

Distribuovaná virtuální laboratoř počítačových sítí

Hlavní řešitel:

Ing. Petr Grygárek, Ph.D.,

Fakulta elektrotechniky a informatiky, VŠB-Technická univerzita Ostrava.

Spoluřešitelé:

Ing. Lukáš Macura,

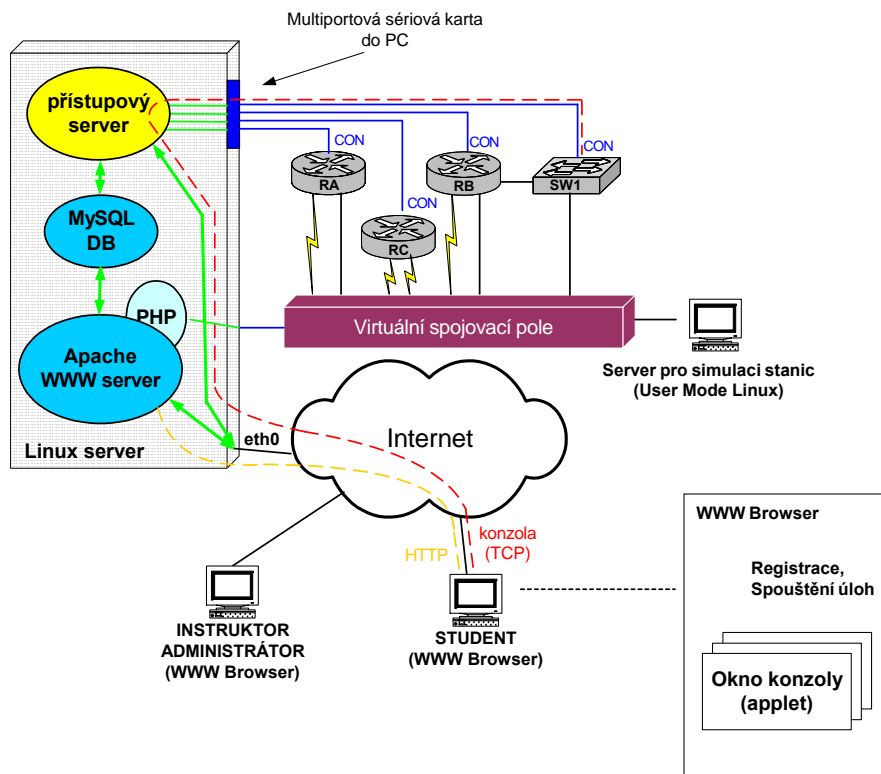
Slezská univerzita v Opavě, Obchodně-podnikatelská fakulta v Karviné

Filip Staněk, Centrum výpočetní techniky, VŠB-Technická univerzita Ostrava

a) Současný stav řešeného problému

Na Fakultě elektrotechniky a informatiky je již po delší dobu cíleně rozšiřována výuka počítačových sítí. V bakalářském studiu garantovaném katedrou informatiky je vyučován předmět Počítačové sítě, kterého se každoročně účastní cca 250 studentů a v inženýrském studiu jsou nabízeny další dva volitelné specializované předměty Směřované a přepínané sítě a Technologie počítačových sítí s kapacitou přibližně 40 studentů ročně. Při FEI byla již v roce 1999 zřízena Regionální akademie neziskového vzdělávacího programu Cisco Networking Academy (CNAP), která v současné době vyučuje 4 kurzy základní úrovně Cisco Certified Network Associate (CCNA) a 4 kurzy pokročilé úrovně Cisco Certified Network Professional (CCNP). Kurzy CNAP studuje v tomto roce celkově asi 60 studentů. Dále jsme s podporou grantu FR Cesnetu č. 180/2006 (Grygárek, P.: Implementace kurzů bezpečnosti počítačových sítí na regionální akademii programu Cisco Networking Academy při VŠB-TU Ostrava) zahájili implementaci kurzů specializované na bezpečnost počítačových sítí a podali jsme přihlášku projektu Fondu rozvoje vysokých škol pro zajištění výuky kurzů CNAP orientovaných na bezdrátové sítě.

