Analýza a návrh modernizace počítačové sítě na FAI UTB ve Zlíně

Analysis and redesign of computer network of FAI TBU in Zlin

Petr Kohout

Diplomová práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Petr KOHOUT**
Osobní číslo:	**A08404**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Téma práce:	**Analýza a návrh modernizace počítačové sítě na FAI UTB ve Zlíně**

Zásady pro vypracování:

1. **Analyzujte současný stav počítačové sítě na FAI UTB ve Zlíně.**
2. **Navrhněte modernizaci aktivních prvků sítě.**
3. **Navrhněte možnosti konfigurace aktivních prvků sítě.**
4. **Zohledněte bezpečnost, zabezpečení, jednoduchost správy.**
5. **Proveďte dílčí realizaci.**
6. **Připravte podklady tak, aby mohly být použity v žádostech pro získání dotací.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **Cisco Systems, Inc.. Catalyst 2950 Desktop Switch Software Configuration Guide [online]. c2010 [cit. 2010-02-01]. Dostupný z WWW: http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_9_ea1/co**
2. **Cisco Systems, Inc.. Catalyst 2960 Switch Software Configuration Guide [online]. c2010 [cit. 2010-02-01]. Dostupný z WWW: http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_25_see/c**
3. **Cisco Systems, Inc.. Catalyst 3550 Multilayer Switch Software Configuration Guide [online]. c2010 [cit. 2010-02-01]. Dostupný z WWW: http://www.cisco.com/en/US/docs/switches/lan/catalyst3550/software/release/12.2_25_see/c**
4. **Cisco Systems, Inc.. Catalyst 3560 Switch Software Configuration Guide [online]. c2010 [cit.2010-02-01]. Dostupný z WWW: http://www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/12.2_25_se/co**
5. **DUBEC, Michal. LAN bezpečnost a ověřování identity [online]. [2007], Last-Modified: Thu, 16 Aug 2007 11:03:05 GMT [cit. 2010-02-01]. Dostupný z WWW: http://www.alefnula.cz/downloads/KC/KC-identita.pdf.**
6. **Internet Systems Consortium. ISC DHCP Documentation, Mailing Lists, FAQ [online]. c2001-2009 [cit. 2919-02-01]. Text v angličtině. Dostupný z WWW: https://www.isc.org/software/dhcp/documentation.**
7. **MILLER, Kevin C.. ISC DHCP Server -- Failover Docs [online]. 2003 [cit. 2010-02-01]. Text v angličtině. Dostupný z WWW: http://www.jny.dk/?q=node/10.**

Vedoucí diplomové práce: **doc. Ing. Martin Sysel, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání diplomové práce: **19. února 2010**

Termín odevzdání diplomové práce: **8. června 2010**

Ve Zlíně dne 19. února 2010

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

prof. Ing. Vladimír Vašek, CSc.
ředitel ústavu

ABSTRAKT

Tato diplomová práce popisuje zavedení nových technologií v počítačové síti FAI UTB a jejich možné nasazení v dalších částech univerzity.

V teoretické části jsou zmíněny základní principy a výhody nového řešení sítě, a to z hlediska bezpečnosti, datové propustnosti, redundance a možného praktického využití.

Praktická část pak ukazuje využitelnost nové sítě v praxi pomocí reálného nasazení některých nových projektů, např. vzdáleného bootování nebo částečného omezování síťového provozu.

Klíčová slova: síť, přepínač, směrovač, přístupová práva, DHCP

ABSTRACT

This thesis describes implementation of new technologies in the computer network of FAI TBU and the possibilities of expansion to other university objects.

Theoretical part contains basic principles and advantages of new network solution, with respect to security, data throughput, redundancy and possible practical use.

Practical part is about usability of the new network in praxis - implementation of new projects, e.g. remote booting or partially limitation of network traffic.

Keywords: network, switch, router, access list, DHCP

Děkuji doc. Ing. Martinu Syslovi, Ph.D. za cenné náměty, připomínky a formulování požadavků na fungování celé sítě FAI UTB ve Zlíně.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- jsem byl jsem seznámen s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo - diplomovou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze dipl. práce a verze elektronická nahraná do IS/STAG jsou totožné.

V Uherském Hradišti, 2. června 2010

.....

Podpis diplomanta

Obsah

Část I
ÚVOD

Počítačová síť na FAI UTB ve Zlíně se fyzicky nachází pouze v budově U5 a je připojena optickým spojem k další infrastruktuře UTB v budově U1. Tento stav trvá od dostavění budovy U5 a začátku jejího užívání, zhruba od roku 2004. Od základního zprovoznění sítě nebyly formulovány žádné speciální požadavky na chod sítě, kromě samozřejmého požadavku na spolehlivý provoz.

Po několikaletém používání sítě ovšem vznikají první požadavky na lepší funkčnost, především směrem k vyšší rychlosti, omezování přístupu některých stanic a uživatelů k síti, odstraňování parazitního provozu na síti, dělení sítě na menší jednotky a další. Původní jednoduchá infrastruktura sítě celé UTB spolu se staršími síťovými prvky ale neumožňuje tyto nové požadavky realizovat, proto je třeba vytvořit analýzu současného stavu a navrhnout modernizaci.

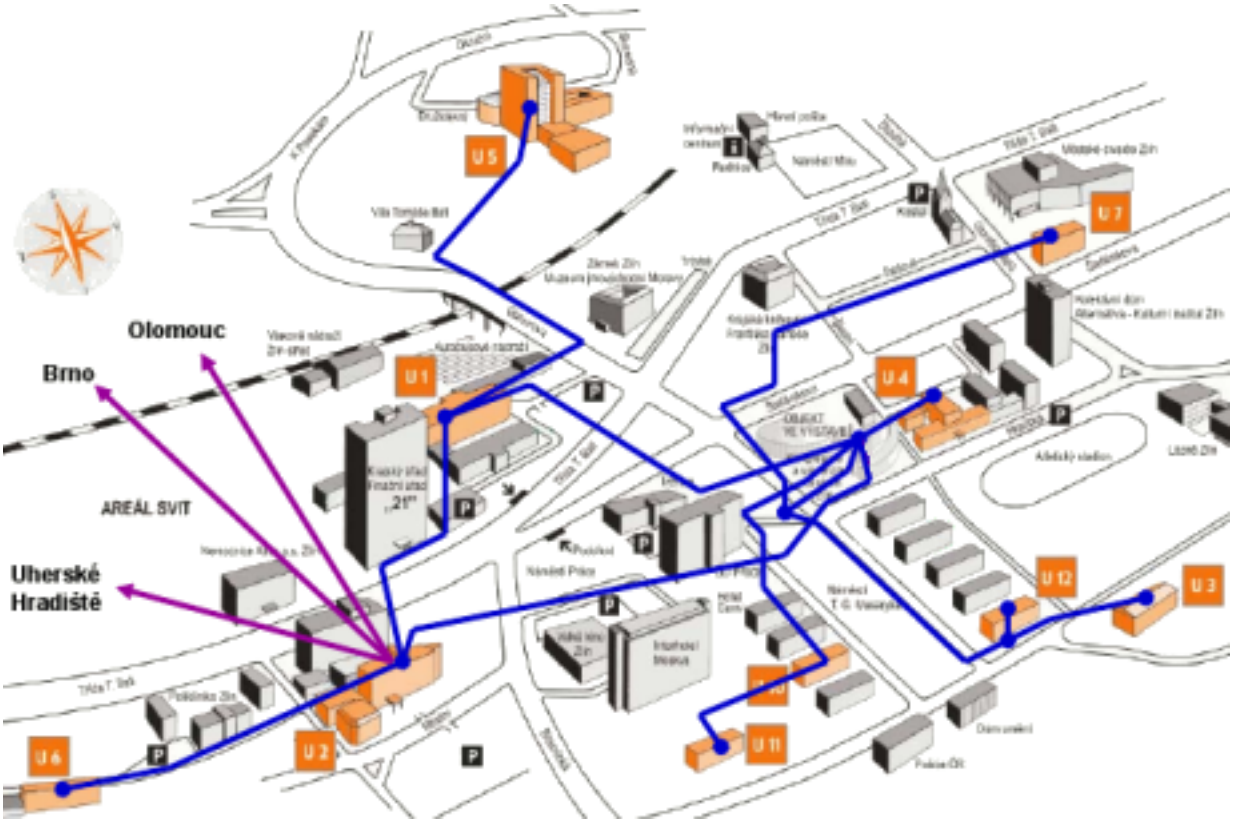
Cílem této práce je navrhnout modernizaci jak fyzické, tak logické struktury celé počítačové sítě na Fakultě aplikované informatiky, tj. sítě v budově U5, aby nové řešení vyhovovalo všem požadavkům jak současným, tak i takovým, které by se mohly objevit v budoucnu. Nové řešení by mělo být snadno aplikovatelné i na další subjekty v rámci UTB, ať už na celé fakulty nebo jiné logické celky (např. budovy nebo orgány fakulty).

Část II
TEORETICKÁ ČÁST

1 Analýza současného stavu sítě

1.1 Páteřní síť UTB ve Zlíně

Celá počítačová síť UTB ve Zlíně (dále jen UTB) je rozmístěna v několika budovách ve Zlíně a dokonce v několika budovách v jiných městech, např. v Uherském Hradišti nebo Přerově. Budova Fakulty aplikované informatiky U5 je propojena s budouvou U1, spoj je realizován pomocí 20 optických vláken (8x single mode, 12x multi mode), využita je zatím ovšem jen jedna dvojice vláken zajišťující jedno full-duplexní připojení celé budovy U5 k páteřní síti UTB a dále k internetu (prostřednictvím sítě firmy Cesnet z.s.p.o.).

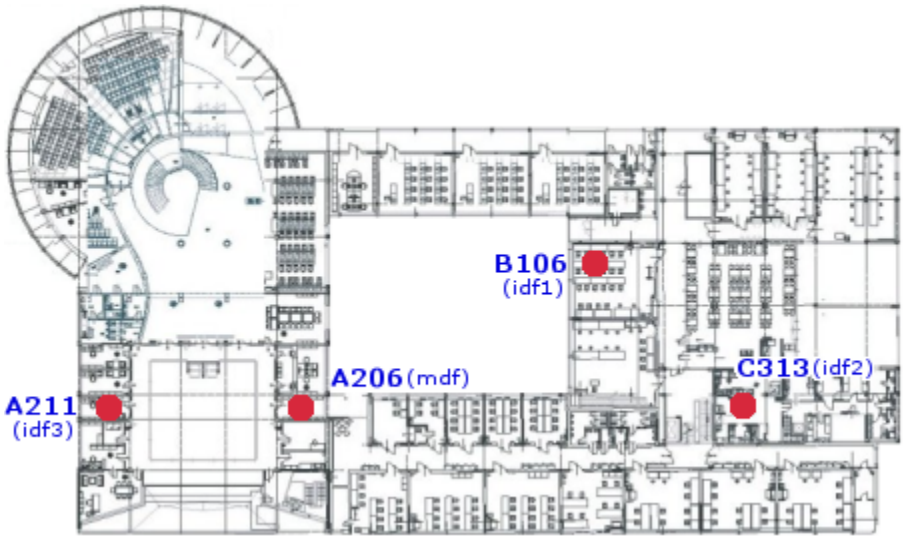


Obrázek 1: Optická síť UTB ve Zlíně. Optické spoje jsou vyznačeny modrou čarou, uzly kolečkem. Fialová barva značí připojení sítě k internetu a částem UTB mimo Zlín.

1.2 Rozvodny v budově U5

Rozvodny jsou obvykle malé místnosti, které slouží jako páteřní spojové uzly počítačové sítě v rámci budovy. Veškeré kabely, které spojují jednotlivé připojené stanice k dalším částem sítě, jsou zakončeny v těchto rozvodnách - konkrétně jsou zde pak zapojeny do

aktivních prvků sítě, ty pak umožňují připojeným stanicím komunikovat mezi sebou i směrem do internetu. V budově U5 se nachází celkem 4 rozvodny - po dvou v západní části budovy a po dvou ve východní, jak ukazuje mapka:

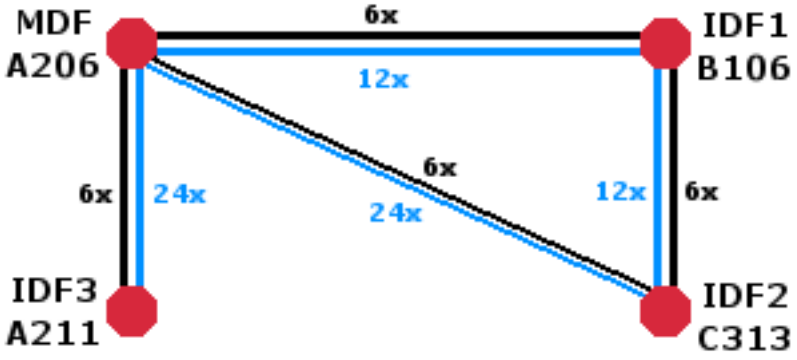


Obrázek 2: Rozmístění rozvoden v budově U5

Hlavní rozvodna je v místnosti A206 (je označována také jako *MDF*[1]), sem jsou vyvedena optická vlákna spojující budovu U5 s budovou U1. Ostatní rozvodny jsou v místnostech B106, C313 a A211 (označované jako *IDF*[2], resp. *IDF1*, *IDF2* a *IDF3*).

Jednotlivé IDF rozvodny jsou spojeny optickou i metalickou kabeláží přímo s hlavní rozvodnou MDF, navíc rozvodny IDF1 a IDF2 mají vlastní propoj. Metalické kabely jsou označeny jako **CAT6**[3], jejich propustnost je tedy 1 $Gb.s^{-1}$ v režimu full-duplex. Optické kabely mají stejnou propustnost, ovšem je třeba brát v úvahu, že pro vytvoření full-duplex spojení je nutné použít 2 optická vlákna. Počet kabelů v jednotlivých spojích je vidět z následujícího obrázku:

[1] z angl. Main Distribution Frame - hlavní rozvodna
[2] z angl. Intermediate Distribution Frame - mezilehlá rozvodna
[3] dle specifikací ANSI/TIA-568-B.2-1



Obrázek 3: Kabeláž mezi rozvodnami v budově U5, optická vlákna jsou značena světle modře, metalické kabely jsou značeny černou barvou, čísla ukazují počet spojů

Z uvedeného obrázku tedy vyplývá, že např. mezi IDF1 a IDF2 lze vytvořit nejvýše 6 full-duplex optických propojů a stejný počet metalických. Z existujících propojů mezi jednotlivými rozvodnami se ovšem k reálnému provozu využívají pouze optické propoje MDF-IDF1, MDF-IDF2 a MDF-IDF3, u všech je využita pouze jedna dvojice optických vláken. Tímto zapojením je de facto nastavena propustnost páteřní sítě U5 na 1 $Gb.s^{-1}$.

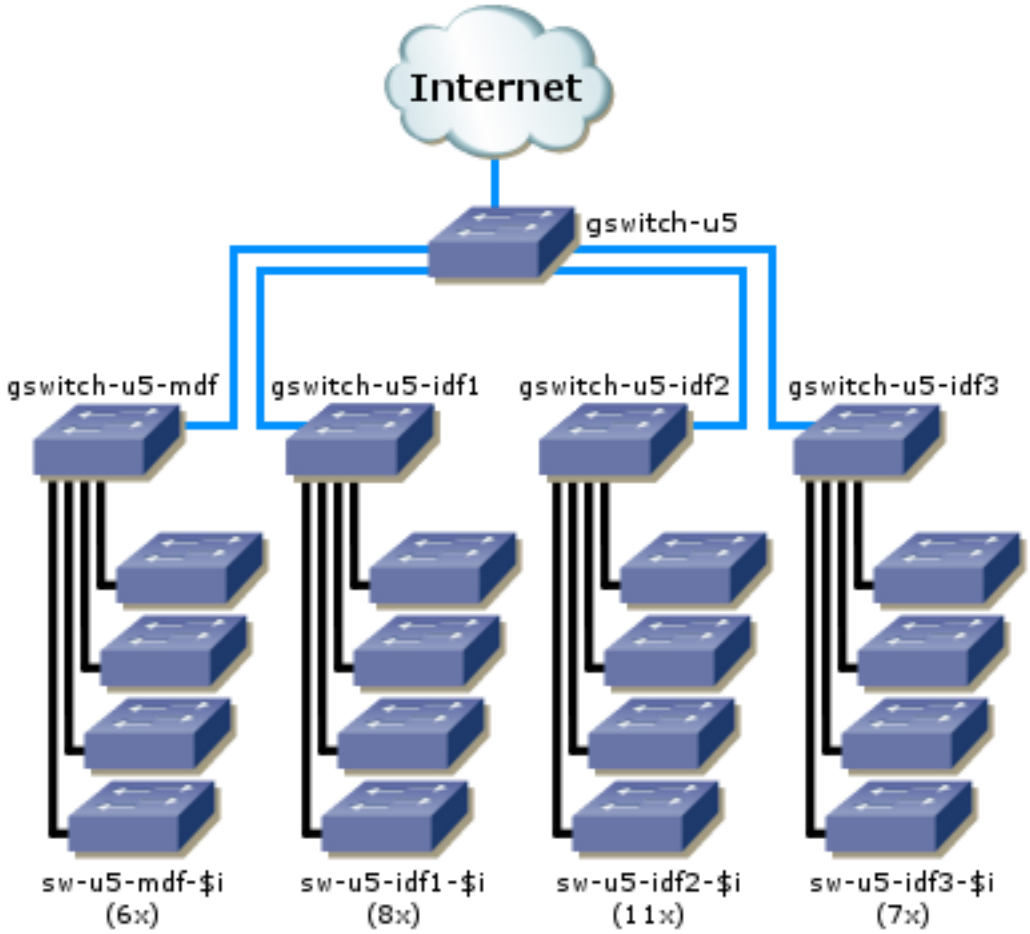
1.3 Hlavní páteřní přepínač

Hlavní páteřní přepínač, který slouží pouze jako propojovací jednotka mezi jednotlivými rozvodnami a internetem, se nachází v hlavní rozvodně MDF, konkrétně se jedná o zařízení `Cisco 3508G-XL`, které má 8 portů o rychlosti 1 $Gb.s^{-1}$ a díky media konvertorům do nich lze zapojit buď dvojici optických kabelů nebo jeden metalický kabel. Tento přepínač má administrativní označení **gswitch-u5**.

Do prvního portu tohoto přepínače je připojen optický spoj do internetu, do dalších 4 portů jsou pak optickými spoji připojeny hlavní páteřní přepínače v jednotlivých rozvodnách.

1.4 Aktivní prvky v rozvodnách

Všechny čtyři rozvodny mají shodnou topologii. V každé je jeden páteřní prvek, přepínač `Cisco 3550-24`, který disponuje 24 porty o rychlosti 100 $Mb.s^{-1}$ (porty jsou typu RJ-45, tedy pro metalickou kabeláž) a dvěma porty o rychlosti 1 $Gb.s^{-1}$, do kterých lze díky media konvertorům připojit buď 2 optické kabely nebo jeden metalický. První z gigabitových portů je vždy spojen s centrálním přepínačem **gswitch-u5**, druhý port je vždy volný. Administrativní názvy těchto přepínačů jsou **gswitch-u5-mdf**, **gswitch-u5-mdf1**, **gswitch-u5-mdf2** a **gswitch-u5-mdf3**.



Obrázek 4: Celková fyzická topologie páteře budovy U5, gigabitové spoje jsou vyznačeny světle modře, spoje s rychlostí 100 $Mb.s^{-1}$ černě

Do metalických portů jsou pak dále připojeny přístupové přepínače `Cisco 2950`, které mají celkem 24 portů o rychlosti 100 $Mb.s^{-1}$, z nichž jeden je použit jako *uplink* a zbylé jsou použity pro připojení koncových stanic pomocí strukturované kabeláže. Vzhledem k faktu, že maximální přenosová rychlost *všech* portů je stejná, má vždy skupina 23 připojených stanic k dispozici pouze sdílené připojení o rychlosti 100 $Mb.s^{-1}$. V některých zvláštních případech jsou koncová zařízení připojena přímo do páteřního přepínače.

Pomocí strukturované kabeláže jsou do některých rozvoden připojeny i Wifi přístupové body, které umožňují připojení k síti pomocí bezdrátové technologie dle norem z rodiny IEEE 802.11. Tyto přístupové body jsou připojeny přímo do hlavních přepínačů jednotlivých rozvoden a de facto mají stejnou funkci jako přístupové přepínače.

V rozvodnách je celkem 32 přístupových přepínačů `Cisco 2950-24` a do nich je připojeno 731 koncových zařízení, která komunikují po síti. V současnosti je pouze **6** volných portů (navíc ne v každé rozvodně), takže není možné připojovat do sítě libovolně další zařízení. Počet přístupových přepínačů v jednotlivých rozvodnách a počet aktivně využívaných portů (připojených zařízení) jsou vyčísleny v následující tabulce:

Rozvodna	Přepínačů	Využité porty	Volné porty
MDF	6	136	2
IDF1	8	184	0
IDF2	11	250	4
IDF3	7	161	0
Celkem:	32	731	6

Tabulka 1: Obsazenost přístupových přepínačů v rozvodnách, stav k 20. 4. 2010

1.5 Logické zapojení sítě

Síť v budově U5 je rozdělena do několika logických celků - virtuálních sítí (VLAN[4]), tím dochází k segmentaci sítě na menší části. Každá taková část má svůj vlastní adresní prostor a data putující z jedné části do druhé musí procházet přes směrovač. Směrovač ale není v budově U5, je v budově rektorátu (U13), kde funguje jako jediný centrální univerzitní směrovací prvek.

Seznam těchto virtuálních sítí je udržován na centrálním univerzitním prvku `Cisco 6500` a protokolem VTP[5] je distribuován na ostatní přepínače v síti UTB. Toto řešení má ale jednu velkou nevýhodu - seznam těchto sítí může mít řádově stovky položek, ale některá zařízení mohou podporovat pouze omezené množství těchto sítí (konkrétně přepínače `Cisco 2950` mají limit 64 sítí). Z toho důvodu je seznam sítí uměle redukován, aby byl udržován v použitelných mezích (stav k 9. 4. 2010 je 110), tím ale vzniká nutnost slučovat malé logické části sítě do větších celků. To je nejpatrnější ve výukových počítačových laboratořích: v ideálním případě by měla mít každá učebna malou lokální síť, aby provoz v jedné laboratoři zbytečeně nebyl distribuován do jiných laboratoří, ve skutečnosti jsou všechny laboratoře v jedné virtuální síti.

[4]Virtual Local Area Network, z angl.
[5]Virtual Trunk Protocol, z angl.

Udržování pouze jednoho centrálního směrovače také znamená, že v budově U5 neexistuje v páteřní síti zařízení, které by zajišťovalo komunikaci na 3. vrstvě[6] referenčního modelu OSI [1]. Tím dochází k tomu, že spojem mezi budovami U5 a U1 (a dále až do budovy rektorátu) prochází data, která by se zde vůbec neměla objevovat: provoz typu *broadcast*[7] nebo data, která směřují z jedné virtuální sítě na U5 do jiné sítě na U5. Tak, jak je k centrálnímu směrovacímu prvku připojena budova U5, jsou připojeny i ostatní části univerzity - to ovšem znamená, že centrální směrovač zpracovává o mnoho více síťového provozu, než by musel, a že v linkách mezi budovami proudí data, která by teoreticky neměla opustit budovu.

Označení sítě	Číslo sítě	Porty
U5-MGMT	50	0
U5-OFFICE	51	2
U5-CLASSROOM	52	379
U5_zamest_OLD	54	337
U5-PUBLIC	55	8
MENZY	82	5
TELEPHONE-CENTRAL	641	1
MAR	642	1
PRINT-SERVICES	644	3
DVP	645	12
ACCESS-SYS	648	20
MONET	664	1

Tabulka 2: Seznam virtuálních sítí v budově U5, stav k 9. 4. 2010

Z tabulky ukazující seznam virtuálních sítí je zajímavá síť č. 50 (U5-MGMT), zařízení komunikující v této síti jsou pouze virtuální rozhraní všech přepínačů a bezdrátových přístupových bodů v budově U5 (proto je počet přiřazených portů roven nule). Problémem jsou ale sítě č. 52 (U5-CLASSROOM) a č. 54 (U5_zamest_OLD), a to hlavně z důvodu velikosti.

V síti č. 52 jsou připojeny všechny počítače ve výukových laboratořích. V síti se používá privátní IP rozsah `10.5.16.0/22` [2], brána[8] pro tuto síť je IP adresa `10.5.16.1`, která je na centrálním univerzitním směrovači. Problém je zřejmý: velké množství připojených koncových stanic (většinou typu PC s nainstalovaným operačním systémem Windows) generuje mnoho síťového provozu typu *broadcast*, navíc počítače v jedné učebně mohou snadno ovlivnit počítače v ostatních učebnách.

[6] zkráceně L3 (z angl. Layer 3)

[7] data určená pro všechna připojená zařízení v jednom síťovém segmentu

[8] z angl. gateway - zařízení, které zajišťuje připojení síťového segmentu k jiným sítím

Podobně v síti č. 54 (U5_zamest_OLD) je zapojené velké množství počítačů, většinou jde o pracovní PC nebo notebooky zaměstnanců univerzity, problémy mohou nastat podobně jako u sítě č. 52. Dalším problémem je používání IP rozsahu - na rozdíl od výukových laboratoří se zde nepoužívají privátní IP adresy, ale veřejné, navíc se nepoužívá jeden IP rozsah, ale hned 3. IP adresa brány pro všechny používané rozsahy je umístěna opět na centrálním univerzitním směrovači.

IP rozsah	Gateway
195.178.89.0/24	195.178.89.1
195.113.96.0/24	195.113.96.1
195.113.98.0/24	195.113.98.1

Tabulka 3: IP rozsahy používané v síti č. 54

1.6 Připojení bezdrátových přístupových bodů

K počítačové síti v budově U5 se dá přistupovat i pomocí bezdrátové technologie Wifi. V budově je rozmístěno několik přístupových bodů, ty jsou pak pomocí strukturované kabeláže v budově zapojeny přímo do páteřních směrovačů. Počet připojených koncových zařízení je samozřejmě variabilní a chování provozu zde nelze příliš ovlivnit ani předvídat. Všechny přístupové body jsou připojeny do páteřních přepínačů a používají 4 virtuální sítě:

Číslo sítě	Název sítě
50	U5-MGMT
56	U5-WIFI-STAFF
57	U5-WIFI-STUDENTS
59	U5-WIFI-EDUROAM

Tabulka 4: Virtuální sítě na bezdrátových přístupových bodech

Síť č. 50 je využívána jen pro administraci (v této síti jsou i administrativní rozhraní přepínačů), ostatní sítě jsou již využívány přímo bezdrátově připojenými zařízeními.

1.7 Bezpečnost

1.7.1 Zabezpečení přepínačů a komunikace na 2. vrstvě OSI

Nastavení aktivních síťových prvků je velmi jednoduché a neposkytuje ochranu připojeným stanicím ani síťovým prvkům. Porty na přístupových přepínačích, kam jsou připojeny koncová zařízení, jsou nastaveny tak, že jsou přiřazeny do konkrétní virtuální sítě a mají nastavenu funkci `portfast` (přepínač začne na tomto portu komunikovat ihned po zapojení kabelu nebo koncové stanice a ignoruje možnost, že by byl připojen další přepínač - tím obchází zdržení několik sekund, během kterého může teoreticky dojít ke změně topologie na 2. vrstvě).

Takto nastavený přístupový přepínač ovšem umožňuje případnému útočníkovi úspěšně provádět několik typů útoků na zachycení komunikace mezi jednotlivými zařízeními, která jsou připojena do stejné virtuální sítě, nebo přesměrování částečné nebo veškeré komunikace přes útočníkovo zařízení.

Pro útočníka nejjednodušší je zřejmě `ARP Cache Poisoning` [3], tato technika spočívá v tom, že útočník si vybere 2 stanice v síti. Za normálních okolností, pokud si chtějí tyto dvě stanice mezi sebou vyměňovat nějaká data, ví nejprve IP adresu svoji a cílové stanice. K tomu je zapotřebí zjistit MAC adresu druhé stanice při použití protokolu ARP[9]: zdroj vysílá broadcastovou zprávu volně přeloženou jako *"jakou MAC adresu má IP adresa a.b.c.d"* a očekává odpověd od jedné stanice ve stylu *"IP adresa a.b.c.d má MAC adresu c0:01:c0:ca:c0:1a"*. Takto získaná informace se uloží do ARP tabulky s tím, že po nějaké době (obvykle kratší než minuta) je tento záznam odstraněn a dotaz na MAC adresu je vyslán znovu. Stanice pak posílá data té stanici, která má příslušnou MAC adresu. Tento systém lze ovšem velmi snadno zneužít: útočník nebude na nic čekat a sám začne odesílat odpovědi napadené stanici, že IP adresa cíle má MAC adresu útočníkovy stanice. Napadená stanice si obnoví údaje v ARP tabulce a začne posílat data stanici útočníka (tam je možné data poslat dále na původní stroj a zároveň je ukládat, zobrazovat nebo analyzovat).

Další druh útoku je `MAC flooding` [4]. Útočník útočí primárně na přepínače, konkrétně na jejich paměť. Každý přepínač má část paměti vyhrazenou pro CAM tabulku, kde má uloženy údaje o tom, která MAC adresa se vyskytuje na kterém fyzickém portu. Velikost této tabulky je ovšem omezena a v případě, že je úplně zaplněna, začne se přepínač chovat jako `hub`, takže data, která přijdou z jednoho portu, automaticky odesílá na všechny ostatní porty. Princip útoku je tedy jasný: útočník bude na své stanici generovat velké množství dat, která začne posílat, zdrojová ani cílová IP adresa zde není zajímavá, důležité je, aby byla vždy jiná MAC adresa. Přepínač po chvíli naplní svou CAM tabulku a začne data rozesílat na všechny porty. Pokud bude útočník dostatečně šikovný, může tímto způsobem zahltit tabulky na více přepínačích - vzhledem ke struktuře sítě v budově U5 může takto zahltit tabulky na všech přepínačích v budově.

[9] Address Resolution Protocol, z angl.

Útočník může mít také stanici se dvěma síťovými rozhraními a ty pak zapojit do dvou různých přístupových přepínačů. Pokud bude následně posílat šikovně BPDU[10] zprávy, může provést úspěšný útok na protokol STP a přesměrovat veškerý provoz mezi těmito dvěma přepínači [5]. Velmi úspěšně může útočník provádět i `Port stealing` [6], kdy pomocí podvrhnutých rámců může přesvědčit přepínače, že cílové síťové zařízení (resp. MAC adresa tohoto zařízení) je právě na útočníkově stroji.

Některé pracovní stanice převážně v zaměstnanecké části sítě používají protokol DHCP, pomocí kterého dostávají od centrálního serveru informace o nastavení sítě a přidělené IP adrese. Přístupové přepínače ovšem nijak nekontrolují, kdo (který server) tyto IP adresy přiděluje. Pro útočníka není nci jednoduššího než pustit vlastní DHCP server a stanicím přidělovat falšené údaje a tím je snadno přesvědčit, aby posílaly veškerý provoz přes zařízení útočníka.

Struktura sítě je tedy snadno napadnutelná. Útočník nemusí provádět útoky tak, aby měl přístup ke komunikaci, ke které by neměl mít přístup, útoky lze zneužík i k prostému zahlcení sítě nesmyslnými daty nebo zastavit veškerý provoz zasíláním nesmyslných ARP odpovědí na všechna dostupná zařízení. Všechny zde zmíněné útoky jsou umožněny díky tomu, že přepínače nijak nekontrolují rámce zasílané z připojených stanic, především nekontrolují počty MAC adres přicházejících na jednom portu. Malá odolnost sítě proti některým popsaným útokům byla ve spolupráci s vedoucím diplomové práce ověřena v reálných podmínkách.

