PŘÍRODOVĚDECKÁ FAKULTA UNIVERZITY PALACKÉHO
KATEDRA INFORMATIKY

BAKALÁŘSKÁ PRÁCE

Systém pro monitorování počítačové sítě

2011 Maroš Gemzický

Anotace

Systém pre monitorovanie počítačovej siete monitoruje linkovú vrstvu referenčného modelu ISO/OSI v rozsahu detekcia prepínačov, ich prepojení, blokovaných portov a sieťovú vrstvu referenčného modelu ISO/OSI v rozsahu detekcia smerovačov a brán. Pomocou oboch vrstiev vytvára a udržuje zoznam aktívnych IP adries a k nim náležiacich MAC adries slúžiaci pri dohľadávaní koncových staníc v prípade rôznych problémov, najčastejšie sťažností tretích strán na porušovanie autorských zákonov. Monitor linkovej a sieťovej vrstvy počítačovej siete Univerzity Palackého v Olomouci je v niektorých technických detailoch prispôsobený súčasnému stavu počítačovej siete UP.

Ďakujem vedúcemu práce Mgr. Jan Outratovi, Ph.D. a konzultantovi Mgr. Petr Volákovi za ich čas, pomoc a cenné pripomienky.

Obsah

1. Úvod **7**

2. Popis riešenia **8**
2.1. Získanie, spracovanie a uloženie dát 8
2.2. Zobrazenie, úprava a vyhľadávanie 8

3. Porovnanie s 3Com Network Director **10**

4. Použité technológie **11**
4.1. Získanie, spracovanie a uloženie dát 11
4.1.1. SNMP protokol 11
4.1.2. SNMPv1 12
4.1.3. SNMPv2, SNMPv2c a SNMPv2u 12
4.1.4. SNMPv3 12
4.2. Zobrazenie, úprava a vyhľadávanie 13

5. Počítačové siete Univerzity Palackého v Olomouci **14**
5.1. Počítačové siete fakúlt a univerzitných zariadení 14
5.2. KolejNET 14

6. Detaily riešenia **15**
6.1. Získanie, spracovanie a uloženie dát 15
6.1.1. História IP a MAC adries 18
6.2. Zobrazenie, úprava a vyhľadávanie 19
6.2.1. Modelové situácie vyhľadávania 27

7. Inštalácia **28**
7.1. Inštalácia časti pre získanie, spracovanie a uloženie dát 28
7.2. Inštalácia časti pre zobrazenie, úpravu a vyhľadávanie 28

Závěr **29**

Conclusions **30**

Reference **31**

A. Obsah priloženého DVD **32**

Seznam obrázků

1. Ukážka úvodnej stránky aplikácie. 20
2. Ukážka mapy prepínačov. 21
3. Ukážka nezoskupenej mapy prepínačov. 22
4. Ukážka ručne zoskupenej mapy prepínačov. 22
5. Ukážka skupín aktívnych prvkov. 23
6. Ukážka okna blokovaných portov. 23
7. Ukážka zoznamu prepínačov s oknom detailov. 24
8. Ukážka vyhľadávacích formulárov s výsledkom vyhľadávania koncovej stanice podľa IP adresy. 25

Seznam tabulek

1. Porovnanie vlastností komerčného produktu a aplikácie UPOL L2/L3 monitor. 10

1. Úvod

Monitor linkovej a sieťovej vrstvy Univerzity Palackého v Olomouci (skrátene **UPOL L2/L3 monitor**) vznikol z potreby nahradiť zastaraný software 3Com Network Director a uľahčiť prácu správcom sietí, najmä vyhľadávanie v histórii IP a MAC adries a sledovanie stavu jednotlivých častí metropolitnej siete UP.

Aktívne využívam software 3Com Network Director na jednom z pomocných serverov KolejNET-u. V začiatkoch KolejNET-u, kedy sme ešte nemali dostatok vedomostí a skúseností, bol prínos tohto softwaru neoceniteľný. Časom mi však začali vadiť jeho nedostatky – hlavne nutnosť po každom reštarte servera prihlásiť sa, spustiť software, vybrať potrebnú mapu, ručne usporiadať jednotlivé skupiny a hlavne dávať si pozor, aby som sa od vzdialenej plochy len odpojil a neodhlásil. Samozrejme kolegovia sa niekoľkokrát odhlásili a chvíľu im trvalo pochopiť, že to nie je klient-server aplikácia. Po každej zmene konfigurácie siete (napr. výmena aktívneho prvku alebo zmena prepojení) som vždy musel ručne vyvolať zistenie stavu siete a zaradiť prípadné nové aktívne prvky do správnych skupín. Tak isto mi vadila absencia akéhokoľvek riadenia prístupu. Zastaranosť softwaru je jediný dôvod, prečo nemôžem preinštalovať daný server. Inštalácia a aktivácia softwaru je značne komplikovaná bez akejkoľvek možnosti zazálohovať licenčné údaje, takže po konzultácii s dodávateľom softwaru som to vzdal – údajne pôvodné sériové číslo sa preniesť nedá a nové už nedostanem, keďže sa produkt nepredáva.

Nástupca softwaru, neskôr spomínaný HP Intelligent Management Center, je modulárny a hlavne značne zložitý. Iné riešenia napr. od firmy Microsoft z rodiny System Center sa buď snažia obsiahnuť podstatne viac ako správu linkovej a sieťovej vrstvy referenčného modelu ISO/OSI, alebo správu týchto vrstiev majú len ako vedľajšiu vlastnosť.

Z týchto dôvodov som sa rozhodol vytvoriť aplikáciu, ktorá splní všetky moje požiadavky. Určite budem chcieť pokračovať v rozširovaní možností mojej aplikácie, či už pre moju vlastnú potrebu, alebo na základe podnetov od ostatných užívateľov.

2. Popis riešenia

Aplikácia UPOL L2/L3 monitor je riešená ako aplikácia typu klient-server. Kládol som veľký dôraz na obecnosť celej aplikácie a možnosť použiť aplikáciu na ľubovoľnú rozľahlú sieť typu MAN až WAN s čo možno najmenšími úpravami. Preto sú neštandardné konfigurácie špecifické pre počítačovú sieť Univerzity Palackého v Olomouci ošetrené na minimálnom počte miest kódu, na ktoré poukážem ďalej v práci. Serverová časť zahŕňa získanie, spracovanie a uloženie dát, klientská časť poskytuje zobrazenie, úpravu a vyhľadávanie vybraných dát.

