UNIVERZITA PARDUBICE
Fakulta elektrotechniky a informatiky

Systémová správa počítačové laboratoře

Roman Diviš

Bakalářská práce
2011

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: **2010/2011**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Roman DIVIŠ**
Osobní číslo:	**I08031**
Studijní program:	**B2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Systémová správa počítačové laboratoře**
Zadávající katedra:	**Katedra informačních technologií**

Zásady pro vypracování:

V práci bude popsán systém správy počítačové laboratoře, který bude obsahovat jako přílohu dokumentaci síťových laboratoří na FEI (NET 101 a NET 102). Součástí práce bude popis, použití a aplikace simulátoru GNS, vztaženého na zařízení instalované v síťových laboratořích FEI. Popis a příklady použití měřících přístrojů, které jsou součástí vybavení síťových laboratořích FEI.

Rozsah grafických prací:

Rozsah pracovní zprávy:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

***Teare D., Návrh a realizace Cisco sítí, Computerpress 2003**
***GNS3 [online]. 2010 [cit. 2010-11-05]. Documentation GNS3 . Dostupné z WWW: http://www.gns3.net/**
***Lammle T., CCNA, Computerpress 2010**

Vedoucí bakalářské práce: **Ing. Soňa Neradová**
Katedra softwarových technologií

Datum zadání bakalářské práce: **17. prosince 2010**

Termín odevzdání bakalářské práce: **13. května 2011**

Univerzita Pardubice Česká republika

L.S.

prof. Ing. Simeon Karamazov, Dr.
děkan

Ing. Lukáš Čegan, Ph.D.
vedoucí katedry

V Pardubicích dne 31. března 2011

Prohlášení autora

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 4. 5. 2011 Roman Diviš

Poděkování

Rád bych touto formou poděkoval vedoucí mé bakalářské práce paní Ing. Soně Neradové za odborné vedení a cenné rady, které mi poskytla v průběhu práce.

Anotace

Tato práce se zabývá popisem a způsobem správy síťové laboratoře. A jejich rozšířením o Eagle server z kurzů CCNA. Dále popisuje použití síťových měřících přístrojů a programu GNS, který slouží jako simulátor počítačové sítě.

Klíčová slova

síťová laboratoř, GNS

Title

System managament of the computer laboratory

Annotation

This work is dedicated to description and method of system management of the network laboratory. And their extension with Eagle server from CCNA courses. Then it describes usage of network measuring devices and GNS program, which serves as a simulator of computer network.

Keywords

network laboratory, GNS

Obsah

Seznam zkratek

AP	Access Point
ARP	Address Resolution Protocol
CCNA	Cisco Certified Network Associate
CCNP	Cisco Certified Network Professional
CDP	Cisco Discovery Protocol
DCE	Data Communications Equipment
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DTE	Data Terminal Equipment
EDP	Extreme Discover Protocol
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
IDS	Intrusion Detection System
IOS	Internetwork Operating System
ISP	Internet Service provider
ISR	Integrated Services Router
LLDP	Link Layer Discovery Protocol
OS	Operační systém
OSPF	Open Shortest Path First
PoE	Power over Ethernet
SMTP	Simple Mail Transport Protocol
SSH	Secure Shell
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol

Seznam obrázků

Seznam tabulek

1 Úvod

Fakulta elektrotechniky a informatiky pro potřeby výuky předmětu Počítačové sítě doposud měla k dispozici jednu síťovou laboratoř v budově FES v kampusu univerzity. Vzhledem k rozšiřování výuky počítačových sítí a v souvislosti s rekonstrukcí budovy na legiích, bylo vybudováno několik počítačových, elektrotechnických učeben a také dvě síťové laboratoře. Laboratoře disponují vybavením pro výuku předmětů počítačové sítě I.-IV., kurzů Cisco CCNA a CCNA Security.

V práci je popsán aktuální stav síťových laboratoří a jejich vybavení. Dále se práce zabývá možností rozšíření laboratoří o Eagle server, který slouží k výuce Cisco kurzů. V práci je navržena a realizována možnost, jak implementovat Eagle server pomocí virtualizace do laboratoří.

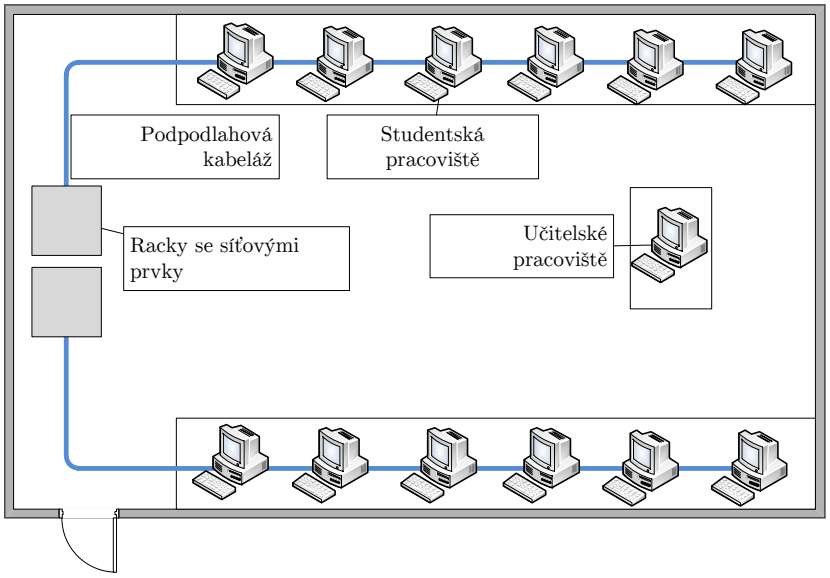
V poslední části se práce zabývá možnostmi simulačního nástroje GNS a problematikou jeho případného použití v laboratořích.

2 Síťové laboratoře

2.1 Požadavky

Síťová zařízení jsou určena k montáži do racku, vzhledem k počtu zařízení jsou potřeba dva racky do každé učebny. V NET101 by současný počet zařízení bylo možné umístit do jediného racku, ale uspořádání učeben a umístění zařízení téměř k zemi by velmi stížilo manipulaci s nimi.

V síťových laboratořích je potřeba kromě pracovního prostoru s počítačem pro studenty mít možnost vytvářet různé síťové topologie pomocí síťových zařízení. Je tedy nutné zajistit možnost propojení zařízení mezi sebou a připojení jejich konzolových portů, které slouží k jejich nastavení, k jednotlivým počítačům. Tahání dlouhých kabelů skrze učebnu by bylo velmi nebezpečné a neefektivní, proto každé pracoviště musí disponovat zásuvkami, které jsou zapojeny do centrálních racků se zařízeními. Patch panely v racku jsou vždy připojeny k jedné řadě pracovišť v učebně. Konzolové porty, které jsou umístěny na některých zařízeních v zadní části je vhodné vyvést na patch panel pro snadnou dostupnost.



Obrázek 1 – Koncept síťové laboratoře

Pro stavbu velmi komplexních topologií je výhodné mít možnost propojit obě laboratoře, racky v obou učebnách jsou propojeny několika linkami.

V operačním systému musí být studentům umožněno nastavovat síťové rozhraní, využívat ho, naslouchat na něm a v některých případech je potřeba i instalování nových programů. V systému musejí mít studenti administrátorská oprávnění.

2.2 Laboratoře

Síťové laboratoře jsou označeny NET101 a NET102 každá má rozlohu zhruba 50 m^2, jejich kapacita je 15 studentů a vyučující. V laboratořích jsou umístěny racky obsahující různé Cisco zařízení, které je možné mezi sebou propojovat. Studenti tak mohou vytvořit jednoduché i komplexní síťové topologie s využitím směrovačů a přepínačů propojených Ethernetem nebo sériovými linkami.

Vyučující má k dispozici vlastní pracoviště vybavené počítačem s připojeným dataprojektorem. V učebnách je také umístěna tabule pro psaní fixem.

2.3 Pracoviště

Na pracovní desce se nacházejí dvě zásuvky se síťovým napětím (pro připojení notebooku nebo Wi-Fi access pointu), dva konektory RJ-45 pro připojení do univerzitní sítě a čtyři konektory RJ-45 připojené do racku se zařízeními v učebně. Každé pracoviště je vybaveno počítačem, který má vyvedeny konektory síťové karty a sériového portu na pracovní desku. S pomocí krátkých přímých kabelů je možné propojit vyvedené konektory z počítače do libovolného místa. Podrobný nákres zapojení jednotlivých zásuvek viz příloha.

2.4 Počítač

Každé pracoviště je vybaveno počítačem Dell OptiPlex 360DT Standard disponující dual-bootem do Linuxu a Windows XP. V obou systémech je předinstalované základní softwarové vybavení pro běžnou kancelářskou práci a software využívaný pro výuku počítačových sítí. Pro potřeby síťových laboratoří jsou počítače vybaveny síťovou kartou a USB Wi-FI adaptérem.

2.4.1 Linux

Nainstalována je distribuce Ubuntu s grafickým prostředím Gnome. V systému je připraveno vše potřebné pro výuku počítačových sítí. Studenti se kromě výuky počítačových sítí seznámí s OS Linux a jeho základním použitím. K dispozici mají administrátorský účet *root* s heslem *rootroot*.
K dispozici je kromě standardního softwaru např.:

- minicom – komunikace přes sériovou linku;
- nmap – síťový skenovací a diagnostický nástroj.

2.4.2 Windows

K dispozici je i operační systém Windows XP s následujícím předinstalovaným softwarem:

- OpenOffice – kancelářský software;

- Acrobat Reader – prohlížeč PDF souborů;
- Wireshark – nástroj pro zachytávání a analýzu síťové komunikace;
- Putty – telnet, SSH klient;
- Cisco Packet Tracer – nástroj pro simulaci počítačových sítí;
- VirtualBox – virtualizační software;
- Cisco SDM – Cisco Security Device Manager.

Studenti mají k dispozici administrátorská oprávnění pro plný přístup.

Někteří studenti dávají přednost platformě Windows, také materiály a cvičení Cisco akademie jsou tvořeny pro OS Windows.

2.4.3 Obnova OS

Studenti mají na počítačích plná oprávnění a jelikož není využita virtualizace operačního systému může snadno dojít k jeho poškození. Pro tyto případy, ale také při potřebě aktualizovat obraz disku na všech počítačích, je k dispozici při bootování počítače volba *Obnova OS*. Volba obsahuje linuxové jádro s připraveným skriptem, který se pokusí ze serveru stáhnout obraz pevného disku a použít ho k aktualizaci počítače. Tento proces přepíše veškerá data na PC. Před použitím obnovy je nutné připojit počítač k Netlab serveru skrze zásuvku univerzitní sítě. Pro provedení obnovy je potřeba znát heslo, které je k dispozici u správce laboratoře. Celý proces obnovy trvá dle vytížení disku serveru a sítě okolo 20 minut.

Pokud by skript selhal je možné obnovit obraz ručně pomocí libovolné linuxové distribuce použitím příkazů:

```
$sudo su
$apt-get install nfs-common
$mkdir /tmp/a
$mount -t nfs 192.168.1.1:/mnt/sdilena /tmp/a
$dd if=/tmp/a/obrazdisku of=/dev/sda
```

Po obnově je nutné opravit hostname pod Linuxem (soubor /etc/hostname) i Windows, při prvním spuštění Windows je nutné počítat s delší dobou detekování *nového* hardwaru. Vhodné je také provést aktualizaci antivirového programu a operačního systému.

Výhodou tohoto postupu je jednoduchost, nevýhodou je, že se přenáší i clustery na disku, které nejsou využity. Tento problém by bylo možné odstranit použitím komprese obrazu před jeho přenosem.

2.5 Netlab server

V učebně NET101 se nachází linuxový server Dell PowerEdge R210, který slouží jako směrovač a firewall pro obě učebny. Veškeré linky v učebnách, které směřují do univerzitní sítě jsou připojeny skrze Netlab server.

Přehled poskytovaných služeb serverem:

- firewall – ochrana univerzitní sítě před pokusy v učebnách;
- DHCP – automatická konfigurace stanic v učebnách;
- NFS – vzdálené souborové úložiště.

Na serveru jsou zálohovány soubory IOS z jednotlivých Cisco zařízení. Pro přístup k zálohám je nutné použít SSH připojení na server, zálohy nejsou dostupné přes NFS.

