Využití technologie EtherChannel a NetFlow v počítačových sítích

Use of EtherChannel and NetFlow technology in computer networks

Bc. Pavel Kaláb

Diplomová práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

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

Jméno a příjmení:	**Bc. Pavel KALÁB**
Osobní číslo:	**A08737**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Počítačové a komunikační systémy**
Téma práce:	**Využití technologie EtherChannel a NetFlow v počítačových sítích**

Zásady pro vypracování:

1. **Proveďte literární rešerši na dané téma.**
2. **Vyhledejte, vyzkoušejte a popište programy pro sběr NetFlow dat.**
3. **Popište další možnosti sledování a analýzy provozu v počítačových sítích.**
4. **Zrealizujte a otestujte konfiguraci EtherChannel a NetFlow na zařízeních učebny.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **Cisco Systems. EtherChannel [online]. [2003] [cit. 2009-06-10]. Dostupný z WWW: http: //www.cisco.com/en/US/tech/tk389/tk213/ tsd_technology_support_protocol_home.html.**
2. **Cisco Systems. Understanding EtherChannel Load Balancing and Redundancy on Catalyst Switches [online]. [2007] [cit. 2009-06-10]. Dostupný z WWW: http://www.cisco.com/en/US/tech/tk389/tk213/ technologies_tech_note09186a0080094714.shtml.**
3. **Cisco Systems. Introduction to Cisco IOS NetFlow – A Technical Overview [online]. [2007] [cit. 2009-06-10]. Dostupný z WWW: http: //www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ ps6555/ps6601/prod_white_paper0900aecd80406232.html.**
4. **OREBAUGH, Angela. Wireshark a Ethereal : kompletní průvodce analýzou a diagnostikou sítí. 1. vyd. Brno : Computer Press, 2008. 444 s. ISBN 978-80-251-2048-4.**
5. **DONDICH, Taylor. Network Monitoring with Nagios. 1st edition. Sevastopol : O'Reilly, 2006. 62 s. Dostupný z WWW: http://knihovna.utb.cz. ISBN 978-0-596-52819-5.**
6. **HORÁK, Jaroslav, KERŠLÁGER, Milan. Počítačové sítě pro začínající správce. 4. rozš. vyd. Brno : Computer Press, 2008. 327 s. ISBN 978-80-251-2073-6.**

Vedoucí diplomové práce: **Ing. Jiří Korbel**
Ústav počítačových a komunikačních systémů

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

Termín odevzdání diplomové práce: **7. června 2010**

Ve Zlíně dne 19. února 2010

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

prof. Ing. Karel Vlček, CSc.
ředitel ústavu

ABSTRAKT

Diplomová práce popisuje problematiku počítačových sítí, přesněji řečeno možnosti agregací a sledováním sítě. Teoretická část je především zaměřena na objasnění základních pojmů v počítačových sítích a na jednotlivé možnosti nastavení technologii EtherChannel a NetFlow. V praktické části je popsáno, jakým způsobem je možno nastavit tyto technologie na prvcích od společnosti CISCO. A následně bylo otestováno, jak je dané nastavení efektivní.

Klíčová slova: počítačová síť, EtherChannel, NetFlow, agregace linek, sledování sítě, IOS.

ABSTRACT

This thesis describes problems of computer networks, more precisely the possibilities of aggregating and monitoring of networks. The theoretical part is mainly focused on clarification of fundamental concepts in computer networks and various options of EtherChannel and NetFlow technology. The practical part describes how these technologies can be configured using elements from CISCO company. The setting effectiveness was tested afterwards.

Keywords: Computer network, EtherChannel, NetFlow, aggregation link, network monitoring, IOS.

Tímto bych chtěl poděkovat vedoucímu diplomové práce ing. Jiřímu Korbelovi za zadání, vedení a další neocenitelnou pomoc při zpracování tématu.

Dále bych rád poděkoval své rodině a blízkým, za morální a finanční podporu při mém studiu.

Bc. Pavel Kaláb

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

Osobní počítače dnes nenalézáme pouze v podnicích a ani nezabírají prostory jedné větší místnosti. Dnes jsou počítače takřka všude. Člověku usnadňují práci, poskytují zábavu a v neposlední řadě poskytují informace a napomáhají k vzdělávání. Ale aby toto všechno mohly počítače poskytnout, je potřeba, aby byly schopny vyměňovat si navzájem informace. Ještě před několika lety měla tato výměna informací podobu diskety a „kurýra“, který disketu přenášel. Jak tedy taková výměna vypadala? Odpověď je velice jednoduchá, pokud bylo potřeba vytisknout dokument a tiskárna zrovna nebyla připojena právě k danému počítači, musel se dokument nahrát na disketu, kterou „kurýr“ přenesl a vložil do jiného počítače, ke kterému již byla připojena tiskárna. Tento postup si v dnešní době umí představit asi málo kdo. Tuto „kurýrní“ službu dnes vykonává počítačová síť.

Počítačová síť má mnohé výhody jak pro firmy, tak pro domácnosti. Dnes již má skoro každý doma více než jeden počítač. Mezi výhody patří: dokumenty jsou aktuální, k tisku postačuje jedna tiskárna, sdílení dokumentů, atd.

Ale jak zabezpečit, že síť bude stále dostatečně rychlá i po několik let. Informační technologie jdou dopředu mílovými kroky. Jednou možností je využití technologie EtherChannel, kdy správce sítě může zvyšovat šířku přenosového pásma pouhým přidáváním kabelů mezi přepínači. To zaručuje, že rychlost sítě je dimenzovaná na pár let dopředu. U této technologie je možná postupná agregace linky, což je v dnešní uspěchané době jistě výhoda.

Druhá technologie, která je popsána v této práci, je taktéž velice aktuální a nazývá se NetFlow. Jedná se o sledování provozu v síti. Pro používání této technologie jsou hned tři celkem vážné důvody. Tím prvním je, že většina firem si hlídá, co její zaměstnanci dělají v síti a tím pádem v pracovní době (např.: jaké stránky si prohlížejí). Druhý důvod: poskytovatelé si účtují peníze za odeslaná/přijatá data. Poslední důvod? Ze zákona musí poskytovatelé telekomunikačních technologií uchovávat data o tom, co klienti na síti dělali. (Např.: jaké stránky navštívili, co si stáhli z Internetu) po několik dní. Daly by se najít jistě i další důvody proč je tato technologie momentálně v „kurzu“, ale tyto tři jsou jistě postačující.

I. TEORETICKÁ ČÁST

1 POČÍTAČOVÁ SÍŤ

1.1 Definice

Počítačová síť je souhrnné označení pro technické prostředky, které realizují spojení a výměnu informací mezi počítači. Umožňují tedy uživatelům komunikaci podle určitých pravidel, za účelem sdílení využívání společných zdrojů nebo výměny zpráv. [1]

1.2 Rozdělení

1.2.1 Podle rozsahu

- PAN (Personal Area Network)

  Jedná se o malé osobní sítě, které mají dosah jenom několik desítek metrů. Slouží potřebám jednotlivců nebo malých skupin lidí. V naprosté většině případů se používají pro propojení např.: mobilních telefonů, osobních počítačů, notebooků, PDA, atd. Tyto spoje bývají provedeny pomocí technologií Bluetooth nebo IrDA.

- LAN (Local Area Network)

  Jedná se o sítě, které svojí velikostí nepřesahují rámec jedné budovy. Většinou se jedná o sítě jednotlivých organizací či podniků. Řádově může síť LAN obsahovat několik desítek nebo až stovek počítačů. Tyto sítě jsou spravovány menší skupinou správců.

- CAN (Cosmopolitan Area Network)

  Tento druh sítě není příliš známý a ani nejsou jasně dané hranice, o jak velký segment sítě se jedná. Dalo by se říci, že se jedná o propojení několika sítí LAN. Např.: síť společnosti, která má ve městě několik budov.

- MAN (Metropolitan Area Network)

  Jak z názvu vyplývá, jedná se o síť v jednom městě. Nastává tu problém s vytyčením hranice, kde tato síť začíná a kde končí. Je to jakýsi přechod mezi CAN a WAN. Např.: propojení několika bytových jednotek.

- WAN (Wide Area Network)

  Skládá se z jednotlivých sítí LAN. Většinou obsahuje až tisíce počítačů a o takto rozlehlou síť se starají správcovské skupiny, které jsou na sobě nezávislé.

- GAN (Global Area Network)

  Jedná se o celosvětovou síť = INTERNET.

Toto je velice podrobné rozdělení sítě ohledně rozlohy ve většině dnes dostupné literatuře se uvádí rozdělení pouze na tři části: LAN, MAN, WAN.

1.2.2 Podle přístupu

- Client – Server

  V této koncepci je v síti umístěna jedna nebo více datových stanic (tzv. SERVER) a ostatní počítače (CLIENT) jsou přes další síťové periferie, k této stanici připojeny. Z toho vyplývá, že je pevně určeno, která stanice (počítač) je klient, a která je server. Tato koncepce je vhodná pro větší sítě (nad cca 10 počítačů).

- Peer to peer

  Tato koncepce je na rozdíl od předešlé vhodnější pro menší sítě (do cca 10 počítačů). Sítě peer to peer se odlišují od sítí klient – server tím, že zde není určeno, která stanice (počítač) je server a která klient. Žádný počítač není

stále server ani klient a zároveň v jakýkoliv okamžik může být jakákoliv stanice klientem nebo serverem.

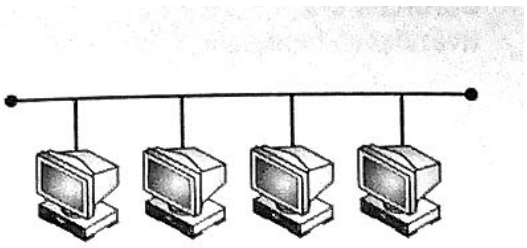
1.3 Topologie

Termín „topologie“ označuje způsob, jakým jsou počítače a další zařízení v síti propojeny kabely. Konkrétní typ kabelu, který je použit, stanovuje topologii dané sítě. Pro instalaci každého konkrétního kabelu je nutné použít správnou technologii. Třemi hlavními topologiemi sítě LAN jsou sběrnicová, hvězdicová a kruhová, ale v této kapitole jsou popsány všechny dosud známé topologie: sběrnicová, hvězdicová, hybridní, hierarchická, kruhová, úplná a bezdrátová.

1.3.1 Sběrnicová topologie

Ve sběrnicové topologii jsou počítače a jiná zařízení propojeny v jedné linii a každý systém je kabelem spojen s dalším systémem. Tato konfigurace se často označuje jako uzavřený cyklus. Všechny signály, přenášené systémy v síti procházejí podél sběrnice v obou směrech všemi systémy, než dosáhnou svého cíle. Sběrnicová topologie má vždy dva otevřené konce, které musí být zakončeny elektrickými rezistory tak, že se signály neodrážejí zpět do opačného směru, což by vedlo k interferenci s novějšími přenášenými signály. Chybějící zakončení u jednoho z konců může zabránit správné komunikaci počítačů připojených k dané sběrnici. Kabeláž může mít ve sběrnicové topologii dvě podoby, tlustý a tenký koaxial. V dnešní době se tato topologie už nevyužívá.

Hlavní nevýhodou sběrnicové topologie je to, že jakékoliv poškození kabelu, vadná koncovka nebo špatný konektor ovlivňují funkčnost celé sítě. [2]

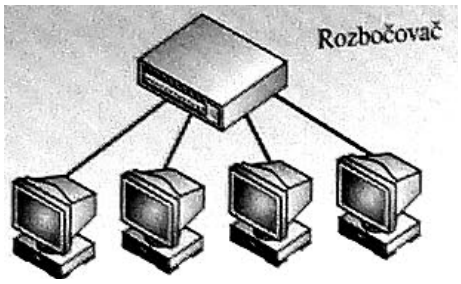


Obr. 1 *Sběrnicová topologie*

1.3.2 Hvězdicová topologie

Hvězdicová topologie používá centrální zařízení nazývané rozbočovač nebo koncentrátor. Každý počítač je připojen k rozbočovači samostatným kabelem. Používaným přenosovým médiem u této topologie je kroucená dvojlinka, jako je 10BaseT a 100BaseT. Hvězdicovou topologii používá většina sítí Ethernet LAN a mnoho sítí LAN používajících jiné protokoly. I když je každý počítač připojen k rozbočovači samostatným kabelem, rozbočovač šíří všechny signály vstupující kterýmkoli z jeho portů do všech dalších portů. Tímto způsobem jsou všechny signály odesílané každým z počítačů v síti přijaty všemi zbývajícími počítači.

Protože má každý počítač vlastní vyhrazené připojení k rozbočovači, je hvězdicová topologie odolnější vůči chybám než sběrnicová topologie, přičemž poškození jednoho z kabelů neovlivňuje zbývající část sítě. Ovlivněn je pouze počítač, který je tímto kabelem připojen. Nevýhodou je použití dalšího hardware – rozbočovač, pokud ten selže, ovlivní to celou síť, která je k němu připojena. [2]



Obr. 2 *Hvězdicová topologie*

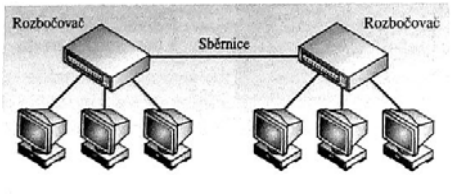
1.3.3 Hvězdicová a sběrnicová topologie

Hvězdicová a sběrnicová topologie je metodou, která se používá k rozšíření velikosti sítě LAN o více než jednu hvězdici. Síť LAN se rozšíří spojením několika hvězdicových se samotným segmentem sběrnicového kabelu pro vzájemné propojení jejich rozbočovačů. Každý rozbočovač odesílá příchozí data prostřednictvím sběrnicového portu a zároveň i hvězdicovým portem, což umožňuje všem počítačům v síti LAN komunikovat mezi sebou. Tato topologie byla původně určena pro rozšíření sítí 10BaseT Ethernet, avšak

kvůli snížení výkonu sítě způsobeného pomalostí koaxiálních sběrnicových sítí se v dnešní době používá jen velmi zřídka. [2]

1.3.4 Hierarchická hvězdicová topologie

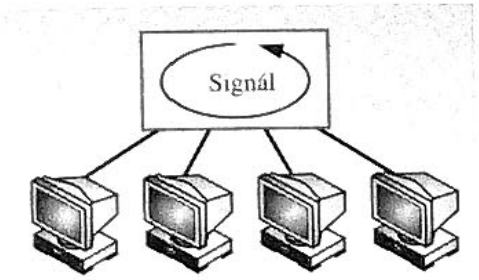
Pokud je potřeba rozšíření hvězdicové sítě z původního rozbočovače, implementuje se hierarchická hvězdicová topologie (též známá jako topologie stromová). Pro rozšíření hvězdicové sítě jednoduše připojíme původní rozbočovač k druhému pomocí standardního kabelu připojeného ke speciálnímu portu, který je označován jako vzestupný port a slouží k tomuto účelu. Data, která dorazí k jednomu z rozbočovačů, jsou předána oběma rozbočovačů stejně jako počítačům připojených k síti. [2]



Obr. 3 *Hierarchická hvězdicová topologie*

1.3.5 Kruhová topologie

Kruhová topologie se podobá sběrnicové topologii v tom, že každý počítač je propojený s dalším počítačem. Místo ukončení obou konců jsou však tyto spojeny dohromady ve formě kruhu. Toto spojení způsobuje, že signály cestují cyklicky od jednoho počítače k dalšímu a nakonec se vrátí k počátečnímu bodu. Ve většině případů je kruhová topologie striktně logickou konstrukcí, a ne fyzickou, protože kabely v kruhové topologii připojují se k rozbočovači a tvoří spíše hvězdici. V kruhové topologii se může použít několik typů kabelů. Sítě FDDI používají kruhovou topologii s optickým kabelem, zatímco sítě Token Ring používají kroucené dvojlinky. Stejně jako topologie BUS se tato topologie už nevyžívá. [2]

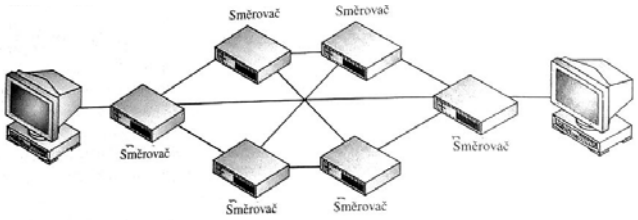


Obr. 4 *Kruhová topologie*

1.3.6 Úplná topologie

Použití úplné technologie v síti LAN není praktické. Každý počítač má vyhrazené připojení ke každému počítači v úplné síti LAN. Tato topologie je praktická pouze ve dvou-uzlové síti. Úplná síť se třemi a více počítači by vyžadovala samostatnou kartu NIC pro každý další počítač v síti. Například sedmiuzlová síť by vyžadovala, aby každý počítač měl nainstalováno 6 karet NIC. Ačkoliv je použití této topologie v síti LAN nepraktické, poskytuje výbornou odolnost vůči chybám. Jedno chybné místo může ovlivnit pouze jeden počítač a ne celou síť.

Tato topologie je běžná u rozsáhlých sítí, protože zajišťuje odolnost vůči možnému chybnému fungování, jako je poškození kabelu, rozbočovače a směrovače. [2]



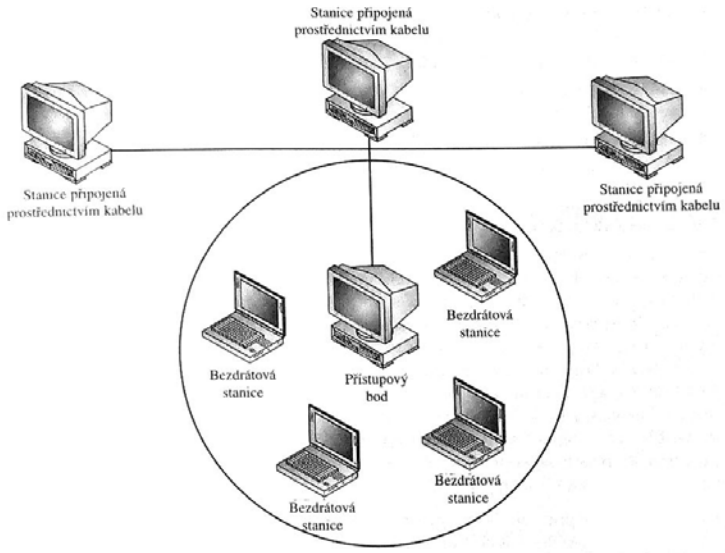
Obr. 5 *Úplná topologie*

1.3.7 Bezdrátová topologie

Ačkoliv termín „topologie“ obvykle označuje uspořádání kabelů v síti, nemusí tak tomu být vždy. Bezdrátové sítě používají to, co se označuje jako nevázaná media, která jsou formou radiových nebo světelných vln tvořících určité vzorky, které mohou počítače používat ke vzájemné komunikaci. Existují dvě základní bezdrátové topologie:

infrastrukturní a ad-hoc. Infrastrukturní síť se skládá z bezdrátově zařízených počítačů, které komunikují se sítí prostřednictvím bezdrátových vysílačů (místa přístupu k síti), které jsou připojeny k síti standardními kabely. V této topologie nekomunikují počítače vzájemně mezi sebou, ale se sítí přes bezdrátové vysílače. Tato topologie je nejvýhodnější pro rozsáhlé sítě s několika bezdrátovými počítači, které spolu nepotřebují komunikovat, jako jsou například přenosné počítače cestujícího obchodního zástupce. Topologie ad-hoc se skládá ze skupiny počítačů, které jsou vybaveny bezdrátovými kartami NIC a jsou schopné komunikovat mezi sebou.

Nevýhodou obou těchto bezdrátových topologii je to, že počítače musí zůstat v komunikační oblasti bezdrátové technologie. Tato topologie je vhodnější pro domácí či menší kancelářské sítě, kde není instalace kabelů praktická. [2]



Obr. 6 *Bezdrátová topologie*

1.4 Části počítačové sítě

1.4.1 Pasivní prvky

Obecně by se dalo říci, že mezi tyto prvky patří vše, co napomáhá k technické realizaci počítačové sítě. Patří mezi ně vodiče (koaxiální kabel, UTP, STP, Optický kabel, atd.) a jejich zakončovací a propojovací součásti (zásuvka RJ-45, Propojka RJ-45,

konektory: RJ-45, SC, ST, BNC, atd.). Dále sem řadíme součásti, které napomáhají realizaci sítě (Patch panely, Racky, atd.).

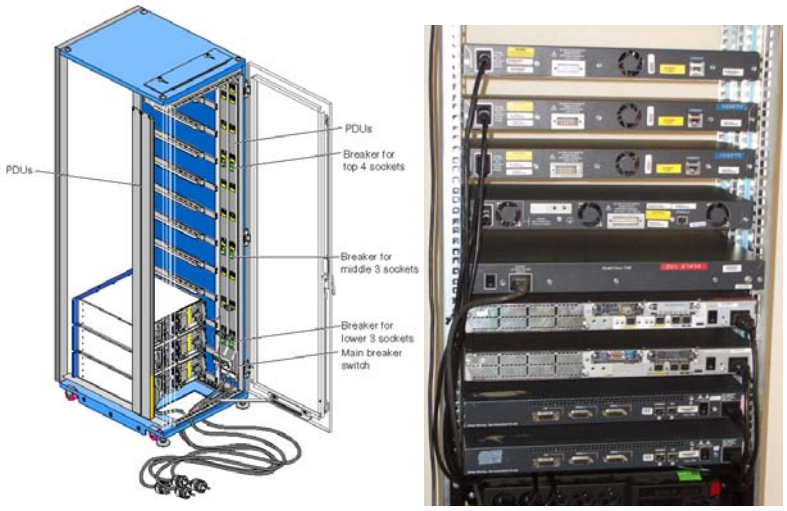
Rack

Rack je standardizovaný systém umožňující přehlednou montáž a propojování různých elektrických a elektronických zařízení spolu s vyústěním kabelových rozvodů do sloupců nad sebe v ocelovém rámu.