2.1. Získanie, spracovanie a uloženie dát

V počítačovej sieti aplikácia UPOL L2/L3 monitor monitoruje aktívne prvky smerovače a prepínače. Pri prvom prieskume siete aplikácia určí adresné rozsahy, v ktorých bude ďalej vyhľadávať aktívne prvky. Vyhľadávanie začína získaním potrebných údajov od všetkých smerovačov. Následne aplikácia vyhľadá všetky prepínače a získa o nich obdobné údaje. Pre zaistenie správnej funkcie v heterogénnej sieti aplikácia vytvorí a udržuje ďalšie detaily ohľadom prepínačov. Týmto je ukončený prieskum siete, čo sa týka identifikácie jednotlivých aktívnych prvkov. V ďalšom kroku aplikácia získa od smerovačov arp tabuľky obsahujúce dvojice IP adresa a MAC adresa a od prepínačov mac tabuľky s dvojicami MAC adresa a označenie portu. Toto sú všetky potrebné údaje pre správnu detekciu vzájomných prepojení prepínačov. Pre efektívnu správu tak rozsiahlych sietí, pre ktoré je táto aplikácia určená, je vhodné poznať aj aktuálny stav funkčných a blokovaných portov jednotlivých prepínačov. Nakoniec aplikácia zo získaných dát vytvorí a naďalej udržuje zoznam koncových staníc siete. Celý proces sa cyklicky opakuje s tým, že málo často predpokladané zmeny sú detekované v dlhších intervaloch v porovnaní s hlavnou úlohou aplikácie – vytváraním a udržiavaním histórie koncových staníc siete.

2.2. Zobrazenie, úprava a vyhľadávanie

Výstup aplikácie UPOL L2/L3 monitor tvorí zobrazenie a vyhľadávanie dát – najmä v histórii IP a MAC adries koncových staníc. Ako rozhranie pre prístup do aplikácie som zvolil webové rozhranie z dôvodu jednoduchosti, nenáročnosti na užívateľa a jeho softwarovú výbavu, prehľadnosti a bezproblémovým aktualizáciám. Prihlasovacie údaje do webovej časti sú pre zvýšenie užívateľského komfortu zhodné s prihlasovacími údajmi do Univerzitného informačného systému. Prihlásením vopred definovaný užívateľ získa oprávnenia adekvátne pre jeho prácu. Ako úvodnú informáciu užívateľ dostane zoznam aktuálne problematických prepínačov. Ďalej má možnosť prezerať dynamickú mapu prepínačov, prepínače zaradené do skupín podľa podsietí a zoznam smerovačov a brán. Zoznam blokovaných portov a potenciálne problematických portov jednotlivých prepínačov zoskupených

podľa podsietí slúži k rýchlej diagnostike stavu siete a jej podsietí. Zoznam smerovačov a brán je prakticky len informatívny – ich správu aplikácia z bezpečnostných dôvodov neumožňuje. Aktívne prvky, ktoré neodpovedali v danom intervale, sú pre lepšiu orientáciu farebne odlíšené. Najdôležitejšiu časť aplikácie tvorí vyhľadávanie v histórii IP a MAC adries. Toto je prakticky použiteľné pre pohodlné dohľadanie problematickej koncovej stanice, prípade forenzné dohľadanie podľa prepínača a portu (ekvivalent fyzickej zásuvky). Aktivity jednotlivých užívateľov aplikácia zaznamenáva a môžu poslúžiť kontrole a eliminácii prípadných kompetenčných konfliktov.

3. Porovnanie s 3Com Network Director

V súčasnosti používaný software 3Com Network Director má niektoré nevhodné vlastnosti, z ktorých hlavné nedostatky sú prehľadne zhrnuté v nasledujúcej tabuľke.

	Software	
Vlastnosť	**3Com Network Director**	**UPOL L2/L3 monitor**
klient-server	**-**	+
spustenie po štarte OS	**ručne**	**automaticky**
viacužívateľský prístup	**-**	**viacúrovňový**
zabezpečenie	**-**	**OpenSSL**
aktualizácia stavu	**ručne**	**automaticky**
zoskupovanie zariadení	**ručne**	**automaticky**
záchyt SNMP trap	+	**neimplementovaný**
stav softwaru	**zastaraný**	**aktívny vývoj**

Tabulka 1. Porovnanie vlastností komerčného produktu a aplikácie UPOL L2/L3 monitor.

Software 3Com Network Director je nahradený komerčným modulárnym produktom HP Intelligent Management Center, ktorý rieši mnohé z vyššie uvedených problémov, ale ktorý nemám k dispozícii.

4. Použité technológie

Použité technológie sa líšia pre obe vyššie uvedené časti. Spojením oboch častí je len databázový server.

Ako RDBMS (relational database management system) som zvolil MySQL, pretože je to jeden z popredných voľne šíriteľných databázových serverov a mám s ním pozitívne skúsenosti. Účet pre prístup do databázy má len nevyhnutné oprávnenia.

4.1. Získanie, spracovanie a uloženie dát

Samotné získavanie, spracovávanie a ukladanie údajov riešim shell skriptovaním na serveri s operačným systémom Slackware Linux 13.37. Zvolil som predvolený shell Bash vo verzii 4.1.010 spolu s utilitami z Coreutils 8.11 a ďalšími programami ako kompromis prehľadnosti a výkonu. Porovnával som celkové vyťaženie a potrebný čas na spracovanie jednotlivých operácii s reťazcami pomocou integrovaných možností Bash shellu a programov gawk, sed, grep, tr, cut a volil podľa možností najvhodnejší postup alebo kombináciu.

Pre získavanie potrebných údajov z aktívnych prvkov som použil protokol SNMP.

4.1.1. SNMP protokol

Protokol SNMP (simple network management protocol) je protokol typu klient-server aplikačnej vrstvy referenčného modelu ISO/OSI. Samotný protokol SNMP nedefinuje, ktoré údaje má zariadenie poskytovať – toto rieši MIB (management information base). Na strane servera poskytuje vybrané údaje agent, ku ktorým pristupuje klient – manager. Agent očakáva požiadavky na UDP porte 161. Agent môže posielať správy bez vyžiadania (napr. upozornenia na prekročenie parametru alebo na kritickú udalosť). Tieto správy sa volajú SNMP Traps alebo InformRequests a manager ich očakáva na UDP porte 162. Rozdiel medzi Trap a InformRequest je ten, že na InformRequest manager odpovedá potvrdením o doručení. Keďže zariadenie väčšinou podporuje definovať len jednu IP adresu managera, ktorému bude tieto správy posielať a to si nastavuje stále používaný 3Com Network Director, túto možnosť zatiaľ nevyužívam.

