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

Datagram

zpravodaj sdružení CESNET číslo 25

březen 2011

Výzkumný záměr Optická síť národního výzkumu ukončen. Co přinesl?

V letech 2004–2010 bylo nejvýznamnější činností sdružení CESNET řešení výzkumného záměru *Optická síť národního výzkumu a její nové aplikace*. O jeho významu pro nás nejlépe svědčí skutečnost, že jeho řešení jsme se věnovali sedm z celkem patnácti let vlastní existence sdružení.

Úspěšné zakončení záměru vybízí k ohlédnutí, čeho se nám během něj podařilo dosáhnout. V tomto čísle *Datagramu* se pokusíme shrnout nejvýznamnější úspěchy a změny v provozované infrastruktuře za uplynulých sedm let. Po obvyklé zprávě o výsledcích oponentního řízení proto následuje tematicky uspořádaný přehled klíčových výstupů.

Ukončením výzkumného záměru rozhodně nekončí naše angažmá v oblasti vědy, výzkumu a vzdělávání. Počínaje rokem 2011 jsme začali řešit projekt *Velká infrastruktura CESNET*, jehož výsledkem má být další rozvoj infrastruktury pro výzkum, vývoj, inovace a vzdělávání a rozšíření jejích služeb.

Oponentní řízení

Závěrečná oponentura výzkumného záměru proběhla 8. března 2011. Kromě výsledků roku 2010 při ní oponentní rada hodnotila i celý výzkumný záměr.

Konstatovala, že vybudovaná e-infrastruktura, která je hlavním výstupem záměru, se svými parametry řadí mezi nejlepší akademické sítě v Evropě a poskytuje dobrý výchozí bod pro další rozvoj. Rada také kladně ohodnotila úspěšný přenos výsledků výzkumu a vývoje do praxe, který významným způsobem přispěl ke kvalitě výsledné infrastruktury. Podle jejího názoru se podařilo velmi dobře skloubit poskytování infrastruktury a služeb s experimentálními aktivitami.

Oponentní rada ocenila vysokou odbornou úroveň řešení, která se odrazila mimo jiné i v zapojení řešitelů do řady relevantních mezinárodních projektů.

Kompletní zápis z oponentního řízení, včetně oponentských posudků, si můžete přečíst na adrese

http://www.cesnet.cz/doc/2010/oponentura/

Součástí podkladů pro oponentní řízení je tradičně i rozsáhlá zpráva, jež na 213 stranách shrnuje naši činnost a výsledky dosažené v loňském roce. Vedle vlastního výzkumného záměru informuje také o mezinárodních projektech, do nichž jsme byli zapojeni. Odkaz na text zprávy najdete u zápisu z oponentního řízení.


Zpráva o řešení výzkumného záměru

2010

Optická síť národního výzkumu a její nové aplikace

identifikační kód MSM6383917201
nositel CESNET, z. s. p. o.
zástupce nositele Ing. Josef Kubíček, předseda představenstva; prof. Ing. Miroslav Tůma, CSc., místopředseda představenstva
hlavní řešitel Ing. Jan Gruntorád, CSc.
kontaktní adresa CESNET, z. s. p. o., Zikova 4, 160 00 Praha 6, tel. 224 352 994, fax 224 313 211, e-mail info@cesnet.cz