1.7.2 Veřejné IP adresy

Většina běžných pracovních stanic zaměstnanců univerzity používá veřejné IP adresy, aniž by byl provoz chráněn firewallem. Tento stav umožňuje vést přímy útok na připojené stanice kýmukoliv, kdo je připojený na internet, z libovolného počítače kdekoliv na světě. Útočník se může pokoušet o tzv. DoS[11] útok, kdy se snaží vybraný cíl buď zahltit tak, že není schopen dále nic zpracovávat, nebo na něm znepřístupnit některou bežící službu.

Útočník se může pokoušet rozpoznávat operační systémy na jednotlivých stanicích a odhadovat jejich verze - u starších verzí se pak může pokoušet o napadání těchto pracovních stanic pomocí veřejně přístupných nástrojů, které mohou být určeny pro využití konkrétní chyby ve starších verzích operačního systému.

V případě, že se útočníkovi povede jakýkoliv druh útoku na konkrtění pracovní stanici a bude mít možnost spustit na ní nějaký program, nic mu nezabrání v instalaci programů, které budou v tichosti na počítači čekat, až se k nim útočník připojí v budoucnu a stanici libovolně využije buď k vedení dalších útoků nebo k útokům přímo uvnitř sítě budovy.

[10] Bridge Protocol Data Unit, z angl.
[11] z angl. Denial of Service - odmítnutí služby

1.7.3 DNS server

Znalost adreasce sítě může útočníkovi velmi usnadnit pokusy o získávání kontroly nad větším množsvím připojených stanic nebo přímo nad síťovými prvky. Informace, které párují IP adresy a názvy zařízení v síti, jsou součástí DNS[12], na UTB je k tomu určený hlavní DNS server `sun.utb.cz` s operačním systémem Debian Linux a DNS softwarem `bind`.

DNS server samotný není příliš zabezpečen, vyřizuje DNS dotazy od kohokoliv z celého internetu, jako svůj primární DNS server si ho tedy může nastavit kdokoliv. To samo o sobě není nic hrozného, nicméně by se tohoto stavu dalo zneužít k DoS útoku na DNS službu z většího množství počítačů, které jsou připojeny k internetu a ke zvýšení síťového provozu na internetovém připojení univerzity. Tento stav se dá také zneužít k útoku na připojení úplně jiného počítače v internetu - útočník pošle dotaz, při kterém požaduje výpis DNS serverů, které mají na starosti např. doménu `.com`, na to stačí vyslat jediný paket o velikosti zhruba 50 B. Protože univerzitní DNS server ochotně odpovídá na jakýkoliv dotaz, odešle zpět odpověď - pro doménu `.com` je ale odpověď velmi rozsáhlá, má zhruba 277 B. Kromě umělého zahlcování připojení samotného DNS serveru (v případě mnohonásobného opakování požadavku nebo v případě, že útok je veden z několika počítačů najednou) lze ovšem v požadavku podstrčit DNS serveru jinou zdrojovou IP adresu. Útočník tak posílá DNS dotazy o velikosti 50 B, zatímco DNS server odpovídá někomu úplně jinému, tomu zasílá nevyžádané pakety o velikosti 277 B. Pokud je takový útok dobře naplánovaný a vedený simultánně z několika strojů, může to vést až k úplnému odstavení oběti od internetu a to za použití univerzitního DNS serveru.

Fakt, že univerzitní DNS server vyřizuje DNS dotazy de facto z celého světa, se může útočníkovi hodit k získávání informací o adresaci sítě. Pokud bude útočník vědět, že páteřní přepínače mají název **gswitch-u5** nebo **gswitch-u5-mdf**, snadno si zjistí jejich IP adresu pohodlně ze svého domácího počítače:

```
$ host gswitch-u5-mdf.utb.cz sun.utb.cz
Using domain server:
Name: sun.utb.cz
Address: 195.178.88.66#53

gswitch-u5-mdf.utb.cz has address 10.5.0.6
```

Podobně tedy může zjistit IP adresy přepínačů v jiných budovách univerzity, při znalosti názvů budov z veřejně známých údajů (např. z www stránek univerzity) si pak může lehce odvodit IP adresaci přepínačů např. v budově rektorátu (U13), v budově univerzitního Technology parku nebo v budově v Uherském Hradišti:

[12]Domain Name System, z angl.

```
$ host gswitch-u13-mdf.utb.cz sun.utb.cz | grep has\ address
gswitch-u13-mdf.utb.cz has address 10.13.0.5

$ host gswitch-u11.utb.cz sun.utb.cz | grep has\ address
gswitch-u11.utb.cz has address 10.11.0.5

$ host gswitch-uh1.utb.cz sun.utb.cz | grep has\ address
gswitch-uh1.utb.cz has address 10.32.0.5
```

DNS server by rozhodně neměl poskytovat informace o privátních IP adresách na základě dotazu z internetu. Také by o sobě neměl prozrazovat vlastní verzi, protože jednotlivé verze používaného softwaru `bind` mohou obsahovat chyby, které lze dále zneužívat k útoku na samotný DNS server nebo DNS službu:

```
$ dig @195.178.88.66 version.bind chaos txt | grep ^version | grep TXT
version.bind.           0       CH      TXT     "9.3.4-P1.2"
```

1.8 Nevýhody současného stavu

Hlavní prvky sítě jsou několik let staré, navíc již v době, kdy se zařízení do budovy montovala, byla na sklonku doby použitelnosti. V současné době by se v ostrém provozu tato zařízení rozhodně neměla vyskytovat a měla by být nahrazena novějším hardwarem:

- hlavní páteřní zařízení `Cisco 3508G-XL`: výrobce toto zařízení již nepodporuje, updaty (ani bezpečnostní) pro operační systém nevydává od **17. 9. 2005** [7]
- páteřní přepínače v rozvodnách `Cisco 3550`: výrobce tato zařízení přestane podporovat **2. 5. 2011**, updaty ale nevydává již od **2. 5. 2007** [8]
- přístupové přepínače `Cisco 2950`: výrobce tato zařízení přestane podporovat **20. 10. 2013**, updaty ale nevydává od **20. 10. 2009** [9]

Kromě vysokého stáří hardwaru je zde ještě další významné omezení: maximální přenosová rychlost jedné koncové stanice je 100 $Mb.s^{-1}$, ovšem toto pásmo je sdílené s dalšími přibližně 20 stanicemi. Některé připravované projekty však mohou mít vyšší nároky na okamžitou přenosovou rychlost, z toho důvodu je třeba přenosovou rychlost v síti zvýšit.

Mezi rozvodnami je položeno velké množství kabelů, které umožňují rychlý přenos dat, ale nejsou nijak využity. Propustnost páteřních propojů mezi rozvodnami by šla snadno několikanásobně zvýšit pouhým zapojením kabelů do příslušných přepínačů.

Celá budova je připojena jen jedním párem optických vláken, navíc pouze přes jeden aktivní prvek - není zde žádná možnost redundance, žádná možnost funkčnosti sítě v případě pádu jednoho zařízení. Na stavu této linky je navíc závislý i datový provoz mezi jednotlivými lokálními sítěmi - data z jedné lokální sítě do druhé jsou směrována až na univerzitním centrálním prvku, který je ale fyzicky umístěný v budově rektorátu, takže mezisíťový provoz je závislý na stavu hlavního přepínače `gswitch-u5`, stavu optického spoje a na stavu dalšího prvku mimo budovu. Pokud bude z jakéhokoliv důvodu mimo provoz centrální páteřní přepínač **gswitch-u5**, centrální univerzitní směrovač nebo optické propoje budov (U5-U1 neno U1-U13), nebude fungovat uživatelům sítě nic kromě komunikace v rámci segmentu, kam jsou připojeni, navíc vzhledem k umístěni DNS serveru také do budovy rektorátu ovšem budou odkázáni pouze na komunikaci pomocí IP adres.

Centrální seznam lokálních sítí, který je navíc velmi omezen, neumožňuje nijak dělit současné sítě v budově U5 na menší nezávislé jednotky, což vede k vytváření velkých sítí o velkém počtu připojených stanic, to pak přináší snížení bezpečnosti provozu a zvýšení parazitního a broadcastového provozu.

Procesory páteřních přepínačů jsou zbytečně zatěžovány tím, že vypočítávají stromovou strukturu pro STP[13], přestože topologie sítě neumožňuje vůbec použití tohoto protokolu (neobsahuje redundantní propojení přenípačů). Výpočet navíc probíhá pro všechny definované virtuální sítě, i když se zařízení v těchto sítích v budově U5 vůbec nenachází.

Pracovní stanice v síti č. 54 používají veřejné IP adresy, přestože se většinou jedná o pracovní stanice zaměstanaců univerzity. To zvyšuje riziko útoku na jendotlivé stanice odkudkoliv z internetu, protože na ně lze směrovat síťový provoz odkudkoliv z internetu. Porty přístupových přepínačů nejsou nijak chráněny proti L2 útokům - útoky lze vést z libovolné připojené stanice, pro útočníka jsou zajímavé např. `MAC flooding` nebo `ARP Cache Poisoning`.

Shrnutí hlavních nevýhod současného stavu:
- staré páteřní prvky
- malá datová propustnost v páteřních spojích
- nevyužitá kabeláž mezi rozvodnami
- nezálohované připojení budovy k síti UTB
- chybějící L3 struktura
- nemožnost dělení sítě na menší části
- málo volných portů pro připojení nových zařízení
- používání veřejných IP adres na pracovní stanice
- zbytečné počítání STP na páteřních přepínačích
- velmi nízké zabezpečení sítě

[13]Spanning Tree Protocol, z angl.

2 Návrh nové struktury sítě

2.1 Požadavky

Od začátku používání sítě v budově již uplynulo několik let, během nichž se postupně formovaly požadavky některých uživatelů sítě na její úpravy, a to jak co se týče běžného denního fungování sítě, tak co se týče nových připravovaných projektů, které s počítačovými sítěmi souvisejí.

1) **Možnost snadného omezení síťového provozu v konkrétní učebně** - studenti často dělají zkoušky v počítačových laboratořích, kde vyplňují testy na počítači, někdy i přes internet, ovšem zkoušející nemůže nijak zabránit tomu, aby zkoušení během testu využívali možnosti internetového připojení pracovních stanic k podvádění (vyhledávání výsledků, komunikace s jinými lidmi, nahlížení do online dokumentací apod.). V současné době mohou zkoušející jen vytáhnout síťový kabel z počítače, tím ale dochází k opotřebení koncovek na těchto kabelech.

2) **Zvýšení datové propustnosti sítě** - připravovaný projekt vzdáleného bootování pracovních stanic v počítačových laboratořích potřebuje rychlejší propustnost sítě. Testy u tohoto projektu ukázaly, že startuje-li najednou 10 pracovních stanic, mohou dohromady během bootovacího procesu vytvořit síťový provoz až 100 $Mb.s^{-1}$ nebo i vyšší, podobně při hromadném startování kancelářského softwaru. V současné síti by start počítačů v jedné učebně mohl velmi nepříjemně zbrzdit provoz v jiné učebně.

3) **Odstranění parazitního provozu ze sítě** - některá zařízení připojená do sítě generují nežádoucí provoz, typicky např. tiskárny s přímým připojením do LAN neustále posílají o sobě do sítě broadcastové informace. V ideálním případě by po detekování takového provozu měla existovat možnost ho zastavit už na přístupovém přepínači.

4) **Implementace DHCP** - projekt vzdáleného bootování pracovních stanic vyžaduje přítomnost protokolu `DHCP` v síti, řídící server musí jednotlivým pracovním stanicím přiřazovat jejich IP adresu (a další údaje o síti) během bootovacího procesu.

5) **Možnost vzdáleného příkazu pro start vypnuté pracovní stanice v počítačové laboratoři** - připravovaný projekt si klade za cíl využít velké množství pracovních stanic, které jsou mimo pracovní dobu vypnuté, k výpočetnímu výkonu, k tomu je ale třeba ve vybraný čas zaslat všem takovým připojeným stanicím z řídícího serveru příkaz na automatické zapnutí pomocí technologie `Wake On Lan`

6) **Nezávislost některých částí sítě na centrálním směrovači** - v případě nedostupnosti centrálního směrovače může dojít k tomu, že během zkoušení nebude dostupný univerzitní směrovač. Některé zkoušky ovšem využívají systém *Moodle* nainstalovaný na jednom ze serverů v síti FAI - propojení pracovních stanic a serveru by nemělo být ohroženo výpadkem připojení budovy. S tím souvisí i umístění záložního DNS serveru v budově U5.

7) **Zálohované připojení** - moderní velká počítačová síť by měla mít v rámci možností zálohované připojení. Pokud selže některý prvek, který je sice pro normální chod sítě nezbytný, ale zároveň ho lze obejít, měla by existovat záloha. To se v případě FAI a budovy U5 týká optického spojení s budovou U1 a centrálního přepínače - zálohy zde neexistují, ale mohly by.

8) **Zvýšení bezpečnosti** - analýzou současné sítě bylo zjištěno, že přístupové přepínače nejsou odolné proti některým útokům a že pracovní stanice zaměstnanců jsou snadno napadnutelná přímo z internetu. Je tedy třeba zavést některá opatření pro zvýšení bezpečnosti jak aktivních síťových prvků, tak připojených stanic.

2.2 Fyzické zapojení

2.2.1 Hierarchické rozdělení

Návrh nové sítě je založen na standardním hierarchickém modelu, který síť dělí do tří úrovní podle funkcí aktivních síťových prvků, které se v dané úrovni nacházejí:

- core vrstva - nejvyšší úroveň, zahrnuje prvky, které celou síť připojují k internetu nebo jiným sítím
- distribuční vrstva - střední úroveň, zajišťuje komunikaci mezi jednotlivými částmi vlastní sítě a zprostředkovává komunikaci mezi zařízeními na přístupové vrstvě a core vrstvou
- přístupová vrstva - obsahuje základné síťové prvky, do kterých jsou již připojeny pracovní stanice, servery a jiná zařízení, která komunikují po síti

Tento model není úplně přesně aplikovatelný na kteroukoliv síť, některé vrstvy se mohou částečně překrývat nebo úplně splynout, záleží vždy na velikosti a struktuře sítě. V konkrétním případě sítě FAI bude sloučena core a distribuční vrstva:

- distribuční vrstva - páteřní přepínače, v každé rozvodně bude jeden páteřní přepínač, všechny budou propojeny mezi sebou a některý z nich bude poskytovat i připojení sítě FAI ke zbytku univerzitní sítě a k internetu (tím plní funkčnost core vrstvy)
- přístupová vrstva - přístupové přepínače, v každé rozvodně jich musí být takový počet, aby odpovídal počtu připojených zařízení v té části budovy, kde je vedena kabeláž z rozvodny k zásuvkám v kancelářích, učebnách aj.

Při úplném uplatnění třívrstvého modelu by core vrstvu měla představovat zařízení v univerzitní páteřní síti, což je v současnosti centrální univerzítní prvek `Cisco 6500`.

2.2.2 Distribuční vrstva

Kvůli zvýšení datové propustnosti páteře je nutná výměna páteřních přepínačů. Současná zařízení `Cisco 3550-24` (v každé rozvodně je jeden kus) neposkytují konektivitu o rychlosti 1 $Gb.s^{-1}$ přístupových přepínačům, navíc touto rychlostí umí komunikovat pouze 2 porty.

Současná zařízení by měla být nahrazena přepínači `Cisco 3560G-48TS-E`, ty mají 48 portů o rychlosti 1 $Gb.s^{-1}$ a další 4 *dual purpose*[14] porty o stejné rychlosti.

Navýšením počtu komunikačních portů na dvojnásobek vznikne možnost agregace linek - spojení mezi dvěma aktivními prvky tedy může zajišťovat více fyzických spojů, ale jednotlivá zařízení s nimi mohou manipulovat jako s jednou logickou jednotkou, celková komunikační rychlost se při tom sčítá. K této agregaci bude použita technologie `Etherchannel`, což je u zařízení od výrobce `Cisco` podporovaná a doporučená technologie pro agrageci linek. Agregovat lze nejvýše 8 fyzických spojů.

Agregovat lze ovšem pouze spojení, která využívají stejnou přenosovou kabeláž - v jednom logickém spoji nelze mít optický a zároveň metalický spoj. Mezi rozvodnami existují jak metalické, tak optické rozvody kabeláže, použití metalické kabeláže je ovšem výhodnější:

- páteřní přepínače mají jen 4 porty schopné komunikovat přes optickou kabeláž
- metalické kabely jsou mnohem levnější
- metalické kabely jsou odolnější proti ohybům

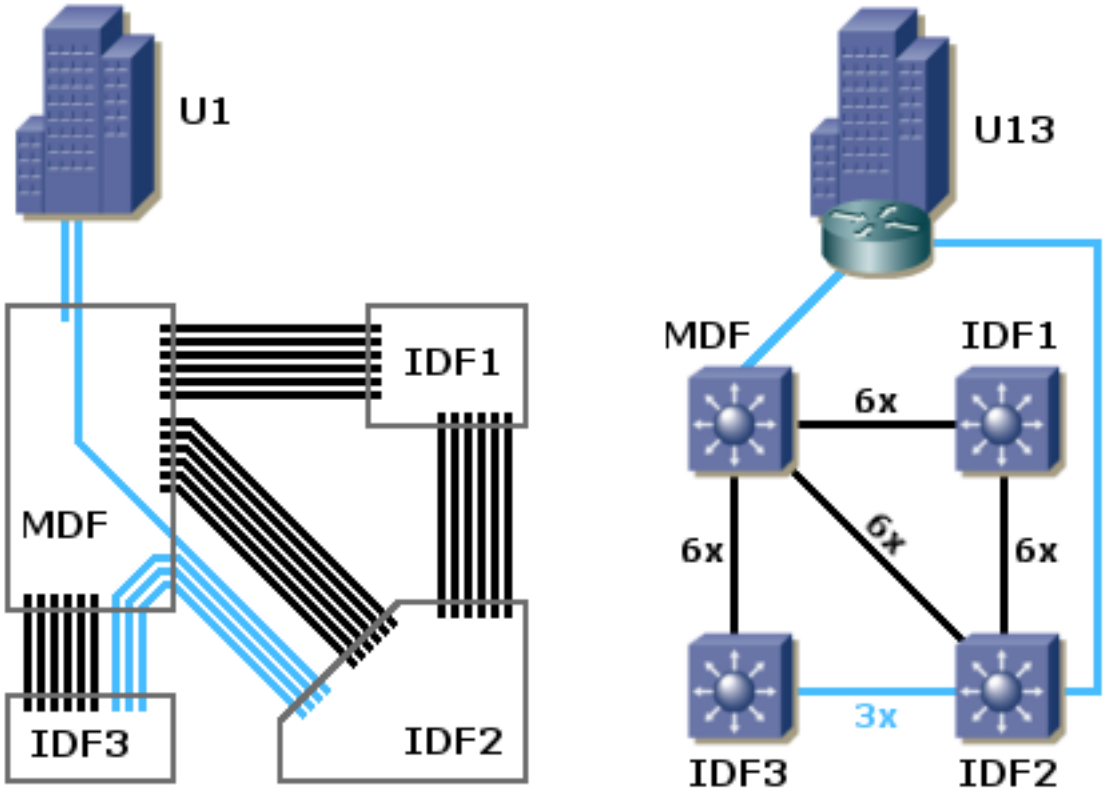
Rozvodny mezi sebou budou propojeny nikoliv topologií *star*[15], ale *partial mesh* (každý s každým, ovšem některé spoje nejsou realizovány). Propojení rozvoden MDF, IDF1 a IDF2 je k dispozici ve formě trojúhelníku (každý s každým), rozvodna IDF3 je sice propojena pouze s MDF, ale propojením patch panelů v rozvodně MDF lze kabely uměle prodloužit do dalších rozvoden, ovšem vzhledem k počtu kabelů, které jsou k dispozici, půjde jen o agregaci tří linek z z IDF3 přes MDF do IDF2. Při maximálním využití současné metalické kabeláže mezi jednotlivými rozvodnami lze páteřní propoje realizovat takto:

- MDF-IDF1: 6x metalický propoj (6 $Gb.s^{-1}$)
- MDF-IDF2: 6x metalický propoj (6 $Gb.s^{-1}$)
- MDF-IDF3: 6x metalický propoj (6 $Gb.s^{-1}$)
- IDF2-IDF1: 6x metalický propoj (6 $Gb.s^{-1}$)
- IDF2-IDF3: 3x dvojice optických propojů (3 $Gb.s^{-1}$)

[14] do těchto portů lze pomocí speciálních media konvertorů připojit jak metalickou, tak optickou kabeláž
[15] hvězda, z angl.

Proti současnému stavu dochází také k redukci počtu zařízení v distribuční vrstvě - funkci současného optického přepínače `Cisco 3508G-XL`, který sloužil jako uzlový prvek hvězdy, převezme hlavní přepínač v rozvodně MDF. Jako zálohu tohoto propoje je zde možnost využít další dvojici optických vláken, propojením patch panelů v rozvodně MDF lze takový spoj protáhnout přímo do další rozvodny IDF2 a tam ho připojit také do hlavního přepínače. Toto řešení lze ještě maximalizovat, pokud by byly takto připojené ještě zbylé dvě rozvodny, což by ale mělo smysl až ve chvíli, kdy by optické propoje z budovy U5 byly zakončeny v jiném síťovém prvku. Vícenásobná záloha připojení v tuto chvíli ale není nutná.

Počet využitých optických vláken mezi budovami U5 a U1 by šel ještě navýšit, pokud by byla nutnost posílit datovou propustnost mezi budovami - opět by se použila technologie `Etherchannel` a agregovaly by se optické propoje.



(a) Využití kabeláže (b) Fyzická topologie

Obrázek 5: Návrh zapojení síťových prvků v distribuční vrstvě - optické kabely jsou světle modré, metalické jsou černé. Jedno optické propojení na obrázku představuje využití dvou vláken z důvodu full duplexního spojení.

Výhody nového návrhu distribuční vrstvy:

- snížení počtu hlavních směrovačů v rozvodnách
- zvýšení přenosové rychlosti mezi jednotlivými rozvodnami na 6 $Gb.s^{-1}$
- zálohované připojení budovy k síti UTB
- změna topologie - výpadek jednoho páteřního přepínače v kterékoliv rozvodně neznamená nedostupnost sítě pro zbytek budovy
- maximální využití kapacity existující kabeláže

2.2.3 Přístupová vrstva

Současná zařízení na přístupové vrstvě komunikují na všech portech maximální rychlostí 100 $Mb.s^{-1}$, a to včetně portu, kterým jsou připojena k prvkům v distribuční vrstvě - tím vzniká pro zařízení připojená do jednoho přepínače sdílená konektivita o rychlosti 100 $Mb.s^{-1}$. Některé projekty připravované na FAI UTB ve Zlíně ale vyžadují, aby už koncová zařízení připojená k počítačové síti měla možnost komunikace rychlostí 1 $Gb.s^{-1}$ (např. vzdálené bootování), a to navíc současně.

Z toho důvodu bude nutné provést povýšení současných přepínačů tak, aby byly připojeny k distribuční vrstvě co nejvyšší možnou rychlostí - ideální bude agregování více metalických kabelů, které budou spojovat porty o rychlosti 1 $Gb.s^{-1}$. Mají-li mít všechna připojená koncová zařízení možnost komunikace o rychlosti 1 $Gb.s^{-1}$, musí mít i přístupové přepínače všechny porty schopné komunikovat touto rychlostí.

K agreagaci spojů páteřních a přístupových přepínačů se použije technologie `Etherchannel`. Ta sice umožňuje agregovat až 8 spojů a tím doáshnout datové propustnosti až 8 $Gb.s^{-1}$, ale propoje páteřních přepínačů jsou navrženy na 6 $Gb.s^{-1}$, takže tak vysoká datová propustnost mezi přístupovým a páteřním přepínačem není žádoucí, smysl dává agregace nejvýše 6 spojů a tedy propustnost 6 $Gb.s^{-1}$.

Další změnou proti současnému stavu je zvýšení počtu portů u přístupových přepínačů. Nynější `Cisco 2950-24` mají celkem 24 portů, navrhovaná zařízení `Cisco 2960G-48TC-L` mají 48 portů. Takovou výměnou se sníží počet přístupových přepínačů v jednotlivých rozvodnách, což znamená snadnější správu, ušetření místa v rozvodnách a menší spotřebu elektrické energie.

Při zachování současného počtu aktivně využitých přístupových portů je třeba do každé rozvodny dodat příslušný počet přístupových přepínačů:

Rozvodna	Přepínače	Porty			
		celkem	uplinky	použité	volné
MDF	4	192	24	135	33
IDF1	5	240	30	184	26
IDF2	6	288	36	245	7
IDF3	4	192	24	161	7
Celkem:	19	912	114	725	73

Tabulka 5: Počty použitých a volných portů přístupových přepínačů (uplinky jsou porty nutné pro připojení přístupového přepínače k distribuční vrstvě, každý přístupový přepínač je připojen pomocí 6 spojů

Rozvodna	Metalické porty				Optické porty			
	celkem	páteř	downlinky	volné	celkem	páteř	uplinky	volné
MDF	48	18	24	6	4	0	1	3
IDF1	48	12	30	6	4	0	0	4
IDF2	48	12	36	0	4	3	1	0
IDF3	48	6	24	18	4	3	0	1

Tabulka 6: Počty použitých a volných portů páteřních přepínačů (páteř: propojení páteřních přepínačů, downlinky: připojení přístupových přepínačů, uplinky: připojení budovy U5 k síti UTB)

Přestože se může zdát, že kapacita sítě z hlediska počtu portů v přepínačích je téměř vyčerpána, není tomu tak. Velká rezerva je právě ve vysoké agregaci linek - celá páteřní síť (propojení přepínačů v distribuční vrstvě i propojení páteřních a přístupových směrovačů) je sice navržena na rychlost 6 $Gb.s^{-1}$, ale ne vždy je nutné tuto rychlost využít. Poměrně snadno lze vyčlenit některé části sítě (resp. koncová zařízení), která nepotřebují tak vysokou přenosoovou rychlost. Ty lze pak zapojit do jednoho přístupového přepínače, který pak může být připojen k páteřnímu přepínači menší rychlostí, např. 2 $Gb.s^{-1}$, čímž vzniknou na páteřním přepínači další volné porty. Další možností je připojování přístupových přepínačů *za sebou*, kdy je jeden připojen k druhému a teprve druhý je připojen do páteřního přepínače. Tento model sítě je tedy velice variabilní a snadno škálovatelný.

V případě, že by bylo nutné do některé z rozvoden přidat další velké množství koncových stanic, přidal by se do topologie nový páteřní přepínač a k němu by se opět připojovaly přístupové přepínače.

2.2.4 Argumenty pro výběr přepínačů

Kvůli snadnější a hlavně jednotnější administraci (administrátorské přístupy, hromadné ovládání, logování, metody měření) je vždy ideální, jsou-li síťové prvky vyrobeny jedním výrobcem a mají společnou platformu. Síťová infrastruktura na celé univerzitě je realizována na zařízeních výrobce `Cisco Systems, Inc.` a všechny mají operační systém `Cisco IOS`. Případná výměna síťových prvků na části univerzity (jako např. v budově U5) by měla tento stav respektovat, proto i nově navrhovaná zařízení jsou z dílny stejného výrobce.

Páteřní přepínače řady `Cisco 3560` mají dostatečné množství funkcí, aby mohly při správném nastavení splnit všechny požadavky, které jsou nyní kladeny na chod sítě - jedná se o multilayer[16] přepínače, které navíc mají podoru směrování (a funkcí s tím souvisejících) a tím mohou nahradit směrovač. Navržený typ `Cisco 3560G-48TS-E` navíc univerzita již vlastní z dřívější doby a příslušný počet byl již určen do budovy U5 - to výrazně snižuje pořizovací náklady.

Přístupový přepínač `Cisco 2960G-48TC-L` je z aktuální řady přístupových přepínačů, které firma `Cisco Systems Inc.` nabízí. Tento typ byl vybrán vzhledem k počtu portů umožňující komunikaci o rychlosti 1 $Gb.s^{-1}$ a funkcím, které zvyšují bezpečnost sítě (především ochranu proti L2 útokům a snadné zachycení parazitního provozu).

Uvedené řešení (páteřní přepínače řady 3560 a přístupové 2960) lze nahradit jiným řešením stejného výrobce, např. do každé rozvodny lze umístit přepínače vyšší řady (např. 4500 nebo 6500) spolu s přepínačovými moduly. Tato zařízení by pak obsluhovala jak přístupovou, tak páteřní část sítě. Cena tohoto řešení je ale mnohem vyšší a jeho pořízení je v současné chvíli nereálné, proto není dále uvažováno.

2.3 Logické zapojení

2.3.1 Používání protokolu STP

Protokol STP se využívá v takových částech sítě, které dovolují vytváření smyček v komunikaci na 2. vrstvě referenčního modelu OSI [10]. Je-li taková smyčka vytvořena (propojení dvou přepínačů dvěma spoji, zapojení přepínačů do trojúhelníku nebo kruhu), může dojít k tzv. *broadcast storm*, kdy datový paket může obíhat ve smyčce neustále dokola a algoritmy používané k jeho dalšímu šíření ho neumí zastavit. V případě, že protokol STP nalezne v síťové topologii takovouto smyčku, jeden z jejich konců (vybírá se podle předem stanovených pravidel) je uměle vypnutý (přepínač nevysílá do takto vybraného portu naprosto žádné údaje, pouze poslouchá příchozí data). V případě, že dojde ke změně topologie, hlavně z důvodu výpadku některého z přepínačů nebo spoje mezi přepínači,

[16] více vrstev, z angl.

dojde v poměrně krátkém časovém intervalu znovu k výpočtu topologie, opětovné detekci smyček a eventuelnímu vypnutí některého portu. V navrhované topologii vznikají dvě smyčky:

- mezi přepínači v rozvodnách MDF, IDF2 a IDF1
- mezi přepínači v rozvodnách MDF, IDF2 a IDF3

Přestože páteřní přepínače v rozvodnách MDF a IDF2 jsou rovnocenné (oba jsou propojeny se všemi ostatními přepínači a oba mají své připojení ke zbytku iniverzitní sítě), přepínač v MDF je méně náchylný k chybovosti - připojení přepínače v IDF2 je realizováno přes uměle protažené optické propoje, které vedou přes rozvodnu MDF, navíc optické spoje spoléhají na media convertory, což vede také k vyššímu riziku, že vznikne chyba nebo nefunkčnost. Z toho důvodu bude přepínač v rozvodně MDF určen jako hlavní, tzv. *root switch*, přepínač v IDF2 bude sloužit jako záložní. Tohoto stavu se dosáhne nastavením prioritního čísla - přepínač v MDF bude mít nejnižší prioritní číslo, přepínač v IDF2 o něco vyšší a ostatní dva přepínače (v IDF3 a v IDF1) ještě vyšší.

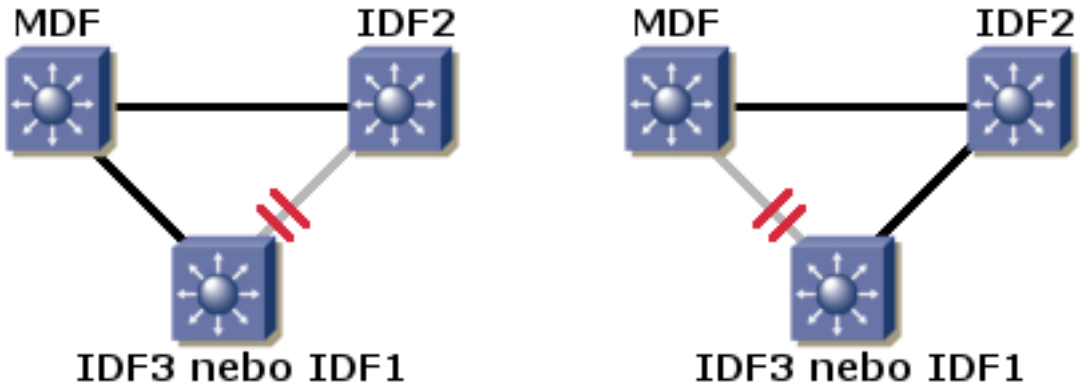
Přepínače v rozvodnách IDF1 a IDF3 budou nastaveny tak, aby primárně posílaly data přes hlavní přepínač v MDF a do spoje k přepínači v IDF2 neposílaly nic. V případě pádu přepínače v MDF (nebo spoje do přepínače) dojde ke změně topologie a přepínače ihned začnou posílat data do IDF2. Pro zmenšení času, kdy dochází k výpočtu nové topologie (jsou definovány timeouty) budou jednotlivé spoje na páteřních přepínačích ještě označeny jako `uplinkfast` [11], což usnadňuje protokolu STP odhadnout síťovou topologii ještě před samotným výpočtem.

