Zkušenosti z nasazení virtuální laboratoře počítačových sítí a další směry jejího rozvoje

Petr Grygárek *
petr.grygarek@vsb.cz

Abstrakt: Příspěvek popisuje současný stav implementace virtuální laboratoře počítačových sítí na katedře informatiky FEI VŠB-TU určené pro vzdálené řešení praktických úloh z počítačových sítí, zkušenosti z testovacího provozu a další plány jejího vývoje a rozšiřování.

Klíčová slova: virtuální laboratoř, síťové prvky, výuka počítačových sítí

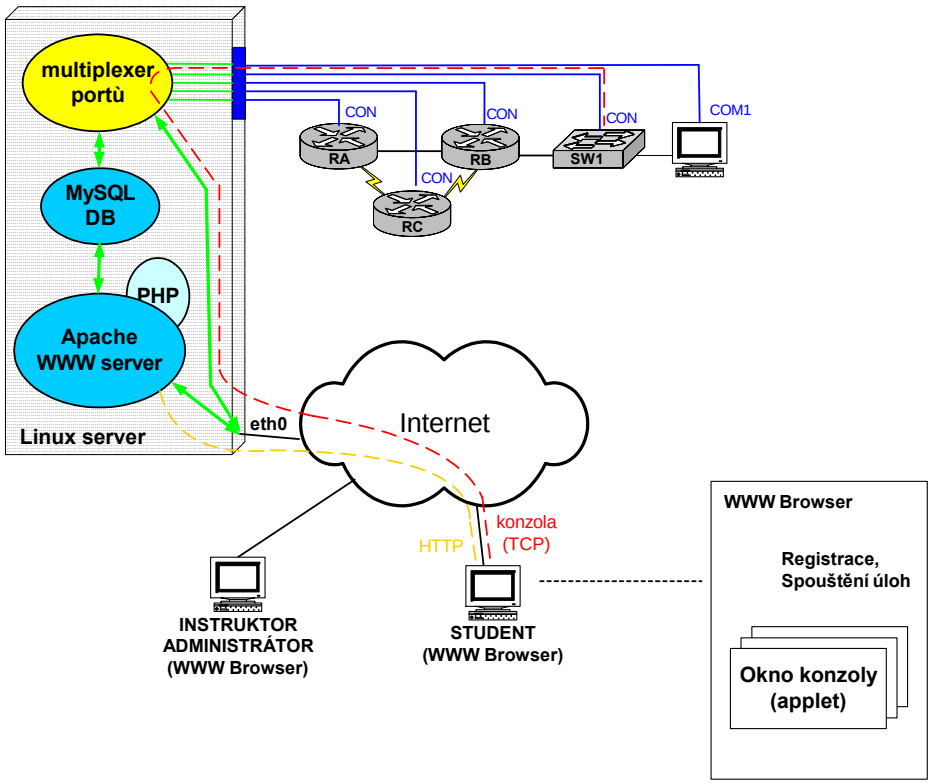
1 Úvod

V souvislosti s rostoucími počty studentů, omezenou kapacitou laboratoře a zejména zařazením nových předmětů i do kombinované formy studia jsme se v minulém akademickém roce rozhodli pro postupné vybudování virtuální laboratoře počítačových sítí. Nejprve byla stanovena základní koncepce a definována témata diplomových prací ([1],[2]), které by jednotlivé části prakticky implementovaly. O dílčích výsledcích již bylo referováno na několika konferencích [[4],[5]), včetně celkového popisu koncepce systému na konferenci TPEV 2005 [3]. Následující článek si klade za cíl popsat první praktické zkušenosti s nasazením systému virtuální laboratoře a nastínit další směry, kterými se bude její další vývoj ubírat.

2 Základní koncepce virtuální laboratoře

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. 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. Uživateli pak pro vzdálenou práci postačí pouze standardní WWW prohlížeč s podporou Java appletů.

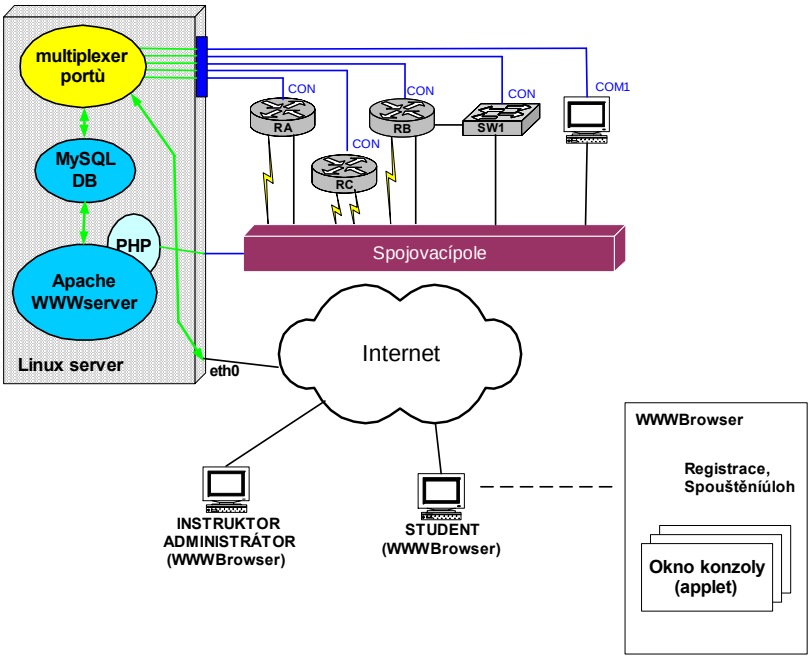
* Vysoká škola báňská – Technická univerzita Ostrava, Ústřední knihovna, 17. listopadu, 708 33 Ostrava-Poruba