Postupne vznikli tri hlavné verzie SNMP protokolu:

- verzia 1
- verzia 2
  - verzia 2c
  - verzia 2u
- verzia 3

4.1.2. SNMPv1

SNMP protokol verzie 1 je prvý štandard protokolu SNMP, ktorý bol najskôr definovaný:
RFC 1065 – Structure and identification of management information for TCP/IP-based internets
RFC 1066 – Management information base for network management of TCP/IP-based internets
RFC 1067 – A simple network management protocol

Neskôr boli nahradené: RFC 1155, RFC 1156 – MIB-1 a RFC 1157.
MIB-1 bol zakrátko nahradený RFC 1213 – Version 2 of management information base (MIB-2) for network management of TCP/IP-based internets.

Túto verziu protokolu SNMP využívam v mojej aplikácii, pretože niektoré aktívne prvky vyššiu verziu nepodporujú a pre potreby mojej práce plne postačuje.

4.1.3. SNMPv2, SNMPv2c a SNMPv2u

Kvôli nízkej (prakticky žiadnej) úrovni zabezpečenia SNMPv1 vznikla verzia 2 (RFC 1441 až RFC 1452), ktorá ale ako príliš komplexná nebola akceptovaná. Preto vznikla verzia SNMPv2c – Community-Based Simple Network Management Protocol version 2 (RFC 1901 až RFC 1908), ktorá prináša nové vlastnosti SNMPv2 okrem zabezpečenia – zachováva jednoduchý model zabezpečenia SNMPv1. Aj keď nie je SNMPv2c oficiálny štandard, je považovaný za de facto štandard.
Ako kompromis vznikla verzia SNMPv2u – User-Based Simple Network Management Protocol version 2 (RFC 1909 a RFC 1910), ktorá prináša vyššiu bezpečnosť v porovnaní s SNMPv1.

4.1.4. SNMPv3

Verzia 3 (RFC 3411 až RFC 3418) pridáva hlavne zabezpečenie rôznej úrovne a vylepšenia vzdialenej konfigurácie.

Dáta pre potreby SNMP protokolu sú uložené v stromovej štruktúre, v ktorej sú dve možnosti navigácie:

- MIB-module – management information base module
- OID – object identifier

Veľmi zjednodušene sa dá MIB (správne MIB-module) považovať za DNS pre OID, tzn. MIB pomenováva jednotlivé skupiny OID.

4.2. Zobrazenie, úprava a vyhľadávanie

Užívateľský prístup zabezpečuje webserver Apache HTTP Server 2.2.19 spoločne s PHP 5.3.6. HTML kód je validovaný ako HTML 4.01, CSS ako 2.1. Funkcionalitu na strane klienta zaisťuje JavaScript.

Pre zobrazenie väčšieho množstva dát som použil namiesto grafického výstupu vnorené tabuľky s možnosťou rozbaliť a zabaliť jednotlivé časti na strane užívateľa, tzn. bez nutnosti znovunačítania stránky. Pre toto nie príliš oslnivé riešenie som sa rozhodol kvôli prehľadnosti, vyhnutiu sa nutnosti meniť zväčšenie (zoom) a možnosti používať aplikáciu z rôznych zariadení vrátane mobilných telefónov.

Zabezpečenie obstaráva modul mod_ssl prostredníctvom OpenSSL 0.9.8r.

Celá aplikácia je z bezpečnostných dôvodov od prihlásenia prístupná len z adresného rozsahu 158.194.0.0/16. Platí to aj pre presmerovanie integrovaného webového managementu prepínačov.

Ako ďalšie stupne zabezpečenia slúžia časové obmedzenie presmerovania integrovaného webového managementu prepínačov, oddelené umiestnenie súborov s triedami PHP, overovanie aktuálnych oprávnení užívateľa prostredníctvom PHP sessions a použitie integrovaných funkcií PHP pre ošetrenie vstupných reťazcov.

V aplikácii sú použité vžité anglické názvy aktívnych prvkov – switch pre prepínač a router pre smerovač. Kliknutie na IP adresu prepínača, ak nie je uvedené inak, umožní prihlásenie do integrovaného webového managementu.

5. Počítačové siete Univerzity Palackého v Olomouci

Počítačová sieť Univerzity Palackého v Olomouci je na úrovni linkovej a sieťovej vrstvy referenčného modelu ISO/OSI rozdelená na dva hlavné celky:

- počítačové siete fakúlt a univerzitných zariadení UP
- KolejNET - počítačová sieť poskytujúca pripojenie pre ubytovaných na kolejích UP

5.1. Počítačové siete fakúlt a univerzitných zariadení

K akademickej sieti Českej republiky CESNET je pripojený smerovač, ktorý definuje, ktoré podsiete z celého rozsahu 158.194.0.0/16 bude obsluhovať Centrum výpočetní techniky UP a ktoré budú presmerované na smerovače KolejNET-u. Smerovanie prenosov fakúlt a univerzitných zariadení UP momentálne poskytuje 13 hardwarových smerovačov. Na úrovni linkovej vrstvy referenčného modelu ISO/OSI poskytuje pripojenie koncových staníc vrátane serverov 261 prepínačov. Ako managovacia VLAN pre tieto prepínače boli zvolené VLAN id 2 a IP adresy z privátneho rozsahu 172.20.20.0/24 až 172.20.220.0/24.

5.2. KolejNET

Počítačová sieť KolejNET je až na pripojenie k akademickej sieti CESNET plne autonómna vrátane vlastného smerovania. Tvoria ju 4 softwarové smerovače postavené na linuxovej distribúcii Slackware Linux pomocou paketového filtru iptables, databázový a webový server (MySQL, Apache, PHP) a ďalšie pomocné servery. Linkovú vrstvu referenčného modelu ISO/OSI tvorí 55 prepínačov. Managovacia VLAN má id 3 a adresný rozsah IP 158.194.3.0/24.

6. Detaily riešenia

6.1. Získanie, spracovanie a uloženie dát

Kvôli veľkému rozsahu IP adries managovacej VLAN id 2 je vhodné zistiť jednotlivé rozsahy, v ktorých bude aplikácia ďalej vyhľadávať aktívne prvky. Skript 10_manag.sh pomocou požiadaviek na odozvu upresní jednotlivé rozsahy a uloží ich do databázy.