2.6 Směrovače, přepínače

Cisco směrovače a přepínače jsou umístěny do dvou racků umístěných na kraji učebny, kde je zajištěn jednoduchý přístup a zároveň nepřekáží v místnosti. Do horní části racků jsou umístěny patch panely, které propojují zásuvky z jednotlivých pracovišť. Níže umístěné patch panely slouží k připojení konzolových portů jednotlivých zařízení, konzolové porty jsou nastálo připojeny jedním kabelem a minimalizuje se riziko poničení častou manipulací studenty. Konzolové porty jsou obvykle umístěny na zadní straně a přístup k těmto portům by bez vyvedení na patch panel mohl být problematický.

2.6.1 Vybavení NET-102

V laboratoři NET-102 se nachází následující zařízení:

- 15x směrovač Cisco ISR 2801 (IOS c2801-advipservicesk9-mz.124-24.T2.bin);
- 15x přepínač Cisco Catalyst 2960 (IOS c2960-lanbase-mz.122-35.SE5.bin).

Zařízení jsou seskupena do tzv. PODů, které tvoří tři směrovače a tři přepínače (tyto skupiny jsou používány v úlohách z kurzů CCNA I.–IV.).

2.6.2 Vybavení NET-101

Laboratoř NET-101 byla pojata jako laboratoř *pokročilých síťových technologií*. Nachází se v ní následující zařízení:

- 8x směrovač Cisco ISR 2811 (IOS c2800nm-adventerprisek9-mz.124-22.T.bin);
- 4x přepínač Cisco Catalyst 2960 (IOS c2960-lanbasek9-mz.122-53.SE1.bin);
- 4x přepínač Cisco Catalyst 3560 (IOS c3560-ipservices-mz.122-35.SE5).

Vybavení laboratoře je použitelné i pro pokročilé kurzy jako je CCNA Security. Zařízení jsou rozdělena rovnoměrně do obou racků.

2.6.3 Propojovací materiály

Pro vytvoření propojení mezi zařízeními jsou na boční straně racku v obou laboratořích zavěšeny volné kabely, které je možné použít pro propojování. K dispozici jsou následující typy kabelů:

- přímé ethernetové kabely, Cat 5e;
- kompletované V.35 sériové kabely DCE-DTE.

Pro případ vytváření rozsáhlých topologií jsou mezi laboratořemi protaženy 4 kabely.

2.7 Linksys WRT-54GL

Pro laborování Wi-Fi jsou k dispozici AP Linksys WRT-54GL. Jejich původní firmware byl nahrazen speciální Linuxovou distribucí OpenWRT, která je zaměřena na nasazení na směrovače a přístupové body. Její možnosti konfigurace jsou rozsáhlejší než původní firmware. Detailní informace o možnostech této distribuce je možné nalézt na [3].

Konfiguraci OpenWRT lze provádět přes webové rozhraní, telnet nebo SSH. Postup nahrání firmwaru do WRT-54GL a jeho obnova je popsána na wiki stránkách OpenWrt [4].

2.7.1 Obnova OpenWRT

Nahrání nového firmwaru je možné provést přes webové rozhraní, pokud dojde k problémům se zařízením může se stát, že webové rozhraní nebude přístupné.

Failsafe režim

První možností obnovy je spuštění OpenWRT v režimu failsafe, případě WRT-54GL se do failsafe režimu vstoupí následujícím postupem:

1. odpojíme AP od napájení;
2. připojíme port LAN1 k počítači;
3. na počítači nastavíme IP adresu 192.168.1.2, masku 255.255.255.0;
4. připojíme zařízení k napájení a vyčkáme na rozsvícení DMZ LED;
5. po rozsvícení DMZ LED několikrát stiskneme libovolné tlačítko na AP;
6. po uvedení zařízení do režimu failsafe by měla DMZ LED blikat rychlostí třikrát za sekundu;
7. připojíme se telnetem na AP na adrese 192.168.1.1.

Ve failsafe režimu jsou data dostupná v režimu pouze pro čtení, pro obnovení možnosti zápisu použijeme příkaz *mount_root*.

Pokud není známé heslo do AP je ho možné obnovit příkazem *passwd*, v případě zapomenutí IP adresy je k dispozici příkaz *uci get network.lan.ipaddr*.

Obnovení bootloaderem

Pokud nebylo možno opravit zařízení přes failsafe režimu zbývá možnost přehrání firmware na zařízení přes TFTP během jeho bootování. Ověřit dostupnost této možnosti je možné připojením k AP a spuštěním *ping* na adresu 192.168.1.1. Během bootování by mělo dojít k odpovědi, doba po kterou zařízení reaguje je velmi krátká, proto může být nutné postup opakovat vícekrát než dojde k navázání spojení.

Pokud byla deaktivována volba *boot_wait* na zařízení, nebude ho možné tímto způsobem obnovit!

Výpis příkazů pro nahrání firmwaru přes TFTP:

```
tftp 192.168.1.1
tftp>binary
tftp>rexmt 1
tftp>timeout 60
tftp>trace
tftp> put firmware.bin
```

Po přenosu dat dojde k aktualizaci flash paměti na zařízení k jeho restartu, během aktualizace musí zůstat připojeno k napájení a musíme vyčkat na jeho restart.

3 Možnosti rozšíření laboratoří

3.1 Eagle Server

Eagle server je předkonfigurovaná distribuce Linuxu distribuovaná firmou Cisco k výuce Networking Academy kurzů. Server je do sítě připojen přes dva směrovače pro „simulování internetu“. Všechna tato zařízení jsou předkonfigurována. Samotný server Eagle je založen na distribuci Linuxu Fedora Core 3 a obsahuje několik různých serverů:

- Instant Messaging (IRC);
- Wiki server (TWIKI);
- DNS server;
- E-mail;
- Web server;
- FTP, TFTP;
- SSH.

Ty poté slouží k experimentování a poznávání chování těchto služeb a protokolů jako v reálném internetu.

3.1.1 Servery

Web server

Webový server je dnes asi nejrozšířenější služba na internetu, na serveru je připravený web server, který poskytuje základní informace o Eagle serveru. Navíc je na serveru nainstalován wiki systém TWiki. Studenti mohou sledovat komunikaci HTTP protokolu a vyzkoušet si možnost sdílení poznámek pomocí TWiki.

FTP

Vedle protokolu HTTP sloužícího primárně k přenosu textu, je k dispozici FTP server, který slouží k přenosu souborů. Studenti jej mohou využívat ke stahování materiálů pro jednotlivé cvičení přímo ze serveru.

Mail

E-mailovou komunikaci dnes mnoho lidí využívá více než klasickou poštu. Na serveru si mohou studenti ozkoušet komunikaci přes e-mail mezi jednotlivými účty pomocí protokolů SMTP a IMAP. Odesílání pošty do internetu není možné.

IRC

IRC je komunikační protokol, který vzhledem ke své jednoduchosti byl populární již v dřívějších dobách. I dnes se můžeme setkat s velkými IRC sítěmi. Komunikace probíhá v kanálech, do kterých se jednotliví uživatelé připojují. Studenti mohou použít např. program GAIM pro připojení na IRC server.

SSH

SSH slouží obdobně jako protokol Telnet ke vzdálené administraci počítače či zařízení. Na rozdíl od Telnetu se jedná o bezpečnou šifrovanou komunikaci. Ve výchozím nastavení se mohou studenti na Eagle připojit pomocí SSH.

3.1.2 Provoz Eagle serveru

Eagle je možné spustit několika různými způsoby [7]:

- jako LiveCD, bez nutnosti instalace;
- nainstalovat systém na počítač;
- virtualizovat ho pomocí VMware nebo jiného nástroje.

Uživatelé

V Eagle serveru je vytvořeno několik různých uživatelů, které mají přístup k jednotlivým službám:

- instructor;
- cisco;
- ccna[1-22].

Všechny účty mají nastaveny výchozí heslo *cisco*. To platí i pro účet *root*. Pro běžný provoz je důležité zabezpečit účet správce, aby nedošlo k poškození serveru neoprávněným přístupem studenty.

3.1.3 Virtualize pomocí VirtualBoxu

Před vlastní instalací na server byl Eagle server otestován ve virtuálním prostředí VirtualBox na učitelském počítači. Vytvoření virtuálního stroje je pomocí grafického průvodce velmi jednoduché. Po spuštění serveru, bylo zjištěno několik omezení, které se týkají instalace na disk.

- Instalace vyžaduje disk s vytvořenými oddíly, ty je možné vytvořit z live spuštění Eaglu.
- Instalace na oddíl FAT nepodporuje bootování z disku, je nutné mít připojeno CD s Eaglem.

Proto bylo nutné spustit Eagle v live režimu a připravit diskové oddíly pro instalaci, poté byla provedena instalace na oddíl typu EXT. Použitím VirtualBoxu se projevila chyba v detekci grafického adaptéru a systém nebyl schopen spustit grafické prostředí. Tuto chybu je možné odstranit úpravou soubor /etc/X11/xorg.conf, v sekci *Videocard0* je nutné ponechat pouze volbu *Identifier* a volbu *Driver* nastavit na *vesa*. Poté je již systém schopen spustit grafické prostředí.

Při instalaci na oddíl EXT nedojde ke správnému zavedení skriptů pro aktivaci síťového adaptéru. Proto je nutné skript zkopírovat na správné místo. V konzoli spuštěného serveru to lze provést pomocí:

```
$su (zadání hesla: cisco)
$cd /etc/sysconfig
$cp networking/devices/ifcfg-eth0 network-scripts/
```

Po restartu je již server schopen správně pracovat.

3.1.4 Virtualizace na Netlab serveru

Pro trvalý provoz na Netlab serveru je potřeba vyhrazená síťová karta pro Eagle server. Dell PowerEdge R210 ve výchozí konfiguraci disponuje pouze dvěma síťovými adaptéry. Rozšíření je možné pomocí PCIe síťových karet, z kompatibilních modelů je to např.:

- Intel PRO/1000 PT Server Adapter,
- Broadcom NetXtreme II 5709 Dual Port Ethernet PCIe Card with TOE;

Adaptér Broadcom NetXtreme II disponuje dvěma gigabitovými porty, což může být výhodné pro další budoucí rozšíření serveru.

Virtualizační platforma

Eagle server je spuštěn jako virtuální stroj pomocí programu Xen. Xen je možné na server doinstalovat nebo aktualizovat server vhodnější Linuxovou distribucí, která již Xen obsahuje. Byla zvolena varianta využití distribuce CentOS 5.6, která je pro virtualizaci připravena. Vzhledem ke staršímu jádru Linuxu v Eagle serveru (2.6.12) je nutné využít úplnou hardwarovou virtualizaci (HVM). Pro použití paravirtualizace by bylo nutné aktualizovat jádro v Eagle serveru [5].

Příprava Xenu

Xen ve výchozí konfiguraci využívá pouze jedinou síťovou kartu, pro naše potřeby je nutné upravit síťové skripty [6]. Vytvořením nového skriptu /etc/xen/scripts/network-eagle s obsahem:

```
#!/bin/sh
dir=$(dirname "$0")
"$dir/network-bridge" "$@" vifnum=0
"$dir/network-bridge" "$@" vifnum=1
"$dir/network-bridge" "$@" vifnum=2
```

Provedeme automatické vytvoření tří síťových mostů napojených na fyzické ethernetové adaptéry. Skript musí být spustitelný (chmod +x network-eagle). Jeho použití je nutné nastavit v souboru /etc/xen/xend-config.sxp úpravou volby network-script na:

```
(network-script 'network-eagle')
```

Vytvoření virtuálního stroje

Eagle bude zaváděn z virtuálního disku, ten může být obrazem reálného disku v počítači nebo souboru. Vzhledem k nutnosti udržovat několik různých variant Eaglu je výhodnější využít ukládání do souboru, které je možné jednoduše klonovat a zálohovat. Soubor disku o velikosti 4 GB připravíme pomocí příkazu:

```
dd if=/dev/zero of=/home/eagle.img bs=1M count=4000
```

Pro vytvoření oddílů je potřeba připojit soubor přes loop zařízení:

```
losetup /dev/loop0 /home/eagle.img
```

Tímto způsobem je možné použít fdisk na vytvoření oddílů: fdisk /dev/loop0, postupným zadáváním kláves:

```
N [enter] P [enter] 1 [enter] 1 [enter] +3000M [enter]
N [enter] P [enter] 2 [enter] [enter]
T [enter] 2 [enter] 82 [enter]
A [enter] 1 [enter]
W [enter]
```

Dojde k vytvoření spustitelného Linuxového oddílu o velikosti 3 GB a SWAP oddílu o velikosti 1 GB. Poté je možné loop zařízení odpojit: losetup -d /dev/loop0.