Obrázek 1 – koncepce virtuální laboratoře počítačových sítí

Aby studenti měli vždy konkrétní zadání, které mají řešit, jsou v různých časových oknech, nabízeny různé úlohy. Úloha vždy obsahuje zadání ve formátu HTML (může zahrnovat i obrázky či jiné multimediální prvky), schema topologie síťových prvků a případně další návodné poznámky pro studenty, včetně správných řešení. Pokud topologie úlohy nevyžaduje všechny síťové prvky, které jsou ve virtuální laboratoři k dispozici, může být v tomtéž časovém okně dáno k dispozici paralelně i více úloh, jestliže se nepřekrývají v konkrétních síťových prvcích používaných jednotlivými úlohami. Popis úlohy lze do systému vložit buďto přes webové rozhraní, v praxi se však mnohem více osvědčila možnost importu popisu úlohy napsaného v jazyce XML, jelikož vytváření popisu úloh v tomto formátu dává další výborné možnosti návazného strojového zpracovávání, např. pro účely elektronické publikace či tisku.

Jednotlivé úlohy nabízené ke vzdálenému řešení studentům mohou vyžadovat různá propojení síťových prvků (topologie). Z počátku byla představa, že úlohy budou studentům nabízeny v blocích časových oken (např. dny) a mezi bloky budou topologie manuálně přepojovány. Z důvodu nepraktičnosti tohoto řešení jsme se však rozhodli zkonstruovat ovladatelné spojovací pole [2], do kterého budou 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 (obr. 2).



Obrázek 2 – architektura systému se začleněním spojovacího pole

3 Uvedení systému do provozu

Protože původní implementace měla charakter spíše ověřovacího prototypu, bylo třeba před praktickým nasazením systém důkladně odzkoušet a realizovat řadu drobných vylepšení. Ta sice nepřinášela významnější změny v architektuře, avšak výrazně vylepšila ergonomickou stránku používání systému. Jelikož byla postupně navrhována další a další užitečná rozšíření a systém se v hardwarové i softwarové části začal značně rozrůstat, bylo potřebné definovat a rozdělit další vývojové práce (témata návazných diplomových prací), ale také organizačně zajistit efektivní spolupráci zvětšujícího se vývojového týmu. Společná práce nad zdrojovými kódy systému je nyní koordinována systémem Subversion [10], pro výměnu obecnějších informací o systému včetně prezentace dílčích výsledků připravujeme nasazení systému Wiki [11]. Pro organizační zajištění ohlašování, evidence a sledování stavu řešení chyb postupně zjišťovaných během testovacího provozu jsme nasadili systém Bugzilla [9]. Ukazuje se, že při práci na projektu studenti získávají užitečné schopnosti týmové spolupráce včetně základních návyků při používání systémů pro koordinovaný vývoj. Do vývoje virtuální laboratoře jsou v současné době zapojeni zejména studenti řešící své diplomové práce, ale i jiní studenti zejména z kurzů naší síťové akademie, které projekt zaujal.

Do praktického provozu jsme systém nasadili od letního semestru 2005/2006, nejprve na pevné topologii. Systém virtuální laboratoře nyní využívá asi 20 studentů kombinovaného studia předmětu Směrované a přepínané sítě, ve kterém studenti během semestru postupně řeší 3 praktické úlohy a případovou studii [12]. Volitelné úlohy jsou nabízeny dále pro samostatné procvičování praktických dovedností pro studenty všech kurzů naší regionální Cisco akademie. V současné době intenzivně pracujeme na začlenění automatizovaného spojovacího pole, jehož koncepci jsme rozšířili (kap. 7) a momentálně jej před uvedením do ostrého provozu intenzivně testujeme.