Ukážka zo skriptu 10_manag.sh:

```
function mng {
    if [ -n "$debug" ]; then
        echo "subnet: " $net.$sub >&2
    fi
    first_ip=""
    last_ip=""
    i="0"
    j="255"
    while [ -z "$first_ip" ]; do
        if [ $i -lt $(($j-3)) ]; then
            let i++
            if [ -n "$debug" ]; then
                echo -n "<" >&2
            fi
            if [ -n "$(echo $net.$sub.$i | arp-scan/arp-scan -f - -t 5 -N -I $vlan -q |\
grep "$net")" ]; then
                first_ip=$net.$sub.$i
                if [ $i -gt 1 ]; then
                    while $(ping -c 1 -I $vlan -n -q -w 1 -W 1 $net.$(($i-1)) 2>&1 > /dev/null); do
                        let i--
                        first_ip=$net.$sub.$i
                    done
                fi
            fi
        else
            first_ip=" "
        fi
    done
```

Tento krok nie je nevyhnutný, avšak výrazne zníži čas prvého zisťovania konfigurácie siete. Keďže sa v čase môžu hranice jednotlivých podsietí posúvať, beží na pozadí skript manag_update.sh, ktorý pomocou programu tcpdump v štandardnom (nepromiskuitnom) móde sleduje komunikáciu na managovacích VLAN a priebežne upravuje jednotlivé hranice. Ďalej je nevyhnutné poznať jednotlivé smerovače, čo zaistia skripty routers.sh (detekcia) a 20_router.sh (získanie bližších detailov – popis, verzia software, umiestnenie a ich import do databázy).

Ukážka zo skriptu 20_router.sh:

```
loc=$($snmpget $router SNMPv2-MIB::sysLocation.0 2>/dev/null |\
    sed 's/SNMPv2-MIB::sysLocation.0 = STRING: \(.*\)/\1/g')
```

Skript routers.sh je značne stresujúci pre počítačovú sieť, preto bude spúšťaný len raz denne v skorých ranných hodinách, kedy je vyťaženie počítačovej siete minimálne. Nasleduje detekcia jednotlivých prepínačov pomocou skriptov z 30_switch. Pri detekcii prepojení jednotlivých prepínačov a neskôr spracovávaní zoznamu IP a MAC adries je nevyhnutné poznať MAC adresy všetkých prepínačov. Podsieť 172.20.140.0/24 (Teoretické ústavy Lekárskej fakulty UP) je odlišná tým, že jej managovacia VLAN je smerovaná, tzn. štandardným spôsobom odpovedá celý rozsah 172.20.140.0/24 jedinou MAC adresou – MAC adresou smerovača danej managovacej VLAN. Tento problém rieši časť skriptu 30_switch\mac_routed. Ku prepínačom ukladá aplikácia oproti smerovačom navyše počet portov. Vzhľadom na heterogenitu počítačovej siete je potrebné zistiť vzájomné vzťahy medzi popisom jednotlivých portov softwarom prepínača a ich reálnym označením – toto zaistí skript 40_port.sh. Import arp tabuľky zo všetkých smerovačov vykonáva skript 50_arp.sh, obdobne import tabuliek MAC adries z prepínačov skript 60_mac.sh.

Ukážka zo skriptov 50_arp.sh a 60_mac.sh:

```
function arp {
    query=$($snmpwalk $ip IP-MIB::ipNetToMediaPhysAddress |\
        egrep -io '158\.194\.[0-9]{1,3}\.[0-9]{1,3} = STRING: ([0-9A-F]{1,2}:){5}[0-9A-F]{1,2}' |\
        awk "{print $id \";\" \$4 \";\" \$1}" |\
        awk -F '[:;]' '{printf "(\"" $1 "\",\""; printf("%02s:%02s:%02s:%02s:%02s:%02s",
$2, $3, $4, $5, $6, $7); print "\",\"" $8 "\"),"}' |\
        tr 'a-f \n' 'A-F0 ')
    if [ -n "$query" ]; then
        echo "insert ignore into arp (router, mac, ip) values ${query%\, };
        update router set last = null where ip = \"$ip\";" | db
    fi
}

cisco=($(snmpwalk -Cc -v 1 -c public@2 $ip .1.3.6.1.2.1.17.4.3.1.2 2>/dev/null |\
egrep -o '([0-9]{1,3}.){5}[0-9]{1,3} = INTEGER: [0-9]*' |\
awk -F '[. ]' '{printf("%02X:%02X:%02X:%02X:%02X:%02X", $1, $2, $3, $4, $5, $6); print ";" $9}'))
if [ -n "$cisco" ]; then
    wait
if [ -n "$debug" ]; then
    echo "mac type cisco: " $ip >&2
fi
query=$(
    map=($(snmpwalk -Cc -v 1 -c public@2 $ip .1.3.6.1.2.1.17.1.4.1.2 2>/dev/null |\
        egrep -o '[0-9]* = INTEGER: [0-9]*' |\
        cut -d ' ' -f '1,4' --output-delimiter ';'))
    for line in ${cisco[@]}; do
        macoid=($(echo $line | tr ';' ' '))
        oid=""
        port=""
        for oid in ${map[@]}; do
            oidport=($(echo $oid | tr ';' ' '))
            if [ ${macoid[1]} -eq ${oidport[0]} ]; then
                port=${oidport[1]}
            fi
        done
        if [ -n "$port" ]; then
            echo "('$id', '$port', '${macoid[0]}'), "
        fi
    done)
fi
```

Vzájomné prepojenia prepínačov detekuje skript 70_link.sh.

Ukážka zo skriptu 70_link.sh:

```
this_mac=$(ifconfig | grep -o '..:..:..:..:..:..' | sort -u)

origIFS=$IFS

for line in $manual_links; do
    IFS=";"
    ip_port=($line)
    IFS=$origIFS
    id=$(echo "select id from switch where $interval and ip = \"${ip_port[2]}\";" | db)
    [ -z "$id" ] && id="null"
    echo "update switch set uplink_port = ${ip_port[1]}, downlink_switch = $id, \
downlink_port = ${ip_port[3]}, link_manual = 1 where ip = \"${ip_port[0]}\";"
done | db
```

Všetky blokované porty zisťuje skript 80_blocked.sh. Nakoniec import nových záznamov alebo aktualizáciu existujúcich vykoná skript 90_history.sh.

Do značnej miery sú jednotlivé skripty limitované rýchlosťou, akou jednotlivé aktívne prvky poskytnú prostredníctvom protokolu SNMP dáta. Aby som dosiahol rozumný celkový čas jedného cyklu, spúšťam úlohy v skriptoch 50_arp.sh (všetky úlohy), 60_mac.sh (maximálne 6 úloh) a celý skript 80_blocked.sh (maximálne 6 úloh) paralelne.

Všetky skripty v uvedenom poradí má význam spustiť len po inštalácii. Pre produkčné nasadenie je určený skript update.sk, ktorý cyklicky spúšťa skripty 50_arp.sh, 60_mac.sh, 80_blocked.sh a 90_history.sh. Každý dvadsiaty cyklus ale prebehne detekcia nových prepínačov – podľa meraní toto nastane približne raz za hodinu, čo je v súlade s požiadavkami získanými praxou.