Vlastní konfiguraci pro spuštění Eagle je vytvořena v souboru /etc/xen/eagle.cfg [9]:

```
import os, re
arch = os.uname()[4]

kernel = "/usr/lib/xen/boot/hvmloader"
builder = "hvm"

memory = 512
shadow_memory = 8
name = "eagle"
vif = [ "type=ioemu, bridge=xenbr2" ]
device_model = "/usr/lib/xen/bin/qemu-dm"
disk = [ "file:/home/eagle.img,ioemu:hda,w",
"file:/home/eagle-server-v2.0.iso,hdc:cdrom,r"]
boot = "dc"
sdl = 0
vnc = 1
vnclisten = "0.0.0.0"
vncconsole = 1
vncpasswd = "eaglepass"
stdvga = 0
serial = "pty"
usbdevice = "mouse"
acpi=1

on_poweroff = "destroy"
on_reboot = "restart"
on_crash = "restart"
```

Provoz

Poté je možné spustit server pomocí příkazu: xm create /etc/xen/eagle.cfg. Administraci je možné provádět připojením se přes VNC a zadáním hesla „eaglepass“. Po nainstalování Eagle serveru na disk je možné z konfiguračního souboru odebrat odkaz na CD-ROM. Po instalaci je nutné zkopírovat skript pro aktivaci síťového adaptéru, jak bylo popsáno v předchozí kapitole.

Pro jednodušší správu přes SSH byl vytvořen skript pro BASH, který umožňuje provádět jednoduchým způsobem potřebné základní úkony automaticky. Skript automaticky vytváří a spouští kopie serveru pro různé skupiny studentů. Kompletní výpis skriptu vizte příloha B. Ovládání skriptu je pomocí několika parametrů:

- eagle start SERVER – spustí virtuální stroj;
- eagle stop – zastaví virtuální stroj;
- eagle create SERVER – vytvoří kopii s označením SERVER;
- eagle remove SERVER – smaže kopii s označením SERVER;
- eagle list – vypíše dostupné kopie a stav aktuálního virtuálního stroje.

Skript je vhodné umístit do adresáře /bin a nastavit mu příznak spustitelnosti.

3.1.5 Použití Eaglu

Jednotlivé klienty je možné přímo připojit k Eagle serveru nebo před ním vybudovat topologii ze dvou směrovačů, tím je možné simulovat „reálné“ chování při internetové komunikaci. Studenti se mohou připojit na jednotlivé servery, vyzkoušet a prozkoumat jejich funkci. Na klientských PC je možné sledovat a analyzovat komunikaci jednotlivých protokolů pomocí programu WireShark. Podrobnější popis programu WireShark se nachází v kapitole 5.2.7.

3.2 Využití GNS

Simulační nástroj GNS může posloužit k demonstracím při přednáškách – živé ukázky probírané látky na připravených topologiích nebo pro rozšíření laborovaných topologií – připravení složité ISP části, která bude připojena do fyzické topologie.

Největším problémem s využitím GNS je nutnost vlastnit IOS soubory pro provoz jednotlivých zařízení, proto jeho přímé využití studenty během výuky není vhodné.

Podrobný popis nástroje GNS se nachází v kapitole 5.

4 Měřící přístroje

V laboratořích jsou dostupné profesionální měřící přístroje firmy Fluke Networks. Lze s nimi testovat kabeláž, vyhledávat vedení nebo provádět testování vyšších vrstev OSI modelu. Studenti je mohou využít během výuky při vytváření vlastní kabeláže pro otestování funkčnosti.

Kompletní manuály k měřícím přístrojům je možné získat na stránkách výrobce [1].

4.1 Praktické použití

4.1.1 Otestování funkčnosti kabeláže

Nejčastějším problémem, který je možné otestovat je správnost zapojení a funkčnost kabeláže. Tento test je možné provést s libovolným měřícím přístrojem. Kabel se připojí do přístroje z obou konců nebo je na druhé straně zakončen speciálním prvkem (dle druhu přístroje).

Tímto způsobem mohou studenti otestovat kabeláž vlastní výroby nebo stávající kabeláž v laboratořích a ověřit tak její funkčnost.

Obrázek 2 – Autotest kabelu s připojeným wiremap adaptérem

4.1.2 Vyhledávání kabeláže

Při řešení problémů s připojením k síti, kdy je nutné zkontrolovat zapojení kabelů, se často setkáváme s nedostatečně popsanou kabeláží nebo se svazky několika kabelů. Pokud ovšem potřebuje vyhledat pouze jeden konkrétní kabel, procházet kabeláž od jednoho konce k druhému může být velmi obtížné a v některých případech i nemožné. Pomocí měřících přístrojů je možné generovat digitální nebo analogový signál, který je možné vyhledávat pomocí sondy. Sonda je schopna detekovat signál v kabelu na vzdálenost asi deseti centimetrů, pokud se nachází mezi kabelem a sondou překážka (např. zeď) vzdálenost se zkracuje.

Studenti mohou v laboratořích zkusit vyhledat vedení mezi zásuvkou a rackem a následovně identifikovat konkrétní zásuvku.

Obrázek 3 – Vyhledávání kabelu s využitím CableIQ

4.2 CableIQ

Přístroj CableIQ slouží především k testování kabeláže, testuje podporované rychlosti, přeslechy, impedanční rozdíly, přerušené vedení a správné propojení jednotlivých vodičů. Také ho lze využít jako zdroj signálu pro sondu IntelliTone Probe. Přístroj podporuje ukládání výsledků a synchronizaci s PC. CableIQ je také možné použít pro testování reproduktorů a spojitosti vedení.

Obrázek 4 – Ovládací prvky CableIQ

4.2.1 Testování kabeláže

Autotest provede otestování kabeláže a zobrazí podporované rychlosti a normy Ethernetu, délku kabeláže a zapojení jednotlivých vodičů. Na rozdíl od jednoduchých měřících přístrojů jsou změřeny hodnoty přeslechu a impedance a je tak možné odhalit další problémy, kromě špatného zapojení vodičů nebo přerušeného vedení.

Otočný přepínač uvedeme do polohy *Autotest*, testovaný kabel zapojíme do přístroje a pokud je to možné tak jeho druhý konec zakončíme wiremap adaptérem. Stiskneme *TEST* a vyčkáme dokončení testování. Po skončení testování se zobrazí seznam podporovaných standardů a pomocí navigačních kláves a funkčních kláves je možné procházet výsledky.

4.2.2 Vyhledávání kabeláže

Vyhledávání kabeláže pomocí sondy IntelliTone Probe provedeme nastavením otočného přepínače do polohy *TONE* a připojením kabelu. Pomocí směrových kláves je možné zvolit digitální či analogový signál. Vlastní vyhledání je poté provedeno pomocí sondy.

4.2.3 Blikání portu na přepínači

Pokud nevíme ke kterému portu na přepínači je připojena zásuvka je možné využít funkce periodického blikání portu. Otočný přepínač uvedeme do polohy *DIAG* a pomocí směrových kláves vybereme funkci *Blink Port Light* a potvrdíme tlačítkem *Enter*. Připojením kabelu k měřícímu přístroji dojde k rozblikání LED signalizující aktivitu portu na přepínači. Frekvenci blikání je možno změnit tlačítkem *F2* a připojený kabel je možné sledovat sondou IntelliTone Probe.

4.2.4 Testování přeslechů a impedančních problémů

Přepneme otočný přepínač do polohy *DIAG* a vybereme volbu *Find Crosstalk Fault* (přeslechy) nebo *Find Impedance Fault* (impedance) a volbu potvrdíme tlačítkem *Enter*. Pokud chceme změnit standard přenosu stiskněte tlačítko *F1*, vybereme standard pomocí směrových kláves a potvrdíme tlačítkem *Enter*. Vybrání páru, který bude otestován provedeme stisknutím směrové klávesy dolů, potvrzením *Enter* a poté vybráním konkrétních páru směrovými klávesami a opětovným potvrzením. Vlastní testování kabelu zahájíme tlačítkem *TEST*.

4.3 MicroScanner^2

Přístroj MicroScanner^2 je možné využít podobně jako přístroj CableIQ, nedisponuje takovým množstvím funkcí a jeho ovládání je značně jednodušší. Přesto však poskytuje komplexní možnosti testování a vyhledávání kabeláže.

Obrázek 5 – Ovládací prvky MicroScanner[2]

4.3.1 Testování kabeláže

Po zapnutí přístroje stačí připojit kabel a zvolit použitý port tlačítkem *PORT*. Testování je provedeno automaticky.

4.3.2 Vyhledávání kabeláže

Vyhledávání kabeláže pomocí sondy IntelliTone Probe vybereme opakovaným stisknutím tlačítka *MODE*, dokud se nezobrazí IntelliTone. Pomocí směrových kláves je možné vybrat generovaný signál.

4.3.3 Testování PoE

Přístroj je možné použít k otestování přítomnosti PoE napájení. Opakovaným stisknutím tlačítka *MODE* uvedeme přístroj do režimu PoE. Přístroj poté otestuje přítomnost napájení a zobrazí výsledky včetně konkrétních vodičů s PoE napájením.

4.4 LinkRunner Pro

LinkRunner Pro lze rovněž použít pro testování zapojení kabeláže, ale zařízení disponuje funkcemi vhodnými pro testování aktivní síťové topologie. S přístrojem je možné testovat pingem router, DHCP a DNS servery. Dokáže rozpoznat připojená zařízení, která disponují protokoly CDP, EDP a LLDP.

Obrázek 6 – Ovládací prvky LinkRunner Pro

Zařízení po spuštění ihned detekuje zda-li je kabel připojený, zobrazí rychlost, délku kabelu, křížení, dostupnost PoE a vytížení linky. Pomocí směrových kláves je možné přepínat mezi jednotlivými režimy přístroje.

4.4.1 Režim PING

V režimu PING se zobrazí IP adresa přístroje, přenesené pakety. Pomocí směrových kláves je možné přepnout na informace o výchozím směrovači, DHCP, DNS a vypsat výsledky PING těchto adres.

4.4.2 Režim LLDP, CDP, EDP

Přístroj zobrazí detekované zařízení, které disponují některým z těchto protokolů. Podle možností zobrazí název, adresu detekovaného zařízení a informace o připojeném portu a VLAN.

4.4.3 Režim Flash hub port

Přístroj generuje signál, kterým pravidelně rozbliká připojený port přepínače. Použitím směrových kláves je možné ovlivnit rychlost blikání.

4.4.4 Režim IntelliTone

Přístroj generuje signál pro vyhledávání kabeláže pomocí sondy IntelliTone Probe. Použitím směrových kláves je možné změnit typ signálu.

4.5 IntelliTone Probe

IntelliTone Probe slouží jako detekční sonda přítomnosti signálu v kabelu. Její pomocí lze vyhledávat vedení ve zdi, lištách a identifikovat konkrétní kabel ve svazku.

Obrázek 7 – Ovládací prvky IntelliTone Probe

4.5.1 Použití sondy

Pomocí otočného přepínače zapneme sondu a uvedeme ji do jednoho z následujících režimů:

- digitální signál, vysoká citlivost;
- digitální signál, nízká citlivost;
- analogový signál.

Nízká citlivost je vhodná pro přesnou identifikaci konkrétního kabelu ve svazku. Po přepnutí sondy do požadovaného režimu pohybujeme hrotem a vyhledáváme kabel, pokud sonda nalezne signál oznámí to zvukovým signálem a rozsvícením určitého počtu LED podle síly signálu.

Samotnou sondu nelze použít pro vyhledávání signálu, je nutné mít do daného kabelu zapojený další přístroj, který bude generovat signál.

4.6 NetTool series II

NetTool series II lze použít pro otestování kabeláže, ale především je ho možné zapojit v inline režimu – měřící přístroj zapojený mezi přepínač a počítač. Přístroj je pak schopen zobrazit informace o komunikaci, vytížení linky nebo otestovat dostupnost internetového připojení.