Rám je tvořen dvěma plochými kolejnicemi, vzdálenými od sebe přibližně 18 palců (457 mm). V kolejnicích jsou čtvercové nebo kulaté otvory, s vodorovnou roztečí 19 palců (483 mm). Ve svislém směru je rack členěn na jednotky (Rack Unit) o velikosti 1,75 palce (44,45 mm). Pro jednu Rack Unit jsou v rámu tři otvory. Zařízení montovaná do rámu mají po stranách úchytky s otvory o stejné rozteči, a jejich výška odpovídá nějakému násobku Rack Unit. Do racku lze umisťovat například různé prvky telefonních a počítačových sítí (routery, switche), počítačové servery, ale i součásti zvukové aparatury (zesilovače a zvukové efekty apod.) a další přístroje.

Obvykle jsou kolejnice součástí ocelové skříně, hluboké nejčastěji 60 cm (pro montáž velkých serverů ale také 80, 90 nebo 100 cm a navíc druhou sadou kolejnic ze zadní strany) a výšce 30-200 cm.

Systém odpovídá normám EIA 310-D, IEC 60297, DIN 41494, SC48D. [3]



Obr. 7 *Rack*

Patch panel

Patch panel si můžeme představit jako řadu zásuvek nejčastěji RJ-45 nebo RJ-11, které jsou připevněny na liště. Patch panely jsou určeny pro montáž do racků a velice zpřehledňují uspořádání kabelů v racku. Všechny kabely, které jsou do racku přitaženy, jsou zakončeny právě v patch panelu a jejich propojení s aktivními prvky se provádí pomocí krátkých kabelů (patch kabel). Používání patch panelu velice zpřehledňuje práci a při změnách nastavení portů i práci velice usnadňuje.

Obr. 8 *Patch panel*

1.4.2 Aktivní prvky

Mezi tyto prvky patří zařízení, která nějakým způsobem upravují signál (přijímají, vysílají, zesilují, rozbočují, směrují).

Síťový adaptér

Síťová karta (NIC – Network interface card) funguje jako rozhraní mezi samostatným počítačem (serverem nebo klientem) a síťovými kabely. Uvnitř musí karta NIC identifikovat počítač v síti a načíst do vyrovnávací paměti data mezi počítačem a kabelem. Při odesílání dat musí karta NIC převést data z paralelních bajtů na sériové bity. Na straně sítě musí karta NIC vygenerovat elektrické signály, které cestují prostřednictvím sítě, řídit přístup k síti a vytvořit fyzické připojení ke kabelu. [2]

Obr. 9 *Síťová karta*

Hub

Ethernetový hub nebo pouze hub, česky rozbočovač, je aktivní prvek počítačové sítě, který umožňuje její větvení a je základem sítí s hvězdicovou topologií. Chová se jako opakovač. To znamená, že veškerá data, která přijdou na jeden z portů (zásuvek), zkopíruje na všechny ostatní porty, bez ohledu na to, kterému portu (počítači a IP adrese) data náleží. To má za následek, že všechny počítače v síti „vidí“ všechna síťová data a u větších sítí to znamená zbytečné přetěžování těch segmentů sítě, kterým data ve skutečnosti nejsou určena. Hub pracuje na fyzické vrstvě modelu OSI.

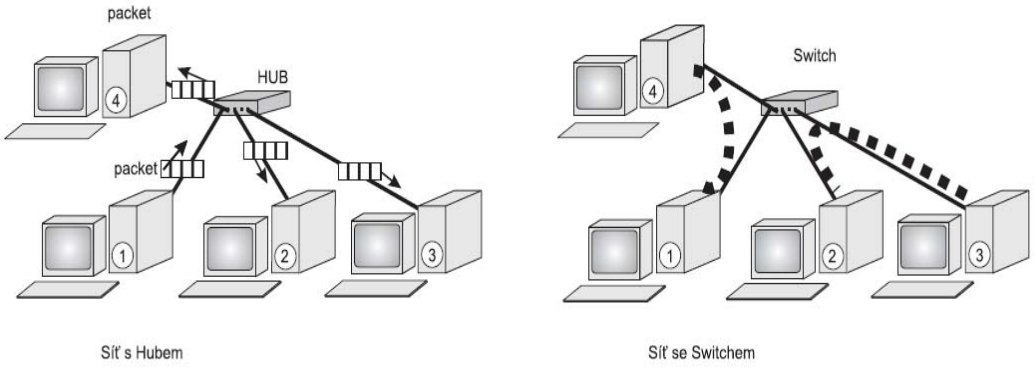
V současné době se huby již nevyrábějí a nalezneme je jen ve starších rozvodech, kde je postupně nahrazují switche. Další nevýhodou je omezení počtu hubů a celková velikost sítě. Pro síť 10 Mbit/s je počet segmentů omezen na 5 (4 huby) mezi dvěma koncovými stanicemi. U sítě 100 Mbit/s je limit snížen na 3 segmenty (2 huby) a to pouze za předpokladu, že mají huby rychlou odezvu. [4]

Obr. 10 *S-Hub Poseidon 800*

Switch

Většina sítí pracuje podle normy Ethernet, pro niž je typická přístupová metoda CSMA – CD. Nevýhodou metody je postupné zahlcování sítě, stoupající s počtem stanic. Switch tuto nevýhodu výrazně eliminuje, odděluje totiž komunikující stanice od zbytku sítě. V podstatě vytvoří virtuální okruh mezi momentálně komunikujícími stanicemi.

Příklad je ilustrován na Obr. 11. Pokud je v síti HUB a stanice 1 posílá paket stanici 4, je paket poslán všem stanicím sítě, ale pouze stanice 4 jej příjme. Vyměníme-li hub za switch vytvoří se mezi komunikujícími stanicemi spojení a ostatní stanice nejsou zatěžovány komunikací, která pro ně není určena a tím pádem se nezahlcuje síť. [5]



Obr. 11 *Rozdíl fungování sítě s hubem a switchem*

Repeater

Jak elektrické signály cestují kabely, jsou degradovány a zkreslovány. Tento efekt se nazývá útlum. Čím je kabel delší, tím se efekt útlumu zhoršuje. Pokud by kabel byl příliš dlouhý (delší než uvádí výrobce), útlum nakonec znemožní rozpoznání poslaného signálu a tím pádem vznikají datové chyby v síti. Instalace repeatrů umožňuje, aby signály cestovaly dále pomocí obnovení signálu. Ve své podstatě repeater vezme slabý signál z jednoho segmentu, signál obnoví a pošle do druhého segmentu. Jak je jasné z předešlého textu, všechny aktivní prvky často fungují jako repeatry. Samotné repeatry jsou používány pro podporu velice dlouhých kabelů.

Aby repeater mohl správně fungovat, musí oba kabely, jenž jsou k němu připojené, používat stejné rámce, logické protokoly a přístupové metody. [2]

Bridge

Bridge neboli most nabízí zatížené síti více funkcí. Most může fungovat jako opakovač k prodloužení délky síťového segmentu. Most však má větší „inteligenci“ a může rozdělit síť pro izolování nadměrného provozu nebo problematických dat. Pokud například svazek z jednoho či dvou počítačů zaplavuje síť daty a zpomaluje tak její činnost, může most tyto počítače izolovat. Mosty také mohou propojovat různá fyzická media, jako je třeba kroucená dvojlinka a optický kabel. [2]

Most má podobné vlastnosti jako switch, je také schopen oddělit od sebe určité části sítě. Most je zařízením starším, jehož hlavním úkolem je oddělení síťových segmentů. Most je inteligentním prvkem, který se zajímá o přenášená data, plní dvě funkce:

- Filtraci paketů: Ta vychází z toho, že most si přečte cílovou adresu rámce. Rámec pak propustí pouze do té části sítě, v níž je obsažen jeho cíl. Filtrováním se podstatně snižuje zatížení sítě, protože rámce neputují do síťového segmentu, kam nepatří.
- Propojení dvou různých standardů: Pracují totiž v linkové vrstvě ISO/OSI, takže fyzické odlišnosti sítí je neovlivňují. Most může být realizován mnoha způsoby. Velmi často bývá integrován do switchů, ty pak nejenže síť rozbočují, ale zároveň filtrují přenášené pakety. Druhá velmi častá realizace mostů je softwarová. Funkci mostu plní síťový operační systém, který filtruje pakety mezi několika síťovými kartami. Pokud most propojuje dvě sítě, musí zajistit, že pokud pakety putují ze stanice v síti 1 do stanice v síti 1, nejsou vpuštěny do sítě 2 (a naopak). Pokud však jsou pakety určeny pro druhou síť, jsou mostem propuštěny. [5]

Access Point

Access point (AP) (česky přístupový bod) je zařízení, ke kterému se klienti připojují pomocí bezdrátové sítě Wi-Fi. Klienti spolu nekomunikují přímo, ale prostřednictvím přístupového bodu, takže mohou být jednodušší a nemusí být ve vzájemném rádiovém spojení. Centralizovaný způsob komunikace též umožňuje použití směrových antén, které zvyšují dosah rádiového signálu. Tento typ uspořádání

nazýváme infrastrukturní síť (topologie). Opakem jsou ad-hoc sítě, kde jsou dva nebo více klientů ve vzájemném přímém rádiovém spojení (bez existence prostředníka).

Přístupový bod je obvykle realizován malým jednoúčelovým zařízením, ale s potřebnou softwarovou výbavou se jím může stát i jakýkoliv počítač s bezdrátovou síťovou kartou.

Obr. 12 *Access point Edimax EW-7206PDg*

Router

Pokud máme rozlehlejší síť, už na propouštění dat mezi jednotlivými segmenty most nestačí a je potřeba instalovat další zařízení. Takováto síť už potřebuje mnohem propracovanější zařízení, která znají adresy každého segmentu, stanoví nejlepší cestu pro odesílání dat a filtrují data vysílaná na místní segmenty. Tento typ zařízení se nazývá router neboli směrovač.

Stejně jako most mohou směrovače filtrovat a izolovat data posílaná sítí a mohou také připojovat segmenty sítě. Směrovače mohou navíc přepínat a směrovat pakety přes více sítí. Činí tak vyměňováním informací o určitém protokolu mezi samostatnými sítěmi. Směrovače mají přístup k více informacím o paketech než most a používají tyto informace ke zdokonalení přenosu paketů. Směrovače se používají ve složitých sítích, protože poskytují lepší správu přenosu dat.

Existují dva základní směrovací protokoly: statické a dynamické. „Statický směrovač“ se někdy také nazývá „ruční směrovač“, protože všechny směrovače musejí být nakonfigurovány ručně. Směrovací tabulky jsou pevně dané, takže statický směrovač používá stále stejnou cestu, což má za následek, že není zaručena nejkratší cesta.

„Dynamické směrovače“ musejí být nejprve nastaveny, avšak přizpůsobí se automaticky měnícím se podmínkám sítě.

Směrování dat

Směrovače udržují své vlastní směrovací tabulky, které se obvykle skládají z cílových adres. Pro stanovení cílové adresy pro příchozí data obsahuje směrovací tabulka všechny známé síťové adresy, logické instrukce pro připojení k jiným sítím, znalost možných cest mezi směrovači, a dokonce náklady na posílání dat prostřednictvím dané cesty. Směrovač tedy použije svou směrovací tabulku k výběru nejlepší trasy pro přenos dat na základě dostupných cest. [2]

Obr. 13 *Router CISCO 2811*

Gateway

Neboli brána funguje jako výkonný překladač určený pro připojení radikálně odlišných sítí. Ačkoliv je pomalejší než most nebo směrovač, může brána provádět složitější funkce (jako je překlad mezi sítěmi), které „hovoří“ různými jazyky. Brány umožňují komunikaci mezi zcela odlišnými architekturami a prostředími. Brána přetváří informace, aby vyhovovaly požadavkům cílového systému, a změní formát zprávy tak, aby se přizpůsobil aplikaci, jež přijímají přenášená data. [2]

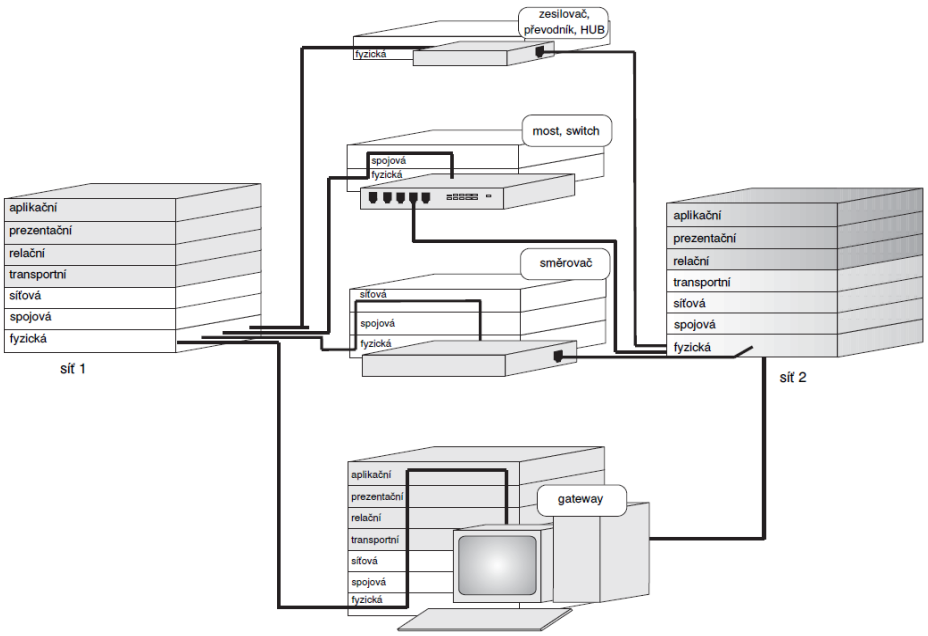
Server

Server je v informatice obecné označení pro počítač (hardware) nebo software, který poskytuje nějakou službu dalším počítačům nebo programům. Služba může být nabízena v rámci jednoho počítače (obsluha připojené tiskárny, správa automatických aktualizací,

atd.) nebo i počítačové sítě (sdílené disky, síťová tiskárna, WWW server, autentizační server, a další). Poskytování služby je pak realizováno pomocí aplikačního síťového protokolu, např.: http pro webový server, LPT pro tiskový server, SMB pro sdílení disků a tiskáren ve Windows.

Aktivní prvek	Funkce	Vrstva ISO/OSI
Síťový adaptér	Komunikace počítače a fyzického media	Aplikační
Hub	Rozvádí signál do všech větví sítě	Fyzická
Switch	Propojuje komunikující stanice	Linková
Repeater	Zesiluje signál	Fyzická
Bridge	Filtruje pakety	Linková
Access Point	Převádí signál z elektronického na magnetické vlny	Síťová
Router	Směruje pakety	Síťová
Gateway	Propojuje dvě rozdílné sítě	Aplikační
Server	Poskytuje služby dalším počítačům	Aplikační

Tab. 1 *Přehled aktivních prvků*

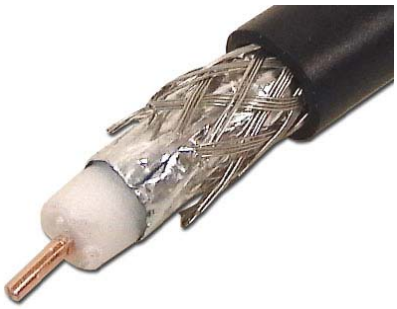


Obr. 14 *Aktivní prvky a model ISO/OSI*

1.5 Přenosová media

1.5.1 Koaxiální kabel

Koaxiální kabely jsou označovány jako asymetrická přenosová média resp. přenosové cesty linkového (též: drátového) typu. Koaxiální kabel totiž přenáší elektrické signály prostřednictvím dvou vodičů, jejichž postavení a role není stejná (resp. je asymetrická): jeden z vodičů je tvořený silnějším, nejčastěji měděným drátkem, a prochází středem celého kabelu. Druhý vodič je tvořený hustou vodivou síťkou, která obepíná izolační vrstvu (tzv. opletení) obklopující středový vodič. Toto vodivé „opletení" má za úkol odstiňovat středový vodič od okolních vlivů a stejně tak bránit vyzařování opačným směrem. Samotný přenášený signál je přitom reprezentován napětím mezi oběma vodiči (středovým a jeho vodivým opletením), neboli rozdílem elektrických potenciálů obou vodičů.



Obr. 15 *Koaxiální kabel*

Ve světě počítačů, a zvláště pak v souvislosti s technologií Ethernetu, se nejvíce proslavily dva druhy koaxiálních kabelů, označované jako „tlustý" a „tenký". To proto, že „tlustý" má průměr cca 1 cm, a „tenký" zhruba poloviční. Historicky starší „tlustý" koaxiální kabel měl několikanásobné vodivé opletení, a vyráběl se nejčastěji v charakteristické žluté barvě (proto se mu také někdy říkalo „žlutý kabel"). Byl ovšem relativně drahý a hlavně málo ohebný, což způsobovalo problémy při jeho instalaci. Proto se později přešlo na „tenký" kabel, který má kromě poloviční průměru i jednodušší provedení - má například jen dvojité či pouze jednoduché vodivé opletení, ale zato je výrazně ohebnější, a samozřejmě také lacinější. Platí za to ovšem menším dosahem, který může mít souvislý segment tohoto kabelu. [6]

1.5.2 Kroucená dvojlinka

Postupem času přestala přenosová kapacita koaxiálního kabelu stačit a hledalo se nové lepší přenosové médium. To dalo za vznik kroucené dvojlince, která vznikla v USA. Její vznik je přisuzován chybě při výstavbě budov, kdy technici natáhli několik telefonních kabelů navíc. Poté když, se v budově dělaly rozvody pro síť. Hledalo se řešení, jestli by se nedaly právě tyto přebytečné kabely využít.

Jak už její název napovídá, kroucená dvojlinka je tvořena dvěma vodiči (resp. párem vodičů), a tyto vodiče jsou po své délce pravidelným způsobem zkrouceny. Oba vodiče jsou přitom v zásadě rovnocenné, a kroucená dvojlinka proto patří mezi tzv. symetrická vedení. Signál, přenášený po kroucené dvojlince, je vyjádřen rozdílem potenciálů obou vodičů.

Důvod, proč jsou kabely zakrouceny, je velice jednoduchý. Nejprve je nutné si vzpomenout na jednu poučku z fyziky: každé dva souběžně vedoucí vodiče se chovají jako anténa. Pokud je jimi přenášen střídavý signál, vyzařují do svého okolí elektromagnetické vlny. Právě tento efekt se dá velice výrazně snížit tím, že vodiče do sebe zakroutíme. Tím ale tento efekt nezmizí úplně, nýbrž pouze se omezí na takovou míru neškodlivosti lidskému organismu a hlavě, že se neruší navzájem a ani jakékoliv vedení v okolí vodiče.

Kroucená dvojlinka se vyrábí ve třech provedeních UTP (Unshielded Twisted Pair), FTP (Foiled Shielded twisted pair), STP (Shielded Twisted Pair). Tyto jednotlivé kabely se liší pouze jedním parametrem a to jaké další stínění vodičů je přidáno. UTP je tvořeno pouze jednotlivými vodiči, spletenými do sebe a chrání je pouze gumová bužírka. FTP je o něco více chráněno, je tu přidána obalová fólie z plastu a alobalu a toto vše je ještě zabaleno gumovou bužírkou. Poslední typ STP je tvořen vodiči, které jsou po páru zabaleny do alobalu, následně jsou všechny takto vzniklé „smotky“ ještě jednou zabaleny alobalem a gumovou bužírkou. Tím, jak moc je kabel chráněn, je dáno prostředí, do kterého je určen. UTP se používá v budovách, zbývající typy jsou použity většinou venku anebo pokud se kabel táhne společně ještě s dalšími kabely. [7]

Obr. 16 *Kabely UTP, FTP a STP*

Kategorie UTP

Kategorie	Šířka pásma [MHz]	Přenosová rychlost [Mbit/s]	Vhodné použití
1	-	1	analogové tel. rozvody, ISDN, ….
2	1,5	4	dig. přenos zvuku, IBM Token Ring, ….
3	16	10	pro datové rozvody 10Base-T Ethernet.
4	20	16	pro přenos dat v Token Ring.
5	100	100 nebo 1000	pro přenos dat.
5e	100	100 nebo 1000	TPDDI, ATM, GigabitEthernet.
6	250	1000	pro ultrarychlé spoje.
6a	500	10000	pro rychlé páteřní spoje.
7	600 – 700	10000	pro přenosy plné šířky videa, teleradiologii.

Tab. 2 *Kategorie kroucené dvojlinky* [8]

1.5.3 Optický kabel

Na začátku dvacátého století bylo zjištěno, že ohnuté skleněné tyčky vedou světlo. V roce 1930 Heinrich Lamm poprvé demonstroval přenos obrazu pomocí svazku optických vláken a tak to šlo dále až k dnešním optickým vláknům.

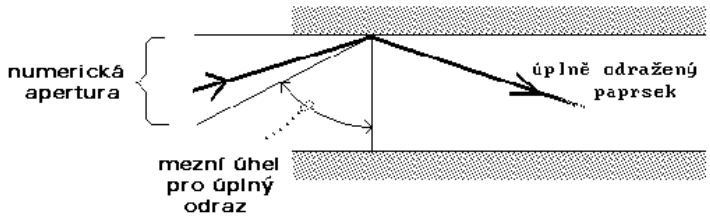
Viditelné světlo, mající frekvenci přibližně 108 MHz a je velmi lákavé pro použití k přenosu dat. Přenášená číslicová data můžeme reprezentovat pomocí světelných impulsů (přítomnost impulsu může představovat např. log1, zatímco jeho nepřítomnost log0). Pro

praktickou realizaci potřebujeme ovšem celý optický přenosový systém, složený ze zdroje, přenosového média a přijímače.

