VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Technologie počítačových sítí

Grafické open source rozhraní pro management sítě s přepínači a směrovači na bázi SNMP

2008 Jan Kordas

Úvod

V úvodu článku je stručně popsán SNMP protokol. Následuje popis nástrojů s grafickým uživatelským rozhraním pro management sítě. Popis je v hojené míře doplněn obrázky jednotlivých programů. Práce se zaměřuje pouze na nástroje, které jsou alespoň v omezené funkčnosti volně dostupné, tedy bez nutnosti jejich koupě. Druh licence je vždy zmíněn. U každého nástroje je také uveden odkaz, kde se dá popisovaný SW stáhnout a kde je možné najít další informace o produktu. Řazení nástrojů v textu je náhodné a nevyjadřuje kvalitu či jiný atribut zařízení. V práci uváděná funkčnost všech nástrojů byla, až na pár výjimek (uvedených v textu), odzkoušena. V příloze jsou uvedeny konfigurace prvků, ze kterých byla vytvořena testovací topologie.

SNMP

SNMP (Simple Network Management Protocol) je protokol aplikační vrstvy pro výměnu informací mezi zařízeními v síti. SNMP umožňuje síťovým administrátorům monitorovat síťové prvky, výkon sítě a řešit nalezené problémy.

SNMP komunikace probíhá mezi managerem (software v sledovacím zařízení) a agentem (software ve sledovaném zařízení). Manager se doptává agenta na požadované informace, nebo agent tyto informace automaticky posílá (překročení nastavené hodnoty, periodické odesílání) na adresu vybraného managera. Informace z jednoho agenta může číst více managerů. SNMP protokol podporuje čtyři příkazy:

- get – používá se k získání hodnoty vybraného objektu z agenta,
- getNext – slouží k získání hodnoty objektu, který se nachází za předchozím dotazovaným,
- trap – je asynchronní zpráva, kterou posílá agent managerovi,
- set – nastaví hodnotu vybraného objektu.

SNMP nyní existuje ve třech verzích SNMPv1, SNMPv2 (experimentální) a SNMPv3. SNMPv3 se od předchozích dvou liší hlavně v zabezpečení. Zatímco předchozí dvě verze používají k zabezpečení tzn. community string, SNMPv3 již nabízí možnost autentizace. Z důvodu chybějícího zabezpečení verze SNMPv1 a v2 někteří výrobci nedovolují operace typu set, aby předešli neoprávněným změnám nastavení. V SNMP agentech je možno typicky možno nastavit více community stringů s různým přístupem. Často se používají tyto dva: public (jen pro čtení) a private (i pro zápis).

Každá hodnota v SNMP je jednoznačně identifikována pomocí OID (Object Identifier). OID je posloupnost čísel oddělených tečkou, tvoří tak stromovou strukturu. Struktura OID je uložena v MIB (Management Information Base) databázi. MIB databáze obsahuje jména a popisy jednotlivých OID.

Spuštění SNMP v Cisco zařízeních

V Cisco zařízeních lze SNMP verze 1 spustit v konfiguračním režimu tímto příkazem:

```
(config)#snmp-server community private rw
```

Přes community string private budou dostupné všechny objekty jak pro čtení, tak pro zápis. Na zařízeních, kde běží SNMP agent, musí být alespoň na jednom rozhraní, které je připojeno do monitorované oblasti, nastavena IP adresa. SNMP agent je dostupný pod adresou libovolného rozhraní směrovače nebo přepínače.

Více informací o SNMP je možné nalézt například na webových stránkách http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm, odkud byly také čerpány výše uvedené informace.

