Inovace automatizovaného systému pro správu datových přípojek na VŠ kolejích UTB a jeho integrace se systémem FlowMon

Innovation of an automatic system for management of network connections in the student dormitory of the TBU and integration with FlowMon system

Bc. Petr Skovajsa

Diplomová práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2010/2011

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

Jméno a příjmení:	**Bc. Petr SKOVAJSA**
Osobní číslo:	**A09519**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Téma práce:	**Inovace automatizovaného systému pro správu datových přípojek na VŠ kolejích UTB a jeho integrace se systémem Flowmon**

Zásady pro vypracování:

1. **Zpracujte literární rešerši na dané téma.**
2. **Inovujte Vámi vytvořený automatizovaný systém pro správu datových přípojek na pokojích studentů VŠ kolejí UTB Zlín.**
3. **Změňte strukturu databáze dle požadavků Správy KMZ o možnost přidělení Internetové přípojky zaměstnancům UTB ubytovaným na kolejích včetně hotelových hostů.**
4. **Integrujte Váš systém se síťovým systémem Flowmon.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **DOOLEY, Kevin – BROWN, Ian J. Cisco IOS Cookbook. 2. vyd. Sebastopol: OREILLY, 2006. 1207 s. ISBN 978-0-596-52722-8.**
2. **CONOLLY, Thomas – BEGG, Carolyn – HOLOWCZAK, Richard. Databáze – Profesionální průvodce tvorbou efektivních databází. 1. vyd. Brno: Computer Press, 2009. 584 s. ISBN 978-80-251-2328-7.**
3. **KRETCHMAR, James – DOSTÁLEK, Libor – VESELSKÝ, Jiří. Administrace a diagnostika sítí – pomocí OpenSource utilit a nástrojů. 1. vyd. Brno: Computer Press, 2004. 216 s. ISBN 978-80-251-0345-5.**
4. **RAINES, Paul. Tcl/Tk pocket reference. 1. vyd. Sebastopol: OREILLY, 1998. 90 s. ISBN 1-56592-498-3.**
5. **DOSTÁLEK, Libor – KABELOVÁ, Alena. Velký průvodce protokoly TCP/IP a systémem DNS. 1. vyd. Praha: Computer Press, 2000. 426 s. ISBN 978-80-7226-323-4.**
6. **MATOUŠOVÁ, Miroslava – HEJLÍK, Ladislav. Osobní údaje a jejich ochrana. 2. vyd. Praha: ASPI, 2008. 468 s. ISBN 978-80-7357-322-5.**
7. **SHAH, Steve – SOYINKA, Wale. Administrace systému LINUX – překlad čtvrtého vydání. 1. vyd. Praha: Grada Publishing, 2007. 428 s. ISBN 978-80-247-1694-7.**
8. **Dokumentace systému 602SQL [online]. [cit. 2010-02-04]. URL: [http://www.602.cz/datainc/winbase/wb81/napoveda].**

Vedoucí diplomové práce: **Ing. Miroslav Matýsek, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání diplomové práce: **24. února 2011**

Termín odevzdání diplomové práce: **18. května 2011**

Ve Zlíně dne 24. února 2011

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Roman Jašek, Ph.D.
ředitel ústavu

ABSTRAKT

Práce popisuje inovaci a rozšíření automatizovaného systému pro správu datových přípojek. Teoretická část popisuje problematiku ubytování a pravidel datové sítě na VŠ kolejích UTB, využití monitorovacího systému FlowMon na datové síti UTB ve Zlíně. V praktické části je řešena inovace stávajícího systému, rozšíření o možnost správy datových přípojek pro ubytované zaměstnance a pro hotelové hosty, inovace databáze, SQL procedur a uživatelského rozhraní pro ubytovatele a www rozhraní pro klienta. Popsán je způsob propojení systému ASDP s ubytovacím programem AT-Koleje, řešeno je vzájemné propojení systému ASDP se systémem FlowMon a způsob řízení rychlosti datových přípojek v závislosti na počtu přenesených dat.

Klíčová slova: správa datových přípojek, AT-Koleje, FlowMon, 602SQL, Cisco, jednoduchý traffic shaping, NFSEN.

ABSTRACT

This work describes the improvement and extension of an automatic system for data connection management. The theoretical part describes the problem of accommodation and the rules of the data network at the dormitory of Tomas Bata University in Zlin (TBU), and the use of the FlowMon monitoring system. The practical part deals with the update of the current system, the extensions allowing the management of data connection for employees and hotel guests, update of the database and SQL stored procedures, as well as the user interface used by the quartermaster, and the web interface targeted at the clients. The method for integration of the ASDP system and the dormitory accommodation system AT-Koleje is described, together with the means of interfacing the ASDP system and the FlowMon software. The method of controlling the data point speed based on the data transferred is outlined as well.

Keywords: network connections management, AT-Koleje, FlowMon, 602SQL, Cisco, simple traffic shaping, NFSEN.

Rád bych poděkoval svému vedoucímu práce Ing. Miroslavu Matýskovi, Ph.D. za odborné vedení a konzultace při zpracování této diplomové práce. Dále bych chtěl poděkovat Miroslavu Janišovi a Ing. Petru Vojtkovi za rady a připomínky a také Ing. Josefu Zelovi za možnost realizace této práce na VŠ kolejích Univerzity Tomáše Bati ve Zlíně.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské 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/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou 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/bakalářskou 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/bakalářské 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/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské 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 diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Vysokoškolské koleje Univerzity Tomáše Bati ve Zlíně jsou ubytovacím zařízením pro studenty, zaměstnance UTB a hotelové hosty. Hlavní provozní činností je ubytování studentů v období od září do června, doplňkovou (vedlejší) činností je poskytování hotelového ubytování v období letních měsíců července a srpna.

Mezi služby, které VŠ koleje poskytují ubytovaným studentům, patří zejména připojení ke kolejní datové síti a Internetu. Správa této rozsáhlé sítě vyžaduje nemalé pracovní úsilí, proto byl v rámci bakalářské práce vytvořen automatizovaný systém pro správu datových přípojek (ASDP). Tento systém umožňuje studentovi aktivovat datovou přípojku ze svého počítače přímo na pokoji kde je ubytován, případně odkudkoliv z Internetu. Administrátorovi sítě poskytuje bezobslužnou konfiguraci aktivních prvků sítě a ubytovateli nabízí propojení s programem pro správu a rezervaci ubytování.

Vznik této diplomové práce byl iniciován dalšími požadavky o rozšíření, vylepšení a inovaci stávajícího systému. V organizaci jako jsou VŠ koleje je kladen důraz zejména na služby pro ubytování studentů, na vedlejší činnost by se však mohlo snadno zapomenout, přestože tvoří téměř čtvrtinu ročního provozu a nabízí významné zvýšení příjmů. Jedná se nejen o ubytování zaměstnanců, ale také o hotelové ubytování. Hotelový host si vybírá ubytování dle ceny, poskytovaných služeb, umístění hotelu apod. Jednou z běžně poskytovaných služeb je právě připojení k Internetu. Hotely bez takového připojení jsou v konkurenční nevýhodě. VŠ koleje mohou díky stávající infrastruktuře datové sítě nabídnout hotelovým hostům kabelové připojení k Internetu přímo na pokoji a to pouze s minimální investicí. Proto jedním z úkolů této práce je návrh a realizace připojení k Internetu pro hotelové hosty.

Hlavním úkolem je inovace a vytvoření komplexního automatizovaného systému pro správu datových přípojek ubytovaných studentů, zaměstnanců a hotelových hostů v podmínkách VŠ kolejí UTB ve Zlíně. Důležitou částí je napojení na databázi ubytovacího programu AT-Koleje, ze které jsou získávány zejména ubytovací data, tj. informace o klientech, jejich ubytování, účtování, pokojích apod. Nezbytná je úprava databáze, SQL procedur systému ASDP, klientských formulářů pro ovládání a správu systému. Inovací by měl projít také automatizovaný způsob správy účetního předpisu v návaznosti na změny ve struktuře systému.

Systém KOLEJE ON-LINE, který je současně webovým rozhraním programu AT-Koleje a automatizovaného systému pro správu datových přípojek, musí umět obsloužit nejen studenty, ale i ubytované zaměstnance a v případě potřeby také hotelové hosty. Klientům by měl nabídnout vylepšené rozhraní pro aktivaci a deaktivaci datové přípojky a také přehled či statistiku přenesených dat.

Samotnou realizaci připojení hotelových hostů by měla předcházet analýza hotelového ubytování na VŠ kolejích UTB a návrh možností, jak takové připojení realizovat, včetně technického řešení a jeho návaznost na systém ASDP.

Dále je požadována integrace se síťovým monitorovacím systémem FlowMon. Integrace by měla spočívat ve využití dat z databáze systému ASDP pro systém FlowMon, což by mělo uspořit čas při dohledávání konkrétních původců různých bezpečnostních incidentů. Naopak ze systému FlowMon by měly být získávány statistiky o počtu přenesených dat pro systém ASDP. Tyto statistiky poslouží také k řízení rychlosti datových přípojek.

I. TEORETICKÁ ČÁST

1 VŠ KOLEJE UTB, DATOVÁ SÍŤ A INTERNET

1.1 Ubytování na VŠ kolejích UTB

VŠ koleje UTB ve Zlíně zajišťují ubytování pro dojíždějící studenty ve třech budovách s různou kategorií ubytování. Na VŠ koleji Štefánikova je ubytování poskytováno ve dvojlůžkových pokojích se společným sociálním zařízením na patře. Na VŠ koleji Antonínova je poskytováno ubytování v jednolůžkových, dvojlůžkových a třílůžkových pokojích, které jsou součástí ubytovací buňky se sociálním zařízením a kuchyňkou. VŠ kolej nám. T. G. Masaryka (dále jen TGM) nabízí ubytování ve dvojlůžkových pokojích, které jsou součástí ubytovací buňky se sociálním zařízením a kuchyňkou. Současná ubytovací kapacita je 858 lůžek pro studenty a hotelové hosty, 38 lůžek pro zaměstnance UTB a 2 lůžka pro imobilní osoby.

Ubytování studentů UTB je hlavní provozní činnost VŠ kolejí v období zimního a letního semestru příslušného akademického roku a to v největší míře od poloviny září do poloviny června. Vedlejší činností je pak hotelové ubytování, které je poskytováno od poloviny června do poloviny září hotelovým hostům. Celoroční činností je poskytování ubytování zaměstnancům a akademickým pracovníkům jednotlivých fakult UTB [13].

Klientem VŠ kolejí se rozumí student, hotelový host a ubytovaný zaměstnanec UTB.

1.2 Datové přípojky na pokojích VŠ kolejí

Datová přípojka je v současnosti běžnou součástí ubytování. Pod pojmem datová přípojka se rozumí označená zásuvka typu RJ-45 na pokoji, která je propojena na nějaký konkrétní port konkrétního přepínače v datovém rozvaděči budovy. Konfigurace portů probíhá prostřednictvím automatizovaného systému pro správu datových přípojek [10]. Připojení ubytovaných zaměstnanců UTB a hotelových hostů k datové síti na VŠ kolejích bude řešeno v rámci této diplomové práce z hlediska technického i metodického v souladu s pravidly sítě CESNET2 (Czech Education and Scientific NETwork 2).

Na VŠ koleji Štefánikova a TGM jsou instalovány datové zásuvky pro každé lůžkové místo, na VŠ koleji Antonínova je jedna datová zásuvka v jednolůžkovém a dvojlůžkovém pokoji a dvojzásuvka ve trojlůžkovém pokoji.

2 AUTOMATIZOVANÁ SPRÁVA DATOVÝCH PŘÍPOJEK

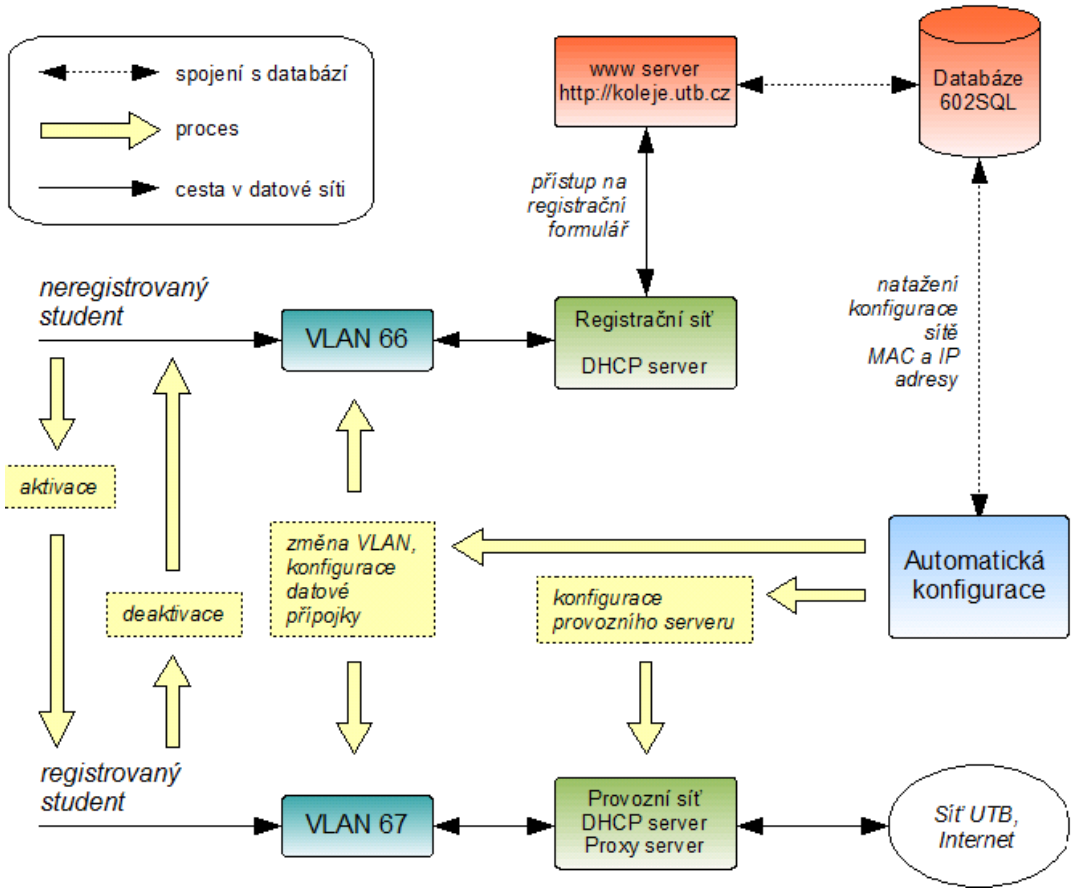
2.1 Systém ASDP – současný stav

V této kapitole je popsána funkce systému pro automatizovanou správu datových přípojek na VŠ kolejích. Systém byl výsledným produktem bakalářské práce [10].

Systém ASDP se skládá ze skriptů, které konfigurují prostřednictvím jazyka EXPECT a protokolu SSH (Secure SHell) síťové přepínače Cisco Catalyst. Programovací jazyk EXPECT umožňuje automatizovat ručně zadávané příkazy prostřednictvím CLI (Command Line Interface) při správě aktivních prvků. Konfigurace spočívá v nastavení provozní sítě VLAN (Virtual Local Area Network) na port přepínače a nastavení omezení přístupu do sítě pouze ze zaregistrované MAC (Media Access Control) adresy a nastavení dalších parametrů jako rychlost portu, maximální počet MAC adres na portu apod. Rozlišuje se registrační a provozní VLAN studentské sítě. Na registrační VLAN je datový provoz omezen a je povoleno pouze zobrazení webového registračního formuláře systému KOLEJE ON-LINE.

Systém ASDP obsahuje skripty, které získávají konfigurační data z databáze 602SQL (Structured Query Language) a do databáze vrací údaje o provedených akcích. Skripty konfigurují také příslušný DHCP (Dynamic Host Configuration Protocol) server a firewall PROXY serveru. Pro DHCP server se spravuje seznam aktivních IP (Internet Protocol) adres přiřazený k příslušným MAC adresám registrovaných počítačů v síti. Firewall se nastavuje prostřednictvím konfiguračních souborů aplikace Shorewall, povolen je provoz pouze aktivovaným IP adresám.

Databáze 602SQL je propojena přímo s ubytovacím software AT-Koleje. Systém ASDP je dále složen z webového rozhraní pro studenty. To umožňuje aktivaci a deaktivaci datové přípojky přímo na pokoji, kde je student ubytován, či kde má rezervováno ubytování. Webové rozhraní je součástí systému KOLEJE ON-LINE, který umožňuje elektronickou správu služeb ubytování pro studenty. Do systému ASDP je dále zahrnuto klientské rozhraní 602SQL pro ubytovatele. Pomocí takového rozhraní může ubytovatel pozastavit přípojku z různých důvodů, např. prodlení platby či porušení pravidel datové sítě. Další podrobné informace k systému ASDP jsou k nalezení v bakalářské práci [10].



Obr. 1. Schéma systému ASDP – současný stav, schéma z [10]

2.2 Systém ASDP – navrhovaný stav

Zde jsou shrnuty bodově nejdůležitější požadavky na inovaci systému ASDP. S inovací souvisí také metodické řešení souvisejících procesů.

- Připojení k Internetu pro hotelové hosty v souladu s pravidly sítě CESNET2.
- Připojení k Internetu pro ubytované zaměstnance UTB.
- Rezervace IP adres (zamezit časté střídání IP adres).
- Návrh a vytvoření uživatelského rozhraní pro ubytovatele.
- Tvorba a inovace procedur pro správu účetního předpisu.
- Získávání statistik přenesených dat z monitorovacího systému FlowMon.
- Stanovení pravidel a datových limitů v síti.
- Odesílat informační email při překročení datových limitů.
- Řízení rychlosti datové přípojky v závislosti na překročení datového limitu.
- Zobrazovat v systému FlowMon detaily IP adres použitých v systému ASDP.

Návrhem a zároveň cílem této diplomové práce je rozšíření stávajícího systému ASDP o možnost automatizované správy datových přípojek pro zaměstnance ubytované na VŠ kolejích a pro hotelové hosty. S tím souvisí také vytvoření uživatelského rozhraní pro ubytovatele. Jelikož došlo k úpravě ubytovacího programu AT-Koleje, je třeba stávající systém také upravit o správu účetního předpisu

Dalším rozšířením systému ASDP je propojení se systémem FlowMon. FlowMon slouží k monitoringu datové sítě UTB. Propojení obou systémů bude spočívat v získávání statistik o přeneseném objemu dat mimo univerzitní síť a zobrazování těchto a dalších statistických údajů v systému KOLEJE ON-LINE. Dále v případě porušení pravidel datové sítě systém ASDP umožní odeslání automatického varování konkrétnímu uživateli, či přímo automaticky nastaví rychlost datové přípojky.

Systém FlowMon a jeho modul NFSEN by měl být obohacen o údaje z databáze systému ASDP, konkrétně o jméno, číslo přípojky a pokoje, koleje a dalších relevantních údajů, které by v případě incidentu měly sloužit centrálnímu správci sítě UTB.

2.2.1 Připojení zaměstnanců UTB k síti Internet na VŠ koleji

Zaměstnanci UTB mají přístup k univerzitní síti umožněn na základě směrnice rektora č. 23/2002 - Pravidla provozu počítačové sítě Univerzity Tomáše Bati ve Zlíně. V současné době jsou zaměstnancům ubytovaným na VŠ koleji přidělovány veřejné IP adresy. Přidělený adresní rozsah nedostačuje počtu připojených uživatelů. V plánu je zavedení neveřejných IP adres a zařazení do systému ASDP, což bude řešeno v praktické části této diplomové práce v kapitole 7.9.

2.2.2 Připojení hotelových hostů k síti Internet

Datová síť VŠ kolejí je připojena k univerzitní síti UTB, která je připojena do sítě CESNET2. Zásady pro přístup do této sítě [14] neumožňují poskytovat internetové připojení třetím stranám, pokud se nejedná o vědu, výzkum a činnosti s tím spojené. Proto je vhodné řešit připojení hotelových hostů obdobně jako v hotelových provozech, tj. externím poskytovatelem internetového připojení (dále jen ISP – Internet Service Provider). Takové datové připojení lze následně poskytovat hotelovým hostům a to buď zdarma v rámci ceny ubytování (zvýšení konkurenceschopnosti a z toho vyplývající vyšší počet hotelových hostů), nebo za samostatně účtovaný poplatek (což s sebou však přináší navýšení administrativních úkonů, zvýšení nákladů a požadavků na systém).

Současný stav umožňuje využití stávajících datových rozvodů a automatizovaného systému pro aktivaci datových přípojek. Variantou pro hotelový Internet může být také bezdrátová WiFi síť. Na VŠ kolejích UTB však taková síť není provozována a její zavedení na všech budovách by vyžadovala nákup a instalaci dalších zařízení.

Hotelový provoz probíhá na VŠ kolejích v průběhu letních prázdnin. V menší míře na volných pokojích v přízemí VŠ koleje Štefánikova i v průběhu akademického roku. Jako doplňková služba ke kabelovému připojení by v těchto místech mohlo být bezdrátové připojení WiFi v budoucnu zavedeno.

Připojení hotelového hosta musí být co nejjednodušší. Jsou navrhovány tyto varianty.

A. Umožnit obsluze na recepci aktivaci Internetu pro konkrétního hotelového hosta (ať už by bylo připojení realizováno bezdrátově nebo pomocí kabelu).
B. Pokoje by měly pro hosty aktivováno připojení k Internetu již od momentu svého zařazení do hotelového provozu.

Stanovení způsobu připojení hotelového hosta k Internetu je popsáno v kapitole 8.2.

Hotelový host by měl mít k dispozici podrobný a velmi jednoduchý návod k aktivaci nebo k připojení k Internetu.

Problematika, která z připojení hotelových hostů vyplývá, je servis a technická podpora. Ta může být poskytována pouze v pracovní dobu technických pracovníků, ta je však odlišná od doby, kdy hosté přicházejí na pokoj a připojují svůj počítač k datové síti. Při variantě, kdy by byl (např. v budoucnu) za Internet hotelových hostů účtován speciální poplatek, měla by být vyřešena také technická podpora a to v období letních prázdnin, kdy jsou VŠ koleje využívány zejména pro hotelové ubytování.