V souvislosti s neustále rostoucími počty studentů ve standardních předmětech i kurzech CNAP, omezenou kapacitou laboratoře a také zařazením předmětů i do distanční formy studia jsme se z důvodu zajištění dostatečného přístupu studentů k síťovým prvkům pro praktickou výuku v minulém akademickém roce rozhodli pro postupné vybudování virtuální laboratoře počítačových sítí. Základní koncepce virtuální laboratoře počítačových sítí je vidět z obrázku 1. Jedná se o vzdálené zpřístupnění ovládacích sériových portů (konzolí) síťových prvků, jejichž prostřednictvím lze chování jednotlivých prvků konfigurovat. Vzdálený přístup oprávněných uživatelů řeší speciální software na serveru vybaveném multiportovou sériovou kartou, který k jednotlivým síťovým prvkům přepojuje síťová spojení od vzdáleně pracujících uživatelů. Síťový prvek může být libovolné zařízení ovladatelné přes sériový asynchronní port, v naší instalaci jsou využívány síťové prvky Cisco. Aby bylo možné přístup k prvkům koordinovat, byla realizována webová aplikace pro rezervaci přístupu na síťové prvky v předem rezervovaných časových oknech. Oprávněné osoby jsou schopny formou tzv. nástěnky zveřejnit, která úloha bude k dispozici k řešení ve kterém časovém okně. Momentálně také pracujeme na rozšíření, kdy student bude moci sám zvolit libovolnou úlohu nebo dokonce navolit svou vlastní topologii v pro sebe rezervovaném časovém okně, pokud pro ni budou právě k dispozici potřebné síťové prvky (v jednom časovém okně může běžet i více úloh paralelně, pokud je síťových prvků dostatek). V době, na kterou si uživatel přístup zarezervoval, může k síťovým prvkům vzdáleně přistupovat pomocí speciálního appletu, který emuluje přímé připojení ke konzoli síťového prvku pomocí terminálu. Uživatelé pak pro vzdálenou práci postačí pouze standardní WWW prohlížeč s podporou Java appletů.