Obrázek 8 – Ovládací prvky NetTool series II

4.6.1 Autotest v inline režimu

Po spuštění přístroje zapojíme do konektoru na levé straně kabel k přepínači nebo směrovači, na pravou stranu je nutné připojit počítač nebo zařízení napájené pomocí PoE. Z menu vybereme *AutoTest* a potvrdíme. Přístroj po dokončení testů zobrazí informace o připojených zařízeních.

4.6.2 Ping, NetProve

V režimu *Ping* je možné otestovat ping na zvolené IP adresy. NetTool ve výchozím nastavení použije DHCP k získání IP adresy a výchozí brány. V případě potřeby je možné přiřadit IP adresu manuálně v nastavení.

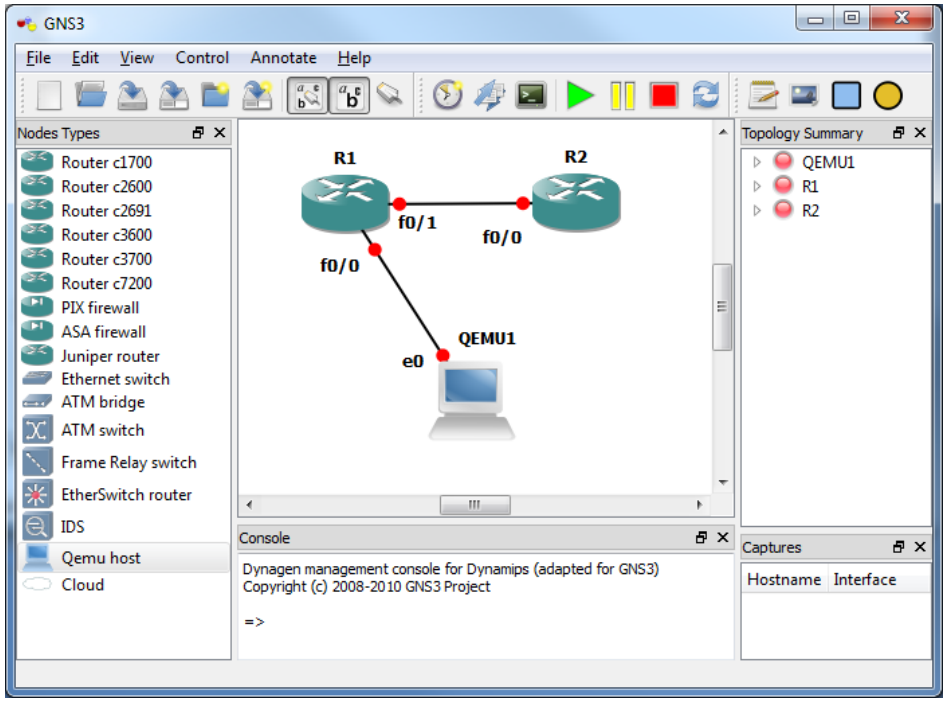
Volba *NetProve* slouží k definování katalogů serverů, které se automaticky otestují pomocí pingu, navíc je možné definovat port a přístroj se pokusí na daný server vytvořit TCP spojení. Tímto způsobem je možné otestovat funkčnost služeb jako je HTTP, FTP nebo SMTP server.

4.6.3 Testování kabelů

Jednotlivé kabely je možné otestovat zapojením obou konců do měřícího přístroje a použitím volby *AutoTest*. Kromě toho je možné použít jednostranné zapojení a na druhé straně zásuvky nebo kabelu připojit Wiremap adaptér. Podobně jako ostatní zařízení je možné NetTool použít pro generování signálů pro IntelliTone Probe.

5 GNS

Program GNS3 slouží jako grafický simulátor počítačových sítí, umožňuje simulování komplexních síťových topologií, Program umožňuje simulovat reálné směrovače firem Cisco a Juniper [2].



Obrázek 9 – Prostředí programu GNS

Je ho možné využít pro přípravu konfigurace pro skutečnou síť, k přípravám na zkoušky CCNA, CCNP a další. GNS je open source program, který je možné použít na platformách Windows, Linux a MacOS X.

Přehled vlastností programu:

- návrh komplexních síťových topologií;
- emulování směrovačů platformy Cisco IOS, IPS, PIX a ASA firewally, JunOS;
- simulace jednoduchých Ethernetových, ATM a Frame relay přepínačů;
- zachytávání paketů a jejich analýza v programu Wireshark;
- propojení simulační části do skutečné sítě.

Samotný program GNS nedisponuje takovými možnostmi, aby bylo možné provést simulaci. Využívá se další software, který poskytuje potřebné služby:

- Dynamips – jádro pro emulování Cisco směrovačů;
- Dynagen – textové rozhraní pro Dynamips;

- Qemu – generický emulátor a virtualizační nástroj pro spuštění virtuálních strojů;
- Putty – telnet, SSH klient; slouží k připojení na konzole virtuálních zařízení;
- Wireshark – nástroj pro zachytávání a analýzu síťového provozu; umožňuje prohlížet komunikaci mezi virtuálními zařízeními.

Dynamips v současnosti dokáže emulovat prostředí pro spuštění směrovačů řady 7200, 3600, 3700 a 2600. Přestože v laboratořích jsou směrovače řady 2800, lze volně použít jinou řadu. Funkce, které se vyučují a používají jsou dostupné na všech podporovaných řadách.

Omezení simulátoru GNS je pouze základní podpora Ethernetových přepínačů, není možné použít plnohodnotné přepínače (např. Cisco Catalyst). Přepínače podporují pouze nastavení VLAN pro daný port, dot1q a QinQ zapouzdření. Funkcionality STP, port security či VTP není možné na přepínačích simulovat. Částečně je možné tuto funkcionalitu simulovat použitím směrovače s přidaným modulem 16ti portového přepínače.

5.1 Instalace GNS

Návod na instalaci GNS na OS Windows:

1. Stáhnout all-in-one balení ze stránky http://www.gns3.net/download.
2. Spustit instalátor a pokračovat dle jeho pokynů, při výběru komponent k instalaci ponechat vše zatržené.
3. Spustit GNS3 z nabídky start.
4. Z menu nabídky *edit* vybereme *preferences*.
5. Na levé straně zvolíme záložku *Dynamips* a stiskneme tlačítko *Test*. Nyní by se mělo zobrazit *Dynamips successfully started*, poté zavřeme nastavení stisknutím *OK*.
6. Z menu nabídky *edit* vybereme *IOS images and hypervisors*.
7. U možnosti *Image file* stiskneme tlačítko *...* a vybereme soubor s OS IOS. Dle možností specifikujeme platformu, model a výchozí nastavení paměti RAM pro daný model. Přidání potvrdíme tlačítkem *Save*. Tento krok opakujeme pro všechny přidávané IOS soubory.
8. Zavřeme nastavení tlačítkem *Close*.
9. Nyní je GNS připraven k použití a můžeme založit simulační projekt.

5.1.1 IOS

K simulaci Cisco zařízení je potřeba vlastnit IOS, pokud již vlastníme směrovač od Cisca, který je kompatibilní s programem Dynamips, je možné stáhnout IOS ze zařízení a využít jej. Zákazníci Cisca mohou IOSy stahovat přímo z jejich webových stránek www.cisco.com. Pro studenty prozatím Cisco nevytvořilo žádnou studentskou verzi, které by bylo možné bezplatně využívat.

5.2 Simulování

Po spuštění GNS zadáme jméno projektu a vybereme umístění na disku. Je vhodné zatrhnout volby pro ukládání konfigurace nvram a startup konfigurace. Ve výchozím nastavení máme po levé straně pracovní plochy zobrazeny veškerá zařízení, které je možné přidat do simulace, přidání se provede přetažením ikony do pracovního prostoru. Pro přidání směrovačů (a ostatních zařízení) je nutné mít předem nastaveny obrazy IOS souborů. Zařízení je nutné následně spustit stisknutím tlačítka *Start/Resume all devices* (▶) z nástrojové lišty nebo stisknutím pravého tlačítka nad zařízením a vybraním volby *Start* z kontextového menu. Po spuštění je možné se připojit na konzoli zařízení z kontextového menu volbou *Console* ().

Pro propojení zařízení slouží ikona konektoru () z nástrojové lišty, kde máme na výběr druh kabelu nebo manuální režim, kdy je možné ručně vybrat port na zařízení. Vlastní propojení provedeme postupným vybráním zařízení na pracovní ploše.

5.2.1 Přídavné karty ve směrovačích

Konfiguraci slotů pro přídavné karty provedeme vybráním volby *Configure* () z kontextového menu zařízení.

Dostupné přídavné karty se liší podle zvoleného zařízení, vkládat lze karty obsahující rozšiřující Ethernetové, FastEthernetové karty. U některých zařízeních jsou dostupné přepínací karty (s jejich pomocí lze simulovat některé další aspekty přepínání) nebo analyzátory provozu (IDS aj.).

Kromě slotových karet je možné přidat WIC moduly WIC-1T a WIC-2T (sériové porty).

5.2.2 Stavy zařízení

Z nástrojové lišty a kontextového menu zařízení je možné přepínat jejich stavy:

- spuštěný ▶ – spustí zařízení nebo dojde k probuzení ze spánku;
- spánek (suspend) ⏸ – zařízení je zavedeno v paměti, nedochází ke ztrátě *running configuration*, ale simulace zařízení není aktivní;
- vypnutý ■ – zařízení je vypnuto, *running config* je zapomenut;
- reload – způsobí restartování zařízení, *running config* je zapomenut.

5.2.3 Zalohování konfiguračních souborů

Volba *Import/Export Startup Configs* slouží k automatickému exportu a importu konfiguračních souborů ze všech zařízení v simulaci. Při použití této volby pouze vybereme složku, kam se konfigurační soubory uloží nebo odkud se načtou. Jednotlivé soubory jsou pojmenovány dle *hostname* zařízení.

5.2.4 Snapshoty

Volba *Take a snapshot* nám umožňuje vytvářet obrazy aktivní topologie a její konfigurace. Tlačítkem *Create* vytvoříme obraz topologie, který se uloží k projektu. Počet obrazů není omezen, vytváření obrazů je možné využít pro zálohování funkční konfigurace nebo pro vytváření různých scénářů. Jednotlivé obrazy je pak možné načíst volbou *Load*. Nebo odstranit z disku volbou *Delete*.

Obrazy na rozdíl od zálohy konfiguračních souborů ukládají i síťovou topologii a je možné měnit zařízení a jejich propojení.

5.2.5 Volba IDLE PC

Simulace po prvním spuštění bude silně vytěžovat procesor, běžně může docházet k 100% vytížení i při nečinnosti. Simulaci je možné optimalizovat konfigurací volby *Idle PC*. Po několika minutách simulace vyvoláme kontextové menu zařízení a vybereme volbu *Idle PC* (). Poté vyčkáme na kalkulaci hodnot a z roletového výběru vybereme zvolenou hodnotu. Hodnoty, které by měly vykazovat lepší výsledky jsou označeny hvězdičkou. Výběr potvrdíme tlačítkem *OK*. Výsledky prvotní optimalizace nemusí být nejlepší, je vhodné po delší době kalkulaci znovu spustit a vyhledat lepší hodnotu.

5.2.6 Cloud

Cloud se obvykle využívá v síťové topologii k vyznačení neznámého místa, kde se může nacházet mnoho zařízení nebo ním může být reprezentován internet. V GNS je prvek Cloud využit ke spojení simulace s reálným světem.