2.2.3 Požadavky na externího ISP

Pro datovou síť hotelového provozu je dostačujícím standardem připojení k Internetu o rychlosti do 10 Mbit/s a veřejná IP adresa. Datové připojení by mělo být spolehlivé. Vzhledem ke vzájemnému propojení všech budov UTB optickými kabely je možné připojit k síti externího ISP kteroukoliv univerzitní budovu, tj. nejlépe tam, kde by byla možnost zřízení přípojky nejméně nákladná. V případě připojení vlastní budovy lze totiž jednoduše toto připojení přesměrovat na příslušné budovy VŠ kolejí UTB.

3 PRAVIDLA DATOVÉ SÍTĚ NA VŠ KOLEJÍCH UTB

Dodržování pravidel je plně v zodpovědnosti uživatele na základě uzavřené smlouvy o aktivaci datové přípojky, na základě směrnice rektora č. 23/2002 – Pravidla provozu počítačové sítě Univerzity Tomáše Bati ve Zlíně a směrnice kvestora č. 6/2002 – Pravidla provozu počítačové sítě na kolejích UTB ve Zlíně.

K datové zásuvce je povoleno připojit pouze osobní počítač nebo notebook, připojování jiných zařízení do sítě je zakázáno. Jeden uživatel může registrovat 1 datovou přípojku na 1 MAC adresu, které je přidělena 1 IP adresa. Výjimky jsou možné.

Datová síť na VŠ kolejích UTB se podílí čtvrtinovým podílem na objemu stažených dat (download) a osminovým podílem na objemu odeslaných dat (upload) z celé univerzitní sítě. Bylo rozhodnuto, že bude zpracován přehled, zda a jaké datové limity mají na VŠ kolejích ostatní VVŠ (Veřejné Vysoké Školy) v ČR. Tento přehled poslouží jako výchozí materiál k rozhodnutí, jak se postavit k případným datovým limitům na datové síti VŠ kolejí UTB ve Zlíně.

Přenosová rychlost datových přípojek na VŠ kolejích je 100 Mbit/s download i upload a nebyla doposud omezena ani na přepínačích, ani na PROXY serveru datové sítě VŠ kolejí UTB.

3.1 Přehled pravidel na ostatních VŠ kolejích v ČR

Tabulka s přehledem obsahuje následující údaje:

- název VŠ případně i kolej
- sledované období
- zda jsou sledovány vnitřní a vnější datové přenosy samostatně
- maximální povolený upload a download
- způsob blokace – odpojením nebo snížením přenosové rychlosti apod. na období

Údaje byly získány z webových stránek příslušných VVŠ a VŠ kolejí v týdnu od 7. – 13. 3. 2011 a v ostatních případech, kdy nebyly údaje dohledatelné, byly získány emailovým dotazem. Tam, kde nebyla získána odpověď ani emailovým dotazem, je uvedeno „nenalezeno“.

Tab. 1. Přehled pravidel datových sítí a datových limitů na ostatních VŠ kolejích v ČR

VVŠ nebo VŠ kolej	sledované období	vnější nebo vnitřní dat. provoz	max. povolený upload	max. povolený download	max. UL+DL	způsob blokace při překročení limitu
Masarykova univerzita, Brno	1den (00:00 až 23:59 hod)	vnější	-	-	3 GB	zbytek dne + následující 3 celé dny
Vysoké učení technické v Brně	4 dny	vnější	4 GB	-	-	na 2 po sobě následující dny, pak se sleduje 30 dnů
	30 dnů	vnější	30 GB	upozornění na nadměrný	-	po celou dobu kdy předchozích 30 dnů překračuje maximum
Univerzita Palackého v Olomouci	7 dní (od pondělí 00:00 do neděle 23:59)	vnější	5 GB	-	-	při překročení kvóty 5 GB odpojen od sítě Internet
Karlova Univerzita, Praha, kolej 17. Listopadu	průběžný týden (plovoucí součet za uplynulých 168 hodin)	vnější	5 GB	-	-	odpojení po dobu překročení plovoucího součtu za sledované období
Univerzita Jana Evangelisty Purkyně v Ústí nad Labem	-	-	neomezeno	neomezeno	neomezeno	-
Univerzita Hradec Králové	-	-	neomezeno	neomezeno	neomezeno	-
Západočeská univerzita v Plzni	nenalezeno					
Vysoká škola báňská Technická univerzita Ostrava	24 hodin	-	-	-	sledováno	email s vysvětlením, upozornění
Vysoká škola ekonomická v Praze	nezjištěno	nezjištěno	-	-	sledováno	blokování 8hodin až 3 dny
Univerzita Pardubice	-	-	neomezeno	neomezeno	neomezeno	-
Mendelova zemědělská a lesnická univerzita v Brně	posledních 7 dní	vnější	-	-	20 GB	odpojení od sítě Internet po dobu 14 dnů
Ostravská univerzita v Ostravě	měsíc	vnější i vnitřní	10 GB	30 GB	-	výrazné snížení rychlosti
ČVUT v Praze, kolej Podolí	posledních 30 dní	vnější	2 GB	-	-	omezení odchozích dat na 5Kbit/s
ČVUT v Praze, kolej Sinkuleho	posledních 30 dní	vnější	5 GB	-	-	odpojení na 30 dnů
VŠCHT v Praze	nenalezeno					
Česká zemědělská univerzita v Praze	nenalezeno					
Jihočeská univerzita v Českých Budějovicích	-	-	neomezeno	neomezeno	neomezeno	-
Technická univerzita v Liberci	-	-	neomezeno	neomezeno	neomezeno	-
Slezská univerzita v Opavě, OPF	měsíc	-		-	sledováno	email s upozorněním
JAMU v Brně	nenalezeno					
Veterinární a Farmaceutická univerzita Brno	nenalezeno					

3.2 Stanovení pravidel řízení datové propustnosti

Tab. 1. ukazuje, že v otázce datových limitů na VŠ kolejích v ČR (České republice) není jednotný postoj a reálně být ani nemůže. Každá VŠ kolej totiž nabízí studentům jiné podmínky, jiný způsob datového připojení a v neposlední řadě také jinou cenu za datovou přípojku na pokoji studenta. Nadměrný počet přenesených dat vzniká z různých důvodů, např. problémy se zavirovaným počítačem, využíváním P2P (peer-to-peer) sítí, nerespektování pravidel sítě CESNET2 apod.

Převážná část uživatelů datové sítě VŠ kolejí UTB však využívá datových služeb v souladu se stanovenými pravidly. Uživatelé, u nichž dojde k porušení pravidel vědomě či nevědomě, budou upozorněni automaticky vygenerovaným emailem.

3.2.1 Průměrné hodnoty přenesených dat

Průměrný denní upload z kolejní datové sítě do sítě Internet na připojeného uživatele v kolejní síti je 113 MB/den a download 722 MB/den. Průměrný denní upload TOP 10 nejaktivnějších uživatelů je 2,99 GB/den a download 4,65 GB/den. Součet byl proveden ze statistik za měsíc únor a březen 2011 (59 dní). Do statistik nejsou započítávána data přenesená v rámci datové sítě VŠ kolejí ani v rámci sítě UTB. Statistiky byly zpracovány na základě výstupů monitorovacího systému FlowMon.

Následující návrh pravidel je doporučením a lze upravit dle aktuálních požadavků.

3.2.2 Návrh pravidel pro upload

Sledované období je průběžný den a počítá se součet odeslaných dat za uplynulých 24 hodin pro každou IP adresu (přípojku). Započítává se pouze datový provoz uskutečněný z datové sítě VŠ kolejí do Internetu. Překročí-li počet odeslaných dat 2 GB za sledované období, rychlost připojení do Internetu se sníží na 1 Mbit/s. Rychlost bude snížena po celou dobu, kdy bude limit ve sledovaném období danou IP adresou překročen.

Výjimka z těchto pravidel může být udělena uživatelům vykonávající činnosti v souladu s pravidly sítě CESNET2.

3.2.3 Pravidla pro download

Počet stažených dat není v současné době omezen. Při překročení 20 GB stažených dat za den (od 00:00 – 24:00), bude odeslán email s upozorněním.

4 SYSTÉM FLOWMON NA UTB

4.1 NetFlow

NetFlow je otevřený protokol vyvinutý společností Cisco Systems, určený původně jako doplňková služba ke směrovačům Cisco. Hlavním účelem NetFlow je monitorování síťového provozu na základě IP toků. Tok je v terminologii NetFlow definován jako sekvence paketů se shodnou pěticí údajů: cílová/zdrojová IP adresa, cílový/zdrojový port a číslo protokolu. Pro každý tok je zaznamenávána doba jeho vzniku, délka jeho trvání, počet přenesených paketů a bajtů a další údaje podle verze protokolu NetFlow. V současnosti je hojně využívána verze 5 a verze 9. NetFlow statistiky neobsahují produkční data, takže nehrozí zneužití utajovaných skutečností [12].

4.2 FlowMon

FlowMon tvoří kompletní řešení dodávané společností Invea-Tech a.s. pro monitorování datových sítí na bázi IP toků (NetFlow). Součástí je výkonná autonomní sonda, kolektor a rozšiřující moduly – softwarové pluginy. FlowMon sonda analyzuje každý procházející paket přímo na monitorované datové lince a na základě těchto dat generuje NetFlow statistiky. Tyto statistiky jsou exportovány na NetFlow kolektor, kde jsou uloženy a připraveny k vizualizaci a analýzu administrátorem sítě pomocí aplikace FlowMon monitorovací centrum. Pomocí rozšiřujících modulů lze na kolektoru provádět pokročilejší analýzy NetFlow statistik.

FlowMon umožňuje zejména monitorování provozu na síti v reálném čase, odhalení vnějších a vnitřních útoků a rozpoznání anomálií jako jsou červi a DDOS (Distributed Denial Of Service) útoky, analýzu dlouhodobých statistik, získávání přehledných výpisů o síťovém provozu [8].

Systém FlowMon byl instalován do sítě UTB v rámci rozvojového projektu v roce 2010. Bude využit mj. pro potřeby získávání statistik pro systém ASDP o počtech přenesených dat z datové sítě VŠ kolejí UTB.

4.3 Sonda FlowMon

Sonda je síťové zařízení určené pro sběr paketů, výpočet statistik o IP tocích a export těchto statistik na FlowMon kolektor ve formátech NetFlow v5/v9. Jedná se o neinvazivní kompaktní zařízení s instalací do stávající síťové infrastruktury pomocí mirror portu

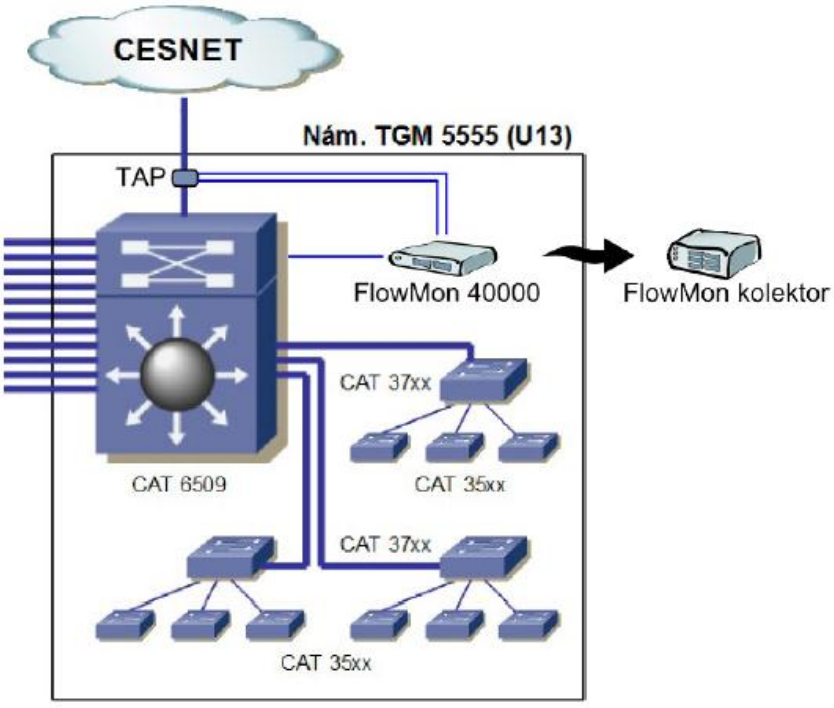
(SPAN port - Switched Port Analyzer) nebo TAPu (optické odbočky pro oba směry in/out). Sondy jsou vybaveny jedním administrativním portem pro vzdálenou konfiguraci a export NetFlow dat a jedním nebo více monitorovacími porty pro sledování sítě (10 M / 100 M / 1 G / 10 G Ethernet).

Obr. 2. Sonda FlowMon

4.4 Zapojení sondy FlowMon na UTB

Sonda nainstalovaná v síti UTB má označení IFP-40000-SFP+ a skládá se ze čtyř monitorovacích portů o rychlosti 10 Gbit/s, z nichž první port je určen pro monitoring komunikace vnitřního provozu, druhý port monitoruje komunikaci ze sítě CESNET2 do sítě UTB (download), třetí port monitoruje komunikaci ze sítě UTB do sítě CESNET2 (upload). Poslední čtvrtý port je volný a je určen pro budoucí potřeby.

Použité porty jsou označeny jako SPAN, UTB-CESNET a CESNET-UTB.



Obr. 3. Schéma zapojení sondy FlowMon na síti UTB

4.5 Kolektor FlowMon

FlowMon kolektor je samostatný server určený pro sběr NetFlow statistik z FlowMon sond a jejich dlouhodobé uchování. Slouží také jako centrální bod pro dohled nad sítí. Kromě sběru a zpracování NetFlow statistik je určen pro vzdálenou konfiguraci FlowMon sond z jednoho místa.

Obr. 4. Kolektor FlowMon

Jako aplikace pro sběr a zpracování NetFlow záznamů je použito aplikace FlowMon Monitoring Center, jehož součástí je balík utilit NFDUMP, který zpracovává získaná data ze sond a grafická nadstavba NFSEN, která umožňuje administrátorům i manažerům přehledně a jednoduše vizualizovat zjištěné statistiky. Pomocí speciálních dotazů lze zobrazit komunikaci mezi konkrétními stanicemi, s využitím dané služby, v určitém časovém rozmezí a mnoho dalších údajů potřebných pro provádění bezpečnostních analýz a dohled nad sítí. Pro efektivnější správu a včasné řešení nastalých problémů lze využít automatické upozorňování na anomální a nežádoucí stavy [3], [11].

4.5.1 Utility NFDUMP

Balík utilit NFDUMP je distribuován pod licencí BSD (Berkeley Software Distribution) a je součástí systému FlowMon.

Utilita **nfcapd** je služba - daemon pro získávání NetFlow dat ze sítě a jejich ukládání do souborů pro pozdější zpracování. Pro každý zdroj NetFlow dat musí běžet samostatný daemon. Jsou-li na UTB 3 zdroje NetFlow dat (SPAN, UTB-CESNET a CESNET-UTB), pak běží tři daemoni. Utilita **nfcapd** zakládá soubor každých 5 minut (v defaultním nastavení). Soubory s daty jsou ukládány v adresářích s přehledně definovanou strukturou. Například pro zdroj SPAN je adresář stanoven jako:

/data/nfsen/profiles-data/live/span/RRRR/MM/DD/nfcapd.RRRRMMDDhhmm

Kde `RRRR` je rok, `MM` je měsíc, `DD` je den, `hh` jsou hodiny a `mm` jsou minuty. Konkrétní cesta k souboru pak může vypadat například takto:

/data/nfsen/profiles-data/live/span/2011/03/15/nfcapd.201103152150

Utilita **nfdump** umožňuje zpracovávat uložená data do statistik (např. TOP N), filtrovat a řadit výsledky podle IP adres, portů, počtu flows, přenesených dat, paketů atd. Je velmi užitečným nástrojem. V aktuální verzi systému FlowMon nese označení **ifrdump.**

Utilita **nfprofile** umožňuje vytvoření vlastního profilu ukládaných dat do vlastních souborů pomocí utility **nfcapd**, jinak řečeno dokáže zpracovat data uložená pomocí **nfcapd** a na základě uživatelsky definovaného filtru (např. upload na kolejní podsíti 10.67.0.0/16) vytvoří vlastní adresářovou strukturu, do které následně ukládá již filtrované NetFlow data:

/data/nfsen/profiles-data/KMZ/koleje/upload-exclude-utb/…

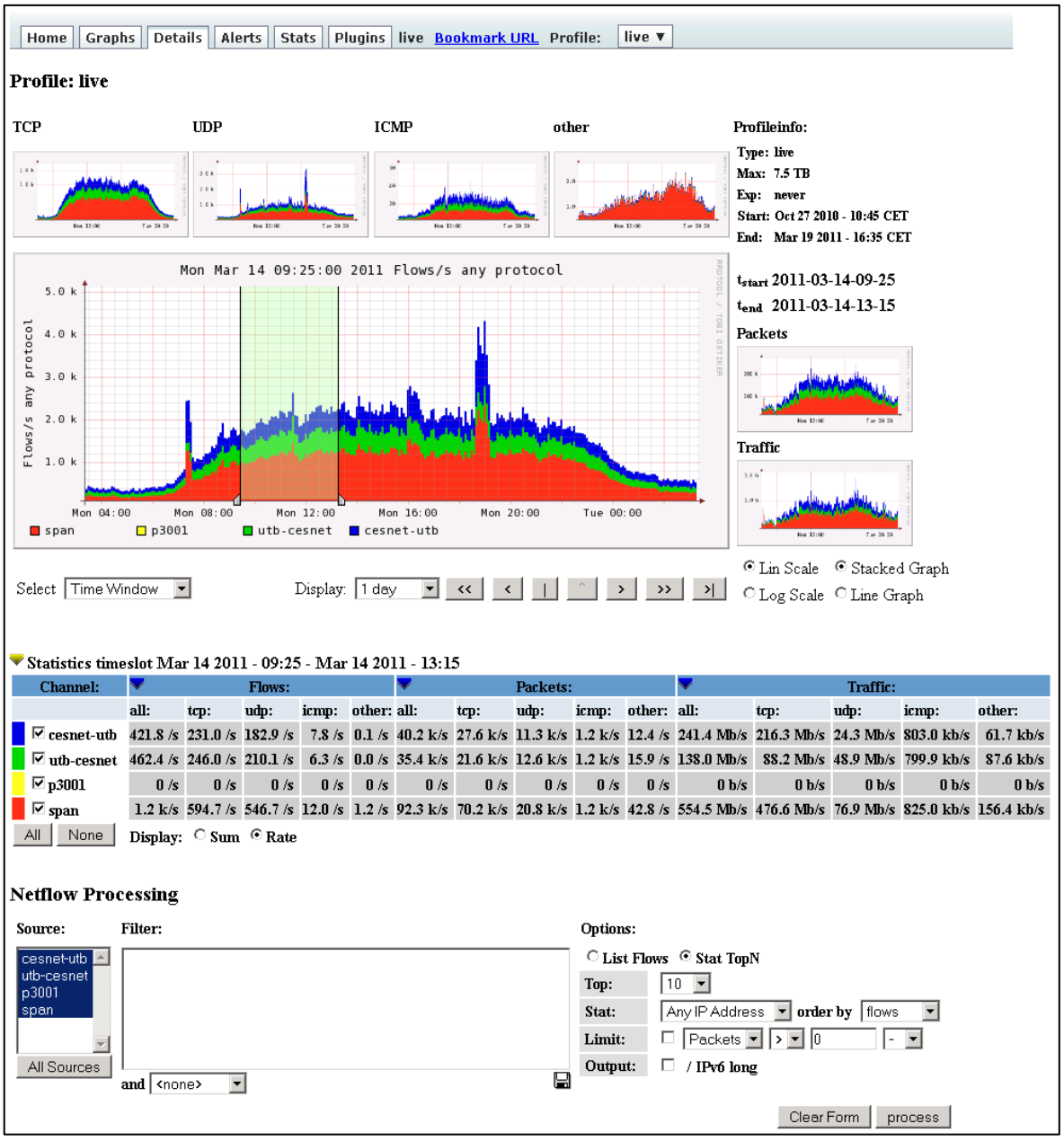
Smysl vytvoření vlastního profilu je v tom, že prohledávání kompletní NetFlow databáze na kolektoru může být zdlouhavé. Jestliže víme, která data často potřebujeme, můžeme si je předem připravit za pomoci vlastního filtru.

Mezi další NFDUMP utility patří **nfreplay**, **nfclean.pl** a **ft2nfdump**, které v rámci této práce nejsou využity [15].

4.5.2 Grafická nadstavba NFSEN

NFSEN umožňuje vizualizovat statistiky pomocí grafů. Skládá se ze dvou částí, horní část slouží k prohlížení NetFlow dat a k volbě konkrétního profilu, časového okna a slotu. Jsou zobrazeny vždy údaje, které se vztahují k otevřenému profilu. Zobrazit lze časový slot za 12 hodin, 1 den, 2 dny, 4 dny, 1 týden, 2 týdny, 1 měsíc. V časovém slotu lze zvolit časové okno určené k výběru období. Světle zelený obdélník výběru je umístěn přímo v grafu (viz. *Obr. 5*). Zvolené časové období představují hodnoty $\mathbf{t_{start}}$ a $\mathbf{t_{end}}$ zobrazené v pravé části stránky.