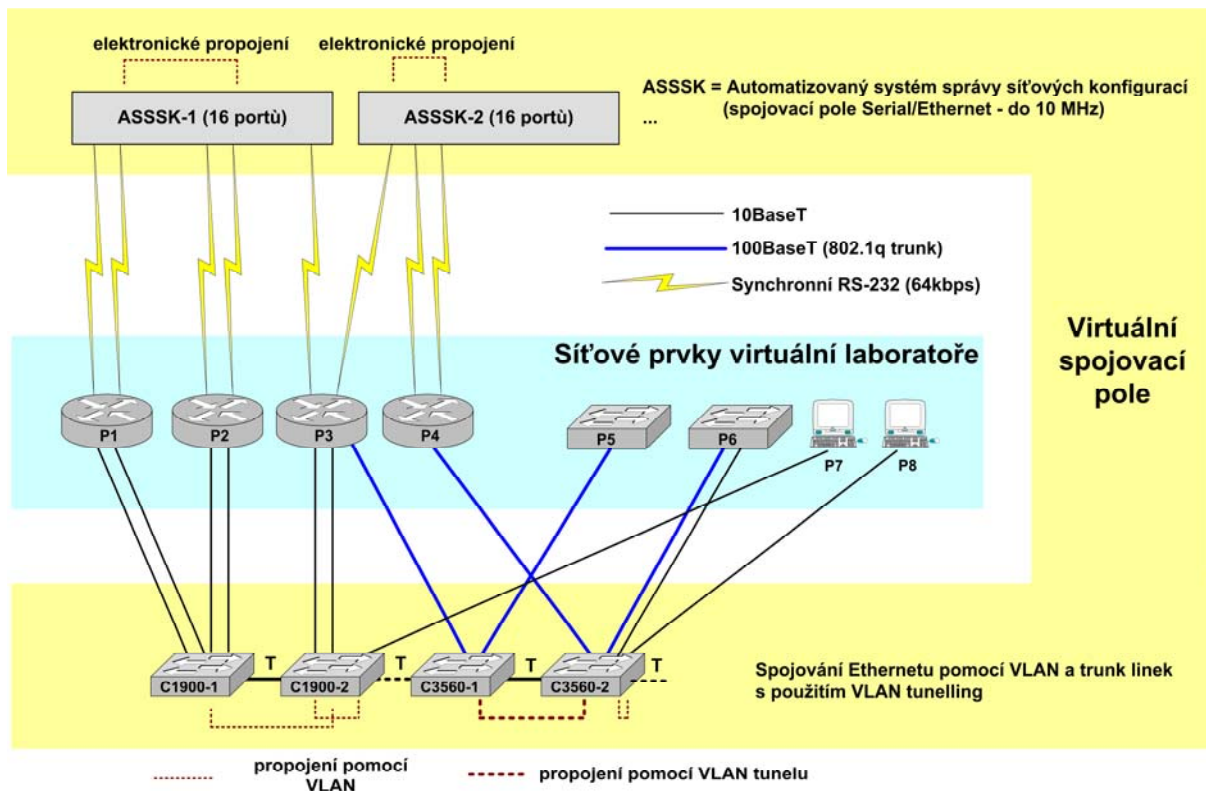


Obr.1 – Základní koncepce virtuální laboratoře počítačových sítí

Jednotlivé úlohy nabízené ke vzdálenému řešení studentům mohou vyžadovat různá propojení síťových prvků (topologie). Proto jsme zkonstruovali ovladatelné elektronické spojovací pole, do kterého jsou svedeny porty všech síťových prvků a které na základě konfiguračního souboru přiloženému ke každé úloze před zpřístupněním úlohy uživatelům automaticky sepne požadované dvojice portů, čímž sestaví požadovanou topologii. Původně jsme implementovali vlastní hardwarové řešení (Automatizovaný systém správy síťových konfigurací - ASSSK, obr. 2), umožňující spojovat jen sériové porty a porty 10BaseT. Později jsme však koncepci zobecnili a vzniklo Virtuální spojovací pole (obr 3), které může s použitím různorodých spojovacích prvků (včetně standardních přepínačů s podporou VLAN) spojovat i porty 100/1000BaseT včetně trunk portů a to při zachování jednotnosti ovládání celého virtuálního spojovacího pole jako celku.