Prepínače si pamätajú MAC adresy na portoch jednu minútu. Pre správnu detekciu prepojení prepínačov je vhodné, aby na daných portoch mali v pamäti MAC adresy ostatných prepínačov. Toto zaistím neustálymi požiadavkami na odozvu smerovanými na IP adresy všetkých prepínačov.

Aj tento cyklus som optimalizoval vynechaním časovo náročných operácii, ak nie sú potrebné – jedná sa o skript 40_port.sh, ktorému skript z 30_switch predá parameter, ak nájde nový prepínač. Je totiž možné, že mapovanie označenia portov tohto typu prepínača v databáze ešte nie je.

Ďalšie zrýchlenie a zníženie záťaže operačného systému som dosiahol použitím cudzích kľúčov a indexov v databáze. Pre tabuľky uchovávajúce dáta dočasného významu a zároveň dáta, s ktorými systém intenzívne pracuje (napr. tabuľky arp a mac), používam tabuľky typu memory.

Špecifické nastavenia pre počítačovú sieť UP v tejto časti aplikácie sú v skriptoch 20_router.sh, 50_arp.sh a samozrejme v súbore settings, ktorý slúži ako centrum všetkých nastavení.

6.1.1. História IP a MAC adries

Jednou z hlavných úloh tejto aplikácie je uchovávanie histórie IP adries, ktoré boli v danom čase priradené MAC adresám. Vzhľadom na vysoký počet aktívnych koncových staníc aplikácia ukladá minimálny počet záznamov pre konfiguráciu IP adresa, MAC adresa, prepínač a port. Kvôli zníženiu réžie som pre procesy týkajúce sa histórie IP a MAC adries koncových staníc zvolil možnosť uloženej procedúry. Momentálne aplikácia vytvára nový záznam len pre kompletnú konfiguráciu, tzn. všetky štyri parametre. Ak ale koncová stanica nemigruje a nekomunikuje prostredníctvom smerovača a zároveň prepínač má v pamäti jej MAC adresu, je záznam aktualizovaný. Ak koncová stanica migruje a pripojí sa k inému prepínaču, je mu vytvorený nový záznam a pôvodný je označený ako archivovaný.

Ukážka uloženej procedúry:

```
create procedure update_history(mac_ char(17), ip_ varchar(39), switch_ bigint(20) unsigned,
port_ smallint)
begin
if exists (select id from history where mac = mac_ and switch = switch_ and port = port_ and
archived = 0) then
    if ip_ != 'nul' then
        set @id = (select id from history where mac = mac_ and ip = ip_ and switch = switch_ and
port = port_ and archived = 0);
        if @id is not null then
            update history set last = null where id = @id;
        else
            insert into history (mac, ip, last, switch, port, login) values (mac_, ip_, null,
switch_, port_);
        end if;
    else
        update history set last = null where mac = mac_ and switch = switch_ and port = port_ and
archived = 0;
    end if;
else
    if ip_ != 'nul' then
        update history set archived = 1 where mac = mac_ and archived = 0;
    end if;
        insert into history (mac, ip, last, switch, port, login) values (mac_, ip_, null, switch_,
port_);
end if;
end //
```

6.2. Zobrazenie, úprava a vyhľadávanie

Webserver Apache HTTP server a PHP sú v podstate v základnej produkčnej konfigurácii s OpenSSL zabezpečením.

Ukážka CSS súboru:

```
body {
    background : #f3f3ff;
    background-image : url(../images/background.png);
    color : #444444;
}
div#AdminLoginFrame {
    background-color : #fcfffc;
    width : 300px;
    margin : 80px auto 80px auto;
    border : 1px solid #4876ff;
    padding : 10px;
}
```

Ako návrhový vzor pre PHP skripty som zvolil vzor Factory. Tento model je založený na jednej triede (factory), ktorá vytvára všetky ostatné objekty. Prínos tohto prístupu je v možnosti zmeniť iné triedy (napr. triedu pre databázové spojenie) bez nutnosti revidovať zvyšok kódu.

Ukážka triedy Factory.php:

```
require_once 'Database.php';

class Factory {

    protected $database;

    function __construct() {
        $this->database = new Database();
```

Základné informácie o prihlásenom užívateľovi uchovávam pomocou sessions. Overovanie užívateľského mena a hesla riešim pomocou PHP a jeho triedy pre pripojenie k LDAP.

Po prihlásení užívateľ vidí **Informácie** – zoznam prepínačov rozdelený do skupín podľa podsietí, ktoré v posledných 10 minútach neodpovedali.

Ukážka z triedy Query.sql:

```
public function SwitchDownGetAll($rack) {
    $sql = "SELECT id, ip, descr, loc, units, rack, last, note FROM switch WHERE rack = '$rack'
AND unit < 2 AND last < DATE_SUB(NOW(),INTERVAL 10 MINUTE) ORDER BY INET_ATON(ip)";
    $result = $this->database->Query($sql);
    $resultArray = array();
    while ($resultRow = $result->fetch_array()) {
        array_push($resultArray, $resultRow);
    }
    return $resultArray;
}
```

Tento zoznam je ako jediný automaticky aktualizovaný na strane klienta každú minútu. Názov skupiny odkazuje na zoznam všetkých prepínačov v danej skupine.

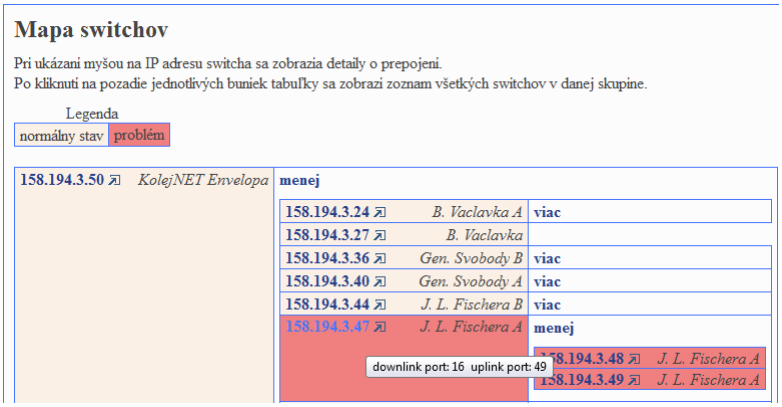
Obrázek 1. Ukážka úvodnej stránky aplikácie.

Mapa switchov je rozbaliteľná mapa všetkých prepínačov. V prípade, že niektorý z prepínačov neodpovedal v posledných 10 minútach, bude jeho pozadie červené.