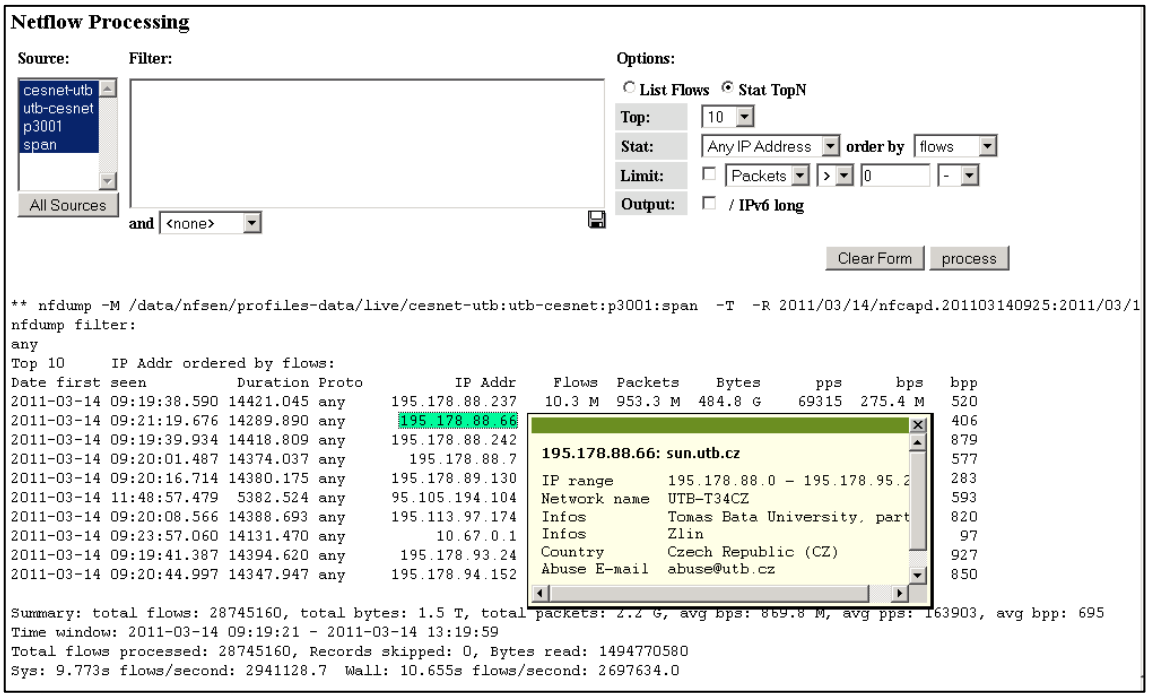
Graf časového slotu může zobrazovat také předdefinované protokoly jako je TCP (Transmission Control Protocol), UDP (User Datagram Protocol), ICMP (Internet Control Message Protocol) a další, dále lze přepínat mezi zobrazením Flows, Packets a Traffic. Přepínat lze pomocí kliknutí na příslušnou zmenšeninu grafu a hlavní graf se automaticky překreslí.



Obr. 5. Uživatelské rozhraní aplikace NFSEN

Ve střední části stránky v tabulce s modrým záhlavím jsou zobrazeny statistické údaje zvoleného časového okna. Tyto údaje se při každé změně období automaticky přepočítají.

Spodní část obsahuje nástroje pro zpracování dat ve zvoleném časovém slotu nebo okně a data jsou generována pomocí utility **nfdump**.



Obr. 6. NFSEN – zobrazená data a whois lookup k příslušné IP adrese

Grafická nadstavba NFSEN nabízí zobrazení reverzního DNS (Domain Name System) záznamu a záznamu WHOIS k příslušné IP adrese v pop-up okénku se zeleným záhlavím (viz. *Obr. 6*). Tímto rychlým způsobem se lze okamžitě dopátrat k původci případného bezpečnostního incidentu. Bohužel principiálně lze zajistit u vnitřních IP adres pouze zobrazení doménového jména z reverzního překladu IP adresy. Podrobnější údaje NFSEN o neveřejných IP adresách nezobrazuje. Zde by bylo možné využít databázi systému ASDP a k příslušným vnitřním IP adresám zobrazovat podrobnosti. Tento požadavek je řešen v rámci kapitoly 9.2.

4.6 Využití NetFlow statistik z kolektoru FlowMon pro systém ASDP

Využití a zpracování statistik NetFlow pro systém ASDP je řešeno v praktické části v kapitole 9.1.

5 DATABÁZOVÝ SERVER 602SQL

5.1 Popis serveru 602SQL

602SQL 8.1 je český relační databázový systém který implementuje jazyk SQL dle normy ANSI/ISO (American National Standards Institute / International Organization for Standardization) na úrovni SQL2 a SQL3. Databázová aplikace obsahuje nejen samotné data v tabulkách a objekty pro jejich zpracování (dotazy, procedury, triggery), ale i aplikační rozhraní, do kterého patří formuláře, sestavy, menu, obrázky, programy v klientském jazyce atd. Navíc obsahuje také kompletní vývojové prostředí pro tvorbu a programování aplikací a databázových procedur. Programovací jazyk aplikačního rozhraní je podobný standardnímu neobjektovému Pascalu, rozšířeného o prostředky komunikace s databází, snadné vytváření uživatelského rozhraní GUI (Graphical User Interface) a spolupráci s Windows.

V 602SQL 8.1 může jediná databázová aplikace obsahovat kompletní informační systém včetně dat a klientských aplikací. Výhodou tohoto modelu je, že po každé úpravě systému není třeba kompilovat a distribuovat k uživatelům konkrétní aplikace, ale změny se projeví u všech klientů v momentě jejich provedení. Další výhodou je, že od verze 8.1c až po verzi 11 je 602SQL zdarma a volně šiřitelný produkt. Nevýhodou je, že u verze 8.1c byl ukončen vývoj a nové verze 602SQL 9, 10 a 11 jsou vyvíjeny bez aplikačního rozhraní [17], [19].

5.2 Využití 602SQL na UTB ve Zlíně

Na VŠ kolejích UTB je v databázovém systému 602SQL provozován ubytovací systém AT-Koleje a systém ASDP pro správu datových přípojek. V rámci VŠ menzy UTB je provozována aplikace pro tvorbu, správu a zobrazování jídelníčku UTB a aplikace pro tvorbu etiket s čárovými kódy pro výrobky VŠ menzy.

6 SOFTWARE PRO SPRÁVU UBYTOVÁNÍ

6.1 Ubytovací program AT-Koleje

Program AT-Koleje je komerční komplexní produkt pro evidenci údajů o ubytovaných studentech, hotelových hostech a zaměstnancích a jejich platbách na VŠ kolejích. Program automatizuje a usnadňuje veškeré činnosti spojené s danou problematikou. Nabízí intuitivní grafické uživatelské rozhraní a průvodce s nápovědou. Je propojen se studijní databází STAG, zpracovává žádosti o ubytování, nabízí množství účetních a ubytovacích sestav, rozbory obsazenosti, podporuje hotovostní i bezhotovostní platební styk a jednoduchou práci s inkasem, hromadnou korespondenci klasickou i elektronickou. Autorem je Mgr. Karel Pečenka a program je vytvořen ve vývojovém prostředí 602SQL 8.1 [9].

Program je využíván ve všech ubytovacích kancelářích VŠ kolejí UTB ve Zlíně, v ekonomickém oddělení, v účtárně a u systémového administrátora.

Vzhledem k tomu, že program AT-Koleje je komerční produkt a vztahují se na něj autorská práva, zpracování dat a funkčnost systému budou vždy popisovány obecnou formou tak, aby byly pochopitelné v kontextu s předkládanými mechanismy.

V roce 2010 došlo k úpravě programu AT-Koleje, která umožnila jednodušší evidenci hotelových hostů a ubytovaných zaměstnanců UTB. Systém byl rozšířen o možnost rezervací a mnoho funkcí bylo inovováno. Důsledkem této úpravy byla i změna struktury databáze, se kterou se musel vypořádat také systém ASDP.

Webovým rozhraním ubytovacího programu je systém KOLEJE ON-LINE, který je naprogramován v programovacím jazyku PHP (Hypertext Preprocessor) a napojen na databázi 602SQL. KOLEJE ON-LINE je systémem vyvíjeným přímo na UTB.

Do ubytovacího programu AT-Koleje a systému KOLEJE ON-LINE je implementován systém ASDP, který byl vyvinut v rámci bakalářské práce [10].

6.1.1 Účetní předpisy

Ubytovací program generuje účetní obraty (platby) klientů na základě účetního předpisu. Účetní předpis je záznam v tabulce `u_predpis` (viz. kapitola 7.2), který doslova předepisuje, jakou platbu má ubytovací program vygenerovat. Platby se z účetních předpisů generují prostřednictvím automatického rozúčtování plateb, což je vnitřní funkce

ubytovacího programu. Jakákoliv průběžná služba má svůj účetní předpis, tedy i aktivace datové přípojky je průběžnou službou splatnou od data aktivace po deaktivaci a ukončení využívání datové přípojky. S autorem ubytovacího programu byly dohodnuty následující standardy, které budou sloužit jako podklady pro návrh a realizaci automatické procedury správy účetního předpisu.

- V jediném měsíci je splatný jeden účetní předpis na datovou přípojku, nesmí se tedy stát, aby v jediném měsíci existovaly dva nebo více účetních předpisů pro datovou přípojku.
- Rozlišuje se otevřený předpis, tj. takový, který je platný. Uzanční datum, které definuje otevřený předpis, je stanoveno na 31.12.2099 a je uloženo v položce `u2_do`. Uzavřený předpis je takový, který má v položce `u2_do` uloženo datum menší než výše uvedené.

Předchozí verze obsahovala pouze nastavení dvou databázových hodnot (od, do), které nereflektovaly možnost historie, neboť při změnách aktivace byly přepisovány. Správa účetního předpisu je součástí SQL procedury `nastav_internet` a `odhlas_internet` (viz. kapitola 7.2.3 a 7.2.4).

6.1.2 Rozdělení klientů do skupin

Klienti jsou rozděleni do tří nejčastěji používaných skupin. Každé skupině je přiděleno identifikační číslo. Údaje jsou obsaženy v tabulce `skupina`.

Jsou definována tato identifikační čísla:

- 0 - studenti
- 3 - hoteloví hosté
- 4 - ubytovaní zaměstnanci

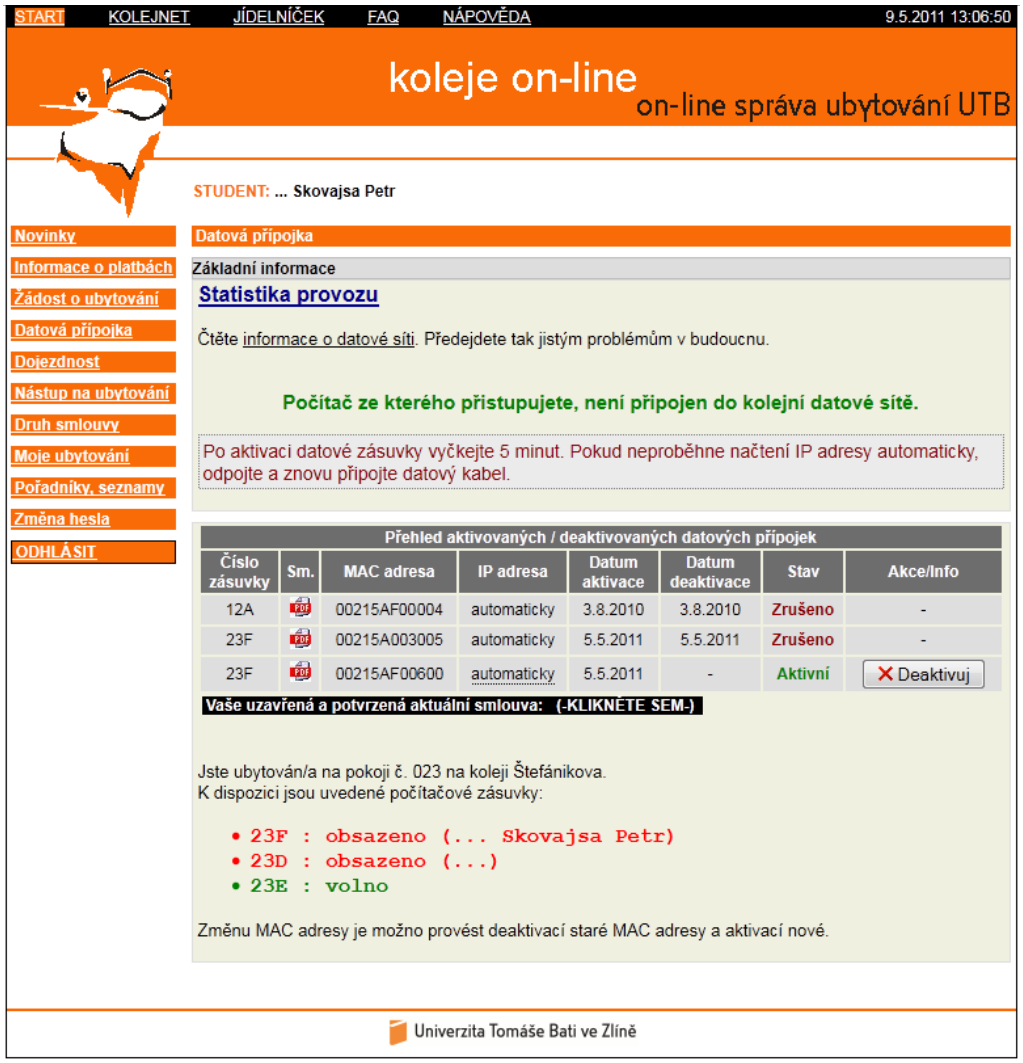
Identifikační čísla 1 a 2 patří skupinám, které již nejsou v rámci ubytovacího programu využívány. Na základě uvedených identifikátorů je umožněno správné účtování při spolupráci systému ASDP s programem AT-Koleje či přihlášení do systému KOLEJE ON-LINE.

6.2 Systém KOLEJE ON-LINE

Umožňuje online správu ubytování pro ubytované studenty a nově i zaměstnance UTB na VŠ kolejích UTB. Systém je přístupný z webové adresy https://koleje.utb.cz. Způsob

přihlášení je pomocí přihlašovacích údajů univerzitní sítě se síťovým SW Novell [10]. Systém KOLEJE ON-LINE je rozdělen do několika sekcí. Obsahuje aktuality, informace o platbách včetně aktuálního účetního stavu konta a kauce. Umožňuje podání elektronické žádosti o ubytování, zpracování a prohlížení pořadníků a seznamů podaných žádostí, kontrolu přidělené hodnoty tzv. časové dojezdnosti a zastávky. Po zveřejnění pořadníků umožňuje výběr lůžka a přímou rezervaci ubytování na konkrétním pokoji, prohlížení spolubydlících, výběr druhu ubytovací smlouvy a volbu termínu data nástupu na ubytování. V sekci datová přípojka umožňuje aktivaci a deaktivaci datové přípojky. Pro ubytovatele nabízí rozšířené přehledy obsazených lůžek prostřednictvím rezervací.

Stránka systému s otevřenou sekcí Datová přípojka je na následujícím obrázku.

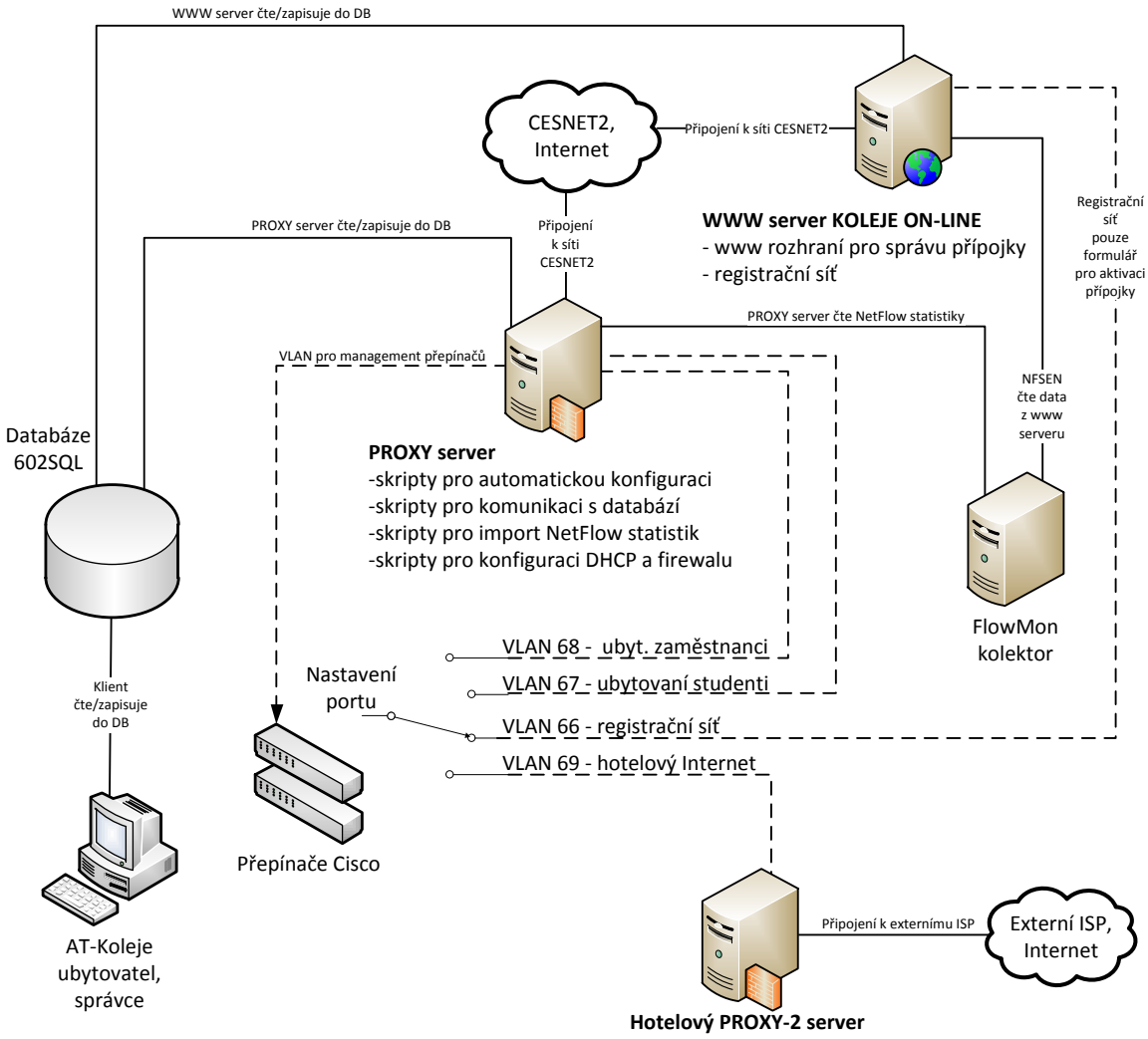


Obr. 7. Stránka systému KOLEJE ON-LINE s otevřenou sekcí Datová přípojka

II. PRAKTICKÁ ČÁST

7 INOVACE AUTOMATIZOVANÉHO SYSTÉMU PRO SPRÁVU DATOVÝCH PŘÍPOJEK

7.1 Návrh a propojení jednotlivých částí systému ASDP



Obr. 8. Schéma propojení jednotlivých částí systému ASDP

7.1.1 Popis návrhu

PROXY server je společně s databází srdcem systému ASDP. Slouží jako firewall a DHCP server pro datovou síť ubytovaných zaměstnanců a studentů. Obsahuje skripty, které provádí konfiguraci portů přepínačů Cisco, DHCP serveru a firewallu. PROXY server dále komunikuje s databází, generuje NetFlow statistiky z FlowMon kolektoru a řídí datovou propustnost.

Databáze 602SQL slouží jako datové úložiště pro systém ASDP, ubytovací program AT-Koleje a jeho webové rozhraní KOLEJE ON-LINE. Obsahuje SQL procedury určené pro zpracování dat.

WWW server KOLEJE ON-LINE poskytuje webové rozhraní pro aktivaci/deaktivaci přípojky, umožňuje přístup pro studenty a zaměstnance UTB, poskytuje službu DHCP pro registrační síť a registrační formulář, generuje data o IP adresách pro kolektor.

FlowMon kolektor poskytuje datové úložiště pro NetFlow statistiky a získává údaje o IP adresách ze systému KOLEJE ON-LINE.

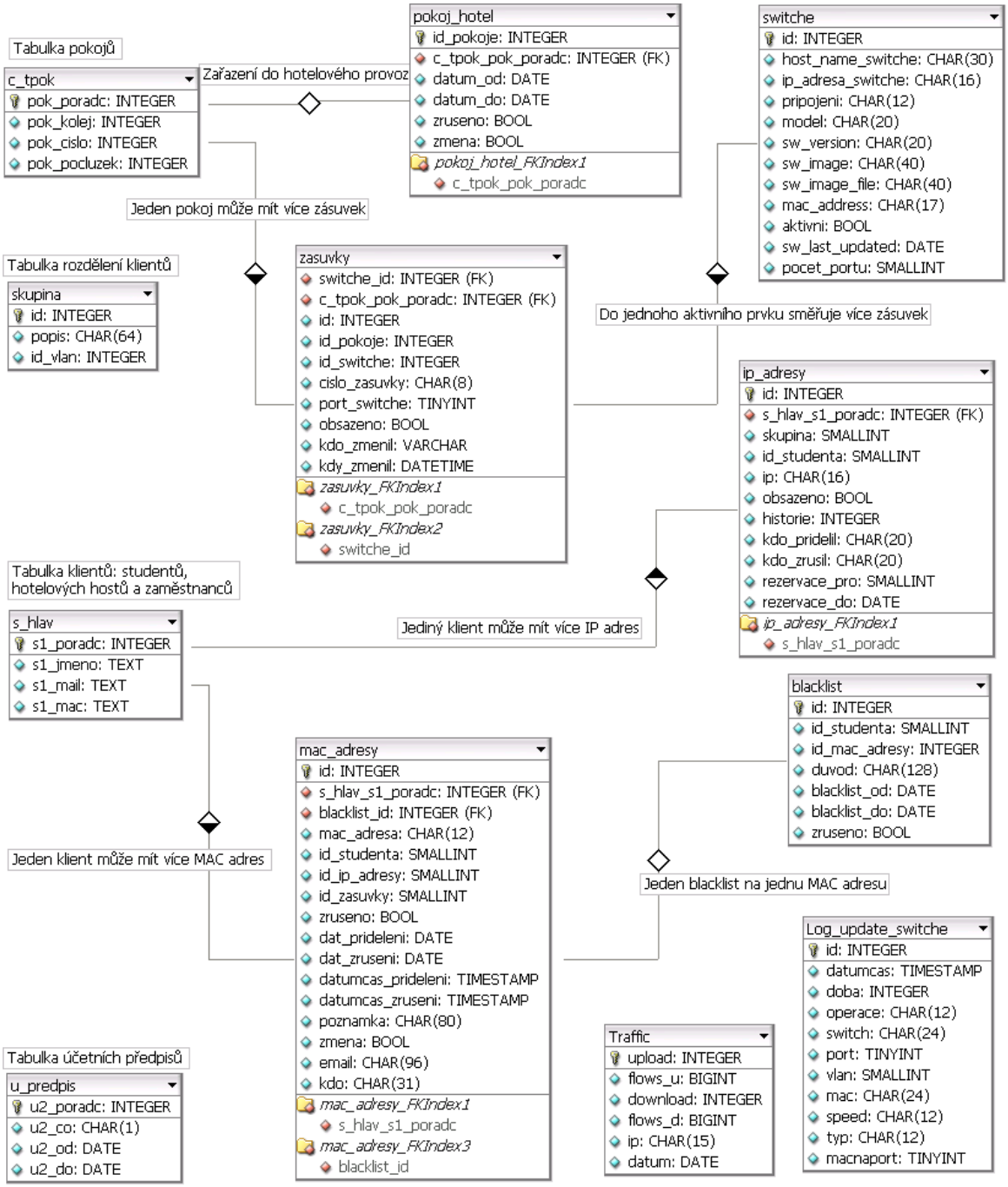
Program AT-Koleje poskytuje GUI pro ubytovatele a administrátora, zajišťuje evidenci ubytování studentů, zaměstnanců a volitelně hostů. Obsahuje také aplikační rozhraní systému ASDP pro správu datových přípojek, umožňuje nastavení pokoje pro hotelový provoz.