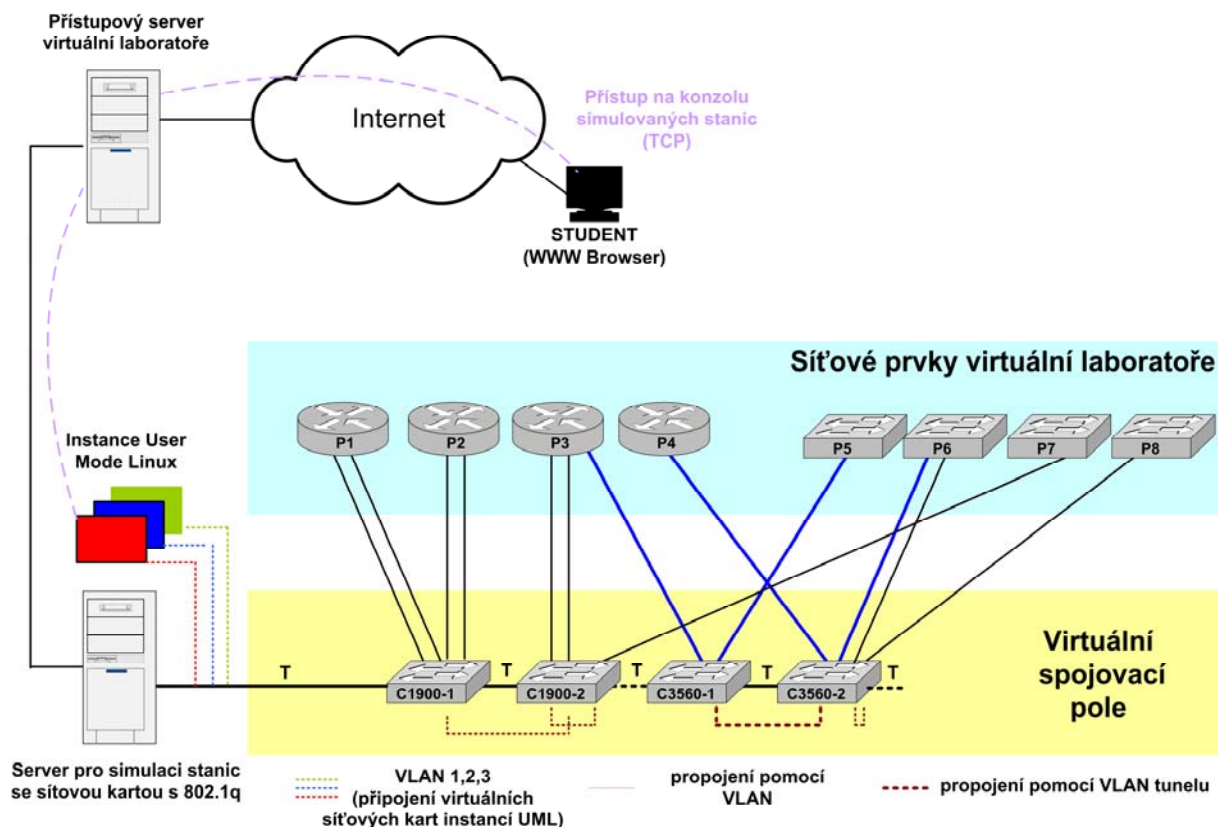


Obr. 2 – Základní deska vlastní konstrukce Automatizovaného systému správy síťových konfigurací



Obr. 3 Virtuální spojovací pole

Dále momentálně dokončujeme řešení, které nám umožní finančně i prostorově efektivním způsobem simulovat koncové stanice, jejichž absence ve virtuální laboratoři se při testovacím provozu zatím citelně projevovала. K tomu účelu bude vyhrazeno jedno PC s instalací User-Mode Linux, který umožní provozovat více nezávislých instancí virtuálních strojů s OS Linux. Virtuální síťové karty jednotlivých instancí User-Mode Linux budou přes VLAN prostřednictvím karty s podporou 802.1q svedeny do virtuálního spojovacího pole, kterým budou moci být připojeny k Ethernet rozhraní libovolného síťového prvku požadované topologie (obr.4). Spojení z appletu vzdáleného uživatele přemostňuje k příslušné instanci User-Mode Linux přístupový server virtuální laboratoře.



Obr. 4 - Virtuální spojovací pole se serverem simulujícím koncové stanice

Do praktického provozu jsme systém nasadili od letního semestru 2005/2006, nejprve na pevné topologii (obr. 5). Před uvedením do ostrého provozu jsme výrazně posílili bezpečnost implementace celého systému, který je v současné době umístěn v DMZ školy a přístupný z volného Internetu.



Obr. 5 – konfigurace virtuální laboratoře pro testovací provoz

Systém virtuální laboratoře nyní využívá asi 15 studentů kombinovaného studia předmětu Směrované a přepínané sítě, ve kterém studenti během semestru postupně řeší 3 praktické úlohy a případovou studii. Volitelné úlohy jsou nabízeny dále pro samostatné procvičování praktických dovedností pro studenty všech kurzů naší regionální Cisco akademie (cca 60 studentů základní úrovně CCNA i pokročilé úrovně CCNP) a studentům denního studia předmětu Směrované a přepínané sítě (cca 30 studentů). V příštím semestru využije systém

ještě cca 35 studentů předmětu Technologie počítačových sítí. Systém je dostupný zájemcům na <http://virtlab.cs.vsb.cz>.