Vlastním zdrojem světla může být obyčejná elektroluminiscenční dioda (dioda LED, Light Emitting Diode) nebo nákladnější laserová dioda (laser diode) emitující světelné pulsy na základě přiváděného proudu. Detektorem na straně přijímače pak bývá fotodioda (photodiode), která naopak převádí dopadající světelné impulsy na elektrické signály.

Úkolem přenosového média je dopravit světelný paprsek od jeho zdroje k detektoru s co možná nejmenšími ztrátami. K tomuto účelu se používá optické vlákno (optical fiber), s tenkým jádrem (core) obaleným vhodným pláštěm (cladding). Jádro má průměr v řádu jednotek až desítek mikrometrů (8-10, 50, 62,5 nebo 100), a je vyrobené nejčastěji z různých druhů skla (eventuelně i z plastu).

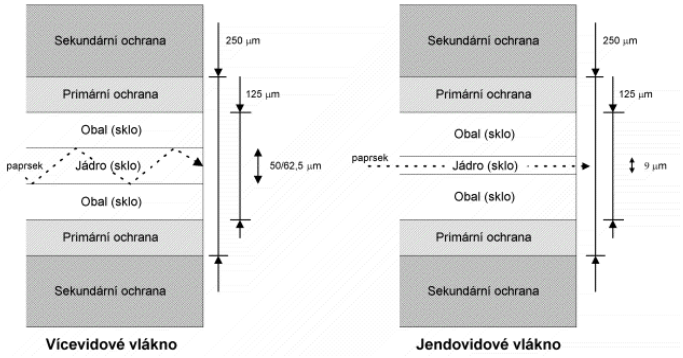
V důsledku opakovaných úplných odrazů, které probíhají bez jakýchkoli ztrát, pak světelný paprsek sleduje dráhu jádra optického vlákna – tedy, je tímto jádrem veden. Rozmezí úhlů, pod nimiž může světelný paprsek dopadat na optické vlákno tak, aby byl veden, definuje tzv. numerickou aperturu.



Obr. 17 *Odraz paprsku v jádře optického kabelu*

Optické vlákno je vždy simplexní spoj, tj. na jedné straně je vysílač a na druhé straně přijímač. Pro duplexní spoje (což je téměř vždy) je nutná dvojice vláken – pro každý směr jedno vlákno.

Optická vlákna jsou velmi citlivá na mechanické namáhání a ohyby. Jejich ochranu proto musí zabezpečovat svým konstrukčním řešením optický kabel obsahující kromě jednoho či více optických vláken obvykle i vhodnou výplň, zajišťující potřebnou mechanickou odolnost.



Obr. 18 *Složení optického kabelu*

Na obr. 18 je znázorněna ochrana optických vláken. Optická vlákna jsou nejprve obalena tzv. primární ochranou zajišťující pružnost vlákna. Bez primární ochrany je vlákno velice křehké. Sekundární ochrana pak zvyšuje ochranu vlákna. S odstraněnou sekundární ochranou se běžně setkáváme u optických propojovacích kabelů.

S optickými kabely, které mají odstraněnou sekundární ochranu, se v běžných podmínkách obtížně pracuje, proto jsou populární optická vlákna s tzv. těsnou sekundární ochranou integrující primární i sekundární ochranu. Takové kabely jsou o něco dražší (proto se nehodí na propojování velkých vzdáleností), ale na druhou stranu je možné na tyto kabely přímo nasadit optické konektory.

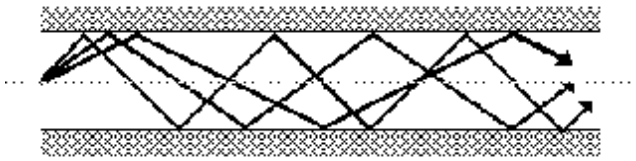
Kromě velké přenosové rychlosti je další velkou výhodou optických vláken jejich naprostá necitlivost vůči elektromagnetickému rušení (což je velmi důležité např. v průmyslových aplikacích). Výhodou je rovněž velká bezpečnost proti odposlechu, malý průměr a malá hmotnost optických kabelů.

Pro počítačové sítě jsou optická vlákna atraktivní především pro vysokou přenosovou rychlost, kterou umožňují dosáhnout s poměrně nízkými náklady. Jde tedy o technologii velmi perspektivní (a to nejen pro počítačové sítě).

Mnohavidová vlákna

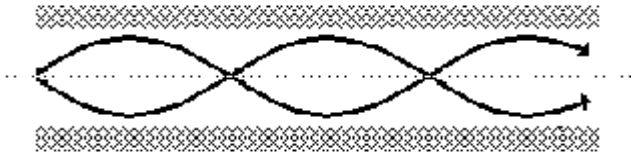
Způsob, jakým optické vlákno paprsek vede, záleží také na tom, jak se mění optické vlastnosti (konkrétně tzv. index lomu - refraction index) na přechodu mezi jádrem vlákna a jeho pláštěm. Mění-li se skokem a je-li průměr jádra dostatečně velký (50-100 mikrometrů), jde o vlákno, schopné vést různé vlny světelných paprsků -

tzv. vidy (modes). Jedná se tedy o mnohovidové vlákno (multimode fiber), v tomto případě se stupňovitým indexem lomu (step index fiber).



Obr. 19 *Šíření paprsku odrazem v mnohovidovém vlákně*

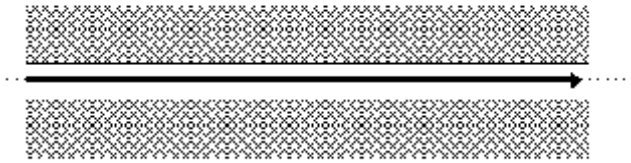
Pokud se index lomu na přechodu mezi jádrem vlákna a jeho pláštěm nemění skokem, ale plynule, jde o mnohovidové vlákno s tzv. gradientním indexem lomu (graded index fiber), které přenášené vidy ohýbá.



Obr. 20 *Šíření paprsku lomem v mnohovidovém vlákně*

Jednovidová vlákna

Nejvyšších přenosových rychlostí (až Gigabity/sekundu na vzdálenosti do 1 km) lze dosáhnout na tzv. jednovidových vláknech (single mode fiber), které přenáší jen jediný vid.



Obr. 21 *Šíření paprsku v jednovidovém vlákně*

Schopnosti vést jediný vid bez odrazů i ohybů se dosahuje buďto velmi malým průměrem jádra (řádově jednotky mikrometrů), nebo velmi malým poměrným rozdílem indexů lomu jádra a jeho pláště. V každém případě jsou jednovidová vlákna dražší než

mnohovidová, lze je ovšem použít pro přenosy na delší vzdálenosti (až 100 km bez opakovače), než vlákna mnohovidová. Pro své buzení však již vyžadují laserové diody. [9]

1.5.4 Bezdrátové spoje

Bezdrátové spoje nebo-li Wi-Fi (nebo také Wi-fi, WiFi, Wifi, wi-fi, wifi) je standard pro lokální bezdrátové sítě (Wireless LAN, WLAN) a vychází ze specifikace IEEE 802.11. Název původně neměl znamenat nic, ale časem se z něj stala slovní hříčka vůči Hi-Fi (tzn. analogicky k high fidelity – vysoká věrnost), která by se dala chápat jako zkratka k wireless fidelity (bezdrátová věrnost).

Původním cílem Wi-Fi sítí bylo zajišťovat vzájemné bezdrátové propojení přenosných zařízení a dále jejich připojování na lokální (např. firemní) sítě LAN. S postupem času začala být využívána i k bezdrátovému připojení do sítě Internet v rámci rozsáhlejších lokalit a tzv. hotspotů. Wi-Fi zařízení jsou dnes prakticky ve všech přenosných počítačích a i v některých mobilních telefonech. Úspěch Wi-Fi přineslo využívání bezlicenčního pásma, což má negativní důsledky ve formě silného zarušení příslušného frekvenčního spektra a dále častých bezpečnostních incidentů.

Typická infrastrukturní bezdrátová síť obsahuje jeden nebo více přístupových bodů (AP – Access Point), vysílající své SSID. Klient si podle názvů sítí vybere, ke které se připojí. Několik přístupových bodů může mít stejný SSID identifikátor a je plně záležitostí klienta, ke kterému se připojí. Může se například přepojovat v závislosti na síle signálu a umožňovat tak klientovi volný pohyb ve větší síti (tzv. roaming). [10]

1.6 Modely počítačových sítí

1.6.1 Model ISO/OSI

V polovině 70. let se začínají budovat komerční počítačové sítě. Tehdy se také objevují první síťové prvky. Problém byl ale v tom, že příslušné produkty byly velice specifické pro konkrétního výrobce a neumožňovaly vzájemnou interoperabilitu. Postupem času se začalo přemýšlet o nějaké síťové architektuře, nezávislé na konkrétním výrobci,

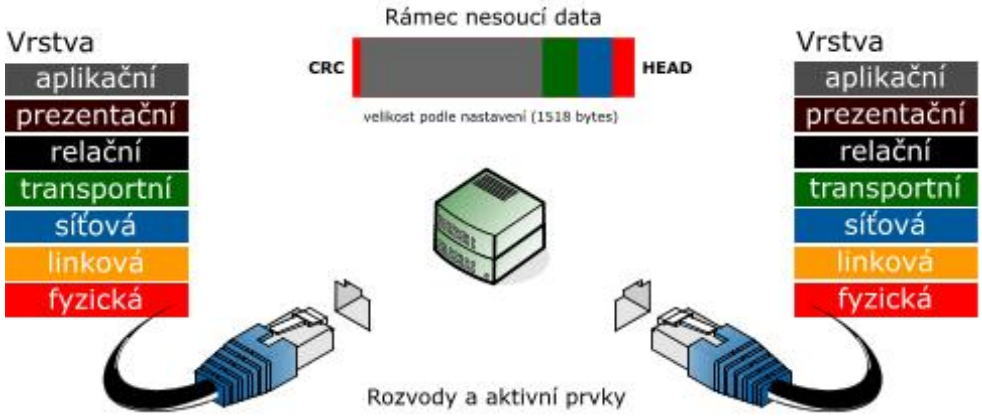
široce dostupnou ve svých specifikacích a umožňující požadovanou kompatibilitu. Tohoto úkolu, vypracovat tuto nezávislou architekturu, se nakonec dobrovolně ujala mezinárodní standardizační organizace ISO (International Standards Organization, správně: International Organization for Standardization).

Konkrétním výsledkem pak byl "Reference Model for Open Systems Interconnection" (doslova "referenční model pro propojování otevřených systémů"). Přitom slovní spojení "referenční model" je zde použito právě pro zdůraznění toho, že jde o obecnou koncepci, vzor, rámec resp. model (a nikoli o konkrétní a striktně definovaný předpis), který bude teprve postupem času naplňován konkrétními návody (protokoly) podle toho, jak tyto budou dostupné.

Autoři referenčního modelu ISO/OSI dospěli k závěru, že hierarchických vrstev, zajišťující fungování celé sítě, by mělo být sedm. Přičemž základní pravidlo komunikace mezi hierarchicky uspořádanými vrstvami je, že každá vrstva sama využívá služeb své bezprostředně nižší vrstvy, sama plní určité úkoly, které ji zadá její bezprostředně vyšší vrstva. [11]

Vrstvy modelu ISO/OSI

1) Fyzická vrstva (physical layer)
2) Linková vrstva (data link layer)
3) Síťová vrstva (network layer)
4) Transportní vrstva (transport layer)
5) Relační vrstva (session layer)
6) Prezentační vrstva (presentation layer)
7) Aplikační vrstva (application layer)



Obr. 22 *Referenční model ISO/OSI*

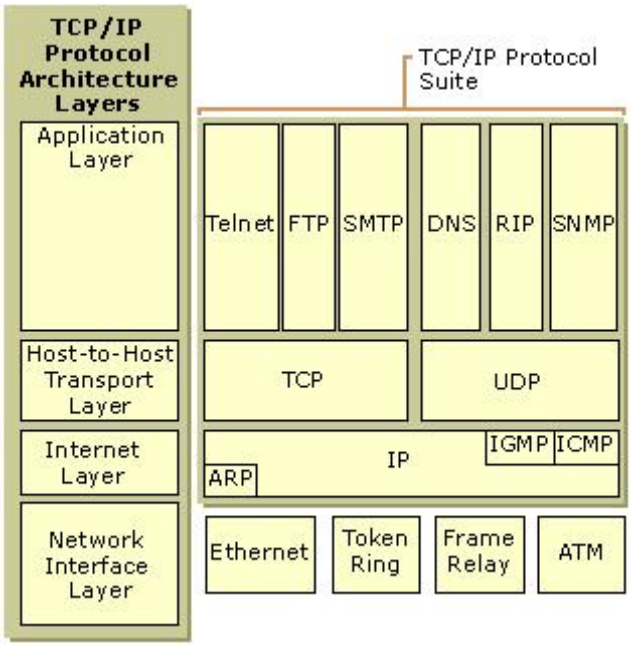
1.6.2 Model TCP/IP

Rodina protokolů TCP/IP obsahuje sadu protokolů pro komunikaci v počítačové síti a je hlavním protokolem celosvětové sítě Internet. Vzhledem ke složitosti problémů je síťová komunikace rozdělena do tzv. vrstev, které znázorňují hierarchii činností. Výměna informací mezi vrstvami je přesně definována. Každá vrstva využívá služeb vrstvy nižší a poskytuje své služby vrstvě vyšší. Celý význam slova TCP/IP je Transmission Control Protocol/Internet Protocol.

Komunikace mezi stejnými vrstvami dvou různých systémů je řízena komunikačním protokolem za použití spojení vytvořeného sousední nižší vrstvou. Architektura umožňuje výměnu protokolů jedné vrstvy bez dopadu na ostatní. [12]

Vrstvy modelu TCP/IP:

1) Vrstva síťového rozhraní (network interface)
2) Síťová vrstva (network layer)
3) Transportní vrstva (transport layer)
4) Aplikační vrstva (application layer)



Obr. 23 *Protokol TCP/IP*

2 CISCO IOS

IOS je zkratka pro Cisco's Internetwork Operating System, což je operační systém, který používá většina Switchů a Routerů firmy Cisco. Celý IOS je uložen v jednom image souboru s příponou bin a má velikost kolem 5 MB. Ve flash paměti může být ještě uloženo webové rozhraní (bývá ve složce HTML).

IOS je propracovaný a na míru provedený systém. Nabízí velké množství možností pro konfiguraci, a pokud víme, co chceme konfigurovat, není to již příliš složité. Obsluha IOSu je založena na CLI – Command Line Interface, tedy na příkazové řádce.

Pokud zadáváme nějaké konfigurační příkazy IOSu, tak ty se okamžitě provádějí, ale ukládají se pouze do running-config, uloženému v RAM (při startu se do něj kopíruje obsah startup-config). To znamená, že aktuálně jsou platné, ale po restartování switche se vymažou. Pokud bychom tedy provedli nějakou konfiguraci, kterou bychom nemohli vrátit zpět, stačí restartovat switch a ten je v takovém stavu, jako při posledním uložení konfigurace. Pokud však chceme zachovat naše změny, je třeba vždy překopírovat běžící konfiguraci do startovací.

2.1 Typy paměti zařízení Cisco

Cisco switche a routery používají pět různých pamětí.

2.1.1 Paměť ROM

ROM paměť je pouze pro čtení a je nezávislá na napájení. Obsahuje procesy, které se provádí při bootování. V ROM paměti je uloženo několik základních funkcí:

- POST (Power-on Self Test) - po zapnutí switche provede tento mikrokód test funkčnosti hlavních částí (paměť, CPU, interfacy)
- Bootstrap Program - inicializace bootování, nahrává IOS
- ROM monitor - speciální diagnostický mód pro řešení problémů
- RxBoot - pokud se nenalezne funkční IOS, tak se načte tato omezená verze IOSu, která umožní instalovat správný IOS image

2.1.2 Paměť Flash

Flash je paměť typu NVRAM (Non-volatile random access memory), do které je možno zapisovat a při odpojení napájení zůstane obsah zachován. Ve flash paměti je primárně uložen IOS (může zde být i více verzí), dále kopie startup-config v souboru config.text a informace o VLANech v vlan.dat. Teoreticky zde můžeme uložit cokoliv.

2.1.3 Paměť NVRAM

Non-volatile random access memory (NVRAM) je obdobně jako Flash zapisovatelná paměť nezávislá na napájení. Je použita pro uložení startup-config.

2.1.4 Paměť RAM

Random Access Memory (RAM) je operační paměť. Jedná se o rychlou zapisovatelnou paměť, závislou na napájení a při restartu switche se vymaže. Standardně rozdělujeme tuto paměť na dvě části - hlavní paměť procesoru a sdílenou paměť I/O. V hlavní části je uložena běžící konfigurace (running-config), běžící IOS, routovací a ARP tabulky. Sdílená paměť je použita jako buffer pro uložení aktuálně zpracovávaných paketů. Zobrazit její obsah můžeme pomocí show memory.

2.1.5 Externí paměť - TFTP

Poslední typ paměti není součástí zařízení, takže by se zde nemusel počítat, ale využívá se pro řadu činností. Používá se zde TFTP (Trivial FTP) server, který můžeme rozběhnout na libovolném počítači. Nejčastěji jej využijeme při provádění zálohy či upgradu IOSu, ale je možné i zavádět IOS přímo z TFTP serveru.

2.2 Základní práce s IOSem

Nejprve je třeba se připojit k zařízení, aby bylo možné pracovat v CLI. Je možné tak učinit přes consoli, tzn. sériovým kabelem přes speciální port na zařízení. To je základní připojení a někdy jediné možné. Pokud již máme provedenu základní konfiguraci, je možné se připojit přes telnet či ssh. Aby fungovala tato připojení, musí být nastavena a musí být vždy nastaveno přihlašovací heslo. Pro některé úkony, třeba i základní konfiguraci, se můžeme připojit přes webové rozhranní či užitečný program Cisco Network Assistant. Ale, ač to tak na první pohled nemusí vypadat, nakonec je jednodušší provádět většinu nastavení přes CLI. Pro připojení přes consoli použijeme hyperterminál nebo putty, který umožňuje připojení i přes ssh a telnet.

2.3 Zadávání příkazů

Veškeré příkazy IOSu se dají zadávat zkráceně, stačí zadat první znaky, které jednoznačně určí příkaz (tedy, aby v daném kontextu neexistoval jiný příkaz, začínající těmito znaky). Klávesa *tabulátor* doplňuje příkaz. Zadáme prvních pár písmen příkazu a po stisknutí *TAB* se příkaz doplní, pokud je jednoznačný, nebo se doplní část, která je pro více příkazů společná. Zadáním *?* (otazníku) se zobrazí seznam příkazů s krátkým popiskem, které můžeme na aktuálním místě použít. Také můžeme zadat prvních pár písmen příkazu a otazník, aby se vypsal seznam příkazů s tímto začátkem. Většina příkazů se skládá z posloupnosti klíčových slov, pokud zadáme *příkaz ?*, dostaneme seznam argumentů či klíčových slov, která se dají zadat na tomto místě.

Klávesa šipka nahoru a šipka dolu slouží k procházení historie, prochází dříve zadané příkazy. Pokud se na obrazovku vypisují údaje, listují se po stránkách. Při vypsání stránky se výpis zastaví. Klávesou *SPACE* se zobrazí další stránka, klávesou *ENTER* se zobrazí další řádek. U příkazů, které generují nějaký informační výstup, můžeme použít výstupní modifikátor | (svislá čára) a pomocí něj omezovat výstup.

Pokud jsme v CLI na nějakém přepínači, tak se můžeme připojit k jinému přepínači zadáním jednoho z příkazů v uživatelském/privilegovaném módu. ssh adresa, telnet adresa, connect adresa či pouze zadáním samotné adresy, pokud neodpovídá nějakému

klíčovému slovu. Adresa je buď IP adresa nebo hostname. Pro přepnutí zpět bez ukončení aktuální session slouží Ctrl+Shift+6 a potom x.

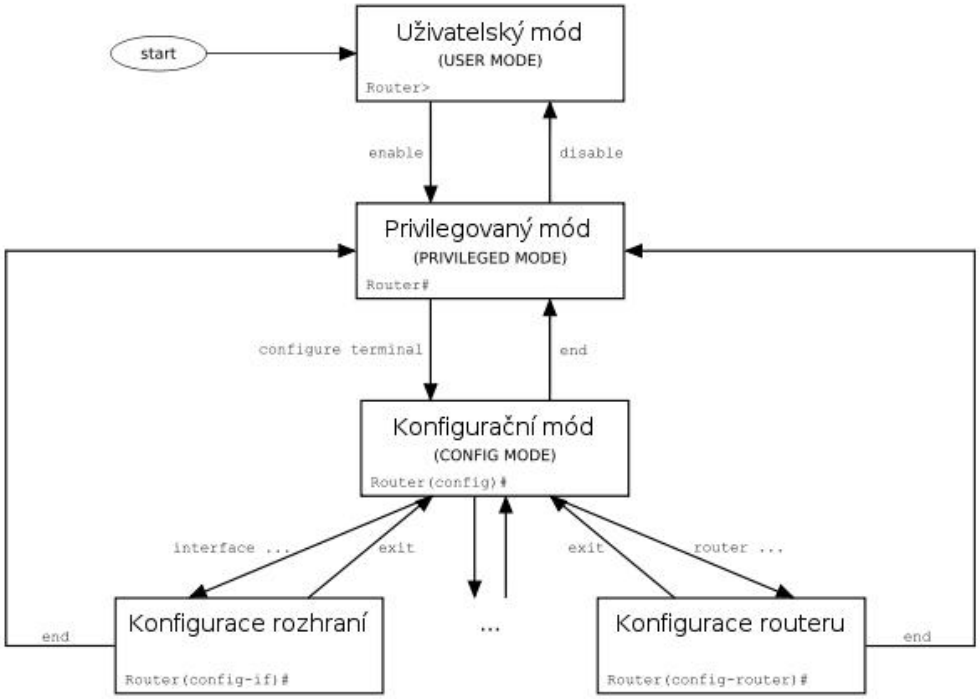
2.3.1 Rušení příkazů

Pokud zadáme nějaký příkaz IOSu a odešleme jej pomocí klávesy ENTER, tak se okamžitě uplatní a uloží do běžící konfigurace. Pokud chceme zrušit nějaké nastavení, tedy odvolat dříve zadaný příkaz, použijeme klíčové slovo *no* a za ním stejný příkaz, jako pro zadání. Tedy všechna nastavení se dají opět rušit pomocí příkazu *no*. Často není třeba zadávat všechny parametry příkazu. Takto provedené změny se opět uplatní pouze na běžící konfiguraci.