CESNET

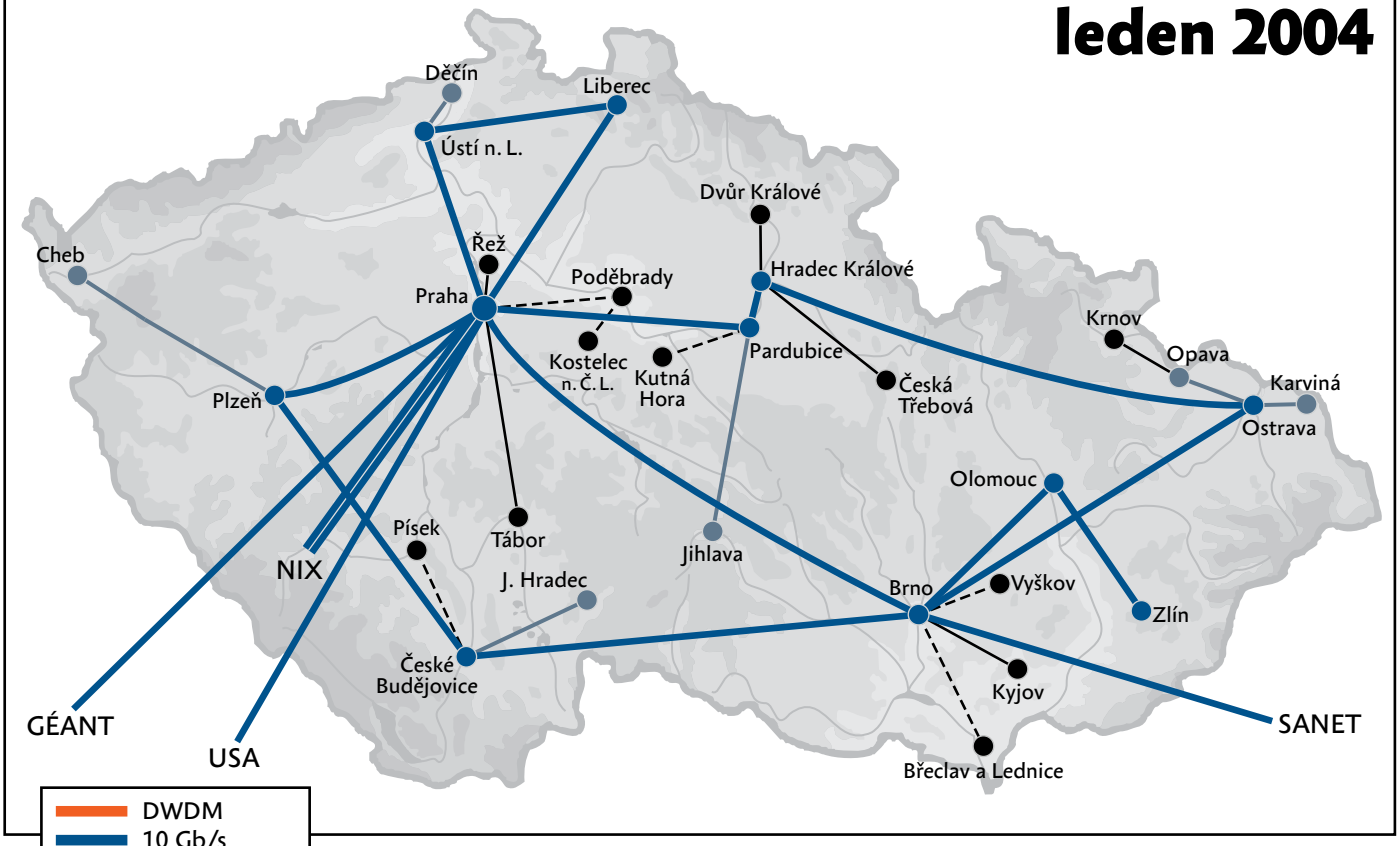
Páteřní síť

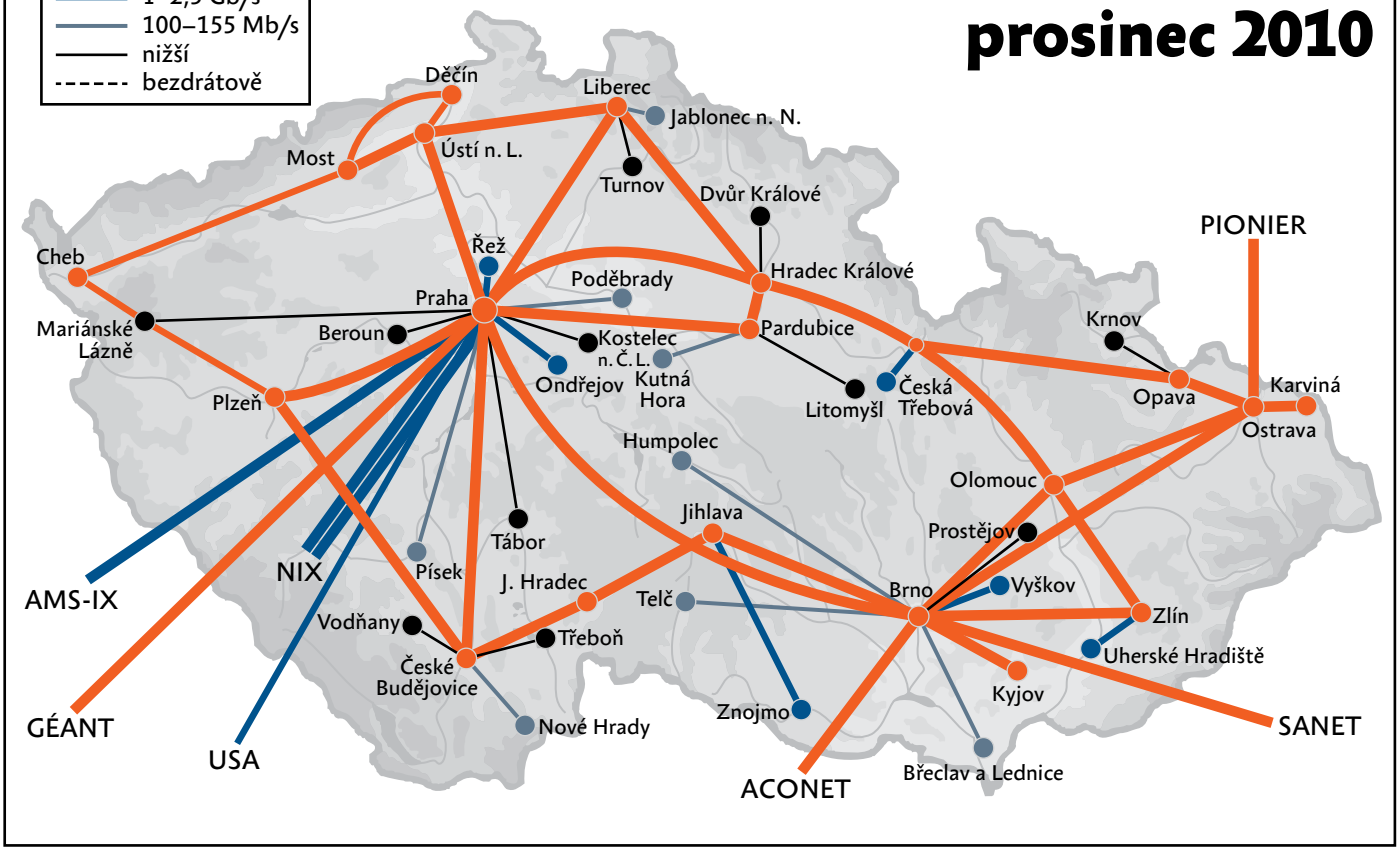
Páteřní síť CESNET2 představuje nejviditelnější a nejvýraznější výstup výzkumného záměru. Má dvojí roli – slouží jednak k ověřování námi vyvíjených komponent a systémů, zejména ji však využívají připojené organizace pro datové komunikace spojené s vlastními aktivitami v oblasti výzkumu, vývoje a vzdělávání.

Změny, jimiž prošla během výzkumného záměru, jsou vpravdě radikální. Abychom je ilustrovali, změnili jsme tentokrát mapovou přílohu *Datagramu* a místo obvyklé aktuální mapy evropské páteře GÉANT jsme zařadili mapu sítě CESNET2 z ledna 2004, kdy výzkumný záměr začínal.

Nárůst přenosových kapacit i „pokrytí“ sítě jsou při srovnání se současným stavem jasně patrné. Kvantitativní parametry však rozhodně nejsou jedinou změnou komunikační páteře. V nízkých vrstvách stojí za pozornost, že počátkem roku 2004 byly stále některé z tras do menších uzlů bezdrátové. O sedm let později je páteřní infrastruktura z valné většiny optická, což přináší s vyšší přenosovou rychlostí i řádově nižší chybovost.

Topologie sítě CESNET2 na začátku a konci výzkumného záměru





Rokem 2004 začal také postupný *přechod na technologii DWDM*, který představoval principiální změnu v charakteru sítě a jejích službách. Klíčové trasy páteřní sítě v době zahájení záměru používaly přenosovou technologii PoS STM-16/OC-48 nebo gigabitový Ethernet. Jejich přenosové rychlosti 2,5 resp. 1 Gb/s dostačovaly tehdejším potřebám, problémem ale byly konflikty mezi experimentálními a provozními prvky páteře. Snaha poskytovat spolehlivé transportní služby připojeným institucím omezovala možnosti využívat síť k experimentálním účelům.

