Zpráva o řešení výzkumného záměru

2005

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. RNDr. Milan Mareš, DrSc.
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

Editor zprávy, redakční a grafické úpravy:
Pavel Satrapa

Autoři jednotlivých částí:
1 Jan Gruntorád
2 Václav Novák, Petr Adamec, Josef Verich
3.1 Stanislav Šíma, Lada Altmannová
3.2 Lada Altmannová, Miloš Lokajíček, Milan Šárek, Stanislav Šíma, Jan Švec
3.3 Jan Radil, Miroslav Karásek, Josef Vojtěch
3.4 Jiří Burian, Jaroslav Čížek, Jaroslav Hrb, Miloš Wimmer
4 Petr Kobierský, Ladislav Lhotka, Tomáš Martínek, Jan Pazdera, Jiří Tobola
5 Tomáš Košňar
6 Sven Ubik, Vladimír Smotlacha
7 Milan Sova
8 Miroslav Vozňák, Radek Holý, Jan Růžička
9 Luděk Matyska a kol.
10 Eva Hladká a kol.
11 Boris Šimák, Tomáš Pitner, Tomáš Zeman
12 Andrea Kropáčová
13 Milan Šárek
14 Helmut Sverenyák a kol.
15 Luděk Matyska
16 Sven Ubik, Vladimír Smotlacha
17 Stanislav Šíma
18 Ladislav Lhotka
19 Stanislav Šíma, Helmut Sverenyák, Pavel Satrapa

ISBN 80-239-6432-1

Obsah

1 Úvod

Předložená zpráva popisuje postup řešení výzkumného záměru "Optická síť národního výzkumu a její nové aplikace" a výsledky dosažené v roce 2005. Rok 2005 byl druhým rokem řešení sedmiletého výzkumného záměru, jehož ukončení je plánováno na rok 2010.

Vzhledem k obrovskému rozsahu výzkumných a vývojových prací a rozsáhlému týmu řešitelů – 29 „kmenových" zaměstnanců sdružení a 137 externích řešitelů, převážně zaměstnanců členů sdružení (vysokých škol a ústavů Akademie věd České republiky) – bylo řešení v roce 2005 rozděleno do dvanácti tématicky vymezených aktivit:

1. Rozvoj páteřní sítě CESNET2
2. Optické sítě
3. Programovatelný hardware
4. Sledování infrastruktury a provozu sítě
5. Sledování a optimalizace výkonnostních charakteristik
6. AAI a mobilita
7. IP telefonie
8. MetaCentrum
9. Virtuální prostředí pro spolupráci
10. Podpora distančního vzdělávání
11. CESNET CSIRT
12. Medicínské aplikace

Řešená problematika zahrnuje oblasti od nejnižších přenosových vrstev, přes middleware, gridové technologie, autentizaci a autorizaci, bezpečnost až po vývoj nových aplikačních služeb. Každá aktivita má určeného svého vedoucího a zástupce, kteří koordinují jednotlivé týmy, zodpovídají za odbornou úroveň a efektivní využití přidělených finančních prostředků. Výsledky dosažené v rámci aktivit jsou interně hodnoceny v rámci sdružení CESNET dvakrát ročně a výsledky hodnocení využíváme pro zefektivnění řešení dané problematiky v dalším období. Velké úsilí věnujeme umožnění spolupráce a interakce jednotlivých aktivit a zajištění zpětné vazby od uživatelů, kterým dáváme výsledky v co nejkratší lhůtě k dispozici.

Interní hodnocení aktivit a celkovou koordinaci řešení výzkumného záměru vykonává Řídící rada výzkumného záměru, která je poradním orgánem hlavního řešitele. V roce 2005 pracovala Řídící rada ve složení:

- Ing. Jan Gruntorád, CSc. – CESNET
- RNDr. Eva Hladká, Ph.D. – MU Brno
- Ing. Tomáš Košňar – CESNET
- Ing. Ladislav Lhotka, CSc. – CESNET
- Doc. RNDr. Luděk Matyska, CSc. – MU Brno

- Ing. Václav Novák – CESNET
- RNDr. Pavel Satrapa, Ph.D. – TU Liberec
- Ing. Helmut Sverenyák – CESNET
- Ing. Stanislav Šíma, CSc. – CESNET
- Dr. Ing. Pavel Šmrha – ZČU Plzeň

Řízení velkého a distribuovaného týmu řešitelů klade vysoké nároky mimo jiné na rozvoj a provoz informačního systému sdružení a na činnost „podpůrných" útvarů sdružení. Situace v roce 2005 byla ještě navíc velmi zkomplikována rozhodnutím MŠMT v květnu 2005, které dramaticky změnilo strukturu uznaných nákladů v roce 2005. Toto rozhodnutí si vyžádalo přepracování plánu činností a rozpočtu většiny aktivit a kladlo zvýšené nároky na celý řešitelský tým. V říjnu 2005 na žádost sdružení vydalo MŠMT nové rozhodnutí, které obsahovalo již přijatelnou strukturu uznaných nákladů a plány práce a rozpočty aktivit jsme mohli upravit do takové formy, aby bylo možno dosáhnout plánovaných výsledků. Není potřeba zdůrazňovat, že takto zásadní změny struktury financování během kalendářního roku velmi komplikují výzkumné a vývojové práce.

Další skutečnost, která velmi komplikuje řešení, je současná legislativa v oblasti výběrových řízení, která nevyhovuje pro oblast výzkumu a vývoje. Na pořízení některých zařízení podle platné legislativy je zapotřebí více než 6 měsíců, což je, vzhledem k dynamice oboru výzkumného záměru, lhůta nepřijatelná.

I přes výše uvedené komplikace se nám v uplynulém roce podařilo realizovat plánované práce a dosáhnout stanovených cílů. V některých oblastech, jako jsou například problematika Customer Empowered Fiber Networks, využití technologií hradlových polí při realizaci hardwarových akcelerátorů pro směrování a monitorování IP provozu, multimediální aplikace, využití gridových technologií a medicínských aplikací jsme dosáhli mezinárodně uznávaných výsledků. Tyto úspěchy v evropském i světovém měřítku mimo jiné potvrzují, že výzkumný záměr je orientován správným směrem a že tématika námi řešená odpovídá aktuálnímu vývoji v daných oborech.

Chtěli bychom touto cestou poděkovat MŠMT za významnou podporu, kterou výzkumnému záměru poskytuje a za řešení problémů, které v souvislosti s řešením a financováním tak rozsáhlého výzkumného záměru nastávají.

V následujících kapitolách najdete podrobnější informace o řešení jednotlivých aktivit a výsledcích, jichž dosáhly. Vzhledem k širokému tématickému záběru těchto projektů byly jednotlivé části dokumentu zpracovány různými autory a čtenář proto může zprávu považovat spíše za sborník vzájemně souvisejících příspěvků.

Část I

Aktivity výzkumného záměru

2 Rozvoj páteřní sítě CESNET2

V rámci rozvoje páteřní sítě CESNET2 jsme se v období roku 2005 zaměřili na rozvoj optické přenosové vrstvy založené na pronajatých optických vláknech osazených vlastní technologií. Současné technické řešení osazení jednotlivých optických tras využívající zejména EDFA zesilovače s jednokanálovým přenosem (tzv. šedé řešení) nedovoluje zvyšování přenosových kapacit na jednom optickém vlákně a je omezujícím faktorem pro poskytování End-to-End (E2E) služeb na úrovni optických přenosových kanálů. Rozšířením optické přenosové technologie DWDM do dalších uzlů a její integrací se stávající DWDM trasou Praha–Brno jsme vytvořili základní kruhovou topologii optické transportní vrstvy. Použitá 32kanálová technologie ROADM (s kapacitou jednotlivých kanálů 10 Gb/s) umožňuje softwarově řízené přidělování optických přenosových kanálů na žádost (provisioning on-demand). Tuto schopnost nabízí mezi libovolnými uzly celého systému. Implementovaná optická přenosová DWDM síť umožní v dalších etapách rozvoje integraci se stávající IP sítí a přechod k hybridní IP/optické páteři řízené protokoly jako je GMPLS, včetně nasazení optických přepínačů pro dynamické přepínání optických přenosových cest.

Na úrovni IP/MPLS vrstvy jsme se zaměřili na povyšování přenosových kapacit uzlů na 10GE s využitím DWDM sítě. Zároveň jsme usilovali o dokončení náhrady zastaralých páteřních směrovačů GSR10216, jejichž vlastnosti neumožňovaly nasazení pokročilých služeb, jako je IPv6 unicast/multicast či přenos velkých rámců dat.

V řadě menších uzlů pokračovala náhrada nevyhovujících směrovačů L2/L3 přepínači, které jsou základním předpokladem pro hybridní IPv4/IPv6 řešení, další povyšování přístupových kapacit a poskytování E2E služeb na základě technologie EoMPLS nebo VPLS účastníkům, kteří nejsou připojeni v uzlech DWDM sítě.

V oblasti síťových protokolů jsme se věnovali zejména ověřování a implementaci přepravy skupinově adresovaných IPv6 datagramů v prostředí páteřní sítě.

Nedílnou součástí rozvoje IP služeb sítě je zavedení služeb s definovanou kvalitou (QoS), které kromě nezbytné technické implementace zahrnuje také nutnost vyřešení mnoha problémů týkajících stanovení všeobecného rámce pravidel uplatňování QoS politiky vůči jednotlivým kategoriím uživatelů. Rozvoj NREN ČR rovněž pokrývá rozvoj a provozování nezbytné podpůrné infrastruktury pro zajištění nepřetržitého a spolehlivého provozu sítě a zajištění podpory na národní a mezinárodní úrovni (koordinace a spolupráce se sítí GÉANT a ostatními evropskými NREN).

Důležitým úkolem byla rovněž příprava připojení na nově vznikající síť GÉANT2 a dosažení kompatibility a interoperability všech provozovaných síťových slu-

žeb, zejména v oblasti E2E. V rámci aktivit projektu GN2, v jehož rámci síť GÉANT2 vzniká, jsme se rovněž zapojili do projektu JRA4 WI3 zabývajícího se přeshraničními vlákny (Cross Border Fibres, CBF).

Vývoj a změny v páteřní síti za uplynulé období lze shrnout do několika bodů:

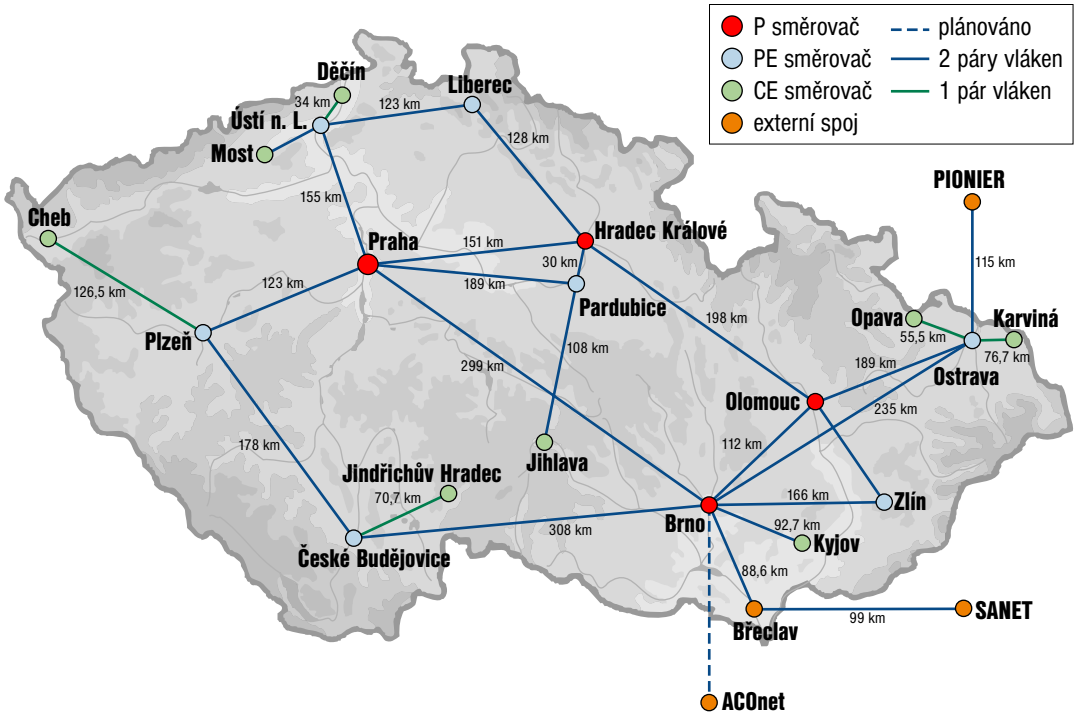
- vybudování základního jádra optické přenosové sítě DWDM v kruhové topologii s využitím technologie ROADM
- dokončení náhrady již nevyhovujících páteřních směrovačů GSR12016
- povýšení uzlů Hradec Králové a Olomouc na 10GE
- povýšení připojení do NIX.CZ na 2×10GE
- připojení na síť GÉANT2 technologií 10GE pro IP síť a 4×1GE pro poskytování E2E služeb
- pilotní ověřování zesilovače PCLight na optické trase Praha–Hradec Králové
- pilotní ověřování přenosů po jednom optickém vlákně
- podpora přenosu velkých rámců dat v celé páteřní síti
- implementace a ověřování IPv6 multicastu
- zvýšení redundance a spolehlivosti sítě CESNET2 (nasazení redundantních procesorů Sup720, nezávislé poslední míle optické sítě)
- zvýšení bezpečnosti sítě proti DoS útokům (implementace Control Plane Policing na páteřních směrovačích)
- celkové zvýšení stability a dostupnosti sítě s využitím Cisco NSA services
- zřízení nového uzlu v Jihlavě
- rozvoj nezbytné podpůrné infrastruktury

2.1 Fyzická topologie páteřní sítě

Základní fyzická topologie sítě (viz obrázek 2.1) je založena na pronajatých párech optických vláken, většinou odpovídajících standartu ITU-T G.652. Některé menší uzly (např. Děčín či Cheb) jsou připojeny pouze jedním vláknem a využívají dostupné technologie Fast Ethernet konvertorů MRV. Zbývající uzly jsou na páteřní síť připojeny rádiovými okruhy 10 a 34 Mb/s nebo pronajatými okruhy.

V návaznosti na dostupnost optických vláken v těchto lokalitách se snažíme i tato připojení postupně nahrazovat optickými vlákny.

V průběhu roku 2005 jsme se věnovali zvýšení redundance připojení páteřních uzlů na optické trasy, neboť zejména úseky posledních mílí byly fyzicky souběžné. Ve spolupráci s poskytovateli optických tras jsme tyto souběhy v páteřních uzlech Praha, Brno, Olomouc a Hradec Králové nahradili nezávislými trasami.



Obrázek 2.1: Fyzická optická topologie páteřní sítě CESNET2

Základní logickou topologii páteřní sítě tvoří 11 uzlů (GigaPoP) vzájemně propojených datovými okruhy s přenosovou kapacitou nejméně 1 Gb/s (viz obrázek 2.6). Páteřní okruhy využívají technologie 10GE LAN PHY (desetigigabitový Ethernet), 1GE (gigabitový Ethernet) a POS STM-16/OC-48 pro přenosové kapacity 2,5 Gb/s. Páteřní uzly jsou připojeny vždy dvěma datovými okruhy pro zálohování přístupu.

Při osazení vlastních optických okruhů přecházíme na preferovanou variantu NIL s optickými EDFA zesilovači umístěnými pouze na koncích tras. Protokolově závislé L2 přepínače ve funkci opakovače umístěného na trase postupně vyřazujeme.

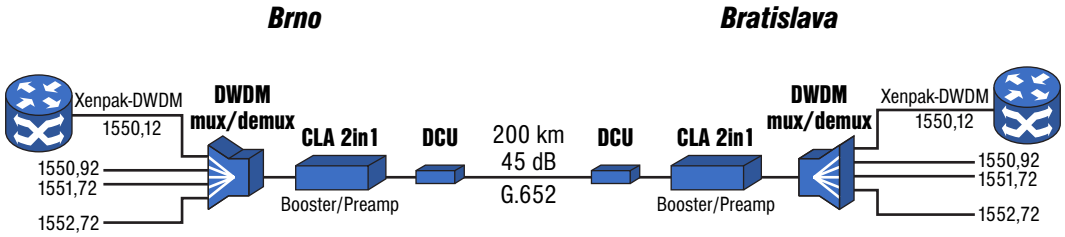
K osazení optických okruhů využíváme různých technologií. Pro gigabitové okruhy na kratší vzdálenosti (do cca. 120–140 km) není potřeba žádná regene-

race či zesílení a používáme výměnné optické transceivery (Pluggable Optics) v rozhraních směrovačů a přepínačů typu CWDM-1550 a DWDM GBIC se 100Ghz rozestupem kanálů dle ITU-T.

Optické okruhy s větším útlumem (nad 32 dB) jsou osazeny optickými EDFA zesilovači Keopsys (předzesilovače a výkonové zesilovače). Používané typy zesilovačů však mají některé problematické vlastnosti, např. po výpadku napájení je nutné je manuálně aktivovat a potřebné úpravy by byly finančně náročné.

V letošním roce jsme na 1 Gb/s okruhu Praha–Hradec Králové (150 km, 35,7 dB, G.652) úspěšně ověřili nasazení optického zesilovače CLA PB01, který vyvíjíme v rámci aktivity *Optické sítě*. Použili jsme metodu OSA (One Side Amplification) s jedním zesilovačem a optickým filtrem umístěným v uzlu Praha.

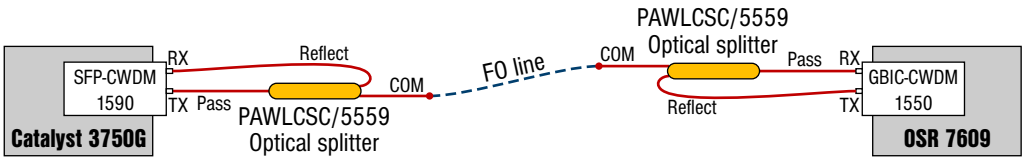
Vlastní ověřování prokázalo, že tento typ zesilovače je z hlediska použití vhodnější a cenově zajímavější než stávající EDFA zesilovače Keopsys. V současné době připravujeme variantu pro 10 Gb/s optické okruhy, kterou plánujeme využít pro osazení optické trasy Brno–Bratislava (viz obrázek 2.2).



Obrázek 2.2: Plánované osazení trasy Brno–Bratislava

Navržené osazení trasy využívá 4kanálové multiplexory/demultiplexory a umožní přenos optických kanálů o kapacitě až 10 Gb/s. Kompenzace disperze bude prováděna Braggovskými mřížkami, které jsou cenově příznivější oproti klasickým kompenzátorům (DCU). Koncová zařízení budou osazena DWDM Xenpak nebo GBIC příslušné vlnové délky. Vlastní realizaci osazení předpokládáme začátkem roku 2006.

V oblasti 1 Gb/s přenosů bez zesílení po jednom optickém vlákně jsme na trase Ostrava–Karviná (76,7 km) ověřili řešení s pasivními optickými splittery (viz obrázek 2.3).



Obrázek 2.3: Osazení jednovláknové trasy 1GE Ostrava–Karviná

V koncových zařízeních používáme CWDM o vlnových délkách 1550 a 1590 nm.

Vybudování optického přenosového systému s využitím technologie DWDM jsme koncipovali jako rozšíření stávající DWDM trasy Praha–Brno s cílem vytvořit základní kruhovou topologii optické sítě s využitím technologie ROADM. Od nově budovaného systému jsme požadovali mimo jiné následující funkce a vlastnosti:

- Podpora alespoň 32 přenosových kanálů s rozestupem 100 GHz dle doporučení ITU-T.
- Přenos optického „barevného“ signálu bez použití 3R regenerace (transpondérů).
- Zaručená hodnota BER 10^{-15} na všech přenášených kanálech.
- Přidání/odbočení nebo přesměrování optických kanálů nesmí vyžadovat dodatečné úpravy osazení optických tras.
- Řešení musí být kompatibilní se stávající technologií včetně systému řízení, dohledu a ovládání optických kanálů.

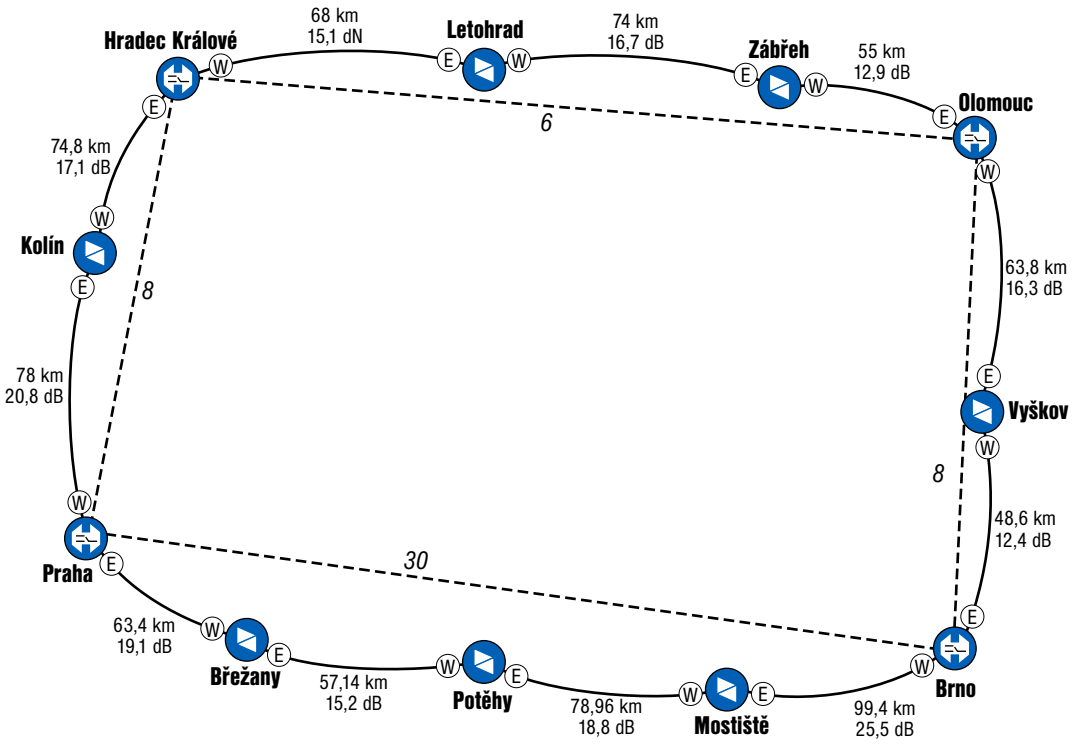
Na základě veřejné obchodní soutěže jsme vybrali řešení Cisco Systems je založené na modulárním DWDM systému ONS 15454 MSTP (podrobný popis systému lze nalézt na stránkách výrobce *www.cisco.com*). Návrh řešení je koncipován s maximální kompenzací chromatické disperze (v kterékoliv části kruhu se blíží nule) pro zajištění bezproblémového přenosu „barevných“ signálů. Celkové schéma osazení optických tras včetně mezilehlých uzlů je uvedeno na obrázku 2.4.

ROADM uzly, které umožňují softwarově řízené vkládání/odbočování optických tras, jsou umístěny v uzlech Praha, Brno, Olomouc a Hradec Králové. Vlastní ROADM obsahuje optický přepínač založený na technologii PLC (Planar-Lightwave-Circuit).

V mezilehlých uzlech jsou umístěny zesilovače a kompenzátory disperze, které jsou potřebné pro zajištění správné funkce DWDM systému, požadovaného počtu přenášených kanálů (32) a zajištění kvality optických kanálů (hodnota BER). Zesilovače jsou rovněž založeny na platformě ONS 15454.

Připojení koncových zařízení (klientů) na DWDM je možné dvěma způsoby:

- Pomocí transpondérů, které převádějí standardní „šedý“ signál 1310 či 1550 nm na „barevný“ DWDM kanál dle ITU (OEO konverze) a zajišťují 3R regeneraci. Transpondéry jsou součástí DWDM systému a jsou SW přeladitelné na více vlnových délek.



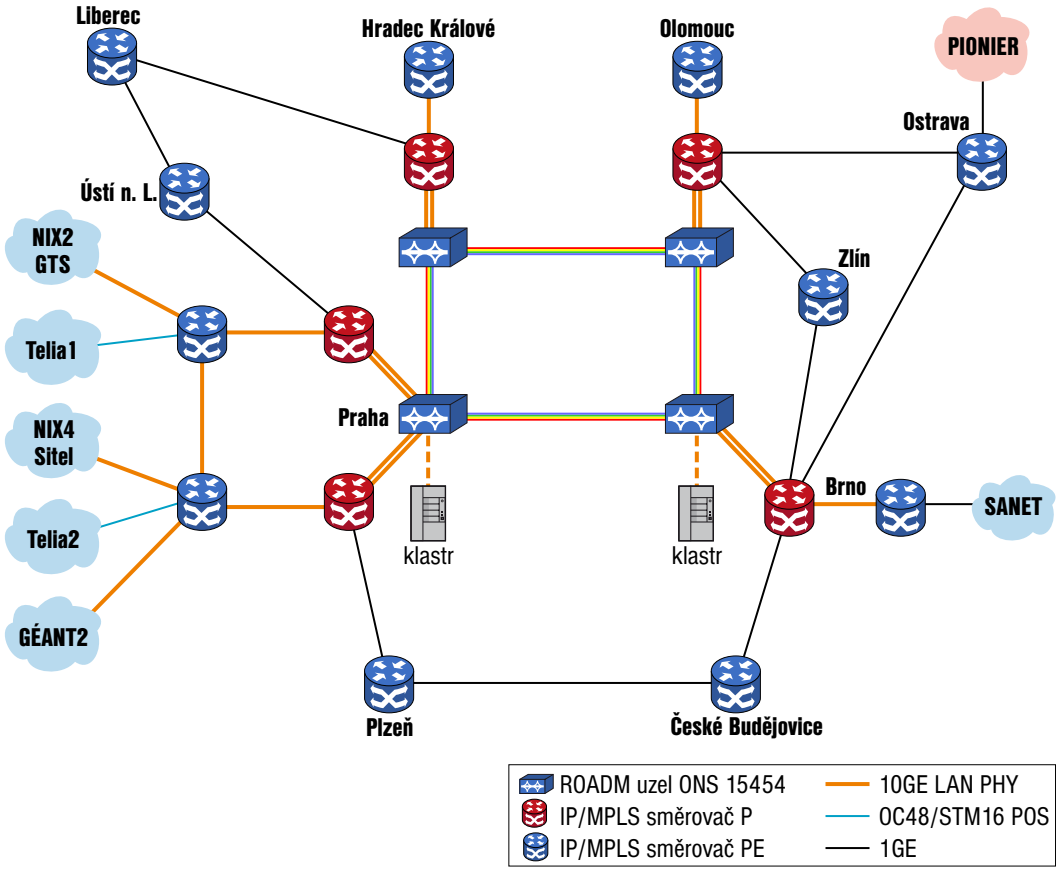
Obrázek 2.4: Topologie optické přenosové DWDM sítě

- Přímo na „barevný“ DWDM kanál. Koncové zařízení musí podporovat výměnné optické DWDM rozhraní (např. Xenpak). Toto řešení je levnější ve srovnání s transpondérem, ale přináší řadu omezení. Výměnná optická rozhraní do směrovačů a přepínačů nepodporují 3R regeneraci, dopřednou opravu chyb a nejsou přeladitelná. Proto je lze bez problémů použít pouze na kratší optické kanály (do cca. 200 km).

Dokončení optického přenosového systému umožnilo povýšení dalších páteřních uzlů na 10GE (viz obrázek 2.5). Při přechodu IP/MPLS na nový DWDM systém jsme zachovali stávající kruhovou topologii páteřní sítě se záložními okruhy a propojením mezi sousedními uzly. Flexibilita DWDM systému umožňuje uspořádat přenosové okruhy do libovolné topologie, která bude z hlediska rozvoje IP/MPLS nejvhodnější.

Optická transportní síť DWDM umožní rovněž vytváření nezávislých a oddělených struktur na nejnižší úrovni (L1) na jedné optické vláknové infrastruktuře.

Důležitým cílem výstavby DWDM systému je poskytovat lambda služby pro potřeby výzkumných projektů a aktivit i pokročilých uživatelů sítě.



Obrázek 2.5: Přenosový systém DWDM a IP/MPLS síť

2.2 Logická topologie páteřní sítě

Základním přenosovým protokolem páteřní sítě je IP/MPLS. Jako IGP protokol MPLS sítě používáme OSPFv2. Vlastní logická topologie sítě (viz obrázek 2.6) je rozdělena do dvou funkčních úrovní, kterým je přizpůsobena topologie jednotlivých uzlů:

- Základní jádro sítě tvoří červeně vyznačené směrovače OSR7609 R105 až R107 v uzlech Praha, Brno, Hradec Králové a Olomouc. Na těchto směrovačích jsou ukončeny páteřní okruhy sítě (v MPLS vrstvě sítě zastávají funkci P směrovačů).
- Přístupovými směrovači v uzlech jsou OSR7609, resp. Cisco 7206-VXR s NPE-G1 v uzlech Ústí nad Labem a Zlín. Zajišťují pro připojené účastníky veškeré funkce a služby páteřní sítě (MPLS, MPLS VPN, QoS, IPv4/IPv6 směrování, IPv4 multicast, export NetFlow statistik, přístupové filtry).

Menší uzly sítě jsou vždy připojeny k přístupovým směrovačům páteřních uzlů. V menších uzlech se používají malé směrovače řady C2621/C2651-XM/C2691 s omezenou funkčností (MPLS CE). Tyto směrovače postupně nahrazujeme přístupovými L2/L3 přepínači Catalyst 3750G, které umožní gigabitové rychlosti a poskytování MPLS VPN služeb.

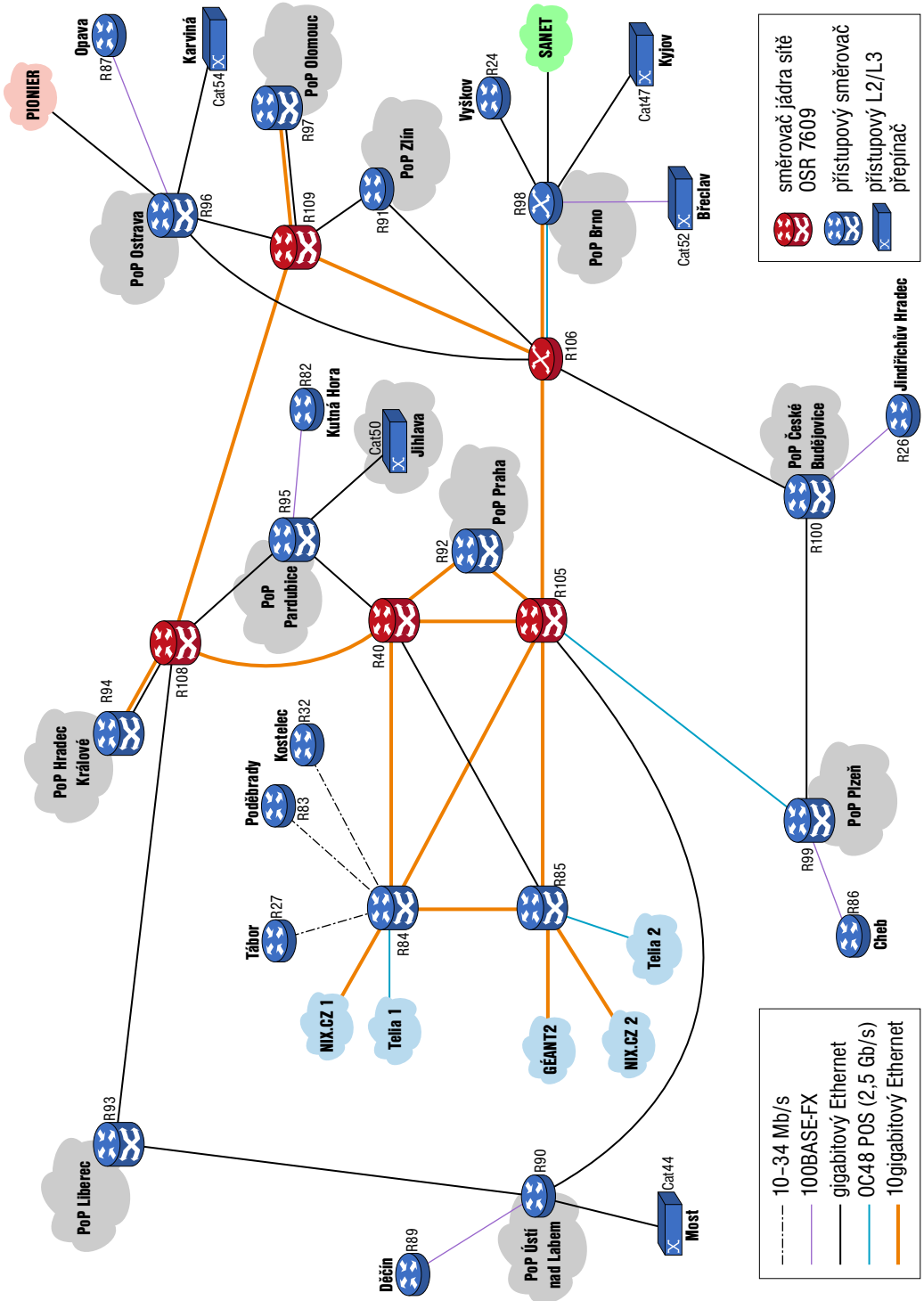
2.3 Individuální směrování IPv4 (IPv4 unicast)

Jako interní směrovací protokol v páteřní síti využíváme interní BGPv4 (iBGP) provozovaný mezi přístupovými PE směrovači. Na externích směrovačích R84, R85 a R98 se nacházejí route-reflectory RR1, RR2 a RR3 pro zajištění redundance směrování (na obrázku 2.7 jsou zobrazeny iBGP vztahy pouze pro RR1). Na ostatních PE směrovačích využíváme route-reflector klienty. Použití route-reflectorů snižuje potřebný počet sousedů v páteřní síti. Na přístupových směrovačích páteřních uzlů používáme statické agregované bloky a neprovádíme redistribuci z vnitřních směrovacích protokolů. Velké metropolitní a univerzitní sítě (PASNET, ČVUT, aj.) využívají privátní autonomní systémy a jsou na páteřní síť připojeny protokolem eBGP. U menších účastníků preferujeme připojení pomocí statických cest.

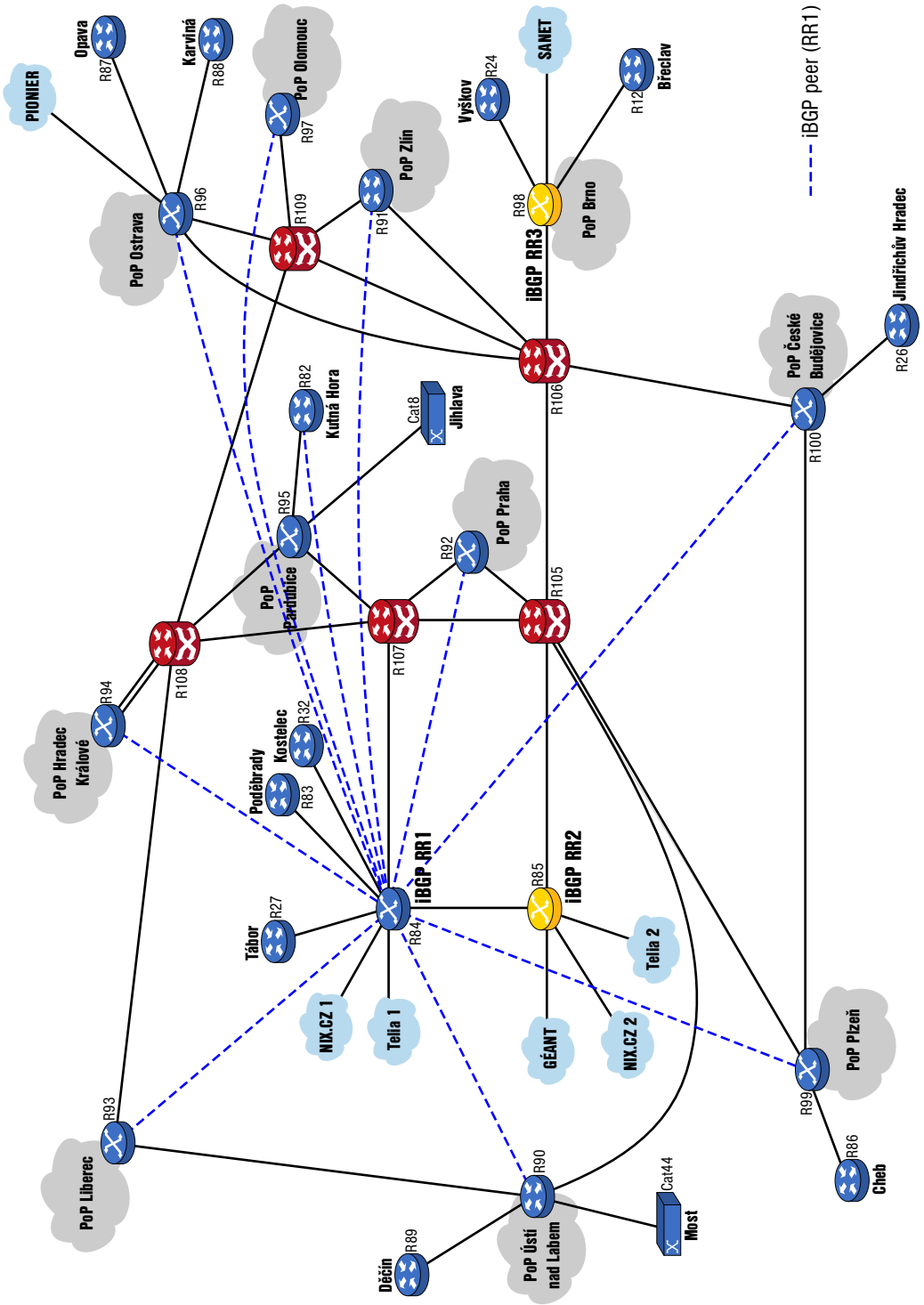
2.4 Skupinové směrování IPv4 (IPv4 multicast)

Pro výměnu skupinových směrovacích informací využíváme interní protokol MBGP. IMBGP využívá opět tři route-reflectory na směrovačích R84, R85 a R98. Route-reflector klienti jsou však na rozdíl od individuálního směrování konfigurováni na všech P a PE směrovačích, neboť i na směrovačích jádra sítě je nutné zajistit správnou funkci RPF (Reverse Path Forwarding), který jako součást předávacího procesu zajišťuje ochranu proti smyčkám či duplicitním skupinovým paketům. Tato kontrola je v prostředí páteřní sítě zajišťována protokolem iMBGP (za předpokladu, že veškeré multicastové zdroje dat jsou oznamovány tímto protokolem).

V celé páteřní síti používáme protokol PIMv2-SM. Celkovou topologii skupinového směrování jsme výrazně zjednodušili a v současné době používáme pouze jeden centrální RP (Rendezvous point) s adresou 195.113.144.2 na směrovačích R85 a R98 implementujících redundantní topologii AnyCast RP. Velké metropolitní a univerzitní sítě nyní provozují své vlastní RP (v rámci nezávislé skupinové



Obrázek 2.6: Logická topologie páteřní sítě CESNET2



Obrázek 2.7: Interní individuální směrování IPv4 (příklad route-reflectoru RR1 na R84)

domény) a aktivní zdroje skupinových dat oznamují protokolem MSDP. Ostatní připojení účastníci mohou využít centrální RP. Jeho oznamování dynamickými protokoly (Cisco Auto-RP nebo BSR) jsme zrušili, adresu RP je třeba konfigurovat staticky na přístupových směrovačích.

Současná logická topologie skupinového směrování je inkongruentní (individuálně adresované pakety jsou přenášeny přes MPLS, skupinové bez MPLS značek). Na úrovni MSDP je rovněž ve všech uzlech prováděna filtrace oznamovaných aktivních zdrojů a skupin dle doporučení Cisco a sítě GÉANT (omezení provozu Novell NDS, ImageCast a dalších služeb využívajících multicast, které nejsou určeny pro oznamování do páteřní sítě a sítě MBone).

Současné řešení ditribuce multicastu na páteřní síti podporuje i SSM/IGMPv3 (Source Specific Multicast), jenž používá vyhrazený IP rozsah 232.0.0.0/8 a ke své funkci nevyžaduje RP.

Mimo tradiční přidělování skupinových adres pomocí dynamických protokolů jako je SDR (SAP) lze tyto adresy přidělovat staticky dle RFC 2770 na základě čísla autonomního systému (AS). Dle daného mechanismu našemu AS 2852 odpovídá rozsah veřejných skupinových adres 233.11.36.0/24, z nějž jsou adresy přidělovány.

2.5 Implementace IPv6

Páteřní síť podporuje hybridní individuální IPv4/IPv6 směrování (dual-stack) prostřednictvím MPLS (technologie PE/6PE).

2.5.1 Testovací síť pro IPv6 multicast

Stejně jako v IPv4 je topologie pro přenos skupinových dat inkongruentní (individuálně adresované datagramy jsou přenášeny MPLS pomocí 6PE, skupinově adresované mimo MPLS). Pro skupinové směrování IPv6 využíváme směrovače Cisco 7500. Jsou propojeny tunely do hvězdy, v jejímž středu se nachází směrovač R62. Vzhledem k tomu, že pro IPv6 multicast nebyl dlouho definován způsob oznamování zdrojů, používá jak síť M6Bone, tak i síť GÉANT2 pouze jeden RP. V současné době je již standardizován embedded RP (RFC 3956), který tuto problematiku řeší. Naše konfigurace umožňuje použití obou variant – jak statického RP, tak i embedded RP. Nevýhodou řešení s embedded RP je, že skupiny je potřeba volit podle adresy nejbližšího embedded RP v součinnosti se správcem sítě.

Abychom mohli komunikovat s ostatními sítěmi ve světě, museli jsme – jak bylo řečeno dříve – nakonfigurovat statické RP, jaké používají ostatní. Tedy RP

francouzské sítě Renater s adresou 2001:660:3007:300:1::. Bohužel tento RP běží na směrovači, který je často využíván i k jiným činnostem (školení, aj.) takže bývá mimo provoz. Tuto skutečnost ale Renater vždy včas oznámil.

Napojení do světa IPv6 multicastu nám poskytuje síť GÉANT a je momentálně řešeno pomocí tunelu ze směrovače R62.

Na příští rok plánujeme přesun konfigurací na provozní směrovače bez použití tunelů. Skupinové směrování IPv6 jsme již testovali na PE směrovači typu OSR v Liberci, k němuž je Technická univerzita připojena nativně. Dále plánujeme využití embedded RP, jež jsme intenzivně testovali mezi Libercem, Prahou a Ostravou, a testy MLD2 (Multicast Lister Discovery).

2.6 Implementace QoS

Zavedli jsme první fázi preferenčních služeb pro přenos určité třídy provozu se zajištěnou kvalitou služby (QoS). Vedle technické implementace jsme museli stanovit i pravidla uplatňování QoS politiky vůči jednotlivým kategoriím uživatelů.

Po ověření v pilotním provozu jsme v síti CESNET2 implementovali architekturu QoS DiffServ domény typu „point-to-cloud“ bez rozlišení cíle (destination unaware). Využíváme techniku E-LSP (Exp-based Label Switched Path) nad páteřní MPLS infrastrukturou v tzv. „short pipe“ tunelovacím režimu MPLS, v němž je při průchodu MPLS páteří zachovávána původní hodnota DSCP transportovaných paketů (DSCP transparency).

QoS DiffServ doména CESNET2 splňuje pro tranzitní provoz dohodnutý provozní profil QoS pro jednotlivé třídy služeb (tj. typicky minimální zaručenou šířku pásma a ostatní kvalitativní charakteristiky jako zpoždění, rozptyl, ztrátovost apod.). V případě nezahlcené páteřní sítě mohou některé QoS třídy navíc využívat zbývající pásmo nad rámec své minimální zaručené šířky (proporcionálně v poměru svých vah). Samozřejmostí implementace QoS v síti CESNET2 je úplná kompatibilita s QoS službami Premium IP (PIP) a Less than Best Effort (LBE) podporovanými v síti GÉANT.

Tabulka 2.1 ukazuje návrh značkování IP paketů pomocí DSCP, jeho mapování do položky Exp MPLS záhlaví a rezervaci šířky pásma pro jednotlivé třídy v rámci Exp-LSP MPLS/DiffServ domény CESNET2. Navržené hodnoty rezervované šířky pásma jednotlivých interních páteřních tras lze chápat jako prvotní doporučení, které však může být modifikováno[1] až do té míry, že zůstanou zachována jen omezení limitující předepsané chování PHB směrovačů:

[1]Na základě provozních zkušeností, konkrétní topologie dané části sítě a možného dohodnutého agregovaného zákaznického provozního provozu v rámci jednotlivých QoS tříd.

Třída služby	*PHB*	*DSCP*	*Exp MPLS*	*Šířka pásma*
Premium IP	EF	EF, CS5	5	25 %
Network Control	AF	CS7, CS6	7, 6	1 %
Gold IP+	AF	AF4x, CS4	4	29 %
Silver IP+	AF	AF3x, CS3, AF2x, CS2	3, 2	14 %
Best Effort	Default	0 (ostatní)	0	30 %
LBE	AF	AF1x, CS1	1	1 %

Tabulka 2.1: Návrh PHB, mapování DSCP/Exp a rezervace šířky pásma pro jednotlivé QoS třídy

- nejvyšší doporučená šířka pásma pro třídu Premium IP je maximálně 33 % z celkové kapacity linky
- třída Best Effort musí mít alokovánu kapacitu nejméně 25 % z celkové kapacity linky

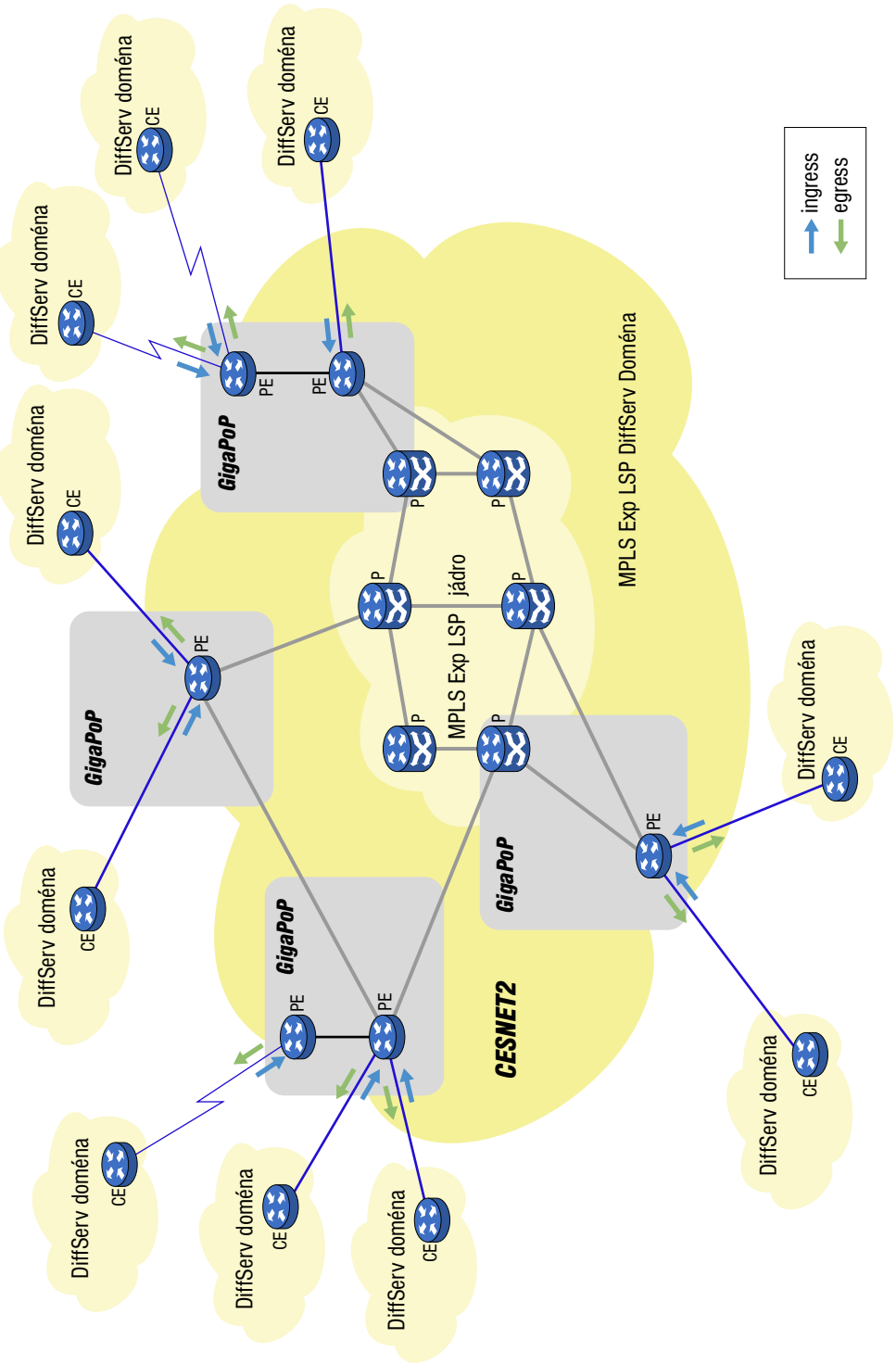
Hodnoty DSCP a Exp MPLS jsou záměrně voleny tak, aby umožňovaly jednoduše využít implicitní metodu přímého mapování nejvyšších tří bitů položky *ToS* IP hlavičky do položky *Exp* MPLS hlavičky (tzv. ToS reflection). Toto mapování provádějí směrovače při zapouzdřování IP paketu do MPLS rámce na hranici MPLS a IP sítě.

Navržená rámcová politika řízení přípustnosti provozu oprávněného využívat tranzit páteřní sítí CESNET2 se zaručenou kvalitou služby z/do jiných DiffServ domén (či Internetu) je založena na tzv. point-to-cloud modelu nevyužívajícím cílovou adresu. Pro každé konkrétní vstupní (výstupní) rozhraní z (do) cizí DiffServ domény do (z) MPLS/DiffServ domény CESNET2 jsou na základě dohodnutého mezidoménového provozního kontraktu pro jednotlivé QoS třídy definovány provozní profily se zaručenou QoS. Jejich dodržování je kontrolováno omezovači (policer) či eventuálně (na výstupu) tvarovači (shaper). Pro danou podporovanou QoS třídu je definována množina vstupních [2] a výstupních [3] parametrů určujících chování trTCM (two rate Three Color Marker) značkovače/omezovače paketů. Ten kontroluje míru překročení reálného provozu vzhledem k dohodnutému provoznímu profilu a provádí eventuální korekční akce (např. reklasifikaci, zahození) pro pakety reprezentující část provozu porušující dohodnutý provozní profil.

Tabulka 2.2 obsahuje velmi benevolentní návrh reklasifikace, přeznačkování vstupního provozu do MPLS DiffServ domény CESNET2 a eventuální následné

[2] Ingress Committed Rate: ICRclass, Ingress Peek Rate: IPRclass, Ingress Burst Conform: IBCclass, Ingress Burst Exceed: IBEclass

[3] Egress Committed Rate: ECRclass, Egress Peek Rate: EPRclass, Egress Burst Conform: EBCclass, Egress Burst Exceed: EBEclass



Obrázek 2.8: Princip point-to-cloud QoS modelu s kontrolou přípustnosti provozu na hranici domén

Třída služby	*Conform* ($t<IBC_t$)	*Exceed* ($IBC_t<t<IBE_t$)	*Violate* ($t>IBE_t$)
Premium IP	Premium IP	Best Effort	Best Effort
Net. control	Network Control	Best Effort	Best Effort
Gold IP+	Gold IP+	Best Effort	Best Effort
Silver IP+	Silver IP+	Best Effort	Best Effort
Best Effort	–	–	–
LBE	–	–	–

Tabulka 2.2: Návrh triviální reklasifikace a přeznačkování provozu podle míry porušení kontraktu

represivní akce podle míry porušení dohodnutého provozního kontraktu v jednotlivých třídách. Cílem je zajistit přijatelné chování sítě (typicky Best Effort) i pro tu část provozu, která porušuje kontrakt. Přitom platí pravidlo, že pokud kterákoliv z tzv. „vyšších“ QoS tříd (Premium IP, Network Control, Gold IP+ a Silver IP+) nevyužije svoji alokovanou šířku pásma, může být zbývající kapacita použita třídou Best Effort a teprve když ani ta ji není schopna celou využít, je zbytek použit třídou Less than Best Effort.

Takto navržená triviální rámcová QoS politika řízení přípustnosti provozu reprezentuje přijatelné řešení pouze pokud je akceptovatelné, že část provozu porušujícího kontrakt v rámci „vyšších“ QoS tříd, která je pak reklasikována do tříd „nižších“ (Best Effort či Less than Best Effort), může způsobit překročení kontrahovaného agregovaného provozu všech QoS tříd dohromady, neboť provoz „nižších“ QoS tříd není v tomto případě nijak omezován. To však nemůže nastat v případě, kdy je celkový kontrahovaný provoz všech QoS tříd dohromady omezen fyzickou přenosovou kapacitou interdoménové přípojky. Jinak je nutné aplikovat hierarchické/dvoustupňové omezení, kdy je prvním omezovačem napřed provedena kontrola přístupnosti celkového agregovaného provozu (bez rozlišení QoS tříd) a převyšující část provozu je zahozena, pak je vyhovující část provozu reklasifikována druhým omezovačem již s ohledem na příslušnost k jednotlivým QoS třídám podle výše uvedené rámcové QoS politiky. Analogicky lze aplikovat obdobnou QoS politiku i na výstupu MPLS DiffServ domény CESNET2.

Nespornou výhodou takto navržené rámcové QoS politiky sítě CESNET2 je zejména jednoduché zřízení a správa kvality služby mezi sousedními QoS/DiffServ doménami, neboť za důvěryhodnost příslušnosti „svého“ provozu do dané QoS třídy je zodpovědná každá sousední QoS/DiffServ doména. Není proto nutné udržovat jakékoliv další informace[4] o důvěryhodnosti zdroje tohoto typu provozu z hlediska požadované QoS[5]. Zároveň je vhodnou implementací

[4] Např. seznamy oprávněných zdrojových IP adres.

[5] Jedinou potenciální výjimkou z tohoto pravidla je třída Network Control, která je typicky ur-

vstupních (čí výstupních) reklasifikátorů/omezovačů možné jednoduše reagovat na porušení dohodnutých provozních mezidoménových QoS kontraktů.

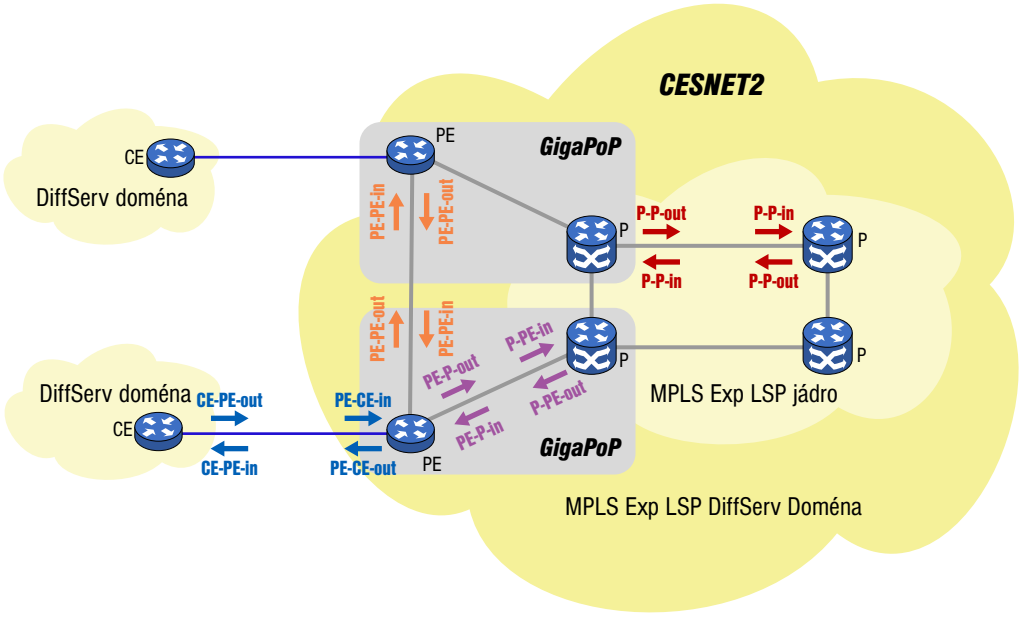
Technická implementace jednotlivých PHB na směrovačích firmy Cisco silně závisí na jejich typu (a druhu/verzi jednotlivých modulů). Proto jsme jak v prostředí IP, tak i MPLS, zvolili pro implementaci EF PHB unifikované řešení využívající techniku front LLQ a pro implementaci AF PHB techniku front CBWFQ, které jsou jednak pro tyto účely doporučovány samotným výrobcem a jednak jsou podporovány prakticky na všech námi používaných směrovačích: Cisco 7600 s OSM moduly, Cisco 7500 a Cisco 7200. Pouze tzv. LAN moduly směrovačů Cisco 7600 tyto techniky nepodporují, a proto musely být nahrazeny vhodně parametrizovanými technikami WRR s prioritní frontou. Konfigurace WRED je implementována u těch zařízení/modulů, které ji podporují.

Kontrola přípustnosti provozu podle jednotlivých QoS tříd se provádí výlučně na vstupu (resp. výstupu) do (z) MPLS/DiffServer domény CESNET2 na rozhraních typu PE-CE-in (PE-CE-out), tedy na hranicích QoS domény podle modelu point-to-cloud bez respektování cílové adresy. Je ovšem otázkou, zda má smysl provádět omezování provozu ještě na výstupu z MPLS/DiffServer domény CESNET2, neboť eventuální část provozu překračující QoS kontrakt již páteří CESNET2 stejně prošla, takže vlastně jediným důvodem pro takovou reklasifikaci/přeznačkování provozu může být jen snaha o vynucení dohodnutého QoS kontraktu se sousední DiffServ doménou.

Obrázek 2.9 představuje jednotlivé typy QoS rozhraní P, PE a CE směrovačů v MPLS/DiffServ doméně CESNET2, na nichž mohou být implementovány vhodné techniky zajištění kvality služby a řízení přípustnosti provozu. V současné době jsou konfigurovány takto:

- PE-CE-in: povinná kontrola přípustnosti vstupního QoS provozu ze sousední/cizí DiffServ domény.
- PE-CE-out: volitelná kontrola přípustnosti výstupního QoS provozu (do sousední/cizí DiffServ domény), povinná implementace PHB (na výstupu).
- PE-PE-out, PE-P-out, P-P-out, P-PE-out: povinná implementace PHB (na výstupu).

čena pro interní přenos prioritních řídicích síťových informací v rámci MPLS/DiffServ domény CESNET2. V některých případech je vhodné tuto třídu podporovat i mezi různými DiffServ doménami (např. pro zaručený přenos některých směrovacích informací). Pak je žádoucí konfigurovat podporu této třídy pomocí vstupního filtru pouze pro bezpečné zdroje v cizích QoS doménách, aby se tak snížila bezpečnostní rizika.



Obrázek 2.9: Typy QoS rozhraní v MPLS/DiffServ doméně CESNET2

2.7 Bezpečnost páteřní sítě

Pro ochranu páteřních směrovačů jsme implementovali CoPP (Control Plane Policing). Snižuje možnost napadení, narušení funkčnosti a pomáhá bránit směrovač před DoS útoky.

CoPP umožňuje nakonfigurovat QoS filtry pro kontrolu provozu. Omezením provozu, kterým se zabývá přímo procesor směrovače, chrání procesor před nadměrným zatížením.

Definovali jsme pět základních tříd – viz tabulka 2.3.

	Účel	*Protokoly*
1.	interní směrování	OSPF, iBGP, PIM, MSDP, IGMP
2.	externí směrování	eBGP, PIM, IGMP, SAP
3.	správa sítě	Telnet, SSH, SNMP, TFTP, NTP, TACACS+, DNS
4.	testování dostupnosti	ICMP echo (ping, traceroute)
5.	nežádoucí provoz	zakazuje veškerý nežádoucí provoz (ICMP, TCP, UDP, IP, OSPF, ...)

Tabulka 2.3: Navržené třídy CoPP

V prvních třech třídách jsme nejdříve vymezili pásmo pro povolený provoz. Provoz, který toto pásmo přesahoval, jsme (dočasně) povolili. Ve čtvrté třídě jsme provoz překračující povolenou šířku pásma zahodili a v páté třídě jsme zakázali

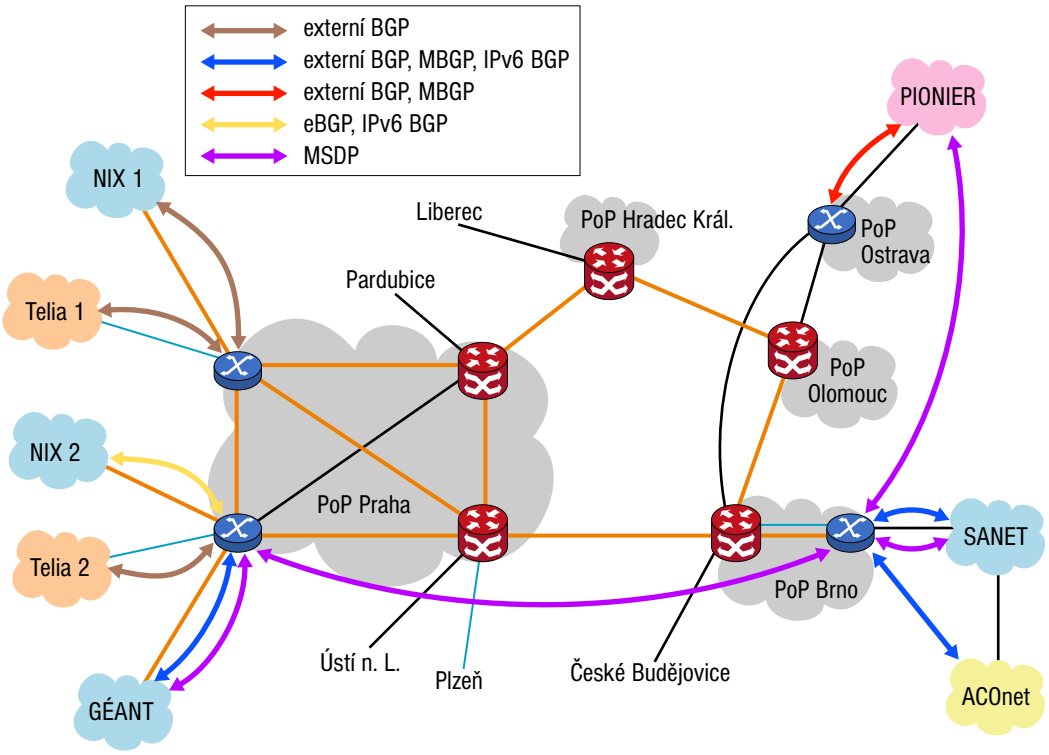
vše. Veškerý provoz, filtry i nastavení QoS pravidelně sledujeme a vyhodnocujeme. Zejména v počátcích byla šířka pásma několikrát měněna. Nasazení proběhlo postupně na všech uzlech a nakonec na hraničních směrovačích.