3.1 Vylepšení zabezpečení systému

Jelikož systém virtuální síťové laboratoře má být dostupný nejen z univerzitního intranetu, ale z důvodu použití pro distanční vzdělávání také odkudkoli z Internetu, bylo nezbytné výrazně

vylepšit bezpečnost implementace prototypového řešení, aby celý systém mohl být umístěn do demilitarizované zóny školy a být trvale v provozu. Proto byla analyzována bezpečnostní rizika stávající implementace serveru zpřístupňujícího konzoly síťových prvků i samotné webové aplikace zajišťující uživatelské rozhraní virtuální laboratoře. Samotný přístup k WWW stránkám systému včetně autentizačního procesu již od začátku probíhal přes šifrovaný protokol HTTPS, ukázalo se však potřebné systém chránit i proti případným nekalým aktivitám korektně přihlášených uživatelů. To spočívalo zejména v odstranění známých bezpečnostních rizik spojených s implementací v jazyce PHP, zejména zamezením možnosti manipulace s hodnotami proměnných serverové aplikace předávaných z formulářů formou parametrů URL a zašifrování komunikace mezi emulátorem terminálu (appletem) a konzolami síťových prvků včetně úvodní autentizace. Důležitá a také pro ladění výhodná se ukázala i možnost protokolování akcí prováděných uživateli (přihlašování do systému, přístup na konzoly, příp. i zaznamenávání veškerých akcí prováděných na jednotlivých síťových prvcích).

3.2 Způsob realizace virtuální laboratoře

Původní představa implementace virtuální laboratoře byla taková, že v době bez výuky se bude zařízení umístěné v učebně - síťové laboratoři - připojovat k tamtéž umístěnému spojovacímu poli a v době kontaktní výuky bude zařízení studentům k dispozici přímo. Prakticky se však brzy ukázalo, že toto je 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 zařázení 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 pří upgrade paměti a instalaci vhodné verze OS 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 umístěné v laboratoři bez potřeby jeho fyzického přenosu snadno dočasně připojit do topologie ostatních prvků umístěných v rozvaděči vyhrazeném virtuální síťové laboratoři.

4 Praktické poznatky z provozu a nezbytné úpravy

Během testovacího provozu jsme narazili na některé skutečnosti a požadavky, které jsme se snažili s velkou prioritou vyřešit. Nečekaným problémem se např. ukázalo mazání konfigurací síťových prvků před zpřístupněním úlohy. Jelikož předchozí uživatel mohl zařízení nechat v jakémkoli stavu, ukázalo se velmi obtížné vyvinout univerzální sekvenci příkazů, která ze kteréhokoli stavu (režimu OS) provede výmaz konfigurace. Pro většinu verzí operačního systému Cisco IOS se toto podařilo, pro zajištění univerzality systémy a možnost práce s obecnými síťovými prvky však bude třeba vyvinout zpětnovazebný systém, který dovolí detekovat režim, ve kterém se zařízení právě nachází a zaslat do zařízení odpovídající mazací příkazovou sekvenci.

Podobně se při provozu zjistilo, že bude třeba výrazně rozšířit systém detekce a blokování vkládání zakázaných příkazů. Jedná se o různé formy zaheslování zařízení, které po uložení do paměti Flash zabrání korektnímu vymazání prvku před další úlohou, případně jakékoli práci se zařízením bez znalosti hesla vloženého předchozím uživatelem. Bohužel se postupně ukázalo, že se nejedná pouze o příkazy pro vkládání hesla, kdy jsme dovolili vložení pouze jednoho konkrétního dohodnutého hesla, ale např. o všemožné příkazy instruující zařízení

k ověřování hesel proti serverům typu RADIUS, TACACS apod. Navíc různá zařízení mají různé příkazové sekvence, které by měly být blokovány. Proto byl systém detekce zakázaných příkazů zobecněn, zakázané příkazy jsou nyní popsány regulárními výrazy a definovány u popisu každého síťového prvku zařazeného do virtuální laboratoře.

Další momentálně uskutečňovanou úpravou je možnost zachytávání obou směrů komunikace vzdáleného uživatele s konzolou síťového prvku do souboru na lokálním souborovém systému uživatele. Tímto způsobem si může uživatel např. snadno zaznamenat konfiguraci síťového prvku a později ji znovu vložit přenesením do virtuální konzoly (appletu) standardním mechanismem cut&paste. Díky zavedení této vcelku implementačně jednoduché možnosti bylo upuštěno od původně plánovaného ukládání konfigurací na serveru, což nejen zjednoduší serverovou část aplikace, ale umožní uživateli přímou další práci s konfigurací, např. tisk, okomentování nebo zaslání vyučujícímu řídícímu distanční výuku (tutorovi). Stejným způsobem může uživatel také zaznamenat do souboru výpisy stavu síťových prvků (směrovací tabulka, debug výpisy apod.), které často vyžadujeme jako doklad úspěšného vyřešení úloh, nebo které mohou sloužit pro analýzu problému při konzultaci postupu řešení s tutorem. Jelikož standardní applety přístup do lokálního souborového systému uživatele nedovolují, bylo použito podepsaného appletu s explicitní definicí přístupových práv.

S ohledem na možnost společného řešení úlohy skupinou studentů studentů se ukázala důležitá také implementace časovače, který automaticky odpojí studenta připojeného ke konzole síťového prvku po jisté době neaktivity (např. 10 min). To umožní ostatním členům řešitelské skupiny zařízení převzít v případech, kdy je některý z členů např. náhle odvolán a neprovede explicitní odhlášení od konzoly všech prvků, ke kterým byl předtím připojen.

