Není datům v síti těsno?
Způsoby monitorování podnikových sítí (preliminary version)

Petr Matoušek

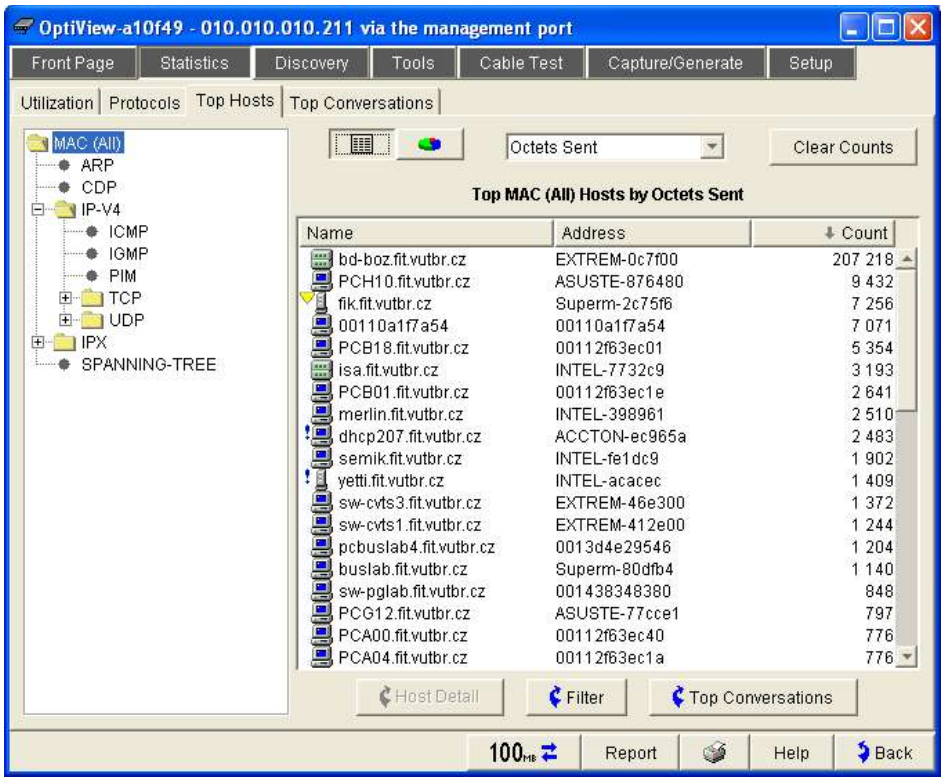
Abstrakt

Nárůst počítačů v podnicích v České republice se za posledních pět let rapidně zvětšil. U většiny firem a organizací už neplatí, že by více lidí sdílelo jeden počítač. I v malé firmě můžeme najít pár desítek počítačů a síťových zařízení. Nejedná se pouze o pevně připojené stroje, ve stále větší oblibě jsou mobilní klienti - notebooky, PDA a další mobilní zařízení. S nárůstem počtu zařízení vznikají nároky na jejich správu a údržbu. Ta se netýká jenom připojení zařízení do sítě, správné nastavení sítě a detekce chyb. Důležitý je také průběžné monitorování provozu, sledování výkonu a využití linek s cílem odhadnout budoucího vývoj a potřeby sítě. Tento článek popisuje některé přístupy ke správě a monitorování sítí a představuje nástroje, které mohou administrátorům ulehčit jejich práci při správě sítě.

Monitorování, sledování, analýza. Není to totéž?

Když se někoho zeptáte, co znamená spravovat síť, obvykle vám odpoví, že jde o propojení počítačů, nastavení základních síťových služeb a údržba sítě. Nebude se mýlit, je to tak. Jenže to není všechno. K činnosti síťového administrátora patří také sledování výkonu sítě, odhalování chyb a výpadků, detekce útoků a reakce na neobvyklé situace. Tyto činnosti můžeme souhrnně nazvat monitorováním nebo sledováním provozu. Pomocí monitorování sítě zjišťujeme – aktivně či pasivně, zda dané zařízení pracuje, zda je linka v provozu a jak je vytížena.