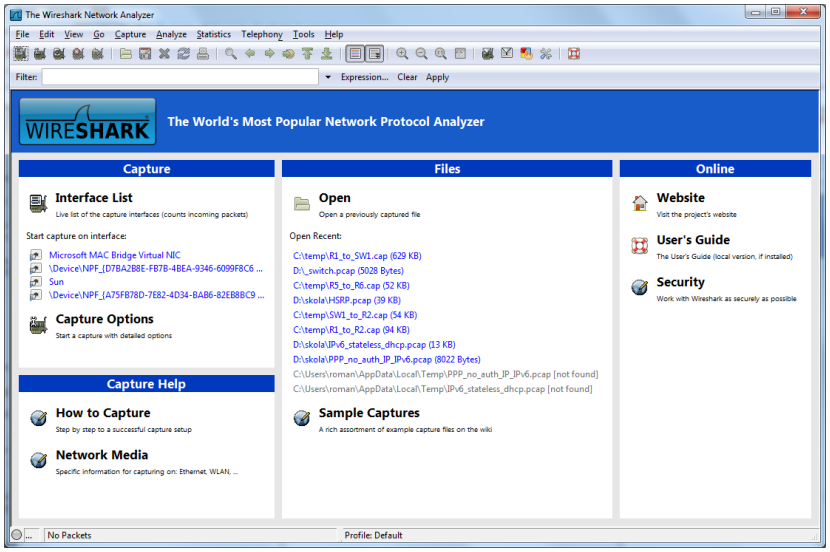
Dostupné volby pro propojení Cloud:

- Ethernet – připojení na fyzické síťové zařízení využitím knihovny WinPcap nebo libpcap;
- TAP – připojení na logické síťové rozhraní typu TAP, rozhraní TAP se využívá jako most mezi fyzickými síťovými zařízeními;
- UDP – připojení na specifikovanou adresu přes protokol UDP, lze takto vytvořit dvoubodové propojení GNS simulátorů;
- UNIX – připojení pomocí UNIXových socketů;

- VDE – připojení na VDE (Virtual Distributed Ethernet) [11] a User-Mode-Linux přepínačů, vhodné na připojení k virtualizovaným strojům, více informací o VDE lze nalézt v [10];
- NULL – připojení nikam nevede, volba vhodná pro debugging a podobné účely.

5.2.7 WireShark

V balíčku GNS se nachází program WireShark, ten slouží k zachytávání a analýze síťového provozu, v současné verzi dokáže analyzovat okolo 1100 různých protokolů a zobrazit přehlednou strukturu paketů.



Obrázek 10 – Prostředí programu WireShark

Zachytávání síťového provozu

Pomocí WireSharku je možné zachytávat síťový provoz v reálném čase z menu vybereme *Capture – Interfaces...*, otevře se nám okno s výpisem aktivním síťových rozhraních. Tlačítkem *Start* můžeme okamžitě zahájit zachytávání provozu, volbou *Options* je možné nastavit rozšířené možnosti zachytávání (zachytávací filtr, omezení velikosti paketu a další). Volbou *Details* je možné zobrazit podrobné informace o daném síťovém rozhraní.

Po aktivování zachytávání se ve střední části obrazovky začne plnit seznam zachycených paketů, kde se zobrazuje čas (doba od počátku zachytávání), zdrojová a cílová adresa (dle druhu paketu se může jednat o MAC, IPv4 či IPv6 adresu), protokol a další informace. Vybráním paketu poklepáním myší se zobrazí další informace pro jeho analýzu ve spodní části. WireShark paket analyzuje a v první části zobrazí stromový výpis paketu dle jednotlivých vrstev či protokolů, ze kterých se skládá. V případě protokolu HTTP je možné jednotlivě procházet pole (hlavičky) všech protokolů Ethernet – IP – TCP – HTTP. V poslední části okna WireSharku je možné vidět celý paket v hexadecimálním vyjádření.

Ukládání, načítání

Zachytávaná data je možné uložit po ukončení zachytávání volbou *File – Save* a později jej načíst volbou *Load*. Velikost vytvořeného souboru bude větší než je celková velikost zachyceného provozu.

Při použití GNS jako zdroje dat pro WireShark, se nevyužívá živé zachytávání provozu, ale výstupem z GNS je soubor, který ve WireSharku načteme. Pro aktualizaci zobrazení v průběhu simulace je nutné WireSharkem znovu soubor načíst.

5.3 Porovnání GNS a PacketTracer

Simulátory GNS a PacketTracer mají mnoho společných rysů, ale využití obou produktů pro určitou zaměření nemusí být vhodné.

PacketTracer

- zdarma pro studenty Netacad akademie;
- vhodný pro simulaci sítí s Cisco zařízeními;
- podporuje směrovače, přepínače a některé další prvky (VoIP, DSL modem, CABLE modem, ...);
- podporuje bezdrátové sítě WiFi;
- simulace není plnohodnotná, některé aspekty simulace nemusejí odpovídat realitě;
- simulaci není možné napojit do reálné sítě;
- simulace lze využít k výuce, tvoření úloh pro studenty.

GNS

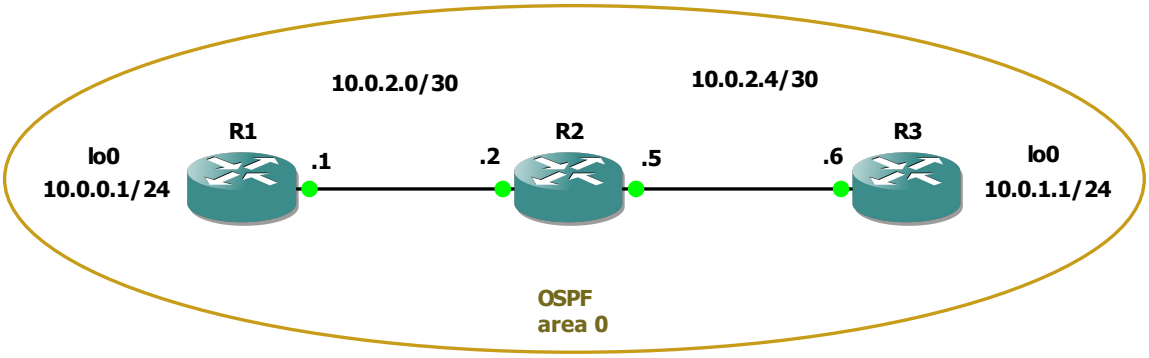
- zdarma (open source produkt), pro simulaci je ale nutné vlastnit visioIOS;
- vhodný pro simulaci sítí s Cisco, Juniper zařízeními;
- omezená podpora přepínačů (Ethernetových, ATM, frame relay);
- možnost využít virtualizové počítače uvnitř simulace;
- simulace je plnohodnotná, v kterémkoliv místě je možné sledovat přenášené pakety;
- simulaci je možné připojit do reálné sítě;
- simulátor nepodporuje tvoření úloh a jejich vyhodnocování.

Z výsledků porovnání vlastností obou produktů je možné říci, že PacketTracer najde využití především u výuky práce s Cisco zařízeními, CCNA kurzů či při výuce počítačových sítí s možností tvoření úloh přímo v simulátoru. Oproti tomu GNS je možné využít pro komplexní simulaci, propojit simulovaný systém do reálného a zkoumat přesné chování uvnitř systému. Nejedná se výukový nástroj, ale je ho například možné využít k prezentování při výuce nové látky a k jiným demonstracím. Při využití simulátoru pro přípravu topologie do reálného světa je nutné zvážit, jestli budeme potřebovat bezdrátové sítě, rozšířené vlastnosti přepínačů a podle toho volit vhodný nástroj. Přednost bych dával GNS, které poskytuje reálný obraz chování zařízení.

5.4 Příklady použití

5.4.1 Směrování s OSPF

V prvním příkladu bude cílem vytvořit topologii o třech směrovačích s dynamickým směrovacím protokolem OSPF. Loopback rozhraní budou sloužit pro simulování sítě připojené ke směrovačům.



Obrázek 11 – Topologie směrovačů

Příprava

Z panelu nástrojů vybereme vhodný směrovač a přesuneme ho do pracovní plochy. Tímto způsobem přeneseme tři směrovače. Propojení provedeme volbou *manual* dle topologie, spustíme simulaci a připojíme se na všechny směrovače přes konzoli.

Konfigurace

Nejprve nastavíme jednotlivá rozhraní FastEthenertu a loopback na všech směrovačích. Vzhledem k reálné simulaci směrovačů je nutné konfiguraci provést přes příkazový řádek, popis jednotlivých konfiguračních voleb je možné nalézt v [8].

```
R1>en
R1#conf t
R1(config)#int lo 0
R1(config-if)#ip add 10.0.0.1 255.255.255.0
R1(config-if)#no sh
R1(config-if)#int f0/0
```

```
R1(config-if)#ip add 10.0.2.1 255.255.255.252
R1(config-if)#no sh

R2>en
R2#conf t
R2(config)#int f 0/0
R2(config-if)#ip add 10.0.2.2 255.255.255.252
R2(config-if)#no sh
R2(config-if)#int f0/1
R2(config-if)#ip add 10.0.2.5 255.255.255.252
R2(config-if)#no sh

R3>en
R3#conf t
R3(config)#int lo 0
R3(config-if)#ip add 10.0.1.1 255.255.255.0
R3(config-if)#no sh
R3(config-if)#int fa 0/1
R3(config-if)#ip add 10.0.2.6 255.255.255.252
R3(config-if)#no sh
```

Správnou funkčnost můžeme ozkoušet příkazem *ping* z R2.

```
R2(config-if)#do ping 10.0.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.2.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 64/77/108 ms

R2(config-if)#do ping 10.0.2.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.2.6, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/27/56 ms
```

Pozn.: První požadavek pingu selže v důsledku prázdné ARP tabulky směrovače.
Po nakonfigurování rozhraní přistoupíme ke konfiguraci OSPF. Ještě předtím spustíme zachytávání paketů na jedné z linek, například mezi R1-R2. Stisknutím pravého tlačítka myši nad linkou zobrazíme kontextové menu ze kterého vybereme *Capture* (). Tím spustíme program Wireshark, který bude zobrazovat zachycená data. Data jsou průběžně ukládána do souboru a okno Wiresharku je nutné ručně aktualizovat tlačítkem *Reload this caputure file* ()
Nyní nakonfigurujeme OSPF.

```
R1(config-if)#ex
R1(config)#router ospf 1
R1(config-router)#network 10.0.0.0 0.0.0.255 a 0
R1(config-router)#network 10.0.2.0 0.0.0.3 a 0

R2(config-if)#ex
R2(config)#router ospf 1
R2(config-router)#net 10.0.2.0 0.0.0.3 a 0
R2(config-router)#net 10.0.2.4 0.0.0.3 a 0

R3(config-if)#ex
R3(config)#router ospf 1
R3(config-router)#net 10.0.2.4 0.0.0.3 a 0
R3(config-router)#net 10.0.1.0 0.0.0.255 a 0
```

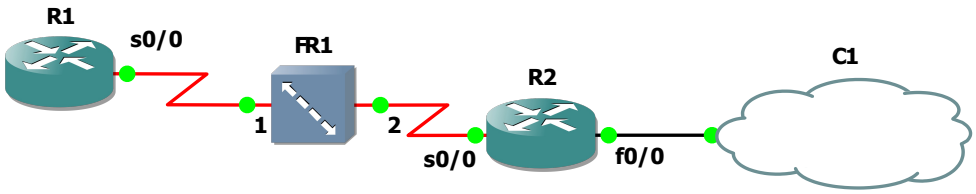
Během konfigurace OSPF bychom měli v konzoli vidět proces navázání OSPF sousedství mezi směrovači.

```
*Mar  1 00:08:28.735: %OSPF-5-ADJCHG: Process 1, Nbr 10.0.0.1 on FastEthernet0/0
from LOADING to FULL, Loading Done
*Mar  1 00:08:36.931: %OSPF-5-ADJCHG: Process 1, Nbr 10.0.1.1 on FastEthernet0/1
from LOADING to FULL, Loading Done
```

Nyní můžeme vyzkoušet ping z R1 na R3, který by měl uspět. V okně Wiresharku je možné sledovat proces navázání partnerství mezi směrovači a následné Hello pakety.

5.4.2 Frame-relay a cloud

Následující příklad demonstruje použití frame-relay přepínače a následné připojení celé topologie do reality pomocí prvku cloud.



Obrázek 12 – Topologie sítě

Příprava

Přenesením prvků prvků do pracovní plochy připravíme znázorněnou topologii. Před propojením kabely otevřeme konfiguraci frame-relay přepínače a přidáme následující mapování.

Tabulka 1 – Mapování frame-relay přepínače

source		destination	
port	DLCI	port	DLCI
1	101	2	102

V laboratořích není dostupný frame-relay přepínač, ale můžeme použít směrovač, který nakonfigurujeme, aby tuto funkcionalitu zajistil.

```
R3>en
R3#conf t
R3(config)#frame-relay switching
R3(config)#int se 0/0
R3(config-if)#encapsulation frame-relay ietf
R3(config-if)#frame-relay lmi-type ansi
R3(config-if)#frame-relay intf-type dce
R3(config-if)#frame-relay route 101 int se 0/1 102
R3(config-if)#no sh
R3(config-if)#int se 0/1
R3(config-if)#encapsulation frame-relay ietf
```

```
R3(config-if)#frame-relay lmi-type ansi
R3(config-if)#frame-relay intf-type dce
R3(config-if)#frame-relay route 102 int se 0/0 101
```

V nastavení prvku cloud vybereme NIO Ethernet a vybereme vhodný adaptér. V případě Linuxu je nutné použít TAP adaptér, jinak nebude možné komunikovat se simulací z lokálního počítače.