Koncem roku 2004 jsme propojili první DWDM trasou nejvýznamnější uzly Praha a Brno. O rok později došlo k uzavření DWDM kruhu Praha–Brno–Olomouc–Hradec Králové–Praha, následovala další a další města až do současné podoby bohatě propojené DWDM sítě, kterou vidíte na spodní mapce. Vedle komerčních systémů Cisco ONS 15454, které najdete v jádru sítě na trasách o celkové délce 1410 km, v síti pracují i prvky *CzechLight* vlastní konstrukce, jimiž je osazeno celkem 2660 km tras. Celková délka DWDM infrastruktury tedy přesahuje 4000 km.

Díky DWDM lze po jednom optickém vlákně přenášet několik zcela nezávislých signálů. To umožňuje dokonale oddělit experimentální provoz od rutinního a navíc díky velkému počtu samostatných (byť virtuálních) spojů nabídnout nové typy služeb – vyhrazené trasy na žádost, využívané například pro přenosy mimořádných datových objemů při experimentech.

Také ve vyšších vrstvách síťové architektury došlo k řadě změn. Z uživatelského pohledu nejzajímavější pokrok představuje schopnost páteře vytvářet *virtuální privátní sítě* a poskytovat *služby s definovanou kvalitou (QoS)*. Podstatně jsme zkvalitnili podporu nového internetového protokolu IPv6. Z původního softwarového směrování jsme přešli na technologii 6PE, která pro nový protokol zajišťuje služby plně srovnatelné se současným IPv4, a později jsme doplnili i plnohodnotnou podporu skupinového směrování (IPv6 multicast).

Velkou pozornost věnujeme robustnosti a spolehlivosti poskytovaných služeb. Páteřní uzly jsou připojeny alespoň dvěma nezávislými okruhy, u nejvýznamnějších uzlů v Praze a Brně jsme přistoupili k fyzickému rozdělení do dvou různých lokalit. Také rozhodující technologické prvky jsou vnitřně redundantní a jejich klíčové komponenty (řídicí procesory, zdroje apod.) jsou zdvojeny.

Výsledkem našeho úsilí je síť s unikátní nabídkou služeb, vysokou spolehlivostí (průměrná dostupnost všech uzlů přesahuje 99,99 %, v případě páteřních uzlů dosahuje 100 %) a potenciálem dalšího rozvoje.

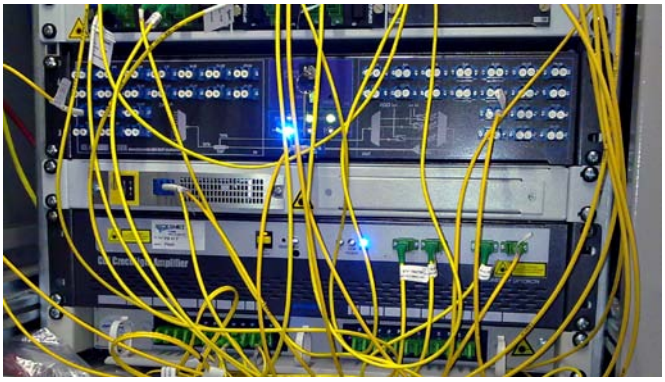
Optické sítě

Základem sítě CESNET2 je optická síť. Vychází z infrastruktury pronajatých optických vláken osazených technologií DWDM, která umožňuje jak vybudování dostatečně propustné (10 Gb/s) a spolehlivé IP sítě pro standardní internetovou komunikaci, tak vytváření vyhrazených kanálů (aktuálně 32, rozšiřitelné na 80) či sítí pro náročné datové přenosy. Tato infrastruktura je připravena i pro vyšší rychlosti, např. 40 Gb/s.

Během řešení výzkumného záměru jsme při jejím rozvoji vycházeli z námi navržených konceptů. Nejvýznamnějším z nich je budování komunikačních sítí řízených uživateli, jejichž fyzickou vrstvu tvoří nenasvícená optická vlákna – *CEF (Customer Empovered Fibre)*. Tento koncept, mezi jehož průkopníky se řadíme, později převzala řada sítí národního výzkumu a je také základem pro budování evropské komunikační páteře pro výzkum a vývoj *GÉANT*. Řešitelé výzkumného záměru se zasadili o uplatnění tohoto konceptu v rámci mezinárodních projektů *SEEFIRE (www.seefire.org)* a *Porta Optica Study (www.porta-optica.org)* a výrazně tak urychlili vývoj sítí národního výzkumu v méně rozvinutých regionech.

CESNET pravidelně pořádá na téma CEF mezinárodní workshop, který je velmi uznávanou akcí a jeho závěry významně ovlivňují světový vývoj v oblasti budování a rozvoje komunikačních sítí pro potřeby výzkumu. V loňském roce proběhl již šestý ročník tohoto setkání, opět s velmi reprezentativní mezinárodní účastí.

Dalším konceptem, který přináší nové možnosti při budování optických sítí propojujících efektivně sousední státy, je takzvaný *CBF (Cross Border Fibers)*. Tímto způsobem je síť CESNET2 propojena nad rámec propojení do sítě GÉANT se sousedními sítěmi výzkumu a vývoje SANET (Slovensko), ACOnet (Rakousko) a PIONIER (Polsko). Podobný přístup začaly používat i další evropské sítě podobného charakteru.



Prvky CzechLight v chebském uzlu sítě CESNET2

Kromě konceptuálních přístupů jsme svou pozornost zaměřili také na techniku, která je k jejich realizaci nezbytná. Vyvinuli jsme řadu *původních plně optických přenosových systémů CzechLight*, která v současnosti zahrnuje prototypy a funkční vzory optického zesilovače CLA, zesilovače CLR, přepínače CLS, multicastujícího přepínače CLM, kompenzátoru CLC, rekonfigurovatelného optického add-drop multiplexoru CL-ROADM, variabilního multiplexoru CL-VMUX, „bezbarvého“ multiplexoru/demultiplexoru, laditelného zdroje více vlnových délek, fotonického konvertoru vlnových délek a monitoru optických kanálů CL-OCM.

