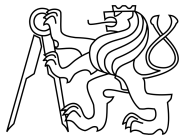
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ



ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Název:	Optimalizace laboratoře pro výuku základů počítačových sítí
Student:	Lukáš Nagy
Vedoucí:	Ing. Viktor Černý
Studijní program:	Informatika
Studijní obor:	Informační technologie
Katedra:	Katedra počítačových systémů
Platnost zadání:	Do konce letního semestru 2016/17

Pokyny pro vypracování

Analyzujte současný stav laboratoře pro výuku základů počítačových sítí.
Na základě Vaší analýzy sestavte seznam nedostatků, které znesnadňují práci v učebně a výuku základů počítačových sítí.
Ve spolupráci s vedoucím práce navrhněte implementaci možných změn, které by mohly vést k efektivnějšímu využívání laboratoře. Zpracujte sadu skriptů pro učitelské a studentské PC, která usnadní detekci chyb v síťové konfiguraci. Ověřte.
V součinnosti se správci sítě v síťové učebně navrhněte dvě možné konfigurace síťové učebny:
- Ideální učebna - nerealizovatelné řešení bez limitů, které jsou v současné učebně.
- Reálná učebna - nejlepší realizovatelné řešení v rámci limitů současné učebny.

Výsledná řešení porovnejte.
Změny, u kterých bude ověřeno, že vedou k efektivnějšímu využití laboratoře, připravte pro produkční nasazení.

Seznam odborné literatury

Dodá vedoucí práce.

L.S.

prof. Ing. Róbert Lórencz, CSc.
vedoucí katedry

prof. Ing. Pavel Tvrdík, CSc.
děkan

V Praze dne 10. prosince 2015

České vysoké učení technické v Praze
Fakulta informačních technologií
Katedra počítačových systémov

Bakalárska práca

Optimalizace laboratoře pro výuku základů počítačových sítí

Lukáš Nagy

Vedúci práce: Ing. Viktor Černý

16. decembra 2016

Poďakovanie

Ďakujem mojej najbližšej rodine za neustálu plnú podporu počas písania tejto práce i počas celého štúdia. Ďalej by som chcel poďakovať môjmu vedúcemu, pánovi Ing. Viktorovi Černému za užitočné pripomienky počas tvorby tejto práce. Pánovi Ing. Martinovi Bílemu za ochotu pri odpovedaní na otázky, týkajúce sa fakultnej sieťovej infraštruktúry.

Prehlásenie

Prehlasujem, že som predloženú prácu vypracoval(a) samostatne a že som uviedol(uviedla) všetky informačné zdroje v súlade s Metodickým pokynom o etickej príprave vysokoškolských záverečných prác.

Beriem na vedomie, že sa na moju prácu vzťahujú práva a povinnosti vyplývajúce zo zákona č. 121/2000 Sb, autorského zákona, v znení neskorších predpisov. V súlade s ustanovením § 46 odst. 6 tohoto zákona týmto udeľujem bezvýhradné oprávnenie (licenciu) k používaniu tejto mojej práce, a to vrátane všetkých počítačových programov ktoré sú jej súčasťou alebo prílohou a tiež všetkej ich dokumentácie (ďalej len „Dielo“), a to všetkým osobám, ktoré si prajú Dielo používať. Tieto osoby sú oprávnené Dielo používať akýmkoľvek spôsobom, ktorý neznižuje hodnotu Diela, ale len pre nezárobkové účely. Toto oprávnenie je časovo, územne a množstevne neobmedzené.

V Prahe 16. decembra 2016 .....

Odkaz na túto prácu

Nagy, Lukáš. *Optimalizace laboratoře pro výuku základů počítačových sítí.* Bakalárska práca. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2016.

Abstrakt

Autor analyzuje stav učebne určenej na výuku počítačových sietí na FIT ČVUT. Poukazuje na problémy, ktoré bránia efektívnej výuke. Práca tiež popisuje dva návrhy takejto učebne, kde pri jednom sa pracuje s ideálnou situáciou bez obmedzení a druhý model prihliada na obmedzenia v súčasnej učebni. Súčasťou je i nástroj pre hlásenie duplicitných adries v sieti napísaný v jazyku Python.

Klíčová slova duplicitné IP adresy, výuka počítačových sietí, analýza sieťového laboratória, návrh počítačovej siete, Python

Abstract

The author analyzes condition of laboratory, used for the teaching of computer networks at FIT CTU. He addresses the problems, which prevents from effective teaching sessions. The thesis also describes two designs of this laboratory, while in first, he works with ideal situation without restrictions and second model considers current constraints in laboratory. Part of the thesis is also a tool for reporting duplicate adresses in network, which is written in Python language.

Keywords duplicate IP addresses, teaching of computer networks, analysis of network laboratory, computer network design, Python

Obsah

Zoznam obrázkov

Zoznam tabuliek

Úvod

Na Fakulte Informačných Technológií Českého Vysokého Učení Technického (FIT ČVUT) bola 10.5.2012 oficiálne otvorené špeciálna Cisco učebňa[1], ktorá slúži ako primárne laboratórium pre výuku počítačových sietí na fakulte. Študenti si môžu v laboratóriu prakticky vyskúšať konfiguráciu sieťových zariadení, keďže učebňa je vybavená potrebným hardwarom.

Zmeny sieťových rozhraní vyžadujú vyššie systémové oprávnenia pre študentov a v produkčnom prostredí fakulty by nebolo možné povoliť takéto zmeny. Jedným z dôvodov je možnosť nedbalo alebo i úmyselne narušiť, prípadne zmeniť funkčnosť počítačov v učebniach. Preto je toto laboratórium súčasťou tzv. „*bouracích učební*“. Tieto izolované učebne sú špecifické tým, že študenti v nich majú práva super-užívateľa a všetky zmeny, ktoré vykonajú sú po reštartovaní počítača zmazané. Slúžia na výuku predmetov o administrácií systémov, sietí alebo na testovanie rôznych operačných systémov.

Izolácia od produkčného prostredia však nezabráni problémom v kontexte samotnej učebni. Nedbalosťou si dokážu študenti zablokovať prístup na užívateľské účty, sieť alebo tiež dokážu narušiť prácu svojich kolegov. Samozrejme sa problém dá riešiť reštartom počítača to však vedie k strate už rozpracovanej práce. Mnohí preto požiadajú učiteľa o pomoc, ten však musí zdĺhavo analyzovať čo študent vlastne spravil aby mu vedel pomôcť, prípadne ho naviesť k riešeniu.

Cieľ práce

Cieľom práce je poskytnúť nástroj pre identifikáciu problémovej konfigurácie sieťových rozhraní na študentských počítačoch v laboratóriu. Ďalším cieľom je vytvorenie návrhu učebne, určenej na výuku počítačových sietí. Poukazuje na typické problémy, s ktorými sa vyučujúci stretáva a slúži ako podklad pre nové

sieťové laboratória. Práca však prináša aj konkrétne riešenia pre učebňu na FIT ČVUT, ktoré môžu byť nasadené za účelom zlepšenia aktuálneho stavu.

Obsah práce

Bakalárska práca je rozdelená do troch častí. Prvá časť je analytická, kde autor popisuje aktuálny stav učebne, topológiu zapojenia a poskytované služby. Autor tu rovnako popíše problémy, ktoré môžu nastať pri výuke.

V druhej časti autor popisuje svoje dva návrhy učebne. Prvým je ideálna učebňa. Tento návrh nie je limitovaný financiami a snahou je vytvoriť laboratórium, kde je možné simulovať i komplexnejšie topológie. Druhým návrhom je učebňa reálna, kde ako konkrétny vzor slúži práve sieťové laboratórium na FIT ČVUT.

V poslednej kapitole autor píše o nástroji pre detekciu duplicitných IP adries, ktorý vytvoril v jazyku Python. Na začiatku je vysvetlená architektúra riešenia, ktorá zahŕňa na akom princípe program nájde duplicitné IP adresy. Potom sa autor dostáva do implementačných detailov, kde sú popísané jednotlivé časti - moduly programu. Nechýba ani vysvetlenie aké knižnice boli použité pre dosiahnutie cieľového stavu. Nasledujú informácie pre užívateľa, kde sa nachádza návod ako nástroj nainštalovať a základné prípady užitia učiteľom. Jednou z príloh v práci je i užívateľská príručka, ktorá popisuje ako program v sieťovej učebni nainštalovať a používať.

Kapitola 1

Analýza súčasného stavu učebne

V tejto kapitole autor popisuje stav učebne T9:344 na FIT ČVUT z roku 2016. Na začiatku je tu zhrnutie histórie vzniku laboratória popisujúce dôvod vytvorenia takejto učebne. Ďalej je popísaná fyzická topológia, ktorá čitateľovi priblíži pre koľkých ľudí učebňa slúži a aké zariadenia sa tu nachádzajú. Nasleduje logická topológia, kde je popísané s akými adresnými rozsahmi sa pracuje a akým spôsobom je učebňa izolovaná od zbytku fakultnej siete.

Ako je uvedené v úvode práce, sieťová učebňa je jednou z búracích učební. Súčasťou kapitoly je popis systému umožňujúci zavádzanie operačných systémov na požiadanie z pohľadu sieťových protokolov.
Posledná sekcia tejto kapitoly sa zaoberá aktuálnymi problémami, ktoré v učebni môžu nastať a čiastočne tak narušujú priebeh výuky. Sú popísané symptómy a dôsledky, ktoré nastanú v prípade výskytu daného problému.

1.1 Historický vývoj učebne

Prvý akreditovaný študijný program na FIT ČVUT, Informatika, platný od roku 2009 do roku 2014 v sebe zahrňoval obor *Informační technologie*. [2] Absolventi tohto oboru boli vystavovaný predmetom zaoberajúcich sa administráciou operačných systémov ale i sietí. Ich uplatnenie by zahrňovalo práve spravovanie serverov, sietí, prípadne ako bezpečnostní analytici.[3] Práve v tejto oblasti je veľmi dôležitá praktická skúsenosť, je nevyhnutné aby si študenti technológie vyskúšali v praxi a simulovali situácie, s ktorými sa môžu vo svojej profesii stretnúť. I toto bolo hnacím motorom vytvorenia laboratória, kde budú mať prístup k sieťovému hardwaru a v roku 2012 došlo k otvoreniu učebne.[1] Cena nových sieťových prvkov v učebni by sa však vyšplhala do desiatok tisíc dolárov, takže v učebni nebol nasadený najnovší hardware. Postačili už použité prvky, ktoré poskytlo Združenie CESNET, či Študentská Únia ČVUT. Pre výukové účely je starší hardware plne postačujúci, keďže rov-

naký operačný systém na týchto prvkoch sa nachádza aj na tých najnovších modeloch a základná funkcionalita je nezmenená.

1.2 Infraštruktúra učebne

1.2.1 Fyzická topológia

V učebni sa nachádza 12 pracovísk, kde jedno súčasne obsluhujú 2 študenti. Sú rozdelené do 4 rád, po 3 pracoviskách. Obaja z dvojice majú k dispozícií stolový počítač s monitorom, ktorý je uložený v rozvádzači. Mimo iné rozvádzač má pripravený i sieťový hardware, od spoločnosti Cisco Systems a to dva prepínače a dva smerovače.

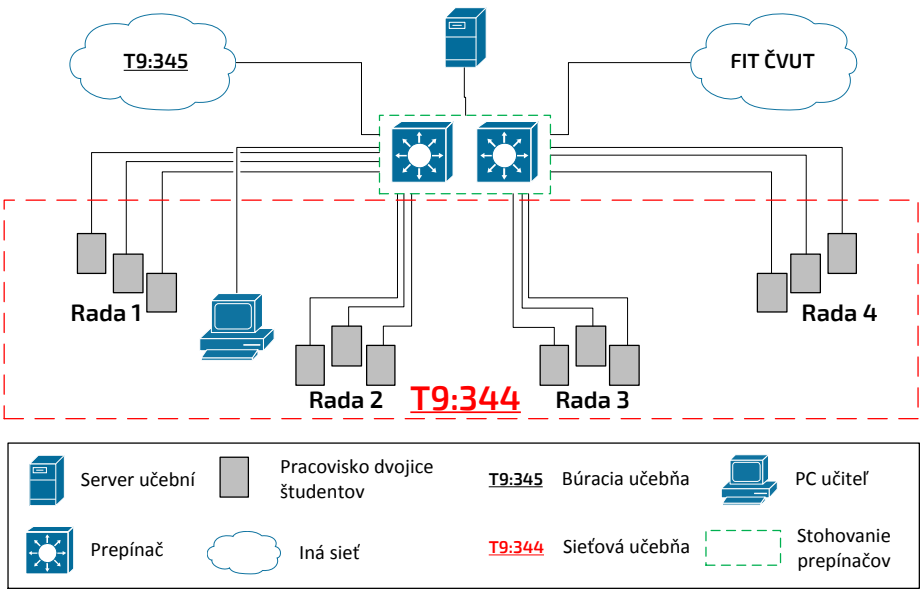
Prepínače[1], vznikli pôvodne z *rozbočovačov*[2], ktorých funkciou bolo prepojenie počítačov v sieti za účelom výmeny dát. Nevýhodou však je, že rozbočovače umožňujú komunikáciu iba jedného zariadenia súčasne. Preto dnes je ich vidieť v sieti iba zriedkavo a nahradili ich práve prepínače, ktoré zvládajú komunikáciu niekoľkých zariadení súčasne a to v oboch smeroch. [4]
Smerovače[3] dokážu toho ešte viac než prepínače. Tieto zariadenia majú vedomosť o cestách do ďalších sietí a slúžia ako prostriedok pre ich prepojenie. Často sa používajú ako *brány*[4] a spájajú tak lokálnu sieť s inou, väčšou, napríklad s Internetom.[4]

Aby bolo prepojenie jednotlivých staníc čo najjednoduchšie, každá stanica má 2 patch panely; pasívne sieťové prvky určené pre ukončenie jednotlivých káblov do panelu s ľahko prístupnými portami. Patch panely v pracovisku majú 24 portov, plne využitých a použiteľných pre študentov. Každý študent má k dispozícií 6 prepojení na ostatné stanice v rovnakej rade. Znamená to, že 12 portov je použitých pre možnosť spolupráce viacerých pracovísk a vytvorenie tak väčšej siete. Ďalších 6 portov je možné využiť pre sériové pripojenie zariadení. Hoci tento spôsob komunikácie so zariadením je už v dnešnej dobe často nahradený pomocou univerzálnej sériovej zbernice (USB), pri sieťovom hardware sa ešte stále stretávame s konzolovým pripojením, realizovaným práve pomocou sériového káblu. Naraz teda počítač dokáže obsluhovať 6 takýchto zariadení. Posledných 6 portov na paneli zaberajú 3 sieťové karty počítača, konzolový port pre prepínač a smerovač a nakoniec pripojenie do Internetu. Celú podobu rozvádzaču pracovnej stanice ilustruje obrázok 1.1. Je v ňom reflektované skutočné usporiadanie zariadení v rozvádzači, kde každé číslo reprezentuje, v ktorom U sa dané zariadenie nachádza. Fyzické pripojenie učebne s fakultnou sieťou sa nachádza na obrázku 1.2. Funkcionalita portov

[1] z angl. switched hubs, prípadne switches
[2] z angl. hub
[3] z angl. router
[4] z angl. gateway

1	Patch Panel 1
2	Patch Panel 2
3 4	PC 1
5	Router 1 (Cisco 2901)
6	Switch 1 (Cisco Catalyst 2960)
7 8	PC 2
9	Router 2 (Cisco 2901 ???)
10	Switch 2 (Cisco Catalyst 2960)
11	Rezerva
12	Nepoužité

Obr. 1.1: Rozvádzač pracovnej stanice v učebni



Obr. 1.2: Fyzická topológia učebne

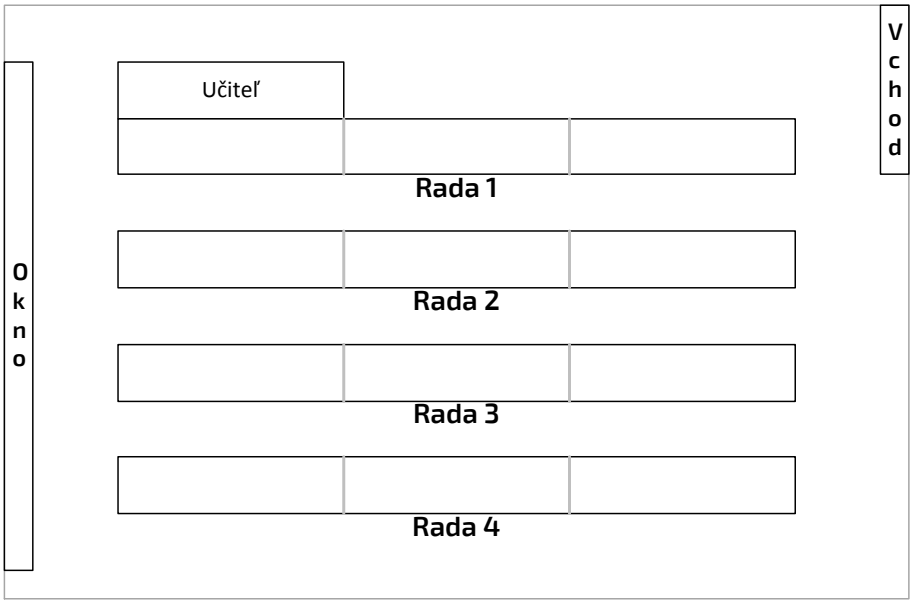
Port	***Účel***
1	Pripojenie do fakultnej siete
2	PC sieťová karta 1
3	PC sieťová karta 2
4	PC sieťová karta 3
5	Konzola smerovač
6	Konzola prepínač
7	PC Konzola 0
8	PC Konzola 1
9	PC Konzola 2
10	PC Konzola 3
11	PC Konzola 4
12	PC Konzola 5
13	Prepojenie s pracoviskom *A*
14	Prepojenie s pracoviskom *A*
15	Prepojenie s pracoviskom *A*
16	Prepojenie s pracoviskom *A*
17	Prepojenie s pracoviskom *A*
18	Prepojenie s pracoviskom *A*
19	Prepojenie s pracoviskom *B*
20	Prepojenie s pracoviskom *B*
21	Prepojenie s pracoviskom *B*
22	Prepojenie s pracoviskom *B*
23	Prepojenie s pracoviskom *B*
24	Prepojenie s pracoviskom *B*

Tabuľka 1.1: Popis portov patch panelu pracovného rozvádzača

patch panelu je zhrnutá v tabuľke 1.1. Pracoviskom A, resp. B, sa rozumie prepojenie k ostatným rozvádzačom v rade. Pozícia je variabilná s polohou práve skúmaného pracoviska. Rozvádzače pri okne učebne majú prepojenie k strednému, resp. krajnému pri vchode do učebne. V strede je to prepojenie k pracovisku pri okne, resp. pri vchode do učebne. Nakoniec, posledné rozvádzače pri dverách sú zrkadlovým obrazom pracovísk pri okne. Pohľad na učebňu a usporiadanie rád je na obrázku 1.3.