CSNMP-Tools

Platforma: MS Windows

Zdroj: http://billythekids.demirdesign.com/

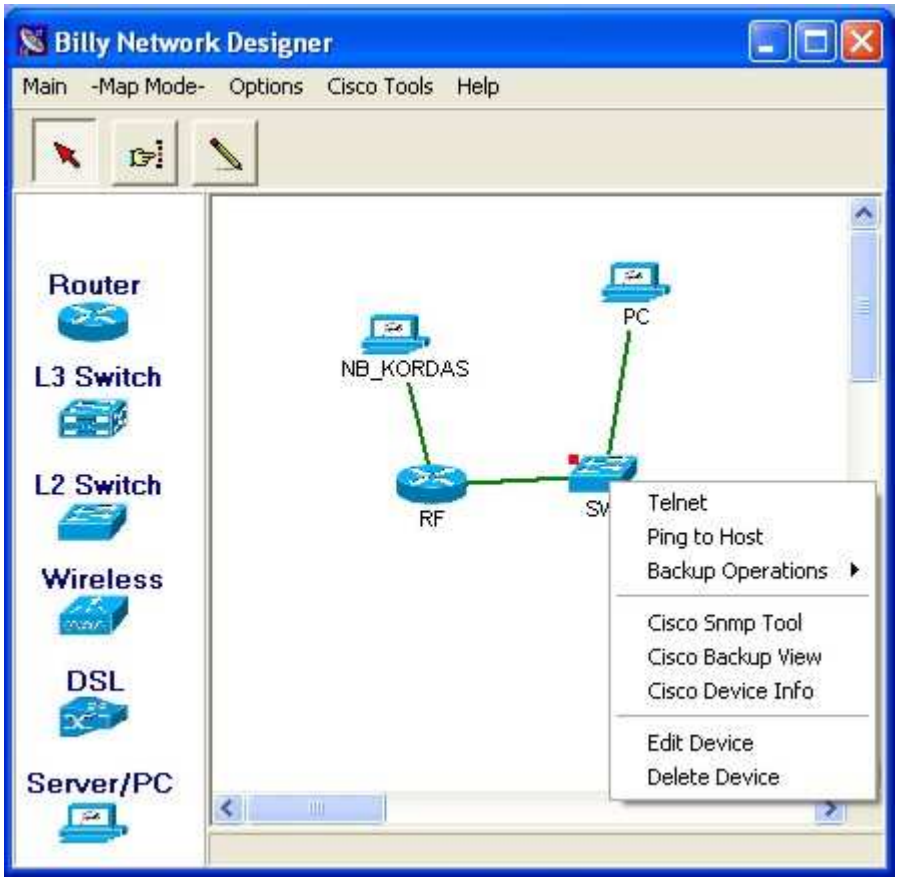
Typ licence: Freeware

Funkčnost: Monitoring a management

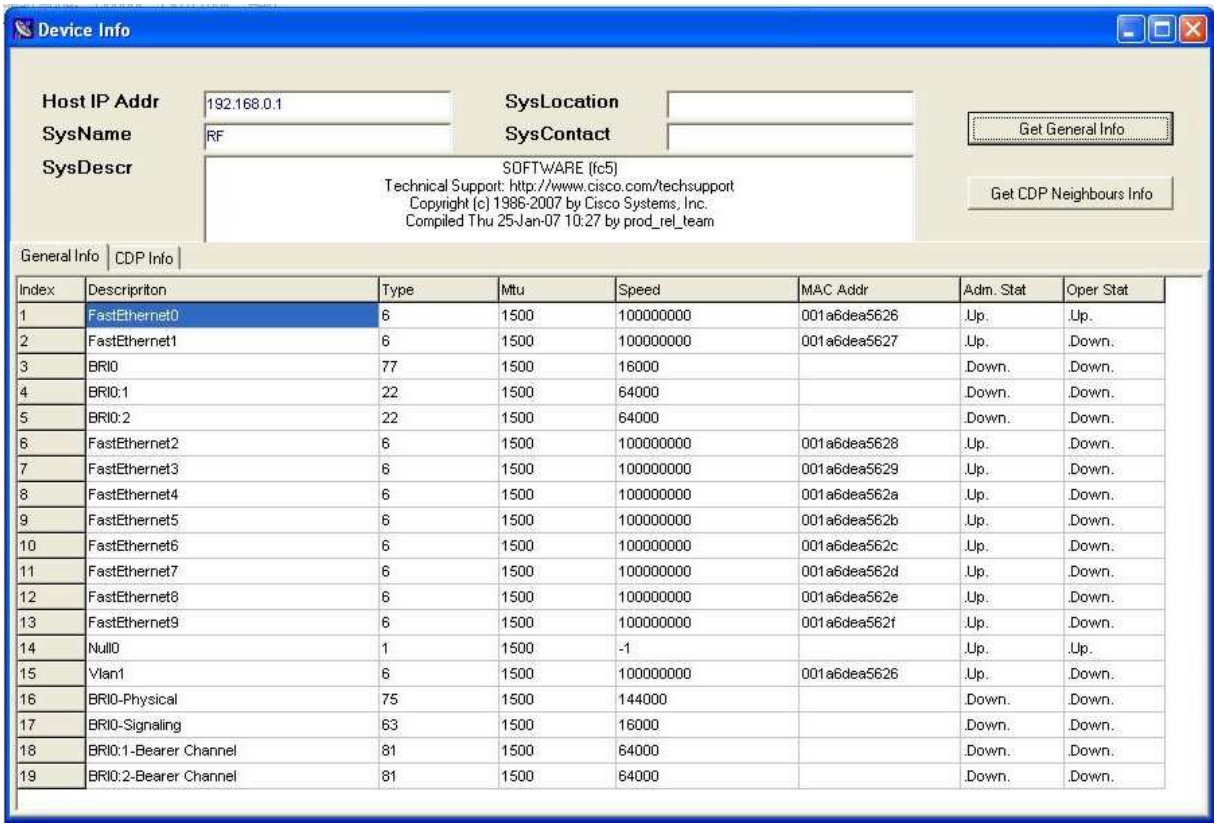
Instalace: Instalace na PC

Jednoduchý nástroj pro MS Windows, který umožňuje testování dostupnosti síťových zařízení pomocí pingu v nastaveném intervalu (10 sekund, 1 minuta, 5 minut). Ze síťových prvků je možné vytvořit celou topologii monitorované sítě, kterou je možné uložit a při opětovném startu načíst. Kromě uvedených monitorovacích funkcí také nabízí možnost stahování, nahrávání a zálohování konfigurace Cisco zařízení (startup i running), připojení se k zařízení pomocí telnetu. Program nabízí volbu odeslání testovacího SNMP řetězce do zařízení, pro otestování správného nastavení SNMP v zařízení a programu. Pomocí protokolu SNMP umí také zobrazit informace o vybraném Cisco zařízení. SNMP je podporován jen ve verzi 1 a je nutné mít v zařízení definován úplný přístup (čtení i zápis). Program má implementovánu také podporu protokolu CDP, což mu umožňuje získávat informace o sousedech vybraného zařízení (tato funkčnost nebyla vyzkoušena).