Protokol STP vypočítává topologii pro každou virtuální síť zvlášť, což může při větším počtu sítí znamenat poměrně vysokou procesorovou zátěž. Proto bude na všech přepínačích použito rozšíření protokolu STP, konkrétně MSTP[17] [11] - ten může sloučit vypočítávání topologie pro několik virtuálních sítí do skupin.

V navrhované topologii sítě jsou vytvořeny dvě identické smyčky, kdy jsou 3 přepínače zapojeny do trojúehlníku. Protože je pevně dána struktura smyček (přesné vymezení hlavního a záložního přepínače a spojení mezi nimi je označeno jako páteřní), existují z pohledu STP pouze dvě možná nastavení přetržení smyčky: páteřní spoj zůstane nepřerušen, přeruší se připojení *třetího* přepínače k MDF nebo IDF2.

Většina provozu, který bude vznikat na koncových stanicích a bude dále distribuován po páteřních spojích, půjde při bezvýpadkovém stavu směrem k páteřnímu přepínači v MDF, proto je výhodné nastavit přepínače tak, aby došlo k přerušení smyčky ve spojení k IDF2. Nicmnéně na FAI je plánovaný projekt vzdáleného bootování pracovních stanic

[17] Multiple Spanning Tree protocol, z angl.



(a) Přerušení spoje k IDF2

(b) Přerušení spoje k MDF

Obrázek 6: Přetržení smyčky pomocí protokolu STP - port, který neposílá žádná data je označen červenými čarami, nepoužívané spojení je šedé. Data jsou posílána pouze po černě vyznačených spojích

ve výukových laboratořích a bootování většího množství pracovních stanic nebo hromadné spouštění některých typů softwaru znamená přenášení velkých objemů dat po síti. Za předpokladu, že stukturovaná kabeláž výukových laboratoří je zakončena v rozvodnách IDF1 a IDF2 a že centrální server, který bude muset komunikovat se všemi učebnami, bude muset být co nejdostupnější pro obě rozvodny (nejlépe již na 2. vrstvě modelu OSI, tedy bez nutného směrování), je zřejmé, že bude umístěn v jedné z těchto rozvoden a že posílat data z IDF1 do IDF2 přes MDF není úplně výhodné.

Z toho důvodu budou na páteřních přepínačích vytvořeny dvě instance protokolu MSTP, kdy jedna instance bude nastavena tak, že bude přerušen provoz k MDF, a druhá bude nastavena tak, že dojde k přerušení provozu k IDF2. Jednotlivé virtuální sítě pak budou přiřazeny do jedné nebo druhé instance dle požadavku na směr toku dat.

2.3.2 Změna směrování v připojení budovy

Hlavní změna nové topolgie spočívá ve směrování. Umístění směrovače mimo budovu (nyní v budově U13) není příliš vhodné, proto jeho funkci přebere páteřní přepínač **gswitch-u5-mdf**, záložní směrovač bude **gswitch-u5-idf2**. Obě zařízení budou mít vlastní propojení s univerzitním směrovačem a v případě výpadku jednoho z nich převezme plně funkčnost druhé.

Tímto krokem dojde k úplnému odstřižení budovy U5 od L2 struktury, tím vzniká možnost rozdělit celou síť v U5 na menší jednotky s vlastní IP adresací. IP rozsah pro budovu U5 již je přidělen - celá univerzita používá privátní rozsah `10.0.0.0/8`, který je dále dělen podle jednotlivých budov, pro U5 je již nyní administrativně vyčleněna síť

10.5.0.0/16. IP adresy z jiných rozsahů v jiných částech univerzity budou dostupné díky směrování na páteřních přepínačích, které budou předávat provoz určený mimo vlastní síť směrem k univerzitnímu směrovači.

Na propojení univerzitního směrovače a páteřních přepínačů v budově U5 bude vyhrazena část IP rozsahu, který vznikne pro propojení páteřních směrovačů univerzity, např. 10.0.0.0/24. IP adresa 10.0.0.1 bude mít centrální směrovač, další IP adresy pak jednotlivá směrovací zařízení v jiných budovách univerzity. U každého přepínače (včetně centrálního) je třeba uvažovat o záložním stroji, to znamená celkem 3 IP adresy (adresa pro hlavní zařízení, pro záložní zařízení a virtuální IP adresa, kterou si budou jednotlivá zařízení předávat mezi sebou). V případě páteřních přepínačů v budově U5 tedy budou adresy přiděleny takto:

Název	IP adresa	Zařízení
c6509	10.0.0.1	centrální univerzitní směrovač
gswitch-u5	10.0.0.4	virtuální adresa
gswitch-u5-mdf	10.0.0.5	páteřní směrovač v MDF
gswitch-u5-idf2	10.0.0.6	páteřní směrovač v IDF2

Tabulka 7: IP adresace propoje budovy U5 a zbytku univerzitní sítě

Směrování je v tomto případě velmi jednoduché: centrální směrovač bude směrovat celou síť 10.5.0.0/16 na IP adresu 10.0.0.4, v obráceném směru postačí nastavit na obou páteřních přepínačích bránu (*default route*) směrem na 10.0.0.1.

Celý adresní prostor 10.5.0.0/16 se bude dále dělit na jednotlivé segmenty podle funkcí jednotlivých připojených koncových stanic. Páteřní segment, který bude obhospodařovat páteřní směrování, nyní obsahuje 4 zařízení, dále je třeba započítat IP adresu pro virtuálni směrovač (použije se protokol HSRP[18]). Ve stejném segmentu mohou být i administrativní IP adresy jednotlivých přístupových přepínačů (celkem 19). Páteřní síť se ale může rozrůstat a přidělený adresní prostor je dostatečně veliký, proto pro tento segment bude vyhrazen prostor 10.5.0.0/24.

Všechna zařízení budou jako bránu využívat IP adresu virtuálního směrovače, protokol HSRP pak zajistí, že ji bude aktivně používat jeden z přepínačů **gswitch-u5-mdf** a **gswitch-u5-idf2**. Oba tyto přepínače mohou zajistit vlastní připojení ke zbytku univerzitní sítě.

[18]Hot Standby Router Protocol, z angl.

IP adresa	Použití
10.5.0.0	IP adresa sítě
10.5.0.1	IP adresa virtuálního směrovače (gswitch-u5)
10.5.0.2 - 10.5.0.15	rezerva
10.5.0.16	gswitch-u5-mdf
10.5.0.17	gswitch-u5-idf1
10.5.0.18	gswitch-u5-idf2
10.5.0.19	gswitch-u5-idf3
10.5.0.20 - 10.5.0.31	rezerva
10.5.0.32 - 10.5.0.47	přístupové přepínače v MDF
10.5.0.48 - 10.5.0.63	přístupové přepínače v IDF1
10.5.0.64 - 10.5.0.79	přístupové přepínače v IDF2
10.5.0.80 - 10.5.0.95	přístupové přepínače v IDF3
10.5.0.96 - 10.5.0.254	rezerva
10.5.0.255	IP adresa pro broadcast

Tabulka 8: IP adresace v administrativním segmentu

Se zavedením tohoto směrování úplně odpadá použití protokolu VTP a odebírání seznamu virtuálních sítí z univerzitního směrovače, tento seznam zde nemá žádný smysl. Naopak je zde prostor pro vytvoření vlastního seznamu virtuálních sítí v rámci budovy a jeho distribuce pomocí protokolu VTP pouze v rámci síťové infrastruktury v budově. Nyní používanou VTP doménu `UTB` nahradí doména `UTB-U5`, funkci hlavního VTP `serveru` zastane **gswitch-u5-mdf**, ostatní přepínače pak budou ve stavu `client` a budou odebírat seznam virtuálních sítí od serveru automaticky.

2.3.3 Používání protokolu HSRP

Protokol `HSRP` pochází z dílny výrobce `Cisco Systems Inc.` a zajišťuje automatickou náhradu směrovače v případě, že primární směrovací zařízení buď nefunguje vůbec nebo některé z jeho spojení není dostupné. Přestože protokol je velmi přesně definován a popsán v dokumentu `RFC 2281` [12], je dostupný pouze na zařízeních tohoto výrobce a licenční podmínky nepovolují jeho užití na jiných zařízeních (resp. toto použití by bylo zpoplatněno).

Protokol funguje za předpokladu, že v síti není jeden směrovače, který pro ostatní stanice v síti zprostředkovává připojení do jiných sítě (tzv. *default gateway*), ale jsou alespoň dva. Každý má svou vlastní IP adresu a je plnohodnotným směrovačem. Kromě IP adresy má také prioritu, podle které je jeden ze směrovačů určený jako `Active` a ostatní jako `Standby` (aktivní je směrovač s nejvyšší prioritou). Není-li aktivní směrovač dostupný nebo se díky dalším nastavením jeho priorita změní, může se aktivním směrovačem stát jiný.

Stanice připojené v síti ale mají nastavenu jen jednu IP adresu směrovače a nemohou si ji sami změnit. Proto je třeba administrativně vyčlenit ještě jednu IP adresu navíc, která bude přiřazena virtuálnímu směrovači. Protokol HSRP pak zajistí, že tato IP adresa virtuálního směrovače bude vždy přiřazena aktivnímu směrovači. Konkrétní nastavení protokolu HSRP na páteřních přepínačích zajišťující připojení budovy U5 ke zbytku univerzitní sítě bude takové:

- priorita **gswitch-u5-mdf** bude 64
- priorita **gswitch-u5-idf2** bude 56
- v případě, že nebude k dispozici spojení mezi páteřním přepínačem a přepínačem v budově U13 (nefunkční optické spojení nebo přepínač v U13), sníží se priorita daného přepínače o 16

Pátařní přepínače `Cisco 3560` mají ovšem u protokolu HSRP omezení, lze ho použít pouze na **32** segmentů. Použití protokolu v jednotlivých segmentech sítě na U5 má tedy smysl pouze v případě, že segment je fyzicky oddělen tak, že jedna jeho část je zapojena do jedné rozvodny a jiná část do druhé rozvodny. V případě, že je celý segment připojený do přístupových přepínačů, které jsou zapojeny do jednoho páteřního přepínače, není nutné protokol HSRP používat, daný páteřní přepínač bude fungovat jako brána pro daný segment.

2.3.4 Směrování v rámci budovy U5

Mezi jednotlivými páteřními přepínači je nutná přítomnost směrování. Virtuální sítě pro výukové laboratoře budou zakončeny vždy na jednom z páteřních přepínačů podle rozvodny, kam je z dané laboratoře svedena strukturovaná kabeláž. Aby se síťový provoz dostal do těchto sítí (např. odpovědní pakety v rámci konexí, které vznikají v učebnách), musí se o těchto sítích dozvědět i ostatní páteřní přepínače v budově, hlavně ty, které zajišťují připojení budovy k internetu.

Páteřní přepínače jsou v tuto chvíli čtyři a do budoucna se dá předpokládat, že jejich počet může ještě vzrůstat, proto nepřipadá v úvahu statické směrováni (ruční nastavení všech sítí na všech přepínačích). Je zde tedy možnost využití některého ze směrovacích protokolů, kdy se informace o existenci (a dostupnosti) sítě rozšíří mezi ostatní páteřní směrovače automaticky z toho přepínače, který síť obsluhuje.

Ideálním protokolem je OSPF[19] [13]. Všechny páteřní přepínače v budově U5 budou dány do jedné logické oblasti, která bude označena samostatným číslem - *area 5*. Oblast číslo 0 (nula) je vyhrazena pro prvky páteřní sítě celé organizace, zatím se nebude používat. Do budoucna je ale možné rozšířit tuto topologii na další části univerzity (podobně jako

[19]Open Shortest Path First, z angl.

budova U5 mohou být řešeny další budovy) a do oblasti 0 by pak byly vloženy ty síťové prvky, které propojují jednotlivé budovy.

Korektní fungování směrování pomocí protokolu OSPF předpokládá správnou konfiguraci na všech zúčastněných přepínačích: musí být zadáno shodné číslo oblasti, přepínače musí komunikovat v rámci jednoho segmentu sítě a musí být správně nastavena autentizace přepínačů [14]. Číslo oblasti v budově U5 je **5**, společný segment je virtuální síť `10.5.0.0/24`.

Dále je třeba vybrat dva přepínače, které budou hrát roli hlavního a záložního směrovače, ovšem v tom smyslu, že budou vypočítávat cesty a jejich ceny ke všem dostupným sítím a tyto informace pak budou předávat přímo ostatním přepínačům - ty pak nemusejí tento výpočet provádět a šetří výkon. Logicky tato volba padá na **gswitch-u5-mdf** a záložní **gswitch-u5-idf2**. Volba těchto dvou směrovačů je ovšem zcela automatická a záleží na prioritě směrovače (není-li nastavena, má hodnotu 1) a jeho IP adrese [15]. Hlavní směrovač je ten s nejvyšší prioritou nebo nejvyšší IP adresou. V konfiguraci OSPF na přepínači **gswitch-u5-mdf** tedy bude priorita nejvyšší, na záložním **gswitch-u5-idf2** bude druhá nejvyšší, u ostatních přepínačů nebude priorita nijak upravována.

Kromě sítí, které mají všechny koncové stanice připojeny pomocí strukturované kabeláže do přepínačů v jedné rozvodně, budou ale existovat ještě další sítě určené k jiným účelům, především jde o sítě pro přístup zaměstnanců a sítě pro servery, které poskytují veřejné služby. Tyto sítě budou zakončeny vždy na páteřních přepínačích **gswitch-u5-mdf** i **gswitch-u5-idf2** a bude zde využit protokol HSRP.

IP rozsah	Použití
10.5.0.0/20	Síťě pro správu aktivních páteřních a síťových prvků
10.5.16.0/20	Sítě pro servery poskytující veřejné služby
10.6.32.0/20	Sítě pro bezdrátově připojené počítače
10.5.64.0/18	Zaměstnanecké sítě
10.5.128.0/20	Menší sítě zakončené na přepínači v MDF
10.5.144.0/20	Menší sítě zakončené na přepínači v IDF1
10.5.160.0/20	Menší sítě zakončené na přepínači v IDF2
10.5.176.0/20	Menší sítě zakončené na přepínači v IDF3
10.5.192.0/18	Rezerva, zatím nevyužito

Tabulka 9: Rozdělení IP adresního prostoru v budově U5

Důležitou součástí směrování je tzv. *default route*. Paket, který má být na směrovači poslán do sítě, kterou směrovač nemá ve své směrovací tabulce, je pak poslán právě tímto směrem. Páteřní přepínače **gswitch-u5-idf1** a **gswitch-u5-idf3** budou mít tuto cestu nastavenou na IP adresu páteřního virtuálního směrovače (`10.5.0.1`), přepínače **gswitch-u5-mdf** a **gswitch-u5-idf2** pak budou mít tuto cestu na IP adresu centrálního univerzitního směrovače (`10.0.0.1`).

2.3.5 Segmentace sítě ve výukových laboratořích

V budově U5 je několik výukových laboratoří, ve kterých je 12-25 počítačů (s výjimkou areálové studovny o cca. 50 počítačích). V učebnách se vede výuka nebo různá měření, popř. dochází k experimentům. Lidé (jak pedagogové, tak studenti) se v učebnách často střídají a podle toho může nastat situace, kdy je třeba provoz v jedné učebně úplně nebo částečně filtrovat (z bezpečnostních důvodů, při vypracovávání testů apod.). Každá učebna tedy musí dostat vlastní virtuální síť a adresní prostor. Strukturovaná kabeláž v budově U5 je vedena tak, že vždy všechny počítače v jedné učebně jsou připojeny do přístupových přepínačů v jedné rozvodně. To se velmi hodí, protože vždy páteřní přepínač v dané rozvodně bude mít jedno síťové rozhraní v každé učebně a bude fungovat pro počítače v učebně jako brána. Zároveň na tomto síťovém rozhraní může páteřní přepínač snadno filtrovat provoz z učebny směrem do dalších částí sítě nebo opačným směrem.

Adresní prostory musí být dostatečně veliké - je třeba počítat s tím, že aktuální počet počítačů v učebně je menší než počet zásuvek strukturované kabeláže a že v budoucnu může nastat situace, kdy v každé učebně bude navíc samostatný bezdrátový přístupný bod, který by umžňoval připojení i bezdrátových pracovních stanic v téže učebně (např. notebooky). Adresní prostor přidělený celé budově je naprosto dostatečný, proto není třeba úplně šetřit a jako omezující hranici můžeme použít velikost jednotlivých učeben. Až na výjimky nebude v učebnách zřejmě více než 30 lidí, takže adresní prostor, kam je možné připojit 61 koncových stanic, by měl být dostatečný. Pokud by praxe ukázala, že tento prostor nestačí, neměl by být problém s readresací na větší prostor.

2.3.6 Segmentace zaměstnanecké části sítě

Část sítě v budově U5, která je nyní určena pro pracovní stanice zaměstnanců univerzity, obsahuje v současné chvíli přes 300 koncových stanic. Síť není dále nijak rozdělena na menší části, takže veškerý síťový provoz typu *broadcast*, který vyšle jedna pracovní stanice, je distribuován všem dalším stanicím. Většina pracovních stanic má nainstalovaný operační systém na platformě `Microsoft Windows`, který generuje velké množství takového provozu ve snaze zjistit co nejvíce informací o dalších koncových zařízeních v síti. Z globálního hlediska nelze tento provoz redukovat jinak než rozdělením sítě na menší části.

Učebna	Počítačů	Adresní prostor	Rozvodna
A218	54	10.5.128.0/24	MDF
B202	13	10.5.144.0/26	IDF1
B203	13	10.5.144.64/26	IDF1
B204	13	10.5.144.128/26	IDF1
B205	13	10.5.144.196/26	IDF1
B206	24	10.5.145.0/26	IDF1
...			
D303	13	10.5.160.0/26	IDF2
D304	25	10.5.160.64/26	IDF2
...			

Tabulka 10: IP adresace učeben. Seznam je zkrácený, výukových laboratoří je několik desítek a adresace je zřejmá.

Požadavky uživatelů na rozdělení sítě nejsou žádné - není třeba oddělovat některé uživatele od ostatních a zamezovat jim různě v přístupech. Proto bude síť segmentována podle logického členění samotné fakulty, tedy každý ústav bude mít vlastní virtuální síť. V budově U5 se ale nachází některé ústavy jiných fakult nebo jiné organizační složky univerzity, na ty bude nahlíženo stejně jako na ústav. V případě potřeby pak není problém vytvořit i separátní virtuální sítě podle jiných kritérií (např. pro technické pracovníky, pro asistentky, studijní oddělení, děkanát apod.). Adresní prostor vyčleněný pro všechny tyto sítě je `10.5.64.0/18`.

Ani u jedné ze zamětaneckých sítí nelze předem říct, že počítače v dané síti budou připojeny vždy do jedné rozvodny, neboť kabeláž v té části budovy, kde zaměstnanci fyzicky jsou, je rozdělena na dvě části (východní, kde je kabeláž svedena do IDF3, a západní, kde je kabeláž svedena do MDF), zatímco ústavy jsou většinou rozděleny po patrech. Ústav, který se nachází na jednom patře, tedy bude mít zcela jistě některé koncové stanice v rozvodně IDF3 a některé v MDF. Z toho důvodu je nutné použít u všech těchto sítí protokol HSRP, funkci brány bude vždy zajišťovat 1. adresa v rozsahu (virtuální směrovač), 2. a 3. adresu budou mít páteřní přepínače **gswitch-u5-mdf** a **gswitch-u5-idf2**, 4. adresa bude volná jako rezerva a ostatní IP adresy mohou být použity pro koncová zařízení (např. u Ústavu počítačových a komunikačních systémů bude IP adresa virtuálního směrovače `10.5.66.1`, síťové rozhraní na **gswitch-u5-mdf** bude mít adresu `10.5.66.2`, **gswitch-u5-idf3** bude mít adresu `10.5.66.3`, IP adresa `10.5.66.4` bude volná a ostatní IP adresy (`10.5.66.5` - `10.5.67.254` včetně) mohou být použity pro koncové stanice).

Všechny zaměstnanecké virtuální sítě mají adresní prostor o velikosti 512 IP adres. Toto číslo je velmi vysoké oproti předpokládaným počtům zařízení, důvodem je ale použití protokolu DHCP v redundatním režimu, což snižuje reálnou využitelnost adresního prostoru

Organizační složka	Adresní prostor
FAI - Ústav informatiky a umělé inteligence	10.5.64.0/23
FAI - Ústav počítačových a komunikačních systémů	10.5.66.0/23
FAI - Ústav automatizace a řídicí techniky	10.5.68.0/23
FAI - Ústav elektroniky a měření	10.5.70.0/23
FAI - Ústav bezpečnostního inženýrství	10.5.72.0/23
FAI - Ústav matematiky	10.5.74.0/23
FAI - Ústav řízení procesů	10.5.76.0/23
FT - Ústav výrobního inženýrství	10.5.78.0/23
FT - Ústav fyziky a materiálového inženýrství	10.5.80.0/23
UNI - Ústav jazyků	10.5.82.0/23
FAME - Ústav tělesné výchovy	10.5.84.0/23

Tabulka 11: IP adresace zaměstnanecké části sítě

na polovinu (bude vysvětleno v jedné z následujících kapitol, která se věnuje tomuto protokolu samostatně). Celý adresní prostor přidělený budově U5 je navíc dostatečně velký, takže není důvod k jakémukoliv šetření.

2.3.7 Samostatná síť pro veřejné služby

Speciální část sítě musí být vyhrazena pro servery poskytující veřejné služby. V současné době jsou tyto servery rozmístěny v jednotlivých rozvodnách podle toho, kde je více místa. Všem serverům bude přidělen jeden adresní prostor `10.5.16.0/24`, brána bude virtuální směrovač `10.5.16.1`, pomocí protokolu HSRP bude tuto IP adresu obsluhovat jeden z páteřních přepínačů **gswitch-u5-mdf** (`10.5.16.2`) a **gswitch-u5-idf3** (`10.5.16.3`). IP adresa `10.5.16.4` bude rezervovaná a ostatní adresy (5 - 254 včetně) budou volně k použití.

Pokud by se v budoucnu vyskytl projekt, který by potřeboval více veřejně dostupných serverů umístit do jedné samostatné virtuální sítě, nebude to problém, vyčlení se pro ni vhodně velký adresní rozsah z `10.5.16.0/20`. Pokud budou všechny servery umístěny v jedné rozvodně, bude virtuální síť ukončena na páteřním přepínači v této rozvodně, v opačném případě bude nutno použít protokol HSRP podobně jako u sítě `10.5.16.0/24`.

Servery, které poskytují veřejné služby, musí být ale dostupné i z internetu, to ale znemožňují jejich privátní adresy. Na centrálním univerzitním směrovači, který zajišťuje připojení univerzity do sítě, bude tedy nastaven překlad adres, kdy se vždy vybraná veřejná IP adresa na tomto směrovači přeloží na příslušnou privátní IP adresu. Např. současný server **vyuka.fai.utb.cz** má IP adresu `195.178.89.7`, umístěním serveru do segmentu

pro veřejné služby ale může dostat adresu `10.5.16.7`. Příchozí konexe z internetu směrem na server **vyuka** (tedy na IP adresu `195.178.89.7`) dojde na univerzitní směrovač, ten zajistí překlad cílové adresy na `10.5.16.7` a spojení je pak úspěšně navázáno.

2.3.8 Malé samoúčelné sítě

V budově U5 již nyní existuje několik malých sítích, ve kterých jsou speciální zařízení (viz Tabulka 2, sítě 82 a 641-664), ty je třeba v novém návrhu posoudit samostatně, a to hlavně z toho hlediska, zda je nutné, aby existovaly v rámci samostatné celouniverzitní virtuální sítě nebo zda by bylo možné z nich udělat separátní malé sítě v rámci budovy U5.

Toto kritérium je nutné vyhodnotit především z důvodu možností nastavení jednotlivých zařízení, která se v sítích nacházejí. V tuto chvíli bohužel není k dispozici veškerá dokumentace (např. u zařízení v síti č. 648 ACCESS-SYS pro ověřování přístupů do učeben nebo jiných místostí pomocí magnetických karet), takže rozhodnutí o jednotlivých sítích by muselo být učiněno až později.

V případě, že by bylo možné tyto sítě separovat od zbytku univerzitní sítě, byly by pro ně vytvořeny menší sítě zřejmě buď z IP rozsahu, který je určen pro veřejné služby, nebo (poku by to bylo možné) z velkého rozsahu, který je přidělen jednotlivým rozvodnám (např. pro síť č. 614 TELEPHONE-CENTRAL by stačilo vyčlenění malé sítě z IP rozsahu 10.5.128.0/20, dle rozdělení v Tabulce 9). Pokud by oddělení sítě nebylo možné, musela by se daná virtuální síť ponechat v současném stavu. Takový stav ale není úplně výhodný z hlediska směrování mezi jednotlivými budovami univerzity, takže do budoucna by se mělo hledat řešení, např. v podobě samostatného směrovače (v budově U5), který by mohl využít funkce protokolu L2TP[20] nebo překladu IP adres, popř portů při komunikaci v rámci protokolu IP.

2.3.9 Připojení bezdrátových zařízení

Nastavení připojení bezdrátových přístupových zůstává stejné, změní se pouze směrování a adresace, všechny 3 nyní používané sítě pro připojení bezdrátových zařízení (viz Tabulka 4) ovšem budou zakončeny na zařízeních **gswitch-u5-mdf** a **gswitch-u5-idf2**, funkcionalita virtuálních síťových rozhraní, která je nyní na celouniverzitním směrovači, bude přenesena na virtuální rozhraní hlavních dvou páteřních přepínačů v budově U5. Adresní prostor bude zvětšen, aby pokryl zvyšující se množství bezdrátově komunikujících zařízení a do budoucna i počet bezdrátových přístupových bodů:

Virtuální síťová rozhraní jednotlivých přístupových bodů, která slouží k jejich administraci, budou zatím ponechána v administrativním segmentu `10.5.0.0/24`, pokud by jejich počet vzrůstal, bude jim vyhrazen vlastní segment.

[20] Layer 2 Tunelling Protocol, z angl.

IP rozsah	Název sítě
10.5.32.0/22	Připojení studentů UTB
10.5.36.0/22	Připojení zaměstanců
10.5.40.0/22	Připojení EDUROAM

Tabulka 12: Nová adresace bezdrátových zařízení

2.3.10 Používání protokolu DHCP

Ve všech virtuálních sítích, které jsou vyčleněny pro učebny, lze pro zjednodušení správy jednotlivých pracovních stanic používat protokol DHCP. Tento protokol slouží především k automatizovanému nastavení síťových rozhraní jednotlivých počítačů v síti. Počítač, který byl právě zapnut, neví nic o nastavení místní sítě, proto (pokud je tak nastaven) vyšle pouze speciální paket *DHCPDISCOVER* (typ broadcast) a čeká, zda se na síti nevyskytuje DHCP server, který by zaslal odpověď (paket *DHCPOFFER*). V této odpovědi se počítač dozví, jaká mu byla přidělena IP adresa, jaká je síťová maska, adresa brány, DNS serveru a někdy i další nastavení. Celý protokol je popsán v dokumentu RFC 2131 [16], jednotlivé parametry pro koncové stanice jsou popsány v RFC 1533 [17].

Používání tohoto protokolu je ve výukových laboratořích velmi výhodné, není nutné nastavovat síť pro každou pracovní stanici zvlášť, DHCP server zajistí, že nově nastartovaný počítač dostane některou z volných adres v přiděleném rozsahu. Navíc používání tohoto protokolu je nutné v případě vzdáleného bootovaní těchto stanic. Ze stejného důvodu je možné používat tento protokol i v zaměstnaneckých sítích, ovšem dá se předpokládat, že někteří uživatelé budou vyžadovat, aby jejich IP adresa byla neměnná (to při standardním běhu DHCP není zaručeno). V té části sítě, do které jsou zapojeny servery poskytující veřejné služby, je možné DHCP server použít, ale obvykle se to nedělá, právě z toho důvodu, že IP adresace je přesně daná a není problém, aby jednotlivé počítače byly nastaveny ručně.

Protože počítače komunikují s DHCP serverem nejprve pomocí paketů typu *broadcast*, musí být DHCP server na stejném síťovém segmentu (tj. musí být umístěn ve stejné síti), protože směrovače tento typ paketu ze sítě ven neposílají. Nejideálnější možnost je tedy umístit DHCP server přímo na směrovač (bránu), v případě sítí v budově U5 tedy na páteřní přepínače. V případě výukových laboratořích bude DHCP server (ve smyslu software) pro každou učebnu umístěn na páteřním přepínači v příslušné rozvodně. Počítačům v učebně pak DHCP server vždy předá následující informace:

- IP adresu pro koncovou stanici a masku sítě
- IP adresu brány
- IP adresu DNS serveru

V případě, že bude třeba omezit síťový provoz z učebny nebo do učebny (např. při testech apod.), bude výhodné, pokud počítač pedagoga bude mít vždy stejnou IP adresu. Aby DHCP server právě učitelskému počítači přiřadil vždy stejnou IP adresu, zjistí se MAC adresa tohoto počítače a DHCP server se nastaví tak, aby této MAC adrese vždy přidělil právě vymezenou IP adresu. Stejně tak lze postupovat i v případě zaměstnaneckých sítí: je-li třeba některému počítači přidělit vždy stejnou IP adresu a uživatel si ji nemůže nebo nechce nastavit sám, sdělí své MAC a IP adresy DHCP serveru a ten si pak bude tuto dvojici pamatovat.

Páteřní přepínače lze také nastavit tak, aby DHCP požadavky od jednotlivých koncových zařízení nezpracovávaly (tj. aby softwarový DHCP server byl vypnutý), ale pomocí směrování je posílaly na konkrétní počítač v libovolné jiné síti (do požadavku ale musí přepínač navíc dodat informace o tom, ze které virtuální sítě požadavek přichází). Takové nastavení by pak umožňovalo mít centrální DHCP server, který by mohl přidělovat IP adresy do všech sítí. takové řešení má ale příliš mnoho nevýhod:

- zpoždění odpovědi - pokud je DHCP server příliš vzdálen od sítě, kterou má řídit, může dojít ke zpoždění nebo úplné ztrátě odpovědi z důvodu přetížení linek nebo nedostupnosti serveru kvůli možným výpadkům síťových zařízení nebo přenosových linek, které jsou mezi sítí a DHCP serverem
- v případě úplné nedostupnosti DHCP serveru nemohou bez ručního zásahu koncové stanice používat tu část sítě, která je pro ně dostupná (a která by jim mohla stačit)
- DHCP server před přidělením IP adresy nejprve pomocí protokolu ICMP[21] zjišťuje, zda je IP adresa opravdu volná (někdo si ji mohl nastavit ručně, aniž by se DHCP serveru zeptal), pakety tohoto protokolu ovšem mohou být mezi DHCP serverem a vlastní sítí blokovány (pokud se po cestě vyskytuje nějaké zařízení, které je schopno omezit síťový provoz na základě nejých podmínek)
- každá nová síť, která se vytvoří na páteřních přepínačích a která má mít dostupný DHCP server, musí být navíc zavedena na DHCP serveru, to znamená administraci jedné věci na více zařízeních a vyšší zátěž pro administrátory
- přenos DHCP paketů zbytečně zatěžuje přenosové linky
- v případě, že se k DHCP paketům dostane nějaký útočník, může si snadno vytvořit detailní adresní mapu celé organizace

V případě umístění DHCP serveru na páteřní přepínače v budově U5 je ovšem třeba počítat ještě s nasazením virtuálních směrovačů na ty sítě, které nejsou zakončeny jen v jedné rozvodně - typicky zaměstnanecké sítě. Funkci brány zde mohou vykonávat dvě zařízení, přičemž jedno musí být schopno plně nahradit druhé. Pokud bude DHCP server

[21] Internet Control Message Protocol, z angl.

umístěn na jednom přepínači, musí být i na druhém, oba DHCP servery musí přidělovat IP adresy ze stejného rozsahu, pokud pak jeden ze serverů přidělí IP adresu, druhý DHCP server ji už přidělit nesmí. Některé softwarové DHCP servery mají možnost navázat spolu kontakt, určit si priority a informovat se navzájem o přidělovaných IP adresách (např. ISC DHCP Server [18]), DHCP server na platformě `Cisco` ovšem něco takového neumí, proto se tato situace řeší pomocí tzv. *Split DHCP* [19].