Prvky řady *CzechLight* našly i praktické uplatnění: v naší licenci je vyrábějí a nabízejí specializované firmy. Jejich největší výhodou je otevřenost. Ta znamená, že softwarové úpravy může provádět majitel nebo správce zařízení sám, nemusí o to žádat CESNET či výrobce. Tím je z hlediska rozhodování o dalším rozvoji sítě nezávislý. Nenabídne-li mu všechny požadované funkce výrobce, může si je doplnit sám nebo požádat o implementaci jiného partnera. To dává majiteli zařízení velkou svobodu a konkurenční výhodu.

Další výhodou je zvládnutí plně optické (all-optical) technologie, jejíž uplatnění přináší nižší ceny a vyšší přenosové rychlosti. Příkladem může být vynechání OEO (opto-elektro-optických) konverzí či obcházení (bypass) elektronických zařízení v uzlech sítě.

CESNET díky výsledkům výzkumného záměru disponuje duševním vlastnictvím pro budování otevřených optických sítí a jejich komponent. Jeho součástí jsou jak postupy a prostředky projektování a dohledu plně optických přenosových systémů, tak návrh prototypů a funkční vzorů pro jejich oživení. Velmi důležité jsou rovněž zkušenosti CESNETu s provozním uplatněním optických prvků a s nasazením v zahraničí.

Monitorování sítě

Informace o zatížení sítě a charakteru přenášených dat jsou velmi důležité jak pro provoz infrastruktury, tak pro plánování jejího rozvoje. Běžně používané prostředky narážejí v naší síti na řadu omezení, věnujeme proto velkou pozornost vývoji vlastních nástrojů pro monitorování sítí. Vedle softwarových systémů popsaných v této části jsme během záměru vyvinuli i několik hardwarových prvků, jimž se věnujeme dále.

Systém G3 slouží především pro souvislé a plošné sledování rozsáhlých síťových vysokorychlostních infrastruktur, ale obecně je použitelný pro sledování jakékoli infrastruktury ze strany síťového rozhraní jejích komponent (např. součásti gridu, serverové systémy, dedikované E2E spoje, virtuální L2 infrastruktury a další). Systém lze dále rozšířit pro sledování sledování specifických technologických celků (v praxi např. videostreaming v rámci sítě CESNET2, zařízení rodiny CzechLight, MTPP a další).

Měřicí část systému se významným způsobem opírá o zabudovanou podporu SNMP, ale pro sběr dat používá i další metody. Systém je schopen provádět sběr dat s libovolným dynamickým časovým krokem, což umožňuje zachytit alespoň určité prvky dynamiky chování sledovaných objektů a zároveň příliš nezatěžovat sledovaná zařízení.

Uživatelské WWW rozhraní je plně interaktivní. Jeho nadstandardní vlastnosti spočívají, kromě jiného, v možnosti ad-hoc řízeného sdružování jednotlivých objektů a generování agregovaného výstupu – v praxi např. souhrnný tok skupinou síťových rozhraní daného účelu nebo dostupnost skupiny zařízení apod.

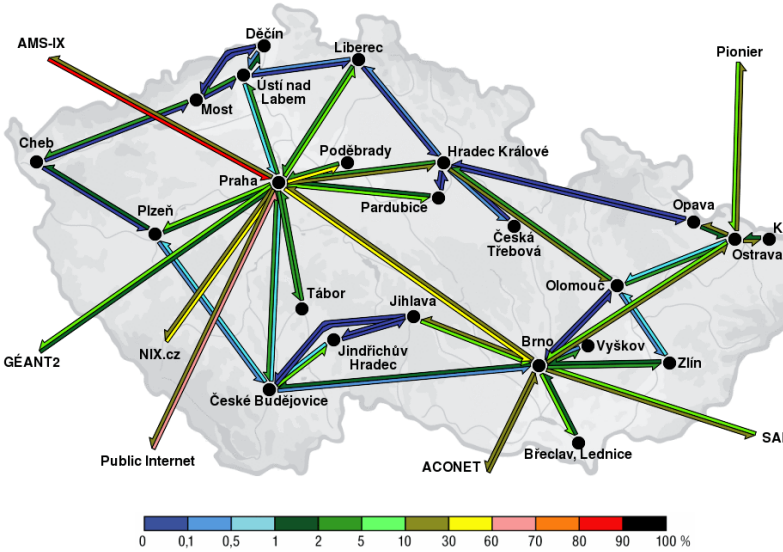
Součástí systému je speciální modul, elektronický klient, který simuluje chování uživatele a je schopen periodicky vytvářet statické výstupy pro konkrétní účely – např. mapu využití infrastruktury. Kromě sítě CESNET2 se systém úspěšně uplatnil např. ve výzkumném projektu FEDERICA 7. rámcového programu EU.

Cílem *systému FTAS* je souvislé plošné sledování IP provozu založené na distribuovaném zpracování informací o tocích v síti (tzv. NetFlow). Systém přijímá informace z primárních zdrojů (směrovače nebo sondy, např. FlowMon) a zpracovává je pro další využití. Základní formou zpracování je ukládání záznamů podle primárních zdrojů jako příprava pro následné obecné vyhledávání.

Schopnost efektivně vyhledat informace o provozu přeneseném v minulosti na základě ad-hoc požadavku je princip, od kterého se odvíjí celá vnitřní architektura systému. Historie uchování provozních informací není systémem omezena, je dána pouze dostupnými zdroji (kapacita úložišť).

Další formou zpracování provozních záznamů je jejich hierarchická klasifikace (aktuálně tři úrovně) podle libovolné kombinace podmínek (např. provoz směřující do IP adresových rozsahů instituce a jejích součástí přenesený konkrétním síťovým rozhraním na určitém zařízení) a uložení informací o provozu se společným jmenovatelem. Tímto způsobem uložená neagregovaná data je možno následně automaticky statisticky zpracovávat na základě agregujících a třídících kritérií a vytvářet datovou základnu pro následné statistické výstupy (top-listy uzlů instituce, rozložení objemu provozu mezi součásti instituce a podobně).