Konfigurace

Po spuštění simulace začneme konfiguraci frame-relay rozhraní. Před vlastní konfigurací si spustíme zachytávání paketů na jedné z linek do Wiresharku, u sériových linek je nutné vybrat správné zapouzdření, v případě frame-relay tedy FR.

```
R1>en
R1#conf t
R1(config)#int se 0/0
R1(config-if)#encapsulation frame-relay ietf
R1(config-if)#frame-relay lmi-type ansi
R1(config-if)#ip add 172.31.0.1 255.255.255.252
R1(config-if)#no sh

R2>en
R2#conf t
R2(config)#int se 0/0
R2(config-if)#encapsulation frame-relay ietf
R2(config-if)#frame-relay lmi-type ansi
R2(config-if)#ip add 172.31.0.2 255.255.255.252
R2(config-if)#no sh
```

Pozn.: V tomto příkladě je použita volba *ietf* u zapouzdření frame-relay, která zaručuje kompatibilitu i se zařízeními jiných výrobců. V GNS je možné simulovat i Cisco rozšíření a není nutné používat tuto volbu.
Po chvíli čekání by mělo dojít k vyhledání druhého konce na frame-relay lince pomocí inverzního ARPu a ping by měl uspět mezi oběma směrovači. Funkčnost frame-relay je dále možno ověřit příkazy *show frame-relay map*, *show frame-relay pvc*. V následujícím kroku nastavíme statické směrování na R1 a připojíme R2 do cloudu, zde se předpokládá, že lokální počítač je v síti 192.168.1.0/24.

```
R1(config-if)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 172.31.0.2

R2(config-if)#exit
R2(config)#int fa 0/0
R2(config-if)#ip add 192.168.1.254 255.255.255.0
R2(config-if)#no sh
```

Nyní zbývá otestovat připojení cloudu, na lokálním počítači spustíme ping na adresu 192.168.1.254, který by měl uspět. Abychom se dostali na R1 je nutné doplnit do směrovací tabulky počítače nový záznam.

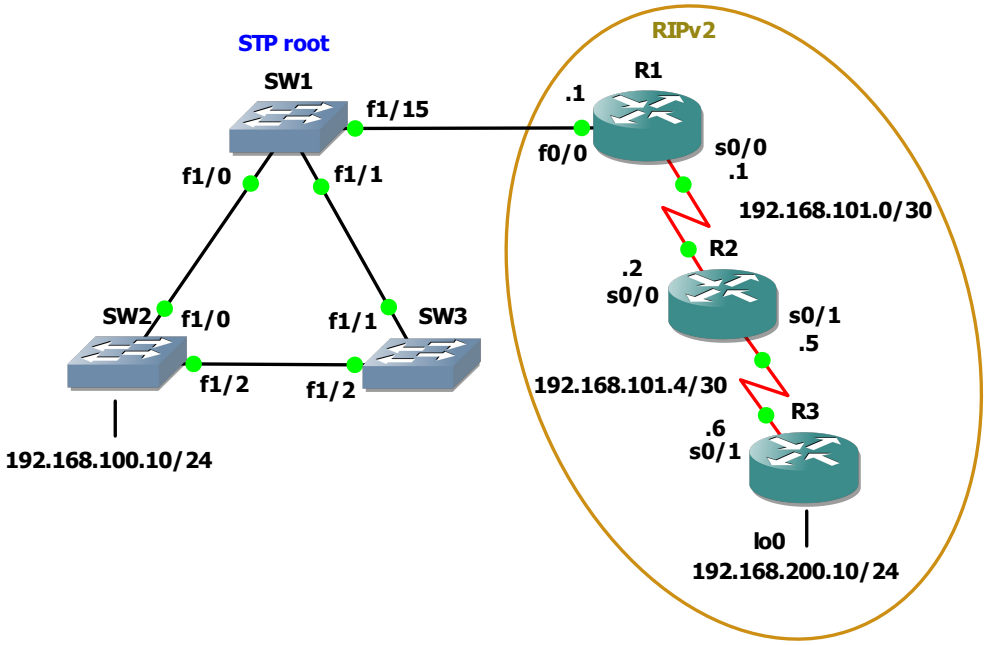
```
route add 172.31.0.0 mask 255.255.255.252 192.168.1.254

route print (zkrácený výpis)
IPv4 Route Table
===========================================================================
```

```
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1    192.168.1.20      10
       172.31.0.0  255.255.255.252    192.168.1.254    192.168.1.20      11
===========================================================================
```

Následně můžeme spustit ping na R1 (172.31.0.1) a měl by uspět. Velmi jednoduchým způsobem jsme tak propojili simulaci v GNS s reálným zařízením. V okně Wiresharku je možné sledovat komunikaci na frame-relay lince.

5.4.3 STP v GNS

Příklad demonstruje využití modulu přepínače pro směrovač 3725, abychom zlepšili možnosti simulování přepínačů v GNS.



Obrázek 13 – Topologie sítě

Příprava

Přeneseme prvky do pracovní plochy, pro „přepínače“ použijeme zařízení *EtherSwitch router* nebo ručně přeneseme směrovač 3725 a v konfiguraci slotů přidáme NM-16ESW. Vizuální symbol zařízení je možné změnit z kontextového menu volbou *Change Symbol* ( ).

Konfigurace

Na všech linkách, které propojují přepínače vytvoříme trunk a zvolíme nativní VLAN 99.

```
interface FastEthernet1/X
switchport trunk native vlan 99
switchport mode trunk
```

Přepínač SW1 nastavíme jako STP root.

```
spanning-tree vlan 1 priority 8192
```

Následně po uplynutí doby konvergence je možné ověřit fungování STP mezi přepínači. Na rozdíl od přepínačů řady Catalyst je přehledný výpis stavu STP protokolu pomocí příkazu *show spanning-tree brief*.

```
SW1#show spanning-tree brief
VLAN1
  Spanning tree enabled protocol ieee
  Root ID     Priority    8192
              Address     c201.0938.0000
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    8192
              Address     c201.0938.0000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface                                   Designated
Name                 Port ID Prio Cost  Sts Cost  Bridge ID            Port ID
-------------------- ------- ---- ----- --- ----- -------------------- -------
FastEthernet1/0      128.41   128    19 FWD     0  8192 c201.0938.0000 128.41
FastEthernet1/1      128.42   128    19 FWD     0  8192 c201.0938.0000 128.42
FastEthernet1/15     128.56   128    19 FWD     0  8192 c201.0938.0000 128.5

SW2#show spanning-tree brief

VLAN1
  Spanning tree enabled protocol ieee
  Root ID     Priority    8192
              Address     c201.0938.0000
              Cost        19
              Port        41 (FastEthernet1/0)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32768
              Address     c203.0938.0000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface                                   Designated
Name                 Port ID Prio Cost  Sts Cost  Bridge ID            Port ID
-------------------- ------- ---- ----- --- ----- -------------------- -------
FastEthernet1/0      128.41   128    19 FWD     0  8192 c201.0938.0000 128.41
FastEthernet1/2      128.43   128    19 BLK    19 32768 c202.0938.0000 128.43
```

Konfiguraci ostatních prvků je možné nalézt ve vyhotoveném projektu.

6 Závěr

Vybudované síťové laboratoře NET101 a NET102 jsou již aktivně využívány pro výuku a splňují veškeré požadavky, které byly definovány. Přesto jsou zde možnosti, jak laboratoře rozšířit a některé varianty byly zmíněny na předchozích stránkách. I přes velký rozsah oprávnění, které studenti mají na počítačích a při práci s Cisco zařízeními je používání laboratoří bezproblémové.

V rámci vylepšení laboratoří byla na Netlab serveru zprovozněna virtualizační platforma Xen a připraveno prostředí pro provoz Eagle serveru. Jednoduchým způsobem je možné vytvořit vlastní virtuální server pro každé cvičení počítačových sítí a využívat jej při výuce počítačových sítí i Cisco kurzů. Eagle server slouží k výuce Cisco kurzů a je ho možné využívat pro snazší pochopení funkčnosti některých síťových služeb. Studenti si mohou prakticky ozkoušet jejich funkčnost a prozkoumat komunikaci jednotlivých protokolů.

Nástroj GNS lze využít jako velmi kvalitní simulátor počítačových sítí, jako pomůcku při prezentaci témat z Cisco kurzů i praktických vlastností chování sítí. Velmi užitečná je možnost zobrazit komunikaci síťových zařízení pomocí programu Wireshark nebo připojení simulace do reálné sítě. Přesto tento nástroj má několik úskalí, které je nutné brát na vědomí (podpora přepínačů, Wi-Fi, licence IOS).

Literatura

[1] *Fluke networks* [online]. 2006–2011 [cit. 8.3.2011]. Test and Troubleshoot. Dostupné na: <http://www.flukenetworks.com/fnet/en-us/products/family.htm?categorycode=LANT>.

[2] *GNS3* [online]. 2011 [cit. 17.2.2011]. Dostupné na: <http://www.gns3.net/>.

[3] *OpenWrt Wiki* [online]. 2011 [cit. 5.3.2011]. Dostupné na: <http://wiki.openwrt.org/doc/start>.

[4] *OpenWrt Wiki* [online]. 2011 [cit. 5.3.2011]. Linksys WRT54G/L/S. Dostupné na: <http://wiki.openwrt.org/toh/linksys/wrt54gl>.

[5] *Xen Wiki* [online]. 2011 [cit. 4.5.2011]. XenOverview. Dostupné na: <http://wiki.xensource.com/xenwiki/XenOverview>.

[6] *Xen Wiki* [online]. 2011 [cit. 29.4.2011]. XenNetworking. Dostupné na: <http://wiki.xensource.com/xenwiki/XenNetworking>.

[7] Lal, D. C. *Introduction to Eagle Server* [online]. 28.7.2007 [cit. 8.3.2011]. Dostupné na: <www.cisco.com/asiapac/academy/academy/files/Eagle_Server.pdf>.

[8] Lammle, T. *CCNA : výukový průvodce přípravou na zkoušku 640-802*. Brno : Computer Press, 2010. 928 s. ISBN 978-80-251-2359-1.

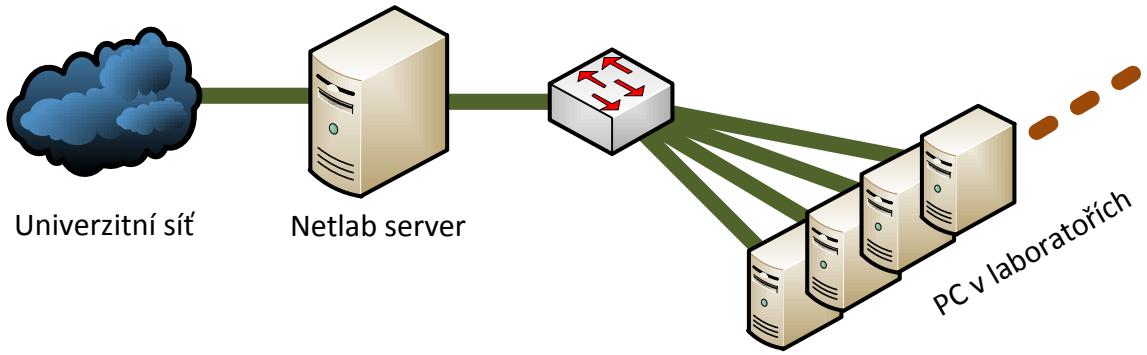
[9] Timme, F. *HowtoForge* [online]. c2009 [cit. 29.4.2011]. How To Run Fully-Virtualized Guests (HVM) With Xen 3.2 On Debian Lenny (x86_64). Dostupné na: <http://www.howtoforge.com/how-to-run-fully-virtualized-guests-hvm-with-xen-3.2-on-debian-lenny-x86_64>.

