http://www.cesnet.cz/doc/datagram/

Datagram

zpravodaj sdružení CESNET

číslo 30

červenec 2013

# Stogigabitová páteřní síť

Hlavní novinkou uplynulých měsíců je nepochybně povýšení páteře sítě CESNET2 na přenosovou rychlost 100 Gb/s. Tuto změnu jsme plánovali a realizovali několik let – vše začalo v roce 2011 a úplné dokončení plánujeme na rok 2014. Během tohoto období postupně pořizujeme odpovídající technologie, nasazujeme je a testujeme jejich reálné chování. Výsledkem je, že všechny páteřní okruhy propojující Prahu, Brno, Olomouc a Hradec Králové přenášejí nyní data stogigabitovou rychlostí.

## Optická infrastruktura

Páteřní datové okruhy jsou realizovány optickými vlákny pronajatými od několika poskytovatelů jako tzv. temná vlákna. To znamená, že si pronajímáme jen samotná vlákna, která kompletně osazujeme vlastní technologií. Tento přístup je označován jako Customer Empowered Fibre (CEF) Network a CESNET patří mezi jeho průkopníky v celosvětovém měřítku.

První technologickou vrstvu páteřních okruhů tvoří DWDM. Jedná se o technologii fyzické vrstvy, která umožňuje po jednom vlákně přenášet několik navzájem zcela nezávislých signálů, a to i různými rychlostmi. Naše síť využívá dva typy DWDM zařízení: Jádro (celkem bezmála 1500 km vláken) je postaveno na komerčním systému Cisco ONS 15454 MSTP. Na méně vytížených trasách (více než 2500 km vláken) používáme prvky vlastní konstrukce CzechLight DWDM. V této části sítě zatím kapacita 100 Gb/s nemá smysl.

Zrychlení páteřní sítě proto začalo povýšením systému Cisco ONS 15454 MSTP na klíčových přenosových trasách, které proběhlo v letech 2011 až 2012. Zvýšil se jak počet paralelních kanálů na jednom vlákně, kterých dnes může být až 80, tak maximální podporovaná přenosová rychlost jednoho kanálu, jež vzrostla z 10 Gb/s na desetinásobek.

Během loňského roku jsme sérií testů prakticky ověřili výsledky teoretických výpočtů a simulací, že naše DWDM infrastruktura je schopna přenášet data rychlostí 100 Gb/s a že je možné tuto rychlost kombinovat s nižšími v rámci téhož vlákna. Navíc jsme potvrdili nezávislost na výrobci – testovali jsme produkty několika dodavatelů a nenarazili na problémy.

## IP a MPLS vrstva

Vyšší síťové vrstvy jsou implementovány v aktivních prvcích, ve kterých jsou zakončeny jednotlivé kanály optické infrastruktury. Jejich postupná výměna představuje finančně nejnáročnější položku této etapy rozvoje páteřní sítě.

V síťové vrstvě samozřejmě využíváme internetový protokol (IP), který je dnes de facto standardem síťové komunikace. Pro jeho přepravu používáme *Multiprotocol Label Switching (MPLS)*, který rozděluje naše směrovače do dvou skupin označovaných P a PE.

Směrovače jádra sítě nesou označení P (Provider) a mají na starosti doručování paketů podle značek, které jim byly přiděleny při vstupu do sítě CESNET2. Jejich funkce není složitá, ale musí pracovat velmi rychle, protože jimi protékají mimořádné objemy dat.

V přístupových bodech sítě se pak nacházejí směrovače PE (Provider Edge), jejichž prostřednictvím se připojují účastnické sítě. Jedná se o nejsložitější zařízení v celé síti, protože právě tyto směrovače přidělují paketům značky, podle nichž budou následně doručovány.