Monitorování sítě může být krátkodobé (zapnu si síťových analyzátor a sleduji typy a počty přenesených dat v daném okamžiku) nebo dlouhodobé (sbírám údaje o přenesených datech po dobu několika dnů, týdnů, měsíců). Výsledkem krátkodobého monitorování sítě jsou informace o výpadcích, chybách, přetečení front apod., které mohou být zasílány administrátorovi ve formě událostí či alarmů. U dlouhodobého sledování sítě jsou výsledkem statistické údaje ve formě grafů, které pomohou detekovat slabá místa v sítích a naplánovat další investice – např. zvýšení kapacity linky, rozdělení služby na více serverů, přesunu rutinních činností serveru mimo hlavní čas přenosů apod. Příklad výsledku krátkodobého monitorování provozu můžeme vidět na následujícím obrázku, kde vidíme počítače s maximálním přenosem zjištěným v konkrétním čase.



Dalším pojmem je analýza dat. Analýzou dat či datového toku rozumíme konkrétní rozbor přenášených dat, kdy nezkoumáme pouze hlavičky linkových či síťových protokolů, ale díváme se na obsah paketů. Datový analyzátor naslouchá na sdíleném médiu a zobrazuje data, která se po něm přenášejí. Zachytávání a zpracování protokolových jednotek on-line je při rychlostech v řádu stovek Mb/s prakticky nerealizovatelné (kromě na specializovaných zařízení). Z tohoto důvodu většina analyzátorů data nejprve snímá (data capturing) a teprve potom nad nimi provádí analýzu. Výsledkem analýzy dat může být např. detekce ARP datagramů, které vysílá špatně nakonfigurovaný přepínač, zjištění existence paketů s privátními adresami na vnějším rozhraní podnikové sítě (což jsme v praxi také řešili) či jiné problémy.

Monitorování sítě, analýza dat a další techniky správy sítí nám pomáhají hledat odpovědi na následující otázky:

- Jaká je vytíženost jednotlivých linek, zejména páteřních spojů – z pohledu časového (v kterou dobu jsou zátěžové špičky a jaké jsou reálné odezvy) a aplikačního (který typ dat/požadavků převažuje)?
- Jaký je objem přenášených dat, jaký je směr největších toků? Které uzly nejvíce komunikující? Jaké protokoly zabírají největší procento šířky přenosového pásma?
- Je komunikace uživatelů bezpečná? Používají uživatelé šifrovaná spojení ?
- Co znamená náhlé zvýšení objemu přijímaných dat např. během víkend? Jedná se o cílený útok na síť? Jak můžeme detekovat a izolovat útočníka?
- Kde se nachází počítač/přepínač, který posílá do sítě chybná data a způsobuje výpadky?

Na čem je založeno monitorování sítí

Než si ukážeme konkrétní typy nástrojů pro sledování a analýzu sítí, podívejme se na základní techniky pro sledování stavu sítě.

Zjišťování informací o stavu sítě – dostupnosti síťových zdrojů, rychlosti přenosu, spolehlivosti spojení – není v oblasti komunikací nic nového. Už při vzniku Internetu byly vytvořeny postupy, jak zajistit základní monitorování sítě. Překvapivé však je, že tyto základní techniky jsou natolik kvalitní, že tvoří základ dnešních nástrojů pro testování stavu sítí. Mám na mysli především stařičký protokol ICMP definovaný standardem RFC 792 v roce 1981, a o trochu novější protokol SNMP z let devadesátých. Podívejme se trošku na ně.

ICMP – Internet Control Message Protocol
Protokol ICMP je součástí IP vrstvy modelu TCP/IP a slouží k předávání chybových hlášek o problémech IP komunikace. ICMP definuje pouze 11 typů zpráv, z nichž nejznámnější jsou asi zprávy Echo (typ 8), Echo Reply (typ 0) a Destination Unreachable (typ 3). Nástroje pro diagnostiku sítí typu ping či traceroute využívají právě protokol ICMP. Nad protokolem ICMP jsou postaveny i další diagnostické nástroje, např. nmap pro skenování portů a jiné. Zájemcům o podrobnější informace doporučuji přímo standard RFC 792, který je dostupný na Internetu a – na rozdíl od jiných RFC – se velice dobře čte.

SNMP – Simple Network Management Protocol
Systém správy sítě postavené nad protokolem SNMP definuje dva druhy zařízení – sledovaná zařízení (managed devices), která uchovávají statistické údaje o své činnosti , a centrální řídící stanici NMS (network management station), která získává informace ze sledovaných zařízení, analyzuje je a zobrazuje administrátorovi sítě.

Samotný protokol SNMP slouží pouze k přenosu údajů o stavu sítě. Je tvořen jednoduchými příkazy typu načti data (get, get-next), zapiš data (set), pošli zprávu (trap, notification) a několika řídícími příkazy (inform, report). Nejzajímavější na architektuře systému správy sítě SNMP je databáze dat obsahující informace např. o síťových přenosech, konfiguraci zařízení apod., které se říká MIB (Management Information Base). MIB definuje typy sledovaných dat v daném zařízení a jejich jednoznačnou identifikaci pomocí hodnoty OID (object identifier). Monitorování sítě pomocí SNMP spočívá ve zjišťování vybraných hodnot SNMP zařízení (počítačů, přepínačů, směrovačů) a jejich následné zpracování.

Příkladem sledovaných hodnot může být například počet přenesených dat na daném portu přepínače (interfaces.ifTable.ifEntry.IfInOctets.6), číslo portu pro danou MAC adresu (dotldTpFdbEntry.dotldTpFdbPort.8.0.9.50.98.244).

Kromě těchto dvou základních techniky můžeme najít i jiné způsoby sledování sítě – specializované aplikace komunikující proprietárními protokoly, vyšší (aplikační) protokoly pro přenášející síťové statistiky a podobně. Nicméně první dva uvedené způsoby patří ke standardům správy sítě.

Chtěl bych podotknout, že dobrá znalost základních monitorovacích technik hodně pomůže při výběru a používání nástrojů pro sledování sítě. Základní pravidlo říká, že nástroj využívající konkrétní techniku (ICMP, SNMP) nemůže provádět více činností, než zmíněný protokol podporuje. Pokud například komunikuji protokolem ICMP, nemůžeme očekávat, že analyzátor zobrazí hodnoty z MIB databáze uložené na sledovaném zařízení. Počet přenesených dat se z ICMP prostě nedozvím. Podobně je na tom i protokol SNMP. Při jeho používání je dobré si uvědomit, že používá nespolehlivý přenos UDP. V případě zahlcení sítě se nám může stát, že SNMP zpráva (např. typu trap) o dosažení kritického zatížení výstupní linky přepínače, nám vůbec nedojde. Přes jednoduché chování mají tyto protokoly v oblasti správy sítí nezastupitelné místo.

Nástroje pro sledování sítě a analýzu datových toků

Kdo se pohybuje v oblasti správy sítí, asi ví, že nástrojů pro sledování a analýzu sítí je velké množství

– ať už hardwarových (síťové analyzátory, testery, specializovaná zařízení) či softwarových (komerčních i volně dostupných). V tomto článku bych chtěl představit základní třídy nástrojů, se kterými se můžeme setkat, popsat jejich základní vlastnosti a uvést příklady těchto nástrojů. Nástroje spíše představím, než abych se zabýval jejich srovnáním. To může být náplní některého dalšího čísla Connectu.

1. Nástroje pro monitorování sítě

Nástroje pro monitorování sítě zjišťují aktuální stav sítě a detekují neočekávaných událostí v síti, např. chyby na aktivních prvcích, útoky, problémy přenosové linky apod. Monitorování stavu sítě je kritické zejména u komerčních organizací, které nabízející připojení dalším subjektům. Každý výpadek nějaké služby či linky musí být okamžitě detekován a vyřešen. Monitorování zahrnuje testování stavu připojených zařízení (serverů, přepínačů, tiskáren) nebo síťových služeb (dostupnost poštovního serveru, WWW serveru, DNS serveru).

1.1 Krátkodobé monitorování

Pro krátkodobé monitorování sítě můžeme použít klasické unixové příkazy typu ping, telnet, netcat, tracerouter, netstat založené především na protokolu ICMP. Existují i specializované aplikace jako např. sysmon (pro sledování stavu zařízení či linky pomocí protokolů třetí a vyšší vrstvy), program Neo vyvinutý na MIT, který zjišťuje údaje o zařízeních připojených na přepínači, přenosové statistky a další, nebo program Oak pro sběr a předávání hlášení z programu syslogd (oba tyto programy lze najít na www.ktools.org).

1.2 Dlouhodobé monitorování

V případě dlouhodobého monitorování sítě sbíráme statistické údaje o činnosti sítě pomocí SNMP. Implementace protokolu SNMP, která bývá součástí unixových systémů (např. balík net-snmp, www.net-snmp.org) není sama o sobě příliš vhodný pro dlouhodobé monitorování. Vhodnější je použít nástroje, které umožňují nejen získání dat, ale i jejich zpracování a prezentaci. Klasickým příkladem je nástroj MRTG (Multi Router Traffic Grapher) pro generování statistik provozu, nebo již dříve zmíněný program Neo.

1.3 Monitorování toku dat

Zvláštní skupinu tvoří nástroje pro sledování toku dat Netflow. Netflow je protokol vytvořený firmou Cisco. Tento protokol analyzuje přenos jako souvislý tok dat mezi vzdálenými uzly. Narozdíl od jiných nástrojů se Netflow nezabývá pouze jednotlivě přenášenými datagramy a pakety, ale sleduje celý tok. Tok je charakterizován zdrojovou adresou a portem, cílovou adresou a portem, číslem IP protokolu, typem služby a případně dalšími hodnotami. Analyzátor Netflow toků vytváří pro každý tok samostatný záznam a zjišťuje dobu například trvání toku, počet přenesených dat.

V současné době se monitorování toku dat stává novou doménou sledování stavu sítě. Analýzu Netflow provádějí především zařízení od firmy Cisco či Juniper, lze však nalézt i softwarové nástroje pro detekci a správu toků – např. Flow-Tools od Marka Fullmera (www.splinetered.net/sw/flow-tools) nebo balík ng_flow, který je součástí portu FreeBSD.

Softwarové analyzátory jsou limitovány rychlostí sledovaných toků. Obvykle jsou schopny analyzovat toky do rychlosti 100 Mb/s. Pro vyšší rychlosti je potřeba použít specializovaný hardware. Příkladem může být například sonda Netflow, která pracuje na rychlostech 300 – 700 Mb/s v závislosti na délce paketů. Tato sonda je vyvíjena v rámci projektu Geant2 a podílejí se na ni i VŠ v ČR (např. FIT VUT, FI MU v Brně). Sonda je implementována na přídavné kartě počítače pomocí programovatelného pole FPGA a umožňuje uchovávat informace až o 64 000 datových tocích.

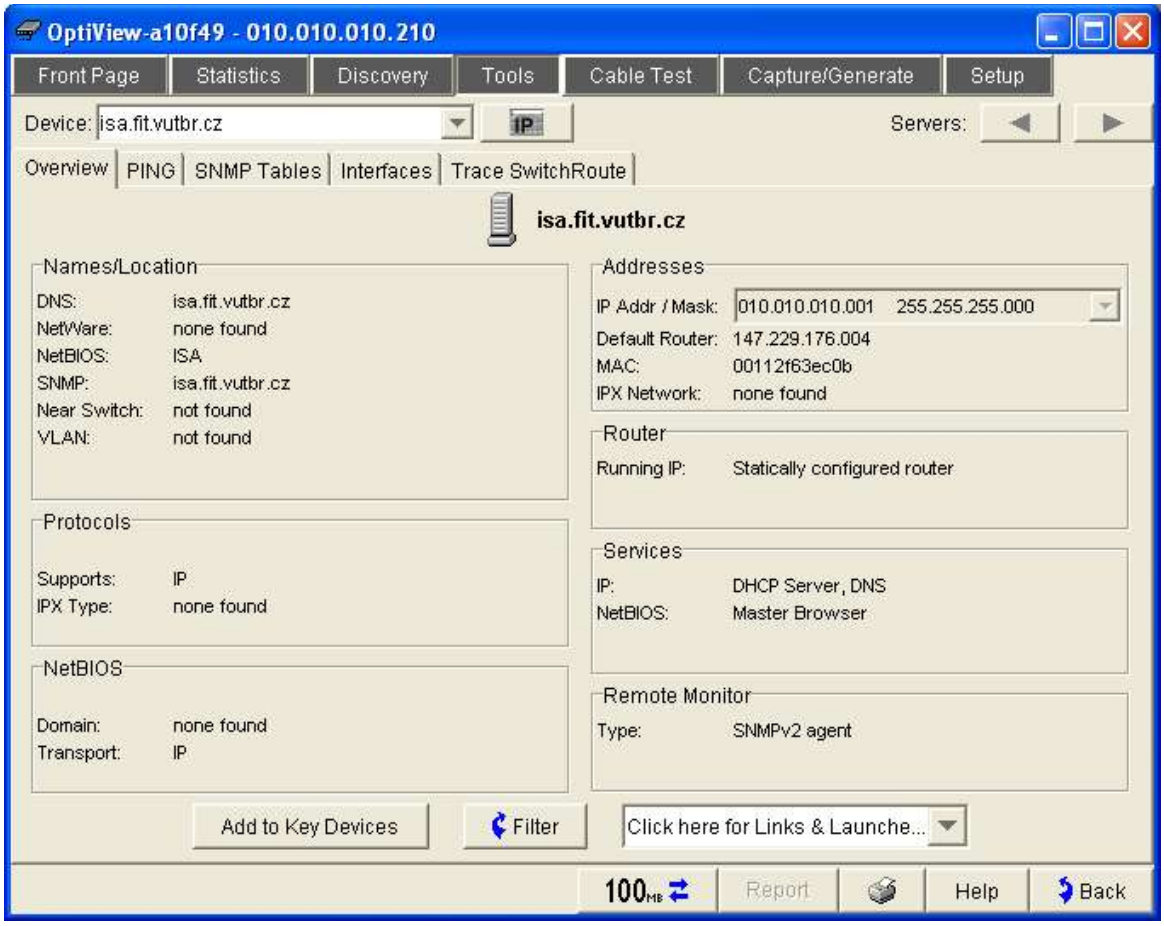
2. Nástroje pro analýzu dat

Druhou skupinou nástrojů jsou nástroje pro analýzu dat. Tyto nástroje jsou opět softwarové či

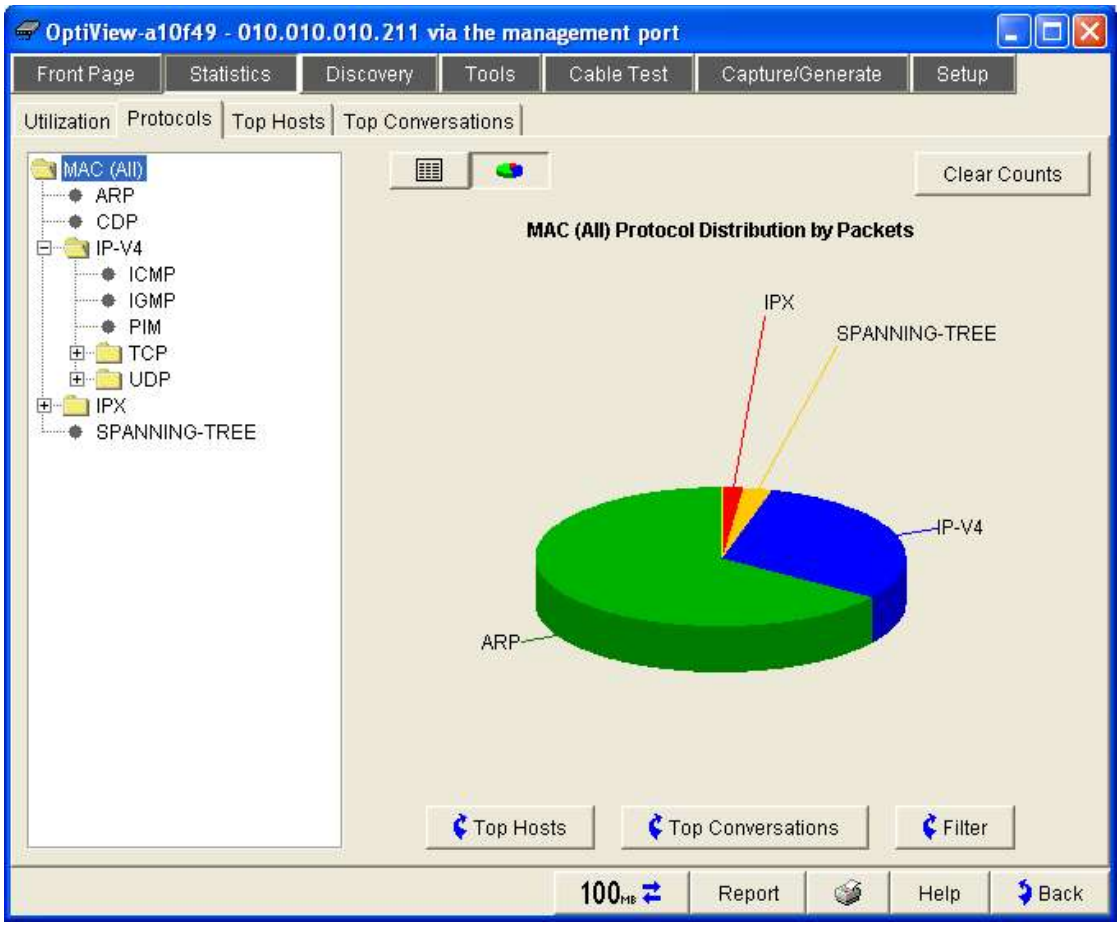
hardwarové. Analýza může probíhat buď v reálném čase (např. pomocí techniky kopírování provozu na daném portu, port mirroring) nebo analýzou zachycených data (uložení zachycených dat a jejich následná analýza).

Asi nejoblíbenější programy pro analýzu jsou tcpdump a ethereal. Oba programy umí zachytávat rámce linkových protokolů a analyzovat. Umožňují sledovat data na rozhraní počítače, kde běží. Pokud nastavíme tzv. promiskuitní režim, zachytávají i datový tok, který není určen přímo pro jejich rozhraní, ale přenáší se po sdíleném médiu. Tcpdump i ethereal (www.ethereal.com) umožňují data filtrovat a analyzovat, získávat různé statistiky a další informace.

Z hardwarových nástrojů můžeme použít například OptiView od firmy Fluke Networks, který kombinuje zkoumání sítě, statistické analýzy a zachytávání paketů. Zařízení sleduje provoz na síti (aktivně i pasivně), vytváří přehled o zapojených zařízeních, detekuje služby a protokoly, s kterými stanice komunikují a vytváří seznamy sítí připojených na přepínač. Slouží i k detekci chyb a nekonzistentních nastavení v síti. Na následujícím obrázku můžeme vidět informace o detekovaném serveru – kromě adres (IP i MAC) vidíme spuštěné služby a podporované protokoly.



Kromě celkové analýzy toků provádí i statistickou analýzu provozu. Při analýze sítě si můžeme nechat vypsat například seznam nejvíce komunikujících uživatelů a sledovat typy přenosu, které daná zařízení využívají.



Kromě výše uvedených nástrojů existují i knihovny pro jazyky Perl, Java, C/C++, které umožňují napsat si vlastní nástroj pro získávání dat ze SNMP zařízení a jejich analýzu. Oblíbené jsou zejména unixové skripty, které sledující kritické hodnoty na zařízeních a v případě jejich překročení pošlou administrátorovi zprávu.

Závěr

V tomto článku jsme si ukázali základní techniky a nástroje pro sledování provozu na síti, zjišťování úzkých míst a detekci chyb. Výběr a jejich nasazení závisí na požadavcích organizace. Cíl je však stejný - napomoci administrátorům při správě sítí.