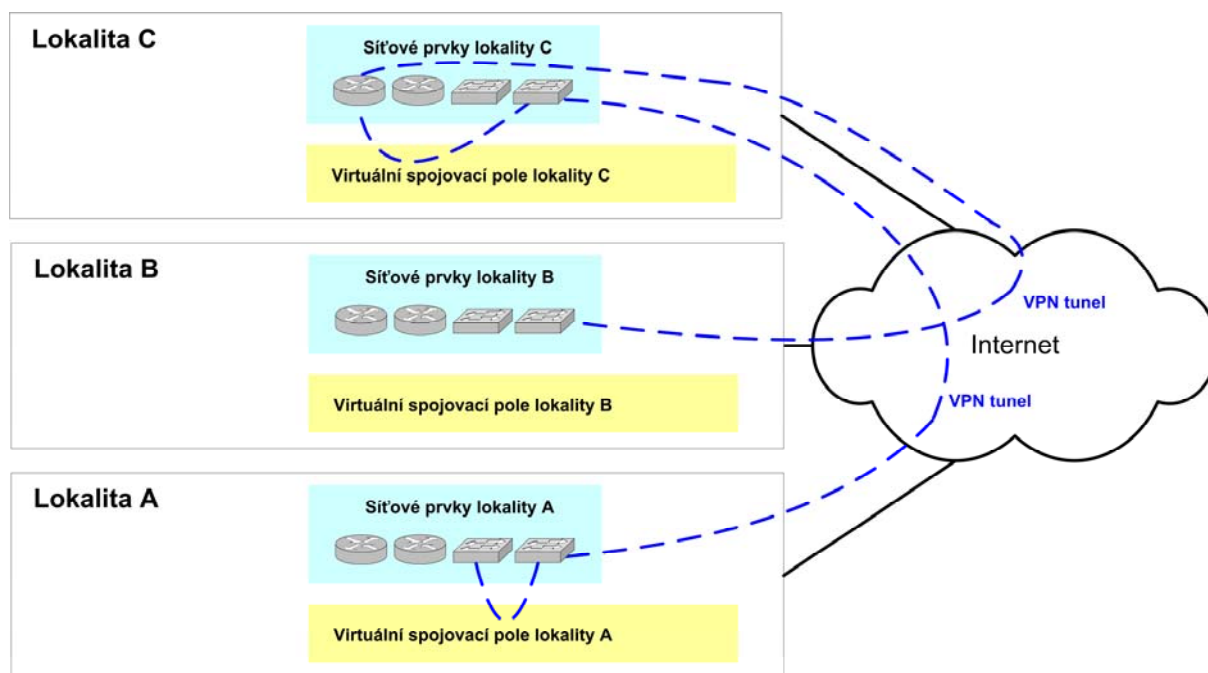
V současné době do ostrého provozu začleňujeme virtuální spojovacího pole. Pro zvýšení výukového efektu zejména pro studenty kombinované formy studia jsme do systému implementovali možnost řízení práce tutorem, který může kdykoli převzít řídicí konzolu kteréhokoli zařízení právě řešené úlohy. Akce prováděné tutorem se podle volby tutora mohou nebo nemusí zobrazovat ve virtuálním terminálu studenta, což umožní tutorovi jak demonstraci správného postupu, tak zkoušení studentů z praktických dovedností diagnostiky sítí provedením studentovi neznámého zásahu na jeho zařízení.

WWW stránky projektu virtuální laboratoře lze najít na <http://rcna.vsb.cz/virtlab>.

b) Cíle řešení

Původní představa implementace virtuální laboratoře byla taková, že v době bez výuky se bude zařízení umístěné v učebně - síťové laboratoři - připojovat k tamtéž umístěnému virtuálnímu spojovacímu poli a v době kontaktní výuky bude zařízení studentům k dispozici přímo. Prakticky se však brzy ukázalo, že toto je s ohledem na značné obsazení laboratoře organizačně velmi obtížné zajistit. Proto jsme se rozhodli realizovat virtuální laboratoř jako samostatný síťový rozvaděč osazený starším zařízením získaným při modernizaci produkční sítě školy a z dalších zdrojů. Získaná zařízení již sice výkonově nevyhovují potřebám reálného provozu, avšak plně postačují pro většinu v současnosti nabízených výukových úloh. Zejména se osvědčily starší směrovače Cisco 2500, které při upgrade paměti a instalaci vhodné verze IOS dokáží pracovat i s velmi pokročilými technologiemi. Protože je však v některých případech do topologie potřebné zahrnout i moderní zařízení umístěné trvale v laboratoři počítačových sítí, činíme nyní kroky, který nám umožní s použitím virtuálních sítí a školní infrastruktury zařízení umístěná v laboratoři bez potřeby jeho fyzického přenosu snadno dočasně připojit do topologie ostatních prvků umístěných v rozvaděči vyhrazeném virtuální síťové laboratoři

Hlavním cílem řešení navrhovaného projektu je rozšířit možnosti současné implementace systému virtuální laboratoře tak, aby mohl být provozován současně na více pracovištích (na naší regionální akademii CNAP a na spolupracujících lokálních akademiích CNAP podléhající naší regionální akademii) s tím, že zařízení bude vzájemně sdíleno a bude možno realizovat dočasné virtuální topologie mezi lokalitami provozujícími virtuální laboratoř s použitím infrastruktury Cesnet 2 (obr. 6). Součástí realizace bude praktické odzkoušení v pilotním projektu ve spolupráci se Slezskou univerzitou v Opavě (SU). Realizací takovéto distribuované virtuální laboratoře počítačových sítí bude možné vytvářet i velmi rozsáhlé výukové topologie realisticky simulující prostředí skutečných WAN sítí.