Přepínače Cisco a strukturovaná kabeláž umožňují připojení k datové síti příslušné VLAN.

Hotelový PROXY-2 server stojí mimo systém ASDP a je bránou do Internetu externího ISP. Poskytuje DHCP pro hotelovou síť a umožňuje přístup k Internetu hotelovým hostům.

Celý systém je navrhován jako dynamický komplexní celek, který má sloužit k zajištění automatizované správy celé sítě na VŠ kolejích UTB ve Zlíně. Propojení jednotlivých částí je popisováno v kapitolách 8 a 9.

7.2 Seznam tabulek, SQL procedur a dotazů



Obr. 9. Schéma inovované databáze systému ASDP

Tabulka pokojů `c_tpok` obsahuje číselník všech pokojů na všech budovách VŠ kolejí UTB. Tabulka klientů `s_hlav` obsahuje základní údaje o klientovi. Tabulka `u_predpis` obsahuje jednotlivé účetní předpisy na jednorázové či průběžné služby (např. datovou přípojku). Tabulky pokojů, klientů a účetních předpisů jsou součástí ubytovacího programu

(viz. *Obr. 9*), proto jsou uvedeny pouze ty základní sloupečky, se kterými pracuje systém ASDP.

7.2.1 Tabulky systému ASDP:

- `Zasuvky` - obsahuje číselník datových zásuvek a jejich vazby na pokoj a port konkrétního přepínače.
- `Ip_adresy` - obsahuje seznam IP adres. V aktuální verzi byla rozšířena o časovou rezervaci IP adresy pro konkrétního klienta pomocí nových sloupečků `rezervace_pro` a `rezervace_do`.
- `Switche` - obsahuje seznam aktivních prvků v síti. Byla rozšířena o sloupeček `aktivni` a `pocet_portu`. Tyto dva údaje jsou využívány skriptem, který obnovuje konfiguraci celé datové sítě do výchozího stavu.
- `Blacklist` - určena ke správě pozastavení datové přípojky.
- `Mac_adresy` - obsahuje aktivované MAC adresy.

7.2.2 Nové tabulky systému ASDP

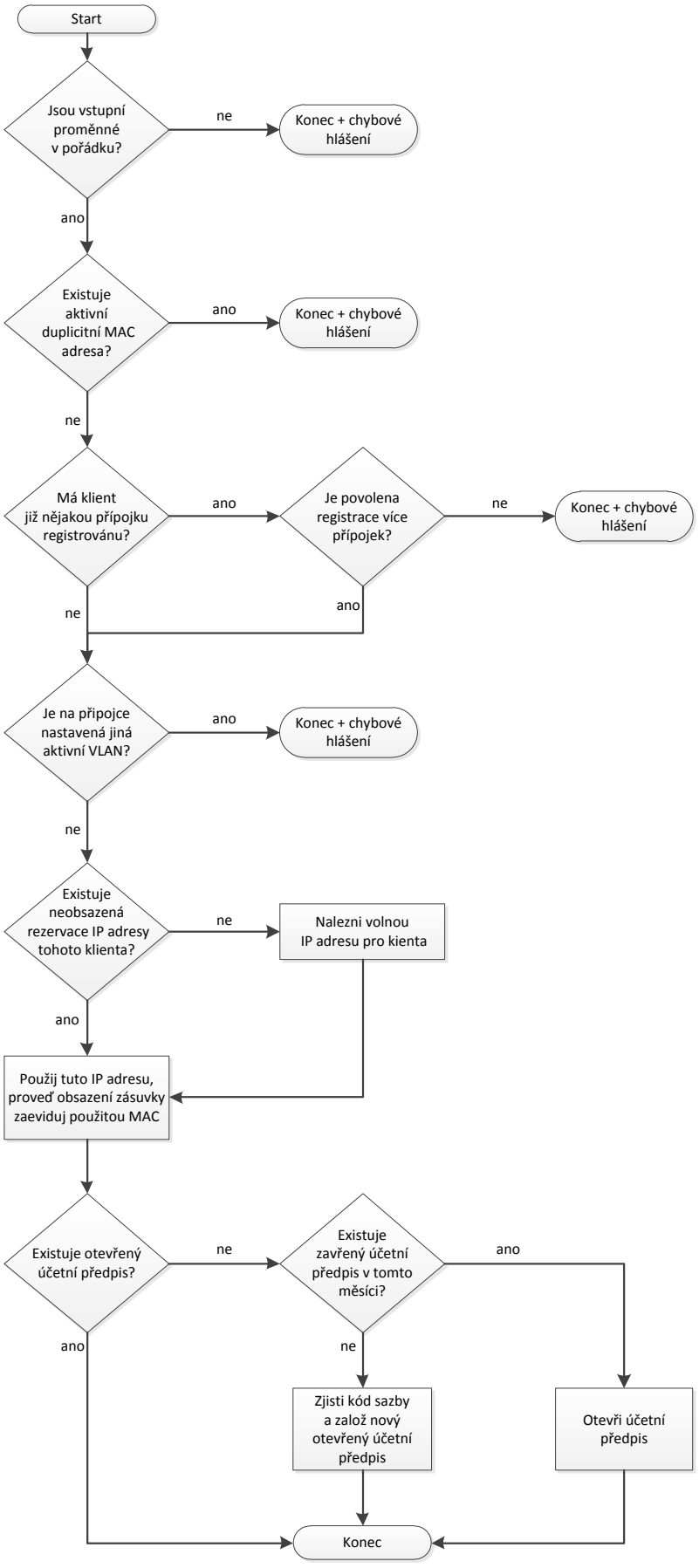
- `Log_update_switche` - je určena pro záznamy skriptu `generuj_zasuvky_sh`, zde je nejdůležitější informací sloupeček `doba`, který uvádí dobu trvání skriptu. Při úspěšném provedení skriptu je doba trvání nejvýše 15s, při neúspěšném provedení skriptu je doba trvání vyšší jak 20s. Uvedené časy jsou platné pro skripty a síť UTB. Další sloupečky slouží k identifikaci zařízení a portu, na kterém skript prováděl konfiguraci.
- `Pokoj_hotel` - obsahuje seznam pokojů, které jsou zařazeny do hotelového provozu.
- `Traffic` - obsahuje souhrnné statistiky o počtu přenesených dat za každý den pro každou IP adresu.

7.2.3 SQL procedura nastav_internet

Tato SQL procedura doznala výrazných změn oproti předchozí verzi. IP adresy již nejsou vybírány způsobem „nejnižší volná“ ale pomocí vlastního způsobu rezervací. IP adresa je při první aktivaci zarezervována do stanoveného data a pro příslušného studenta či ubytovaného zaměstnance. Zcela přepracována byla správa účetního předpisu.

Činnost SQL procedury `nastav_internet`:

- Kontrola vstupních proměnných: ID studenta, ID zásuvky, MAC adresa, email.
- Získání pomocných proměnných: VLAN a skupina klienta.
- Kontrola duplicity v tabulce `mac_adresy`. Kontroluje se, zda vkládaná MAC adresa nekoliduje s nějakou stávající aktivní zaregistrovanou MAC adresou.
- Provede se kontrola, zda klient již má nějakou datovou přípojku aktivovánu. Kontrolu řídí vnitřní parametr SQL procedury `vicepripojek`, při hodnotě 0 (FALSE) není možno registrovat na jednoho klienta více datových přípojek, při hodnotě 1 (TRUE) je možné na jednoho klienta zaregistrovat více datových přípojek.
- Provede se kontrola, zda na příslušné zásuvce není zaregistrována další přípojka s odlišnou VLAN.
- Při výběru IP adresy se nejprve zkontroluje, zda existuje neobsazená rezervace IP adresy v tabulce `ip_adresy`. Pokud existuje, přidělí se pro klienta rezervovaná IP adresa. Pokud neexistuje, nalezne se taková IP adresa, které uplynula doba rezervace a zároveň je neobsazená nebo se vyhledá zcela volná IP adresa. Pokud by měl klient rezervovaných více IP adres, procedura vybere vždy tu s nejvyšším datem `rezervace_do`.
- Při správě účetního předpisu se provede kontrola, zda existuje otevřený účetní předpis (viz. kapitola 6.1.1), pokud takový neexistuje, pak procedura zkontroluje, zda existuje účetní předpis, který byl uzavřen v aktuálním měsíci. Pokud ano, pak se tento předpis otevře. Pokud neexistuje žádný z výše uvedených, založí se nový otevřený účetní předpis pro datovou přípojku.



Obr. 10. Vývojový diagram SQL procedury nastav_internet

7.2.4 SQL procedura odhlas_internet

Vnitřní činnost se oproti předchozí verzi změnila méně. Úkolem této procedury je odhlášení datové přípojky – zrušení registrace MAC adresy a nově správa účetního předpisu. Inovace spočívá v tom, že pokud klient nemá aktivní žádné další datové přípojky, je předpis uzavřen, v opačném případě je ponechán beze změny. Vstupními parametry procedury jsou ID studenta a ID MAC adresy [10].

7.2.5 SQL procedura del2blacklist_automaticky

Kontroluje vypršení blacklistu a nastavuje u přípojky opětovnou aktivaci. Vychází z procedury `del2blacklist`, která je spouštěna pouze z klientského prostředí 602SQL ubytovatelem nebo správcem. Procedura je spouštěna automaticky (viz. kapitola 7.3).

7.2.6 SQL procedura is_blacklist

Tato procedura zjišťuje, zda je příslušná MAC adresa v tabulce `blacklist` či nikoliv. Vstupním parametrem je ID záznamu z tabulky `mac_adresy`. Procedura prohledává, zda toto ID je zavedeno v tabulce `blacklist` a zda je aktivní. Pokud ano, procedura vrátí hodnotu 1 (TRUE), pokud ne, vrátí hodnotu 0 (FALSE).

7.2.7 SQL procedura dej_proxy_list

Generuje řádek naformátovaných vstupních proměnných pro konfiguraci síťových přepínačů. Vstupem je ID řádku z tabulky `mac_adresy` a parametr `add` nebo `del`, výstupem je uspořádaný seznam hodnot oddělených středníkem, formát a způsob konfigurace je popsán v [10]:

```
0_8;10.67.1.10;00:14:85:8C:06:93;47;67;SW1;10.6.0.1;10;SSH;6;5;del
```

Tento konfigurační řádek je určen pro dotaz `proxy`, který je volán z linuxového bash skriptu `generuj_proxy.sh`, jenž tato data využívá ke konfiguraci přepínačů a PROXY serveru. Procedura `dej_proxy_list` nahrazuje předchozí způsob generování řádku přímo v dotazech `proxy_add`, `proxy_del` a `proxy_snapshot`.

7.2.8 SQL procedura dej_pocet_aktivnich

Vstupem procedury je ID zásuvky, návratová hodnota je aktuální počet MAC adres, které jsou na dané zásuvce registrovány. Procedura je určena pro kartu číselníku datových zásuvek (viz. kapitola 8.1.4) kde pomáhá vizualizovat, zda je zásuvka volná či obsazena.

7.2.9 Další SQL procedury

SQL procedury, které jsou podrobně popsány v bakalářské práci [10]:

- `Add2blacklist` – zavede aktivovanou přípojku do tabulky `blacklist`.
- `Del2blacklist` – odstraní aktivovanou přípojku z tabulky `blacklist`.
- `Napln_ip` – naplní tabulku `ip_adresy` při uvedení sítě do provozu. Byly přidány defaultní rozsahy IP adres pro datovou síť ubytovaných zaměstnanců UTB.

7.2.10 Dotazy systému ASDP

Dotazy jsou popsány v [10]. Dotazem je objekt databáze, který z tabulek vybírá data a uspořádává výsledek podle definice SQL příkazu v textové formě. Dokáže soustředit údaje z více tabulek a pomáhá zjednodušit práci s daty.

Nové dotazy jsou:

- `Proxy_hotel_add` – generuje seznam zásuvek, které je potřeba nastavit pro hotelový provoz.
- `Proxy_hotel_del` – generuje seznam zásuvek, které je potřeba deaktivovat z hotelového provozu.
- `Proxy_hotel` – spojuje dotazy `proxy_hotel_add` a `proxy_hotel_del`.
- `Test_caste_zmeny` – generuje seznam klientů a k nim počet aktivací, je to vhodné pro kontrolu, zda někdo příliš často neprovádí aktivaci a deaktivaci přípojky.
- `Traffic_nadmerny_upload` – generuje z tabulky `traffic` seznam uživatelů s nadměrným počtem odeslaných dat za příslušné datum.
- `Traffic_nadmerny_download` – generuje z tabulky `traffic` seznam uživatelů s nadměrným počtem stažených dat za příslušné datum.
- `Traffic_nadmerny_flows` – generuje z tabulky `traffic` seznam uživatelů s nadměrným počtem flows za příslušné datum.

7.3 Automatická aktivace přípojky po vypršení pozastavení

Je-li přípojka pozastavena, existuje příslušný záznam v tabulce `blacklist` s ID studenta a ID MAC adresy. V záznamu je také uvedeno počáteční datum, konec platnosti pozastavení. Denně v 01:00 je automaticky spouštěn bash skript `sql_cron_daily.sh`, který kontroluje, zda u některého ze záznamů v tabulce `blacklist` došlo k vypršení

pozastavení. Pokud ano, spouští automaticky SQL proceduru, která deaktivuje status pozastavení u příslušné MAC adresy.

Skript `sql_cron_daily.sh` obsahuje příkazy:

```
cat /root/conf-sql/sql_cron_daily.sql | /root/conf-
sql/602cli8 -s SERVER -l UZIVATEL -p HESLO -a APLIKACE -dm1
```

Soubor `sql_cron_daily.sql` obsahuje volání procedury:

```
CALL Del2blacklist_automaticky()
```

SQL procedura `Del2blacklist_automaticky` u příslušného záznamu v tabulce `blacklist` nastaví hodnotu `zruseno = TRUE`. Tím dojde k deaktivaci pozastavení datové přípojky a dále v tabulce `mac_adresy` nastaví `zmena = TRUE`, což zajistí opětovnou aktivaci přípojky pomocí automatického bash skriptu `generuj_zasuvky.sh`, který je spouštěn každých 5 minut.

7.4 Rezervace IP adresy

IP adresy jsou přidělovány z tabulky `ip_adresy`. Původně navržený způsob přiděloval klientovi vždy nejnižší volnou IP adresu. Způsob přidělování IP adres je v současné verzi inovován. Vznikl požadavek, aby IP adresa příliš často nestřídala majitele. Důvody vycházejí z potřeb popsaných v kapitole 9, to je např. sledování počtu přenesených dat, řízení přenosové rychlosti datové přípojky a jednoznačná identifikace klienta podle IP adresy i po delší době.

IP adresa je při první rezervaci přípojky klientovi zarezervována na stanovený počet dnů. Nastavena byla rezervace na 270 dnů od provedené aktivace. Nastavení této hodnoty je závislé na fluktuaci klientů a jejich počtu, využití zásuvek a počtu volných IP adres. V případě studentského ubytování je k dispozici 858 zásuvek pro studenty a cca 2024 volných IP adres určených pro studenty. Je tedy počítáno s tím, aby konkrétní IP adresa vydržela studentovi po dobu jeho pobytu na VŠ koleji. Pokud by došlo k vyčerpání rozsahu, což je při uvedených počtech málo pravděpodobné, lze snížit dobu rezervace IP adresy nebo navýšit počet IP adres.

Přidělování IP adres provádí procedura `nastav_internet` (viz. kapitola 7.2.3).

7.5 Ochrana sítě proti nežádoucímu DHCP serveru

Na PROXY serveru je spuštěna služba DHCP serveru, která na vyžádání přiděluje počítačům v síti IP adresu a další údaje potřebné pro správné nastavení sítové konfigurace klientského počítače. Informace k DHCP lze najít v [30]. V datové síti studentů a zaměstnanců by se neměl vyskytovat další aktivní DHCP server. Bohužel dochází ze strany uživatelů k záměrnému či nežádoucímu připojení WiFi routeru. Ten obsahuje svůj vlastní DHCP server, který by mohl při neodborné instalaci způsobit distribuci nežádoucích IP adres pro připojené stanice v síti. Datové připojení bude v takovém případě buď nefunkční, nebo bude provoz uskutečňován přes tento cizí router.

K zamezení vlivů neautorizovaného DHCP serveru lze na přepínačích Cisco použít příkazy CLI (Command Line Interface) sloužící k nastavení důvěryhodných portů, na nichž se nachází autorizovaný DHCP server. Tato ochranná metoda se nazývá DHCP snooping a nastavuje se následovně:

```
1.  switch> ena
2.  switch# configure terminal
3.  switch(config)# ip dhcp snooping
4.  switch(config)# ip dhcp snooping vlan 66 69
5.  switch(config)# interface range gi0/1 – 2
6.  switch(config-if)# ip dhcp snooping trust
7.  switch(config-if)# end
8.  switch# write memory
```

Pomocí příkazu 1. se provede vstup do privilegovaného režimu, ze kterého se přejde do 2. globálního konfiguračního režimu, příkazem 3. se zapíná DHCP snooping na síťovém přepínači a příkazem 4. se upřesňuje rozsah VLAN, na které je vztažen. Pomocí příkazu 5. se provede přepnutí do příslušného síťového rozhraní, na tomto rozhraní se pomocí příkazu 6. zapne důvěryhodný port, ze kterého budou akceptovány odpovědi DHCP serveru. Příkazem 7. je ukončeno zadávání a příkazem 8. se provede uložení aktuální konfigurace.

Uvedené nastavení má také bezpečnostní důvod, umožňuje eliminovat nebezpečný útok typu man-in-the-middle, jehož podstatou je snaha útočníka o odposlech komunikace mezi účastníky tak, že se stane aktivním prostředníkem [16].

7.6 Zapnutí portu síťového přepínače ze stavu err-disabled

Na portech datových přepínačů dochází výjimečně k případům vypnutí portu, resp. přepnutí do stavu err-disabled. Důvody mohou mít bezpečnostní a ochranný charakter, při vzniku jsou zapsány do logu přepínače. Výpis logu z příslušného přepínače lze provést pomocí příkazu CLI:

```
9.  switch# show logging
```

V defaultním nastavení tento stav přetrvá do doby, než správce provede ruční zapnutí portu do stavu enabled pomocí příkazů CLI. Lze jej také vyřešit automaticky pomocí detekce stavu err-disabled a následném zapnutí portu. Nastavení automatické detekce stavu err-disabled a následné automatické zapnutí portu lze provést následovně:

```
10. show errdisable recovery
11. errdisable detect cause all
12. errdisable recovery cause interval 300
```

Příkazem 10. lze zobrazit stav, které důvody jsou nastaveny pro automatické obnovení, příkaz 11. nastavuje zapnutí portu, který byl vypnut ze všech důvodů, příkaz 12. nastavuje časový interval, tj. každých 300 sekund dojde k otestování portů na stav err-disabled. Nebývá však obvyklé nastavení, aby obnovení portu reagovalo na všechny chybové stavy.

V závažných případech bývá vhodnější, když jsou tyto události vyhodnoceny prostřednictvím SNMP (Simple Network Management Protocol) protokolu a nějakého vlastního monitorovacího serveru.

7.7 Nastavení rychlosti portu přepínače

Z praktického hlediska se zdá výhodné řízení rychlosti přímo na portu aktivního prvku. Nevýhodou je však to, že na VŠ koleji Antonínova mohou být k jedinému portu připojeni dva uživatelé současně a omezení jednoho uživatele by způsobilo omezení druhého. Navíc ne všechny CLI příkazy je možno využít kvůli starším typům aktivních prvků a v té souvislosti s jinou verzí Cisco IOS (Internetwork Operating System).

Nejjednodušším způsobem je řízení rychlosti nastavením přímo na portu. Podle maximální rychlosti portu lze nastavovat rychlosti na 10, 100 nebo 1000 Mbit/s. Příklad:

```
speed 10
```

Omezení rychlosti na 10 Mbit/s není natolik patrné, aby jej uživatel pocítil.

Další způsob řízení rychlosti přímo na portu aktivního prvku vyžaduje zapnutí MLS QOS (Multi-Layer Switching Quality Of Service) a omezení rychlosti procentuálně na 10 - 90% pomocí příkazu:

```
srr-queue bandwidth limit 10
```

Takže při současném použití příkazu `speed 10` lze snížit rychlost portu až na 1 Mbit/s. Tato kombinace je však možná pouze na přepínači Cisco Catalyst 2960, který máme začleněn v síťové infrastruktuře. Bohužel se omezí pouze download (na portu je to směr OUT). Na typu Catalyst 2950 příkaz `srr-queue` není implementován.

Je možno využít další způsob omezení pomocí politiky a tříd, který umí omezit odchozí data z počítače uživatele (na portu je to směr IN). Příklad nastavení je z [21]:

```
mls qos map cos-dscp 0 10 16 18 24 26 32 34
class-map match-all alltraffic
  match access-group 133
policy-map 1m-bandwidth
  class alltraffic
    police 1000000 65536 exceed-action drop
access-list 133 permit ip any any
```

Na příslušném portu se nastaví:

```
ip access-group 133 in
load-interval 30
service-policy input 1m-bandwidth
```

Kombinací výše popsaných způsobů lze na portu dosáhnout omezení rychlosti v obou směrech. Bohužel tato nastavení jsou závislá na konkrétních typech síťových přepínačů, ne každý student je připojen k jediné zásuvce a navíc správa této konfigurace by byla poměrně složitější v porovnání s řešením popisovaným v kapitole 9.3.