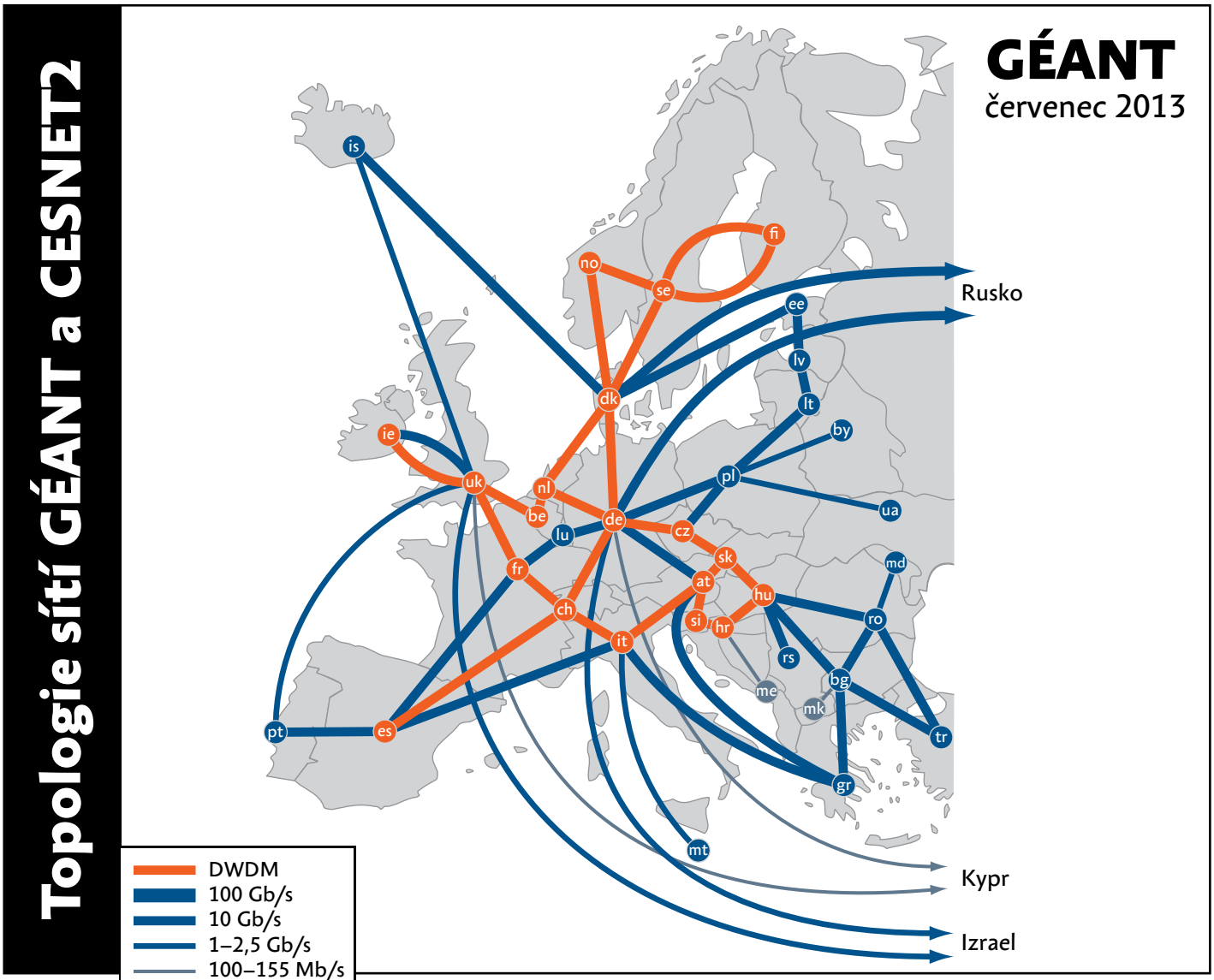
Aktuálně byly nahrazeny či posíleny všechny P směrovače. Starší a méně výkonná zařízení jsme postupně vyměnili za špičkové terabitové směrovače Cisco CRS-3 v konfiguraci podporující 100 Gb/s na jednotlivých rozhraních. Následně jsme mohli převést jádro sítě na tuto rychlost.