V průběhu testování se ukázalo, že některé nástroje sledující provoz a „kvalitu“ sítě používají pro testy převážně *ping* (ICMP echo/echo-reply). Po nasazení CoPP tak byla naše síť vyhodnocena jako nespolehlivá. Opět se tedy ověřila skutečnost, že většina uživatelů považuje síť za funkční, pokud *ping* či *traceroute* dostanou odpověď v rozumném čase.

Dalším, spíše zanedbatelným problémem se ukázala být IP adresace páteřní sítě. Tím, že naše síť vznikala postupně, máme v některých částech roztříštěný adresní prostor. Z tohoto důvodu jsou přístupové seznamy definující pravidla pro jednotlivé třídy delší, než kdyby adresace byla navrhována v současné době. Pokusíme se proto najít prostor pro změnu interních adres celé páteřní sítě.

2.8 Externí připojení

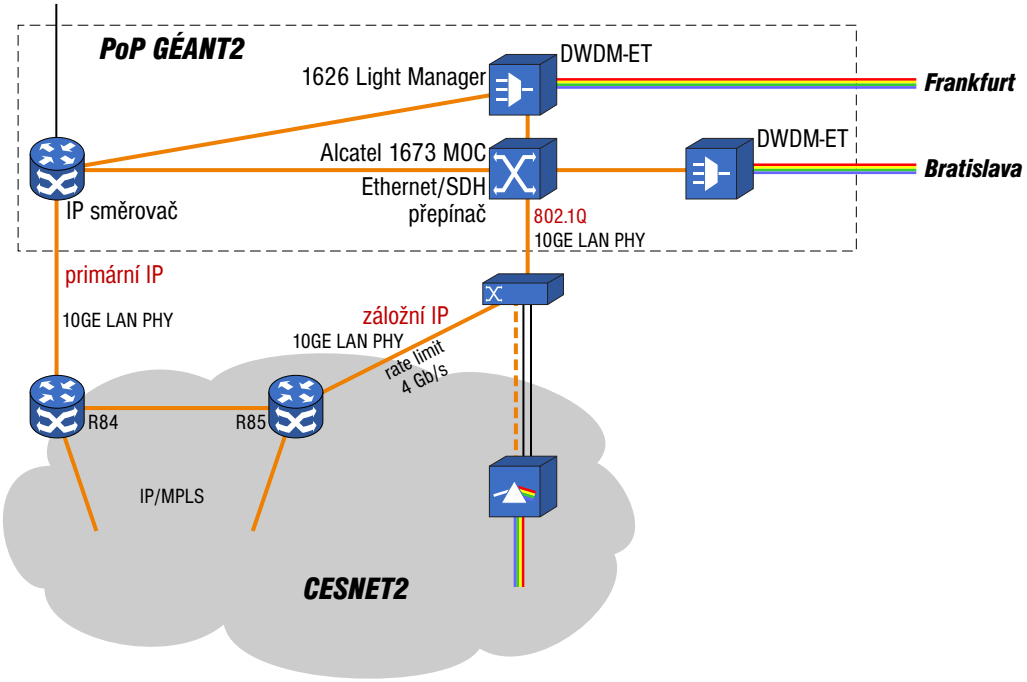
Síť CESNET2 využívá následující externí připojení a peering:



Obrázek 2.10: Externí spoje sítě CESNET2

Zahraniční připojení (běžný provoz): Globální zahraniční připojení nám poskytuje Telia International Carrier. Kapacita spoje je 2,5 Gb/s (POS STM-16/OC-48 na R84) s omezením na 800 Mb/s. Záložní připojení je zajištěno dalším 2,5 Gb/s okruhem na druhý směrovač uzlu Telia (peering směrovač R85).

Připojení do sítě GÉANT2: Nově budovaná celoevropská síť GÉANT2 bude zaměřena na poskytování E2E služeb se zaručenou kvalitou. Její architektura je založena na kombinaci směrované IP sítě a přepínacích prvků s DWDM transportní sítí. Větší flexibility ethernetových služeb ve druhé vrstvě je dosahováno Ethernet/SDH přepínači mapujícími rámce Ethernetu do SDH s využitím zapouzdření GFP-F/VCAT/LCAS. Síť CESNET2 bude mít dva typy připojení: IP a připojení na Ethernet/SDH přepínač GN2 pro poskytování E2E služeb (viz obrázek 2.11). Připojení E2E je plánováno technologií 10GE s podporou 802.1Q VLAN pro agregaci jednotlivých datových toků. V počáteční fázi bude E2E připojení poskytovat 4×1GE, později bude povýšeno do cílového stavu. Předpokládáme, že poskytování E2E služeb bude zahájeno v roce 2006 (po uvedení sítě GÉANT2 do plného provozu). V současné době je funkční IP připojení (na obrázku 2.11 označeno jako „Primary IP“).



Obrázek 2.11: Topologie pražského uzlu sítě GÉANT2 a připojení sítě CESNET2

Národní peering v NIX.CZ: Přístup do NIX.CZ je zajištěn dvěma 10GE LAN PHY okruhy zakončenými na externích směrovačích R84 a R85. Okruhy

jsou realizovány na pronajatých optických vláknech. Peering je zajišťován na úrovni IPv4/IPv6. Dvě nezávislá připojení umožňují rozkládání zátěže a vzájemně se zálohují.

Peering se sítěmi SANET, PIONIER a ACOnet: Propojení se slovenskou akademickou sítí SANET je realizováno optickými vlákny Brno–Bratislava. Trasa je osazena CWDM-GBIC-1550 a je zde použit přepínač Catalyst 3524 jako opakovač. Připojení na polskou akademickou síť PIONIER je rovněž realizováno prostřednictvím optických vláken Ostrava–Bielsko Biala s CWDM-GBIC-1550. Tato trasa je kratší, měří cca. 120 km, a nebylo zde nutné zesílení.

Pro připojení obou sítí používáme zapouzdření 802.1Q. Síť SANET nám umožňuje propojení s rakouskou sítí ACOnet (přes vyhrazenou VLAN).

Kromě vzájemného peeringu našich sítí poskytujeme na tomto propojení přístup SANETu do NIX.CZ a naopak SANET síti CESNET2 připojení do centra SIX, což oběma sítím šetří zahraniční konektivitu. Vzájemné oznamování sítí do peeringových center provádíme na základě BGP komunit (tagů). Síť ACOnet nám rovněž umožňuje peering v rakouském peeringovém centru VIX.

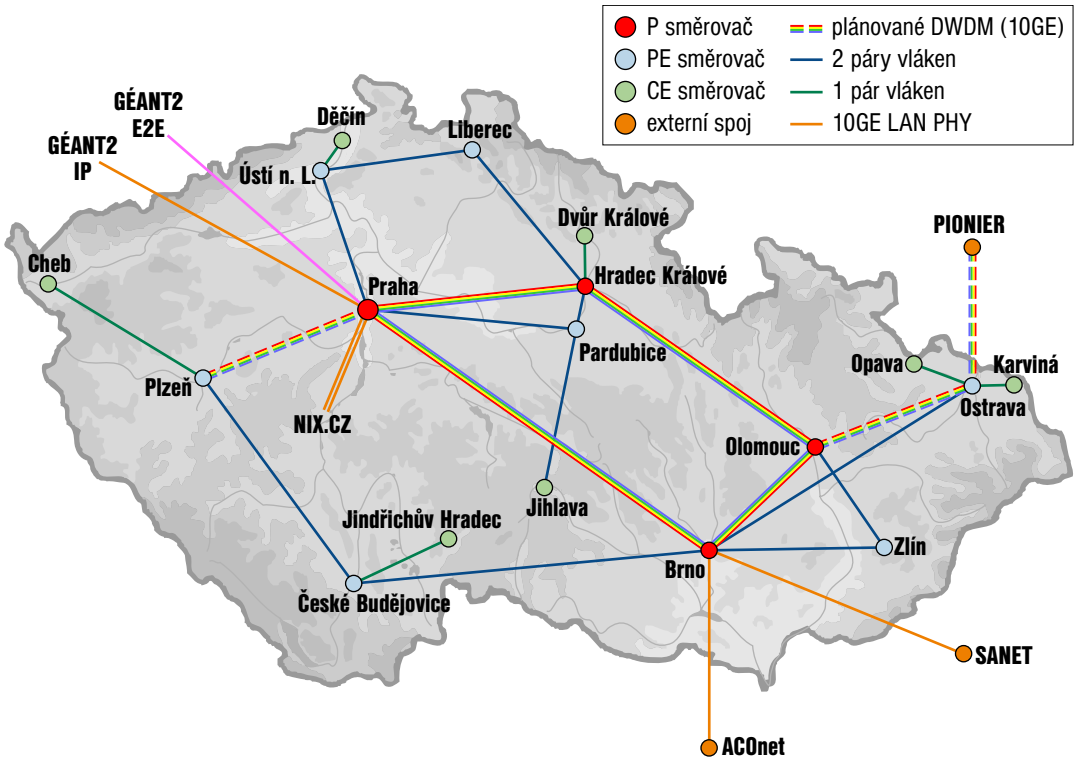
Stávající kapacita propojení 1 Gb/s nepostačuje (nelze například umožnit peering sítě PIONIER s VIX). V současné době připravujeme povýšení spoje Brno–Bratislava na 10 Gb/s s využitím optického zesilovače CLA PB01 (viz obrázek 2.2).

2.9 Plány rozvoje páteřní sítě v dalším období

V následujícím období se budeme zabývat rozvojem všech vrstev sítě CESNET2 se zaměřením na poskytování E2E služeb a zajištění interoperability se sítí GÉANT2. Nedílnou součástí E2E služeb je výzkum a ověřování v oblasti integrace IP/MPLS a optické přenosové vrstvy s cílem vytvořit a zjednodušit mechanismy pro vytváření přenosových E2E kanálů, jejich monitorování a odstraňování problémů. Na úrovni optické přenosové vrstvy budeme pokračovat v rozšiřování DWDM, abychom byli schopni poskytovat lambda služby ve všech klíčových uzlech sítě CESNET2. Nedílnou součástí rozvoje DWDM je i propojení nových úseků na hlavní DWDM okruh tak, aby bylo možné automaticky vytvářet optické přenosové kanály v rámci celého systému bez nutnosti manuálních zásahů.

Na úrovni IP/MPLS vrstvy páteřní sítě se budeme věnovat implementaci nových protokolů a vlastností, jako je IPv6 multicast a VPLS. Rovněž bude pokračovat přepojování uzlů na 10GE. Pro toto povýšení částečně využijeme optické

transportní vrstvy DWDM, částečně i jednodušší a levnější nasazení CLA PB01 (v uzlech, které nebudou připojeny na DWDM v této etapě) na přístupových optických trasách.



Obrázek 2.12: Plánovaný rozvoj DWDM v roce 2006

Očekávanou topologii optické přenosové sítě obsahuje obrázek 2.12.

Jednotlivé aktivity lze shrnout do následujích úkolů:

Rozvoj optické přenosové sítě DWDM

- osazení nových tras Praha–Plzeň a Olomouc–Ostrava
- propojení těchto tras na základní DWDM okruh
- rozšíření DWDM systému z Ostravy do sítě PIONIER a propojení DWDM systémů
- ověřování přenosu „barevných“ signálů
- nasazení CLA PB01 s 4–8kanálovými multiplexory/demultiplexory, ověření přenosu „barevného“ signálu páteřním DWDM systémem
- osazení trasy Brno–Bratislava a Brno–Vídeň

Rozvoj IP/MPLS vrstvy sítě

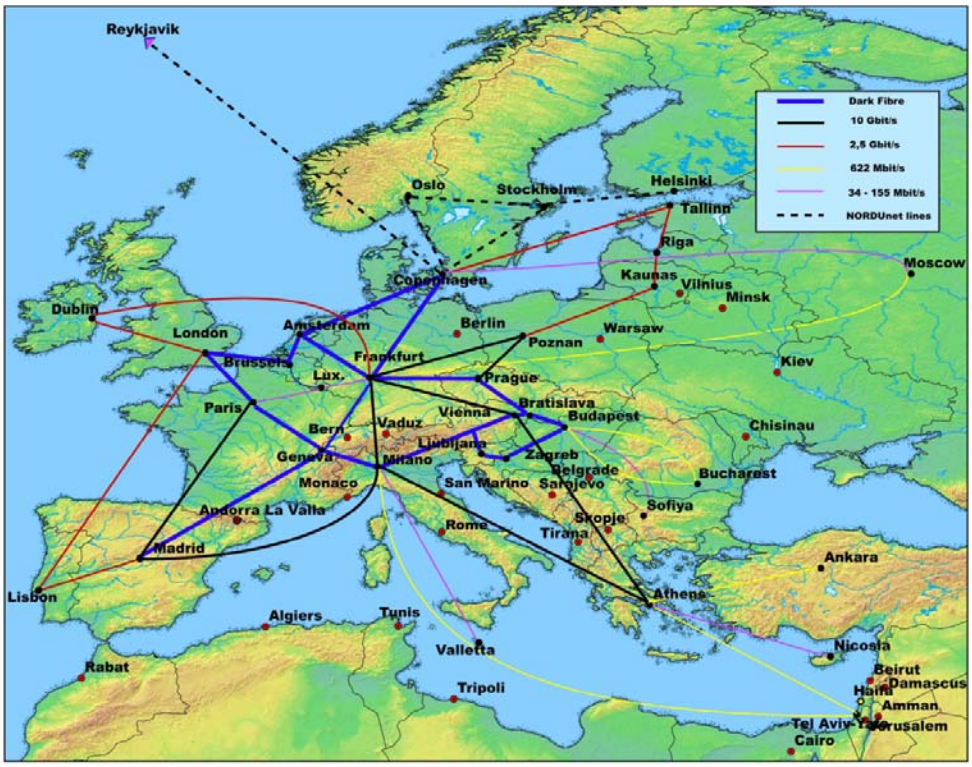
- nativní přenos IPv6 multicastu
- VPLS služby
- NetFlow verze 9

- pokračování migrace na 10GE
- posilování bezpečnosti páteřní sítě (Cisco Guard XT, MARS)
- správa páteřní sítě
- zajištění návaznosti na nově budovanou síť GÉANT2 a zpřístupnění jejích E2E služeb projektům a uživatelům sítě CESNET2

3 Optické sítě

3.1 Výzkum a vývoj CEF Networks

V roce 2005 se ve výzkumu ve světě rozšiřovala snaha prakticky ověřit nové možnosti síťování, založené zejména na užití optických vláken a nových technologií jejich nasvícení a na levných a rychlých nevláknových optických nebo mikrovlnných přenosech. V tom mají CEF Networks jako vláknové sítě řízené hlavními účastníky velmi významné postavení a je výhodou CESNETu, že s tímto zaměřením pracuje již od roku 1999. Spojeným úsilím mnoha evropských NREN se nyní podařilo dosáhnout, že i panevropská síť GÉANT2 je založena na temných vláknech a jiné telekomunikační služby jsou užívány pouze přechodně v místech, kde není přijatelná nabídka pronájmu vláken. GÉANT2 je tedy CEF Network, i když sama toto označení nepoužívá. Užití temných vláken a ostatních služeb pro síť GÉANT2 ukazuje obrázek 3.1.



Obrázek 3.1: Počáteční topologie sítě GÉANT2

Významný vliv na výzkum a vývoj má i „gridová“ idea umožnit koncovým uživatelům sítí řídit a dimenzovat jejich vzájemné propojení a přidělování síťo-

vých prostředků v heterogenním prostředí, sestávajícím z odlišně řízených a technicky různých sítí (multidomain, multivendor) a požadavek snížit rozdíly v možnosti přístupu ke kvalitním vysokorychlostním síťovým službám v různých regionech, zemích a kontinentech (digital divide) a tak přispět k posílení výzkumných kapacit a k rozvoji prosperity a kultury.

Považuje se za zřejmé, že existující produkční počítačové sítě (včetně sítí poskytujících služby pro výzkum a vzdělávání) nedávají dostatečné možnosti k výzkumu v samotné oblasti počítačových sítí. Tím se rozvoj síťování zpomaluje a řešení známých problémů odkládá. Důvodem je zejména požadavek vysoké spolehlivosti služeb produkčních sítí, který velmi omezuje možnosti experimentů a ověřování nových technologií a metod. Tento požadavek také zvyšuje náklady na stavbu a provoz sítí a tím silně limituje možnosti síťování v rozvíjejících se regionech.

Zajímavé možnosti změny situace ukazuje například myšlenka diferenciace spolehlivosti a ceny lambda služeb v rámci jedné sítě, uplatněná například v NLR (National Lambda Rail) v USA. „Core wavelengths" jsou dražší a mají vyšší zaručenou dostupnost než „Flexible wavelengths". Lambda s dostupností například 97 % může být pro některé výzkumné práce dobře použitelná a lambda s „čtyřdevítkovou" dostupností 99,99 % cenově neefektivní. Pronajímatelé vláken ostatně dostupnost 99,99 % obvykle negarantují a dostupnost lambdy nebude vyšší než dostupnost použitého vlákna, vyšší požadavky se řeší redundancí (obvykle zřízením druhé fyzicky odlišné trasy). Málo koncových pracovišť ovšem takovou druhou fyzicky odlišnou vláknovou přístupovou trasu má, takže „vícedevítkovou" dostupnost služeb stejně nemá zajištěnu. Uvedenou diferenciací spolehlivosti a ceny služeb se také poněkud uvolňují možnosti výzkumu síťování, i když požadavek nedestruktivnosti testů na fyzické úrovni a na úrovni čistě optického propojování lambd (bez konverze na elektrický signál) i na úrovni optoelektrického propojování lambd většinou zůstává. Příležitost k testům v produkčních sítích dává spíše redundance součástí sítě (například použití některé vláknové trasy pro pilotní ověření přenosových technologií).

Pro výzkum a vývoj globálních, kontinentálních nebo národních sítí jsou kromě analytických, simulačních a laboratorních prací nezbytné přiměřeně rozlehlé experimentální sítě (nazývané obvykle testbed) nebo experimentální síťové prostředí (network facility), umožňující stavět sítě a optické cesty různých vlastností na určitý počet dnů až měsíců. Vzrůstající snahu učinit výzkum a testování sítí nezávislé na existujících produkčních sítích národního výzkumu a vzdělávání lze pozorovat v USA. Ředitelství CISE (Computer and Information Science and Engineering) programu NSF plánuje iniciativu nazývanou *GENI (Global Environment for Networking Investigations)*, zkoumající nové schopnosti sítí posunout vědu vpřed a stimulovat inovace a ekonomický růst: „The GENI Initiative responds to an urgent and important challenge of the 21st Century to advance

significantly the capabilities provided by networking and distributed system architectures.“, viz stránky iniciativy[1].

Lambdy produkčních sítí také mohou být užívány k vytváření virtuálních testbedů umožňujících experimenty na vyšších vrstvách sítě. Výhodou je levnější možnost provádění geograficky rozsáhlých experimentů, nevýhodou omezené možnosti výzkumu, vývoje a testování technologií pro plně optické sítě (virtuální testbed lambdy používá, ale neimplementuje).

CESNET se od počátku v roce 2003 účastní budování *GLIF (Global Lambda Integrated Facility)* i předchozích experimentálních prací a zabývá se také budováním a experimentálním využíváním CEF testbedu *CzechLight*, který mj. umožňuje účastníkům přístup do GLIFu. Kombinujeme tedy obě hlavní možnosti testování nových sítí a síťových služeb. Na rozdíl od některých jiných síťově rozvinutých zemí se výrazněji zabýváme i otázkou nízké ceny sítí a jejich služeb, částečně vzhledem k vlastním potřebám a částečně vzhledem ke svým dobrým možnostem mezinárodní výzkumné spolupráce se zájemci o takové technologie.

Společně s TERENA a dalšími NREN jsme získali projekt *SEEFIRE* (podporovaný EU od března 2005), v rámci kterého pomáháme v podpoře rozšíření a uplatnění CEF sítí v jihovýchodní Evropě – viz *www.seefire.org*[2]. V druhé polovině roku 2005 jsme se zapojili do příprav projektu EU *Porta Optica Study*, který podporuje stavbu sítí založených na temných vláknech pro potřeby NREN ve východní Evropě. Projekt byl schválen a začne od ledna 2006.

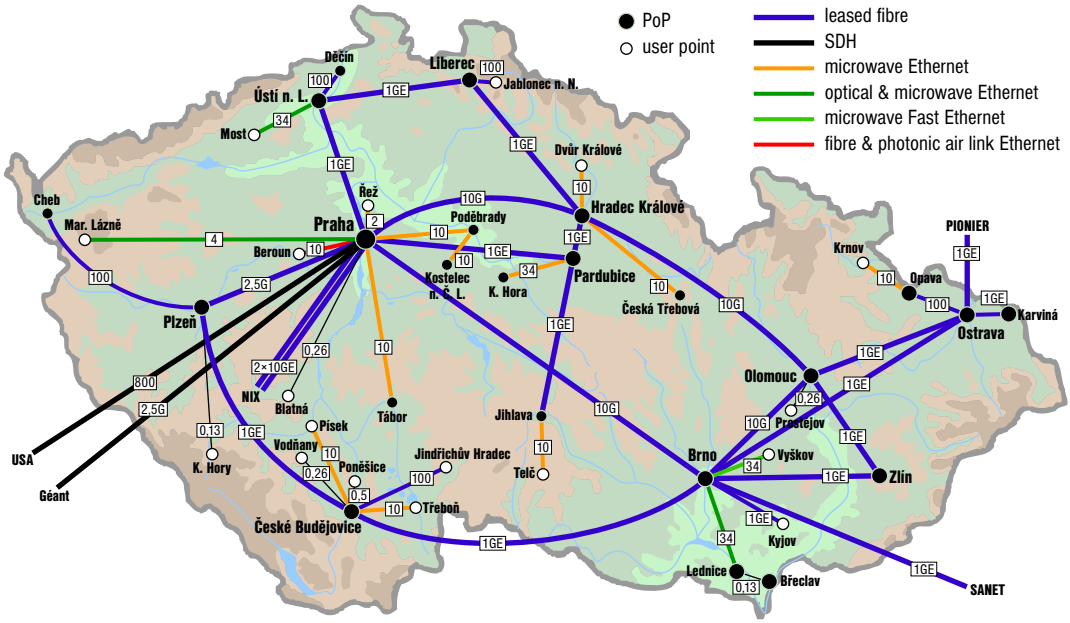
V květnu 2005 jsme v Praze uspořádali druhý mezinárodní *CEF Networks workshop*[3]. Zkušenosti v oblasti navrhování a provozování těchto zákaznických sítí si tři dny vyměňovali zástupci národních vědeckovýzkumných sítí z 26 zemí a zástupci nejvýznamnějších dodavatelů. Ocenili jsme zejména otevřenou výměnu myšlenek a záměrů výzkumníků optických sítí z téměř celé Evropy a z USA, což nám umožňuje efektivně uplatnit náš vlastní výzkumný potenciál. Letos jsme souhrnně prezentovali i městské akademické CEF sítě v ČR[4], které patřily ve světě k prvním (Brno, Praha, Plzeň, Olomouc, Hradec Králové). Workshop byl velmi úspěšný, účastníci vysoce ocenili prezentace a přípravu semináře a doporučili pokračovat v této formě podpory CEF Networks a výměny informací.

Důležitý význam pro výzkum sítí má nynější velký zájem o možnosti vláknového pohraničního propojení NREN sousedních zemí (CBF, Cross Border Fibre connection). Vláknové propojení CESNETu a SANETu z Brna do Bratislavy pou-

[1] *http://www.nsf.gov/cise/geni/*
[2] *http://www.seefire.org/*
[3] *http://www.ces.net/doc/seminars/20050516/*
[4] *http://www.ces.net/doc/seminars/20050516/pr/slavicek-andrs-bic-potuznik-smrha.ppt*

živané od roku 2003 a osazené vlastním transmisním zařízením bylo jedno z prvních na světě. Nyní je již takových mezistátních propojení NREN řada (viz GN2 JRA4 v Evropě) a obdobný vývoj probíhá mezi státy a regiony v USA (vláknové propojování RONs – Regional Optical Networks), viz QUILT. Na takových CBF lze implementovat lambdy propojující NREN/RONs nebo procházející jimi až na koncová pracoviště účastníků a tak potenciálně (na žádost) propojit univerzity a výzkumné ústavy na celém kontinentu lambdami. To ovšem vyžaduje určitý čas, počítaný na měsíce a možná roky. Vzniká ale otázka, jak takové cenově efektivní a velmi flexibilní možnosti síťování nejlépe uplatnit a jakou roli budou mít potom následníci dnešních sítí NLR, Abilene a GÉANT2, které teď používají vlastní (překryvnou) vláknovou strukturu na daném kontinentu. Náklady na pronájem nebo vlastnictví vláken obvykle představují přes 60 % nákladů na rozlehlé sítě, takže optimalizace bude velmi důležitá. Tuto problematiku jsme prezentovali na Fall 2005 Internet2 International Task Force meeting, v sekci „Interconnecting RONs and NRENs and national infrastructure: emerging models for dark-fiber based networks and other optical networking trends in the global R&E community“ – viz prezentace[5] – a na jejím řešení a dalších výzkumech spolupracujeme v panevropském projektu GN2.

Pokračujeme i v práci na rozšíření a zkvalitnění vláknové infrastruktury a doplňujících telekomunikačních služeb pro síť CESNET2. Aktuální topologii sítě CESNET2 ukazuje obrázek 3.2.



Obrázek 3.2: Topologie sítě CESNET2 – prosinec 2005

[5] *http://www.internet2.edu/presentations/fall05/20050919-itf-sima.ppt*

Pro potřeby sítě CESNET2 a testbedu CzechLight jsme realizovali dva průzkumy možností pronájmu vláken na další pracoviště členů a pracoviště připojených účastníků v případech, kdy stávající kapacita připojení se ukazuje jako nedostačující, nebo kde vznikl nový požadavek na speciální kapacity a přenosy. Předpokládáme, že připojení účastníků se postupně stane vícebarevné, tj. že kromě IP služeb na jedné lambdě budou někteří používat i další lambdy poskytované sítěmi CESNET2 a GÉANT2, testbedem Czechlight a GLIFem. Z 22 poptávaných případů plyne, že je většinou velmi nákladné dobudovat vlákno až na určené pracoviště, ale nabídky dobudování se zřizovací cenou do 1 mil. Kč na kilometr optického kabelu jsou k dispozici (mimo zastavěné oblasti je cena nižší). Tato situace je typická i v jiných zemích EU a v USA: hospodářsky vzato umíme zřídit gigabitové a desetigigabitové trasy na velká univerzitní a výzkumná pracoviště, ale ne na větší počet malých pracovišť rozptýlených po některých regionech. Využitelné nabídky pronájmu vláken nevyžadující velký zřizovací náklad byly z 22 poptávaných míst zatím pouze dvě. Další dvě využitelné nabídky jsou od dodavatele, který za zřizovací poplatek vybuduje vláknovou první míli, ale nepronajímá vlákna a nabízí na nich službu 10 Mb/s až 1 Gb/s.

Dlouhé mikrovlnné trasy 10 Mb/s a 34 Mb/s používané zatím v síti CESNET2 pro připojení menších pracovišť nejsou plně vyhovující z hlediska spolehlivosti (příčinou jsou atmosférické jevy, výpadky napájení na retranslačních místech apod.). Proto se snažíme získat L1 nebo L2 okruhy s přenosovou rychlostí alespoň 10 Mb/s užívající vláknové trasy s první mílí řešenou relativně krátkým mikrovlnným spojem nebo vzdušnou optikou zálohovanou mikrovlnou. Z poptaných lokalit se nyní realizuje 7 tras 10 Mb/s, u kterých je možno v případě potřeby později zvýšit přenosovou rychlost. Zároveň jsme s dodavateli zahájili jednání o spolupráci na pilotním řešení rychlejší první míle 100 Mb/s a více za přijatelnou cenu, neboť CESNET získal s takovými trasami vlastní zkušenosti.

3.2 GLIF a CzechLight

GLIF se ukazuje jako unikátní a velmi užitečné prostředí pro výzkum sítí, síťových služeb a síťových aplikací. Uživateli tohoto prostředí jsou různé mezinárodní týmy připravující experimenty, které obvykle mají síťovou i aplikační složku. To znamená, že na přípravě a provedení experimentu se podílejí síťoví výzkumníci ze zemí na trase experimentu a výzkumníci z příslušného oboru využívajícího sítě ze zúčastněných „koncových“ zemí. Existence nebo vytvoření takového týmu je předpokladem úspěšného využití GLIFu pro experimenty. Úkol je tedy podstatně složitější než je využití standardních síťových služeb, je však možno ověřit myšlenky a provést práce a testy, které budou na „pevných“ sítích možné až za několik měsíců nebo let. Tato možnost předstihu může při

správném využití pochopitelně mít z hlediska rozvoje vědy, výzkumu, výroby a obchodu zásadní význam.

Dalším předpokladem je připojení pracovišť členů týmu do GLIFu s takovou přenosovou rychlostí a parametry, které umožňují se na experimentu podílet. Potřebná přenosová rychlost je obvykle 1 Gb/s nebo 10 Gb/s a další požadavky mohou být kladeny na nízké zpoždění, rozptyl ap. Zpravidla je proto potřebné připojit pracoviště vláknem nebo lambdou na uzel GLIFu.

V rámci aktivity *Optické sítě* jsme v roce 2005 koordinovali nebo podporovali vytvoření týmů připravujících a provádějících experimenty, účastnili se těchto prací a řešili připojení potřebných pracovišť v ČR.

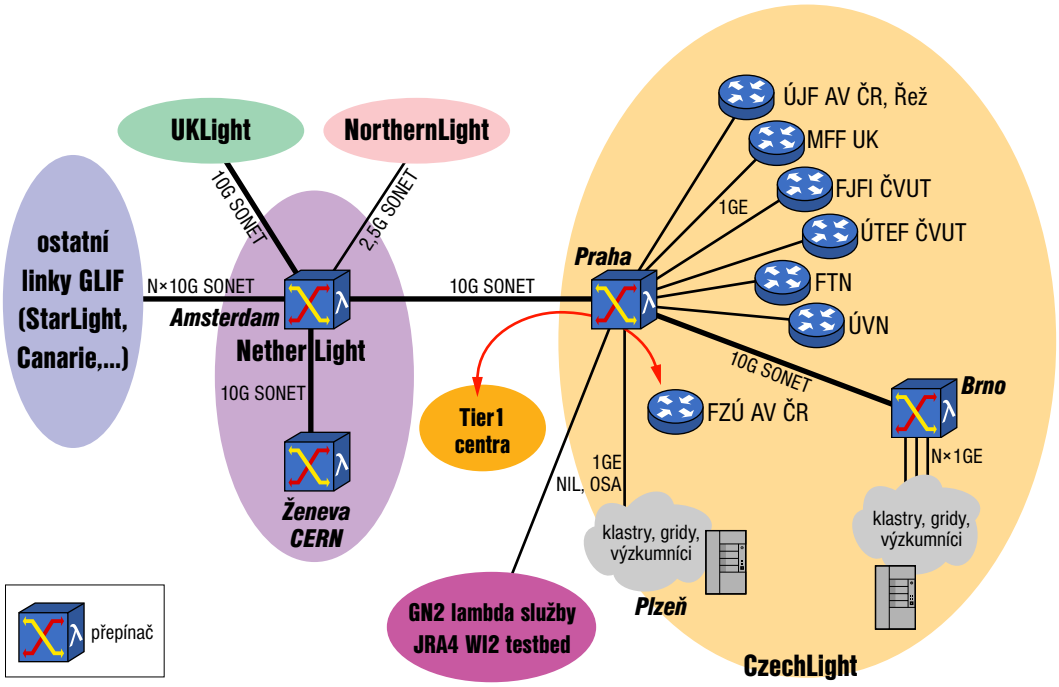
Testbed CzechLight se podařilo rozšířit o další uzel v Brně a vybudovat 10 Gb/s spojení mezi Prahou a Brnem. Na trase je nasazen od konce března 2005 jeden prototyp linkového zesilovače CLA DI01. Je používána pro jednobarevné přenosy a je možno ji využít pro přenos až 8 barev. Původní pokusy realizovat počátkem roku 2005 tuto trasu v délce 295,8 km jako NIL se nepodařily kvůli velké délce a pravděpodobně i nehomogenitě trasy (užití různých typů vláken). V srpnu 2005 se podařilo dohodnout zkrácení trasy využitím nových úseků optických kabelů v oblasti Prahy (nyní je 283,9 km).

Spolehlivost této trasy byla podmínkou zapojení MU v Brně do přípravy a realizace demonstrace vícebodové videokonference v HDTV kvalitě na konferenci *iGrid* v září 2005 mezi MU Brno, San Diegem a Baton Rouge (Luisiana State University), užívající 10 Gb/s propojení přes Prahu (CzechLight), Amsterdam (NetherLight) a Chicago (StarLight) prostředky GLIF. Demonstrace proběhla úspěšně se značným ohlasem, je dostupný i popis přenosu[6]. Podrobnější informace obsahuje kapitola 10.2.1. Tato trasa byla pak využita MU v Brně a CESNETem i pro následné akce.

Koncem roku 2005 byla sestavena nová vláknová trasa CzechLight z Masarykovy univerzity v Brně do Polského Těšína na vlákna polské sítě PIONIER. Tato trasa umožní testování nových přenosových technologií mezi Prahou a Poznaní a dává i možnost zapojení polských výzkumníků do GLIF. Pro trasy CzechLight jsou využita vlákna získaná převážně jako bonus při zajišťování dodávek pro síť CESNET2. Rozvoj CzechLight a propojení na GLIF souhrnně ukazuje obrázek 3.3. Služby CzechLight a GLIF budou přístupné i prostřednictvím lambda služeb sítě CESNET2.

Ve Fyzikálním ústavu AV ČR (FZÚ) Na Slovance bylo na CzechLight připojeno Regionální výpočetní centrum pro fyziku částic. Centrum zajišťuje výpočetní a úložnou kapacitu pro náročné výpočty experimentů D0 na urychlovači TEVATRON ve FNAL a ATLAS a ALICE na budovaném urychlovači LHC v CERN, který

[6] *http://www.cesnet.cz/doc/tisk/2005/prenos.pdf*



Obrázek 3.3: CzechLight – prosinec 2005

zahájí provoz v roce 2007. Pro běžící experiment D0 se provádějí v Centru počítačové simulace činnosti detektoru D0 a zpracování experimentálních dat, pro experimenty ATLAS a ALICE probíhají počítačové simulace v rámci přípravy fyzikálního programu pro tyto experimenty. Součástí centra je výpočetní farma Goliáš, která má v současné době 200 procesorů a 40 TB diskového prostoru. Centrum je integrováno do prostředí mezinárodního gridu *LCG (LHC Computing Grid)*.

V roce 2005 jsme s podporou CESNETu a PASNETu dokončili propojení pražských laboratoří spolupracujících na experimentech fyziky částic vyhrazenými spoji 1 Gb/s. K testování průchodnosti této sítě mezi jednotlivými institucemi v Praze byl použit program *iperf* verze 1.7.0, který byl vždy spuštěn na jednom ze serverů clusteru Goliáš ve FZÚ a současně na serveru, umístěném za směrovačem v každé připojené instituci (případně přímo na směrovači). Podrobnější popis propojení a vybavení jednotlivých pracovišť a záznam zátěžových testů uvádíme v technické zprávě číslo 21/2005. Trasy realizované vyhrazenými temnými vlákny lze povýšit na 10GE s vícebarevným propojením dle potřeby (například i pro využití připravovaných lambda služeb GÉANT2 a CESNET2). Přes síť GÉANT2 by mohla být vybudována například lambda mezi FZÚ a Tier1 centrem v Karlsruhe. V zásadě platí, že experimenty a služby již dostupné na CESNET2 a GÉANT2 nebudou zajišťovány na GLIF a CzechLight a že prostředky GLIF a CzechLight jsou odnímatelné (například v důsledku provádění testů no-

vých technologií na vrstvě L1) a nejsou experimentu přiděleny trvale, ale podle dohodnutého plánu. Například se předpokládá, že v roce 2006 bude již pro připojení CzechLight na NetherLight použita 10 Gb/s lambda sítě GÉANT.

Pro výzkumy a experimenty pracovišť zabývajících se částicovou fyzikou se podařilo na GLIF a CzechLight zprovoznit dvě mezinárodní lambdy 1 Gb/s do Tier1 center. První z nich je do Fermiho národní laboratoře v USA (FNAL), druhá do ASGCC (Academia Sinica Grid Computing Center) v Taipei na Taiwanu. Obě trasy vedou přes NetherLight v Amsterdamu. Trasa do FNAL byla využívána již v polovině roku, propojení do Taipei bylo ověřeno krátce na to, ale zorganizovat využití se podařilo až od prosince 2005. Důvodem byla zejména rezervace plné 10 Gb/s kapacity trasy Praha–Amsterdam pro *iGrid* a následné experimenty.

Spoj do Fermiho národní laboratoře byl intenzivně využíván pro přenos vstupních dat a zpětně i výsledků simulací a rekonstrukcí pro experiment D0, spoj do ASGCC začal být využíván pro přenos dat mezi FZÚ a Tier1 centrem v ASGCC v rámci projektu LCG. Pro další období plánujeme zřídit centrální úložiště dat v rámci společného fyzikálního projektu s University of Alberta (Kanada) a jeho propojení s Kanadou prostřednictvím GLIF a CzechLight.

Experimentální užití GLIF a CzechLight je otevřeno pro všechny obory výzkumu, které mohou podobné prostředí využít pro ověření nových aplikací. Perspektivní se ukazují zejména aplikace spojené s vizualizací, geografickými informačními systémy, mapami, zpracováním grafických informací apod. Vedle fyziky částic se jako další obor schopný v ČR účelně využít takové prostředí ukazuje zdravotnictví. Experimenty v této oblasti připravujeme ve spolupráci s příslušnou aktivitou našeho výzkumného záměru.

Jedním z prvních subjektů z oblasti špičkového zdravotnictví, který vyjádřil svůj zájem se zapojit do nových aplikací, byla Ústřední vojenská nemocnice (ÚVN) v Praze Střešovicích. Druhým klíčovým subjektem je Fakultní Thomayerova nemocnice (FTN) v Praze Krči, která má zájem a potenciál stát se komunikačním centrem pro zpracování obrazových dat v pražské oblasti a navázat tak na aktivity brněnského MeDiMedu. Dalším spolupracujícím subjektem je v současné době Masarykova nemocnice v Ústí nad Labem (MNÚL). Jedná se o nemocnici vybavenou systémem bezfilmového zpracování obrazové informace, která se snaží sledovat nejmodernější trendy. V současné době je například zapojena do projektu programu Informační společnost Akademie věd *MediGRID*. Uvedené tři nemocnice již jsou připojeny temným vláknem, což dovoluje zahájit testování aplikací.

Například FTN má zájem o konzultace na špičkovém pracovišti v oblasti neurověd v ÚVN. Protože obě nemocnice mají vybavení pro bezfilmové zpracování PACS (Picture Archiving and Communication System), nabízí se možnost propojení přes počítačové sítě. Takové propojení však musí splnit minimálně dva

požadavky: dostatečnou rychlost přenosu snímků z FTN do ÚVN a zabezpečení datových přenosů proti nežádoucímu odposlechu. Oba aspekty splňuje propojení lambda službou, které umožňuje přenos se zanedbatelným zpožděním a navíc využití vyhrazené vlnové délky zajišťuje oddělení tohoto provozu. Během pilotního provozu budeme analyzovat možnosti budování příslušné bezpečnostní politiky a rovněž možnosti propojení diskových polí archivu medicínských dat s přímým propojením protokolem FC (Fibre Channel).

Jiná situace je v případě připravovaného propojení MNÚL a ÚVN, kde se od začátku řeší výzkum v oblasti propojení a zálohování datových skladů systémů PACS. V uvedených lokalitách budeme testovat spolehlivost ukládaných dat a způsoby řešení v případě výpadku nebo odstavení datového skladu v jedné lokalitě (servis, profylaxe), případně zda systém umožní práci s daty v druhé lokalitě s akceptovatelnou dobou odezvy. Nezanedbatelnou výhodou je také geografická vzdálenost datových úložišť ÚVN A MNÚL přibližně 100 km od sebe, což téměř vylučuje souběžné poškození obou systémů i v případě katastrofických scénářů. To je důležité zejména pro ÚVN, která je zapojena do systému NATO.

Napojení ÚVN na CzechLight a GLIF nám navíc umožňuje zahájit přípravné práce k zapojení této nemocnice do světového projektu *Biomedical Informatics Research Network (BIRN)* s koordinačním centrem v University of California, San Diego, který v současné době zajišťuje propojení výzkumných týmů v oblasti neurověd z 30 univerzit a 21 dalších organizací USA a Evropy.

3.3 Metody přenášení dat v CEF sítích

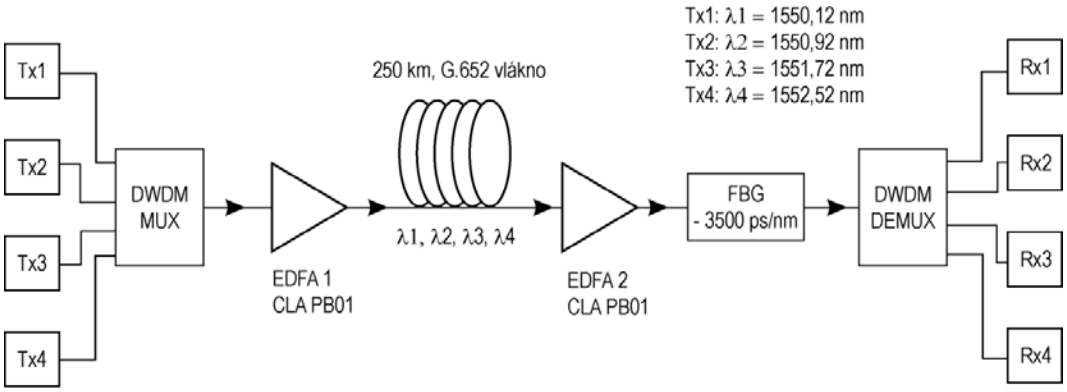
Pomocí komerčního simulačního software jsme analyzovali možnosti vícenásobného (DWDM) přenosu signálů s přenosovou rychlostí 10 Gb/s (zejména pro 10GE) pro délky tras až 1000 km. Praktické ověření bylo limitováno počtem 4 kusů EDFA zesilovačů které jsme měli k dispozici pro laboratorní ověření. Další testy jsou naplánovány s využitím zesilovačů *CzechLight Amplifiers (CLA)*. Teoretické i experimentální výsledky využijeme při dalším rozvoji experimentální sítě CzechLight, konkrétně pro vláknové propojení Brno–Poznaň.

Experimentálně jsme ověřili možnost přenosu 4 DWDM kanálů s přenosovou rychlostí 10 Gb/s na vzdálenost 250 km po vlákně G.652 metodou NIL. Blokové schéma je uvedeno na obrázku 3.4. Na této trase jsme také testovali fixní a laditelné vláknové Braggovské mřížky (FBG) firmy TeraXion. Kompenzací chromatické disperze přenosového vlákna pomocí FGB jsme nahradili nákladné moduly kompenzačních vláken a zároveň snížili počet potřebných EDFA. První výsledky vícekanálových 10GE přenosů metodou NIL byly prezentovány na konferenci ONDM v Miláně. Na této konferenci byly pracovníky TU Copenhagen prezen-

továny podobné výsledky s 10GE přenosy na stejnou vzdálenost (252 km), ale s využitím linkového zesilovače.

Prototyp zesilovače CLA PB01 nasazený v síti CESNET2 v unikátním OSA (One Side Amplification) zapojení na lince Praha–Hradec Králové přešel v březnu z experimentálního do běžného provozu a pracoval bez nejmenších problémů až do osazení linky jinou technologií. Předpokládáme jeho další nasazení na lince Praha–Ústí n. L. sítě CESNET2. Další prototyp CLA DI01 úspěšně pracuje na lince CzechLight Praha–Brno ve funkci jediného linkového zesilovače.

V současné době se připravuje licenční výroba zařízení CLA.

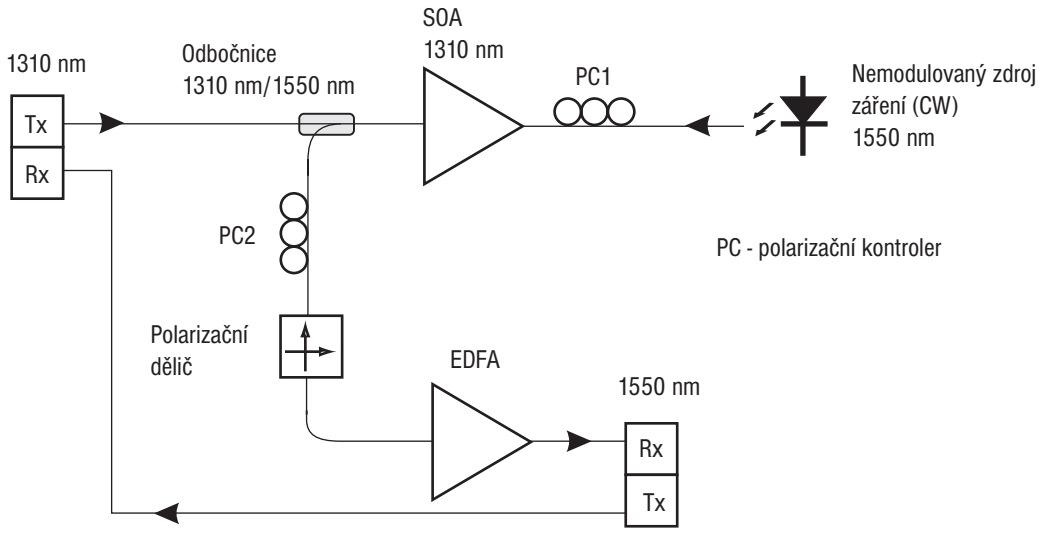


Obrázek 3.4: Přenos 4 DWDM kanálů přes 250 km vlákna G.652

Zahájili jsme stavbu laditelného kompenzátoru disperze s použitím vícekanálových laditelných FBG (další prototyp zařízení na bázi CLA). Ověřili jsme možnosti nasazení FBG na trase CzechLight Praha–Brno. Dále jsme navrhli nové řešení s kompenzací chromatické disperze pomocí FBG pro trasy Brno–Bratislava a Brno–Vídeň pro síť CESNET2. Pro tyto trasy a další aplikace je rozpracován další prototyp EDFA zesilovačů na bázi CLA – výkonový zesilovač.

Další oblast, ve které jsme provedli mnoho experimentů, se týká zvětšení dosahu přenosových zařízení pracujících v pásmu 1310 nm. To je velmi výhodné pro eliminaci nákladných transpondérů nutných pro připojení výkonných serverů a clusterů s 10GE LR rozhraními. Při využití ramanovského distribuovaného zesilování v přenosovém vláknu byl základní deklarovaný NIL dosah 10 km prodloužen na 135 km. Dále pak s užitím jednoho linkového zesilovače na 200 km. Ověřili jsme použití optických polovodičových zesilovačů (SOA), které se stávají dostupnějšími než praseodymem dopované vláknové zesilovače. Tyto výsledky jsme prezentovali například na mezinárodní konferenci ICTON v Barceloně a na konferenci OK2005.

Ověřili jsme možnosti plně optické konverze modulovaných signálů z pásma 1310 nm do pásma 1550 nm v polovodičovém optickém zesilovači. Blokové schéma je znázorněno na obrázku 3.5.

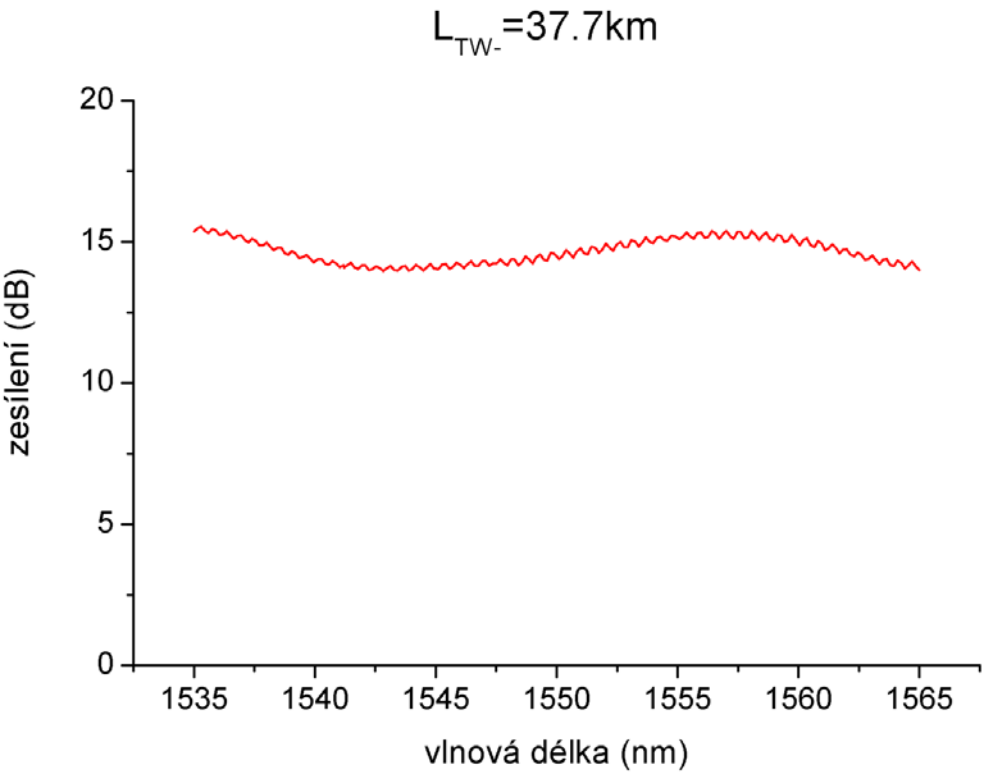


Obrázek 3.5: Blokové schéma SOA konvertoru 1310 nm/1550 nm

Testovali jsme SOA firmy InPhenix typu IPSAD1301 a IPSAD1303. Konverze signálu byla úspěšná při modulační rychlosti 1 Gb/s a 2,5 Gb/s. Při přenosové rychlosti 10 Gb/s byl očkový diagram signálu 1550 nm zavřený, náběžné a sestupné hrany málo strmé. Použité typy SOA nejsou vhodné pro bitovou rychlost 10 Gb/s, proto se budeme zabývat testováním dalších typů SOA, které budou vhodné i pro tyto přenosové rychlosti (zejména pro použití s 10GE síťovými kartami pro výkonné servery). Ověřili jsme možnosti použití SOA různých výrobců (InPhenix , CIP, Covega) v aplikaci výkonových zesilovačů v systémech CWDM.

Jako další důležitý prvek pro stavbu CEF sítí jsme realizovali zdroj čerpání pro ramanovské vláknové zesilovače. Architektura toho čerpacího zdroje je opět převzata z návrhu zařízení CLA a je v něm použit komerční modul se čtyřmi polovodičovými lasery firmy Amonics s celkovým výkonem 500 mW určený pro zesilování v pásmu 1530 nm až 1560 nm. Spektrální závislost zesílení distribuovaného ramanovského zesilovače (změřeno s vláknem NZ DSF délky 37 km) je znázorněna na obrázku 3.6.

Dalším prvkem, který je nutný pro stavbu plně optických sítí, je optický přepínač. V průběhu roku jsme se snažili získat vhodný prvek, který by nám umožnil pokračovat ve stavbě dalšího zařízení na bázi CLA. Vhodný optický přepínač se podařilo zakoupit od firmy DuPont. Jedná se o 8×8portový plně optický přepínací modul, který je možné ovládat pomocí rozhraní RS-232. V současné

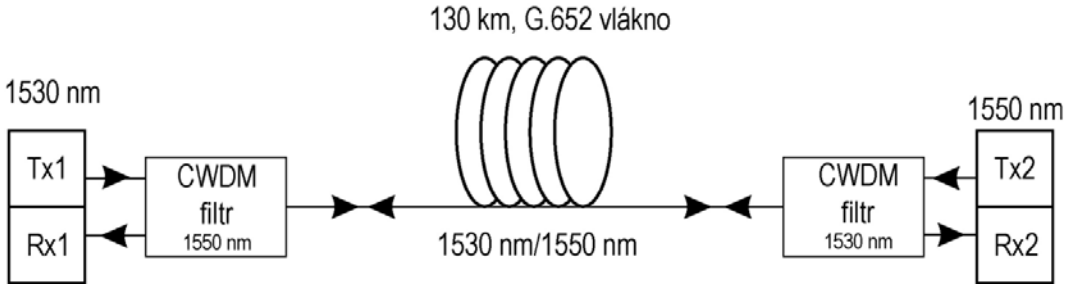


Obrázek 3.6: Spektrální závislost zesílení 37 km NZ DSF čerpaného realizovaným zdrojem

době pracujeme na prvním prototypu tohoto zařízení a plánujeme laboratorní ověření.

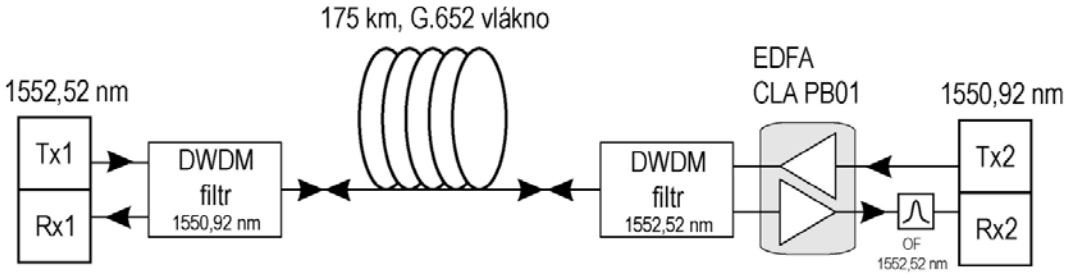
Ověřovali jsme také možnosti obousměrných optických přenosů po jediném vlákně, a to jak v čistě pasivních zapojeních (bez užití optického zesilování signálu), tak i v cenově efektivních zapojeních využívajících zesilování pouze na jedné straně linky (OSA – One Side Amplification).

V pasivních zapojeních jsme porovnali užití optických rozbočnic (50/50), cirkulátorů a filtrů. Pro nenáročné aplikace je nejvhodnější použít optické rozbočnice. Ty mají sice vyšší vložný útlum, ale ve srovnání s cirkulátory a filtry jsou to jednoduché a levné součástky. Nasazení těchto rozbočnic při použití 1GE CWDM transceiverů (1530 nm/1550 nm, dosvit cca 120 km) umožnilo překonat vzdálenost 95 km po jednom vlákně. Optické cirkulátory se pro tuto aplikaci ukázaly jako méně vhodné a dosažená vzdálenost je shodná jako při použití rozbočnic. Důvodem je to, že značně citlivé přijímače těchto transceiverů jsou již ovlivňovány signálem vracejícím se z trasy vlivem zpětného Rayleighova rozptylu. Vzdálenosti až do 130 km (na jednom vlákně) je možné překonat se shodnými CWDM transceivery při použití CWDM filtrů v tříportových verzích, blokové schéma je znázorněno na obrázku 3.7.



Obrázek 3.7: Jednovláknový obousměrný pasivní přenos přes 130 km G.652

Pro další zvýšení překlenutelné vzdálenosti jsme ověřovali zapojení využívající metodu OSA při použití EDFA. V této konfiguraci jsme prověřili možnosti nasazení jak výše zmíněných CWDM transceiverů, vhodných pro přenos pouze jednoho obousměrného kanálu (omezeno pracovní oblastí EDFA), tak i 1GE DWDM transceiverů umožňujících případný přenos více obousměrných kanálů současně. V prvním případě byl deklarovaný dosah 120 km na páru vláken zvýšen na 180 km při použití jednoho vlákna, pro DWDM transceivery se podařilo zvýšit dosah ze 105 km na 175 km (pro vzdálenosti nad 150 km bylo nutno nasadit další filtr před přijímač pro odstranění zesílené spontánní emise). Schéma je znázorněno na obrázku 3.8, použité DWDM filtry jsou tzv. reflexivní 3-portové filtry. V těchto experimentech budeme pokračovat a plánujeme použít novější transceivery, které dosvítí až na vzdálenost 160 km.



Obrázek 3.8: Jednovláknový obousměrný DWDM OSA přenos přes 175 km vlákna G.652

3.4 Vysokorychlostní přenosy vzduchem

V oblasti vysokorychlostních sítí představuje realizace první míle ke koncovému účastníkovi významnou otázku. Ideální variantou je použití optického vlákna, ale to je v mnoha případech příliš nákladné nebo stavebně nemožné. Proto se zabýváme i vyhledáváním vhodných alternativních přenosových technologií

mezi vzdušnými optickými spoji (Free Space Optics, FSO) a rádiovými spoji. Přenosové rychlosti jsou nižší než u vláknových přípojek, nižší jsou však i ceny. Každá z těchto uvedených technologií má své výhody i nevýhody.

Systémy FSO nabízí obecně vyšší přenosové rychlosti, běžně dosahují 100 Mb/s i více, ale při použití na větší vzdálenosti může být jejich výkon degradován povětrnostními vlivy – například mlhou nebo velkými výkyvy teplot doprovázenými rozladěním optického zaměření spoje.

Rádiová zařízení jsou naopak vůči povětrnostním vlivům odolná, dokáží pracovat i v režimech point-to-multipoint a lze je použít i pro spoje s nepřímou viditelností, jejich propustnost však bývá nižší. Uvažujeme-li systémy pohybující se v cenových kategoriích do 100 tisíc Kč na jeden skok a pracující v nelicencovaných pásmech 2,4 a 5 GHz, musíme počítat také s možností rušení jejich signálu. V případě účastníků požadujících vysokou propustnost spoje bez možnosti použití optického vlákna proto doporučujeme zvolit kombinaci primárního FSO systému zálohovaného sekundárním rádiovým spojem.

V roce 2005 došlo k významné změně v možnosti využívání volného kmitočtového pásma. Na základě všeobecného oprávnění VO-R/12/08.2005-34 vydaného Českým telekomunikačním úřadem je nyní povolen provoz v oblasti 5 GHz s tím, že pásmo 5,15–5,35 GHz lze využít pouze uvnitř budov a pásma 5,470–5,725 GHz a 5,725–5,875 GHz i ve venkovním prostředí. Z pohledu výstavby první míle znamená především legalizace pásma 5,4 GHz znatelný posun vpřed, protože dovoluje výstavbu trasy ve venkovním prostředí s 10× vyšším vyzářeným výkonem než v pásmu 2,4 GHz a 100× vyšším než v do této doby povoleném pásmu 5,725–5,875 GHz (zkráceně 5,8 GHz). Zařízení pro pásmo 5,4 GHz jsou znatelně dražší než přístupové body pro použití uvnitř budov a pro „domácí“ použití (jejich ceny se pohybují od 25 tisíc Kč výše) a budou se zřejmě i nadále vyrábět hlavně v provedení pro venkovní sítě. To by společně s odlišnou regulací vnitřních a vnějších sítí i vzhledem k pásmu 11 nepřekrývajících se kanálů mělo (alespoň podle optimistických předpovědí) významně snížit potíže se vzájemným rušením sítí, jak je známe z pásma 2,4 Ghz. Další výhodou zařízení této kategorie obvykle je vyšší úroveň zabezpečení přenášených dat.

V roce 2005 jsme se v rámci aktivity *Optické sítě* orientovali na obě oblasti bezdrátových technologií. V případě FSO jsme se soustředili na vývoj vlastního prototypu nízkonákladového zařízení a provedli jsme technické srovnání existujících produktů a prototypů. V oblasti rádiových spojů jsme zmapovali situaci na trhu zařízení pro nově uvolněné pásmo 5 GHz a v reálném provozu jsme ověřili produkt WinLink. Výsledky těchto prací jsou podrobněji uvedeny ve zprávách „Gigabitové a 100 Mb/s přenosy vzduchem“, „Soudobé trendy v oblasti moderních bezdrátových spojů“ a „Bezdrátový spoj pro pásmo 5 GHz – WinLink 1000“.

Práce na prototypech nízkonákladových zařízení pro optický přenos vzduchem spočívaly v přestavbě mechanické části původního pojítka 10 Mb/s pro zvýšení odolnosti a stability a také v hledání a vyhodnocování funkčních vzorů elektronické části pro přenos 100 Mb/s, včetně možností vyšších rychlostí přenosu. Pro jejich uplatnění v první míli spojů L2 je potřebné nahradit v pojítku dosavadní konvertor optika-Ethernet konvertorem optika-optika a vytvořit autonomní systém s bezdrátovou zálohou spoje a možností on-line monitorování stavu optického pojítka.

Pro ověření zařízení FSO 100 Mb/s jsme hledali, porovnávali a testovali zařízení dostupná na trhu i zařízení, která jsou dosud ve vývoji (například u původních autorů zařízení FSO 10 Mb/s). Výsledkem ověření byla identifikace vhodných i problematických prvků konstrukčního řešení.

Ze srovnání a ověření jednotlivých optických pojítek vychází nejvýhodněji (z hlediska poměru cena/výkon i technických parametrů) pojítko Elspeedy 100, se kterým bylo dosaženo velice zajímavých výsledků v porovnání s komerčně dostupnými výrobky (testován byl přenos 100 Mb/s na vzdálenost 3000 m). Prodejní cena tohoto pojítka po ukončení vývoje by se mohla pohybovat kolem 80 000,– Kč. Elspeedy 100 vyžaduje značné úpravy, protože jeho stávající mechanika je výrobně relativně nákladná a nelze docílit snadného a přesného zaměření optického svazku na větší vzdálenosti. Při výrobě by bylo vhodnější využít přesných tažených hliníkových profilů, čímž by bylo dosaženo ještě zajímavější prodejní ceny.

Na základě těchto rozborů a testů jsme navrhli pro přestavěnou mechanickou část připravovaného prototypu novou elektroniku nazývanou „LightShuttle“. Provedli jsme návrh plošných spojů a výběr součástek pro cílové modulární řešení elektroniky 100 Mb/s i jejich postupné oživování. Testování nového prototypu plánujeme provést v prvním pololetí 2006. Připravované pojítko s novou mechanickou konstrukcí má proti optickému pojítku Elspeedy 100 čtyřnásobnou plochu čočky pro příjem signálu, zvýšenou přesnost zaměřování a odolnější provedení pro „dálkové“ spoje. Výsledky dosavadního vývoje a testů se jeví jako využitelné i z hlediska pokračování ve vývoji pojítka s rychlostmi nad 100 Mb/s.

Zahájení výroby vlastními silami není pochopitelně cílem výzkumného záměru. Jako nejvhodnější se jeví vždy dokončit vývoj určitého prototypu a pak poskytnout výrobní licence. Výhodou sdružení je možnost ověřit prototypy i následná dodavatelská řešení v testbedu CzechLight nebo na pilotní trase produkční sítě CESNET2.

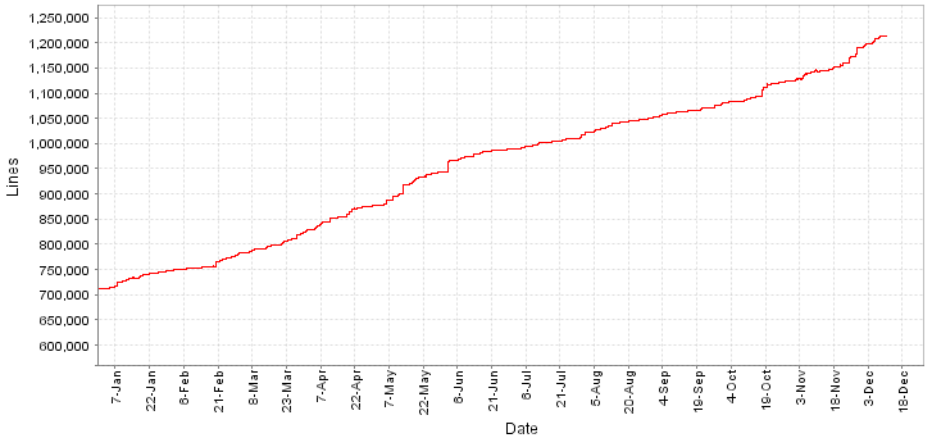
4 Programovatelný hardware

Aktivita *Programovatelný hardware* pokračovala v roce 2005 bez významných změn ve svém zaměření oproti předchozímu roku. Naší snahou bylo zkoncentrovat vývojové kapacity na hlavní úkoly, ale přitom zcela neztratit ze zřetele další možné aplikace programovatelného hardwaru.