7.8 Inovace webového rozhraní pro klienty

Webové rozhraní je součástí systému KOLEJE ON-LINE, jednou z úprav bylo také přidání možnosti pro přihlášení ubytovaného zaměstnance. Součástí uvedeného systému je sekce **Datová přípojka**, kde může klient provádět aktivaci, deaktivaci přípojky, tisk či stažení smlouvy, sledovat statistiku přenesených dat. Inovace této sekce je popsána v kapitolách 7.8.1, 7.8.2 a 9.1.5.

7.8.1 Odeslání emailu při aktivaci datové přípojky

Po aktivaci datové přípojky je vhodné odeslat uživateli email o provedené akci a další instrukce k pravidlům datové sítě. Odeslání emailu je provedeno přímo PHP skriptem na stránce registrace datové přípojky v systému KOLEJE ON-LINE. Je využito knihovny PHPMAILER, která je distribuována pod licencí GPL (General Public Licence). Knihovnu lze najít na webové stránce http://phpmailer.worxware.com.

Knihovnu lze nakopírovat do adresářové struktury webových stránek a použít v PHP kódu skriptu pomocí příkazu:

```
require "phpmailer/class.phpmailer.php";
```

Před odesláním emailu se nastavují následující proměnné:

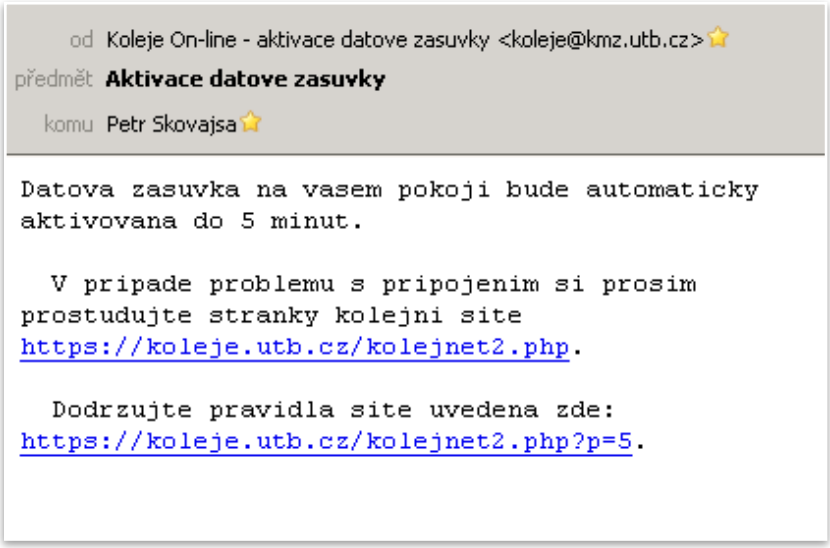
```
13. $mail = new PHPMailer();
14. $mail->IsSMTP();
15. $mail->Host = "smtp.utb.cz";
16. $mail->SMTPAuth = false;
17. $mail->Username = "";
18. $mail->Password = "";
19. $mail->From = "email@utb.cz";
20. $mail->FromName= "KOLEJE ON-LINE – aktivace datove zasuvky";
21. $mail->AddAddress($email);
22. $mail->Subject = "Aktivace datove zasuvky";
23. $mail->Body = "text zprávy";
24. $mail->WordWrap = 50;
25. $mail->CharSet = "cp-1250";
```

Příkazem 13. se vytvoří instance objektu. Použití SMTP (Simple Mail Transfer Protocol) se nastaví příkazem 14. a pomocí 15. se definuje adresa SMTP serveru. Pokud vyžaduje server autentizaci, nastavíme příkazem 16. hodnotu `true`, jinak `false`. Příkazem 17. a 18. se definuje případné uživatelské jméno a heslo pro připojení k SMTP serveru. Adresa odesílatele emailu se definuje v 19. a jméno odesílatele v 20. Pomocí 21. lze přidat do instance jednoho či více příjemců. Předmět emailu lze nastavit pomocí 22. a pomocí 23. vložit text samotné zprávy. Zalamování řádku v emailu se nastaví příkazem 24. Znaková sada (např. cp-1250) pomocí příkazu 25.

Samotné odeslání emailu se provede příkazem 26:

```
26. $mail->Send();
```

Došlý email může mít následující formát a text (viz. *Obr. 11*):



Obr. 11. Vzorový email aktivace datové přípojky

7.8.2 Vygenerování elektronické smlouvy do PDF

Byla implementována možnost zobrazení či stažení smlouvy o užívání datové přípojky ve formátu PDF (Portable Document Format). Do přehledu historie aktivovaných přípojek byl doplněn sloupeček **Sm.** (smlouva) a kliknutím na ikonku PDF v příslušném řádku lze otevřít či uložit smlouvu vztaženou k příslušnému záznamu o aktivované přípojce.

Přehled aktivovaných / deaktivovaných datových přípojek							
Číslo zásuvky	Sm.	MAC adresa	IP adresa	Datum aktivace	Datum deaktivace	Stav	Akce/Info
12A		00000AF73664	automaticky	3.8.2010	3.8.2010	Zrušeno	-
519L.1A		000000000011	automaticky	11.4.2011	11.4.2011	Zrušeno	-
12A		00000AF73665	automaticky	20.4.2011	-	Aktivní	✕ Deaktivuj

Obr. 12. Přehled aktivovaných přípojek s možností tisku smlouvy do PDF

Pro generování PHP souboru byla využita knihovna FPDF (ke stažení na www.fpdf.org). Knihovnu lze nakopírovat do adresářové struktury webových stránek a do stávajícího PHP kódu se implementuje příkazem:

```
require('pdf/fpdf.php');
```

Následně lze využít třídy FPDF ke generování dokumentu. Níže je uveden způsob jakým jsou generovány smlouvy v systému KOLEJE ON-LINE. Pro tento účel byl vytvořen PHP skript s názvem `generuj_pdf.php`. Skript je zavolán po kliknutí na ikonku PDF a obsahuje tyto příkazy potřebné k práci s PDF:

```
27.   $pdf=new FPDF();
28.   $pdf->AddPage();
29.   $pdf->AddFont('verdana', '', 'verdana.php');
30.   $pdf->SetFont('verdana', '', 12);
31.   $pdf->SetTitle('Elektronicka smlouva);
32.   $pdf->SetDisplayMode('fullpage');
33.   $pdf->SetAuthor('SYSTEM KOLEJE ON-LINE');
34.   $pdf->Write(5,$text_smlouvy);
35.   $pdf->Output("Smlouva_".$sml.".pdf",D);
```

`$pdf` je instance třídy `FPDF`, do ní vložíme pomocí příkazu `AddPage` novou stránku a aktivujeme příslušný font příkazem `AddFont` a velikost fontu `SetFont`. Pomocí `SetTitle` a `SetAuthor` lze vyplnit doplňující údaje o souboru. Příkaz `SetDisplayMode` způsobí implicitní zobrazení celého dokumentu na jediné stránce v PDF prohlížeči. Příkaz `Write` uloží text smlouvy s řádkováním 5. Poslední `Output` generuje PDF soubor, první parametr obsahuje dynamicky tvořený název souboru a druhý parametr D způsobí odeslání vygenerovaného PDF souboru ze serveru do prohlížeče [26].

7.9 Aktivace datové přípojky pro ubytované zaměstnance

Způsob správy datové přípojky pro ubytované zaměstnance je podobný jako pro studenty. Datová síť na VŠ kolejích pro ubytované zaměstnance bude mít vlastní VLAN 68 a vlastní rozsah IP adres (10.68.0.0/22). Na stávajícím PROXY serveru bude nastavena konfigurace síťové karty pro provoz ve více VLAN. Příslušné úpravy si vyžádá také nastavení firewallu PROXY serveru. Aktivace datové přípojky bude probíhat v systému KOLEJE ON-LINE, kam se zaměstnanec může přihlásit pomocí uživatelského jména a hesla univerzitní sítě NOVELL. Ubytovaný zaměstnanec musí být zaveden v evidenci ubytovacího programu AT-Koleje a musí mít přidělen příslušný pokoj. Ubytovaný zaměstnanec také potvrzuje pravidla datové sítě a uzavírá elektronickou smlouvu o aktivaci datové přípojky. Cena za připojení ubytovaného zaměstnance je stanovena v číselníku databáze programu

AT-Koleje (tabulka `c_inter`), v případě VŠ kolejí UTB má ubytovaný zaměstnanec datovou přípojku zdarma.

Provedené úpravy: stávající IP adresy rozsahu 10.67.0.0/22 z tabulky `ip_adresy` jsou přidělovány studentům. Do tabulky je přidán další rozsah IP adres 10.68.0.0/22 pro ubytované zaměstnance. Příslušnost každé IP adresy je definována novým sloupečkem `skupina`, jehož obsah je popsán v kapitole 6.1.2. Příslušnou úpravu pro práci se skupinami vyžaduje také SQL procedura `nastav_internet` i dotazy `proxy_add` a `proxy_del`, které slouží jako zdroj údajů pro bash skript `generuj_zasuvky.sh`.

7.10 Nastavení síťové karty PROXY serveru pro provoz ve více VLAN

Aby mohl být používán na síťové kartě PROXY serveru provoz ve více VLAN současně, musí být port přepínače (se kterým je síťová karta PROXY serveru propojena) nastaven do režimu TRUNK. V tomto režimu je komunikace směrována na příslušnou podsíť VLAN 67 a 68 pomocí následujícího nastavení přepínače Cisco:

```
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 67-68
switchport mode trunk
```

Nastavení síťové karty na distibuci linuxu Debian vyžaduje instalaci balíku `vlan`. To se provede příkazem:

```
apt-get install vlan
```

PROXY server má síťovou kartu eth0, která je připojena do sítě CESNET2 (Internet) a síťovou kartu eth1 která je připojena do portu přepínače, který je nakonfigurován do režimu TRUNK pro VLAN 67 a 68. Nastavení síťové karty se provede konfigurací souboru `/etc/network/interfaces`.

```
auto vlan67
iface vlan67 inet static
   address 10.67.0.1
   netmask 255.255.248.0
   vlan_raw_device eth1
auto vlan68
iface vlan68 inet static
```

```
address 10.68.0.1
netmask 255.255.248.0
vlan_raw_device eth1
```

Zapnutí všech interfaces se provede příkazem:

```
ifup –a
```

7.11 Nastavení Firewallu PROXY serveru

Shorewall (Shoreline Firewall) je nástroj pro konfiguraci firewallu iptables [23]. Instalace se provádí na distribuci Debian pomocí příkazu: `apt-get install shorewall`.

V adresáři `/etc/shorewall/` je potřeba umístit konfigurační soubory, z nichž pro naše potřeby využijeme `maclist`, `zones`, `interfaces`, `masq`, `policy`, `rules`, `routestopped`.

Pro správnou funkci firewallu je třeba povolit forwardování paketů, které je v Debianu implicitně zakázáno. Provede se v souboru `/etc/sysctl.conf` pomocí parametru `net.ipv4.ip_forward=1`. Následně se provede aktivace pomocí příkazu `sysctl –p /etc/sysctl.conf`, který slouží pro konfiguraci prostředků běžícího jádra systému.

Soubor `maclist` obsahuje seznam IPadres, rozhraní a MAC adres, kterým povoluje provoz na firewallu. Nyní obsahuje navíc také IP adresy z rozsahu IP adres pro ubytované zaměstnance. Soubor je generován automaticky pomocí bash skriptu `generuj_zasuvky.sh` [10].

Příklad obsahu souboru `maclist`:

```
#DISPOSITION    INTERFACE  MAC                IP ADDRESSES
ACCEPT          vlan67     00:11:22:33:AA:BB  10.67.0.101
ACCEPT          vlan68     11:33:66:AA:CC:EE  10.68.0.101
```

Soubor `zones` definuje základní síťové zóny. Zóna `net` je určena pro Internet, `loc1` a `loc2` pro lokální sítě a `fw` pro firewall. Příklad konfigurace je následující:

```
#ZONE   TYPE
fw      firewall
net     ipv4
```

```
loc1    ipv4
loc2    ipv4
```

Dalším konfiguračním souborem je `interfaces`. Zde se definují jednotlivá síťová rozhraní a jejich příslušnost k zóně. Doplňky ve sloupečku OPTIONS: volba `tcpflags` nepovolí nestandardní navázání TCP spojení, volba `routefilter` kontroluje příchozí pakety, zda nemají pozměněnu zdrojovou IP adresu, volba `maclist` povolí spojení pouze adresám v souboru `maclist`. Příklad konfigurace:

```
#ZONE  INTERFACE  BROADCAST      OPTIONS
net    eth0       -              routefilter,tcpflags
loc1   vlan67     -              maclist
loc2   vlan68     -              maclist
```

V konfiguračním souboru `masq` se nastavuje maškaráda resp. překlad síťových adres NAT (Network Address Translation) [28], což je zjednodušeně skrývání vnitřních IP adres za IP adresu routeru, resp. PROXY serveru. Do prvního sloupečku se zadává síťové rozhraní připojené do Internetu a do druhého rozhraní vnitřní sítě:

```
#INTERFACE      SOURCE
eth0            vlan67
eth0            vlan68
```

Soubor `policy` definuje bezpečnostní síťovou politiku, obecně ze které zóny do které mohou pakety přecházet a pro příslušnou kombinaci sítí je uvedena akce (ACCEPT | DROP | REJECT). Příklad nastavení souboru `policy`:

```
#SOURCE    DEST       POLICY     LOG
loc1       net        ACCEPT
loc2       net        ACCEPT
$FW        net        ACCEPT
net        all        DROP
all        all        REJECT     info
```

Z uvedené konfigurace vyplývá, že z lokální sítě `loc1` a `loc2` a z `fw` (firewallu serveru) je povolena veškerá komunikace směrem do Internetu. Zahazována je nevyžádaná

komunikace z Internetu a zamítnuty jsou nevyžádané pakety ze všech zón (komunikace nepovolena). Parametr `info` znamená, že informace o dané akci jsou uloženy do syslogu.

V souboru `routestopped` je uvedeno síťové rozhraní `eth0`, které bude přístupné, pokud se nepodaří Shorewall z nějakého důvodu spustit.

Posledním souborem, který vyžaduje nastavení je soubor `rules`, kde se nastavují pravidla již pro konkrétní IP adresy, služby, porty apod. Podrobná nastavení včetně příkladů lze najít v [23], [24].

7.12 Hotelový PROXY-2 server

Hotelový PROXY-2 server je samostatný server, který bude zprostředkovávat hotelovým hostům přidělování IP adres a přístup na Internet prostřednictvím sítě externího ISP.

Jako operační systém byl zvolen GNU/LINUX distribuce Debian ve verzi 6.0 Squeeze. Server obsahuje dvě síťové karty, z nichž `eth0` je připojena do sítě externího ISP a druhá `eth1` je připojena do lokální VLAN 69, která je určena pro hotelové hosty.

Server bude poskytovat služby DHCP, DNS a NAT (Network Address Translation). Nastavení firewallu je obdobné, jako je popsáno v kapitole 7.11.

7.12.1 Nastavení DNS

Systém DNS umožňuje převod doménových jmen a IP adres. Jako caching DNS lze použít balíček `pdns_recursor` [29], který odpovídá na všechny DNS dotazy kromě autoritativních, neboť na PROXY-2 serveru nebudou žádné zónové záznamy. Instalace se provede příkazem:

```
apt-get install pdns_recursor
```

Po instalaci je třeba nastavit hodnoty parametrů v konfiguračním souboru `/etc/powerdns/recursor.conf`:

- `allow-from=10.69.0.0/22` – uvádí seznam sítí, které mají povoleno DNS používat
- `daemon=yes` – povolí běžet jako daemon
- `local-address=10.69.0.1` – adresa na které odpovídá na DNS dotazy
- `local-port=53` – port na kterém poslouchá, 53 je výchozí port pro DNS dotazy

7.12.2 Nastavení DHCP

Pro DHCP server je použit balíček `isc-dhcp-server` [25]. Instalace se provede příkazem: `apt-get install isc-dhcp-server`.

Konfigurace je uložena v souboru `/etc/dhcp/dhcpd.conf` a je zvolena následující:

```
36. option domain-name-servers 10.69.0.1, 195.178.88.66;
37. default-lease-time 3600;
38. max-lease-time 7200;
39. authoritative;
40. subnet 10.69.0.0 netmask 255.255.248.0 {
41.     range 10.69.1.1 10.69.7.250;
42.     option broadcast-address 10.69.7.255;
43.     option routers 10.69.0.1; }
```

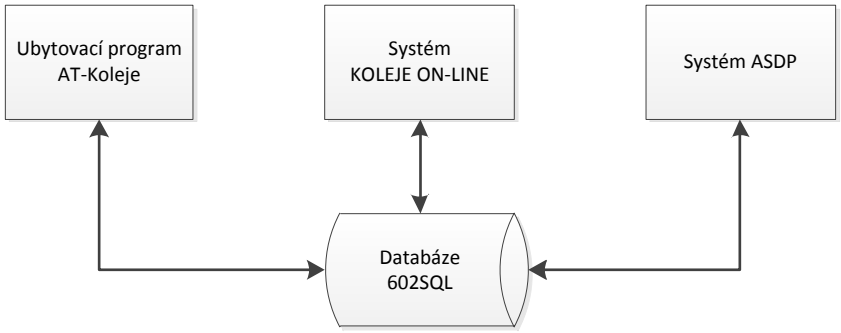
Řádek 36 definuje seznam DNS serverů. Řádek 37 implicitní dobu platnosti zapůjčené IP adresy a řádek 38 maximální dobu platnosti výpůjčky IP adresy. Řádkem 39 se označuje server jako autoritativní. Na řádku 40 začíná konfigurace DHCP pro příslušnou podsíť která je zde definována. Na řádku 41 se uvádí rozsah zapůjčovaných IP adres, na řádku 42 je uvedena broadcast adresa, na řádku 43 IP adresa směrovače.

Restart DHCP serveru se provede příkazem: `/etc/init.d/isc-dhcp-server restart`.

8 PROPOJENÍ S UBYTOVACÍM PROGRAMEM AT-KOLEJE

Předchozí verze systému ASDP umožňovala chod v oddělené databázi. Z několika důvodů, jako je např. pohodlí obsluhy a lepší propojení obou systémů, bylo uživatelské rozhraní pro ubytovatele integrováno přímo do ubytovacího programu AT-Koleje. Systém ASDP je v databázi stále možno odlišit tak, že všechny jeho součásti jako tabulky, SQL procedury, pohledy, formuláře a další součásti jsou umístěny ve vlastní složce nazvané `Internet`.

Centrálním zdrojem dat pro všechny subsystémy je databáze 602SQL (viz. *Obr. 13*).



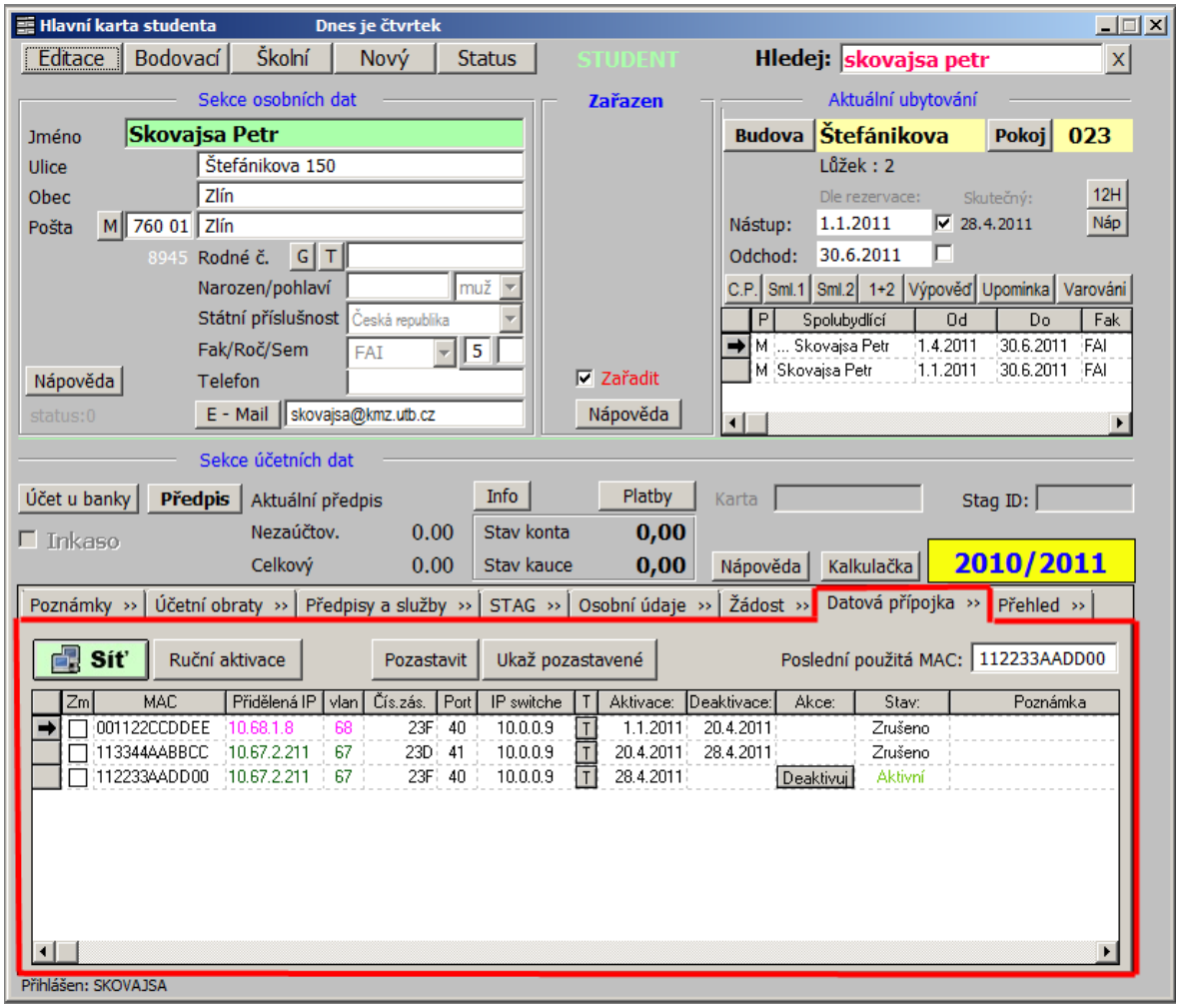
Obr. 13. Napojení systémů na databázi 602SQL

8.1 Inovace klientského prostředí ASDP v 602SQL pro ubytovatele

8.1.1 Správa datové přípojky na hlavní kartě klienta v programu AT-Koleje

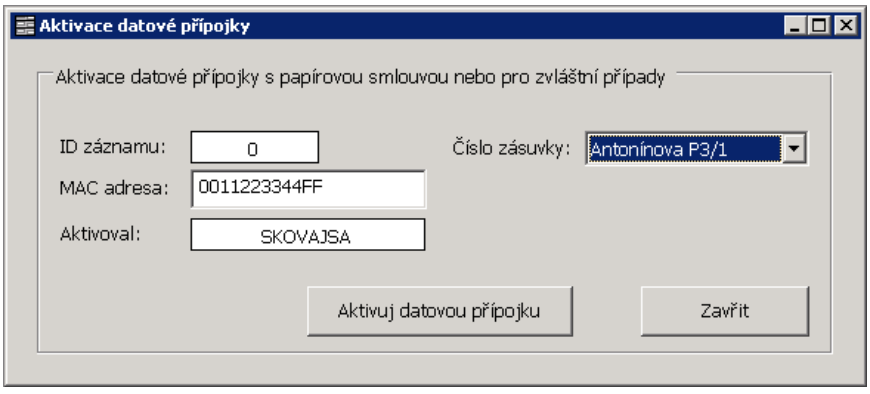
Formulář správy datové přípojky pro ubytovatele je umístěn na hlavní kartě klienta v ubytovacím programu AT-Koleje v záložkovém menu pod záložkou Datová přípojka (viz. *Obr. 14*) – příslušná sekce je orámována červenou barvou.