Systém je plně kompatibilní s IPv6 – je schopen zpracovávat (a v případě sítě CESNET2 se tak rutinně děje) informace o provozu přenášeném protokolem IPv6 a zároveň je schopen přijímat a redistribuovat provozní záznamy pomocí IPv6. Systém je vybaven interaktivním uživatelským WWW rozhraním s komplexním vyhledávacím a vizualizačním aparátem.



Mapa zatížení sítě CESNET2 – výstup monitoringu

Kromě nasazení v páteři sítě CESNET2 (cca 13 uzlů), kde systém slouží bezpečnostnímu týmu CESNET-CERTS, správcům páteřní sítě a správě a bezpečnostním týmům připojených institucí, je systém nasazen ve vnitřních sítích některých připojených organizací (např. MU, TUL, ZČU, MNUL) i mimo síť CESNET2 (např. Seznam.cz, a. s.).

Sledování a optimalizace výkonnostních charakteristik

Část našich aktivit se věnovala výzkumu metod sledování výkonnostních charakteristik sítě, vývoji souvisejících nástrojů a jejich nasazení v síti. Spolupracovali jsme s partnery v mezinárodních projektech SCAMPI, LOBSTER, GN2 a GN3, nichž první dva byly přímo zaměřeny na návrh a nasazení škálovatelné architektury MAPI (Monitoring Application Programmable Interface) pro vývoj přenositelných aplikací pro pasivní monitorování sítí do rychlosti 10 Gb/s. Práce pokračují i v projektu GN3, ve kterém vyvíjíme nástroje pro klasifikaci síťového provozu s využitím metod počítačového učení.

Pro hardwarovou akceleraci monitorování jsme vyvinuli platformu *MTPP10 (Modular Traffic Processing Platform)*. Její unikátní vlastností je možnost sestavování hardwarově akcelerovaných aplikací uživatelem bez programování a vývojových nástrojů, jež vychází z principu částečné dynamické rekonfigurace. Všechny vytvořené moduly pracují do rychlosti 10 Gb/s. Verze MTPP40 používá pevný firmware, podporující rychlosti až 43 Gb/s. K dispozici je modul pro testování bitové chybovosti (BERT).

Univerzální koncepce platformy MTPP, původně určené pro monitoring, umožnila její úpravy pro jiné typy aplikací. Největší ohlas vzbudila platforma *MVTP (Modular Video Transport Platform)*, která umožňuje přenos až 8 kanálů obrazu s vysokým rozlišením (HD) paketovou sítí na libovolnou vzdálenost. Obrazové kanály lze použít v kombinacích pro stereoskopické přenosy (3D) nebo velmi vysoká rozlišení až do 4K (4096×2160). Platforma umožňuje spolupráci distribuovaných týmů a přináší nové možnosti výuky. Byla využita při postprodukci v audiovizuálním průmyslu nebo přenosech operací z lékařských robotů. Tyto možnosti jsme demonstrovali na velkou vzdálenost na mezinárodních akcích. Funkční vzorek platformy je připravován k výrobě v rámci projektu POVROS programu Alfa.

V průběhu řešení výzkumného záměru jsme věnovali pozornost také budování *časových služeb*. Navrhli jsme vlastní řešení NTP serverů, které obsahují obvody pro zvýšení přesnosti i stability času. Instalovali jsme nové přijímače GPS jako referenční zdroje času, stabilitu jsme dále zvýšili pomocí rubidiových hodin, které jsou schopny udržet časovou stupnici po dobu několika dní i v případě poruchy GPS přijímače. V současné době provozujeme 4 primární (Stratum 0) NTP servery.

Další časovou službou jsou časová razítka (TSA). Na bázi otevřeného systému OpenTSA jsme zprovoznili dva TSA servery. Jejich zdrojem časové informace jsou opět rubidiové hodiny, čímž je zaručena přesnost časových razítek lepší než 1 ms.

Od roku 2009 se věnujeme přesným přenosům času (v metrologickém smyslu) v prostředí plně optické sítě. Navrhli a sestavili jsme vlastní adaptéry, které jsou schopny přenášet čas s přesností lepší než 1 ns na vzdálenost okolo 1000 km. Metodu jsme ověřili v experimentální provozu mezi českou a rakouskou národní referenční laboratoří času (UFE AV ČR v Praze a BEV ve Vídni). Průběžně publikujeme naše výsledky a připravujeme rutinní provoz systému. Výsledky našeho výzkumu jsou také chráněny užitnými vzory a patenty.

Programovatelný hardware

O programovatelný hardware jsme se začali zajímat v roce 2002, tedy ještě během předchozího výzkumného záměru, původně ve spojení s IPv6. Prvním velkým úkolem byl vývoj hardwarově akcelerovaného směrovače IPv6 na bázi osobního počítače. Tento ambiciózní záměr, s nímž se CESNET účastnil také mezinárodního projektu *6NET*, byl sice naplněn jen částečně, vývojový tým na něm však získal potřebné zkušenosti a většina dokončených komponent byla později využita v jiných zařízeních, určených především pro monitorování vysokorychlostních sítí.

Základem pro hardwarově akcelerované zpracování datových paketů je námi vyvinutá rodina karet *COMBO*, z nichž lze podle potřeby sestavovat různě konfigurované adaptéry, sestávající vždy z páru navzájem propojených karet: základní karty a karty rozhraní. Karty COMBO jsou osazeny výkonnými obvody typu FPGA, v nichž lze realizovat i komplikované algoritmy.

Na základě získaných zkušeností jsme v roce 2008 navrhli rodinu karet COMBO verze 2, která svými parametry míří k přenosovým rychlostem 40 Gb/s a vyšším. Prvotní testy 40GbE jsme s těmito kartami realizovali v roce 2010 a dále na nich pracujeme.

Pro karty COMBO jsme vytvořili firmwarovou platformu *NetCOPE*, která umožňuje rychlý vývoj hardwarově akcelerovaných aplikací. *NetCOPE* poskytuje vývojáři jednotné prostředí nezávislé na konkrétně použitých kartách, v němž jsou k dispozici často používané komponenty, jakými jsou třeba buffery pro síťovou komunikaci nebo jednotka pro realizaci rychlých datových přenosů sběrnicí PCI Express.