Tato technologie funguje tak, že adresní prostor je rozdělen na poloviny, IP adresy z jedné poloviny přiděluje jeden DHCP server, IP adresy z druhé poloviny přiděluje druhý. Koncová stanice, která dostane na jeden požadavek 2 odpovědi, si pak může vybrat (obvykle si zvolí tu odpověď, kterou dostane dříve). Případné výjimky, kdy je třeba na základě MAC adresy přidělit konkrétní IP adresu, musí být zavedeny do konfigurací obou DHCP serverů. Konkrétně v případě zaměstnanecké sítě Ústavu počítačových a komunikačních systémů by adresní prostor `10.5.66.0/23` mohl být rozdělen takto:

IP adresa	Účel
10.5.66.0	IP adresa sítě
10.5.66.1	IP adresa virtuálního směrovače
10.5.66.2	IP adresa síťového rozhraní na **gswitch-u5-mdf**
10.5.66.3	IP adresa síťového rozhraní na **gswitch-u5-idf2**
10.5.66.4	rezervovaná IP adresa
10.5.66.5 - 10.5.66.255	IP adresy, které přiděluje **gswitch-u5-mdf**
10.5.67.0 - 10.5.67.254	IP adresy, které přiděluje **gswitch-u5-idf2**
10.5.67.255	IP adresa pro pakety typu *broadcast*

Tabulka 13: Rozdělení adresního prostoru zaměstnanecké sítě

Adresní prostory, ze kterých jednotlivé přepínače přidělují IP adresy, není úplně symetrický, to ale vůbec nevadí, podstatné je, že se rozsahy nepřekrývají. Teoreticky je možné přidělit celý rozsah na oba dva DHCP servery, rozdělením adresního prostoru na dvě části se ale vyhneme možným potížím s přidělením jedné IP adresy více strojům. Technologie *Split DHCP* je hlavním důvodem pro velký adresní prostor přidělený jednotlivým zaměstnaneckým sítím.

2.3.11 Vlastní DNS v budově U5

Přestože komunikace mezi jednotlivými síťovými zařízeními probíhá pouze na základě znalosti IP adres jednotlivých zařízení, uživatel se s nějakou adresací nemusí ani setkat, neboť přirozeně místo číselných adres používá jmenné názvy. Protokol DNS pak převádí jednotlivé názvy na IP adresy automaticky. Aby byla budova U5 více nezávislá na stavu

centrálního univerzitního serveru, měla by mít vlastní DNS server. Ten by měl být umístěn ve virtuální síti `10.5.16.0/24` spolu s dalšími servery, které poskytují veřejné služby. Všechny počítače v budově U5 by pak měly používat pro DNS dotazy právě tento DNS server.

Server by měl být standardně zabezpečen: neměl by poskytovat informace o své verzi a rekurzivní DNS dotazy (tj. dotazy na názvy a IP adresy, které jsou mimo budovu nebo mimo univerzitu a DNS server musí sám vytvářet vlastní dotazy na vzdálené počítače do internetu) by měl zpracovávat jen pro počítače v budově.

Aby se trochu ušetřil DNS provoz směrem z budovy ven, měl by mít tento DNS server roli sekundární DNS serveru pro celou doménu **utb.cz**. Obsah celé zóny **utb.cz** by dostával pravidelně automaticky od primárního DNS serveru (**sun.utb.cz**), samozřejmě bez možnosti změny. Doménu třetího řádu **fai.utb.cz** pak bude kompletně obsluhovat pouze tento server (centrální **sun.utb.cz** pak na oplátku může být sekundární server pro tuto doménu, opět bez možnosti změny, navíc tímto krokem dojde k delegaci části administartivních úkonů správce celouniverzitního DNS serveru na odpovědné osoby na U5).

Jednotlivé počítače v budově U5, které potřebují i vlastní jméno (některé pracovní stanice toto jméno nepotřebují) pak budou mít vlastní záznam v DNS serveru v budově U5 v rámci domény **fai.utb.cz** (např. kohout.fai.utb.cz). Tuto doménu je pak možné dále členit, např. pro přepínače lze vytvořit doménu **backbone.fai.utb.cz**, pro všechny výukové laboratoře **lab.fai.utb.cz** a tu pak dále dělit podle názvu laboratoře (b204.lab.fai.utb.cz). Tímto dělením lze pak jednotlivé sítě a počítače, které se vyskytují ve velkém množství, snáze administrovat, DNS dotazy do jednotlivých zón lze navíc snadno omezovat.

Počítače pracovníků z jiných fakult, kteří ale pracují v budově U5 a potřebují název svého počítače v DNS, pak buď musí mít záznam v DNS serveru své fakulty (DNS server umístěný v budově U5 může zastat sekundární DNS server i pro další fakulty) nebo v centrálním univerzitním DNS serveru.

DNS server ovšem musí obsluhovat i dotazy do domény **fai.utb.cz** z internetu. V jedné z předchozích kapitol byl popsán překlad IP adresy servery **vyuka.fai.utb.cz** (195.178.89.7 na 10.5.16.7). Fakultní DNS server musí ovšem vracet obě dvě IP adresy - pro dotazy z privátní sítě musí vracet privátní adresu, pro ostatní zdrojové dotazy musí vracet veřejnou IP adresu. Toho lze snadno docílit pomocí *splitdns* [20], kdy právě na základě zdrojové IP adresy DNS dotazu server správně odpovídá. V případě použití běžného DNS softwaru **bind** budou existovat dva zónové soubory pro doménu **fai.utb.cz**, jeden bude obsahovat privátní adresy a druhý bude obsahovat veřejné. Pomocí konfiguračních direktiv *view* se pak na základě zdrojové IP adresy DNS dotazu použijí data z jednoho nebo druhého souboru. Servery poskytující veřejné služby tak budou snadno dostupné jak z internetu,

tak z univerzitní sítě, při tom všechen provoz v rámci univerzitní sítě bude správně veden přes privátní IP adresy.

2.4 Bezpečnost

2.4.1 Porty přístupových přepínačů

Porty na přístupových přepínačích, do kterých jsou připojeny koncové stanice, jsou vstupním bodem, kterým stanice do sítě posílají data k dalšímu doručení. Je to tedy ideální místo, kde se bránit nechtěnému síťovému provozu, kde lze včas zamezit šíření škodlivé informace na síťové prvky nebo další koncové stanice.

Přenos dat na 2. vrstvě referenčního modelu OSI je snadno ovlivnitelný, jednotlivá zařízení se spoléhají na informace, které dostanou od jiných zařízení, bez ověřování. Tento postup je často zneužíván útočníky k tomu, aby podstrčili falešné informace, zejména co se týče MAC adres nebo mapování MAC adres na IP adresy. Drtivá většina těchto útoků využívá možnost vyslat z jednoho připojenho zařízení více rámců, které obsahují různé MAC adresy. Pokud se na připojeném zařízení vyskytuje více MAC adres, může to znamenat, že se někdo pokouší o nějaký druh útoku proti L2 komunikaci.

Ochrana je zdánlivě snadná - nastavit přepínač tak, aby na přístupovém portu povolil právě jednu MAC adresu, v případě výskytu další je pak třeba ihned jednat, např. přístupový port vypnout. Tento postup ovšem může být někdy rizikový: pokud se vymění koncová stanice (např. zaměstnanec zapojí do zásuvky strukturované kabeláže místo stolní pracovní stanice svůj notebook nebo v případě výměny vadné síťové karty), objeví se během krátkého času na přístupovém portu dvě MAC adresy. Ruční ošetření takových stavů ze strany administrátora by při velkém počtu zaměstnanců a studentů ovšem znamenala velkou zátěž - na druhou stranu povolení 2 MAC adres už může vést k úspěšnému útoku pomocí *ARP Cache Poisoning*. Vhodným řešením není ani centrální databáze *povolených* MAC adres, ať už takových, jejichž komunikace je povolena, nebo takových, jejichž komunikace je povolena na konkrétním portu - případný útočník si může snadno tyto informace zjistit z běžného síťového provozu a po úplném odstavení povolené stanice si připojit vlastní s podvrženými údaji a úplně se tím vydávat za počítač nic netušícího jiného uživatele. Správa těchto údajů je navíc opět administrativně velmi náročná - již nyní je v budově FAI několik stovek počítačů, jen pořízení úvodních dat může trvat dlouho.

I přes rizika spojená s omezením počtu MAC adres, které se mohou vyskytovat na jednom přístupovém portu, se jedná o dobré bezpečnostní opatření. Dopad rizik na běžné uživatele, kteří by se tímto omezením mohli dostat do problémů, se dá velmi zmírnit, přístupové přepínače `Cisco` mají relativně velké možnosti ohledně nastavení celé této technologie. Nastavením *port-security* na přístupových portech se nejprve omezí počet MAC adres na přístupových portech na 1, výskyt většího množství MAC adres již znamená automatické vypnutí portu (nastavení portu do režimu *error-disable*). Port se z tohoto nastavení do

normálního režimu dá nastavit buď ručně (zásahem administrátora) nebo automaticky - přepínač si každé 2 minuty zkontroluje, které porty jsou ve stavu *error-disable*, a opět je zapne. Takové nastavení znemožňuje většinu útoků na L2 komunikaci a zároveň umožňuje i výměnu koncových zařízení, byť s malou časovou prodlevou.

Toto nastavení může být velmi kritické pro ty uživatele, kteří chtějí rozšířit možnost připojení k síti tak, že si do zásuvky strukturované kabeláže zapojí další přepínač (to jim umožní do jedné zásuvky připojit více počítačů). Tento scénář je opravdu zakázaný, zapojení přepínače do velké síťové infrastruktury může způsobit mnoho problémů: uživatel může nevědomky vytvořit smyčku na 2. vrstvě OSI, může obcházet obcházet pravidlo jedné MAC adresy a provádět útoky proti L2 komunikaci jiných účastníků sítě. Pokud tedy nastane situace, kdy uživatel potřebuje zapojit více počítačů, musí se využít větší množství zásuvek strukturované kabeláže v místnosti a koncová zařízení pak budou zapojena standardním způsobem do přístupových přepínačů (i za cenu zvýšení množství přístupových přepínačů v rozvodnách).

Pokud je množství připojených koncových stanic větší než počet zásuvek strukturované kabeláže, může se vyčlenit jeden přístupový přepínač pouze pro danou místnost nebo skupinu koncových stanic a bude umístěn přímo v místnosti (mimo rozvodnu). Druhou možností je instalace směrovače pro místnost nebo skupinu koncových stanic: jedno síťové rozhraní směrovače bude připojeno do přístupového přepínače v rozvodně a z hlediska páteřní sítě bude vystupovat jako běžná koncová stanice. Další síťové rozhraní směrovače již může být připojeno do libovolného lokálního přepínače, popř. samo směrovací zařízení již může přepínač obsahovat v sobě. Podmínkou správného fungování je ovšem vhodný výběr adresace sítě za směrovačem (nejlépe privátní rozsah mimo univerzitního `10.0.0.0/8`) a překlad IP adres koncových stanich na IP adresu směrovače při komunikaci koncových stanic do sítě v budově U5 (nebo dále do internetu).

Navrhované přístupové přepínače `Cisco` řady `2960` umožňují kontrolu příchozích paketů v komunikaci na 3. vrstě OSI již na přístupových portech, každý příchozí paket může být zkontrolován proti definovaným pravidlům a případně může být přepínačem úplně ignorován (nebude puštěn do další části sítě). Tato funkcionalita je sice trochu omezená (platí pouze na pakety, které přichází na port, nikoliv na odchozí pakety), ale plně postačující na filtrování parazitního provozu - např. u tiskáren se síťovým rozhraním lze snadno zakázat, aby tiskárna posílala pakety protokolem *NetBIOS* a byla tak snadno přístupná uživatelům, podobně lze i specifikovat pouze seznam IP adres, se kterými koncové zařízení smí komunikovat, popř. protokol nebo omezení protokolu.

Porty na přepínačích, které nejsou přiřazeny do konkrétní virtuální sítě, ale umožňují přenos ve více virtuálních sítích (tzv. *trunk*), musí mít speciální nastavení. Obecně platí, že aby bylo takové spojení funkční, musí být na obou stranách spojení nastavena stejná rychlost, duplexita a metoda zapouzdření. Dále se musí zařízení na obou stranách spojení

dohodnout, že jde opravdu o spojení typu *trunk*, přepínače `Cisco` k tomu používají protokol DTP[22]. Z bezpečnostního hlediska není používání tohoto protokolu doporuené, neboť koncová stanice (u které může být i útočník) by mohla vyjednat, že se jedná o spojení typu *trunk*, a tím se dostat i do jiných virtuálních sítí [5].

Používání protokolu DTP se vypne automaticky, je-li přístupový port nastaven do režimu *access* - takové nastavení bude na všech přístupových portech. Na portech, kde se předpokládá spojení typu *trunk*, bude tento protokol také vypnut, spojení se úspěšně naváže až při správném nastavení i na druhé straně spoje - to se v případě nové struktury sítě vztahuje na spoje mezi páteřními přepínači a na spoje mezi přístupovými a páteřními přepínači [21].

2.4.2 Protokol STP

Hlavní functionalitu protokolu STP zajišťují malé zprávy, které se periodicky zasílají mezi jednotlivými přepínači, nazývají se *BPDU*[23]. Přepínač pak díky datům, které dostává pomocí těchto zpráv, dokáže určit topologii sítě na 2. vrstě OSI, detekovat v nich smyčky a vybírat nejvhodnější body k jejich přerušení. Přepínač sám také tyto zprávy posílá dále, aby i ostatní přepínače měly shodný náhled na topologii sítě.

Tyto zprávy ovšem může přepínači podstrčit i útočník, ze své stanice může odesílat zprávy, které vnutí spolupracujícím přepínačům jiný pohled na topologii (především díky upravené prioritě útočníkova zařízení), a úspěšně přesměrovat veškerý síťový provoz přes vlastní zařízení [5]. Proti tomuto druhu útoku se mohou přepínače aktivně bránit zapnutím funkcionality `BPDU Guard`. Princip spočívá v tom, že administrátor sítě má znalost o její skutečné topologii a dokáže tak předem určit, na kterých portech přepínače se mohou tyto zprávy objevit a na kterých se naopak objevit nesmějí.

U portů na přístupových přepínačích se předpokládá, že budou nastaveny v režimu *portfast*, výjimkou budou pouze spojení k páteřním přepínačům. Jako aktivní ochrana proti útokům pomocí BPDU zpráv bude tedy `BPDU Guard` zapnutý globálně: v případě, že přepínač obdrží BPDU zprávu z portu v režimu *portfast*, okamžitě port vypne, resp. přepne ho do stavu *error-disable*.

Vzhledem k vysokému počtu přístupových portů a malému počtu administátorů není úplně ekonomické, aby se každý takto vypnutý port musel obnovovat ručně. Navíc by útočník mohl uměle vypnout funkcionalitu sítě odesláním BPDU zpráv do různých zásuvek strukturované kabeláže. Z toho důvodu budou přepínače nastaveny tak, že každé 2 minuty přepínač sám zkontroluje porty a v případě, že najde některý z nich vypnutý pomocí funkce `BPDU Guard`, opět ho zapne. Administrátor je o takové akci informován pomocí logových

[22]Dynamic Trunk Protocol, z angl.
[23]Bridge Protocol Data Unit, z angl.

zpráv, systém, který logovací zprávy zpracovává, pak může sám vyhodnotit, kdy dochází k opakovanému problému a teprve potom vyzvat administrátora k ručnímu zásahu.

V případě, že některá zařízení připojená do infrastruktury sítě nemohou být v režimu *portfast*, nelze využít `BPDU Guard` globálně pro celé zařízení - v tom případě pak musí být zapnut na jednotlivých portech. Typickým příkladem mohou být páteřní přepínače, kde většina portů bude určena pro připojení dalších přepínačů a BPDU zprávy zde budou nutností, ale do některých portů mohou být zapojeny servery nebo přístupové body pro bezdrátová zařízení.

Pokud by bylo nutné k síti v budově U5 připojit další přepínače, nad kterými by měl administrátor omezenou nebo žádnou kontrolu, nastaví se na příslušném portu (nebo více portech) ještě ochrana *Root Guard*. Tato ochrana pak zajistí, že vlastní topologie v páteřní síti nebude nijak narušena ani v případě, že tato připojená zařízení budou zasílat BPDU zprávy, které by mohly vést k nutnosti tuto topologii přepočítávat.

2.4.3 Protokol VTP

Protokolem VTP se šíří mezi jednotlivými přepínači informace o seznamu virtuálních sítí (názvy a čísla). Aby se jednotlivé virtuální sítě daly dobře používát, musí být tento seznam jednotný na všech zařízeních v celé přístupové i distribuční vrstvě, to je v případě budovy U5 na všech přepnačích. Díky protokolu VTP postačí, pokud bude seznam administrován pouze na jednom přepínači (**gswitch-u5-mdf** bude vybrán jako hlavní, bude tedy *VTP server*), ostatní přepínače budou tento seznam pouze odebírat a nebudou mít možnost ho nijak měnit (budou v režimu *VTP client*). VTP server posílá přes spojení typu *trunk* oznámení o změnách, ostatní přepínače pak změny promítnou automaticky do své konfigurace.

Protokol VTP prošel během několika let vývojem a na zařízeních `Cisco` je k dispozici ve verzích 1, 2 nebo 3 (verze musí být nastavena na všech přepínačích shodně). V případě sítě budovy U5 bude použita verze 3 [22]:

- jediná umí spolupracovat s protokolem MSTP
- umožňuje zabezpečení VTP dat pomocí kontrolního součtu (předchozí dvě verze umožňovaly pouze vkládání čitelného hesla)
- použití protokolu VTP lze vypnout na každém portu v režimu `trunk`, je-li to třeba
- lze určit záložní (*secondary*) přepínač, který se chová jako VTP klient, ale může si přijmutou konfiguraci uložit (v případě sítě U5 půjde o všechny páteřní přepínače) - při restartu přepínače pak není nutné čekat, až dojde seznam virtuálních sítí od VTP serveru, navíc záložní VTP server se v případě nutnosti může stát i primárním serverem

Na všech přístupových přepínačích je navíc výhodné zapnout *VTP pruning* [22]. Tato technologie spočívá v tom, že přístupové přepínače oznamují páteřním přepínačům seznam virtuálních sítí, které opravdu potřebují. Data typu *broadcast* nebo *unicast* na neznámou adresu, která by pak spojením typu *trunk* za běžných okolností byla distribuována z páteřní sítě k přístupovým přepínačům, pak distribuována nejsou, pokud páteřní přepínač nemá žádné porty přiřazené do té virtuální sítě, ve které se data nacházejí. Tato technologie se v protokolu VTP verze 3 musí zapnout na každém přepínači zvlášť.

2.4.4 Protokol DHCP

Hlavním bezpečnostním rizikem u protokolu DHCP je instalace více DHCP serverů v jednom síťovém segmentu. Klienstká stanice, která požaduje od DHCP serveru informace především o nastavení své sítě, si v případě, že jí dojdou na takový požadavek dva nebo více odpovědí, může vybrat - obvykle si vybírá první došlou odpověď [16].

Této situace může zneužít teoreticky každý, kdo má připojený počítač do stejného segmentu, koncová stanice totiž vysílá svůj požadavek v paketu typu *broadcast*, takže síťové prvky zajistí, že paket dojde na síťová rozhraní všech počítačů v segmentu. Zde je příležitost po útočníka - může na takový požadavek snadno odpovědět, navíc mnohem dříve než reálný fungující DHCP server, neboť mu nic nebrání obejít pravidla DHCP protokolu (např. pomocí ICMP paketů ověřovat, zda přidělená IP adresa již v síti neexistuje) a reagovat na požadavek okamžitě. V podstrčené odpovědi pak samozřejmě koncová stanice dostane *chybné* údaje, hlavně co se týče IP adresy brány (to bude samozřejmě počítač útočníka). Aniž by tedy uživatel něco tušil, nevědomky může posílat *všechny* údaje přes počítač útočníka [23].

Tomuto druhu útoku se snadno zabrání pomocí technologie `DHCP Snooping` [11]. Tato obrana spočívá v tom, že na přístupových přepínačích se označí přístupové porty, kde se může vyskytovat DHCP server, provoz na ostatních portech bude přepínač aktivně sledovat: pokud se nich vyskytne paket typu `DHCPOFFER`, tedy odpověď od DHCP serveru, je zahozen [24].

Při použití `DHCP Snooping` si přepínač navíc vytváři tabulku, ve které má uloženy údaje od DHCP serveru: které MAC adrese byla přiřazena konkrétní IP adresa. Této informace pak může při zapnutí funkce `Dynamic ARP Inspection` využít při kontrole paketů protokolu ARP - pokud by se útočník pokoušel do sítě posílat ARP pakety, které neodpovídají záznamům v tabulce, přepínač tyto pakety nebude dále nijak zpracovávat (zahodí je).

V navrhovaném modelu sítě budovy U5 budou přístupové přepínače nastaveny tak, že spoje k páteřním přepínačům budou označeny jako `trusted` (DHCP odpovědi od páteřních přepínačů budou akceptovány), DHCP provoz na ostatních (přístupových) portech bude ale kontrolován. V sítích, kde se bude používat protokol DHCP, bude navíc zapnuta funkce `Dynamic ARP Inspection`, se shodným nastavením portů jako u `DHCP Snooping`.

2.4.5 Protokol HSRP

Protokol HSRP používá pro komunikaci mezi jednotlivými zařízení IP adresu typu *multicast*[24] `224.0.0.2` a při standardním zapnutí protokolu nejsou údaje v nich nijak chráněny. Útočník, který by získal přístup do segmentu sítě, ve kterém se tyto pakety nachází, by pak mohl snadno vytvářením vlastních takových paketů přesměrovat provoz přes svůj vlastní počítač.

Proti takovýmto falešným paketům existují dvě možnosti obrany: přidání hesla (heslo ovšem putuje přímo v paketu a útočník ho snadno přečte) a počítání kontrolního součtu pomocí algoritmu MD5. V konfiguraci všech zařízení, mezi kterými má HSRP protokol fungovat, musí být tajný klíč (sekvence znaků), před vysláním HSRP paketu pak zařízení nejprve spočítá kontrolní součet údajů v paketu a klíče a přidá ho na konec paketu. Příjemce takového paketu pak opět spočítá kontrolní součet datové části příchozího paketu a klíče a porovná se součtem, který je součástí paketu - pokud se součty liší, je paket ignorován [25].

V nové topologii sítě v budově U5 je protokol HSRP uvažován mezi zařízeními **gswitch-u5-mdf** a **gswitch-u5-idf2**, protokol bude chráněn využitím kontrolního součtu počítaným algoritmem MD5.

2.4.6 Protokol OSPF

Pakety v protokolu OSPF jsou posílány po síti podobně jako pakety v protokolu HSRP, také na IP adresu typu *multicast* - využívají se adresy `224.0.0.5` a `224.0.0.6`. Pakety samotné nejsou nijak chráněny proti odposlechu nebo proti přítomnosti falešného OSPF směrovače, lze ale opět zapnout ochranu pomocí kontrolního součtu algoritmem MD5 a tajného hesla, které je v konfiguracích všech směrovačů - příchozí pakety, jejichž kontrolní součet neodpovídá, jsou ignorovány. Sdílený tajný klíč může mít několik verzí (aby se předešlo výpadkům ve směrování během výměny klíčů) a musí být shodný v jedné OSPF oblasti [26].

Návrh nové struktury sítě počítá s tím, že směrování pomocí protokolu OSPF bude nastaveno na všech páteřních přepínačích, které budou v jedné OSPF oblasti. Předpokladem správného zabezpečení tohoto směrovacího protokolu je tedy samozřejmě i využívání kontrolního součtu.

2.4.7 Omezování síťového provozu při směrování

Navrhované páteřní přepínače `Cisco 3560` umožují navíc omezení provozu během směrování, tedy v místě, kdy data z jednoho síťového segmentu putují do jiného. K tomu slouží tzv. *access-listy*, seznamy pravidel, proti kterým je testován každý paket. Na základě

[24] pakety určené vybrané skupině stanic

těchto pravidel lze snadno zabránit některým nechtěným paketům v další cestě, ať se již jedná o pakety, které jdou ze segmentu nebo do segmentu [11].

Tato funkce se využije především na virtuálních síťových rozhraních páteřních přepínačů, které slouží jako vstupní/výstupní body jednotlivých učeben: seznamy pravidel lze snadno upravovat podle požadavků na konkrétní výuku nebo psaní testu. Pravidla mohou být také uplatněna při kontrole přístupů zvenku na servery, které poskytují veřejné služby.

2.4.8 Administrace přepínačů a dohled

Při velkém množství přepínačů není úplně výhodné spravovat administrativní přístupy na každém zařízení zvlášť, každá změna znamená příliš mnoho práce pro administrátora. Zařízení výrobce `Cisco` umožňují centralizovanou správu - přepínač může provést jednak autentizaci uživatele proti serveru `TACACS+`, navíc může uživatele omezit tím, že přímo některé příkazy, které uživatel zadává na příkazové řádce, může zakázat. Správa uživatelů, jejich hesel a přístupových práv je tak snadno udržovatelná na jednom místě [11].

Komunikaci mezi přepínači a serverem TACACS+ je ale třeba také zabezpečit, aby případný útočník nepodstrčil přepínači falešné údaje. Tuto komunikaci lze šifrovat použitím sdíleného tajného klíče, který musí být shodný pro server i pro přepínač.

Přepínače mohou o sobě administrátorům poskytovat velké množství užitečných informací - množství dat přenášených na jednotlivých spojích, zátěž procesoru, využití paměti, stav hardwaru (teplota, stav větráků, stav napájecího zdroje) aj. Tyto informace jsou nejdostupnější pomocí protokolu `SNMP`. Protokol ovšem musí být správně nastaven, neboť ve vyšších verzích tohoto protokolu je také možné přímo přepínače nastavovat bez nutnosti přihlášení. Základní zabezpečení přístupu k přepínači protokolem SNMP představuje omezení IP adres, které smějí protokol používat a nastavení uživatelského účtu a hesla pro SNMP verzi 3, která umožňuje šifrování přenášených dat pomocí sdíleného klíče. Bohužel u tohoto protokolu nelze zavést autentizaci proti vzdálenému serveru (např. proti TACACS+), takže je nutné na všech přepínačích nastavit uživatele i heslo ručně.

Přepínače mohou navíc samy aktivně zasílat některé informace, které mohou být užitečné, např. o přihlášení administrátora, o zadání příkazu, o chybném portu atd. Většinu těchto zpráv má jen informativní charakter, proto je mohou přepínače zasílat určenému serveru pomocí protokolu `syslog`, server je pak na základě zdrojové IP adresy (nebo jiných kritérií) roztřídí a uloží pro pozdější zpracování.

Některé informace ale mohou být natolik důležité, že je třeba ihned informovat správce nebo podniknout nějakou jinou akci, takové zprávy jsou pak doručovány na server pomocí SNMP notifikací. Tímto způsobem jsou také předávány detailnější informace než pomocí protokolu `syslog`, který je určen především pro zasílání obecných informací. Přepínač

lze nastavit tak, aby zprávy posílal jen v určitých situacích, např. při změně konfigurace přepínače, při změně topologie sítě nebo při změně směrování v protokolu OSPF.

Všechny zde uvedené protokoly (TACACS+, SNMP, syslog) lze umístit na jeden fyzický server. V ideálním případě by měl být server umístěný v administrativním segmentu sítě a fyzicky by měl být v budově, nejlépe poblíž centrálního bodu, tedy **gswitch-u5-mdf**.

Část III
PRAKTICKÁ ČÁST

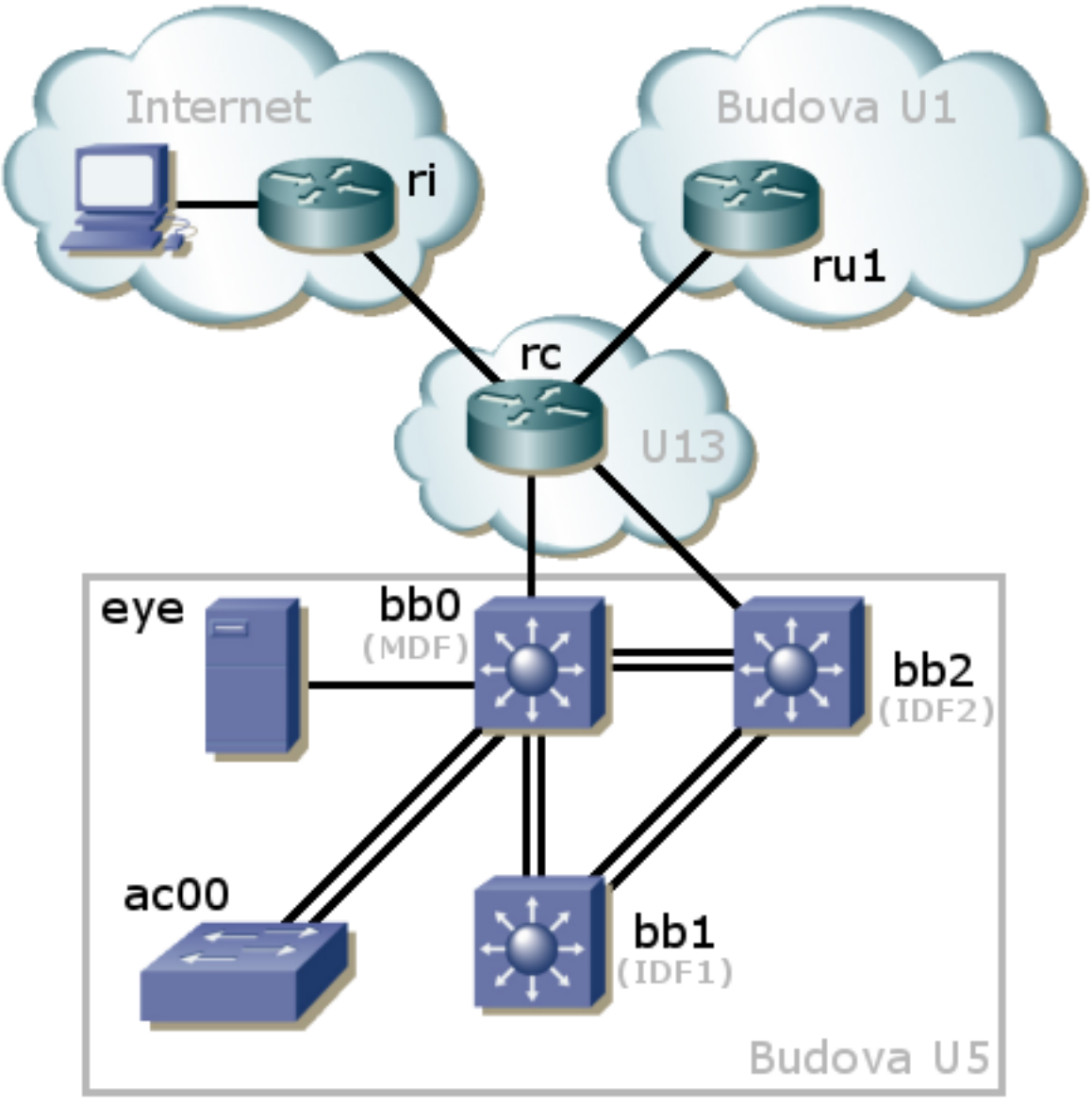
3 Simulační zapojení

Celá nová navrhovaná koncepce sítě byla i částečně realizována. V simulaci bylo zapojeno několik zařízení, která měla za úkol suplovat jednotlivé prvky v novém návrhu:

- **Cisco 2610 + Cisco NM-4E** - směrovač s 5 ethernetovými porty, který nahrazuje centrální univerzitní směrovač, pro účely simulace označen jako **rc**
- **Cisco 2610** - směrovač s jedním ethernetovým portem, který simuluje připojení další budovy v rámci UTB, označen jako **ru1**
- **Cisco 3610 + Cisco NM-1FE-TX + Cisco NM-1E-2W** - směrovač s dvěma ethernetovými porty, představující směrovač kdekoliv v internetu, označený jako **ri**
- **3x Cisco 3560G-48PS** - páteřní přepínače s 52 porty o rychlosti 1 $Gb.s^{-1}$, určené do nové struktury sítě FAI, označené jako **bb0** (určený do MDF), **bb1** (IDF1) a **bb2** (IDF2)
- **Cisco 2960-24TT-L** - přístupový přepínač s 24 porty o rychlosti 100 $Mb.s^{-1}$ a dvěma porty o rychlosti 1 $Gb.s^{-1}$, označený jako **ac00**
- **Sun Netra X1** - server s OS Sun Solaris, představuje řídicí server s pomocným softwarem, označený jako **eye**

Přestože některá uvedená zařízení jsou již velmi stará (a výrobcem nijak nepodporovaná) a disponují porty o velmi malých přenosových rychlostech (některá rozhraní povolují rychlost jen 10 $Mb.s^{-1}$), pro simulaci externí části sítě (mimo budovu U5) plně postačují, neboť důležité je zde ověření funkčnosti. Prvky plánované dovnitř budovy U5 jsou buď úplně nebo téměř totožné s plánovanými prvky. Počet páteřních přepínačů je sice menší než je uvedeno v návrhu, ale navrhovanou topologii lze rozdělit na dvě téměř shodné části, v simulaci je tedy realizována jen jedna část. Přesné zapojení je vidět z obrázku 7.