Takto vypadá základní editační obrazovka nástroje a menu po stisku pravého tlačítka myši na vybraném zařízení.



Informace o zařízení získané pomocí protokolu SNMP nástrojem CSNMP-Tools. K těmto informacím se dostaneme pomocí pravého kliku myší na zařízení a vybráním položky „Cisco Device Info“.



Index	Descripriton	Type	Mtu	Speed	MAC Addr	Adm. Stat	Oper Stat
1	FastEthernet0	6	1500	100000000	001a6dea5626	.Up.	.Up.
2	FastEthernet1	6	1500	100000000	001a6dea5627	.Up.	.Down.
3	BRI0	77	1500	16000		.Down.	.Down.
4	BRI0:1	22	1500	64000		.Down.	.Down.
5	BRI0:2	22	1500	64000		.Down.	.Down.
6	FastEthernet2	6	1500	100000000	001a6dea5628	.Up.	.Down.
7	FastEthernet3	6	1500	100000000	001a6dea5629	.Up.	.Down.
8	FastEthernet4	6	1500	100000000	001a6dea562a	.Up.	.Down.
9	FastEthernet5	6	1500	100000000	001a6dea562b	.Up.	.Down.
10	FastEthernet6	6	1500	100000000	001a6dea562c	.Up.	.Down.
11	FastEthernet7	6	1500	100000000	001a6dea562d	.Up.	.Down.
12	FastEthernet8	6	1500	100000000	001a6dea562e	.Up.	.Down.
13	FastEthernet9	6	1500	100000000	001a6dea562f	.Up.	.Down.
14	Null0	1	1500	-1		.Up.	.Up.
15	Vlan1	6	1500	100000000	001a6dea5626	.Up.	.Down.
16	BRI0-Physical	75	1500	144000		.Down.	.Down.
17	BRI0-Signaling	63	1500	16000		.Down.	.Down.
18	BRI0:1-Bearer Channel	81	1500	64000		.Down.	.Down.
19	BRI0:2-Bearer Channel	81	1500	64000		.Down.	.Down.