Z hlediska praktické spravovatelnosti systému virtuální laboratoře se ukázalo potřebné kategorizovat uživatele, tj. přiřadit každému uživateli jméno skupiny, do které patří. To umožní do systému vkládat uživatele-studenty určitého předmětu vždy na dobu běhu tohoto předmětu a celou skupinu ze systému po skončení předmětu snadno odstranit. Jednotlivé skupiny mohou mít nastaveny různé týdenní kvóty na hodinové využití systému. U každého uživatele lze navíc individuálně definovat datum expirace účtu. Byly vytvořeny skripty pro přímý přenos studentů zapsaných na určitý předmět ve fakultním informačním systému KATIS. Z praktických důvodů jsme systém rozšířili tak, aby hesla uživatelů byla ověřována proti centrálně uloženým heslům na LDAP serveru, takže si uživatelé nemusejí pro virtuální laboratoř pamatovat speciální heslo a správci virtuální laboratoře odpadá práce s obvyklým obnovováním zapomenutých hesel. Pro usnadnění správy systému se ukázalo užitečné implementovat skupinu pomocných skriptů, umožňující například automatické vkládání úloh na nástěnku k rezervaci vždy v periodicky se opakujících časech nebo zjišťování aktuálně přihlášených uživatelů Kvůli zjednodušení řešení občasných incidentů a automatizovatelnosti vyhledávání významných událostí v chodu systému jsme také sjednotili formát log souborů generovaných jednotlivými částmi systému, takže v nich lze jednoduše vyhledávat na základě regulárních výrazů standardními prostředky pro zpracování textu v OS Unix.

5 Možnost řízení výuky tutorem

Pro zvýšení výukového efektu zejména pro studenty kombinované formy studia jsme se rozhodli do systému vnést podporu řízení práce tutorem. Implementace této podpory je v současné době před dokončením v rámci DP [7]. Uživatel s rolí tutora bude moci kdykoli převzít řídící konzolu kteréhokoli zařízení právě řešené úlohy. Akce prováděné tutorem se podle volby tutora budou nebo nebudou 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. Jako

zásadu jsme však stanovili, že studentovi musí být převzetí jeho konzoly instruktorem v každém případě indikováno, aby měl student (stejně tomu obvykle bývá v praxi) jistotu, že současně s ním nezasahuje do síťového prvku i jiná osoba.

6 Realizace uživatelských stanic pro ověřování síťových konfigurací

Významnou zkušeností, kterou jsme již v začátcích používání systému učinili bylo, že nebude dostačující do konfigurací úloh zahrnout pouze síťové prvky, ale i koncové uživatelské stanice. Nejvýrazněji se to projevilo hlavně u úloh zaměřených na přepínané sítě, kde je sledovatelnost funkce bez koncových stanic velmi omezená (simulace koncových stanic směrovači se ukázala pro studenty matoucí). Začleněním konfigurace koncových stanic do realizovaných síťových topologií navíc studenti procvičují často opomíjené činnosti na stanicích jako konfigurace výchozí brány, mohou stanice používat jako servery síťových služeb, proti nimž se ověřuje správná konfigurace bezpečnostních politik na směrovačích nebo například správná konfigurace serverů pro dynamické přidělování síťových adres. S ohledem na existující mechanismus zpřístupnění síťových prvků se jako nejvýhodnější ukázalo připojit koncové stanice sériovou linkou a provozovat na nich operační systém Linux, který se nám i při kontaktní výuce síťových technologií z důvodu transparentosti, spolehlivosti a rychlosti procedur konfigurace síťového připojení a služeb velmi osvědčuje. S použitím vhodného nastavení přístupových práv (sudo) zamezíme studentům v porušení operačního systému samotného, avšak dáme jim k dispozici veškeré administrátorské příkazy nutné pro konfiguraci a monitorování síťového připojení (ifconfig, arp, dhclient, route, netstat, ping, traceroute, tcpdump, telnet).

Problémem, který bylo při implementaci koncových stanic do virtuální laboratoře nutné vyřešit, byla volba hardwarové platformy. Není samozřejmě finančně ani prostorově efektivní stanice realizovat formou trvale běžících stolních PC standardní velikosti. První volbou, která byla zkoumána a je v současné době v omezené míře realizována, byl nákup procesorových desek pro vestavné systémy softwarově kompatibilních s PC (WRAP PC). Dále momentálně vyvíjíme alternativní řešení, kdy chceme pro simulaci nezávislých koncových stanic vyhradit jedno PC s instalací User-Mode Linux [8], který umožní provozovat více nezávislých instancí virtuálních strojů. Všechny instance budou přístupny pomocí služby Telnet (na různých portech) a budou prostřednictvím serveru virtuální laboratoře přesměrovány příslušné datové toky z emulátorů terminálů od vzdálených uživatelů. PC s User-Mode Linux bude dále vybaveno několika multiportovými Ethernet kartami (alternativně uvažujeme o použití USB hubu a několika USB Ethernet modulů), z nichž každá karta bude vyhrazena jedné instanci User-Mode Linux a před ostatními instancemi skryta. Jednotlivé síťové karty pak budou svedeny do spojovacího pole, kterým budou mocí být připojeny k Ethernet rozhraní libovolného síťového prvku podle topologie požadované aktuálně nabízenou úlohou. Celý systém je implementován jako část v současné době dokončované diplomové práce [6].