2.3.2 Příkazové módy

Uživatelské rozhranní IOSu je děleno do řady různých módů, které nám umožňují provádět jiné činnosti. Hlavní módy jsou:

- **Uživatelský mód** (EXEC) – user EXEC – v tomto módu jsme hned po přihlášení a má pouze omezené příkazy.
- **Privilegovaný mód** (EXEC) – privileged EXEC - výchozí mód pro přestup do dalších konfigurací, umožňuje zobrazovat různé údaje
- **Globální** konfigurační mód – global configuration - zde se konfigurují funkce, ovlivňující celý systém
- **Konfigurace** interfacu – interface configuration - v tomto módu konfigurujeme vlastnosti určitého interfacu [13]



Obr. 24 *Příkazové módy IOS*

3 TECHNOLOGIE ETHERCHANNEL

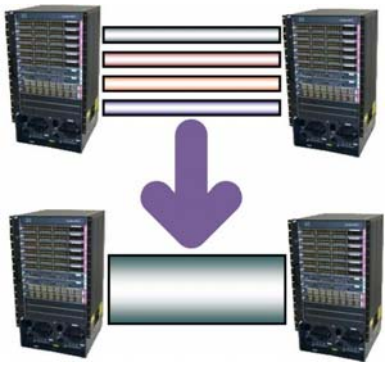
EtherChannel je technologie, která se především používá na přepínačích Cisco. EtherChannel byl vynalezen společností Kalpana na začátku 1990. Tuto společnost později odkoupila společnost Cisco Systems v roce 1994. V roce 2000 prošel standard IEEE 802.3ad, který je otevřeným standardem verze EtherChannel. [15]

Agregace nebo IEEE 802.1AX-2008 je v počítačových sítích pojem, popisující použití více síťových kabelů/portů současně ke zvýšení rychlosti linky za hranicemi jakéhokoliv jednoho kabelu nebo portu, a zvýšit tak redundanci pro vyšší dostupnost. [16]

EtherChannel umožňuje sloučením několika fyzických ethernetových spojení vytvořit jeden logický ethernetový spoj za účelem poskytování odolnosti proti chybám a rychlejší spojení mezi přepínači, směrovači a servery. EtherChannel může být vytvořen ze dvou až osmi aktivních Fast Ethernet, Gigabit Ethernet nebo 10-Gigabit Ethernet portů. EtherChannel je primárně používán v páteřní síti, ale může být také použit pro připojení strojů koncového uživatele. [14]

Jinak řečeno, tato technologie je určena pro agregaci linek na přepínačích, routerech a serverech většinou společnosti CISCO.

EtherChannel můžeme konfigurovat ručně nebo využít proprietární protokol Cisco Port Aggregation Protocol (PAgP) nebo standardizovaný Link Aggregation Control Protocol (LACP). Tato technologie se používá mezi přepínači, ale je možno ji využít i pro připojení serveru, zde se označuje jako NIC Teaming nebo Bonding. [16]



Obr. 25 *Princip fungování technologie EtherChannel*

Jak již bylo uvedeno výše, EtherChannel je metoda, která zařizuje odesílání a přijímání dat přes více interfaců a mohou k tomu být použity dva protokoly, jenž jsou standardem IEEE 802.3ad nebo jak se dnes uvádí novější označení 802.1ax. Protokoly PAgP a LACP slouží k automatickému vyjednání a vytvoření EtherChannelu. Pro vytvoření EtherChannelu můžeme použít 2 až 8 fyzických interfaců (L2 nebo L3) pro PAgP nebo až 16 interfaců pro LACP (ale pouze 8 je active a ostatní jsou standby). Podmínkou je, aby byly stejného typu a rychlosti, zařazené do stejné VLAN nebo v trunk módu se stejnými parametry. Na přepínači můžeme vytvořit až 48 (skupin) EtherChannelů. Původně byla podmínka, aby se všechny porty jedné strany skupiny, nacházely na jednom přepínači. Dnes je možno, aby porty byly součástí jednoho tracku.

Původní použití EthernetChannelu bylo pro propojení páteře sítě, kdy se dosáhlo vyšší spolehlivosti a hlavně vyšší rychlosti. Dnes je častým použitím i připojení serveru přes více portů/síťových karet.

Když vytvoříme EtherChannel, tak se vytvoří jeden virtuální port, s kterým dále pracují všechny technologie. Takže například Spanning Tree vidí skupinu portů jako jeden port a vše tudíž pracuje jak má a nedojde k blokování takto vzniklých redundantních linek.

EtherChannel používá Load Balancing, aby rozložil zátěž na všechny linky ve skupině. Když odesílá data, tak podle MAC adresy, IP adresy, zdrojové či cílové určuje, přes jakou linku data odešle (není to závislé na vytížení nebo rychlosti linky). Je snaha, aby rámce z jedné TCP session byly odesílány přes stejnou linku, jinak by mohlo dojít k doručení mimo pořadí a dalším problémům. Příchozí data se sdružují ze všech interfaců do virtuálního portu. Když se jedna linka přeruší, tak se provoz bez přerušení přesměruje na zbývající (dojde asi ke vteřinovému zpoždění, ale nepřeruší se session a třeba kopírování po síti funguje dál). [16]

3.1 Load Balancing

Vyvažování zátěže, nebo-li load balancing, je v informatice technika pro rozložení zatížení mezi dva nebo více počítačů, síťových linek, procesorů, pevných disků nebo jiných zařízení, aby bylo dosaženo optimálního využití, prostupnosti nebo času odezvy.

Použití více zařízení pro vyvážení zátěže může poskytnout i větší odolnost proti výpadkům. [17]

Počet portů v EtherChannel	Load Balancing
8	1:1:1:1:1:1:1:1
7	2:1:1:1:1:1:1
6	2:2:1:1:1:1
5	2:2:2:1:1
4	2:2:2:2
3	3:3:2
2	4:4

Tab. 3 *Závislost počtu portů v EtherChannelu na Load Balancing*

3.2 NIC Teaming

Umožňuje spojit 2 nebo více fyzických NIC (síťových karet) do jednoho logického adaptéru, který se označuje jako bound (svazek). Může využívat standard IEEE 802.3ad. Pokud máme správný ovladač pro síťovou kartu, tak na ní můžeme konfigurovat VLAN a NIC Teaming. Pomocí VLAN rozdělíme jeden fyzický adaptér na více virtuálních. Pomocí Teamingu naopak spojíme více fyzických portů do jednoho virtuálního.

NIC Teaming může fungovat i s obyčejným switchem/hubem, jenž nepodporuje Link Aggregation. Tehdy konfigurujeme pouze na straně serveru a uplatňuje se (primárně) pro odchozí provoz. Síťové adaptéry mohou být zapojeny i do různých switchů a mohou mít jinou rychlost a duplex. Vytvořením teamu podle 802.3ad se vytvoří jeden virtuální interface, který získá MAC adresu jednoho z fyzických interfaců a můžeme mu nastavit jednu nebo více IP adres. Pokud použijeme některý mód nezávislý na přepínači, tak všechny fyzické porty (uvnitř virtuálního) používají svoji MAC adresu.

Pokud máme možnost nastavit Teaming, tak většinou můžeme volit jednu z řady metod nebo typů teamingu:

- **Adapter Fault Tolerance**, kdy je jeden adaptér aktivní a ostatní jsou standby (přepnou se v případě výpadku), nenastavuje se na straně switche.

- **Switch Fault Tolerance** podporuje dvě linky připojené do dvou různých switchů, jedna je aktivní a druhá standby (nenastavuje se na straně switche).
- **Adaptive Load Balancing** odesílaný provoz je vyvažován přes všechny adaptéry, zároveň poskytuje fault tolerance, může provádět load balancing i na příchozím provozu (nenastavuje se na straně switche).
- **Static Link Aggregation** je použití manuálního EtherChannelu, kdy je na přepínači nastaven mód on.
- **Dynamic Link Aggregation**, který využívá LACP protokol podle IEEE 802.3ad.

3.3 Port Aggregation Protocol - PAgP

Jedná se o protokol vytvořený firmou Cisco a podporovaný, téměř výlučně, pouze na Cisco zařízeních. PAgP podporuje vytvoření EtherChannelu pouze z interfaců na jednom přepínači.

PAgP může pracovat buď v aktivním módu, kdy se aktivně snaží vyjednat ustanovení EtherChannelu (ten se označuje jako desirable) nebo v pasivním módu, kdy se EtherChannel začne vyjednávat, pouze když přijde požadavek z druhé strany (sám nikdy nezačne vyjednávání), to je mód auto.

3.4 Link Aggregation Control Protocol - LACP

LACP má dva módy, obdobné jako PAgP. Jejich označení je active, tehdy sám odesílá pakety pro vyjednání spojení, a passive, kdy čeká na začátek vyjednávání.

Manuální EtherChannel

EtherChannel můžeme ustanovit i manuálně. Zde je třeba, aby porty na obou stranách byly nastaveny do módu on. Nezasílají se žádná LACP PDU ani pakety PAgP protokolu. [16]

Vlastnost	Tovární nastavení
Channel group	není určena.
Port-channel logical interface	není definován.
PAgP mode	není nastaven.
PAgP learn method	na všech portech.
PAgP priority	128 na všech portech.
LACP mode	není nastaven.
LACP learn method	na všech portech.
LACP port priority	32768 na všech portech.
LACP system priority	32768.
LACP system ID	LACP system priority and switch MAC address.

Tab. 4 *Základní nastavení EtherChannel*

3.5 Konfigurace technologie EtherChannel

3.5.1 Pravidla pro konfiguraci EtherChannelu

Pokud se nesprávně nakonfigurují některé porty EtherChannelu, tak jsou automaticky zablokovány, aby se zabránilo dalším problémům v síti. Následné pokyny zabraňují výskytu problémů s konfigurací.

- Nezkoušejte konfigurovat více než 6 EtherChannelů na jednom přepínači.
- Nekonfigurujte PAgP EtherChannel s více než 8 ethernetovými porty toho samého typu.
- Nekonfigurujte LACP EtherChannel s více než 16 ethernetovými porty toho samého typu. Pouze 8 jich může být aktivních a až 8 portů může být v pohotovostním režimu.
- Konfigurujte všechny porty v EtherChannelu tak, aby pracovaly se stejnou rychlostí a duplexem.
- Povolte všechny porty v EtherChannelu. Port v EtherChannelu, zakázaný pomocí konfiguračního příkazu *shutdown* se považuje za spojení, vedoucí

k selhání a provoz po této trase je převeden na jeden ze zbývajících portů EtherChannelu.

- Je-li skupina portů v EtherChannelu vytvořena poprvé, všechny porty jsou nastaveny stejně, jako první port. To platí pro všechny porty, které jsou ve stejné skupině. Pokud změníte nastavení jednoho z parametrů, musíte tyto změny provést na všech portech ve skupině:
    - Povolení VLAN listu
        - Spanning-tree path cost pro každou VLAN
        - Spanning-tree port priority pro každou VLAN
        - Spanning-tree Port Fast petting
- Nekonfigurujte:
    - Port, který by mohl být členem více než jedné skupiny EtherChannelu.
    - EtherChannel v obou režimech PAgP a LACP. EtherChannel skupiny mohou fungovat pouze v PAgP režimu nebo LACP režimu, zároveň fungovat nemohou.
    - Switched Port Analyzer (SPAN) jako součást EtherChannelu.
    - Bezpečnostní port jako součást EtherChannelu a naopak.
    - Port, který je aktivní, nebo v režimu not-yet-aktiv členem EtherChannelu jako IEEE802.1x port. Pokusíte-li se o to, objeví se chybová zpráva.
- Pokud EtherChannel je nastaven na přepínání rozhraní, odstraňte konfigurace EtherChannelu z rozhraní.
- Pro 2 vrstvu na EtherChannelu:
    - Přiřadit všechny porty v EtherChannelu na stejnou VLAN, nebo je nakonfigurovat jako trunk. Porty s různými VLAN nemohou tvořit EtherChannel.
    - Pokud konfigurujete EtherChannel přes trunk porty ověřte, zda režim trunking (ISL, nebo IEEE 802.1Q) je stejný pro všechny trunk porty.

Nekonzistentní způsoby trunk na portech EtherChannelu může mít nečekané následky.

- EtherChannel podporuje stejný rozsah VLAN na všech portech v trunking Layer 2 EtherChannel. Pokud je povolený rozsah VLAN různý, porty netvoří EtherChannel PAgP, i když jsou nastaveny v auto nebo disirable mode.
- Porty s různou spanning-tree path cost mohou tvořit EtherChannel pokud jsou jinak kompatibilně nakonfigurovány.

3.5.2 Konfigurace Layer 2 EtherChannelu

Konfigurace Layer 2 EtherChannelu se provádí přiřazením portů do skupiny (Channelu) příkazem *channel-group*. Tento příkaz automaticky vytvoří port-channel, což je logický interface. Po spuštění switche je potřeba zadat příkaz *enable* pro vstup do privilegovaného módu EXEC a postupujeme takto pro přiřazení Layer 2 Ethernet port do Layer 2 EthrChannel. Tento postup je nutný.

Krok	Příkaz	Účel
1	configure terminal	Vstup do globálního konfiguračního módu
2	interface *interface-id*	Určuje fyzický port a vstup do konfigurace rozhraní režimu. Platné rozhraní včetně fyzických portů. Pro PAgP EtherChannel můžete nakonfigurovat až 8 portů stejného typu a rychlosti pro stejnou skupinu. Pro LACP EtherChannel můžete nastavit až 16 Ethernet portů stejného typu. Až 8 portů může být aktivních a až 8 portů může být v režimu standby.
3	switchport mode {access|trunk} switchport access vlan *vlan-id*	Přiřadí všechny porty jako static-access port ve stejné VLAN nebo je konfiguruje jako trunks. Potřebujete-li nakonfigurovat port jako stati-access port, který přiřadíte pouze jedné VLAN. Rozsah je od 1 do 4094.
4	channel-group *channel-group-number* mode	Přiřadí port do channel group a určuje, zda se použije PAgP nebo LACP.

	{auto [non-silent] | desirable [non-silent] | on} | {active | passive}	Pro *channel-group-number* je rozsah 1-6. Pro **mode** je možno vybrat několik možností: • **auto** – Umožňuje PAgP pouze tehdy, pokud je zařízení PAgP detekováno. Port je kladen do pasivního stavu, ve kterém port reaguje na PAgP pakety, které obdrží, ale nespustí PAgP. • **desirable** – Bezpodmínečně umožňuje PAgP. Klade port do aktivního statusu, kde port začíná jednat s dalšími porty o zaslání PAgP paketů. • **On** - Síly portu na kanálu bez PAgP nebo LACP. V provozním režimu, EtherChannelu existuje pouze tehdy, když jsou porty skupiny v provozním režimu a připojeny k jinému portu skupiny v provozním režimu. • **Non-silent** – Pokud je switch připojen s dalším switchem, který je PAgP-capable (schopný), je možná konfigurace portu na přepínači pro non-silent operace. Pokud zadáte non-silent, silent se nepředpokládá. Silent nastavení je pro připojení k souborovým serverům nebo paketovým analyzátorům. Toto nastavení umožňuje pracovat PAgP, připojit k portu channel group a používat port pro přenos. • **Aktive** – Umožňuje LACP pouze tehdy, pokud je zařízení LACP dekováno. Klade port do aktivního statusu, ve kterém začíná jednat s dalšími porty o zaslání LACP paketů. • **Passive** – Umožňuje LACP na portu a vloží jej do pasivního stavu, ve kterém reaguje na LACP pakety, které obdrží, ale nepustí LACP paket negotiation.
5	end	Vrácení do privilegovaného EXEC mode.
6	show runnig-config	Ověření záznamů.
7	copy runnig-config startup-config	Uloží všechny příkazy do konfiguračního souboru.

Tab. 5 *Konfigurace Layer 2 EtherChannelu*

Pro odebrání portu z EtherChannelu se používá příkaz *no channel-group*. Tento příklad ukazuje jak konfigurovat EtherChannel. Spojení dvou portů jako static-access port v VLAN 10 pro channel 5 s PAgP režimem **desirable**:

Switch# *configure terminal*

Switch(config)# *interface range gigabitethernet0/1 -2*

Switch(config-if-range)# *switchport mode access*

Switch(config-if-range)# *switchport access vlan 10*

Switch(config-if-range)# *channel-group 5 mode desirable non-silent*

Switch(config-if-range)# *end*

Tento příklad ukazuje, jak konfigurovat EtherChannel. Spojení dvou portů jako static-access port v VLAN 10 pro channel 5 s LACP režimem **aktive**:

Switch# *configure terminal*

Switch(config)# *interface range gigabitethernet0/1 -2*

Switch(config-if-range)# *switchport mode access*

Switch(config-if-range)# *switchport access vlan 10*

Switch(config-if-range)# *channel-group 5 mode active*

Switch(config-if-range)# *end*

3.5.3 Konfigurace EtherChannel Load Balancing

Krok	Příkaz	Účel
1	configure terminal	Vstup do globálního konfiguračního módu
2	port-channel load-balance {dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac}	Konfigurační metody EtherChannel Load Balancing. Defaultní nastavení je src-mac. Můžeme vybrat jednu z těchto metod: • dst-ip – rozložení zátěže je založeno na koncové IP adresy hosta. • dst-mac – rozložení zátěže je založeno na koncové MAC adresy příchozích paketů. • src-dst-ip – rozložení zátěže je založeno na zdrojové a koncové IP adresy hosta. • src-dst-ip – rozložení zátěže je založeno na zdrojové a koncové MAC adresy hosta. • src-ip – rozložení zátěže je založeno na zdrojové IP adresy hosta. • src-mac – rozložení zátěže je založeno na

		zdrojové MAC adresy příchozích paketů.
3	end	Návrat do privilegovaného módu.
4	show etherchannel load-balance	Ověření vstupních záznamů.
5	copy running-config startup-config	Uloží vstupy do konfiguračního souboru.

Tab. 6 *Postup konfigurace EtherChannel Load Balancing*

Pokud chceme návrat do základního nastavení EtherChannel Load Balancing, použijeme příkaz *no-channel load balance*.

3.5.4 Konfigurace PAgP linkovací metody a priority.

Krok	Příkaz	Účel
1	configure terminal	Vstup do globálního konfiguračního módu.
2	interface *interface-id*	Specifikuje port pro přenos.
3	pagp learn-method *physical port*	Výběr PAgP linkovací metody. Ve výchozím nastavení, je vybrán **aggregation-port learning**, což znamená, že přepínač odesílá zdrojové pakety pomocí některého z portů v EtherChannelu. Spolu s aggregate-port leasing, kde není důležité, na který z fyzických portů paket přichází. Zvolte **physical-port** pro připojení dalšího přepínače, který je „fyzický linkovač“. Také je potřeba ujistit se, že konfigurace port-channel load-balance je prováděn globálním konfiguračním příkazem. Metoda leasing musí být nastavena stejně na obou koncích.
4	pagp port-priority *priority*	Přiřazení priority tak, aby zvolený port byl vybrán pro přenos paketu. Pro nastavení *priorit* se používá rozsah 0 až 255. V základu je nastavena hodnota Priority na 128. Čím vyšší priorita, tím je větší pravděpodobnost, že port bude používán pro přenos PAgP.
5	end	Návrat do privilegovaného EXEC módu.
6	show running-config	Ověření vstupů.

	nebo show pagp *channel-group-number* internal	
7	copy running-config startup-config	Uložení vstupů do konfiguračního souboru.

Tab. 7 *Konfigurace PAgP linkovací metody a priority.*

3.5.5 Konfigurace LACP systém priority

Můžete konfigurovat systém priority pro všechny EtherChannels, které jsou povoleny pro LACP pomocí *lacp system-priority*. Nemůžete nastavit systém priorit pro všechny LACP konfigurační kanály. Změnou této hodnoty z defaultu, můžete ovlivnit, jak systém vybere aktivní a pohotovostní režim.

Můžete použít příkaz *show etherchannel summary* v privilegovaném módu EXEC na to, které porty jsou v hot-standby módu.

Krok	Příkaz	Účel
1	configure terminal	Vstup do konfiguračního módu.
2	lacp system-priority *priority*	Konfiguruje LACP systém priority. Pro *priority*, je používán rozsah 1 – 65535. V základním nastavení je nastaven na 32768. Čím nižší hodnota, tím vyšší priorita systému.
3	end	Návrat do privilegovaného módu.
4	show running-config nebo show lacp sys-id	Ověření vstupů.
5	copy running-config startup-config	Uložení vstupů do konfiguračního souboru.

Tab. 8 *Příkazy pro konfiguraci LACP systém priority*

3.5.6 Konfigurace LACP port priority

Ve výchozím nastavení mají všechny porty nastavenou stejnou prioritu. Pokud místní systém má nižší hodnotu priority systému a systému ID než vzdálený systém, můžete ovlivnit, které z hot-standby linek se stanou aktivními prvotní změnou portu priority LACP portů EtherChannelů na nižší hodnoty, než výchozí. Hot-standby porty, které mají nižší čísla portů, mohou být aktivní kanál. Můžete použít příkaz *show etherchannel summary* a zjistit tím, které porty jsou na hot-standby režimu.