V roce 2005 byly úspěšně zakončeny dva projekty 5. rámcového programu IST EU s naší účastí: SCAMPI a 6NET. Při závěrečném hodnocení projektu *SCAMPI*, které se konalo v lednu 2005 v Brně, doporučili oponenti prozkoumat možnosti komerčního využití výsledků projektu, především tedy námi vyvinutého monitorovacího adaptéru SCAMPI. CESNET pak v průběhu roku vyvinul v tomto směru značné úsilí, jehož některé výsledky se již rýsují, ačkoli jednání ještě nejsou dokončena a definitivní rozhodnutí zatím nepadlo.

Řešitelský tým aktivity se dále rozšířil a na konci roku 2005 čítal 74 aktivních členů. Největší nárůst byl ve skupině vývojářů VHDL, neboť se ukázalo, že efektivní zapojení studentů do náročných vývojových prací se neobejde bez předchozího získávání zkušeností na jednodušších úkolech a následné selekce těch nejlepších. Snažíme se proto podchycovat zájemce o spolupráci v oblasti vývoje VHDL z řad studentů v raných fázích jejich studia, ponechat jim zhruba rok na aklimatizaci a osvědčení svých schopností a teprve poté je zařazujeme na zodpovědná místa ve vývojových týmech.

Na obrázku 4.1 je vidět roční průběh růstu počtu řádků v našem úložišti CVS, kde se přechovávají zdrojové kódy veškerého firmwaru a softwaru a také dokumentace. I při vědomí problematičnosti takové statistiky se domníváme, že tento graf poskytuje jistou představu o rozsahu vývojových prací v rámci aktivity.



Obrázek 4.1: Graf růstu počtu řádků v CVS během roku 2005

Ve vnitřní organizaci týmu došlo v roce 2005 k poměrně významné změně: Zatímco dříve byli spoluřešitelé zařazeni a vedeni především v rámci tématicky orientovaných skupin (VHDL, systémový software, atd.), v polovině roku 2005 jsme zavedli hierarchii řízení založenou primárně na *projektech*. Projektové skupiny zahrnují všechny vývojáře a podpůrné spolupracovníky, kteří se mají podílet na výsledcích daného projektu. Od této změny si slibujeme zkvalitnění řízení, především ve smyslu lepšího plnění stanovených termínů. V běhu je nyní následujících pět projektů:

1. Netflow – vývoj monitorovací sondy Netflow, vedoucím projektu je Martin Žádník (VUT Brno).
2. Liberouter – vývoj směrovače IPv6/IPv4, vedoucím projektu je Jiří Tobola (VUT Brno).
3. SCAMPI – vývoj monitorovacího adaptéru SCAMPI, vedoucím projektu je Tomáš Martínek (VUT Brno).
4. IDS – příprava vývoje zařízení pro monitoring obsahu paketů, vedoucím projektu je Petr Kobierský (VUT Brno).
5. PAGEN – příprava vývoje generátoru paketů, vedoucím projektu je Jan Pazdera (VUT Brno).

Všechny uvedené projekty budou podrobněji popsány v následujících oddílech.

4.1 Nové karty

Rodina karet COMBO se v roce 2005 rozšířila o několik významných přírůstků:

1. Základní karta *COMBO6X* pro sběrnice PCI 64bit/66 MHz a PCI-X. Tato karta byla již otestována a některé drobné nedostatky, které byly při testech odhaleny, jsme promítli do upraveného návrhu karty.
2. Základní karta *COMBO6E* pro sběrnici Express PCI je nyní ve výrobě.
3. Karta rozhraní *COMBO-4SFPRO* je k dispozici ve dvou variantách, s podporou buď pro gigabitový Ethernet nebo SDH STM-16. Karta již byla otestována a je připravena k nasazení.
4. Karta rozhraní *COMBO-2XFPRO* s podporou pro 10gigabitový Ethernet. U této karty jsme narazili na vážné problémy se součástkami (viz níže). Karta v této podobě zřejmě nebude použitelná a pro podporu desetigigabitových rozhraní bude nutno navrhnout zcela novou kartu.

Přínos této nové rodiny karet COMBO je trojí:

- Implementací moderních sběrnic PCI-X a Express PCI s vysokou propustností se otevírají nové možnosti koncipování síťových zařízení s kartami COMBO: Sběrnice ve většině případů přestává být úzkým hrdlem a využití procesoru hostitelského počítače je proto snazší.
- Specializované čipy byly nahrazeny novými funkcemi anebo naprogramovanými moduly přímo v hradlových polích: Místo phyterů jsou pro síťová rozhraní využívány rychlé sériové obvody Rocket IO v hradlových polích Xilinx Virtex-II Pro a dále PCI bridge PLX, jímž byla osazena původní karta COMBO6, byl nahrazen hradlovým polem s komerční implementací příslušného PCI bridge ve formě tzv. *Intellectual Property Core*.
- Hradlová pole řady Virtex-II Pro přímo v sobě obsahují jeden nebo více procesorů PowerPC, které podstatně rozšiřují paletu nástrojů dostupných přímo na kartě. V současné době je pomocí těchto procesorů implementována funkce *Busmaster DMA*.

Desetigigabitový Ethernet byl implementován již na kartách COMBO-2XFP vyvinutých pro projekt SCAMPI. Poté, co byly vyrobeny dva kusy této karty, firma Intel oznámila konec výroby phyterů DS12010, které jsou na kartě použity. U nové generace desetigigabitových karet rozhraní jsme se proto rozhodli místo čipů tohoto typu použít sériové obvody Rocket IO. Podle specifikace výrobce (Xilinx) měly tyto obvody v hradlových polích Virtex-II Pro XC2VP20 (speed grade 7) plně podporovat rozhraní 10GE. Navrhli jsme proto nové karty COMBO-2XFP s těmito hradlovými poli, firma Xilinx však následně podporu 10GE u těchto čipů odvolala bez uvedení bližších podrobností. Rozhodli jsme se proto vývoj karty COMBO-2XFPRO zastavit a navrhnout ji znovu s použitím nového hradlového pole Virtex-4, u něhož by měla být desetigigabitová rozhraní již podporována bez výhrad.

4.2 Sonda Netflow

Projekt vývoje sondy Netflow byl zahájen v roce 2004 v rámci aktivity JRA2 (Bezpečnost) projektu GN2. Cílem je samostatné monitorovací zařízení pro získávání informací o datových tocích IP ve vysokorychlostních sítích.

V říjnu 2005 jsme dokončili a do konce roku úspěšně otestovali prototyp sondy, který je založen na standardním PC s přidaným hardwarovým akcelerátorem pro analýzu datového provozu.

Průmyslovým standardem pro výměnu statistických dat o tocích je protokol Cisco Netflow, jehož nejnovější verze 9 je popsána v informativním RFC 3954.

Data Netflow jsou obvykle generována směrovači. Použití autonomní sondy má proti tomuto tradičnímu uspořádání několik výhod:

- Sonda není v síťové infrastruktuře viditelná na úrovni síťové ani linkové vrstvy. Vzdálené útoky jsou proto prakticky nemožné.
- Hlavním úkolem směrovačů je směrování a předávání datagramů, jiné operace, zejména jsou-li náročné na výpočetní výkon, lze dělat jen ve velmi omezené míře. Samostatné zařízení je v tomto směru mnohem pružnější.
- Speciálním případem předchozího bodu je vzorkování provozu, které je u některých směrovačů povinné. Pro některé aplikace, zejména v oblasti bezpečnosti, je však vzorkování velmi nevhodné.

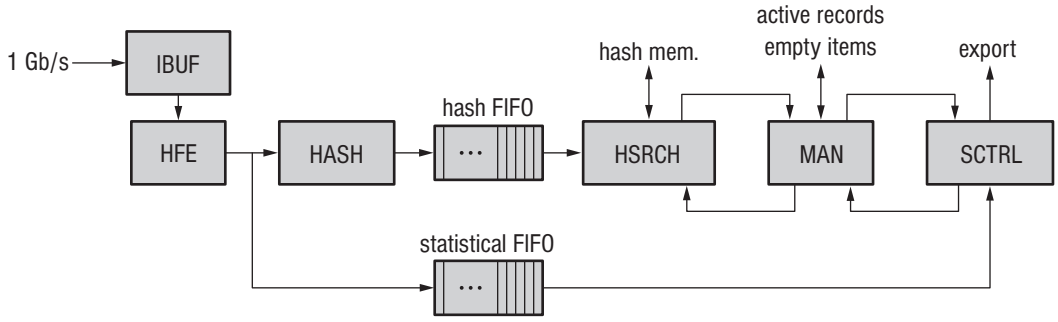
Další technické podrobnosti o sondě lze nalézt v technické zprávě [ŽáL05] a článku [ZPK05].

4.2.1 Hardware

Hardwarový akcelerátor pro sondu Netflow je založen na kombinaci základní karty COMBO6 a dceřiné karty rozhraní pro gigabitový Ethernet, tj. buď COMBO-4MTX (metalické porty) anebo COMBO-4SFP (transceivery SFP). Z hlediska síťové infrastruktury funguje akcelerátor jako opakovač: datový tok přicházející do jednoho z portů je bezprostředně vysílán z jiného portu a kopie těchto dat se předává firmwaru k analýze.

4.2.2 Firmware

Firmware akcelerátoru Netflow v jazyku VHDL je postaven na zcela novém designu. Je schopen současně zpracovávat datový provoz IPv4 i IPv6. Aktuální verze firmwaru je schopna udržovat v paměti informace o 65 536 tocích.



Obrázek 4.2: Blokové schéma firmwaru sondy Netflow

Obrázek 4.2 znázorňuje blokové schéma firmwaru. Pakety přijaté vstupní vyrovnávací pamětí (Input Buffer, IBUF) jsou postoupeny analyzátoru hlaviček (Header Field Extractor, HFE). Tato jednotka analyzuje hlavičky 2., 3. a 4. vrstvy, extrahuje z nich všechna potřebná pole a uloží je do pevné datové struktury nazývané unifikovaná hlavička (UH), jež se uloží do statistické fronty (statistical FIFO). Paralelně s tím jsou určitá *klíčová pole* UH použita jako vstup rozptylovací funkce CRC-64, která je implementována jednotkou HASH. Z výsledných 64 bitů funkce CRC-64 používáme 57 bitů jako unikátní identifikátor toku. Klíčových polí je obvykle pět: zdrojová a cílová adresa IP, čísla zdrojového a cílového portu a číslo protokolu třetí vrstvy. Firmware lze konfigurovat tak, že se libovolná podmnožina bitů těchto pěti klíčových polí zamaskuje a jako vstup rozptylovací funkce se použijí pouze zbylé bity.

Použití hodnoty rozptylovací funkce jakožto identifikátoru toku znamená, že pakety s rozdílnými hodnotami klíčových polí mohou občas dostat stejný identifikátor a tudíž mohou být nesprávně zařazeny do téhož toku. Vzhledem ke statisticky rovnoměrnému rozdělení hodnot funkce CRC-64 je pravděpodobnost *nedetekované* kolize $N \times 2^{-57}$, kde N je skutečný počet toků v paměti. Paměť však nemůže nikdy zároveň obsahovat více než 2^{16} toků, a proto je pravděpodobnost nedetekované kolize nejvýše 2^{-41}, tedy asi $4{,}55 \times 10^{-13}$. Při současné maximální propustnosti firmwaru – půl milionu paketů za vteřinu – to znamená v průměru nejvýše 7 kolizí za rok. I když je tato pravděpodobnost pro většinu aplikací dostatečně nízká, je nutné počítat i s cíleným útokem na rozptylovací funkci: Útočník může napřed podvrhnout vhodně připravený tok a pak spustit vlastní útok, který však bude nesprávně klasifikován jako první (podvržený) tok. Tento scénář není příliš obtížné zrealizovat, neboť rozptylovací funkce je známa. Tomuto nebezpečí se čelí tím, že je jednotka HASH inicializována náhodným číslem, takže její výsledné hodnoty nejsou predikovatelné.

Identifikátory toku jsou ukládány do fronty Hash FIFO, odkud je po jednom vybírá vyhledávací jednotka (Hash Search Unit, HSRCH) a zjišťuje, zda je tento identifikátor již v paměti přítomen. Je-li tomu tak, upraví se statistika příslušného existujícího toku, v opačném případě se v paměti založí nová položka.

Řídící jednotka (Manager Unit, MAN) spravuje seznamy identifikátorů toků a též udržuje seznam volných paměťových míst. Záznamy o tocích jsou uspořádány v obousměrném seznamu setříděném podle časové značky poslední změny záznamu. Neaktivní toky lze pak snadno rozpoznat, jakmile jejich stáří překročí stanovenou hranici (tzv. neaktivní časovač).

Konečně, úložná jednotka (Storage Unit, SCTRL) shromažďuje statistiky o aktivních tocích a exportuje záznamy podle instrukcí obdržených od jednotky MAN.

Aktuální verze firmwaru podporuje též experimentální vzorkovací proceduru nazývanou *sample-and-hold*. Od běžného statistického vzorkování, které je rov-

něž implementováno, se liší tím, že vzorkování vstupních paketů je potlačeno u všech toků, které již existují v paměti. Tímto postupem lze získat velmi přesné informace o velkých tocích.

Činnost firmwaru závisí na hodnotách několika numerických parametrů, které lze měnit i za běhu:

- vypršení aktivních toků (active timeout) v rozmezí 0–1200 sekund
- vypršení neaktivních toků (inactive timeout) v rozmezí 0–60 sekund
- vzorkovací frekvence v rozmezí 1–65 536
- vzorkovací frekvence pro sample-and-hold v rozmezí 1–65 536
- práh pro sample-and-hold – vzorkování nezačne dříve než počet toků v paměti dosáhne této hodnoty

4.2.3 Softwarový ovladač akcelerátoru

Ovladač hardwarového akcelerátoru Netflow je k dispozici pro Linux 2.4 a 2.6. Umožňuje současný přístup několika aplikací k záznamům o tocích: Vyhrazený blok sdílené paměti se používá pro uložení až 16 384 záznamů v logické struktuře kruhové vyrovnávací paměti. Jakmile se kruh zaplní, jsou nejstarší záznamy přepisovány novými. Každá aplikace si přitom udržuje vlastní ukazatel do této vyrovnávací paměti a navíc může uzamknout až 1024 položek – pokud například není hotova s jejich čtením – a zabrání tak jejich přepsání.

Aplikace mohou k ovladači přistupovat výhradně prostřednictvím speciální nízkoúrovňové knihovny *libcsflow*. Tato knihovna implementuje některé společné funkce a kromě toho také umožňuje testovat aplikace bez přístupu k hardwarovému akcelerátoru – záznamy o tocích se v tomto případě načtou z diskového souboru.

4.2.4 Program pro export dat Netflow verze 9

První aplikací, která používá sondu Netflow, je exportér toků podporující formát Netflow verze 9. Prozatím umožňuje posílat data jedinému kolektoru prostřednictvím transportu IPv4/UDP. IP adresu a cílový port kolektoru lze nastavit z příkazového řádku.

Formát Netflow v9 je pružný v tom, že umožňuje prakticky libovolně stanovit obsah odesílaných záznamů o tocích. Použitá uspořádání dat jsou kolektoru sdělena pomocí takzvaných předloh (templates). Náš exportér zatím podporuje šest předloh pro všechny možné kombinace IPv4 a IPv6 na jedné straně a

transportních protokolů TCP, UDP a ICMP na straně druhé. Další dvě předlohy (IPv4/OTHER a IPv6/OTHER) jsou používány pro ostatní protokoly třetí vrstvy.

Všechny předlohy sdílejí následujících sedm datových polí:

- FIRST_SWITCHED – časová značka prvního datagramu v toku
- LAST_SWITCHED – časová značka posledního datagramu v toku
- OUT_PKTS – počet datagramů patřících toku
- OUT_BYTES – počet oktetů patřících toku
- IPV4_SRC_ADDR a IPv6_SRC_ADDR – zdrojová IP adresa
- IPV4_DST_ADDR a IPv6_DST_ADDR – cílová IP adresa
- PROTOCOL – protokol třetí vrstvy

Další datová pole jsou již specifická pro jednotlivé předlohy. Jejich výskyt ukazuje tabulka 4.1.

Pole	TCP	UDP	ICMP	Popis
L4_SRC_PORT	X	X		zdrojový port
L4_DST_PORT	X	X		cílový port
DST_TOS	X	X		oktet typu služby
TCP_FLAGS	X			příznaky TCP (TCP flags)
ICMP_FLAGS			X	příznaky ICMP (ICMP flags)

Tabulka 4.1: Datová pole v protokolově specifických předlohách

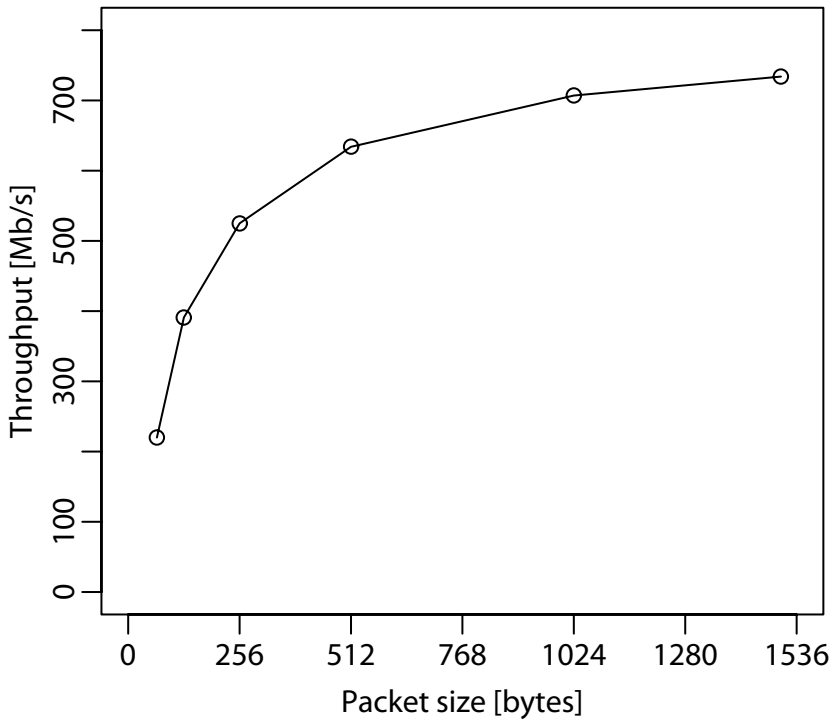
Bez znalosti příslušné předlohy nemůže kolektor data interpretovat, a proto je důležité všechny používané předlohy občas posílat. Prostřednictvím řádkového parametru je možné nastavit periodu jejich posílání.

4.2.5 Testy prototypu

V listopadu a prosinci 2005 jsme realizovali první úspěšné testy sondy, a to jak v laboratorním prostředí, tak i v produkční síti. Další nezávislé testy jsou připravovány ve spolupráci s našimi partnery v projektu GN2, jimž CESNET zapůjčil nebo zapůjčí prototypy sondy. Jeden z nich je již instalován v Utrechtu (Nizozemsko) a testován kolegy ze SURFnetu. Testování zatím obecně naráží na neexistující nebo chabou podporu Netflow v9 v kolektorech.

Propustnost firmwaru jsme testovali pomocí síťového analyzátoru Spirent AX/4000. Výsledky jsou graficky znázorněny v obrázku 4.3, z něhož je vidět, že propustnost současné verze designu je limitována dvěma faktory:

- Firmware běží s frekvencí hodin 50 Mhz, což při datové cestě o šířce 16 bitů znamená, že maximální (teoretická) propustnost je 800 Mb/s. Tento faktor omezuje křivku propustnosti pro velké pakety (pravý horní roh v obrázku 4.3.)



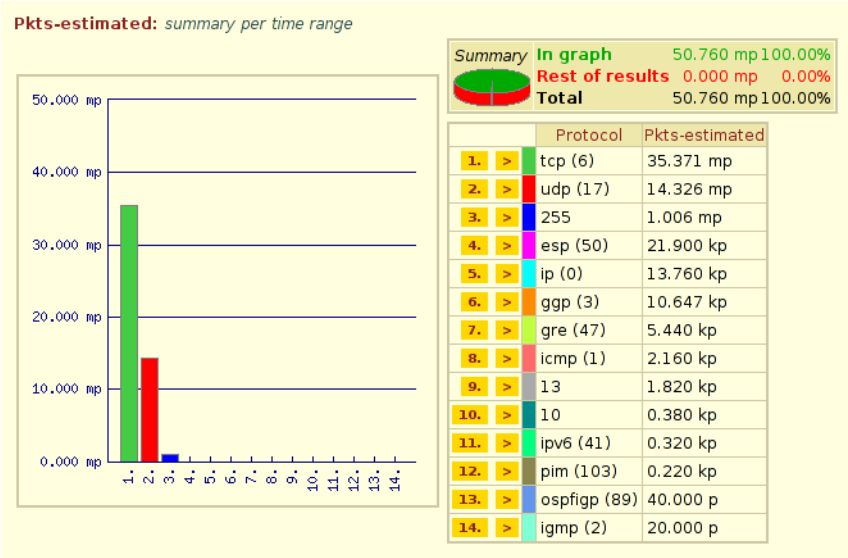
Obrázek 4.3: Propustnost sondy Netflow pro různé velikosti paketů

- Analyzátor hlaviček HFE je schopen zpracovat zhruba 500 tisíc paketů za vteřinu, čímž je omezena zejména propustnost malých paketů v levém dolním rohu křivky.

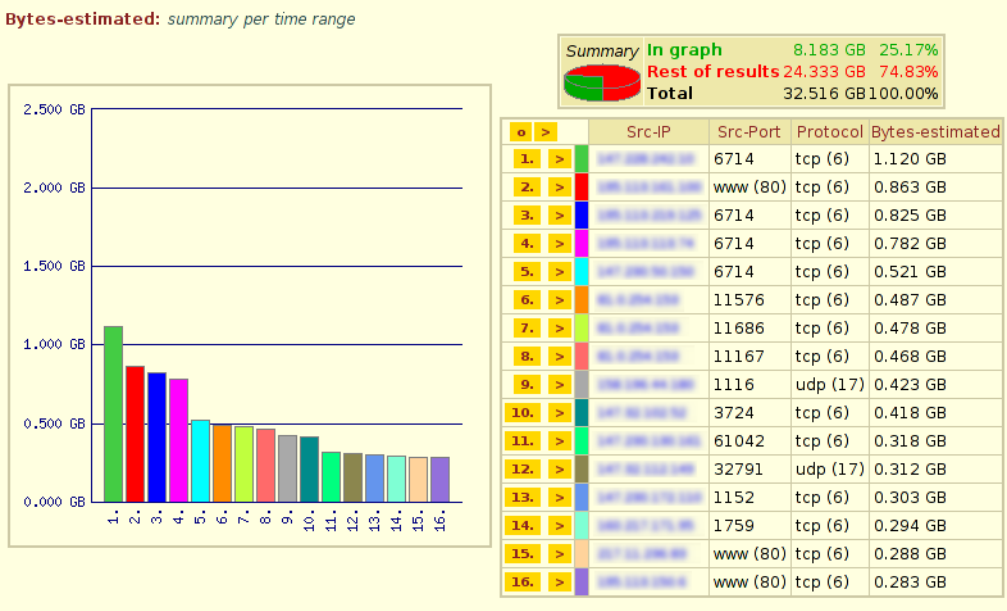
Na odstranění obou omezení v současné době pracujeme: Nová základní karta COMBO6X umožní zvýšit hodinovou frekvenci na 100 MHz a tím hrubou propustnost na 1,6 Gb/s. Ve fázi testů je též optimalizovaná implementace HFE, která by měla být schopna zpracovat minimálně 2 milióny paketů za vteřinu. Po těchto vylepšeních by měl být firmware sondy schopen zpracovat plnou rychlost 1 Gb/s bez ohledu na velikost paketu.

Sondu jsme rovněž testovali s reálnými daty z páteřní sítě CESNET2. Připojili jsme ji na port přístupového směrovače v brněnském uzlu, do něhož byl zrcadlen veškerý provoz přicházející do metropolitní sítě BAPS. Data generovaná sondou byla zpracovávána systémem FTAS (viz kapitolu 5.2). Následující obrázky ukazují vybraný vzorek výsledků[1]. Z nich je zřejmé, že data poskytovaná sondou jsou kvalitativně správná, neboť se shodují s nezávislými pozorováními. Pro přesnější kvalitativní srovnání ještě připravíme test, který porovná výsledky poskytované sondou s těmi, které získáme ze sousedícího směrovače.

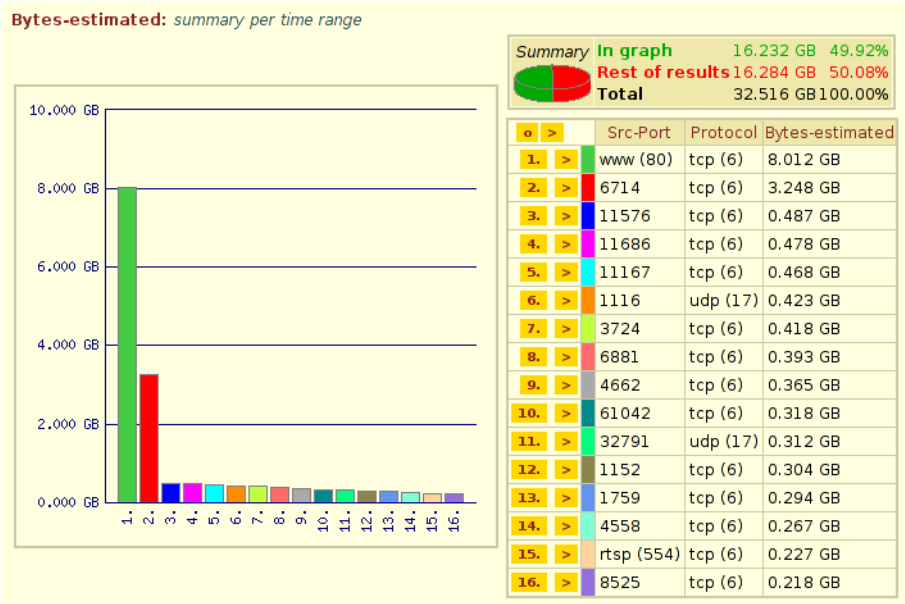
[1] Z důvodu ochrany citlivých dat jsou všechny IP adresy rozmazány.



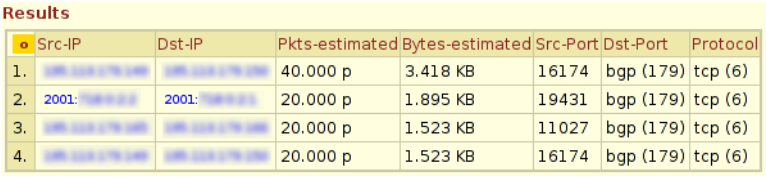
Obrázek 4.4: Spektrum protokolů transportní vrstvy



Obrázek 4.5: Nejvýznamnější datové zdroje a služby



Obrázek 4.6: Složení provozu podle jednotlivých služeb



Obrázek 4.7: Viditelné relace BGP nad IPv4 i IPv6

4.2.6 Výhled do budoucnosti

Sonda Netflow spolu s programy FTAS a Netflow Monitor, vyvíjenými rovněž sdružením CESNET v rámci výzkumného záměru, poskytuje již v současné době vcelku komplexní a použitelné zařízení, které může být užitečné pro řadu aplikací nejen v oblasti bezpečnostní analýzy provozu, ale též sledování kvality služby, účtování přenesených dat či plánování kapacity sítě.

Plány pro nejbližší období (do konce února 2006) zahrnují především rozšíření a zpřehlednění softwaru. Počítáme s implementací následujících nových funkcí:

- Export ve formátu Netflow v5
- Posílání dat většímu počtu kolektorů zároveň
- Filtrace záznamů: každý kolektor by pak měl dostávat jen ta data, která má právo či potřebu vidět.

Základním prostředkem konfigurace sondy by se mělo stát textové uživatelské rozhraní systému Netopeer, viz oddíl 4.3.2.

Během prvního pololetí 2006 plánujeme dokončení nové verze sondy založené na základní kartě COMBO6X a kartě rozhraní COMBO-4SFPRO. Tato verze bude mít propustnost 1,6 GBit/s a kromě gigabitového Ethernetu bude podporovat i rozhraní SDH STM-16. Nové karty budou mít také větší kapacitu paměti SSRAM, což umožní zvýšit počet současně uchovávaných toků na 512 tisíc.

V delší časové perspektivě sledujeme především výzkumně orientované směry, jako je implementace protokolu IPFIX (RFC 3917) anebo různé strategie vzorkování.

4.3 Směrovač Liberouter

Cílem projektu *Liberouter* je vyvinout multigigabitový směrovač pro IPv6 a IPv4 založený na platformě PC a přídavné akcelerační kartě COMBO6, která umožňuje rozložit zátěž při směrování mezi hardware a software podle myšlenky hardwarově-softwarového kodesignu. S využitím tohoto přístupu je možné odstranit hlavní nevýhodu čistě softwarových směrovačů, kterou je nedostatečná propustnost pro dnešní vysokorychlostní linky. Projekt byl také financován z projektu 6NET, jenž byl součástí 5. rámcového programu EU.

Na počátku roku 2005 jsme při průběžném hodnocení projektu 6NET úspěšně prezentovali první funkční prototyp Liberouteru, kterým byla síťová karta s hardwarovou filtrací paketů. Architektura tohoto prototypu je popsána v loňské zprávě. V roce 2005 se pak vývoj směrovače rozdělil do dvou vývojových větví, kterými jsou vývoj síťové karty s hardwarovou filtrací a hardwarovým přeposíláním paketů (projekt NIFIC) a vývoj původně navrženého směrovače Liberouter. Pro obě vývojové větve je dnes vytvořena dokumentace ve formátu XML, jež je k dispozici na stránkách projektu *www.liberouter.org*.

4.3.1 Projekt NIFIC

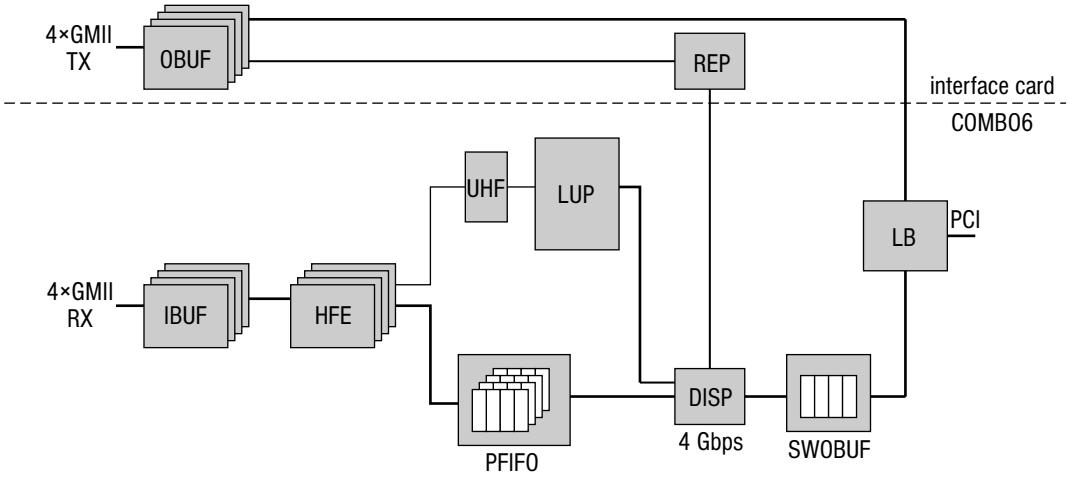
Firmware

V první polovině roku jsme soustředili vývoj na dokončení projektu NIFIC, který navazuje na první prototyp Liberouteru a dále rozšiřuje jeho schopnosti o hardwarové přeposílání a replikaci paketů. Toho lze využít například k filtrování síťového toku ve vysokých rychlostech, protože paket je zpracováván pouze v hardwaru a není nutné jej dále softwarově zpracovávat. Dalším možným využitím je například posílání potenciálně nebezpečných toků do honeypotů nebo jakékoliv jiné rozdělení toků na základě informací z hlaviček paketů. Vý-

hodou tohoto zařízení je jeho možná „neviditelnost“ v síťové vrstvě, ale zároveň schopnost provádět klasifikaci na základě informací z této a vyšších vrstev.

Proti prvnímu prototypu se změnila zejména hardwarová architektura výstupní části zařízení – viz obrázek 4.8. Po přijetí vstupním rozhraním (IBUF) je paket zpracován procesorem HFE (Header Field Extractor), který uloží data paketu do fronty paketů (PFIFO) a informace z hlaviček potřebné pro klasifikaci do fronty unifikovaných hlaviček (UH FIFO). Tyto informace jsou dále zpracovány ve vyhledávacím procesoru (LUP), jehož výstupem je informace určující další zpracování paketu, které je následně provedeno v jednotce DISP (Dispatcher). Možnosti zpracování jsou:

- Filtrace – paket je zahozen.
- Zaslání do softwaru – paket je přes vyrovnávací jednotku (SWOBUF) odeslán do softwaru, kde je zpracován ovladačem COMBO karty. Náležitě upravený pak může být odeslán výstupní jednotkou (OBUF) na síťové rozhraní.
- Přímé přeposlání na výstup – paket je odeslán do replikátoru (REP), kde na základě řídící informace může být zreplikován na více výstupních rozhraní, odkud je přímo, aniž by byl zpracován v softwaru, odeslán do sítě.



Obrázek 4.8: Schéma firmware projektu NIFIC

Firmware projektu NIFIC je v současnosti k dispozici na kartách COMBO6, COMBO-4MTX a COMBO-4SFP. Přestože složitost firmwaru je menší, než je tomu

u původní koncepce směrovače Liberouter, už nyní je využití zejména hradlového pole na kartě COMBO6 na velmi vysoké úrovni, a proto byla implementace kompletního směrovače přesunuta na novou platformu karet COMBO6X a COMBO6E.

Software

Softwarová část projektu NIFIC je do značné míry společná s projektem Liberouter, zejména pak filtrování paketů pomocí klasifikačního procesoru, kde pokračuje hledání nejvhodnějšího způsobu rozdělení filtrovacích pravidel do struktur asociativní a statické paměti – viz technická zpráva [Ant05]. Specifickou částí pouze pro tento projekt jsou ovladače poskytující přístup k síťovým rozhraním COMBO6. Tyto ovladače jsou dostupné pro operační systémy Linux a NetBSD. V souvislosti s přechodem na novou generaci karet COMBO6 intenzivně pracujeme na verzi ovladače, využívajícího k řízení systémové sběrnice procesor PowerPC, který je přímo integrován v programovatelném hradlovém poli. Tím bude sníženo zatížení procesoru počítače a bude možné dosáhnout vyšších propustností při přenosech po sběrnici.

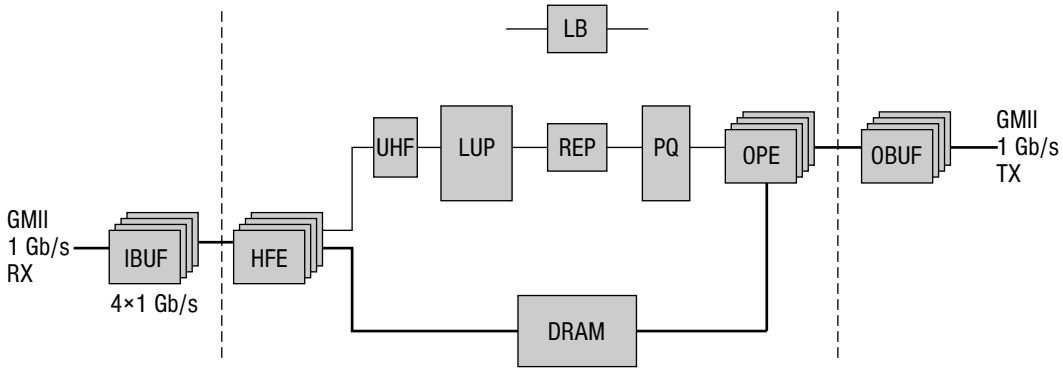
V souvislosti s distribucí karet COMBO6 externím zájemcům vznikl systém pro přípravu balíčků, obsahujících všechny soubory příslušející k danému projektu. Cílem tohoto systému je zjednodušit instalaci softwaru a konfiguraci hardwaru jak pro externí zájemce, tak pro testovací skupinu. Výsledné balíčky, které obsahují zdrojové soubory softwaru a konfigurační soubory pro hradlová pole, jsou zveřejněny na stránkách projektu. Systém balíčků se v projektu NIFIC osvědčil, proto jej využíváme i pro další řešené projekty (Netflow, NIC).

4.3.2 Projekt Liberouter

Firmware

Souběžně s dokončováním projektu NIFIC část VHDL vývojářů intenzivně pracovala na komponentách nutných pro další posun ve vývoji původního směrovače Liberouter a ke konci roku pak byly všechny tyto komponenty integrovány do jednoho celku. Přestože některé z komponent ještě nejsou plně funkční, v softwarových simulacích už Liberouter přesměroval svůj první paket. V příštím roce hodláme soustředit vývoj na rozšiřování funkcí kritických komponent a přechod ze simulací k hardwarové implementaci na nových kartách COMBO6X a COMBO6E.

Architektura firmwaru směrovače Liberouter je znázorněna na obrázku 4.9. Vstupní část odpovídá architektuře projektu NIFIC, novými komponentami pak jsou:



Obrázek 4.9: Schéma firmware projektu Liberouter

REP (Replicator): Jednotka pro hardwarovou implementaci multicastu. Jejím úkolem je replikace záznamů o paketech a přiřazování těchto záznamů do prioritních front.

PQ (Priority Queues): Systém prioritních front pro každé výstupní rozhraní. Umožňuje realizaci QoS.

OPE (Output Packet Editor): Výstupní paketový editor modifikující data paketu před jejich odesláním ze směrovače (změna L2, L3 adresy, zmenšení TTL atd.).

DRAM (SDRAM Scheduler + SDRAM Controller) : Plánovač přístupu k dynamické paměti umožňující práci s touto pamětí více jednotkám zároveň (HFE, REP, OPE) a řadič dynamické paměti zajišťující přístup do DDR SDRAM paměti.

V současné době jsou z nových komponent plně implementovány jednotky Replicator a DRAM scheduler. U ostatních jednotek jsme implementace rozdělili do dvou fází. První verze těchto komponent s omezenými funkcemi již jsou dostupné (OPE, PQ, SDRAM_CTRL) a umožní testování Liberouteru v hardwaru. V příštím roce pak budou tyto jednotky implementovány v plné verzi bez omezení funkcí. Současně s implementací nových jednotek probíhá přepracování výkonově kritických jednotek na vstupu (HFE, LUP) tak, aby bylo dosaženo vyšší propustnosti, lepšího využití prostředků hradlového pole a větší obecnosti těchto jednotek (úprava a rozšíření instrukční sady).

Software

Softwarová podpora pro akceleraci paketů sestává z démona *combod*. Operační systém udržuje směrovací tabulky, ARP tabulky pro překlad L3 adres na L2

a nastavení paketového filtru. Tyto zdroje je nutno zkombinovat do jedné vyhledávací struktury pro LUP. Dokončili jsme metodu kombinace směrování a ARP do jedné vyhledávací struktury (routing-ARP tabulky) a formální model této metody. Přidání paketového filtru je založeno na vložení filtrů reprezentovaných intervalovými rozhodovacími diagramy do relevantních částí adresového prostoru směrovací tabulky. Tento postup jsme implementovali v prototypu. Vyvíjíme formální model metody a pracujeme na stanovení kvantitativních charakteristik chování výsledné struktury. Průběžné výsledky této práce jsou shrnuty ve výše zmíněné technické zprávě [Ant05].

Mimo práce na akceleračním démonovi jsme dále doplnili sadu řídících nástrojů pro hardwarové komponenty. Cílem je vytvořit kompletní sadu těchto nástrojů s jednotným rozhraním pro nastavení a testování všech komponent firmwaru Liberouteru. Funkce nutné ke směrování paketů poté přesuneme do knihovny *libcombo*, kterou využívá démon *combod* pro řízení nanoprocesorů a uložení aktuálních směrovacích a filtrovacích pravidel na kartu COMBO6.

Formální verifikace

V oblasti formální verifikace jsme se zaměřili na ověření správnosti VHDL designu komponenty TX_BUFFER a generických komponent synchronních a asynchronních front FIFO a FIFO BRAM. Verifikace bloku TX_BUFFER potvrdila správnost příslušných VHDL programů vzhledem k nemožnosti přetečení bufferu. Formulace temporálních vlastností umožnila navíc upřesnění chování některých signálů a upřesnění předpokladů nezbytných ke správné činnosti bloku.

Verifikace parametrizované fronty FIFO BRAM vedla pro více než 5bitový adresní prostor ke kritické stavové expanzi. Správnost fronty byla tedy ověřována zjednodušením designu na 5bitový adresní prostor. Výsledky vedly k nalezení chyb v designu, které byly díky verifikaci lokalizovány a opraveny. Jednalo se o řízení signálu LSTBLK ohlašujícího poslední volný blok fronty. Nové verze designu jsme podrobili verifikaci vzhledem ke stejným vlastnostem, jako původní verze. Možnost znovupoužití formální specifikace byla u komponenty FIFO BRAM využita poprvé, a její výsledky umožnily rychle lokalizovat a odstranit nově zanesené chyby.

Přesné výsledky výše uvedených verifikací, včetně historie verifikací jednotlivých verzí komponent, jsou zveřejněny na stránkách projektu Liberouter v sekci formální verifikace.

Konfigurační systém Netopeer

Součástí projektu Liberouter je také konfigurační systém *Netopeer*, který má umožnit konzistentní konfiguraci směrovačů či jiných síťových zařízení. Pro vnitřní reprezentaci konfigurací používá Netopeer jazyk XML.

V roce 2005 jsme se soustředili na dokončení textového uživatelského rozhraní. Toto rozhraní, založené na knihovně *ncurses*[2], má již v současné době všechny požadované funkce a probíhá jeho testování.

Jako prostředek pro přenos konfigurace do síťového zařízení a hlášení případných chyb v opačném směru jsme zvolili protokol *netconf*, který je vyvíjen v rámci IETF. Software vyvinutý jako součást diplomové práce [Zlo05] je jednou z prvních implementací tohoto protokolu.

Dále pokračoval vývoj metakonfigurační aplikace [Mat05], která umožňuje konfigurovat celé sítě na vyšší úrovni abstrakce a automaticky připravovat konfigurace jednotlivých směrovačů v jazyku Netopeer. Vytvořili jsme též modul pro grafické znázornění sítě ve formátu SVG.

Koncem roku 2005 jsme zahájili práce na přizpůsobení systému Netopeer pro konfiguraci sondy Netflow, viz oddíl 4.2. Na základě specifikace předpokládaných funkcí hardwaru i softwaru sondy jsme vytvořili odpovídající XML schéma a upravili textové rozhraní. Nyní zbývá vytvořit back-end, který konfiguraci v jazyku Netopeer zpracuje a nastaví podle ní sondu Netflow.

4.4 Adaptér SCAMPI

Cílem evropského projektu *SCAMPI* v rámci 5. rámcového programu IST bylo vyvinout adaptér pro monitorování vysokorychlostních sítí s přenosovou kapacitou 10 Gb/s a vyšší. Na těchto rychlostech již není možné monitorovat vstupní datové toky pomocí konvenčních počítačů se síťovým rozhraním (úzké hrdlo tvoří především propustnost sběrnice mezi procesorem a síťovým rozhraním). V rámci vývoje adaptéru SCAMPI byla proto rozdělena funkce monitorovacího systému mezi software (běžící na konvenčním počítači) a specializovaný hardware (v podobě karet rodiny COMBO6), který zpracovává výkonově náročné části s využitím technologie FPGA.

V rámci projektu SCAMPI bylo úlohou našeho týmu především navrhnout a implementovat firmware monitorovacího systému a nízkoúrovňový software pro komunikaci s kartou COMBO6. Pro podporu projektu jsme navíc vyvinuli a oživili specializovanou kartu COMBO-PTM fungující jako zdroj přesných časových značek (použito pro účely statistik).

[2] *http://www.gnu.org/software/ncurses/ncurses.html*

4.4.1 Firmware

Úlohou firmwaru v projektu SCAMPI bylo zajistit příjem paketu ze vstupního rozhraní, přiřadit paketu přesnou časovou značku a dále jej analyzovat a klasifikovat podle požadavků uživatelské aplikace. Dále byly požadovány tyto funkce: možnost sběru statistik, filtrování/vzorkování paketů a detekce specifických posloupností znaků v datovém obsahu paketu.

Na základě požadavků jsme navrhli firmware, který podporuje sběr až 256 různých statistik založených na délce paketu nebo časovém intervalu mezi pakety. K dispozici je též 16 vzorkovacích jednotek, které lze nakonfigurovat pro následující režimy vzorkování:

- deterministické – propustí každý n-tý paket
- pravděpodobnostní – propouští náhodně pakety s předepsanou pravděpodobností
- paket s n-tým bajtem – pro každý n-tý bajt v proudu dat propustí paket, který tento bajt obsahuje

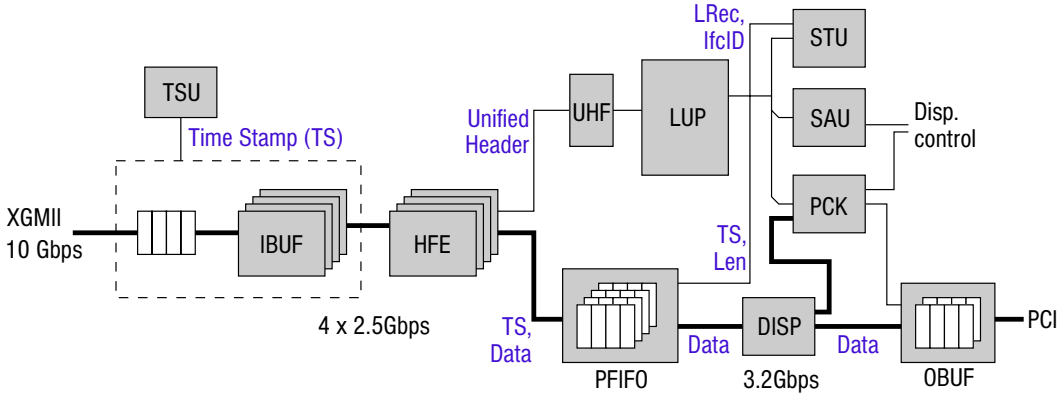
Firmware je díky použité asociativní paměti schopen detekovat až 512 různých vzorků při rychlosti 3,2 Gb/s.

Vývoj firmware jsme rozdělili do dvou fází. V první fázi jsme navrhli a implementovali verzi monitorovacího adaptéru pro rychlost 1 Gb/s. Podrobnější popis této verze je k dispozici v závěrečné zprávě z roku 2004.

Druhá fáze byla zaměřena na vývoj monitorovací adaptéru pro rychlost 10 Gb/s. Z důvodu vysoké propustnosti bylo potřeba rozdělit vstupní datový tok do několika cest, použít zcela jiné vstupní buffery, replikovat některé komponenty (HFE, FIFO) a rozdělit návrh mezi kartu COMBO6 a přídavnou kartu. Oproti designu první fáze, jsme navíc použili nové výkonnější moduly pro výpočet kontrolního součtu, vypracovali obecnější systém komunikačních sběrnic na čipu a implementovali mnoho dalších vylepšení. Architektura monitorovacího adaptéru pro 10 Gb/s je znázorněna na obrázku 4.10.

Činnost adaptéru lze shrnout do následujících bodů

1. Na vstup adaptéru přicházejí data rychlostí 10 Gb/s standardním rozhraním XGMII. Ve vstupním bufferu (IBUF) je ověřen jejich kontrolní součet a celkový datový tok je rozdělen do čtyř menších toků o rychlosti 2,5 Gb/s. Ke každému paketu je navíc připojena přesná časová značka získaná z jednotky přesného času (TSU).



Obrázek 4.10: Architektura monitorovacího adaptéru pro 10 Gb/s

2. Vstupní pakety jsou v dalším kroku analyzovány pomocí čtyř HFE procesorů konstruovaných speciálně pro účely analýzy datový toků na vysokých rychlostech. Výsledkem analýzy je pevná datová struktura (Unified Header, UH) sloužící pro klasifikaci datového toku.

3. V dalším kroku probíhá proces klasifikace, kde jsou jednotlivé pakety rozdělovány do skupin na základě požadavků uživatele systému. Pro akceleraci tohoto procesu jsme použili specializovaný procesor (LUP), využívající rychlé asociativní paměti CAM.

4. Na základě klasifikace paketu jsou v jednotce STU aktualizovány statistické informace založené na délce paketu a jeho časové značce. V závislosti na nastavení systému mohou být dále pakety určených toků vzorkovány jednotkou SAU (pro další analýzu v softwaru). V poslední fázi je možné vybrané datové toky prohledat jednotkou PCK, zda neobsahují výskyt vybraných řetězců.

5. Pakety, které je třeba z určitého důvodu analyzovat v softwaru, jsou odesílány z vyrovnávací paměti (PFIFO) přes Dispatcher do jednotky OBUF, kde čekají na odeslání do paměti počítače po sběrnici PCI.

4.4.2 Systémový software

Systémový software pro projekt SCAMPI se skládá z ovladačů pro komunikaci s kartou COMBO6 a knihovny pro transformaci vstupních konfigurací monitorovacího systému do její reprezentace pro hardwarovou úroveň.

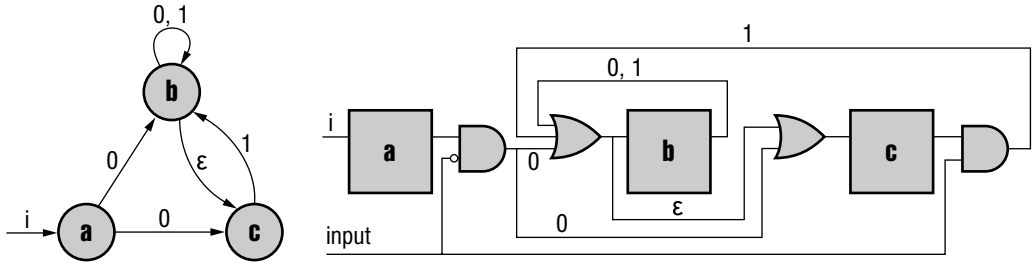
Ovladače poskytují nízkoúrovňový přístup do interních registrů, pamětí a čítačů COMBO6. Architekturu nástrojů pro klasifikaci paketů (původně vyvinutou pro projekt Liberouter) jsme zobecnili a doplnili o podporu pro statistickou (STU), vzorkovací (SAU) a vyhledávací (PCK) jednotku.

Komunikace mezi aplikacemi na uživatelské úrovni a monitorovacím systémem probíhá prostřednictvím aplikačního programového rozhraní MAPI vyvinutého též v rámci projektu SCAMPI. Toto rozhraní pak dále používá námi vyvinutou knihovnu *Scampidump* sloužící ke zpracování a zavedení monitorovacích pravidel do adaptéru. *Scampidump* přijímá pravidla vyjádřená v podmnožině syntaxe Berkeley Packet Filter (BPF). Pravidla jsou analyzována, převedena do formy nanoprogramu pro klasifikační jednotku LUP a nahrána do karty COMBO6.

4.5 Sonda IDS

Úkolem projektu *IDS* je vyvinout zařízení pro detekci nebezpečného síťového provozu (NIDS – Network intrusion detection system). NIDS jsou systémy, které se na základě analýzy hlaviček a vyhledávání vzorů v tělech paketů snaží odhalit potenciální útok, šíření virů nebo případně detekovat, že síť opouštějí důvěrná data. O možném útoku mohou informovat administrátora nebo systém, který může na útok reagovat a zabránit mu již v počáteční fázi. Právě vyhledávání řetězců a regulárních výrazů je kritickou operací, kterou musí NIDS řešit. Stávající softwarová řešeni se sekvenčním zpracováním, např. běžně používaný program *Snort*[3], dosahují v závislosti na výkonu použitého procesoru propustnosti maximálně v řádu stovek Mb/s. Taková propustnost je však pro multigigabitové sítě nedostatečná.

V posledních letech v této oblasti probíhá intenzivní výzkum a vzniklo několik přístupů na bázi FPGA pro rychlé vyhledávání řetězců a regulárních výrazů. Nejlepších výsledků dosahuje přístup na bázi nedeterministických konečných automatů (NFA) [ClS04]. Jeho principem je vytvoření NFA pro všechny vyhledávané řetězce a regulární výrazy. NFA je pak možné převést na ekvivalentní hardwarovou reprezentaci, viz obrázek 4.11. Stavy jsou nahrazeny registry a přechody logickými členy AND a OR.



Obrázek 4.11: Hardwarová reprezentace nedeterministického konečného automatu pro vyhledávání regulárních výrazů

[3] *http://www.snort.org/*

Při použití nedeterministického automatu, který přijímá jeden znak v jednom taktu hodin, je možné dosáhnout při frekvenci 100 Mhz propustnosti až 800 Mb/s. Netriviální transformací NFA na rozšířený automat, který přijímá *k* znaků v jednom hodinovém cyklu, lze propustnost *k*-krát zvýšit a dosáhnout hodnoty jednotek až desítek Gb/s. Limitujícím faktorem pro dosažení propustnosti v řádu desítek Gb/s je velikost čipu. Je proto nutné hledat optimalizace, které umožní umístit celou databázi typu pravidel programu Snort na jeden čip i pro takto vysoké propustnosti.

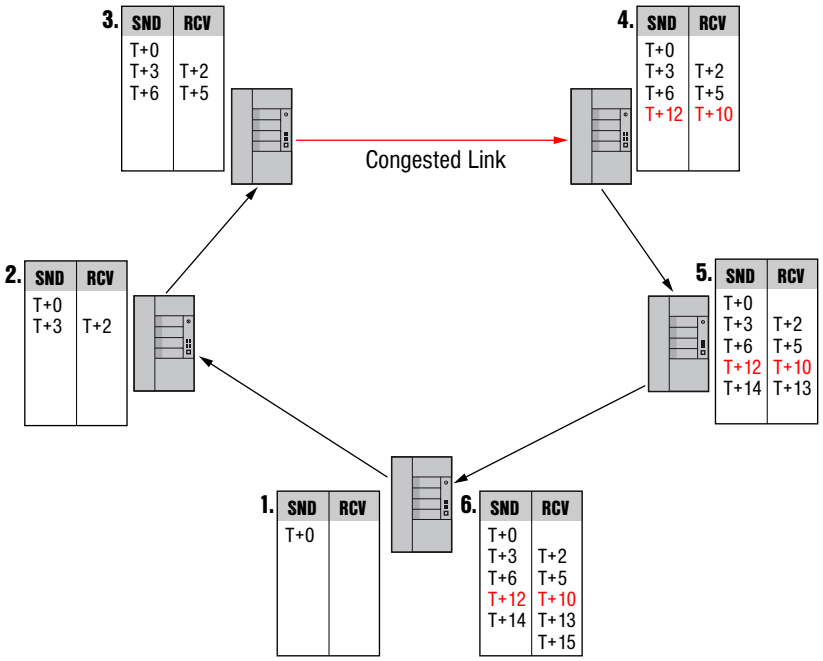
V rámci projektu jsme na základě statistické analýzy databáze pravidel systému Snort identifikovali možné směry dalšího vývoje a výzkumu v této oblasti. Největší důraz bude kladen na optimalizaci hardwarové reprezentace rozšířeného NFA s ohledem na kapacitu čipu, což nám umožní do jednoho čipu vložit větší množinu řetězců a regulárních výrazů a zároveň zvýšit celkovou propustnost systému. V současné době jsme začali pracovat na prvním prototypu NIDS, který bude implementován na nových kartách COMBO6X a COMBO-4SFPRO.

4.6 Paketový generátor

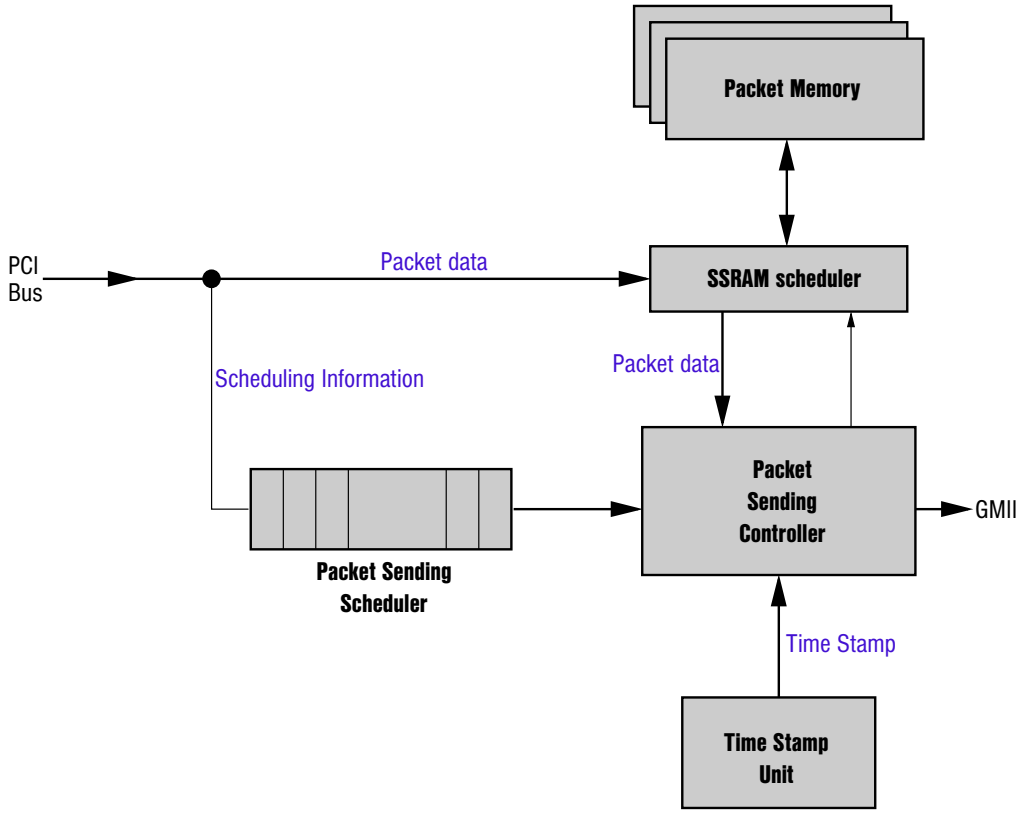
Cílem projektu Paketový generátor (PAGEN) je tvorba výkonného paketového generátoru vybaveného aparátem pro generování přesných časových značek. Navržená architektura je schopna generovat hlavičky a data paketů dle nastavení uživatele a odesílat je s různým časovým rozložením nebo v přesný časový okamžik. Časové značky jsou generovány s přesností 32 ns. Navrhovaná propustnost je 10 Gb/s. Projekt je primárně navržen k implementaci na kartách COMBO6X, resp. COMBO6E vzhledem k vysoké propustnosti sběrnic PCI-X a PCI Express. Druhá část designu zajišťující generování přesných časových značek je implementována na kartě COMBO-PTM.

Architekturu jsme navrhli tak, aby zařízení mohlo mimo jiné sloužit jako analyzátor propustnosti počítačové sítě mezi jednotlivými uzly. Na obrázku 4.12 vidíme několik serverů vybavených paketovým generátorem a umístěných v analyzovaných uzlech. Tyto servery jsou zapojeny do smyčky a pomocí speciálního protokolu mají vzájemně synchronizovaný čas. Vznikne-li na některém uzlu požadavek na analýzu propustnosti, vygeneruje tento uzel speciální paket, k němuž je připojena časová značka značící čas odeslání. Jednotlivé uzly postupně připojují přesné časy, kdy paket obdržely a odeslaly, a svůj jedinečný identifikátor. Po návratu paketu provede odesílající server analýzu připojených značek.

Projekt Paketový generátor je rozdělen do dvou fází. Firmware první fáze je navržen k odesílání ethernetových rámců generovaných softwarem v přesný časový okamžik na základě časové značky, a to s propustností 1 Gb/s. Architektura firmwaru je znázorněna na obrázku 4.13.



Obrázek 4.12: Využití PAGENu jako analyzátoru propustnosti sítě



Obrázek 4.13: Architektura Paketového generátoru (fáze 1)

Zobrazené komponenty mají následující funkce:

Packet Memory (PM): slouží k ukládání rámců generovaných softwarem. Její obsah může být měněn kdykoli za běhu prostřednictvím sběrnice PCI.

Time Stamp Unit (TSU): zajišťuje generování přesných časových značek šířky 64 bitů s přesností až 32 ns. Její hlavní část se nachází na kartě COMBO-PTM, která je vybavena přesným krystalem (2 ppm).

Packet Sending Scheduler (PSS): slouží jako plánovač pro odesílání rámců. Software zde ukládá záznamy, kdy má být který rámec odeslán.

Packet Sending Controller (PSC): zajišťuje odesílání rámců z PM na základě času uloženého v PSS a přesné časové značky generované TSU. PSC provádí generování Preambule, Starting Delimiteru, Ending Delimiteru a FCS.

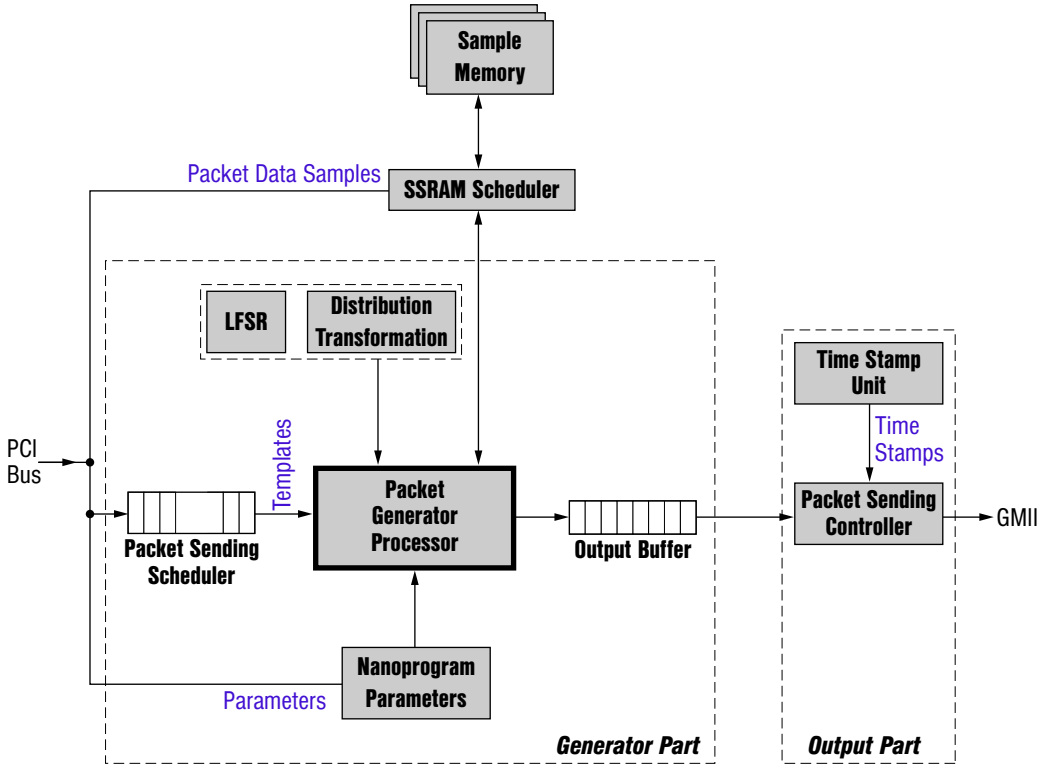
Software první fáze je navržen jako skriptovací jazyk řídící generování dat rámců a jejich ukládání do PM a dále vkládání záznamů do PSS.