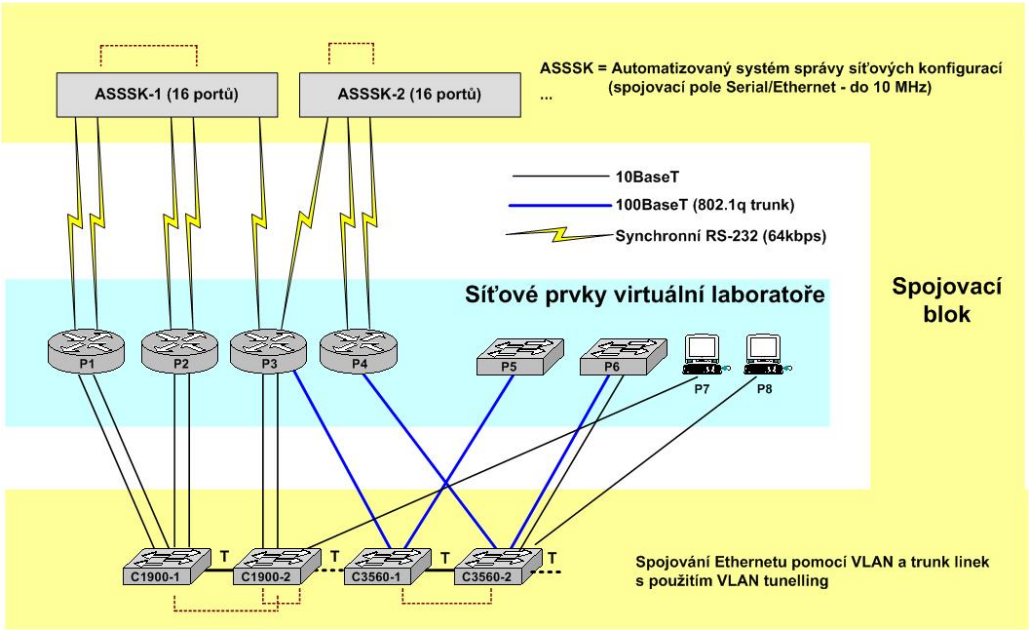
7 Zobecnění koncepce automatizovaného spojovacího pole

V předchozích fázích návrhu systému se počítalo s využitím speciálního konfigurovatelného spojovacího pole ASSSK ([2]) pro fyzické zapojení požadované topologie před zpřístupněním úlohy. Během používání systému se však ukázalo, že použití ASSSK pro spojování rozhraní Ethernet není efektivní – jednak proto, že moduly ASSSK je lepší využít na propojování sériových rozhraní, které nejsme schopni propojovat jiným standardním zařízením a jednak proto, že ASSSK dovoluje spojovat z důvodu frekvenčních omezení použitých součástek pouze Ethernet 10Mbps. Proto bylo rozhodnuto spojovat Ethernet porty laboratorních

síťových prvků s použitím standardního přepínače a vhodnou konfigurací virtuálních sítí (VLAN) tak, že dvojice portů síťových prvků, které mají být propojeny, budou zařazeny do společné VLAN. K tomuto účelu jsme byli schopni s výhodou použít starších přepínačů Cisco Catalyst 1900, které jsou momentálně vyřazovány ze síťové infrastruktury školy, avšak díky podpoře VLAN a dobré konfigurovatelnosti jsou pro náš účel zcela dostačující a to i přesto, že disponují pouze porty 10Mbps. Omezení rychlosti linek Ethernet na 10Mbps totiž ve většině výukových konfigurací není na závadu. Pro situace, kde je skutečně třeba spínat linky Ethernet 100Mbps nebo 1000Mbps, je možné pro spojování použít jiný přepínač, např. řady Cisco 2900 nebo i levnější model jiného výrobce.

Poněkud speciální situace nastává, když potřebujeme propojit dvojici portů síťových prvků v režimu trunk. Zde se ukázalo jediným řešením použití tzv. tunelování VLAN [13], kdy je možné vícenásobně označkovávat a v „metro VLAN“ přenášet rámce již jednou označkované podle standardu IEEE802.1q. K takovémuto způsobu propojování trunk portů však potřebujeme vyšší model přepínače, zatím se jako jediný s přístupnou cenou osvědčil L3 přepínač řady Cisco 3500.