O pripojenie do fakultnej siete a Internetu, ktoré sú vyvedené na patch panel sa starajú dva prepínače Cisco Catalyst 3750 s 48 a 24 portami. Dochádza tu k *stohovaniu*[5] prepínačov, teda dva fyzické prepínače sa logicky chovajú ako jeden, čo prináša jednoduchšiu správu aktívneho prvku.[5]

[5]z angl. stacking



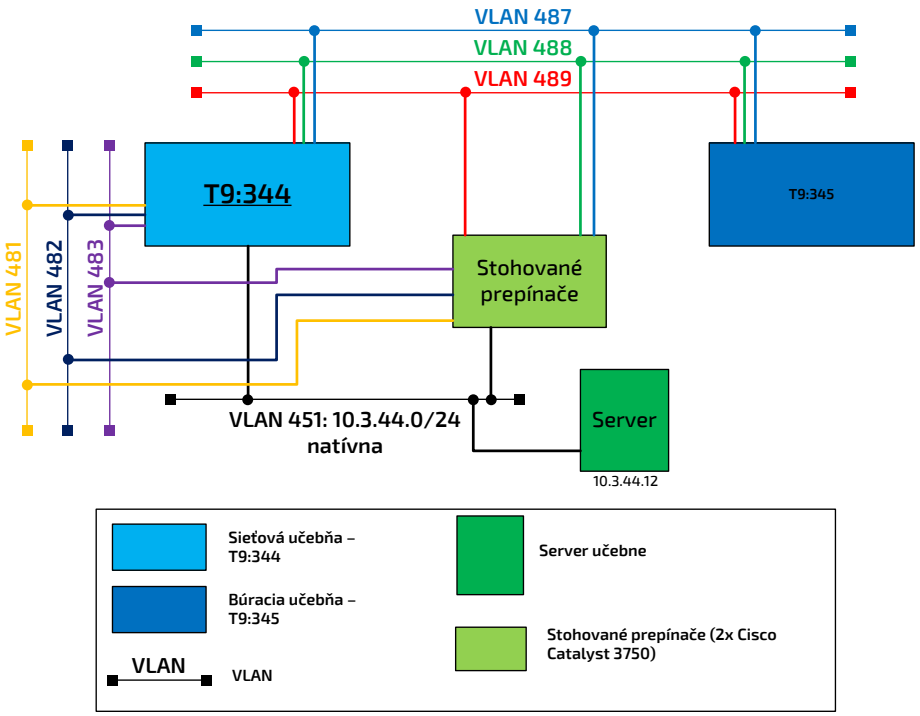
Obr. 1.3: Rozmiestnenie rád v učebni

1.2.2 Logická topológia

Ako autor v úvode práce zmienil, táto učebňa je súčasťou búracích učební. Študenti pracujú s právami superužívateľa a ich činnosť nesmie ovplyvniť produkčnú sieť fakulty. Nejedná sa však o absolútnu izoláciu od zbytku siete. Stále je nutné poskytovať pre stanice pripojenie do Internetu a počítače potrebujú zavádzať operačné systémy, ktoré sú poskytované cez sieť.
Prístup k webovým stránkam na Internete majú iba členovia akademickej obce[6]. To znamená, že stroje, na ktorých pracujú musia identifikovať aktuálneho užívateľa, či sa jedná o študenta, prípadne iného člena akademickej obce. V búracích učebniach sa však nachádzajú modifikované systémy, ktoré nie sú súčasťou produkčnej siete a implementácia overovania priamo do systému by narušila základnú myšlienku týchto systémových obrazov. Nebola by umožnená voľná práca so systémom a študenti by tak nemali plnú kontrolu. K vyriešeniu tejto situácie je nasadený v sieti *proxy server*. Jeho úlohou je overiť a spracovávať požiadavky od užívateľov, komunikovať s externým zdrojom a vrátiť výsledok žiadateľovi. Je teda možné riadiť prístup k webu, kde externí užívatelia nemajú možnosť žiadnej komunikácie, zatiaľ čo prístup členov akademickej obce je kontrolovaný a v prípade problému je identifikácia jednoduchšia.[4] Aby užívatelia neboli zaťažený ručným nastavením proxy ser-

[6]Výnimkou sú hostia počas akcií usporiadaných na pôde fakulty. V týchto prípadoch sa často nachádza v budove verejná bezdrôtová sieť.

veru pri každom spustení systému, automatické objavenie je zaistené pomocou Web Proxy Autodiscovery Protocol (WDAP).[6] Hoci sa nejedná o oficiálny štandard, je implementovaný v mnohých webových prehliadačoch. Systémový obraz používaný počas výuky používa primárne ako webový prehliadač Firefox od spoločnosti Mozilla, ktorý implementuje tento protokol.



Obr. 1.4: Logická topológia učebne - VLAN a podsiete

Pri pohľade na logickú topológiu učebne na obrázku 1.4 existuje prepojenie medzi búracou učebňou a sieťovou učebňou. Obe tieto učebne je možné prepojiť a vytvoriť tak väčšie a komplikovanejšie laboratórne cvičenia. V základe však stanice neznačkujú jednotlivé rámce a tým sú teda tieto učebne oddelené. Počítače sú pripojené v trunkoch, takže v prípade potreby priradenia do inej virtuálnej siete postačí spustenie značkovania rámcov na koncovej stanici. V základnej konfigurácií, však k žiadnemu značkovaniu nedochádza a takéto rámce sa dostávajú do natívnej VLAN, 451. V tejto sieti operuje i server pre zavádzanie systémových obrazov. Zvyšné VLAN, 481 až 483, sú voľne dostupné pre potrebu výuky. Príkladom využitia je jednoduché priradenie pracovných staníc do rôznych podsietí, bez nutnosti fyzického spojenia prepínačov v učebni a definície virtuálnych sietí na týchto prepínačoch. Stačí len spustiť pridávanie 802.1Q hlavičiek do odchádzajúcich rámcov z koncovej

stanice.

Zachytením sieťovej komunikácie v učebni bolo autorom zistené, že pre propagáciu VLAN medzi ostatnými prepínačmi je použitý VLAN Trunking Protocol (VTP). Jedná sa o uzavretý protokol spoločnosti Cisco Systems. Hlavný princíp spočíva v určení VTP Serveru na ktorom sú definované VLAN a klienti alebo servery v rovnakej doméne preberajú po trunk spojeniach informácie o VLAN. Každou zmenou databáze VLAN sa zvýši konfiguračné číslo, vďaka čomu je jasné, ktorá verzia je aktuálna a všetky prepínače so staršou verziou sa synchronizujú s najnovšou. Použitie protokolu však môže byť i nebezpečné. V prípade, že pripojíme do siete prepínač s vyšším konfiguračným číslom a môže nastať situácia, že nastavené VLAN v produkčnej sieti budú zmazané nastavením v novom prepínači.[7] Autor však analýzou zistil, že VTP protokol v učebni je zabezpečený proti tejto situácií. VTP používa pre ochranu heslo, ktoré je použité spolu s názvom VTP domény pre výpočet MD5 hešu.[8] Súčasťou správ je teda i tento heš a v prípade nezhody je žiadosť o aktualizáciu databáza ignorovaná.

O automatické adresovanie počítačov sa stará DHCP server. Počítače vždy dostanú rovnakú IP adresu na základe svojej MAC adresy. Rozsahy použité sú znázornené v tabuľke 1.2.

Zariadenie	**IP adresa**	**Maska podsiete**
Učiteľský počítač	10.3.44.100	255.255.255.0
Študentský počítač 1 – 24	10.3.44.101 – 124	255.255.255.0
Brána	10.3.44.1	255.255.255.0
DNS	10.3.44.12	255.255.255.0
NTP	10.3.44.12	255.255.255.0
WWW Proxy	10.0.1.13	255.255.255.0

Tabuľka 1.2: Adresné schéma sieťovej učebne T9:344

1.3 Zavádzanie systémových obrazov

Hlavná výhoda búracích učební, ako už bolo spomenuté, je flexibilita vo výbere operačného systému pre aktuálnu potrebu výuky. Všetky tieto obrazy sú centrálne uložené na serveri, ktorý obsluhuje práve 2 búracie učebne, T9:345 a sieťovú učebňu T9:344. Tento prístup má radu výhod. Eliminuje duplicity, kde by systémové obrazy boli uchovávané na rôznych strojoch a konzistencia by bola takto ohrozená. Správa obrazov a riadenie prístupu je zjednodušené, keďže je riešené na jednom mieste. Obrazy sú zavádzané cez sieť, nie sú potrebné žiadne inštalačné médiá a tento postup je veľmi dobre škálovateľný aj pre vyšší počet zariadení.

Prostredie, umožňujúce zavádzanie systému z LAN siete sa nazýva *Preboot Execution Enviroment*. Pre integráciu do prostredia siete využíva otvorené

štandardy ako DHCP, TFTP a UDP/IP. Úlohou DHCP serveru v tomto prostredí je poskytnúť klientovi sieťové parametre a IP adresu TFTP serveru, kde sa nachádza zavádzací súbor a príslušné súbory k nemu. Výhodou je, že klient pri žiadosti používa štandardný DHCPDISCOVER paket s PXE parametrami. V prípade, že DHCP server v sieti neposkytuje PXE službu, stále takémuto paketu bude rozumieť a klient dostane IP adresu. Po spracovaní DHCPOFFER paketu od DHCP serveru s podporou PXE, klient si nastaví IP adresu a bude vedieť kde sa nachádzajú zavádzacie súbory, ktoré nahrá do svojej RAM pamäte pomocou TFTP. V momente, keď je zavádzací súbor uložený v RAM, klient môže zaviesť minimalistický systém, ktorého úlohou je nahrať ovládače sieťovej karty a TCP/IP zásobník. Zvyšné inštrukcie nutné pre zavedenie alebo inštaláciu plnohodnotného operačného systému sa už neposielajú pomocou TFTP ale sú využité robustnejšie protokoly ako HTTP alebo NFS.[9]

Keďže v učebni je typické zavádzať všetky počítače súčasne, bolo by veľmi neefektívne aby server poskytoval potrebné súbory pre stanice jednotlivo. Sieťou prechádzajú gigabajty dát operačného systému a jednotlivé počítače požadujú rovnakú množinu dát. Aby sa predošlo duplicitnému rozosielaniu paketov pomocou *unicast*, počítače sa počas zavádzania systémového obrazu pripoja do *multicast* skupiny. Dáta sú týmto spôsobom posielané ako jeden prúd, takže zdrojovú stanicu nezaťažuje zvyšujúci sa počet klientov, žiadajúci o rovnaký obsah.[10].

Autor v samotnom nasadení tohto systému pre zavádzanie obrazov nenašiel problémy, ktoré narušili efektívnu prácu v učebni. Platí však, že nedochádza k overeniu zariadení, ktoré môžu zavádzať pripravené obrazy. Pripojením vlastného zariadenia a povolením sieťového zavádzania systému je možné nainštalovať tieto obrazy aj na súkromné zariadenia nespravované fakultou. V prípade použitia Linux distribúcií sa nejedná o komplikáciu, avšak k dispozícií sú i komerčné operačné systémy ako Oracle Solaris alebo skupina systémov Microsoft Windows. Je preto vhodné overiť, či nainštalovaním takéhoto systému na zariadenie, ktoré nemusí byť nutne použité na edukačné účely nedochádza k porušeniu licenčných podmienok.

1.4 Problémy počas výuky

Prevádzka učebne sa nezaobíde bez problematických miest. Do istej mieri nie je možné eliminovať všetky riziká, ktoré by mohli narušiť výuku. Úplná kontrola nad strojom znamená, že študenti sa môžu chovať i deštrukčne a zhodiť si svoj systém, ak sa budú chovať nerozvážne. Dôsledok však nie je príliš vážny - postačí reštart počítača a nahranie systému nanovo. Ovplyvnený je len študent, ktorý si problémy sám spôsobil a pri dizajne búracích učební ani nebolo cieľom takéto riziko eliminovať. Dôležitejšie je, aby študenti nemohli ovplyvniť ostatných kolegov v práci.

1.4.1 Duplicita IP adries v učebni

Narušenie správneho fungovania siete spôsobí výskyt rovnakých IP adries na dvoch zariadeniach. Je nutné, aby adresy boli unikátne, pretože ostatné aktívne prvky pri komunikácií s takýmito nesprávne nakonfigurovanými zariadeniami nedokážu jednoznačne určite MAC adresu cieľovej stanice. V učebni často dochádza k zmenám IP adries a tieto zmeny sú vykonávané študentami počas výuky, kde sa práve učia o správnej IP adresácií. Ľahko sa preto stane, že použijú adresu počítača kolegy. Operačný systém Windows na túto skutočnosť užívateľa upozorní. Pri výuke sa však používa linuxová distribúcia Ubuntu, ktorá žiadnu takúto detekciu nemá a naďalej sa systém tvári, že všetko je v poriadku. Rovnako táto detekcia sa nenachádza ani na prepínačoch a smerovačoch. Tieto systémy predpokladajú, že užívateľ, ktorý manuálne nastaví IP adresu si sám skontroluje, či ju už niekto iný nepoužíva. V prípade dynamického získania IP adresy sa systém spolieha na správne nastavenie služby poskytujúcej informáciu o adresácií a ďalšie kontroly nerobí. Je zrejmé, že tento scenár môže nastať počas výuky veľmi jednoducho. Vážnejšie problémy však nastanú, ak užívateľ použije adresu brány alebo serveru, ktorý poskytuje systémové obrazy pre nahrávanie. Pri ARP žiadosti o MAC adresu serveru, totižto odpovedia obe stanice - server i študentom nastavené zariadenie s rovnakou IP adresou. Keďže žiadateľ vezme prvú odpoveď ako správnu, stáva sa, že prvá odpoveď je od študentovho zariadenia, pretože sa nachádza v topológií siete bližšie k žiadateľovi. Ten sa preto nedostáva k službám, ktoré očakáva na danej IP adrese.

1.4.2 Konfiguračné problémy v systémovom obraze

Po zavedení systému a prihlásení sú od užívateľa vyžadované ďalšie kroky k plnohodnotnému používaniu systému. Systémový obraz po štarte totižto nežiada automaticky DHCP server o IP adresu a počítač zostáva nepripojený. Aktuálne doporučené riešenie, nachádzajúce sa v príručke používania, je manuálne spustenie DHCP klienta na rozhraní s pripojením do fakultnej siete. Tento krok však nie je nutný a dá sa automatizovať a to jednoduchou zmenou konfigurácie sieťových rozhraní v systéme. Po tejto zmene užívateľ získa IP adresu a otvorenie webového prehliadača, čo je jeden z prvých krokov po spustení, bude užívateľ požiadaný o prihlásenie k proxy serveru, ktorý bol popísaný v sekcii 1.2.2.

1.4.3 Bezpečnostné problémy v sieti

Vnútorná sieť laboratória je každou vyučovacou hodinou iná a nie je ani žiadúce implementovať vyššie zabezpečenie tejto siete. Prinieslo by to komplexnosť a keďže sa študenti učia chovaniu počítačových sietí, nie je nutné ich pri spoznávaní sietí zaťažovať pokročilou bezpečnosťou, ktorá je bežnou súčasťou produkčných sietí. Bezpečnostné riziko však predstavuje práve hranica medzi

produkčnou sieťou a učebňou.
Topológia na obrázku 1.2 ukazuje priame spojenia z produkčného prepínaču do učebne. Sú zakončené na patch panely každého pracovného rozvádzaču a primárne poskytujú pripojenie k fakultnej sieti a Internetu. Odpočúvaním komunikácie na pripojení autor zistil, že informácie vysielané z produkčného prepínaču nie sú určené do takéhoto nechráneného a premenlivého prostredia učebne.
Jeden z nedostatkov je vysielanie rámcov CDP, teda Cisco Discovery Protocol. Jedná sa o protokol druhej vrstvy ISO/OSI modelu vyvinutý pre zariadenia spoločnosti Cisco Systems. Jeho úlohou je zjednodušenie správy ostatných Cisco zariadení a to tým, že ich dokáže objaviť a čiastočne zistiť ich konfiguráciu [11]. Svoje uplatnenie nájde pre správcov a pomáha pri dokumentácií siete, kde z jednotlivých zariadení sa ľahko dajú objaviť priamo pripojený susedia. Keďže sa jedná o proprietárny protokol, IEEE štandardizovala Link Layer Discovery Protocol (LLDP), ktorý má podobnú funkcionalitu ako CDP.[12].
Informácie, poskytované týmito protokolmi sú iste užitočné, avšak nepatria užívateľom. Odpočúvaním komunikácie je veľmi jednoduché pre útočníka zistiť aká verzia systému sa nachádza na prepínači, akým portom je k nemu pripojený a i tieto informácie môžu byť použité k útoku. Je snahou poskytovať verejne čo najmenej informácií o sieti a preto je vhodné vypnúť CDP na rozhraniach, kde sú pripojené cudzie zariadenia.

Kapitola 2

Návrh novej učebne

Pri návrhu novej učebne je nutné uvedomiť si, že sa jedná o špecifický druh siete. Používatelia sú študenti s rôznou úrovňou znalostí počítačových sietí, od úplných začiatočníkov až po pokročilých. Laboratórium by malo slúžiť pre všetky tieto skupiny používateľov.
Sieťová učebňa môže byť vytvorená niekoľkými spôsobmi ako napríklad:

- Simulácia sieťového prostredia
- Virtualizované prostredie
- Fyzická infraštruktúra

Simulácia sieťového prostredia sa používa najmä vtedy, ak by bolo vytvorenie požadovanej topológie príliš drahé a náročné. Preto sa použije softwér, v ktorom definujeme topológiu a príslušné chovanie v sieti môžeme pozorovať priamo v softwari. Príkladom takéhoto simulačného softwaru je psimulator2[13] vyvíjaný na FIT ČVUT alebo populárny ns-3[14], či GNS3[15].
Virtualizované prostredie je postavené na použití virtuálnych strojov. Vďaka nim dokážeme spustiť mnoho inštancií serverov, klientov ale i sieťových prvkov na jednom fyzickom počítači. Software ako VMware vSphere[16] umožňuje vytvorenie veľkej množiny serverov, sieťových prvkov alebo klientov s použitím malého množstva fyzických systémov. Zároveň je jednoduché obnoviť nastavenie strojov do východzieho stavu po ukončení práce v laboratóriu, vďaka možnosti použiť snapshot strojov, teda snímok systému v čase, ktorý uchováva kompletný stav stroja.
Fyzická infraštruktúra používa reálne zariadenia pre vytvorenie prostredia na výuku. Táto možnosť má blízko k podmienkam z praxe, pretože študenti pracujú so skutočným sieťovým hardwarom. Nasadenie tohto modelu môže byť centralizované alebo distribuované. Pri možnosti centralizovaného nasadenia má laboratórium jedno centrálne miesto kde sa nachádzajú všetky aktívne prvky. Pri distribuovanom nasadení je laboratórium rozdelené do menších pracovných staníc, ktoré majú dostatok hardwaru na základné sieťové topológie.

Pre vytvorenie komplexnejších scenérií sa tieto pracovné stanice prepoja medzi sebou.[17]

2.1 Ideálna učebňa

Pre ideálnu učebňu som sa rozhodol implementovať distribuovaný model fyzickej infraštruktúry. Táto voľba je finančne najnáročnejšia, avšak poskytuje komfort pre užívateľov laboratória. Učebňa slúži pre 24 študentov a jedného učiteľa. Pri komplexných sieťach sa predpokladá spolupráca tímov študentov, kde každý má na starosť inú časť siete. Je pripravená i na vzdialenú prácu, takže po príprave fyzickej infraštruktúry je možné pracovať i na diaľku cez Internet. Počas výuky môže učiteľ pomocou správcovského počítaču ovládať všetky aktívne zariadenia v učebni, či už sa jedná o počítače alebo sieťové prvky. Využíva sa i virtuálna infraštruktúra, kde sú pred-pripravené systémy so sieťovými službami. Študent alebo učiteľ tak môže pripojiť server do laboratória už s pripravenou sieťovou službou, bez toho aby sa musel zdržiavať inštaláciou a konfiguráciou danej služby na svojom stroji.

2.1.1 Hardwarové vybavenie učebne

Fyzická vrstva zahrňuje všetku výpočtovú techniku v učebni spolu s prepojením jednotlivých komponentov. Patria sem teda hardwarové zariadenia ako sú pracovné stanice študentov, servery, smerovače, prepínače a iný sieťový hardware. Prepojenie zariadení zabezpečuje štrukturovaná kabeláž a v učebni sú tiež pripravené ďalšie sieťové káble, ktoré slúžia na vytvorenie topológii potrebných pre výuku.
V učebni sa nachádzajú dva druhy 19 palcových rozvádzačov, kde je uložená výpočtová technika. *Dátový rozvádzač* alebo tiež rack je definovaný ako *„systém pre prehľadnú montáž a prepojenie rôznych elektronických zariadení spolu s vyústením káblových rozvodov do stĺpcov nad sebou v oceľovom ráme.“*[18, str. 1]. Výrobcovia hardwaru často označujú veľkosť svojich zariadených určených do rozvádzačov pomocou *rack jednotiek*[7]. Rack unit (označovaná ako *RU* prípadne *U*) je skupina troch otvorov v konštrukcii racku, určených na uchytenie zariadenia. Podľa normy EIA-310 je výška RU 44,45 mm. Bežný rozvádzač v dátovom centre má veľkosť 42U a viac, čo stačí pre zariadenia približne do výšky 1,8 m.[19]

Centrálny rozvádzač tvorí jadro infraštruktúry učebne. Jedná sa o štandardný rozvádzač veľkosti 42U. Z tohto miesta je riadená distribúcia elektrickej energie k jednotlivým pracovným staniciam. Združuje všetky dátové

[7] z angl. rack unit

pripojenia na jedno miesto a preto je možné jednoducho prepojiť študentské pracoviská medzi sebou. Nachádza sa tu i vyhradená sieť pre správu sieťových prvkov v učebni. Nechýba tu ani server, na ktorom majú študenti možnosť vytvoriť si vlastné virtuálne stroje vhodné pre ich topológiu.

Pracovná stanica je miesto pre dvojicu študentov. Pozostáva z *pracovného rozvádzaču*, kde sa nachádzajú všetky zariadenia pre oboch študentov. Tento rozvádzač je inštalovaný pod stolom o veľkosti 15U. Študent sa však o vybavenie deliť nemusí, pretože v rozvádzači sa nachádzajú vždy dvojice rovnakých zariadení. K dispozícií má preto každý študent všetky druhy sieťových prvkov v učebni. Celkový počet pracovných staníc je 12, čo stačí pre plnohodnotnú prácu 24 študentov súčasne.