[10] Virtualsquare Team. *Virtual Distributed Ethernet* [online]. 2011 [cit. 5.3.2011]. Dostupné na: <http://vde.sourceforge.net/>.

[11] Wenzel, E. *Linux man page* [online]. 2011 [cit. 17.2.2011]. hypervisor_mode(7). Dostupné na: <http://linux.die.net/man/7/hypervisor_mode>.

Příloha A – Dokumentace laboratoří NET101, NET102

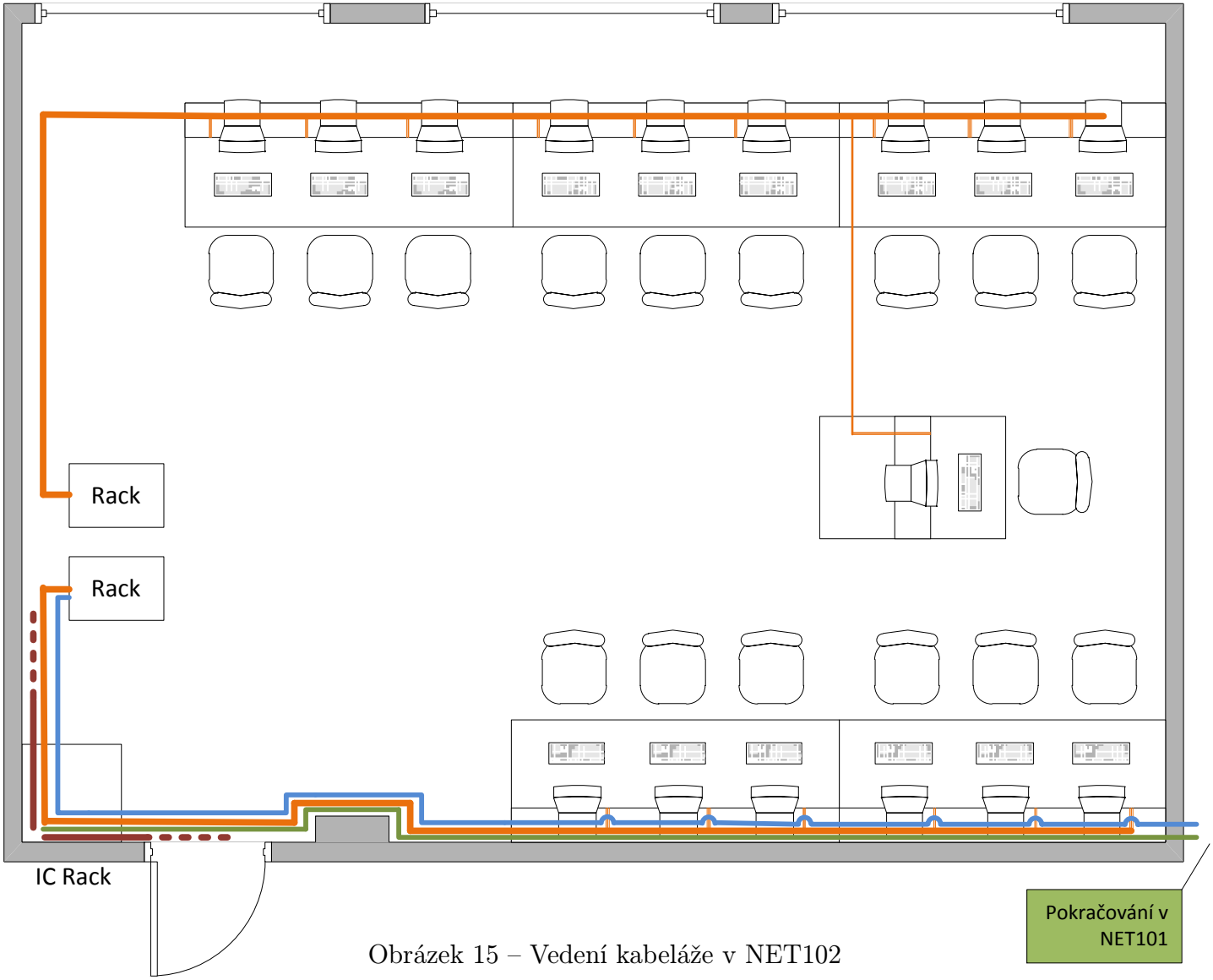
Kabeláž v laboratořích je provedena kategorií Cat 5e, podle normy T568A. Veškerá kabeláž byla otestována přístrojem CableIQ a splňuje požadavky na standard 1000BASE-T.



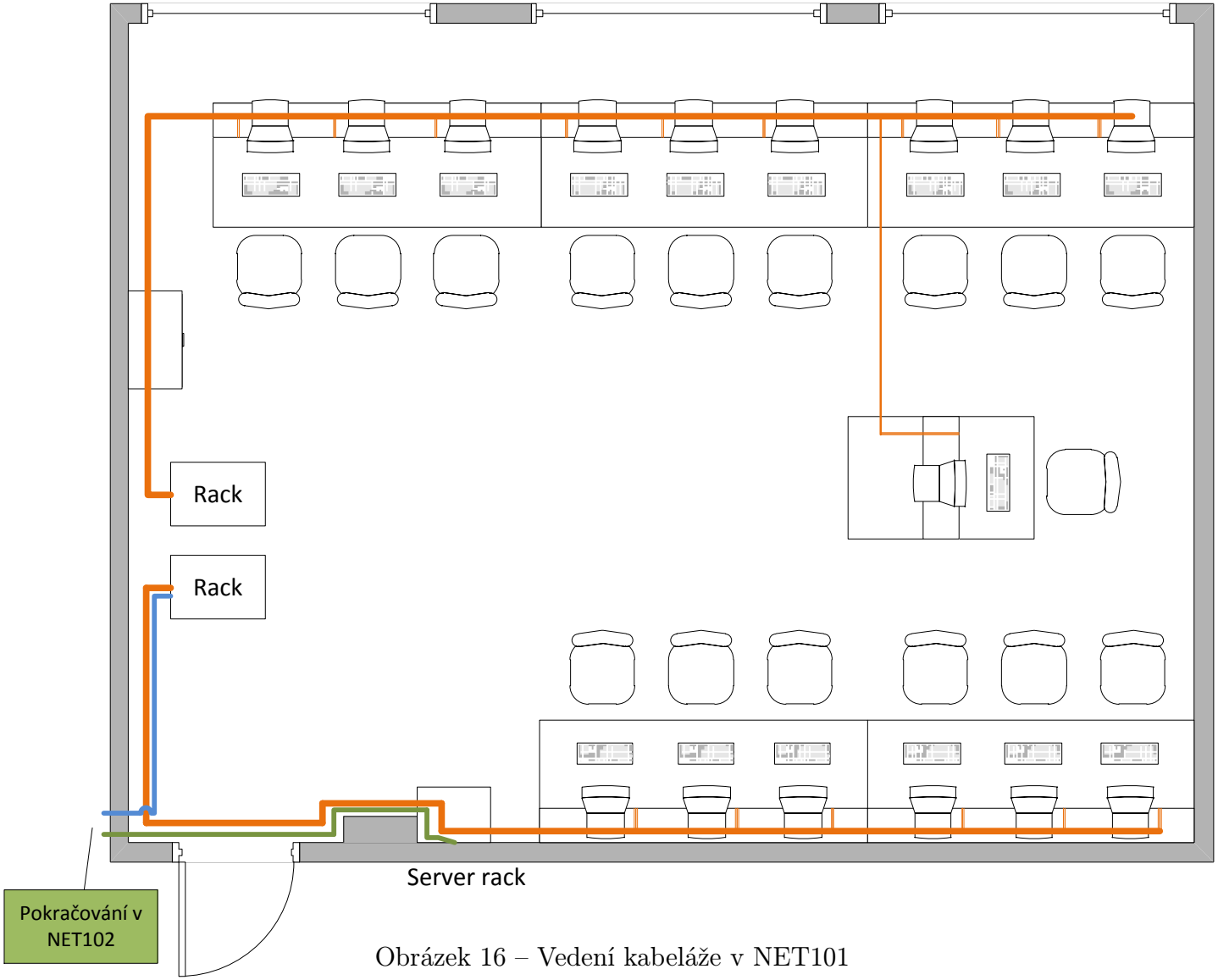
Obrázek 14 – Logická topologie laboratoří

Legenda barev na nákresech kabeláže v laboratořích:

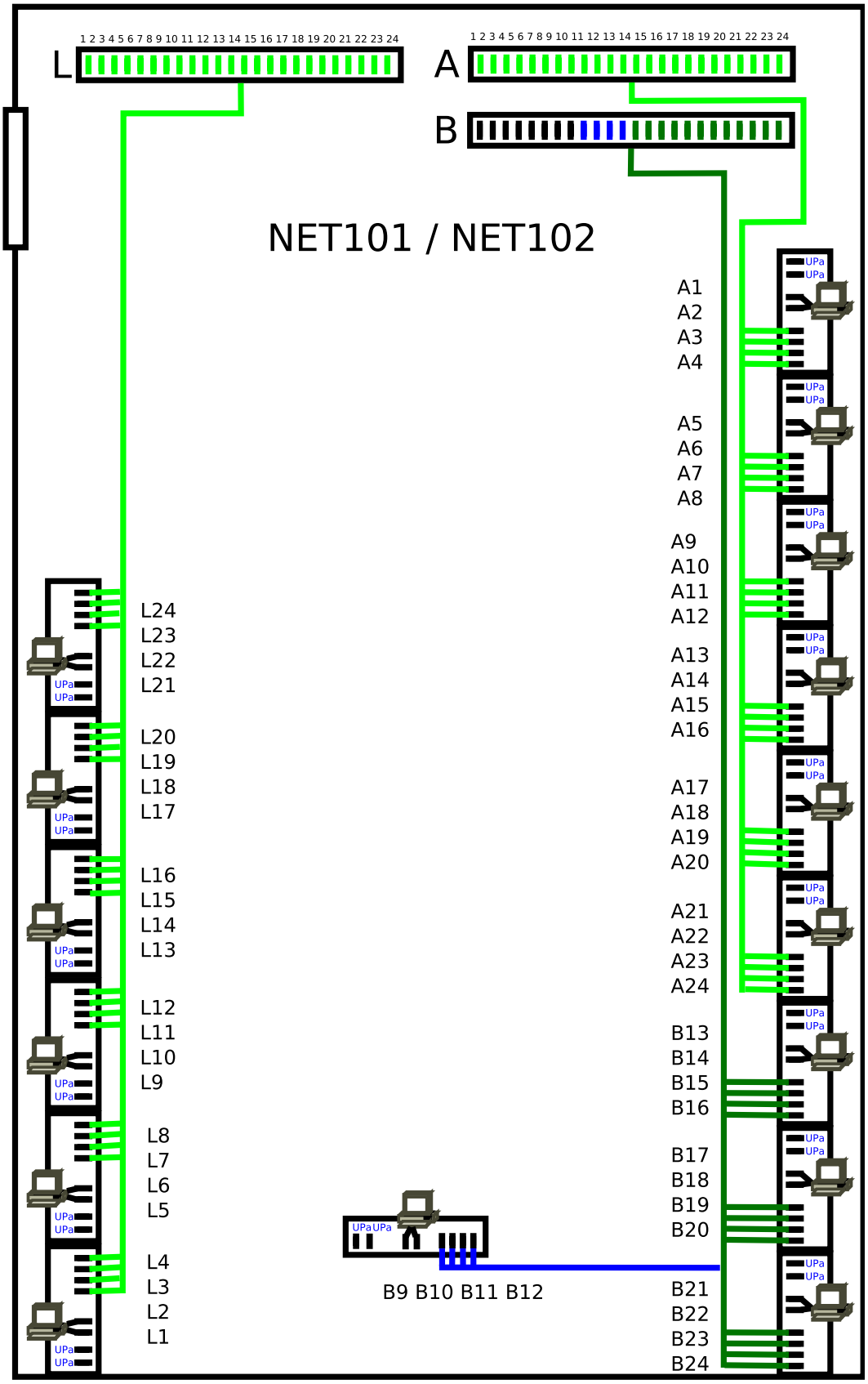
- oranžová (▬) – propojení racků se zařízeními k jednotlivým pracovištím, každé pracoviště má k dispozici čtyři zásuvky;
- modrá (▬) – propojení racků mezi laboratořemi pro možnost tvoření komplexních topologií, k dispozici jsou čtyři kabely;
- zelená (▬) – propojení racku s Netlab serverem do IC racku, čtyři kabely, v současnosti jsou dva nevyužité;
- hnědá (▬) – propojení z IC racku k jednotlivým pracovištím (připojení přes Netlab server k univerzitní síti), každé pracoviště má k dispozici dvě zásuvky, k učitelským pc jsou protaženy čtyři kabely (pouze dva jsou připojeny); kabeláž je tažena z IC racku do obou laboratoří; na výkresech není IC kabeláž detailně vyznačena.