Cílem celé simulace bylo zapojení všech prvků tak, aby byla simulována část celouniverzitní sítě včetně připojení k internetu a aby bylo otestováno možné zapojení páteřních a přístupových přepínačů v rámci sítě buovy U5. Výsledkem by měly být konfigurace přepínačů, které by mohly sloužit jako inspirace při jejich reálném nasazení do provozu. Výsledné konfigurace všech zapojených síťových prvků jsou součástí příloh této práce.

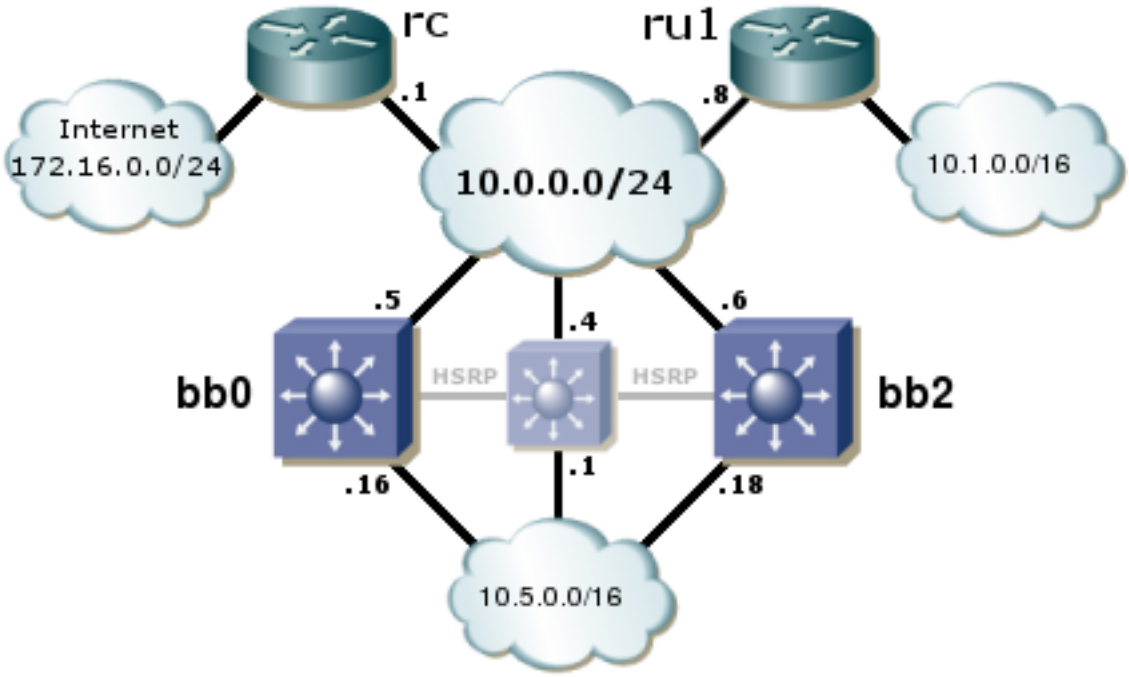


Obrázek 7: Zapojení síťových prvků při simulaci

4 Nastavení páteřní sítě UTB

V simulaci byl v páteřní síti UTB (tj. propoje mezi *budovami* a připojení k internetu) použit směrovací protokol OSPF:

- **area 0** - síť 10.0.0.0/24, směrovače **rc**, **ru1**, **bb0** a **bb2**, použita autentizace pomocí algoritmu MD5, sdílený klíč `qwerty`
- **area 1** - síť 10.1.0.0/16, směrovač **ru1**, na směrovači byly nakonfigurovány statické IP adresy na třech virtuálních rozhraních typu *loopback* z tohoto rozsahu
- **area 5** - síť 10.5.0.0/16, směrovače **bb0**, **bb1** a **bb2**, použita autentizace pomocí algoritmu MD5, sdílený klíč `qwerty`
- směrovač **rc** oznamuje pomocí protkolu OSPF ostatním směrovačům, že funguje jako brána
- směrovače **ru1**, **bb0** a **bb2** neoznamují ostatním směrovačům v rámci *area 0* informace o jednotlivých subsítích uvnitř svých oblastí, pouze oznamují adresu celé sítě (jakýsi součet menších subsítí v oblasti)



Obrázek 8: IP adresace při simulaci páteřní sítě UTB

4.1 Nastavení směrovače ri

Konfigurace směrovače **ri** je velmi jednoduchá - dvě síťová rozhraní simulují připojení jednoho počítače v internetu, který je připojen do směrovače. Směrovač **ri** je pak připojen k centrálnímu prvku **rc**. Není třeba žádných extra směrovacích informací nebo překlad adres, jde jen o směrování mezi koncovou stanicí a sítí UTB.

```
!
hostname ri
!
interface FastEthernet0/0
 ip address 192.168.6.1 255.255.255.0
!
interface Ethernet1/0
 ip address 172.16.0.1 255.255.255.0
!
```

```
ri# show ip route | in (Gateway|Ethernet)
Gateway of last resort is not set
C       172.16.0.0 is directly connected, Ethernet1/0
C       192.168.6.0 is directly connected, FastEthernet0/0
```

4.2 Nastavení směrovače ru1

Směrovač **ru1** simuluje centrální směrovač v budově U1. Má jen jedno fyzické síťové rozhraní, kterým je připojen ke směrovači **rc**, další připojené sítě budou na virtuálních rozhraních typu *loopback*.

```
 1: !
 2: hostname ru1
 3: !
 4: interface Loopback0
 5:  ip address 10.1.0.1 255.255.255.0
 6: !
 7: interface Loopback1
 8:  ip address 10.1.32.1 255.255.255.0
 9: !
10: interface Loopback2
11:  ip address 10.1.64.1 255.255.255.0
12: !
13: interface FastEthernet0/0
14:  ip address 10.0.0.8 255.255.255.0
15:  ip ospf authentication message-digest
16:  ip ospf message-digest-key 1 md5 7 051A110A335857
17: !
18: router ospf 1
19:  router-id 10.0.0.8
20:  log-adjacency-changes
21:  area 0 authentication message-digest
22:  area 1 range 10.1.0.0 255.255.0.0
23:  passive-interface Loopback0
24:  passive-interface Loopback1
25:  passive-interface Loopback2
26:  network 10.0.0.0 0.0.0.255 area 0
27:  network 10.1.0.0 0.0.255.255 area 1
28: !
```

Z uvedeného nastavení je vidět, že jsou definovány pouze statické připojené sítě, žadné další směrování není nastaveno (dokonce ani IP adresa brány). Vysvětlení některých řádek:

- řádky 15 a 16 říkají, že v protokolu OSPF při komunikaci na rozhraní `FastEthernet0/0` se má použít autentizace pomocí MD5 s definovaným klíčem, řádek 21 navíc říká, že tento druh autentizace platí pro oblast *area 0*
- řádek 19 definuje identifikátor směrovače, který bude použitý v protokolu OSPF
- řádek 22 definuje součet sítí v rímci *area 1* - směrovač tedy nebude ostatním směrovačům oznamovat včechny 3 sítě definované na rozhraních *loopback*, ale pouze jejich součet
- řádky 23 - 25 vypínají zasílaní OSPF zpráv na tato rozhraní
- řádky 26 a 27 přiřazují jednotlivé sítě do OSPF oblastí

```
ru1# show ip route | in (Gateway|10)
Gateway of last resort is 10.0.0.1 to network 0.0.0.0
     10.0.0.0/8 is variably subnetted, 5 subnets, 3 masks
C       10.0.0.0/24 is directly connected, FastEthernet0/0
C       10.1.0.0/24 is directly connected, Loopback0
O       10.1.0.0/16 is a summary, 02:04:56, Null0
O IA    10.5.0.0/16 [110/26] via 10.0.0.5, 00:48:52, Ethernet0/0
C       10.1.32.0/24 is directly connected, Loopback1
C       10.1.64.0/28 is directly connected, Loopback2
O*E2 0.0.0.0/0 [110/1] via 10.0.0.1, 00:48:52, Ethernet0/0
```

Ve výpisu směrovací tabulky jsou vidět jednotlivá statická směrování (uvozeno písmenem `C`) a IP adresa brány, kterou poskytl směrovač **rc** v rámci protokolu OSPF (poslední řádka, směr `0.0.0.0/0`). Směrovač je navíc informován o síti `10.5.0.0/16`, jejíž dostupnost zajišťuje směrovač `10.0.0.5`, což je páteřní směrovač **bb0** v *budově* U5.

4.3 Nastavení centrálního směrovače rc

Centrální směrovač je připojen jedním spojením se směrovačem **ri** (simulace připojení k internetu) a třemi spojeními se směrovači v *budovách* (jedním k U1 a dvěma k U5). Protože ale všechna 3 spojení jsou ve stejném IP adresním prostoru, je vytvořeno virtuální rozhraní typu *bridge*, které tato 3 fyzická připojení sdruží do virtuálního rozhraní `BVI11`[25].

```
 1: !
 2: hostname rc
 3: !
 4: bridge irb
 5: !
 6: interface Ethernet0/0
 7:  ip address 172.16.0.2 255.255.255.0
 8:  ip nat outside
 9: !
10: interface Ethernet1/0
11:  description u1
12:  no ip address
13:  bridge-group 11
```

[25]Bridge Virtual Interface, z angl.

```
14: !
15: interface Ethernet1/1
16:  description u5 - mdf
17:  no ip address
18:  bridge-group 11
19: !
20: interface Ethernet1/2
21:  description u5 - idf2
22:  full-duplex
23:  bridge-group 11
24: !
25: interface Ethernet1/3
26:  no ip address
27:  shutdown
28: !
29: interface BVI11
30:  ip address 10.0.0.1 255.255.255.0
31:  ip nat inside
32:  ip ospf authentication message-digest
33:  ip ospf message-digest-key 1 md5 7 0217135E191216
34:  ip ospf priority 64
35: !
36: router ospf 1
37:  router-id 10.0.0.1
38:  log-adjacency-changes
39:  area 0 authentication message-digest
40:  network 10.0.0.0 0.0.0.255 area 0
41:  default-information originate
42: !
43: ip nat inside source list nat interface Ethernet0/0 overload
44: ip nat inside source static 10.5.0.2 172.16.0.32
45: ip route 0.0.0.0 0.0.0.0 172.16.0.1
46: !
47: ip access-list standard nat
48:  permit 10.0.0.0 0.255.255.255
49: !
50: bridge 11 protocol ieee
51: bridge 11 route ip
52: !
```

Řádky 4, 50 a 51 definují konfiguraci virtuálního rozhraní typu *bridge*, jednotlivá fyzická rozhraní jsou pak přiřazena k virtuálnímu pomocí příkazu `bridge-group` (řádky 13, 18 a 23).

Řádky 47 a 48 definují seznam vnitřních IP adres (tedy IP adres použitých v rámci sítě UTB). Tento seznam se pak použije při překladu adres - při vytváření konexí z vnitřních IP adres směrem ven mimo síť UTB pak musí být tyto adresy přeloženy na veřejnou IP adresu připojení univerzity, to zajišťují příkazy na řádcích 8, 31 a 43. Řádek 44 zajišťuje statický překlad vnitřní IP adresy `10.5.0.2` (dohledový server **eye**) na vnější IP adresu `172.16.0.32`, a to obousměrně. Příchozí konexe z *internetu* směrem na `172.16.0.32` se tedy dostanou až k server **eye** (využije se např. u DNS).

Autentizaci v protkolu OSPF zajišťují řádky 32, 33 a 39 (pouze v rámci oblasti *area 0*, jiné oblasti zde nejsou třeba). Řádek 34 definuje prioritu tohoto směrovače (měla by být

nejvyšší v porovnání s ostatními směrovači), řádek 40 pak definuje oblast *area 0* a IP rozsah v této oblasti.

Posledním zajímavým údajem je IP adresa brány. Ta je zde specifikována staticky na řádku 44, řádek 41 pak zajistí, že směrovač **rc** bude sdělovat protokolem OSPF ostatním směrovačům, že pro ně může plnit úlohu brány.

```
rc# show ip route | ex -
Gateway of last resort is 172.16.0.1 to network 0.0.0.0
     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.0.0 is directly connected, Ethernet0/0
     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.0.0.0/24 is directly connected, BVI11
O IA    10.1.0.0/16 [110/11] via 10.0.0.8, 01:00:45, BVI11
O IA    10.5.0.0/16 [110/26] via 10.0.0.5, 01:00:45, BVI11
S*   0.0.0.0/0 [1/0] via 172.16.0.1
```

Ve směrovací tabulce jsou dostupné všechny sítě: připojení do internetu přes rozhraní `Ethernet0/0` (včetně nastavení brány na posledním řádku), páteřní síť `10.0.0.0/24` a jednotlivé sítě v *budovách* U1 a U5 (řádky uvozené písmenem **O**).

4.4 Nastavení páteřních přepínačů bb0 a bb2

Celkové nastavení přepínačů bude ukázáno v dalších kapitolách, nyní bude osvětlena pouze ta část, která zajišťuje připojení *budovy* U5 ke zbytku univerzitní sítě a nastavuje směrování pomocí protokolu OSPF.

```
 1: !
 2: hostname bb0
 3: !
 4: interface GigabitEthernet0/1
 5:  description uplink
 6:  switchport access vlan 11
 7:  switchport mode access
 8:  switchport nonegotiate
 9: !
10: interface Vlan11
11:  ip address 10.0.0.5 255.255.255.0
12:  ip ospf message-digest-key 1 md5 7 051A110A335857
13: !
14: interface Vlan501
15:  ip address 10.5.0.16 255.255.255.0
16:  ip ospf message-digest-key 1 md5 7 051A110A335857
17:  ip ospf priority 8
18: !
19: router ospf 1
20:  router-id 10.0.0.5
21:  log-adjacency-changes
22:  area 0 authentication message-digest
23:  area 5 authentication message-digest
24:  area 5 range 10.5.0.0 255.255.0.0 cost 16
25:  network 10.0.0.0 0.0.0.255 area 0
26:  network 10.5.0.0 0.0.255.255 area 5
27: !
```

```
 1: !
 2: hostname bb2
 3: !
 4: interface GigabitEthernet0/1
 5:  description uplink
 6:  switchport access vlan 11
 7:  switchport mode access
 8:  switchport nonegotiate
 9: !
10: interface Vlan11
11:  ip address 10.0.0.6 255.255.255.0
12:  ip ospf message-digest-key 1 md5 7 051A110A335857
13: !
14: interface Vlan501
15:  ip address 10.5.0.18 255.255.255.0
16:  ip ospf message-digest-key 1 md5 7 051A110A335857
17:  ip ospf priority 4
18: !
19: router ospf 1
20:  router-id 10.0.0.6
21:  log-adjacency-changes
22:  area 0 authentication message-digest
23:  area 5 authentication message-digest
24:  area 5 range 10.5.0.0 255.255.0.0 cost 32
25:  network 10.0.0.0 0.0.0.255 area 0
26:  network 10.5.0.0 0.0.255.255 area 5
27: !
```

Konfigurace jsou velmi podobné, hlavní odlišnost je v nastavení *hostname*, IP adres virtuálních rozhraní `Vlan11` a `Vlan501` a *router-id* na řádku 20. Důležité je rozdílné nastavení *cost* na řádku 24 - díky nižší hodnotě v konfiguraci **bb0** pak ostatní směrovače vypočítají, že výhodnější cesta směrem do sítě `10.5.0.0/16` je právě přes **bb0**. Cesta přes **bb2** se pak použije automaticky pouze v případě nedostupnosi **bb0**. Další rozdílné hodnoty jsou pak v prioritizaci OSPF směrovače na řádku 17, tyto hodnoty se uplatní při volbě hlavních OSPF směrovačů v rámci oblasti.

Nastavení směrování je tedy zřejmé: univerzitní páteřní síť `10.0.0.0/24` je v oblasti *area 0*, síť `10.5.0.0/16` (a případné podsítě) jsou v oblasti *area 5*. Řádky 12, 16, 22 a 23 zajišťují autentizaci pomocí MD5 a sdíleného klíče. IP adresa brány zde není specifikována, tuto informaci obdrží směrovače od centrálního **rc**.

V současnosti univerzita protokol OSPF nepoužívá, nastaveny jsou jen statické směry na jednom centrálním prvku. Z hlediska sítě budovy U5 to nepředstavuje problém, jen se v protokolu OSPF nebude definovat *area 0*. Redundantní připojení se pak zajistí protokolem HSRP a IP adresou virtuálního směrovače `10.0.0.4`.

```
 1: !
 2: hostname bb0
 3: !
 4: interface GigabitEthernet0/1
 5:  description uplink
 6:  switchport access vlan 11
 7:  switchport mode access
 8:  switchport nonegotiate
 9: !
10: interface Vlan11
11:  ip address 10.0.0.5 255.255.255.0
12:  standby 1 ip 10.0.0.4
13:  standby 1 priority 64
14:  standby 1 preempt
15:  standby 1 authentication md5
       key-string 7 095D590C0B110E
16:  standby 1 track GigabitEthernet0/1 16
17: !
18: ip route 0.0.0.0 0.0.0.0 10.0.0.1
19: !
```

```
 1: !
 2: hostname bb2
 3: !
 4: interface GigabitEthernet0/1
 5:  description uplink
 6:  switchport access vlan 11
 7:  switchport mode access
 8:  switchport nonegotiate
 9: !
10: interface Vlan11
11:  ip address 10.0.0.6 255.255.255.0
12:  standby 1 ip 10.0.0.4
13:  standby 1 priority 56
14:  standby 1 preempt
15:  standby 1 authentication md5
       key-string 7 095D590C0B110E
16:  standby 1 track GigabitEthernet0/1 16
17: !
18: ip route 0.0.0.0 0.0.0.0 10.0.0.1
19: !
```

Při tomto nastavení je IP adresa virtuálního směrovače `10.0.0.4` podle dostupnosti jednotlivých směrovačů a stavu linky na rozhraní `GigabitEthernet0/1` buď umístěna na **bb0** nebo **bb2**. IP adresa brány je pak definována staticky. K bezchybnému fungování je pak ještě třeba nastavit statické směrování na centrálním prvku:

```
!
hostname rc
!
ip route 10.5.0.0 255.255.0.0 10.0.0.4
!
```

Nevýhodou tohoto směrování je skutečnost, že síťový provoz jdoucí z jedné budovy do jiné (např. z U5 do U1) musí projít přes směrování na centrálním směrovači **rc**, zatímco

použití protokolu OSPF umožňuje toto směrování obejít a posílat data přímo. Protokol OSPF také umožňuje větší flexibilitu univerzitní páteřní sítě a možnosti redundantních připojení mezi jednotlivými budovami.

5 Dohledový server

Dohledový server má IP adresu `10.5.0.2` (je přímo v páteřní síti budovy U5, zapojen do portu `Gi0/2` přepínače **bb0**). Jeho primárním účelem je poskytování základních služeb pro aktivní síťové prvky, navíc může poskytovat i další služby (např. DNS). Server má administrativní název **eye**.

5.1 Autentizační server TACACS+

Tento software má jeden konfigurační soubor. Pro účely sítě UTB (server může být připojen přímo do páteřní sítě UTB a poskytovat tuto službu pro aktivní prvky celé univerzity) stačí, pokud bude obsahovat seznam uživatelů a jejich hesel. Výpis souboru `tac_plus.conf` [28]:

```
 1: key = "bHsbowfdjGxru47S"
 2: accounting file = "/var/log/cisco/commands.log"
 3:
 4: user = kohout {
 5:  name = "Petr Kohout"
 6:  login = des qwDyM1db9iOPI
 7:  member = admin
 8: }
 9:
10: group = admin {
11:   service = exec { priv-lvl = 15 }
12: }
```

V uvedeném konfigurační souboru je na 1. řádku definovaný klíč - řetězec, který slouží k šifrování komunikace, musí být stejně definovaný i na přepínačích (klíč použitý v této konfiguraci byl vygenerován náhodně). Na druhém řádku je definován soubor pro tzv. *accounting*, server TACACS+ do něj bude zaznamenávat každý příkaz, který administrátor zadal při správě aktivního prvku. Na řádcích 4-8 je definován uživatel `kohout`, který je členem skupiny `admin`, uživatelé ve skupině získají po přilogování na síťový prvek nejvyšší administrátorská práva (úroveň 15).

5.2 Logovací software syslog-ng

Software pro logování informací, které zasílají aktivní síťové prvky pomocí protokolu syslog, je také na serveru **eye**. Konfigurace, která zajišťuje příjem těchto zpráv a třídí je do souborů podle zdrojové IP adresy zprávy, je následující (soubor `syslog-ng.conf` [29]):

```
source s_ext { udp(); };
filter f_cisco { host("^10.5.0.[0-9]+$"); };
destination d_cisco { file("/var/log/cisco/$HOST" owner("root") group("other") perm(0600)); };
log { source(s_ext); filter(f_cisco); destination(d_cisco); };
```

Zprávy z přepínače **bb0** tak budou ukládány do souboru `/var/log/cisco/10.5.0.16`, zprávy z **bb1** do `/var/log/cisco/10.5.0.17` atd. Soubory jsou čitelné pouze pro systémového uživatele `root`, to lze ale v případě potřeby jakkoliv změnit.

Autentizace uživatele na aktivních prvcích pak funguje následovně: uživatel je dotázán na uživatelské jméno a heslo. Tyto informace se ověří proti serveru TACACS+ a uživatel je buď přihlášen nebo je mu odepřen přístup. V případě, že server TACACS+ není dostupný, se pak síťový prvek snaží ověřit uřivatele proti svému vlastnímu seznamu. Pro tento případ bude tedy na všech přepínačích definován vlastní uřivatel `root` s heslem. Uživatel `root` ovšem nesmí být definován v systému TACACS+.

5.3 Logovací software pro zprávy SNMP

Logování zpráv pomocí protokolu SNMP zajišťuje program `snmptrapd`. Veškeré obdržené zprávy (a další činnosti) umí tento program zaslat dále programu `syslog`, který je uloží do souboru, a navíc na základě typu zprávy může spustit nějakou akci (další program) - typicky se může jednat o varování administrátora o tom, že nějaké zařízení bylo restartováno, že je chyba na síťovém rozhraní apod. Program se spouští s těmito parametry:

```
# snmptrapd -c /etc/snmptrapd.conf -n -p /var/run/snmptrapd.pid -Ls 2 -m ALL
```

Parametr `-c` definuje konfigurační soubor, parametr `-n` znamená, že program bude ukládat informace o zdroji zprávy v podobě IP adresy a nikoliv doménového jména, parametr `-p` specifikuje soubor s informací o čísle běžícího procesu, parametr `-Ls 2` značí oznámení programu `syslog` typu *local2* a poslední parametr `-m` značí zpracovávání všech typů SNMP zpráv. Konfigurace programu `syslog-ng` [29] pro logování zpráv z programu `snmptrapd`:

```
source s_loc { sun-stream("/dev/log" door("/etc/.syslog_door")); internal(); };
destination d_snmptrapd { file("/var/log/snmptrapd.log" owner("root") group("other") perm(0600)); };
filter f_snmptrapd { facility(local2); };
log { source(s_loc); filter(f_snmptrapd); destination(d_snmptrapd); };
```

V hlavním konfiguračním souboru `snmptrapd.conf` se definuje, ze kterých zařízení bude program zprávy zpracovávat. K tomu je třeba znát unikátní *engineID* zdrojového zařízení (na zařízeních `Cisco` lze tento údaj získat příkazem `show snmp engineID`). Po té se do konfiguračního souboru přidá řádek, který definuje uživatele, heslo a *engineID* [30]. Kromě těchto základních údajů lze navíc definovat akci pro některé druhy zpráv [31]. Ukázková konfigurace obsahuje definici jednoho uživatele z jednoho zařízení a příkaz, který se spustí v případě, že je zařízení restartováno:

```
createUser -e 800000090300001C57A93C01 reporter MD5 qwerty123
authUser log reporter

traphandle SNMPv2-MIB::coldStart /usr/local/bin/trap coldstart
traphandle SNMPv2-MIB::warmStart /usr/local/bin/trap warmstart
```

Přidání nového zařízení do síťové struktury znamená přidání další řádky do konfiguračního souboru a restart programu `snmptrapd`.

5.4 Software pro synchronizaci času

Zejména kvůli logování zpráv od jednotlivých síťových zařízení je nutné na nich synchronizovat čas. Na dohledovém serveru **eye** běží program `ntpd`, který pak bude protokolem NTP zajišťovat stejný čas na ostatních zařízeních. Server sám je synchronizován podle NTP serverů v síti poskytovatele připojení k internetu, firmy Cesnet z.s.p.o. `tik.cesnet.cz` a `tak.cesnet.cz`, které odebírají přesný čas ze systému GPS. Výpis konfiguračního souboru `/etc/ntp.conf` [32]:

```
 1: server 195.113.144.201 prefer
 2: server 195.113.144.238
 3: driftfile /var/lib/ntp/ntp.drift
 4:
 5: restrict default ignore
 6: restrict 195.113.144.201
 7: restrict 195.113.144.238
 8: restrict 127.0.0.1
 9:
10: restrict 10.0.0.0 mask 255.0.0.0 nomodify notrap
```

Řádky 1 a 2 definují zdroj přesného času, řádek 3 nastavuje soubor, ve kterém si `ntpd` vytváří statistiky dostupnosti, chybovosti a zpoždění jednotlivých časových zdrojů a podle nich pak provádí zpřesňování svého času. Řádky 5-8 omezují přístup: je zakázán jakýkoliv přístup vyjma serverů se zdojem času (ty musejí mít právo upravit lokální čas) a vlastního serveru (řádek 8).

Řádek 10 pak opravňuje všechna zařízení v síti `10.0.0.0/8` (tedy celý privátní adresní prostor UTB) k tomu, aby získávala od serveru **eye** údaje o čase, ale nemohla ho nijak měnit. Stav synchronizace na serveru **eye** lze vypsat příkazem `ntpq -p`:

```
# ntpq -p
     remote           refid      st t when poll reach   delay   offset jitter
==============================================================================
*tik.cesnet.cz   .GPS.            1 u   95  256  377    7.626   14.294 3.906
+tak.cesnet.cz   .GPS.            1 u   33  256  377    8.007   15.347 3.981
```

5.5 DNS server

Použitý DNS program `bind` bežící na serveru **eye** je v tzv. *chroot* prostředí: je pro něj vyčleněn adresář a případný útok znamenající získání nějakých vyšších práv pro útočníka pak neznamená nebezpečí pro celý server, ale jen pro tento adresář. Vyčleněný adresář `/var/chroot/bind` pak obsahuje tyto podadresáře:

- **dev** - obsahuje speciální soubory
- **etc** - konfigurace a nastavení jednotlivých zón
- **lib** - systémové knihovny
- **sbin** - binární soubory ke spuštění

- **var/log** - úložiště logů
- **var/named** - soubor s číslem procesu

V různých operačních systémech se tento seznam adresářů může lišit, záleží na verzi softwaru **bind**, na umístění systémových knihoven apod. Celý program se pak spouští s parametry `-t` (změna kořenového adresáře) a `-u` (definice uživatele, který nemá administrátorská práva):

```
# named -t /var/chroot/bind -u named
```

Celkové nastavení je v souboru `etc/named.conf`:

```
 1: acl local { 127.0.0.1; };
 2: acl slaves { 195.178.88.66; };
 3: acl fai { 10.5.0.0/16; };
 4: acl utb { 10.0.0.0/8; };
 5:
 6: options {
 7:   version "surely you must be joking";
 8:   listen-on port 53 { any; };
 9:
10:   directory "/etc/zones";
11:   pid-file "/var/named/named.pid";
12:   statistics-file "/var/named/named.stats";
13:   memstatistics-file "/var/named/named.memstats";
14:   dump-file "/var/named/named.dump";
15:
16:   notify no;
17:   auth-nxdomain no;
18:   zone-statistics yes;
19:   transfer-format many-answers;
20:   max-transfer-time-in 8;
21:   interface-interval 0;
22:
23:   allow-query { local; };
24:   allow-recursion { fai; };
25:   allow-transfer { slaves; };
26: };
27:
28: logging {
29:   channel "lames" { file "/var/log/dns-lames.log" versions 14 size 5M;  severity info; print-time yes; };
30:   channel "def_log" { file "/var/log/dns.log" versions 14 size 5M; severity dynamic; print-time yes; };
31:   channel "zones" { file "/var/log/zones.log" versions 14 size 5M; severity dynamic; print-time yes; };
32:   channel "update" { file "/var/log/update.log" versions 14 size 5M; severity dynamic; print-time yes; };
33:   channel "query" { file "/var/log/query.log" versions 14 size 5M; severity dynamic; print-time yes; };
34:   category "security" { def_log; };
35:   category "default" { def_log; };
36:   category "config" { def_log; };
37:   category "lame-servers" { lames; };
38:   category "notify" { zones; };
39:   category "xfer-out" { zones; };
40:   category "update" { update; };
41:   category "update-security" { update; };
42:   category "client" { query; };
43:   category "queries" { query; };
44:   category "database" { query; };
45: };
46:
47: view "chaos" chaos {
```

```
48:   match-clients { any; };
49:   allow-recursion { none; };
50:   allow-transfer { none; };
51:   allow-query { local; };
52:   recursion no;
53:
54:   zone "." { type master; file "/dev/null"; };
55:   zone "bind" { type master; file "chaos.hint"; };
56: };
57:
58: view "internal" in {
59:   match-clients { utb; local; };
60:   allow-recursion { fai; local; };
61:   allow-transfer { slaves; };
62:   allow-query { utb; local; };
63:   recursion yes;
64:
65:   zone "." in { type hint; file "root.hint"; };
66:   zone "net.fai.utb.cz" in { type master; file "internals/net.fai.utb.cz"; };
67:   zone "fai.utb.cz" in { type master; file "internals/fai.utb.cz"; };
68:   zone "5.10.in-addr.arpa" in { type master; file "internals/rev.10.5"; };
69: };
70:
71: view "external" in {
72:   match-clients { any; };
73:   allow-recursion { none; };
74:   allow-transfer { slaves; };
75:   allow-query { any; };
76:   recursion no;
77:
78:   zone "fai.utb.cz" in { type master; file "externals/fai.utb.cz"; };
79:   zone "utb.cz" in { type slave; file "externals/utb.cz"; masters { 195.178.88.66; }; };
80: };
```

Řádky 1-4 definují bloky IP adres, které se použijí později v konfiguraci k omezení přístupu. Seznam `utb` definuje celý adresní prostor univerzity, seznam `fai` definuje adresní prostor v budově U5. Seznam `slaves` obsahuje seznam IP adres serverů, které si mohou stahovat celé zóny a mohou být záložními DNS servery.