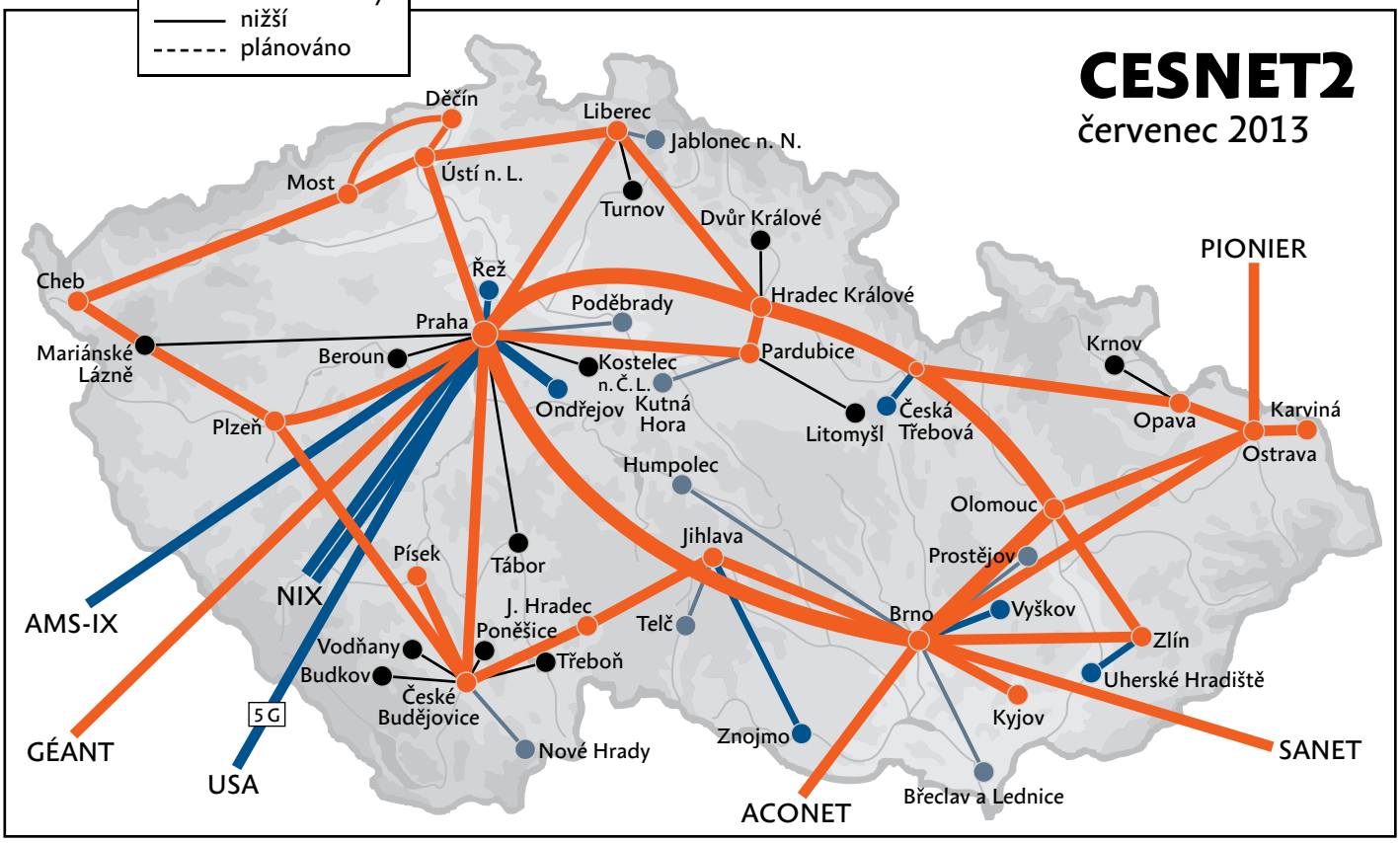
V další fázi, která zakončí tuto etapu rozvoje naší komunikační infrastruktury, nahradíme výkonnějšími modely stávající PE směrovače, což umožní povýšit přenosové rychlosti dalších uzlů sítě. Počítáme s okamžitou instalací 2×10 Gb/s ve všech inovovaných uzlech a postupným přechodem na 100 Gb/s podle potřeby.