Zobrazené záznamy o aktivovaných přípojkách jsou vztaženy vždy k příslušnému klientovi, který je na hlavní kartě zobrazen. Zobrazuje se MAC adresa, přidělená IP adresa a číslo zásuvky. Pomocí tlačítka **T** může administrátor sítě provést okamžité připojení k aktivnímu prvku prostřednictvím protokolu SSH nebo TELNET. Další údaje jsou číslo portu a IP adresa přepínače, kde je klient připojen. Důležité je také datum aktivace a datum deaktivace. Sloupeček **Stav** informuje, zda je přípojka zrušena, pozastavena nebo aktivní. Tlačítkem **Deaktivuj** lze přípojku ručně deaktivovat. Deaktivace se pomocí tohoto tlačítka provádí při přestěhování na jiný pokoj, nebo při ukončení ubytování daného studenta či zaměstnance. Tlačítkem **Síť** lze otevřít kartu přehledu všech aktivních datových přípojek.



Obr. 14. Hlavní karta ubytovacího programu AT-Koleje se záložkou Datová přípojka

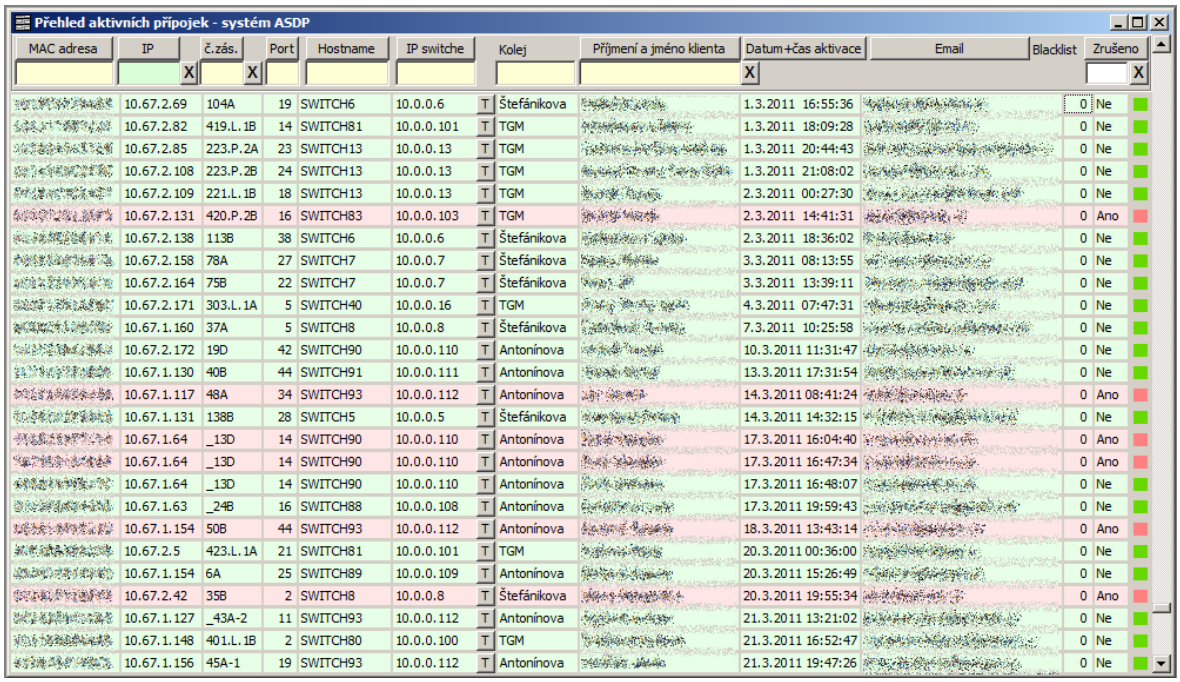
Nově přibylo tlačítko Ruční aktivace. Je dostupné pouze administrátorovi sítě a otevírá kartu aktivace datové přípojky (viz. *Obr. 15*). Ruční aktivace přípojky se používá u počítačů ve studovnách, které jsou také registrovány v systému ASDP, nebo pro případ uzavření papírové smlouvy. Uloženo je také jméno uživatele, který tuto akci provedl.



Obr. 15. Karta ruční aktivace datové přípojky pro speciální užití

8.1.2 Karta přehledu aktivních datových přípojek

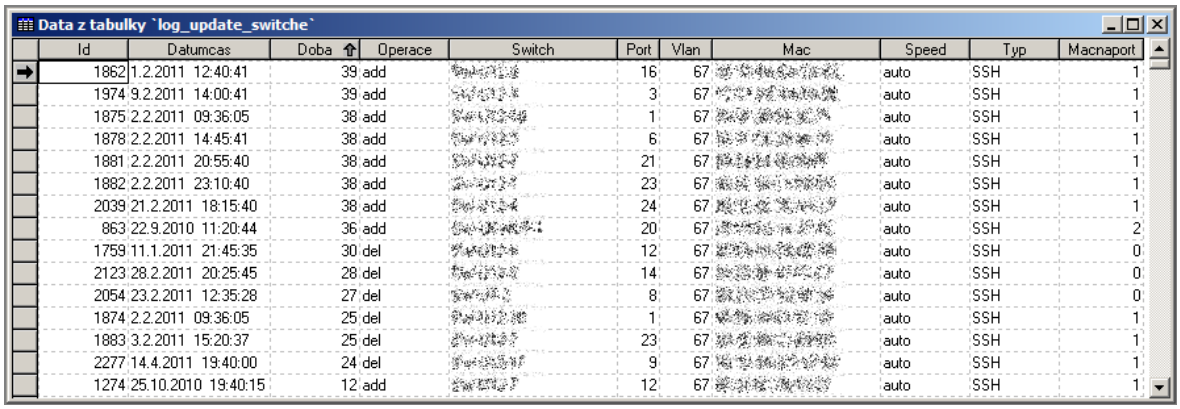
Tato karta slouží k přehledu a k vyhledávání datových přípojek podle MAC adresy, IP adresy a jména uživatelů, čísla zásuvky. Obsahuje dynamické filtrování a řazení dle příslušných sloupců. Karta zobrazuje záznamy z dotazu `int_vsechno` - zobrazuje všechny záznamy o aktivovaných přípojkách z tabulky `mac_adresy`. Jména a adresy jsou z bezpečnostních důvodů rozmazány, nebo pozměněny.



Obr. 16. Karta přehledu aktivních datových přípojek

8.1.3 Karta přehledu provedených aktivací

Karta zobrazuje přehled jednotlivých proběhlých aktivací datových přípojek se všemi parametry. Sloupce se dají řadit dvojklikem na jejich záhlaví. Karta zobrazuje data z tabulky `log_update_switche`.



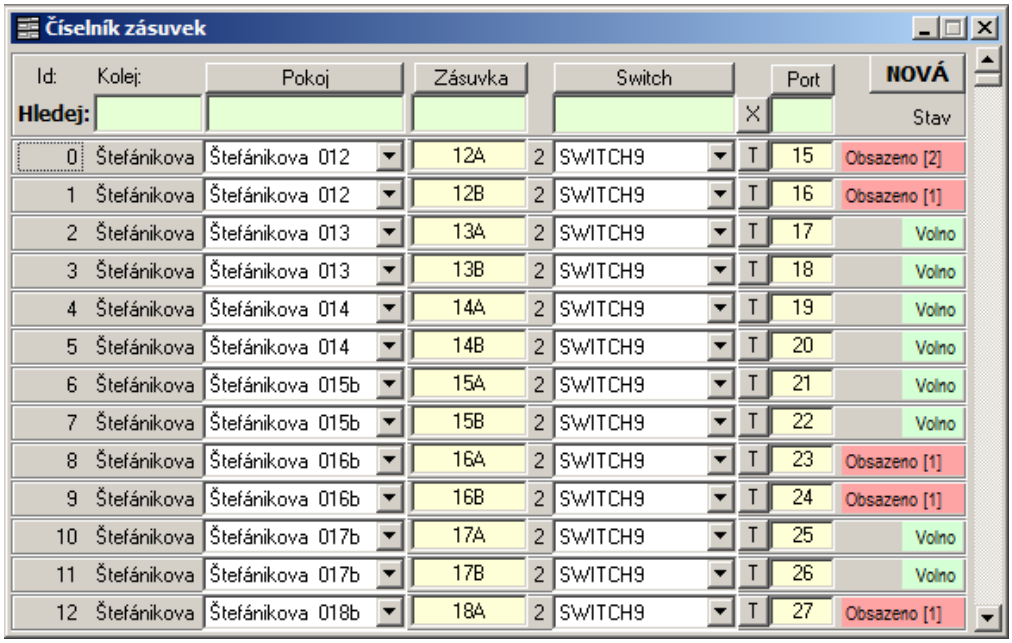
Obr. 17. Karta přehledu provedených aktivací

Z přehledu provedených aktivací lze zjistit, že za sledované období 8 měsíců (od srpna 2010 do března 2011) proběhlo celkem 2200 automatických konfigurací aktivních prvků. Z toho skripty trvající do 12 sekund lze hodnotit jako skripty úspěšně proběhlé, zatímco skripty s dobou trvání větší než 20 sekund lze hodnotit jako neproběhlé, či proběhlé s chybou. Takových bylo celkem 13 a tyto neproběhly převážně z důvodu výpadků napájení elektrické energie nebo vypršení časového limitu připojení na přepínač Cisco. Úspěšnost systému ASDP při automatické konfiguraci datových přípojek lze v rámci uvedeného období hodnotit na 99,45%.

Zpětnou vazbou je v současnosti manuální činnost administrátora, který kontroluje pravidelně kartu přehledu proběhlých aktivací. Tuto činnost by bylo možno převést na zpětnou vazbu tak, že datové přípojky, při jejichž konfiguraci byla detekována doba trvání skriptu > 20 sekund, by mohly být ihned zařazeny do dalšího zpracování. To však není zcela vhodné, neboť při dlouhodobějším výpadku by mohlo dojít ze strany klienta k dalším deaktivacím a aktivacím, což by mohlo způsobit zbytečnou kumulaci požadavků. Vhodné by bylo v takovém případě automatické odeslání informačního emailu přímo administrátorovi, který zkontroluje aktuální stav přípojky vůči databázi.

8.1.4 Karta číselníku datových zásuvek

Inovace karty spočívá v přidání sloupečku Stav, který informuje o tom, zda je zásuvka momentálně volná či obsazena.



Obr. 18. Číselník datových zásuvek

8.2 SW modul pro aktivaci Internetu hotelovému hostu

Při návrhu koncepce internetového připojení pro hotelové hosty bylo nutné posoudit stávající organizaci práce na recepcích VŠ kolejí UTB ve Zlíně.

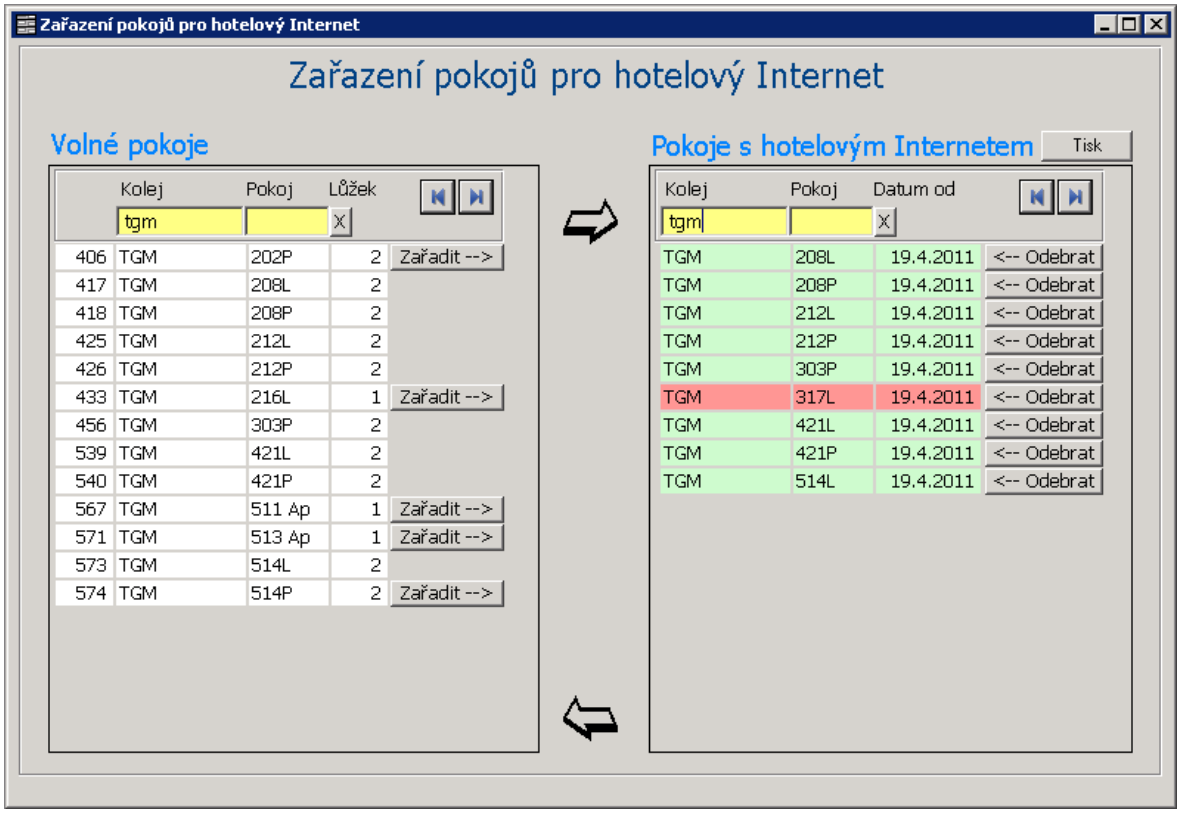
Rezervace hotelových hostů probíhají telefonicky nebo emailem a požadavky jsou evidovány ručně v ubytovacích knihách ubytovatelkou nebo recepční. Na recepcích není umístěn počítač a veškerá správa hotelového ubytování probíhá manuálně. Návrh umístění počítačů s ubytovacím programem na recepci byl vedením VŠ kolejí v současné době zamítnut. Důvodem je, že pracovníci recepce nejsou kmenoví zaměstnanci UTB ve Zlíně, ale zaměstnanci externí strážní služby.

Na základě uvedeného stavu nelze řídit aktivaci datové přípojky pro konkrétního hotelového hosta pomocí žádného ubytovacího software. Bylo tedy potřeba navrhnout způsob, jak zpřístupnit hotelovým hostům Internet bez využití ubytovacího programu, případně s jeho částečným využitím.

Jako nejjednodušší varianta se nabízí zařazení pokojů do hotelového provozu přímo ubytovatelem. Pokoje, které se uvolní z ubytování studentů, jsou v ubytovacím programu vedeny jako prázdné a obvykle jsou využívány pro hotelové ubytování. Zařazení pokoje by měl provádět ubytovatel, který spravuje studentské ubytování a zároveň plánuje využití pokojů pro hotelový provoz. Na takto označených pokojích by byly datové přípojky automaticky zapnuty a zařazeny do VLAN hotelové sítě. V takovém případě může hotelový Internet využít každý hotelový host.

Využita bude stávající infrastruktura datových rozvodů. Hotelovým hostům je možné po dobu pobytu zapůjčit na požádání (nebo za zálohu) síťový kabel RJ-45 na recepci příslušné VŠ koleje včetně jednoduchého návodu k připojení do sítě Internet.

8.2.1 Návrh formuláře pro zařazení pokoje do hotelového provozu



Obr. 19. Formulář pro zařazení pokojů pro hotelový Internet

Formulář je rozdělen na dvě části. V levé části se nachází přehled volných pokojů. Pomocí tlačítka **Zařadit** se provede zařazení pokoje do hotelového provozu. Pokud je pokoj již zařazen, tak se tlačítko **Zařadit** nezobrazuje. V pravé části formuláře je přehled pokojů, které jsou již do hotelového provozu zařazeny. Vyřazení se provede tlačítkem **Odebrat.** Vyřazený pokoj ze seznamu zmizí a opět se u něj v přehledu volných pokojů zobrazí tlačítko **Zařadit**. Pomocí tlačítka **Tisk** si ubytovatel může vytisknout seznam pokojů, které jsou zařazeny do hotelového provozu. Červeně jsou zvýrazněny pokoje, kde již probíhá jiné ubytování a ubytovatel by ho měl vyřadit z hotelového provozu.

Formulář je v databázi nazván `hpok` a obsahuje dva subformuláře `sub_hpok_nabidka` a `sub_hpok_nastavene`. Formuláře jsou napojeny na dotazy `pokoje_nabidka` a `pokoje_nastavene`. Oba vybírají data zejména sloučením dat z tabulky `c_tpok` a `pokoj_hotel`.

8.2.2 Automatické skripty pro správu datové sítě hotelových pokojů

Nastavení či odebrání pokojů pro hotelový Internet je aktivita, po které musí následovat automatické nastavení datových zásuvek. Pro tuto potřebu byl vytvořen databázový dotaz `proxy_hotel` se seznamem zásuvek, které jsou určeny ke konfiguraci pro hotelový provoz, nebo které je nutno zařadit zpět do defaultního nastavení registrační sítě. Řídícími sloupečky jsou sloupeček `zmena` a `zruseno`.

Po stisknutí tlačítka **Zařadit** se vloží do tabulky `pokoj_hotel` nový záznam s ID daného pokoje a hodnota `zmena` se nastaví na TRUE. Po stisknutí tlačítka **Odebrat** se u příslušného řádku tabulky `pokoj_hotel` nastaví hodnota `zmena=true` a `zruseno=true`.

- `zmena` - při hodnotě `true` uvádí, že příslušný záznam byl vytvořen či změněn
- `zruseno` - v případě hodnoty `false` se nastavuje port přepínače do hotelové VLAN, v případě `true` se nastavuje port přepínače zpět do registrační VLAN

Data z dotazu `proxy_hotel` zpracovává bash skript `generuj_hotel.sh`, spouštěný automaticky každou hodinu cronem na PROXY serveru. Pokud nenalezne žádné záznamy v dotazu `proxy_hotel`, ukončí svou činnost, v opačném případě provede automatické nastavení dle požadavků.

Potřebná data z dotazu `proxy_hotel` jsou shrnuta v sloupečku `seznam`, který obsahuje následující strukturu řádku:

```
ip_switche;name_switche;port;vlan;speed;pripojeni;operace
```

Uvedený řádek obsahuje parametry s konfigurací pro daný port na aktivním prvku. Skript provede tolik nastavení portů, kolik řádků bude dotazem `proxy_hotel` předáno. Provedené záznamy jsou po úspěšné akci potvrzeny zpět do databáze a to nastavením hodnoty `zmena=false` do příslušných řádků tabulky `pokoj_hotel`.

8.2.3 Další varianty

Navrženou variantu je možno chápat i jako dočasné řešení do doby, než budou na recepcích VŠ kolejí umístěny PC s ubytovacím programem. Softwarové vedení agendy hotelového ubytování následně umožní využití i jiných variant aktivace datové přípojky. Mezi ně může patřit např. možnost aktivace datové přípojky přímo z recepce konkrétnímu hotelovému hostu a tím i jeho jednoznačná identifikace.

9 PROPOJENÍ SYSTÉMU ASDP A SYSTÉMU FLOWMON

Propojení systému ASDP se systémem FlowMon spočívá v návrhu a realizaci rozhraní pro získávání statistik o počtu přenesených dat, jejich uložení do databáze a zobrazování v systému KOLEJE ON-LINE. Dále ve využití informací z databáze ASDP pro systém FlowMon. Součástí je také vytvoření automatických skriptů, které v případě překročení stanovených limitů sníží rychlost přípojky, nebo odešlou klientovi informační email.

9.1 Import statistik o počtu přenesených dat do databáze systému ASDP

Import statistik je spouštěn každý den v čase 00:15. Na PROXY serveru byl k tomu účelu vytvořen bash skript `stats_daily.sh`, který vykonává následující činnosti:

- Připraví strukturu parametru datum a čas pro `nfdump`
- Vzdáleně spustí program `nfdump` na kolektoru a vygeneruje statistiky
- Zkontroluje a uloží statistiky do databáze systému ASDP

Popis jednotlivých činností začíná popisem způsobu napojení na FlowMon kolektor.

9.1.1 Napojení na kolektor prostřednictvím protokolu SSH

Protokol SSH umožňuje terminálové připojení ke vzdálenému zařízení. Při přihlášení je vyžadováno uživatelské jméno a heslo. V našem případě je využit program OpenSSH. Abychom mohli proces napojení zjednodušit, nastavíme přihlášení bez hesla za pomoci privátního a veřejného přístupového klíče [18].