Celý blok `options` ovlivňuje celkové chování DNS serveru - upravuje verzi, kerou o sobě server tvrdí, nastavuje cesty k souborům apod [27]. Důležité je omezení dotazů na řádce 23: pouze *localhost* - tedy vlastní server **eye** - může klást naprosto libovolné dotazy. IP adresy z adresního prostoru definovaném v bloku `fai` mohou dávat dotazy i na jiné domény, DNS server takové požadavky vyřídí a vrátí správnou odpověď - toto chování umožňuje nastavit server `eye`, resp. jeho IP adresu `10.5.0.2` jako DNS server na pracovních stanicích (tato informace je i součástí nastavení DHCP serverů). Řádek 25 omezuje stahování celých zónových souborů - omezení pouze na IP adresy definované v bloku `slaves`.

Konfigurační blok `logging` (řádky 28-45) definuje logování různých zpráv do různých souborů. Uvedené nastavení zajišťuje rozsáhlé logování každého dotazu, což může generovat velmi obsáhlé logy, to lze samozřejmě zastavit zakomentováním příslušných řádků.

Blok `view chaos` na řádcích 47-56 pak definuje, jak má server reagovat na dotazy typu `chaos` (využívaných především k získávání informací o DNS serveru jako takovém) - server bude vracet pouze údaje definované v souboru `chaos.hint`.

Definice `view internal` (řádky 58-69) definují chování DNS serveru v případě, že dotazy pocházejí z vnitřní sítě (nebo *localhostu*), to je nastaveno na řádku 59. Zóny definované v tomto bloku by měly obsahovat pouze privátní IP adresy. Tím bude zaručena funkčnost DNS serveru pro vnitřní IP adresní prostor. Řádky 60-62 definují omezení na jednotlivé druhy dotazů a řádky 65-68 již definují jednotlivé zóny. Zóna na řádku 65 obsahuje soubor s celosvětovými kořenovými DNS servery, což je nezbytné k získávání základních informací o doménách 1. řádu (např. `.org`, `.sk` apod.).

Poslední blok (řádky 71-80) definuje reakci DNS serveru na dotazy z internetu. Řádky 73 a 75 říkají, že tyto dotazy mohou být pouze do definovaných zón, žádné jiné dotazy nebudou obslouženy. Údaje v těchto zónách by měly obsahovat informace o veřejných IP adresách.

Soubor `chaos.hint` pouze zabezpečuje, že se případný útočník nebo zvědavec nedostane k údajům o verzi běžícího softwaru [27]:

```
$ORIGIN bind.
@       CHAOS SOA       localhost.      root.localhost. ( 2010051001 28800 14400 604800 14400 )
@       CHAOS NS        localhost.

version.bind.   CHAOS TXT       "surely you must be joking"
authors.bind.   CHAOS TXT       "surely you must be joking"
```

Obsah souboru `internals/net.fai.utb.cz`:

```
$ORIGIN net.fai.utb.cz.
@       IN SOA  eye.net.fai.utb.cz.     admin.utb.cz ( 2010051002 28800 14400 604800 14400 )
@       IN NS   eye

gw      IN A    10.5.0.1
eye     IN A    10.5.0.2
bb0     IN A    10.5.0.16
bb1     IN A    10.5.0.17
bb2     IN A    10.5.0.18
bb3     IN A    10.5.0.19
ac00    IN A    10.5.0.32
ac01    IN A    10.5.0.33
ac02    IN A    10.5.0.34
ac03    IN A    10.5.0.35
```

Obsah souboru `internals/fai.utb.cz`:

```
$ORIGIN fai.utb.cz.
@       IN SOA  eye.fai.utb.cz. admin.utb.cz ( 2010051003 28800 14400 604800 14400 )
@       IN NS   eye
net     IN NS   eye

eye     IN A    10.5.0.2
vyuka   IN A    10.5.16.7
```

Obsah souboru `internals/rev.10.5`:

```
$ORIGIN 5.10.in-addr.arpa.
@       IN SOA  eye.fai.utb.cz. admin.utb.cz ( 2010051003 28800 14400 604800 14400 )
@ IN NS eye.fai.utb.cz.
; backbone
1.0 IN PTR gw.net.fai.utb.cz.
2.0 IN PTR eye.fai.utb.cz.
16.0 IN PTR bb0.net.fai.utb.cz.
17.0 IN PTR bb1.net.fai.utb.cz.
18.0 IN PTR bb2.net.fai.utb.cz.
19.0 IN PTR bb3.net.fai.utb.cz.
32.0 IN PTR ac00.net.fai.utb.cz.
33.0 IN PTR ac01.net.fai.utb.cz.
34.0 IN PTR ac02.net.fai.utb.cz.
35.0 IN PTR ac03.net.fai.utb.cz.
; servers
7.16 IN PTR vyuka.fai.utb.cz.
```

Dotazy do interní domény `net.fai.utb.cz` by bylo možné ještě omezit tak, aby byly zpracovávány jen pro zařízení, která jsou v této síti a navíc např. pro pracovní stanice administrátorů, stejné omezení by pak mělo platit i na reverzní záznamy (při rozdělení zóny `5.10.in-addr.arpa` na menší jednotky). Nastavení by pak mohlo vypadat takto:

```
acl admin { 10.1.45.2; 10.5.66.13; };
acl fai-backbone { 10.5.0.0/24; };
zone "net.fai.utb.cz" in {
  type master; file "internals/net.fai.utb.cz";
  allow-query { fai-backbone; admin; };
};
zone "0.5.10.in-addr.arpa" in {
  type master; file "internals/net.fai.utb.cz";
  allow-query { fai-backbone; admin; };
};
```

Zónový soubor `externals/utb.cz` se vytvoří sám, jakmile si ho DNS server stáhne z centrálního univerzitního DNS serveru, není třeba ho nijak zakládat. Jeho obsah pak plně záleží na obsahu definovaném na hlavním serveru. Zbývá tedy vypsat obsah souboru `externals/fai.utb.cz`:

```
$ORIGIN fai.utb.cz.
@       IN SOA  eye.fai.utb.cz. admin.utb.cz ( 2010051002 28800 14400 604800 14400 )
@       IN NS   eye
@       IN MX 1 sun.utb.cz.
@       IN MX 4 rs.cesnet.cz.

eye     IN A    172.16.0.32
vyuka   IN A    172.16.0.33

web     IN CNAME        luna.utb.cz.
www     IN CNAME        moon.utb.cz.
```

Ukázky DNS dotazů z vnější sítě (počítač zapojený do směrovače **ri**, viz Obrázek 7, IP adresa `192.168.6.6`) ukazují správnou funkčnost, server vrací pouze dotazy do domény `fai.utb.cz`, ostatní dotazy jsou odmítnuty:

```
$ host eye.fai.utb.cz 172.16.0.32
eye.fai.utb.cz has address 172.16.0.32

$ host vyuka.fai.utb.cz 172.16.0.32
eye.fai.utb.cz has address 172.16.0.33

$ host gw.fai.utb.cz 172.16.0.32
Host gw.fai.utb.cz not found: 5(REFUSED)

$ host 10.5.0.1 172.16.0.32
Host 1.0.5.10.in-addr.arpa not found: 5(REFUSED)

$ host a.root-servers.net 172.16.0.32
Host a.root-servers.net not found: 5(REFUSED)
```

Oproti tomu dotazy z vnitřní sítě (zdrojová IP adresa `10.5.66.6`) jsou zpracovány, v odpovědích jsou vidět IP adresy z privátního rozsahu:

```
$ host eye.fai.utb.cz 10.5.0.2
eye.fai.utb.cz has address 10.5.0.2

$ host vyuka.fai.utb.cz 10.5.0.2
vyuka.fai.utb.cz has address 10.5.16.7

$ host gw.net.fai.utb.cz 10.5.0.2
gw.net.fai.utb.cz has address 10.5.0.1

$ host 10.5.0.1 10.5.0.2
1.0.5.10.in-addr.arpa domain name pointer gw.net.fai.utb.cz.

$ host a.root-servers.net 10.5.0.2
a.root-servers.net has address 198.41.0.4
```

6 Nastavení aktivních síťových prvků

6.1 Společné nastavení aktivních prvků v síti FAI

Před vlastním nastavení síťových prvků byl rozčleněn celý IP adresní prostor `10.5.0.0/16` na jednotlivé subsítě, jak bylo popsáno v teoretické části této práce. Páteřní univerzitní síti (resp. její virtuální části na zařízeních **bb0** a **bb2**) bylo přiděleno číslo 11, páteřní síť budovy U5 dostala číslo 501, pro spojení typu *trunk* (resp. pro protokol sestavující takové spojení) bylo rezervováno číslo 502. Jednotlivým zaměstnaneckým sítím jsou postupně přidělována čísla 520-549, výukové laboratoře pak dostávají čísla 550-599.

Při simulaci nebyly vytvořeny úplně všechny sítě, pouze některé, neboť smyslem celé simulace bylo ověřit funkčnost všech protokolů a zadávání úplně všech sítí by znamenalo de facto pouze velmi robustní rozšíření konfigurace, přičemž funkce nastavení je totožná.

6.1.1 Základní nastavení

Mezi základní nastavení každého aktivního prvku patří nastavení jeho názvu (tzv. *host-name*), základních síťových služeb a zabezpečení nebo vypnutí některých služeb, které jsou standardně zapnuty.

```
 1: !
 2: service password-encryption
 3: !
 4: hostname ac00
 5: !
 6: ip subnet-zero
 7: ip domain-name net.fai.utb.cz
 8: ip domain-list net.fai.utb.cz
 9: ip name-server 10.5.0.2
10: ip classless
11: !
12: no ip http server
13: no ip http secure-server
14: !
15: ip access-list standard localhost_access
16:  remark >> List of IPs allowed to connect to this box
17:  permit 10.5.0.2
18:  permit 10.6.66.0 0.0.1.255
19: !
20: line vty 0 4
21:  access-class localhost_access in
22: line vty 5 15
23:  access-class localhost_access in
24: !
```

Seznam IP adres definovaných na řádcích 17 a 18 lze měnit na základě toho, kdo skutečně má mít ke správě zařízení přístup. V tomto nastavení není definována IP adresa a brána zařízení, protože toto nastavení je různé pro páteřní a přístupové přepínače a bude popsáno v dalších kapitolách.

6.1.2 Synchronizace času

Čas je synchronizován na všech zařízeních podle dohledového serveru **eye**. Tento čas je ale distribuován pro celosvětový univerzální čas a nebere ohled na lokální časovou zónu ani na případný letní čas, to je třeba v konfiguraci upravit:

```
!
clock timezone CET 1
clock summer-time CEST recurring last Sun Mar 2:00 last Sun Oct 3:00
!
ntp server 10.5.0.2
!
```

Časovou synchronizaci lze i snadno zkontrolovat:

```
rc# show ntp associations
      address         ref clock     st  when  poll reach  delay  offset disp
*~10.5.0.2         195.113.144.201   2    99   256  377     5.7    7.55 5.1
 * master (synced), # master (unsynced), + selected, - candidate, ~configured

rc# show clock
22:30:50.657 CEST Wed May 19 2010
```

6.1.3 Autentizace a autorizace uživatelů

Administrátoři mají přístup na síťové prvky pouze protokolem SSH[26] verze 2. Tento protokol zajistí šifrování celé komunikace mezi pracovní stanicí administrátora a síťovým zařízením. Nešifrované připojení pomocí programu `telnet` není povoleno.

```
!
ip ssh authentication-retries 2
ip ssh logging events
ip ssh version 2
!
line vty 0 4
 transport input ssh
line vty 5 15
 transport input ssh
!
```

Při konfiguraci nového zařízení je třeba před zadáním příkazu `ip ssh` definovat název a doménu zařízení (příkazy `hostname` a `ip domain-name`) a vygenerovat dostatečně dlouhé šifrovací klíče příkazem `crypto key generate rsa general-keys modulus 2048`.

Autentizace a autorizace uživatelů probíhá proti seznamu definovanému na serveru **eye** pomocí protokolu TACACS+. Stejným způsobem je server **eye** také informován o akcích jednotlivých uživatelů (tzv. *accounting*). V případě, že TACACS+ server není dostupný, budou brát přepínače v úvahu vlastní seznam uživatelů a vlastní heslo pro získání administrativních práv.

[26] Secure Shell, z angl.

```
 1: !
 2: enable secret 5 $1$COi.$bLGbUM6d3GDy0BZ.IS4iD0
 3: !
 4: username root privilege 15 secret 5 $1$IKjZ$KfAapgv.si29c6fUcJKyu0
 5: !
 6: !
 7: aaa new-model
 8: !
 9: !
10: aaa authentication login default group tacacs+ local
11: aaa authorization exec default group tacacs+ local
12: aaa accounting exec default start-stop group tacacs+
13: aaa accounting commands 0 default start-stop group tacacs+
14: aaa accounting commands 1 default start-stop group tacacs+
15: aaa accounting commands 15 default start-stop group tacacs+
16: !
17: tacacs-server host 10.5.0.2 timeout 5
18: tacacs-server directed-request
19: tacacs-server key 7 104C210A0718050D080E0D33363D676211
20: !
```

Sdílený klíč definovaný na řádku 19 musí být samozřejmě shodný s definicí klíče v konfiguračním souboru TACACS+, uživá se k šifrování spojení, aby nebyla prozrazena hesla uživatelů.

6.1.4 Logování na vzdálený server

Logování běžných zpráv pomocí protokolu `syslog` na vzdálený server `eye` je snadné, v konfiguraci na to stačí jediná řádka:

```
logging host 10.5.0.2
```

Další nastavení musí být pro logování zpráv protokolem SNMP, verze 3. Nejprve je třeba vytvořit uživatelskou skupinu, pak uživatele (s přiřazením do skupiny) a nastavit heslo [33]. Posledním krokem tohoto nastavení je definice cílového serveru, kam se mají zprávy zasílat, a seznamu, který druh zpráv se bude tímto způsobem zasílat.

```
snmp-server group reporter v3 auth
snmp-server user reporter reporter v3 auth md5 qwerty123
snmp-server host 10.5.0.2 traps version 3 auth reporter
snmp-server host 10.5.0.2 informs version 3 auth reporter
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps tty
snmp-server enable traps cpu threshold
snmp-server enable traps vtp
snmp-server enable traps port-security
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
```

Příkaz `snmp-server enable traps` definuje poměrně obsáhlý seznam, co všechno se má reportovat, v reálném provozu pak ale záleží na požadavcích administrátora, kterými zprávami se bude aktivně zabývat a které si dovolí ignorovat.

V této konfiguraci je definována skupina `reporter` s uživatelem `reporter` a heslem `qwerty123`. Zprávy bude uživatel zasílat na dohledový server **eye**, nicméně aby tento server zprávu přijal, musí do své konfigurace zadat tohoto uživatele, jeho heslo a *engineID* tohoto zařízení (viz předešlé kapitoly). Zjištění unikátního *engineID* vypadá následovně:

```
ac00# show snmp engineID | in Local
Local SNMP engineID: 800000090300001C57A93C01
```

6.1.5 Povolení monitoringu pomocí SNMP

Aktivní monitoring jednotlivých síťových zařízení je pro administrátora velmi výhodný: dlouhodobě lze uchovávat informace o množství přenášených dat, zátěži procesoru nebo využití paměti, pak z nich lze vyčíst dlouhodobý pokles nebo stoupání sledovaných hodnot nebo definovat kritické parametry. Aby byl pravidelný sběr dat možný, je třeba ho povolit, samozřejmě s omezením na uživatele a heslo ze zdrojové IP adresy dohledového serveru [34]:

```
 1: !
 2: snmp-server location u5.mdf
 3: snmp-server chassis-id bb0.net.fai.utb.cz
 4: snmp-server view all 1 included
 5: snmp-server group utb v3 auth read all access snmp
 6: snmp-server user watchdog utb v3 auth md5 qwerty123 access snmp
 7: !
 8: ip access-list standard snmp
 9:  remark >> SNMP hosts allowed to connect to this box
10:  permit 10.5.0.2
11: !
```

Řádky 2 a 3 slouží pouze pro snadnější identifikaci zařízení. Řádek 4 vytváří *view*, tedy seznam věcí, které budou při dotazu zobrazeny, v tomto případě má název `all` a zobrazeny budou všechny informace, které v číselném formátu začínají jedničkou (je možné použít i jména, např. `system` nebo `ifOutOctets`, nastavení jedničky ale obsahuje téměř všechny hodnoty). Dále se vytváří skupina `utb` (řádek 5), která má k hodnotám definovaným ve *view* `all` přístup pouze pro čtení pouze z IP adres definovaných v seznamu `snmp`. Na řádku 6 je pak definovaný uživatel `watchdog`, patřící do skupiny `utb`, s heslem `qwerty123` - smí ovšem přistupovat také jen z IP adres definovaných v seznamu `snmp`. Seznam IP adres `snmp` je pak definován na řádcích 8-10 (standardní chování seznamu je takové, že adresy, které nejsou povolené pomocí *permit*, jsou zakázány).

Pro zjišťování dat ze serveru **eye** lze pak použít příkazy `snmpwalk` nebo `snmpget`, popřípadě využít funkcí z knihovny SNMP pro vytvoření vlastního programu.

```
$ snmpget -v 3 -a MD5 -A qwerty123 -u watchdog -l authNoPriv 10.5.0.16 SNMPv2-MIB::sysName.0
SNMPv2-MIB::sysName.0 = STRING: bb0.net.fai.utb.cz
```

6.2 Nastavení páteřních přepínačů

6.2.1 Základní síťová konektivita

Veškerá komunikace mezi jednotlivými páteřními přepínači probíhá v rámci sítě č. 501 (`u5_backbone`) - nastavení IP adresy zařízení se provede na virtuálním síťovém rozhraní `Vlan501`. IP adresa brány je `10.5.0.1`, ta je na virtuálním směrovači, obsluhovat ho bude pomocí protokolu HSRP jeden z dvojice přepínačů **bb0** a **bb2**. Tato dvě zařízení nebudou mít nastavenu žádnou IP adresu brány, protože tuto informaci budou dostávat pomocí protokolu OSPF z centrálního směrovače. Ostatní dva přepínače (**bb1** a **bb3**) budou mít IP adresu brány nastavenou pevně.

```
1: !
2: hostname bb0
3: !
4: ip routing
5: !
6: interface Vlan501
7:  ip address 10.5.0.16 255.255.255.0
8: !
```

```
1: !
2: hostname bb2
3: !
4: ip routing
5: !
6: interface Vlan501
7:  ip address 10.5.0.18 255.255.255.0
8: !
```

```
1: !
2: hostname bb1
3: !
4: ip routing
5: !
6: interface Vlan501
7:  ip address 10.5.0.17 255.255.255.0
8: !
9: ip route 0.0.0.0 0.0.0.0 10.5.0.1
10: !
```

```
1: !
2: hostname bb3
3: !
4: ip routing
5: !
6: interface Vlan501
7:  ip address 10.5.0.19 255.255.255.0
8: !
9: ip route 0.0.0.0 0.0.0.0 10.5.0.1
10: !
```

Příkaz `ip routing` na řádku 4 podstatně ovlivňuje chování celého přepínače. Bez něho totiž celé zařízení funguje v továrním nastavení pouze jako přepínač, bez jakýchkoliv směrovacích funkcí. Zadáním tohoto příkazu je však možné směrovací funkce využívat, to se hodí především pro protokol OSPF.

6.2.2 Nastavení HSRP

Nastavení protokol HSRP zajišťujícího funkčnost virtuálního směrovače bude shodná pro všechna virtuální rozhraní, kde bude nastaven - přepínač **bb0** bude primární (priorita 64) a přepínač **bb2** bude záložní (priorita 58). V případě nefunkčnosti spojení s centrálním směrovačem **rc** klesne priorita o 16, což umožní snadné přebrání funkce směrovače v případě výpadku.

```
1: !
2: hostname bb0
3: !
4: interface Vlan501
5:  description U5 backbone network
6:  ip address 10.5.0.16 255.255.255.0
7:  standby 1 ip 10.5.0.1
8:  standby 1 priority 64
9:  standby 1 preempt
```

```
1: !
2: hostname bb2
3: !
4: interface Vlan501
5:  description U5 backbone network
6:  ip address 10.5.0.18 255.255.255.0
7:  standby 1 ip 10.5.0.1
8:  standby 1 priority 56
9:  standby 1 preempt
```

```
10:  standby 1 authentication md5
          key-string 7 0217135E191216
11:  standby 1 track GigabitEthernet0/1 16
12: !
13: interface Vlan520
14:  description Network FAI UIUI
15:  ip address 10.5.64.2 255.255.254.0
16:  standby 1 ip 10.5.64.1
17:  standby 1 priority 64
18:  standby 1 preempt
19:  standby 1 authentication md5
          key-string 7 095D590C0B110E
20:  standby 1 track GigabitEthernet0/1 16
21: !
22: interface Vlan521
23:  description Network FAI UPKS
24:  ip address 10.5.66.2 255.255.254.0
25:  standby 1 ip 10.5.66.1
26:  standby 1 priority 64
27:  standby 1 preempt
28:  standby 1 authentication md5
          key-string 7 095D590C0B110E
29:  standby 1 track GigabitEthernet0/1 16
30: !
```

```
10:  standby 1 authentication md5
          key-string 7 0217135E191216
11:  standby 1 track GigabitEthernet0/1 16
12: !
13: interface Vlan520
14:  description Network FAI UIUI
15:  ip address 10.5.64.3 255.255.254.0
16:  standby 1 ip 10.5.64.1
17:  standby 1 priority 56
18:  standby 1 preempt
19:  standby 1 authentication md5
          key-string 7 095D590C0B110E
20:  standby 1 track GigabitEthernet0/1 16
21: !
22: interface Vlan521
23:  description Network FAI UPKS
24:  ip address 10.5.66.3 255.255.254.0
25:  standby 1 ip 10.5.66.1
26:  standby 1 priority 56
27:  standby 1 preempt
28:  standby 1 authentication md5
          key-string 7 095D590C0B110E
29:  standby 1 track GigabitEthernet0/1 16
30: !
```

Nastavení na obou přepínačích je téměř totožné, liší se pouze v IP adresách jednotlivých virtuálních rozhraní (řádky 6, 15 a 24) a nastavením priority směrovače (řádky 8, 17 a 26).

Stejné nastavení protokolu HSRP (jedná se jen o řádky začinající klíčovým slovem `standby`) je pak nutné zadat na všech virtuálních rozhraních pro zaměstnanecké sítě a pro sítě, které nejsou zakončeny na přepínači v jedné rozvodně.

6.2.3 Nastavení DHCP serveru

Pro ty virtuální sítě, jejichž koncová zařízení jsou zapojena do přepínačů v různých rozvodnách (např. zaměstnanecké sítě), je nutné přidělený adresní prostor rozdělit na dvě části, jednu část pak přiřadit na DHCP server přepínače **bb0** a druhou část na **bb2**, jak je vidět v příkladu sítě ÚPKS s adresním prostorem `10.5.66/23`:

```
 1: !
 2: hostname bb0
 3: !
 4: ip dhcp excluded-address 10.5.66.0 10.5.66.4
 5: ip dhcp excluded-address 10.5.67.0 10.5.67.255
 6: !
 7: ip dhcp pool fai_upks
 8:    network 10.5.66.0 255.255.254.0
 9:    default-router 10.5.66.1
10:    dns-server 10.5.0.2
11:    domain-name fai.utb.cz
12:    lease 0 1
13: !
14: ip dhcp-server 10.5.66.2
15: !
```

Na řádcích 4 a 5 je definován seznam IP adres, které DHCP server *nesmí* přidělit žádné koncové stanici. IP adresy na na řádku 4 jsou určeny pro bránu (zde je třeba počítat se

4 IP adresami: virtuální směrovač, dvě IP adresy pro virtuální zařízení přepínačů **bb0** a **bb2** a jedna IP adresa do rezervy, např. při výměně směrovačů apod.). IP adresy na řádku 5 bude přidělovat DHCP server na přepínači **bb2**.

Řádky 7-12 definují adresní prostor, ze kterého se budou přidělovat IP adresy jednotlivým koncovým zařízením: je definována síť a její maska (řádek 8), IP adresa brány (řádek 9), DNS server (řádek 10) a lokální DNS doména používaná v této síti (řádek 11). Řádek 12 říká, na jak dlouho budou IP adresy přidělovány (0 dní, 1 hodina). Řádek 14 pak již spouští DHCP server pro virtuální síť s IP adresou `10.5.66.2`.

```
 1: !
 2: hostname bb2
 3: !
 4: ip dhcp excluded-address 10.5.66.0 10.5.66.255
 5: !
 6: ip dhcp pool fai_upks
 7:    network 10.5.66.0 255.255.254.0
 8:    default-router 10.5.66.1
 9:    dns-server 10.5.0.2
10:    domain-name fai.utb.cz
11:    lease 0 1
12: !
13: ip dhcp-server 10.5.66.3
14: !
```

Nastavení DHCP serveru na přepínači **bb2** se liší pouze v seznamu nepřidělovaných IP adres. Na řádce 4 je vidět, že IP adresy nebudou přidělovány z první části adresního prostoru. Ostatní natavení je totožné (vyjma IP adresy síťového rozhraní na řádku 13).

U sítí, které jsou připojeny do jedné rozvodny, není třeba adresní prostor nijak dělit. Nastavení je velmi podobné, jak je vidět z ukázky pro učebnu B202:

```
 1: !
 2: hostname bb1
 3: !
 4: ip dhcp excluded-address 10.5.144.1 10.5.144.4
 5: !
 6: ip dhcp pool lab_b202
 7:    network 10.5.144.0 255.255.255.192
 8:    default-router 10.5.144.1
 9:    dns-server 10.5.0.2
10:    domain-name b202.lab.fai.utb.cz
11:    lease 0 1
12: !
13: ip dhcp pool lab_b202_teacher
14:    host 10.5.144.4
15:    hardware-address 0000.c001.babe
16:    client-name teacher
17: !
18: ip dhcp-server 10.5.144.1
19: !
20: interface Vlan555
21:   ip address 10.5.144.1 255.255.255.192
22: !
```

Z adresního prostoru `10.5.144.1/26` se nebudou přidělovat první 4 IP adresy (řádek 4). Konfigurační blok na řádcích 7-11 definuje opět parametry přidělování IP adres a další blok na řádcích 13-16 ukazuje statické přiřazení IP adresy pro učitelský počítač v laboratoři. Parametry nastavení DHCP v síti `10.5.144.0/26` jsou dědičné a proto pro učitelský počítač budou v rámci DHCP odpovědi zaslány i údaje o IP adrese brány, DNS serveru i doméně (řádky 8-10). Staticky přidělovaná IP adresa `host 10.5.144.4` sice koliduje s definicí přidělovaných IP adres v seznamu na řádce 4, to ale nevadí, protože prostor na řádku 4 se týká pouze dynamického přidělování IP adres.

Administrátorovi se může často hodit seznam přidělených IP adres, ať už k okamžitému prohlížení nebo pro zpětné dohledávání. DHCP server na zařízeních `Cisco` tuto informaci podává přímo použitím příkazu v administrativním prostředí, na todaz pomocí protokolu SNMP nebo tento seznam může ve formě textového souboru periodicky nahrávat na vzdálený server. Z hlediska zpětného dohledání je ideální poslední možnost, ovšem získaná data na serveru je třeba také periodicky zpracovávat - definované URL[27] může přímo zpracovávat externí program.

```
!
ip dhcp database http://dhcp@qwerty:10.5.0.2/dhcp-server
!
```

Ukázka přidělení IP adres jednotlivým koncovým zařízením:

```
bb0# show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
10.5.64.5           0003.ba98.8d71          May 25 2010 03:11 PM    Automatic
10.5.66.7           0001.4acb.2475          May 25 2010 03:00 PM    Automatic
10.5.66.9           0003.ba98.8d70          May 25 2010 03:11 PM    Automatic
```

Stejné údaje zapsané do souboru pomocí `ip dhcp database`:

```
*time* May 25 2010 02:14 PM
*version* 1
!IP address     Type  Hardware address   Lease expiration       VRF
10.5.64.5       1     0003.ba98.8d71     May 25 2010 03:11 PM
10.5.66.7       1     0001.4acb.2475     May 25 2010 03:00 PM
10.5.66.9       1     0003.ba98.8d70     May 25 2010 03:11 PM
!Vrf
*end*
```

V případě, že spuštění DHCP serveru na páteřních přepínačích nebude z možné, např. z důvodu zavádění centrálního DHCP serveru, je nutné na páteřních zařízeních pro každou virtuální síť nastavit tento DHCP server zvlášť. DHCP pakety z koncových stanic pak bude páteřní přepínač předávat k vyřízení přímo tomuto DHCP serveru. Funkce DHCP serveru na páteřním zařízení musí být samozřejmě vypnuta.

[27] Uniform Resource Locator, z angl.

```
!
interface Vlan520
 ip helper-address 10.0.0.1
!
```

6.2.4 Nastavení VTP

Všechny páteřní přepínače budou v rámci protokolu VTP používat jeho verzi 3 a budou označeny jako `VTP Server`. V této verzi protokolu VTP totiž každý VTP server funguje de facto jako VTP klient, tj. nemůže měnit konfiguraci VTP domény, dokud neproběhne tzv. *takeover*[28]. To je ruční administrátorský zásah, který pak umožňuje provádět změny. Nastavení VTP není součástí viditelné konfigurace, nastavení probíhá takto:

```
1: bb0# configure terminal
2: bb0(config)# vtp version 3
3: bb0(config)# vtp mode server vlan
4: bb0(config)# vtp mode server mst
5: bb0(config)# vtp domain u5
6: bb0(config)# vtp password qwerty
7: bb0(config)# vtp pruning
8: bb0(config)# exit
9: bb0#
```

V nastavení je definována používaná verze (řádek 2), VTP doména (řádek 5) a heslo (řádek 6). Na řádcích 3 a 4 je definováno základní chování VTP - zařízení bude pracovat v režimu `server`, a to jak pro definici virtuálních sítí, tak pro definici jednotlivých instancí protokolu MSTP. Na 7. řádku je pak zapnutá funkce *pruning*, která omezuje rozesílání některých rámců mezi jednotlivými přepínači.

V případě, že je třeba měnit seznam virtuálních sítích nebo MSTP instancí, je třeba provést na přepínači nejprve *takeover*, jinak přepínač nedovolí administrátorovi provádět žádné změny. Protože konfigurace VTP je chráněna heslem, bude administrátor při této akci na heslo dotázán, pak teprve k převzetí dojde:

```
bb0# vtp primary vlan
Enter VTP password: (qwerty)
This system is becoming primary for feature vlan
bb0# vtp primary mst
Enter VTP password: (qwerty)
This system is becoming primary for feature mst
```

Po zadání těchto příkazů (nebo jen jednoho z nich) lze pak provádět změny, které pak budou automaticky distribuovány ostatním přepínačům v doméně `u5`. Server zůstává tzv. *primárním serverem* až do doby, kdy dojde k jeho vypnutí nebo k převzetí kontroly jiným (do té doby sekundármín) VTP serverem.

[28] převzetí, z angl.