Krok	Příkaz	Účel
1	configure terminal	Vstup do globálního konfiguračního módu.
2	interface *interface-id*	Specifikuje port, který musí být nastaven a zadáváte konfiguraci rozhraní režimu.
3	lacp port-priority *priority*	Konfiguruje LACP port priority. Pro *priority* se používá rozsah 1 až 65535. V továrním nastavení je nastaveno 32768. Čím nižší hodnota, tím větší je pravděpodobnost, že port bude použit pro přenos LACP.
4	end	Návrat do privilegovaného módu.
5	show running-config nebo show lacp [*channel-group-number*] internal	Ověřuje záznamy.
6	copy running-config startup-config	Uloží záznamy do konfiguračního souboru.

Tab. 9 *Příkazy pro konfiguraci LACP port priority*

3.5.7 Zobrazení EtherChannel, PAgP a LACP statusu.

Pro zobrazení informačního statusu EtherChannelu, PAgP a LACP, použijte v privilegovaném režimu tyto příkazy popsané v tabulce, kterou naleznete pod tímto odstavcem. [18]

Příkaz	Účel
show etherchannel [*channel-group-number* {detail | port | port-channel | protocol | summary}] {detail | load-balance | port | port-channel | protocol | summary}	Zobrazí informace o EtherChannel v krátkém detailním shrnutí. Také zobrazuje load-balance nebo line-distribution systém, port, port-channel a informace o protokolu.
show pagp [*channel-group-number*] {counters | internal | neighbor}	Zobrazuje informace o PAgP režimu jako třeba informace o provozu vnitřní konfigurace PAgP a informace o sousedech.
show lacp [*channel-group-number*] {counters | internal | neighbor}	Zobrazuje informace o LACP režimu jako třeba informace o provozu vnitřní konfigurace LACP a informace o sousedech.

Tab. 10 *Příkazy pro zobrazení informací o EtherChannel, PAgP a LACP režimu*

4 TECHNOLOGIE NETFLOW

NetFlow je otevřený protokol vyvinutý společností Cisco Systems, určený původně jako doplňková služba k Cisco směrovačům. Jeho hlavním účelem je monitorování síťového provozu na základě IP toků, které poskytuje administrátorům i manažerům podrobný pohled do provozu na jejich síti v reálném čase. Proto tvoří důležitou a nepostradatelnou součást zabezpečení každé počítačové sítě a je užitečný pro ISP (Internet Service Providers - poskytovatelé připojení), kteří na základě NetFlow statistik mohou svým zákazníkům účtovat ceny služeb v závislosti na množství přenesených dat. S pomocí NetFlow statistik lze odhalovat vnější i vnitřní incidenty, úzká místa v síti, dominantní zdroje provozu, efektivněji plánovat budoucí rozvoj sítě, sledovat, kdo komunikoval s kým, jak dlouho a s pomocí kterého protokolu. [19]

Firma Cisco ve svých směrovačích implementovala funkce pro export informací o jednotlivých datových tocích, založené na technologii NetFlow Switching. Tyto exporty jsou nazývány NetFlow Data Export, ale vžilo se již i zjednodušené označení NetFlow. Výstupy jsou v pravidelných intervalech posílány na monitorovací server, který je může dále zpracovávat, většinou do podoby tabulek a grafů, přístupných přes webové rozhraní.

Použití NetFlow:

- **Monitorování sítě**

  Umožňuje monitorování sítě téměř v reálném čase. Techniky založené na analýze NetFlow exportů se používají k přehlednému zobrazování datových toků procházejících jednotlivými směrovači. Poskytují aktivní detekci problémů na síti a jejich odstraňování.

- **Monitorování a analýza aplikací**

  Detailní statistika používání aplikací v časových úsecích. Toho se dá využít k plánování a navržení správné topologie sítě. Například umístění a nastavení Web serveru.

- **Monitorování a analýza uživatelů**

  Detailní statistika aktivit jednotlivých uživatelů na síti. Statistika je výhodná pro efektivní plánování rozložení zatížení, umístění cache serverů apod. Také je užitečná pro detekci a řešení potenciálních bezpečnostních problémů.

- **Účtování a platby**

  Informace o datovém toku v sobě zahrnuje informaci o zdrojovém a cílovém bodě spojení (IP adresy), počtu přenesených paketů a bytů v čase, použitých portech nebo typu služby. To je vhodné pro podrobné účtování mezi jednotlivými poskytovateli připojení. Poskytovatelé tyto statistiky používají k proplacení svých služeb, a to ve většině případů na základě přeneseného objemu dat.

- **Plánování a analýza sítě**

  NetFlow Exporty se dají použít pro optimalizaci strategického plánování sítě (například kdo s kým komunikuje, plánování rozšiřování páteřních linek a bezpečnostních pravidel). Hlavním cílem je minimalizace celkové ceny síťových operací při maximalizaci výkonu sítě, kapacity a dostupnosti.

- **Ukládání dat**

  NetFlow datové exporty mohou být uloženy k pozdější analýze, v níž se dá rekonstruovat veškerý síťový provoz. Tyto služby jsou často využívány pro generování statistik a grafů vytíženosti jednotlivých linek. Zjišťují, které služby používají uživatelé vnitřních sítí a které uživatelé z vnějšího světa.

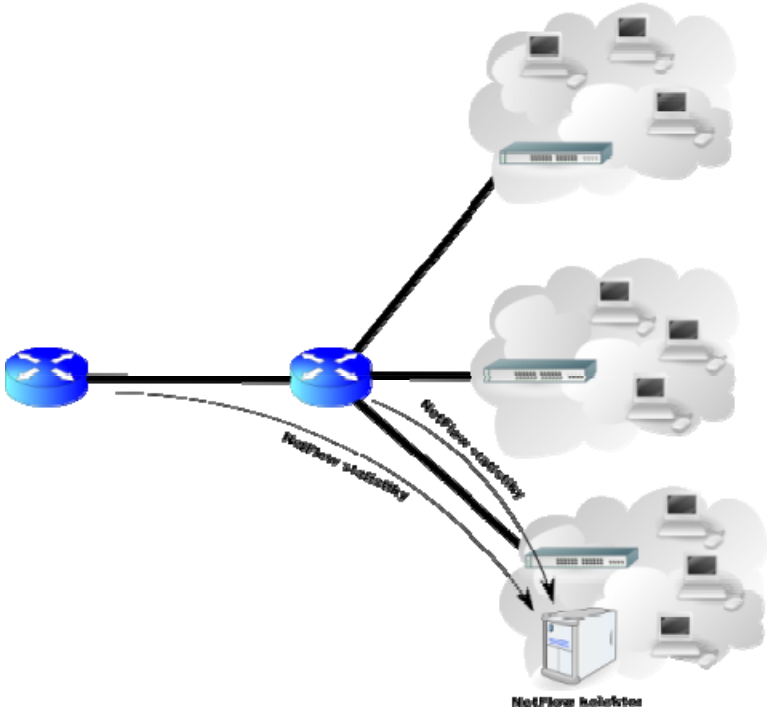
Analýza NetFlow exportů v neposlední řadě přináší informace typu kdo, kde, s kým, o čem a jak dlouho komunikoval. [20]

4.1 Architektura technologie NetFlow

NetFlow architektura se typicky skládá z několika NetFlow exportérů a jednoho NetFlow kolektoru. NetFlow exportér je připojen k monitorované lince a analyzuje procházející pakety. Na základě zachycených IP toků generuje NetFlow statistiky a ty exportuje na NetFlow kolektor. NetFlow kolektor je zařízení s velkou úložnou kapacitou, které sbírá statistiky z většího počtu NetFlow exportérů a ukládá je do dlouhodobé databáze. Nad těmito daty obvykle běží aplikace, která je umí efektivně vizualizovat a generovat z nich přehledy v podobě grafů a tabulek, které umožňují jednoduše analyzovat monitorovaný provoz i běžnému uživateli. [19]

4.1.1 Tradiční architektura

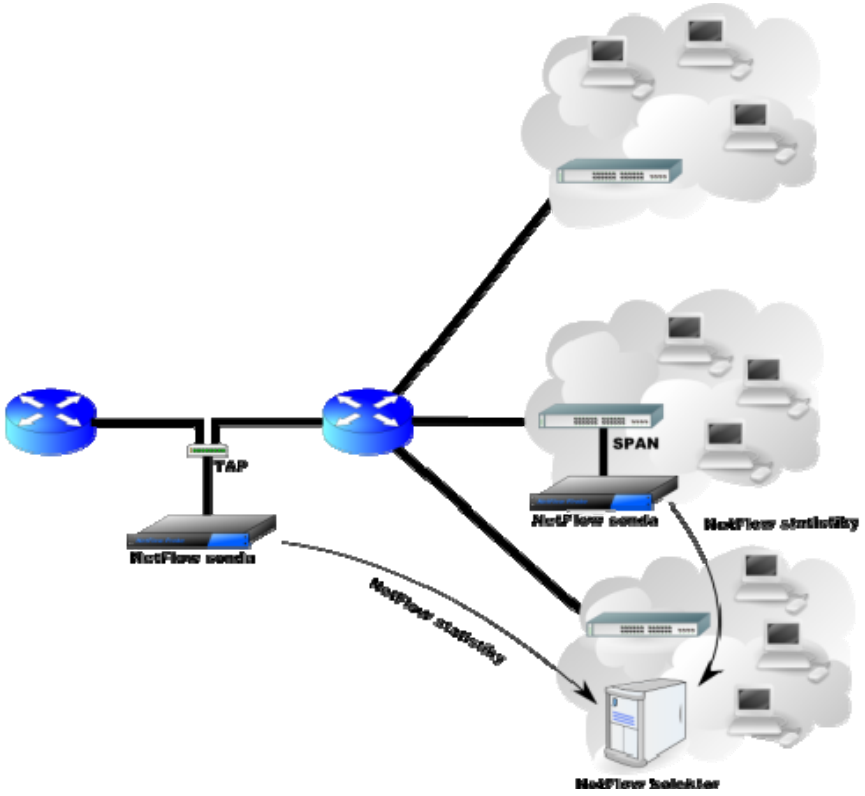
Tradiční architektura podle Cisco předpokládá na pozici NetFlow exportérů směrovače, které vedle své hlavní činnosti provádějí také výpočet NetFlow statistik. Tradiční architektura však trpí několika nevýhodami. Především se jedná o vysokou pořizovací cenu podobného zařízení, které brání jeho nasazení v malých a středních sítích. Výpočet NetFlow statistik také omezuje směrovací výkon celého zařízení, proto většina směrovačů s podporou NetFlow (s výjimkou těch nejdražších) využívá na vstupu vzorkování, tzn. pro výpočet statistik se využívá jen každý n-tý paket. Kromě snížené přesnosti měření omezuje vzorkování také pravděpodobnost odhalení bezpečnostních incidentů.



Obr. 26 *Tradiční architektura technologie NetFlow*

4.1.2 Moderní architektura

Proto se v poslední době stávají velmi oblíbenými řešení, využívající pasivní NetFlow sondy (v ČR např. FlowMon od firmy INVEA-TECH), což jsou zařízení specializovaná na monitorování a export NetFlow statistik, která jsou díky své jednoduchosti velmi levná. NetFlow sondy odstraňují všechny nevýhody tradiční architektury a na rozdíl od směrovačů je lze připojit do libovolného bodu v síti a to transparentním způsobem. Sondy procházející data pouze monitorují a nijak do nich nezasahují (proto pasivní sondy). Exportované statistiky jsou na kolektor odesílány dedikovanou linkou a díky tomu jsou na monitorované lince zcela neviditelné (na vrstvách L2 a výše). Tento rys z nich činí velmi obtížný cíl pro případné útočníky.



Obr. 27 *Moderní architektura technologie NetFlow*

4.2 IP Tok – Definice

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, bajtů a další údaje. NetFlow statistiky, vytvořené nad IP provozem poskytují informace o tom, kdo komunikoval s kým, kdy, jak dlouho, jak často, nad kterým protokolem a kolik bylo přeneseno dat. [21]

Obr. 28 *IP Tok*

4.3 Popis protokolu NetFlow

NetFlow protokol vznikl v několika verzích, první masově používanou se však stala až verze 5 (NetFlow v5) a v současnosti se začíná hojně využívat i verze 9. Na základě protokolu NetFlow v9 vznikl v nedávné době nový IETF standard Internet Protocol Flow Information eXport (IPFIX), který je taktéž velmi oblíbený a výrobci síťových technologií jej začínají hojně podporovat ve svých nejvýkonnějších směrovačích a přepínačích. Lze očekávat, že se v blízké budoucnosti pravděpodobně stane průmyslovým standardem. NetFlow nezahrnuje žádný protokol určený pro konfiguraci spojení mezi exportéry a kolektory. Kromě připojení sond nevyžaduje žádné zásahy do prvků na monitorované síti, proto běžný uživatel vůbec nepozná, že nějaké monitorování probíhá.

Verze	Popis
v1	První verze.
v2-v4	Nebyly uvedeny.
v5	Nejpoužívanější verze
v6	Podpora pro tunelovaný provoz
v7	Informace ze switchů
v9	Má strukturu danou šablonou, umožňuje mnoho kombinací
IPFIX	V podstatě v10, používá IETF standard.

Tab. 11 *Verze protokolu NetFlow*

NetFlow záznamy produkované směrovači nebo NetFlow sondami jsou exportovány na kolektor pomoci User Datagram Protokolu (UDP) nebo Stream Control Transmission Protokolu (SCTP). Jakmile je NetFlow záznam exportován, je z důvodů větší efektivity exportérem zahozen. To má za následek ztrátu NetFlow záznamu v případě, že se paket vlivem nepříznivých okolností nepodaří doručit. V případě UDP protokolu už

neexistuje možnost, jak tento NetFlow záznam znovu odeslat, a je proto ztracen navždy. Export NetFlow paketů probíhá obvykle na portech 2055, 3000-3010, 9555 nebo 9995.

NetFlow záznam obsahuje důležité statistiky o síťovém provozu. V paketu NetFlow v5 jsou obsaženy následující položky:

- Číslo verze
- Sekvenční číslo
- SNMP index vstupního a výstupního rozhraní (umožňuje sledovat vytížení jednotlivých síťových rozhraní, vyžaduje seznam rozhraní přístupný pomocí SNMP)
- Čas začátku a konce IP toku (tzn. výskyt prvního a posledního paketu tohoto toku)
- Počet bajtů a paketů v toku
- Údaje z L3 hlavičky:
    - Zdrojové a cílové IP adresy
    - Zdrojové a cílové porty
    - IP protokol
    - Type of Service (ToS)
- U TCP toků obsahuje množinu tvořenou sjednocením všech TCP flagů, které se v toku vyskytly.
- Směrovací informace:
    - IP adresa příštího skoku (důležité pro analýzu routovacích postupů)
    - Maska cílové a zdrojové IP adresy (délky prefixů podle CIDR notace)

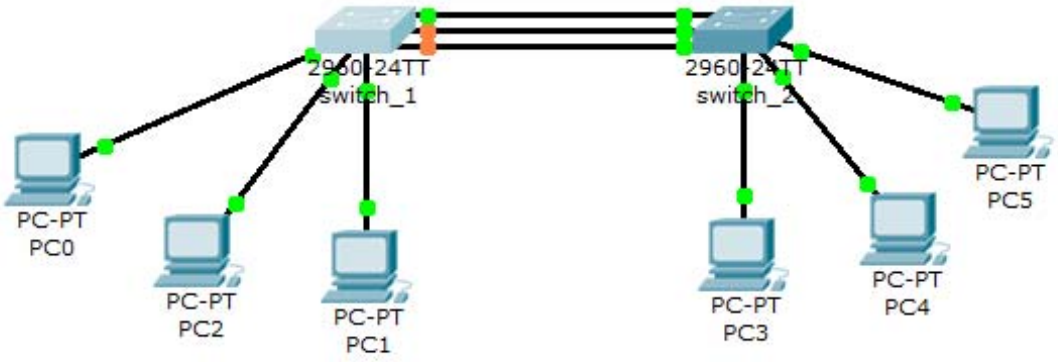
Některé exportéry také uvádějí hodnotu zdrojového a cílového autonomního systému (AS). Tato hodnota však nemusí být vždy přesná. NetFlow v9 je definována jako flexibilní formát. Může obsahovat všechny hodnoty verze 5 a další volitelné položky, např. MPLS, IPv6 adresy a porty atd. [19]

II. PRAKTICKÁ ČÁST

5 ETHERCHANNEL

5.1 Topologie

Typická topologie pro EtherChannel je naznačena na Obr. 29 *Topologie*. U této topologie jsou dva přepínače, které jsou navzájem propojeny pomocí technologie EtherChannel a k nim je připojen zbytek sítě.

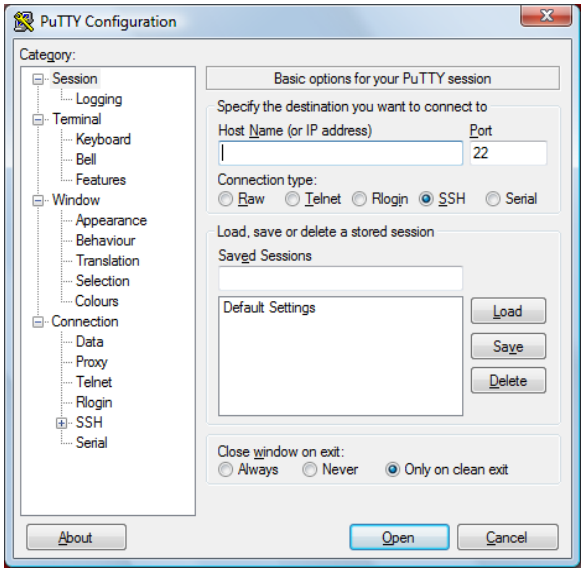


Obr. 29 *Topologie EtherChannelu*

5.2 Nastavení přepínačů

Nejprve je potřeba se připojit k zařízení přes speciální port, který je označen konsole. U routerů ho ve většině případů nalezneme na přední části, mezi ostatními porty, u přepínačů je obyčejně umístěn v zadní části, proto je hůře dostupný. Pro připojení mezi přepínačem a počítačem byl použit sériový port.

Pro nastavení přepínačů byl použit freeware program Putty. Tento program podporuje připojení pomocí několika protokolů (Telnet, SSH, COM). V učebně bylo použito připojení pomocí COMu.



Obr. 30 *Program Putty*

Na obou přepínačích byl postupně nastaven EtherChannel pro 2, 4, 6 a 8 portů pro oba protokoly (jak PAgP tak LACP). Každé nastavení bylo uloženo do flash paměti přepínače. Kvůli značnému opakování takřka stejných příkazů je zde uvedeno pouze ukázkové nastavení přepínače pro 4 porty v EtherChannelu (pro 2, 6 a 8 portů je nastavení takřka totožné).

5.2.1 Příkazy pro nastavení EtherChannelu na 4 porty s protokolem PAgP

Switch>enable
Switch#configure terminal
Switch (config)#interface range fastethernet0/1 -4
Switch (config-if-range)#switchport mode access
Switch (config-if-range)#switchport access vlan 1
Switch (config-if-range)#channel-group 1 mode desirable non-silent
Creating a port-channel interface Port-channel 1

Switch (config-if-range)#end
Switch#copy running-config flash:
Destination filename [running-config] ? chan_4P_pagp

Switch#configure terminal
Switch (config)#port-channel load-balance src-mac
Switch (config)#end
Switch#copy running-config flash:
Destination file name [running-config] ? chan_4_pagp

Switch#configure terminal
Switch (config)#interface range fastethernet0/1 -4
Switch (config-if-range)#pagp learn-method physical-port
Switch (config-if-range)#pagp port-priority 200
Switch (config-if-range)#end
Switch# copy running-config flash:
Destination filename [running-config] ? chan_4P_pagp

5.2.2 Příkazy pro nastavení EtherChannelu na 4 porty s protokolem LACP

Switch>enable
Switch#configure terminal
Switch (config)#interface range fastethernet0/1 -4
Switch (config-if-range)#switchport mode access
Switch (config-if-range)#switchport access vlan 1
Switch (config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1

Switch (config-if-range)#end
Switch#copy running-config flash:
Destination filename [running-config] ? chan_4P_lacp

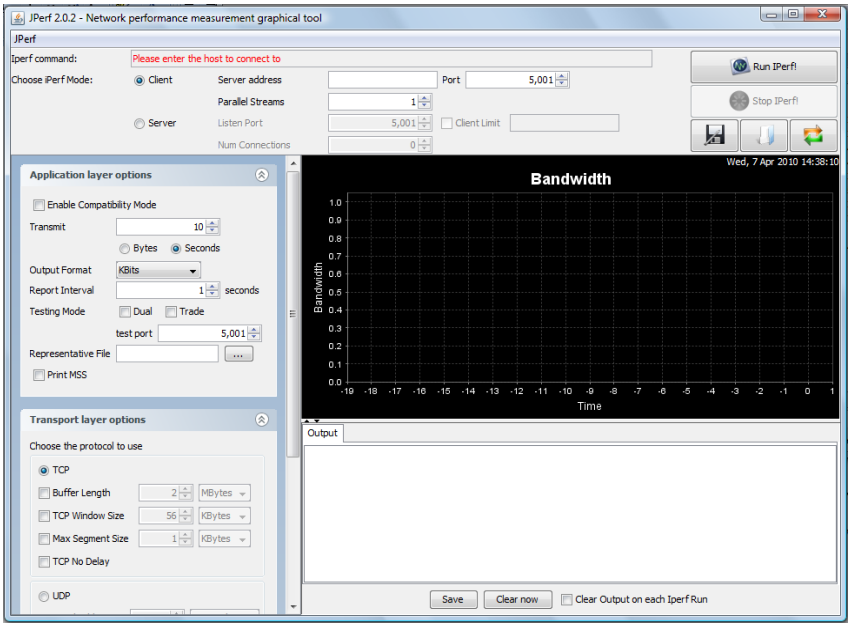
Switch#configure terminal
Switch (config)#port-channel load-balance src-mac
Switch (config)#end
Switch#copy running-config flash:
Destination file name [running-config] ? chan_4P_lacp

Switch#configure terminal
Switch (config)#lacp system-priority 20000
Switch (config)#end
Switch#copy running-config flash:
Destination filename [running-config] ? chan_4P_lacp

Switch#configure terminal
Switch (config)#interface range fastethernet0/1 -4
Switch (config-if-range)#lacp port-priority 15000
Switch#end
Switch#copy running-config flash:
Destination filename [running-config] ? chan_2P_lacp

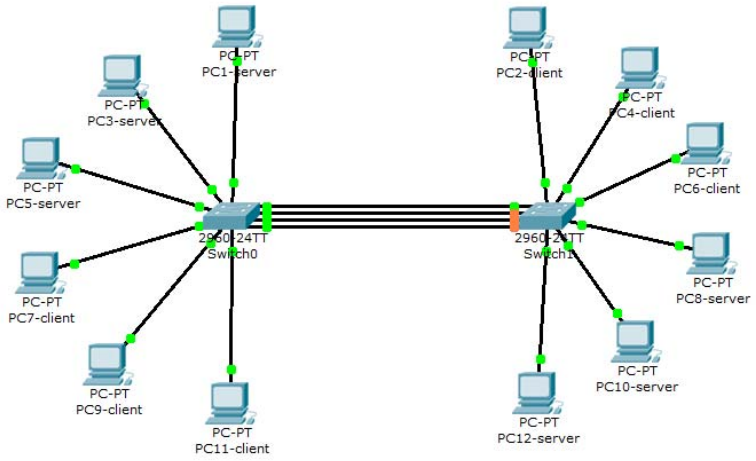
5.3 Testování EtherChannelu

Testování EtherChannelu bylo provedeno pomocí programu Iperf 2.0.2. Program je potřeba spustit na dvou počítačích, mezi kterými se má měřit maximální přenosová kapacita média. Iperf se na jednom počítači spouští jako client a na druhém jako server (client se vždy připojuje k serveru). Program po určitých intervalech zjišťuje jaká je maximální propustnost média mezi zařízením. U testování EtherChannelu to má tu nevýhodu, že přepínače mohou „stíhat“ předávat pakety i bez použití této technologie nebo ji budou využívat je omezeně. Tato nevýhoda se dá značně snížit za použití velice krátkých intervalů a větším počtem komunikujících stanic.