Nejprve zjistíme verzi OpenSSH na obou serverech (v případě že jsou nainstalovány):

```
ssh –v
```

Pokud čísla verzí neodpovídají, je vhodné verze sjednotit. Dále vygenerujeme klíče:

```
ssh-keygen –t rsa –b 4096
```

Klíče `id_rsa` a `id_rsa.pub` jsou uloženy do adresáře `/home/username/.ssh/`

Následně zkopírujeme veřejný klíč na vzdálený server (např. 10.0.0.2), server zatím ještě pořád vyžaduje zadání hesla:

```
ssh-copy-id –i /home/username/.ssh/id_rsa username@10.0.0.2
```

Provedeme test přihlášení, tentokrát již bez nutnosti zadání hesla:

```
ssh username@10.0.0.2
```

Na vzdáleném serveru by se měl ve složce `/home/username/.ssh` nacházet soubor s názvem `authorizer_keys`, jehož obsahem je veřejný klíč `id_rsa.pub`, který tam byl uvedeným způsobem přenesen.

9.1.2 Vzdálené spuštění příkazu nfdump + tvorba skriptu

Vygenerování statistik z kolektoru pomocí příkazu `nfdump` vyžaduje zadat přesně definovanou strukturu adresářů (viz. kapitola 4.5.1) a časový rozsah požadovaných dat. Pro tento účel je využit bash příkaz `date`.

Je-li potřeba generovat statistiku za předchozí den (od 00:00 do 24:00), připraví se proměnné `F_FROM` a `F_TO` s následujícími hodnotami:

```
F_FROM=`date '+%Y/%m/%d/nfcapd.%Y%m%d0000' --date='1 days ago'`
F_TO = `date '+%Y/%m/%d/nfcapd.%Y%m%d0000'`
```

Spuštění příkazu pro získání statistik z kolektoru bude vypadat např. následovně:

```
ssh username@10.0.0.2 nfdump -M /data/nfsen/
profiles-data/KMZ/koleje/upload-exclude-utb  -T  -R
$F_FROM:$F_TO -n 5000 -s srcip/bytes -o CSV > upload.tmp
```

Kde parametry:

`-M`	čtení z více adresářů
`-T`	použito časové okno
`-R`	rozsah od – do
`-n`	maximální počet záznamů
`-s`	požadovaná statistika (v uvedeném případě zdrojové adresy)
`-o`	výstupní formát dat

Pokud se zpracovává statistika pro download, mění se adresář z `upload-exclude-utb` na adresář `download-exclude-utb` a požadovaná statistika z `srcip/bytes` na `dstip/bytes`. Statistiky pro upload jsou ukládány do souboru `upload.tmp` a pro download do souboru `download.tmp`. S těmito soubory se dále pracuje.

9.1.3 Zpracování NetFlow dat a uložení do databáze

Data jsou z kolektoru vygenerována v následující CSV struktuře (Comma-Separated Values - hodnoty oddělené čárkami):

```
ts,te,td,pr,val,fl,flP,ipkt,ipktP,ibyt,ibytP,pps,pbs,bpp
```

Ze souborů `upload.tmp` a `download.tmp` nás zajímá pouze 5, 6, a 10 položka v řádcích, což je IP adresa, počet flows a počet přenesených dat. Položky jsou odděleny čárkou a lze je jednoduše separovat a uložit do souboru `upload.csv` pomocí příkazu:

```
cat upload.tmp | grep "-" | cut -d"," -f 5,6,10 > upload.csv
```

Podmínku `grep "-"` je třeba definovat tak, aby byly vybrány pouze řádky s definovanou strukturou. Čtením a zpracováním jednotlivých řádků souboru `upload.csv` lze následujícím postupem vygenerovat SQL skript `insert_db.sql`:

```
cat ./upload.csv | while read i;
do
  IP     =`echo ${i} | cut -d"," -f1`
  FLOWS  =`echo ${i} | cut -d"," -f2`
  UPLOAD =`echo ${i} | cut -d"," -f3`
  echo "INSERT INTO traffic (flows_u, upload, ip, datum)
      VALUES ($FLOWS,$UPLOAD,'$IP','$DATE')" >> insert_db.sql
done
```

Vygenerovaný SQL skript obsahuje na jednotlivých řádcích SQL příkazy a je odeslán do databáze prostřednictvím řádkového SQL klienta 602cli8:

```
cat ./insert_db.sql | 602cli8 -s server -l user -p heslo
-a aplikace -dm1 > /dev/null 2>&1
```

Uvedený příklad posílá do databáze statistiky pro upload. Pro odesílání download statistik je využito stejné konstrukce, avšak SQL příkaz neprovádí insert ale update již vložených záznamů k aktuálnímu dni.

9.1.4 Odeslání informačního emailu

V případě překročení stanovených datových limitů (viz. kapitola 3.2), je možno odeslat informační email s upozorněním. Emailové adresy jsou uloženy v databázi v tabulce `s_hlav` nebo `mac_adresy`.

Odeslání informačního emailu bude probíhat po importu denních statistik do databáze, tedy po akci popsané v předchozí kapitole. Využit je program `mail`, jehož syntaxe odeslání zprávy je uvedena na následujícím příkladu:

```
mail -a "From: koleje@utb.cz" -s "$PREDMET" "$EMAIL" < $ZPRAVA
```

Kde `$PREDMET`, `$EMAIL`, `$ZPRAVA` jsou vložené textové proměnné.

Příklad znění emailové zprávy:

> *Vážený uživateli,*
>
> *automatická kontrola datové sítě na VŠ kolejích detekovala dne **24.3.2011** výrazné zvýšení počtu přenesených dat z Vašeho počítače do sítě Internet – upload: **10 GB**.*
>
> *Pokoj (č. zásuvky): **100A***
>
> *MAC adresa: **00112233AAFF***
>
> *Tato vysoká hodnota může souviset např. s narušením zabezpečení Vašeho počítače, nebo využíváním služeb P2P sítí apod. Doporučujeme provést kontrolu PC, revizi nastavení P2P klienta nebo další kroky k prověření zabezpečení Vašeho PC.*
>
> *Doplňující informace:*
>
> - *V systému KOLEJE ON-LINE můžete v sekci **Datová přípojka → Statistika** sledovat počty přenesených dat Vašeho počítače.*
> - *Bezpečnost v síti**: https://koleje.utb.cz/kolejnet2.php?p=9**.*
> - *Pravidla datové sítě naleznete zde: **https://koleje.utb.cz/kolejnet2.php?p=5.***
> - *V případě dalších dotazů se můžete obrátit na email: koleje@kmz.utb.cz, nebo na tel. 57603 6119.*
>
> *Tato zpráva byla vygenerována automaticky.*

Pro samotné odeslání emailu byl vytvořen bash skript `posliemail.sh`. Je spuštěn na konci jiného bash skriptu s názvem `stats_daily.sh`, popsaného v předchozích kapitolách. Skript `posliemail.sh` vykonává tyto operace:

- Získá z databáze data s počtem přenesených dat upload, email, MAC adresu, číslo datové zásuvky a uloží si je do souboru `emaily.csv`.
- Na základě každého řádku souboru `emaily.csv` odešle informační email

Struktura CSV řádku je následující:

```
datum,upload,email,MAC,číslo_zásuvky
```

Email může být odesílán také administrátorovi sítě.

9.1.5 Zobrazení statistik v systému KOLEJE ON-LINE

Zobrazení statistik o datové přípojce je dostupné po přihlášení v systému KOLEJE ON-LINE v sekci **Datová přípojka → Statistika**. Červeným fontem jsou zvýrazněny hodnoty, které překračují hodnoty stanovené v pravidlech sítě.

Statistika datové přípojky

Číslo zásuvky	MAC adresa	IP adresa	Datum	Počet flows	Upload	Download	Stav	Akce/Info
413.P.2A	B8AC6F550DB4	10.67.2.189	27.4.2011	77411	2.26 GB	4.39 GB	Aktivní	-
			26.4.2011	86060	1.96 GB	9.47 GB		
			25.4.2011	307307	2.3 GB	5.99 GB		
			24.4.2011	79827	2.83 GB	337.8 MB		
			23.4.2011	40266	5.74 GB	737.2 MB		
			21.4.2011	28537	467.2 MB	129.1 MB		
			20.4.2011	70057	4.41 GB	277.4 MB		

Počet přenesených dat do Internetu za posledních 24 hodin - UPLOAD

10.67.2.189: 1.55 GB

Obr. 20. Zobrazení statistiky k datové přípojce

9.2 Export údajů do systému FlowMon a jejich zobrazování

9.2.1 Požadavky a analýza

Požadavkem je zobrazování detailních informací k neveřejným IP adresám v uživatelském rozhraní aplikace NFSEN (viz. kapitola 4.5.2), která je součástí FlowMon Monitoring Centra (viz. *Obr. 6*). Detailní informace z whois a lookup se zobrazí v pop-up okénku po kliknutí na požadovanou IP adresu.

Analýzou zdrojového kódu bylo zjištěno, že překlad IP adresy na doménové jméno a funkci whois obsluhuje PHP skript kolektoru `lookup.php`. Předání IP adresy probíhá HTTP (HyperText Transfer Protocol) metodou GET - hodnota i její název jsou předány webovému serveru jako součást URL (Uniform Resource Locator).

Např.:

```
http://localhost/nfsen/lookup.php?lookup=195.178.88.66
```

9.2.2 Návrh a vlastní úprava programu NFSEN

Návrhem byla možnost automaticky generovat reverzní záznamy IP adres pro univerzitní DNS server. Výsledkem by však bylo pouze získání názvu domény bez potřebných detailů.

Mnohem praktičtěji se jeví získání detailů k příslušné IP adrese přímo z databáze systému ASDP. Bylo potřeba navrhnout jednoduchý a nejméně invazivní způsob implementace do stávajícího kódu aplikace NFSEN na kolektoru FlowMon. Po dohodě se zástupci společnosti Invea-Tech a.s. byl zpřístupněn samostatný adresář s PHP skripty aplikace NFSEN pro účely vlastních úprav a ladění.

Detaily k neveřejné IP adrese budou obsahovat následující údaje: Jméno uživatele, budova, místnost či zásuvka, datum registrace a datum ukončení držení IP adresy, volitelně MAC, VLAN a email.

Způsob předání dat byl zvolen prostřednictvím systému KOLEJE ON-LINE a webové stránky, která vygeneruje požadované záznamy k příslušné IP adrese. IP adresa bude předána opět prostřednictvím HTTP metody GET za pomoci PHP skriptu. Skript byl pojmenován `show_ip_description.php`. Přístup je omezen pouze na požadavky z IP adresy FlowMon kolektoru, z jiných IP adres je skript nedostupný.

Způsob volání PHP skriptu na straně systému KOLEJE ON-LINE např.:

```
show_ip_description.php?ip=10.67.1.2
```

Vygenerovaný obsah je naformátován do tabulky.

Jméno:	Petr Skovajsa
Kolej a zásuvka:	Štefánikova, 23F
Email:	skovajsa@kmz.utb.cz
Datum (od-do):	12.9.2010 - dosud
MAC | VLAN:	001122334455 | 67
Jméno:	Předchozí uživatel
Kolej a zásuvka:	Antoninova, 43C
Email:	koleje@kmz.utb.cz
Datum (od-do):	7.9.2010 - 12.9.2010
MAC | VLAN:	001188AABBFF | 67

Obr. 21. Tabulka údajů k neveřejné IP adrese

K příslušné IP adrese může být vygenerováno více majitelů za období od zahájení akademického roku, neboť rezervace IP adres (viz. kapitola 7.4) byla implementována až v březnu 2011. Nový způsob neomezuje, ale výrazně snižuje u IP adres střídání majitelů.

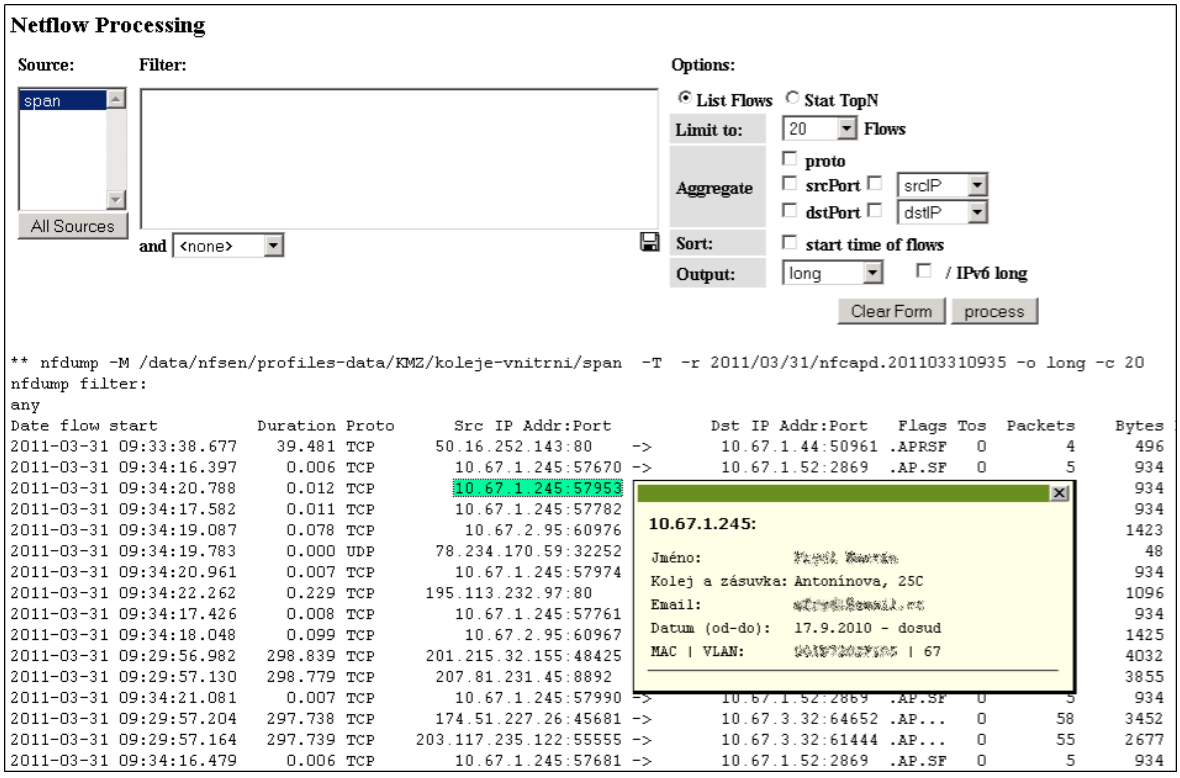
9.2.3 Implementace

Implementace je provedena následovně. Kliknutím na IP adresu v rozhraní aplikace NFSEN na FlowMon kolektoru se otevře pop-up okénko, které zobrazí obsah vygenerovaný PHP skriptem `lookup.php`.

Do skriptu `lookup.php` byl vložen následující PHP kód:

```
44. $utb_link="https://koleje.utb.cz/show_ip_description.php?ip=
    $lookup";
45. $HTTPRequest = @fopen($utb_link, 'r');
46. @stream_set_timeout($HTTPRequest, 6);
47. $utb_html = @fread($HTTPRequest, 32768);
48. @fclose($HTTPRequest);
49. echo $utb_html;
```

Tato část kódu pracuje na straně FlowMon kolektoru a vzdáleně si otevře webovou stránku systému KOLEJE ON-LINE definovanou v proměnné `$utb_link`. Do proměnné `$utb_html` si uloží celý obsah vygenerované stránky - tabulku (viz. *Obr. 21*) a tento obsah vloží pomocí příkazu `echo` přímo do pop-up okénka. Výsledek implementace je znázorněn na následujícím obrázku.



Obr. 22. Zobrazení detailů k neveřejné IP adrese v aplikaci NFSEN

Přínos realizovaného návrhu spočívá v tom, že hlavní administrátor sítě UTB a další pracovníci zabývající se bezpečnostními incidenty mají požadované informace k dispozici a není nutné je dohledávat v navazujících systémech. Výsledkem je tedy úspora práce při následném dohledávání.

9.3 Řízení rychlosti na PROXY serveru

Shorewall (Shoreline Firewall) nainstalovaný na PROXY serveru nabízí jednoduché řízení rychlosti pomocí definování maximální šířky pásma a zařazování paketů do tříd na základě IP adresy uživatele. Jelikož popis technologie traffic shaping přesahuje rámec této práce, budou zde popsány pouze nezbytné souvislosti. Podrobné informace a dokumentaci lze dohledat na www adrese: http://www.shorewall.net/traffic_shaping.htm.

V rámci této práce jsou využity konfigurační soubory **`tcdevices`**, **`tcclasses`** a **`tcrules`**, které se umístí do adresáře `/etc/shorewall/`, pokud nejsou přítomny, lze je najít (v Debianu) na cestě `/usr/share/doc/shorewall/default-config`.

Soubor `tcdevices` slouží pro definování příchozí a odchozí šířky pásma na konkrétním síťovém zařízení (resp. síťovém rozhraní), na němž má být zapnutý traffic shaping. V našem případě se jedná o síťové rozhraní `vlan67`, které je připojeno do studentské provozní sítě a síťové rozhraní `eth0`, které je připojeno do sítě CESNET2 (do Internetu).

9.3.1 Tcdevices

Konfigurace souboru **`tcdevices`** je následující:

```
#INTERFACE    IN-BANDWITH    OUT-BANDWIDTH    OPTIONS
eth0          1000mbit       1000mbit
vlan67        1000mbit       1000mbit
```

V uvedeném případě je nastavena maximální příchozí a odchozí rychlost 1 Gb/s na obě síťová rozhraní, což odpovídá rychlosti síťových karet na PROXY serveru.

9.3.2 Tcclasses

Dalším souborem, který je nutno nastavit, je soubor tříd **`tcclasses`**. Prostřednictvím tříd lze pásmo rozdělit v našem jednoduchém případě na rychlé a pomalé. Pro pomalé pásmo definujeme rychlost 1 Mbit/s (MARK 1) a pro rychlé pásmo 999 Mbit/s (MARK 2).

```
#INTERFACE:    MARK    RATE:      CEIL     PRIORITY    OPTIONS
eth0           1       1mbit      1mbit    2
eth0           2       999mbit    full     1           default
vlan67         1       1mbit      1mbit    2
vlan67         2       999mbit    full     1           default
```

RATE nastavuje minimální garantovanou šířku pásma.

CEIL nastavuje maximální možnou šířku pásma kterou lze využít.

V našem případě má RATE a CEIL stejnou hodnotu, to znamená, že datový provoz zařazený do MARK 1, se dělí o minimální stanovenou šířku pásma 1 Mbit/s.

PRIORITY – určuje prioritu třídy, nejvyšší priorita má nejnižší číslo. Pakety ve třídě s nejvyšší prioritou jsou zpracovávány nejdříve. Doplňující položka `default` ve sloupečku OPTION znamená, že veškerý další síťový provoz na daném rozhraní, který nebyl zařazen do některé ze tříd, bude zařazován do této třídy.

9.3.3 Tcrules

Posledním konfiguračním souborem je `tcrules`. Datový provoz definovaných IP adres bude zařazován do příslušného (v našem případě pomalého) pásma. Konfigurace souboru `tcrules` je následující:

```
#MARK    SOURCE          DEST            PROTO
1:F      10.67.0.11      0.0.0.0/0       all
1:F      0.0.0.0/0       10.67.0.11      all
```

Pro příklad je použita IP adresa 10.67.0.11. Veškerý odchozí datový provoz z příslušné IP adresy (první řádek) a veškerý příchozí datový provoz (druhý řádek) na tuto IP adresu bude zařazován do třídy MARK 1, písmeno F značí, že bude označován při forwardingu paketu.

9.3.4 Automatizované skripty pro řízení rychlosti

Dle pravidel stanovených v kapitole 3.2.2 byl vytvořen bash skript `stats_last24h.sh`, který je spouštěn každých 5 minut a získává statistické údaje z FlowMon kolektoru za uplynulých 24 hodin.

Skript vykonává následující činnosti:

- Připraví se struktura parametru datum a čas pro `nfdump`.

- Vzdáleně se spustí program `nfdump` na FlowMon kolektoru a vygenerují se statistiky o počtu přenesených dat.
- Vygeneruje se seznam IP adres, které překračují stanovený datový limit do souboru `tcrules`.
- Provede se restart Shorewallu.

Příklad kompletního skriptu je zde:

```
50. F_FROM=`date '+%Y/%m/%d/nfcapd.%Y%m%d%H00'
    --date='1 days ago'`
51. F_TO=`date '+%Y/%m/%d/nfcapd.%Y%m%d%H00'`
52. LIMIT=2147483648
53. ssh username@10.0.0.2 nfdump -M /data/nfsen/profiles-
    data/KMZ/koleje/upload-exclude-utb –T -R $F_FROM:$F_TO
    -n 5000 -s srcip/bytes -o CSV > upload24h.tmp
54. cat up24h.tmp | grep "-" | cut -d"," -f 5,6,10 > up24h.txt
55. cat ./up24h.txt | while read i;
56. do
57.    IP=`echo ${i} | cut -d"," -f1`
58.    FLOWS=`echo ${i} | cut -d"," -f2`
59.    UPLOAD=`echo ${i} | cut -d"," -f3`
60.    if [ "$UPLOAD" -gt "$LIMIT" ]
61.    then
62.       echo "1:F   $IP   0.0.0.0/0   all" >> tcrules.part2
63.       echo "1:F   0.0.0.0/0   $IP   all" >> tcrules.part2
64.    fi
65. done
66. cat tcrules.part1 tcrules.part2 > /etc/shorewall/tcrules
67. /etc/init.d/shorewall restart
```

Jednotlivé funkce byly popsány v kapitole 9.1.2. Použitá podmínková konstrukce `if - fi` porovnává hodnotu proměnné `$LIMIT` a `$UPLOAD` a parametr `-gt` znamená „je větší než“. V adresáři se nachází ještě soubor `tcrules.part1`, kde mohou být ručně zavedeny IP adresy pro dlouhodobé zařazení do některé z tříd. Oba soubory jsou spojeny pomocí příkazu `cat` do souboru `tcrules` a uloženy do adresáře s konfiguračními soubory. Shorewall je následně restartován.