6.2.5 Nastavení STP

Na všech přepínačích v budově U5 bude použit protokol STP ve formě `Multiple STP` (MSTP), jednotlivé virtuální sítě tedy budou sdruženy do jednotlivých instancí, pro které se bude vypočítávat L2 topologie. Pro potřeby simulace byly všechny sítě počítačových laboratořích přiřazeny do jedné skupiny a ostatní do druhé:

```
1: !
2: spanning-tree mode mst
3: !
4: spanning-tree mst configuration
5:  name u5
6:  revision 2
7:  instance 1 vlan 11, 500-549
8:  instance 2 vlan 550-599
9: !
```

Aby správně fungovaly různé výpočty topologií pro jednotlivé instance, musí se nastavit páteřním přepínačům **bb0** a **bb2** různé priority:

```
1: !                                      1: !
2: hostname bb0                           2: hostname bb2
3: !                                      3: !
4: spanning-tree mst 1 root primary       4: spanning-tree mst 1 root secondary
5: spanning-tree mst 2 root secondary     5: spanning-tree mst 2 root primary
6: !                                      6: !
```

Příkazy na řádcích 4 a 5 nastavují prioritu jednotlivých zařízení - v nezměněném továrním nastavení je tato priorita rovna `32768`, označení *root primary* mění tuto hodnotu na `24576`, označení *root secondary* na `28672`.

Nastavení jednotlivých instancí musí být totožné na všech přepínačích, které jsou propojeny na 2. vrstvě OSI, jednotná konfigurace je tedy šířena automaticky pomocí protokolu VTP.

Páteřní přepínače **bb1** a **bb3** mají v rámci obou instancí MSTP dvě možné fyzické cesty, kudy dostat data k přepínačům **bb0** a **bb2**. V případě, že primární cesta je z nějakého důvodu nedostupná (výpadek linky nebo přepínače), může trvat i několik desítek sekund, než protokol STP vypočítá novou cestu (výpočet je zdržován především předepsanými časovými prodlevami při čekání na odpovědi od jednotlivých zařízení). Aby se tato doba zkrátila, bude na **bb1** a **bb3** zapnuta funkce *uplinkfast* - ta neustále sleduje cestu k *root* přepínači a v případě změny topologie zareaguje rychleji (v řádu několika sekund) [36].Tato funkce má smysl pouze na přepínačích, které v L2 topologii nejsou *root* přepínače a k *root* přepínači mají alespoň 2 různé cesty.

```
!                                 !
hostname bb1                      hostname bb3
!                                 !
spanning-tree uplinkfast          spanning-tree uplinkfast
!                                 !
```

6.2.6 Směrování pomocí protokolu OSPF

Všechny páteřní přepínače jsou přiřazeny dovnitř OSPF oblasti *area 5*. Protože tato oblast má jen jedno připojení k páteřní síti (i když je realizováno dvěma spoji), je tato oblast typu *stub*[29]. Informace o dostupných směrech do jiných oblastí zde není nutné distribuovat, přepínačům v této oblasti plně postačí, pokud si navzájem sdělí pouze informace o svých vlastních sítích a směrování do dalších částí univerzity jim zajistí hraniční směrovače. Nastavení protokolu OSPF je téměř shodné u dvojice **bb0** - **bb2**:

```
 1: !                                                  1: !
 2: hostname bb0                                       2: hostname bb2
 3: !                                                  3: !
 4: interface Vlan11                                   4: interface Vlan11
 5:  ip address 10.0.0.5 255.255.255.0                 5:  ip address 10.0.0.6 255.255.255.0
 6:  ip ospf message-digest-key 1 md5 7 051A110A335857  6:  ip ospf message-digest-key 1 md5 7 051A110A335857
 7: !                                                  7: !
 8: interface Vlan501                                  8: interface Vlan501
 9:  ip address 10.5.0.16 255.255.255.0                9:  ip address 10.5.0.18 255.255.255.0
10:  ip ospf message-digest-key 1 md5 7 051A110A335857 10:  ip ospf message-digest-key 1 md5 7 051A110A335857
11:  ip ospf priority 8                               11:  ip ospf priority 4
12: !                                                 12: !
13: router ospf 1                                     13: router ospf 1
14:  router-id 10.0.0.5                               14:  router-id 10.0.0.6
15:  log-adjacency-changes                            15:  log-adjacency-changes
16:  area 0 authentication message-digest             16:  area 0 authentication message-digest
17:  area 5 authentication message-digest             17:  area 5 authentication message-digest
18:  area 5 stub no-summary                           18:  area 5 stub no-summary
19:  area 5 range 10.5.0.0 255.255.0.0 cost 16        19:  area 5 range 10.5.0.0 255.255.0.0 cost 32
20:  passive-interface default                        20:  passive-interface default
21:  no passive-interface Vlan11                      21:  no passive-interface Vlan11
22:  no passive-interface Vlan501                     22:  no passive-interface Vlan501
23:  network 10.0.0.0 0.0.0.255 area 0                23:  network 10.0.0.0 0.0.0.255 area 0
24:  network 10.5.0.0 0.0.225.255 area 5              24:  network 10.5.0.0 0.0.225.255 area 5
25: !                                                 25: !
```

Většina nastavení byla již vysvětlena v kapitole 4.4, ovšem některé řádky jsou zde navíc. Řádek 18 definuje oblast *area 5* jako *stub*, směrovače tedy do této oblasti nebudou posílat informace o sítích, které obdržely od externích směrovačů (např. od **rc** nebo **ru1**). Řádky 20-22 definují, na která síťová rozhraní mají směrovače zasílat informace o směrování: tyto informace budou zasílány pouze směrovačům připojeným do sítí č. 11 a 501. Zasílání těchto informací jinam by nemělo smysl a mohlo by to být i považováno za prozrazování citlivých informací.

Sítě, které jsou připojeny do **bb0** i **bb2** (např. zaměstnanecké sítě) jsou oznamovány přepínačům **bb1** a **bb3**, ty se ovšem musí rozhodnout, zda budou preferovat cestu přes **bb0** nebo **bb1**. Toto rozhodování jim usnadní nastavení *ceny* cesty přes jednotlivé přepínače (vybrána bude nižší hodnota):

[29] pahýl, z angl.

```
 1: !                                          1: !
 2: hostname bb0                               2: hostname bb2
 3: !                                          3: !
 4: interface Vlan520                          4: interface Vlan520
 5:  ip address 10.5.64.2 255.255.254.0        5:  ip address 10.5.64.3 255.255.254.0
 6:  ip ospf cost 16                           6:  ip ospf cost 32
 7: !                                          7: !
 8: interface Vlan521                          8: interface Vlan521
 9:  ip address 10.5.66.2 255.255.254.0        9:  ip address 10.5.66.3 255.255.254.0
10:  ip ospf cost 16                          10:  ip ospf cost 32
11: !                                         11: !
12: interface Vlan522                         12: interface Vlan522
13:  ip address 10.5.68.2 255.255.254.0       13:  ip address 10.5.68.3 255.255.254.0
14:  ip ospf cost 16                          14:  ip ospf cost 32
15: !                                         15: !
```

Rozdílné nastavení *ceny* je vidět na řádcích 6, 10 a 14. Toto nastavení je nutné udělat pro všechny sítě zapojené tímto způsobem, jde o ty sítě, na nichž se používá protokol HSRP. Nastavení OSPF na ostatních dvou přepínačích je jednodušší:

```
 1: !                                                    1: !
 2: hostname bb1                                        2: hostname bb3
 3: !                                                   3: !
 4: interface Vlan501                                   4: interface Vlan501
 5:  ip address 10.5.0.17 255.255.255.0                 5:  ip address 10.5.0.19 255.255.255.0
 6:  ip ospf message-digest-key 1 md5 7 051A110A335857  6:  ip ospf message-digest-key 1 md5 7 051A110A335857
 7: !                                                   7: !
 8: router ospf 1                                       8: router ospf 1
 9:  router-id 10.5.0.17                                9:  router-id 10.5.0.19
10:  log-adjacency-changes                             10:  log-adjacency-changes
11:  area 5 authentication message-digest              11:  area 5 authentication message-digest
12:  area 5 stub                                       12:  area 5 stub
13:  passive-interface default                         13:  passive-interface default
14:  no passive-interface Vlan501                      14:  no passive-interface Vlan501
15:  network 10.5.0.0 0.0.255.255 area 5               15:  network 10.5.0.0 0.0.255.255 area 5
16: !                                                  16: !
```

Výpis směrovací tabulky na **bb0**:

```
 1: bb0# show ip route
 2: Gateway of last resort is 10.0.0.1 to network 0.0.0.0
 3:      10.0.0.0/8 is variably subnetted, 8 subnets, 4 masks
 4: C       10.0.0.0/24 is directly connected, Vlan11
 5: O IA    10.1.0.0/16 [110/2] via 10.0.0.8, 00:16:02, Vlan11
 6: C       10.5.0.0/24 is directly connected, Vlan501
 7: C       10.5.68.0/23 is directly connected, Vlan522
 8: C       10.5.66.0/23 is directly connected, Vlan521
 9: C       10.5.64.0/23 is directly connected, Vlan520
10: O       10.5.144.0/26 [110/2] via 10.5.0.17, 00:16:02, Vlan501
11: O       10.5.144.64/26 [110/2] via 10.5.0.17, 00:16:02, Vlan501
12: O*E2 0.0.0.0/0 [110/1] via 10.0.0.1, 00:16:02, Vlan11
```

V tomto výpisu jsou vidět sítě, do nichž je přepínač přímo připojen (řádky 4, 6-9), informace o bráně, kterou dostal přepínač protokolem OSPF (řádek 12), a sítě, o nichž se přepínač dozvěděl díky protokolu OSPF: síť v *budově* U1 (řádek 5) a další dvě sítě v *budově* U5 (řádky 10 a 11). Výpis směrovací tabulky **bb2** je totožný, výpis směrovací tabulky na **bb1** je ale jiný:

```
 1: bb1# show ip route
 2: Gateway of last resort is 10.5.0.1 to network 0.0.0.0
 3:      10.0.0.0/8 is variably subnetted, 7 subnets, 3 masks
 4: C       10.5.0.0/24 is directly connected, Vlan501
 5: O       10.5.68.0/23 [110/17] via 10.5.0.16, 00:03:30, Vlan501
 6: O       10.5.66.0/23 [110/17] via 10.5.0.16, 00:03:30, Vlan501
 7: O       10.5.64.0/23 [110/17] via 10.5.0.16, 00:03:30, Vlan501
 8: C       10.5.144.64/26 is directly connected, Vlan556
 9: C       10.5.144.0/26 is directly connected, Vlan555
10: S*   0.0.0.0/0 [1/0] via 10.5.0.1
```

Na řádcích 5-7 jsou sítě na jiných směrovačích v *budově* U5, řádky 4, 8 a 9 ukazují přímo připojené sítě a na řádku 10 je zobrazena informace o statickém nastavení brány.

6.2.7 Propojení jednotlivých přepínačů

Propojení páteřních směrovačů je realizováno pomocí agregace jednotlivých fyzických spojů. Během simulace byly použity dva fyzické spoje. Logické spoje jsou typu *trunk* (umožňuje vedení více virtuálních sítí v rámci jednoho spojení), s použitou *nativní* sítí č. 502. Tato síť je vyhrazena pro sestavování tohoto spojení, žádná data v rámci této sítě se ale přenášet nesmí, jako prevence proti útoku typu `VLAN Hopping` [35].

```
 1: !
 2: hostname bb0
 3: !
 4: interface Port-channel10
 5:  description bb1
 6:  switchport trunk encapsulation dot1q
 7:  switchport trunk native vlan 502
 8:  switchport trunk allowed vlan 501,503-599
 9:  switchport mode trunk
10: !
11: interface GigabitEthernet0/3
12:  description bb1
13:  switchport trunk encapsulation dot1q
14:  switchport trunk native vlan 502
15:  switchport trunk allowed vlan 501,503-599
16:  switchport mode trunk
17:  channel-group 10 mode desirable
18: !
19: interface GigabitEthernet0/4
20:  description bb1
21:  switchport trunk encapsulation dot1q
22:  switchport trunk native vlan 502
23:  switchport trunk allowed vlan 501,503-599
24:  switchport mode trunk
25:  channel-group 10 mode desirable
26: !
```

Uvedené nastavení ukazuje vytvoření logického agregačního spojení `Port-channel10` (řádek 4) a nastavení spojení typu *trunk* (řádky 6 a 9). Řádek 7 definuje *nativní* virtuální síť a řádek 8 definuje seznam virtuálních sítí, ve kterých je umožněn přenos dat v tomto spojení. Toto nastavení je shodné pro všechny fyzické porty, které jsou součástí tohoto virtuálního spoje, přiřazení je pak vidět na řádcích 17 a 25. Nastavení dalších agregačních spojů je totožné s touto ukázkou, to se týká jak jednotlivých propojů páteřních přepínačů, tak připojení přístupových přepínačů.

6.3 Nastavení přístupových přepínačů

6.3.1 Základní síťová konektivita

Základní připojení k síti má každý přístupový přepínač v rámci virtuální sítě č. 501 (`u5_backbone`). Na virtuálním síťovém rozhraní `Vlan501` je tedy definována jediná IP adresa zařízení a k ní IP adresa brány.

```
!
interface Vlan501
 ip address 10.5.0.32 255.255.255.0
!
ip default-gateway 10.5.0.1
!
```

6.3.2 Nastavení protokolu STP

Přepínače budou pracovat v režimu MSTP, L2 topologie tedy nebude vypočítávána pro každou virtuální síť zvlášť, ale vždy pro skupinu sítí, u jejichž členů jsou požadavky na shodnou topologii. Nastavení je jednoduché:

```
1: !
2: spanning-tree mode mst
3: spanning-tree portfast bpduguard default
4: !
```

Řádek 2 nastavuje režim MSTP, řádek 3 pak říká, že u všech přístupových portů, u kterých bude navíc u protokolu STP nastavena funkce `portfast`, bude zapnutá automaticky funkce `BPDU Guard`. Pokud přepínač obdrží na tomto portu BPDU zprávu, bude to považovat za chybu připojeného zařízení a port vypne (dá ho do stavu `err-disable`).

6.3.3 Nastavení protokolu VTP

Všechny přístupové přepínače používají protokol VTP k tomu, aby měly aktuální seznam virtuálních sítí a jednotlivých instancí pro MSTP. Nastavení tohoto protokolu není součástí běžně viditelné konfigurace, po jeho nastavení se ale konfigurace přepínače upravuje automaticky.

```
1: ac00# configure terminal
2: ac00(config)# vtp version 3
3: ac00(config)# vtp mode client vlan
4: ac00(config)# vtp mode client mst
5: ac00(config)# vtp domain u5
6: ac00(config)# vtp password qwerty
7: ac00#
```

Tímto jednoduchým nastavením je řečeno, že se bude používat protokol VTP ve verzi 3 (rádek 2) a že se mají akceptovat informace o virtuálních sítích (řádek 3) a o instancích protokolu MSTP (řádek 4) - to vše v režimu `client`, přepínač tedy informace sbírá a akceptuje, ale nemůže je nijak měnit. Na řádku 5 je pak nastavena VTP doména a na řádku 6 heslo k této doméně. Při výpisu konfigurace je pak již vidět konkrétní nastavení MSTP:

```
!
spanning-tree mst configuration
 name u5
 revision 2
 instance 1 vlan 11, 500-549
 instance 2 vlan 550-599
!
```

Podobně je pak vidět i seznam virtuálních sítí:

```
ac00# show vlan brief | in ^52[0-3]
520  fai_uiui                         active    Fa0/9, Fa0/10, Fa0/11, Fa0/12
521  fai_upks                         active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
522  fai_uart                         active
523  fai_uem                          active
```

6.3.4 Zvýšená ochrana komunikace před útoky

Na přístupových přepínačích je zapnuta ochrana před existencí nechtěného DHCP serveru, *DHCP Snooping*. Při zapnutí této technologie (je možné jen pro konkrétní seznam virtuálních sítí) je nutno ručně definovat porty, ne kterých se smí vyskytovat DHCP server - v případě přístupových přepínačů je to vždy připojení k páteřnímu přepínači, na ostatních přepínačích jsou některé druhy paketů z DHCP komunikace automaticky zahozeny.

```
!
ip dhcp snooping vlan 520-599
ip dhcp snooping
!
```

Zapnutím této funkce přepínač aktivně sleduje přenos DHCP paketů a na základě jeho analýzy si sestavuje tabulku, ve které jsou provázány informace o MAC adrese, o fyzickém portu, kde se zařízení s touto MAC adresou nachází, a o IP adrese, kterou přidělil DHCP server a kterou koncová stanice akceptovala. Tato tabulka se dá i zobrazit:

```
ac00# show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN
Interface
------------------  ---------------  ----------  -------------  ---- --------------------
00:00:C0:CA:C0:1A   10.5.66.66       66327       dhcp-snooping   521 FastEthernet0/1
00:00:FE:ED:BE:EF   10.5.66.36       3502        dhcp-snooping   521 FastEthernet0/8
Total number of bindings: 2
```

Tyto informace lze využít ke kontrole paketů typu ARP - každý paket typu ARP, který přepínač obdrží, bude zkontrolován, zda MAC a IP adresa obsažené v tomto paketu odpovídají záznamům v této tabulce. Vyskytne-li se ARP paket s chybnými údaji, je to považováno za útok na L2 komunikaci a port bude okamžitě vypnut (nastaven jako `err-disable`). Tato funkce se nazývá `IP ARP Inspection` a má podobné nastavení jako `DHCP Snooping`, musí se definovat seznam virtuálních sítí, ve kterých bude kontrola probíhat a lze označit porty, na kterých se kontrola provádět nebude (připojení přepínače k páteřním přepínačům):

```
!
ip arp inspection vlan 520-599
ip arp inspection validate src-mac dst-mac
!
```

6.3.5 Připojení k páteřnímu přepínači

Připojení v simulaci využívá dvou portů o rychlosti 1 $Gb.s^{-1}$ spojených pomocí technologie `etherchannel` do jednoho logického rozhraní. V původních plánech se uvažují až šestinásobné spoje, nastavení všech portů je ale identické, proto pro testování dvojnásobné spojení postačuje. Spojení je samozřejmě typu *trunk*, to znamená, že v rámci tohoto spojení je možné vést více virtuálních sítí najednou.

Zabezpečení tohoto spojení spočívá v nastavení tzv. *nativní virtuální sítě*. Komunikace mezi obě zařízeními, která jsou tímto spojením propojena a která vytváří a udržuje spojení typu *trunk*, probíhá v této síti. Z bezpečnostních důvodů bude mít tato *nativní* síť vlastní číslo (502 - `u5_trunk`) jako prevence před útokem typu `VLAN hopping` [35]. Tato síť nebude určena k žádným jiným účelům.

Spojení typu *trunk* umožňuje přenos dat v kterékoliv definované virtuální síti. Seznam sítí, které mohou spojením procházet, lze ale omezit. Páteřní přepínače potřebují pouze sítě v rozmezí 501-599, síť 502 bude zakázána. Není třeba omezovat tyto sítě ještě více (např. jsou-li přístupové porty jen ve 3 různých virtuálních sítí, mohl by se tento seznam omezit právě na ně a na administrativní síť 501), to pak přináší administrativní zátěž při změnách na síti.

```
 1: !
 2: interface Port-channel1
 3:  description uplink
 4:  switchport trunk native vlan 502
 5:  switchport trunk allowed vlan 501,503-599
 6:  switchport mode trunk
 7:  ip dhcp snooping trust
 8:  ip arp inspection trust
 9: !
10: interface GigabitEthernet0/1
11:  switchport trunk native vlan 502
12:  switchport trunk allowed vlan 501,503-599
13:  switchport mode trunk
14:  ip arp inspection trust
15:  channel-group 1 mode desirable
16:  ip dhcp snooping trust
17: !
18: interface GigabitEthernet0/2
19:  switchport trunk native vlan 502
20:  switchport trunk allowed vlan 501,503-599
21:  switchport mode trunk
22:  ip arp inspection trust
23:  channel-group 1 mode desirable
24:  ip dhcp snooping trust
25: !
```

Nastavení logického portu (`Port-channel`) je shodné s nastavením jednotlivých fyzických portů, u těch je navíc jen definice přiřazení k logickému portu (řádky 15 a 23). Řádky 7, 16 a 24 označují tyto porty za takové, kde se mohou vyskytovat DHCP servery, řádky 8, 14 a 22 vypínají na těchto portech funkci `Dynamic ARP Inspection` (pakety typu `ARP` nebudou nijak kontrolovány).

6.3.6 Nastavení přístupových portů

Přístupový port je takový, do kterého je připojeno koncové zařízení (např. stolní počítač, tiskárna, notebook atd.), které má přístup do jedné virtuální sítě. Nastavení všech těchto portů je stejné, liší se jen číslem virtuální sítě, do které jsou přiřazeny.

```
 1: !
 2: interface FastEthernet0/2
 3:  switchport access vlan 521
 4:  switchport mode access
 5:  switchport nonegotiate
 6:  switchport port-security maximum 1 vlan access
 7:  switchport port-security
 8:  switchport port-security violation shutdown vlan
 9:  no vtp
10:  no cdp enable
11:  spanning-tree portfast
12:  ip verify source
13: !
```

Řádek 3 přiřazuje port do virtuální sítě č. 521, řádek 4 říká, že tento port je přístupový (neočekává se, že by do něj byl připojen další přepínač). Řádek 5 vypíná protokol DTP - útočník by tento protokol mohl využít k tomu, aby přesvědčil přepínač, že na portu má nastavit spojení typu *trunk*.

Řádky 6-8 omezují počet MAC adres, které se současně mohou vyskytnout na tomto portu. Připojená koncová stanice za normálních okolností komunikuje se sítí právě z jedné MAC adresy, pokud stanice začne vysílat rámce s jinou zdrojovou MAC adresou, může to znamenat problém nebo spíše nějký druh útoku. V případě, že se vyskytne druhá adresa, bude port okamžitě vypnut (řádka 8), přesněji bude nastaven do stavu `err-disable`.

Na řádku 9 je příkaz pro vypnutí protokolu VTP. Informace šířené tímto protokolem (seznam virtuálních sítí a instancí MSTP) není nutné šířit na přístupové porty, ani se nepředpokládá, že by přepínač měl touto cestou tyto informace dostávat.

Řádek 10 vypíná komunikaci protokolem CDP[30] na tomto portu. Tento protokol je standardně zapnut, aby bylo snadné rozpoznat zařízení připojené na druhé straně spojení, to ale na přístupových portech jednak nemá smysl a jednak tím přepínač zbytečně prozrazuje svoji identifikaci.

[30]Cisco Discovery Protocol, z angl.

Protože do portu nebude připojen přepínač, ale koncová stanice, lze zde urychlit protokol STP. To zajišťuje řádek 11 - protokol STP nebude vyčkávat několik sekund po připojení zařízení na to, zda bude nebo nebude dostávat BPDU zprávy.

Poslední nastavení je na řádku 12 - zapnutí funkce `IP Source Guard`: u všechny paketů, které připojená stanice vyšle, bude zkontrolována zdrojová IP i MAC adresa proti údajům, které přidělil DHCP server. Paket, jehož zdrojové adresy nesouhlasí, je přepínačem zahozen (není dále nijak zpracováván ani poslán dále do sítě).

Všechny porty, u kterých se předpokládá, že do nich není nic připojeného, musí být z bezpečnostního hlediska ve stavu `shutdown`. I v případě, že se do portu připojí nějaké zařízení, nebude přepínač nijak komunikovat (nebude žádný signál ani nic odesílat, ani ho přijímat). Na portu nejsou definována žádná další nastavení.

```
1: !
2: interface FastEthernet0/20
3:  shutdown
4: !
```

6.3.7 Automatické zapnutí vypnutých portů

V případě, že síťový provoz na některém přístupovém portu způsobí, že přepínač nastaví port do stavu `err-disable` (de facto vypnutí portu), např. z důvodu překročení maximálního povoleného počtu vyskytujících se MAC adres, je pak nutné pro obnovení provozu port znovu zapnout. To může udělat administrátor ručně, ale při velkém množství takto spravovaných zařízení by to znamenalo zbytečnou administrativní zátěž. Proto je definován seznam důvodů, které mohly způsobit tento stav a kde není ruční zásah nutný. Tam pak bbude postačovat krátký časový interval, po jehož uplynutí se port opět samočinně zapne.

```
1: !
2: errdisable recovery cause bpduguard
3: errdisable recovery cause psecure-violation
4: errdisable recovery cause mac-limit
5: errdisable recovery cause arp-inspection
6: errdisable recovery interval 120
7: !
```

Toto nastavení říká, že každé dvě minuty (řádek 6) přepínač zkontroluje všechny porty, které jsou ve stavu `err-disable`, a opět ho zapne, pokud byla příčinou vypnutí portu jeda z těchto možností:

- koncové zařízení vyslalo BPDU zprávu, to znamená, že toto zařízení může být přepínač, což znamená riziko vzniku smyčky nebo pokus o útok na L2 strukturu sítě (řádek 2)
- bylo porušeno některé z pravidel `port-security` nebo koncové zařízení vyslalo více rámců s různými zdrojovými MAC adresami, počet těchto adres je pak vyšší než definované maximum (řádky 4 a 5)

- připojené zařízení poslalo chybný ARP paket (chybná MAC nebo IP zdrojová adresa paketu, resp. tyto údaje neodpovídají údajům, které přidělil DHCP server) - řádek 5

6.4 Filtrování síťového provozu

6.4.1 Filtrování mezisíťového provozu

Provoz jdoucí z jedné virtuální sítě do druhé prochází přes virtuální síťová rozhraní na páteřních směrovačích, ke kterým lze přiřadit pravidla pro filtrování síťového provozu. Seznamy těchto pravidel (tzv. *access list*) lze aplikovat buď na pakety, které přicházejí na síťové rozhraní, nebo pakety, které opouštějí síťové rozhraní. Výhodnější je filtrování příchozích paketů, u filtrování odchozích musí přepínač před samotným testem jednotlivých pravidel ještě udělat tzv. *routing decision*, tj. musí u paketu určit podle směrovací tabulky, kterým síťovým rozhraním má odejít a pokud se pak má paket ignorovat, protože neodpovídá nastaveným pravidlům, byl výpočet cesty zbytečný. V některých případech je ovšem nutné provádět kontrolu až odchozích paketů, nicméně počet těchto případů je třeba minimalizovat.

Směrovače `Cisco 3560` obsahují základní funkce pro toto filtrování, tím mohou hrát roli jakéhosi základního *firewallu*. V ukázkovém nastavení je vidět nastavení pravidel pro učebnu B202:

```
 1: !
 2: hostanem bb1
 3: !
 4: interface Vlan555
 5:  description Lab B202
 6:  ip address 10.5.144.1 255.255.255.192
 7:  ip access-group lab_b202 in
 8: !
 9: ip access-list extended lab_b202
10:  permit icmp 10.5.144.1 0.0.0.63 any
11:  permit udp 10.5.144.1 0.0.0.63 host 10.5.0.2 eq 53
12:  permit tcp 10.5.144.1 0.0.0.63 host 10.5.16.7 eq 80
13:  permit tcp 10.5.144.1 0.0.0.63 host 10.5.16.7 eq 443
14:  deny ip any any log
15: !
```

Řádek 7 definuje, že seznam pravidel `lab_b202` se má aplikovat na všechny pakety, které přicházejí do rozhraní `Vlan555`. Samotná pravidla tohoto seznamu jsou pak definována na řádcích 10-14: povolení protokolu ICMP kamkoliv, povolení DNS dotazů na server `10.5.0.2` a povolení spojení se serverem `10.5.16.7` (server `vyuka`) na TCP porty 80 a 443 (protokoly HTTP a HTTPS). Poslední pravidlo na řádku 15 pak způsobí, že každý paket, který neodpovídá předchozím pravidlům, bude ignorován a navíc zaznamenán.

Typickým síťovým rozhraním, kde je třeba filtrovat odchozí pakety, může být síťové rozhraní pro síť, kde jsou servery poskytující veřejné služby, tam má smysl aplikovat

pravidla pro oba směry. V případě, že jde o síť, na které je definováno využívání protokolu HSRP, je třeba tento seznam pravidel udržovat stejný na obou hlavních páteřních směrovačích, na **bb0** i **bb2**.

```
 1: !
 2: hostname bb0
 3: !
 4: interface Vlan510
 5:  description Public servers
 6:  ip address 10.5.16.2 255.255.255.0
 7:  standby 1 ip 10.5.16.1
 8:  standby 1 priority 64
 9:  standby 1 preempt
10:  standby 1 authentication md5 key-string 7 095D590C0B110E
11:  standby 1 track GigabitEthernet0/1 16
12:  ip access-group public_in in
13:  ip access-group public_out out
14: !
15: ip access-list extended public_out
16:  remark >> Permit ICMP
17:  permit icmp any 10.5.16.0 0.0.0.255
18:  remark >> Permit established connections
19:  permit tcp any 10.5.16.0 0.0.0.255 established
20:  remark >> Permit DNS answers
21:  permit udp host 10.5.0.2 eq 53 10.5.16.0 0.0.0.255
22:  remark >> Permit traffic to vyuka.fai.utb.cz
23:  permit tcp any host 10.5.16.7 eq 80
24:  permit tcp any host 10.5.16.7 eq 443
25:  permit tcp 10.5.66.0 0.0.1.255 host 10.5.16.7 eq 22
26:  remark >> Deny anything else
27:  deny ip any any log
28: !
29: ip access-list extended public_in
30:  remark >> Permit ICMP
31:  permit icmp 10.5.16.0 0.0.0.255 any
32:  remark >> Permit established connections
33:  permit tcp 10.5.16.0 0.0.0.255 any established
34:  remark >> Permit DNS questions
35:  permit udp 10.5.16.0 0.0.0.255 host 10.5.0.2 eq 53
36:  remark >> Permit traffic from vyuka.fai.utb.cz
37:  permit tcp host 10.5.16.7 host 195.178.88.66 eq 25
38:  permit tcp host 10.5.16.7 any eq 80
39:  permit tcp host 10.5.16.7 any eq 443
40:  permit tcp host 10.5.16.7 range 20 21
41:  remark >> Deny anything else
42:  deny ip any any log
43: !
```

Na řádcích 12 a 13 je svázán název seznamu pravidel se síťovým rozhraním a směrem, na nějž budou pravidla aplikována. Odchozí pakety (tedy pakety jdoucí směrem na jednotlivá zařízení ve virtuální síti) jsou testovány proti pravidlům definovaným na řádcích 15-27: jsou povoleny ICMP pakety (řádek 17), již existující konexe (řádek 19, to se týká především paketů v rámci TCP spojení, která byla navázána z počítačů ve virtuální síti) a DNS odpovědi od dohledového serveru **eye** - `10.5.0.2` (řádek 21). Na řádcích 23-25 jsou definovány konexe jdoucí směrem na server `10.5.16.7`, a to na TCP porty 80 a 443 (odkudkoliv) a na TCP port 22 (pouze z adresního prostoru `10.5.66.0/23`). Pakety, které nebyly povoleny žádným z předchozích pravidel, budou ignoráovny a zaznamenány (řádek 27).

V bloku na řádcích 19-42 je pak definován seznam pravidel pro příchozí pakety, tedy takové, které vysílají servery ve virtuální síti a jdou do jiných sítí. Opět je povolen protokol ICMP (řádek 31) a již existující TCP konexe (řádek 33), navíc jsou povoleny DNS dotazy na dohledový server **eye** (řádek 35). Na řádcích 37-40 jsou pak povoleny odchozí konexe ze serveru `10.5.16.7`: směrem na `195.178.88.66` TCP port 25, kamkoliv na porty 80, 443 a 20-21 (předpokládají se protokoly HTTP, HTTPS a FTP). Každý nepovolený paket je pak opět zaznamenán a ignorován (řádek 42).