Druhá fáze vývoje je zaměřena na plnohodnotný paketový generátor a editor s cílovou propustností 10 Gb/s. Firmware druhé fáze je rozdělen do dvou částí. Část zajišťující generování (Generator Part) bude schopna generovat L2/L3/L4 hlavičky i data rámce na základě uživatelem specifikovaných pravidel (např náhodně generované hodnoty podle daného rozložení, vzorky dat a další). Jako generátor a editor bude použit vysoce výkonný proudový procesor vybavený univerzálním procesorovým jádrem GENA, vyvinutým v rámci aktivity *Programovatelný hardware*. Druhá část (Output Part) zajišťuje odesílaní rámců v intervalech generovaných podle různých rozložení (normální, exponenciální a další). Architektura firmwaru je znázorněna na obrázku 4.14.

Software druhé fáze je rovněž navržen jako skriptovací jazyk, který bude sloužit k popisu pravidel pro generování a odesílání rámců (tzv. šablon). Software na základě skriptu zajistí volbu vhodné množiny nanoprogramů, které budou vykonávány výše zmíněným proudovým procesorem, a vygenerování správných šablon. Jako nadstavbu nad skriptovacím jazykem zvažujeme uživatelsky intuitivní a jednoduchou aplikaci usnadňující uživateli obsluhu paketového generátoru.

Projekt PAGEN ja na samém počátku. V současné době je hotova specifikace[4], dokončena jednotka přesného času (Time Stamp Unit) a navržena architektura proudového procesoru.

[4] *http://www.liberouter.org/~pazdera/pagen.pdf*



Obrázek 4.14: Architektura Paketového generátoru (fáze 2)

5 Sledování infrastruktury a provozu sítě

5.1 Sledování infrastruktury sítě

Primárním cílem v této oblasti je postupný vývoj systému G3 určeného pro souvislé, plošné sledování infrastruktury počítačových sítí.

5.1.1 Měřící modul systému G3

Systém se opírá především o protokol *SNMP (Simple Network Management Protocol)*, který je v této souvislosti využíván jako základní zdroj pro získávání informací z jednotlivých prvků síťové infrastruktury. Použití SNMP je v této oblasti naprosto standardní. Naší snahou je hledat nové cesty k jeho efektivnějšímu využití v oblasti sběru primárních dat, tedy zvyšovat celkovou vypovídací hodnotu získaných a zpracovaných dat a zároveň zachovat nebo lépe snižovat agresivitu (množství generovaných požadavků) vůči poptávaným prvkům síťové infrastruktury. Pokusy v této oblasti vyústily v roce 2004 ve vytvoření základu měřícího modulu systému G3. Tento základní stavební prvek systému byl nasazen ve druhém čtvrtletí roku 2005 do ověřovacího provozu.

Měřící modul jsme v dalším průběhu roku 2005 postupně stabilizovali a zároveň jsme experimentální měření v několika krocích rozšířili na většinu prvků páteřní sítě CESNET2. Tím bylo zajištěno testování systému vůči poměrně širokému spektru zařízení – v souhrnu je měřeno přes 80 síťových prvků s více než 3500 rozhraními. Na základě výsledků a zkušeností s první fází experimentálního provozu se ukázalo jako nezbytné změnit architekturu ukládání dat – z důvodu vysokých nároků na vstupně/výstupní operace. To se týkalo především průběhových numerických veličin, pro které je cílovým úložištěm databáze RRD (Round Robin Database). Základní mechanismus ukládání dat jsme rozšířili o vyrovnávací paměti s dávkovým zápisem do úložiště a strukturu dat jsme začali postupně měnit směrem od individuálního ke skupinovému modelu. Výsledkem je možnost nastavit v okamžiku inicializace systému počet položek, které budou ukládány do jedné datové sady. Přestože je inovovaný měřící modul stále ještě velmi „čerstvou“ záležitostí, je jeho doposud dosažená stabilita dostatečná k zajištění dlouhodobého měření.

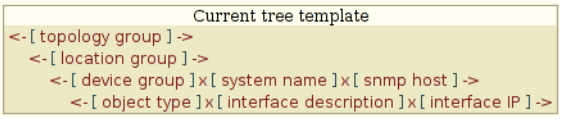
5.1.2 Prototyp základního uživatelského rozhraní systému G3

Vytvoření prototypu uživatelského rozhraní systému G3 bylo hlavním úkolem aktivity pro rok 2005. Naším záměrem bylo promítnout do první verze především klíčové vlastnosti vyplývající z návrhu systému jako celku. Uživatelské rozhraní sestává ze dvou základních komponent – z části *navigační* a z části *vizualizační*. Obě jsou podrobněji popsány v technické zprávě [Koš05].

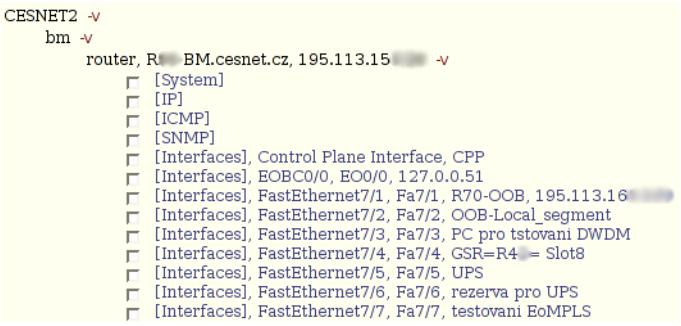
5.1.3 Navigace v uživatelském rozhraní systému G3

Obecně neexistuje způsob navigace, který by beze zbytku vyhovoval všem administrátorům sítí. Ve většině případů však panuje shoda v tom, že navigace formou stromové struktury je rozumným východiskem pro práci s obdobnými systémy. Naším cílem je zajistit především maximální flexibilitu systému, a proto jsme se snažili základní myšlenku rozvést a implementovali funkce, které mají uživatelům umožnit zvolit si a případně i interaktivně nakonfigurovat optimální navigační vlastnosti. Zde jsou stručně popsány některé z nich:

Interaktivně konfigurovatelná předloha (template) pro zobrazení navigační struktury je vlastnost, která umožňuje uživatelům interaktivně měnit obsah i hierarchické uspořádání navigačního stromu.

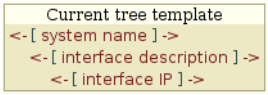


Obrázek 5.1: Předloha – nastavení 1

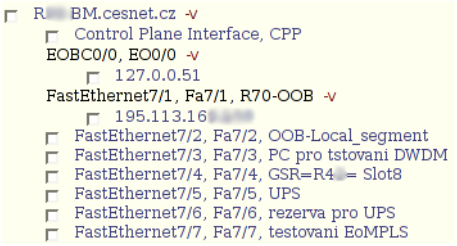


Obrázek 5.2: Navigační struktura podle nastavení 1

Součástí mechanismu vytváření navigačního stromu je zatím **experimentální základní filtr objektů**. Uživatelské rozhraní aktuálně umožňuje zadat i více



Obrázek 5.3: Předloha – nastavení 2

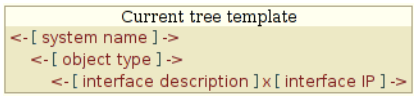


Obrázek 5.4: Navigační struktura podle nastavení 2

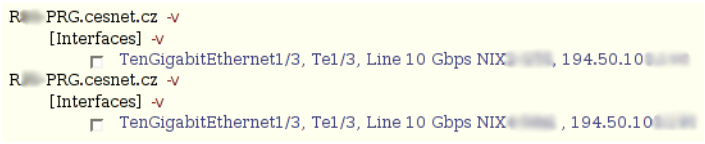
podmínek současně (zatím jednoduchá AND, OR logika) a případně tyto filtrační podmínky svázat s konkrétním typem údaje (popisnou položkou). Podmínky mohou být interpretovány jako hledané podřetězce nebo jako regulární výrazy.

Automatická agregace objektů svázaná s konstrukcí navigačního stromu na základě aktuální předlohy umožňuje odkazovat jedním navigačním návěštím více reálných objektů. Tato vlastnost v souvislosti s komplementární funkcí ve vizualizační části (viz níže) může být efektivní v případě potřeby zobrazit více objektů majících v reálném světě stejný význam jako jeden – např. vícenásobná paralelní propojení. V následující sérii obrázků je naznačeno postupné „slévání“ objektů pod jedno návěští v navigačním stromu. Východiskem pro dosažení požadovaného výsledku bylo v tomto případě zadání odpovídající filtrační podmínky.

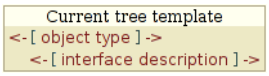
Navigační strom může být zobrazován volitelně buď jako plně „rozbalený“ – obvykle při současném omezení počtu objektů prostřednictvím filtru – nebo jako po částech a interaktivně „rozbalovaný“ a „zavíraný“.



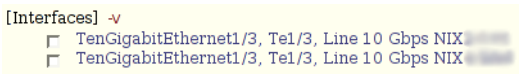
Obrázek 5.5: Výchozí předloha



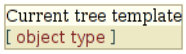
Obrázek 5.6: Odpovídající navigační struktura



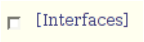
Obrázek 5.7: Předloha v jednom z mezikroků



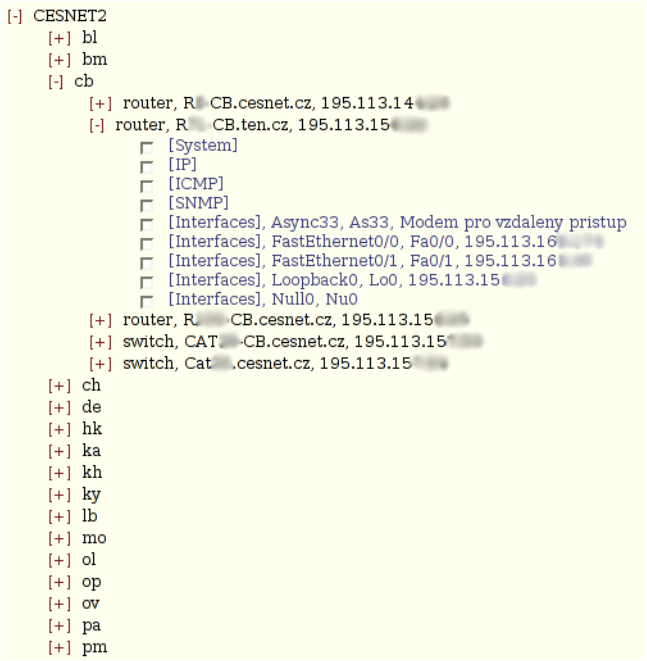
Obrázek 5.8: Odpovídající navigační struktura



Obrázek 5.9: Výsledná předloha

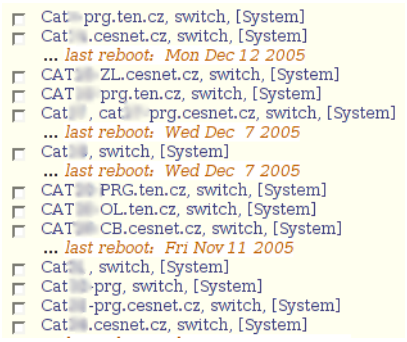


Obrázek 5.10: Odpovídající navigační struktura

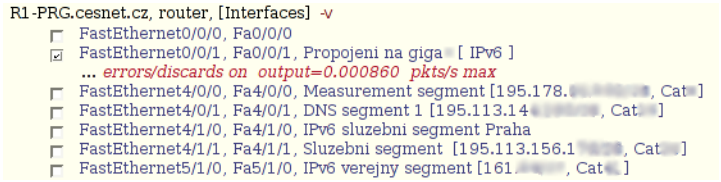


Obrázek 5.11: Ukázka navigačního stromu „rozbalovaného“ po částech

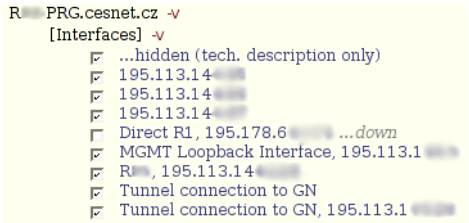
Speciální rozšiřující funkce jsou zamýšleny jako nástroj pro zefektivnění administrace sítě. V principu mají buď zjednodušit orientaci uživatele nebo promítnout do navigačního stromu rozšiřující informace získané výběrem ze všech odpovídajících hodnot naměřených uvnitř uživatelem zadaného časového rámce. Zpravidla se jedná o sumarizaci a/nebo limity položek nesoucí informace např. o chybovosti síťových rozhraní, restartech systémů apod. I v tomto případě se uplatňuje výše zmiňovaná automatická agregace objektů, takže získaná informace může být skutečně souhrnná. Na druhou stranu se jedná o operaci značně náročnou na zdroje, tudíž je žádoucí aplikovat tyto funkce na omezený počet objektů – nejlépe opět pomocí nakonfigurované filtrace.



Obrázek 5.12: Rozšiřující informace o restartu systémů v rámci sledovaného časového intervalu



Obrázek 5.13: Identifikace potenciálně problémových síťových rozhraní

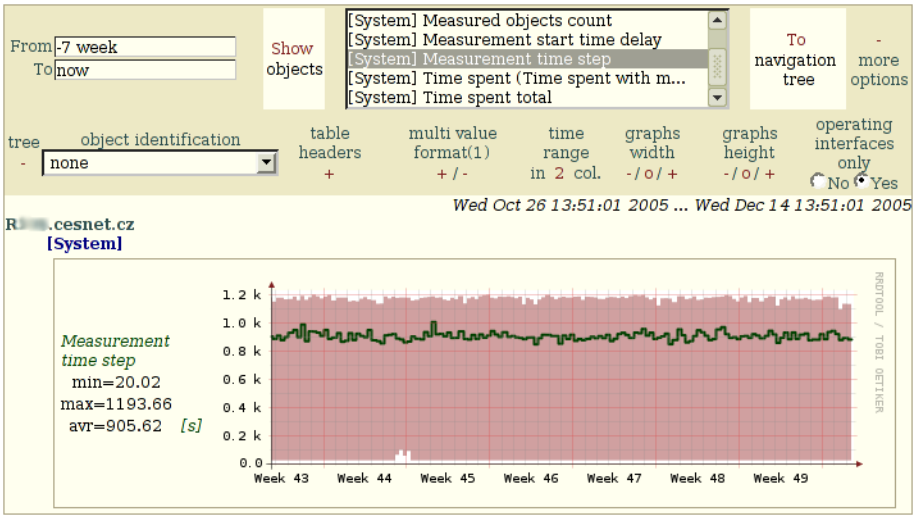


Obrázek 5.14: Usnadnění orientace volitelným potlačením technologických částí popisků rozhraní a identifikace neaktivních rozhraní

5.1.4 Vizualizace naměřených dat v uživatelském rozhraní systému G3

Mechanismus vizualizace naměřených dat koresponduje se snahou o částečné zachycení dynamiky jevů v síťové infrastruktuře a současně navazuje na vlastnosti uvedené v popisu navigačních vlastností.

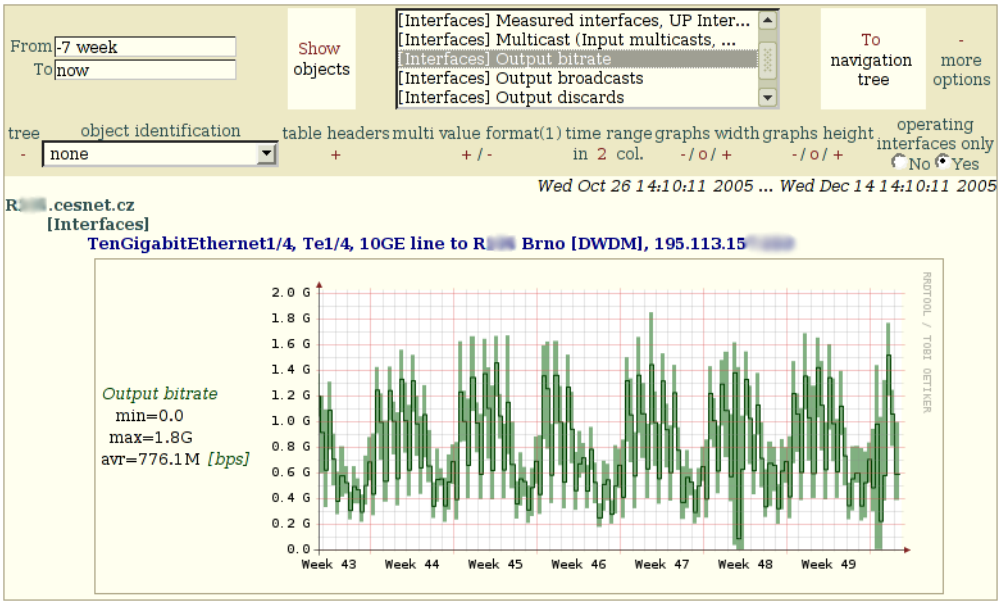
Běžné nástroje systémů pro sledování infrastruktury, které vizualizují průběhy veličin v čase, pracují obvykle s průměrnou hodnotou v rámci jednotkového vizualizačního časového intervalu. Někdy dokonce i v případě, že se jedná o dlouhodobé agregace. V případě systému G3, kdy měření je prováděno s cílem zachytit alespoň základní náznak dynamiky v síti, je nezbytně nutné zobrazovat i rozptyl hodnot od průměru.



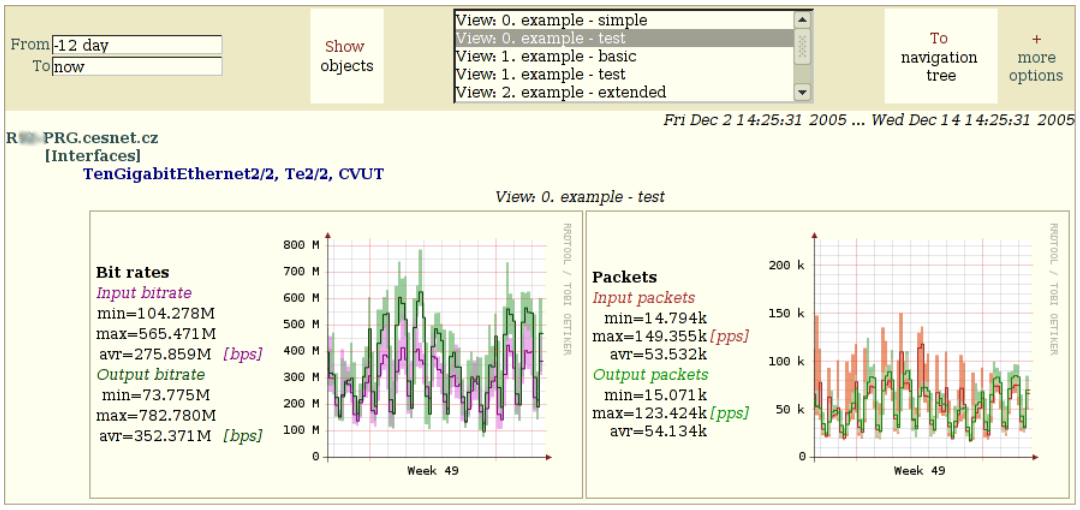
Obrázek 5.15: Ukázka průběhu časového kroku mezi po sobě jdoucími požadavky na data z konkrétního zařízení

Z praxe vyplývá, že je vhodné mít možnost zobrazit do jednoho grafu více průběhových položek. Na druhou stranu dva průběhy tvoří horní hranici pro ještě snesitelnou orientaci při vizualizaci obsahující i obalové křivky. Implementovaný mechanismus pro vizualizaci průběhových hodnot umožňuje snadno změnit resp. přiřadit (mimo uživatelské rozhraní) příslušným měřeným položkám vhodný způsob vizualizace pro daný účel (např. kombinaci jinou položkou).

Pro promítnutí agregačních vlastností navigační části systému je zobrazovací modul vybaven analogickými funkcemi, takže se implicitně předpokládá možnost vytváření průběhů z více než jednoho datového zdroje. Výsledkem jsou agregované průběhy, založené na sumarizaci nebo limitách podle toho, co je pro příslušné veličiny a typ průběhu přirozené.

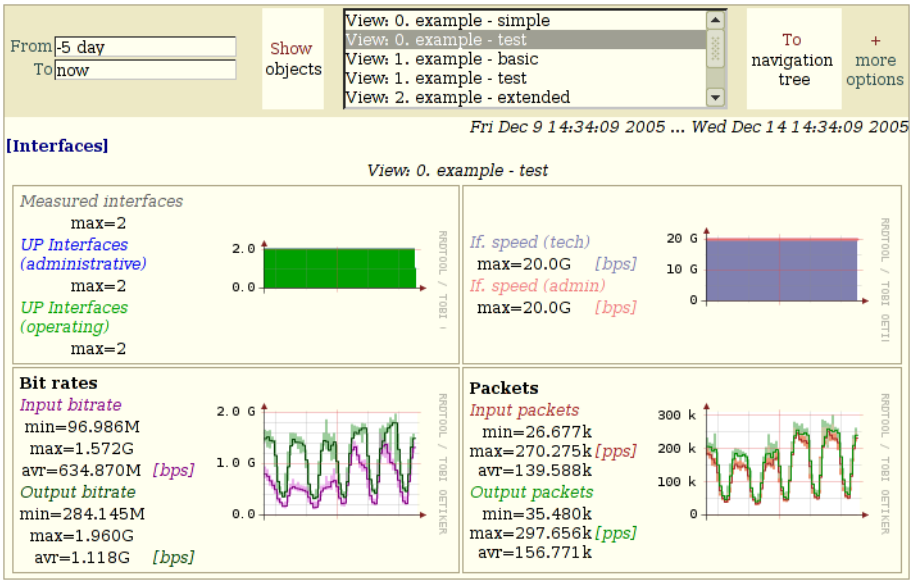


Obrázek 5.16: Jednosměrný tok včetně rozptylu hodnot – sběr dat podle výše zobrazeného časového scénáře

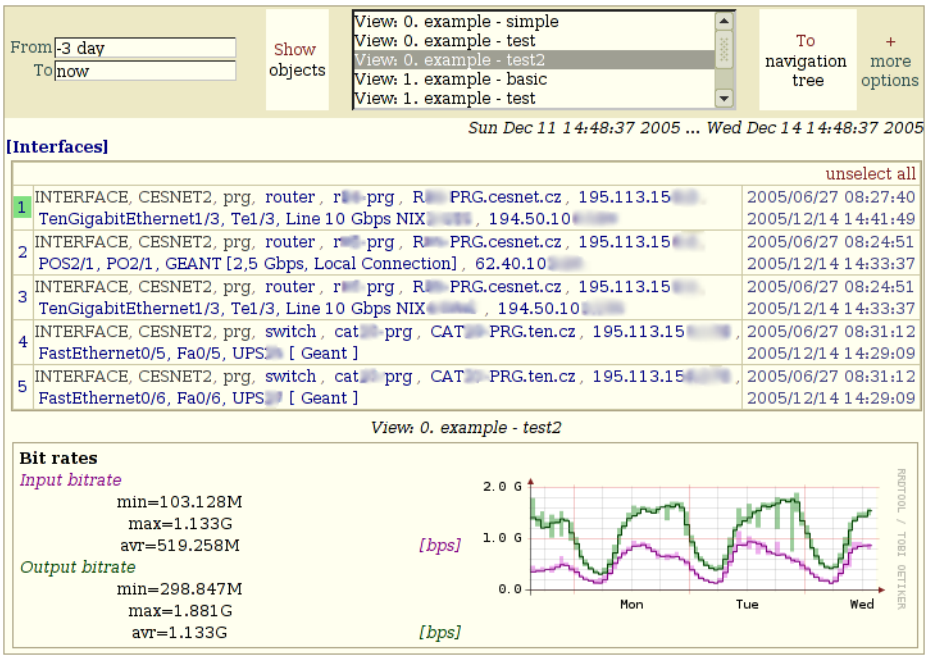


Obrázek 5.17: Ukázka více průběhů v jednom grafu včetně rozptylu hodnot

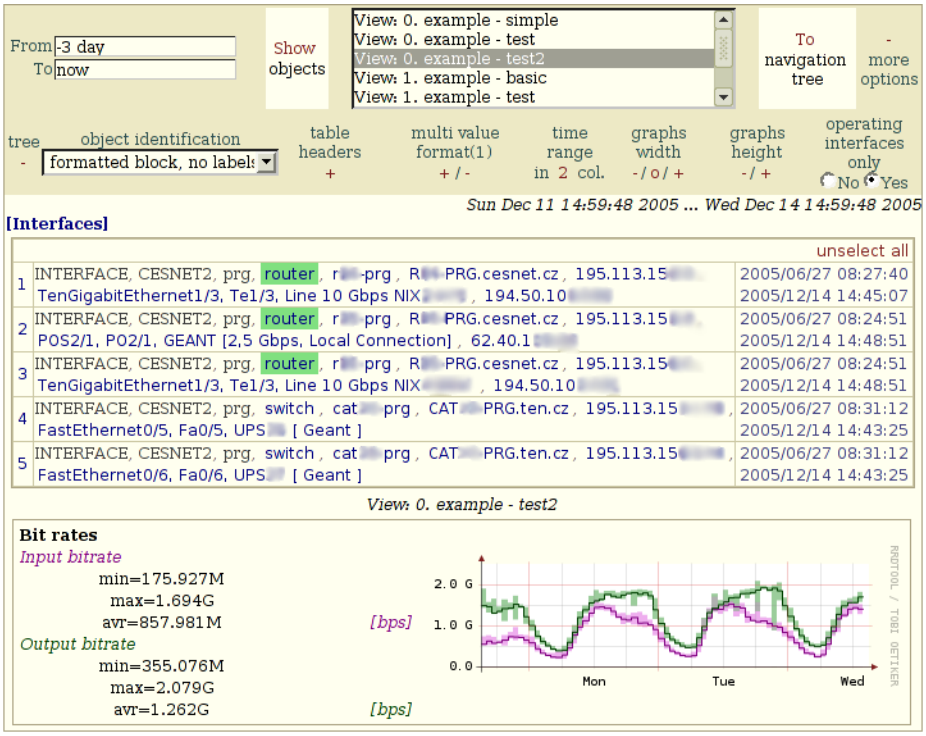
V některých případech může být žádoucí vyčlenit jeden nebo více objektů z množiny všech původně skrytých za příslušným návěštím navigačního stromu. Pro tyto případy jsme implementovali sub-navigační modul, který toto umožňuje. Sekundární výběr je možné provést jak na základě identifikátoru objektu v rámci nakonfigurované předlohy, tak na základě konkrétních hodnot popisných položek objektu.



Obrázek 5.18: Agregovaný průběh toků dvou síťových rozhraní



Obrázek 5.19: Výběr objektu na základě identifikátoru záznamu v sub-navigačním formuláři



Obrázek 5.20: Výběr objektů na základě hodnoty v sub-navigačním formuláři

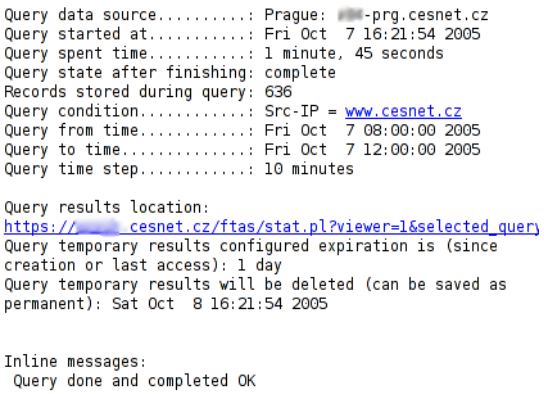
Funkce obsažené v prototypu uživatelského rozhraní systému G3 jsou východiskem pro jeho další vývoj. V aktuální podobě reprezentuje toto uživatelské rozhraní určitý způsob přístupu k problematice a typovou funkčnost. Teprve dlouhodobé praktické testy systému a zpětná vazba od správců sítě ukáže, zda je tento směr vývoje přijatelný a perspektivní.

5.2 Sledování provozu sítě

V roce 2005 jsme prakticky veškeré práce zaměřili na další vývoj experimentálního uživatelského rozhraní systému FTAS.

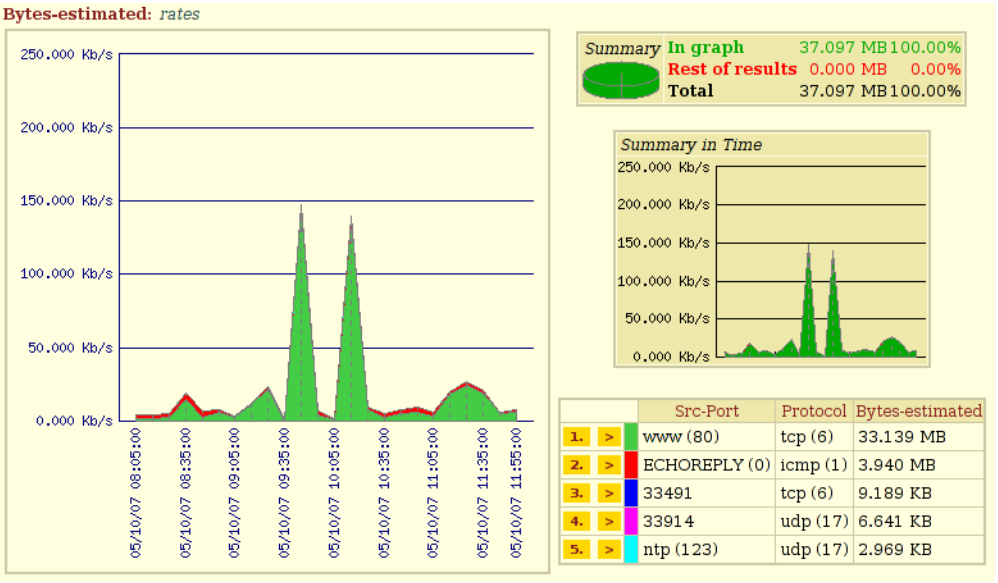
Zkušenosti správců páteřní sítě užívajících tento systém ukázaly, že v případě vyhledávání z primárních dat v rámci relativně dlouhého časového intervalu je čistě interaktivní model chování systému poměrně neefektivní, neboť nutí uživatele k opakované interakci v rámci jednoho vyhledávání. Naprostá většina obdobných požadavků na systém souvisí s útoky nebo pokusy o útoky, takže se jedná o frekventovanou záležitost. Jako řešení tohoto problému jsme umožnili vybavení požadavku na pozadí.

S takto zadaným a zpracovávaným požadavkem souvisí i další rozšíření uživatelského rozhraní – notifikace uživatele o dokončení zpracování požadavku. Na uživatelem zadanou poštovní adresu je odeslána krátká zpráva obsahující stavové informace o zpracovaném požadavku a zároveň lokátor odkazující přímo na výsledky. Případná chyba v zadání adresáta neznamená riziko z hlediska neoprávněného přístupu k systému – přístup k výsledkům podléhá i v této situaci stejnému autorizačnímu mechanismu jako v případě interaktivní práce.

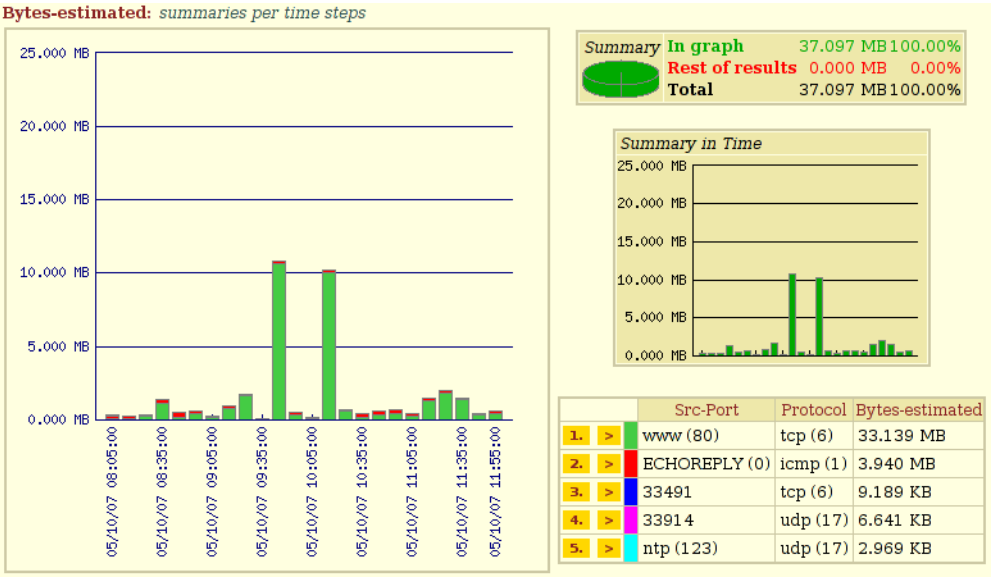


Obrázek 5.21: Ukázka zprávy o dokončeném požadavku na pozadí

Někteří uživatelé požadují při práci se systémem výsledky v podobě sumarizovaných hodnot za jednotlivé agregační časové intervaly v rámci zadaného časového rozsahu. Např. hodinové sumarizace konkrétního provozu během posledních 24 hodin. Původní podoba systému zobrazovala pouze rychlostní veličiny (pakety/s, bity/s) a velikost agregačního intervalu byla generována automaticky systémem. To znamená, že v první fázi bylo nutné umožnit uživatelům zadat velikost agregačního intervalu – tu je nutné specifikovat při zadání požadavku pro vyhledávání. Prozatím jsme zvolili „experimentálně-ověřovací“ variantu – uživatel nevolí z možností, může zadat libovolnou hodnotu s tím, že systém případně tuto hodnotu zkoriguje tak, aby bylo vyhledávání proveditelné. Navazující rozšíření jsme implementovali do zobrazovací části uživatelského rozhraní, kde má uživatel možnost interaktivně přepínat mezi průběhovou a sumarizovanou podobou.



Obrázek 5.22: Ukázka zobrazení – průběhová podoba



Obrázek 5.23: Ukázka zobrazení – sumarizace v rámci agregačního intervalu

6 Sledování a optimalizace výkonnostních charakteristik

Aktivita *Sledování a optimalizace výkonnostních charakteristik* se zabývá teoretickými a praktickými stránkami zajištění vysoké propustnosti a dalších kvalitativních parametrů vyžadovaných aplikacemi při komunikaci přes rozlehlé vysokorychlostní sítě.

Aktivita má svoje WWW stránky[1], kde je možné nalézt naše články, technické zprávy, prezentace, výsledky experimentů a vytvořený software. Shrnutí nejdůležitějších výsledků aktivity dosažených v roce 2005 uvádíme dále.

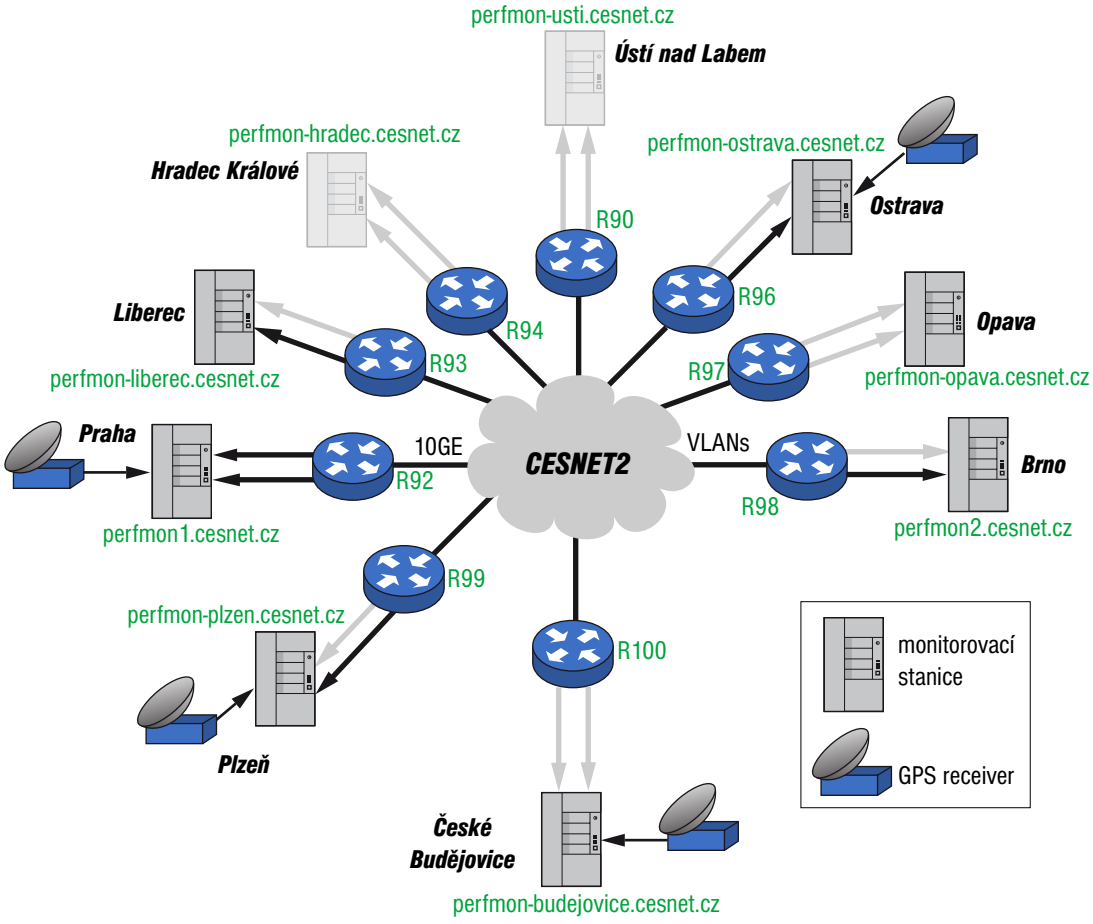
6.1 Monitorování výkonnostních charakteristik sítě CESNET2

Abychom měli přehled o základních výkonnostních charakteristikách sítě CESNET2 rozhodli jsme se instalovat postupně v každém významném uzlu jednu monitorovací stanici. V současné době je instalováno 7 monitorovacích stanic, jak je znázorněno na obrázku 6.1. Instalace dalších 2 stanic znázorněných v šedé barvě bude realizována do konce roku. Každá stanice je vybavena jedním síťovým rozhraním pro konektivitu a aktivní měření a jedním až dvěma dalšími rozhraními připravenými pro pasivní monitorování. Aktivní měření nám umožňuje monitorovat zpoždění, ztrátovost a propustnost. Spouštění jednotlivých měření a zpracování výsledků je řešeno našimi vlastními skripty. V příštím roce plánujeme vývoj aplikací pasivního monitorování a jejich nasazení. Rovněž plánujeme využití systému pro plánování výkonnostních testů *perfSONAR*, který je vyvíjen v rámci aktivity JRA1 projektu GN2 a na jehož vývoji se také podílíme.

6.2 Synchronizace času

Měření některých charakteristik, zejména jednosměrného zpoždění, vyžaduje přesnou časovou synchronizaci mezi monitorovacími stanicemi. V principu je možné použít synchronizaci přes síť pomocí protokolu NTP, ale tímto způsobem nelze dosáhnout požadované přesnosti a zejména by nešlo věrohodně měřit zpoždění na linkách, po nichž se synchronizace provádí. Rozhodli jsme se proto vybavit každou monitorovací stanici nezávislým externím zdrojem času.

[1] *http://www.ces.net/project/qosip/*



Obrázek 6.1: Monitorovací stanice v síti CESNET2

Po vyhodnocení cenové náročnosti několika variant přijímačů GPS a DCF jsme zvolili následující typové řešení:

- přijímač Garmin GPS 18 (nebo GPS 35)
- konvertory rozhraní RS-232 <-> RS-422
- připojení přijímače na sériový port

Měřicí stanice mají instalován operační systém Linux, jádro 2.4.29 s tzv. „nanokernel patch“ (pro jádra řady 2.6 není nanokernel k dispozici). Synchronizaci času zajišťuje program *ntpd* ve verzi 4.2.0.

V současné době je typové řešení instalováno v Brně, Plzni, Českých Budějovicích a Olomouci. Instalace se připravuje v Ústí nad Labem a v Hradci Králové. V Praze je synchronizace monitorovací stanice zajištěna GPS přijímačem Trimble Acutime 2000, jehož signál je rozveden na serverovém sále. Také v Ostravě byl použit signál již existujícího přijímače (geodetický GPS přijímač Topcon GB-1000). V Liberci se zatím bohužel nepodařilo GPS přijímač instalovat.

Pro zvýšení kvality synchronizace jsme instalovali rubidiové hodiny PRS-10 firmy Stanford Research System s frekvenční stabilitou 5×10^{-12}. V praxi to znamená, že naše časové servery budou schopny udržet přesnost času v řádu mikrosekund po dobu několika dnů i bez GPS.

V roce 2006 plánujeme vytvořit systém pro kontrolu stavu a kvality synchronizace času v jednotlivých měřicích stanicích a časových serverech. Systém bude schopen doložit přesnost časové synchronizace a upozornit na případný chybový stav. Tím se zvýší věrohodnost našich budoucích měření.

6.3 Paralelní přenosy

Řízení zahlcení ovládané ve standardním protokolu TCP algoritmem AIMD(1, 0.5) je pro rozlehlé vysokorychlostní sítě příliš pomalé a není schopné plně využít šířku pásma. Možným řešením je použít některou z implementací „fast TCP“ s agresívnějším řízením zahlcení nebo například AIMD patch vyvinutý v rámci naší aktivity. To ale vyžaduje přístup uživatele root do operačního systému a restartování počítače. Alternativní možností zvýšení propustnosti je použití paralelních přenosů. V této oblasti jsme začali pracovat již v roce 2004, v letošním roce jsme zcela přepracovali paralelní soketovou knihovnu *psock*, která je univerzálním prostředkem pro využití paralelních přenosů v aplikacích. Knihovnu je možné získat na WWW stránkách[2] naší aktivity.

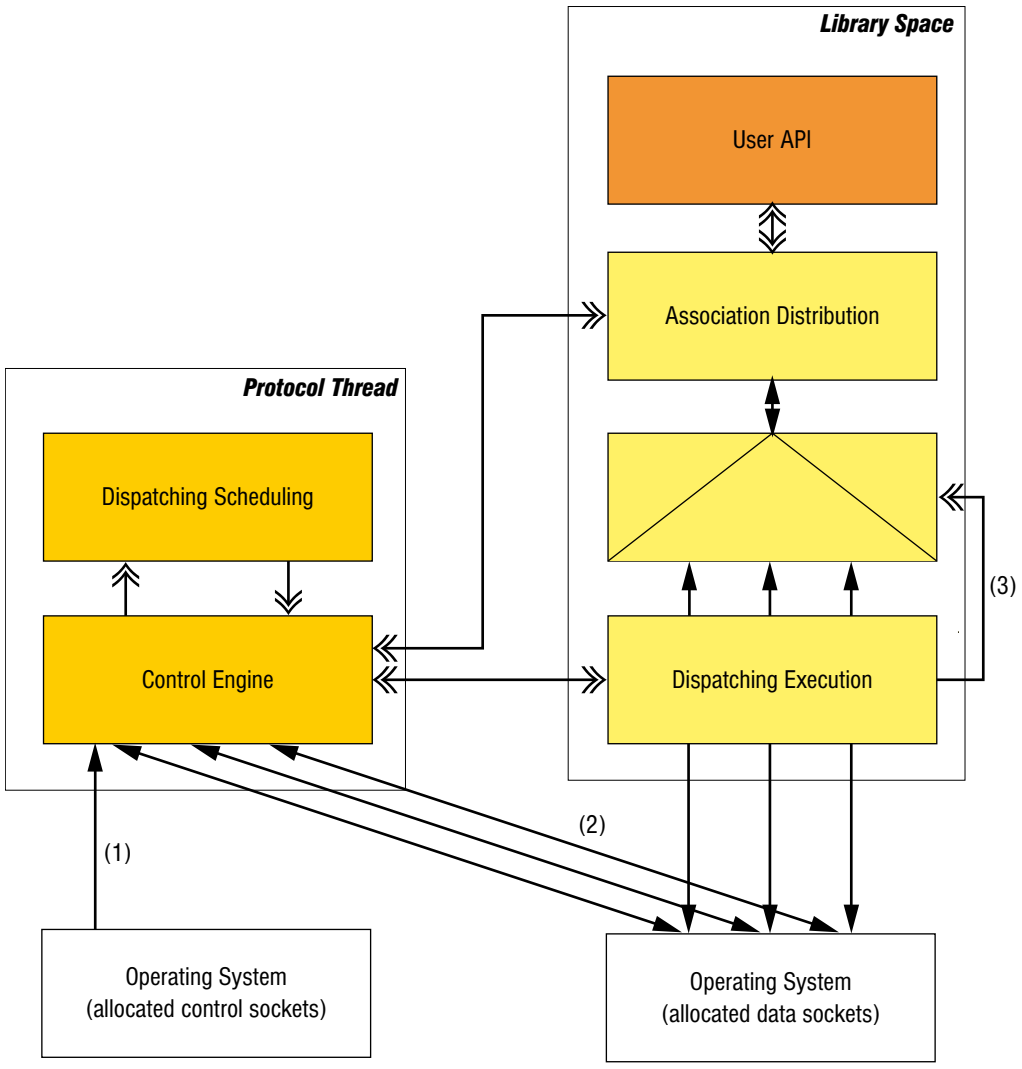
6.3.1 Implementace knihovny psock

Pro implementaci jsme si stanovili následující požadavky:

- Paralelní přenosy musí být snadno použitelné v existujících síťových aplikacích využívajících standardní soketovou knihovnu BSD.
- Distribuce dat do dílčích přenosů musí umět využít různou a měnící se šířku pásma dílčích přenosů, pomalejší dílčí přenos nesmí brzdit rychelší.
- Metoda distribuce dat do dílčích přenosů musí být konfigurovatelná.
- Architektura musí umožnit paralelní provádění na paralelním počítači.

Aplikace používající knihovnu *psock* běží ve *vlákně knihovny*. *Psock* dále vytvoří nové *vlákno protokolu*, které posílá data do dílčích přenosů a řídí paralelní přenos. Obě vlákna spolu komunikují asynchronně předáváním zpráv přes rozhraní *PSCIF (Parallel Socket Control Interface)*. Architektura knihovny *psock* je znázorněna na obrázku 6.2.

[2] *http://www.cesnet.cz/english/project/qosip/*



Obrázek 6.2: Architektura knihovny *psock*

Vlákno protokolu používá řídící soket (1) k výměně řídicích informací s druhou stranou. Mezi tyto informace patří například dohoda o počtu dílčích přenosů, oznámení čísel portů nebo dohoda použitého ovladače paralelního přenosu.

Vlákno protokolu dále čeká na události na soketech dílčích přenosů (2), čte z nich hlavičky bloků a připravuje *plánovací tabulku paralelního přenosu*. Vlákno knihovny používá tuto tabulku k řízení multiplexování a demultiplexování dat do a z dílčích přenosů.

6.3.2 Plánovací tabulka paralelního přenosu

Plánovací tabulka paralelního přenosu je tvořena dvěma kruhovými buffery, jedním pro odesílání a jedním pro příjem dat. Tyto buffery neobsahují přímo vlastní data, uvnitř knihovny nedochází k žádnému kopírování dat. Každá položka bufferu obsahuje číslo dílčího přenosu, který má být použit jako následující pro posílání nebo čtení dat, a počet bajtů, jež mohou být daným dílčím přenosem odeslány nebo z něj přijaty. Ke každému bufferu je udržován ukazatel na položku, která má být jako další použita vláknem knihovny. Je-li tato položka prázdná (žádný dílčí přenos není k dispozici pro odeslání nebo příjem dat), musí vlákno knihovny počkat, až bude tato položka naplněna vláknem protokolu. Stav tabulky pro tři dílčí přenosy může vypadat následovně:

Další přenos pro čtení / počet bajtů	2/1448	-	0/1448
Další přenos pro zápis / počet bajtů	-	0/1448	1/1448

Tabulka 6.1: Plánovací tabulka paralelního přenosu

Ukazatel pro čtení	0
Ukazatel pro zápis	1

Tabulka 6.2: Ukazatele do plánovací tabulky

6.3.3 Ovladač round-robin

Způsob distribuce dat do dílčích přenosů je určen *ovladačem paralelního přenosu*. Součástí implementace *psock* jsou zatím dva ovladače. Prvním z nich je ovladač round-robin, který posílá data v blocích stejné délky cyklicky jednotlivými dílčími spojeními. Propustnost paralelního přenosu je $c{=}n{\times}min(c_i)$, kde c_i je propustnost i-tého dílčího přenosu a n je počet dílčích přenosů.

6.3.4 Ovladač poll-all

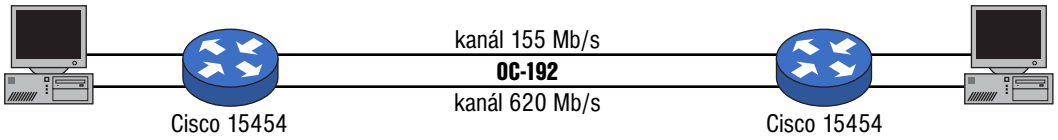
Ovladač poll-all používá volání `poll()` na soketech všech dílčích přenosů. Data jsou distribuována do dílčích přenosů podle jejich připravenosti k odesílání. Vysílač může využít různou a měnící se propustnost dílčích přenosů. Datové bloky jsou číslovány, aby mohly být sestaveny do původního pořadí. Pokud některý blok předběhne jiné bloky tak, že záznam o něm se nevejde to plánovací tabulky, je poznamenán do struktury `farsched_list` připojené k položce bufferu, do které bude záznam později přemístěn.

6.3.5 Ověření vlastností knihovny psock

Knihovnu *psock* jsme testovali v řadě situací. Zde vybíráme dva zajímavé scénáře.

Ovladače round-robin a poll-all na různých fyzických cestách

Mezi vysílačem a přijímačem vzdálenými asi 260 km (umístěnými v Praze a v Brně) byly dvě samostatné fyzické cesty. Jejich instalovaná propustnost byla 155 Mb/s a 620 Mb/s. Konfigurace je znázorněna na obrázku 6.3.



Obrázek 6.3: Konfigurace pro test ovladačů paralelního přenosu

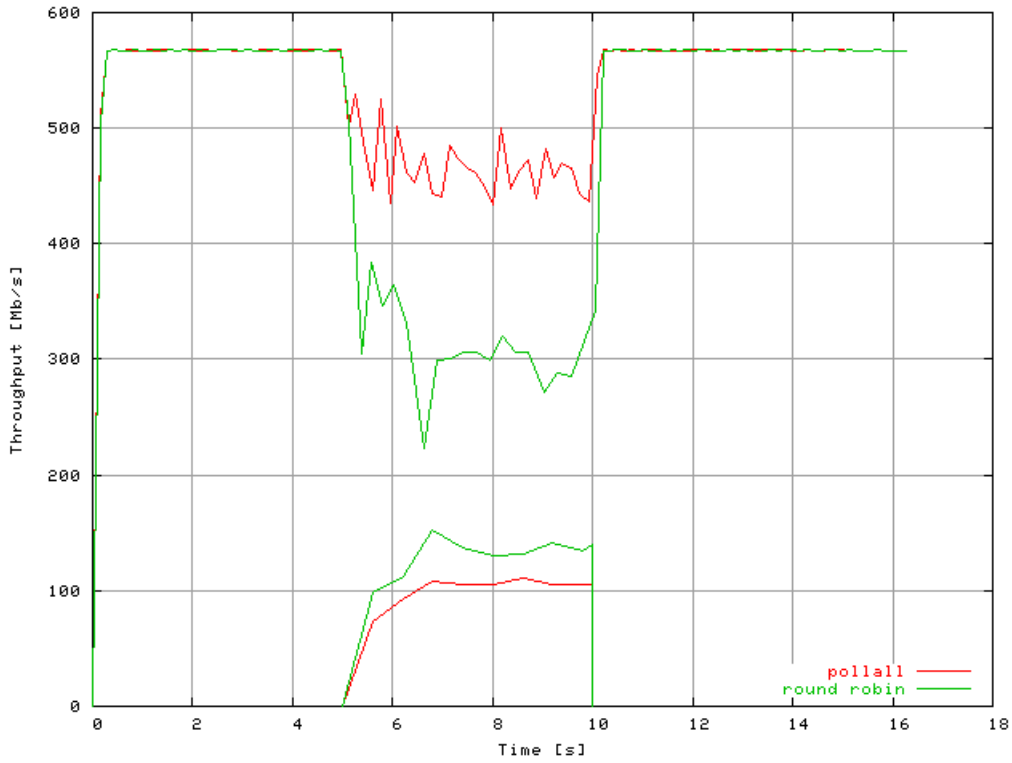
Měřili jsme propustnost pomocí programu *iperf*. Soketové buffery byly o něco větší než součin propustnosti každého dílčího přenosu a RTT.

- TCP propustnost dílčích spojení byla 142 Mb/s a 567 Mb/s, což bylo velmi blízko fyzické propustnosti.
- TCP propustnost paralelního přenosu s ovladačem round-robin byla 282,6 Mb/s, což bylo podle očekávání blízko dvojnásobku propustnosti pomalejšího dílčího přenosu.
- TCP propustnost paralelního přenosu s ovladačem poll-all byla 707,1 Mb/s, což bylo podle očekávání blízko součtu propustnosti dílčích spojení.

Test potvrdil schopnost ovladače poll-all využít různé kapacity paralelních tras použitých k přenosu.

Ovladače round-robin a poll-all a kolísání volné kapacity

Obě linky jsme zkonfigurovali na stejnou fyzickou propustnost 310 Mb/s. Měřili jsme propustnost paralelního přenosu pomocí programu *iperf* po dobu 15 sekund. V době 5 až 10 sekund jsme přidali další tok TCP jako zátěž v pozadí. Naměřená propustnost je znázorněna na obrázku 6.4. V dolní části obrázku je znázorněna i propustnost toku v pozadí. Můžeme vidět, že ovladač poll-all dokázal udržet podstatně větší propustnost paralelního přenosu než ovladač round-robin využitím aktuální volné kapacity linek jen s malým snížením propustnosti toku v pozadí.



Obrázek 6.4: Propustnost se změnou volné kapacity

Výhody naší knihovny *psock* oproti existujícím implementacím paralelních přenosů představují možnost použití existující implementace TCP v jádře operačního systému (standardní TCP nebo „fast TCP“), jednoduchá úprava stávajících síťových aplikací a možnost využití šířky pásma různých paralelních kanálů, jakož i možnost experimentů s algoritmy pro distribuci dat do paralelních kanálů.

6.4 Rozvoj firmware pro hardwarovou podporu monitorování

CESNET ve spolupráci s Masarykovou univerzitou a VUT v Brně již delší dobu pracuje na vývoji firmware pro hardwarovou podporu monitorování na kartách COMBO, vyvinutých v rámci projektů *Liberouter* a *SCAMPI*. Kapacita stávajícího týmu vývojářů je však již vyčerpána a protože se objevují další aktivity a projekty, pro které může být využití programovatelného hardware velmi užitečné, rozhodli jsme se vytvořit nové pracoviště pro vývoj programovatelného hardware. Pracoviště vzniká ve spolupráci s Katedrou telekomunikační techniky a Katedrou počítačů FEL ČVUT v rámci projektu Fondu rozvoje sdružení CESNET.

Do konce roku 2005 budou instalovány dva počítače vybavené kartami COMBO a potřebným vývojovým software. Tyto počítače budou využity během výuky. Nezávisle na tom jsme úspěšně rozběhli vývoj programovatelného hardware pro anonymizaci dat v hlavičkách paketů.

6.4.1 Hardwarová anonymizace hlaviček paketů

Při pasivním monitorování pracujeme přímo s pakety odeslanými uživatelskými aplikacemi (nikoliv s testovacími pakety). Odchycené toky reálného provozu jsou velmi užitečné pro výzkum v různých oblastech – od bezpečnostních aplikací přes směrovací protokoly. Zároveň je však důležité zajistit důvěrnost dat uživatelů. Proto je třeba z odchycených paketů odstranit důvěrné informace, avšak zachovat původní dynamiku provozu.

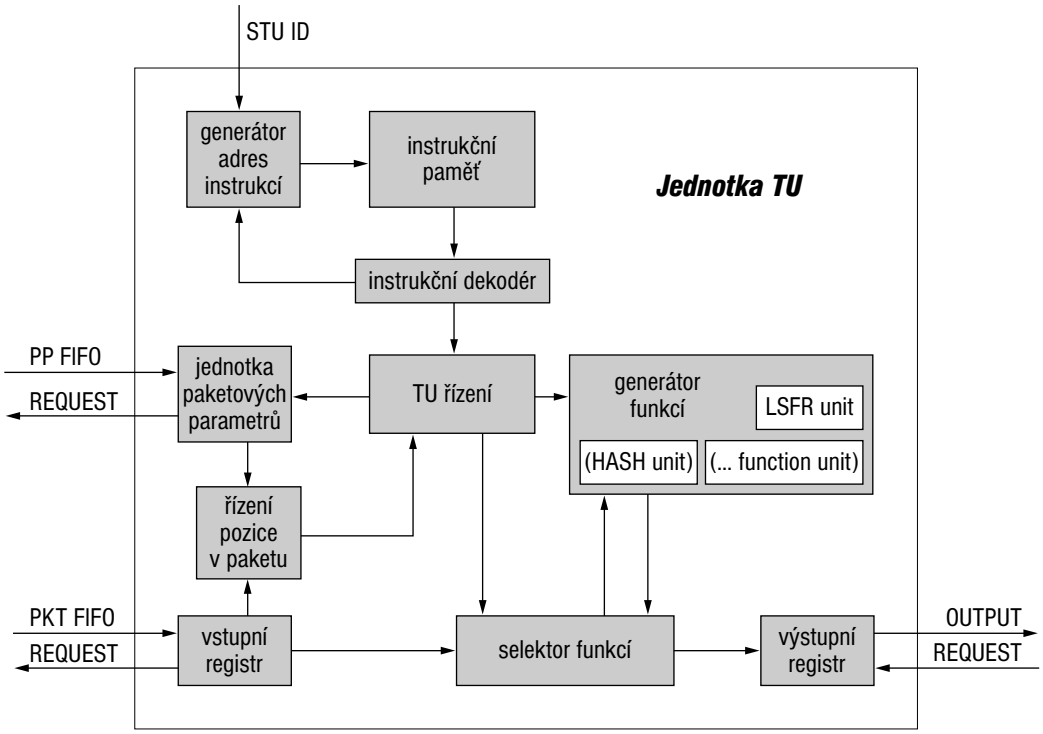
V rámci projektu LOBSTER pracujeme na programovatelné anonymizaci dat. Ta probíhá ve dvou úrovních. Nižší úroveň (first-tier) bude realizována přímo v hardware monitorovacího adaptéru. Vyšší úroveň (second-tier) bude probíhat dále v monitorovacím software. Anonymizace v software může být složitější, výhodou anonymizace v hardware je vyšší rychlost a to, že se citlivá data vůbec nedostanou do počítače, v němž je umístěn monitorovací adaptér. CESNET je v rámci projektu zodpovědný za hardwarovou anonymizaci.

Hardwarovou anonymizaci jsme navrhli a implementovali v podobě nové jednotky TU (Transformation Unit) přidané do monitorovacího firmware vytvořeného v rámci projektu SCAMPI. Struktura jednotky TU je znázorněna na obrázku 6.5. Jednotka TU je navržena jako tzv. nanoprocesor. Jde o hardwarovou jednotku, která pro každý přijatý paket provede specifikovaný nanoprogram z instrukční sady rozpoznávané jednotkou.

Jednotka TU umí v současné době zpracovávat následující položky v hlavičkách paketů:

- Zdrojová a cílová IP adresa
- Zdrojový a cílový TCP nebo UDP port
- Jakákoliv položka o šířce 16 nebo 8 bitů, jejíž pozice je zadána vůči některé z předcházejících položek

Jednotka TU tedy může pracovat v podstatě s jakýmikoliv položkami v hlavičkách paketů. Transformace, které může jednotka TU nad těmito položkami provádět, jsou následující:



Obrázek 6.5: Struktura jednotky TU

- nastavení na zadanou hodnotu
- nastavení na pseudonáhodnou hodnotu
- operace XOR se zadanou hodnotou

Jednotku TU jsme implementovali a úspěšně otestovali na hardware COMBO karty. V současné době pracujeme na dalších typech transformací. Nejzajímavější bude mapování IP adres se zachováním délek prefixů.

7 AAI a mobilita

Činnosti probíhající v rámci aktivity *AAI a mobilita* lze rozdělit do tří oblastí:

- rozvoj roamingové infrastruktury
- podpora autentizačních a autorizačních federací
- rozvoj infrastruktury veřejných klíčů.

Práce ve všech třech oblastech probíhá v těsné vazbě na mezinárodní aktivity v evropském i celosvětovém kontextu. Tato spolupráce má nezanedbatelný vliv na postup prací na národní úrovni; v některých případech ovlivňuje priority jednotlivých úloh a zadání.

7.1 Roaming uživatelů mezi institucemi

Rok 2005 byl velmi významný pro rozvoj roamingu uživatelů mezi akademickými institucemi. Probíhal pilotní projekt *eduroam.cz* (viz. [Sov04]), v jehož rámci bylo připojeno pět nových institucí a lokalit. Ke konci roku na pilotním projektu spolupracovaly instituce uvedené v tabulce 7.1. Možnost využívat přístupu k Internetu prostřednictvím bezdrátových sítí zúčastněných organizací je díky tomu dostupná tisícům uživatelů.

Instituce	*Lokalita*
CESNET z. s. p. o	Praha 6, Zikova 4
Karlova Univerzita	Areál Jinonice, Praha 5, U kříže 10
	FAF, Hradec Králové, Heyrovského 1203
	FF, Praha 1, Jana Palacha 2
	PRF, Praha 1, nám. Curieových 7
	Rektorát, Praha 1, Ovocný trh 5
ČVUT	FEL, Praha 6, Technická 2
	FJFI, Praha 1, Břehová 7
OSU	Dvořákova 7, Ostrava
TUL	Liberec 1, Hálkova 6
UHK	Hradec Králové 3, Rokitanského 62
UJEP	Ústí nad Labem, Hoření 13
VŠCHT	Praha 6, Technická 5
ZČU	Plzeň, Univerzitní 8

Tabulka 7.1: Účastníci pilotního projektu *eduroam.cz*

O neustále rostoucí popularitě projektu svědčí i zájem dalších institucí připojit se v průběhu příštího roku, jakmile budou schopny vybavit své lokality odpovídajícím technickým zařízením.

Pro většinu uživatelů a administrátorů připojených sítí představuje projekt *eduroam.cz* službu na úrovni velice blízké provozní. Infrastruktura poskytuje stovkám aktivních uživatelů očekávanou službu – přístup k Internetu nejen v rámci ČR ale i v sítích partnerských organizací v Evropě i některých dalších zemích. Před převodem služby do rutinního provozu je ovšem nutné dořešit ještě některé její vlastnosti.