GNetWatch

Platforma: MS Windows, Linux

Zdroj: http://gnetwatch.sourceforge.net/

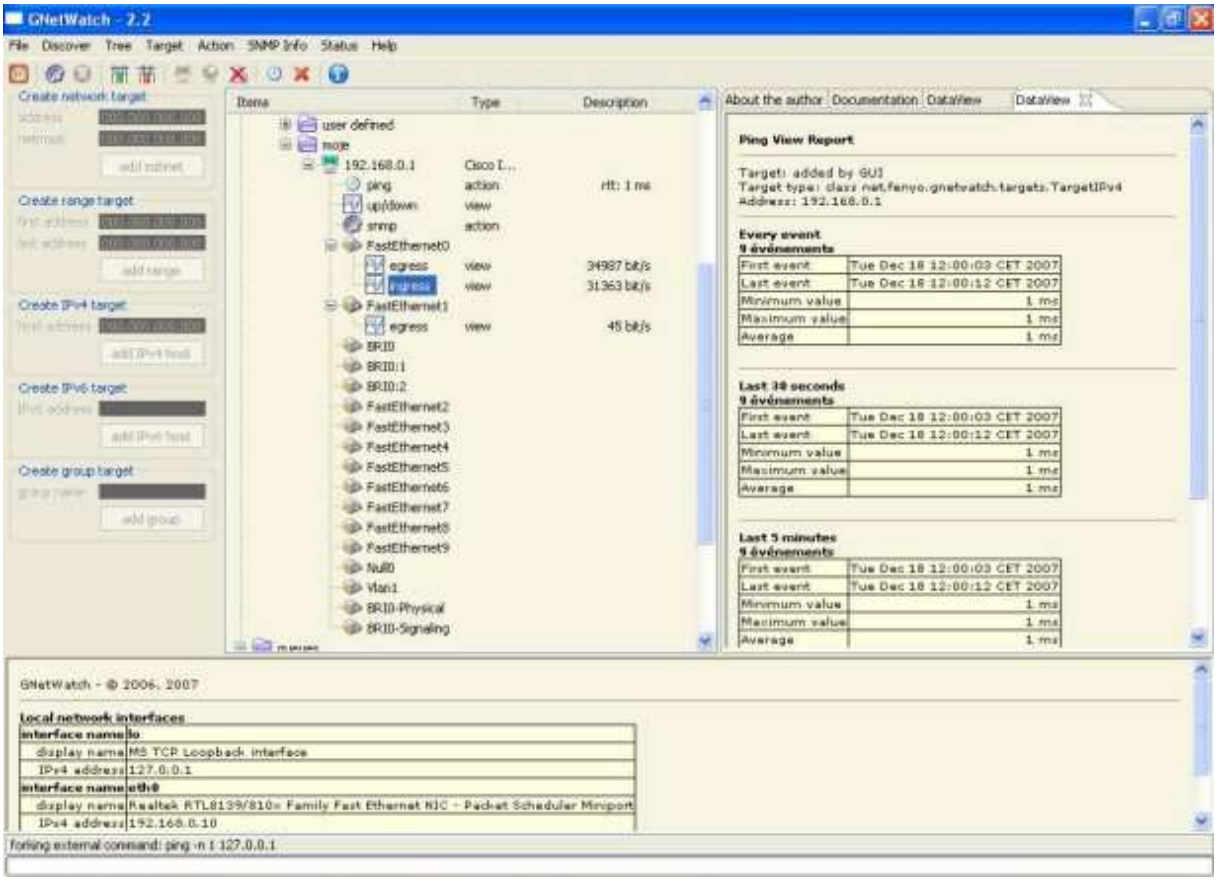
Typ licence: Open source

Funkčnost: Monitoring a management

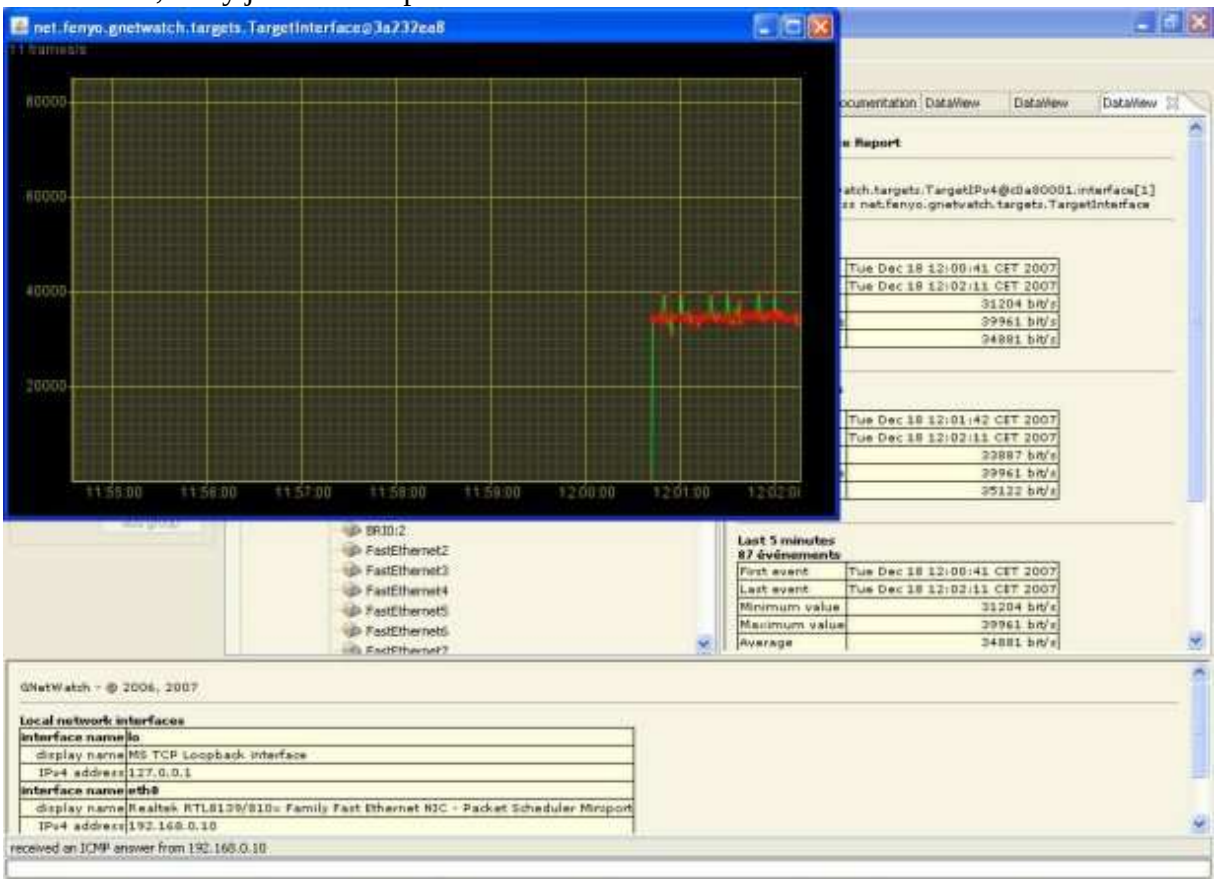
Instalace: Spuštění GNetWatchBundle.jar (musí být nainstalováno JRE verze 5 a vyšší)

GNetWatch je nástroj pro monitorování sítě v reálném čase pomocí SNMP (ve všech aktuálně dostupných verzích 1, 2c, 3) a ICMP. Jedná se open source aplikaci napsanou v programovacím jazyce Java. Monitorovaná zařízení jsou zobrazena ve stromové struktuře. Kromě jednotlivých zařízení (target) je také možné do stromu přidávat celé rozsahy zařízení a sítě. Zařízení je ve stromě definováno pomocí IP adresy. Všechny tyto prvky je možné vkládat do skupin. Každému cíli (nebo rozsahu cílů) je možné přiřadit akce. Akce jsou ping, zaplavení cíle (flood target), http zátěž (program generuje zátěž posíláním http požadavků na http server, který na vybraném cíli běží), průzkum přes SNMP a Nmap (netestováno). Aplikace také nabízí automatický průzkum sítě. Pro tuto funkčnost musí být nainstalován program Ethereal a v PATH musí být nastavena k němu cesta. Velkým nedostatkem aplikace GNetWatch je, že nejde aktuální strom uložit a tudíž se po spuštění musí znovu vše nastavovat.