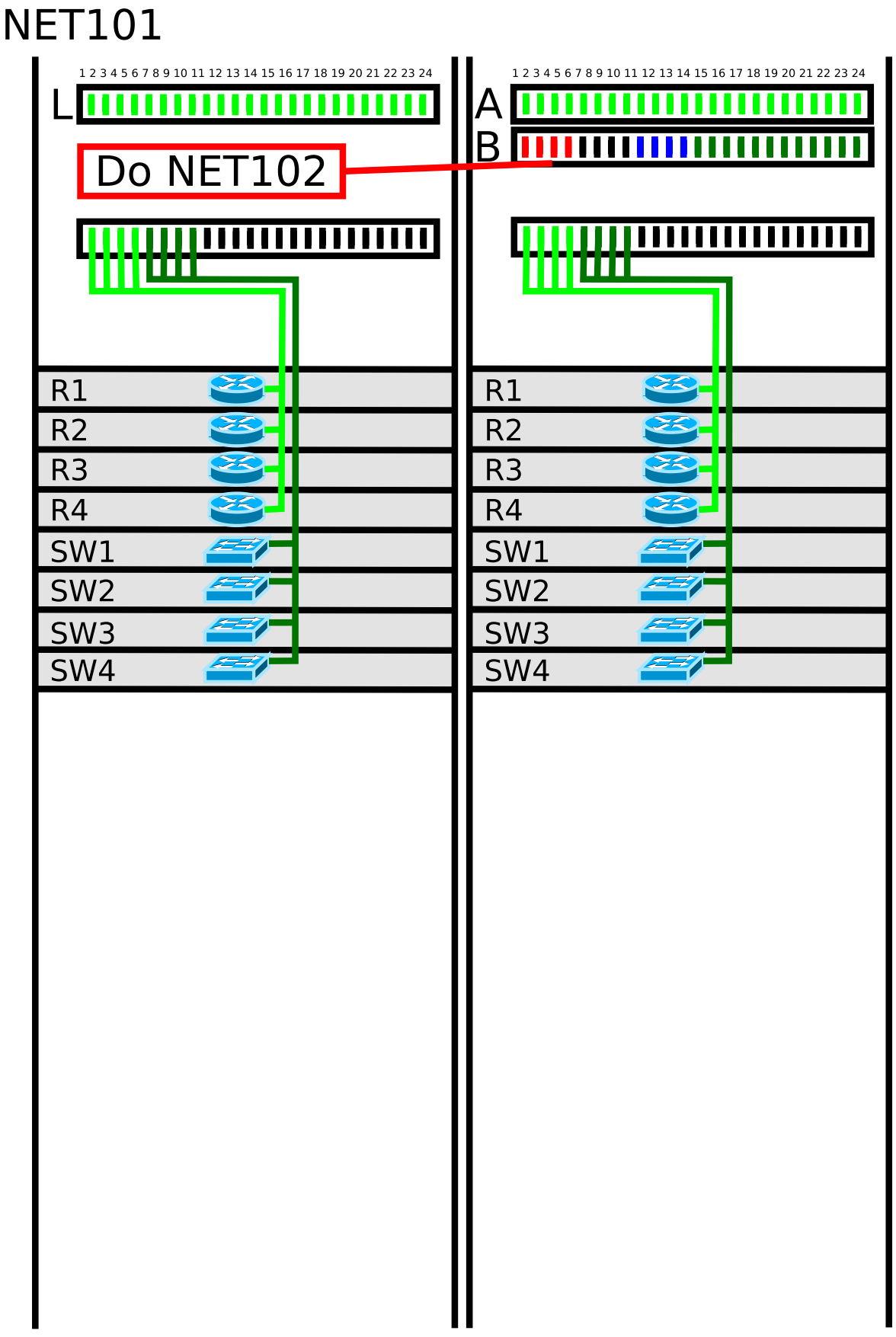
Obrázek 15 – Vedení kabeláže v NET102



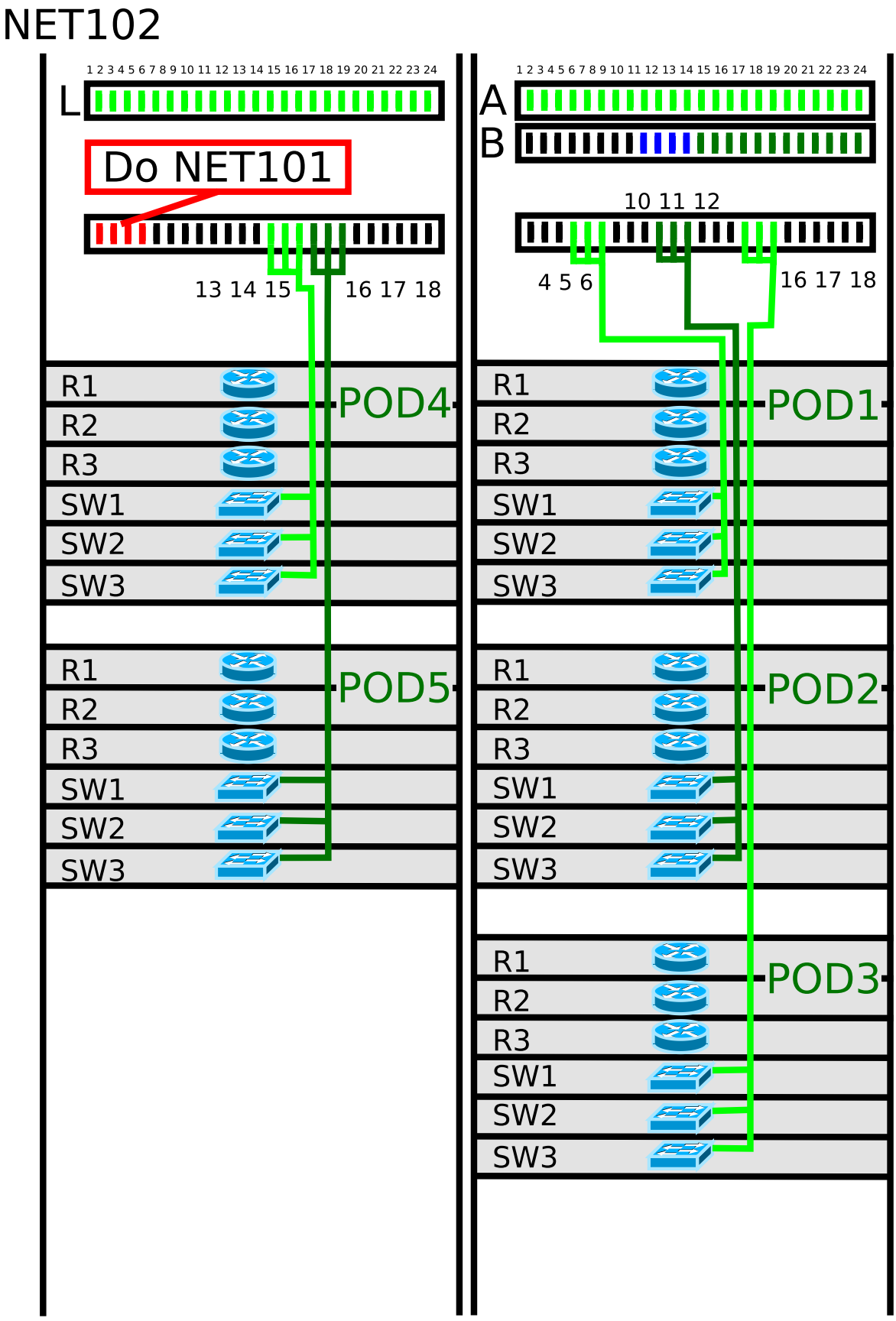
Obrázek 16 – Vedení kabeláže v NET101



Obrázek 17 – Zapojení zásuvek do racků v NET učebnách



Obrázek 18 – Zapojení patch panelů v NET101



Obrázek 19 – Zapojení patch panelů v NET102

Tabulka 2 – Přehled vybavení a zařízení v NET101

Zařízení (produkt / model)	**Počet**	**Poznámka**
Dell OptiPlex 360DT Standard	9	počítač, monitor, klávesnice, myš
dataprojektor Acer	1	
Dell PowerEdge R210	1	Netlab server
AP Linksys WRT54GL	9	firmware nahrazen OpenWRT
Cisco 2811 ISR	8	c2800nm-adventerprisek9-mz.124-22.T.bin
Cisco Catalyst 2960	4	c2960-lanbasek9-mz.122-53.SE1.bin
Cisco Catalyst 3560	4	c3560-ipservices-mz.122-35.SE5.bin
Fluke CableIQ	2	
Fluke IntelliTone Pro 100 probe	3	
Fluke LinkRunner Pro	2	
Fluke MicroScanner^2	1	
Fluke NetTool series II	1	

Tabulka 3 – Přehled vybavení a zařízení v NET102

Zařízení (produkt / model)	**Počet**	**Poznámka**
Dell OptiPlex 360DT Standard	16	počítač, monitor, klávesnice, myš, USB Wi-Fi
dataprojektor Acer	1	
Cisco 2801 ISR	15	c2801-advipservicesk9-mz.124-24.T2.bin
Cisco Catalyst 2960	15	c2960-lanbase-mz.122-35.SE5.bin
AP Cisco Aironet 1232AG-E-K9	1	Netlab Wi-Fi

Příloha B – Ovládací skript pro Eagle server

```
#!/bin/bash
echo EAGLE MANAGER
INSTANCE=`xm list | grep eagle | cut -f 1 -d " "`

case "$1" in
'start')
    if [[ -n "$INSTANCE" ]]; then
        echo Jiz je spustena instance $INSTANCE
        exit
    fi

    if [[ -e "/etc/xen/eagle-$2.cfg" ]]; then
        echo Spoustim eagle-$2
        xm create /etc/xen/eagle-$2.cfg
    else
        echo Zvoleny server neexistuje!
    fi
    ;;

'stop')
    if [[ -n "$INSTANCE" ]]; then
        echo Ukoncuji instanci $INSTANCE
        xm shutdown $INSTANCE
    else
        echo Neni spusten zadny eagle server!
    fi
    ;;

'create')
    if [[ -z "$2" ]]; then
        echo Prazdne jmeno!
        exit
    fi

    echo Vytvari se kopie Eagle serveru s oznacenim - eagle-$2
    echo Proces potrva nekolik minut...
    sed s/eagle.img/eagle-$2.img/ /etc/xen/eagle.cfg | \
    sed "s/name = \"eagle/name = \"eagle-$2/" \
    > /etc/xen/eagle-$2.cfg
    cp /home/eagle.img /home/eagle-$2.img &
    FULLSIZE=`du -b /home/eagle.img | cut -f 1`
    while [[ 1 = 1 ]]
    do
            NEWSIZE=`du -b /home/eagle-$2.img 2>/dev/null | cut -f 1`
            PERCENT=`echo "$NEWSIZE * 100 / $FULLSIZE" | bc`
            echo -ne "Dokonceno: $PERCENT %   \r"

            if [[ "$FULLSIZE" -eq "$NEWSIZE" ]]; then
                    echo "Kopie dokoncena."
                    break
            fi
            sleep 2
    done
    ;;

'remove')
    if [[ -e "/etc/xen/eagle-$2.cfg" ]]; then
        echo Mazi server eagle-$2
        rm /etc/xen/eagle-$2.cfg
        rm /home/eagle-$2.img
    else
        echo Zvoleny server neexistuje!
    fi
```

```
    ;;

'list')
    echo Bezici Eagle instance:
    xm list | grep "eagle\|Name"
    echo ----------------------
    echo Dostupne Eagle servery:
    ls /etc/xen/eagle*.cfg | cut -c 10- | sed s/.cfg//
    ;;

*)
    echo eagle \{ start \| stop \| create \| remove \| list\ }
    ;;
esac
```