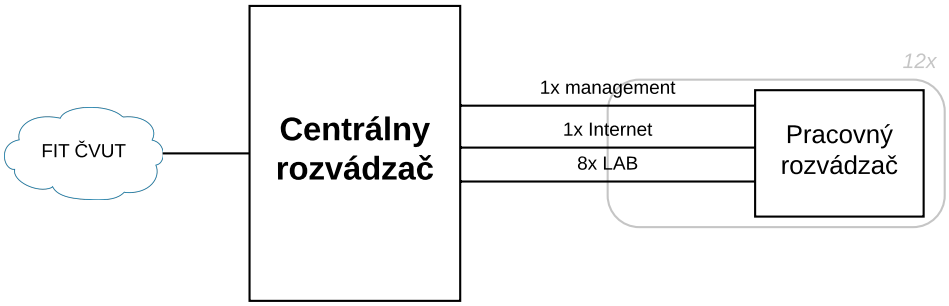
2.1.1.1 Pracovný rozvádzač

Pracovný rozvádzač je miesto, kde sa bude študent počas výuky zdržiavať a primárne bude pracovať so zariadeniami v tomto rozvádzači. Od tohto rozvádzača je vyžadované:

- Všetky aktívne zariadenia rozvádzaču sú v páre.
- Pohodlný prístup k všetkým sieťovým rozhraniam na zariadeniach.
- Rozvádzač je nutné uložiť pod stolom, výška je preto obmedzená.
- Pripojenie do centrálneho rozvádzaču.

Hlavným obmedzením je maximálna výška pracovného rozvádzaču. Doporučená výška pre pracovnú dosku stola je 70 cm nad podlahou[20] a vhodnou konštrukciou dosiahneme maximálny rozmer 15U, reálne však je možné počítať s 11U. Použité sú aktívne sieťové prvky s rozmerom 1U a počítače pre študentov sú v rozmere 2U. Tento kompaktný rozmer dodáva dostatočný priestor pre všetky zariadenia oboch študentov.

Práca študentov zahrňuje aj vytváranie fyzických topológii, preto je nutné aby mali ľahko dostupné všetky potrebné sieťové rozhrania. Väčšina aktívnych sieťových prvkov má práve na prednej strane všetky rozhrania, takže prístup je bezproblémový. Počítače, ktoré sú tiež súčasťou rozvádzača však na toto nie sú prispôsobené a rozhrania majú na zadnej strane. Tento problém je riešený pomocou pasívneho sieťového prvku *patch panel*. Je rozmeru 1U a je vybavený 24 portami, na ktoré je možné pripojiť sieťové rozhrania. Týmto je zabezpečený pohodlný prístup aj pre počítače a iné sieťové prvky, ktoré majú prístup k rozhraniam . Porty patch panelu sú využité i pre prepojenie pracovného rozvádzača s centrálnym. Každá pracovná stanica má 8 nezávislých pripojení do centrálneho rozvádzaču. Dvojica portov patch panelu je použitá pre pripojenie do vonkajšej siete a ďalšia dvojica je priame spojenie do správcovskej siete. Pohľad na prepojenie medzi centrálnym a pracovným rozvádzačom je na obrázku 2.1



Obr. 2.1: Prepojenie centrálneho a pracovných rozvádzačov

2.1.1.2 Centrálny rozvádzač

Pri návrhu bolo potrebné vziať do úvahy, aké všetky funkcie sú očakávané. Ciele, ktoré má tento rozvádzač splniť sú:

- Centralizované miesto pre všetky dátové pripojenia v učebni
- Prístupný počas výuky s možnosťou zmeny zapojenia
- Dostatočné množstvo portov pre zapojenie všetkých zariadení i s možným rozšírením v budúcnosti
- Prehľadné uloženie kabeláže.
- Miesto pre distribúciu elektrickej energie do pracovných staníc.
- Centrálny bod pre konfiguráciu všetkých aktívnych prvkov v učebni.

Do centrálneho rozvádzaču ústia pripojenia zo všetkých pracovných staníc a rovnako poskytuje hranicu medzi sieťou laboratória a zvyškom siete budovy. Výhodou centralizovanej topológie je jednoduché pripojenie ďalších uzlov do siete. Všetky dátové toky, ktorých cieľom je iná pracovná stanica musia prechádzať cez centrálny prvok. Takto je pre prepojenie jednej pracovnej stanice s ostatnými nutné použiť iba jeden kábel. Tento model siete je často pri návrhu používaný a označuje sa tiež ako *hviezdicová topológia*.[21]
Keďže sa všetky pripojenia zhlukujú do jedného bodu, počet zariadení v tomto rozvádzači nie je zanedbateľný. Použitie rozvádzača vo veľkosti 42U však poskytuje dostatočný priestor i v prípade, že bude nutné pridávať ďalšie zariadenia v budúcnosti. Model si však nesie so sebou i nevýhodu. V prípade zlyhania alebo výpadku zariadenia v centrálnom rozvádzači sú ovplyvnené všetky pripojené pracovné stanice v laboratóriu. Ak sa jedná o kritické aplikácie, tento nedostatok je často riešený pomocou *redundancie*. Spočíva v replikácií sieťových zariadení za účelom vytvorenia tolerancie voči výpadku. V prípade výpadku, dochádza k automatickému nahradeniu nefunkčného zariadenia.[22]

Sieťové laboratórium však nie je až tak kriticky dôležité aby bežalo v režime 24/7 a výpadok po dobu fyzickej výmeny zariadenia je tolerovaný. Preto v tomto návrhu sa s redundanciou prvkov sa nepočíta.

Rozvádzače sú z pravidla uzavreté zámkom. Je žiadúce aby do rozvádzača mali prístup iba povolené osoby, aby nedošlo k náhodnej alebo cielenej manipulácií so zapojením. Sieťové laboratórium je však výnimkou. Prepojenie sa často mení podľa potreby výuky a udržiavať rozvádzač uzamknutý je nepraktické. Naopak, návrh učebne predpokladá otvorený prístup do rozvádzača, pretože pre prepojenie pracovných staníc je nutné aby študenti sami zapojili potrebné rozhrania. Centrálne miesto pre prepájanie staníc v učebni vedie k vyhnutiu sa situácie s dlhými káblami vedúcich cez celú miestnosť až k jednotlivým staniciam.
Združuje sa tu však aj podporná infraštruktúra učebne, s ktorou nesmie byť manipulované. Je nutné udržiavať jej stav, pretože narušenie by viedlo k obmedzeniu alebo až vyradeniu služieb v laboratóriu ako vzdialené pripojenie do učebne, konzolový prístup na sieťové prvky, či spojenie so zvyškom infraštruktúry budovy. Riešením by bolo fyzicky oddeliť túto časť siete do druhého, uzamknutého rozvádzača. Toto však pridá do návrhu zložitosť a rozštiepilo by centralizovaný model na dva menšie centrálne rozvádzače. Z pracovných staníc by sa museli riešiť dve fyzické trasy, jedna pre prepojenie pracovných staníc a druhá pre poskytovanie služieb v učebni. Tento návrh však fyzické zabezpečenie neimplementuje. Časť infraštruktúry, ktorá nesmie byť zmenená, používa farebne odlíšené káble a užívatelia laboratória sú informovaní o tom, že do tejto časti nemajú zasahovať. Prístup do učebne je obmedzený a možný iba v sprievode vyučujúceho, táto úroveň zabezpečenie je teda dostatočná.

Pri výbere zariadení, je dôležité počítať s rozmermi a voľným miestom v rozvádzači. Je rozumné predpokladať, že môže dôjsť k výmene strojov vo väčších rozmeroch, pridaním čiastočnej redundancie kritických zariadení v infraštruktúre. Užívateľom laboratória sa snaží byť poskytnutý čo najväčší komfort pri práci a pretože majú k dispozícií až osem liniek do rozvádzača, požiadavky na počet portov nie sú zanedbateľné. Výrobcovia sieťového hardwaru našťastie s týmito požiadavkami počítajú a pri zachovaní kompaktného rozmeru 1U dokážu v prepínači poskytnúť až 48 rozhraní pre klientov. Aby sa prepínače mohli prepojiť i s ďalšími prepínačmi, bez straty rozhraní pre užívateľov, sú vybavené ešte dvomi až štyrmi rozhraniami, určené práve na tento účel. V centrálnom rozvádzači je snahou využiť čo najviac rozhraní pri zachovaní minimálnych rozmerov, preto sú použité prepínače a patch panely so 48 portami.

S vysokým množstvom rozhraní, ktoré môžu užívatelia využiť, sa kabeláž v centrálnom rozvádzači bez organizácie stáva veľmi chaotickou. Manipulácia a zmena prepojení je náročná a nepohodlná, čo je v prípade sieťového

laboratória, kde sa očakáva častá zmena topológie, neprijateľné. Preto všetky rozhrania na patch panely používajú identifikátor, ktorý je totožný s identifikátorom na druhej strane prepojenia. Je viditeľne umiestnený nad každým rozhraním a užívateľ na prvý pohľad vie, kam vedie dané rozhranie. Vyplnením všetkých portov patch panelu však dostávame bez ďalšieho usporiadanie rovnako chaotický stav. Preto je ešte rozvádzač vybavený *organizérmi* ako horizontálnymi tak i vertikálnymi. Do tohto príslušenstva sa ukladá kábel a v kombinácií s vertikálnymi organizérmi je možné viesť celú trasu od jedného rozhrania k druhému bez toho, aby sa krížila cesta naprieč rozvádzačom. Pri vyššom počte káblov však dochádza k zaplneniu organizéru a manipulácia je nepohodlná. Využité su hlavne pri prepojeniach v časti rozvádzača kde sa nepredpokladá častá zmena prepojení, teda v podpornej infraštruktúre laboratória.

Pre zvýšenie miery orientácie v rozvádzači a to najmä, keď spolupracuje viac skupín, je vhodné farebne odlíšiť káble. Každá pracovná stanica má priradenú farbu káblu a len tieto káble môže použiť v centrálnom rozvádzači na prepojenie s ďalšou skupinou. Na prvý pohľad je takto možné učiteľom i študentami rozlíšiť, ktorá pracovná stanice je pripojená kde a veľmi rýchlo tak odhalia prípadnú chybu v zapojení. Pre podpornú infraštruktúru je rovnako použitá iná farba, ktorá dá jasne najavo užívateľom, že s týmito prepojeniami nesmú manipulovať.

V rozvádzači však nemusia byť centralizované len dátové pripojenia. Z jedného miesta je distribuovaná i elektrická energia pre pracovné stanice. Z centrálneho rozvádzača je do každej pracovnej stanice vyvedená dvojica elektrických káblov, ktoré sú zakončené viacnásobnou zásuvkou s ôsmimi zásuvkami pre zariadenia. Tieto zásuvky sú osadené zo zadnej strany v rozvádzači pracovnej stanice. Jedna viacnásobná zásuvka dodáva napájanie pre každý typ zariadenia v pracovnom rozvádzači. Znamená to, že zapnutím jednej zásuvky sú pre študenta spustené všetky jeho zariadenia. V centrálnom rozvádzači sú použité manažovateľné PDU[8], do ktorých sú zapojené jednotlivé viacnásobné zásuvky z pracovných rozvádzačov. Výhodu, ktorú manažovateľné PDU dáva, je možnosť ovládať napájanie zásuviek a to i na diaľku pomocou pripojenia cez IP. Táto funkcionalita je kľúčová pre vzdialený prístup do laboratória, pretože je možné zapnúť zariadenia v učebni, ktoré sú potrebné bez fyzickej prítomnosti v učebni. Rovnako to pomôže učiteľovi pri príprave staníc pred výukou, keď ich dokáže spustiť z jedného miesta a nemusí tak v učebni prechádzať stanice a zapínať ich manuálne.

Posledný cieľ, ktorý je žiadaný od rozvádzaču je poskytnúť priestor pre centrálnu konfiguráciu prvkov. Na počítače ale i sieťové prvky sa pre pripoje-

[8]Power Distribution Unit

nie v bežnom režime použije IP a užívateľ sa dostáva či už do riadkového alebo grafického režimu pre ovládanie zariadenia. V prípade, že protokol IP je chybne konfigurovaný alebo nie je vôbec spustený, je možné použiť sériové pripojenie na konzolu zariadenia. Tento prístup sa nazýva *out-of-band*, čo znamená, že pre daný prvok je dedikovaný kanál pre správu.[23] Bežne sa používa pri prvej konfigurácií, kde vo výrobnom nastavení nenájdeme žiadnu konfiguráciu IP. V sieťovom laboratóriu táto situácia nastáva veľmi často, keďže z pravidla po výuke dochádza k obnove výrobných nastavení na sieťových prvkoch. Nevýhodou sériového pripojenia je, že vyžaduje fyzický prístup k zariadeniu a to pri konfigurácií väčšieho množstva zariadení alebo pri nutnosti nastavenia vzdialene je problém.
Riešenie poskytuje *terminálový server*. Toto zariadenia má porty pripravené pre sériovú linku a samé o sebe má tiež LAN rozhranie na ktoré je možné sa pripojiť.[23] Pre zachovanie out-of-band prístupu sú terminálové servery vybavené záložným pripojením k Internetu, v prípade, žeby LAN sieť zlyhala a je nutné mať k zariadeniam prístup. V laboratóriu budú užívatelia k sieťovým prvkom pristupovať práve pomocou terminálového serveru, čo umožní konfigurovať všetky zariadenia v učebni z jedného miesta i keď sa nachádzajú vo výrobnom nastavení a nemajú nakonfigurovaný IP.

2.1.1.3 Potrebné aktívne prvky pre učebňu

Pri výbere hardwaru je cieľom pokryť čo najväčšie množstvo technológií pre študentov na vyskúšanie v laboratóriu. Naďalej sa udržiava koncept učebne ako Cisco laboratória, preto väčšina sieťových prvkov je práve od spoločnosti Cisco Systems. Pracovné stanice by mali byť dostatočné pre vytvorenie malých, jednoduchých topológií, preto budú obsahovať:

- 2 počítače s tromi sieťovými kartami
- 2 smerovače s rozhraním pre sériovú linku (napr. Cisco 2901 ISR)
- 2 viacvrstvové prepínače[9] rozmeru 1U s možnosťou PoE na rozhraniach (napr. Cisco Catalyst 3560)
- 2 bezpečnostné smerovače (napr. Cisco ASA 5505)
- 1 patch panel s 24 portami
- 2 viacnásobné zásuvky s ôsmimi zásuvkami

Voľba sieťových prvkov do centrálneho rozvádzaču bolo hlavným kritérium vysoká hustota portov pri čo najkompaktnejších rozmeroch. Preto všetky prvky v rozvádzači majú rozmer 1U. Nutný hardware pre centrálny rozbočovač:

[9] z angl. multi-layer switch

- 3 48-portové terminálové servery
- 3 48-portové viacvrstvové prepínače
- 1 48-portový prepínač
- 6 patch panelov so 48 portami
- 5 manažovateľných PDU s ôsmimi vzdialene kontrolovanými výstupmi elektrickej energie
- 12 horizontálnych organizérov
- 2 vertikálne organizéry
- 1 server pre potreby virtualizácie

Vytvorenie jednoduchých topológii, ktoré demonštrujú základy sietí ako komunikáciu medzi dvomi zariadeniami, ukážku adresovania a zapúzdrenia nevyžaduje veľké množstvo hardwaru. Na všetky tieto procesy stačí užívateľovi priradený hardware v pracovnej stanici. K dispozícií má smerovač i prepínač, čo stačí ako na prácu v rámci jednej pracovnej stanice tak i na spoluprácu s ostatnými študentami, kde tento hardware bude zaobstarávať funkciu prepojenia jednotlivých staníc.

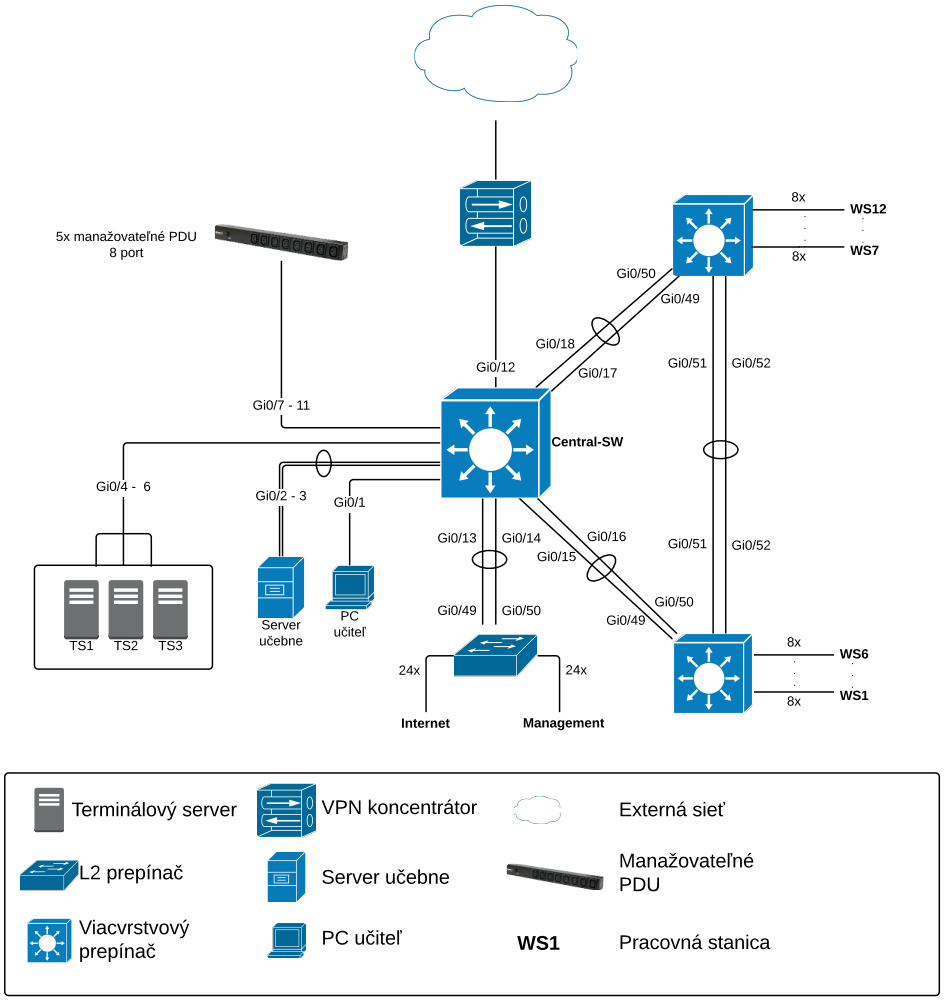
2.1.1.4 Topológia siete - fyzická

V nasledujúcej časti práce sa nachádzajú schémy fyzickej topológie siete. Tieto schéma definujú fyzické zapojenie prvkov v sieti i usporiadanie v dátových rozvádzačoch. Každá počítačová sieť by mala mať takéto schémy ako súčasť dokumentácie. V budúcnosti sa pri zmenách môže použiť ako referencia práve topológia a uľahčuje tak sieťovým inžinierom orientáciu v komplexnej sieti. Jedná sa samozrejme o živý dokument, čo znamená, že každá zmena musí byť zaznamenaná a schéma musí byť aktualizované aby boli v prípade potreby relevantné.

Nie je cieľom zahrnúť všetky informácia do jedného veľkého obrázku. Takéto schéma je nabité informáciami, avšak vo veľmi neprehľadnej forme. I pre samotného autora sa s odstupom času môže zdať nepochopiteľné a takýto dokument sa stáva nepoužiteľný. V práci je preto celá fyzická topológia rozdelená do niekoľkých schém:

- Fyzické zapojenie - centrálny dátový rozvádzač (obr. 2.2)
- Fyzické zapojenie - pracovná stanica (obr. 2.3)
- Uloženie prvkov v dátovom rozvádzači - centrálny dátový rozvádzač (obr. 2.4)

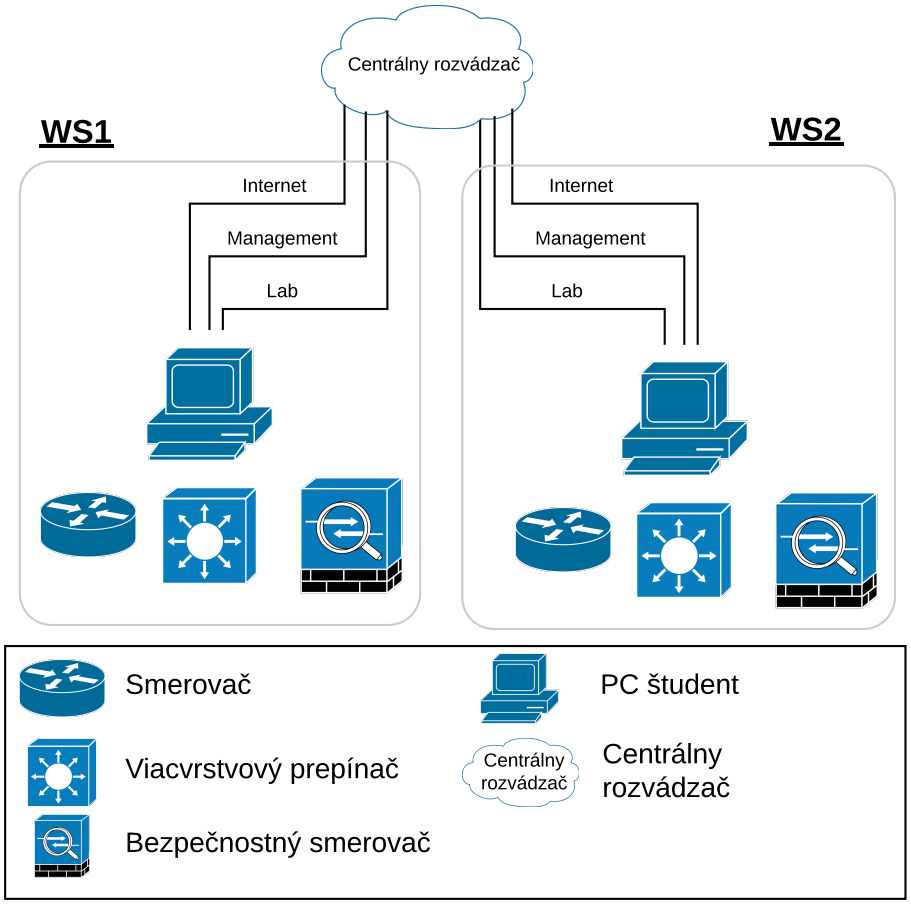
- Uloženie prvkov v dátovom rozvádzači - pracovná stanica (obr. 2.5)



Obr. 2.2: Fyzické zapojenie - centrálny dátový rozvádzač

Obrázok 2.2 ukazuje zapojenie učebne do fakultnej siete a poskytuje pohľad na prepojenie jednotlivých prepínačov v centrálnom dátovom rozvádzači. Prvý prepínač tvorí hlavný stred hviezdy, kde sa nachádzajú najdôležitejšie služby ako pripojenie do Internetu, terminálové servery a inteligentné PDU pre distribúciu elektrickej energie. Je použitých niekoľko fyzických spojení k ostatným prepínačom, ktoré poskytujú pripojenie pracovným staniciam.