Jelikož se spojování různých typů portů síťových prvků realizuje různými zařízeními, ukázalo se užitečné vytvořit virtuální spojovací pole, které bude složeno z různých reálných spojovacích prvků (obr. 3). Proto jsme opustili koncepci připojování konfiguračních souborů pro spojovací prvek přímo k definicím úloh a nahradili jej abstraktním popisem propojení na úrovni textového pojmenování dvojic rozhraní konkrétních síťových prvků, které mají být propojeny. Z tohoto popisu a z jednorázově vytvořeného konfiguračního souboru definujícího, který port kterého síťového prvku je (trvale) zapojen do kterého portu kterého spojovacího prvku virtuálního spojovacího pole, jsme schopni s použitím shell skriptu čistě na bázi manipulace s textem vygenerovat konfigurační soubory, pro jednotlivé spojovacích prvků virtuálního spojovacího pole. Skript pro generování konfigurací je navíc vytvořen modulárně, takže můžeme vcelku snadno použít i jiné typy spojovacích prvků, konfigurovatelné odlišným způsobem.



Obrázek 3 – architektura virtuálního spojovacího pole

Pro samotný ASSSK, určený v nové situaci pro propojování synchronních sériových portů, se chystáme zrealizovat následující rozšíření

- Možnost specifikace rozdílných taktovacích frekvencí pro jednotlivé spínané WAN linky, což umožní simulovat reálné WAN prostředí s linkami o velmi rozdílných přenosových rychlostech
- Implementace parametrizovatelné simulace střídavých výpadků a náběhů (flapping) WAN linky pro praktický nácvik postupů při diagnostice rozlehlých sítí
- Podpora pro spojování přes více ASSSK, propojených několika linkami. Nalezení optimálního počtu linek mezi jednotlivými ASSSK bude předmětem praktického odzkoušení a bude závislé na charakteru převládajících topologií potřebných pro realizované úlohy. Jelikož ASSSK disponuje 16 moduly a je tedy schopno spojit 8 WAN linek, předpokládáme s ohledem na plánovaný rozsah nabízených úloh, že potřeba propojování mezi více ASSSK bude spíše výjimečná pro obzvláště rozlehlé topologie

Pro uživatele dosti zásadní úpravou systému, na které v současné době pracujeme, je možnost specifikace libovolné požadované topologie propojení síťových prvků v době rezervace časového okna pro řešení úlohy. Student si v tomto případě nevybírá některou z předdefinovaných úloh, ale popíše požadovanou topologii stejným jazykem, jako to dělá tvůrce úloh při vytváření popisu úloh vkládaných do systému. Před zpřístupněním úlohy v rezervovaném časovém intervalu studentovi pak systém automaticky vygeneruje konfigurační soubory pro prvky virtuálního spojovacího pole a tyto soubory do spojovacích prvků zašle, čímž se studentem požadovaná topologie fyzicky propojí.

8 Další plány rozvoje systému

Jelikož se systém ukazuje jako životaschopný a užitečný jak pro distanční studium, tak pro samostatné procvičování studentů denního studia, navrhli jsme postupně další rozšíření systému, jejichž realizaci zabezpečíme nově vypsanou skupinou návazných diplomových prací. Nejdůležitější z plánovaných rozšíření dále popíšeme.

8.3 Režim vzdáleného zpřístupňování úloh

Nejzásadnějším poznatkem z organizace režimu virtuální laboratoře je časový harmonogram vzdáleného zpřístupňování úloh. Protože se ukázalo, že virtuální laboratoř je velmi výhodná pro studenty distanční (resp. kombinované) formy studia, kteří postrádají dostatečnou časovou dotaci pro kontaktní výuku v laboratoři nutnou pro mnohé praktičtěji zaměřené předměty, bylo zpřístupnění virtuální laboratoře těmto studentům stanoveno jako priorita. Na druhou stranu se však ukázalo, že je prakticky nemožné příliš omezit časový interval, kdy je určitá úloha nabízena k řešení (rezervaci časového okna pro řešení), jelikož časové možnosti studentů kombinovaného studia studujících při zaměstnání jsou velmi různorodé. Stávalo se tak, že jedna úloha musela být zpřístupněna např. po celé dva (lépe však tři) dny v týdnu, avšak jen velmi malé množství nabízených časových oken bylo studenty skutečně zarezervováno a využito k řešení úlohy. Studenti se zájmem o jinou úlohu však nevyužitá časová okna využít nemohli. V souvislosti s velkým množstvím předmětů, ve kterých je virtuální laboratoř využívána a tedy i množství úloh, které musí být postupně během semestru nabídnuty k řešení, se ukázalo umístění všech úloh do časového rozvrhu dosti problematické.