Obr. 6 – Virtuální topologie realizované přes infrastrukturu Cesnet 2

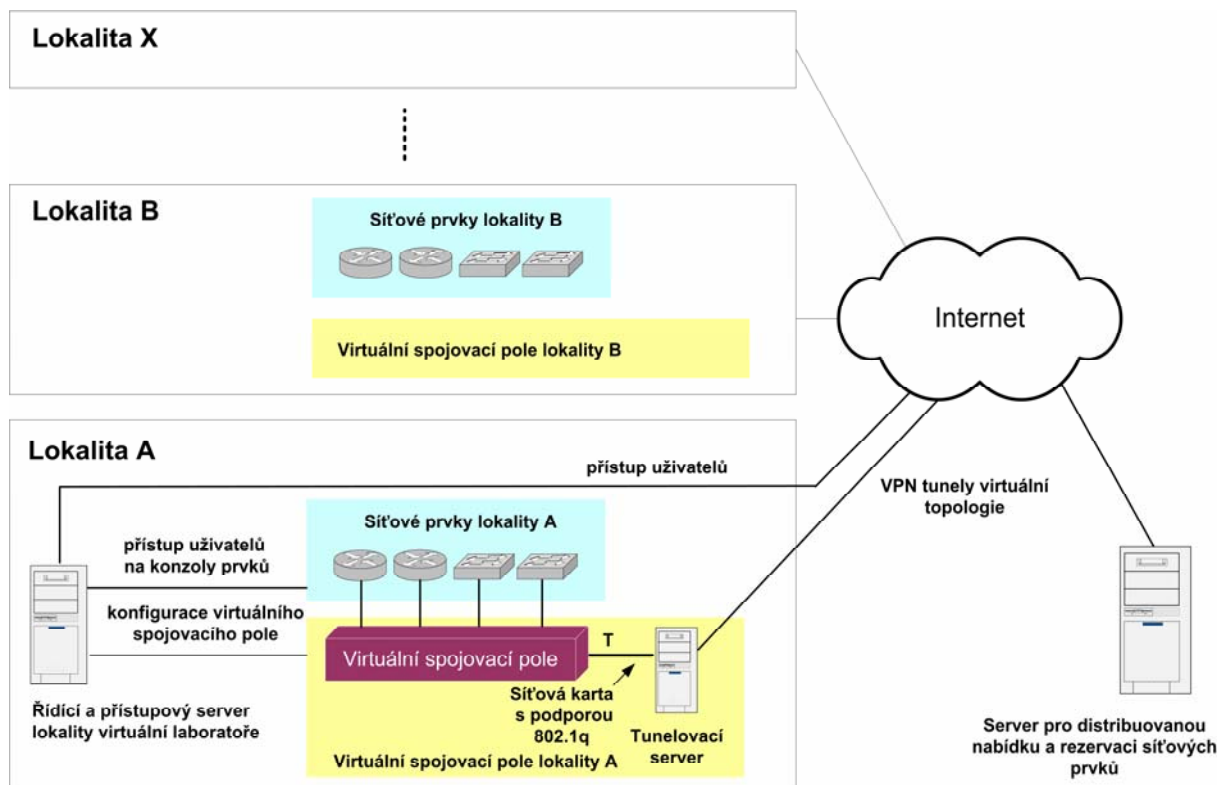
Primárním smyslem řešení však není pouze nabídnout možnosti realizace rozsáhlých konfigurací, ale hlavně efektivní sdílení nákladnějšího specializovaného vybavení mezi akademii CNAP. Naše regionální akademie nyní realizuje s podporou grantu sdružení Cesnet implementaci kurzů Fundamentals of Network Security. O kurzy bezpečnosti je v současné době značný zájem i mezi studenty jiných škol – námi podporovaných lokálních akademií CNAP, avšak pořizování vybavení na všechna tyto pracoviště není finančně efektivní. Proto plánuje VŠB-TU v rámci tohoto projektu pořídit zařízení pro výuku bezpečnostních technologií, které bude moci být formou distribuované virtuální laboratoře se spolupracujícími výukovými institucemi sdíleno. Také bychom chtěli pro virtuální laboratoř VŠB-TU dokoupit 4 přepínače Cisco Catalyst 2960 a jeden L3 přepínač Cisco Catalyst 3560, jelikož zde citelně chybí možnost realizace výukových konfigurací moderních přepínaných sítí včetně přepínání na 3. vrstvě (mnoho let staré přepínače C1900 jsou již s ohledem na absenci podpory řady dnes běžných vlastností nedostačující).