S rostoucím počtem zapojených institucí a lokalit narůstá potřeba kvalitního monitorování autentizační infrastruktury projektu. V průběhu roku se velmi osvědčil systém automatického dozoru IPsec spojení mezi jednotlivými RADIUS servery. Systém vyhodnocuje dostupnost RADIUS serverů a posílá denně statistiku dostupnosti správcům jednotlivých serverů. I s jeho pomocí se nám podařilo i přes dílčí problémy se stabilitou a robustností některých implementací IPsec dosáhnout ke konci roku celkové prostupnosti infrastruktury blízké 100 %.

Pro monitorování vlastní funkčnosti autentizační infrastruktury projektu *eduroam.cz* využíváme dohledový systém *Nagios*. Systém v pětiminutových intervalech provádí ověřovací pokus o autentizaci na RADIUS serverech připojených institucí. Výsledky jsou prostřednictvím serveru *saint.cesnet.cz* k dispozici provoznímu dohledu sítě CESNET2 a správcům systému. Pro ověření autentizace používáme zatím standardní RADIUS plugin pro *Nagios*. Jeho nevýhodou je, že nepracuje s autentizačními mechanismy běžně používanými uživateli při připojování k síti (EAP/TTLS, EAP/TLS, PEAP/MSCHAPv2, ...). V rámci projektu jsme připravili vlastní ověřovací pluginy schopné provést autentizaci libovolným z mechanismů běžně užívaných 802.1x suplikanty. Jejich nasazení do dohledového systému sítě plánujeme na začátek roku 2006.

Své zkušenosti s monitorováním infrastruktury RADIUS serverů sdílíme se zahraničními kolegy na půdě pracovní skupiny TF-Mobility asociace TERENA, kde připravujeme vznik globálního dohledového systému v rámci mezinárodního projektu *eduroam*.

Po vyhodnocení pilotního projektu na podzim roku 2005 (viz [Fur05]) bylo rozhodnuto navázat druhou fází pilotu se zaměřením na dobudování dohledového systému a jeho začlenění do vznikajícího mezinárodního systému.

7.2 Podpora autentizačních a autorizačních federací

Základní představa autentizační a autorizační federace je prostá: Federaci tvoří množina institucí, které se dohodly na společném využívání zdrojů a které navzájem akceptují své lokální autentizační a autorizační mechanismy a postupy.

Uživatel jedné z účastnických institucí pak může využívat služeb poskytovaných libovolným dalším členem federace, aniž by musel být zaregistrován a ověřen jako lokální uživatel poskytovatele. Autentizaci a informace potřebné pro autorizační rozhodnutí poskytuje domovská organizace uživatele.

Funkční federace musí být definována na několika vrstvách: od komunikačních protokolů a datových formátů přes sémantiku předávaných dat až po provozní a organizační pravidla ([Sov05]). S ohledem na stále se rozšiřující mezinárodní spolupráci je nutné při přípravě národní federace brát v úvahu situaci v evropském i celosvětovém kontextu. Problém výstavby autentizačních a autorizačních federací je v současné době řešen jak na půdě asociace TERENA (pracovní skupina TF-EMC2), tak v rámci projektu EU GÉANT2 (pracovní skupina JRA5). Příkladem specializovaných federací mohou být i některé Gridové projekty. Se všemi výše uvedenými komunitami úzce spolupracujeme, abychom zajistili kompatibilitu budoucí národní federace s mezinárodními aktivitami v oboru.

Základním předpokladem pro vznik federace je existence lokálních autentizačních a autorizačních systémů. Jejich výběr musí provést jednotlivé instituce samy podle lokálních požadavků. Hodnocení systému *WebAuth*, jednoho z potenciálních kandidátů je popsáno v [Gro05]. Systém WebAuth je nasazen na ZČU.

Přestože vznik generické autentizační a autorizační infrastruktury je technicky i organizačně náročný (jak je vidět i na postupu prací na mezinárodním poli), můžeme již dnes pro některé specifické účely s výhodou využít existující federativní infrastrukturu vybudovanou v rámci projektu *eduroam*. Příkladem takového využití může být projekt SIP telefonie CESNET2[1], který využívá autentizaci prostřednictvím infrastruktury *eduroam.cz* při registraci uživatelů.

7.3 Infrastruktura veřejných klíčů

V polovině roku 2006 (27. června) skončí platnost původního kořenového certifikátu certifikační autority CESNET CA. Vzhledem k tomu, že certifikáty koncových entit byly vydávány s platností 12 měsíců, bylo potřeba zajistit přechod na nový kořenový certifikát do 27. června 2005. Začátkem roku 2005 vyhlásila EUGridPMA (mezinárodní orgán, u nějž je CESNET CA akreditována) některé významné změny svých minimálních požadavků na CA. Rozhodli jsme se využít této příznivé časové shody a nahradit stávající provozní systém certifikační autority novým, odpovídajícím novým minimálním požadavkům.

Stará implementace CA byla koncipována jako off-line systém, tzn. vlastní pracoviště certifikační autority je instalováno na počítači, který se nikdy nepřipojuje

[1] *https://sip.cesnet.cz/dokuwiki/*

k datové síti. Tím je zajištěna vysoká bezpečnost privátního podpisového klíče, na druhou stranu to ale klade vysoké nároky na obsluhu systému. Všechny žádosti o certifikáty nebo o jejich revokaci se musí přenášet na pracoviště CA na výměnných mediích, zpět se pak přenášejí vydané certifikáty a revokační seznamy a manuálně se kopírují na servery dostupné po internetu. Tento režim práce neumožňuje v podmínkách CESNET CA zajistit nepřetržitý provoz certifikační autority, což může mít za následek i několikadenní zdržení (víkend) při vydávání či zneplatňování certifikátů.

Z výše uvedených důvodů jsme se rozhodli implementovat nový systém CESNET CA jako on-line certifikační autoritu. Pro zajištění bezpečnosti privátního klíče on-line CA požaduje EUGridPMA použití hardwarového bezpečnostního modulu (HSM) certifikovaného podle normy FIPS 140-2 úroveň 3. Abychom mohli nabídnout uživatelům bezpečné, robustní a komfortní prostředí, zvolili jsme pro implementaci nové CESNET CA produkty firmy Entrust: *Entrust Authority Security Manager* pro vlastní systém CA a *Entrust Authority Enrollment Server for Web* jako uživatelské rozhraní pro koncové uživatele. Pro uložení privátního klíče jsme vybrali HSM *Luna CA3* firmy SafeNet, se kterým Security Manager spolupracuje a který odpovídá požadavkům EUGridPMA.

Produkty firmy Entrust jsou obvykle charakterizovány jako plně integrované PKI řešení pro komerční či vládní organizace. Ukázalo se, že potřeby CESNET CA jako víceméně otevřené služby mohou být v některých případech odlišné. Abychom zajistili pracovní toky pro vydávání certifikátů odpovídající našim požadavkům, připravili jsme obslužný systém *LAI*, který umožňuje uživatelům registrovat data určená k certifikaci v prostředí české akademické komunity.

Vzhledem k vlastnostem softwarového toolkitu *OpenSSL*[2], který tvoří základ middleware většiny Gridových aplikací, jsme pro novou certifikační autoritu definovali nový jmenný prostor. Subjekty nových certifikátů jsou součástí datového informačního stromu *dc=cesnet-ca,dc=cz*.

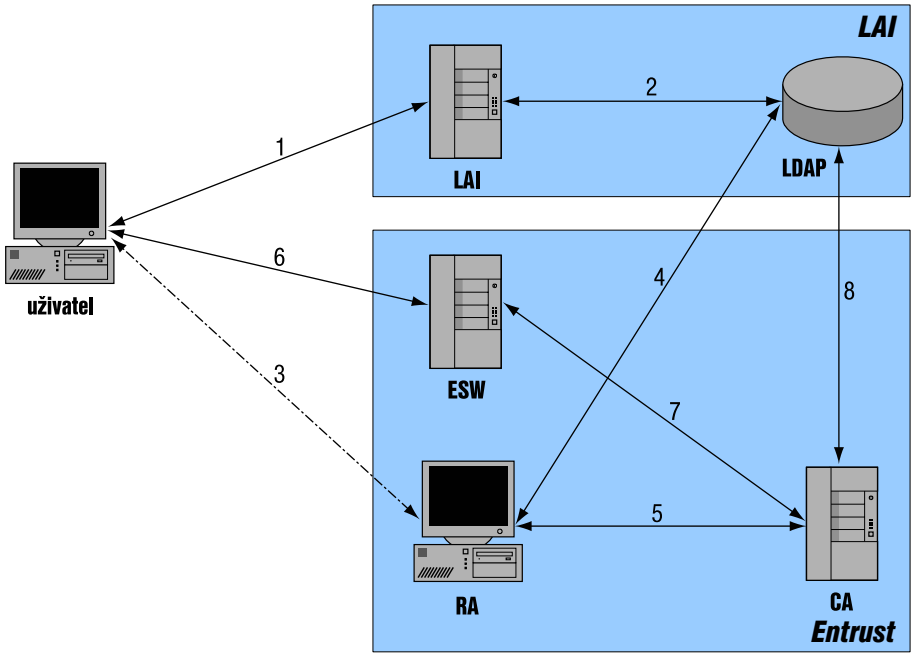
Celý systém byl připraven tak, že 17. června 2005 mohla být nová certifikační autorita uvedena do provozu. Architektura nového systému je znázorněna na obrázku 7.1.

Činnosti při vydávání certifikátu pak probíhají následovně:

1. Uživatel vyplní ve webovém rozhraní systému LAI informace, které mají být uvedeny v certifikátu.

2. Systém přidělí uživateli rozlišovací jméno (*DN*), ověří vložená data a zanese záznam koncové entity (uživatel nebo jím spravovaný počítač) do databáze LDAP.

[2] *http://www.openssl.org/*



Obrázek 7.1: Vydání certifikátu CESNET CA

3. Uživatel navštíví pracoviště registrační autority s požadovanými doklady. (Jde-li o certifikát pro počítač/službu, může poslat žádost o zpracování záznamu elektronickou poštou opatřenou digitálním podpisem).

4. Operátor registrační autority znovu ověří data v záznamu subjektu uložená v databázi LDAP.

5. Je-li záznam-žádost v pořádku, vloží ji do interní databáze systému certifikační autority a předá uživateli přístupové kódy pro vydání certifikátu. (V případě žádosti o certifikát pro počítač/síťovou službu mu je odešle elektronickou poštou zašifrované veřejným klíčem z uživatelova certifikátu.)

6. Uživatel zadá ve webovém rozhraní Enrollment Server for Web obdržené přístupové kódy a žádost o certifikát (ta může být automaticky generována uživatelovým webovým prohlížečem).

7. Enrollment Server for Web předá uživatelem zadaná data k vyřízení softwaru certifikační autority. CA vydá požadovaný certifikát a

8. publikuje jej do příslušného záznamu v LDAP serveru.

Systém LAI je podrobněji popsán v [Tom05].

Při implementaci systému jsme zjistili, že komunikace mezi komponentami systému Entrust (registrační autorita, certifikační autorita) a LDAP serverem neprobíhá šifrovaně. Entrust plánuje odstranit tento nedostatek v nové verzi svých produktů v roce 2006. Do té doby jsme na uvedené systémy nasadili program *stunnel*[3], kterým komunikaci šifrujeme.

Jedním z hlavních důvodů pro nasazení nového systému CESNET CA bylo co nejvíce usnadnit uživatelům získávání certifikátů. Očekávaného výsledku bylo dosaženo u nových uživatelů. Paradoxně nejvíce problémů s přechodem na nový systém měli zavedení uživatelé zvyklí na staré postupy, které nové uživatelské rozhraní občas překvapilo. Po vyhodnocení uživatelské odezvy plánujeme na příští období úpravu WWW rozhraní tak, abychom uživatelům vyšli co nejvíce vstříc.

Mezi často zmiňovaná úskalí využití PKI patří správa a zabezpečení uživatelských privátních klíčů. Za vhodné řešení tohoto problému považujeme vybavit uživatele hardwarovými šifrovacími tokeny, na kterých je uložený privátní klíč chráněn heslem a nikdy je neopouští. Požadované kryptografické operace pak provádí token sám na žádost aplikace prostřednictvím ovladače v operačním systému. Zaměřili jsme se na výběr vhodných zařízení tohoto typu pro uživatele a zejména pro privátní klíče operátorů registračních autorit. Výsledky testů jsou uvedeny v [Jin05]. Operátory registračních autorit a vybrané uživatele plánujeme vybavit hardwarovými šifrovacími tokeny začátkem roku 2006 pro projednání na půdě EUGridPMA.

[3] *http://www.stunnel.org/*

8 IP telefonie

IP telefonie patří k progresivním aplikacím a získává čím dál více uživatelů. Sdružení CESNET věnuje patřičné úsilí rozvoji a zkvalitnění služeb IP telefonní infrastruktury. V roce 2005 jsme řešili otázky související s transformací výstupu do veřejné sítě, zabývali jsme se hodnocením kvality hovoru, připravili jsme pro členy možnost adresování využívající ENUM, věnovali jsme se implementacím IP telefonie na otevřených řešeních jako je GnuGK, SER a Asterisk. V závěru roku se v rámci aktivity uskutečnil seminář o IP telefonii, kde byli posluchači informováni o rozsahu stávajících služeb a připravovaných novinkách.

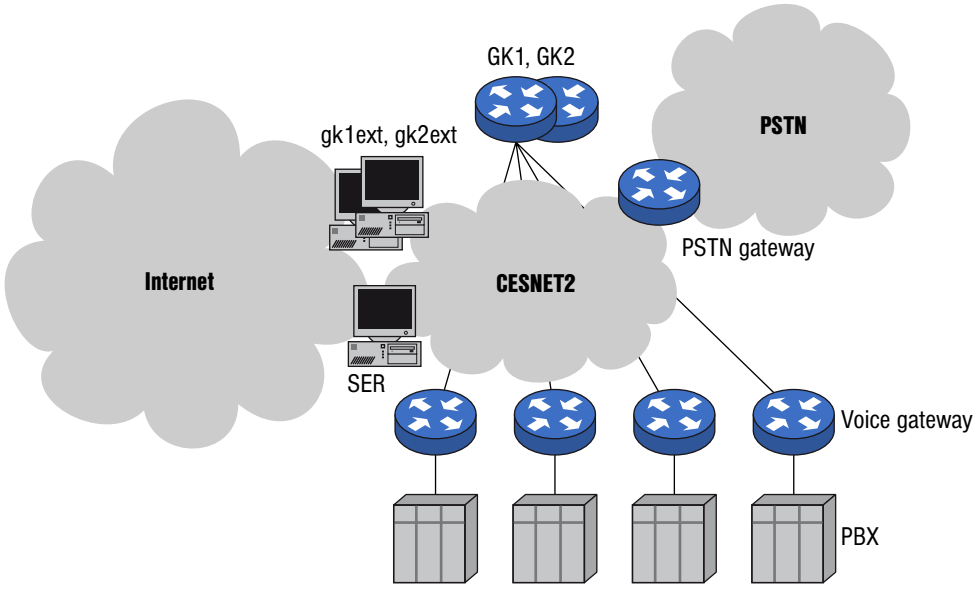
Během letošního roku bylo přes síť CESNET2 uskutečněno více než 1,5 mil. hovorů a VoIP infrastruktura umožnila letos prohovořit celkově 4,5 mil. minut, přičemž mezi univerzitami v rámci CESNET2 to bylo téměř 0,7 mil. minut. Tato čísla jsou nepřehlédnutelná.

8.1 Stávající stav

Jako každoročně jsme i letos zaznamenali zájem o připojení dalších ústředen členů sdružení, konkrétně se jednalo o SLU Opava v Karviné, MZLU v Brně a tři pražské ústavy AV ČR – Geologický ústav, Ústav chemických procesů a Ústav experimentální botaniky. Aktuální seznam institucí zapojených do projektu IP telefonie lze nalézt na stránce s informacemi o naší síti[1]. Připojené instituce používají stejná telefonní čísla jako ve veřejné síti, ale CESNET má od ČTÚ navíc přidělen i prefix pro přístup do sítě IP telefonie ve tvaru 950 0, pro IP telefony tedy máme k dispozici sto tisíc čísel. Dostupnost těchto čísel byla prověřena ze sítí Českého Telecomu, GTS Novera a Oskar. V souvislosti s transformací výstupu sdružení CESNET do veřejné telefonní sítě se ale objevil problém s voláním do VTS, jelikož identifikace volajícího je vázána na výstup umístěný v sídle sdružení. Proto jsme pozastavili distribuci těchto čísel mezi členy.

Na obrázku 8.1 najdete schéma sítě s prvky infrastruktury IP telefonie. Jednotlivé hlasové brány členů jsou registrovány na vnitřní GK1 a GK2. Dostupnost z Internetu zajišťují hraniční *gk1ext* a *gk2ext*. Veškeré brány jsou schopné komunikovat obousměrně protokolem H.323 a většina je schopna přijmout příchozí spojení protokolu SIP. Pokud je zapotřebí překlad mezi SIP a H.323, spojení prochází přes překladovou bránu. Můžeme tedy konstatovat, že máme funkční síť s podporou obou signifikantních protokolů používaných ve VoIP. Kromě řídících prvků GK1, GK2, *gk1ext* a *gk2ext* pro H.323, máme nasazen SIP server SER, který obsluhuje volání protokolem SIP.

[1] *http://www.cesnet.cz/iptelefonie/voip-cesnet.html*



Obrázek 8.1: Schéma sítě s prvky infrastruktury IP telefonie

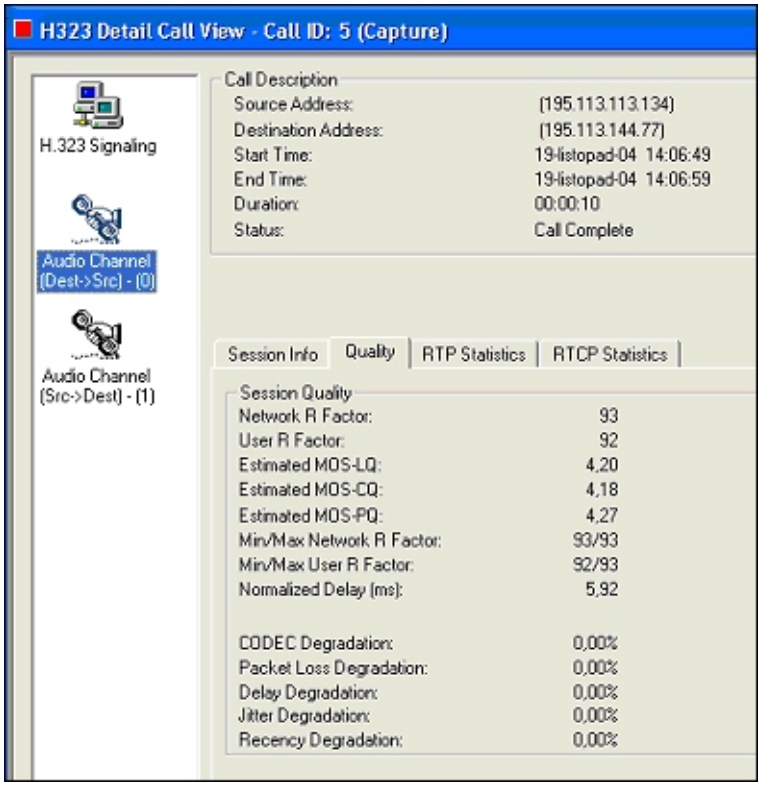
8.2 Kvalita hovoru

Jako kritéria pro určování kvality hovoru používáme R-faktor a MOS. K měření používáme analyzátor *Surveyor*, který umožňuje konvertování získaného R-faktoru na parametry Mean Opinion Score (MOS), Listener Quality (MOS-LQ), Mean Opinion Score PESQ (MOS-PQ) a Conversational Quality (MOS-CQ). Síťový R-faktor (Network R-factor) je generován na základě zhoršení způsobeného fyzickým zařízením. Uživatelský R-faktor (User R-factor) sčítá vnímavostní efekty se zhoršením způsobeným zařízením (např. aktuálnost a zpoždění). Komponenty pro výpočet R-faktoru jsou popsány v doporučení ITU-T G.107. Výpočet je založen na E-modelu a kombinuje všechny přenosové parametry důležité pro zvažované spojení. Obecně lze oblast měření kvality volání rozdělit na tři základní typy:

Listening Quality: Měření odvolávající se na skutečnost, jak uživatelé hodnotí, co slyší během volání.

Conversational Quality: Měření se odkazuje na skutečnost, jak uživatelé hodnotí celkovou kvalitu volání, a to na základě kvality poslechu a jejich schopnosti konverzace během tohoto volání.

Transmission Quality: Měření se odkazuje na kvalitu síťového spojení používaného pro přenos hlasového signálu. Konkrétně se tedy jedná o měření kvality síťové služby, a to jako protikladu ke specifické kvalitě volání.



Obrázek 8.2: Zobrazení statistik pro Details – Audio Channel Quality

Obrázek 8.2 obsahuje zobrazení statistik pro Details – Audio Channel Quality z analyzátoru. Při měření získáváme kvalitativní parametry spojení, jimiž jsou:

- Jitter,
- MOS-CQ,
- MOS-LQ,
- MOS-PQ,
- Network R-factor,
- User R-factor.

Výstupem z oblasti měření kvality hovorů jsou v roce 2005 dvě technické zprávy [VoZ05a] zabývající se kvalitou hlasu v prostředí VoIP s praktickými výsledky a [VoZ05] popisující analýzu pomocí aplikace Surveyor.

8.3 Podpora H.323

V letošním roce jsme pokračovali v rekonfiguraci hraničního *gk1ext.cesnet.cz* a řešili jsme problémy autentizace, volání přes NAT a začlenění do GDS.

V současné době se autentizují pouze IP telefony, které jsou přímo registrovány na *gk1ext*. Autentizace vyžaduje uživatelské jméno a heslo (hash MD5), účty jsou vytvářeny na vyžádání. Zaregistrovali jsme několik požadavků na propojení GK, z nichž nejvýznamnější bylo propojení s národním GK akademické sítě v Litvě. Každopádně bilaterární dohody o propojení nejsou zajímavé, protože v rámci NREN je strategie orientována na použití GDS (Global Dialing Scheme), což obnáší vytvoření národního gatekeeperu a jeho propojení na světové GK. Přínosem je možnost volat a být volán ze všech registrovaných sítí (převážně národní akademické sítě, univerzity a výzkumné ústavy). Sdružení CESNET využívá GDS a českým národním GK je *gk1ext.cesnet.cz*.

Problémy, které mají uživatelé s NAT, jsme se pokusili vyřešit nasazením proxy režimu pro neveřejné adresy na *gk1ext*. Mechanismus je takový, že pokud detekuje *gk1ext* přihlášení uživatele, který je za NATem, funguje pro tohoto uživatele jako signalizační i RTP proxy a veškerá komunikace probíhá přes *gk1ext*. Ověřili jsme funkčnost pro Full Cone NAT, pro symetrický NAT ovšem nastavení proxy režimu nestačí. Řešením je použití VPN klienta a přístup na VPN koncentrátor konkrétní instituce. V případě řešitelů výzkumného záměru sdružení lze pochopitelně využívat CESNET VPN, na kterém jsou řešitelé autorizováni pomocí TACACS+ účtu.

Výstupem z oblasti konfigurace *gk1ext* je technická zpráva [VoN05] s názvem „GNU Gatekeeper a jeho nasazení v síti CESNET2“.

V první polovině roku 2005 jsme otestovali IP telefony, které byly zapůjčeny od VoIP operátorů v ČR prostřednictvím redakce časopisu *Connect!*. Výsledky byly publikovány v květnovém vydání časopisu. Pro použití s H.323 a GnuGK doporučujeme každopádně IP telefon, který umožňuje autentizaci. Pokud autentizaci nezvládá, je možné nastavit aspoň ověření uživatele proti IP adrese, což je rovněž popsáno v technické zprávě [VoN05].

8.4 Asterisk

V letošním roce jsme se zabývali podporou protokolu IAX2, SIP a dostupností H.323 kanálu. Testovali jsme telefony AT-320, a to v režimu IAX2, H.323 i SIP. Zajímavou oblastí je ovládání Asterisku prostřednictvím příkazového řádku (Command Line Interface, CLI), stejně jako ovládání GnuGk pomocí rozhraní pro Telnet.

IAX2 je velmi dobrou volbou pro průchod přes NAT. Největším problémem je, že není dosud standardizován. V současné době vyšel nový internet draft, který nahradil předchozí verzi návrhu s prošlou platností, dokončení standardizace se očekává v polovině roku 2006. Dokument popisuje protokol určený pro řízení aplikační vrstvy a přenášené médium, vytvoření, modifikaci a ukončení relace

prostřednictvím sítě s protokolem IP. IAX2 je primárně určen pro řízení přenosu hlasu přes IP, může být však použit také pro streaming různorodých dat (audio, video). Primárním cílem protokolu je minimalizovat nezbytnou šířku pásma určenou pro signalizaci a vlastní přenášené médium. Cílem je také poskytnout přirozenou podporu pro NAT transparentnost. Je použit pouze jeden UDP port, pro nějž není problémem nakonfigurovat konkrétní firewall.

Základní vlastnosti protokolu:

- signalizační a přenosový protokol typu peer-to-peer
- základním přístupem k návrhu IAX2 je multiplexování signalizace a vícenásobných mediálních toků do jediného UDP spojení mezi dvěma hostiteli (UDP port 4569)
- IAX2 je binární protokol, efektivně využívá dostupné přenosové pásmo
- základní komunikační jednotkou v IAX2 je rámec (Full frame, Mini frame, Meta frame, Information element)
- podporuje opatření pro zabezpečení prostřednictvím vícenásobných metod uživatelské autentifikace a autorizace

8.4.1 Kanál H.323

V současnosti existuje několik nezávislých implementací kanálu H.323 do systému Asterisk (h323, oh323, ooh323c, woomera). V našem případě jsme se zabývali implementací kanálu oh323 a možností jeho využití pro komunikaci H.323 terminálů. Tento kanál se nám podařilo společně s GnuGk přivést do stavu částečné funkčnosti. V současnosti jsme schopni k softwarové ústředně Asterisk připojit terminály typu SIP, IAX2 a H.323. V souvislosti s použitím telefonů *optiPoint* (300 advance, 400 standard) se vyskytl problém korektního zobrazení příchozího telefonního čísla. Tyto telefony v současnosti nezobrazují číslo korektně, například softwarový telefon *SJPhone* však ano.

H323: Jedná se o kanál obsažený ve zdrojové distribuci Asterisku v adresáři */channels/h323*. Tento kanál funguje pouze jako H.323 gateway, ne však jako gatekeeper.

Oh323: Implementace H.323 kanálu (ve skutečnosti vůbec první implementace) nazvaná Asterisk-oh323, která je stále aktivně vyvíjena, a to projektem firmy InAccess Network[2].

[2] *http://www.inaccessnetworks.com/projects/asterisk-oh323*

V současné době se u implementací H.323 do Asterisku potýkáme s následujícími problémy:

- h323 – neobsahuje jitter buffer, tato implementace používá Asterisk RTP Stack.
- oh323 – používá RTP/RTCP stack a implementaci adaptivního jitter bufferu z OpenH323, nepoužívá kodeky systému OpenH323, ale kodeky Asterisku.
- Použití oh323 odstraňuje problémy plynoucí z použití h323 (stabilita), nicméně přibližně 10–15krát zvyšuje využití procesoru.

GnuGk je využit ve funkci gatekeeperu potřebného pro podporu H.323 kanálu v softwarové ústředně Asterisk. Zatím jsme testovali pouze konfigurace umožňující přihlášení libovolného terminálu, omezené požadavkem na tvar telefonního čísla a příslušnou definicí čísla v souboru číslovacího plánu. Pokročilejší autorizace je řešena v technické zprávě [VoN05].

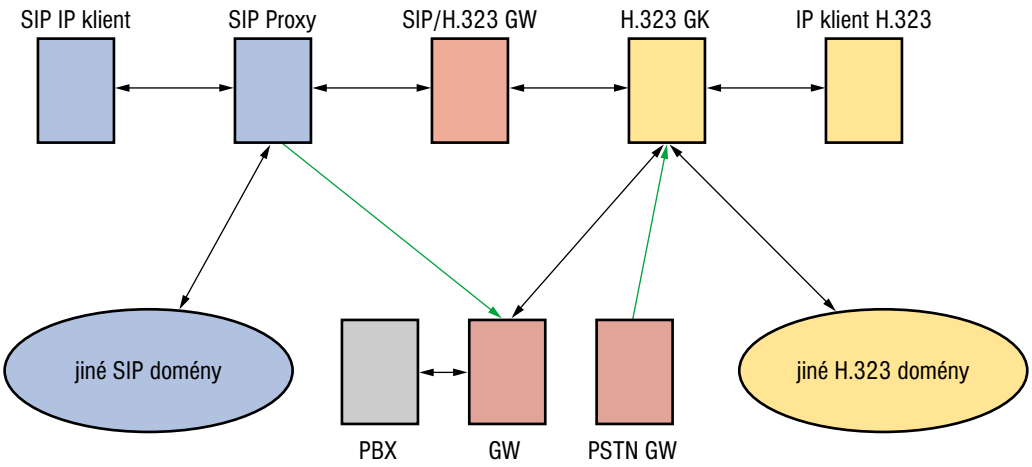
Výstupem z oblasti implementace softwarové ústředny Asterisk je technická zpráva [WZV05] s názvem „Asterisk a jeho použití“.

8.5 SIP

Základním řídícím prvkem implementace protokolu SIP v síti CESNET2 je SIP proxy server běžící na platformě Linux a SIP Express Router (SER). Server plní funkci registračního a proxy serveru. Na tento prvek mohou být zaregistrováni SIP klienti ve formě softwarových balíčků i hardwarových telefonů a komunikovat přes něj s okolním světem. SIP proxy provádí také směrování hovorů na brány připojených institucí podle telefonních prefixů. Většina bran je připojena přímo protokolem SIP. Pouze tam, kde to hardware nedovoluje, jsou hovory směrovány přes SIP/H.323 bránu. Proxy server také obsluhuje příchozí a odchozí hovory do jiných SIP domén, jako například *iptel.org*, *bts.sk*, *aarnet.edu.au*.

Hovory (iniciované z ústředen za branami, z veřejné telefonní sítě a z H.323 IP klientů) směřující do SIP sítě, procházejí přes SIP/H.323 bránu. S nasazením nového směrovacího systému v příštím roce bude všude, kde je to možné, použit přímo protokol SIP bez překladu. Jako SIP/H.323 bránu momentálně používáme zařízení CISCO IOS IP2IP gateway. Její schopnosti nejsou například v oblasti ENUM pro nás zcela vyhovující, proto se pokusíme i o využití Asterisku, který má však zatím rezervy v implementaci H.323.

SIP proxy funguje v takzvaném multidoménovém režimu. To znamená, že kromě své mateřské domény *cesnet.cz* je schopna obsloužit i domény jiných institucí.



Obrázek 8.3: Schéma propojení SIP a H.323 sítí

Naším záměrem je, aby si instituce tímto způsobem vyzkoušely SIP systém a pak přenesly SIP proxy přímo k sobě a integrovaly SIP do svých systémů ještě lépe, než tomu může být v případě naší multidoménové proxy.

Zřízení domény na multidoménové proxy je nutné doprovodit vytvořením SRV záznamu v příslušné DNS doméně instituce, aby bylo zajištěno správné směrování požadavků. Potenciální uživatelé si zřizují účet pomocí webového formuláře. Identita žadatele je ověřena prostřednictvím infrastruktury *eduroam*, která využívá AA systémů domovských institucí. V následujících letech, s nástupem nové distribuované AAI, předpokládáme ještě lepší a důslednější využití AAI systémů, především v oblasti mezidoménové autentizace a přístupu ke sdíleným službám.

Spolu se SIP serverem jsme spustili nový web *IpTelWiki*[3] věnovaný především implementaci SIPu v síti CESNET2. Na *IpTelWiki* je možné získat informace o vlastním protokolu SIP, o jeho integraci do IP-telefonní sítě CESNET2, o vytvoření SIP účtu a volání přes SIP. Naším cílem je, aby se tento web stal místem pro sdílení informací o IP telefonii v rámci co nejširší komunity uživatelů a správců. Tyto stránky se postupně stanou webem celé aktivity *IP telefonie*, který doposud naleznete na webu sdružení. Kromě informačních stránek je součástí systému také webové rozhraní SIP serveru *SerWeb*, které umožňuje uživatelům správu účtů a klientských registrací a poskytuje další údaje o jeho využívaní, jako jsou záznamy o provedených hovorech.

[3] *https://sip.cesnet.cz/dokuwiki/*

8.6 ENUM

Sdružení CZ.NIC, držitel delegace národní domény *0.2.4.e164.arpa*, připravuje testovací provoz. Delegace domén pro prefixy 234 680 a 950 0, které jsme získali již před spuštěním testovacího provozu, jsou momentálně jedinými delegacemi v celém stromu *0.2.4.e164.arpa*.

Abychom mohli naplno využít potenciál technologie ENUM, připravili jsme pro členy sdružení zapojené do projektu IP telefonie možnost vyřízení delegace našim prostřednictvím. Cílem je dosáhnout úplného pokrytí IP telefonní sítě CESNET2 ENUM záznamy. Instituce si mohou spravovat své záznamy na svých jmenných serverech, nebo jim nabízíme možnost správy koncových záznamů na DNS serverech sdružení. Mezi těmito variantami je možné přecházet bez nutnosti interakce s držitelem delegace národní domény. S přechodem do ostrého provozu, který se předpokládá na začátku roku 2007, požádají instituce pouze některého z registrátorů o registraci podle nově vytvořených pravidel pro *0.2.4.e164.arpa* a záznamy zůstanou funkční. Zde je vhodné připomenout, že registrace v doméně *0.2.4.e164.arpa* probíhají odlišně od klasických domén, kvůli své vazbě na veřejné telefonní číslo. Odezva na připravený postup byla příznivá a předpokládáme vyřízení delegace pro valnou většinu prefixů připojených institucí ještě do konce roku 2005.

V rámci organizace TERENA jsme se zapojili do diskusí o novém směrovacím systému, který postupně nahradí GDS hierarchii. Jednou z možností je právě využití technologie ENUM. Nevýhodou GDS je jeho pevná vazba na H.323, kterou by ENUM řešil. Vzhledem k různé úrovni národních implementací ENUM, půjde pravděpodobně o použití privátního stromu. To pro nás znamená pouze jednoduchou operaci, kdy informace již publikované do stromu veřejného budou publikovány i do privátního stromu.

8.7 CCM a aplikace

V průběhu letošního roku jsme provedli pokusné připojení IVR (Interactive Voice Response) aplikací na rozhraní SW a HW klientů. V první fázi jsme použili IVR integrované v CCM a jako aplikaci jsme použili VoiceBox pro zanechání hlasových zpráv nepřítomnému uživateli. Problémy nastaly při využití distribuované architektury jednotlivých komponent takto navrženého systému. Vypadávalo spojení mezi úložištěm dat a vlastním CCM, který řešil signalizační a distribuční část této aplikace. V další fázi jsme se snažili o vybudování takovéhoto systému v návaznosti na jakoukoliv obecnou databázi, v níž jsou uloženy záznamy hlasových zpráv, a o jednotnou autentizaci uživatele VoIP klienta pro všechny aplikace s ním svázané. Jako základní postup jsme úspěšně vyzkou-

šeli rozhraní LDAP. Předpokládáme zprovoznění hlasového záznamníku v první polovině následujícího roku. Současně budou prováděny zkoušky pro klienty komunikující jinými signalizačními protokoly a zapojení jakýchkoliv obecných IVR do tohoto systému.

9 MetaCentrum

Gridy – rozsáhlé distribuované systémy počítačů, datových skladů a dalších zařízení, propojených počítačovou sítí – se stávají nezbytnou součástí globální výzkumné a vývojové infrastruktury. Provoz a další rozvoj gridové infrastruktury v České republice je hlavním cílem aktivity *MetaCentrum*, která tak vytváří nezbytné zázemí pro napojení nejen do mezinárodních gridově orientovaných aktivit, ale především poskytuje podmínky pro rozvoj všech vědních disciplin. Činnosti v rámci MetaCentra jsou úzce koordinovány jednak s dalšími aktivitami v rámci výzkumného záměru sdružení CESNET – především v oblasti bezpečnosti (spolupráce a intenzivní využívání výsledků práce kolem certifikační autority) a prostředí pro spolupráci – jednak s mezinárodními aktivitami v oblasti budování a rozvoje Gridů, zejména pak intenzivním zapojením do řešení celoevropského projektu EGEE (více viz samostatný text o tomto projektu dále ve zprávě). Aktivita MetaCentrum rovněž intenzivně spolupracuje s dalšími projekty, které přímo využívají budované gridové prostředí nebo je dále rozvíjejí specifickými požadavky (např. vývoj workflow a integrace ontologií v rámci projektu *MediGRID*).

Vlastní činnosti aktivity MetaCentrum lze obecně rozdělit do následujících oblastí:

Provoz: včetně nezbytného rozvoje výpočetních a datových zdrojů.

Uživatelská podpora: zajišťující kontakt mezi infrastrukturou (provozem) a vlastními uživateli; zprostředkovává rovněž zpětnou vazbu od uživatelů k vývoji.

Bezpečnost: zejména pak rozvoj nových přístupů, které vyvažují stále rostoucí potřeby zajištění bezpečnosti poskytované infrastruktury s požadavky a představami (a pohodlím) uživatelů.

Výzkum a vývoj: ve vybraných oblastech, zejména pak monitorování Gridů, tj. sledování provozních, spolehlivostních, výkonnostních a dalších charakteristik gridové infrastruktury.

V rámci aktivity MetaCentrum jsme se věnovali všem výše uvedeným oblastem, hlavní pozornost jsme v roce 2005 zaměřili na první dva, tj. provoz a uživatelskou podporu. Rozvoj bezpečnostní infrastruktury byl po většinu roku realizován v rámci samostatného projektu hardwarových tokenů Fondu rozvoje sdružení CESNET (hlavním řešitelem byla Masarykova univerzita). MetaCentrum výsledky projektu začalo přebírat od druhé poloviny roku. Výzkum byl úzce koordinován zejména s prací související se sítí excelence EU *CoreGRID*, do níž je zapojena Masarykova univerzita.

9.1 Provoz

Hlavním úkolem provozní skupiny MetaCentra je údržba a další rozvoj technického vybavení, které je tvořeno především výpočetními clustery, datovými kapacitami a zálohovacím zařízením. Provoz MetaCentra dále úzce spolupracuje s provozními skupinami jednotlivých uzlů (na ZČU, UK a MU) a garantuje tak plnohodnotné transparentní propojení lokálních a centrálně spravovaných výpočetních i úložných kapacit.

Veškeré výpočetní i datové zdroje MetaCentra jsou rozmístěny ve čtyřech lokalitách (všechny clustery jsou budovány z dual CPU uzlů s procesory Intel Pentium nebo AMD Opteron):

- V sídle sdružení v Praze Dejvicích je umístěn cluster *skurut*, jehož kapacity jsou využívány primárně v rámci mezinárodní spolupráce s projektem EGEE.
- V Praze na Ústavu výpočetní techniky UK na Ovocném trhu jsou do Gridu MetaCentra zapojeny výpočetní a diskové kapacity Univerzity Karlovy, především pak výpočetní systémy HAL, Mat a Acharon (všechny SGI) a související diskové kapacity (na ÚVT UK není umístěn řádný z vlastních clusterů MetaCentra).
- V Plzni na Západočeské univerzitě v Borech je umístěn výpočetní systém Pasifae (DEC/Compaq/HP) a clustery Nympha (vlastní cluster MetaCentra) a Minos (cluster patřící ITI ZČU spravovaný provozní skupinou MetaCentra).
- V Brně na ÚVT MU na Botanické ulici byly v roce 2005 k dispozici výpočetní systémy Eru, Grond a Gandalf a clustery Skirit (vlastní systém MetaCentra) a Perian (majetek NCBR MU ve správě MetaCentra). Je rovněž k dispozici dual CPU Power4+ počítač od IBM pro experimentální účely (majetek MetaCentra). Dále jsou na ÚVT k dispozici disková pole pro AFS (majetek MU) a rovněž pásková knihovna s kapacitou 12 TB nekomprimovaných on-line dat (majetek MetaCentra).

V průběhu roku došlo k postupnému vyřazení zastaralých systémů z provozu. Konkrétně šlo o počítače SGI s procesory MIPS (s výjimkou počítače Mat na UK) a počítač Pasifae na ZČU – výkon těchto strojů již neodpovídal současným požadavkům a očekávání uživatelů a jejich údržba již byla příliš drahá, případně ji výrobci zcela přestali poskytovat.

V roce 2005 nedošlo k významnému povýšení výpočetní ani diskové kapacity MetaCentra, investiční prostředky jsme použili primárně na plánovanou renovaci zálohovacího systému. Po předběžném průzkumu trhu jsme se rozhodli

nahradit stávající zálohovací systém založený na páskové knihovně o kapacitě 12 TB, která již přestala vyhovovat z kapacitních důvodů, páskovou knihovnou založenou na technologii LTO-3 (kapacita jedné pásky zde činí 60 GB). Zvolená technologie kromě vysoké úložné kapacity zajišťuje i dlouhodobou ochranu investic, neboť se jedná o novou technologii, která bude na trhu dostatečný počet let. Ve vypsaném výběrovém řízení vyhrála pásková knihovna *NEO8000* firmy Overland Storage s 500 úložnými pozicemi pro média. Nabídková cena umožnila nákup dvou rovnocenných knihoven, což poskytuje teoretickou kapacitu až 400 TB bez komprese.

Každá knihovna je vybavena čtyřmi páskovými mechanikami Hewlett-Packard Ultrium 3 a jedním výměnným mechanismem. Každý knihovna je obsluhována zálohovacím serverem (dual CPU AMD Opteron s 4 GB RAM), který je připojen třemi kanály SCSI Ultra320. Knihovny jsou umístěny v prostorách Západočeské univerzity v Plzni a Masarykovy univerzity v Brně a jsou ovládány kombinací zálohovacího software EMC Legato NetWorker a vlastními prostředky vyvinutého software (náhrada modulu Autochanger, viz dále). K serveru na ZČU je připojeno diskové pole EasySTOR 1606RPSA o kapacitě cca 8 TB, které slouží jako předřazená vyrovnávací paměť, umožňující provoz páskové knihovny s maximální rychlostí bez ohledu na rychlost přísunu dat přes počítačovou síť (zastavování pásek při nedostatečně rychlém přísunu dat negativně ovlivňuje životnost mechanik i médií i jejich využitelnou kapacitu). Analogické pole bude pořízeno v roce 2006 pro páskovou knihovnu v Brně.

V průběhu roku 2005 jsme vyvinuli programové vybavení, které nahrazuje funkce modulu *Autochanger* systému *Legato NetWorker* potřebné pro provoz páskové knihovny v našem prostředí. Tento postup jsme zvolili jednak z úsporných důvodů (cena příslušného modulu pro jednu páskovou knihovnu se pohybuje v řádu 1,2 milionu korun), jednak umožňuje přidání vlastních rozšíření pro správu médií, která by byla velmi obtížně integrovatelná, pokud by knihovnu řídil modul Autochanger. V příštím roce plánujeme další vývoj tohoto programového vybavení, především přidání funkce detailního sledování stavu mechanik a médií (chybovost, historie použití atd.).

Vytvořené distribuované řešení garantuje odolnost zálohovacího systému i proti „katastrofickým“ událostem, při nichž by došlo k úplné havárii jednoho z uzlů MetaCentra. Přestože výběrové řízení bylo vypsáno začátkem druhého čtvrtletí, zákonné lhůty umožnily dodání páskových knihoven až v prosinci. Do rutinního provozu tak budou uvedeny až v roce 2006, v současné době probíhá pouze experimentální ověřování celého systému.

Součástí budování infrastruktury národního Gridu bylo i připojení brněnského uzlu MetaCentra na vysokorychlostní optickou síť CzechLight, budovanou v rámci aktivity *Optické sítě*. Konkrétně byl v první polovině roku pořízen přepínač Cisco Catalyst 6506 vybavený 24 porty 1GE (gigabitový Ethernet), třemi 10GE

porty LAN PHY (pro napojení lokálních počítačů) a jedním zapůjčeným 10GE WAN PHY portem pro připojení do rozlehlé sítě (WAN). Přepínač byl připojen na 10 Gb/s trasu do Prahy, přes kterou se tak může brněnský uzel MetaCentra zapojit do mezinárodních vysokorychlostních aktivit (zejména prostřednictvím GLIF). Byla rovněž zakoupena jedna karta Chelsio T210 s akcelerovaným zpracováním TCP proudů s rozhraním 10GE. Vysokorychlostní připojení, zakoupené karty a přepínač byly intenzivně využívány při přípravě a vlastní realizaci demonstrace pro konferenci *iGrid 2005* v San Diegu a při dalších podobných demonstracích (podrobněji viz kapitola *Virtuální prostředí pro spolupráci*). V roce 2006 počítáme s využitím pro experimenty vysokorychlostního přenosu mezi páskovými knihovnami.

Skupina provozu se dále zabývala následujícími činnostmi:

- Zvýšení odolnosti celého provozu proti poruchám a výpadkům v jednotlivých uzlech. Jednalo se zejména o úpravy klíčových služeb a jejich konfigurací k odstranění závislostí, které nejsou nezbytně nutné. Konkrétně to bylo např. odstranění závislosti funkce obnovování kerberovských lístků a AFS tokenů (což jsou činnosti nezbytné pro spuštění každé úlohy v prostředí MetaCentra) na funkčnosti služeb systému Kerberos ve všech MetaCentrem obhospodařovaných realmech. Původní závislost vyplývá ze standardní implementace funkce vytváření AFS tokenů. Vylepšená implementace umožňuje spustit úlohu i v případě úplné- nedostupnosti některého realmu. Úloha se nespustí (a uživatel dostane hlášení o chybě) pouze v případě, že nedostupný je realm, který úloha nezbytně potřebuje.

  Další oblastí bylo posílení redundance služeb a vlastní oprava chyb používaného programového vybavení, zejména pak v systému plánování úloh *PBSPro*. Konkrétně jsme vytvořili repliky v AFS systému pro nejpoužívanější programové vybavení, což snižuje pravděpodobnost nedostupnosti v případě výpadku (či nedostupnosti) pouze některého souborového serveru MetaCentra (v průběhu roku 2005 došlo k několika neplánovaným výpadkům napájení, zejména v brněnském uzlu, které následně znemožnily spuštění úloh i v dalších uzlech). V případě systému PBSPro jsme pak opravili chybné plánování úloh pro subclustery s vlastností typu „switch“ – to jsou subclustery vnitřně propojené vysokorychlostní nízkolatenční sítí Myrinet, ale vzájemně propojené přes WAN IP sít – dále zhroucení celého plánovače při pokusu o spuštění velmi rozsáhlých paralelních úloh a vylepšení chybových hlášení tak, aby bylo možné snazší nalezení původní příčiny chyby. Rovněž jsme opravili chybný způsob analýzy některých příkazů v nástroji pro administraci, kde nebylo možné upravovat konfiguraci některých prostředků nabízenými nástroji. V systému *Heimdal* (volná implementace systému Kerberos, na jejímž vývoji se rovněž podílíme) jsme odstranili chybu v knihovně *libkrb525* ve funkci

pro automatické obnovování kerberovských lístků v dávkovém systému. Tato chyba způsobovala přeplnění tabulky souborových deskriptorů, což po jisté době používání vedlo k úplnému zhroucení dávkového systému. V systému Heimdal jsme dále odstranili chybu ve funkci pro zjištění adresy síťových rozhraní – tato chyba způsobovala náhodné zablokování procesů, využívajících služby systému Kerberos.

- Údržba provozního software, zejména pak plánovacích systémů, a odborná pomoc uživatelům s vlastními aplikacemi, především v oblasti přizpůsobení a optimalizace pro prostředí MetaCentra. Jednalo se především o konzultace o problémech, na jejichž zvládnutí již uživatelům nestačí pouhé pročtení poskytnuté dokumentace.

- Běžná správa clusterů, sledování stavu a řešení hardwarových závad. V průběhu roku 2005 přešel provoz MetaCentra na záznam všech problémů a výpadků v systému RT (Request Tracker) verze 3. Celkem bylo během roku 2005 založeno přes 200 lístků, z toho cca 100 uživateli (ostatní jsou interní, založené administrátory MetaCentra). Koncem prosince 2005 bylo v databázi RT systému 166 vyřešených lístků a 60 otevřených. Během roku bylo řešeno 15 hardwarových závad na vlastních clusterech MetaCentra a zhruba stejný počet závad na clusterech, které byly MetaCentru svěřeny do péče.

- Podpora vysokorychlostních experimentů na vysokorychlostní síti CzechLight.

Provoz MetaCentra spravuje a dále rozvíjí i systém *Perun*, vyvinutý v rámci předchozího výzkumného záměru sdružení CESNET. Tento systém slouží ke správě informací o uživatelích i některých komponentách Gridu a významným způsobem usnadňuje práci administrátorů a nepřímo i uživatelů (např. minimalizací chyb v osobních údajích). V roce 2005 jsme tento systém rozšířili o komponenty umožňující snazší („inteligentnější“) komunikaci s uživateli, nové možnosti autentizace (použití uživatelských certifikátů) a podporu virtuálních organizací. konkrétně se rozvoj systému Perun soustředil do následujících činností:

- Podpora virtuální organizace VOCE pro projekt EGEE. Vytvořili jsme nástroje pro zavádění a správu údajů o certifikačních autoritách a jejich šíření na jednotlivé stroje MetaCentra. Perun nyní spravuje i informace o uživatelských certifikátech, včetně údajů o jejich platnosti, rozdělení na jednotlivé stroje a rovněž příslušnosti k externím organizacím. Vytvořili jsme celou řadu nástrojů, které umožňují komunikaci mezi databází systému Perun a portálem VOCE. Tyto nástroje budou v dalším období zobecněny pro podporu nových virtuálních organizací a jejich portálů.

- Rozšíření portálu MetaCentra o podporu nových vlastností, zejména správu certifikátů, registraci do virtuálních organizací a dále nástroje pro uživatelské změny v účtech (např. změna interpretu příkazů, kvóty).

- Administrátorskou část jsme rozšířili o lepší práci s notifikacemi, především hlídání termínů vypršení účtů, opakování nevyřízených notifikací atd.

V roce 2005 jsme rovněž pokračovali v rozvoji monitorovacích nástrojů pro sledování stavu infrastruktury Gridu a v jejich postupném nasazení v provozních podmínkách. Vzhledem ke komplexnímu charakteru těchto činností jsou do nich zapojeni pracovníci prakticky všech skupin MetaCentra. Ve spolupráci se studentem FI MU (obhájená bakalářská práce *Monitorovací služba pro MetaCentrum*) jsme navrhli a implementovali rozšíření systému *Ganglia* pro potřeby MetaCentra, zejména pak možnost modulárního přidávání senzorů, možnost definovat formát ukládaných dat podle jejich typu a rovněž jednoduchou podporu pro notifikace podle nastavených podmínek (situace, událost atd.). Upravená verze systému Ganglia je instalována na všech clusterech MetaCentra, webové rozhraní je dostupné na adrese *http://lindir.ics.muni.cz/ganglia*. Informace získané ze systému Ganglia jsou samozřejmě dostupné i na portálu MetaCentra.

Systém Ganglia měřené hodnoty pravidelně publikuje pomocí multicastu na další uzly clusteru, čímž je zaručena spolehlivost i při výpadku jednoho uzlu. Vybrané uzly (zpravidla front-endy) pak ukládají naměřené hodnoty do databází (RRD, textové logy), což zpřístupňuje pomocí webového rozhraní i dlouhodobé statistiky provozu.

Aktuální informace o clusterech poskytuje i systém *PBSPro*, který má také informační proces na každém uzlu clusteru. PBSPro je sice primárně určen pro plánování úloh, pro tento účel ale potřebuje aktuální informace o uzlech, zaplnění disku a dalších charakteristikách, které může též zpřístupnit uživatelům. Hlavní rozdíl mezi informačními systémy Ganglia a PBSPro je v tom, že Ganglia poskytuje poslední naměřenou hodnotu, zatímco v rámci PBSPro je hodnota vygenerována na žádost (jako součást dotazu). PBSPro tak poskytuje jednak skutečně aktuální hodnoty, jednak může poskytovat i údaje, nedostupné přes systém Ganglia (např. velikost kvóty konkrétního uživatele na konkrétním stroji).

Protože se podpora notifikací v systému *Ganglia* ukázala jako nedostatečná pro potřeby plně distribuované správy (Ganglia je primárně určena pro sledování clusterů, ne celého Gridu), pracujeme na integraci systému Ganglia do standardního notifikačního nástroje *Nagios*. To nám umožní propojení s lokálně provozovanými instalacemi systému Nagios v jednotlivých uzlech MetaCentra a zrychlení reakce na výpadky a nepředvídané stavy.

9.2 Bezpečnost

Bezpečnostní skupina odpovídá za další rozvoj bezpečnostní infrastruktury MetaCentra. Ta je založena primárně na systému *Kerberos*, kdy je elektronická identita uživatele prokazována lístkem, vygenerovaným před prvním přistoupením k MetaCentru nebo v průběhu první autentizace. Zatímco se systém Kerberos používá jako výhradní bezpečnostní protokol *uvnitř* MetaCentra, doposud jsme uživatelům umožňovali použít i dvojici jméno/heslo při primární autentizaci např. do portálu nebo při přihlašování na jednotlivé výpočetní uzly pomocí *ssh*. K dispozici je rovněž přístup pomocí OTP (One Time Password), ten je však využíván primárně administrátory a nikoliv vlastními uživateli.

Důsledkem různých možností autentizace prvního přístupu je narušení principu SSO (Single Sign-On), tj. principu, v němž uživateli stačí prokázat svou identitu pouze jednou (pro určitý časový interval, zpravidla 8 hodin) při přístupu k prvnímu zdroji MetaCentra a při dalších přístupech je již využívána vygenerovaná (dočasná) elektronická identita. Dalším nedostatkem bezpečnostní infrastruktury MetaCentra bylo nedůsledné využívání možností PKI, tedy uživatelských certifikátů. Ty přitom představují převažující (či v řadě případů jediný) autentizační prostředek v rámci mezinárodní spolupráce. V roce 2005 jsme se proto soustředili na postupný přechod na důsledně SSO autentizační infrastrukturu, která je i nadále interně založena na systému Kerberos, ale která bude ve stále větší míře vyžadovat při autentizaci buď uživatelský certifikát (preferované řešení) nebo předem vygenerovaný TGT lístek systému Kerberos. Předpokládáme, že uživatelé tak budou přistupovat ke zdrojům MetaCentra již s připravenou elektronickou identitou, kterou budou používat všechny subsystémy MetaCentra.

V souvislosti s touto vizí jsme jednak v průběhu první poloviny roku odstranili nedůslednosti dosavadní implementace a postupně vytvořili jednotné autentizační rozhraní pro všechny služby MetaCentra. Ve druhé polovině roku jsme se pak soustředili na integraci technologie čipových karet a hardwarových tokenů do prostředí MetaCentra. Zde jsme navázali na výsledky projektu *Univerzální autentizace pomocí hw tokenů* Fondu rozvoje sdružení CESNET (hlavním nositelem projektu byla Masarykova univerzita, na projektu se dále podílela většina organizací zapojených do MetaCentra). Do produkčního provozu jsme nasadili rozšíření bezpečnostní architektury o podporu PKI (ta byla v roce 2004 pouze ve zkušebním provozu pro vybrané administrátorské aktivity). Pro uživatele MetaCentra jsme začali organizovat školení, v jejichž rámci jim přidělujeme hardwarové tokeny s jejich osobními certifikáty. Úzce spolupracujeme s Certifikační autoritou sdružení CESNET, na MU jsme ustanovili Registrační autoritu pro CESNET CA určenou pro uživatele MetaCentra a využívanou zejména během zmíněných školení.

Dále jsme rozvíjeli mechanismy vzájemné spolupráce bezpečnostních gridových architektur založených na protokolech Kerberos a PKI, vytvořili jsme mechanismy pro plnohodnotný přístup do prostředí MetaCentra s využitím uživatelských certifikátů případně jejich proxy variant. Všechna implementovaná řešení jsou dostupná na více platformách, přinejmenším v prostředí MS Windows a Linux. Ve spolupráci s provozní skupinou jsme rozšířili systém *Perun* tak, aby podporoval překlad uživatelských identit bez ohledu na uživatelem použitou autentizační metodu. Rozšířili jsme technologii hardwarových tokenů o generování proxy certifikátů z tokenů. Pro prostředí MS Windows jsme upravili knihovny *Globusu* a klienty *PuTTY* a *WinSCP* tak, aby přímo podporovaly použití certifikátů uložených na tokenech. Veškerý vyvinutý software je dostupný pod open licencí z portálu MetaCentra (pro uživatele vytváříme variantu Travelkitů známých z distribuce klientů systému Kerberos).

Provedli jsme nezbytné úpravy přístupových metod na portálu MetaCentra tak, aby podporovaly autentizaci přímo pomocí uživatelského certifikátu. Hlavní částí těchto úprav je modul pro podporu mechanismu Kerberos, jehož vývoj jsme zveřejnili na portále *SourceForge*[1] a který v současnosti patří k nejpoužívanějším modulům pro autentizaci Kerberem v prostředí http.

V závěru roku jsme se soustředili na podporu mobilních uživatelů, kterým poskytujeme možnost plnohodnotné práce na Internetu i zpoza restriktivních firewallů. Instalovali jsme *OpenVPN* server, autentizovaný pomocí uživatelských certifikátů, klientská část podporuje přímé použití hardwarových tokenů.

Bezpečnostní skupina dále v průběhu roku 2005 navázala spolupráci s dalšími skupinami, orientovanými na bezpečnost v síťovém (distribuovaném) prostředí. V rámci dalšího pokračování aktivit souvisejících s nasazením a dalším rozvojem čipových technologií jsme zahájili spolupráci se skupinou na FI MU a FIT VUT, která se zaměřuje na vývoj nových hardwarových tokenů. V rámci sdružení CESNET pak připravujeme spolupráci s aktivitou AAI pro vybudování jednotné národní AAI infrastruktury, která nebude rozlišovat mezi čistě síťovým a gridovým prostředím.

9.3 Uživatelská podpora

Skupina uživatelské podpory MetaCentra odpovídá za komunikaci uživatelů a pracovníků MetaCentra a současně poskytuje primární rozhraní pro řešení uživatelských problémů a požadavků. S ohledem na rozptýlení uživatelů po celé republice (a často i v zahraničí u mobilnějších uživatelů) jsou veškeré služby uživatelské podpory poskytovány prostřednictvím elektronických ná-

[1] *http://www.sourceforge.net/projects/modauthkerb/*

strojů, především portálu, systému zpracování požadavků a elektronické pošty, ve výjimečných případech i telefonicky.

Portál MetaCentra[2] byl radikálně přebudován již v průběhu roku 2004, v roce 2005 jsme se soustředili na jeho další rozvoj a rozšiřování. Portál má veřejnou (neautentizovanou) i soukromou (autentizovanou) část, v rámci autentizovaných stránek pak poskytuje i specifickou podporu administrátorům MetaCentra. Přebudovali jsme úvodní stránku portálu, která byla rozšířena o rychlý rozcestník odkazující na klíčové části a související projekty. Vylepšili jsme anglickou část portálu, která mimo jiné nyní umožňuje i generování anglické verze přihlášky v PDF (podle uživatelem zadaných údajů). Implementovali jsme automatické generování novinek a informací o výpadcích podle uživatelských preferencí. Tyto informace jsme současně rozšířili o možnost příjmu prostřednictvím RSS kanálu. Veškeré novinky a informace jsou generovány dynamicky a mají přiřazenu dobu expirace, po níž jsou automaticky staženy a uloženy do archivu. Aktuální informace jsou poskytovány vždy v české i anglické verzi.

Ve spolupráci s bezpečnostní skupinou jsme doplnili portál o autentizaci pomocí uživatelských X.509 certifikátů. V rámci podpory širokého využití hardwarových tokenů a zvýšení celkové bezpečnosti jsme se rozhodli postupně přejít na autentizační metody bez zadávání explicitního jména a hesla, s preferencí použití právě uživatelských certifikátů z tokenů. V sekci *Můj účet* jsme přidali tři nové položky – změna interpretu příkazů, změna kvóty a zaslání prioritního požadavku do RT systému – které jsou přístupné pouze po autentizaci uživatelským certifikátem. Postupně počítáme s přidáváním dalších služeb – např. přístup k plné historii požadavku v RT systému – a postupným zavíráním služeb dostupných autentizací pomocí jména a hesla. Současně chceme usnadnit celý proces přihlašování tak, že zájemci s již vygenerovaným certifikátem CESNET CA nebudou muset vyplňovat a zasílat papírovou přihlášku – registrace platného certifikátu bude plně postačující.

Na portálu MetaCentra jsme postupně doplňovali nebo aktualizovali dokumentaci k jednotlivým modulům a programovému vybavení, které je v rámci MetaCentra dostupné. Pozornost jsme soustředili zejména na doplnění anglických mutací.

Vytvořili jsme novou sekci portálu s názvem *USB tokeny*, která obsahuje veškeré informace nutné pro řádné použití hardwarových tokenů v prostředí MetaCentra. Uživatelé tak mají k dispozici kompletní dokumentaci pro inicializaci tokenu, vygenerování certifikátu nebo jeho nahrání, pokud již uživatel certifikát má, postup pro import a použití v prohlížečích Mozilla, Firefox a MS Internet Explorer. K dispozici jsou rovněž informace o použití USB tokenů v prostředí OS Linux, MS Windows, stejně jako spolupráce s Globus GSI aplikacemi. V této sekci je také

[2] *http://meta.cesnet.cz/*

k dispozici veškerý relevantní software. Celkem byla v roce 2005 uspořádána tři uživatelská školení v souvislosti s distribucí tokenů.

Vytvořili jsme formát (DTD) dokumentace programových modulů, který umožňuje generovat jak vlastní dokumentaci určenou pro portál, tak i nápovědu dostupnou on-line při přístupu ke konkrétnímu modulu.

Zatímco vlastní RT systém pro sledování požadavků je obhospodařován provozní skupinou MetaCentra, skupina uživatelské podpory třídí a přiděluje požadavky, které nemůže přímo vyřídit sama. Skupina rovněž odpovídá za eskalaci déle neřešených požadavků (statistiky jsou k dispozici v části věnované provozu MetaCentra). Zahájili jsme rovněž práci na integraci RT systému do jednotného SSO prostředí MetaCentra autentizací pomocí uživatelských certifikátů.

Uživatelská skupina dále zorganizovala přednášku zástupců John von Neumann Institute of Computing (NIC) z Juelichu (SRN), kteří prezentovali způsob přístupu k významným výpočetním zdrojům superpočítačového centra Juelich[3].

9.4 Další výzkumné aktivity

Kromě výzkumných a vývojových činností zmíněných v předchozích částech jsme se v rámci MetaCentra v roce 2005 věnovali dalšímu rozvoji systémů monitorování Gridové infrastruktury.

V první polovině roku jsme rozvíjeli architekturu decentralizovaného monitorování stavu gridových prostředků s robustním decentralizovaným ukládáním výsledků. Vycházeli jsme z toho, že klasický monitoring, realizovaný pravidelným testováním dostupnosti a funkčnosti prováděným centrálně z jednoho místa nevypovídá dostatečně o skutečném stavu gridové infrastruktury. Zkušenost s maticově prováděnými testy (např. spojení z každého stroje na každý, přenos dat mezi každou dvojicí strojů atd.) ukázala, že centrálně sbírané údaje mnohdy nevypovídají o tom, zda jednotlivé uzly Gridu budou vzájemně spolupracovat. Častým důvodem je nastavení firewallů, které jsou staticky nastavené pro konkrétní spojení, ale nejsou adaptovány na rychle dynamicky se měnící prostředí Gridu, zejména pak přidání nových strojů. I dříve povolená komunikace bývá zastavena, pokud nebyla delší dobu používána.

