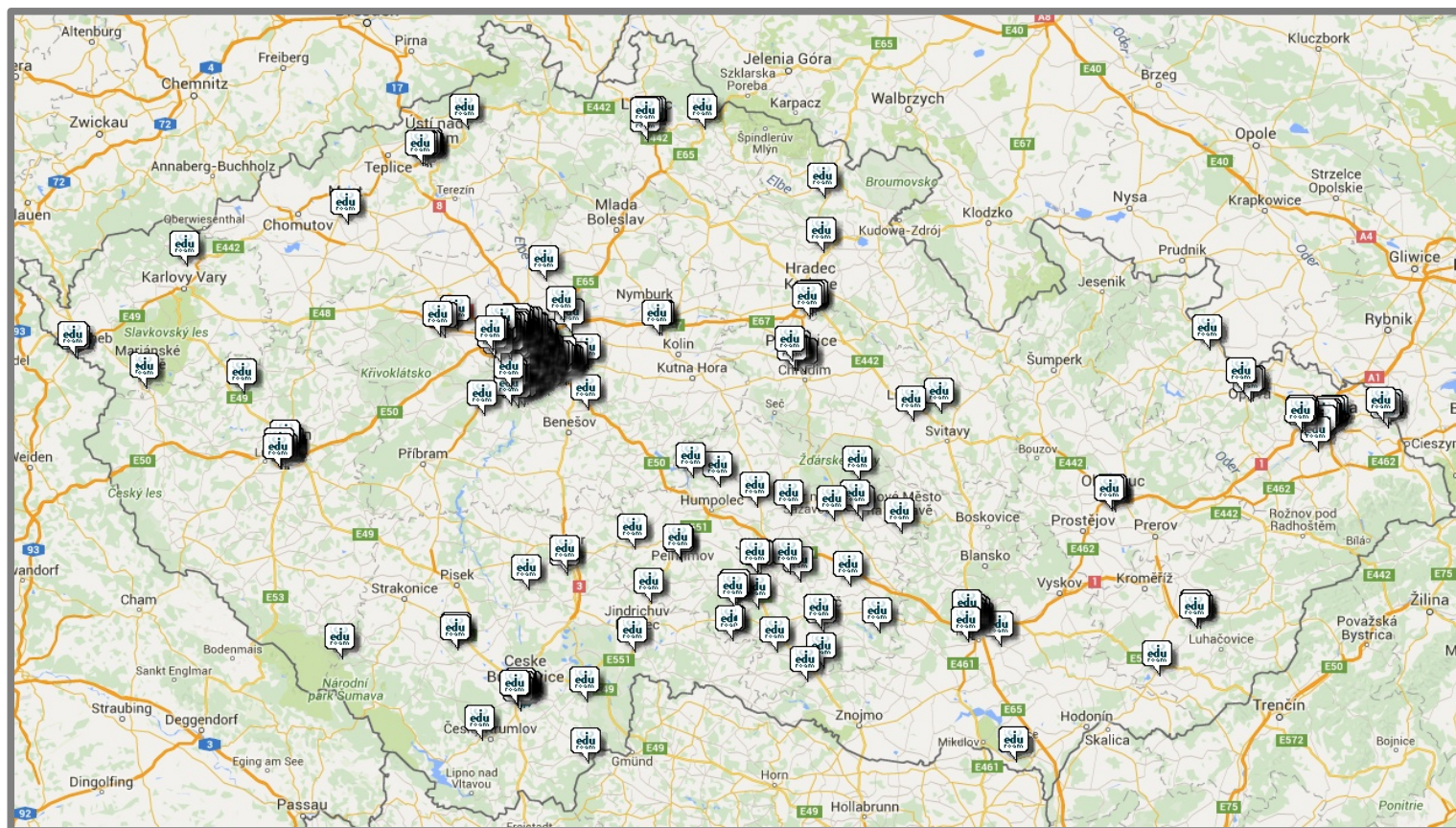
- **Jednotný systém správy účtů v e-Infrastruktuře**

- Některé služby odebírané na individuální bázi
- Strukturování uživatelské komunity
- Řízený přístup ke zdrojům





- **eduroam** - „služba na pomezí“: služba z oblasti ověření uživatelů, z pohledu koncového uživatele síťová služba - **roaming uživatelů v hostitelské síti**
  - Síťovou infrastrukturu zajišťuje hostitelská síť; síťová infrastruktura je opřena o autentizační infrastrukturu (technicky RADIUS server hostitelské organizace zapojený do národní hierarchie)



- **Monitorování kvalitativních charakteristik sítě**
  - Propustnost, zpoždění, jitter, ztrátovost apod.
  - Pro uživatele náročných aplikací, správce sítí apod.
- **Časové služby**
  - Časová synchronizace (NTP servery – Stratum 1)
  - Časová razítka (Time-Stamp Authority)
- **Technické konzultace**
  - Ve všech odborných oblastech



**<https://www.cesnet.cz/sluzby/>**

**[sluzby@cesnet.cz](mailto:sluzby@cesnet.cz)**

*Díky za trpělivost a pozornost...*

???