Na následujícím obrázku je možné vidět informace získané z Cisco routeru pomocí SNMP.



Na tomto obrázku je zachycen graf toku dat rozhraním FastEthernet1 směrovače s adresou 192.168.0.1, který je vidět i na předchozím obrázku.



InterMapper

Platforma: Multiplatformí

Zdroj: http://dartware.com

Typ licence: Komerční (14-ti denní zkušební veze zdarma, verze pro 5 zařízení zdarma)

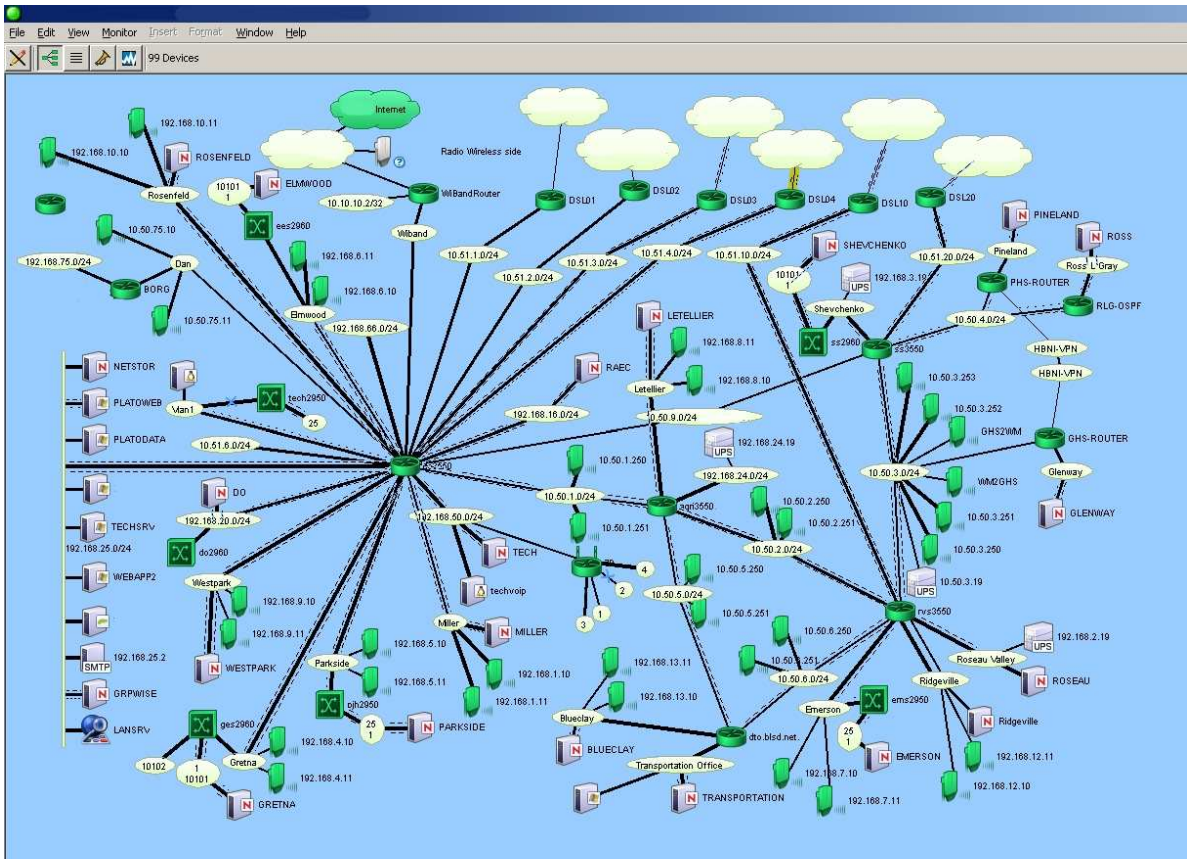
Funkčnost: Monitoring

Instalace: Instalace na PC

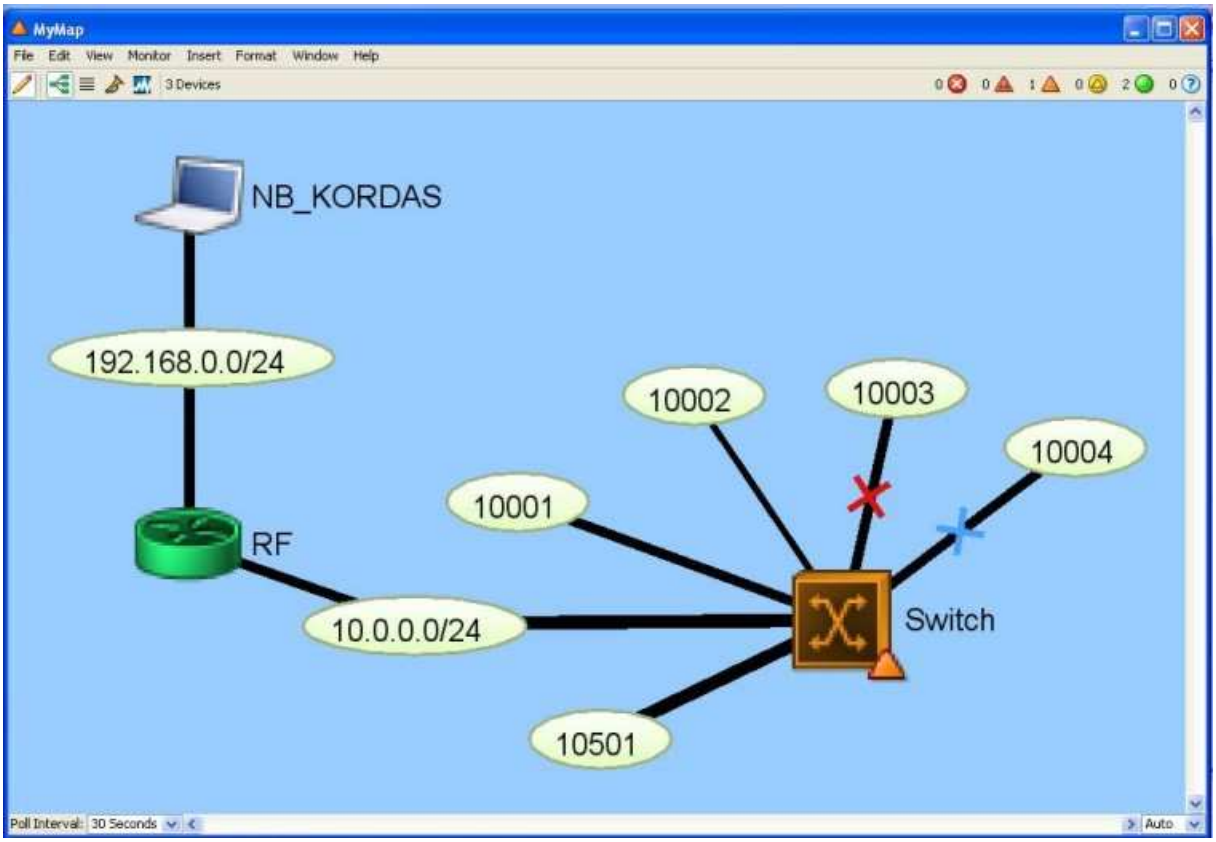
Graficky velice pěkně zpracovaný nástroj, který umožňuje monitorování toku dat, ztrát paketů, výkonu síťových zařízení, výpadků sítě, zobrazuje topologii sítí ve více úrovních. Funkčnost zařízení a informace z nich získává pomocí protokolu SNMP. Pokud zařízení tento protokol nepodporuje, zjišťuje dostupnost alespoň pomocí pingů. Perioda dotazů je nastavitelná.