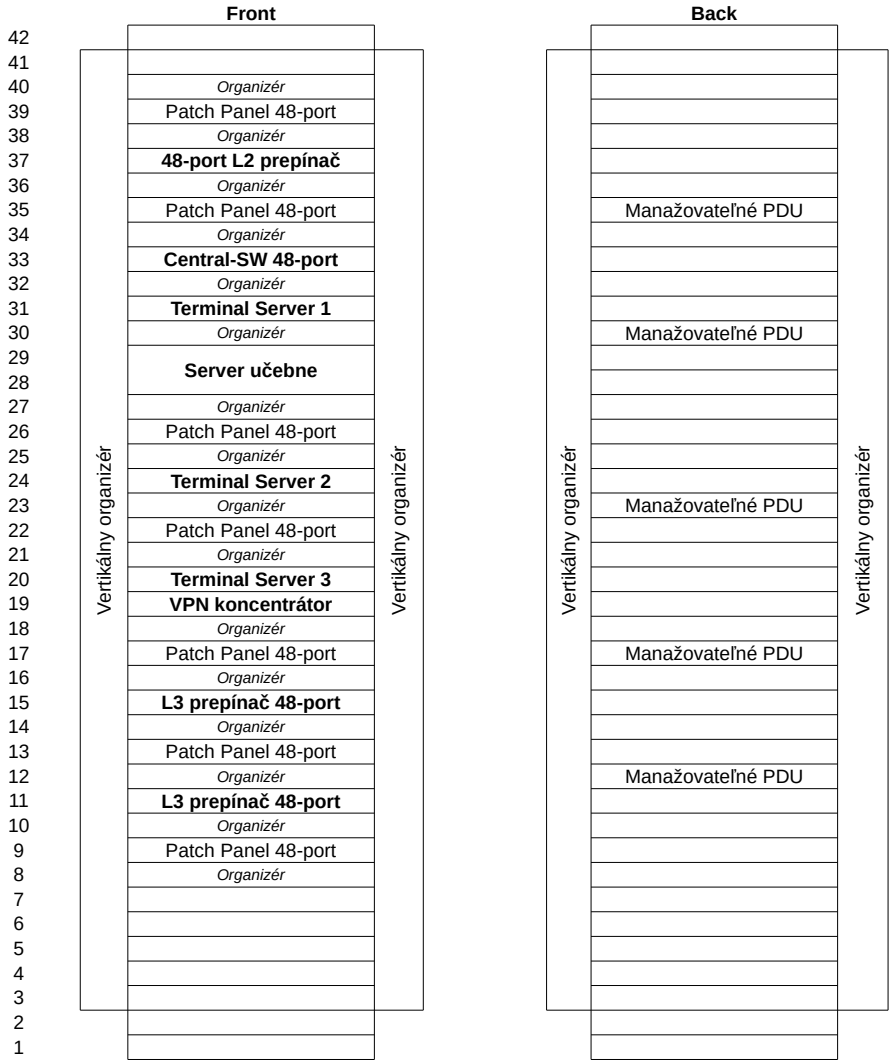
Zapojenie pracovných staníc zobrazené na obrázku 2.3 tvorí omnoho menej prepojení ako to bolo pri 2.2. Na prvý pohľad je očividné, že sieťové prvky nie sú vôbec zapojené do zvyšku siete a zostávajú v sieti iba počítače. To je však



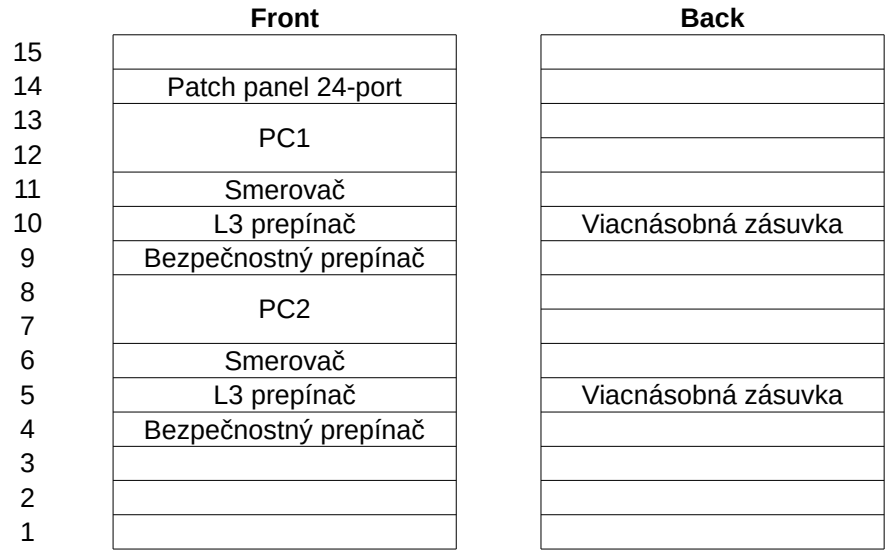
Obr. 2.3: Fyzické zapojenie - pracovná stanica

zámer, pretože jednotlivé zariadenia budú pripájať práve užívatelia laboratória v závislosti na ich potrebách.

Na obrázkoch 2.4 a 2.5 je zobrazenie skutočné uloženie prvkov v dátovom rozvádzači a to ako pre centrálny rozvádzač tak i pre pracovnú stanicu. Obrázky tiež popisujú celkovú výšku v rack jednotkách U. Pri centrálnom rozvádzači mnoho pozícií vyplnili práve organizéri. Pri 48-portových patch paneloch sú vždy po skupinách *organizér-patch panel-organizér* aby pre všetky káble bolo dostatok miesta na uloženie. Za zdôraznenie stojí i pohľad zo zadu rozvádzača pracovnej stanice, kde sa nachádzajú viacnásobné zásuvky, slúžiace pre celú pracovnú stanicu.



Obr. 2.4: Uloženie prvkov v dátovom rozvádzači - centrálny dátový rozvádzač



Obr. 2.5: Uloženie prvkov v dátovom rozvádzači - pracovná stanica

2.1.2 Logická vrstva

V tejto časti práce sú popísané sieťové protokoly, ktoré sú v ideálnej učebni využívané. Nezaoberá sa zapojením jednotlivých káblov v rozhraniach ale naopak sa zaoberá tým, aké dáta prechádzajú týmito káblami. Táto sekcia rozoberá protokoly na linkovej vrstve, adresnú schému sieťovej vrstvy a i aplikačné protokoly, ktoré poskytujú sieťové služby. Patrí sem i problematikou bezpečného vzdialeného prístupu do laboratória.

2.1.2.1 Topológia siete - linková vrstva

Pohľad na sieť z perspektívy linkovej vrstvy zahrňuje VLAN[10], riešenie cyklických zapojení v topológií pomocou protokolu STP[11] a zvýšenie priepustnosti agregáciou fyzický liniek na jedno logické rozhranie.

Virtuálna LAN je, ako už z názvu vyplýva, softwarové rozdelenie fyzickej LAN siete na niekoľko logických sietí. Tieto siete sa chovajú úplne rovnako ako fyzicky oddelené LAN siete.[4] Zariadenia v rôznych VLAN sú si navzájom nedostupné bez použitia smerovaču a to i v tom prípade, že sú pripojené na jednom prepínači.

Rozdelenie siete do niekoľkých virtuálnych prináša radu výhod. Keďže zariadenia medzi sebou nemôžu komunikovať na linkovej vrstve, nachádzajú sa v nezávislých skupinách. Toto rozdelenie môže byť napríklad podľa oddelenia

[10] Virtual LAN
[11] Spanning Tree Protocol

vo firme alebo určenia zariadenia. V tomto návrhu sa používajú štyri virtuálne siete. Jedna pre pripojenie do infraštruktúry fakulty, ďalšia je vyhradená pre správu prvkov a prístup ku konzolám a samotná sieť použitá pre laboratórium, teda prepojenie jednotlivých pracovných staníc. Posledná virtuálna sieť plní rolu „čiernej diery“, teda dostávajú sa sem neštandardné dátové toky, ktoré by sa nemali objaviť v bežnej prevádzke. Je dôležité poznamenať, že vo väčšine prípadov koncové zariadenia nemajú o virtuálnych LAN sieťach žiadnu informáciu. Celý proces rieši prepínač, ktorý má niekoľko oddelených tabuliek MAC adries[12]. Pre bezproblémové fungovanie na koncových staniciach je však nutné, aby port na prepínači patril práve do jednej VLAN. Návrh však počíta s tým, že učiteľ má prístup do niekoľkých VLAN súčasne a že i server dokáže mať pripojenie do fakultnej siete a zároveň poskytuje služby sieti laboratória a to všetko s použitím jedného fyzického rozhrania.
Prepínače od spoločnosti Cisco Systems riešia tento problém pomocou *trunk rozhraní*. Jedná sa o prepojenia bod-bod a sú schopné prenosu niekoľkých VLAN cez jedno prepojenie, čo pre prístupové porty nie je možné. Pre identifikáciu, ktorý rámec patrí do ktorej VLAN je možné použiť napríklad *značkovanie* podľa štandardu IEEE 802.1Q. Prepínač na tieto rozhrania posiela špeciálne rámce, takzvané *VLAN-značkované rámce*[13]. Formát takéhoto rámcu špecifikuje štandard IEEE 802.1Q ako: *„A VLAN-tagged frame is a tagged frame whose tag header carries both VLAN identification and priority information.“*[24, str. 31] *Hlavička značky*[14] je definovaná podľa IEEE 802.1Q takto: *„A header that allows priority information, and optionally, Virtual Local Area Network (VLAN) identification information, to be associated with frame.“*.[24, str.31] Vďaka tomu, že sa jedná o otvorený, priemyselný štandard, podpora nie je obmedzená na jedného výrobcu. Prepínače i zariadenia implementujú tento štandard a preto, keď na rozhraní príjmu VLAN-značkovaný rámec, vedia ho správne spracovať. Vyplnením hlavičky značky identifikátorom VLAN dokáže učiteľský počítač pracovať s niekoľkými VLAN súčasne v celej sieti laboratória. Rovnako i serveru je umožnené poskytovať služby pre sieť laboratória, zatiaľ čo si udržuje pripojenie do fakultnej siete.

V obrázku 2.2 je vidieť, že medzi prepínačmi sa nachádza viac ako jedno fyzické prepojenie. Existuje preto viac ako jedna cesta pre dáta na dosiahnutie zdrojov a zariadení v sieti. Takéto zapojenie vytvára v topológií cykly, čo do Ethernet siete prináša problémy. Ethernet rámce, narozdiel od IP paketov, neobsahujú v hlavičke pole *time-to-live*. Toto pole vyjadruje čas v sekundách, ktorý môže zostať paket v sieti. Zároveň však musí každý smerovač, ktorý paket spracuje a prepošle ďalej, znížiť toto pole o jedna. Akonáhle je táto hodnota v poli rovná nule, tento paket musí byť smerovačom zahodený. Ne-

[12] tabuľka, ktorá je tvorená párom linkovej adresy spolu s portom, kde bola daná adresa objavená
[13] z angl. VLAN-tagged frame
[14] z angl. tag header

môže sa preto stať, žeby sa v sieti nachádzali IP pakety donekonečna.[25] Ethernet rámce sa však do nekonečných cyklov dostanú veľmi jednoducho. V situácií keď sa jeden prepínač dokáže do druhého dostať dvomi rôznymi cestami je všesmerné vysielanie uviaznuté v cykle a neprestáva sa množiť, až sa dosiahne kritická hodnota množstva všesmerných rámcov a prepínače prestanú správne fungovať. Popísaná situácia, je tiež známa pod názvom *všesmerná búrka.*[26][15]

Jedno z riešení cyklov v Ethernet sieti je jednoducho nedovoliť fyzické cyklické zapojenie. Nie vždy je to však možné a sieť prichádza o výhodu redundantných ciest, ktoré je možné použiť v prípade výpadku hlavnej cesty. Štandard IEEE 802.1Q-2016 začlenil do seba protokoly, ktoré majú za úlohu zabrániť vzniku slučiek v aktívnej topológií. Jeden zo zástupcov týchto protokolov je Rapid Spanning Tree Protocol. Protokol poskytuje rýchle obnovenie siete v prípade zlyhania sieťových komponentov, použitých fyzickej redundantnej cesty v sieti, bez zasiahnutia správcu. RSTP vznikol evolúciou staršieho protokolu, Spanning Tree Protocol. Pôvodný STP je od roku 2004 plne nahradený RSTP.[27] Hlavným nedostatkom pôvodného STP bola dlhá doba obnovenia siete po výpadku. Táto doba sa mohla vyšplhať až na 50 sekúnd, čo je v dnešnej dobe neprijateľné. RSTP využíva princípy zavedené v pôvodnej verzii, avšak pridáva do protokolu funkcionalitu, ktorá zníži dobu výpadku na 1 až 2 sekundy.

Pre vytvorenie takejto aktívnej topológie, RSTP preberá algoritmus použitý už v pôvodnej špecifikácií STP. Je rozdelený na štyri kroky a výsledkom je aktívna topológia tvoriaca kostru grafu.

1. Voľba *koreňového prepínača.*

2. Voľba *koreňových portov* každého prepínača.

3. Určenie *vybraných portov* každého prepínača.

4. Blokovanie všetkých *nevybraných portov* z aktívnej topológie.

Voľba koreňového prepínača je založená na nájdený najmenšieho identifikátoru (BID[16]) medzi prepínačmi. Ten je tvorený MAC adresou a prioritou. Prioritu je možné zmeniť, takže voľba je ovplyvniteľná administrátorom. Prepínače rozosielajú *BPDU Hello správy* zo všetkých svojich rozhraní a táto správa obsahuje mimo iné i identifikátor aktuálne známeho koreňového prepínača. Akonáhle na rozhranie prepínača príde BPDU Hello správa s koreňovým prepínačom, ktorý má menší BID, než aktuálne uložené v prepínači, stará informácia sa zahodí a je nahradená za prijatú.

[15] z angl. broadcast storm
[16] z angl. Bridge Identifier

Po zvolení koreňového prepínača je nutné aby všetky prepínače určili svoj *koreňový port*[17]. Ten sa nachádza na rozhraní s najnižšou cenou ku koreňu[18], ktorá je tvorená ako suma všetkých cien cesty ku koreňovému prepínaču. V prípade, že existuje viac ako jedna cesta ku koreňovému prepínaču s rovnakou cenou, koreňový port sa určí podľa najlepšieho identifikátoru portu.
V ďalšej fázy musia prepínače zvoliť svoje *vybrané porty*[19]. Voľba je podobná ako pri volení koreňového portu. Porty na danom segmente spočítajú svoju cenu ku koreňu, teda cenu cesty cez tento segment ku koreňovému prepínaču. Ako vybraný port je určený port, ktorý má nižšiu cenu ku koreňu. V prípade zhody ceny týchto ciest má na tomto segmente vybraný port prepínač s nižším BID. Všetky porty, ktoré po voľbe nie sú označené za vybrané budú blokované a nebudú spracovávať prijaté dátové rámce a ani žiadne cez toto rozhranie odosielať. Stále však nie sú vypnuté, pretože musia prijímať kontrolné správy BPDU.

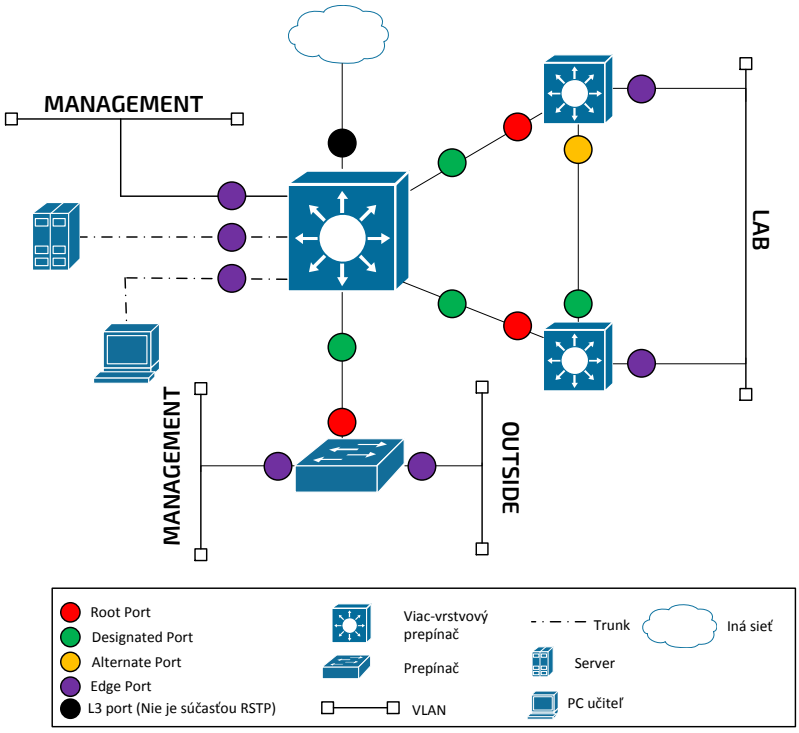
RSTP priradí každému rozhraniu prepínača stav a rolu. Používa tri rôzne stavy, *discarding, learning, forwarding*. Role koreňového a vybraného portu zostala nezmenená, avšak blokujúci port môže mať dve rôzne role a to *alternate* a *backup* rola. Obe tieto role získava rozhranie keď sa nachádza v stave discarding. Alternate port určuje alternatívnu cestu ku koreňovému prepínaču a nachádza sa na inom prepínači v rámci segmentu. Narozdiel od toho backup port určuje náhradnú cestu do segmentu, avšak negarantuje, že vedie ku koreňovému prepínaču, pretože sa nachádza na tom istom prepínači ako je vybraný port pre segment.[28].

Obrázok 2.6 ukazuje topológiu v centrálnom rozvádzači z pohľadu RSTP. Jednotlivé role portov sú vyznačené a je vidieť že fyzické prepojenie vytvára cyklus. Tento sa v rozvádzači nachádza iba jeden a to vo VLAN určenej pre laboratórium. Implementácia RSTP na prepínačoch Cisco, s názvom Rapid-PVST+ rezervuje jednu inštanciu RSTP pre každú VLAN[29], čo je možné využiť pri optimalizácií tokov. Pre jednu VLAN je port blokovaný, zato iná VLAN môže tento port využiť. Táto možnosť však nie je využitá, pretože v cykle sa nachádza iba jedna VLAN.

Jeden z mechanizmov RSTP, ktorý pomáha k rýchlej konvergencii je použitie takzvaných *okrajových portov*[20]. Tieto porty môžu ihneď prejsť do stavu forwarding, bez toho aby boli blokované. Zmena stavu linky na okrajovom porte nevyvoláva zmenu aktívnej topológie. Akonáhle však port príjme BPDU, okamžite sa mení okrajový port na štandardný. Preto sú tieto rozhrania pripojené na koncové zariadenia.

RSTP pri rozhodovaní o tom, či daný port prejde do stavu forwarding využíva sekvenciu *Proposal* a *Agreement* správ. Proces ilustruje obrázok 2.7.