Navrhli jsme proto architekturu testovacích programů, nazvaných *červi (worms)*, které putují samostatně po strojích začleněných v Gridu a provádějí předepsané testy (chovají se tedy z pohledu Gridu jako standardní aplikace). Dohled nad červy, jejich řízení a sběr výsledků pak provádí další vrstva programů, zvaných *pastýři (shepherds)*. Pastýři jsou organizováni v peer-to-peer struktuře, s re-

[3] *http://www.fz-juelich.de/nic/*

dundantním ukládáním dat a možností převzetí spravovaných červů v případě výpadku některého pastýře.

Testy prováděné červy jsou tří druhů – jedno, dvou a tříbodové. Jednobodové testy zjišťují dostupnost nějaké služby nebo správnou konfiguraci na konkrétním stroji (na němž je červ aktuálně spuštěn). Příkladem je test na konfiguraci všech uznávaných certifikačních autorit.

Dvoubodové testy zjišťují dostupnost služeb na jiných strojích ze stroje, na němž se červ aktuálně nachází. Příkladem je test proveditelnosti *gsissh* spojení. Tříbodové testy pak zjišťují možnost využití dvojice jiných strojů, příkladem je řízení *gridFTP* přenosu souboru mezi dvěma jinými stroji. Kandidáty pro dvoubodové a tříbodové testy dostává červ prostřednictvím pastýře, případně je náhodně generuje z předem zadaného seznamu.

Červi testují gridovou infrastrukturu nejen vlastními testy, ale i samotným procesem plánování a spuštění – jakékoliv problémy jsou zaznamenány pastýři a nahlášeny.

Vlastní červi jsou velmi jednoduché programy, které mohou být spuštěny na strojích s libovolnou architekturou (od uzlů běžných clusterů přes SMP počítače až po vektorové superpočítače), prováděné testy jsou přidělovány pastýři. Selhání konkrétního testu (včetně nemožnosti jeho spuštění) nemá vliv na další činnost červa. Červi mohou být spouštěni pod libovolnou identitou (správce, konkrétní uživatel atd.), takže je možné identifikovat i problémy spojené pouze s konkrétními uživateli.

Testování pomocí červů lze kombinovat s výsledky pasivního monitorování (hlášení komponent gridové infrastruktury o běžném provozu). To umožňuje minimalizovat zátěž infrastruktury – např. není nutné testovat přenos mezi souborů mezi uzly, pokud mezi nimi v nedávné době uživatelé úspěšně přenesli své soubory.

Ve druhé polovině roku jsme se více zaměřili na další rozvoj architektury *C-GMA* jako obecného protokolu, zajišťujícího spolupráci konkrétních implementaci GMA. C-GMA značí *Capability-based Grid Monitoring Architecture* a je postavena na rozšíření konceptu producentů a konzumentů standardní Grid Monitoring Architecture o metadata v podobě atributů a vlastních capabilit. Každý datový proud (resp. každá událost) přenášený monitorovací architekturou, nese ve svých atributech i informaci o tom, jaké vlastnosti musí splňovat jednotlivé uzly monitorovací infrastruktury, aby jimi mohl být přenášen (např. se jedná o jedinečnou událost, která nesmí být ztracena – taková data mohou přenášet pouze uzly garantující persistenci). Jednotlivé komponenty pak publikují své schopnosti – capability. Je úkolem *mediátoru* najít odpovídající páry. Definicí specifických atributů je možno propojit dvě a více konkrétních implementací

GMA a definovat přechodové prvky, které mohou data mezi těmito implementacemi převádět.

Navrhli a publikovali jsme model se třemi úrovněmi abstrakce, současně máme k dispozici prototypovou implementaci mediátoru postavenou na použití specifické formy popisu metadat pomocí Classad. Tato implementace nám umožnila ověřit, že navržené současné srovnávání tří classadů – nezbytné pro složitější výběr celých skupin vzájemně spolupracujících komponent monitorovací infrastruktury – je funkční.

9.5 Shrnutí

Součinnost jednotlivých skupin aktivity MetaCentrum zajistila v roce 2005 další rozvoj národní gridové infrastruktury České republiky. Nezbytnost zajištění provozu indukovala výzkumné, vývojové a implementační činnosti, které dále přispěly k snazšímu využívání zdrojů MetaCentra, výraznému zlepšení interakce s uživateli a současně vedly k postupnému nasazování nových technologií.

Řada činností byla ovlivněna rozhodnutím přechodu na PKI autentizaci s využitím USB tokenů. Odpovídajícím způsobem jsme modifikovali portál MetaCentra, vytvořili jsme samostatné sekce, které jsou přístupné pouze po autentizaci uživatelským certifikátem. Organizovaná školení umožnila bližší kontakt s uživateli, zkušenosti jsme následně převedli do dalších verzí portálu a skladby zpřístupněných informací.

Vlastní portál jsme dále doplňovali o anglické verze stránek, orientaci v něm jsme usnadnili vytvořením navigačních prvků a centrálního rozcestníku. V roce 2005 jsme také začali důsledně využívat RT systém pro práci s uživatelskými požadavky i s vlastními úlohami provozu MetaCentra. Více jak 150 vyřešených lístků ukazuje intenzitu používání. Ta současně odhalila nezbytnost další definice interních politik při zpracování požadavků (přidělování lístků, procesy eskalace, kontroly, zpřístupnění historie lístků uživatelům) a rovněž vlastní práce s RT systémem (rychlé vyřešení konkrétního požadavku, případné administrátorské vygenerování souvisejících požadavků namísto „nabalování“ i souvisejících úkolů na původní lístek, který kvůli tomu zůstává trvale otevřený). Začlenění rozhraní RT systému do jednotného autentizačního procesu MetaCentra je dalším úkolem pro rok 2006.

V průběhu roku 2005 se rovněž podařilo úspěšně uzavřít výběrové řízení na páskovou knihovnu. Dosažená nabídková cena umožnila realizovat distribuované řešení s dvojnásobnou kapacitou proti původním předpokladům. To povede k realizaci velmi robustního zálohovacího systému MetaCentra s dostatečnou úložnou kapacitou.

V roce 2005 se také vyjasnily hranice spolupráce s výzkumným záměrem *Paralelní a distribuované systémy*, jehož nositelem je Masarykova univerzita, jmenovitě Fakulta informatiky a Ústav výpočetní techniky. Výzkum v oblasti plánování zdrojů bude nadále primárně realizován na MU, která se dále zaměří na využití gridového prostředí dle specifických požadavků vybraných aplikací (primárně zpracování obrazu), včetně nezbytného rozvoje nástrojů pro přenos aplikací na Grid. Vlastní výzkum v rámci MetaCentra se tak i nadále soustředí především na oblast bezpečnosti a na další rozvoj gridových monitorovacích architektur.

10 Virtuální prostředí pro spolupráci

Aktivita *Virtuální prostředí pro spolupráci* zastřešuje řadu dílčích projektů, jejichž základ tvoří multimediální přenosy dat vysokorychlostními sítěmi. Celou aktivitu lze rozdělit na část zabývající se synchronní komunikační infrastrukturou pro interaktivní komunikaci (tedy s požadavky na zpoždění, např. videokonference) a na část zabývající se asynchronními nástroji bez požadavku na omezení zpoždění. Tyto nástroje často pracují s jednosměrnými datovými přenosy. V obou částech se výzkum a vývoj pohybuje od čistě teoretického až po praktickou implementaci. V rámci aktivity také podporujeme provoz produkčního prostředí pro spolupráci.

10.1 Synchronní komunikační infrastruktura

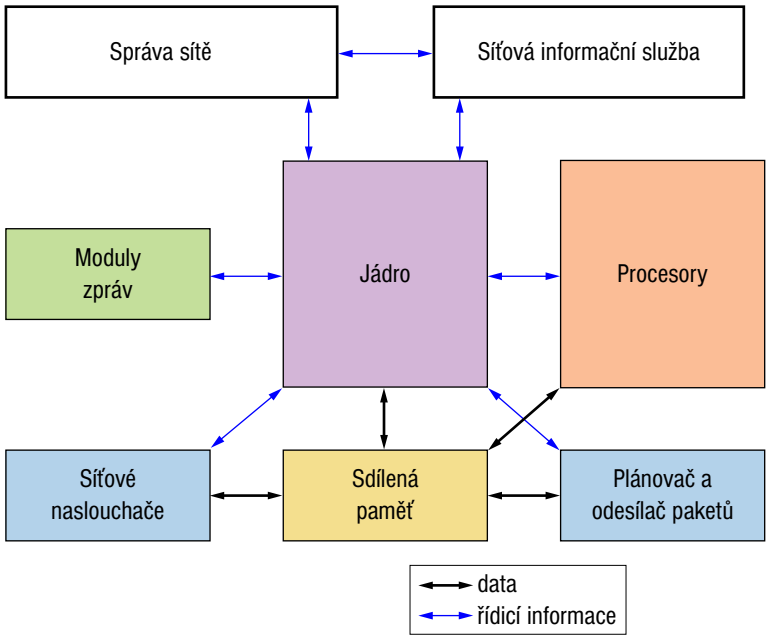
Hlavním problémem synchronního (též on-line nebo interaktivního) zpracování je vybudování prostředí včetně datových přenosů tak, aby bylo minimalizováno zpoždění. Soustředili jsme se na vybudování uživatelem řízené síťové podpory pro synchronní vícebodovou distribuci dat, která dobře škáluje vzhledem k počtu koncových bodů (klientů) a je dostatečně robustní s ohledem na možné výpadky linek i vnitřních prvků sítě. Tento výzkum navázal na náš vývoj aktivního (programovatelného) směrovače, reflektorů (replikačních prvků) a aktivních prvků, které byly založeny na stejných principech a myšlenkách.

10.1.1 Aktivní prvky

Virtuální spolupráce v reálném čase nezbytně potřebuje distribuční síť, která má vysokou přenosovou kapacitu a nízké zpoždění. Takovou síť je možné vytvořit z navzájem propojených obslužných prvků, tzv. *aktivních prvků (Active Element, AE)* – viz [HHM05]. Tyto prvky jsou zobecněním uživatelem řízeného programovatelného reflektoru popsaného v [HHD04]. Reflektor je programovatelný síťový prvek, který replikuje (a případně zpracovává) vstupní data (obvykle ve formě UDP datagramů) a rozesílá je klientům výhradně s použitím dvoubodového spojení (IP unicast). Jestliže jsou data zasílána všem naslouchajícím klientům, počet kopií je roven počtu klientů a množství odchozích dat nepřekročí $n(n–1)$, kde n je počet obsluhovaných klientů. Reflektor pracuje v uživatelském prostoru operačního systému, takže nevyžaduje administrátorská práva na hostitelském stroji. Jedná se tedy o aplikaci principu řízení uživatelem. Reflektor i

aktivní prvek jsou vytvořeny na základě návrhu aktivního směrovače [HlS01], modulárního přístupu a principu řízení uživatelem.

Aktivní prvky, na rozdíl od reflektorů, mají moduly pro vzájemnou síťovou komunikaci a schopnost distribuce modulů na úzce propojeném clusteru. Schopnost vzájemné komunikace je základem pro škálovatelné prostředí popsané v této zprávě. Výzkum distribuovaných aktivních prvků byl v tomto roce zahájen a hlavní výsledky očekáváme v roce následujícím. Systém řízení sítě je v aktivním prvku implementován dvěma moduly dynamicky připojenými v době běhu. Jsou to moduly pro správu sítě (NM) a pro síťovou informační službu (NIS), viz obrázek 10.1. NM zajišťuje vytvoření a řízení sítě aktivních prvků, přidávání nových skupin, odstraňování neaktuálních skupin a reorganizaci sítě v případě výpadků linek. NIS shromažďuje a zveřejňuje informace o jednotlivých prvcích (např. o volné kapacitě pro zpracování a zátěži linek), o sítích prvků, o vlastnostech důležitých pro synchronní multimediální distribuci (např. zpoždění mezi uzly sítě, RTT, odhadu kapacity linek) a informaci o obsahu a formátech dostupných na síti.



Obrázek 10.1: Architektura aktivního prvku s modulem pro správu sítě a modulem síťové informační služby

Pro odesílání řídicích zpráv se používají sítě samoorganizujících se aktivních prvků, známé jako P2P sítě. Řídicí zprávy se týkají informací o okolních aktivních prvcích, dostupných službách a obsahu, udržování topologie a kontroly a řízení datových kanálů. P2P princip řídicí sítě poskytuje robustnost i možnost řízení uživatelem. Malá efektivita této řídicí sítě nemá vliv na efektivitu samotné sítě

datové. Prototypová implementace využívá JXTA P2P prostředí [JXTA] a byla popsána v [HoH05].

10.1.2 Operace vyrovnání zátěže a reakce na chyby

Topologie typické sítě a způsoby jejího použití se často mění, proto překryvná síť musí tyto změny zohledňovat. Předpokládáme dva základní scénáře:

1. vyrovnání zátěže v síti je plánováno na základě změny způsobu použití nebo vzniku nových spojů či prvků, nikoli však výpadku linky nebo aktivního prvku
2. jako reakce na náhlý výpadek

V prvním případě infrastruktura obnoví a vyrovná zátěž v nové topologii a poté se převede do stavu zasílání dat. Proti tomu při náhlém selhání ve druhém scénáři dojde ke ztrátě dat (pro nezajištěný přenos, UDP) nebo zpoždění (pro zajištěné přenosy, TCP), pokud distribuční model neobsahuje stálé redundantní kapacity. Pravděpodobnost výpadku jednotlivých linek je poměrně malá oproti častým výpadkům, které jsou patrné při globálním pohledu na rozlehlé sítě. Proto je dvojnásobné jištění (k=2) pro většinu aplikací dostatečné a pro speciální aplikace je možné jeho zvýšení (k>2).

10.1.3 *Sítě aktivních prvků*

Oddělení řízení sítě od vlastní distribuce dat umožňuje implementovat více distribučních modelů s různými vlastnostmi. Studovali jsme několik modelů pro distribuci dat v sítích aktivních prvků [HHM05], které se lišily hlavně z pohledu robustnosti a výkonu:

úplná 2D síť: nejjednodušší model s vysokou robustností, takže selhání aktivního prvku ovlivnilo pouze přímo připojené klienty a minimalizovalo počet průchodů aktivními prvky

vrstvená 3D síť: tento model byl efektivnější než 2D model, ačkoliv si udržel schopnost obnovení a minimalizaci hopů

vrstvená 3D síť s mezilehlými AE: další zlepšení oproti 3D vrstvenému modelu, na které se lze dívat jako na přechod k topologii koster (spanning tree)

redundantní (minimální) kostry: model, který umožňuje maximální pružnost, efektivní zotavení při výpadcích sítě, optimalizaci distribuce dat s ohledem na vytížení linek; rozšíření na více redundantních koster přinese schopnost velmi rychlého zotavení po výpadku.

10.2 Interaktivní prostředí pro spolupráci s videem s vysokým rozlišením

Současné vysokorychlostní sítě umožňují přenos videa s vysokým rozlišením (HD video), jež lze využít jako nástroj pro mnoho aplikací. Provoz vskutku interaktivního prostředí s HD videem je dosud problematický, protože vyžaduje časové omezení zpracování ve prospěch interaktivity (nejlépe nižší než 100 ms), a proto data nelze komprimovat. Z toho samozřejmě vyplývají vysoké nároky na síťovou infrastrukturu, obzvláště pro vícebodovou distribuci dat, protože každý z datových proudů znamená tok 1,5 Gb/s. Během roku 2005 jsme vyvinuli a úspěšně předvedli prototyp nízkolatenčního vícebodového prostředí pro spolupráci s HD-SDI nekomprimovaným videem dle SMPTE 292M, které bylo též využito pro kolaborativní vizualizaci. Demonstrace ukázala, že celý systém je velmi zajímavým příkladem integrace špičkových aplikací infrastruktury optických sítí. Podrobné technické informace naleznete na adrese *https://sitola.fi.muni.cz/igrid/*.

Celý systém se skládá ze dvou základních částí: klientské aplikace a síťové distribuce včetně zpracování. Vyvinuli jsme klientské nástroje založené na kartách DVS Centaurus[1], Chelsio 10GE a programu *UltraGrid* Colina Perkinse [PGL02], který byl rozšířen o podporu plného 1080i HD videa (původní software podporoval pouze nižší rozlišení 720p) a softwarové zobrazování. Vzhledem k tomu, že karta Centaurus může být také použita pro zobrazování videa, rozšířili jsme UltraGrid pouze o podporu softwarového zobrazování včetně algoritmu pro deinterlace a podvzorkování barevného prostoru z 10 na 8 bitů na barevnou složku, abychom se vyhnuli nutnosti používat karty DVS Centaurus na obou koncích HD přenosu. Část UltraGridu zabývající se intenzivními výpočty a manipulací s daty byla optimalizována v assembleru pro procesor AMD64 (Opteron). Celkové zpoždění v laboratorních podmínkách, kde oba počítače byly připojeny na jeden 10GE přepínač Cisco Catalyst 6506, bylo 175 ± 5 ms a stále se snažíme o jeho další snížení.

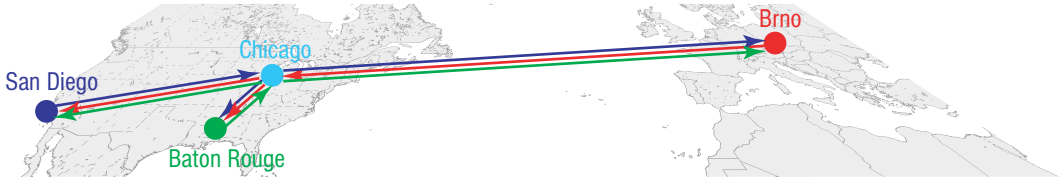
Distribuční síť bylo nutné doplnit o vícebodovou distribuci dat, abychom zajistili, že data od každého účastníka dostanou všichni ostatní. Kvůli nepříliš dobrým

[1] *http://www.dvs.de/english/products/oem/centaurus.html*

zkušenostem s vícebodovým vysíláním (multicast) v prostředí heterogenní sítě a heterogennímu vybavení jsme použili výše popsané aktivní prvky pro replikaci dat. Ověřili jsme jejich použitelnost v prostředí 10GE sítí, kde každý aktivní prvek replikoval datový proud 1,5 Gb/s od jednoho partnera dvěma ostatním na běžném PC se dvěma procesory AMD64.

10.2.1 iGrid 2005 demo

Workshop *iGrid* je konference konající se jednou za dva roky, kde se všechny zúčastněné týmy snaží ukázat nejpokročilejší aplikace využívající lambda služby a vysokorychlostní IP sítě. Na konferenci *iGrid 2005*, která se konala v září 2005 v San Diegu, USA, se CESNET účastnil dvou demonstrací: CZ101 (HD vícebodová konference organizovaná CESNETem) a US127 (Interaktivní dálkově řízená vizualizace přes LONI – Louisiana Optical Network – a National LambdaRail organizovaná Lousiana State University, LSU). V demonstraci CZ101 jsme ukázali využití nízkolatenčního prostředí pro spolupráci mezi partnery z CESNETu a Masarykovy univerzity v Brně, LSU v Baton Rouge v Luisianě a místem konání iGridu v San Diegu. Posílání 1,5 Gb/s datového proudu z každého místa znamenalo, že každé místo musí být schopno přijímat 3 Gb/s dat z ostatních dvou zdrojů, takže agregovaný datový objem na jedno místo činil 4,5 Gb/s. Vícebodová distribuce dat byla zajištěna třemi aktivními prvky v uzlu StarLight v Chicagu, kam ústily lambda služby ze všech tří míst. V demonstraci US127 byl přenos a distribuce vizualizovaných dat z Baton Rouge založen na stejném principu přenosu nekomprimovaného HD videa jak bylo popsáno výše, včetně vícebodové distribuce na aktivních prvcích v Chicagu.



Obrázek 10.2: Topologie experimentu pro iGrid 2005

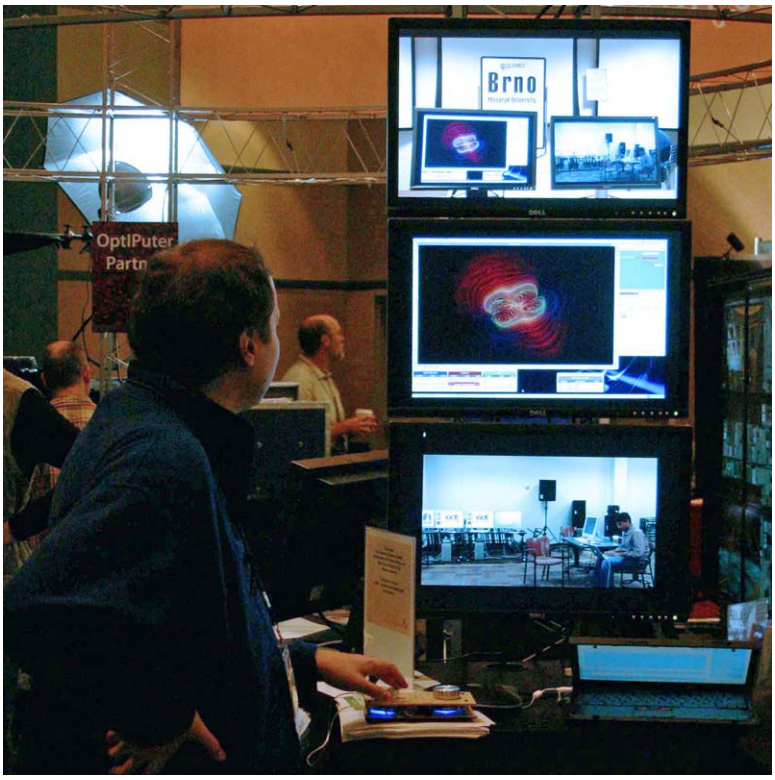
Během přípravy a realizace demonstrace, která vyžadovala úzkou spolupráci mezi aktivitami *Virtuální prostředí pro spolupráci*, *Metacentrum* a *Optické sítě* uvnitř CESNETu, ale také pečlivou koordinaci se síťovými partnery ze SurfNetu, StarLightu a National LambdaRail, se potvrdilo, že dnešní vysokorychlostní sítě postavené na lambda službách jsou velmi vhodné pro tento druh aplikací a přenos 4,5 Gb/s dat citlivých na ztráty a rozptyl zpoždění lze provádět bez vážných problémů.

Naše demonstrace na konferenci iGrid byla přijata mezinárodní komunitou velmi příznivě a byli jsme pozváni na další dvě akce: demonstraci interaktivní vizuali-

zace pro Dr. Jacka Marburgera, vědeckého poradce presidenta USA G. W. Bushe a předvedení téhož na konferenci *SuperComputing 2005*.

10.2.2 Demonstrace SuperComputing 2005

Další demonstrace, k níž jsme byli pozváni, se týkala opět distribuované interaktivní vizualizace a byla organizována týmem z LSU během konference *SuperComputing 2005*, která se konala v Seattle, USA. Podobně jako v demonstraci US127 byla vizualizační data generována na LSU v Baton Rouge a přes síť LONI distribuována do tří účastnících se míst. Každé místo bylo schopno spolupracovat na vizualizaci a měnit interaktivně její parametry díky speciálním periferiím – haptickým ovladačům vizualizace (viz obrázek 10.3). Díky přenosům obrazu a zvuku mezi jednotlivými místy bylo možné diskutovat o vizualizaci a analyzovat ji v reálném čase.



Obrázek 10.3: *SuperComputing 2005* demonstrace na stánku National Lambda-Rail

10.3 Aktivity proudování (streaming)

V roce 2005 jsme se soustředili na řešení následujících výzkumných a vývojových cílů:

1. rozvoj portálu pro živé přenosy
2. rozvoj portálu pro vyhledávání
3. proudování videa ve vysoké kvalitě

Zároveň jsme pracovali na podpoře akademické a výzkumné obce při proudování videa a snažili jsme se navázat spolupráci se subjekty mimo akademickou obec – podmínkou byla spolupráce na nových aplikacích síťových technologií.

10.3.1 Rozvoj proudovací infrastruktury CESNETu

Pokračovali jsme v rozvoji dle požadavků mezinárodní pracovní skupiny TERENA TF-VVC. Rozšířili jsme funkčnost o filtrování zobrazení podle jednotlivých jazyků a provedli jsme některé menší změny v uživatelském rozhraní. Zároveň jsme implementovali prototyp rozhraní pro integraci portálu do webových serverů pracujících s jiným zobrazováním. Prozatím se v rámci skupiny TF-VVC nepodařilo nalézt zájemce o implementaci. Portál pro živé přenosy prezentujeme na zasedáních TF-VVC a prezentaci jsme provedli také na konferenci DIVERSE, jejímž předmětem je využití audiovizuálních prostředků v oblasti distančního vzdělávání a e-learningu.

Vyhledávací portál jsme rozšířili o funkci náhledů. U každého multimediálního souboru, který portál indexuje, pořídíme náhledy v definovaných časech (0, 30, 50 s). Tyto náhledy následně převedeme do shodného formátu (PNG a JPEG) a rozlišení (96×72 bodů). K záznamu vydestilovaných metadat do databáze ukládáme i odkazy na náhledy. Vzhledem k rozšíření funkcí a plánovanému kvalitativnímu rozšíření zpracování dat (jiné typy vstupů) jsme se rozhodli prozatím neměnit datový formát systému. Srovnáním formátů MPEG-7 a Dublin Core jsme dospěli k závěru, že použití nekvalifikovaného formátu Dublin Core je pro náš účel vhodnější. Vyhledávač jsme rozšířili o další země. Nyní indexujeme domény *.cz*, *.dk*, *.sk*, *.hu*, *.nl*, *.pl* a část domény *.edu*. Celkově pracujeme s více než 2 000 000 unikátními adresami. Vzhledem k práci s metadaty si stále udržujeme náskok před systémy, které nasazuje komerční sféra. Vyhledávačům jako Google nebo Yahoo! nemůžeme konkurovat v oblasti objemu zpracovávaných adres, nicméně náš systém vyhledává s větší relevancí. Vyhledávač jsme prezentovali na konferencích Internet2 a DIVERSE.

V oblasti proudování ve vysoké kvalitě jsme se soustředili na dvě oblasti. První je nasazení systému vysílání v kvalitě PAL s velkou cílovou skupinou. Proto jsme navázali spolupráci se skupinou MAFRA, která provozuje hudební kanál *Stanice O*. Vysíláme ve dvou kvalitách. Cílem vysílání v nižší kvalitě je ověření proudování IPv6 v režimu dvojitého protokolového zásobníku (dual-stack) a proudování na mobilní platformy (PDA). Vysílání v PAL rozlišení (datový tok 1,5 Mb/s) pak slouží k ověření možností distribuce IPTV. Druhou oblastí je zpracování videa v HD rozlišení. Zde se orientujeme na zpracování HDV formátu (především rozlišení 1080i). V roce 2005 jsme povýšili produkční řetězec (střižny, diskové pole pro střih, proudovací servery) tak, aby pracoval s HDV formátem. Pokud je nám známo, jsme první organizací, která pracuje s HDV formátem v prostředí rozlehlé počítačové sítě.

Spolupráce s Českým rozhlasem úspěšně pokračuje. V roce 2005 jsme začali spolupracovat s novou na vědu orientovanou stanicí *Leonardo*. Pokračujeme v projektech podporujících přechod na digitální vysílání. Podíleli jsme se na přípravě projektu živého vysílání ze studia *Leonardo* (ve formátu RealVideo a OGG Theora) a jako každoročně se podílíme na dalších zajímavých projektech ČRo. Za zdůraznění stojí multimediální projekt *Odhalení – trochu jiná reality show*. Streamujeme experimentálně v OGG Theora jeden ze živých streamů a také zajišťujeme distribuci videa v plném PALu pro další zpracování v MPEG-2, transkódujeme do MPEG-4 a kombinací unicast, multicast dopravujeme na odběrová místa (např. výloha ČRo na Vinohradské třídě). V rámci projektu *Odhalení* jsme pokusně ověřili naše současné technické možnosti řešení ochrany distribuce digitálního obsahu ve vyšších bitových tocích. V této problematice chceme pokračovat i v dalším období.

10.4 Produkční infrastruktura a podpora

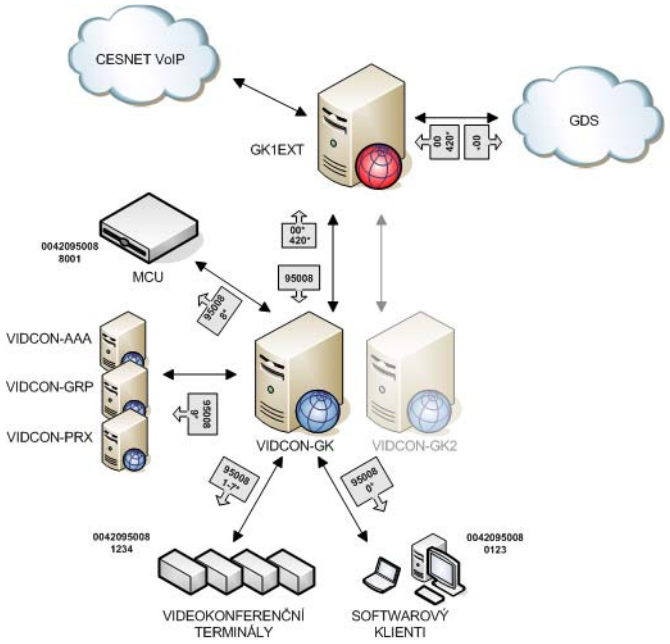
10.4.1 Proudovací infrastruktura

Proudovací platforma byla rozšířena o proudování ve formátu Ogg využívajícím kodek Theora. V současnosti má tedy akademická komunita k dispozici jednotnou platformu s těmito formáty: Real Video, Windows Media, MPEG-1/2/4, QuickTime a Ogg Theora. S tímto množstvím podporovaných formátů patří naše proudovací servery na přední místo v evropské akademické komunitě.

10.4.2 H.323 and SIP infrastruktura

V letošním roce jsme dořešili číslovací plán a přešli jsme plně na prefix 950 08 delegovaný aktivitou IP telefonie. Díky tomu jsme schopni plně komunikovat s organizacemi zapojenými do projektu *ViDe.Net*. Všechny H.323 komponenty

zakoupené v tomto roce jsou oživeny a integrovány do videokonferenční infrastruktury H.323 (viz obrázek 10.4), u většiny komponent máme k dispozici podporu H.323 i SIP.



Obrázek 10.4: H.323 infrastruktura

Vytvořili jsme podpůrné nástroje pro systém správy řízení zdrojů MCU pomocí Polycom XML API. Distribuujeme novou verzi personálního videokonferenčního klienta PVX s novými funkcemi pro podporu mobility a průběžně zajišťujeme aktualizaci programového vybavení videokonferenčních stanic a dalších prvků infrastruktury.

10.4.3 Přímá podpora

V přímé podpoře jsme se zaměřili na distribuci videokonferenčních klientů dle individuálních požadavků řešitelů, spolupráci při výběru komponent v jiných aktivitách, ověřování vlastností nových prvků videokonferenčních sestav a zajišťování technické podpory na vlastních akcích. Dále se zabýváme spoluprací při vývoji ovladačů těchto prvků pro OS Linux. Samozřejmou činností jsou konzultace v rámci CESNETu i pro další členy sdružení v oblastech AV technologií.

11 Podpora distančního vzdělávání

Základním cílem aktivity *Podpora distančního vzdělávání* je kvalitativní posun elektronické podpory výuky na vysokých školách s maximálním využitím současných možností v oblasti progresivních síťových i lokálních digitálních technologií, jako jsou nástroje pro záznamy, zpracování, ukládání a prezentaci multimediálních dat a nástroje pro vzdálenou spolupráci.

Aktivita vyvíjí metodiku, pilotní projekty a příklady využití zmíněných technologií ve výuce tak, aby byly reprodukovatelné v širším rámci sdružení CESNET. Aktivita zasahuje rovněž širokou studentskou obec, která se vzdělává na vysokých školách v oblasti technických a přírodních věd.

11.1 Údržba a rozšiřování portálu eLearning.cesnet.cz

V předchozím období jsme uvedli do provozu portál *eLearning.cesnet.cz* a provedli jeho technickou revitalizaci, včetně stanovení postupu jeho dalšího rozvoje.

Revitalizace spočívala jednak ve vytvoření nové struktury, designu a dále vlastní obsahové náplně. Průběžně jsme také doplňovali vybrané aktuality.

V současné době je dokončeno technické řešení. Hlavním úkolem pro příští rok je věcná revitalizace, tj. zvýšení atraktivity portálu (pravidelně doplňované aktuální informace, klíčové články o eLearningu, návody, zkušenosti, prostor pro publikování příspěvků). Tohoto stavu je možné dosáhnout zejména zvýšením počtu renomovaných přispěvatelů.

Portál jsme představili na několika konferencích formou samostatného příspěvku.

11.2 Standardy v oblasti eLearningu

Vytvořili jsme API v jazyku Java pro práci s testy podle specifikace IMS QTI a systém pro vizuální tvorbu těchto testů.

Dále jsme vypracovali návrh a započali práce na implementaci systému pro indexování a prohledávání videozáznamů přednášek, který je založen na technologiích rozpoznávání mluvené řeči.

Z hlediska softwarové architektury systémů řízení výuky jsme věnovali pozornost především adaptivním a personalizovaným systémům a jejich vztahu ke standardům sdílení obsahu výukových objektů (např. SCORM). Identifikovali jsme možnosti personalizace adaptivity standardizovaných výukových objektů a navrhli příslušné architektury.

Zpracovali jsme možnosti využití synchronizace streamovaného videa s ostatními typy médií (text, obrazy, animace) v prostředí systémů pro podporu výuky (LMS Class Server).

11.3 Blended-learning a metodiky nových postupů

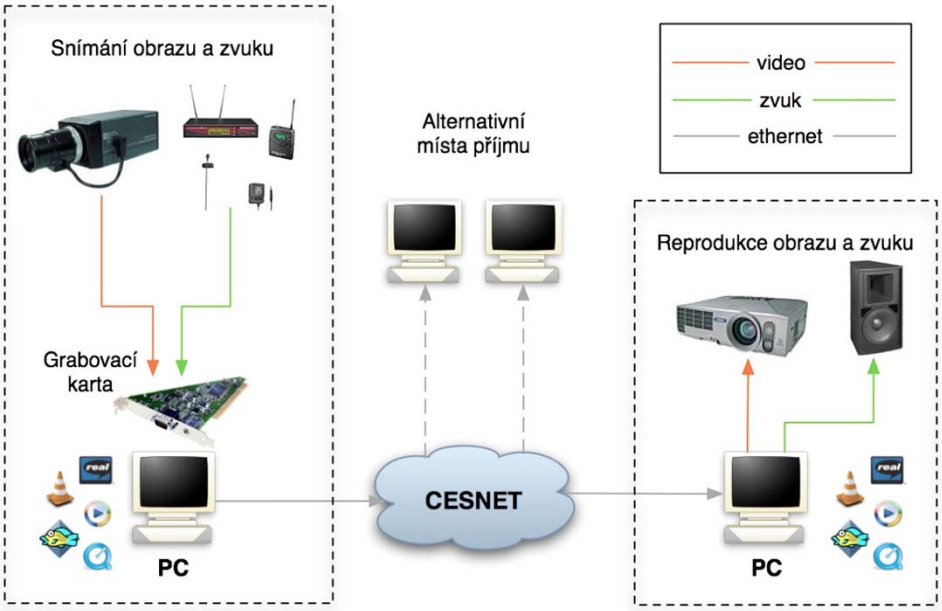
Z Univerzity ve Vídni byl převzat a adaptován systém *CEWebS*. Na něm jsme ověřili některé vzory pro blended-learning a systém je používán pro týmové studentské projekty. Pro účely rozšiřování CEWebS i dalších projektů jsme sestavili prostředí pro řízení javových softwarových projektů na bázi systému Maven.

Analyzovali jsme architekturu CEWebS a naplánovali společné práce na jeho vývoji a aplikacích ve výuce. Připravili jsme školení Jürgena Manglera k architektuře a použití rámce CEWebS. Cílem bylo přenést znalosti nutné k tvorbě vlastních webových služeb pro CEWebS a k modifikacím jeho architektury.

Na základě podrobného seznámení s architekturou CEWebS bylo možné v průběhu podzimního semestru použít tento rámec pro elektronickou podporu výuky a současně na něm realizovat pokročilé studentské výukové softwarové projekty. Ověřili jsme možnost psát pro CEWebS webové služby v Javě nezávislé na platformě. Na zprovozněných instancích systému CEWebS v Brně a Vídni byly testovány existující i nově vytvořené webové služby z hlediska robustnosti a výkonu.

V oblasti vývoje metodiky pro optimální komunikaci klientů ve zpětném směru jsme navrhli dva základní přístupy: ryze textovou komunikaci a řízenou hlasovou, popř. obrazovou komunikaci uživatelů ve zpětném směru. Pro řízení hlasové komunikace lze využít navrženého webového systému (založeného na technologii Java). Obrazová, tedy plně interaktivní komunikace, je založena na principu virtuálních místností na společném serveru.

V oblasti metodiky nových postupů v oblasti eLearningu jsme se v tomto období věnovali převážně následujícím činnostem: První z nich bylo najít vhodnou formu technického řešení sdílené přednášky. Možností se nabízí několik, od nejdražších až po ty běžné, spojené většinou s operačním systémem uživatele. Rozhodujícím faktorem tohoto výběru byla jednak technická vybave-



Obrázek 11.1: Technická realizace jednosměrně sdílené přednášky

nost potenciálních účastníků a v druhé řadě i typ dané přednášky/konference. Z toho také vzešlo několik jednoduchých metod a postupů pro komunikaci účastníků/studentů s přednášejícím. Dalším rozhodujícím faktorem, který bylo třeba vzít v úvahu při výběru jednotlivých metodik, je samotný obsah přednášky/konference (ukázka detailů apod.). Předpokládáme, že problematikou komunikace ve zpětném směru se budeme zabývat i nadále v dalším období. Z této problematiky vznikla rozsáhlá technická zpráva (16/2005), která definuje některé základní pojmy a dopodrobna ukazuje jednotlivá technická řešení.

Na obrázku 11.1 je znázorněna technická realizace jednosměrně sdílené přednášky s použitím softwarových streamingových prostředků. Kamera a mikrofon snímající přednášejícího jsou přes digitalizační grabovací kartu připojeny k PC. Zde je signál komprimován a odesílán na streamovací server, jenž jej dále distribuuje všem klientům, kteří si zažádají o spojení. K tomuto účelu lze použít celou řadu softwarových produktů (záleží na požadovaném formátu výstupního toku).

Další činností, kterou jsme rozvíjeli v první polovině roku, byla optimalizace mobilního pracoviště pro zavedení bezdrátových přenosů videosignálu. Pro bezdrátový přenos videosignálu jsme pro experimentální provoz použili zařízení GigaLink. Existuje pro ně rozhodnutí o schválené technické způsobilosti rádiového zařízení k provozu v ČR (ČTÚ 1998 1 r 790). Rádiový (bezdrátový) přenos se uskutečňuje v pásmu 2,4 GHz. Pásmo (2,4–2,4835 GHz) je rozděleno na 5 kanálů s roztečí 14 MHz. Systém jsme volili s ohledem na místo kde bude

obvykle používán. Ve většině případů se jedná o rozsáhlé místnosti, kde tento systém dosahuje objektivní kvality přenosu signálu na vzdálenost 30 m. Systém byl mimo jiné nasazen v nepřetržitém dvoudenním provozu na konferenci *EMTECH 2005*, ze které byl po celou dobu pořizován videozáznam. Systém se osvědčil zejména díky své vysoké mobilitě.

12 CESNET CSIRT

Spolu s nárůstem počtu uživatelů, kteří mají přístup do celosvětové sítě Internet, stoupá i počet bezpečnostních incidentů, jichž se uživatelé dopouštějí svou nedbalostí, neznalostí nebo úmyslně. Přitom požadavky na bezpečnost sítí a služeb vzhledem k vývoji Internetu, provozovaným aplikacím a charakteru přenášených dat neustále rostou. Proto je nutné se otázkám počítačové bezpečnosti systematicky věnovat, řešit vzniklé bezpečnostní incidenty a snažit se jim pokud možno předcházet. Tento nelehký úkol mají v rámci svých domovských organizací za úkol tzv. *bezpečnostní týmy*. V rámci sdružení CESNET působí od roku 2004 bezpečnostní tým CESNET-CERTS.

12.1 Aktivity CESNET-CERTS týmu

CESNET-CERTS tým[1] byl vytvořen na přelomu let 2003 a 2004, oficiálně existuje od ledna 2004, kdy jsme jej formální cestou deklarovali v mezinárodním kontextu jako CSIRT (Computer Security Incident Response Team) tým a zveřejnili jeho existenci v rámci aktivity TF-CSIRT[2], kterou zaštituje organizace TERENA[3]. Aktivita TF-CSIRT má za cíl vytvořit v Evropě síť národních a institucionálních bezpečnostních týmů, které spolu úzce spolupracují na prevenci a řešení bezpečnostních incidentů. Důraz je kladen zejména na osobní kontakty, znalost členů ostatních týmů a sdílení a předávání informací.

Členy týmu CESNET-CERTS se v roce 2004 stali tři zaměstnanci sdružení, kteří k práci v bezpečnostním týmu měli vzhledem ke svému dosavadnímu pracovnímu zaměření v rámci sdružení nejblíže. Základními aktivitami týmu se staly následující činnosti:

- příjem a řešení bezpečnostních incidentů sítě CESNET2
- rozvoj a provoz IDS (Intrusion Detection System) a Audit systému
- bezpečnostní strategie provozu služeb (např. antispamová a antivirová ochrana)
- tvorba a realizace strategie bezpečnostních otázek v síti CESNET2
- osvětová činnost v síti CESNET2

CESNET-CERTS se snaží aplikovat získané poznatky ve prospěch celé sítě CESNET2 a cílově dosáhnout lepší organizovanosti při řešení bezpečnostních otázek v síti CESNET2.

Nyní po dvou letech existence týmu a po rozšíření aktivit se počet tří členů ukazuje jako nedostatečný. Příjem a zpracování hlášení bezpečnostních inci-

[1] *http://www.cesnet.cz/csirt/*
[2] *http://www.terena.nl/tech/task-forces/tf-csirt/*
[3] *http://www.terena.nl/*

dentů členům CESNET-CERTS zabírá hodně času, a přitom v převážné většině vyžaduje jen použití zdravého selského rozumu a znalost základních principů Internetu (IP rozsahů, domén).

CESNET-CERTS tým je totiž hlavním kontaktem pro řešení bezpečnostních otázek pro celou síť CESNET2, tzn. pro autonomní systém AS2852. V roce 2005 přijal CESNET-CERTS přibližně 800 hlášení bezpečnostních incidentů, která bylo třeba přeposlat koncovým správcům připojených organizací se žádostí o vyřešení.

Každého asi napadne, proč nejsou incidenty hlášeny přímo do koncových institucí. Na tuto otázku není tak snadné odpovědět. Částečně je to způsobeno historickým vývojem Internetu – řada systémů pro hlášení incidentů se plní staticky a nedokáže tedy reflektovat změny kontaktních informací v databázích regionálních internetových registrátorů a registrátorů domén. Je proto běžné, že takovéto systémy celá léta nejsou schopny zaznamenat změny v kontaktních informacích přidělených IP rozsahů. A částečně se jedná o úmysl – hlášení o incidentu se cíleně posílá na hlavní kontakt pro řešení bezpečnostních incidentů daného autonomního systému. V případě sítě CESNET2 je to adresa *abuse@cesnet.cz*, kterou přijímá a vyřizuje tým CESNET-CERTS.

Abychom udrželi kvalitu své práce a měli čas na další rozvoj, rozhodli jsme se tým posílit. Jako optimální řešení nás napadlo začlenit do něj pracovníky CESNET Monitoring Centra (CMC). Jedná se o pracoviště s nepřetržitým provozem (24 hodin denně, 365 dní v roce), které má na starosti dohled nad sítí CESNET2 a koordinaci při řešení výpadků sítě a provozovaných služeb. Naším cílem je přesunout příjem hlášení incidentů, základní analýzu a zpracování incidentu na CMC.

Z tohoto důvodu jsme se v letošním roce pustili do prozkoumání možností, které nabízí tiketovací systémy. Používají se na příjem hlášení incidentu, jeho zpracování a zaznamenání postupu při řešení. Tři lidé zvyklí spolupracovat, jako je to v případě tří členů CESNET-CERTS, se totiž ještě pohodlně dokáží domluvit na pravidlech při elektronické komunikaci, ale u většího počtu lidí je potřeba systém odolný proti chybám, aby nedocházelo ke ztrátě důležitých dat, intuitivní pro ovládání a v neposlední řadě autentizovaný a autorizovaný.

V průběhu roku jsme otestovali téměř desítku tiketovacích systémů a dlouho se zdálo, že žádný našim nárokům nevyhoví. U těch, které se nám svými funkcemi nejvíce líbily, bohužel chyběla podpora S/MIME a PGP, které jsou pro naši práci vzhledem k ochraně identity a integrity obsahu nezbytné. Zvažovali jsme nasazení webového poštovního rozhraní, nebo doprogramování funkčního rozhraní do poštovního klienta Thunderbird. Nakonec jsme se ale rozhodli pro nasazení již v loňském roce testovaného systému *OTRS (Open Ticket Report System)*, a to především proto, že jeho vývoj začal jít prudce vpřed a v posledních měsících do něj byla implementována podpora S/MIME a PGP. Nyní systém OTRS

běží ve zkušebním provozu a plánujeme jeho nasazení na CMC. Přesun fáze příjmu a přeposlání incidentu koncovému správci zodpovědnému za danou síť na pracovníky CMC bude mít navíc ten pozitivní efekt, že se k cílovému správci dostane mnohem dříve, protože služba CMC je nepřetržitá.

12.1.1 Vývoj bezpečnostní strategie pro síť CESNET2

V prvním pololetí roku 2005 jsme při řešení bezpečnostních incidentů získávali zkušenosti, jež nám posloužily hned v několika oblastech. Ke zlepšení práce týmu, definování základních pravidel a postupů při řešení bezpečnostních incidentů, které se finálně staly základem interní politiky CESNET-CERTS týmu. Dále jsme všechny získané zkušenosti použili pro realizaci odborného semináře cílově zaměřeného na správce sítí a výpočetní techniky CESNET2 a odborníky zabývající se bezpečností sítí a služeb. Seminář s názvem „Bezpečnost na síti“ se konal 14. listopadu 2005 v Konferenčním centru v Dejvicích a zúčastnilo se jej více než 40 zástupců z institucí připojených k síti CESNET2.

Skladbu a náplň přednášek jsme koncipovali tak, abychom zúčastněným podali základní přehled problematiky bezpečnosti počítačových sítí a služeb, možnosti předcházení bezpečnostním incidentům, vytvoření bezpečnostního týmu v rámci instituce a jeho činnosti. Do programu jsme zařadili také přednášku na téma „Právní aspekty spojené s bezpečností sítí a služeb na ní provozovaných“. V roce 2005 se na seminářích řešitelů výzkumného záměru a při komunikaci mezi CESNET-CERTS a koncovými správci ukázalo, že nastal pravý čas, aby do této problematiky vnesl vhodnou formou jasno erudovaný odborník a dále se nešířily mylné představy o stavu českého a mezinárodního práva komolenou ústní formou.

Dále jsme v tomto roce pracovali na vývoji dokumentů definujících bezpečnostní politiku sítě CESNET2. Vzhledem k akademickému charakteru sítě jsme se rozhodli dát členským organizacím možnost se na tvorbě politik a jejich zavádění do praxe aktivně podílet. V posledním čtvrtletí bylo vytvořeno fórum složené z vybraných odborníků členů sdružení CESNET, kteří v roli zástupců svých domovských institucí budou mít možnost oponovat navržené politiky a další plány, jež v oblasti řešení bezpečnostních incidentů v síti CESNET2 připravujeme. Bezpečnostní politiky by měly být nasazeny do praxe v průběhu roku 2006.

12.1.2 IDS a Audit systém

V oblasti IDS systému v roce 2005 pokračoval vývoj programů pro analýzu dat získaných ze serveru *LaBrea*[4] v dejvické síti CESNETu. Tento stroj zaznamenává a brzdí útoky směřující do dosud nealokovaného adresového prostoru CESNETu. Data o zaznamenaných útocích se zpracovávají dvakrát denně (pouze v pracovní dny) a poté se automaticky rozešlou upozornění správcům těch sítí CESNET2, z nichž útoky pocházely. Užitečnost této služby lze posoudit např. podle toho, že za posledních 5 měsíců roku 2004 byly zaznamenány útoky z 590 strojů, za prvních 5 měsíců roku 2005 z 202 strojů a za posledního 6,5 měsíce (1. 6.–13. 12. 2005) z 204 strojů připojených k síti CESNET2 – navzdory stále rostoucímu počtu bezpečnostních incidentů v celosvětovém Internetu a navzdory tomu, že frekvence rozesílání upozornění se od konce října zdvojnásobila. Na vývoji a rozšíření systému pro automatickou detekci nekalých síťových aktivit budeme pokračovat i následujících měsících.

Dále jsme se soustředili na vývoj systému pro bezpečnostní audit strojů CESNETu a zabezpečeného poštovního rozhraní k serveru *NESSUS*[5]. Zabezpečené poštovní rozhraní je v dejvické síti CESNETu ve zkušebním provozu, takže umožňuje libovolnému jejímu uživateli jednoduše detekovat potenciální problémy v zabezpečení počítače bez nutnosti instalovat klienta nebo server NESSUSu. Uživatelé si jeho prostřednictvím mohou požádat o audit svého stroje a tím si otestovat jeho zabezpečení. Pokročilí uživatelé mohou samozřejmě i nadále využívat grafického nebo řádkového klienta instalovaného na některém svém počítači. Předpokládáme další vývoj systému podle potřeb uživatelů a nabytých zkušeností.

[4] *http://labrea.sourceforge.net/*
[5] *http://www.nessus.org/*

13 Medicínské aplikace

V průběhu roku 2005 byly v rámci aktivity řešeny následující projekty:

- Standardní prostředí medicínských aplikací
- Medicínské aplikace v návaznosti na GRID technologii
- Medicínské aplikace v rámci projektu CzechLight
- Rozvoj projektu MEDIMED

Na aktivitě se přímo podíleli pracovníci Masarykovy univerzity v Brně a 2. Lékařské fakulty UK v Praze. V rámci pracovních skupin při řešení jednotlivých projektů a přípravě společných projektů na další období spolupracovali pracovníci EuroMISE (společné pracoviště Akademie věd ČR a UK Praha), Ústavního soudu v Brně, Vysokého učení technického v Brně, Fakultní nemocnice u sv. Anny, Fakultní Thomayerovy nemocnice, Ústřední vojenské nemocnice, Masarykova onkologického ústavu, Masarykovy nemocnice v Ústí nad Labem, Univerzity Palackého v Olomouci, Univerzity Karlovy, Fakultní nemocnice Na Bulovce, nemocnice Znojmo, Městské nemocnice v Litoměřicích, nemocnice Hořovice a společnosti Medtel o. p. s. Vývoj specializovaného technického i programového vybavení probíhal ve spolupráci s firmou TatraMed s. r. o. z Bratislavy, IMA s. r. o. a Intercom Systems a. s. z Prahy.

13.1 Standardní prostředí medicínských aplikací

V prvním pololetí jsme vytvořili na základě spolupráce s pracovištěm EuroMISE centrum Ústavu informatiky AV ČR základní interní materiál „Vybrané právní aspekty vedení zdravotnické dokumentace a telemedicíny z českého a evropského pohledu“. Další pokračování tohoto úkolu bylo zahájeno od 1. 10. 2005 formou doktorandské práce na téma „Právní aspekty elektronické komunikace v telemedicíně“ v oboru Biomedicínská informatika na 1. LF UK, kde je vedoucí aktivity školitelem. Důležitá je rovněž možnost právních konzultací u doc. JUDr. P. Matese z VŠE, který se touto problematikou zabývá.

13.2 Medicínské aplikace v návaznosti na gridové technologie

Další vývoj v oblasti medicínských aplikací v návaznosti na GRID technologie probíhal v koordinaci s projektem programu Informační společnost Akademie

věd *MediGRID*. Další dva mezinárodní projekty *EuroCareCF* (výzkum v oblasti cystické fibrózy – genetické systémové onemocnění řady tkání lidského těla) a *MedGeNet* (podpora výzkumu thalasémie – geneticky podmíněné onemocnění krvetvorby) byly připraveny v rámci kapacit této aktivity. V případě úspěšného podpisu smluv bude další řešení probíhat v rámci aktivity *Virtuální prostředí pro spolupráci*, a to s ohledem na požadovanou technologickou podporu.

13.3 Medicínské aplikace v rámci projektu CzechLight

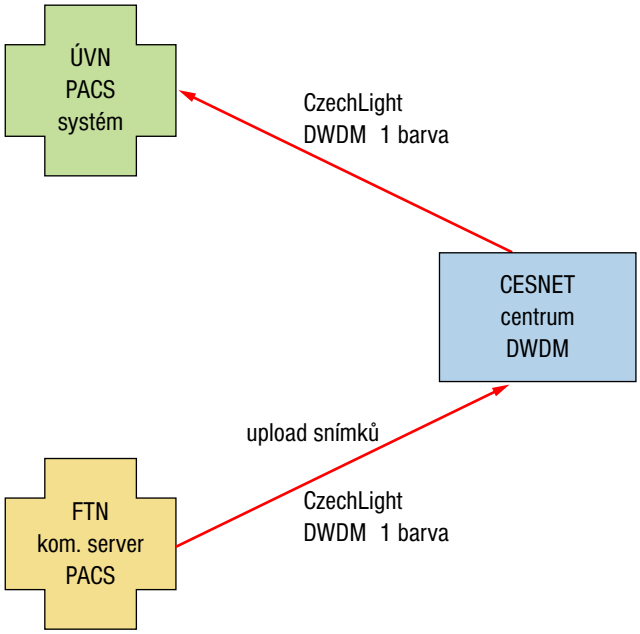
Původní záměr vytvořit komunikační infrastrukturu pro Centrum buněčné terapie byl ovlivněn zpožděním, ke kterému došlo při napojování klíčové lokality FN Motol na optickou síť. Hlavní překážkou byla stavební uzávěra vyhlášená v souvislosti s výstavbou nového energocentra. Dalším limitujícím faktorem byla migrace síťové infrastruktury nemocnice z ATM na technologii gigabitového Ethernetu koncem letošního roku.

K podobné situaci došlo v případě původně plánovaného propojení tří fakultních nemocnic v pražské lokalitě a vytvoření jednoho komunikačního celku. Ke komplikaci došlo s ohledem na změnu řízení pražského zdravotnictví, která odpovídala změnám na Ministerstvu zdravotnictví ČR. Původní záměr propojit Všeobecnou fakultní nemocnici na Karlově náměstí s Fakultní nemocnicí na Bulovce a Fakultní Thomayerovu nemocnici v Krči do jednoho „virtuálního“ celku platil asi jeden rok. Během této doby byly zahájeny aktivity, které měly umožnit vytvořit dostatečně propustnou infrastrukturu těchto propojených nemocnic. Ke změně došlo těsně před podpisem příslušných smluv a v současné době se jednotlivé nemocnice vrací k modelu samostatného fungování.

Další vývoj byl z hlediska komunikační infrastruktury popsán v kapitole *Optické sítě*. V této části budou zmíněny pouze záležitosti týkající se vlastních medicínských aplikací. Nad připravenou infrastrukturou lze uskutečnit řadu experimentů, ale v současné době jsme se zaměřili na následující dvě aplikace.

Prvním okruhem je problém *konzultací*. Z napojených nemocnic projevila velký zájem v této oblasti Fakultní Thomayerova nemocnice (FTN), která potřebuje neurochirurgické konzultace v Ústřední vojenské nemocnici ve Střešovicích (ÚVN), protože ošetřuje komplikovaná polytraumata (nejčastěji oběti dopravních nehod) a nemá svůj neurochirurgický tým. Často stojí před rozhodnutím, zda pokračovat v léčbě v rámci úrazové chirurgie, nebo předat pacienta na neurochirurgické oddělení k neodkladné operaci. Jejich požadavek na konzultace přináší z organizačního hlediska řadu problémů. Přenos dat musí být dostatečně rychlý a spolehlivý. Musí být zajištěno zabezpečení přenášených pacientských

dat. Další nekompromisní, ale na druhou stranu pochopitelný požadavek specialistů v ÚVN je, že konzultace pro FTN je nebude příliš zatěžovat. Lékaři proto požadují, aby konzultovaný snímek mohli zpracovávat ve svém standardním prostředí. Z hlediska nemocničních informačních systémů se jedná vlastně o systém uploadu, kde snímky přicházející z FTN se zařazují do systému ÚVN, jako by se jednalo o snímky z jednoho jejich specializovaného oddělení. Základní schematické zobrazení je uvedeno na obrázku 13.1.



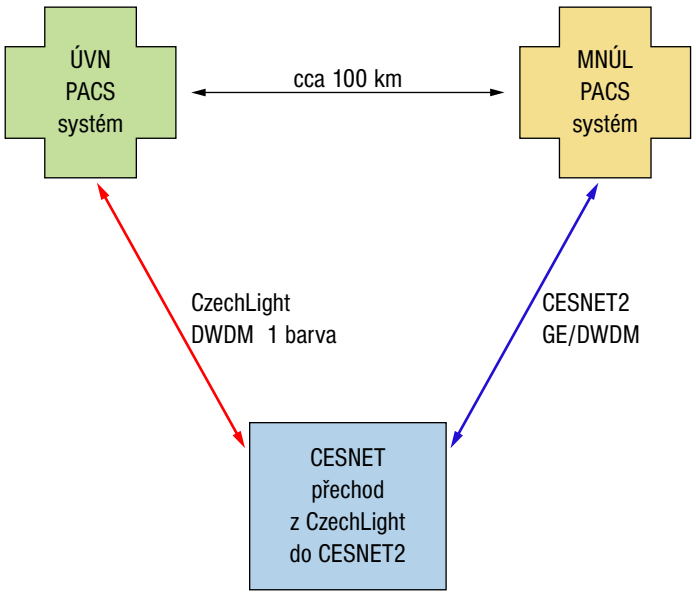
Obrázek 13.1: Konzultace

Vytvořili jsme, jak už bylo zmíněno v kapitole *Optické sítě*, gigabitové spoje sítě CzechLight do FTN i do ÚVN. Oba spoje jsou vedeny z centra sdružení CESNET v Praze Dejvicích. Díky tomu je možné vyřešit v rámci pilotního provozu první problém, kterým byla nedostatečná rychlost připojení specializovaných služeb. Zejména přenos sekvencí z počítačového tomografu (CT), což je pro vyšetření v oblasti neurologie a neurochirurgie typické, je schopen způsobit problémy, pokud je celý provoz nemocnice veden pouze přes linku 100 Mb/s. Přenos musí být rychlý a spolehlivý i z toho důvodu, protože se jedná o život ohrožující stavy a pokud je technika spojení nespolehlivá nebo pomalá, snímek se pro jistotu posílá sanitkou rychlé záchranné služby, což představuje zpoždění vyhodnocení snímků o 30 až 45 minut dle hustoty silničního provozu.

Druhým požadavkem nemocnic, které jsou již v současné době vybaveny bezfilmovým zpracováním dat, je technologie *archivace obrazových dat*. Zatím byla většinou realizována centrální úložiště dat. Jen v rámci projektu *MeDiMed* je možné najít prvky distribuce dat. Ať už se jedná o vlastní zálohování nebo o vytváření specializovaných databází, například pro účel výuky.

Podle našeho názoru jde o obecný problém. Utvrdil nás v tom požadavek dvou nemocnic, které se podílí na projektech v oblasti digitálního zpracování medicínských dat. V tomto případě se opět na jedné straně jedná o Ústřední vojenskou nemocnici v Praze Střešovicích, což je pro nás výhodné, neboť můžeme s výhodou využít vlastnosti optické sítě DWDM a použít pro tento účel stejný optický kabel, který je již připraven pro systém konzultací ve FTN. V této části projektu je druhým spolupracujícím subjektem Masarykova nemocnice v Ústí nad Labem, která je již v současné době vybavena kompletním bezfilmovým zpracováním medicínské obrazové informace.

V tomto případě se již nejedná o přenos jednotlivých vyšetření, ale o systematickou spolupráci v oblasti vytváření archivu dat. Režim je přibližně takový, že se každodenně v době mimo pracovní špičku provádí replikace pracovních částí archivu dat, a to nejen na vlastním pracovišti, ale také na diskovém prostoru spolupracující nemocnice. Toto řešení umožňuje zásadně zvýšit spolehlivost uložených dat. Například ÚVN si již v současné době vytváří pracovní kopii dat v rámci svého areálu, v samostatných budovách s nezávislým napájením. I při tomto zabezpečení však není možné vyřešit všechny problémy, které jsou dány nepřetržitým provozem nemocničních systémů, jako je pravidelná údržba archivačního systému, optimalizace využívání datových skladů, řešení náhradního chodu v případě poškození jednoho ze spolupracujících center a samozřejmě možnost velmi jednoduchého sdílení dat pro definované účely medicínského výzkumu. Základní uspořádání navrženého řešení je na přiloženém schématu.



Obrázek 13.2: Distribuovaný archivační systém

Předpokladem vytvoření tohoto systému je vybavení obou pracovišť technikou podporující FCoIP (Fibre Channel over IP), jež mimo konverzi protokolů zajistí

jejich kódování z důvodu zabezpečení dat, správu celého systému přenosu dat na vzdálenost přesahující běžné metropolitní vzdálenosti (více než přibližně 20 km), řešení příslušných problémů časování a zpoždění na meziměstských linkách.

13.4 Rozvoj projektu MeDiMed

Rozvoj a rozšíření projektu *MeDiMed* probíhá v řadě směrů. Byla zahájena jednání s ÚVT MU a MOÚ Brno o napojení MNÚL Ústí n. L. na centrální komunikační server PACS. MNÚL má speciální zájem o spolupráci v oblasti onkologie (přenos a hodnocení obrazových dat), protože Masarykův onkologický ústav je celostátní autoritou a nejvyšším pracovištěm v tomto oboru.

V rámci nové spolupráce s FN Bulovka začal vývoj unikátních metod fúzí obrazových informací z různých zdrojů (např. CT, MR) s využitím moderních metod grafického zpracování ve spolupráci s FN Bulovka, MFF UK (ÚVT a KSVI). Mezi připravované projekty patří techniky k rozlišování objektů s nízkou densitou (cévní systém zastíněný kostmi, modelování vnitřních částí kloubního spojení).

Dalším zahájeným projektem nad rámec původního plánu aktivity je *zpracování vícedimenzionálních modelů* z obrazových modalit *v reálném čase*. Projekt probíhá s využitím centrálního komunikačního serveru PACS, infrastruktury sdružení CESNET, za účasti FN u sv. Anny v Brně a Ústavu počítačové grafiky a multimédií FIT VUT v Brně. Moderní medicína využívá stále více nejrůznějších technických zařízení a přístrojů, které umožňují zlepšovat úroveň diagnostiky a ošetření pacientů. Dobrým příkladem jsou zobrazovací diagnostické metody počítačová tomografie (CT) a magnetická rezonance (MR). Tyto metody dokáží získat prostorovou (3D) informaci o vnitřních strukturách v těle pacienta. Využití takto získaných 3D dat však dnes převážně zůstává na úrovni subjektivního posouzení lékařem, jako tomu bylo u 2D snímků, a na vytvoření textového popisu nálezu. Jedním z moderních trendů v této oblasti je 3D modelování tkání na základě CT/MR dat a aplikace vytvořených modelů zpět v klinické praxi například při plánování chirurgických a rekonstrukčních operací, simulaci jejich průběhu, navigaci a zaměřování nástrojů, realistickém tréninku lékařů na simulátoru atd.