Ovládání programu je intuitivní. Program pracuje ve dvou režimech, editačním a sledovacím. V editačním režimu je možné přidávat síťová zařízení a nastavovat parametry potřebné pro komunikaci s nimi (IP adresa, …). Nakreslené mapy sítě je možné ukládat a načítat. Program umožňuje automaticky vyhledat zařízení v síti. Vyhledávání se provádí pomocí pingu a lze nastavit v jakém rozsahu se má vyhledávat (kolik přeskoků od počáteční adresy). Díky tohoto vyhledávání není nutné vše zadávat ručně (pokud je odpověď ping u zařízení v síti povolena). Ve sledovacím režimu pak vidíme nakreslený graf sítě spolu s informacemi o stavu jednotlivých prvků. Přes pravé tlačítko se dostaneme k podrobnějším informacím o jednotlivých zařízeních. Je možno nastavit parametry různých varování a alarmů.

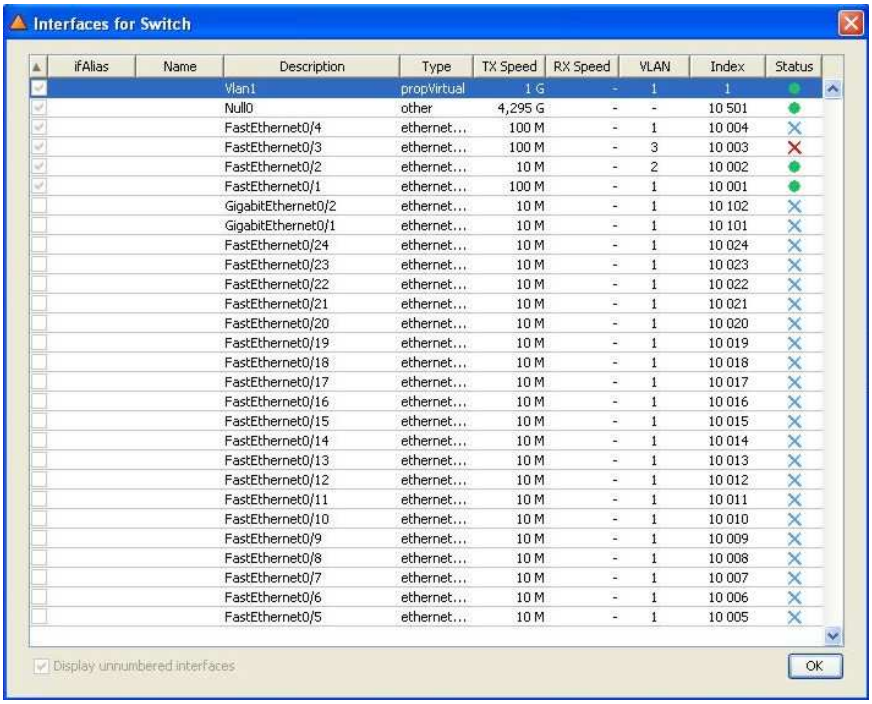
Na následujícím obrázku je graf sítě, který je stažen ze stránek výrobce. Na obrázku je vidět jen podmnožina dostupných grafických symbolů, které lze zařízením přiřazovat.