Ukážka zo skriptu map.php:

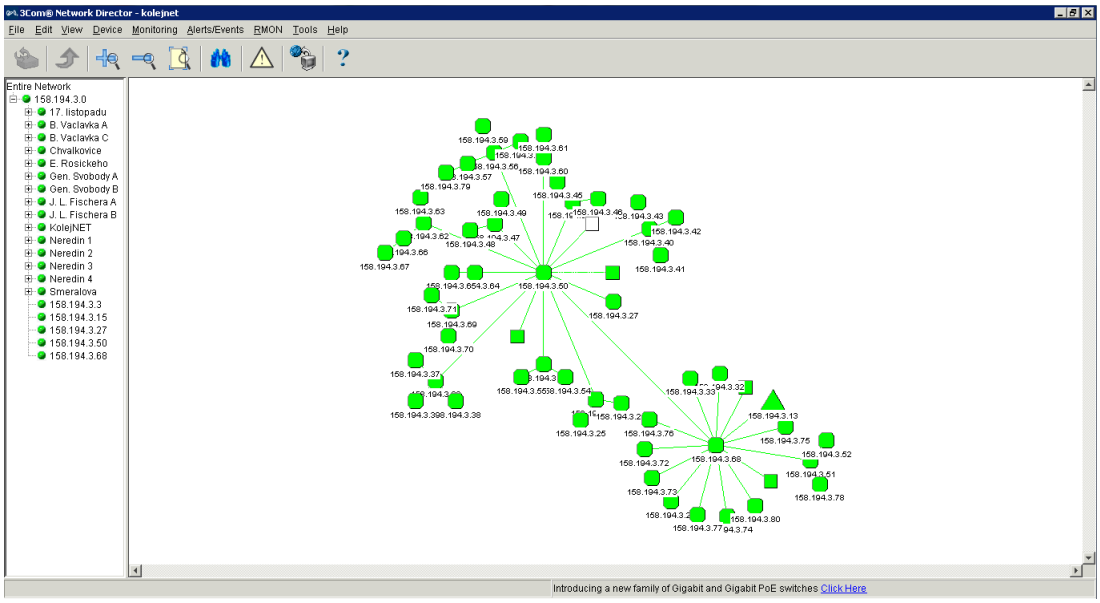
```
foreach ($switch->GetMap() as $mapRow) {
    if (is_null($mapRow['downlink_switch'])) {
        $mapArray[$mapRow['id']] = $mapRow;
    } else {
        $Childs[$mapRow['downlink_switch']][$mapRow['id']] = $mapRow;
    }
}

function gettree($mapArray) {
    global $Childs;
    foreach ($mapArray as $key => $value) {
        ?><tr>
            <?php
            if ((strtotime($value['last']) < strtotime("- 10 minutes")) && ($value['units'] < 2)) {
                $td = "class=\"down\" style=\"cursor: help\" ..
```

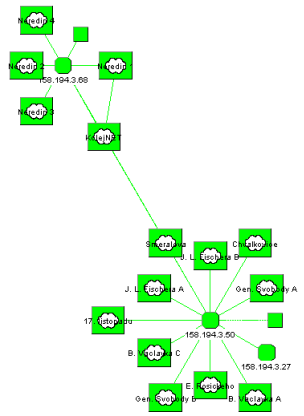


Obrázek 2. Ukážka mapy prepínačov.

Pre porovnanie uvádzam nasledujúce obrázky z aplikácie 3Com Network Director. Aplikácia, ku ktorej mám prístup, monitoruje len 55 prepínačov.

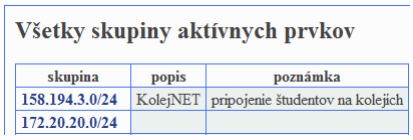


Obrázek 3. Ukážka nezoskupenej mapy prepínačov.



Obrázek 4. Ukážka ručne zoskupenej mapy prepínačov.

Skupiny sú momentálne preddefinované ako podsiete managovacích VLAN. V budúcnosti je možné doplniť kód o funkcionalitu pridania vlastnej skupiny, ale to záleží na požiadavkách od užívateľov. Názov skupiny znovu odkazuje na zoznam všetkých prepínačov v danej skupine.

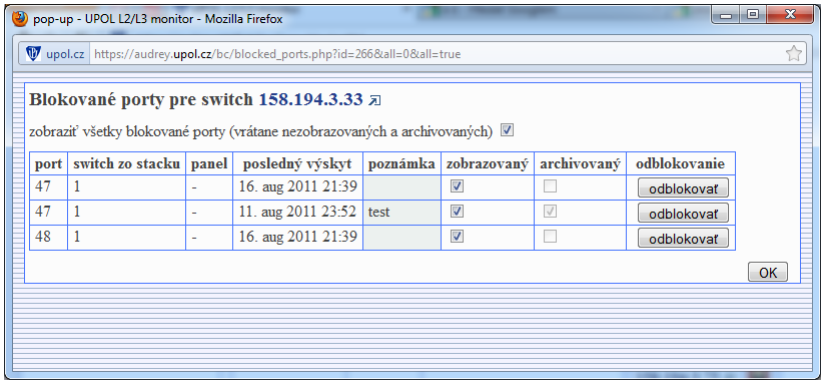


Všetky skupiny aktívnych prvkov

skupina	popis	poznámka
158.194.3.0/24	KolejNET	pripojenie študentov na kolejích
172.20.20.0/24		

Obrázek 5. Ukážka skupín aktívnych prvkov.

Blokované porty umožňujú zobraziť a upraviť blokované porty jednotlivých prepínačov. Možnosť **zobrazovaný** umožňuje nezobrazovať port v bežnom výpise – je to vhodné pre dlhodobo blokované porty ako napr. nevyužité porty. Ak má prihlásený užívateľ dostatočné oprávnenia, môže port **odblokovať** priamo z aplikácie. Príznak **archivovaný** nie je užívateľsky meniteľný, aplikácia ho nastaví odblokovanému portu, ak sa vyskytne znovu medzi blokovanými portami.