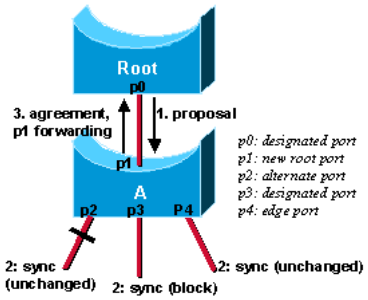
[17] z angl. Root Port
[18] z angl. Root Path Cost
[19] z angl. Designated Port
[20] z angl. Edge Port



Obr. 2.6: Centrálny rozvádzač z pohľadu RSTP

Po pripojení nového prepínaču A majú oba porty rolu vybraného portu, avšak nachádzajú sa v stave discarding, takže žiadne datové rámce cez tieto porty neprechádzajú. V tomto stave zostávajú dovtedy pokiaľ si oba nevymenia svoje BPDU. V hlavičke BPDU sa nastaví Proposal bit na 1 a prepínač A dostane BPDU, ktoré je lepšie než jeho odosielané. Je teda zrejmé, že na danom porte sa nachádza nový koreňový port a prepínač začne synchronizáciu svojich ostatných rozhraní s touto novou informáciou. Podmienkou synchronizácie portu je, že sa jedná buď o port v stave discarding alebo ide o okrajový port. Ak sa port nespĺňa podmienku synchronizácie je dočasne v stave discarding ale v roli vybraného portu, čím sa dostáva do rovnakej situácie ako bol čerstvo pripojený port prepínaču A. Akonáhle sú všetky porty synchronizované, prepínač A pošle koreňovému prepínaču Agreement správu. Nové prepojenie koreňového prepínaču a prepínaču A prechádza na oboch portoch zo stavu discarding do stavu forwarding. Rozhrania prepínaču A, ktoré boli zablokované počas synchronizácie opakujú proces Proposal a Agreement. [28]

Medzi prepínačmi v topológií na obrázku 2.2 existuje niekoľko liniek a vytvárajú tak cyklus v sieti. RSTP zabezpečí, že aktívna bude iba jedna cesta,



Obr. 2.7: Výmena Proposal a Agreement správ pri pridaní nového prepínaču do siete[28]

avšak existuje možnosť využiť tieto linky a nie je nutné aby boli neaktívne pokiaľ hlavná cesta je funkčná. Pomocou *agregácie liniek* je možné zlúčiť tieto fyzické prepojenia do jedného logického rozhrania. Výhodou tohto prístupu je:

- Zvýšená priepustnosť
- Zvýšená dostupnosť

Agregáciou liniek dokážeme dosiahnuť lineárny nárast v rýchlosti linky. Prináša teda alternatívu k zvýšeniu priepustnosti, kde už rýchlosť 1 Gbit/s nemusí stačiť avšak nákup sieťovej karty s rýchlosťou 10 Gbit/s je zbytočne finančne náročný, prípadne by bol využitý iba zlomok dostupného pásma. Samotná agregácia liniek môže fungovať automaticky. O toto sa stará Link Aggregation Control Protocol (LACP). Poskytuje štandardný spôsob výmeny informácií medzi dvomi prepínačmi linkami, ktoré majú byť agregované do jednej. Dokáže reagovať i na výpadky jednotlivých liniek v agregovanej skupine a automaticky tak rozdelí záťaž na zvyšné, fungujúce spojenia. [30] Všetky linky v návrhu, kde je agregácia žiadúca, majú aktivovaný LACP. I keď výrobcovia sieťového hardwaru stále ponúkajú ich vlastné protokoly na agregáciu liniek, rozhodol som sa použiť otvorené štandardy všade kde výrobcom definované protokoly neprinášajú výraznú výhodu nad priemyselným štandardom v prostredí učebne. Dôsledkom spojenia fyzických rozhraní do jedného logického sa vyrieši problém s blokáciou redundantných spojení medzi dvomi prepínačmi. RSTP sa bude chovať k skupine portov ako k jednému portu. V prípade však vytvorenia cyklu zablokuje celú skupinu portov naraz.
Implementácia agregácie na prepínačoch použitých v učebni sa nazýva Cisco Etherchannel®.[31] Zátaž však nie je rovnomerne rozdelená na jednotlivé linky v agregovanom spojení. Pri rozhodovaní, ktoré rozhranie bude použité, vypočíta prepínač identifikátor portu pomocou hešovania[21], definovaného ako: „*Hashing is the process of calculating a numeric value from one or more data*

[21] z angl. hashing

items.“[4, str. 342]. Algoritmus použitý pri hešovaní na prepínačoch vracia hodnoty 0-7, pretože maximálny počet agregovaných liniek v jednej skupine na prepínačoch v učebni je 8.
Zdrojové hodnoty, na ktoré je hešovací algoritmus spustený záleží od nastavenia administrátorom. Môže sa rozhodnúť pre zdrojovú alebo cieľovú MAC adresu, prípadne kombinácia oboch hodnôt. To isté platí aj pre IP adresy, prípadne na niektorých platformách i čísla portov.
Pre priradenie indexu k fyzickému portu sa používa 1 až 3 bity v závislosti koľko liniek sa nachádza v skupine. Je preto vhodné, aby počet portov v Etherchannel skupine bol mocnina 2.[32] Skupiny v učebni dodržiava toto pravidlo a sú tvorené 4 alebo 2 linkami. I tak však samotné rozloženie záťaže nie je podľa jednotlivých paketov ale je podľa daného toku dát. To znamená, že v prípade komunikácie z rovnakého zdroju na rovnaký cieľ je vždy použitý ten istý fyzický port. [32]
Pre plné využitie Etherchannel v učebni, je nutné identifikovať typické dátové toky v sieti. Väčšina zariadení pripojených do VLAN pre laboratórium budú pristupovať na server, prípadne centrálny prepínač `Central-SW`. Znamená to, že rôzne MAC adresy budú smerovať na jednu konkrétnu MAC adresu, preto je ako parameter pre rozloženie záťaže použitá zdrojová MAC adresa, ktorá vytvára separátny dátový tok pre každú zdrojovú MAC adresu. Naopak, odpovede z centrálneho prepínača budú typicky smerovať z jednej MAC adresy na niekoľko zdrojových, preto je vhodné použiť opačný postup a to rozloženie zátaže podľa cieľovej MAC adresy.

Už aj na linkovej vrstve je vhodné riešiť bezpečnosť siete. Typické útoky sú podvrhnutie adries, teda snaha útočníka vydávať sa za legitímneho užívateľa v sieti prípadne vygenerovať veľké množstvo falošných adries k zahlteniu prepínačov a následné odpočúvanie dátových tokov. Útočník sa môže pokúsiť i o takzvaný *VLAN-hopping*, čo je získanie neoprávneného prístupu do inej VLAN, kde sa útočník nachádza. Pokročilé prepínače použité v návrhu sú však na tieto typy útokov pripravené a majú integrované nástroje pre obranu proti týmto útokom.
Navrhovaná učebňa by mala byť pripravená brániť sa. Je dôležité aby boli VLAN pre prístup do fakultnej siete a do správy prvkov ochránené a aby nebola narušená výuka. Zároveň však učebňa poskytuje VLAN pre laboratórium, ktorá tieto nástroje neimplementuje a môže preto slúžiť i ako sieť pre testovanie týchto útokov počas výuky.
Jednoduchý útok, ktorého cieľom môže byť odpočúvanie komunikácie je zahltenie tabuľky MAC adries prepínača. Prepínač dokáže naraz uchovať obmedzený počet MAC adries a v prípade, že sa táto tabuľka naplní, začne rozosielať komunikáciu zo všetkých rozhraní a toto je práve cieľ útočníka. V útoku je zneužitý princíp fungovanie prepínaču. Prepínač si počas komunikácie ukladá informáciu o zdrojovej MAC adrese ku konkrétnemu rozhraniu z konkrétnej VLAN. V prípade, že cieľovú MAC adresu nemá priradenú k žiadnemu rozhra-

niu, rozošle rámec zo všetkých portov, okrem toho, odkiaľ mu rámec prišiel. Cieľové zariadenie odpovie a odpoveďou sa prepínač znovu naučí, kde sa daný cieľ nachádza, znovu pomocou zdrojovej MAC adresy. Naspäť už prepínač dokáže odpoveď bez toho aby rozoslal správu zo všetkých rozhraní. Prostriedkom na obranu je obmedzenie počtu MAC adries naučených na jednom rozhraní. Toto zabráni zahltiť prepínač falošnými adresami. Takýto pokus môže vyvolať správu do logu prípadne vypnúť daný port. Správca siete potom môže vyriešiť tento bezpečnostný incident.

Ďalší zástupca útoku, ktorého cieľom je odpočúvanie komunikácie, je *DHCP spoofing*. Princíp spočíva v nasadení neoprávneného DHCP serveru, ktorý rozdáva IP adresy klientom. Keďže DHCP klient si vyberie prvú ponuku na adresu akú dostane, často sa stane, že práve neoprávnený DHCP server dorazí ako prvý. Legitímny DHCP server je väčšinou v sieti vzdialený niekoľkými prepínačmi a nedokáže tak rýchlo odpovedať ako server pripojený napríklad v rovnakom prepínači spolu s klientom. Na tento útok však prepínače v návrhu implementujú *DHCP snooping*. Princíp fungovania spočíva v označení rozhraní prepínača na dôveryhodné a nedôveryhodné. Z nedôveryhodných rozhraní nie sú povolené žiadne správy, ktoré vedú k ponuku adries pre DHCP klienta. Naopak pri dôveryhodných nie sú blokované žiadne správy a teda iba z týchto portov je možné získať správu od DHCP serveru. Dôležitým dôsledkom DHCP snooping je i vytvorenie tabuľky v prepínačoch, ktorá drží informáciu o tom, akú IP adresu dostal klient s danou MAC adresou z konkrétneho portu. Táto tabuľka slúži ako referencia pre ďalšie bezpečnostné funkcie prepínača.[33]

Zraniteľný je i *Address Resolution Protocol*. Jeho úlohou je priradiť k adrese sieťovej vrstvy TCP/IP modelu adresu z vrstvy sieťového prístupu. Bez neho by nebolo možné dokončiť zapúzdrenie dát ak by stanica, ktorá chce komunikovať nepoznala adresu druhej vrstvy, teda MAC adresu. Stanica pred odoslaním rámcu do siete musí vyplniť cieľovú MAC adresu v Ethernet hlavičke. Skontroluje najskôr svoj obsah *ARP tabuľky*, čo nie je nič iné ako páry IP adries a MAC adries v sieti. V prípade, že pre cieľovú IP adresu nemá záznam v ARP tabuľke, pozastaví stanica odosielanie dát a vytvorí *ARP žiadosť*. Tá obsahuje zdrojovú MAC adresu počítača i zdrojovú IP adresu, z ktorého je vyslaná a cieľovú IP adresu, ku ktorej chce stanica zistiť MAC adresu. Táto žiadosť je zapúzdrená do Ethernetového rámca, kde je pole s identifikátorom protokolu vyplnené hodnotou 0x80. Nakoniec je tento rámec odoslaný ako všesmerné vysielanie a tak sa dostane do všesmerovej domény. Odpoveďou na dotaz je *ARP odpoveď*, ktorá obsahuje zdrojovú MAC a IP adresu a cieľovú MAC a IP adresu, podľa toho, ako boli vyplnené v žiadosti. Tentokrát sa však odpoveď už neposiela na všesmerové vysielanie ale ako cieľová MAC adresa je použitá adresa, ktorá bola uvedená ako zdrojová v ARP žiadosti.
Podľa RFC 826 stanica, ktorá prijme ARP žiadosť jej určenú upraví svoju

lokálnu ARP tabuľku novým záznamom.[34] Pre útočníka nie je problém vytvoriť ARP odpovede, ktoré vedú užívateľa na zariadenie útočníka. Aby však útok prebehol nepozorovane, musí byť zaistená konektivita užívateľa, preto sa odošle ešte odpoveď pre východziu bránu, ktorá po úprave svojej ARP cache bude predpokladať, že užívateľ má MAC adresu ako útočník. Všetky dátové toky prechádzajú cez zariadenie útočníka a odpočúva tak komunikáciu užívateľa. Moderné prepínače však dokážu takémuto *otrávaeniu ARP*[22] zabrániť. Prepínače v učebni využívajú pre tento účel *dynamickú inšpekciu ARP*[23][35], ktorá využíva tabuľku DHCP snoopingu. V tejto tabuľke sú páry MAC adries a IP adries priradené dôveryhodným DHCP serverom. Každá ARP odpoveď, ktorá dorazí na nedôveryhodné rozhranie je skontrolovaná, či sa nejedná o podvrhnutý pár. V prípade, že tak nastane, tento dotaz nie je rozoslaný ďalej. Udalosť môže byť zaznamenaná v logu, dokonca je možné i limitovať množstvo ARP packetov na rozhranie a v prípade prekročenia dôjde k zablokovaniu rozhrania.
V učebni táto kontrola je spustená na VLAN, do ktorých by nemali študenti zasahovať. Preto všetky porty v pracovnom rozvádzači, ktoré slúžia ako pripojenie do externej siete, prípade do siete správy prvkov sú zaradené ako nedôveryhodné. Kontrola teda zabráni útokom na ARP.

Dynamická inšpekcia ARP ochráni sieť proti otráveniu ARP, avšak útočník stále môže zmeniť MAC adresu a IP adresu svôjho zariadenie s cieľom tváriť sa ako legitímne zariadenie v sieti. Ak prepínač dostane na novom rozhraní MAC adresu, ktorú už pozná, predpokladá, že zariadenie sa presunulo a upraví svoju tabuľku MAC adries. Toto sa deje stále akonáhle prepínač príjme dáta na porte. Legitímny stroj by tak mohol prebiť podvodnú MAC adresu, ale útočník môže neustále tvoriť dátový tok na prepínač a skutočné zariadenie sa tak nikdy nedostane k tomu, aby bol záznam v MAC tabuľke upravený.

Riešenie, implementované v prepínačoch od Cisco, je funkcia *IP Source Guard*. Funguje veľmi podobne ako dynamická inšpekcia ARP, s tým rozdielom, že kontroluje nie len ARP pakety ale všetky pakety, ktoré prechádzajú prepínačom. Opäť využíva vytvorenú tabuľku trojice IP adresa - MAC adresa - port prepínaču, k overeniu legitímnosti MAC adresy a IP adresy na nedôveryhodných portoch. IP Source Guard dynamicky udržuje pravidlá filtru, ktoré sú pre každý port unikátne. Na začiatku po pripojení zariadenia do portu je zakázaná akákoľvek komunikácia s výnimkou DHCP. Až po tom, čo zariadenie získa adresu z dôveryhodného DHCP serveru, vytvorí sa na rozhraní filter, ktorý dovolí iba komunikáciu s IP adresou od DHCP a MAC adresou, ktorá tvorí pár s IP adresou v tabuľke DHCP snoopingu. [33]

[22] z angl. ARP poisoning
[23] z angl. Dynamic ARP Inspection

2.1.2.2 Topológia siete - sieťová vrstva

Presunutím z linkovej vrstvy TCP/IP modelu vyššie sa dostávame na *sieťovú vrstvu*. Už v názve TCP/IP sa nachádza práve protokol používaný na tejto vrstve, *Internet Protocol*. Rozšírené sú práve verzie 4 a 6, ktoré zabezpečujú smerovanie a adresáciu medzi sieťami v Internete. Hlavná funkcia protokolu je adresácia zariadení, ktorá narozdiel od linkovej vrstvy, je platná i mimo LAN. Každé zariadenie, ktorým komunikácia prechádza, implementuje IP a rozumie tak formátu adries[25]. Pri komunikácií sa cieľová a zdrojová adresa nemení[24] a nezáleží akým médiom dáta prechádzajú.
IP definuje formát adresy a rôzne verzie používajú iný formát. Preto nie je možné komunikovať medzi zariadeniami, ktoré podporujú iba IPv4 so zariadeniami podporujúce len IPv6. Jeden z hlavných dôvodov vzniku novej verzie IP je vyčerpanie dostupných adries v IP verzie 4[36]. Predpokladalo sa, že veľkosť adresy 32 bitov bude dosť veľká na to, aby pokryla všetky zariadenia na svete, avšak rozmach Internetu presvedčil o opaku. Tento problém spomalilo zavedenie *privátnych IP adries*, ktoré sa nemohli objaviť na Internete a boli určené iba na komunikáciu v rámci siete spravované jedným subjektom, či už to bola firma alebo domácnosť [37]. Aby však bolo možné aj tieto siete pripojiť do Internetu, zaviedol sa mechanizmus *prekladu adries*, tiež známy ako Network Address Translation (NAT). Privátne IP adresy prekladá na *verejné IP adresy* a pod jednou verejnou adresou je možné udržovať jednu, niekoľko alebo i všetky privátne adresy v danej sieti[38]. NAT poskytuje krátkodobé riešenie, preto sa do budúcnosti počíta s nahradením IP verzie 4 za novší, IPv6. Adresy majú až 128-bitov, čo rapídne zvyšuje dostupný adresný priestor[39].

Nekompatibilita medzi IPv4 a IPv6 zdržiava prechod na novšiu verziu. Nie je nutné prejsť z jedného protokolu na druhý za jeden deň a toto tvrdenie podporuje i existencia prechodových mechanizmov na IPv6. V učebni je využitá technológia dual-stack, teda IPv4 a IPv6 fungujú paralelne a nezávisle na sebe.[40] Zariadenia teda dokážu spracovať požiadavky prijaté z oboch verzií protokolu. V laboratóriu sa nachádza niekoľko logicky oddelených sietí, tak ako boli definované v tejto kapitole a tieto logické siete potrebujú tiež vlastnú adresáciu. Vo zvolených rozsahoch 3. oktet IPv4 adresy je rovnaký ako identifikačné číslo VLAN, do ktorej daný rozsah platí. Administrátor sa tak vie ľahšie zorientovať, ktorá podsieť patrí do ktorej VLAN. Adresáciu popisuje tabuľka 2.1 a 2.2.

I v návrhu ideálnej učebni sa využíva DHCP server pre priradenie IP adries jednotlivým staniciam. Nenachádza sa vo všetkých virtuálnych LAN, ale iba vo VLAN *OUTSIDE* a *MANAGEMENT*. Nie je dôvod udržiavať DHCP server vo VLAN *LAB*, pretože táto je využívaná počas výuky, kde DHCP server nie je žiadúci a mohol by narúšať pripravené úlohy. Virtuálne LAN, kde

[24] s výnimkou pri použití mechanizmov na preklad IP adries

[25] nejedná sa o reálne použité IPv6 adresy. Použitý rozsah je preferovaný spôsob pre dokumentáciu podľa RFC 3849[41]

Názov VLAN	VLAN ID	IPv4 adresa	Maska podsiete	IPv4 adresa brány
LAB	10	10.0.10.0	255.255.255.0	10.0.10.1
MANAGEMENT	20	10.0.20.0	255.255.255.0	10.0.20.1
OUTSIDE	30	10.0.30.0	255.255.255.0	10.0.30.1
BLACKHOLE	40	-	-	-

Tabuľka 2.1: IPv4 adresné schéma učebne

Názov VLAN	VLAN ID	IPv6 adresa siete[25]	IPv6 prefix	IPv6 adresa brány
LAB	10	2001:db8:0:10::0	64	2001:db8:0:10::1
MANAGEMENT	20	2001:db8:0:20::0	64	2001:db8:0:20::1
OUTSIDE	30	2001:db8:0:30::0	64	2001:db8:0:30::1
BLACKHOLE	40	-	-	-

Tabuľka 2.2: IPv6 adresné schéma učebne

je DHCP používané, implementujú ochranu DHCP serveru už na vrstve sieťového prístupu a zároveň všetky zariadenia v týchto VLAN používajú statické záznamy. Samotný priebeh priradenia adresy koncovému zariadeniu popisuje RFC 2131.[42].

Vo svete IPv6 sa naviac, oproti IPv4, často využíva *lokálná linková adresa*[26] rozhrania. Tá je platná iba v rámci segmentu a každé rozhranie, ktoré používa IPv6 musí mať aspoň jednu lokálnu linkovú adresu.[39] Adresa je generovaná automaticky, no rozhraniu je možné priradiť manuálne adresu z rozsahu `fe80::/64`. Požiadavok na unikátnosť platí len v rámci segmentu, takže smerovač môže mať na všetkých rozhraniach rovnakú lokálnu linkovú adresu. Koncové zariadenia teda použijú jednu IPv6 adresu pre východziu bránu, nech sa nachádzajú v ľubovolnej VLAN. Rovnaký princíp je možné použiť aj s inými sieťovými službami ako napríklad DNS alebo NTP.