V průběhu výzkumného záměru jsme nad kartami COMBO a platformou *NetCOPE* vyvinuli tyto hlavní síťové aplikace:

- *FlowMon* je sonda pro sběr informací o IP tocích (IP traffic flows) a jejich export v některém z formátů NetFlow5, NetFlow9 a IPFIX. Její vývoj byl zahájen v rámci mezinárodního projektu GN2 a pokračoval až do konce výzkumného záměru. Poslední verze této sondy s kartami COMBOv2 umožňuje zpracovat obousměrný provoz na plně zatížené lince 10GE bez ohledu na velikost paketů a patří v této oblasti ke světové špičce.
- *NIFIC* je hardwarově akcelerovaný bezstavový firewall, jehož hlavní funkcí je filtrovat pakety na základě stanovených pravidel. Aktuální verze této aplikace zahrnuje i poměrně bohaté možnosti filtrování provozu IPv6 a je také schopna provozu na plně zatížené lince 10GE bez jakýchkoli ztrát paketů.
- *HAMOC* (Hardwarově Akcelerované MOnitorovací Centrum) je obecnější aplikace, která umožňuje monitorování sítě pružně uspořádat podle potřeby a situace. Hardwarově akcelerován je výpočet hodnoty rozptylovací funkce z vybraných polí hlavičky paketu, na jejímž základě lze příchozí datový tok efektivně rozdělit do více DMA kanálů a dílčí toky zpracovat na různých procesorových jádrech standardními softwarovými aplikacemi.

Ke konfiguraci výše uvedených síťových aplikací používáme vlastní implementaci konfiguračního protokolu NETCONF zvanou *Netopeer*. V souvislosti s vývojem tohoto softwaru jsme se také zapojili do standardizačních aktivit v rámci IETF, výsledkem je mimo jiné RFC 6110.

Karta rozhraní COMBOI10G4 se čtyřmi porty 10GE

Výzkumné výsledky jsme úspěšně převedli do praxe. V letech 2007 a 2008 podepsal CESNET smlouvy se společností INVEA-TECH, a.s., na jejichž základě tato firma získala licence ke komerčnímu využití výsledků a některé z nich (např. *FlowMon* nebo *NetCOPE*) také v upravené podobě nabízí na trhu.

Naše činnost byla založena na těsné spolupráci s několika vysokými školami a významném zapojení jejich studentů do vývojového týmu. Vznikla tak řada bakalářských, diplomových a disertačních prací, z nichž některé získaly i významná národní a mezinárodní ocenění.

Autentizace, autorizace a mobilita

Metody ověřování totožnosti uživatelů a řízení jejich přístupových práv prodělávají v posledních letech intenzivní rozvoj. S rostoucím počtem on-line služeb roste i zájem o pohodlné, ale zároveň bezpečné metody autentizace a autorizace uživatelů. Vzhledem k charakteru sdružení jsme se zabývali především vývojem a implementací infrastruktury pro federalizované sdílení služeb a zdrojů. Těmito zdroji mohou být jak síťové aplikace tak i samotná síťová konektivita.

Mezi klíčové úspěchy naší práce patří vznik a bouřlivý rozvoj projektu *eduroam.cz (www.eduroam.cz)* podporujícího mobilitu uživatelů. 35 zapojených organizací poskytuje přístup k síťové konektivitě ve více než 460 lokalitách v ČR. Zapojení infrastruktury *eduroam.cz* do mezinárodního projektu *eduroam* umožňuje našim uživatelům přístup k Internetu v sítích partnerů po celé Evropě a v mnoha dalších akademických sítích po celém světě.

Využití domovské identity uživatelů pro přístup ke službám provozovaným jinými institucemi umožňuje národní akademická federace identit *eduID.cz (www.eduID.cz)*, již jsme založili v roce 2008. V průběhu řešení výzkumného záměru jsme vybudovali plnohodnotnou federaci založenou na standardech SAML. Uživatelé z 18 akademických institucí dnes mohou využívat více než 30 služeb nabízených akademickými i komerčními poskytovateli (např. poskytovatelé digitálního obsahu jako EBSCO, Elsevier, IEEE, Ovid, Thomson Reuters nebo licencovaného software jako Microsoft). Propojení s federacemi mimo ČR zabezpečujeme s pomocí projektu *eduGAIN* vyvíjeného v rámci GN3.

Byli jsme aktivními spolutvůrci projektů *TERENA SCS (Server Certificate Service)* a nástupnického *TCS (TERENA Certificate Service)*, které poskytují X.509 certifikáty pro servery a uživatele vydané akceptovanými komerčními certifikačními autoritami. V prosinci 2010 bylo českým akademickým institucím vydáno téměř dva tisíce TCS certifikátů. V průběhu řešení výzkumného záměru jsme také poskytovali našim uživatelům služby certifikační autority *CESNET CA (pki.cesnet.cz)*. Ta vydala bezmála čtyři tisíce certifikátů převážně gridovým uživatelům a správcům gridových služeb.

MetaCentrum

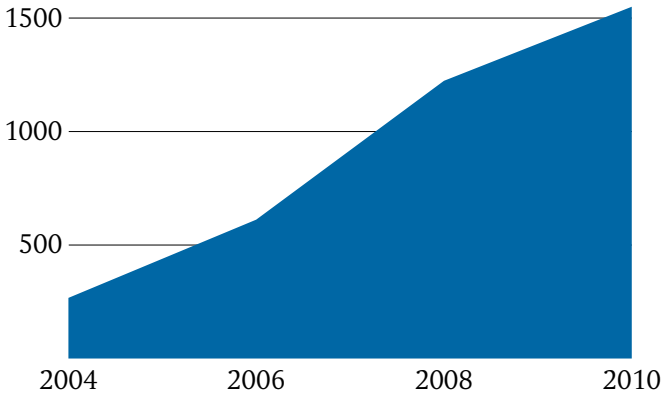
Úkolem *MetaCentra* po celou dobu trvání výzkumného záměru byl provoz a další rozvoj národní distribuované výpočetní infrastruktury – národního gridu – a její integrace do analogické evropské infrastruktury. Národní grid je tvořen souborem clusterů postavených na technologii IA-32 a později IA-32/64. *MetaCentrum* nabízelo i přístup k architektuře IA-64, ale pro její finanční náročnost a funkční náhradou architekturou IA-32/64 nikdy nedošlo k jejímu většímu rozšíření. Celková výpočetní kapacita je tvořena kombinací vlastních zdrojů a výpočetních systémů poskytnutých partnery, především SCB na Masarykově univerzitě, ÚVT Univerzity Karlovy a CIVT Západočeské univerzity. Po celou dobu se však dařilo do národního gridu připojovat i další systémy, např. z JČU, MZLU, UTB. Veškerá výpočetní kapacita a související úložné prostory byly k dispozici studentům, akademickým a dalším výzkumným pracovníkům vysokých škol, ústavů Akademie věd ČR i dalších výzkumných organizací bez jakýchkoliv poplatků. Vědecké výsledky, dosažené s využitím zdrojů *MetaCentra*, jsou shrnuty v jeho ročenkách.