Obr. 31 *Program Iperf 2.0.2*

Dále byla vytvořena testovací topologie, na které bylo prováděno testování funkčnosti technologie EtherChannel. Pro testování se využilo všech dvanácti počítačů, které v počítačové učebně U52B204 byly k dispozici. Tyto počítače byly rozděleny do dvou sítí, které byly propojeny pomocí přepínačů, mezi nimiž byla nastavena technologie EtherChannel viz. Obr. 32. V každé síti byly tři počítače, na kterých byl program Iprerf spuštěn jako server a 3 počítače, na kterých byl spuštěn jako client. Clienti se vždy připojovali k serverům z druhé sítě. V praxi by tato síť mohla být rozšířena ještě o routery, které by „dohlížely“ na provoz v jednotlivých sítích.



Obr. 32 *Testovací topologie*

Z paměti přepínače do running-configu (příkazem *copy*) byly postupně nahrány jednotlivá nastavení EtherChannelu pro 2, 4, 6 a 8 portů pro oba protokoly (PAgP, LACP) vždy ve stejném pořadí a na všech počítačích byl spuštěn program Iperf pro měření maximální kapacity média na 100 sekund. Po uplynutí měřící doby program zobrazil průměrnou hodnotu propustnosti sítě, která byla zapsána do tabulky. Celé měření se opakovalo 5 krát pro každé nastavení. Výsledky měření jsou uvedeny v tabulkách níže:

Propojení bez EtherChannelu						
č. m.	Rychlost mezi jednotlivými počítači [kBit/s]					
	PC1 - PC2	PC3 - PC4	PC5 - PC6	PC7 - PC8	PC9 - PC10	PC11 - PC12
1	34 579	33 329	30 907	31 004	32 505	33 813
2	34 951	34 197	31 774	31 851	34 538	36 016
3	34 052	33 346	30 983	30 964	32 885	33 435
4	34 313	33 628	31 076	31 037	32 816	33 670
5	34 810	33 573	31 185	31 016	32 688	33 682
Průměr:	34 541	33 615	31 185	31 174	33 086	34 123
Celkový průměr:	**32 954**					

Tab. 12 *Propustnost média (bez EtherChannelu)*

Propojení s Etherchannelem (channel_2P_pagp)						
č. m.	Rychlost mezi jednotlivými počítači [kBit/s]					
	PC1 - PC2	PC3 - PC4	PC5 - PC6	PC7 - PC8	PC9 - PC10	PC11 - PC12
1	79 123	81 374	45 250	47 724	46 631	47 745
2	83 098	81 019	46 515	48 926	47 259	47 758
3	83 772	79 346	45 153	46 921	46 962	47 163
4	84 621	79 924	44 730	46 099	45 790	45 032
5	85 557	80 926	46 235	48 302	46 719	44 532
Průměr:	83 234	80 518	45 577	47 594	46 672	46 446
Celkový průměr:	**58 340**					

Tab. 13 *Propustnost média (EtherChannel, 2 porty, PAgP)*

Propojení s Etherchannelem (channel_4P_pagp)						
č. m.	Rychlost mezi jednotlivými počítači [kBit/s]					
	PC1 - PC2	PC3 - PC4	PC5 - PC6	PC7 - PC8	PC9 - PC10	PC11 - PC12
1	90 475	89 952	82 386	82 815	74 837	85 412
2	90 442	89 906	82 541	83 246	74 223	83 159
3	89 760	89 442	82 073	81 072	75 881	84 579
4	90 879	89 954	82 329	80 573	75 749	85 586
5	89 394	90 487	81 813	83 238	74 951	84 890
Průměr:	90 190	89 948	82 228	82 189	75 128	84 725
Celkový průměr:	**84 068**					

Tab. 14 *Propustnost média (EtherChannel, 4 porty, PAgP)*

Propojení s Etherchannelem (channel_6P_pagp)						
č. m.	Rychlost mezi jednotlivými počítači [kBit/s]					
	PC1 - PC2	PC3 - PC4	PC5 - PC6	PC7 - PC8	PC9 - PC10	PC11 - PC12
1	89 616	89 896	85 118	86 169	78 955	83 508
2	88 612	89 319	84 381	85 444	78 770	83 642
3	90 395	88 360	84 249	85 490	79 824	84 247
4	90 593	89 971	85 127	84 692	85 829	83 965
5	90 578	89 891	85 108	81 608	82 268	84 414
Průměr:	89 959	89 487	84 797	84 681	81 129	83 955
Celkový průměr:	**85 668**					

Tab. 15 *Propustnost média (EtherChannel, 6 portů, PAgP)*

Propojení s Etherchannelem (channel_8P_pagp)						
č. m.	Rychlost mezi jednotlivými počítači [kBit/s]					
	PC1 - PC2	PC3 - PC4	PC5 - PC6	PC7 - PC8	PC9 - PC10	PC11 - PC12
1	89 961	90 586	87 698	90 477	84 913	87 649
2	89 906	90 512	87 750	90 485	79 852	87 878
3	90 126	89 840	87 752	90 397	78 116	87 487
4	90 075	90 045	87 993	88 934	82 960	87 645
5	89 590	89 997	89 898	87 547	80 340	87 632
Průměr:	89 932	90 196	88 218	89 568	81 236	87 658
Celkový průměr:	**87 801**					

Tab. 16 *Propustnost média (EtherChannel, 8 portů, PAgP)*

Propojení s Etherchannelem (channel_2P_lacp)						
č. m.	Rychlost mezi jednotlivými počítači [kBit/s]					
	PC1 - PC2	PC3 - PC4	PC5 - PC6	PC7 - PC8	PC9 - PC10	PC11 - PC12
1	83 555	84 835	45 831	46 666	45 918	45 012
2	86 261	78 806	45 966	47 749	44 581	44 267
3	81 851	81 074	44 295	45 789	44 983	44 314
4	84 699	80 485	44 293	45 694	46 488	46 863
5	85 334	79 436	48 479	46 064	46 308	47 143
Průměr:	84 340	80 927	45 773	46 392	45 656	45 520
Celkový průměr:	**58 101**					

Tab. 17 *Propustnost média (EtherChannel, 2 porty, LACP)*

Propojení s Etherchannelem (channel_4P_lacp)						
č. m.	Rychlost mezi jednotlivými počítači [kBit/s]					
	PC1 - PC2	PC3 - PC4	PC5 - PC6	PC7 - PC8	PC9 - PC10	PC11 - PC12
1	86 679	89 296	79 804	81 098	80 067	84 683
2	90 753	90 150	73 931	82 128	80 074	85 101
3	90 651	89 250	78 971	81 656	80 590	84 820
4	89 871	88 791	76 555	81 389	77 128	84 767
5	88 991	90 027	74 960	81 590	82 258	85 193
Průměr:	89 389	89 503	76 844	81 572	80 023	84 913
Celkový průměr:	**83 707**					

Tab. 18 *Propustnost média (EtherChannel, 4 porty, LACP)*

Propojení s Etherchannelem (channel_6P_lacp)						
č. m.	Rychlost mezi jednotlivými počítači [kBit/s]					
	PC1 - PC2	PC3 - PC4	PC5 - PC6	PC7 - PC8	PC9 - PC10	PC11 - PC12
1	88 071	90 036	81 897	85 785	86 911	83 443
2	90 740	89 420	79 188	80 987	82 059	83 096
3	88 761	89 584	80 345	84 333	80 922	83 534
4	89 186	89 912	79 580	83 288	81 911	82 885
5	88 696	89 627	79 192	83 353	85 667	83 599
Průměr:	89 091	89 716	80 040	83 549	83 494	83 311
Celkový průměr:	**84 867**					

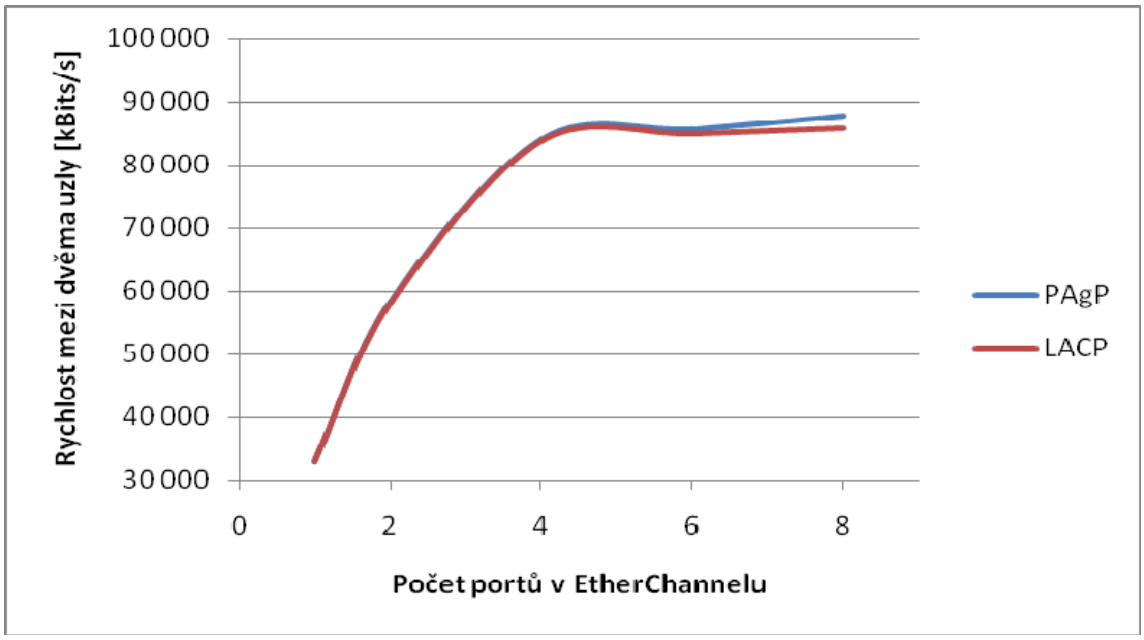
Tab. 19 *Propustnost média (EtherChannel, 6 portů, LACP)*

Propojení s Etherchannelem (channel_8P_lacp)						
č. m.	Rychlost mezi jednotlivými počítači [kBit/s]					
	PC1 - PC2	PC3 - PC4	PC5 - PC6	PC7 - PC8	PC9 - PC10	PC11 - PC12
1	90 110	90 037	83 349	90 477	85 227	87 924
2	90 334	89 243	79 673	89 336	83 539	87 888
3	89 579	90 249	83 149	90 489	52 883	87 626
4	89 536	90 484	80 955	90 395	78 405	87 997
5	89 736	89 766	83 944	89 102	77 090	87 666
Průměr:	89 859	89 956	82 214	89 960	75 429	87 820
Celkový průměr:	**85 873**					

Tab. 20 *Propustnost média (EtherChannel, 8 portů, LACP)*

5.4 Rekapitulace technologie EtherChannel

Jak je zřejmé z naměřených hodnot rychlostí, je důležité si při sestavování EtherChannelu dobře rozmyslet, kolik portů využijeme pro tuto technologii v závislosti na počtu komunikujících stanic v síti. Tento fakt je dobře vidět z grafu na Obr. 33. Pokud by se mělo dosáhnout optimální rychlosti za použití přiměřeného počtu portů, tak by byl v tomto případě použit EtherChannel pouze pro 4 porty, což by měl být optimální poměr rychlost k počtu využitých portů.



Obr. 33 *Graf závislosti počtu portů na výsledné rychlosti*

5.4.1 Na co si dávat při nastavování EtherChannelu pozor

- Vždy musí být obě zařízení stejně nastavena.
- Zjistit si kolik portů v EtherChannelu dané zařízení podporuje. Např.: switch Catalyst 2960 podporuje 8 portů v EtherChannelu pro protokol PAgP a až 16 portů pro protokol LACP.
- Zjistit si na jaké vrstvě zařízení pracuje, pro správné nastavení rozložení zátěže. Např.: switch Catalyst 2960 pracuje pouze na druhé vrstvě, proto jde nastavit rozložení zátěže (load balancing) pouze podle fyzických adres.
- Při nastavování mít všechny porty vypnuté (shutdown) a po nastavení je nezapomenout zapnout.
- Na správné označování ethernetových portů a jejich rozsahu.

5.4.2 Marketingový tah společnosti Cisco

Technologie EtherChannel je jistě velice výhodná a cenově přijatelná investice pro mnoho firem, kde se stále zvyšují nároky na rychlost připojení do sítě. Správce sítě může stále zvyšovat rychlosti jen pouhým přidáváním kabelů.

Podle oficiálních prospektů společnosti Cisco je zřejmé, že pokud by do EtherChannelu byly připojeny čtyři 100Mbps porty měl by vzniknout jeden logický svazek o kapacitě 400Mbps. Ale proč takové hodnoty nebyly naměřeny? Protože deterministické, automatické rozložování zátěže směřuje provoz vždy přes jednu linku. Ale i přes tuto malou marketingovou „lež“ se dá říci, že se jedná o velice jednoduchý způsob zrychlení provozu po síti.

6 NETFLOW

6.1 Testovací topologie

Pro otestování technologie NetFlow byla nejprve vytvořena vhodná topologie sítě, v které se bude sledovat provoz. Podobně jako u technologie EtherChannel byly počítače v učebně rozděleny na dvě poloviny, každá polovina tvořila jednu síť. Každá síť byla připojena do switche Catalyst 2960 a ten byl připojen k routeru série 2800, routery byly propojeny přes sériovou linku, která značně síť zpomalovala, ale pro testovací účely byla postačující. K druhému routeru byl připojen ještě notebook, který zde zastával roli NetFlow kolektoru. Topologie pro technologii NetFlow je naznačena na Obr. 34.

Následně byly vypočítány IP adresy, které jsou pro zprovoznění sítě velice potřebné. Byla vybrána síť s IP adresou 192.168.10.0. Aby nedošlo k plýtvání IP adresami, celá síť byla rozdělena na několik podsítí a pro každou z nich byl vypočítán potřebný rozsah IP adres.

Síť 1:

IP: 192.168.10.1 až 192.168.10.14

Maska: 255.255.255.240

Síť 2:

IP: 192.168.10.17 až 192.168.10.30

Maska: 255.255.255.240

Síť 3:

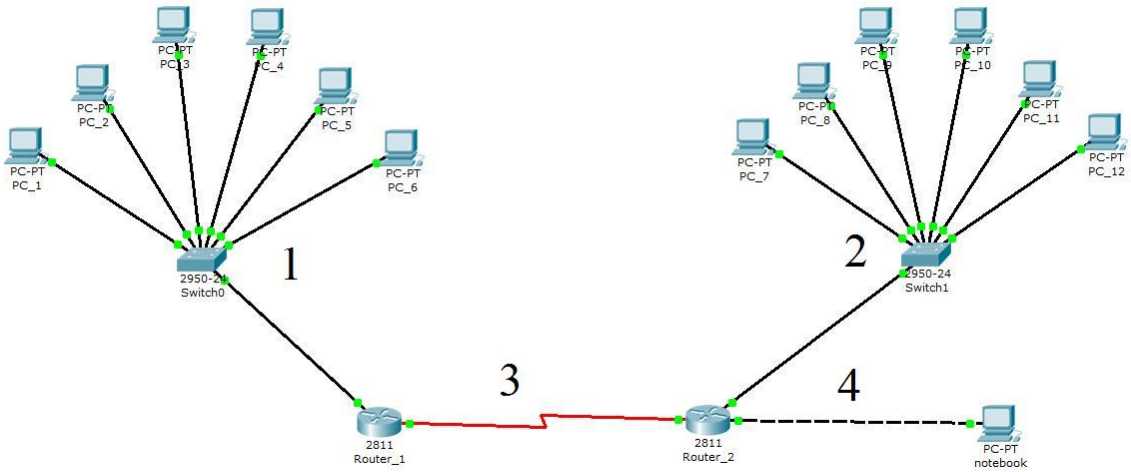
IP: 192.168.10.33, 192.168.10.34

Maska: 255.255.255.252

Síť 4:

IP: 192.168.10.37, 192.168.10.38

Maska: 255.255.255.252



Obr. 34 *Topologie pro technologie Netflow*

6.2 Nastavení technologie NetFlow

Připojení k routeru přes konzoli bylo provedeno naprosto stejně jako v případě switche. I v tomto případě byl použit program PuTTY, který se připojoval přes sériovou linku (COM). V tomto případě bylo zapotřebí nastavit oba routery. Jako routovací protokol byl využit protokol RIP verze 2.

6.2.1 Nastavení prvního routeru

Router>enable
Router#configure terminal
Router(config)#hostname Router_1
Router_1(config)#interface FastEthernet0/0
Router_1(config-if) # ip address 192.168.10.1 255.255.255.240
Router_1(config-if) #no shutdown
Router_1(config-if) #exit
Router_1(config) #interface serial0/1/1
Router_1(config-if) #clock rate 9600

Router_1(config-if) # ip address 192.168.10.33 255.255.255.252

Router_1(config-if) #no shutdown

Router_1(config-if) #exit

Router_1(config) #router rip

Router_1(config-router) #version 2

Router_1(config-router) #network 192.168.10.0

Router_1(config-router) #end

Router_1#copy running-config flash:

Destination file name [running-config]? router_1_netflow

6.2.2 Nastavení druhého routeru

Router>enable

Router#configure terminal

Router(config)#hostname Router_2

Router_2(config)#interface FastEthernet0/0

Router_2(config-if) # ip address 192.168.10.17 255.255.255.240

Router_2(config-if) #no shutdown

Router_2(config-if) #exit

Router_2(config)#interface FastEthernet0/1

Router_2(config-if) # ip address 192.168.10.37 255.255.255.252

Router_2(config-if) #no shutdown

Router_2(config-if) #exit

Router_2(config) #interface serial0/1/0

Router_2(config-if) #clock rate 9600

Router_2(config-if) # ip address 192.168.10.34 255.255.255.252

Router_2(config-if) #no shutdown

Router_2(config-if) #exit

Router_2(config) #router rip

Router_2(config-router) #version 2

Router_2(config-router) #network 192.168.10.0

Router_2(config) #end

Router_2#copy running-config flash:

Destination file name [running-config]? router_2_netflow

6.2.3 Nastavení odesílání sběru NetFlow dat na druhém routeru

Router>enable
Router#configure terminal
Router_2(config)#ip cef
Router_2(config) #interface serial0/1/0
Router_2(config-if) #ip flow ingress
Router_2(config-if) #exit
Router_2(config) #ip flow-export version 9
Router_2(config) #ip flow-export destination 192.168.10.38 9997
Router_2(config) #ip flow-export source FastEthernet0/1
Router_2(config) #end
Router_2#copy running-config flash:
Destination file name [running-config]? router_2_netflow

6.3 Programy pro sledování sítě

Pro sledování provozu po síti byly vybrány celkem 3 programy. ManageEngine NetFlow Analyzer 7.5, PRTG Network Monitor a Observer. Všechny tři verze jsou placené a jsou vydávány v několika verzích. Pro odzkoušení byly staženy 30-ti denní trial verze těch nejlepších verzí od každého programu. Postupně byly odzkoušeny všechny tři programy.