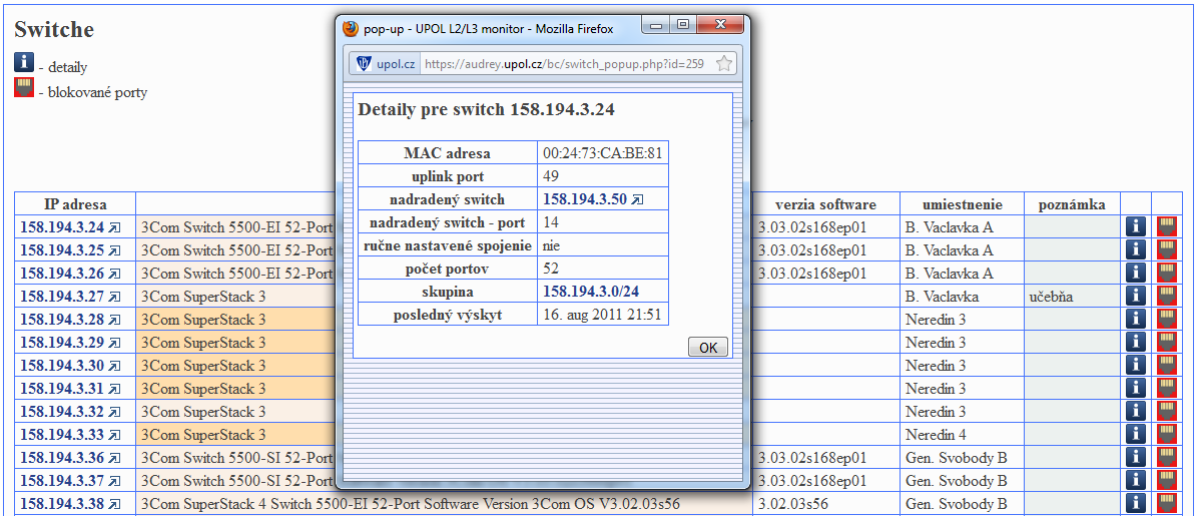
Obrázek 6. Ukážka okna blokovaných portov.

"malé" switche je zoznam prepínačov a ich portov, kde sa vyskytlo viac MAC adries za posledných 7 dní. Jednoduché nemanagovateľné prepínače sú častým zdrojom problémov typu nízka priepustnosť siete alebo náhodné inak ťažko dohľadateľné výpadky.

Ukážka z triedy Query.sql:

```
public function SwitchPortMac2Get($rack, $count) {
    $sql = "SELECT id, ip, rack, port, COUNT(id) as c FROM
((SELECT id, ip, rack FROM switch WHERE rack = '$rack' AND last > DATE_SUB(NOW(),INTERVAL 1 HOUR))
AS s JOIN (SELECT switch, port FROM history WHERE last > DATE_SUB(NOW(),INTERVAL 1 WEEK) GROUP BY
mac, switch, port) AS h ON s.id = h.switch) GROUP BY id, port HAVING COUNT(id) > '$count' ORDER BY
INET_ATON(ip), port ASC";
    $result = $this->database->Query($sql);
    if (!$result)
        return false;
    $resultArray = array();
    while ($resultRow = $result->fetch_array()) {
        array_push($resultArray, $resultRow);
    }
    return $resultArray;
}
```

Switche je kompletný zoznam všetkých prepínačov. Zvlášť zvýraznené sú prepínače tvoriace tzv. stack. Stack je prepojenie prepínačov neštandardným spôsobom, čo na jednu stranu prináša výhody typu vyššia rýchlosť spojenia (bežne 2Gbit/s), na druhú stranu to ale prináša rôzne problémy typu výpadky, prípadne neštandardná funkčnosť.



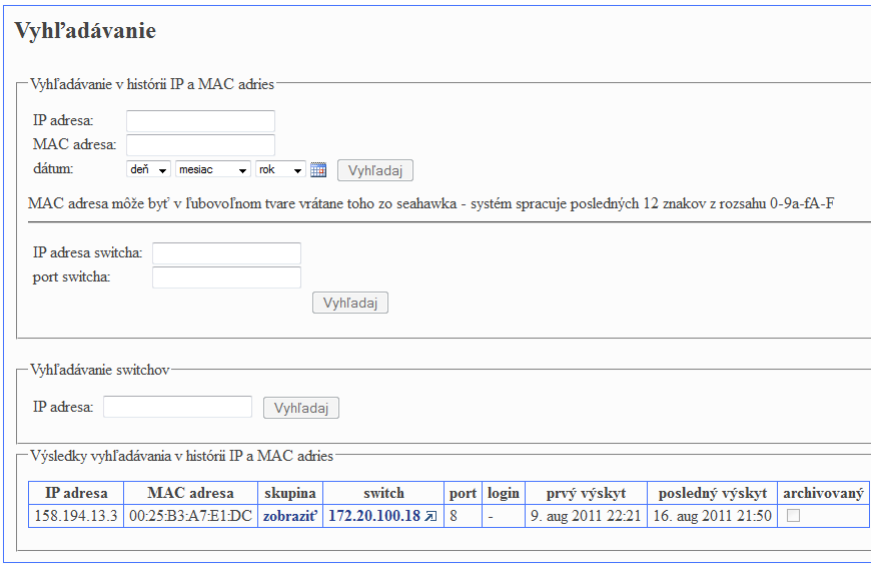
Obrázek 7. Ukážka zoznamu prepínačov s oknom detailov.

Routre a **brány** sú zoznamy smerovačov a brán s predvoleným filtrom na smerovače a brány pod správou CVT UP.

Vyhľadávanie umožňuje vyhľadávať podľa IP adresy alebo MAC adresy s možným upresnením dátumu výskytu. Je prispôsobené potrebám správcov sietí. Pole pre MAC adresu povoľuje aj neštandardný tvar typu 01-00dead00babe, ktorý používa univerzitný DHCP server.

Ukážka zo skriptu search.php:

```
<?php if ($_POST['ip'] || $_POST['mac']) { ?>
    <fieldset>
        <legend>Výsledky vyhľadávania v histórii IP a MAC adries</legend>
        <?php
        if ($_POST['ip']) {
            $historyArray = array();
            $historyArray = $switch->GetHistory('ip', trim($_POST['ip']), $_POST['kalendar']);
        } elseif ($_POST['mac']) {
            $mac = preg_replace('/[^0-9a-fA-F]/', '', $_POST['mac']);
            if (strlen($mac) > 11) {
                if (strlen($mac) > 12)
                    $mac = substr($mac, -12);
                $macArray = str_split($mac, 2);
                $mac = implode(':', $macArray);
            } else {
                ?>
                <p class="error">Nesprávny tvar MAC adresy.</p>
                <?php
                return;
            }
```



Obrázek 8. Ukážka vyhľadávacích formulárov s výsledkom vyhľadávania koncovej stanice podľa IP adresy.

Administrácia je pre užívateľov len informácia, aké oprávnenia sú priradené k ich účtu, prípadne v **Log** si môžu dohľadať akciu, ktorá ich zaujíma (napr. odblokovanie portu).