## Mezinárodní kontext

CESNET samozřejmě neusiluje o vysoké přenosové rychlosti sám. Na 100 Gb/s postupně přechází i evropská akademická páteřní síť GÉANT, k níž jsme připojeni. Letos v květnu pak sítě GÉANT, Internet2, NORDUnet, ESnet, SURFnet a CANARIE společně ohlásily *Advanced North Atlantic 100G Project*, který by měl propojit evropské a severoamerické výzkumné sítě stogigabitovou kapacitou.

# Topologie sítí GÉANT a CESNET2



# Warden – nový přístup k zabezpečení sítí

Problematika bezpečnosti počítačových sítí, detekce, řešení a prevence incidentů na své aktuálnosti v dohledné době jistě neztratí. Neustále se hledají způsoby, jak komunikační infrastrukturu a služby ochránit před útoky a návštěvami nezvaných hostů. Systém *Warden*, který jsme navrhli a postupně vyvíjíme, je naším příspěvkem ke zlepšení situace.

## Motivace

Bezpečnost počítačových infrastruktur a řešení problémových situací mívají na starosti specializované týmy, označované CERT (Computer Emergency and Response Team) nebo CSIRT (Computer Security Incident Response Team).

Ke své činnosti využívají řadu technických prostředků, z nichž některé slouží ke zjišťování útoků (IDS, analýza síťového provozu či záznamů o činnosti počítačových systémů) nebo dokonce představují pasti na přicházející útočníky (tzv. honeypot). Tyto systémy generují různá varování a upozornění na aktuální či potenciální problémy, na něž příslušný bezpečnostní tým reaguje – bezpečnostní tým na základě varování podnikne patřičné kroky, například upraví pravidla firewallu nebo dohodne se správcem napadeného stroje způsob nápravy.

Využití informací z varovných systémů by však mohlo být efektivnější. Dnes často zůstává na lokální úrovni a omezuje se na obranu napadeného. Zpráva o napadení stroje či scanování sítě je však důležitá nejen pro správce cíle útoku, ale také pro správce stroje, ze kterého byl útok veden, a případně i správce transportních sítí – záleží na charakteru konkrétního útoku. Bezpečnostní tým sice může kontaktovat správce útočícího stroje nebo odpovídající části sítě, ale znamená to ruční vyhledání příslušného kontaktu a komunikaci elektronickou poštou, která ne vždy padne na úrodnou půdu.