Společný projekt v oblasti 3D modelování lidských tkání na základě CT/MR uskutečnil první experimenty ve spolupráci Ústavu počítačové grafiky a multimédií na Fakultě informačních technologií VUT v Brně, Kliniky zobrazovacích metod Fakultní nemocnice u sv. Anny v Brně a sdružení CESNET. V tomto týmu byl navržen klinicky použitelný systém zpracování CT/MR dat pro tvorbu 3D počítačových modelů lidských tkání. Zároveň hledáme a připravujeme apli-

kaci těchto modelů v klinické praxi řady oborů: ortopedie, plastická chirurgie, stomatologie.

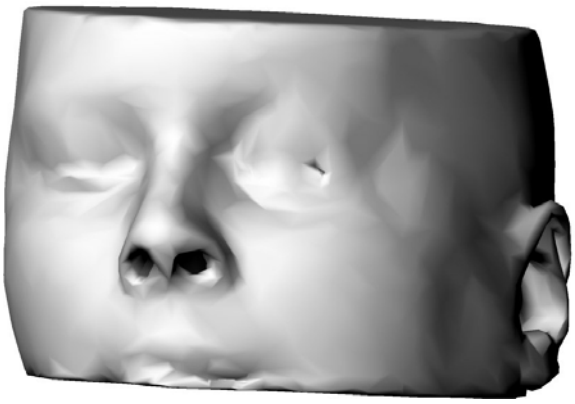
Jedná se o výrazně interdisciplinární spolupráci, která využívá moderní poznatky medicíny, informačních technologií (IT), strojírenství a dalších oborů. Je velmi náročné (finančně, personálně, technicky) vybudovat jednotné pracoviště, které by bylo schopno efektivně a na požadované úrovni zabezpečovat vývoj a testování dosažených výsledků v klinické praxi. Proto byly v letošním roce zahájeny práce na vybudování tzv. „virtuálního vývojového a aplikačního pracoviště". Zapojení pracovníci zůstávají organizačně i prakticky na svých mateřských pracovištích (FIT VUT v Brně, FN u sv. Anny v Brně, Úrazová nemocnice, atd.). To se týká i speciálního technického vybavení (CT, MR, 3D tiskárna, grafické pracovní stanice, atd.). Veškerá datová a komunikační integrace je zabezpečena prostřednictvím akademické počítačové sítě CESNET2.

Díky již funkčnímu síťovému spojení se zabezpečeným přenosem citlivých dat nemusí odborníci (lékaři ani technici) cestovat mezi jednotlivými pracovišti, která jsou rozmístěna po celém městě. Přenos CT/MR dat z nemocnice na technické pracoviště, segmentace obrazu tkání, příprava 3D modelů, ověření jejich správnosti atd. je zabezpečeno, dohodnuto, provedeno nebo schváleno prostřednictvím sítě CESNET2. V akutních případech, kdy jde o čas, to může mít velký význam pro zdraví a život pacienta. Je také možné mnohem lépe využít čas vysoce odborných pracovníků (lékařů i techniků) a kapacity specializovaného a drahého technického vybavení (CT, MR, 3D tiskárna, atd.). Dále také může být toto „virtuální pracoviště" bez větších problémů rozšířeno o další klinická i technická pracoviště v regionu i v rámci kraje nebo republiky.

13.4.1 Elektronický podpis při přenosu a zpracování medicínské obrazové informace

Metropolitní centrum zpracování obrazové informace v medicíně řešené v rámci projektu *MeDiMed* využívá technologie založené na celosvětovém komunikačním standardu DICOM (Digital Image Communication in Medicine). Problematika zabezpečených přenosů medicínských dat včetně problematiky autentizace uživatelů apod. v rámci uzavřeného systému jedné nemocnice se obvykle řeší vlastními prostředky, které nabízí konkrétní dodavatel PACS ve spolupráci s konkrétním dodavatelem nemocničního systému, bez ambicí na vyřešení požadavku kompatibility mimo areál daného zdravotnického zařízení.

Vyřešení autentizovaného přístupu k medicínským obrazovým datům napříč spektrem zdravotnických zařízení spolupracujících v rámci projektu *MeDiMed* přináší novou kvalitu poskytovaných služeb, zejména podporu přenosů obra-



Obrázek 13.3: 3D model počátečního tvaru obličeje s viditelným poškozením tkání

Obrázek 13.4: Doplnění deformované části ze zdravé strany s využitím symetrie

Obrázek 13.5: Vytvořený doplněk pro korekci deformace, který je v závěrečné fázi převeden do trojrozměrného modelu pomocí 3D tiskárny

zových informací mezi jednotlivými pracovišti (nemocnicemi), která pacient v průběhu léčby navštíví, případně jsou nutná pro konzultace specialistů. Ve svém důsledku jednoznačně vede k usnadnění a urychlení formulace správné diagnózy, vyloučení opakovaných vyšetření, úspoře času pacienta i lékaře a tím i finančních prostředků.

Zařízení rozličných výrobců v současnosti připojená k metropolitnímu PACS serveru (prohlížecí stanice, specializované stanice pro primární diagnostiku, archivační zařízení, terapeutická zařízení,. . .) tvoří velmi heterogenní prostředí. Pro rozlišení pracovišť jednotlivých nemocnic je v současnosti rozhodující IP adresa pracovních stanic tohoto pracoviště, resp. její transformace do unikátního adresního prostoru privátní sítě metropolitního PACSu. Toto řešení je dostačující např. pro zdroje obrazových dat, případně pro prohlížecí stanice, které jsou využívány jediným uživatelem. Alternativa autentizovaného přístupu je zcela logickým požadavkem lékařů (služby v jiných nemocnicích, mobilní pracoviště, domácí pracovny lékařů,. . .).

Tento problém jsme vyřešili pomocí IPSec tunelu s přidělováním privátní IP adresy IPSec klientům na základě jejich autentizace. Uživatelé, kteří sdílí pracoviště s dalšími, budou pro komunikaci s PACS serverem používat IPSec tunel, kde jim bude na základě autentizace pomocí PKI přidělena „jejich“ privátní unikátní IP adresa.

Pro řešení jsme se rozhodli zvolit autentizaci pomocí PKI (Private Key Infrastructure) s privátním klíčem uživatele umístěným na USB klíči.

Zpočátku jsme zvažovali tyto dvě varianty řešení:

- PKI s klíčem uloženým na čipové kartě. Toto řešení je však dražší o čtečky čipových karet, které by bylo nutno připojit ke všem používaným stanicím.
- OTP (One Time Password) generované pomocí autentizačního kalkulátoru. Toto řešení přináší jednak nutnost pořízení příslušného OTP serveru a jednak je pro uživatele méně komfortní, protože heslo je nutno přenést z kalkulátoru do stanice ručně.

Na straně IPSec serveru jsme použili dvojici směrovačů Cisco 3845 s hardwarovou akcelerací šifrování. Naše řešení je postaveno na přidělování privátní IP adresy IPSec klientům na základě jejich autentizace. Proto není možné použít zařízení řady Cisco PIX, neboť PIX umožňuje pouze přidělování adresy z rozsahu sdíleného všemi IPSec klienty. Vybírali jsme tedy pouze mezi VPN koncentrátorem řady Cisco VPN 3000 a běžným Cisco směrovačem s dostatečným výkonem pro šifrování. Zde jsme vybrali na základě ekonomických parametrů Cisco 3845, koncentrátor VPN 3000 ve stejné cenové relaci by poskytoval přibližně třetinový výkon.

Pro uložení veřejných PKI klíčů jednotlivých uživatelů byla zřízena certifikační autorita v rámci Masarykovy univerzity a dvojice publikačních serverů. Provoz této certifikační autority bude zpočátku zajišťovat Masarykova univerzita. V závislosti na množství uživatelů lze do budoucna zvažovat jiné operativnější varianty, které byly projednávány se zástupci sdružení CESNET zodpovědnými za tuto oblast.

Na straně klienta lze podle druhu operačního systému použít buď IPSec klient Cisco řady VPN 3000, který nevyžaduje žádný licenční poplatek, případně nativní IPSec klient daného operačního systému. Jako USB úložiště privátních PKI klíčů jsme použili USB klíče vyvinuté firmou Alladin. Toto zařízení již bylo testováno proti prvkům Cisco. Pro účely tohoto projektu jsme pořídili minimální objednatelné množství, tj. 25 kusů USB klíčů a příslušných SW licencí. Vybavení dalších uživatelů bude následně řešeno z jiných prostředků.

Komponenty navrhovaného řešení jsou z důvodu bezpečnosti umístěny ve dvou vzdálených lokalitách Masarykovy univerzity v Brně a propojeny vysokorychlostní sítí. Primární lokalitou je Ústav výpočetní techniky Masarykovy univerzity, sekundární lokalitou je budova Lékařské fakulty Masarykovy univerzity.

Dosažené cíle

- Autentizovaný přístup ke službám poskytovaným v rámci metropolitního PACS systému.
- Procedura autentizace uživatelů probíhá z jejich pohledu snadno a rychle a přitom je zachována dostatečná míra bezpečnosti.
- Celkově vyšší úroveň zabezpečení medicínské obrazové informace.
- Spolehlivé vysoce profesionální řešení, které přispěje k využití kapacit vysokorychlostní sítě za účelem integrace služeb obrazových informačních systémů v medicíně.

13.4.2 Dostupnost distribuované medicínské obrazové informace při poruše přenosových tras

Prozkoumali jsme dostupnost různých variant řešení záložního spojení pro vzdálené nemocnice připojené přes veřejnou datovou síť. Zálohu datového spoje pro tyto nemocnice je možno řešit prostřednictvím následujících typů datových okruhů.

Pevné duální připojení nemocnice do veřejné datové sítě

Řešení má dvě zásadní nevýhody:

- Neřeší případný výpadek internetové konektivity na straně Ústavu výpočetní techniky. Problém není kritický, protože tato konektivita je řešena dostatečně robustně.
- Toto řešení je velmi nákladné. Nemocnice by musela mít konektivitu ke dvěma různým operátorům nebo alespoň do dvou různých PoP téhož operátora. Jedná se o méně spolehlivou variantu závisející na spolehlivosti a redundanci sítě tohoto operátora.

V obou případech je potřeba pronajmout dva nezávislé datové okruhy.

Komutovaný datový okruh k dalšímu operátorovi veřejné datové sítě

Existuje řada operátorů, kteří nabízejí komutované připojení přes veřejnou telekomunikační síť zdarma. Toto připojení však nemá dostatečnou přenosovou kapacitu.

Komutovaný datový okruh „nemocnice–Ústav výpočetní techniky"

Toto řešení se jeví jako jediné ekonomicky schůdné s dostatečnou přenosovou kapacitou. Komutovaný spoj plánujeme řešit pomocí protokolu multikino PPP. Pomocí něj je teoreticky možné sdružovat libovolné množství přenosových kanálů nižší kapacity. Protokol multikino PPP je náročný na výkon procesoru zařízení, kde je ukončen. V současné době hledáme cenově výhodné zařízení s dostatečným výkonem CPU.

13.4.3 Mezinárodní ocenění

Medimed prezentoval ČR během konference *eHealth 2005* v Tromso na výstavce úspěšných projektů a na *eHealth – Impact Case Studies 2005* v Tunisu. Tento projekt vybralo a doporučilo MI ČR.

Část II

Mezinárodní projekty

14 Projekt GN2

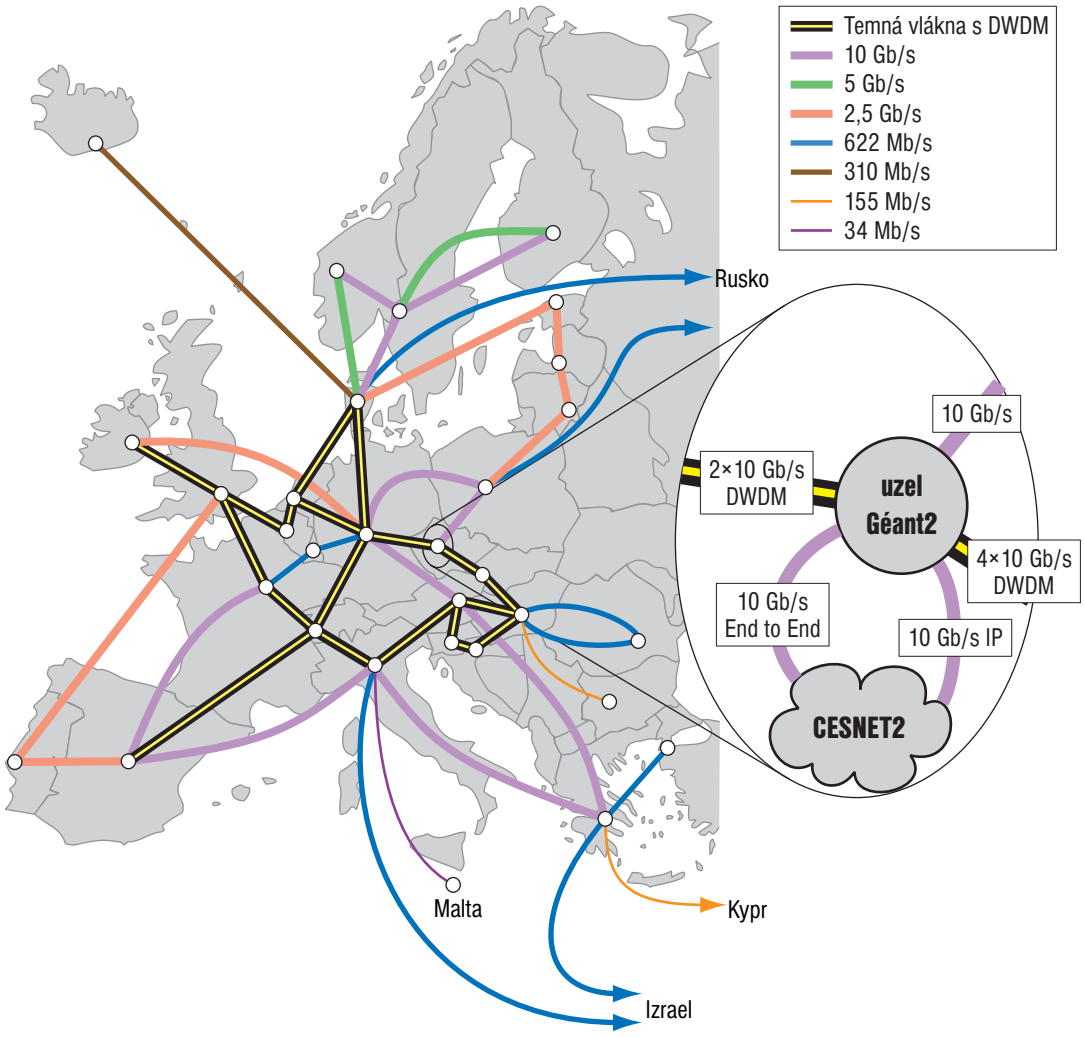
Soustavný rozvoj evropské infrastruktury propojující sítě národního výzkumu (jako je i CESNET2) je strategickým zájmem Evropské Unie a je již od roku 1996 postupně podporován prostřednictvím rámcových programů EU. V září roku 2004 úspěšně skončil čtyřletý projekt *Géant* a již od 9. září téhož roku začalo konsorcium třiceti dvou organizací budovat evropskou páteřní síť nové generace. Projekt nese název *Multi-Gigabit European Academic Network*, veřejnosti však patrně bude známější pod zkratkou *GN2*. Na jeho řešení se podílejí organizace zabývající se problematikou vysokorychlostních sítí pro vědu a výzkum, koordinátorem je společnost DANTE Ltd. Pro potřeby výzkumu, vývoje a vzdělávání by tak mělo být nejpozději na konci projektu v roce 2008 k dispozici komunikační prostředí, které bude schopno uspokojit požadavky vědecké komunity od zajištění mobility v evropském výzkumném prostoru (European Research Area – ERA) po poskytování vyhrazených vysokokapacitních spojení mezi konkrétními koncovými zařízeními. Celkový plánovaný rozpočet projektu *GN2* činí cca 180 miliónů Euro, přičemž EU přispěje 93 milióny Euro.

14.1 Síť GÉANT2

Základem výše zmíněného komunikačního prostředí bude páteřní síť, která ponese název *GÉANT2* (její plánovanou topologii v okamžiku spuštění najdete na obrázku 14.1). Tato síť je od počátku projektována jako síť hybridní, tzn. že kromě základní IP komunikace bude podporovat také vytváření dočasných účelových infrastruktur (gridů) či spojení bod–bod, a to jak na bázi virtuálních privátních sítí, tak na bázi vyhrazených vlnových délek (tzv. lambda služby). Vývoj ukázal, že optimálním základem pro budování hybridních sítí jsou takzvané CEF (Customer Empowered Fibre) sítě, tedy sítě, jejichž provozovatel si pronajme pouze optická vlákna a osadí si je vlastními technologiemi podle svých potřeb. Cílem konsorcia projektu *GN2* je uplatnit koncept CEF v co největší části nově budované sítě. Síť by měla být uvedena do provozu v prvním čtvrtletí roku 2006. Jelikož sdružení CESNET patří mezi průkopníky konceptu CEF, podíleli se naši pracovníci jako jedni z mála na projektování topologie sítě *GÉANT2*, výběru vhodných optických tras a přenosových technologií během tohoto roku.

Portfolio služeb, které budou poskytovány v rámci sítě *GÉANT2*, lze rozdělit do následujících oblastí:

Služby pro „běžného“ uživatele: Základem této skupiny jsou služby již poskytované v síti *GÉANT*, tedy přeprava IP, a to duálně protokoly IPv4 a IPv6 se špičkovými parametry – s vysokou kapacitou připojení, ztrátovostí blížící se nule a minimální dobou odezvy. Pro potřeby aplikací vyžadujících



Obrázek 14.1: Plánovaná topologie sítě *GÉANT2* v roce 2006

zaručení některých parametrů přenosu bude stejně jako v síti *GÉANT* k dispozici služba Premium IP a pro potřeby rychlého přenosu velkého množství dat s minimálními dopady na ostatní provoz pak služba Less than Best Effort. Pro aplikace na úrovni gridů pak síť *GÉANT2* bude schopna poskytovat virtuální privátní sítě, přičemž cílem je nahradit centrální zřizování a konfiguraci těchto sítí nástroji, jež tuto činnost umožní uživatelům. Akademičtí pracovníci, kteří často cestují, mohou očekávat větší komfort díky roamingu v akademických sítích, kdy uživatel bude moci využít služeb hostitelské organizace při autentizaci u organizace domovské. Velký důraz je také kladen na zajištění kvalitního spojení do NREN mimo Evropu.

„Nadstandardní“ služby: Stejně jako sítě národního výzkumu, tak i síť, která je vzájemně propojuje, musí splnit další podmínku – dostatek zdrojů pro

uspokojení potřeb poměrně malé části uživatelů, která však potřebuje přenášet velké objemy dat nejlépe v reálném čase. Tito uživatelé přenášejí mezi omezeným počtem lokalit data takového objemu, že jejich provoz mnohonásobně převyšuje provoz generovaný zbytkem uživatelů. Současné technologie umožňují pro tyto uživatele vytvářet na pronajaté vláknové infrastruktuře vyhrazená spojení bod–bod, či dokonce privátní sítě na úrovni vyhrazených vlnových délek a optického přepínání okruhů. Poskytování takového typu služeb, nazývaného obvykle lambda služby, bude záviset na postupu budování infrastruktury a výsledcích výzkumných aktivit projektů, které se zabývají hledáním mechanismů pro rutinní zřizování, konfiguraci a provoz takovýchto subsystémů. To znamená, že tyto služby nebudou poskytovány zároveň se zprovozněním sítě *GÉANT2*.

V podstatě jsou plánovány tři modely těchto služeb:

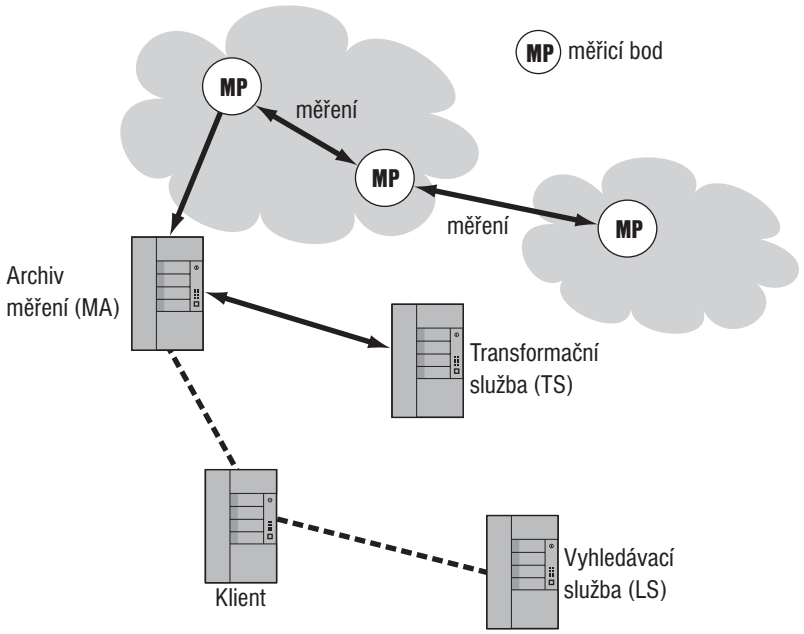
- Pro dlouhodobé projekty s velkými požadavky na pásmo, které však nevyžadují častou rekonfiguraci, budou operátorem sítě nastavena požadovaná optická spojení. S nasazením tohoto typu služby se počítá ve druhém roce projektu.
- Vyšší variabilitu a dynamičnost ve správě lambda služeb otevírá použití rekonfigurovatelných add-drop multiplexorů. To umožní dynamické zřizování a konfiguraci optických spojení pro různé projekty, pokud koncová zařízení leží prakticky ve stejných lokalitách.
- Optické přepínání okruhů bude vhodné pro zájemce, kteří potřebují pro své projekty variabilní geometrii sítě, možnost dynamicky rekonfigurovat komunikační infrastrukturu a jejichž požadavky jsou krátkodobé. Technologie, které toto umožní, jsou stále ve vývoji a jejich nasazení do rutinního provozu se očekává v horizontu dvou let.

14.2 Výzkumné aktivity projektu GN2

Cílů projektu *GN2* nelze dosáhnout pouze navržením topologie sítě a následným nákupem služeb či zařízení a správou takto vybudované sítě. Předpokládané nároky na novou generaci sítě pro výzkum, vývoj a vzdělávání vyžadují také velkou míru inovativního přístupu. Proto, na rozdíl od předchozích projektů na budování evropské akademické infrastruktury, jsou součástí projektu *GN2* také výzkumné aktivity. CESNET se podílí na následujících:

14.2.1 JRA1 – Měření a řízení výkonu sítě

Cílem je vyvinout univerzální systém pro provádění různých typů výkonnostních testů v počítačových sítích a prezentaci jejich výsledků. Systém je založen na kombinaci několika nezávisle běžících služeb a byl nazván *perfSONAR*. Architektura systému je znázorněna na obrázku 14.2.



Obrázek 14.2: Systém *perfSONAR*

CESNET byl v roce 2005 v rámci aktivity JRA1 zodpovědný za specifikaci požadavků na monitorovací systém a za nasazení pasivního monitorování do systému *perfSONAR*. Navrhli jsme koncepci několika pasivních monitorovacích aplikací, jejich rozhraní do systému *perfSONAR* a nyní pracujeme na implementaci. Dále jsme ve sdružení CESNET instalovali dvě stanice pro pasivní monitorování provozu mezi sítěmi GÉANT a CESNET2 a jednu aktivní monitorovací stanici pro měření zpoždění a ztrátovosti mezi sítí CESNET2 a ostatními evropskými NREN.

Protože CESNET je jediným členem konsorcia projektu *GN2* spolupracujícím jak na aktivitě JRA1 tak na projektu *LOBSTER*, byli jsme konsorciem projektu *LOBSTER* pověřeni vedením pracovní skupiny (Task Force) pro integraci infrastruktury *LOBSTER* do systému *perfSONAR*.

14.2.2 JRA2 – Bezpečnost

Aktivity v oblasti bezpečnosti jsou v projektu GN2 zaměřeny především na problematiku zabezpečení aktivních prvků a služeb sítě *GÉANT2*, včetně vybudování proaktivního systému detekce incidentů a boje s nimi (vybudování

systému monitorování a detekce anomálií i útoků, databáze incidentů, poplachového systému,. . .). Dalším cílem je návrh infrastruktury pro koordinované řešení bezpečnostních incidentů a její pilotní implementace. Sdružení uplatnilo v této části projektu *GN2* své zkušenosti s vývojem programovatelného hardware a přispělo vývojem NetFlow sondy – viz kapitola 4.2.

14.2.3 JRA3 – Vývoj nových služeb

Úkolem této aktivity je připravit podmínky pro poskytování vyhrazených přepínaných spojení, a to především poskytování tzv. lambda služeb. Budou vyhledávány, navrhovány a testovány technologie vhodné pro automatické zřizování a správu optických spojení na základě požadavků uživatelů. V tomto roce jsme se podíleli především na definici požadavků a výběru vhodných technologií pro řízení výše uvedených „nadstandardních“ služeb popsaných výše.

14.2.4 JRA4 – Testování služeb a technologií

Součástí projektu *GN2* je také návrh a realizace testovací infrastruktury oddělené od *GN2* určené pro ověřování nových přenosových technologií a síťových aplikací. Tato testovací infrastruktura má vzniknout propojením národních testovacích infrastruktur složených z temných vláken, která budou osazována potřebným zařízením v závislosti na typu experimentu. Odborníci sdružení CESNET se podíleli na návrhu vhodné topologie testovací infrastruktury a výběru experimentů v oblasti optických přenosových technologií. V průběhu roku 2005 vznikla v rámci této aktivity nová podaktivita zabývající se problematikou propojení sítí národního výzkumu a vzdělávání v sousedících zemích za použití temných vláken (Cross Border Fibre, CBF), do které je sdružení CESNET zapojeno pilotní implementací CBF spojení mezi sítí *CESNET2* a polskou sítí národního výzkumu *PIONIER*. Po pilotní fázi by se toto propojení mělo stát součástí sítě *GÉANT2*.

14.2.5 JRA5 – Mobilita a roaming

Jedním z hlavních cílů projektu *GN2* je umožnit v nové síti transparentní a jednoduchý přístup uživatelům k síťovým prostředkům z jakékoli lokality v rámci Evropského výzkumného prostoru (ERA), což předpokládá vyřešení roamingu. Zástupci sdružení se v této aktivitě podíleli na řešení problematiky roamingu v rámci iniciativy *eduroam* a taktéž se podíleli na stanovení zásad společné autentizační a autorizační infrastruktury.

14.2.6 SA3 – End to End Quality of Service

Kromě výše zmíněných výzkumných aktivit je sdružení CESNET zapojeno také do aktivity, jejímž úkolem je umožnit koncovým uživatelům přenášet mezi sebou prostřednictvím sítě *GÉANT2* data se zaručenými parametry přenosu. Účastníme se podaktivity *PERT (Performance Response and Enhancement Team)* s cílem ustavení a zajištění rutinního chodu distribuované pracovní skupiny odborníků řešících výkonnostní problémy při síťové komunikaci.

CESNET se v rámci PERTu střídá s ostatními NREN v pravidelné službě trvající vždy jeden týden. Pro tuto službu jsme provedli školení pracovníků síťového operačního centra sdružení CESNET, kteří mají za úkol přijímat hlášení nových problémů. Jednotlivé problémy pak řeší odborníci na konkrétní technické oblasti.

14.3 Podpora uživatelů

Problematika vysokorychlostní datové komunikace v prostředí výzkumu a vzdělávání je v tomto projektu pojata velmi komplexně. Kromě aktivit zabývajících se budováním a provozem příslušné infrastruktury či výzkumu v oblasti informačních a komunikačních technologií je proto velký důraz kladen na podporu koncových uživatelů a podporu rozvoje jednotlivých NREN. Cílem těchto aktivit, zahrnujících kromě technických také organizační a ekonomické aspekty implementace nejmodernějších informačních a komunikačních technologií, je především setřít stávající rozdíly v technické úrovni NREN a připravit tak prostor pro vybudování homogenního prostředí pro výměnu vědeckých informací.

Podrobnější informace o projektu *GN2* lze nalézt na oficiálních stránkách projektu[1].

[1] *http://www.geant2.net/*

15 Projekt EGEE

V průběhu celého roku 2005 se sdružení CESNET podílelo na řešení projektu *EGEE (Enabling Grids for E-sciencE)* 6. rámcového programu Evropské unie. Cílem tohoto dvouletého projektu je vytvoření stabilní (provozní) celoevropské gridové infrastruktury, která by se měla stát základem celosvětového Gridu. Projekt vedený z CERNu sdružuje 70 partnerů prakticky ze všech zemí Evropy včetně Ruska a několika mimoevropských (USA), mezi přidružené partnery pak patří i Korea.

Grid budovaný v rámci EGEE odpovídá primárně potřebám komunity, která projekt iniciovala – částicovým fyzikům. EGEE Grid je tvořen z clusterů počítačů vybavených procesory kompatibilními s architekturou IA-32 a IA-64 (případně AMD64) s operačním systémem Linux propojených s rozsáhlými datovými sklady (s předpokládanou agregovanou kapacitou řádu desítek PB). Projekt neplatí vlastní technické vybavení, cca 1/4 celkových přidělených prostředků (35 milionů Euro) je určena na vývoj middleware s názvem gLite, ostatní prostředky jsou určeny na provoz (cca 1/2) a podporu uživatelů včetně školení a diseminace informací. Projekt sdružuje národní, regionální i aplikačně orientované gridové aktivity, které poskytují vlastní technické i programové vybavení a lidskou kapacitu pro správu clusterů. Orientace na clusterová řešení je plně kompatibilní s rozvojem MetaCentra v rámci výzkumného záměru sdružení CESNET.

Partneři projektu jsou rozděleni do administrativních domén, zvaných „federace“, které jsou organizovány na geografickém principu. Česká republika je součástí tzv. Středoevropské federace (CE Federation), kam dále přísluší Polsko, Rakousko, Slovensko, Maďarsko, Slovinsko a od prosince 2005 také Chorvatsko. CESNET je jednou organizací České republiky, která je zapojena do řešení projektu EGEE – toto je plně v souladu se snahou dosáhnout postupně naplnění principu „Jedna země – jeden zástupce“, který je plánem pro gridovou infrastrukturu v 7. rámcovém programu EU. Každá federace má jednoho zástupce v Project Management Boardu (PMB), zástupcem Středoevropské federace se v lednu 2005 stal zástupce CESNETu Luděk Matyska. Získali jsme tak možnost nejen se podílet na rozhodování v rámci EGEE, ale především se plně zapojit do přípravy návazného projektu *EGEE II*.

Projekt EGEE je rozdělen do řady aktivit – výzkumných, provozních a integrujících. CESNET je jako jediný partner z CE federace (ve skutečnosti jako jeden z velmi malého počtu partnerů ze všech federací) zapojen do všech skupin aktivit.

Výzkumné aktivity – Joint Research Activities, JRA – jsou soustředěny na vývoj middleware (JRA1), kontrolu kvality (JRA2), bezpečnost (JRA3) a sítě (JRA4). V rámci JRA1 je CESNET součástí tzv. italsko/českého clusteru a odpovídá za

rozvoj *Logging and Bookkeeping Service (LB)*, služby, která sleduje průchod úloh gridovým prostředím a rekonstruuje stav úlohy na základě událostí zasílaných jednotlivými komponentami. Další komponentou v plné kompetenci sdružení CESNET je *Job Provenance*, dlouhodobé úložiště dat o úlohách počítaných na EGEE Gridu. Mezi hlavní výsledky roku 2005 patří zájem kolegů z USA o začlenění LB do systému *VDT*, což je specifické úložiště ověřených gridových komponent, využívaných v řadě gridových projektů v USA i mimo ně. Zahrnutí LB služby do VDT bude oceněním kvality a užitečnosti tohoto software. V roce 2005 jsme rovněž úzce spolupracovali s JRA2 na využití dat ukládaných v LB databázi (a posléze dostupných prostřednictvím Job Provenance) pro výpočty statistik využívání EGEE Gridu a jeho spolehlivosti. Poskytujeme tzv. „Job History Record", který obsahuje veškeré relevantní informace o významných událostech při zpracování úlohy na Gridu. O LB služby projevila dále zájem skupina zabývající se zpracováním dat – cílem je sledování stavu přenosu rozsáhlých souborů mezi jednotlivými komponentami Gridu. V rámci italsko/českého clusteru CESNET rovněž poskytuje napojení na bezpečnostní skupinu (JRA3) a podílí se na dalším rozvoji MyProxy serveru (úložiště uživatelských certifikátů, používané pro generování časově omezených proxy certifikátů).

CESNET je dále intenzivně zapojen do řešení aktivity SA1 – Provoz, správa a podpora Gridu. Kromě běžných činností v rámci Středoevropského Regionálního operačního centra (ROC) CESNET převzal odpovědnost za ustavení a provoz *VOCE*, virtuální organizace pro střední Evropu. EGEE Grid je primárně aplikačně orientován, uživatelé se musí nejprve identifikovat s nějakou aplikační virtuální organizací (případně musí založit vlastní) a teprve poté mohou zdroje EGEE Gridu využívat. Toto však není vhodný model pro nové uživatele se specifickými aplikacemi či pro skupiny „malých" uživatelů, pro které správa a provoz vlastní virtuální organizace představuje příliš velkou zátěž. VOCE je koncipována jako aplikačně neutrální a je určena právě pro uživatele bez konkrétní příslušnosti k některé z „velkých" VO. CESNET odpovídá za všechny služby, provozuje User Interface pro VOCE a spravuje uživatele (za využití systému Perun, vyvíjeného v rámci aktivity MetaCentrum). Do VOCE poskytují zdroje jednotliví partneři ze Středoevropské federace a VOCE je určena uživatelům tohoto regionu (ovšem zájem o zapojení již projevily i jiné země, např. Itálie). V současné době je koncept, zavedený VOCE, zvažován jako modelové řešení pro EGEE II.

NA3 – školení – a NA4 – podpora aplikací – jsou dvě integrující aktivity, do jejichž řešení je CESNET také zapojen. V rámci NA3 jsme v roce 2005 uspořádali dvě školení uživatelů a rozvíjíme specifický EGEE portál[1] jako součást portálu MetaCentra. Podpora aplikací je v CESNETu orientována jednak na komunitu částicových fyziků – zejména prostřednictvím zapojených řešitelů z Fyzikálního

[1] *http://egee.cesnet.cz/*

ústavu AV ČR – jednak na komunitu výpočetní chemie (ta je rovněž hlavním potenciálním uživatelem VOCE). CESNET vyvinul systém *Charon* – řádkové rozhraní pro snazší přípravu a manipulaci s rozsáhlými úlohami. Systém Charon byl úspěšně demonstrován na 2. EGEE konferenci v říjnu 2005 a byl představen uživatelům z ČR na listopadovém školení.

Projekt EGEE končí v březnu 2006, v první polovině roku 2005 proto probíhala příprava nového projektu – pod názvem *EGEE II* – který má být zahájen od dubna 2006 tak, aby byla zajištěna návaznost obou projektů. Projekt EGEE II je rovněž dvouletý (má pokrýt dobu do zahájení 7. rámcového programu) a se svými 80 partnery a rozpočtem přes 50 milionů Euro (z toho 38 milionů je plánovaný příspěvek EU) je dokonce rozsáhlejší než stávající projekt EGEE. CESNET zůstává zapojen do všech výše uvedených aktivit, v rámci JRA1 je dokonce „povýšen" na samostatný cluster s nárůstem plánovaných lidských kapacit. Celkově má CESNET přiznán 20% nárůst rozpočtu. V prosinci 2005 bylo potvrzeno, že návrh projektu byl přijat v plném rozsahu, což zajišťuje významný finanční zdroj pro zapojení do mezinárodních gridových aktivit i sdružení CESNET. Současně pozice největšího partnera z CE federace (a reálně jednoho ze středně velkých partnerů v rámci celého projektu) představuje i uznání dosavadního zapojení CESNETu do rozvoje národního i mezinárodního gridového prostředí.

Podrobnější informace o projektu EGEE je možno nalézt jednak na našem portálu (*http://egee.cesnet.cz/*), jednak na portálu celého projektu (*http://www.eu-egee.org/*).

16 Projekty SCAMPI a LOBSTER

16.1 SCAMPI

Projektu SCAMPI se CESNET účastnil v období od dubna 2002 do března 2005. Cílem projektu bylo navrhnout a implementovat platformu pro pasivní monitorování vysokorychlostních sítí s hardwarovou akcelerací. V roce 2005 proběhla závěrečná fáze projektu. Důležitou událostí bylo poslední review v lednu 2005, na kterém byl projekt hodnocen jako velmi úspěšný. Do konce projektu bylo třeba ještě dokončit některé části software a zejména provést integraci systému. Projekt má své WWW stránky[1], kde je možné získat všechny vytvořené dokumenty a deliverables. Hodnotící komise požádala řešitele o vytvoření firmy (spin-off) pro převedení výsledků projektu do reálných produktů. Proces založení této firmy v současné době probíhá.

16.2 LOBSTER

LOBSTER je projekt 6. rámcového programu Evropské Unie, který navazuje na projekt SCAMPI. Jeho cílem je rozšíření architektury SCAMPI o některé další funkce, zejména o distribuované monitorování a anonymizaci dat a nasazení systému v rozsáhlém měřítku v praxi. Projektu se účastní 8 partnerů ze 6 zemí a je plánován na dobu 27 měsíců. Důraz je kladen na bezpečnostní aplikace, jako je detekce různých typů počítačových útoků. Podrobnější informace najdete na WWW stránkách projektu[2]. V tomto roce proběhlo 5 pracovních schůzek včetně review projektu a jeden seminář pro veřejnost. Bylo vytvořeno 7 deliverables.

CESNET byl v tomto roce zodpovědný za Workpackage 0 – specifikace požadavků, ve kterém jsme navrhli a distribuovali dotazník potenciálním uživatelům z různých oblastí. Následně jsme výsledky analyzovali a zpracovali do deliverable D0.1.

CESNET je dále zodpovědným za návrh a implementaci hardwarové anonymizace hlaviček paketů. Pro splnění tohoto úkolu bylo třeba vytvořit novou skupinu vývojářů hardware. První funkční verze hardwarové anonymizace byla úspěšně prezentována na review projektu v listopadu 2005.

[1] *http://www.ist-scampi.org/*
[2] *http://www.ist-lobster.org/*

17 SEEFIRE

SEEFIRE je Special Support Study podporovaná EU. Projektu se účastní NREN zemí jihovýchodní Evropy, sdružení CESNET, DANTE a TERENA jako koordinátor. Projekt má tři základní skupiny cílů:

První skupina zahrnuje určení strategických cílů pro rozvoj sítí pro podporu výzkumu a vzdělávání v regionu, zdůvodnění a obhajobu rolí regionálních NREN, určení zemí kde pro získání temných vláken bude nutná podpora vlády a rozšiřování výsledků projektu mimo region, zejména k rozvíjejícím se NREN v dalších částech světa (Jižní Afrika, Latinská Amerika, Středozemí a Asie).

Druhá skupina cílů zahrnuje vytvoření aktuálního přehledu potenciálně dostupných temných vláken v regionu včetně jejich typů a vlastníků a zdokumentování existujících technických a administrativních zkušenosti s vláknovou infrastrukturou v regionu.

Poslední skupina cílů zahrnuje identifikaci vhodných technických řešení optických přenosových systémů se zřetelem na technickou pokročilost při zachování přijatelných cen a nalezení společností, které mají zkušenosti s pokládkou nových optických kabelů. Předmětem zájmu je i zjištění podmínek a cen těchto pokládek se zvláštním zřetelem na poslední míle.

CESNET koordinuje splnění cílů týkajících se nalezení transmisních technologií vhodných pro region jihovýchodní Evropy a zpracování popisů a návrhů budování vybraných optických tras.

18 6NET

Mezinárodní projekt 6NET (IST-2001-32063), který byl součástí 5. rámcového programu EU, skončil v červnu 2005. Jeho hlavní cíle byly následující:

- Realizace a testování panevropské sítě používající výhradně IPv6.
- Vývoj nových protokolů a technologií pro sítě IPv6 a jejich integraci do současného Internetu.
- Popularizace a propagace IPv6.

Síťová infrastruktura projektu byla na začátku roku 2005 kompletně odstavena. Poslední půlrok projektu byl věnován jednak dokončení některých výzkumných aktivit, zejména v oblasti IPv6 multicastu a dále pak vytváření dalších publikací, které by dokumentovaly a také popularizovaly výsledky projektu.

V lednu 2005 pořádal CESNET v Praze 5. mítink projektového konsorcia. Ve spolupráci s aktivitou *Virtuální prostředí pro spolupráci* byl celý jeho program vysílán on-line.

V únoru 2005 se v Bruselu konalo pravidelné hodnocení projektu. Na něm jsme formou videa[1]demonstrovali možnosti využití směrovače *Liberouter* (viz kapitola 4.3)pro směrování a filtrování multicastových přenosů. Prezentace byla velmi kladně přijata a setkala se s živým zájmem oponentů.

Konsorcium 6NET vydalo v roce 2005 knižní publikaci [Dun05], v níž byly souborně zpracovány formální výstupy projektu (deliverables) rozšířené o obecné pasáže popisující základní principy a protokoly IPv6. Jako spoluautoři se na obsahu významně podíleli dva zástupci CESNETu:

- Ladislav Lhotka – kapitola 9 (Applications), část kapitoly 6 (Routing)
- Pavel Satrapa – kapitola 2 (IPv6 Basics), kapitola 3 (Addressing)

V červnu 2005 se konalo závěrečné hodnocení projektu. To skončilo výrazným úspěchem, neboť oponenti udělili projektu nejvyšší známku ve všech deseti hodnocených kategoriích.

[1] *http://server1.streaming.cesnet.cz:8080/ramgen/cesnet/6net-demo.rm*

Část III

Závěr a přílohy

19 Závěr

Řešení výzkumného záměru v roce 2005 probíhalo podle plánu s mírnými úpravami. Ty odrážely současný stav a tendence v oblasti informačních a komunikačních technologií pro potřeby výzkumu a vývoje. Kromě toho jsme museli reagovat na změny struktury financování dané rozhodnutím MŠMT.

Rok 2005 předznamenal důležité změny ve výzkumu týkajícím se počítačových sítí a distribuovaných systémů a jejich aplikací. V Evropě je v pokročilém stadiu realizace panevropské výzkumné a vzdělávací sítě GÉANT2, která vedle již tradičních až desetigigabitových IP služeb poskytne uživatelům také vyhrazené gigabitové a desetigigabitové digitální okruhy (lambda služby) kontinentálního rozsahu. Zároveň v tomto evropském projektu nazvaném *GN2* probíhají výzkumné práce zabývající se dalším rozvojem služeb sítě GÉANT2, rozvojem podpůrných nástrojů nutných pro vytvoření transparentního virtuálního prostředí pro spolupráci výzkumných týmů i jednotlivců v rámci Evropy, ale také budováním testovací infrastruktury pokrývající více zemí pro testování nových síťových technologií. Začínají také přípravy následnického projektu ke *GN2*. Úkolem jednotlivých NREN zapojených do projektu GN2 je vytvořit technické a organizační podmínky pro to, aby služby evropské páteře byly k dispozici připojeným uživatelům.

CESNET patří k účastníkům projektu, kteří se na všech těchto pracích významně podílejí. Zároveň pracujeme na zpřístupnění lambda služeb z akademických měst v ČR a na budování testovací infrastruktury CzechLight. Významná je také účast na projektech EU *SEEFIRE* a připraveném projektu *Porta Optica Study*, které podporují zavádění optických sítí v zemích jihovýchodní a východní Evropy. Zavádění méně nákladných technologií nasvícení vláken se ukazuje jako jeden z klíčových momentů pro snížení „digitální nerovnosti“ mezi zeměmi a zmírnění ekonomických a kulturních nevýhod, které s tím souvisí.

Také ve Spojených státech došlo v roce 2005 k velmi důležitému vývoji, který směřuje k vytvoření globálního prostředí pro zkoumání sítí. Je jím iniciativa NSF (National Science Foundation) nazývaná *GENI (Global Environment for Networking Investigations)*. NSF se tím možná vrací ke své původní významné roli v podpoře rozvoje Internetu. Toto globální prostředí má umožnit zkoumání a vytváření nových síťových architektur a distribuovaných systémů. Na rozdíl od Evropy se předpokládá výrazná účast výrobních a obchodních společností na výzkumných projektech (tj. nikoli jen nákup zařízení a služeb). To je ostatně tradicí již u sítí Abilene a NLR (National Lambda Rail). Důležité je poznamenat, že tyto dvě sítě směřují ke sloučení, neboť mají z velké části stejné uživatele a CEF síť NLR může poskytovat 10G lambdy, které jsou základním stavebním kamenem sítě Abilene. Do budoucna se tedy rýsují v oblasti výzkumných a vzdělávacích sítí dva vzájemně se doplňující se směry:

- produkční sítě pro výzkum a vzdělávání, orientované především na poskytování služeb výzkumníkům z různých aplikačních oborů (a lišící se od komerčních sítí především vzájemnou koordinací, zaváděním nových služeb potřebných pro výzkum a parametry potřebnými pro některé vysoce náročné výzkumné aplikace) – a to v globálním, kontinentálním, národním i místním měřítku

- prostředí pro zkoumání, jak mají vypadat budoucí sítě (produkční sítě pro výzkum a vzdělávání i komerční sítě), které mají přinést pokrok vědy, inovace a ekonomický růst, přičemž toto prostředí má rovněž své globální, kontinentální, národní i místní vybavení (facilities).

Představiteli druhého směru jsou zejména GLIF a testovací infrastruktury různých rozsahů. Očekáváme, že GENI postupně přispěje k významnému zdokonalení toho výzkumného prostředí. CESNET je mezi organizacemi, které již mají s budováním a využíváním GLIF a testbedu zkušenosti.

Důležitou součástí předpokládaného výzkumného prostředí je testování a nasazování nových optických a bezdrátových technologií. Přitom bychom měli počítat s tím, že v letech 2006–2007 pravděpodobně dojde k poměrně významnému uplatnění koncových stanic a serverů na bázi PC vybavených gigabitovým a desetigigabitovým rozhraním, což spolu s relativně levnými optickými přenosovými systémy začne měnit vzhled sítí zejména v okrajových částech. Taková okrajová část ovšem může mít díky dosvitu transcieverů (přes 100 km) značnou rozlohu. Uplatnění lze očekávat zejména v CEF sítích. Tyto sítě ovšem přestaly být doménou výzkumu a vzdělávání a rozšiřují se do zdravotnictví, armády, městské správy i do průmyslu a obchodu.

Vytvoření dokonalejšího prostředí pro zkoumání sítí a jejich prvků změní i vztah k organizacím obchodu a průmyslu. Takové prostředí umožňuje testovat výrobky a služby v podmínkách blížících se produkčním nebo komerčním, ať již vznikly kdekoli. To je dosti odlišné od situace, kdy jsme jen od obchodníků nakupovali pro síť výrobky nebo služby. Nyní například vznikají prototypy zařízení, které jsou předmětem testování v síťovém prostředí a které CESNET formou licence nebo spin-off připravuje k předání do výroby. Tento trend máme zájem prohlubovat.

Odráží se to i v našem vývoji vlastních optických zesilovačů CzechLight Amplifier (CLA) určených pro CEF sítě. V roce 2005 jsme jejich první prototypy úspěšně ověřili na gigabitové lince Praha–Hradec Králové a desetigigabitové lince Praha–Brno. Vedle vlastního vývoje optických přenosových technologií jsme však také významně posílil „produkční“ síť CESNET2. Základní trasu Praha–Brno jsme v roce 2005 rozšířili na DWDM okruh Praha–Brno–Olomouc–Hradec Králové–Praha. Tato DWDM infrastruktura představuje významný krok v rozšíření schopností sítě a v přípravě na zprostředkování pokročilých služeb

evropské sítě GÉANT2 domácím uživatelům. Do budoucna počítáme s jejím dalším rozšiřováním, včetně napojení do zahraničí.

Celosvětový vývoj také potvrdil naši vizi uplatnění programovatelného hardwaru (zejména hradlových polí, FPGA) v síťových technologiích – na trhu se začínají objevovat komerční produkty na bázi FPGA. Svou velmi dobrou pozici v této oblasti hodláme využít při dalším rozvoji rodiny karet COMBO, o něž projevuje zájem řada zahraničních partnerů. Podle doporučení závěrečné oponentury projektu SCAMPI také usilujeme o uplatnění výsledků našeho vývoje.

Nedílnou součástí sítě národního výzkumu a vzdělávání se stávají specifické síťové služby a aplikace, které jsou označovány jako middleware. V souvislosti s budováním komunikačního prostředí pro spolupráci nabývají tyto služby stále většího významu, a to především při integraci služeb.

Zásadním problémem řešeným v této oblasti je zajištění zabezpečeného přístupu k síťovým zdrojům v souvislosti s mobilitou uživatelů. Certifikační autorita sdružení CESNET CA byla v říjnu jedním se zakládajících členů mezinárodní federace, jejímž cílem je zlepšit integraci a kompatibilitu autentizačních systémů a usnadnit tak přístup uživatelů především ke gridovým prostředkům. V rámci sítě CESNET2 se úspěšně rozšiřuje roamingový systém *eduroam*.

Zajištění bezpečnosti sítě je globálním problémem, který vyžaduje koordinaci na mezinárodní úrovni, takže kromě vývoje technických nástrojů pro odhalování útoků jsme zapojeni do mezinárodní pracovní skupiny TF-CSIRT a v průběhu roku 2005 jsme nabídli připojeným institucím podporu při budování a formalizaci jejich bezpečnostních týmů. Součástí tohoto úkolu bylo vytvoření metodik pro komunikaci uvnitř bezpečnostního týmu a i mezi těmito týmy navzájem.

Velká pozornost je také věnována vývoji prostředků pro sledování stavu sítě a její optimalizaci. Vyvinuli jsme nástroje pro efektivní zpracování informací o provozu a rozšířili monitorovací infrastrukturu. Sdružení se zapojilo do mezinárodních struktur pro řešení výkonnostních problémů sítě (PERT).

V oblasti aplikací se jako nejvýznamnější uživatelé vysokorychlostních sítí vyprofilovaly především aplikace přenášející velké datové objemy v reálném čase: distribuované výpočetní a úložné systémy (gridy), videokonference se špičkovou kvalitou a dálkové experimenty přenášející velké objemy naměřených dat. Je potěšitelné, že CESNET a s ním spolupracující řešitelé výzkumného záměru jsou zapojeni do všech tří uvedených oblastí.

Prostřednictvím aktivity MetaCentrum hrajeme významnou úlohu v evropském projektu EGEE budujícím rozlehlý grid pro zpracování náročných vědeckých výpočtů. V nadcházejícím nástupnickém projektu EGEE II by se pak naše role měla ještě posílit. Fungující gridová platforma nám umožňuje zapojovat se i do experimentů s videokonferencemi nejvyšší kvality. V roce 2005 jsme zazna-

menali významný úspěch v podobě demonstrací na konferencích iGrid 2005 a SuperComputing 2005, od nějž očekáváme ještě vyšší zájem mezinárodních partnerů o spolupráci s našimi videokonferenčními aktivitami.

V oblasti distribuovaných vědeckých experimentů jsou naši řešitelé zapojeni především do projektů z oblasti fyziky elementárních částic. V České republice se bohužel nenacházejí unikátní zařízení, jež by sloužila jako zdroje vědeckých dat. Domácí týmy se proto zapojují především jako konzumenti a zpracovatelé dat získaných na zahraničních zařízeních. Domníváme se, že využití naší sítě v této oblasti by mohlo být vyšší, proto jsme se pokusili získat nové uživatele uspořádáním semináře *Vysokorychlostní sítě pro výzkum* a hodláme v těchto aktivitách pokračovat i v budoucnu.

Jedním ze strategických cílů, které si sdružení stanovilo, je také akcelerovat využívání informačních a komunikačních technologií v oblasti medicíny. Potvrzením významné role sdružení CESNET v této oblasti je pozvání koordinátora těchto aktivit v rámci CESNETu, Ing. Milana Šárka, CSc. do českého panelu expertů Světové zdravotnické organizace (WHO) v oblasti eHealth, která se zabývá možnostmi využití informačních a komunikačních technologií při péči o lidské zdraví.

V roce 2006 CESNET oslaví desáté výročí své existence. Při této příležitosti jsme se rozhodli uspořádat mezinárodní konferenci na téma „sítě pro výzkum, výzkum pro sítě“. Její hlavní tématické oblasti – optické sítě, IP verze 6, middleware, monitoring, gridy a aplikace – odpovídají tématickému zaměření výzkumného záměru. Lze od ní tedy očekávat vedle výměny zkušeností v daných oblastech i další rozvoj naší mezinárodní spolupráce a nové podněty pro naši další činnost.

A Připojené instituce

A.1 Členové CESNET, z. s. p. o.

instituce	*přípojka [Mb/s]*
Akademie múzických umění v Praze	100
Akademie věd České republiky	1000
Akademie výtvarných umění v Praze	10
Česká zemědělská univerzita v Praze	1000
České vysoké učení technické v Praze	10 000
Janáčkova akademie múzických umění	1000
Jihočeská univerzita	1000
Masarykova univerzita v Brně	1000
Mendelova zemědělská univerzita v Brně	1000
Ostravská univerzita	1000
Slezská univerzita	1000
Technická univerzita Ostrava	1000
Technická univerzita v Liberci	1000
Univerzita Hradec Králové	1000
Univerzita Jana Evangelisty Purkyně v Ústí nad Labem	1000
Univerzita Karlova	10 000
Univerzita obrany se sídlem v Brně	1000
Univerzita Palackého v Olomouci	1000
Univerzita Pardubice	1000
Univerzita Tomáše Bati ve Zlíně	1000
Veterinární a farmaceutická univerzita Brno	1000
Vysoká škola chemicko-technologická v Praze	1000
Vysoká škola ekonomická v Praze	1000
Vysoká škola uměleckoprůmyslová v Praze	100
Vysoké učení technické v Brně	1000
Západočeská univerzita	1000

A.2 Využívání sítě CESNET2 účastníky zabývajícími se vědecko-výzkumnou nebo vzdělávací činností

Funkce a parametry sítě CESNET2 coby výstupu výše zmíněných aktivit jsou permanentně ověřovány v reálném provozu generovaném v prostředí výzkumu a vývoje. Síť CESNET2 a její služby jsou proto zpřístupněny nejen členům sdružení (Akademii věd ČR a vysokým školám) ale také všem organizacím, které se zabývají především vědou, výzkumem a vývojem, včetně uplatnění jejich výsledků v praxi.

V Centrální evidenci výzkumných záměrů (CEZ) pro rok 2005 je uvedeno celkem 297 výzkumných záměrů, které jsou řešeny 94 výzkumnými organizacemi nebo pracovišti. 186 z těchto výzkumných záměrů řeší členové sdružení CESNET (26 organizací). 111 výzkumných záměrů je řešeno dalšími 68 organizacemi, z toho 23 organizací využívá v současné době síť národního výzkumu a vzdělávání CESNET2.

Oslovili jsme řešitele výzkumných záměrů dosud nepřipojených organizací a poskytli jim informace o možnostech sítě CESNET2 s nabídkou připojení. Obdobně jsme oslovili i zástupce soukromých vysokých škol. S organizacemi, které projevily zájem, jednáme o možnostech připojení a využívání sítě CESNET2.

Pro rozšíření informovanosti a případné navázání či rozšíření spolupráce jsme zástupce výzkumných organizací pozvali na seminář *Vysokorychlostní sítě pro vědu a výzkum* o možnostech, které špičkové počítačové sítě nabízejí pro tuto oblast. Vedle příkladů stávajících projektů a aplikací byla jeho součástí i diskuse, kam by měl směřovat další vývoj sítí pro vědu, výzkum a vzdělávání.

Síť CESNET2 využívají i další organizace zabývající se vědecko-výzkumnou nebo vzdělávací činností. Jsou to například vědeckotechnické parky, nemocnice, školy, knihovny či muzea. Podíl některých z těchto institucí na zatížení páteřní sítě již není zanedbatelný, například Národní knihovna České republiky je pro řešení svých projektů připojena rychlostí 1 Gb/s, Fakultní nemocnice Plzeň 155 Mb/s, Fakultní nemocnice v Hradci Králové 155 Mb/s, Moravská zemská knihovna v Brně 100 Mb/s a najdou se i další příklady.