IPv6 ponúka niekoľko možností automatického priradenia IP adresy zariadeniu a nespolieha sa iba na DHCP ako je to vo verzii 4. RFC 4862 uviedlo Stateless Adress Autoconfiguration, teda SLAAC. Mechanizmus umožní zariadeniu vygenerovať unikátnu globálnu IPv6 adresu, bez zásahu užívateľa a bez nutnosti serverov v sieti a na smerovačoch je vyžadovaná iba minimálna konfigurácia, prípadne žiadna. Tento spôsob je vhodný pre prostredie, kde pre nás nie je dôležité aká IPv6 adresa sa objaví na koncových zariadeniach ale zaujíma nás hlavne aby bola smerovateľná a unikátna.[43]

Vyššiu kontrolu nad priraďovaním adries ponúka DHCP verzie 6 a to rovno v dvoch variantách - *bezstavový DHCPv6* a *stavový DHCPv6*. Rozdiel medzi týmito dvomi variantami je v tom, aké údaje ponúkajú klientovi. Pri bezstavovom DHCPv6 je úlohou serveru ponúknuť iba doplňujúce informácie ako adresu DNS alebo NTP. Nerozdáva klientské IPv6 adresy, takže nie je nutné aby udržoval stav, ktorým zariadeniam aké IP adresy rozdal. Zvyšné informácie ako prefix siete zistí koncová stanica od smerovaču a unikátnu adresu si vygeneruje pomocou mechanizmu SLAAC. Narozdiel od predchádza-

[26] z angl. link-local address

júceho, stavový DHCPv6 server zabezpečuje pre klientov všetky informácie, rozdáva globálne IPv6 adresy a udržuje stav klientov, rovnako ako to je pri DHCPv4.[44] Posledná možnosť je teda ideálna pre potrebu učebne. Jednotlivé stanice budú mať vytvorené statické záznamy IPv6 adries rovnako ako to bolo pri IPv4. DHCPv6 server sa bude nachádzať vo VLAN 20 a 30, čiže sa nejedná o žiadnu zmenu oproti nasadeniu DHCPv4.

Ak by sa v budúcnosti mala meniť adresácia laboratória, prináša to niekoľko problémov. Odhliadnuc od správneho naplánovania migrácie a zaistenie konfiguračných zmien na všetkých zariadeniach, ktoré pracovali s IP adresami učebne, je nutné udržovať aktuálny stav o adresách použitých v sieti. Mnohokrát sa dokumentácia neaktualizuje, pretože bola vyrobená ručne počas prvotného návrhu a zmeny, ktoré sa za čas udiali už nikto nezaznamenal. Skutočne aktuálny stav ponúka IP address management, ktorý integruje do seba DNS a DHCP v sieti, takže obe služby vidia jednotlivé zmeny dynamicky, podľa toho ako nastanú. Nástroj rovnako ponúkne prehľad rezervovaných adries.[45]

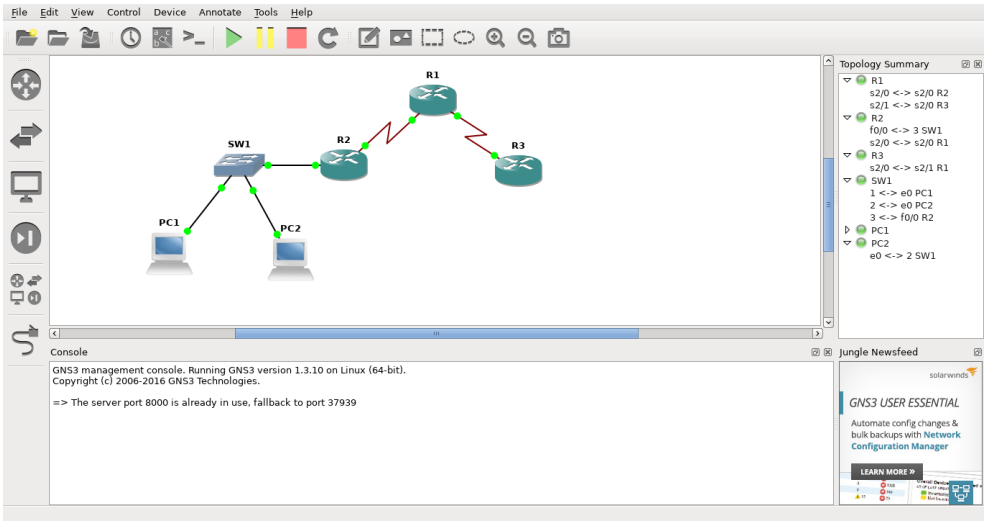
2.1.2.3 Sieťové služby

Sieťové laboratórium nie je len o veľkom množstve sieťového hardwaru ale vyžaduje i servery, ktoré doplňovať topológiu laboratórnej siete o sieťové služby. Študenti by mali vedieť konfigurovať základné služby ako DHCP server, DNS server, web server, autentifikačné služby a iné. Centrálny rozvádzač je preto vybavený i fyzickým serverom, ktorý slúži pre beh niekoľkých virtuálnych operačných systémov. Virtualizáciu zabezpečuje *hypervizor* typu 1. Jeho úlohou je vytvárať prostredie pre hosťovské operačné systémy a rovnako ich aj spravuje. Hypervizor tohto typu beží priamo na hardwari a stará sa o alokáciu všetkých prostriedkov pre hosťovské systémy. [46] O virtualizáciu v učebni sa stará produkt vSphere od spoločnosti VMWare, ktorého súčasťou je i hypervizor typu 1, ESXi.[16]
Fyzicky je tento server pripojený k všetkým VLAN v učebni. Prístup k Internetu je potrebný pre sťahovanie softwaru a aktualizácií. Prístup do VLAN pre manažment prvkov je dôležitý aby bolo možné sa pripojiť priamo do hypervizoru a spravovať ho cez sieť. Nakoniec by mali mať hosťovské systémy, bežiace na serveri prístup do VLAN pre učebňu. Práve služby, ktoré budú spustené na týchto systémoch je potrebné zaviesť do siete laboratória aby študenti mohli vidieť ich chovanie v sieti.
Server bude vybavený šablonami systémov, ktoré budú mať prednastavené a nainštalované bežné sieťové služby. Študenti si môžu vybrať, či si spustia do učebne web server, alebo im bude stačiť DHCP server. Nič im nebráni v inštalácií ďalšieho software do systému, nemôžu len modifikovať nastavenia šablony. Dôvod tohto opatrenia je, aby boli serveri udržiavané v konzistentnom stave,

do ktorého sa dá i po pokusoch študentov bez problémov vrátiť. K vytvoreniu virtuálneho stroju zo šablony sa použije webové rozhranie vSphere Web Client, pomocou ktorého sa pripoja k vCenter Server, ktorý združuje všetky ESXi hypervizory. Pre autentifikáciu užívateľov nie je nutné vytvárať nové účty, pretože vCenter podporuje napojenie na zdroje identít. Je preto možné využiť už existujúce študentské účty, ktoré používajú na prístup do ostatných fakultných systémov. Po vytvorení virtuálneho stroju sa môžu na neho užívatelia pripojiť pomocou SSH klienta na počítači a konfigurovať ho, prípadne použiť konzolové pripojenie priamo z webového rozhrania, ak by daný stroj nemal správne nakonfigurované pripojenie do siete.

Sieťová učebňa je plne vybavená aktívnymi prvkami spoločnosti Cisco Systems a prepojením jednotlivých pracovných rozvádzačov je možné vytvoriť komplexnú topológiu. I to však nemusí vždy stačiť. V prípade poruche hardwaru bude jedna z pracovných staníc neplnohodnotná a študent tak nebude mať možnosť pracovať na zadaní. Riešením je využiť emulačný software Graphical Network Simulator 3, známy pod skratkou GNS3. Jedná sa o veľmi vyspelí software, používaný viac než pol miliónom sieťových inžinierov na svete.[15] Ponúka grafické rozhranie, kde topológiu siete je možné vytvoriť pretiahnutím ikôn do pracovnej plochy. Smerovače, prepínače, virtuálne počítače a iné zariadenia sa prepoja rozhraniami, kde užívateľ vyberie myšou konkrétne rozhranie zariadenia a prepojí ho s iným. Ukážka rozhrania a jednoduchej topológie je na obrázku 2.8. GNS3 dokáže do topológie zahrnúť emulované systémové obrazy sieťových operačných systémov rôznych výrobcov, ako sú Cisco, Juniper a iný. Rovnako dokáže pridať i virtuálne stroje, používajúce VMWare, VirtualBox alebo QEMU ako hypervizor. Medzi zariadeniami je možné sledovať dáta v reálnom čase a preto je GNS3 výborný nástroj pre výuku a testovanie sietí. Využitie nástroju v učebni sa nájde v prípade nedostupnosti fyzického hardwaru. Či už sa jedná o výpadok alebo topológia je natoľko komplexná, že vybavenie učebne nestačí. GNS3 je možné pripojiť i do reálnej siete, takže spolupráca pracovných staníc môže byť docielená i s emulovanými zariadeniami. Rozpracované zadanie je možné si uložiť a pracovať na ňom neskôr. Topológia a konfigurácia zostane uložená a stačí ju znova otvoriť v GNS3 ako súbor v akomkoľvek inom programe. To naväzuje i na to, že študenti môžu dostať praktické domáce úlohy, ktoré zvládnu spraviť i keď nemajú prístup do učebne.

Každé spustené zariadenie v topológií vyžaduje na emuláciu prostriedky počítaču. Pri komplexných topológiách s veľkým počtom zariadení, sú kladené vysoké nároky na operačnú pamäť a procesor. GNS3 sa preto dá spustiť i vzdialene, kde jednotlivé zariadenia v topológií sú spustené na výkonnejšom serveri, zatiaľ čo užívateľ môže ovládať a vytvárať topológiu na svojom, menej výkonnom počítači. V učebni je pre tieto účely využitý server, ktorý sa nachádza v centrálnom rozvádzači a GNS3 má pre seba vyhradené zdroje a vlastnú inštanciu virtuálneho stroja. Užívatelia laboratória môžu použiť server



Obr. 2.8: Program GNS3 - ukážka rozhrania pracovnej plochy

pre spúšťanie komplexných topológií.

2.1.2.4 Vzdialený prístup

Učebňa v návrhu je pripravená byť ovládaná z jedného centrálneho miesta, zvyčajne sa predpokladá práve učiteľský počítač v učebni. Dokáže spustiť jednotlivé pracoviská, vďaka manažovaným PDU a má konzolový prístup k všetkým zariadeniam v učebni, čím vzniká dojem, že učiteľ pracuje pred všetkými stanicami s fyzickým prístupom. V prípade, že ovládanie je možné z počítaču v miestnosti, dá sa toto ovládanie rozšíriť na akýkoľvek počítač pripojený k sieti. Ak by bol však prístup k zariadeniam otvorený do Internetu, hocikto na svete by dokázal ovládať infraštruktúru v učebni, čo je neprijateľné.

Riešenie poskytuje virtuálna privátna sieť[27], ktorou úlohou je bezpečne preniesť dáta medzi dvoma stanicami cez nezabezpečenú sieť, akou je napríklad Internet.[4] Prenesené dáta sú šifrované, takže i v prípade odpočúvania komunikácie, útočník nedokáže prečítať obsah.
V učebni sa o vytváranie týchto šifrovaných tunelov stará *VPN koncentrátor*. Jedná sa o smerovač, doplnený o funkcie pre vytváranie VPN spojení. V učebni je ako VPN koncentrátor použitý ASA 5505 od spoločnosti Cisco. Podobne ako hypervizor, i VPN koncentrátor bude napojený na už existujúcu infraštruktúru poskytovateľa identity. Nie je nutné vytvárať nové užívateľské účty pre vzdialený prístup.
O bezpečnú komunikáciu sa stará skupina protokolov Internet Protocol Security (IPSec). O autentifikáciu, integritu a dôvernosť dát má na starosť Encapsulating Security Payload (ESP), definovaný v RFC 4303.[47] Pre úspešnú

[27] z angl. virtual private network

komunikáciu potrebujú mať obe strany rovnaké parametre použité pri zabezpečovaní komunikácie. IPSec používa Security Assosiations (SA), ktoré tvoria balíček algoritmov a dát potrebných pre správne fungovanie ESP. Pre výmenu týchto parametrov medzi dvoma stranami sa používa Internet Security Assosiations and Key Management Protokol (ISAKMP).[48] Až po dohodnutí týchto parametrov a naviazaní SA vedia obe strany aké algoritmy majú použiť pre zabezpečenie komunikácie. Skutočná komunikácia je s použitím režimu tunelu celá šifrovaná a autentifikovaná. Tento šifrovaný IP paket je znovu zabalený do nového IP paketu s novou hlavičkou, ktorá pri zdrojovej a cieľovej IP adrese obsahuje IP adresu peera. [47]

Využitie určite nájdu študenti v kombinovanej forme štúdia a študenti so zníženou schopnosťou pohybu. Táto skupina sa nemôže vždy fyzicky dostaviť do laboratória. Po dohode s vyučujúcim dostanú určený časový blok, kedy sa môžu pripojiť do laboratória. Vyučujúci predtým, než študent začne pracovať pripraví fyzické zapojenie zariadení. V čase práce by študentovi nemal nikto zasahovať, takže VPN koncentrátor obmedzí na dané časové obdobie počet aktívnych spojení. Pripojený užívateľ má prístup ku konzolám prvkov a môže tak absolvovať cvičenie i keď sa fyzicky nenachádza v učebni. Po vypršaní času v rezervovanom bloku, dôjde k nahraniu pôvodných konfigurácií a vypnutie použitých zariadení.

Na vytváranie šifrovaných spojení je v učebni použitý vyhradený hardware, avšak nie je to jediné riešenie. VPN je možné poskytovať i ako službu na serveri a to dokonca i zdarma, v prípade použitia open-source nástroju ako napríklad OpenVPN. Pre šifrovanie používa knižnicu OpenSSL[49] a rovnako ako na ASA autentifikácia funguje aj s existujúcou infraštruktúrou poskytujúcu identitu. V tomto prípade sa však už nejedná o IPSec VPN ale o SSL VPN.[50]

2.2 Reálna učebňa

Druhá časť tejto kapitoly popisuje zmeny v návrhu učebne, ktoré je možné reálne implementovať do sieťového laboratória T9:344 na FIT ČVUT. Analýza učebne v kapitole 1 odhalila problémy a myšlienky v návrhu bez obmedzení v sekcii 2.1 môžu odstrániť tieto problémy. Predpokladom je, že na zmeny v učebni nie sú vyhradené žiadne finančné prostriedky, z čoho vyplýva, že sa bude jednať o konfiguračné zmeny. Nákup hardware a rozvádzačov nie je možný, rovnako ako vytváranie a zmena súčasnej kabeláže v učebni. Zostáva teda možnosť komfortného prepojenia iba v rámci jednej rady, v prípade nutnosti sa použijú dlhšie káble v učebni a zariadenia mimo jednej rady sa budú prepájať napriamo a nie cez patch panel. Rovnako nie je možné počítať s implementáciou vzdialeného prístupu do učebne, tak ako je to popísané v ideálnom návrhu. Infraštruktúra nie je na to pripravená z technického pohľadu - bolo by nutné zakúpiť VPN koncentrátor a ani z pohľadu bezpečnostných

politík inštitúcie - nie je možné predpokladať povolenie prístupu neoverených, študentských zariadení do internej siete, hoci len jednej učebne. Pre správnu a bezpečnú implementáciu vzdialeného prístupu je nutné jasne definovať bezpečnostné politiky a akým spôsobom budú vynucované. Táto problematika však zasahuje mimo rozsah tejto bakalárskej práce.

2.2.1 Riešenie problémových miest učebne

Reálne však je možné vyriešiť problémy, zistené analýzou v kapitole 1. Najväžnejší problém tvoria duplicitné IP adresy a toto sa dá vyriešiť nasadením IP Source Guard technológie na prepínačoch, ktoré pripájajú počítače v učebni do fakultnej siete. Prepínače Cisco Catalyst 3750X s licenciou LAN Base, ktorá na nich aktívna, túto funkciu podporujú.[51] Ako bolo spomenuté v ideálnom návrhu, táto funkcia vyžaduje aktívny DHCP Snooping. Pre správne fungovanie by mali všetky zariadenia získavať adresu z DHCP serveru, vrátane serverov. V prípade vytvorenia statických DHCP záznamov, ktoré už počítače v učebni majú definované, sa adresácia nemusí vôbec meniť. Akonáhle by však študent nastavil adresu na rozhraní do fakultnej siete manuálne, port by bol zablokovaný a nedošlo by k problému s duplikovanými adresami. Ak by tento spôsob zamedzeniu neoprávnených IP adries nevyhovoval, je možné aktívne monitorovať IP adresy z učiteľskej stanice. Popis a implementácia nástroju, ktorý toto umožňuje je náplňou 3. kapitoly bakalárskej práce.

V časti 1.4.3 bola objavená minoritná bezpečnostná chyba a to rozposielanie CDP rámcov k študentským počítačom. Nejedná sa o závažnú chybu, poskytuje však potenciálnemu útočníkovi informácie o infraštruktúre. Určite však pomôže pri analýze, kde a na akom porte je prvok zapojený, avšak do produkčného prostredia táto informácia nepatrí. Vypnutie CDP na jednotlivých rozhraniach učebne stačí vykonať pomocou príkazu `no cdp enable`.

Zmenám sa nevyhne ani systémový obraz, používaný počas výuky predmetu Počítačové sítě. Problém, popísaný v 1.4.2 sa vyrieši úpravou konfiguračného súboru sieťových rozhraní, `/etc/network/interfaces`. Tam je treba povoliť automatické spustenie DHCP klienta i po naštartovaní počítača. Správna konfigurácia vyzerá takto:

```
# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet dhcp
```

2.2.2 Nasadenie virtuálnych strojov

Myšlienka použitia centrálneho serveru vSphere od spoločnosti VMWare pre spúštanie virtuálnych strojov so sieťovými službami, spomenuté v 2.1.2.3, sa dá

zjednodušiť tak, aby boli náklady čo najmenšie. Virtualizácia je dostupná i pre počítače a s použitím open-source nástrojov Vagrant[52] a VirtualBox[53] je nasadenie serverových systémov ľahko replikovatelné. Do systémového obrazu používaný pri výuke by sa nainštaloval Vagrant a VirtualBox a pripravili by sa odľahčené virtuálne stroje s požadovanými službami. Po príprave virtuálnych strojov do formátu, ktorému rozumie Vagrant - *vagrant box* a nahranie na server učebne, je spustenie pre užívateľa otázkou niekoľkých príkazov. Študent alebo učiteľ potrebuje vedieť iba názov boxu a URL, o všetko ostatné sa už postará Vagrant. Nasadenie predpripraveného virtuálneho stroja, s názvom `network-server.box` by preto mohlo vyzerať takto:

```
vagrant init network-server https://boxes.fit.cvut.cz/network-server.box
vagrant up
```

V konfiguračnom súbore `Vagrantfile` je možné nastaviť akým spôsobom má byť virtuálny stroj pripojený k sieti a študent tak môže ovplyvniť jeho dostupnosť v rámci učebne. Ovládanie je pomocou SSH a použitím príkazu `vagrant ssh` sa dostáva užívateľ do serveru, kde môže nainštalovať ďalšie služby alebo konfigurovať už tie pripravené. Výhodou oproti ručnému vytváraniu virtuálnych strojov vo VirtualBox je opakovateľnosť tohto procesu. S rovnakým konfiguračným súborom `Vagrantfile` sú stroje identické a v prípade potreby zmeny stačí prepísať parametre v tomto konfiguračnom súbore.

Pri výuke úvodného kurzu do počítačových sietí využije virtualizáciu hlavne učiteľ. Pre demonštráciu princípu fungovania sieťovej aplikácie ako napríklad DHCP server, nemusí učiteľ inštalovať na čistý systémový obraz DHCP server a konfigurovať ho pred každým cvičením. Stačí ak si stiahne príslušný *vagrant box*, ktorý už má DHCP server nakonfigurovaný a tento virtuálny stroj spustí a deleguje mu priamy prístup do siete. V pokročilejších kurzoch, ako napríklad BI-ADS, kde pre topológiu bude predpokladom správne fungovanie vybranej služby (napríklad web server s ukážkovým obsahom) si môže aj študent uľahčiť prácu tým, že použije už pripravený virtuálny stroj a môže sa sústrediť na náplň cvičenia, kde úlohou nie je konfigurácia a spojazdnenie web serveru ale napríklad vytvorenie skriptu, ktorý bude hľadať informácie zo všetkých web serverov v učebni.

2.3 Porovnanie návrhov učební

Už na začiatku sekcie 2.2 je jasne zmienené, že zmeny vo fyzickom zapojení reálnej učebne nebudú možné. Táto učebňa je už vybudovaná, kde naproti tomu v návrhu ideálnej učebne sa predpokladá stav, keď sa učebňa ešte len vytvára. Hoci stoly a pracovné rozvádzače sú usporiadané rovnako, prepojenie v reálnej učebni zostane len v rámci jednej rady. Nenachádza sa tu ani centrálny rozvádzač, tak ako to bolo v návrhu ideálnej učebne.

V konfigurácií prvkov sa však reálna učebňa môže inšpirovať. V oboch prípadoch je doporučené nasadenie IP Source Guard na prepínačoch učebne. Použitie virtualizácie v návrhu reálneho laboratória je obmedzené na študentovu stanicu a nenachádza sa tu centrálny server, ktorý by tieto virtuálne stroje združoval. Obe učebne môžu použiť emulačný nástroj GNS3 pre ľahké rozšírenie topológií, prípadne ako záložné riešenie keď nebude dostupný sieťový hardware.
S produkčným použitím IPv6 reálny návrh nepočíta. Nasadenie by vyžadovalo dôkladné plánovanie a sprevádzala by ho aj úprava bezpečnostných politík. Takéto nasadenie by malo zmysel, keby sa rieši v rámci celej fakulty a nie izolovane v jednej učebni. Podobným prípadom je aj vzdialený prístup do učebne, kde problémy nasadenia boli popísané v sekcii 2.2.