S ohledem na to, že máme k dispozici výše popsané virtuální spojovací pole pole pro automatizované zapojování topologií vyžadovaných jednotlivými úlohami, jsme se rozhodli změnit základní filosofii zpřístupňování úloh. Její implementace byla v současnosti zahájena formou diplomové práce. Princip změny spočívá v oddělení popisu úloh od identit konkrétních síťových prvků virtuální laboratoře. Úloha pouze popisuje požadavky na jednotlivé síťové prvky a jejich vzájemné propojení. Momentálně se pro popis požadavků jeví postačující počty síťových rozhraní jednotlivých typů každého síťového prvku, popis však chceme pojmout obecněji, aby bylo možné v budoucnu např. specifikovat verzi operačního systému síťového prvku, který může být pro skutečné řešení použit). Na „nástěnce“ pak nebudou v jednotlivých časových oknech nabízeny k řešení konkrétní úlohy, ale pouze samotná časová okna, jež mohou být použita k řešení libovolné úlohy. O tom, kterou úlohu bude student chtít v jemu rezervovaném časovém okně řešit, rozhodne student sám v okamžiku rezervace časového okna. Teprve při této rezervaci budou jednotlivým „logickým“ síťovým prvkům úlohy přiřazeny vyhovující fyzické síťové prvky virtuální laboratoře a přiřazení bude zaznamenáno, aby z něj a z popisu topologie úlohy mohla být před zpřístupněním úlohy automaticky vygenerována konfigurace pro virtuální spojovací pole. Jedno časové okno tak bude možné zarezervovat i nezávisle více studenty, pokud bude dostatek fyzických síťových prvků, na které se namapují logické prvky jednotlivých rezervovaných úloh. Může se tak stát, že uživateli v jistém časovém okně bude odepřena rezervace jisté úlohy, protože s ohledem na dřívější rezervace již v tomto časovém okně nejsou k dispozici pro úlohu potřebné síťové prvky, avšak alespoň úloha s menším počtem síťových prvků (nebo bez síťových se speciálními požadavky) bude moci být zarezervována. Zde je prostor pro mnohé optimalizace algoritmu mapování logických síťových prvků úloh na prvky fyzické a také pro další zobecňování virtuálního spojovacího pole, které zatím počítalo pouze s možností vzájemného propojování synchronních sériových rozhraní síťových prvků pouze v rámci jednotlivých ASSSK. To vnáší do mapovacího algoritmu dodatečné podmínky, o nichž teprve praktické používání ukáže, zda jsou pro reálný provoz příliš omezující či nikoli.

8.4 Další plánovaná vylepšení

Další úpravou, na které na základě zkušeností z provozu pracujeme, je možnost předkonfigurace síťových prvků před zpřístupněním úlohy. Studenti se tak budou moci koncentrovat na procvičovanou pokročilejší problematiku a nebudou muset ztrácet čas se základní konfigurací (IP adres, směrování atd.), čímž se výrazně zvýší efektivita využití virtuální laboratoře.

Ne příliš náročnou, avšak potřebnou se ukazuje implementace „chatovacího“ kanálu mezi studenty společně řešící úlohu. V prvotním návrhu bylo předpokládáno, že případný komunikační kanál mezi uživateli bude řešen standardními prostředky typu IRC/ICQ nebo Skype, to však vyžaduje další nepříjemnou organizační práci při ustavení takovéhoto systému (další nezávislé identifikátory uživatelů, zprovoznění serveru, instalace klientů uživateli apod.). Proto je plánováno, že do appletu zpřístupňujícího konzoly síťových prvků bude implementován komunikační kanál umožňující komunikovat právě jen se studenty řešícími danou úlohu a to jednak na základě identit, pod kterými jsou vedeni v systému virtuální laboratoře a jednak s možností komunikace s uživatelem, který právě konfiguruje určený síťový prvek, bez ohledu na jeho identitu. Užitečná bude i možnost zaslání oznámení všem uživatelům. Z důvodu využití systému i pro tutorem řízenou výuku (resp. přezkušování) musí být možné povolenou komunikaci také omezit, např. dovolit komunikaci pouze s tutorem, avšak nikoli mezi studenty vzájemně.

Mezi vylepšení naplánovaná na nejbližší dobu patří také celkové vyčištění systému s ohledem na nejnovější standardy W3C. Přestože se snažíme zajistit (zejména formou kaskádových stylů) dobrý vzhled aplikace ve všech WWW prohlížečích, narážíme často na problémy s kompatibilitou implementací JavaScriptu. Proto jsme se rozhodli orientovat na převládající prohlížeče Mozilla (aktuálně Firefox) a Interet Explorer, ve kterých je aplikace intenzivně testována a dále se důrazně držet standardů W3C s předpokladem, že použité prohlížeče budou standardy rovněž respektovat.

Z vylepšení orientovaných na hardware jmenujme alespoň plánovanou instalaci zásuvek napájení síťových prvků (230V) vypínatelných s použitím telnetového připojení z LAN. Fyzické vypnutí síťových prvků je užitečné pro některé speciální operace nad směrovači a přepínači Cisco, jako např. pro proceduru odstranění neznámého hesla, seznámení s ROM monitorem a podobně.