6.4.2 Filtrování provozu na přístupových portech

Přístupové přepínače umožňují v omezené míře filtrovat síťový provoz vznikající na koncových zařízeních, a to již na přístupovém portu. Seznamy pravidel podobné těm, které se používají k filtrování mezisíťového provozu, lze vytvářet na přístupových přepínačích a aplikovat je přímo na fyzické porty, ovšem pouze v příchozím směru [37].

```
!
hostname ac00
!
interface GigabitEthernet0/13
 description Foyer printer
 switchport access vlan 505
 switchport mode access
 switchport nonegotiate
 switchport port-security maximum 1 vlan access
 switchport port-security
 switchport port-security violation shutdown vlan
 no vtp
 no cdp enable
 spanning-tree portfast
 ip verify source
 ip access-group foyer_printer in
!
ip access-list extended foyer_printer
 deny tcp any any range 137 139
 deny tcp any any eq 445
 permit ip any any
!
```

V této ukázce je pro tiskárnu připojenou do přístupového přepínače definován seznam pravidel, který povoluje všechen síťový provoz jdoucí ze zařízení, kromě paketů, jejichž cílové porty jsou 137-139 nebo 445 (tím pádem bude připojené zařízení *neviditelné* pro ostatní počítače připojené ve stejném segmentu sítě protokolem NetBIOS, tj. neměla by být možnost ho *sdílet* v operačních systémech platformy Windows).

6.4.3 Propouštění paketů pro funkci Wake-On-Lan

Připravované projekty na FAI UTB počítají s možností vzdáleného hromadného zapínání pracovních stanic ve výukových laboratořích. Na vybraném serveru (např. dohledový server **eye**) bude uložen seznam MAC adres pracovních stanic a jejich přiřazení do konkrétní virtuální sítě. Server pak vyšle na každou pracovní stanici tzv. *magic packet*, speciální paket posílaný protokolem UDP na cílový port 9 o speciálním formátu. Pracovní stanice

pak budou nastaveny tak, že i když bude stanice vypnuta, síťové rozhraní bude na takový paket reagovat a způsobí zapnutí počítače.

Vypnutý počítač ale nemá přiděleou žádnou IP adresu, probouzecí paket tedy nelze poslat přímo. Dohledový server tedy vyšle paket na cílovou IP adresu typu *broadcast*, ta je určena pro všechny počítače v síti. Paket sice dorazí všem stanicím v síti, ale jen jedna na něj bude reagovat. Posílání paketů na tuto adresu se ale musí explicitně povolit na směrovači:

```
 1: !
 2: hostname bb1
 3: !
 4: ip forward-protocol udp 9
 5: !
 6: interface vlan555
 7:  ip address 10.5.144.1 255.255.255.192
 8:  ip directed-broadcast 9
 9: !
10: access-list 9 remark >> Source of wake-on-lan packets
11: access-list 9 permit 10.5.0.2
12: !
```

Na řádku 4 je definován protokol, u něhož je povoleno směrování paketů na adresu typu *broadcast*. Protože by toho ale mohl využít i útočník, je třeba omezit seznam zdrojových IP adres, které tyto pakety mohou posílat - řádek 8 tedy říká, že tyto pakety mohou být pouze takové, které jsou v seznamu pravidel č. 9, tento seznam je pak definován na řádcích 10 a 11.

Dohledový server **eye** bude tedy posílat *magic* pakety protokolem UDP na cílový port 9, v případě výukové laboratoře B202 na IP adresu `10.5.144.63`.

7 Pokusné útoky

V rámci simulace nového zapojení sítě byly provedeny i některé útoky s cílem ověřit odolnost sítě pro nim. Do vybrané sítě č. 521 byly zapojeny 2 počítače, kterým byla přidělena IP adresa z DHCP serveru, v síti se tedy vyskytují 3 počítače:

- 10.5.66.1, brána, MAC adresa 0004.dd80.b8f0
- 10.5.66.7, útočník, MAC adresa 0001.4acb.2475
- 10.5.66.9, oběť, MAC adresa 0003.ba98.8d70

7.1 ARP Cache Poisoning

Prvním pokusem byl útok typu `ARP Cache Poisoning`. Útočník se snaží přesvědčit oběť, že MAC adresa brány je **0001.4acb.2475**, vysílá tedy příslušný ARP paket. Paket je ovšem zachycen na přístupovém přepínači, ignorován a celá akce je zazanamenána. Útok je tedy neúspěšný díky použité technologii `Dynamic ARP Inspection`.

```
May 25 15:29:04 10.5.0.32 311: May 25 13:29:36.178:
  %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa0/1, vlan 521.
  ([0001.4acb.2475/10.5.66.1/0000.0000.0000/10.5.66.9/15:29:35 CEST Tue May 25 2010])
```

7.2 Více MAC adres na jednom přístupovém portu

Útočník se může pokusit o zahlcení paměťové tabulky pomocí generování rámců nebo paketů s různou zdrojovou MAC adresou, i tento druh útoku byl vyzkoušen. Útočník vyšle dva pakety s náhodně generovanými zdrojovými MAC adresami (0000.600d.c01a a 0000.0bad.c01a) na neexistující IP adresu `10.5.66.66`.

Již vyslání prvního paketu způsobilo porušení pravidla, že na přístupovém portu se smí objevit nejvýše 1 zdrojová MAC adresa. První MAC adresa, o které přepínač ví, je běžně používaná MAC adresa zařízení (0001.4acb.2475), každá další tedy může znamenat problém. Přepínač proto přístupový port vypne - celá pracovní stanice útočníka je tedy úplně nedostupná a nemůže nijak komunikovat. Tento stav se po nastavených dvou minutách vrátí opět do normálního stavu, tj. port se samočinně zapne a stanice může dále komunikovat. Celá akce je zaznamenána:

```
May 25 15:47:12 10.5.0.32 313: May 25 13:47:44.531: %PM-4-ERR_DISABLE_VP:
  psecure-violation error detected on Fa0/1, vlan 521. Putting in err-disable state.
May 25 15:47:13 10.5.0.32 314: May 25 13:47:44.531: %PORT_SECURITY-2-PSECURE_VIOLATION:
  Security violation occurred, caused by MAC address 0000.600d.c01a on port FastEthernet0/1.
May 25 15:49:13 10.5.0.32 315: May 25 13:49:44.532: %PM-4-ERR_RECOVER_VP:
  Attempting to recover from psecure-violation err-disable state on Fa0/1, vlan 521.
```

7.3 Krádež IP adresy

Útočník nemusí používat k útokům jen protokol ARP. Zná IP i MAC adresu brány a teoreticky mu nikdo nemůže zabránit v tom, aby si z IP adresního prostoru vzal sám IP adresu, jaká se mu zlíbí. Útočník tedy nastaví svůj počítač tak, že si bez vědomí DHCP přivlastní IP adresu `10.5.66.10` a začne posílat libovolné pakety směrem na stanici oběti (v testu bude použit příkaz *ping*).

Pokud útočníkova stanice nezná MAC adresu oběti, musí ji zjistit nejprve protokolem ARP. Už vyslání takového požadavku ale neodpovídá zaznámům, které dostává přepínač od DHCP serveru. Takový paket je tedy zaznamenán a ignorován:

```
May 25 15:57:34 10.5.0.32 321: May 25 13:58:04.600:
  %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa0/1, vlan 521.
  ([0001.4acb.2475/10.5.66.10/0000.0000.0000/10.5.66.9/15:58:04 CEST Tue May 25 2010])
```

Útočník ale může protokol ARP obejít a upravit si svoji vlastní ARP tabulku podle potřeby, může do ní vnést statické informace o tom, že ip adresa `10.5.66.9` patří k MAC adrese 0003.ba98.8d70. Tím se bude snažit obejít kontrolu protokolu ARP a znovu vyšle pakety pomocí programu *ping*.

Ani tyto pakety ovšem neprojdou přístupovým přepínačem díky funkci `IP Source Guard`. Hodnoty uvnitř paketu (zdrojová MAC a IP adresa) nejsou přepínači známy a proto je paket ignorován. Tato akce ovšem není nijak zaznamenána, neboť použití této funkce funguje uvnitř přepínače tak, že se vytvoří jednoduchý skrytý seznam pravidel, který se přiřadí na fyzický port [37].

Útočník však nemusí použít neexistující IP adresu, může se sám pokusit vydávat za již existující zařízení v síti, proto byla otestována i možnost, že útočník si nastaví IP i MAC adresu brány a bude vysílat směrem k oběti pakety s těmito zdrojovými adresami.

Ani tyto pakety ovšem přes páteřní přepínač neprošly, MAC i IP adresa byly sice v pořádku, ovšem vyskytovaly se na chybném fyzickém portu přepínače. Tabulka, která se používá pro ověření všech těchto údajů, vypadá takto:

```
ac00# show ip source binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN Interface
------------------  ---------------  ----------  -------------  ---- --------------------
00:01:4A:CB:24:75   10.5.66.7        1782        dhcp-snooping   521 FastEthernet0/1
00:03:BA:98:8D:71   10.5.64.5        3289        dhcp-snooping   520 FastEthernet0/9
00:03:BA:98:8D:70   10.5.66.9        3282        dhcp-snooping   521 FastEthernet0/8
Total number of bindings: 3
```

8 Ekonomické aspekty

8.1 Páteřní přepínače

Páteřní přepínače `Cisco 3560G-48TS-E` již univerzita vlastní, 4 kusy jsou vyčleněny k použití v budově FAI. Pořizovací náklady jsou tedy v tomto ohledu nulové. Náklady jsou ale v podobě lidské práce. Přepínače již delší dobu ležely ve skladu, takže je třeba u nich provést aktualizaci operačního systému, zapojit je v laboratorních podmínkách, otestovat jejich vzájemné propojení a nastavit všechny sítě. Taková práce u čtyřech zařízení může zabrat až 2 pracovní dny, vetně rezervy a pořízení dokumentace nebo základního popisu.

Zařízení je dále třeba namontovat do současných rozvoden a provést výměnu kabeláže, taková akce by mohla trvat půl pracovního dne. Celkové náklady na konfiguraci, nastavení a nasazení páteřních přepínačů tvoří celkem **2.5** pracovních dnů.

8.2 Přístupové přepínače

Jeden přepínač `Cisco 2960G-48-TC-L` lze pořídit zhruba za **66 500,- Kč** (cena se odvíjí od aktuálního kursu české koruny k americkému dolaru a slevy, kterou jednotliví prodejci dávají z oficiálního ceníku výrobce, tyto slevy jsou v řádu desítek procent). Při navrhovaném počtu 19 kusů se tedy jedná o celkový náklad **1 263 500,- Kč**.

Konfigurace těchto prvků není tak složitá jako konfigurace páteřních přepínačů, navíc je možné použít základní šablonu, která vznikne při nastavení prvního instalovaného zařízení. Tuto šablonu lze pak nahrát i na ostatní přepínače a pak na nich jen konfigurovat jednotlivé přístupové porty. Konfigurace všech zařízení by tedy neměla být delší než jeden pracovní den.

Instalace jednoho zařízení do rozvoden znamená poměrně dost práce: je třeba vymontovat staré zařízení a předělat kabeláž v rozvodných skříních. Instalace jednoho přístupového přepínače by mohla zabrat až půl hodiny, je tedy třeba počítat s 10 pracovními hodinami, tedy **1.2** pracovního dne.

8.3 Dohledový server

Nároky na dohledový server nejsou příliš vysoké, software, který by zde měl být nainstalovaný, nemá žádné vyšší nároky ani na paměť, ani na procesor, ani na diskový prostor. Operační systém může být libovolná distribuce OS Linux, kde jsou pořizovací náklady nulové. Server bude umístěn v rozvodně, takže by měl mít velikost 1U[31], odhadovaná cena je maximálně **10 000,- Kč**.

[31] 1 rack unit - standardizovaná výška 44.5 mm pro zařízení umísťovaná do rozvodných skříní

Operační systém a jednotlivé podpůrné softwary však musí nainstalovat administrátor, u tohoto konkrétního případu by práce neměla přesáhnout **1.5** pracovního dne.

8.4 Pořizovací náklady

Náklady jsou velmi ovlivněny cenou za lidskou práci. V případě administrátora je předpokládaný náklad **3 000,- Kč** na jeden pracovní den. V této částce jsou zahrnuty jak mzdové náklady (včetně odvodů sociálního a zdravotního pojištění), tak náklady na pracovní místo (kancelářský nábytek, počítač, telefon) a náklady na spotřebu energií (elektřina, teplo apod.).

Zařízení	Počet	Jednotková cena	Celková cena
Cisco 3560G-48-TS-E	4	0	0
Cisco 2960G-48TC-L	19	66 500	1 263 500
Dohledový server	1	10 000	10 000
		Celkem:	1 273 500

Tabulka 14: Pořizovací náklady na modernizaci sítě (Kč bez DPH)

Pracovní úkon	Počet dnů	Celkový náklad
Instalace páteřních přepínačů	2.5	7 500
Instalace přístupových přepínačů	1.2	3 600
Instalace dohledováho serveru	1.5	4 500
	Celkem:	15 600

Tabulka 15: Náklady na práci při modernizaci sítě (v Kč)

8.5 Náklady na provoz

Náklady na správu nově zapojené sítě se nebudou nijak lišit od současných nákladů - univerzita zaměstnává skupinu administrátorů, jejichž práce se sítí FAI se sice může lehce lišit od jejich současné, ale časové vytížení by mělo zůstat stejné, vzhledem k možné automatizaci některých úkonů správy, snadnějšímu monitorování funkčnosti nebo chybovosti

nových prvků a jejich menšímu počtu by mohla být údržba dokonce i časově méně náročná než nyní.

Ke zvýšení nedojde ani v nákladech na elektřinu. V nově navrhované topologii je místo 37 současných zařízení pouze 24, celková spotřeba elektřiny by tedy měla klesnout.

8.6 Odhad životnosti

Životnost nového návrhu struktury sítě je odhadována na 7 let. Odhad je ovlivněn předpokládanou dobou životnosti výrobků `Cisco`, po této době výrobce pravděpodobně nebude prodávat nebo poskytovat podporu pro navrhované přepínače řady `2960` ani `3560`, spíše bude nabízet podobná zařízení vyšší řady s novými funkcemi a vyšší datovou propustností (již nyní jsou nabízeny nově prvky řady `2960-S` s dvěma porty o rychlosti 10 $Gb.s^{-1}$).

Po uplynutí uvedené doby je velmi pravděpodobné, že dojde k požadavku na zvýšení datové propustnosti a popsaná datová propustnost nebude stačit. Dá se také předpokládat posun ve vývoji útoků na počítačové sítě nebo komunikace, které budou vyžadovat nové druhy obrany, které bude třeba nově implementovat.

Tato doba se může zkrátit nebo prodloužit v závislosti na růstu celé univerzity (počet budov, počet připojených zařízení) a požadavcích na jednotlivé funkce sítě. Po uplynutí této doby bude muset dojít k rozhodnutí, zda model vyhovuje nárokům uživatelů a používaným technologiím, zda dojde k úplné nebo částečné renovaci nebo zda se síť ponechá v tomto stavu.

Část IV
ZÁVĚR

Tato práce ukazuje, že současné zapojení počítačové sítě FAI UTB ve Zlíně lze v mnohých směrech vylepšit, především co se týče datové propustnosti sítě, zabezpečení přenášených dat, zálohování spojů mezi aktivními prvky i zálohování aktivních prvků samotných. Fakultní síť potřebuje renovaci síťových prvků a zavedení technologií, které usnadňují její správu a zvyšují její bezpečnost.

Pokusným zapojením aktivních prvků v laboratorních podmínkách bylo ověřeno, že modernizace sítě je možná a že se by se měla dotknout i sítě celouniverzitní. Současná univerzitní topologie, kdy pro celou univerzitu existuje jen jeden směrovač, neumožňuje růst sítě v tak rychlém tempu, jakým se v posledních letech rozšiřuje celá organizace. Do budoucna je třeba počítat s decentralizací sítě, používaných technologií i správy.

Postupy a principy navržené v této práci mohou být aplikovány na další objekty univerzity - stejná nebo podobná topologie sítě jako v budově U5 je použita i v jiných budovách, shodné jsou i použitá síťová zařízení a jejich nastavení. Text práce lze použít pro přípravu projektů, jejichž cílem je získání dotací na renovaci síťových zařízení.

CONCLUSION

Actual network in FAI TBU in Zlín can be improved in many ways, especially in case of bandwidth increase, carried data security and backup of links between active network elements and these elements themselves. The faculty network needs renovation of network equipment and implementation of technologies which make the administration easier and increase security.

It has been confirmed in experiments, that the modernization of the network is possible and that it should affect the network all over the university. Actual university network topology with just one existing router does not allow as fast growth as is the growth of the organisation itself. In near future, the network, used technologies and administration have to be decentralised.

Practices and principles described in this thesis can be applied to other buildings of the university, the network topology currently used in these buildings is the same or analogous to the network in building U5. The same network equipment uses almost the same configuration. Text of this thesis can be used for preparation of grant projects which can ensure renovaition of network devices.

Seznam obrázků

Seznam tabulek

Seznam použitých zkratek

ARP	Address Resolution Protocol - protokol pro získávání informace o IP adrese síťového zařízení v rámci jednoho segmentu počítačové sítě
BPDU	Bridge Protocol Data Unit - malé datové zprávy, které se posílají mezi přepínači v rámci virtuální sítě prostřednictvím protokolu STP, slouží ke zjištění topologie na 2. vrstvě referenčního modelu OSI
CAM	Content Addresable Memory - takto vyhrazená část paměti přepínačů se používá k vytváření databáze, ve které jsou jednotlivé MAC adresy síťových zařízení přiřazeny k existujícímu portu na přepínači
CDP	Cisco Discovery Protocol - slouží k výměně identifikačních údajů dvou síťových zařízení, která jsou na obou koncích fyzického spoje
DHCP	Dynamic Host Configuration Protocol - protokol, který umožňuje počítačům v síti získat nastavení vlastního síťového rozhraní na základě údajů, které dostane od serveru
DNS	Domain Name System - systém doménových jmen, slouží primárně k převodu IP adres na textový řetězec a obráceně, rozšířením tohoto systému lze distribuovat další informace důležité např. pro doručování e-mailů apod.
DTP	Dynamic Trunkting Protocol - protokol vyvinutý a používaný výrobcem síťových zařízení `Cisco` k automatizovanému sestavování spojení typu *trunk*, kdy v rámci jednoho fyzického propojení dvou síťových prvků může vést více virtuálních sítí
GPS	Global Positioning System - družicový systém pro určení polohy a přesného času kdekoliv na planetě Zemi
HSRP	Hot Standby Router Protocol - protokol vyvinutý a používaný výrobcem síťových zařízení `Cisco` ke snadnému zastoupení jednoho směrovače druhým v případě jeho částečné nebo úplné nefunkčnosti
ICMP	Internet Control Message Protocol - protokol používaný v komunikaci v počítačových sítích, nese především informace o nedostupnosti jednotlivých zařízení nebo síťových služeb
IDF	Intermediate Distribution Frame - rozvodna strkturované kabeláže, ovšem menšího rozsahu než MDF (např. pro patro v budově), slouží jako propojovací uzel mezi koncovými stanicemi a centrální rozvodnou

IP	Internet Protocol - základní soubor pravidel pro komunikaci počítačů po síti
L2TP	Layer 2 Tunneling Protocol - protokol, který umožňujě komunikaci mezi zařízeními na 2. vrstvě referenčního modelu, přestože mezi nimi existuje spojení pouze na 3. vrstvě
LAN	Local Area Network - počítačová síť, která je na menším omezeném území, podle velikosti organizace a jejich jednotek může jít o síť v kanceálři, patře nebo budově
MAC	Medium Access Control - sada pravidel pro komunikaci mezi jednotlivými zařízeními v jednom segmentu sítě
MDF	Main Distribution Frame - hlavní centrální rozvodna strukturované kabeláže (obvykle v rámci budovy), obsahuje centrální síťové prvky a zajišťuje připojení k dalším částem organizace, k internetu apod.
MSTP	Multiple Spanning Tree Protocol - rozšíření protokolu STP tak, aby umožňoval vypočítávání síťové topologie pro několik virtuálních sítí najednou, tím může dojít k výraznému snížení zátěže procesoru jednotlivých přepínačů
NTP	Network Time Protocol - protokol pro synchronizaci času na jednotlivých zařízeních v počítačové síti
OS	Operační systém - základní programové vybavení počítače, řídí spouštění a správu jednotivých programů, poskytuje funkce pro přístup k hardwaru, obsahuje správu paměti
OSI	Open System Interconnection - snaha o zavedení obecně platných pravidel (nezávislých na výrobcích) pro komunikaci v počítačových sítích
OSPF	Open Shortest Path First - smerovací protokol, používaný většinou v rámci autonomního systému nebo organizace, upravuje dynamicky směrovací údaje na základě dostupnosti jednotlivých zařízení nebo částí sítě
PC	Personal Computer - osobní počítač, kterým se obvykle rozumí pracovní koncová stanice, u níž sedí jeden člověk

RFC	Request For Comments - označení dokumentů, které se snaží o standardizaci protokolů většinou používaných v počítačových sítích nebo programech, tyto dokumenty nejsou závazné, ale obecně bývají jednotlivými výrobci respektované
SNMP	Simple Network Management Protocol - protokol, který slouží především pro periodický sběr dat ze zařízení, která jsou připojena k počítačové síti
SSH	Secure Shell - šifrovaný komunikační kanál, který umožňuje uživateli připojit se k jinému zařízení připojenému v počítačové síti
STP	Spanning Tree Protocol - protokol, který se využívá na 2. vrstvě referenčního modelu OSI k detekci a přerušení smyček, které mohou v této komunikační vrstvě vzniknout a tím způsobit problémy
TACACS+	Terminal Access Controller Access-Control System Plus - software poskytující detailní informace pro autentizaci uživatelů a autorizaci jejich činností
URL	Uniform Resource Locator - standardizovaný popis umístění souboru na vzdáleném serveru, obsahuje přenosový prokol, název serveru, autentizační a další údaje
VLAN	Virtual Local Area Network - logická síť existující uvnitř fyzické topologie sítě
VTP	VLAN Trunking Protocol - protokol, který distribuje seznam virtuálních sítí (převážně jejich jména a čísla) mezi jednotlivými přepínači v počítačové síti

Seznam použité literatury

[1] PETERKA, Jiří. Archiv článků a přednášek Jiřího Peterky [online]. 1. 2. 1999 [cit. 2010-05-06]. *Referenční model ISO/OSI*. Dostupné z WWW: <http://www.earchiv.cz/anovinky/ai1552.php3>.

[2] REKHTER, Y,, et al. *Internet FAQ Archives* [online]. February 1996 [cit. 2010-05-06]. RFC1918 - Address Allocation for Private Internets. Dostupné z WWW: <http://www.faqs.org/rfcs/rfc1918.html>.

[3] NACHREINER, Corey. *Anatomy of an ARP Poisoning Attack* [online]. WatchGuard Technologies, Inc., c1996-2010 [cit. 2010-05-06]. Dostupné z WWW: <http://www.watchguard.com/infocenter/editorial/135324.asp>.

[4] DEGU, Christian; BASTIEN, Greg; NASSEH, Sara. *Informit* [online]. Jul 7, 2006 [cit. 2010-05-06]. CCSP SNRS Exam Self-Study: Mitigating Layer 2 Attacks. Dostupné z WWW: <http://informit.com/articles/article.aspx?p=474239&seqNum=2>.

[5] CONVERY, Sean. *Hacking Layer 2 : Fun with Ethernet Switches* [online]. San Francisco. [s.l.] : Cisco Systems, Inc., 2002 [cit. 2010-05-06]. Dostupné z WWW: <http://blackhat.com/presentations/bh-usa-02/bh-us-02-convery-switches.pdf>.

[6] *Ettercap* [online]. 28 Jul 2004 [cit. 2010-05-06]. How Port Stealing Works. Dostupné z WWW: <http://ettercap.sourceforge.net/forum/viewtopic.php?t=2329>.

[7] Cisco Systems, Inc. *Cisco Catalyst 3500 XL Series Switches* [online]. c1992-2010 [cit. 2010-05-06]. EOS/EOL Announcement for the Cisco Catalyst 3508G XL Switch and Cisco IOS Software 12.0WC. Dostupné z WWW: <http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps637/prod_end-of-life_notice0900aecd8021a948.html>.

[8] Cisco Systems, Inc. *Cisco Catalyst 3550 Series Switches* [online]. c1992-2010 [cit. 2010-05-06]. EOS/EOL Announcement Cisco Catalyst 3550 Series Switches. Dostupné z WWW: <http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps646/prod_end-of-life_notice0900aecd8029f777.html>.

[9] Cisco Systems, Inc. *Cisco Catalyst 2950 Series Switches* [online]. c1992-2010 [cit. 2010-05-06]. EOS and EOL Announcement of Five Additional Cisco Catalyst 2950 Series Switches . Dostupné z WWW: <http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps628/prod_end-of-life_notice0900aecd806ea1da.html>.

[10] Cisco Systems, Inc. *Cisco Dcumentation* [online]. c1989-1997 [cit. 2010-05-06]. Understanding Spanning-Tree Protocol. Dostupné z WWW: <http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/sw_ntman/cwsimain/cwsi2/cwsiug2/vlan2/stpapp.htm>.

[11] Cisco Systems, Inc. *Catalyst 3560 Switch Software Configuration Guide* [online]. San Francisco : Cisco Systems, Inc., c1992-2010 [cit. 2010-05-06]. Dostupné z WWW: <http://www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/12.2_20_se/configuration/guide/3560scg.html>.

[12] LI, T., et al. *Internet FAQ Archives* [online]. March 1998 [cit. 2010-05-07]. RFC2281 - Cisco Hot Standby Router Protocol (HSRP). Dostupné z WWW: <http://www.faqs.org/rfcs/rfc2281.html>.

[13] Gough, Clare. *CCNP BSCI : Exam Certification Guide*. Third Edition. Indianapolis, USA : Cisco Press, 2004. 882 s. ISBN 1-58720-085-6.

[14] Cisco Systems, Inc. *IP Routing* [online]. Aug 23, 2005 [cit. 2010-05-07]. Sample Configuration for Authentication in OSPF. Dostupné z WWW: <http://www.cisco.com/en/US/tech/tk365/technologies_configuration_example09186a0080094069.shtml>.

[15] GRYGÁREK, Petr. Směrovací protokol OSPF [online]. 2004 [cit. 2010-05-07]. Dostupné z WWW: <http://www.cs.vsb.cz/grygarek/SPS/lect/OSPF/ospf.html>.

[16] DROMS, R. *Internet FAQ Archives* [online]. March 1997 [cit. 2010-05-07]. RFC2131 - Dynamic Host Configuration Protocol. Dostupné z WWW: <http://www.faqs.org/rfcs/rfc2131.html>.

[17] ALEXANDER, S.; DROMS, R. *Internet FAQ Archives* [online]. October 1993 [cit. 2010-05-07]. RFC1533 - DHCP Options and BOOTP Vendor Extensions. Dostupné z WWW: <http://www.faqs.org/rfcs/rfc1533.html>.

[18] HENLEIN, Paul. *Failover with ISC DHCP* [online]. November 6, 2005, Most recent revision: April 11, 2008 [cit. 2010-05-07]. Dostupné z WWW: <http://www.madboa.com/geek/dhcp-failover/>.

[19] JAROTEK, Vladimír. *Pokročilé možnosti DHCP serveru v Cisco IOS* [online]. 2009 [cit. 2010-05-07]. Dostupné z WWW: <http://wh.cs.vsb.cz/sps/images/4/43/DHCP-IOS-Jarotek.pdf>.

[20] Internet Systems Consortium, Inc. *BIND 9 Administrator Reference Manual* [online]. 2004 [cit. 2010-05-07]. Advanced DNS Features. Dostupné z WWW: <http://www.bind9.net/manual/bind/9.3.1/Bv9ARM.ch04.html>.

[21] BOUŠKA, Petr. *Cisco IOS 7 - konfigurace VLAN, VTP* [online]. 18. 06. 2007, Upraveno 23. 04. 2009 [cit. 2010-05-07]. Dostupné z WWW: <http://www.samuraj-cz.com/clanek/cisco-ios-7-konfigurace-vlan-vtp/>.

[22] Cisco Systems, Inc. *Catalyst 6500 Series Software Configuration Guide* [online]. 8.7. c1992-2010 [cit. 2010-05-07]. Configuring VTP. Dostupné z WWW: <http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/catos/8.x/configuration/guide/vtp.html>.

[23] CÍSAŘ, Tomáš. *Bezpečnost LAN, způsoby ověřování identity* [online]. 30 Nov 2009 [cit. 2010-05-07]. Dostupné z WWW: <http://www.alefnula.cz/downloads/KC/KC-identita.pdf>.

[24] GURECKÝ, Petr. *DHCP snooping* [online]. Ostrava : Vysoká škola báňská - Technická univerzita Ostrava, 2006. 9 s. Semestrální práce. Dostupné z WWW: <http://www.cs.vsb.cz/grygarek/SPS/projekty0506/DHCPsnooping.pdf>.

[25] Cisco Systems, Inc. *HSRP MD5 Authentication* [online]. c1992-2010 [cit. 2010-05-07]. Dostupné z WWW: <http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gthsrpau.html>.

[26] Cisco Systems, Inc. *Sample Configuration for Authentication in OSPF* [online]. c1992-2010 [cit. 2010-05-07]. Dostupné z WWW: <http://www.cisco.com/en/US/tech/tk365/technologies_configuration_example09186a0080094069.shtml>.

[27] THOMAS, Rob. *Secure BIND Template* [online]. Version 7.1. 14 May 2009 [cit. 2010-05-19]. Dostupné z WWW: <http://www.cymru.com/Documents/secure-bind-template.html>.

[28] Cisco Systems, Inc. *Linux Certif* [online]. 1 August 2006 (mandriva - 22/10/07). 2006 [cit. 2010-05-19]. Man tac_plus.conf. Dostupné z WWW: <http://www.linuxcertif.com/man/5/tac_plus.conf/>.

[29] OLIVIEIRA, Jose Pedro. *Linux man page* [online]. c1999-2004 [cit. 2010-05-19]. Syslog-ng config file. Dostupné z WWW: <http://linux.die.net/man/5/syslog-ng.conf>.

[30] *Net-SNMP Wiki* [online]. 2009, Last modified 13:22, 24 February 2009 [cit. 2010-05-19]. TUT:snmptrap SNMPv3. Dostupné z WWW: <http://www.net-snmp.org/wiki/index.php/TUT:snmptrap_SNMPv3>.

[31] *Net-SNMP Wiki* [online]. 2010, Last modified 06:51, 29 April 2010 [cit. 2010-05-19]. TUT:Configuring snmptrapd. Dostupné z WWW: <http://www.net-snmp.org/wiki/index.php/TUT:Configuring_snmptrapd>.

[32] WIRZENIUS, Lars, et al. *Linux System Administrators Guide* [online]. Version 0.9. 2005 [cit. 2010-05-19]. Basic NTP configuration. Dostupné z WWW: <http://tldp.org/LDP/sag/html/basic-ntp-config.html>.

[33] Cisco Systems, Inc. *SNMPv3* [online]. c1992-2010 [cit. 2010-05-19]. Dostupné z WWW: <http://www.cisco.com/en/US/docs/ios/12_0t/12_0t3/feature/guide/Snmp3.html>.

[34] MAURO, Douglas R.; SMITH, Kevin J. *Essential SNMP* [online]. First edition. Sebastopol, USA : O'Reilly & Associates, 2001 [cit. 2010-05-19]. Configuring SNMPv3. Dostupné z WWW: <http://docstore.mik.ua/orelly/networking_2ndEd/snmp/appf_02.htm>. ISBN 0-596-00020-0.

[35] Cisco Systems, Inc. *VLAN Security White Paper* [online]. c1992-2010 [cit. 2010-05-21]. Dostupné z WWW: <http://scc.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml>.

[36] Hucaby, David. *CCNP BCMSN : Exam Certification Guide*. Third Edition. Indianapolis, USA : Cisco Press, 2006. 586 s. ISBN 1-58720-142-9.

[37] Cisco Systems, Inc. *Catalyst 2960 and 2960-S Software Configuration Guide, 12.2(53)SE1* [online]. c1992-2010 [cit. 2010-05-25]. Dostupné z WWW: <http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_53_se/configuration/guide/2960scg.html>.

Seznam příloh

1. CD s textem DP a s konfiguracemi zařízení `Cisco`, které byly použity při simulaci zapojení nově navrhované struktury sítě