Síť národního výzkumu a vzdělávání České republiky v současnosti využívají například tyto organizace:

- Ústav jaderného výzkumu Řež, a. s.
- Výzkumný ústav geodetický, topografický a kartografický
- Výzkumný ústav veterinárního lékařství
- Technický a zkušební ústav stavební Praha, s. p.
- Výzkumný ústav zemědělské ekonomiky

- Technologické inovační centrum, s. r. o.
- TESTCOM - Technický a zkušební ústav telekomunikací a pošt
- Výzkumný ústav potravinářský Praha
- Výzkumný ústav rostlinné výroby
- Polymer Institute Brno, s. r. o.
- Výzkumný ústav práce a sociálních věcí
- LOM Praha s.p. odštěpný závod VTÚL a PVO
- Vědeckotechnický park Plzeň, a. s.
- INOTEX, s. r. o.
- BIC Plzeň, s. r. o.
- Fakultní nemocnice Brno
- Fakultní nemocnice Královské Vinohrady
- Fakultní nemocnice na Bulovce
- Fakultní nemocnice Olomouc
- Fakultní nemocnice Plzeň
- Fakultní nemocnice s poliklinikou Ostrava
- Fakultní nemocnice u Svaté Anny v Brně
- Fakultní nemocnice v Hradci Králové
- Fakultní nemocnice v Motole
- Všeobecná fakultní nemocnice
- Masarykův onkologický ústav
- Anglo-americká vysoká škola, o. p. s
- Vysoká škola Jana Amose Komenského, s. r. o.
- Vysoká škola ekonomie a managementu, s. r. o.
- Vysoká škola hotelová v Praze 8, s. r. o.
- Bankovní institut vysoká škola, a. s.
- University of New York in Prague, s. r. o.
- Vysoká škola polytechnická, Jihlava
- Policejní akademie ČR
- Soukromá vysoká škola ekonomických studií, s. r. o.
- Vysoká škola evropských a regionálních studií, o. p. s.
- Centrum pro studium vysokého školství
- Národní knihovna České republiky
- Národní lékařská knihovna
- Moravská zemská knihovna v Brně
- Státní vědecká knihovna v Olomouci
- Středočeská vědecká knihovna v Kladně
- Státní vědecká knihovna Liberec
- Státní vědecká knihovna
- Státní technická knihovna
- Severočeská vědecká knihovna v Ústí nad Labem
- Moravskoslezská vědecká knihovna v Ostravě
- Jihočeská vědecká knihovna v Českých Budějovicích

- Národní památkový ústav
- Moravská galerie v Brně
- Moravské zemské muzeum
- Uměleckoprůmyslové museum v Praze

B Seznam řešitelů

Adamec Petr	TU Liberec
Adámek Petr Ing.	MU Brno
Altmannová Lada Ing.	CESNET, z. s. p. o.
Andrš Jindřich Ing.	FAF UK Hradec Králové
Antoš David Mgr.	MU Brno
Bažant Ivo Ing.	ČVUT Praha
Bouzková Helena PhDr.	Národní lékařská knihovna Praha
Buchta Martin	VŠE Praha
Burian Jiří Ing.	OSVČ
Cejp Jiří Ing.	ČVUT Praha
Cimbal Pavel Ing.	ČVUT Praha
Cvrková Eva	CESNET, z. s. p. o.
Čamajová Jana RNDr., Ph.D.	2.LF UK Praha
Čegan Ondřej	CESNET, z. s. p. o.
Čejka Rudolf Ing.	VUT v Brně
Čížek Jaroslav Ing.	ZČU Plzeň
Čížek Martin	ČVUT Praha
Diviš Zdeněk Prof. Ing., CSc.	VŠB-TU Ostrava
Doležal Ivan Ing. BcA.	VŠB-TU Ostrava
Dostál Otto Ing.,CSc.	MU Brno
Dvořák František Ing.	ZČU Plzeň
Feit Josef MUDr., CSc.	LF MU Brno
Fiala Lukáš	FzÚ AV ČR
Filip Ondřej Mgr.	OSVČ
Friedl Štěpán Ing.	VUT v Brně
Fučík Otto Dr. Ing.	VUT v Brně
Fürman Jan Ing.	CESNET, z. s. p. o.
Grolmus Petr Ing.	ZČU Plzeň
Gruntorád Jan Ing., CSc.	CESNET, z. s. p. o.
Hájek Jiří Ing.	ČVUT Praha
Halák Jiří	ČVUT Praha
Hamera Erik	Úřad Městské Části Praha 6
Havelka Zdeněk MUDr.	FN Motol
Hažmuk Ivo Ing.	VUT v Brně
Hejnarová Jaroslava RNDr.	ÚOP Na Plši
Hladká Eva RNDr., Ph.D.	MU Brno
Hlůže Lukáš	UK Praha
Holeček Jáchym	MU Brno
Holub Petr Mgr., Ph.D.	MU Brno
Holý Radek Ing.	UK Praha
Hrad Jaromír Ing., Ph.D.	ČVUT Praha
Hrb Jaroslav Ing.	OSVČ

Hulínský Ivo	CESNET, z. s. p. o.
Chudoba Jiří RNDr., Ph.D.	FzÚ AV ČR
Chvála Ondřej Mgr.	Ustav částicové a jaderné fyziky, MFF UK
Janáková Jiřina	ČVUT Praha
Jarolímková Adéla Mgr.	IKEM Praha
Javorník Michal RNDr.	MU Brno
Jindra Pavel Ing.	ZČU Plzeň
Kácha Pavel	CESNET, z. s. p. o.
Karásek Miroslav Ing. DrSc.	AV ČR Praha
Karczubová Gabriela Mgr.	Český helsinský výbor
Kmuníček Jan Mgr., Ph.D.	MU Brno
Kňourek Jindřich Ing.	ZČU Plzeň
Kořenek Jan Ing.	VUT v Brně
Kosina Jiří Mgr.	FzÚ AV ČR
Košňar Tomáš Ing.	CESNET, z. s. p. o.
Kouřil Daniel Mgr.	MU Brno
Král Antonín Ing.	PRAGONET
Kratochvíla Tomáš	MU Brno
Kraus Michal	ČVUT Praha
Krejčí Iva Mgr.	MU Brno
Kreuzwieser Tomáš Ing.	VUT v Brně
Krise Jan	CESNET, z. s. p. o.
Kropáčová Andrea	CESNET, z. s. p. o.
Krsek Michal Bc.	OSVČ
Křenek Aleš Mgr.	MU Brno
Kuba Martin Mgr.	MU Brno
Kulhánek Petr RNDr.	MU Brno
Kysela Jaroslav Bc.	OSVČ
Lesná Petra MUDr.	FN Motol
Lesný Petr MUDr.	LF Motol, Praha
Lhotka Ladislav Ing., CSc.	CESNET, z. s. p. o.
Líčko Miroslav Ing.	OSVČ
Lokajíček Miloš RNDr., CSc.	AV ČR Praha
Macek Milan Prof.MUDr., DrSc.	FN Motol
Marek Tomáš	ČVUT Praha
Martínek Tomáš Ing.	VUT v Brně
Matoušek Petr Ing.	VUT v Brně
Matuška Miroslav Ing.	VŠE Praha
Matyska Luděk Doc. RNDr., CSc.	MU Brno
Míchal Martin Ing.	CESNET, z. s. p. o.
Michalík Pavel	VŠE Praha
Moučka Bohuslav RNDr.	MU Brno
Mrázek Jiří MUDr.	Nemocnice Most
Mulač Miloš Ing.	MU Brno

Nedbal Robert	ČVUT Praha
Nejman Jan Ing.	CESNET, z. s. p. o.
Neuman Michal Ing.	ČVUT Praha
Novák Václav Ing.	CESNET, z. s. p. o.
Novakov Ivan Ing.	ČVUT Praha
Novotný Jiří Ing.	MU Brno
Nytra Daniel Ing.	OSVČ
Okrouhlý Jan Ing.	ZČU Plzeň
Pavlík Vladimír Ing.	CESNET, z. s. p. o.
Petřek Martin Ing.	MU Brno
Pitner Tomáš RNDr., Ph.D.	MU Brno
Podermanski Tomáš Ing.	VUT v Brně
Poláček Pavel Ing.	UJEP
Pospíšil Jan Ing.	ZČU Plzeň
Procházka Michal Bc.	MU Brno
Průša Richard Doc. MUDr., CSc.	2.LF UK Praha
Pustka Martin Ing.	VŠB-TU Ostrava
Radil Jan Ing., Ph.D.	CESNET, z. s. p. o.
Rohleder David Mgr.	MU Brno
Roškot Stanislav Ing.	ČVUT Praha
Ruda Miroslav Mgr.	MU Brno
Rudinský Jan Ing.	Výzkumné a vývojové centrum v Praze
Růžička Jan Ing.	CESNET, z. s. p. o.
Salvet Zdeněk Mgr.	MU Brno
Satrapa Pavel RNDr., Ph.D.	TU Liberec
Sebestianová Zora RNDr.	MU Brno
Seemanová Eva Prof. MUDr., DrSc.	2.LF UK Praha
Sitera Jiří Ing.	ZČU Plzeň
Skokanová Jana Mgr.	VUT Brno
Slabý Kryštof MUDr.	UK Praha
Slavíček Karel Mgr., Ph.D.	MU Brno
Smotlacha Vladimír RNDr. Ing.	CESNET, z. s. p. o.
Smrž Pavel RNDr., Ph.D.	MU Brno
Smutná Zuzana	LF Motol, Praha
Sova Milan Ing.	CESNET, z. s. p. o.
Studený Daniel Ing.	CESNET, z. s. p. o.
Sverenyák Helmut Ing.	CESNET, z. s. p. o.
Svoboda Vladimír	UK Praha
Šárek Milan Ing., CSc.	CESNET, z. s. p. o.
Šíma Stanislav Ing., CSc.	CESNET, z. s. p. o.
Šimák Boris Doc.Ing., CSc.	ČVUT Praha
Šimeček Ivan Ing.	ČVUT Praha
Škrabal Jiří Mgr.	MU Brno
Šmejkal Ivo Ing.	VŠE Praha

Šmejkal Kamil Ing.	ČVUT Praha
Šmrha Pavel Dr. Ing.	ZČU Plzeň
Šnorek Michal	2.LF UK Praha
Špála Milan Doc.MUDr., CSc.	1.LF UK Praha
Štefl Michal	VŠMIE
Šumová Věra	CESNET, z. s. p. o.
Švec Jan	FzÚ AV ČR
Tlučhořová Lenka Ing.	ČVUT Praha
Tomášek Jan Ing.	CESNET, z. s. p. o.
Třeštík Vladimír Ing.	CESNET, z. s. p. o.
Turnovec Marek MUDr.	FN Motol
Ubik Sven Dr. Ing.	CESNET, z. s. p. o.
Urbanec Jakub Ing.	ZČU Plzeň
Vachek Pavel Ing.	CESNET, z. s. p. o.
Valach Soběslav Ing.	VUT v Brně
Valdman Jan Ing., Ph.D.	ZČU Plzeň
Vandrovec Petr Ing.	ČVUT Praha
Vejvalka Jan MUDr.Ing.	LF Motol, Praha
Vejvalková Šárka MUDr.	FN Motol
Velc Radek Ing. arch.	OSVČ
Verich Josef Ing.	VŠB-TU Ostrava
Veselá Bohumila Ing.	VŠE Praha
Vlastibor Jaroslav	CESNET, z. s. p. o.
Vlček Petr Doc. MUDr., CSc.	LF Motol, Praha
Voců Michal Mgr.	UK Praha
Vojnar Tomáš Ing., Ph.D.	VUT v Brně
Vojtěch Josef Ing.	CESNET, z. s. p. o.
Vozňák Miroslav Ing., Ph.D.	VŠB-TU Ostrava
Wija Tomáš Ing.	VŠB-TU Ostrava
Wimmer Miloš Ing.	ZČU Plzeň
Zdařil Petr	2.LF UK Praha
Zeman Tomáš Ing., Ph.D.	ČVUT Praha
Zemčík Pavel Doc. Dr. Ing.	VUT v Brně
Zukal David Ing.	VŠB-TU Ostrava
Žádník Martin Bc.	VUT v Brně
Žejdl Petr	ČVUT Praha

C Vlastní publikace a výstupy

C.1 Samostatné publikace

kolektiv autorů: *Optická síť národního výzkumu a její nové aplikace*.
CESNET, 2005, 150 stran, ISBN 80-239-4256-5

kolektiv autorů: *Optical National Research Network and its New Applications*.
CESNET, 2005, 163 stran, ISBN 80-239-4531-9

kolektiv autorů (editor Dunmore M.): *6net: An IPv6 Deployment Guide*.
University of Lancaster, 2005, 425 stran, ISBN 1-86220-173-0

C.2 Recenzované publikace

C.2.1 Články v odborných periodicích

Avellino G., Beco S., Cantalupo B., Maraschini A., Terracina A., Colling D., Ronchieri E., Gianelle A., Mazzucato M., Peluso R., Sgaravatto M., Guarise A., Piro R., Werbrouck A., Kouřil D., Křenek A., Matyska L., Mulač M., Pospišil J., Ruda M., Salvet Z.: *The DataGrid Workload Management System: Challenges and Results*.
v časopise *Journal of Grid Computing*, číslo 4, 2005, str. 353–367, ISSN 1570-7873

Cornwall L., Jensen J., Kelsey D., Frohner A., Kouřil D., Bonnassieux F., Nicoud S., Lorentey K., Hahkala J., Silander M., Cecchini R., Ciaschini V., Dell'Agnello L., Spataro F., O'Callaghan D., Mulmo O., Volpato G., Groep D., Steenbakkers M., Mcnab A.: *Authentication and Authorization Mechanisms for Multi-Domain Grid Environments*.
v časopise *Journal of Grid Computing*, číslo 4, 2005, str. 301–311, ISSN 1570-7873

Furman J.: *Jak komunikují akademici?*.
v časopise *Connect!*, číslo 11, 2005, str. 52–53, ISSN 1211-3085

Furman J.: *Mobilita a roaming v sítích národního výzkumu*.
v časopise *Pražská technika*, číslo 2, 2005, str. 42–43, ISSN 1213-5348

Grolmus P., Švamberg M.: *Identity federation nejen v univerzitním prostředí*.
v časopise *Data Security Management*, číslo 1, 2005, str. 14–17, ISSN 1211-8737

Hladká E., Liška M.: *Videokonference na MU – otázky a praxe*.
v časopise *pravodaj Ústavu výpočetní techniky Masarykovy univerzity v Brně*, číslo 1, 2005, str. 5–7, ISSN 1212-0901

Holub P., Liška M.: *High-Definition Video Transmissions for Medical Applications and Education*.
v časopise *Technology and Health Care*, číslo 5, 2005, str. 398–400, ISSN 0928-7329

Holub P., Liška M., Ledvinka J., Kovalský D.: *Vysílání koncertu k výročí 50 let sboru Kantiléna*.
v časopise *Zpravodaj Ústavu výpočetní techniky Masarykovy univerzity v Brně*, číslo 16, 2005, str. 16–20, ISSN 1212-0901

Karásek M., Kaňka J., Radil J., Vojtěch J.: *Large Signal Model of TDM-Pumped Raman Fiber Amplifier*.
v časopise *IEEE PHOTONICS TECHNOLOGY LETTERS*, číslo 9, 2005, str. 1848–1850, ISSN 1041-1135

Kouřil D.: *Bezpečnost v distribuovaném prostředí*.
v časopise *Zpravodaj ÚVT MU*, číslo 4, 2005, str. 2–6, ISSN 1212-0901

Kouřil D.: *Správa soukromých klíčů pomocí hardwarových tokenů*.
v časopise *Zpravodaj ÚVT MU*, číslo 5, 2005, str. 12–16, ISSN 1212-0901

Krsek M.: *Nové vysílání Óčka na internetu*.
v časopise *Pixel*, číslo 12, 2005, str. 50–51, ISSN 1211-5401

Matyska L.: *Softwarové patenty*.
v časopise *Zpravodaj ÚVT MU*, číslo 4, 2005, str. 16–20, ISSN 1212-0901

Novák V.: *Rozvoj páteřní sítě Cesnet2*.
v časopise *Professional Computing*, číslo 6, 2005, str. 58–59, ISSN 1214-5335

Satrapa P.: *Spolehlivý šedý pes*.
v časopise *Click!*, číslo 9, 2005, str. 72–73, ISSN 1801-2345

Vozňák M.: *Co je nového v protokolu SIP*.
v časopise *Connect!*, číslo 01, 2005, str. 52–55, ISSN 1211-3085

Vozňák M.: *Úvodní slovo k IP telefonii*.
v časopise *Connect!*, číslo 05, 2005, str. 6–6, ISSN 1211-3085

Vozňák M., Machálek P.: *ENUM*.
v časopise *Connect!*, číslo 05, 2005, str. 16– 18, ISSN 1211-3085

Vozňák M., Zukal D.: *Hodnocení kvality hlasu v IP sítích*.
v časopise *TECHNOLOGIES & PROSPERITY*, číslo 05, 2005, str. 21–22, ISSN 1213-7162

C.2.2 Příspěvky ve sbornících

Antoš D., Minaříková K., Pospíšil M.: *Programovatelné vyhledávání v síťovém hardwarovém akcelerátoru na principech hardware/software co-designu*.
ve sborníku *Širokopásmové sítě a jejich aplikace*, CESNET a UP Olomouc, 2005, str. 186–195, ISBN 80-244-1035-4

Bažant I., Hrad J.: *Support of Education Using LMS*.
ve sborníku *Proceedings of 16th EAEEIE Annual Conference on Innovation in Education for Electrical and Information Engineering*, Lappeenranta University of Technology, 2005, str. 12, ISBN 952-214-052-X

Ceccanti A., Krajíček O., Křenek A., Matyska L., Ruda M.: *Towards Scalable and Interoperable Grid Monitoring Infrastructure*.
ve sborníku *Proceedings of the first CoreGRID Integration Workshop*, CoreGird, 2005, str. 10–18

Denemark J., Hladká E.: *Pokročilé řízení kolaborativního prostředí*.
ve sborníku *Širokopásmové sítě a jejich aplikace*, CESNET a UP Olomouc, 2005, str. 94–99, ISBN 80-244-1035-4

Denemark J., Kulshrestha A., Allen G.: *Deploying Legacy Applications on Grids*.
ve sborníku *Thirteenth Annual Mardi Gras Conference – Frontiers of Grid Applications and Technologies*, Louisiana State University, 2005, str. 29–34

Dostál O., Javorník M.: *Regionální řešení zpracování medicínských obrazových informací*.
ve sborníku *XXVII. konference EurOpen.CZ*, EurOpen.CZ, 2005, str. 125–130, ISBN 80-86583-09-0

Dostál O., Javorník M., Petrenko M., Slavíček K.: *Projekt MEDIMED – metropolitní PACS archiv v Brně*.
ve sborníku *Širokopásmové sítě a jejich nové aplikace*, CESNET a UP Olomouc, 2005, str. 138–143, ISBN 80-244-1035-4

Furman J.: *Eduroam – mobilita v rámci akademických sítí*.
ve sborníku *Širokopásmové sítě a jejich aplikace*, CESNET a UP Olomouc, 2005, str. 196–201, ISBN 80-244-1035-4

Grolmus P., Švamberg M.: *Single Sign-On řešení pro webové aplikace*.
ve sborníku *XXVII. konference EurOpen.CZ*, EurOpen.CZ, 2005, str. 87–100, ISBN 80-86583-09-0

Hejtmánek L., Matyska L.: *Distribuované Datové Sklady*.
ve sborníku *Širokopásmové sítě a jejich aplikace*, CESNET a UP Olomouc, 2005, str. 168–175, ISBN 80-244-1035-4

Hladká E., Denemark J.: *Communication Support as the User Tool*.
ve sborníku *Proceedings of the 4th International Conference on Emerging e-learning Technologies and Applications*, elfa s. r. o., 2005, str. 283–288, ISBN 80-8086-016-6

Hladká E., Hrdlička T.: *Mobilní přístup k streamovanému videu*.
ve sborníku *Širokopásmové sítě a jejich aplikace*, CESNET a UP Olomouc, 2005, str. 89–93, ISBN 80-244-1035-4

Hladká E., Liška M.: *Infrastruktura pro zpracování záznamů přednášek*.
ve sborníku *Sborník 2. ročníku konference o elektronické podpoře výuky SCO 2005*, MU Brno, 2005, str. 169–174, ISBN 80-210-3699-0

Hladká E., Liška M., Rebok T.: *Stereo Video over IP networks*.
ve sborníku *International Conference on Networking and Services 2005*, 2005, CD

Holub P., Hladká E.: *Ubiquitous User-Empowered Networks of Active Elements*.
ve sborníku *TERENA Networking Conference 2005*, TERENA, 2005, str. 1–3

Holub P., Hladká E., Matyska L.: *Scalability and Robustness of Virtual Multicast for Synchronous Multimedia Distribution*.
ve sborníku *ICN 2005: 4th International Conference on Networking*, Springer-Verlag GmbH, 2005, str. 876–884, ISBN 3-540-25338-6

Javorník M., Dostál O., Andres P.: *Výukový PACS na LF MU*.
ve sborníku *Brněnské onkologické dny. Edukační sborník*, Masarykův onkologický ústav v Brně, 2005, str. 182–183, ISBN 80-7226-798-1

Karásek M., Kaňka J., Radil J.: *Optimization of all-optical gain-clamped lumped Raman fibre amplifier for dynamic performance*.
ve sborníku *Proceedings of 2005 7th International Conference on Traansparent Optical Networks*, Marian Marciniak, 2005, str. 43–46, ISBN 0-7803-9236-1

Karásek M., Peterka P., Radil J.: *Transmission of 2×10 GE channels over 252 km without in-line EDFA*.
ve sborníku *2005 Conference on Optical Network Design and Modelling*, IEEE, 2005, str. 55–58, ISBN 0-7803-8956-5

Kouřil D., Basney J.: *A Credential Renewal Service for Long-Running Jobs*.
ve sborníku *Proceedings of the 6th IEEE/ACM International Workshop on Grid Computing (GRID'05)*, IEEE Computer Society, 2005, str. 63–68, ISBN 0-7803-9493-3

Kouřil D., Matyska L.: *Bezpečnostní infrastruktura METACentra*.
ve sborníku *Širokopásmové sítě a jejich aplikace*, CESNET a UP Olomouc, 2005, str. 117–125, ISBN 80-244-1035-4

Krčmařová G.: *Možnosti spolupráce v rámci sítě národního výzkumu CESNET2*.
ve sborníku *REDEM 05. Management ve výzkumu a vývoji*, MARQ, 2005,
str. 32–38, ISBN 80-86840-11-5

Křenek A., Sebestianová Z.: *Perun – Fault-Tolerant Management of Grid Resources*.
ve sborníku *Cracow Grid Workshop'04 Proceedings*, Academic Computer Centre
CYFRONET AGH, 2005, str. 133–140, ISBN 83-915141-4-5

Krsek M., Doležal I., Illich M.: *Vyhledávání multimediálních záznamů v rozsáhlých heterogenních sítích a Internetu*.
ve sborníku *Knihovny současnosti 2005*, Sdružení knihoven ČR, 2005,
str. 275–280, ISBN 80-86249-33-6

Liška M.: *Snímání, přenos a zobrazování stereoskopického videa ve formátu DV*.
ve sborníku *Širokopásmové sítě a jejich nové aplikace*, CESNET a UP Olomouc,
2005, str. 84–88, ISBN 80-244-1035-4

Martínek T., Zemčík P., Kořenek J.: *FPGA-Based Platform for Network Applications*.
ve sborníku *Proc. of 8th IEEE Design and Diagnostic of Electronic Circuits and Systems Workshop*, University of West Hungary, 2005, str. 194–197,
ISBN 96-393-644871

Matoušek P., Smrčka A., Vojnar T.: *High-Level Modelling, Analysis, and Verification on FPGA-Based Hardware Design*.
ve sborníku *13th International Conference on Correct Hardware Design and Verification Methods – Charme'05*, Springer Verlag, 2005, str. 371–375,
ISBN 000-0302-9743

Matuška M.: *Metaconfiguration of the Computer Network*.
ve sborníku *11th Conference on Information Systems Analysis and Synthesis: Proceedings Vol. 2*, International Federation of Systems Research, 2005,
str. 153–158, ISBN 980-6560-43-4

Mikušek P.: *Návrh a implementace jednotky pro analýzu paketů*.
ve sborníku *Proceedings of the 11th Conference and Competition STUDENT EEICT 2005*, VUT v Brně, 2005, str. 145–148, ISBN 80-214-2888-0

Novák V., Slavíček K.: *Přenos IPv4 multicastu v síti CESNET2*.
ve sborníku *Širokopásmové sítě a jejich aplikace*, UP Olomouc, 2005, str. 100–104,
ISBN 80-244-1035-4

Pazdera J.: *Priority Queues System for Multi-gigabit Network Devices*.
ve sborníku *Proceedings of the International Interdisciplinary Honeywell EMI 2005 Student Competition and Conference*, VUT Brno, 2005, str. 33–35,
ISBN 80-214-2942-9

Pazdera J.: *Systém prioritních front pro IPv6 směrovač*.
ve sborníku *Proceedings of the 11th Conference and Competition STUDENT EEICT 2005*, VUT v Brně, 2005, str. 151–153, ISBN 80-214-2888-0

Pečenka T.: *At-speed Wiring Interconnects Testing on COMBO6 Card*.
ve sborníku *Proc. of 8th IEEE Design and Diagnostic of Electronic Circuits and Systems Workshop*, IEEE, 2005, str. 221–223, ISBN 963-9364-48-7

Petrenko M., Dostál O.: *High Speed Transfer And Archivation of Digital Medical Images*.
ve sborníku *5Th EURASIP Conference*, Slovak University of Technology in Bratislava, 2005, str. 107–113, ISBN 80-86793-05-2

Pitner T.: *Podpora aplikační logiky v J2EE aplikačních rámcích*.
ve sborníku *Sborník konference Objekty 2005*, VŠB-TU Ostrava, 2005, str. 130–142

Pitner T., Adámek P.: *Nástroje pro týmové studentské projekty*.
ve sborníku *Technologie pro e-vzdělávání*, ČVUT Praha, 2005, str. 53–58,
ISBN 80-01-03274-4

Pitner T., Drášil P.: *Standardy v procesech elektronicky podporované výuky*.
ve sborníku *Sborník konference BELCOM 2005*, ČVUT Praha, 2005, str. 100

Pitner T., Ráček J.: *Blended Learning for Building Environmental Awareness*.
ve sborníku *Proceedings of Enviroinfo 2005 Intl. Conference*, MU Brno, 2005, str. 100–107

Procházka M., Rebok T., Holub P.: *Implementace P2P sítě zrcadel v prostředí JXTA*.
ve sborníku *Širokopásmové sítě a jejich aplikace*, CESNET a UP Olomouc, 2005, str. 144–152, ISBN 80-244-1035-4

Rebok T.: *Protokoly transportní vrstvy a jejich kategorizace, transportní protokol ARTP*.
ve sborníku *Širokopásmové sítě a jejich aplikace*, CESNET a UP Olomouc, 2005, str. 153–161, ISBN 80-244-1035-4

Satrapa P.: *Vývoj DNS standardů a technologií*.
ve sborníku *XXVII. konference EurOpen.CZ*, EurOpen.CZ, 2005, str. 21–29, ISBN 80-86583-09-0

Sebestianová Z., Křenek A.: *Evidence gridových uživatelu ve středoevropské virtuální organizaci*.
ve sborníku *DataKon – proceedings of the Annual Database Conference*, MU Brno, 2005, str. 233–240, ISBN 80-210-3813-6

Sitera J., Matyska L., Křenek A., Ruda M., Voců M., Salvet Z., Mulač M.: *Capability and Attribute Based GRID Monitoring Architecture*.

ve sborníku *Cracow Grid Workshop Proceedings*, Academic Computer Centre CYFRONET AGH, 2005, str. 176–183, ISBN 83-915141-4-5

Smrž P., Fapšo M.: *Vyhledávání v záznamech přednášek*.
ve sborníku *Technologie pro e-vzdělávání*, ČVUT Praha, 2005, str. 21–26

Sova M.: *Federativní přístup k autentizaci*.
ve sborníku *Automatizace knihovnických procesů – 10*, ČVUT Praha, 2005, str. 9–15, ISBN 80-01-03228-0

Sverenyák H.: *Co přinese Géant2?*.
ve sborníku *Širokopásmové sítě a jejich aplikace*, CESNET a UP Olomouc, 2005, str. 7–11, ISBN 80-244-1035-4

Šárek M.: *Medicínské aplikace a sdružení CESNET*.
ve sborníku *Širokopásmové sítě a jejich aplikace*, CESNET a UP Olomouc, 2005, str. 136–137, ISBN 80-244-1035-4

Šárek M.: *Telemedicínské aplikace*.
ve sborníku *MEDSOFT 2005 Sborník příspěvků*, Zeithamlová Milena, Ing. – Agentura Action M, 2005, str. 183–186, ISBN 80-86742070-5

Šimák B., Vodrážka J., Boháč L., Hrad J., Zeman T., Bažant I., Bešťák R.: *Modern Forms of Education – Perspectives and Visions*.
ve sborníku *4th International Conference on Emerging E-Learning Technologies and Applications – Conference proceedings. (Information and Telecommunications Technologies in Education)*, ELFA, 2005, str. 421–424, ISBN 80-8086-016-6

Tlučhořová L., Zeman T.: *New Portal eLearning.cesnet.cz – The Way to Edification University Community in the Czech Republic*.
ve sborníku *Proceedings of 16th EAEEIE Annual Conference on Innovation in Education for Electrical and Information Engineering*, Lappeenranta University of Technology, 2005, str. 16, ISBN 952-214-052-X

Tlučhořová L., Zeman T.: *Portal for Elearning Community*.
ve sborníku *Proceedings EC-SIP-M 2005*, STU, FEI, 2005, str. 65–68, ISBN 80-227-2257-X

Tlučhořová L., Zeman T.: *Portál eLearning.cesnet.cz*.
ve sborníku *Proceedings of Emtech 2005 Conference*, ČVUT, 2005, str. 0017_0041, ISBN 80-01-03336-8

Tobola J.: *Rychlé vyhledávání řetězců s využitím FPGA a TCAM*.
ve sborníku *Proceedings of the 11th Conference and Competition STUDENT EEICT 2005*, VUT v Brně, 2005, str. 142–144, ISBN 80-214-2888-0

Ubik S., Cimbál P.: *Tools for TCP Performance Debugging*.
ve sborníku *TERENA Networking Conference 2005*, TERENA, 2005

Vojtěch J., Karásek M., Radil J.: *Další možnosti optického zesilování v pásmu 1310 nm*.
ve sborníku *Optické komunikace 2005*, Zeithamlová Milena, Ing. – Agentura Action M, 2005, str. 145–150, ISBN 80-86742-10-5

Vojtěch J., Karásek M., Radil J.: *Extending the Reach of 10GE at 1310 nm*.
ve sborníku *Proceedings of 2005 7th International Conference on Traansparent Optical Networks*, Marian Marciniak, 2005, str. 39–42, ISBN 0-7803-9236-1

Vojtěch J., Karásek M., Radil J.: *Možnosti dálkových 10 GE přenosů s PC LAN adaptéry*.
ve sborníku *Širokopásmové sítě a jejich aplikace*, CESNET a UP Olomouc, 2005, str. 38–43, ISBN 80-244-1035-4

Vozňák M.: *Autentizace v H.323 a její praktické použití*.
ve sborníku *Sborník příspěvků 6. ročníku semináře KETT*, VŠB-TU Ostrava, 2005, str. 51–54, ISBN 80-248-0833-1

Vozňák M.: *IP telefonie v síti sdružení vysokých škol*.
ve sborníku *Sborník přednášek 4. ročníku odborného semináře Broadband Vision*, Wirelesscom s. r. o. Praha, 2005, str. 76–81

Vozňák M.: *Projekt IP telefonie v síti CESNET2*.
ve sborníku *Sborník příspěvků na mezinárodní konferenci Informatika a kybernetika*, STU Bratislava, 2005, str. 273–278

Vozňák M., Lyko E.: *GNU Gatekeeper jako otevřené řešení komunikace na H.323*.
ve sborníku *Sborník příspěvků 6. ročníku semináře KETT*, VŠB-TU Ostrava, 2005, str. 59–62, ISBN 80-248-0833-1

Vozňák M., Lyko E.: *Otevřené standardy a řešení IP telefonie*.
ve sborníku *Širokopásmové sítě a jejich aplikace*, CESNET a UP Olomouc, 2005, str. 66–70, ISBN 80-244-1035-4

Vozňák M., Zukal D.: *Assessment of VoIP Quality*.
ve sborníku *Proceeding 6th International Conference RTT 2005*, VŠB-TU Ostrava, 2005, str. 641–645, ISBN 80-248-0897-8

Vozňák M., Zukal D.: *E-model pro stanovení kvality hlasu*.
ve sborníku *Sborník příspěvků 6. ročníku semináře KETT*, VŠB-TU Ostrava, 2005, str. 67–71, ISBN 80-248-0833-1

Vozňák M., Zukal D.: *Hodnocení kvality VoIP*.
ve sborníku *Širokopásmové sítě a jejich aplikace*, CESNET a UP Olomouc, 2005, str. 59–65, ISBN 80-244-1035-4

Vozňák M., Zukal D.: *Softwarové analyzátory a jejich využití*.
ve sborníku *Sborník příspěvků EaTT 2005*, VŠB-TU Ostrava, 2005, str. 73–76, ISBN 80-248-0833-1

Wija T.: *Using ENUM with Asterisk*.
ve sborníku *Research in Telecommunication Technology 2005*, VŠB-TU Ostrava, 2005, str. 652–656, ISBN 80-248-0897-8

Wija T., Zukal D.: *Standard ENUM a jeho použití v SW ústředně Asterisk*.
ve sborníku *3. vedecká konferencia Komunikačné a informačné technológie*, Akadémia ozbrojených síl gen. M. R. Štefánika, 2005, str. 131–134, ISBN 80-8040-269-8

Wija T., Zukal D.: *VoIP by Asterisk*.
ve sborníku *Research in Telecommunication Technology 2005*, VŠB-TU Ostrava, 2005, str. 657–660, ISBN 80-248-0897-8

Zeman T., Tlučhořová L.: *Development of eLearning.cesnet.cz Portal*.
ve sborníku *RTT 2005 Proceedings*, VŠB-TU Ostrava, 2005, ISBN 80-248-0897-8

Zeman T., Tlučhořová L.: *Portál k eLearningu*.
ve sborníku *3. vedecká konferencia Komunikačné a informačné technológie*, Akadémia ozbrojených síl gen. M. R. Štefánika, 2005, str. 259–262, ISBN 80-8040-269-8

Zeman T., Tlučhořová L.: *Zvyšování efektivity e-learningu pomocí portálu elearning.cesnet.cz*.
ve sborníku *Sborník příspěvků ze semináře a soutěže eLearning 2005*, Gaudeamus, 2005, str. 401–404, ISBN 80-7041-595-9

Zukal D., Wija T.: *IAX Protokol*.
ve sborníku *3. vedecká konferencia Komunikačné a informačné technológie*, Akadémia ozbrojených síl gen. M. R. Štefánika, 2005, str. 209–212, ISBN 80-8040-269-8

Žádník M.: *Design of Network Monitoring Adapter*.
ve sborníku *Interdisciplinary Student Competition and Conference*, Ing. Zdeněk Novotný CSc., 2005, str. 36–38, ISBN 80-214-2942-9

Žádník M.: *Novel Architecture of NetFlow Adapter*.
ve sborníku *Proceedings of the 11th Conference and Competition STUDENT EEICT 2005*, VUT v Brně, 2005, str. 154–156, ISBN 80-214-2888-0

Žádník M., Pečenka T., Kořenek J.: *NetFlow Probe Intended for High-Speed Networks*.
ve sborníku *Proceedings of the 15th International Conference on Field-Programmable Logic and Applications*, IEEE CS, 2005, str. 695–698

C.3 Částečně recenzované a nerecenzované publikace

C.3.1 Prezentace v oblasti VaV

Dostál O., Brechlerová D.: *Vybrané právní aspekty vedení zdravotnické dokumentace a telemedicíny*.
Praha, EuroMISE centrum
http://www.euromise.cz/

Kňourek J., Šašek J.: *Paralelní MSC.MARC na clusterech METACentra*.
Brno, MSC.Software s. r. o., Brno, 2005
http://zsc.zcu.cz/download/marc2005.pdf

Satrapa P., Adamec P., Novák V.: *IPv6 in CESNET2 Network – 6PE Deployment Experience*.
Global IPv6 Summit, Consulintel, IPv6 Forum
http://www.ipv6-es.com/05/in/i-documentos.php

Ubik S., Čížek M.: *Paralelizace datových přenosů na transportní vrstvě*.
Olomouc, CESNET, z. s. p. o., ISBN 80-244-1035-4

Vojtěch J., Radil J., Šíma S.: *Deliverable 2.1. Dark Fibre Lighting Technologies*.
http://www.seefire.org/content/modules/downloads/SEEFIRE-WP2-Deliverable2.1-p-20051115-v1.pdf

C.3.2 Odborné publikace výukové

Červenka A.: *Webové rozhraní pro administraci UDP reflektoru*.
Fakulta informatiky, Masarykova univerzita v Brně, 2005

Filip T.: *Testování spojů na desce COMBO6*.
Fakulta informačních technologií, Vysoké učení technické v Brně, 2005

Havlík A.: *Automatická indexace FTP a SMB serverů 2*.
Fakulta informatiky Masarykovy univerzity v Brně, 2005

Holeček J.: *Formal Verification of Memory Scheduler*.
Faculty of Informatics, Masaryk University, Brno, 2005

Holer V.: *Systém správy multimediální místnosti*.
FI MU, 2005

Holub P.: *Network and Grid Support for Mulitmedia Distribution and Processing*.
Fakulta informatiky, Masarykova univerzita v Brně, 2005

Janoušek M.: *Řadič Gb rozhrani implementovaný v CPLD*.
FIT, VUT Brno, 2005

Kratochvíla T.: *Formal Verification of Hardware Design*.
Faculty of Informatics, Masaryk University Brno, 2005

Kubalec J.: *Routování v Internetu*.
FJFI ČVUT, 2005

Liška M.: *Design and Implementation of Capturing, Transmission, and Display of Stereoscopic Video in DV Format*.
FI MU, 2005

Mikušek P.: *Návrh a implementace procesní jednotky pro analýzu vstupních paketů*.
Fakulta informačních technologií, Vysoké učení technické v Brně, 2005

Minaříková K.: *Computing Look-up Programs of Routing Accelerator*.
FI MU, 2005

Pazdera J.: *Implementace systému prioritních front v FPGA*.
FIT, VUT Brno, 2005

Pospíšil M.: *SCAMPIDUMP – monitorování provozu sítě v hardwaru*.
FI MU, 2005

Rybka T.: *Generické křížové nástroje pro procesory implementované v hradlových polích*.
Masarykova univerzita, 2005

Tobola J.: *Vyhledávání řetězců v payloadu paketu s využitím TCAM*.
FIT, VUT Brno, 2005

Zachr V.: *Simulační model nanoprocesorů směrovače COMBO6*.
Masarykova univerzita, Fakulta informatiky, 2005

Zloský O.: *Protokol komunikace směrovačů s konfiguračním systémem Netopeer*.
Fakulta informatiky, Masarykova univerzita, Brno, 2005

Žádník M.: *Design of network traffic monitoring adapter*.
FIT, VUT Brno, 2005

C.3.3 Popularizační články

Hladká E., Matyska L.: *Mobilita napříč sítěmi*.
v časopise *Zpravodaj ÚVT MU*, číslo 4, 15, str. 13–16, ISSN 1212-0901

Holub P., Radil J.: *Akademické lambda sítě u nás a ve světě*.
v časopise *Zpravodaj ÚVT MU*, číslo 3, 15, str. 6–12, ISSN 1212-0901

Kmuníček J.: *Gridy jako klíčový fenomén informačních technologií nového tisíciletí*.
v časopise *Zpravodaj ÚVT MU*, číslo 2, 16, str. 1–5, ISSN 1212-0901

Krčmařová G.: *CESNET a výzkum a vývoj*.
v časopise *Inovační podnikání a transfer technologií*, číslo 4/2005, Neuveden, str. 7–8, ISSN 1210-4612

Krsek M.: *RealProducer 10*.
v časopise *Pixel*, číslo 3, 2005, str. 22–23, ISSN 1211-5401

Krsek M.: *Telestream FlipFactory*.
v časopise *Pixel*, číslo 10, 2005, str. 30–31, ISSN 1211-5401

Lhotka L.: *Obecná veřejná licence GNU*.
v časopise *Zpravodaj ÚVT MU*, číslo 5, 15, str. 16–20, ISSN 1212-0901

Lhotka L.: *Svobodný software a základní otázka programování*.
v časopise *Zpravodaj ÚVT MU*, číslo 3, 15, str. 12–16, ISSN 1212-0901

Pužmanová R.: *Dostupné gigabitové sítě*.
v časopise *Connect!*, číslo 7-8/2005, 10, str. 53–55, ISSN 1211-3085

Pužmanová R.: *Konečně svítá. Revitalizace zájmu o IPv6*.
v časopise *Connect!*, číslo 12/2005, 10, str. 44–46, ISSN 1211-3085

Pužmanová R.: *Monitoring a analýza sítě*.
v časopise *Professional Computing*, číslo 10/2005, 6, str. 51–53, ISSN 1214-5335

Pužmanová R.: *Optické sítě zažívají druhý boom*.
v časopise *Professional Computing*, číslo 12/2005, 6, str. 29–31, ISSN 1214-5335

Pužmanová R.: *Optický datový spoj bez kabelu*.
v časopise *Sdělovací technika*, číslo 7/2005, 2005, str. 7–9, ISSN 0036-9942

C.3.4 Články v elektronických časopisech

Krsek M.: *Jak vystavit video na Internetu*.
v časopise *Lupa*, číslo 7.9., 2005, str. 1–1, ISSN 1213-0702

Pužmanová R.: *Mezinárodní peering jednodušší díky EoMPLS*.
v časopise *Lupa*, číslo 30.12.2004, 2005, ISSN 1213-0702

Satrapa P.: *6PE – nenásilné zavedení IPv6 do páteřní sítě*.
v časopise *Lupa*, číslo 3. 3., 2005, ISSN 1213-0702

Satrapa P.: *Dosahy IPv6 adres*.
v časopise *Lupa*, číslo 15. 9., 2005, ISSN 1213-0702

Satrapa P.: *E2Epi a JRA1 – výkon až na stůl*.
v časopise *Lupa*, číslo 28. 4., 2005, ISSN 1213-0702

Satrapa P.: *GÉANT2 – co se chystá*.
v časopise *Lupa*, číslo 27. 10., 2005, ISSN 1213-0702

Satrapa P.: *IPv6 Global Summit v Barceloně*.
v časopise *Lupa*, číslo 16. 6., 2005, ISSN 1213-0702

Satrapa P.: *Jak jsou na tom čeští ISP s IPv6?*.
v časopise *Lupa*, číslo 17. 3., 2005, ISSN 1213-0702

Satrapa P.: *Jaké jsou perspektivy DNS?*.
v časopise *Lupa*, číslo 12. 5., 2005, ISSN 1213-0702

Satrapa P.: *NAT vesus NAP*.
v časopise *Lupa*, číslo 30. 6., 2005, ISSN 1213-0702

Satrapa P.: *Netiketa*.
v časopise *Lupa*, číslo 31. 3., 2005, ISSN 1213-0702

Satrapa P.: *Pohnou se hranice v IPv6 adresách?*.
v časopise *Lupa*, číslo 13. 10., 2005, ISSN 1213-0702

Satrapa P.: *SEEFIRE – temná vlákna pro jihovýchodní Evropu*.
v časopise *Lupa*, číslo 14. 4., 2005, ISSN 1213-0702

Satrapa P.: *Shibboleth – identifikujte se jen jednou*.
v časopise *Lupa*, číslo 8. 12., 2005, ISSN 1213-0702

Satrapa P.: *Síťové rychlostní rekordy – tak trochu dekadence*.
v časopise *Lupa*, číslo 29. 9., 2005, ISSN 1213-0702

Satrapa P.: *TERENA kompendium 2005*.
v časopise *Lupa*, číslo 10. 11., 2005, ISSN 1213-0702

Satrapa P.: *Unikátní lokální adresy pro IPv6*.
v časopise *Lupa*, číslo 24. 11., 2005, ISSN 1213-0702

Satrapa P.: *Věrohodné DNS čili DNSSEC*.
v časopise *Lupa*, číslo 26. 5., 2005, ISSN 1213-0702

C.3.5 Technické zprávy

Svoboda J., Těthal O.: *Čipové technologie v prostředí VŠ pro ID-karty a aplikace s elektronickým podpisem*.
technická zpráva číslo 1/2005, CESNET, 2005
http://www.cesnet.cz/doc/techzpravy/2005/cipidkarty/cipidkarty.pdf

Bažant I.: *Metodika tvorby výukových materiálů v Authorwaru podle SCORM*.
technická zpráva číslo 2/2005, CESNET, 2005
http://www.cesnet.cz/doc/techzpravy/2005/scorm/

Šmejkal I., Veselá B.: *Microsoft Producer – racionalizace tvorby multimediálních prezentací*.
technická zpráva číslo 3/2005, CESNET, 2005
http://www.cesnet.cz/doc/techzpravy/2005/msproducer/

Antoš D.: *Combining routing and ARP to a single lookup operation*.
technická zpráva číslo 4/2005, CESNET, 2005
http://www.cesnet.cz/doc/techzpravy/2005/singlelookup/singlelookup.pdf

Adamec P., Satrapa P.: *Konfigurace lokální sítě připojené k eduroam.cz*.
technická zpráva číslo 5/2005, CESNET, 2005
http://www.cesnet.cz/doc/techzpravy/2005/eduroamcfg/

Hájek J.: *Optimalizace pracoviště pro zavedení bezdrátových přenosů videosignálu*.
technická zpráva číslo 6/2005, CESNET, 2005
http://www.cesnet.cz/doc/techzpravy/2005/bezdr-video/bezdr-video.pdf

Grolmus P.: *WebISO – Single Sign-On řešení pro WWW*.
technická zpráva číslo 7/2005, CESNET, 2005
http://www.cesnet.cz/doc/techzpravy/2005/webiso/

Matoušek P., Smrčka A., Vojnar T.: *High-level Modelling, Analysis and Verification on FPGA-based Hardware Design*.
technická zpráva číslo 8/2005, CESNET, 2005
http://www.cesnet.cz/doc/techzpravy/2005/lup/

Košňar T.: *G3 System User Interface Prototype*.
technická zpráva číslo 9/2005, CESNET, 2005
http://www.cesnet.cz/doc/techzpravy/2005/g3/

Vozňák M., Neuman M.: *GNU Gatekeeper a jeho nasazení v síti CESNET2*.
technická zpráva číslo 10/2005, CESNET, 2005
http://www.cesnet.cz/doc/techzpravy/2005/voip/gnugk.pdf

Vozňák M., Zukal D.: *Kvalita hovoru v prostředí VoIP*.
technická zpráva číslo 11/2005, CESNET, 2005
http://www.cesnet.cz/doc/techzpravy/2005/voip/kvalitahovoru.pdf

Wija T., Zukal D., Vozňák M.: *Asterisk a jeho použití*.
technická zpráva číslo 12/2005, CESNET, 2005
http://www.cesnet.cz/doc/techzpravy/2005/voip/asterisk.pdf

Vozňák M., Zukal D.: *Analýza VoIP aplikací Surveyor 7.0*.
technická zpráva číslo 13/2005, CESNET, 2005
http://www.cesnet.cz/doc/techzpravy/2005/voip/surveyor.pdf

Kácha P.: *Přehled a doporučení antispamových řešení*.
technická zpráva číslo 14/2005, CESNET, 2005
http://www.cesnet.cz/doc/techzpravy/2005/antispam/

Sitera J.: *LDAP service for VOCE*.
technická zpráva číslo 15/2005, CESNET, 2005
http://www.cesnet.cz/doc/techzpravy/2005/voceldap/

Hájek J., Svítek J.: *IP videokonference – nástroj pro sdílenou přednášku s možností obousměrné komunikace*.
technická zpráva číslo 16/2005, CESNET, 2005
http://www.cesnet.cz/doc/techzpravy/2005/sdileneprednasky/sdileneprednasky.pdf

Bažant I.: *Využití streamovaného videa ve výukových kurzech*.
technická zpráva číslo 17/2005, CESNET, 2005
http://www.cesnet.cz/doc/techzpravy/2005/streamvideo/

Tlučhořová L.: *Údržba a rozšiřování portálu eLearning.cesnet.cz*.
technická zpráva číslo 18/2005, CESNET, 2005
http://www.cesnet.cz/doc/techzpravy/2005/elearning/

Vachek P.: *Bezpečnostní audit lokálních strojů*.
technická zpráva číslo 19/2005, CESNET, 2005
http://www.cesnet.cz/doc/techzpravy/2005/lansec/

Kropáčová A., Kácha P.: *Řešení bezpečnostních incidentů*.
technická zpráva číslo 20/2005, CESNET, 2005
http://www.cesnet.cz/doc/techzpravy/2005/inchandling/

Beneš P., Čermák P., Davídek T., Fiala L., Hampl J., Chvála O., Král J., Lokajíček M., Sandler K., Švec J.: *Realizace optických sítí pro aplikace zpracování dat ve fyzice částic, aktualizace v roce 2005*.
technická zpráva číslo 21/2005, CESNET, 2005
http://www.cesnet.cz/doc/techzpravy/2005/optsite/optsite.pdf

Šmejkal I., Michalik P., Veselá B.: *ConferenceXP*.
technická zpráva číslo 22/2005, CESNET, 2005
http://www.cesnet.cz/doc/techzpravy/2005/conferencexp/

Krsek M.: *Streaming multimediálního obsahu s vysokým rozlišením*.
technická zpráva číslo 23/2005, CESNET, 2005
http://www.cesnet.cz/doc/techzpravy/2005/hirestreaming/

Čížek J., Wimmer M.: *Bezdrátový spoj pro pásmo 5 GHz – WinLink 1000*.
technická zpráva číslo 24/2005, CESNET, 2005
http://www.cesnet.cz/doc/techzpravy/2005/winlink/

Wimmer M., Čížek J.: *Soudobé trendy v oblasti moderních bezdrátových spojů*.
technická zpráva číslo 25/2005, CESNET, 2005
http://www.cesnet.cz/doc/techzpravy/2005/trendy/

Hulínský I.: *Videokonferenční H.323 infrastruktura v síti CESNET2*.
technická zpráva číslo 26/2005, CESNET, 2005
http://www.cesnet.cz/doc/techzpravy/2005/h323infra/

Hlávka P., Kratochvíla T., Řehák V., Šafránek D., Šimeček P., Vojnar T.: *CRC64 Algorithm Analysis and Verification*.
technická zpráva číslo 27/2005, CESNET, 2005
http://www.cesnet.cz/doc/techzpravy/2005/crc64/

Wimmer M.: *Vysílání a přenos audio signálu ve velmi vysoké kvalitě*.
technická zpráva číslo 28/2005, CESNET, 2005
http://www.cesnet.cz/doc/techzpravy/2005/audio/

Doležal I., Sullivan E.: *Semi-automated Mass Production of E-Learning Content*.
technická zpráva číslo 29/2005, CESNET, 2005
http://www.cesnet.cz/doc/techzpravy/2005/autenc/

Vojtěch J.: *Nasazení prototypu CLA PB01 v testbedu CzechLight a síti CESNET2*.
technická zpráva číslo 30/2005, CESNET, 2005
http://www.cesnet.cz/doc/techzpravy/2005/clapb01/clapb01.pdf

Šárek M., Slavíček K., Kršek P., Krupa P.: *Komunikační podpora Virtuálního vývojového a aplikačního pracoviště*.
technická zpráva číslo 31/2005, CESNET, 2005
http://www.cesnet.cz/doc/techzpravy/2005/virtprac/virtprac.pdf

Žádník M., Lhotka L.: *Hardware-Accelerated NetFlow Probe*.
technická zpráva číslo 32/2005, CESNET, 2005
http://www.cesnet.cz/doc/techzpravy/2005/nflowhw/

Čeleda P., Kováčik M., Krejčí R., Kysela J., Špringl P.: *Software for NetFlow Monitoring Adapter*.
technická zpráva číslo 33/2005, CESNET, 2005
http://www.cesnet.cz/doc/techzpravy/2005/netflow/

Jindra P.: *USB token v prostředí CESNET CA*.
technická zpráva číslo 34/2005, CESNET, 2005
http://www.cesnet.cz/doc/techzpravy/2005/usbtokeny/

Furman J.: *Pilotní projekt eduroam.cz*.
technická zpráva číslo 35/2005, CESNET, 2005
http://www.cesnet.cz/doc/techzpravy/2005/eduroampilot/

Tomášek J.: *Systém LAI – předregistrace požadavků o certifikát*.
technická zpráva číslo 36/2005, CESNET, 2005
http://www.cesnet.cz/doc/techzpravy/2005/lai/

C.4 Ostatní

C.4.1 Odborná vystoupení bez publikace

Altmanová L.: *Fibre lease contracts*.
http://www.seefire.org/content/modules/downloads/SEEFIRE-Sofia-Altmannova.ppt

Antoš D.: *Routing and Filtering Decision in a Single Operation*.
TERENA Networking Conference 2005, Poznan Poland, TERENA

Antoš D., Řehák V.: *Routing and Filtering in a Single Operation*.
Znojmo, FI MU a FIT VUT Brno

Chudoba J.: *Large scale simulations on the EGEE Grid*.
http://www.egee.hu/grid05/download/day_3/Wednesday_Chudoba.ppt

Chudoba J.: *Some operational activities in the Czech Republic*.
3rd EGEE conference
http://grid.cyfronet.pl/egee/tiki-index.php?page=Athens+CE+ROC+Meeting

Chudoba J.: *Zpracování dat v částicové fyzice*.
CESNET, z. s. p. o.
http://www.cesnet.cz/doc/seminare/20051107/

Dostál O.: *Vybrané právní aspekty využití informačních technologií v medicíně*.
Sdělovací technika
http://www.convergence.cz

Dvořák F., Kouřil D., Křenek A., Matyska L., Mulač M., Pospíšil J., Ruda M., Salvet Z., Sitera J., Škrabal J., Voců M.: *Services for Tracking and Archival of Grid Job Information*.
ACC Cyfronet AGH
http://www.cyfronet.krakow.pl/cgw05/programme.html

Holub P.: *Grid Video Processing: Distributed Approach to Video Processing*.
Philadelphia, USA, Internet 2 Fall Member Meeting 2005

Holub P.: *High-Definition Video at CESNET*.
Philadelphia, USA, Internet 2 Fall Member Meeting 2005

Holub P., Liška M.: *Lecture Recording, Processing, Archiving, and Streaming Workflow Based on Grids and Distributed Storage*.
Atlanta, Georgia, USA, SURA/ViDe
http://vide.net/conferences/spr2005/show4.shtml

Holub P., Rebok T., Liška M.: *Videokonferenční technologie a přenosy videa*.
Srní, EurOpen, 2005

Javorník M., Dostál O.: *Výuka v rámci projektu MeDiMed*.
Radiologické společnosti ČLS JEP
http://www.symma.cz

Karásek M., Radil J., Vojtěch J.: *Optical amplifiers in CzechLight and CESNET2*.
Praha, CESNET
http://www.ces.net/doc/seminars/20050516/pr/karasek-radil-vojtech.ppt

Kmuníček J.: *Comments concerning user support within CE region*.
Athens, Greece, EGEE Third Conference, CE ROC Meeting

Kmuníček J.: *Current status of EGEE activities within CE region*.
Pisa, Italy, EGEE Fourth Conference, CE ROC Meeting

Kmuníček J.: *Úvod do použití Gridů*.
Praha, Seminář pro uživatele EGEE Gridu

Kmuníček J.: *VOCE Status*.
Pisa, Italy, EGEE Fourth Conference, NA3 CE Meeting

Kmuníček J.: *VOCE Status*.
Praha, Seminář pro uživatele EGEE Gridu

Kmuníček J., Kouřil D., Chudoba J., Fiala L., Kosina J., Lokajíček M., Matyska L., Ruda M., Švec J.: *VOCE - A Grid Environment for Central Europe*.
Cracow, Poland, Cracow Grid Workshop 2005

Kmuníček J., Kulhánek P., Petřek M.: *CHARON System*.
Pisa, Italy, EGEE Fourth Conference, NA3 CE Meeting

Kmuníček J., Kulhánek P., Petřek M.: *CHARON System - A Framework for Comfortable Grid Applications & Jobs Management*.
Pisa, Italy, EGEE Fourth Conference

Kmuníček J., Kulhánek P., Petřek M.: *CHARON System – Framework for Applications and Jobs Management in Grid Environment*.
Cracow, Poland, Cracow Grid Workshop 2005

Kouřil D., Matyska L.: *The VOCE (VO Central Europe) Environment*.
Budapest, Hungary
http://www.egee.hu/grid05/download/day_4/egee05-voce.pdf

Kovács A., Vojtěch J.: *Optical technologies: XENPAK, XFP and DWDM*.
http://czechlight.cesnet.cz/2/publications/SEEFIRE-WP2-Sofia-Kovacs-b-2005-07-12.ppt

Křenek A.: *Sledování gridových úloh z pohledu uživatele*.
Praha, CESNET
http://egee.cesnet.cz/cs/events/third.html

Křenek A., Krajíček O., Matyska L., Ruda M., Sitera J.: *Capability Languages in C-GMA*.
Krakov, Polsko, Cracow Grid Workshop
http://www.cyf-kr.edu.pl/cgw05/presentations/c10-1.pdf

Krsek M.: *Internet search in multimedia data*.
http://www.vanderbilt.edu/DIVERSE2005/

Krsek M., Doležal I.: *Role knihoven v zašíťovaném světě*.
Seč u Chrudimi, Sdružení knihoven ČR

Krsek M., Doležal I., Illich M.: *Metaarchive for Multimedia Assets*.
http://events.internet2.edu/2005/fall-mm/demos.html#meta

Kuba M.: *Tutoriál Web Services*.
Monínec, EurOpen.CZ
http://www.ics.muni.cz/ makub/soap/europen2005/TutorialWebServicesMakub.pdf

Kulhánek P.: *Systém CHARON*.
Prague, Czech republic, Seminar for Users of EGEE Grid

Lhotka L.: *Autonomous Netflow Probe*.
Wien, Austria, Telecommunications Research Centre Vienna
http://www.ftw.at/ftw/events/telekommunikationsforum

Lhotka L., Novotný J.: *Liberouter*.
Longyearbyen, Svalbard, NORDUnet
http://www.nordunet2005.no/presentation.php?uniqueidentifier=41495c59e8a8d

Lhotka L., Žádník M.: *Autonomous Netflow Probe*.
Lisabon, Portugalsko, TERENA
http://www.terena.nl/tech/task-forces/tf-csirt/meeting16/netflow-probe-lhotka.pdf

Liška M.: *HDTV: The new quality for video transmissions*.
Znojmo, Memics2005
http://www.fi.muni.cz/memics05/

Liška M.: *Stereoscopic Video Using DV Format*.
Philadelphia, USA, Internet2
http://www.internet2.edu/presentations/fall05/20050921-video-liska.pdf

Matyska L., Fiala L., Chudoba J., Kosina J., Krásová J., Lokajíček M., Švec J., Kmuníček J., Kouřil D., Ruda M., Salvet Z., Mulač M.: *Particle Physics Grid Deployment in the Czech Republic*.
Varna (Bulgaria), International Symposium on Nuclear Electronics and Computing

Novák V.: *Optical Network and DWDM Deployment in Cesnet2*.
interní zpráva, CESNET

Novotný J.: *Panel Discussion about the Future of Network Monitoring*.
Poznań, Terena
http://www.terena.nl/conferences/tnc2005/core/getfile.php?file_id=320

Novotný J.: *Programmable Hardware in Networking*.
Wien, Austria, Telecommunications Research Centre Vienna
http://www.ftw.at/ftw/events/telekommunikationsforum

Petřek M., Kulhánek P., Kmuníček J.: *Distribuované výpočty a GRID: prostředky a zkušenosti*.
Ostrava, Czech republic, Institute of Geonics

Procházka M.: *Distributed system for multimedia data distribution*.
Znojmo
http://sitola.fi.muni.cz/\%7Etauceti/?download=abstract.pdf

Radil J.: *Optical Signals Modulation and Compensation of Chromatic Dispersion*.
http://czechlight.cesnet.cz/2/publications/SEEFIRE-Sofia-Radil.pdf

Rebok T., Denemark J.: *Data Distribution Models in Network of Active Elements*.
MEMICS'05, Znojmo, ČR, MEMICS'05

Ruda M.: *EGEE middleware for grid application developers*.
http://agenda.cern.ch/askArchive.php?base=agenda&categ=a055706&id=a055706s0t3/transparencies

Smotlacha V.: *Full Packet Monitoring Sensors: Hardware and Software Challenges*.
Poznan, Poland
http://www.terena.nl/conferences/tnc2005/programme/presentations/show.php?pres_id=137

Smotlacha V.: *SCAMPI – architecture for monitoring of high speed networks*.
http://www.nordunet2005.no/presentation.php?uniqueidentifier=414ae9b7e9fe7

Sova M.: *NRENs supporting Grids using current Grid Technology*.
TERENA
http://www.terena.nl/tech/grid/workshop-02/ws02-milan.ppt

Sova M.: *PKI*.
TERENA
http://www.terena.nl/tech/eurocamp/nov05/slides/day1/PKI-ms.pdf

Šárek M.: *Komunikační infrastruktura pro eHealth*.
Sdělovací technika
http://www.convergence.cz

Šárek M.: *Medical applications and high speed networking*.
Praha, EMBEC'05 & IFMBE, 20051120

Šárek M.: *Technické aspekty eZdraví*.
Medtel o. p. s, Praha
http://www.medtel.cz

Šárek M.: *Telemedicínské aplikace*.
Radiologické společnosti ČLS JEP
http://www.symma.cz

Šíma S.: *CEF network design*.
http://www.seefire.org/content/modules/downloads/SofiaSima1ext.ppt

Šíma S.: *Cross Border CEF Networks*.
http://www.internet2.edu/presentations/fall05/20050919-itf-sima.ppt

Šíma S., Altmanová L.: *Development of CEF networks design*.
http://www.ces.net/doc/seminars/20050516/

Vojtěch J.: *CzechLight & CzechLight Amplifiers*.
Zurich,Switzerland, TERENA
http://www.terena.nl/tech/task-forces/tf-ngn/presentations/tf-ngn17/vojtech-czechlight.pdf

Vojtěch J.: *Optical Amplifiers and Line Spans*.
http://czechlight.cesnet.cz/2/publications/SEEFIRE-WP2-Sofia-Vojtech-a-2005-07-14.ppt

C.4.2 Prototypy

Hejtmánek L.: *libxio – IBP enabling library*.

Hladká E., Denemark J., Holub P.: *rum – User-Empowered Packet Reflector and Processor*.

Košňar T.: *Prototyp uživatelského rozhraní systému G3*.

Kouřil D., Křenek A., Matyska L., Mulač M., Škrabal J., Pospišil J., Ruda M., Salvet Z., Sitera J., Voců M., Dvořák F.: *Job Provenance Service*.

Kouřil D., Křenek A., Matyska L., Mulač M., Škrabal J., Pospišil J., Ruda M., Salvet Z., Sitera J., Voců M., Dvořák F.: *Proxy Renewal Service*.

Kouřil D., Křenek A., Matyska L., Pospišil J., Ruda M., Salvet Z., Sitera J., Škrabal J., Voců M., Mulač M., Dvořák F.: *Logging and Bookkeeping Service*.

Krsek M.: *Platforma pro streaming multimediálního obsahu s vysokým rozlišením*.

Kuba M., Sebestianová Z., Kmuníček J.: *Prototyp portálového uživatelského rozhraní pro gridové prostředí*.

Kulhánek P., Petřek M., Kmuníček J.: *CHARON System*.

Novotný J., Bardas R.: *COMBO-4SFPRO*.

Novotný J., Bardas R.: *COMBO6X*.

Novotný J., Smotlacha V., Bardas R.: *COMBO-PTM*.

Novotný J., Šíma S., Bardas R.: *COMBO-BOOT*.

Sebestianová Z., Křenek A., Kuba M.: *Perun – systém pro správu uživatelských účtu*.

Vojtěch J., Radil J., Šíma S.: *CLA DI01*.

Vojtěch J., Radil J., Šíma S.: *CLA PB01*.

C.4.3 Uspořádané semináře a konference

CEF Networks Worshop 2005
16.–18. 5. 2005
http://www.ces.net/doc/seminars/20050516/

Širokopásmové sítě a jejich aplikace
24.–25. 5. 2005, společně s Univerzitou Palackého v Olomouci
http://cvt.upol.cz/konference/

All hands JRA1
20.–22. 6. 2005
seminář řešitelů aktivity JRA1 a schůze EGEE Design týmu

Roaming – mobilita – projekt eduroam
22. 6. 2005
http://www.cesnet.cz/doc/seminare/20050622/

Vysokorychlostní sítě pro vědu a výzkum
7. 11. 2005
http://www.cesnet.cz/doc/seminare/20051107/

Bezpečnost na síti
14. 11. 2005
http://www.cesnet.cz/doc/seminare/20051114/

IP telefonie
15. 11. 2005
http://www.cesnet.cz/doc/seminare/20051115/

IBM WebSphere portál
24. 11. 2005, společně se Západočeskou univerzitou v Plzni
http://www.cesnet.cz/doc/seminare/20051124/

Seminář pro uživatele EGEE Gridu
13. 12. 2005
http://www.cesnet.cz/doc/seminare/20051213/

D Literatura

Literatura

[ABK01] Andersen D., Balakrishnan H., Kaashoek F., Morris R.: *Resilient overlay networks*.
v *18th ACM Symp. on Operating Systems Princpiles (SOSP)*, Ban, Canada, 2001

[Ant05] Antoš, D.: *Combining routing and ARP to a single lookup operation*.
Technická zpráva CESNET 4/2005, CESNET, 2005

[ClS04] Clark Ch., Schimmel D.: *Scalable Pattern Matching for High-Speed Networks*.
ve sborníku *IEEE Symposium on Field-Programmable Custom Computing Machines (FCCM)*, Napa, California, 2004, str. 249–257

[Dun05] Dunmore M. (editor): *6net: An IPv6 Deployment Guide*.
University of Lancaster, 2005, 425 stran, ISBN 1-86220-173-0

[Fur05] Fürman J: *Pilotní projekt eduroam.cz*
technická zpráva CESNET 35/2005, CESNET, 2005

[Gro05] Grolmus P: *WebISO – Single Sign-On řešení pro WWW*.
technická zpráva CESNET 7/2005, CESNET, 2005

[HHD04] Hladká E., Holub P., Denemark J.: *User Empowered Virtual Multicast for Multimedia Communication*.
v *ICN'04 Conference Proceedings*, 2004, ISBN 0-86341-325-0, str. 338–343

[HlS01] Hladká E., Salvet Z.: *An active network architecture: Distributed computer or transport medium*.
v *P. Lorenz (editor): Networking - ICN 2001: First International Conference*, Colmar, France, Part II, volume 2094 of Lecture Notes in Computer Science, Springer-Verlag, str. 612–619

[HoH05] Holub P., Hladká E.: *Ubiquitous User-Empowered Networks of Active Elements*.
v *TERENA Networking Conference 2005*, Poznan, Poland

[HHM05] Holub P., Hladká E., Matyska L.: *Scalability and Robustness of Virtual Multicast for Synchronous Multimedia Distribution*.
v *Networking – ICN 2005: 4th International Conference on Networking*, Reunion Island, France, Part II. Lecture Notes in Computer Science 3421, Springer-Verlag GmbH, 2005, ISBN 3-540-25338-6, str. 876–883

[Jin05] Jindra P: *USB token v prostředí CESNET CA*.
technická zpráva CESNET 34/2005, CESNET, 2005

[JXTA] *JXTA*.
http://www.jxta.org/

[Košˇ05] Košňar, T.: *G3 System User Interface Prototype*.
technická zpráva CESNET 9/2005, CESNET, 2005

[Mat05] Matuška, M.: *Metaconfiguration of the computer network*.
ve sborníku *Proceedings of the 11th Conference on Information Systems Analysis and Synthesis, Orlando, Florida* IFSR, 2005, ISBN 980-6560-43-4, str. 153–158

[PGL02] Perkins C., Gharai L., Lehman T., Mankin A.: *Experiments with delivery of HDTV over IP networks*.
v *12th International Packet Video Workshop*, Pittsburgh, PA, USA, 2002

[Sov04] Sova M: *AAI a mobilita*.
v *Optická síť národního výzkumu a její nové aplikace 2004*, CESNET, 2005, ISBN 80-239-4256-5

[Sov05] Sova M.:*Federativní přístup k autentizaci*.
ve sborníku *Automatizace knihovnických procesů – 10*, ČVUT, 2005, ISBN 80-01-03228–0, str. 9–15

[Tom05] Tomášek J.: *Systém LAI – preregistrace koncových entit*.
technická zpráva CESNET 36/2005, CESNET, 2005

[VoN05] Vozňák M., Neuman M.: *GNU Gatekeeper a jeho nasazení v síti CESNET2*.
technická zpráva CESNET 10/2005, CESNET, 2005

[VoZ05] Vozňák M., Zukal D.: *Analýza VoIP aplikací Surveyor 7.0*.
technická zpráva CESNET 13/2005, CESNET, 2005

[VoZ05a] Vozňák M., Zukal D.: *Kvalita hovoru v prostředí VoIP*.
technická zpráva CESNET 11/2005, CESNET, 2005

[WZV05] Wija T., Zukal D., Vozňák M.: *Asterisk a jeho použití*.
technická zpráva CESNET 12/2005, CESNET, 2005

[Zlo05] Zloský O.: *Protokol komunikace směrovačů s konfiguračním systémem Netopeer*.
diplomová práce Fakulty informatiky MU, Brno, 2005

[ŽáL05] Žádník M., Lhotka L.: *Hardware-Accelerated NetFlow Probe*.
technická zpráva CESNET 32/2005, CESNET, 2005

[ZPK05] Žádník M., Pečenka T., Kořenek J.: *NetFlow Probe Intended for High-Speed Networks*.
ve sborníku Rissa, T., Wilton, S., Leong, P. (Ed.), *Proceedings of the International Conference on Field Programmable Logic and Applications (FPL05)*, Tampere, IEEE CS, 2005, ISBN 0-7803-9362-7, str. 695–698