Bash skript `stats_last24h.sh` tedy automaticky zajišťuje, že při překročení datového limitu odeslaných dat do sítě Internet bude příslušná IP adresa zařazena do pomalého pásma. V tomto pásmu setrvá tak dlouho, dokud bude počet odeslaných dat převyšovat stanovený limit, tedy dokud bude platná podmínka.

Skript byl původně spouštěn každou hodinu. Praktické testy však ukázaly potřebu častějšího spouštění, neboť v průběhu jedné hodiny byli schopni někteří uživatelé odeslat do sítě Internet i několik GB dat, a do doby, než došlo k vyhodnocení počtu odeslaných dat, byl limit překročen mnohonásobně. Spouštění probíhá nyní každých 5 minut v rámci bash skriptu konfigurace datové sítě `generuj_zasuvky.sh` na jeho začátku tak, aby se nejdříve provedly operace v bash skriptu `stats_last24h.sh` a následně v `generuj_zasuvky.sh`.

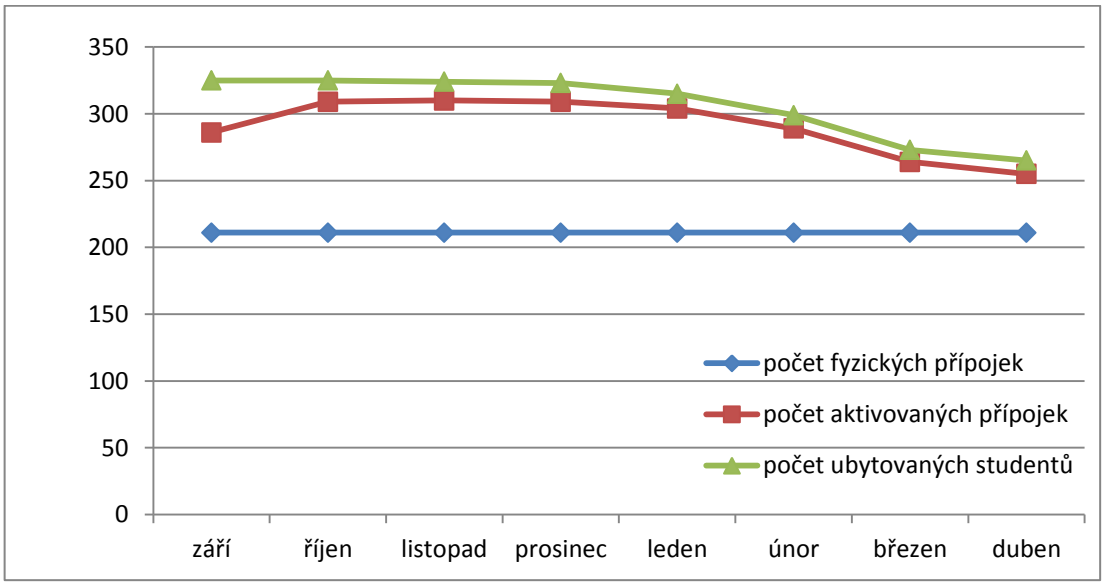
Dále byla zařazena kontrola, zda došlo k nějaké změně v seznamu IP adres zařazených do pomalého pásma. Pokud ke změnám došlo, je restartován Shorewall, pokud nedošlo, není třeba restartovat. Tím se zamezilo zbytečně častému restartování Shorewallu.

V případě potřeby lze u pomalého pásma jednoduše změnit rychlost, případně pomocí zařazování paketů do tříd směrovat přes toto pásmo jiný nežádoucí provoz.

10 INOVACE DATOVÉ SÍTĚ NA VŠ KOLEJI ANTONÍNOVA

Datová síť na VŠ koleji Antonínova je nejdéle provozovanou sítí, a jako jediná dosud neprošla rekonstrukcí. Výměna strukturované kabeláže byla sice naplánována, ale projekt byl vzhledem k návaznosti na rekonstrukci bytových jader odložen. Počet datových zásuvek na této VŠ koleji je nižší, než lůžková kapacita.

Počet studentských lůžek na VŠ koleji Antonínova je 328. Počet fyzických datových přípojek pro studenty je 211. Závislost registrovaných přípojek na počtu ubytovaných studentů zobrazuje následující graf za dobu od září 2010 do dubna 2011.



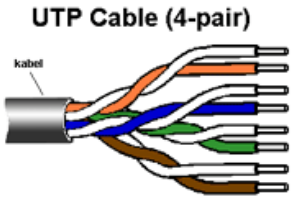
Obr. 23. Graf počtu aktivovaných a fyzických přípojek a počtu ubytovaných studentů

Aby se mohl k datové síti připojit každý ubytovaný student, byly vytvořeny tzv. virtuální datové zásuvky. Například na dvojlůžkovém pokoji je k dispozici jedna fyzická datová zásuvka s označením **2A** a ta je navázána na konkrétní port přepínače. Byla vytvořena virtuální datová zásuvka s označením **_2A**, která je navázána na stejný port přepínače. V praxi je tedy umožněno, aby se na jednu fyzickou přípojku mohli zaregistrovat dva uživatelé, tzn., že na příslušném portu přepínače je povolen provoz pro dvě MAC adresy. Samotné připojení na pokoji je pak realizováno prostřednictvím opakovače (tzv. HUB). Toto zařízení lze i s kabelem zapůjčit u ubytovatelky proti vratné záloze.

Tento způsob byl navržen jako dočasný a to do doby rekonstrukce sítě.

Vzhledem k tomu, že rekonstrukce datové sítě je v současnosti odložena na dobu neurčitou, nabízí se i další možnosti, jak s minimálními náklady navýšit počet fyzických zásuvek na pokojích.

Stávající strukturovaná kabeláž je typu UTP (Unshielded Twisted Pair) kategorie 5, což znamená provoz do rychlosti 100 Mbit/s a typ 100Base-TX. Při této rychlosti jsou pro datovou komunikaci využity 2 páry vodičů. Další 2 páry vodičů využity nejsou [20].



Obr. 24. UTP kabel

Tyto nevyužité vodiče pak lze využít jako přenosovou cestu pro druhou datovou zásuvku. V praxi se realizuje prostřednictvím rozdvojky.

Obr. 25. Rozdvojka 2x RJ45 UTP

Rozdvojky musí být dvě. První rozdvojka se umístí na vstupní straně, která je v RACKU (v rozvodné skříni datové sítě). Propojí se prostřednictvím RJ-45 datových kabelů se dvěma porty přepínače. Druhá rozdvojka se zapojí do příslušné datové zásuvky na pokoji a lze využít pro připojení dvou počítačů bez nutnosti použití HUBu.

Zapojení rozdvojek bude zkušebně realizováno v několika pokojích VŠ koleje Antonínova, aby se prakticky ověřila provozuschopnost z dlouhodobější perspektivy.

Po rekonstrukci datové sítě na VŠ kolejích Štefánikova zůstalo mnoho RJ-45 konektorů, ze kterých lze rozdvojky vyrobit, čímž by se opět uspořily vstupní náklady do doby plánované rekonstrukce. Rozhodnutí je na vedení VŠ kolejí a případné brigádnické činnosti ze strany ubytovaných studentů.

ZÁVĚR

Byl popsán současný stav správy datových přípojek a datové sítě a zpracován přehled pravidel ostatních VŠ kolejí v ČR, na jehož základě byly navrženy pravidla řízení rychlosti pro datovou síť na VŠ kolejích UTB.

Byl představen monitorovací systém FlowMon provozovaný na datové síti UTB ve Zlíně, jeho zapojení a účel. Navrženy byly možnosti jeho využití pro systém ASDP.

Dále byl krátce popsán databázový systém 602SQL, který je datovým úložištěm pro systém ASDP a ubytovací program AT-Koleje, jenž slouží pro správu ubytování na VŠ kolejích UTB ve Zlíně.

V praktické části byla navržena úprava databáze dle požadavků na rozšíření systému ASDP a řešily se jednotlivé dílčí inovace databázových SQL procedur, tabulek a dotazů. Způsob rezervace IP adres přidělovaných DHCP serverem prošel inovací tak, aby nedocházelo k jejich častému střídání u klientů. Webové rozhraní systému ASDP a programu AT-Koleje, které představuje systém KOLEJE ON-LINE, bylo inovováno o možnost přihlášení, aktivaci a deaktivaci datové přípojky ubytovaným zaměstnancům UTB a nově nabízí možnost stažení elektronické smlouvy ve formátu PDF, odeslání informačního emailu po aktivaci datové přípojky, nebo stránku se statistikou počtu přenesených dat. Byly také vyřešeny problémy, které se projevily v dosavadním provozu, tím je např. ochrana sítě proti nežádoucímu DHCP serveru, nebo opětovné zapnutí portu přepínače Cisco z chybového stavu.

Systém ASDP je kompletně implementován do ubytovacího programu AT-Koleje včetně grafického rozhraní pro ubytovatele a administrátora, které umožňuje deaktivaci, pozastavení a obnovení datové přípojky. Obnovení přípojky může být nově prováděno automatizovaným systémem a to v případě časového vypršení pozastavení přípojky. Systém ASDP je dále rozšířen o přímou správu účetního předpisu v ubytovacím programu, tj. automatické založení účetního předpisu při aktivaci a uzavření při deaktivaci přípojky. Byla přidána karta přehledu aktivních přípojek a karta provedených aktivací, která slouží pro zpětnou vazbu či kontrolu správnosti provedených konfigurací sítě. Inovací prošel také číselník datových zásuvek.

Způsob aktivace připojení k Internetu pro hotelové hosty byl vyřešen vytvořením uživatelského rozhraní v programu AT-Koleje pro zařazení volných pokojů do hotelového

provozu. Přípojky takto zařazených pokojů jsou následně automaticky přepnuty do sítě hotelového Internetu. Hotelový Internet bude poskytován prostřednictvím komerčního ISP, v souladu se Zásadami užití sítě CESNET2. Internet poskytovaný sdružením CESNET2 je využíván pro připojení ubytovaných studentů a zaměstnanců UTB.

Dalším úkolem bylo propojení systému ASDP s monitorovacím systémem FlowMon. Propojení systémů je obousměrné. Do databáze systému ASDP jsou importovány statistiky o počtu přenesených dat. Na základě těchto statistik se podle stanovených pravidel provádí řízení rychlosti datové přípojky tak, že datový provoz IP adres, které překročily stanovený limit, je zařazován do pomalého pásma.

Systém FlowMon poskytuje administrátorům prostřednictvím napojení na databázi systému ASDP možnost rychlého dohledání původců bezpečnostního incidentu bez nutnosti dohledávání relevantních údajů v podřízených systémech.

Dále byl představen technický návrh inovace datové sítě na VŠ koleji Antonínova. Aby se mohli kvůli nedostatku datových přípojek na pokojích připojit všichni uživatelé, byl realizován princip virtuálních zásuvek. Do uskutečnění realizace celkové rekonstrukce sítě je navrženo navýšení počtu přípojek prostřednictvím rozdvojek.

Výsledkem této práce je komplexní automatizovaný systém pro správu datových přípojek na VŠ kolejích UTB ve Zlíně. Systém se neustále rozvíjí a jeho inovace je v podstatě průběžná a popisem v této diplomové práci nekončí. Minimálně další dílčí inovace čeká systém v momentě, kdy bude hotelový provoz automatizován prostřednictvím ubytovacího programu a nebude spravován manuálně jako nyní. Systém lze obecně využít na kterýchkoliv VŠ kolejích či hotelech, které využívají uvedený SW pro správu ubytování a připojení uživatelů k síti je realizováno prostřednictvím konfigurovatelných aktivních prvků pomocí CLI. S příslušnými úpravami lze využít také jiný zdroj ubytovacích dat.

Systém pomáhá významně eliminovat činnosti spojené se správou sítě a účtováním, jak pro ubytované klienty, tak pro ubytovatele a administrátory sítě. Je provozován na VŠ kolejích UTB ve Zlíně.

Provedená inovace naznačuje další směry, kudy by se vývoj mohl ubírat. Nové cíle vznikají s novými výzvami, požadavky a změnami, a to nejen v legislativě vysokého školství v ČR, ale i v přístupu ke službám pro ubytované studenty, zaměstnance a hotelové hosty.

CONCLUSION

The current state of the data connection and data network management was described. An outline of the rules used by other university dormitories in Czech Republic was prepared, and based on them new set of rules for controlling the data network speed at TBU was recommended. The FlowMon monitoring system was introduced, including its application and purpose. Possibilities for its use in the automatic system for management of network connections (ASDP) system was suggested.

In addition, short overview of the 602SQL Database system was presented. The 602SQL serves as the data store for both the ASDP system and the accommodation software AT-Koleje, used by the TBU Zlin dormitory.

In practical part of the work, the changes to the database were prepared, as necessary in order to implement the ASDP extensions. The changes targeted both the SQL tables and the stored procedures and database queries. A method for reservation of IP addresses in the DHCP server was suggested so, that the addresses assigned to the individual clients don't change too often. The web interfaces of the ASDP and AT-Koleje systems (KOLEJE ON-LINE) was updated with the possibilities to register, activate and deactivate a data connection for the TBU employees accommodated, and now it also supports the possibility to download electronic version of the contract in PDF, sending email notification about the newly activated connection, and important statistics about the data amounts transferred. Problems, presented in the current system, were solved, such as protection against unwanted DHCP server, or error state recovery for the CISCO switch ports.

The ASDP system was integrated into the AT-Koleje system completely, including the user interface for administrators and quartermasters, allowing deactivation, temporary disconnection and reactivation of the data connection. The reconnection of the data point can now be done automatically when the temporary disconnect expires. The ASDP system was extended with direct support of accounting, that is automatic opening of accounting record when the data connection is activated and deactivated. A new tab with overview of all active connections was added, as well as a tab with list of all the activations done. The later one can be used to verify the network configuration. The index of the data connections was updated.

The Internet connection for the hotel guests was solved by creating new user interface in AT-Koleje, which allows to assign free rooms into the hotel system. Data connections

in such rooms are then automatically connected into the hotel Internet network. The hotel Internet connection will be provided by a commercial ISP, as required by the CESNET2 usage rules. Connection provided by CESNET2 itself will be used for connecting the accommodated students and TBU employees.

Another task was the connection between ASDP and the monitoring system FlowMon. The connection was implemented in both directions. Statistics about the data transferred is imported into the ASDP database. Based on the statistics and the usage rules the individual connection speed is then modified. IP addresses, which have passed their designated usage quote, are moved into a slow lane.

The FlowMon system, together with the ASDP integration, allows administrators to quickly locate originators of security incidents without having to search all the required information in each subsystem independently.

Further, a technical design for the Antoninova domitory network update was presented. Because the dormitory doesn't have sufficient amount of data points, a system of virtual sockets was used. Using the split adaptors is suggested as a way to increase the number of available network connections until the complete network reconstruction is realized.

An complex automatic system for the management of data connections in the TBU Zlin dormitories was implemented. The system is in continuous development and its updates don't end up in the state described in this master thesis. The hotel system used on the dormitories is about to be automated, and that will require another update of ASDP.

The system can be implemented in any dormitory, which is using the software mentioned, and where the data connection is realised using the active CLI configurable network elements. With more modifications, other sources of accommodation data can be integrated.

The systems substantially reduces the amount of tasks needed to handle during the network management and accounting, not only for the clients accommodated, but also for the quartermaster and the network administrators.

The updates, as implemented, suggest further possible development of the whole system. The new targets appear as new needs, requirements and modifications are formulated, not only in the legal system of the university education in Czech Republic, but by offering other services to the accommodated students, employees and hotel guests.

SEZNAM POUŽITÉ LITERATURY

[1] DOOLEY, Kevin – BROWN, Ian J. Cisco IOS Cookbook. 2nd ed. Sebastopol: O'REILLY, 2006. 1027 s. ISBN 978-0-596-52722-8.

[2] CONOLLY, Thomas – BEGG, Carolyn – HOLOWCZAK, Richard. Databáze – Profesionální průvodce tvorbou efektivních databází. 1. vyd. Brno: Computer Press, 2009. 584 s. ISBN 978-80-251-2328-7.

[3] KRETCHMAR, James – DOSTÁLEK, Libor – VESELSKÝ, Jiří. Administrace a diagnostika sítí - pomocí OpenSource utilit a nástrojů. 1 vyd. Brno: Computer Press, 2004. 584 s. ISBN 978-80-251-0345-5.

[4] RAINES, Paul. Tcl/Tk pocket reference. 1. vyd. Sebastopol: O'REILLY, 1998. 90 s. ISBN 1-56592-498-3.

[5] DOSTÁLEK, Libor – KABELOVÁ, Alena. Velký průvodce protokoly TCP/IP a systémem DNS. 1. vyd. Praha: Computer Press, 2000. 426 s. ISBN 978-80-7226-323-4.

[6] MATOUŠOVÁ, Miroslava – HEJLÍK, Ladislav. Osobní údaje a jejich ochrana. 2. vyd. Praha: ASPI, 2008. 468 s. ISBN 978-80-7357-322-5.

[7] SHAH, Steve – SOYINKA, Wale. Administrace systému LINUX – překlad čtvrtého vydání. 1. vyd. Praha: Grada Publishing, 2007. 428 s. ISBN 978-80-247-1694-7.

[8] FlowMon – Kompletní řešení pro monitorování sítí na bázi NetFlow – INVEA-TECH [online]. [cit. 2011-04-04]. URL: <http://www.invea.cz/produkty-sluzby/flowmon>.

[9] AT-Koleje – Mgr. Karel Pečenka [online]. [cit. 2011-04-04]. URL: <http://karel.pecenka.sweb.cz/koleje.html>.

[10] SKOVAJSA, Petr. Návrh a realizace automatizovaného systému pro správu datových přípojek na pokojích studentů VŠ kolejí UTB ve Zlíně. Zlín, 2009. 78 s. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky.

[11] Zařízení v síti pod kontrolou – Samuraj-cz.com [online]. [cit. 2011-04-04]. URL: <http://www.samuraj-cz.com/clanek/zarizeni-v-siti-pod-kontrolou>.

[12] Netflow – Wikipedie [online]. [cit. 2011-04-04].
URL: <http://cs.wikipedia.org/wiki/Netflow>.

[13] Koleje a menza Zlín – základní informace [online]. [cit. 2011-04-04].
URL: <http://web.kmz.utb.cz/?id=0_0&lang=cs&type=0>.

[14] CESNET2: Zásady pro přístup do sítě národního výzkumu a vzdělávání [online]. [cit. 2011-04-04]. URL: <http://www.cesnet.cz/doc/podminky.html>.

[15] NFDUMP [online]. [cit. 2011-04-04]. URL: <http://nfdump.sourceforge.net>.

[16] Man in the middle – Wikipedie [online]. [cit. 2011-04-04].
URL: <http://cs.wikipedia.org/wiki/Man_in_the_middle>.

[17] Dokumentace systému 602SQL [online]. [cit. 2011-03-04].
URL: <http://www.software602.cz/datainc/winbase/wb81/napoveda>.

[18] SSH your Debian servers without password [online]. [cit. 2011-04-05]. URL: <http://www.debianadmin.com/ssh-your-debian-servers-without-password.html>.

[19] 602SQL Server - Wikipedie [online]. [cit. 2011-05-02].
URL: < http://cs.wikipedia.org/wiki/602SQL_Server>.

[20] Ethernet – Wikipedie [online]. [cit. 2011-04-04].
URL: <http://cs.wikipedia.org/wiki/Ethernet>.

[21] Inbound Rate Limiting on Cisco Catalyst Switches – Slaptijack.com [online]. [cit. 2011-04-04]. URL: <http://slaptijack.com/networking/inbound-rate-limiting-on-cisco-catalyst-switches>.

[22] KOLEJE ON-LINE – Online správa ubytování UTB [online]. [cit. 2011-04-19].
URL: <https://koleje.utb.cz>.

[23] Shoreline Firewall – Shorewall Documentation [online]. [cit. 2011-04-15].
URL: <http://www.shorewall.net>.

[24] Shorewall, 1. díl – Linux Expres [online]. [cit. 2011-04-08].
URL: <http://www.linuxexpres.cz/praxe/shorewall-1-dil-1>.

[25] ISC DHCP Documentation & FAQ – Internet Systems Consortium [online]. [cit. 2011-04-04]. URL: <http://www.isc.org/software/dhcp/documentation>.

[26] FPDF Library – PDF generator [online]. [cit. 2011-04-16].
URL: <http://www.fpdf.org>.

[27] Jak změnit parametr jádra za chodu systému [online]. [cit. 2011-04-19]. URL: <http://www.phil.muni.cz/~letty/linuxfaq/25-proc-sys.html>.

[28] Network address translation – Wikipedie [online]. [cit. 2011-04-20]. URL: <http://cs.wikipedia.org/wiki/Network_address_translation>.

[29] PowerDNS – Agaton.cz [online]. [cit. 2011-04-22]. URL: <http://www.agaton.cz/index.php/linux/powerdns>.

[30] Dynamic Host Configuration Protocol - Wikipedie [online]. [cit. 2011-05-08]. URL: <http://cs.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ANSI/ISO	American National Standards Institute
ASDP	Automatizovaná Správa Datových Přípojek
BSD	Berkeley Software Distribution
CESNET2	Czech Education and Scientific NETwork 2
CLI	Command Line Interface
CSV	Comma-Separated Values (hodnoty oddělené čárkami)
ČR	Česká republika
DDOS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
GNU	General Public Licence
GUI	Graphical User Interface
HTTP	HyperText Transfer Protocol
ID	IDentifikátor
IOS	Internetwork Operating System (Cisco)
ISO	International Organization for Standardization
ISP	Internet Service Provider
MAC	Medium Access Control
MLS QOS	Multi-Layer Switching Quality Of Service
NAT	Network Address Translation
P2P	Peer To Peer
PDF	Portable Document Format
PHP	Hypertext Preprocessor
SMTP	Simple Mail Transfer Protocol

SNMP	Simple Network Management Protocol
SPAN	Switched Port Analyzer
SQL	Structured Query Language
SSH	Secure SHell
TCP/IP	Transmission Control Protocol / Internet Protocol
Telnet	Telecommunication Network - protokol
TGM	Vysokoškolská kolej nám. T. G. Masaryka
UDP	User Datagram Protocol
URL	Uniform Resource Locator
UTB	Univerzita Tomáše Bati
UTP	Unshielded Twisted Pair
VLAN	Virtual Local Area Network
VŠ	Vysokoškolské
VVŠ	Veřejná Vysoká Škola

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PI: Disk CD s programy a diplomovou prací v PDF.