Na dalším obrázku je schéma sítě, které InterMapper detekoval sám. Pro přehlednost je skryta většina portů přepínače. Dostupnost notebooku detekuje InterMapper pomocí pingu. Dostupnost směrovače a přepínače a funkčnost jejich jednotlivých rozhraní se zjišťuje pomocí SNMP. Jelikož je port s označením 10003 v poruše, je to signalizováno výstražným trojúhelníkem u zařízení. Pokud by bylo zařízení nedostupné, bylo by na místě trojúhelníku červené kolečko s křížkem uprostřed. V pravém horním rohu se sumární zobrazuje informace o stavu všech zařízení a ikonka programu zobrazuje nejhorší stav zařízení v síti.



Poslední obrázek zachycuje podrobný přehled rozhraní switche s dostupnými informacemi vyčtenými pomocí SNMP.



Paessler SNMP Tester 2.2

Platforma: MS Windows

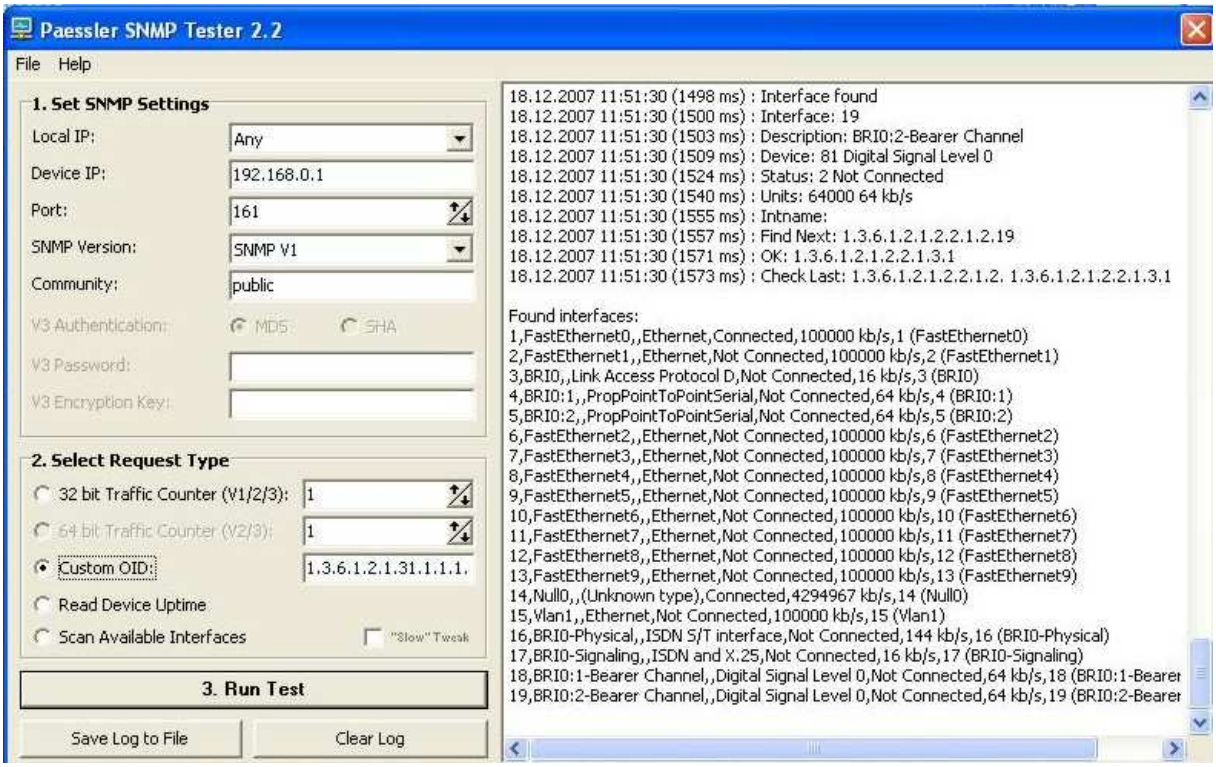
Zdroj: http://www.paessler.com/download/freeware/snmptester

Typ licence: Freeware

Funkčnost: SNMP Tester

Instalace: přímé spouštění

Paesler SNMP Tester je, jak už název napovídá, tester SNMP protokolu. Umožňuje testování SNMP všech verzí (1, 2c, 3). Tento nástroj není určen pro monitoring sítě, spíš je určen na testování a diagnostiku SNMP a doplňuje výše uvedené nástroje. Má jednoduché uživatelské rozhraní, které je zachyceno na obrázku níže. Kromě několika předdefinovaných SNMP OID je možné odeslat i vlastní (Cystom OID). Tento prográmek je možné využít pro ověření nastavení SNMP agenta v síťových zařízeních.