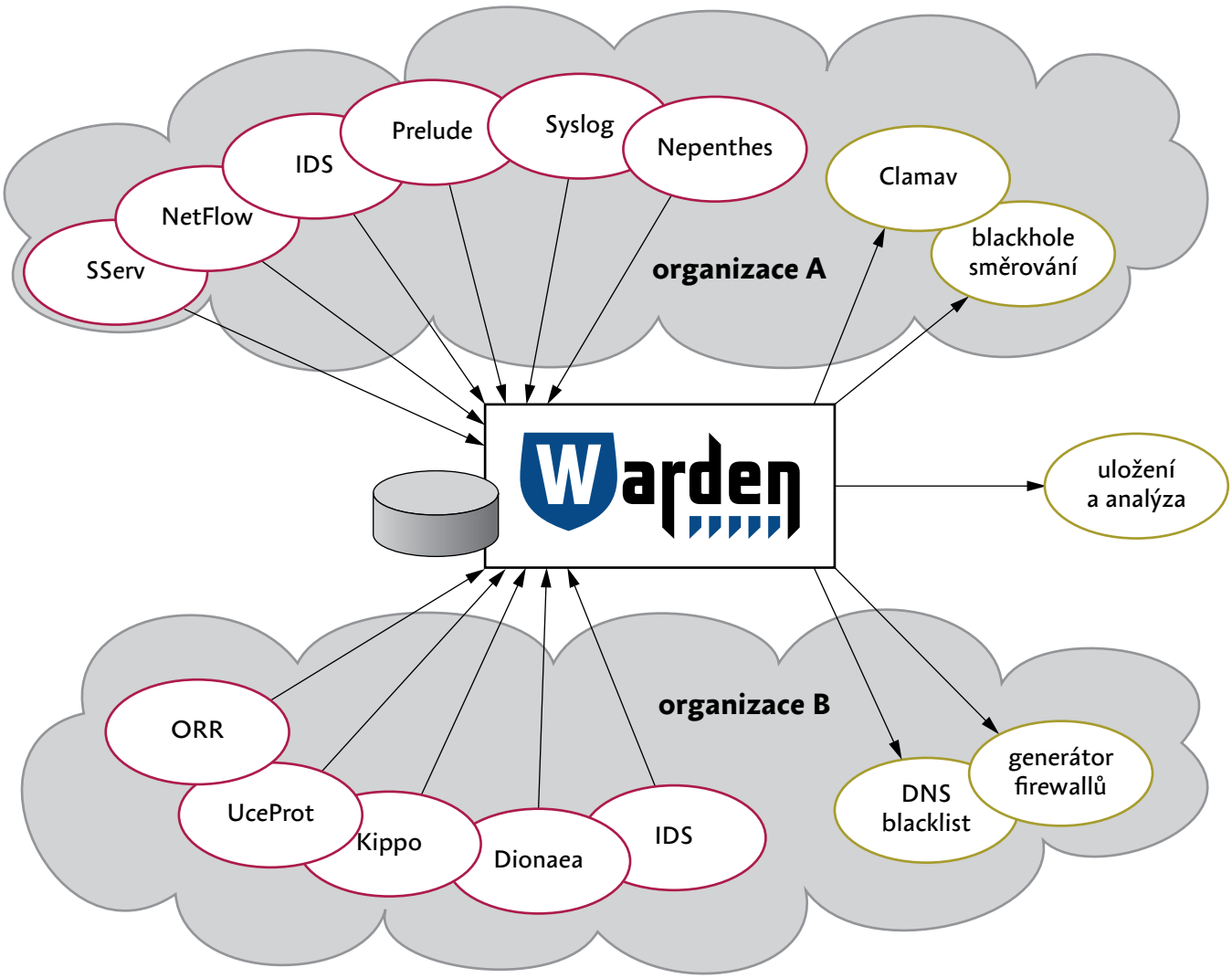
Alternativou je nahlásit incident některému z globálních sběrných míst, jako jsou projekty *Shadowserver*, *Mynetwatchman* či *Team Cymru*. To je ovšem druhý extrém, protože v těchto velkých projektech se zabývají především globálními trendy počítačových útoků.

Projekt *Warden* se snaží být střední cestou mezi lokálním a globálním zpracováním. V podstatě poskytuje infrastrukturu pro komunitní přístup k výměně informací o bezpečnostních problémech.

## Technické řešení

Systém *Warden* je postaven na principu klient-server. Jeho základem je server, který ve své centrální databázi

*pokračování na straně 4*



*pokračování ze strany 3*

ukládá data o zjištěných anomáliích a problémech. V terminologii systému *Warden* jsou označovány jako *události*. Pro každou událost eviduje řadu údajů, jako je místo a čas jejího vzniku, typ události či původce.

Zdrojem událostí je tak zvaný *odesílající klient*. Jedná se obvykle o jednoduchou nadstavbu či modul existujících systémů pro analýzu a detekci bezpečnostních rizik. Odesílající klient zajistí oznámení vzniklé události systému *Warden*, který ji následně uloží do své databáze. Jejich vzájemná komunikace probíhá formou webových služeb (HTTPS + SOAP).

Cílem systému je shromažďovat co nejkomplexnější informace, proto sbírá data od řady různých odesílajících klientů z několika organizací. Díky tomu jsou do databáze vkládány události detekované různými metodami v různých částech sítě, což je přínosné zejména u rozsáhlých útoků.