Kapitola 3

Monitorovací systém učebne

3.1 Analýza

Kapitola 1 popísala aktuálne problémy v učebni a jedným z nich bol výskyt duplicitných IP adries v sieti učebne. Práve teraz však nie je nasadený IP Source Guard, ktorý by situáciu dokázal vyriešiť, tak ako bolo popísané v 2.2. Učiteľ by však chcel mať i prehľad, ktoré zariadenie má nesprávnu IP adresu a bez prístupu na prepínač učebne to v riešení pomocou IP Source Guard nie je možné. Hoci nástroj nezabráni študentovi nastavenie duplicitnej adresy a ani ho o tom nijak neupozorní, učiteľ bude o tejto situácií oboznámený pri pohľade na spustený nástroj. Nasadenie je preto voči infraštruktúre učebne neinvazívne, pre správne fungovanie stačí aby bol nástroj nainštalovaný iba na jednom zariadení, na učiteľskej stanici. Žiadne zmeny v konfiguráciách prepínačov nie sú nutné. Ak by sa vyučujúci rozhodol nástroj nepoužívať, nemusí preto vypínať žiadne spustené služby ale len ho jednoducho vypne. Stratí tak informáciu o aktuálnom stave zariadení z pohľadu IP adries, takže sa dostáva naspäť do pôvodnej situácie, keď žiadny mechanizmus v učebni neexistoval.

Počas písanie práce a v neskorších fázach testovania nástroju v učebni bol objavený problém keď počítač s niekoľkými sieťovými kartami odpovedal na ARP dotazy týkajúce sa všetkých jeho IP adries na všetkých rozhraniach. Linux, narozdiel od iných systémov, berie IP adresu ako informáciu, ktorá patrí celému systému a nie konkrétnemu rozhraniu, aj napriek tomu, že IP adresa sa konfiguruje na konkrétnom rozhraní. V prípade, že počítač príjme na rozhraní ARP dotaz, kde Target Protocol Address je jednou z IP adries stroja, počítač odpovie, že danú adresu vlastní, hoci sa vôbec nenachádza na rozhraní, kde bol ARP dotaz prijatý.[54] Toto chovanie sa však dá zakázať nastavením premennej `ARP_IGNORE` na hodnotu 1. Po nastavení bude systém odpovedať na ARP dotazy iba v tom prípade, keď Target Protocol Address je lokálnou adresou prijatou na rozhraní.[55] Pre správne fungovanie nástroju je teda nutné nastaviť hodnotu `ARP_IGNORE` a to pomocou príkazu:

```
echo 'net.ipv4.conf.all.arp_ignore=1' >> /etc/sysctl.conf
```

3.2 Architektúra programu

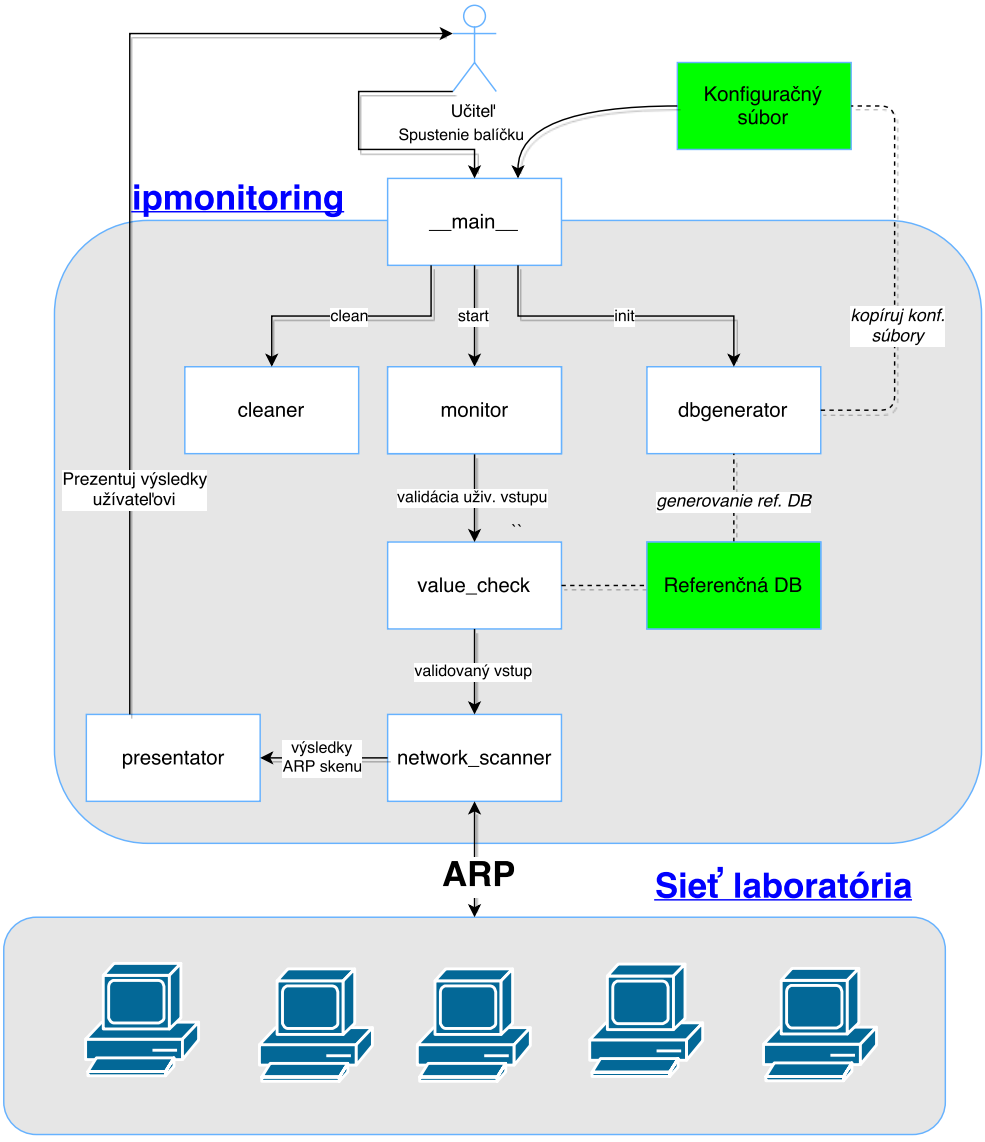
Program pre detekciu duplicitných IP adries využíva funkcionalitu ARP. Na každú IP adresu skenovanej podsiete je odoslaných ARP dotaz a všetky odpovede sú zachytené. Situáciu, kde na jeden ARP dotaz s konkrétnou IP adresou prišla od dvoch rôznych zariadení viac ako jedna odpoveď, vyhodnotí program ako duplicitnú IP adresu v sieti. Prípad, keď na ARP dotaz odpovie jedno zariadenie, nestačí na vyhodnotenie, či je stroj korektne nakonfigurovaný. Nástroj potrebuje referenčnú databázu vo formáte JSON, ktorý obsahuje správne dvojice `MAC adresa : IP adresa` a rovnako aj názvy zariadení v dvojiciach `MAC adresa : názov zariadenia`. Referenčná databáza otvára možnosť zistiť, či dané zariadenie IP adresu iného zariadenia, ktoré je zhodou okolností vypnuté. Rovnako tiež filtruje výsledok pre učiteľa, ktorého nezaujíma stav desiatok neodpovedaných adries, ktoré ani nie sú priradené žiadnemu zariadeniu. Odpadá tiež nutnosť hľadať zariadenie s konkrétnou MAC adresou pre ručnú kontrolu, keďže databáza obsahuje aj preklad MAC adries na zrozumiteľný názov zariadenia. Referenčná databáza je vygenerovaná pomocou skriptu, ktorý získa MAC adresy a priradí ich k správnym IP adresám podľa adresného plánu učebne. Rovnako zvládne vygenerovať i mená zariadení.

Užívateľ môže nastaviť parametre formou konfiguračného súboru alebo prepínačov na príkazovom riadku. Medzi nastaviteľné položky patrí interval skenovania, cesta k referenčnej databázy, skenované rozhranie, podsieť pre skenovanie a časový limit pre odpoveď na ARP dotaz. Pohľad na architektúru programu ilustruje obrázok 3.1

3.3 Implementácia

Program je napísaný v jazyku Python, vo verzii 3.4. Jedná sa o multiplatformový interpretovaný jazyk, šírený ako open-source. Tento jazyk som si pre implementáciu vybral, pretože s ním mám osobnú skúsenosť a má veľmi bohatú štandardnú knižnicu. Program využíva i externé knižnice, ktoré uľahčili vývoj.

Nástroj sa chová i inštaluje ako Python balíček a zároveň je pripravený na priame spustenie. Po spustení dochádza k spracovaniu užívateľského vstupu spolu s typovou kontrolou argumentov, ktoré zadal užívateľ. Možnosti užívateľského vstupu sa delia na dve časti. Prvou je určenie príkazu, ktorý chce užívateľ spustiť a druhou časťou sú predvoľby týkajúce se zvoleného podprogramu. Pod jedným balíčkom je teda možné spustiť viac podprogramov. Konfigurácia môže byť zadaná aj pomocou konfiguračného súboru spolu s kombináciou prepínačov na príkazovom riadku. O túto integráciu sa stará externá



Obr. 3.1: Architektúra programu

knižnica *ConfigArgParse*, ktorá vytvára jednotné rozhranie nad užívateľským vstupom z rôznych zdrojov ako konfiguračný súbor alebo argumenty príkazovej riadky.[56]. Príkazy dostupné pre užívateľa sú:

- init
- start
- clean

3.3.1 init

Tento podprogram má za úlohu vytvoriť referenčnú databázu, ktorá bude slúžiť pre nasledujúce skenovanie siete. Pre úspešné generovanie je nutné špecifikovať dôveryhodný zdrojový súbor vo formáte JSON. Tento súbor obsahuje zoznam adries, ktoré sa majú vyskytovať v sieti. V prípade, že skenovanie objaví adresu, ktorá nie je špecifikovaná alebo adresa v súbore nie je dostupná, program vyhlási chybu. Pre zaistenie správneho skenovania je nutné určite rozhranie, z ktorého budú ARP dotazy poslané a počet bitov v maske siete. Posledným nutným parametrom je mapovanie adries na názov zariadenia. To je využité pri zariadeniach, ktoré nie sú študentské počítače a majú unikátny identifikátor.

Program tiež vytvorí adresáre pre uloženie konfigurácie a rovnako sem pridá u ukážkový konfiguračný súbor pre skripty `start` a `init`.

3.3.2 start

Hlavná funkcionalita skenovania adries je obsiahnutá práve v tomto podprograme. Konečný výsledok zobrazenia aktuálneho stavu rozhraní v sieti je prácou troch modulov, `value_checker`, `network_scanner` a `presentator`.

`value_checker` je poslednou kontrolou užívateľského vstupu. Preveruje sa, či sú dodržané minimálne časy skenovania a intervalu alebo či skenovacie rozhranie má skutočne IP adresu zo skenovaného rozsahu. Ďalšiemu modulu sú už potom odoslané len údaje potrebné pre skenovanie, cesty k súborom špecifikované v konfigurácií sú odstránené.

Modul `network_scanner` vytvára a posiela ARP dotazy do siete. Pre vytváranie paketov je použitá externá knižnica *scapy* vo verzii určenej pre Python 3[57]. Odpovede sú spracované do slovníku, kde kľúčom je MAC adresa známa z referenčnej databázy a hodnotou je žiadna alebo niekoľko IP adries, ktoré boli súčasťou odpovede na ARP dotaz. Po získaní všetkých odpovedí je tento slovník predaný ďalšiemu modulu.

Posledný modul v podprograme je `presentator`. Jeho úlohou je zobrazenie výsledkov skenovanie užívateľovi tak, aby bolo na prvý pohľad jasné, kde sa

nachádza problémová konfigurácia. O vykreslenie sa stará knižnica *NCurses*, konkrétne modul *curses*, ktorý je súčasťou jazyka Python a ponúka tak natívne rozhranie nad knižnicou NCurses napísanou v jazyku C.[58] Užívateľovi sa zobrazia dvojice `<názov zariadenia> <STAV>`, kde `STAV` môže nadobudnúť tieto hodnoty:

- OK
- OFFLINE
- Duplicate with `<názov zariadenia>`
- Incorrect IP address on device. Should be `<správna IP adresa>`
- More than one IP found on interface. Should be only `<správna IP adresa>`

Stav *OK* nadobudne zariadenie, ak zdrojová MAC adresa a IP adresa v ARP odpovedi sú rovnaké ako v referenčnej databázi. Stav *OFFLINE* nastane ak MAC adresa sa neobjaví v žiadnej z ARP odpovedí. Ostatné stavy indikujú chybu v konfigurácií. *Duplicate with <názov zariadenia>* znamená, že počítač má rovnakú IP adresu ako ďalšie zariadenie v sieti a táto adresu mu podľa referenčnej databáze nepatrí. *Incorrect IP address on device. Should be <správna IP adresa>* nastane, ak dané zariadenie nemá správnu IP adresu podľa referenčnej databáze ale iba v tom prípade, že táto adresa je v sieti unikátna. Posledný stav popisuje situáciu, keď jedna MAC adresa odpovie na ARP dotaz viacerými unikátnymi adresami. Znamená to, že študent nastavil na rozhranie viac IP adries, čo nie je úplne štandardná situácia a mala by byť skontrolovaná.

3.3.3 clean

Úlohou podprogramu je odstrániť vytvorené adresáre a konfigurácie `init` skriptom. Toto je vhodné použiť pred odinštalovaním programu, keďže balíčkovací manažér nedokáže odstrániť tieto moduly sám. Užívateľ je počas spustenie informovaný, ktoré cesty sa mažú.

Záver

V práci som sa zaoberal analýzou súčasného stavu sieťovej učebne, návrhom siete nového sieťového laboratória, vylepšením toho súčasného a nakoniec i implementáciou nástroja pre detekciu chybnej konfigurácie sieťových rozhraní na počítačoch v učebni.

Analýzou boli objavené problémy ako výskyt duplicitných IP adries v učebni, chyby v konfigurácií systémových obrazov a i komunikácia, ktorá by mohla predstavovať bezpečnostné riziko. Návrh ideálnej učebne popísal koncept sieťového laboratória pre 24 študentov a zaoberal sa od usporiadania prvkov v rozvádzačoch až po adresáciu a služby daného laboratória. Návrh reálnej učebne schválne nezasahoval do finančného rozpočtu a priniesol podnet na zmeny v konfigurácií prvkov, ktoré sa tam súčasnej dobe nachádzajú. Zmeny vyplývali z analýzy súčasného stavu a poskytli riešenie objavených problémov. Návrh prebral i myšlienku nasadenia virtuálnych strojov v učebni z návrhu ideálnej učebne. Implementovaný nástroj úspešne detekuje duplicitné adresy v rámci nastaviteľného rozsahu a rozhrania. Dokáže upozorniť učiteľa na to, že stroj má nastavenú nesprávnu IP adresu na rozhraní, kde by študent nemal zasahovať. K identifikácií problémového stroja pomáha i zrozumiteľný názov, ktorý korešponduje s označením počítačov v učebni a je naviazaný na MAC adresu rozhrania daného počítača.

V budúcnosti by bolo možné nástroj rozšíriť o kontrolu IP konfigurácie rozhraní na sieťových prvkoch a pridaním grafického rozhrania pre zobrazovanie stavu, zmenu konfigurácie a generovanie referenčnej databázy. Návrhy učební sa nezaoberajú integráciou učebne do autentizačného schéma univerzity, vďaka čomu by študenti mohli byť aj v špeciálnych učebniach overovaný ako v produkčnej sieti. Túto problematiku a vytvorenie bezpečnostných politík by mohlo byť náplňou ďalšej práce.

Bibliografia

1. *CISCO den 10.5.2012*. Praha: Fakulta informačních technologií ČVUT, 2012. Dostupné tiež z: <http://fit.cvut.cz/akce/cisco>. [Online], [cit. 2016-05-10].
2. *Informatika pro nastupující v roce 2009 až 2014*. Praha: Fakulta informačních technologií ČVUT, 2009. Dostupné tiež z: <http://fit.cvut.cz/student/bakalarsky-program/informatika09_14>. [Online], [cit. 2016-9-16].
3. *Studijní obor Informační technologie (1802R007)*. Praha: Fakulta informačních technologií ČVUT, 2009. Dostupné tiež z: <http://fit.cvut.cz/student/bakalar/informacni-technologie>. [Online], [cit. 2016-9-16].
4. BURDETT, Arnold; BURKHARDT, Diana. *BCS glossary of computing and ICT*. 13th ed. Swindon [England]: BCS, 2013. ISBN 9781780171517. Dostupné tiež z: <http://site.ebrary.com/lib/techlib/detail.action?docID=10662629>. [Online], [cit. 2016-9-2].
5. *Cisco StackWise and StackWise Plus Technology*. San Jose (California): Cisco Systems, 2003. Dostupné tiež z: <http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3750-series-switches/prod_white_paper09186a00801b096a.html>. [Online], [cit. 2016-10-03].
6. *Web Proxy Auto-Discovery Protocol*. Internet Engineering Task Force(IETF), 1999. Dostupné tiež z: <https://tools.ietf.org/html/draft-ietf-wrec-wpad-01>. [Online], [cit. 2016-9-28].
7. *Understanding VLAN Trunk Protocol (VTP)*. San Jose (California): Cisco Systems, 2014. Dostupné tiež z: <http://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/10558-21.html>. [Online], [cit. 2016-10-18].

8. CCIEPURSUIT. *VTP MD5 Hash Utilizes VTP Domain Name*. 2007. Dostupné tiež z: <https://cciepursuit.wordpress.com/2007/06/29/vtp-md5-hash-utilizes-vtp-domain-name/>. [Online], [cit. 2016-10-18].

9. *Preboot Execution Environment*. San Francisco (CA): Wikimedia Foundation, 2001-. Dostupné tiež z: <https://en.wikipedia.org/w/index.php?title=Preboot_Execution_Environment%5C&oldid=739563064>. [Online], [cit. 2016-10-21].

10. *IP Multicast Technology Overview*. San Jose (California): Cisco Systems, 2002. Dostupné tiež z: <http://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/ip_multicast/White_papers/mcst_ovr.html>. [Online], [cit. 2016-10-21].

11. *Cisco Discovery Protocol Configuration Guide, Cisco IOS Release 15M&T*. San Jose (California): Cisco Systems, 2016. Dostupné tiež z: <http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cdp/configuration/15-mt/cdp-15-mt-book/nm-cdp-discover.html?referring_site=RE%5C&pos=1%5C&page=http://www.cisco.com/c/en/us/td/docs/ios/12_2/configfun/configuration/guide/ffun_c/fcf015.html>. [Online], [cit. 2016-9-27].

12. IEEE Standard for Local and metropolitan area networks - Station and Media Access Control Connectivity Discovery. *IEEE Std 802.1AB-2016 (Revision of IEEE Std 802.1AB-2009)*. 2016, s. 1–146. Dostupné z DOI: 10.1109/IEEESTD.2016.7433915. [Online], [cit. 2016-9-27].

13. *Psimulator2*. Praha: FIT ČVUT, 2015. Dostupné tiež z: <https://gitlab.fit.cvut.cz/psimulator2/Psimulator2>. [Online], [cit. 2016-10-29].

14. *Ns-3*. NS Community, 2011-2015. Dostupné tiež z: <https://www.nsnam.org/>. [Online], [cit. 2016-10-29].

15. *GNS3 | The software that empowers network professionals*. (Calgary): GNS3 Technologies, Inc., 2016. Dostupné tiež z: <https://www.gns3.com/>. [Online], [cit. 2016-10-28].

16. *Server Virtualization with VMware vSphere*. (Palo Alto): VMWare Inc., 2016. Dostupné tiež z: <http://www.vmware.com/products/vsphere.html>. [Online], [cit. 2016-10-28].

17. CAICEDO, Carlos E.; CERRONI, Walter. Design of a computer networking laboratory for efficient manageability and effective teaching. *2009 39th IEEE Frontiers in Education Conference*. 2009, s. 1–6. ISBN 978-1-4244-4715-2. Dostupné z DOI: 10.1109/FIE.2009.5350782.

18. *Rack*. San Francisco (CA): Wikimedia Foundation, 2001-. Dostupné tiež z: <https://sk.wikipedia.org/w/index.php?title=Rack%5C&oldid=6141534>. [Online], [cit. 2016-10-29].

19. *Define: EIA-310*. RackSolutions, 2007. Dostupné tiež z: <https://www.server-racks.com/eia-310.html>. [Online], [cit. 2016-10-29].