Ukážka zo skriptu user.php:

```
    <?php if ($session->Get('type') == 0) { ?>
        <fieldset>
            <legend>Pridanie užívateľa</legend>
            <form name="adduser" action="" method="POST">
.
.
if ($_POST['login']) {
    $addloginArray = array();
    $addloginArray = $admin->AddAdmin(trim($_POST['login']));
}
```

Všetky úpravy popisov a poznámok som riešil kliknuteľnou bunkou tabuľky a JavaScript-om s odlíšením pomocou farby pozadia. Tak isto som sa snažil o maximálnu mieru unifikácie, tzn. vždy po kliknutí na IP adresu prepínača z ktorejkoľvek časti aplikácie (ak nie je uvedené inak) sa vytvorí tunel
[IP adresa prepínača]:port 80 — [IP adresa servera]:[port 50001 až 59999]
a otvorí sa nové okno s integrovaným webovým managementom prepínača. Jedna takáto relácia je z bezpečnostných dôvodov obmedzená na 10 minút.

6.2.1. Modelové situácie vyhľadávania

Časté využitie vyhľadávania koncových staníc bude napr. pri riešení sťažností tretích strán.

Ukážka časti sťažnosti:

```
Palacky University of Olomouc
Computer Centre
Biskupske nam. 1
Olomouc,   771 46  CZ

RE:  Unauthorized Distribution of the Copyrighted Television Series Entitled
        Dexter
.
.
Since you own this IP address (158.194.182.75), we request that you immediately do the following:

1) Remove or disable access to the individual who has engaged in the conduct described above; and

2) Take appropriate action against the account holder under your Abuse Policy/Terms of Service Agreement.
.
.
Infringing Work: Dexter
First Found: 9 Jun 2011 14:04:44 EDT (GMT -0400)
Last Found: 9 Jun 2011 14:04:44 EDT (GMT -0400)
IP Address: 158.194.182.75
IP Port: 13237
Protocol: BitTorrent
```

Možnosť vyhľadávať všetky koncové stanice podľa IP adresy prepínača a portu môže slúžiť napr. pri neznalosti mapovania fyzických zásuviek na jednotlivé porty prepínačov a dohľadávaní miesta, kde bola pripojená hľadaná koncová stanica.

7. Inštalácia

Vzhľadom na určenie aplikácie UPOL L2/L3 monitor pre rozsiahle siete typu MAN až WAN neodporúčam pokúšať sa o inštaláciu nedostatočne skúseným správcom. Snažil som sa vyhnúť neštandardným postupom, ale aj tak je nutné aspoň zbežne pochopiť podstatu celej aplikácie a kód prekontrolovať, či bude vykazovať očakávané výsledky v inom prostredí. Je vhodné použiť minimálne vyššie uvedené spôsoby zvýšenia zabezpečenia.

7.1. Inštalácia časti pre získanie, spracovanie a uloženie dát

Aplikácia je určená pre UNIX-like operačné systémy. Požiadavky na softwarovú výbavu nie sú nijak zvláštne. Sú potrebné všetky použité utility a programy, z nie úplne štandardných by som spomenul snáď len program redir použitý na presmerovanie prístupu k integrovanému webovému managementu prepínačov. Program arp-scan je použitý len pri prvom spustení v skripte 10_manag.sh a je jednoducho nahraditeľný napr. programom ping. SQL skript potrebný pre inštaláciu databázy je súčasťou aplikácie. Pre spúšťanie jednotlivých skriptov je možné použiť čokoľvek, ja používam cron.

7.2. Inštalácia časti pre zobrazenie, úpravu a vyhľadávanie

Keďže sú obe časti prepojené len databázou, je možné nainštalovať ich oddelene. Konfigurácia webservera Apache HTTP server spoločne s PHP je prakticky štandardná. Nevyužívam žiadne neštandardné moduly ani konfiguračné voľby.

Závěr

UPOL L2/L3 monitor je špecializovaná aplikácia slúžiaca pre potreby monitorovania počítačovej siete upravená v niektorých detailoch počítačovej sieti Univerzity Palackého v Olomouci. Jej cieľom je uľahčiť prácu správcov počítačovej siete na rôznych úrovniach. Integruje monitorovanie dostupnosti a hlavných parametrov aktívnych prvkov smerovačov a prepínačov. Vytvára a uchováva históriu koncových staníc v súlade s potrebami poskytovateľa služby Internet. Je užívateľsky prívetivá a nenáročná na údržbu.

Po vhodne dlhom čase pilotného nasadenia plánujem rozšíriť aplikáciu o možnosť monitorovať vyťaženie zvolených spojov, či už celkových dátových prenosov, alebo pomeru broadcast paketov k unicast, prípadne multicast paketom. Tak isto po skúsenostiach z praktického používania možno nastane potreba uchovávať históriu MAC adries aj bez platnej IP adresy, čo síce výrazne zvýši nároky aplikácie na zdroje, ale jej samotná úprava bude minimálna. Na užívateľoch bude tiež záležať, či doimplementujem upraviteľné zobrazovanie pomocou cookies.

Conclusions

UPOL L2/L3 monitor is a specialized application for monitoring computer networks. It is customized for the computer network of Palacký University Olomouc in some details. Its aim is to facilitate the work of a computer network administrators at various levels. It integrates monitoring of availability and main parameters of routers and switches. It creates and retains a history of end stations in accordance with the needs of Internet service provider. It is user friendly and easy to maintain.

After a suitably long time of pilot deployment I plan to extend the application to monitor the utilization of selected links, whether the total data transmission, or the ratio of broadcast packets to unicast or multicast packets. Likewise, the experience of practical use might ask for keeping a history of MAC addresses without a valid IP address, which, while significantly increasing demand for applications resources, but the modification itself will be minimal. Also implementation of customizable display using cookies will depend on users.

Reference

[1] normy. *IETF Documents.* Elektronický zdroj, 2011.

[2] Cooper, Mendel. *Advanced Bash-Scripting Guide.* Elektronická publikácia, 2011.

[3] manuálové stránky. *Linux Man Pages* Elektronická publikácia, 2011.

[4] tým autorov. *MySQL 5.1 Reference Manual* Elektronická publikácia, 2011.

[5] Achour, Mehdi., Betz, Friedhelm., Dovgal, Antony., Lopes, Nuno., Magnusson, Hannes., Richter, Georg., Seguy, Damien., Vrana, Jakub. a ďalší *PHP Manual.* Elektronická publikácia, 2011.

A. Obsah priloženého DVD

`bin/`
: Obsahuje dve časti:
sh – časť pre získanie, spracovanie a uloženie dát
www – časť pre zobrazenie, úpravu a vyhľadávanie

`doc/`
: Dokumentácia

`src/`
: Obsahuje dve časti:
sh – časť pre získanie, spracovanie a uloženie dát a program arp-scan
www – časť pre zobrazenie, úpravu a vyhľadávanie a program redir

`readme.txt`

Naviac DVD obsahuje:

`install/`
: Zdrojový kód arp-scan-1.8.1
Zdrojový kód redir-2.2.1