Pilotní projekt distribuovaného řešení plánujeme ve spolupráci se Slezskou univerzitou v Opavě, Obchodně-podnikatelskou fakultou v Karviné, jejíž pracovník je spoluřešitelem tohoto projektu. Mimo oblasti bezpečnosti sítí vidíme jako další vhodný cíl sdílení zařízení distribuovaného mezi spoluřešiteli tohoto projektu výuku technologií Voice over IP, jelikož obě pracoviště disponují softwarovou ústřednou Asterisk a směrovači vybavenými FXS porty pro připojení analogových telefonů, avšak pouze VŠB-TU vlastní moduly pro připojení do školní sítě ISDN a výukovou analogovou ústřednu připojitelnou do cvičné konfigurace prostřednictvím směrovače s FXO porty. Jelikož SU nemá k dispozici dostatek síťových prvků, které by mohly být do virtuální laboratoře nabízeny ke sdílení trvale, chceme z tohoto projektu pořídit i k tomuto účelu několik nových síťových prvků i pro karvinskou lokalitu.

c) Způsob řešení

Koncepce řešení a způsob technické realizace byly navrženy hlavním řešitelem projektu. Dílčí části jsou řešeny jednak formou diplomových prací a semestrálních projektů vedených hlavním řešitelem (Hrabálek, T.: Podpora vytváření virtuálních topologií ve virtuální laboratoři počítačových sítí s využitím technologie tunelování; Vavříček, J.: Rozvoj řídicího software virtuální laboratoře počítačových sítí; Miklošek, J.: Virtuální počítačová síť v Linuxu; Sedlář, P.: Rozšíření možností spojovacího pole pro automatizovanou tvorbu síťových topologií) a jednak samotnými řešiteli projektu. Hlavní řešitel rovněž koordinuje integraci dílčích výsledků do funkčního řešení. Ověření distribuovaného řešení v testovacím provozu bude provedeno za účasti obou spoluřešitelů projektu.

Distribuovaná virtuální laboratoř má za cíl umožnit nezávislý provoz instalací v jednotlivých lokalitách a současně zajistit možnost sdílení síťových prvků vytvořením virtuální topologie přes veřejný Internet. Proto momentálně pracujeme na rozšíření virtuálního spojovacího pole tak, aby bylo možné vést virtuální spoje (tunely) mezi několika fyzicky oddělenými virtuálními spojovacími poli. Bude implementována dynamická konfigurace tunelů, které zajistí přenos rámců 2. vrstvy OSI RM Internetem mezi jednotlivými geograficky oddělenými částmi virtuálního spojovacího pole - lokalitami virtuální laboratoře. Konce tunelu budou implementovány pomocí PC s OS Linux který bude připojen jednak k lokální části virtuálního spojovacího pole pomocí trunk linky a jednak pomocí dynamicky konfigurovaných tunelů ke vzdáleným částem virtuálního spojovacího pole v jiných lokalitách. Mezi virtuálními rozhraními příslušných VLAN a rozhraními tunelů přenášejících provoz VLAN ke vzdálené části virtuálního spojovacího pole bude konfigurováno přemostění na druhé vrstvě OSI RM (obr. 7).



Obr. 7 – Základní filosofie implementace distribuované virtuální laboratoře

Z důvodu zachování funkčnosti lokálních instalací i při výpadku konektivity do Internetu nebo rozpadu řízení distribuovaného systému sdílení zařízení předpokládáme, že každá lokalita bude provozovat svůj nezávislý systém pro nabízení úloh a rezervaci časových oken pro jejich řešení. Každá lokalita však bude schopna podle svého rozhodnutí v určitých časových oknech dát k dispozici některé síťové prvky pro zájemce o realizaci virtuální topologie z distribuovaných síťových prvků. Při realizaci rozsáhlejších virtuálních topologií přes Internet tak bude možné kombinovat tyto topologie ze všech prvků, které v daném časovém okně budou k dispozici ve kterékoli lokalitě účastníci se sdílení prvků. Metoda explicitního nabízení zařízení pro sdílení je výhodná mj. proto, že vždy budou upřednostňovány zájmy lokálních uživatelů a nebude se stávat, že by prvky lokality nasdíleli uživatelé ostatních lokalit a na uživatele lokality samotné, nabízející své zařízení ke sdílení, by se již její vlastní síťové prvky nedostaly.