Od roku 2006 *MetaCentrum* prosazuje koncept virtualizace výpočetní a následně i úložné infrastruktury jako nástroje řešení dříve nezvládnutelných problémů, zejména pak možnosti uspokojit i protichůdné požadavky uživatelů. Od nabídky jednotného prostředí postaveného na principu „one size fits all“ *MetaCentrum* přešlo k nabídce virtuálních počítačů, na nichž mohou běžet různé operační systémy (včetně MS Windows) a které lze optimalizovat pro konkrétní aplikace. Vlastní výzkum a vývoj se zaměřil na celou řadu oblastí:

- nové systémy plánování virtualizované infrastruktury – *Magrathea* a rozšíření systému *Torque*,
- informační systém a správu uživatelů – *Perun*,
- řízení virtualizované síťové infrastruktury – *Virt-Cloud*,
- bezpečnostní aspekty – *Pakiti* a
- související techniky autentizace a řízení přístupu.

MetaCentrum patřilo mezi průkopníky federalizovaných přístupů pro autentizaci v distribuovaném prostředí. Ve spolupráci s MU vybudovalo federalizovanou službu práce s histopatologickými atlasy, která je aktuálně zapojena do 14 národních federací a je tak unikátní i ve světovém měřítku. Výzkum se rovněž zaměřil na kombinaci PKI s federalizovanými a dalšími autentizačními systémy (zejména Kerberos), což umožňuje uživatelům přistupovat k národní i mezinárodní infrastruktuře bez nutnosti zvládat další autentizační systémy.

MetaCentrum bylo po celou dobu řešení výzkumného záměru významným partnerem celoevropských projektů gridové infrastruktury. V sérii projektů *EGEE* (2004–2010) zastával vedoucí *MetaCentra* pozici člena řídícího výboru (Project Management Board), kde zastupoval celou oblast střední Evropy. Jedno funkční období byl i předsedou tohoto výboru. *MetaCentrum* bylo zapojeno i do dalších projektů 7. rámcového programu



Počet jader dostupných v MetaCentru

EU, např. *EPIKH* či *EUAsiaGrid*, nejvýznamnější mezinárodní aktivitou však byla koordinace klíčového projektu *EGI_DS (European Grid Initiative Design Study)*. Tento projekt navrhl organizační a funkční strukturu budoucí gridové celoevropské infrastruktury, která je v současné době realizována v rámci projektu *EGI InSPIRE*, jehož se *MetaCentrum* opět jako partner účastní. V rámci série projektů *EGEE* se *MetaCentrum* podílelo nejen na zajištění provozu celoevropské gridové infrastruktury, ale bylo i výzkumným partnerem odpovídajícím za službu Logging and Bookkeeping a v posledních letech i za některé součásti bezpečnostní infrastruktury.

V roce 2009 bylo sdružení CESNET pověřeno vystupovat na mezinárodní úrovni jako reprezentant *Národní Gridové Iniciativy (NGI)*, realizaci této reprezentace zajišťuje opět *MetaCentrum*.

Multimédia a prostředí pro vzdálenou spolupráci

Jedním z významných přínosů současných komunikačních infrastruktur je, že usnadňují spolupráci distribuovaných týmů. V této oblasti jsme se věnovali jak úkolům výzkumným a vývojovým, tak budování příslušné infrastruktury pro připojené instituce.

Součástí infrastruktury je IP telefonní síť pokrývající téměř všechny členy sdružení (v současnosti čítá 46 bran, 3 samostatné SIP domény a několik IP telefonních ústředen), videokonferenční infrastruktura s prvkem pro vícebodové videokonference a více než šedesáti registrovanými hardwarovými zařízeními v institucích, webkonferenční systém a vysokokapacitní multiformátové úložiště/archiv audiovizuálních souborů spolu se streamovací farmou a vyhledávačem v audiovizuálních souborech na Internetu. Komunikační infrastruktura se neomezuje pouze na Českou republiku, ale je propojena i s partnery v zahraničí, například pomocí hierarchického systému signalizačních prvků (GDS) pro videokonference.

Výzkumná a vývojová práce v oblasti IP telefonie vyústila ve vytvoření analytického modelu chování zpoždění ve směrovači RTP toků a popisu vlivu síťového zabezpečení na kvalitu hovoru, který prokázal souvislosti mezi šifrováním a kvalitou řeči. Významnou oblastí zájmu byla a je bezpečnost, kde jsme navrhli a implementovali pro otevřenou softwarovou ústřednu Asterisk metodu obrany proti spamu v IP telefonii a aplikaci pro bezpečnostní analýzu prvků IP telefonie (penetrační testy), která umožňuje ověřit úroveň zabezpečení SIP prvků. Řadu reakcí jsme zaznamenali na náš návrh a implementaci výkonnostního testování SIP infrastruktury, kde dosud neexistuje jednotná metodika.

V oblasti speciálních přenosových systémů patří mezi naše úspěchy vývoj paralelních a distribuovaných aktivních elementů *RUM2* s možností uživatelem řízené distribuce a zpracování dat v síti a systém *UltraGrid* pro přenos nekomprimovaného videa HD i post HD (2K, 4K). Pomocí *UltraGridu* byla realizována světově první vícebodová nekomprimovaná videokonference na konferenci iGrid2005 (současně s projektem iHDTV ResearchChannelu). Přenos nekomprimovaného videa je doplněn i podporou nízkolatenčních kompresí a v rámci integrace se systémem *CoUniverse* také o uživatelem řízenou alokaci BoD okruhů pro přenos obrazových dat. Nízkolateční komprese je realizována například pomocí námi vyvíjené efektivní paralelizace JPEG2000 na GPU (bpcuda). S využitím *UltraGridu* jsme demonstrovali možnosti širokopásmového řiditelného optického multicastu.