Získávání dat má na starosti *přijímající klient*. Organizace, která by ráda využívala informace shromážděné systémem *Warden*, nastaví odpovídajícím způsobem své přijímající klienty – typicky pro příjem událostí, které se týkají jejího adresního prostoru. Může tak získávat veškeré relevantní události bez ohledu na to, od kterého odesílajícího klienta pocházejí.

Činnost přijímajících klientů může být velmi pestrá. Mohou se omezovat na prosté oznamování zjištěných událostí, případně jejich vkládání do lokálních systémů pro sledování a vyřizování požadavků, až po automatické úpravy firewallových pravidel nebo jiné způsoby strojového blokování problémových aktivit.

## Stav projektu

Vývoj systému *Warden* jsme zahájili v roce 2011. U jeho kolébky stály potřeby bezpečnostních týmů CESNET CERTS (který stále tvoří jádro vývojového týmu) a CSIRT Masarykovy univerzity. Na experimentálním nasazení v síti CESNET se sběrem a/nebo využíváním dat aktuálně podílí osm organizací:

- CESNET,
- Masarykova univerzita,
- Vysoké učení technické v Brně,
- Slezská univerzita v Opavě,
- Západočeská univerzita v Plzni,
- Vysoká škola báňská – Technická univerzita Ostrava,
- Technická univerzita v Liberci a
- Univerzita Karlova

Samozřejmě uvítáme zájem dalších organizací. Více se dozvíte na adrese

*https://csirt.cesnet.cz/Warden/*

# Akce uspořádané a připravované

## CESNET Days

Naše e-infrastruktura se rychle rozvíjí a rozšiřuje nabídku služeb pro své uživatele. Velmi podstatná je pro nás zpětná vazba a vaše názory, kterými směry by se další vývoj nabízených služeb měl ubírat. Proto jsme pod názvem *CESNET Days* začali pořádat sérii neformálních setkání se zástupci připojených organizací.

Setkání jsou výjezdní a jsou organizována „na míru". Skupiny odborníků CESNETu postupně navštěvují jednotlivé organizace a diskutují s jejich zástupci. Cílem těchto setkání je představit novinky v našich službách. Zejména ale chceme diskutovat s lokálními odborníky o způsobech, jak a k čemu by nabízené možnosti mohli využívat, a jaké další služby či změny by zdejší výzkumné týmy uvítaly.

Doposud proběhly čtyři *CESNET Days* v následujících organizacích a termínech:

- Univerzita Pardubice (únor)
- Masarykova univerzita (únor)
- Vysoká škola báňská – Technická univerzita Ostrava (březen)
- Jihočeská univerzita v Českých Budějovicích (červen)

Seznam samozřejmě není konečný, rádi navštívíme všechny organizace, které budou mít o tuto akci zájem. Pokud stojíte o *CESNET Day*, kontaktujte Gabrielu Krčmařovou (*Gabriela.Krcmarova@cesnet.cz*), která s vámi ráda dohodne podrobnosti.

## TNC2013

*TERENA Networking Conference* se letos konala počátkem června v nizozemském Maastrichtu. Tradičně jsme měli zastoupení v programu konference: Josef Vojtěch mluvil o fotonických službách a vysokých přenosových rychlostech a Martin Žádník představil naše aktivity při monitorování a detekci bezpečnostních incidentů. Kromě toho Helmut Sverenyák, který je viceprezidentem sdružení TERENA pro konference, vedl závěrečné plenární jednání.

Archiv příspěvků najdete na stránce

*https://tnc2013.terena.org/*

## V říjnu chystáme seminář o službách

Na podzim připravujeme velký seminář o službách naší e-infrastruktury. Bude se konat *21. října* v Modré posluchárně Univerzity Karlovy v Celetné ulici v Praze. Na programu budou především informace o nejvýznamnějších novinkách a aktuálním stavu služeb, které nabízíme uživatelům. Podrobnější informace zveřejníme na *www.cesnet.cz* během září. Budeme rádi, když si pro nás rezervujete termín ve svém diáři.