d) Prezentace výsledků

Informace o výsledcích řešení bude uvedena na WWW stránkách regionální akademie CNAP při VŠB-TU, lokální akademie při SU i na hlavních WWW stránkách programu CNAP pro ČR. Vždy bude uvedeno, že výsledků bylo dosaženo za přispění sdružení Cesnet.

e) Charakteristika řešitelského kolektivu, odborný životopis řešitele a spoluřešitelů

Hlavním řešitelem projektu je Ing. Petr Grygárek, Ph.D., odborný asistent na katedře informatiky od r. 1995. Garantuje předměty Počítačové sítě, Technologie počítačových sítí, Směřované a přepínané sítě. Přednášel předměty Paralelní a distribuované systémy a Distribuované objektové systémy, vedl cvičení předmětů Operační systémy, Strojově orientované jazyky a Programovací jazyk C. Vedl projekt vývoje výukového operačního systému TUOX založeného na filosofii OS Unix. Podílel se na přípravě praktické výuky předmětů z oblasti počítačového hardware. Je koordinátorem a lektorem programu Cisco Networking Academy na regionální akademii při VŠB-TU. Organizačně a odborně zajišťuje chod a rozvoj laboratorní počítačových sítí a vývoj virtuální laboratoře počítačových sítí. Je držitelem certifikátů Cisco Certified Network Professional (CCNP), Cisco Certified Network Associate (CCNA) a Cisco Certified Academic Instructor (CCAI).

Grant FRVŠ 757/2000 – Vondrák, I., Grygárek, P., Olivka, P.: Laboratoř praktické výuky počítačů a sítí – spoluřešitel.

Grant FRVŠ 538/2002 – Tichý, P., Grygárek, P. Přístrojové vybavení laboratoře pro praktickou výuku technických předmětů – spoluřešitel.

Grant FRVŠ 470/2002 – Grygárek, P., Olivka, P.: Rozšíření souboru laboratorních úloh technicky orientovaných předmětů – řešitel.

Grant CESNET 006/2002: Grygárek, P., Grygárek, J., Malík, J.: Rozšíření výukových možností regionální síťové akademie při VŠB TU Ostrava – řešitel.

Grant CESNET 053/2003: Grygárek, P., Grygárek, J., Malík, J.: Vybudování regionální síťové akademie úrovně CCNP programu Cisco Networking Academy Program na VŠB-TU Ostrava.

Grant FRVŠ 338/2004: Grygárek, P., Verich, J.: Integrace mobilních zařízení do univerzitní sítě a jejich využití ve výuce – řešitel

Vondrák, Szturc, Rapant, Ďuráková, Grygárek, Stoklasa: HP Technology for Teaching Grant Initiative – University Education Edition, 2004. (výsledkem

implementace mobilních technologií do vysokoškolské
výuky)

Grant FR CESNET 2005: Nevlud, P., Grygárek, P., Macura, L., Jahelka, M., Vozňák, M.,
Zdrálek, J.: Prostředí pro vývoj embedded systémů.

Grant FRVŠ 2678/2006: Grygárek, P.: Praktická výuka moderních technologií počítačových
sítí

Grant FR CESNET č. 180/2006: Grygárek, P., Staněk, F., Aprias, R., Nevlud, P., Grygárek,
J.: Implementace kurzů bezpečnosti počítačových sítí na regionální akademii programu Cisco
Networking Academy při VŠB-TU Ostrava

Prvním spoluřešitelem projektu zastřešujícím projekt ze strany plánované lokality na SU je
Ing. Lukáš Macura. Je správcem počítačové sítě OPFNET na Slezské univerzitě Opava –
Obchodně podnikatelské fakultě v Karviné a současně správcem tamního uzlu CESNETu. Je
instruktorem programu Cisco Networking Academy. Byl členem řešitelského týmu
CESNETu pro IP telefonii.

Druhým spoluřešitelem je Filip Staněk, zaměstnanec Centra výpočetní techniky při VŠB-TU
s orientací na operační systémy. Je lektorem CNAP a držitelem certifikátů CCNA a CCAI.

f) Navrhovaná doba trvání projektu (počet měsíců) - navrhovaná délka trvání

Jelikož do vývoje distribuované virtuální laboratoře jsou zapojeni také studenti formou
diplomových prací obhajovaných v červnu 2007 a s ohledem na to, že po jejich obhájení bude
třeba výsledky prací integrovat a získat alespoň základní zkušenosti s praktickým provozem,
navrhujeme dobu řešení projektu 18 měsíců.