Přenos robotické operace

Díky experimentům, know-how, infrastruktuře a spolupráci s alšími aktivitami jsme byli schopni realizovat přenosy vysoce kvalitního videa v medicíně (přenosy z operačních sálů *Live Surgery*) a přinesli jsme tak nové možnosti komunikace a vzdělávání. Vytvořením několika prototypů pro distribuovanou spolupráci ve filmové a televizní postprodukci multimediálního obsahu, vytvořením sítě *PragueMedia.Net* a zapojením do *CineGridu* jsme prohloubili spolupráci s filmovým průmyslem a uměleckými vysokými školami při zpracování obsahu ve vysokém rozlišení (4K, 3D HD) a maximální kvalitě.

Bezpečnost – CESNET-CERTS

Stranou naší pozornosti nezůstaly ani bezpečnostní aspekty provozu sítí a služeb, především oblast bezpečnostních incidentů – jejich řešení, detekce a prevence. Ustanovili jsme oficiální CSIRT (Computer Security Incident Response Team) nazvaný *CESNET-CERTS (csirt.cesnet.cz)*, který byl pověřen řešením a koordinací řešení bezpečnostních incidentů pocházejících ze sítě CESNET2. Světová komunita CERT/CSIRT týmů oficiálně přijala tým CESNET-CERTS v lednu roku 2004 a v lednu roku 2008 dosáhl tým tzv. akreditace u úřadu Trusted Introducer, čímž se stal platným členem světové bezpečnostní komunity.

Tým CESNET-CERTS je prvním oficiálně konstituovaným týmem typu CSIRT v České republice. Každoročně je mu hlášeno několik tisíc bezpečnostních incidentů a díky neustále se zlepšující práci správců sítě a služeb se zlepšuje trend v počtu úspěšně vyřešených. Dalším úspěchem je několik de facto CSIRT týmů, které vznikly v prostředí velkých univerzit. Jeden z nich, tým Masarykovy univerzity v Brně, se rovněž zapojil do spolupráce světové komunity a je oficiálně akreditován.

Za zmínku stojí i rozvinuté prostředí týmu, které kromě pravidel, politik a doporučení zahrnuje také nástroje pro automatickou detekci podezřelých aktivit v síti CESNET2 (např. systémy na bázi IDS), nástroje pro kontrolu zabezpečení serverů a pracovních stanic (CESNET Audit Systém), systém pro sledování celého životního cyklu bezpečnostního incidentu a další.

V roce 2007 jsme zkušenosti získané při budování týmu CESNET-CERTS a jeho spolupráci se světovou bezpečnostní infrastrukturou využili při budování modelového pracoviště *CSIRT.CZ* v rámci grantu *Kybernetické hrozby z hlediska bezpečnostních zájmů České republiky* financovaného Ministerstvem vnitra ČR, jehož spoluřešitelem bylo sdružení CESNET. V prosinci 2010 MV ČR

prohlásilo tým CSIRT.CZ za oficiální Národní CSIRT tým České republiky. V současné době probíhá předání agendy a provozu CSIRT.CZ jeho novému provozovateli, sdružení CZ.NIC.

Podpora aplikací

Vedle vlastních aktivit se soustřeďujeme také na přímou podporu projektů řešených uživateli sítě CESNET2, často v rámci významných projektů v celoevropském nebo celosvětovém kontextu. Postupně se vyprofilovaly tři velké tematické oblasti, z nichž pocházejí naši nejvýznamnější partneři: medicína, fyzika a informační technologie, kde hrají významnou roli zejména projekty zapadající do evropského programu *Future Internet*. Společným znakem podpořených skupin je potřeba specifického síťového prostředí, jako jsou vyhrazené spoje s vysokou rychlostí, nízkou latencí, vysokým stupněm zabezpečení a podobně.

V oblasti medicíny jsme během celého záměru podporovali několik projektů: POSN, MeDiMed/ReDiMed, Global Medicus, kooperativní 3D model a Video Surgery. Projekty vznikly izolovaně, ale časem se některé z nich začínají prolínat díky společné infrastruktuře nebo shodným uživatelům. V roce 2010 se velmi viditelně mezinárodně prosadil přenos 3D videa z operací realizovaných robotem da Vinci. Snoubí se v něm propojení několika významných výsledků celého záměru, vysokorychlostní přenosy s aplikací výzkumu v oblasti FPGA a moderním zobrazením medicínské problematiky. Jeho praktické použití vidíme zejména v oblasti moderní výchovy špičkových chirurgů.

V případě fyziky se nedá podpora jednoznačně rozdělit na jednotlivé projekty, i když několik aplikačních projektů existuje (ATLAS, LHC, STAR, Auger). Naše podpora byla poskytována komunitě fyziků jako celku, zmíněné projekty jsou organizovány na široké mezinárodní bázi a česká komunita fyziků na nich významně participuje. Největší podporou těmto projektům je zajištění exkluzivní konektivity na národní i mezinárodní úrovni. CESNET vedle vysokého standardu IP konektivity ve směru do evropské akademické páteře GÉANT poskytuje fyzikální komunitě několik vyhrazených spojů typu end-to-end (E2E) k datovým a výpočetním centrům v celém světě.

Do informačních technologií patří projekty typu PlanetLab, VINI, C2C (Cave-to-Cave) a další. Spadá sem i spolupráce na nových evropských projektech, jakým byl projekt FEDERICA. Zde se naše podpora významně lišila v závislosti na konkrétním projektu – do některých jsme byli aktivně zapojeni, jiným jsme nabídli nadstandardní infrastrukturu.

Řešitelský tým

Výzkumný záměr vyžadoval enormní množství inventní práce. Tomu odpovídá i velikost a struktura řešitelského týmu. Byl rozdělen do několika tematicky vymezených aktivit, jejichž složení odpovídá struktuře tohoto čísla *Datagramu*. Celkem se během sedmi let do řešení zapojilo bezmála 350 odborníků, z nichž mnozí budou pokračovat v práci na navazujícím strategickém projektu, *Velké infrastruktuře CESNET*. Rádi bychom všem poděkovali a vyjádřili naději, že při této činnosti dosáhnou podobně zajímavých výsledků.

Řešitelé na výjezdním semináři ve Skalském Dvoře, 2009