20. MAREK, Jakub; SKŘEHOT, Petr. *Základy aplikované ergonomie*. Vyd. 1. Praha: VÚBP, 2009. ISBN 9788086973586.

21. REILLY, Edwin D. *Concise encyclopedia of computer science*. Chichester: Wiley, 2004. ISBN 0470090952.

22. STERBENZ, James P. G.; HUTCHISON, David; ÇETINKAYA, Egemen K.; JABBAR, Abdul; ROHRER, Justin P.; SCHÖLLER, Marcus; SMITH, Paul. Redundancy, diversity, and connectivity to achieve multilevel network resilience, survivability, and disruption tolerance invited paper. *Telecommunication Systems* [online]. 2014, roč. 56, č. 1, s. 17–31 [cit. 2016-06-30]. ISSN 1018-4864, 1572-9451. ISSN 1018-4864, 1572-9451. Dostupné z DOI: 10.1007/s11235-013-9816-9.

23. *Out-of-band management*. San Francisco (CA): Wikimedia Foundation, 2001-. Dostupné tiež z: <https://en.wikipedia.org/w/index.php?title=Out-of-band_management%5C&oldid=751704929>. [Online], [cit. 2016-12-9].

24. IEEE Standard for Local and metropolitan area networks–Bridges and Bridged Networks. *IEEE Std 802.1Q-2014 (Revision of IEEE Std 802.1Q-2011)*. 2014, s. 1–1832. Dostupné z DOI: 10.1109/IEEESTD.2014.6991462. [Online], [cit. 2016-6-28].

25. POSTEL, Jon. *Internet Protocol* [Internet Requests for Comments]. RFC Editor, 1981. ISSN 2070-1721. Dostupné tiež z: <http://www.rfc-editor.org/rfc/rfc791.txt>. STD. RFC Editor. [Online], [cit. 2016-7-20].

26. *Broadcast radiation*. San Francisco (CA): Wikimedia Foundation, 2001-. Dostupné tiež z: <https://en.wikipedia.org/w/index.php?title=Broadcast_radiation%5C&oldid=750242286>. [Online], [cit. 2016-12-9].

27. IEEE Standard for Local and metropolitan area networks: Media Access Control (MAC) Bridges. *IEEE Std 802.1D-2004 (Revision of IEEE Std 802.1D-1998)*. 2004, s. 1–277. Dostupné z DOI: 10.1109/IEEESTD.2004.94569. [Online], [cit. 2016-7-20].

28. *Understanding Rapid Spanning Tree Protocol (802.1w)*. San Jose (California): Cisco Systems, 2006. Dostupné tiež z: <http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/24062-146.html>. [Online], [cit. 2016-8-26].

29. *Catalyst 3560 Switch Software Configuration Guide, Cisco IOS Release 15.0(2)SE and Later: Configuring STP [Cisco Catalyst 3560 Series Switches]*. San Jose (California): Cisco Systems, 2016. [Online], [cit. 2016-8-26].

30. IEEE Standard for Local and metropolitan area networks – Link Aggregation. *IEEE Std 802.1AX-2014 (Revision of IEEE Std 802.1AX-2008)*. 2014, s. 1–344. Dostupné z DOI: 10.1109/IEEESTD.2014.7055197. [Online], [cit. 2016-9-1].

31. *Cisco EtherChannel Technology*. San Jose (California): Cisco Systems, 2006. Dostupné tiež z: <http://www.cisco.com/en/US/tech/tk389/tk213/technologies_white_paper09186a0080092944.shtml> [Online], [cit. 2016-9-3].

32. *Implementing EtherChannel in a Switched Network*. Indianapolis: Cisco Press, 2015. Dostupné tiež z: <http://www.ciscopress.com/articles/article.asp?p=2348266%5C&seqNum=3> [Online], [cit. 2016-9-2].

33. *Catalyst 3560 Switch Software Configuration Guide, Cisco IOS Release 15.0(2)SE and Later: Chapter: Configuring DHCP Features and IP Source Guard*. San Jose (California): Cisco Systems. Dostupné tiež z: <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/15-0_2_se/configuration/guide/scg3560/swdhcp82.html>. [Online], [cit. 2016-12-9].

34. PLUMMER, David C. *Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware* [Internet Requests for Comments]. RFC Editor, 1982. ISSN 2070-1721. Dostupné tiež z: <http://www.rfc-editor.org/rfc/rfc826.txt>. STD. RFC Editor. [Online], [cit. 2016-12-9].

35. *Catalyst 3560 Switch Software Configuration Guide, Cisco IOS Release 15.0(2)SE and Later: Chapter: Configuring Dynamic ARP Inspection*. San Jose (California): Cisco Systems. Dostupné tiež z: <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/15-0_2_se/configuration/guide/scg3560/swdynarp.html>. [Online], [cit. 2016-12-9].

36. SMITH, Lucie; LIPNER, Ian. *Free Pool of IPv4 Address Space Depleted*. The Number Resource Organization, 2011. Dostupné tiež z: <https://www.nro.net/news/ipv4-free-pool-depleted> [Online], [cit. 2016-9-3].

37. REKHTER, Yakov; MOSKOWITZ, Bob; KARRENBERG, Daniel; GROOT, Geert Jan de; LEAR, Eliot. *Address allocation for private internets*. 1996. Dostupné tiež z: <https://tools.ietf.org/html/rfc1918>. Technická správa. [Online], [cit. 2016-9-11].

38. SRISURESH, Pyda; EGEVANG, Kjeld. *Traditional IP network address translator (Traditional NAT)*. 2000. Dostupné tiež z: <https://www.rfc-editor.org/rfc/rfc3022.txt>. Technická správa. [Online], [cit. 2016-9-11].

39. HINDEN, Robert M; DEERING, Stephen E. *IP version 6 addressing architecture*. The Internet Society, 2006. Dostupné tiež z: <https://tools.ietf.org/html/rfc4291> [Online], [cit. 2016-9-11].

40. NORDMARK, Erik; GILLIGAN, Robert. Basic transition mechanisms for IPv6 hosts and routers. 2005. Dostupné tiež z: <https://tools.ietf.org/html/rfc4213>. [Online], [cit. 2016-9-3].

41. HUSTON, G.; LORD, A.; SMITH, P. *IPv6 Address Prefix Reserved for Documentation* [Internet Requests for Comments]. RFC Editor, 2004. ISSN 2070-1721. Dostupné tiež z: <https://www.rfc-editor.org/rfc/rfc3849.txt>. RFC. RFC Editor. [Online], [cit. 2016-10-25].

42. DROMS, Ralph. *Dynamic Host Configuration Protocol* [Internet Requests for Comments]. RFC Editor, 1997. ISSN 2070-1721. Dostupné tiež z: <http://www.rfc-editor.org/rfc/rfc2131.txt>. RFC. RFC Editor. [Online], [cit. 2016-10-24].

43. THOMSON, S.; NARTEN, T.; JINMEI, T. *IPv6 Stateless Address Autoconfiguration* [Internet Requests for Comments]. RFC Editor, 2007. ISSN 2070-1721. Dostupné tiež z: <http://www.rfc-editor.org/rfc/rfc4862.txt>. RFC. RFC Editor. [Online], [cit. 2016-10-25].

44. DROMS, R.; BOUND, J.; VOLZ, B.; LEMON, T.; PERKINS, C.; CARNEY, M. *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)* [Internet Requests for Comments]. RFC Editor, 2003. ISSN 2070-1721. Dostupné tiež z: <http://www.rfc-editor.org/rfc/rfc3315.txt>. RFC. RFC Editor. [Online], [cit. 2016-10-25].

45. *IP address management*. San Francisco (CA): Wikimedia Foundation, 2001-. Dostupné tiež z: <https://en.wikipedia.org/w/index.php?title=IP_address_management%5C&oldid=745324305>. [Online], [cit. 2016-10-25].

46. GRAZIANO, Charles David. *A performance analysis of Xen and KVM hypervisors for hosting the Xen Worlds Project*. Iowa State University, 2011. Dostupné tiež z: <http://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=3243&context=etd>. [Online], [cit. 2016-10-26].

47. KENT, S. *IP Encapsulating Security Payload (ESP)* [Internet Requests for Comments]. RFC Editor, 2005. ISSN 2070-1721. Dostupné tiež z: <http://www.rfc-editor.org/rfc/rfc4303.txt>. RFC. RFC Editor. [Online], [cit. 2016-10-29].

48. MAUGHAN, Douglas; SCHNEIDER, Mark; SCHERTLER, Mark. *Internet Security Association and Key Management Protocol (ISAKMP)* [Internet Requests for Comments]. RFC Editor, 1998. ISSN 2070-1721. Dostupné tiež z: <http://www.rfc-editor.org/rfc/rfc2408.txt>. RFC. RFC Editor. [Online], [cit. 2016-10-29].

49. *OpenSSL*. 1999-2016. Dostupné tiež z: <https://www.openssl.org/>. [Online], [cit. 2016-10-29].

50. *What is OpenVPN?* (Pleasanton): OpenVPN Technologies, Inc., 2016. Dostupné tiež z: <https://openvpn.net/index.php/open-source/333-what-is-openvpn.html>. [Online], [cit. 2016-10-29].

51. *Cisco IOS Software Packaging and Licensing White Paper*. San Jose (California): Cisco Systems, 2016. Dostupné tiež z: <http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3560-x-series-switches/white_paper_c11-579326.html>. [Online], [cit. 2016-10-29].

52. *Vagrant by HashiCorp*. San Francisco: HashiCorp. Dostupné tiež z: <https://www.vagrantup.com/>. [Online], [cit. 2016-10-29].

53. *Oracle VM VirtualBox*. Redwood Shores (California): Oracle Corporation. Dostupné tiež z: <https://www.virtualbox.org/>. [Online], [cit. 2016-10-29].

54. BENVENUTI, Christian. *Understanding Linux network internals*. Sebastapol, CA: O'Reilly, 2006. ISBN 0596002556.

55. */proc/sys/net/ipv4/* Variables:* California: The Linux Kernel Organization, 2002. Dostupné tiež z: <https://www.kernel.org/doc/Documentation/networking/ip-sysctl.txt>. [Online], [cit. 2016-11-27].

56. BW2. *ConfigArgParse*. 2016. Dostupné tiež z: <https://github.com/bw2/ConfigArgParse>. [software].

57. DOBELIS, Eriks. *scapy for python3 (aka scapy3k)*. 2016. Dostupné tiež z: <https://github.com/phaethon/scapy>. [software].

58. *Curses — Terminal handling for character-cell displays*. Python Software Foundation, 2001-2016. Dostupné tiež z: <https://docs.python.org/3.4/library/curses.html>. [Online], [cit. 2016-11-21].

Dodatok **A**

Zoznam použitých skratiek

SNMPv3 Simple Network Management Protocol version 3

LAN Local Area Network

FIT Fakulta Informačných Technológií

ČVUT České Vysoké Učení Technické

SSH Secure Shell

PoE Power over Ethernet

ASA Adaptive Security Appliance

ISR Integrated Services Router

VLAN virtual LAN

STP Spanning Tree Protocol

RSTP Rapid Spanning Tree Protocol

ARP Address Resolution Protocol

DHCP Dynamic Host Configuration Protocol

IEEE Institute of Electrical and Electronics Engineers

IP Internet Protocol

IPv4 Internet Protocol verzia 4

IPv6 Internet Protocol verzia 6

RFC Request for Comments

DHCPv4 Dynamic Host Configuration Protocol version 4

DHCPv6 Dynamic Host Configuration Protocol version 6

VPN Virtual Private Network

IPSec Internet Protocol Security

ESP Encapsulating Security Payload

SA Security Assosiation

ISAKMP Internet Security Assosiations and Key Management Protokol

SLAAC Stateless Address Autoconfiguration

Dodatok B

Príručka použitia nástroju pre monitorovanie učebne

B.1 Systémové požiadavky

Pre inštaláciu nástroju je nutné mať v systéme nainštalované tieto balíčky:

- Python verzia 3.4
- python3-venv

Je vhodné pre každú Python aplikáciu vytvoriť separátne virtuálne prostredie pomocou *python3-venv*, ktoré zaistí, že závislosti budú od jednotlivých aplikácií izolované. Nemôže sa potom stať, že aktualizácia balíčku používaného v inom projekte by znefunkčnila inú aplikáciu, ktorá potrebuje staršiu verziu.

Nástroj sám o sebe používa nasledujúce externé knižnice. Počas inštalácie budú nainštalované ako závislosť do vytvoreného virtuálneho prostredia:

- scapy-python3 >= 0.18 (testované na 0.18)
- netifaces >= 0.10.5 (testované na 0.10.5)
- configargparse >= 0.11.0 (testované na 0.11.0)

B.2 Inštalácia

O inštaláciu nástroju sa stará balíčkovací manažér *pip3*, ktorý je už pripravený vo virtuálnom prostredí. Celý postup inštalácie nástroju je popísaný v nasledujúcich krokoch.

1. Funkčnosť pripojenia k Internetu je v učebni závislá na nastavení proxy serveru. Nastavením premenných prostredia `http_proxy` a `https_proxy` na hodnotu:

```
http://<meno užívateľa>:<poč. systémové heslo>@10.0.1.13:3128
```

je dosiahnuté správne fungovanie programov *apt-get* a *pip3*.

2. Inštalácia systémovej závislosti *python3-venv* sa vykoná príkazom:

```
apt-get install python3.4-venv
```

3. Vytvorenie nového virtuálneho prostredia pomocou príkazu

```
python3 -m venv <nazov virt. prostredia>
```

4. Balíčkovacím manažérom *pip3* z virtuálneho prostredia sa nainštaluje balíček *ipmonitoring* príkazom:

```
<nazov virt. prostredia>/bin/pip3 install ipmonitoring-1.0.0.tar.gz
```

Ten stiahne do virtuálneho prostredia všetky závislosti a po inštalácií je možné spustiť balíček interpreterom virtuálneho prostredia príkazom

```
<nazov virt. prostredia>/bin/python -m ipmonitoring
```

B.3 Použitie

B.3.1 Vygenerovanie referenčnej databázy

Prvým spustením je potrebné vytvoriť referenčnú databázu pomocou podprogramu `init`. Generátor predpokladá naplnený súbor s dôveryhodnou databázou, ktorý je v pôvodnom nastavení uložený v inštalačnom adresári balíčka v sekcii `configuration/trusted_IPs.json`. Cestu k referenčnej databázi je možné zadať i z príkazovej riadky pomocou prepínaču `--trusted_db_path`. Všetky adresy uvedené v dôveryhodnej databázy musia byť v momente generovania dostupné. Prepínačom `--db_name` je možné vybrať názov referenčnej databázy, v prípade konfliktu názvov bude pôvodný súbor prepísaný novým.

Ak už je referenčnú databázu vytvorená, nie je nutné ju generovať pred každým spustením. Je však nutné ju spustiť ak dôjde k výmene počítačov, resp. sieťových kariet.

B.3.2 Spustenie a ukončenie programu

Spustenie monitorovania, v prípade inštalácie vo virtuálnom prostredí, je možné príkazom:

```
<názov virt. prostredia>/bin/python3 -m ipmonitoring start
```

Vyžadované sú práva superužívateľa, kvôli knižnici *scapy*, ktorá pracuje so sieťovými rozhraniami. Pre ukončenie programu je nutné vyslať signál prerušenia `SIGINT` kombináciou kláves `Ctrl+C`

B.3.3 Zmena východzích hodnôt programu

Spustením podprogramu `init` sa vytvoria v domovskom adresári užívateľa resp. v `/etc` adresáre `.ipmonitoring/` resp. `ipmonitoring/` spolu s ukážkami konfiguračných súborov pre podprogramy `init` a `start`. Slúžia ako základ pre definíciu vlastných konfiguračných súborov, ktoré potom užívateľ pre použitie špecifikuje na príkazovom riadku pomocou prepínaču `--config`. Ukážka konfiguračných súborov pre podprogram `start` resp. `init` je v B.1 resp. B.2.

```
# This is sample default configuration. Uncomment lines to change it

#[db]
# Path to generated database
# db_path = /etc/ipmonitoring/address_db

#[scan_settings]
# How often should new scan be executed in seconds
# scan_interval = 5

# What interface should be user
# scan_interface = eth0

# How many second should scanner wait for reply
# scan_timeout = 1

# What subnet will be scanned
# scan_subnet = 10.3.44.0/24
```

Listing B.1: Východzí konfiguračný súbor scanner.default.conf

```
# This is sample default configuration. Uncomment lines to change it.

# Location of trusted IPs source
# trusted_db_path = /etc/ipmonitoring/trusted_IPs.json
```

```
    # Location of reference database
    # configuration_path = /etc/ipmonitoring/

    # Name of the database
    # db_name = address_db
```

Listing B.2: Východzí konfiguračný súbor generator.default.conf

Zdrojový súbor dôveryhodných adries je vo formáte JSON. Ukážka tohto súboru, s ktorým pracuje generátor je v B.3

```
{
    "trusted_ips":  ['10.3.44.1',   '10.3.44.12',   '10.3.44.100',
                     '10.3.44.101',  '10.3.44.102',  '10.3.44.103',
                     '10.3.44.104',  '10.3.44.105',  '10.3.44.106',
                     '10.3.44.107',  '10.3.44.108',  '10.3.44.109',
                     '10.3.44.110',  '10.3.44.111',  '10.3.44.112',
                     '10.3.44.113',  '10.3.44.114',  '10.3.44.115',
                     '10.3.44.116',  '10.3.44.117',  '10.3.44.118',
                     '10.3.44.119',  '10.3.44.120',  '10.3.44.121',
                     '10.3.44.122',  '10.3.44.123',  '10.3.44.124'  ],
    "subnet_size": 24,
    "scan_interface": "eth1",
    "known_names": {
        "10.3.44.100":  "teacher-pc",
        "10.3.44.1":  "gateway",
        "10.3.44.12":  "server"
        }
}
```

Listing B.3: Zdrojový súbor s dôveryhodnými adresami pre generovanie databáze

B.3.4 Nastavenie parametrov z príkazovej riadky

Sekcia prináša referenčný zoznam dostupných prepínačov všetkých troch podprogramov. Všetky možnosti majú ekvivalent v konfiguračnom súbore. B.4 resp. B.5 zobrazujú časť výpisu po zavolaní pomocníka podprogramov `init` resp. `start`.

```
usage: ipmonitoring init  [-h] [-c CONFIG_FILE]
[--trusted_db_path TRUSTED_DB_PATH]
[--configuration_path CONFIGURATION_PATH]
[--db_name DB_NAME]
```

```
optional arguments:
−h, −−help
        show this help message and exit
−c CONFIG_FILE, −−config CONFIG_FILE
        config file path
−−trusted_db_path TRUSTED_DB_PATH
        Path to Trusted DB.
−−configuration_path CONFIGURATION_PATH
        Path where DB will be created
−−db_name DB_NAME
        Name of generated database.
```

Listing B.4: Pomocník ipmonitoring init

```
usage: ipmonitoring start [−h] [−c CONFIG_FILE] [−−db_path
    DB_PATH]
[−−scan_interval SCAN_INTERVAL]
[−−scan_interface SCAN_INTERFACE]
[−−scan_timeout SCAN_TIMEOUT]
[−−scan_subnet SCAN_SUBNET]

optional arguments:
−h, −−help
        show this help message and exit
−c CONFIG_FILE, −−config CONFIG_FILE
        config file path
−−db_path DB_PATH
        Path to MAC−IP JSON database
−−scan_interval SCAN_INTERVAL
        Seconds between period scans
−−scan_interface SCAN_INTERFACE
        Interface used for scanning
−−scan_timeout SCAN_TIMEOUT
        Seconds to wait for reply
−−scan_subnet SCAN_SUBNET
        Subnet to scan
```

Listing B.5: Pomocník ipmonitoring start

Dodatok C

Obsah priloženého CD

- `readme.txt` ..... stručný popis obsahu CD
- `src`
  - `impl` ..... zdrojové kódy implementácie
    - `ipmonitoring` ..... zdrojový kód balíčku nástroju
      - `backend` ..... zdrojový kód balíčku so sieťovým skenerom
        - `__init__.py`
        - `exceptions.py`
        - `network_scanner.py`
      - `configuration` ..... východzie konfiguračné súbory
        - `generator.default.conf`
        - `scanner.default.conf`
        - `trusted_IPs.json`
      - `frontend` .... zdroj. kód spracovanie vstupu a výstupu pre uživ.
        - `__init__.py`
        - `presentator.py`
        - `value_checker.py`
      - `tests` ..... unit testy modulov v backend a frontend
        - `unittest_test_backend.py`
        - `unittest_test_frontend.py`
        - `unittest_test_presentation.py`
      - `utils` ..... balíček jednotlivých podprogramov
        - `__init__.py`
        - `cleaner.py`
        - `dbgenerator.py`
        - `monitoring.py`
      - `__init__.py`
      - `__main__.py` ..... zdroj. kód balíčku, určenému k spusteniu.
    - `setup.py` ..... modul pre vytvorenie inštalačného balíčku
  - `thesis` ..... zdrojová forma práce vo formáte LaTeX
    - `pictures` ..... obrázky použité v práci
- `text` ..... text práce
  - `BP_Nagy_Lukas_2016.pdf` ..... text práce vo formáte PDF