Závěr

Pro grafický monitoring sítě lze v Internetu nalézt několik programů, které jsou uvedeny výše. Výčet zřejmě není kompletní, ale měl by obsahovat ty nejzajímavější volně dostupné programy. S volně dostupnými nástroji pro management sítě je situace o dost horší. Žádný s nalezených programů nepodporoval dostatečně jednoduchý a pohodlný management síťových prvků. Možná je tato situace způsobena také nedostatečným zabezpečením SNMPv1, který je stále nerozšířenější verzí SNMP protokolu.

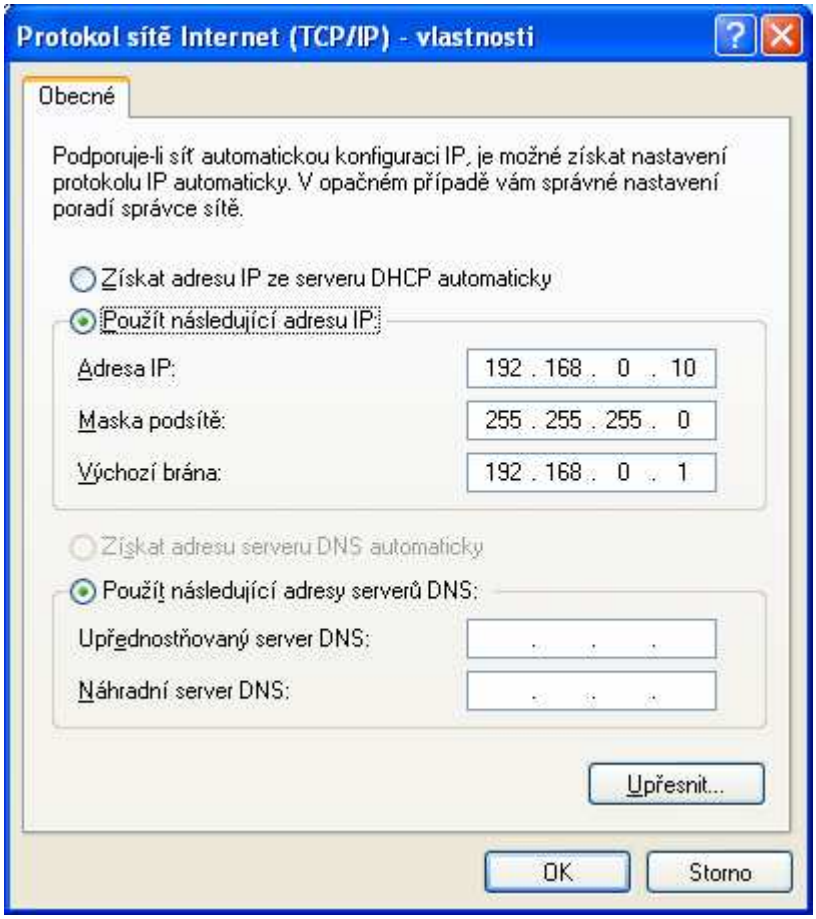
Na monitoring sítě je dle mého názoru zajímavý program InterMapper, který má však tu nevýhodu, že je zdarma jen pro 5 zařízení v síti, což by ale například pro většinu domácích použití mělo stačit. Pro management Cisco zařízení je zajímavý nástroj CSNMP, který umožňuje vyčítání, nahrávání a zálohování konfigurace.

Seznam zkratek

CDP	Cisco Discovery Protocol
JRE	Java Runtime Environment
MIB	Management Information Base
OID	Object Identifier
SNMP	Simple Network Management Protocol

Příloha

Konfigurace počítače NB_KORDAS



Konfigurace směrovače RF

Konfigurace je vyčtená pomocí výše uvedeného nástroje CSNMP-Tools. Významné řádky konfigurace jsou tučně.

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RF
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
!
ip cef
!
!
!
multilink bundle-name authenticated
!
```

```
!
!
!
!
!
!
!
!
!
interface FastEthernet0
 ip address 192.168.0.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1
 ip address 10.0.0.1 255.255.255.0
 duplex auto
 speed auto
!
interface BRI0
 no ip address
 encapsulation hdlc
 shutdown
!
interface FastEthernet2
!
interface FastEthernet3
!
interface FastEthernet4
!
interface FastEthernet5
!
interface FastEthernet6
!
interface FastEthernet7
!
interface FastEthernet8
!
interface FastEthernet9
!
interface Vlan1
 no ip address
!
!
!
no ip http server
no ip http secure-server
!
snmp-server community private RW
!
!
!
!
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
end
```

Konfigurace přepínače SW4

Konfigurace je vyčtená pomocí výše uvedeného nástroje CSNMP-Tools. Významné řádky konfigurace jsou tučně.

```
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname SW4
!
!
no aaa new-model
ip subnet-zero
!
!
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
```

```
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 10.0.0.2 255.255.255.0
 no ip route-cache
!
ip http server
snmp-server community private RW
!
control-plane
!
!
line con 0
line vty 5 15
!
end
```