9 Plány pro budoucnost

V rámci dalšího vývoje systému jsme naplánovali implementaci spolupráce několika nezávislých instalací virtuální laboratoře. Implementace má za cíl umožnit nezávislý provoz jednotlivých instalací a současně zajistit možnost sdílení síťových prvků vytvořením virtuální topologie přes veřejný Internet. Proto momentálně pracujeme na rozšíření virtuálního spojovacího pole, aby bylo možné vést virtuální spoje mezi několika fyzicky oddělenými virtuálními spojovacími poli. Je uvažováno využití tunelování na 4. vrstvě s použitím systému OpenVPN, kdy dynamicky konfigurované tunely zajistí přenos rámců 2. vrstvy OSI RM Internetem mezi jednotlivými geograficky oddělenými částmi virtuálního spojovacího pole. Orientace na tunelování rámců 2. vrstvy je výhodná z důvodu nezávislosti na síťovém protokolu, takže budeme schopni v takovéto distribuované virtuální laboratoři simulovat nejen úlohy zaměřené na sítě s IP protokolem, ale i na přepínané sítě. 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 přemosťující provoz VLAN ke vzdálené části virtuálního spojovacího pole bude konfigurován klasický most (bridging) implementovaný přímo jádrem OS, pouze s vypnutou podporou protokolu Spanning Tree.

Distribuované řešení bude vyžadovat nejen realizaci dynamického vytváření virtuální topologie s použitím tunelů přes Internet, ale také transparentní přístup uživatelů ke konzolám zařízení rozložených ve více lokalitách. Z analýzy současného řešení však vyplývá, že z pohledu přístupu na řídící konzoly je distribuce zařízení do více geograficky oddělených lokalit do systému relativně snadno doplnitelná.

Z důvodu zachování funkčnosti lokálních instalací i při výpadku konektivity do Internetu nebo rozpadu řízení distribuovaného systému řízení 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 distribuované topologie. 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 účastnící se sdílení zdrojů. Metoda explicitního nabízení zařízení pro sdílení je výhodná mj. proto, že vždy budou upřednostňovány zájmy lokálních uživatelů a nebude se

stávat, že by zařízení lokality nasdíleli uživatelé ostatních lokalit a na uživatele lokality samotné, nabízející své zařízení ke sdílení, by se již síťové prvky nedostaly.

Distribuované řešení se pro praktické použití jeví velice výhodné, jelikož by umožnilo efektivní sdílení zdrojů výukových institucí a realizaci jinak nedosažitelných simulací i velmi rozsáhlých rozlehlých sítí. S ohledem na naši účast v programu Cisco Networking Academy předpokládáme, že bude možné vybudovat společnou virtuální laboratoř s jinými institucemi začleněnými do tohoto programu, které již o tuto možnost projevily velký zájem. Velký zájem o tuto aktivitu projevilo i vedení programu CNAP pro Českou republiku.

10 Závěr

V článku jsme popsali současný stav a představili mnohá rozšíření stávající implementace virtuální síťové laboratoře počítačových sítí, která je provozována na katedře informatiky FEI VŠB-TU Ostrava a realizována ve spolupráci s regionální síťovou akademií Cisco Networking Academy Program. Na trvale běžící server virtuální laboratoře se lze připojit na adrese http://virtlab.cs.vsb.cz.

Seznam odborné literatury:

1. NĚMEC, Pavel. Virtuální síťová laboratoř. Diplomová práce, FEI VŠB-TU Ostrava, květen 2005.
2. SEIDL, David. Automatizovaný systém pro správu síťových konfigurací. Diplomová práce, FMMI VŠB-TU Ostrava, květen 2005.
3. GRYGÁREK, Petr, SEIDL, David, NĚMEC, Pavel. Zpřístupnění prvků laboratoře počítačových sítí pro praktickou výuku prostřednictvím Internetu, Sborník konference Technologie pro e-vzdělávání, ČVUT Praha 2005
4. GRYGÁREK, Petr, SEIDL, David. Systém pro automatizovanou správu síťových topologií , Seminář Opensource řešení v sítích 3, SLU Karviná, 2005, http://uit.opf.slu.cz/docs/events/ors3
5. GRYGÁREK, Petr, SEIDL, David., NĚMEC, Pavel. Virtuální síťová laboratoř pro CNAP, Výroční konference Cisco Networking Academy Program, Brno 2005
6. MIKLOŠEK, Jiří. Virtuální počítačová síť v Linuxu. Diplomová práce, FEI VŠB-TU Ostrava, k ohajobě v červnu 2006
7. KUBÍN, Roman. Zajištění bezpečnosti a implementace nových prvků řídícího systému virtuální laboratoře, Diplomová práce, FEI VŠB-TU Ostrava, k ohajobě v červnu 2006
8. The User-mode Linux Kernel Home Page. http://user-mode-linux.sourceforge.net.
9. http://www.bugzilla.org/
10. http://subversion.tigris.org/
11. http://wiki.org
12. http://www.cs.vsb.cz/grygarek/SPS
13. http://www.cisco.com/en/US/products/hw/switches/ps646/products_configuration_guide_chapter09186a00801cdf50.html