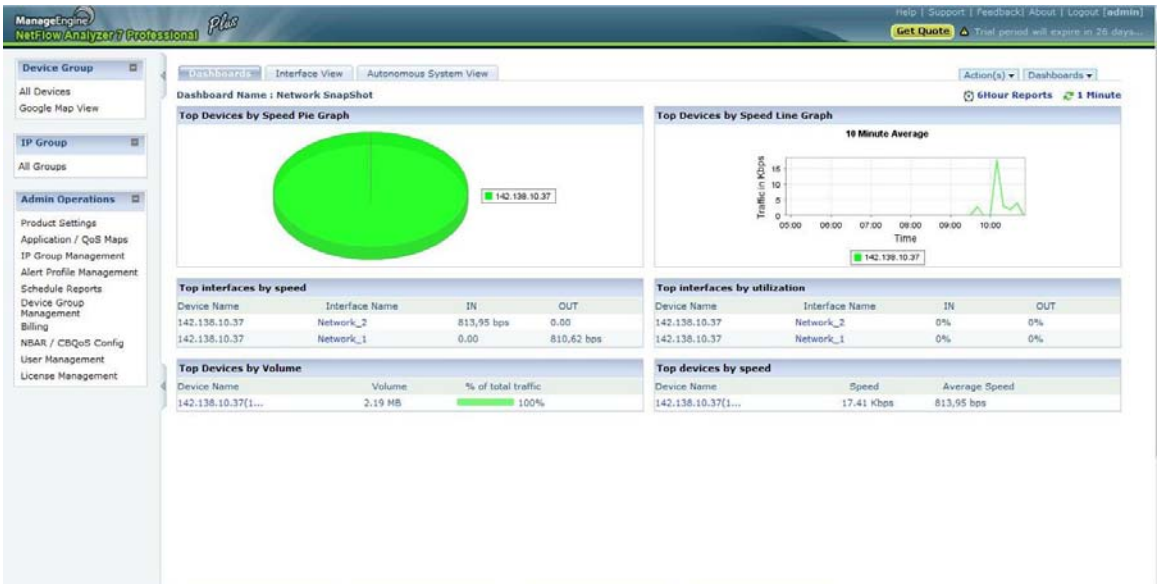
6.3.1 ManageEngine NetFlow Analyzer

Program byl stažen z http://www.manageengine.com/products/netflow/. Při instalaci se program do počítače nainstaluje jako služba, která se zapíná automaticky. Zároveň s programem se do počítače nainstaluje MySQL databáze a webový server. Při instalaci se nás instalační program ještě zeptá, jaký používáme webový port (standardně je to port 8080) a ještě na jakém portu má „odposlouchávat“ provoz (v našem případě 9997). Další nastavování již není nutné.

Program se ovládá přes webové rozhraní výchozího webového prohlížeče, v tomto případě se jednalo o webový prohlížeč Google Chrome. Při spuštění programu se spustí

webový prohlížeč s úvodní stránkou programu, kde je potřeba zadat uživatelské jméno a heslo. Defaultně je zde nastaveno admin jako uživatelské jméno a heslo je také admin. Po přihlašovacím procesu jsou zobrazeny statistiky provozu po síti. Program také nabízí rozsáhlé možnosti nastavení sledování z jednotlivých segmentů sítě.

Cena tohoto programu se pohybuje od 800 do 100 000 amerických dolarů. Záleží na počtu sledovaných linek, a jestli si klient připlatí za roční údržbu a technickou podporu zdarma.



Obr. 35 *Prostředí programu NetFlow Analyzer 7 Profesional*

Obr. 36 *Zobrazení provozu mezi jednotlivými sítěmi*

Obr. 37 *Podrobnější výpis provozu v jedné síti*

Přednosti ManageEngine NetFlow Analyzer

Z webových stránek produktu (http://www.manageengine.com/) bylo vybráno několik hlavních předností tohoto programu:

- **Monitorování šířky pásma**

  Ve většině podniků, neudržování pásma vede k tomu, že nežádoucí aplikace má přednost před důležitými podnikovými aplikacemi ve chvíli, kdy je nejvíce potřeba. NetFlow Analyzer ukáže přesně to, co každá aplikace využívá. To pomáhá při kontrole šířky pásma a prosazování lepších politik v rámci celého podniku. NetFlow Analyzer se stává velmi dostupnou alternativu pro podniky, které potřebují sledovat využití šířky pásma, ale nechtějí investovat zbytečně moc finančních prostředků.

- **Důkladná analýza přenosů**

  Bez použití hardwarových sond nebo speciálních zařízení, NetFlow Analyzer umožňuje analýzu provozu velice jednoduše a účinně. Kromě nastavení směrovacích / přepínacích zařízení na export NetFlow dat do NetFlow Analyzer není žádná další konfigurace potřebná. NetFlow Analyzer používá NetFlow ®, sFlow ®, cflowd ®, J-Flow ®, IPFIX ®, NetStream ® a Cisco NBAR ® pro zobrazení běžících aplikací, hostů a konverzací, které využívají danou šířku pásma.

Tyto informace jsou životně důležité pro pochopení provozu ve špičce, dále jako podpora pásma pro kapacitní plánování a prosazování bezpečnostní politiky.

- **QoS validace pomocí Cisco CBQoS**

Aby bylo zajištěno, že důležité obchodní aplikace obdrží nejvyšší prioritu v síti, mohou správci sítě implementovat QoS politiku a doladit ji pomocí Cisco CBQoS technologie, která ji snadno podporuje v NetFlow Analyzer. Pomocí NetFlow Analyzer je možné vidět jaká politika používá jaké rozhraní a je možné si ověřit tyto QoS politiky pomocí monitoringu před-politikou a po-politice.

- **Varování na limity**

NetFlow Analyzer generuje výstrahy, když využití linky je větší než nastavený limit, v takovém případě může například přijít email. Také dopředu varuje před SNMP trapy, NMS / EMS aplikacemi pro kritické záznamy v síti. To pomáhá k rychlejšímu stanovení problému v síti.

- **Vytváření skupin**

Umožňuje vytvářet oddělení / divize na základě IP adres, s možností filtrace na základě žádosti a rozhraní. Pak můžete zobrazit statistiky využití šířky pásma pro určitou skupinu IP.

- **Vlastní zprávy**

NetFlow Analyzátor je aktivní nástroj, který nejen sleduje, ale přináší efektivní hlášení. Hlášení o chybách naleznete v NetFlow analyzer velice jednoduše a následně uvidíte i konkrétní parametry chybového hlášení. Například můžete zobrazit pásmo, které využívá specifický hostitel nebo síť, pro přístup

k jednotlivé aplikaci v průběhu určitého týdne. Tyto možnosti poskytují větší pružnost při plnění vašich potřeb monitorování šířky pásma.

- **Snížené provozní náklady**

NetFlow Analyzer snižuje náklady tím, že zjednodušuje úkoly managementu. Řešení problémů trvá mnohem kratší dobu, než s paket analyzátory, které vyžadují mnohem více času na analýzu výsledků, aby dospěly k potřebným závěrům. Šířka pásma zprávy a sloučení určitých možností umožňuje provést analýzu provozu rychleji, účinněji a efektivně s využitím klíčových zdrojů podniku.

- **Snížené náklady na školení**

NetFlow Analyzer snižuje náklady na vzdělávání tím, že poskytuje jednoduchý a uživatelsky příjemný web klient, ve kterém se provádějí všechny operace. Zahrnuje také MySQL databázi pro ukládání dat Flow, což přinese úsporu času správci, který nemusí pracovat s více balíčky a zajišťovat, tak kompatibilitu mezi nimi.

- **Efektivní ukládání dat**

Data jsou uložena v souhrnných a nesouhrnných formátech. Souhrnných může být 100 a jsou uloženy navždy a poskytují zprávy pro plánování kapacity a dlouhodobé podávání zpráv. Nesouhrnné (nebo RAW) data mohou být uložena po dobu až 1 měsíc a umožňují řešení potíží.

- **Přístupné všude**

NetFlow Analyzer je zcela on-line, což usnadňuje zobrazení provozu na síti přes sítě WAN odkudkoli v síti pouze pomocí webového prohlížeče. NetFlow

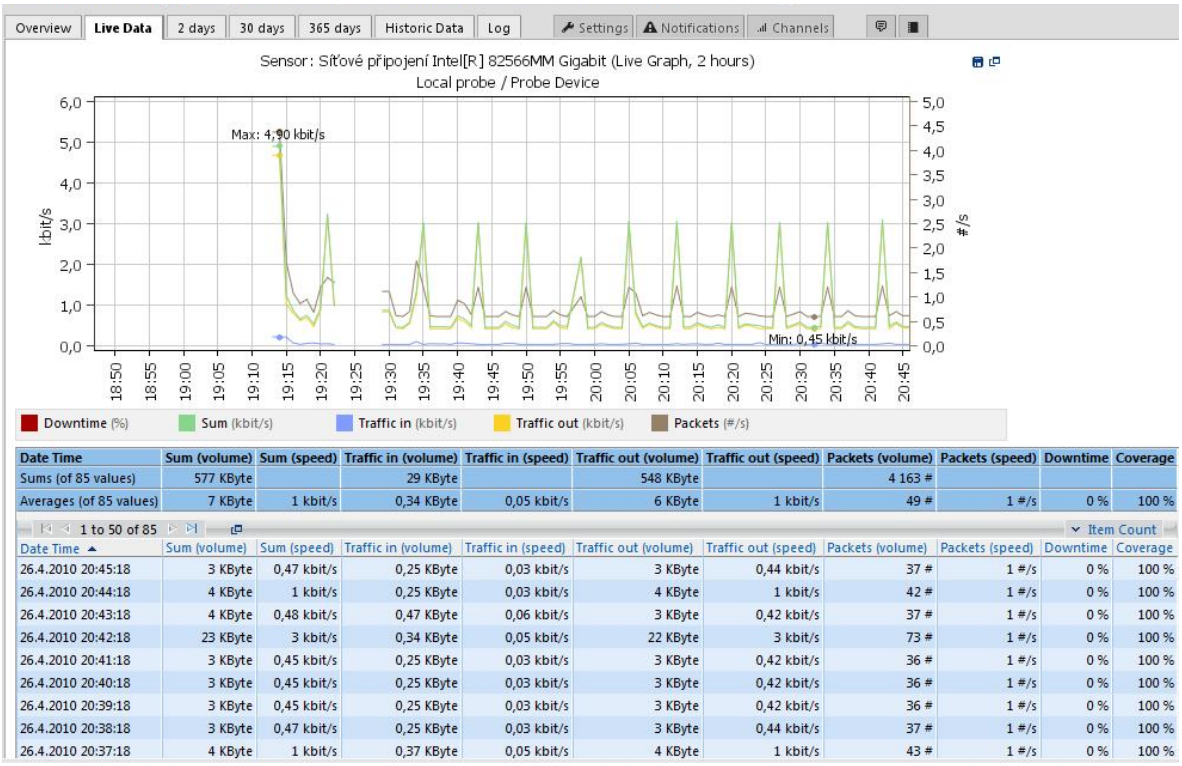
Analyzer je vydáván ve dvou verzích jedna je pro platformu Windows a druhá pro Linux.

6.3.2 PRTG Network Monitor

Program je ke stažení na http://www.paessler.com/prtg/download, kde je potřeba si vybrat verzi a následně začne stahování. Dále na této stránce jste vyzváni k vyplnění formuláře. Po vyplnění formuláře vám dojde email se sériovým číslem, jenž je potřeba k instalaci tohoto softwaru.

K dokončení instalace je ještě potřeba vyplnit další formulář, kde je potřeba si vytvořit uživatelské jméno a heslo. Dále je zde potřeba zadat číslo webového portu a několik dalších informací podobně jako v předešlém případě. PRTG Network Monitor se spouští buď ve webovém prohlížeči, nebo jako aplikace GUI je tu ještě jedno možnost pomocí iPhone App. Záleží na uživateli, jaký způsob preferuje.

Cena tohoto programu se pohybuje od 250 do 5 850 euro. Cena se odvíjí od počtu sledovaných linek. Samozřejmostí je možnost si připlatit za další nadstandardní služby.



Date Time	Sum (volume)	Sum (speed)	Traffic in (volume)	Traffic in (speed)	Traffic out (volume)	Traffic out (speed)	Packets (volume)	Packets (speed)	Downtime	Coverage
Sums (of 85 values)	577 KByte		29 KByte		548 KByte		4 163 #			
Averages (of 85 values)	7 KByte	1 kbit/s	0,34 KByte	0,05 kbit/s	6 KByte	1 kbit/s	49 #	1 #/s	0 %	100 %

1 to 50 of 85 — Item Count

Date Time	Sum (volume)	Sum (speed)	Traffic in (volume)	Traffic in (speed)	Traffic out (volume)	Traffic out (speed)	Packets (volume)	Packets (speed)	Downtime	Coverage
26.4.2010 20:45:18	3 KByte	0,47 kbit/s	0,25 KByte	0,03 kbit/s	3 KByte	0,44 kbit/s	37 #	1 #/s	0 %	100 %
26.4.2010 20:44:18	4 KByte	1 kbit/s	0,25 KByte	0,03 kbit/s	4 KByte	1 kbit/s	42 #	1 #/s	0 %	100 %
26.4.2010 20:43:18	4 KByte	0,48 kbit/s	0,47 KByte	0,06 kbit/s	3 KByte	0,42 kbit/s	37 #	1 #/s	0 %	100 %
26.4.2010 20:42:18	23 KByte	3 kbit/s	0,34 KByte	0,05 kbit/s	22 KByte	3 kbit/s	73 #	1 #/s	0 %	100 %
26.4.2010 20:41:18	3 KByte	0,45 kbit/s	0,25 KByte	0,03 kbit/s	3 KByte	0,42 kbit/s	36 #	1 #/s	0 %	100 %
26.4.2010 20:40:18	3 KByte	0,45 kbit/s	0,25 KByte	0,03 kbit/s	3 KByte	0,42 kbit/s	36 #	1 #/s	0 %	100 %
26.4.2010 20:39:18	3 KByte	0,45 kbit/s	0,25 KByte	0,03 kbit/s	3 KByte	0,42 kbit/s	36 #	1 #/s	0 %	100 %
26.4.2010 20:38:18	3 KByte	0,47 kbit/s	0,25 KByte	0,03 kbit/s	3 KByte	0,44 kbit/s	37 #	1 #/s	0 %	100 %
26.4.2010 20:37:18	4 KByte	1 kbit/s	0,37 KByte	0,05 kbit/s	4 KByte	1 kbit/s	43 #	1 #/s	0 %	100 %

Obr. 38 *Provoz sledovaný programem PRTG Network Monitor*

Přednosti PRTG Network Monitor

Z webových stránek produktu (http://www.peassler.com/) bylo vybráno několik hlavních předností tohoto programu:

- **Snadné použití: Vyberte si mezi třemi uživatelskými rozhraními**
  - Rozhraní webového prohlížeče
  - Windows GUI: nativní Windows aplikace, zejména pro velké instalace
  - iPhone app (je třeba zakoupit samostatně)
  - Všechny uživatelské rozhraní umožňuje zabezpečené SSL a pro vzdálený přístup a mohou být použity současně

- **Komplexní Network Monitoring**
  - Monitorování šířky pásma pomocí SNMP, WMI, NetFlow, sFlow, Packet Sniffing.

- Aplikace pro sledování
- SLA monitoring
- VoIP / QoS Monitoring
- LAN, WAN, VPN, atd.
- Rozsáhlé protokolování událostí
- Více než 50 sledovaných položek

- **Flexibilní Varování**
  - 10 možností oznámení: e-mail, SMS / Pager, Instant messaging, syslog a SNMP Trap, HTTP požadavek, Event log vstup, Play soubory - zvuk alarmu, nebo jakékoliv externí soubory, které mohou být spuštěny (EXE nebo dávkový soubor)
  - Status upozornění (nahoru, dolů, varování)
  - Záznamy Limit (hodnota, nad / pod x)
  - Záznamy Threshold (nad / pod x za y minut)
  - Vícenásobná podmínka záznamů (X a Y jsou dole)
  - Eskalace upozornění (extra oznámení každých x minut během výpadku)

- **Podrobné výkazy**
  - Zprávy ve formátu HTML nebo PDF formátu
  - Historické údaje z monitorování je možné exportovat do HTML, XML, CSV
  - Více než 30 šablon zahrnuje
    - Podrobné grafy a tabulky dat pro jeden nebo více senzorů
    - Doba bezporuchovosti / výpadcích (% a sekundy)
    - Top 100 Využití šířky pásma
    - Top 100 CPU využití

- Top 100 Ping Times
- Top 100 místo na disku
- Top 100 Doba bezporuchovosti / výpadek

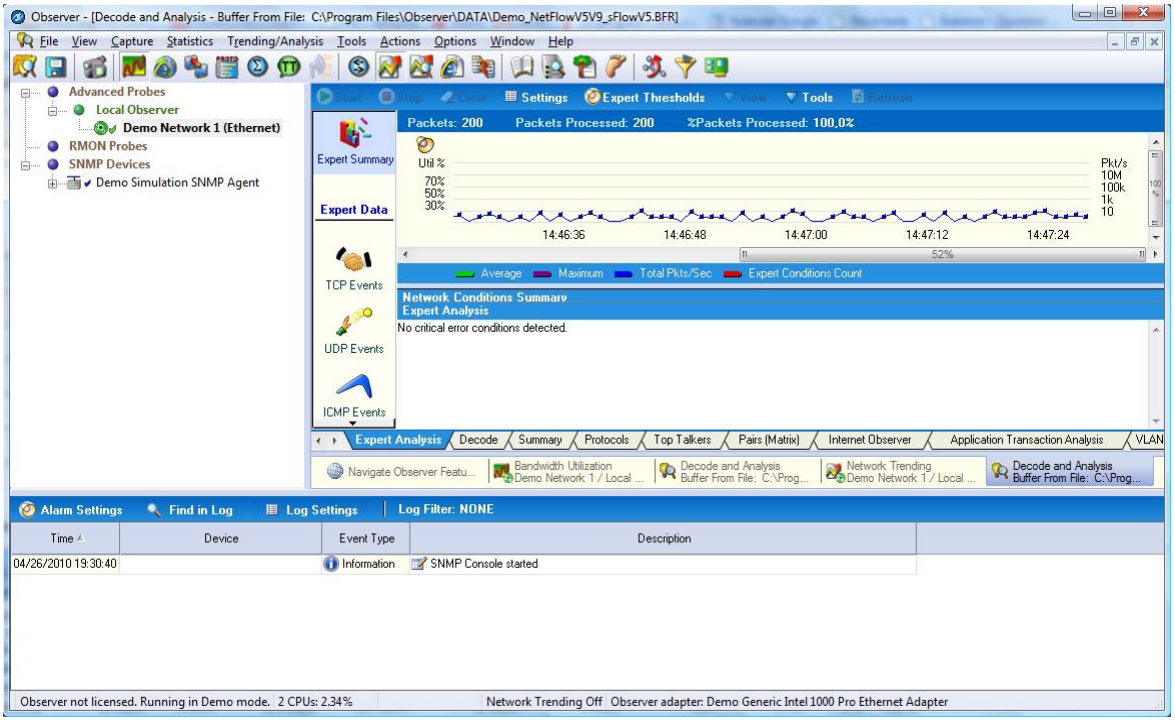
- **Vysoký výkon Design a vysoký bezpečnostní standard**
  - PRTG podporuje monitoring od 1 do 30.000 rozhraní na jedno zařízení (max. počet čidel za optimálních podmínek)
  - Paessler je proprietární databázový systém, je vysoce optimalizován pro monitorování dat (data jsou přístupná přes API)
  - Mnohem rychlejší než SQL servery s menším využitím CPU
  - Dostatečně silný k ukládání roky data pro tisíce rozhraní
  - Nízké systémové požadavky: I Netbook může monitorovat 1.500 rozhraní
  - SSL zabezpečené web server (HTTPS) pro Web, Windows a iPhone GUI

6.3.3 Observer Expert

Program je ke stažení na http://netinst.com/downloads/observer_form.html, kde je formulář a po jeho vyplnění začne stahování programu. S instalací se samozřejmě nainstaluje všechno potřebné k vytváření statistik o provozu v síti. Po instalaci je pouze nutné nastavit, na kterém rozhraní se má daný provoz odposlouchávat.

Program je velice přehledný a srozumitelný. Umožňuje velké množství nastavení, co sledovat a také je zde možnost nastavení jak má program vypadat. Podporuje velké množství statistik a typů grafů, takže jsou statistiky velice přehledné takřka pro každého.

Cena programu se pohybuje od 1 000 do zhruba 4 000 britských liber. Jako v předešlých případech záleží na množství sledovaných stanic, tak na způsobu podpory.



Obr. 39 *Statistika provozu zobrazená v programu Observer*

Přednosti Observeru

Z webových stránek produktu (http://www.netinst.com/) bylo vybráno několik hlavních předností tohoto programu:

- **Více než 600 odborných akcí**

  The Observer Expert je síťový analyzátor, který obsahuje velké množství odborných akcí, které vás upozorní na možné problémy a pomohou vám je rychle řešit. Observer Expert události pracují v reálném čase a umožňují vám mnohé funkce a flexibilitu pro řešení problémů, které nastanou. Jakmile vás Observer Expert upozorní na problém, nabízí pravděpodobnou příčinu a možnost jak ji opravit.

- **Analýza komunikace**

  Observer Expert vás upozorní na mnohé věci, jako jsou nadměrné přenosy a poskytuje vysvětlení problému a možnost jak problém odstranit. Observer je připojený dynamicky a vykresluje jednotlivé síťové konverzace graficky, takže

můžete vidět, kde přesně je problém. Přenosy ze záznamu a zahozené pakety jsou označeny červenou barvou, takže můžete, na první pohled vidět, kde problémy jsou. Stejně tak velké mezery mezi konverzacemi jsou jednoduchý způsob, jak najít místo latence nebo problém s dobou odezvy.

- **Sjednocená komunikace**

Sjednocená komunikace přinesla zcela nové břemeno do počítačových sítí. Observer je síťový analyzátor, který pomáhá zajistit kvalitní přenos hlasu, videa a dat. Ať už je to hovor v určité síti nebo máte svoji další mezinárodní videokonferenci nebo poskytujete VoIP zákazníkům, Observer se snaží, aby měli uživatelé co nejlepší zážitek ze své komunkace, Observer Expert je cenným nástrojem pro plánování, implementace dalších prvků a údržby. Observer Expert vám umožní sledovat Quality of Service (QoS) jednotlivé úrovně a kvality, ukládat a přehrávat hlasové a video zprávy, zobrazit žalovatelné volání a jeho detaily, získat na vysoké úrovni provozní souhrny a další.

- **Aplikační výkon**

Observer Expert se může pochlubit hloubkovou analýzou sítě a detailně jedinečnými prostředky pro analýzu sítě. Řešení pomocí Observer vám pomůže zajistit uplatnění provozuschopnosti a produktivity podniku v jedné síti s dostačujícím výkonem v jednom aplikačním balíčku.

6.4 Rekapitulace technologie Netflow

Hledání optimálního programu pro sledování sítě s tzv. tradiční architekturou není příliš jednoduché. Existuje nespočet programů, které běží na různých platformách. Nejvíce je asi programů pro platformu Linux a tyto programy bývají převážně zdarma, ale nemají tak velké možnosti nastavení jako placené verze. Pro platformu Windows moc freeware programů pro sledování NetFlow statistik bohužel není. V praktické části byly odzkoušeny celkem tři programy, všechny pro platformu Windows. Všechny tři mají velké množství nastavení, jejich ceny jsou také velmi rozdílné. Jak tedy vybrat ten ideální? Naštěstí jsou

tyto verze dostupné v 30-ti denní trial verzi, která dává možnost správci sítě několik takových programů vyzkoušet a poté se rozhodnout jaký program se mu nejlépe ovládá a dává pro něj ty nejlepší nebo alespoň přinejmenším uspokojivé statistiky za rozumnou cenu. Kdyby se měl z již zmiňovaných a testovaných programů vybrat ten ideální, každý správce by si jistě vybral jiný, ale z těchto tří dával velmi přehledné statistiky program Observer, který je jednoduše nastavitelný a také má velkou škálu dobrých funkcí.

7 DALŠÍ MOŽNOSTI SLEDOVÁNÍ SÍTĚ

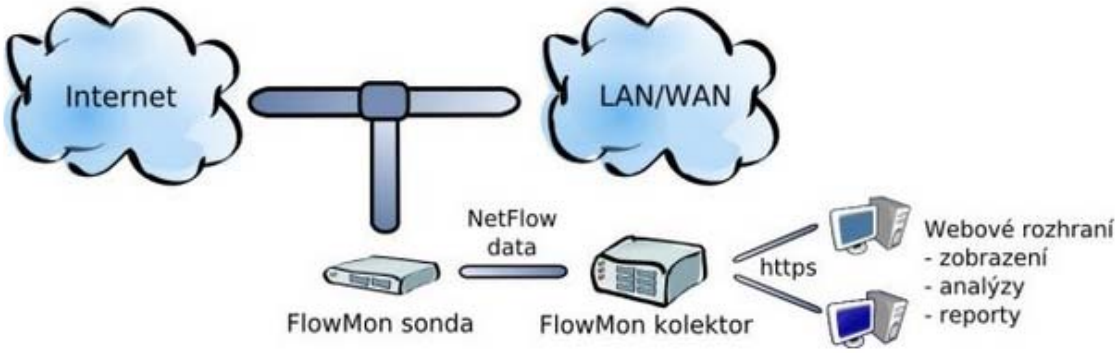
V praktické části je zatím popsán pouze jeden způsob sledování sítě. Existuje ještě jeden způsob, který je o něco praktičtější a dalo by se říci, že i jednoduší. Kdy router neexportuje statistiky provozu do daného zařízení. Tento druhý způsob je založen na používání dalšího zařízení místo routeru, které automaticky vyhodnocuje provoz na síti. Tyto zařízení jsou tzv. NetFlow sondy. Tyto sondy se dají připojit do jakéhokoli místa v síti, podle toho, kde je zapotřebí sledovaní provozu. Jedná se o tzv. moderní architekturu technologie NetFlow, která je popsána v teoretické části. Jednou z předních společností zabývající se právě tímto způsobem monitoringu sítě je česká společnost Invea-Tech, která sídlí v Brně a jejím produktem je FlowMon sonda.

7.1 FlowMon sonda

FlowMon sonda je výkonná autonomní NetFlow sonda, která monitoruje provoz na počítačové síti a vytváří statistiky o tomto provozu ve formátech NetFlow v5/v9 či IPFIX. Tyto měřené statistiky poskytují uživateli informace o tom, kdo komunikoval s kým, kdy, jak dlouho, jak často, kolik bylo přeneseno dat a mnohé další. Takové informace jsou nezbytné pro zajištění síťové bezpečnosti, řešení incidentů na síti, účtování služeb založené na množství přenesených dat, plánování kapacit linek či monitorování uživatelů a služeb.

Hlavní předností FlowMon sondy je její schopnost zaznamenat v reálném čase každý paket a to i na linkách s propustností až 10 Gb/s. Sondy jsou navíc zařízení, která jsou neviditelná na L2 i L3 vrstvě a na rozdíl od směrovačů s podporou NetFlow tak nejsou pravděpodobným cílem útoků a lze je umístit do libovolného bodu v síti. FlowMon sonda se typicky umisťuje na vstupní a výstupní body sítě, kritická místa či linky s největším přenosem dat.

Konfigurace FlowMon sondy probíhá vzdáleně pomocí intuitivního webového rozhraní FlowMon konfiguračního centra. Nastavení sondy je velmi jednoduché a umožňuje zákazníkovi mít plně funkční NetFlow monitorovací řešení během několika minut po instalaci do sítě. Jakmile je sonda zapojena a nakonfigurována, pracuje plně automaticky bez nutnosti vnějších zásahů.



Obr. 40 *Způsob připojení FlowMon sondy*

7.1.1 Modely FlowMon sond

Standardní model je realizován jako kompaktní 1U zařízení a jedná se o vhodné řešení pro menší a střední sítě. Je vybaven 1 až 4 monitorovacími porty pro 10/100/1000 Ethernet nebo 1 monitorovacím rozhraním pro desetigigabitový Ethernet. Jedná se o modely FlowMon Probe 1000/2000/4000/10000.

Obr. 41 *Standardizovaný model FlowMon sondy*

Hardwarově akcelerovaný model využívá technologie programovatelného hardware (FPGA). Poskytuje maximální výkon a stabilitu zajišťující bezeztrátové zpracování až 6 milionů paketů za sekundu. Je vhodný pro nasazení ve velkých sítích a na páteřních linkách. Tento model je vybaven 2 monitorovacími rozhraními pro 10/100/1000 Ethernet nebo 1 monitorovacím rozhraním pro desetigigabitový Ethernet. Jedná se o

modely FlowMon Probe 2000 Pro a 10000 Pro. Hardwarově akcelerovaný model je dále vybaven Ethernet rozbočovačem (TAPem) pro snadné vložení do linky. [22]

Obr. 42 *Hardwarově akcelerovaný model*

7.2 Prodávané modely a jejich cenová relace

Standardní modely:

P/N	Název produktu	Výkon na port	Monitorovací rozhraní	Konektor	Kabeláž	Formát	Rozměry (VxŠxH) cm	Rozměry (VxŠxH) in	HDD
IFP-100-CU	Invea FlowMon Probe 100 Office	150 kp/s	1x 10/100 Ethernet	Měď RJ-45	CAT5	Mini-ITX	26,4x11,2x23	10,4x4,4x9	80GB
IFP-1000P-CU	Invea FlowMon Probe 1000 Portable	0,3 Mp/s	1x 10/100/1000 Ethernet	Měď RJ-45	CAT5	MiniPC	5x16,5x16,5	1,9x6,5x6,5	160GB
IFP-1000-CU	Invea FlowMon Probe 1000	0,5 Mp/s	1x 10/100/1000 Ethernet	Měď RJ-45	CAT5	1U	4,3x45,1x50,8	1,7x17,8x20	500GB
IFP-2000-CU	Invea FlowMon Probe 2000	0,5 Mp/s	2x 10/100/1000 Ethernet	Měď RJ-45	CAT5	1U	4,3x45,1x50,8	1,7x17,8x20	500GB
IFP-2000-MM	Invea FlowMon Probe 2000 Fiber	0,5 Mp/s	2x 1000 Ethernet	Optika LC	MMF 62.5/50 µm	1U	4,3x45,1x50,8	1,7x17,8x20	500GB
IFP-4000-CU	Invea FlowMon Probe 4000	0,5 Mp/s	4x 10/100/1000 Ethernet	Měď RJ-45	CAT5	1U	4,3x45,1x50,8	1,7x17,8x20	500GB
IFP-4000-MM	Invea FlowMon Probe 4000 Fiber	0,5 Mp/s	4x 1000 Ethernet	Optika LC	MMF 62.5/50 µm	1U	4,3x45,1x50,8	1,7x17,8x20	500GB
IFP-4000-SFP	Invea FlowMon Probe 4000 SFP	0,5 Mp/s	4x 10/100/1000 Ethernet	SFP klec	Podle transceiveru	1U	4,3x45,1x50,8	1,7x17,8x20	500GB
IFP-6000-SFP	Invea FlowMon Probe 6000 SFP	0,5 Mp/s	6x 10/100/1000 Ethernet	SFP klec	Podle transceiveru	1U	4,3x45,1x50,8	1,7x17,8x20	500GB
IFP-10000-CU	Invea FlowMon Probe 10000	1,1 Mp/s	1x 10G Ethernet	Měď CX4	CX4	1U	4,3x45,1x50,8	1,7x17,8x20	500GB
IFP-10000-SFP+	Invea FlowMon Probe 10000 SFP+	1,1 Mp/s	1x 10G Ethernet	SFP+ klec	Podle transceiveru	1U	4,3x45,1x50,8	1,7x17,8x20	500GB
IFP-20000-SFP+	Invea FlowMon Probe 20000 SFP+	1,1 Mp/s	2x 10G Ethernet	SFP+ klec	Podle transceiveru	1U	4,3x45,1x50,8	1,7x17,8x20	500GB

Hardwarově akcelerované modely:

P/N	Název produktu	Výkon na zařízení	Monitorovací rozhraní	Konektor	Kabeláž	Formát	Rozměry (VxŠxH) cm	Rozměry (VxŠxH) in	HDD
FP-4000PRO-SFP	FlowMon Probe 4000 Pro	6 Mp/s	4x 10/100/1000 Ethernet	SFP klec	Podle transceiveru	2U	8,9x43,7x45,0	3,5x17,2x17,7	500GB
FP-10000PRO-XFP	FlowMon Probe 10000 Pro	15 Mp/s	1x 10G Ethernet	XFP klec	Podle transceiveru	2U	8,9x43,7x45,0	3,5x17,2x17,7	500GB
FP-20000PRO-XFP	FlowMon Probe 20000 Pro	15 Mp/s	2x 10G Ethernet	XFP klec	Podle transceiveru	2U	8,9x43,7x45,0	3,5x17,2x17,7	500GB

Obr. 43 *Tabulky nabízených modelů sond FlowMon*

Cena tohoto řešení se pohybuje od 33 000 Kč až do několika set tisíc. Přičemž záleží na konkrétním modelu a jeho výkonnosti.

ZÁVĚR

V teoretické části byly popsány základní pojmy z oblasti počítačových sítí, jenž je potřeba znát při budování počítačové sítě. Následně byly v teoretické části popsány technologie EtherChannel a NetFlow, jejich historický vývoj a také jejich možnosti nastavení na zařízeních Cisco.

V praktické části byly nejprve prostudovány možnosti nastavení technologie EtherChannel a byla vybrána jedna možnost nastavení, pro oba protokoly PAgP a LACP. Následně byla na přepínačích Cisco nastavena technologie EtherChannel a byla otestována.

Druhým bodem teoretické části byla technologie NetFlow. Prvním krokem pro úspěšné sledování sítě bylo vytvoření „zkušební“ sítě, ve které se bude sledovat provoz. Následně byla provedena nastavení a celá síť byla otestována. Otestování správnosti nastavení směrovačů bylo provedeno pomocí příkazu ping z příkazového řádku. Z testu sítě vyplynulo, že vše bylo správně nastaveno. Druhým krokem bylo nastavení odesílání NetFlow dat z druhého směrovače na kolektor a vyzkoušení několika programů pro vyhodnocování sledování provozu po síti. Celkem byly vyzkoušeny 3 programy: ManageEngine NetFlow Analyzer 7.5, PRTG Network Monitor a Observer. Tyto programy jsou placené a tak byly vyzkoušeny jako 30-ti denní trial verze. Všechny programy mají své výhody a nevýhody, zde záleží přímo na správci sítě, který program mu vyhovuje.

Posledním bodem diplomové práce bylo vyhledat další možnost sledování vytíženosti sítě. Pro tuto možnost bylo vybráno měření provozu v síti pomocí NetFlow sond. Byla zmíněna jedna z předních společností v česku zabývající se touto metodou měření sítě, Invea-Tech, která vyrábí FlowMon sondy.

ZÁVĚR V ANGLIČTINĚ

Basic concepts of computer networks, needed to be known to build a computer network were described in the theoretical part. Subsequently EtherChannel and NetFlow technology, their historical development and possible configuration using Cisco equipment were described in the theoretical part as well.

Possibilities of EtherChannel technology settings were studied at first place and then one possibility of settings for both PAgP and LACP protocols was chosen. Setting the EtherChannel technology to Cisco switches and testing was accomplished as a next step.

The second goal of the theoretical part was NetFlow technology. The first step to a successful network monitoring was creation of a "test" network, where traffic will be monitored. Setting and testing of the whole network was performed then. Testing of correct setting of routers was done using a ping command from command line. The test result showed that everything was set correctly. The second step was to set up NetFlow data sending from the second router on a collector and to test several programs for evaluation network traffic monitoring. Three programs were tested overall: ManageEngine NetFlow Analyzer 7.5, PRTG Network Monitor a Observer. These programs are paid and that is why they have been tested as a 30-day trial version. All mentioned programs have their advantages and disadvantages; it depends directly on the network administrator, which program suits him.

The last goal of this thesis was to find some additional possibility to track network utilization. Measuring of traffic on the network using NetFlow probes was chosen for this task. Invea-Tech, one of the leading companies in Czech engaged in this method of measuring network was mentioned as well as their product FlowMon probe.

SEZNAM POUŽITÉ LITERATURY

[1] Počítačová síť In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 10.3.2005, 23.2.2010 [cit. 2010-03-05]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_s%C3%AD%C5%A5>.

[2] BIGELOW, Stephen J. Mistrovství v počítačových sítích : správa, konfigurace, diagnostika a řešení problémů. 1. vyd. Brno : Computer Press, 2004. 990 s. ISBN 8025101789.

[3] Rack In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 12.1.2005, 17.7.2009 [cit. 2010-03-05]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Rack>.

[4] Hub In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 20.9.2006, 27.1.2010 [cit. 2010-03-05]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Hub>.

[5] HORÁK, Jaroslav, KERŠLÁGER, Milan. Počítačové sítě pro začínající správce. 4. rozš. vyd. Brno : Computer Press, 2008. 327 s. ISBN 978-80-251-2073-6.

[6] PETERKA, Jiří. *EArchiv.cz* [online]. 1996 [cit. 2010-03-05]. Koaxiální kabel. Dostupné z WWW: <http://www.earchiv.cz/a96/a643k150.php3>.

[7] PETERKA, Jiří. *EArchiv.cz* [online]. 1996 [cit. 2010-03-05]. Kroucená dvoulinka. Dostupné z WWW: <http://www.earchiv.cz/a96/a644k150.php3#ixzz0h7MBC3AU>.

[8] Kroucená dvojlinka In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 2006, 17.12.2009 [cit. 2010-03-05]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Kroucen%C3%A1_dvojlinka>.

[9] MALLAT, Jaroslav. *Zábava a informace pro IT člověčky* [online]. 03. 09. 2009 [cit. 2010-03-05]. HPS v IT. Dostupné z WWW: <http://hps.mallat.cz/view.php?cisloclanku=2003090203>.

[10] Wi-Fi In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 1.5.2007, 11.12.2009 [cit. 2010-03-05]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Wi-Fi>.

[11] PETERKA, Jiří. *EArchiv.cz* [online]. 1999 [cit. 2010-03-06]. Referenční model ISO/OSI. Dostupné z WWW: <http://www.earchiv.cz/anovinky/ai1552.php3>.

[12] TCP/IP In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 10.12.2007, 4.3.2010 [cit. 2010-03-06]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/TCP/IP>.

[13] BOUŠKA, Petr. *Www.samuraj-cz.com* [online]. 8.3.2007 [cit. 2010-03-06]. Cisco IOS 1 - úvod, příkaz show. Dostupné z WWW: <http://www.samuraj-cz.com/clanek/cisco-ios-1-uvod-prikaz-show/>.

[14] EtherChannel In *Wikipedia : the free encyclopedia* [online]. St. Petersburg : Wikipedia Foundation, 2009, 25.2.2010 [cit. 2010-03-09]. Dostupné z WWW: <http://en.wikipedia.org/wiki/EtherChannel>.

[15] Link aggregation In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 28.5.2005, 19.5.2006 [cit. 2010-03-09]. Dostupné z WWW: <http://en.wikipedia.org/wiki/Link_aggregation>.

[16] BOUŠKA, Petr. *Www.samuraj-cz.com* [online]. 8.6.2009, 1.7.2009 [cit. 2010-03-09]. Cisco IOS 21 - EtherChannel, Link Agregation, PAgP, LACP, NIC Teaming. Dostupné z WWW: <http://www.samuraj-cz.com/clanek/cisco-ios-21-etherchannel-link-agregation-pagp-lacp-nic-teaming/>.

[17] Vyvažování zátěže In *Wikipedia : the free encyclopedia*[online]. St. Petersburg (Florida) : Wikipedia Foundation, 6.1.2008, 10.1.2010 [cit. 2010-03-09]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Vyva%C5%BEov%C3%A1n%C3%AD_z%C3%A1t%C4%9B%C5%BEe>.

[18] *Catalyst 2960 Switch : Software Configuration Guide* [online]. San Jose, USA : Cisco Systems, Inc., 2006 [cit. 2010-03-24]. Dostupné z WWW: <http://www.cisco.com>.

[19] Netflow In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 14.3.2008, 26.3.2009 [cit. 2010-03-24]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Netflow>.

[20] *Zeal.cz* [online]. 2006 [cit. 2010-03-24]. Cisco NetFlow Export. Dostupné z WWW: <http://www.zeal.cz/view.php?nazevclanku=management-siti&cisloclanku=2007010018>.

[21] *Invea.cz* [online]. 2007 [cit. 2010-03-24]. Co je to NetFlow?. Dostupné z WWW: <http://www.invea.cz/cs/main/netflow>.

[22] *Invea.cz* [online]. 2007 [cit. 2010-04-26]. FlowMon. Dostupné z WWW: <http://www.invea.cz>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

100BaseT	Označení typu sítě, která využívá kroucenou dvojlinku a má max. rychlost 100Mbps.
10BaseT	Označení typu sítě, která využívá kroucenou dvojlinku a má max. rychlost 100Mbps.
AP	Access point.
ARP	Address Resolution Protocol
AS	Autonomní systém.
atd.	A tak dále.
ATM	Asynchronous Transfer Mode.
bin	Koncovka souboru.
BNC	Bayonet Nut Coupler
CAN	Cosmopolitan Area Network
CBQoS	Cisco Class-Based Quality of Service
CLI	Command Line Interface
cm	Centimetr
COM	Označení výstupu sériového portu.
CPU	Central Processing Unit
CSMA-CD	Carrier Sense Multiple Access with Collision Detection
DIN 41494	Deutsche Industrie Norm
EIA 310-D	Environmental Impact Assessment
EMS	Electronic Mail System
FDDI	Fiber Distributed Data Interface
FPGA	Field Programmable Gate Array
FTP	Foil-shielded Twisted Pair
GAN	Global Area Network

Gb/s	Gigabit za sekundu
GUI	Graphic User Interface
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol - Secure
IBM	International Business Machines
ID	IDentification
IEC 60297	International Electrotechnical Commision
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
I / O	Input / Output
IOS	Internetwork Operating System
IOSI	Reference Model for Open Systems Interconnection
IP	Internet Protocol
IPFIX	Internet Protocol Flow Information eXport
IPv4	Internet Protocol verze 4
IPv6	Internet Protocol verze 6
ISDN	Integrated Services Digital Network
ISL	Inter-Switch Link
ISO/OSI	lnternational Organization for Standardization/Open Systems Interconnection
ISP	Internet Service Provider
km	kilometr
L2	Layer 2
L3	Layer 3
LACP	Link Aggregation Control Protocol

LAN	Local Area Network
LED	Light Emitting Diode
log	Logarimus
LPT	Line PrinTer
MAC	Media Access Control
MAN	Metropolitan Area Network
MB	MegaByte
Mbit/s	Megabit za sekundu
Mbps	Mega bit per sekund
Mhz	Mega Hertz
mm	Milimetr
MPLS	MultiProtocol Label Switching
NIC	Network Interface Card
NVRAM	Non-volatile random access memory
OSI	Open Systems Interconnection
PAgP	Port aggregation protocol
PAN	Personal Area Network
POST	Power On Self Test
RAM	Random Access Memory
RAW	Read After Write
RJ-11	Typ koncovky u kroucené dvojlinky (pro telefonní rozvody)
RJ-45	Typ koncovky u kroucené dvojlinky (pro datové rozvody)
ROM	Read Only Memory
QoS	Quality of services
SC	Typ koncovky pro optické kabely

SCTP	Stream Control Transmission Protocol
SMB	Server Message Block
SMS	Short message service
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SPAN	Switched Port Analyzer
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
ST	Koncovka pro optické kabely
STP	Shielded Twisted Pair
TAB	Tabulátor
TAP	Telocator Alphanumeric Protocol
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
UTP	Unshielded Twisted Pair
VLAN	Virtual Local Area Network
VoIP	Voice Over IP
WAN	Wide Area Network
WMI	Windows Management Instrumentation
WWW	World Wide Web

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH