Univerzita Hradec Králové
Filozofická fakulta
Katedra pomocných věd historických a archivnictví

PŘIPOJENÍ VZDÁLENÝCH POBOČEK PŘES ŠIROKOPÁSMOVÝ INTERNET A TECHNOLOGII ŠIFROVANÝCH TUNELŮ ASTARO/SOPHOS

Diplomová práce

Autor: Bc. René Šmída
Studijní program: N7105 Historické vědy
Studijní obor: Archivnictví
Vedoucí práce: Ing. Monika Borkovcová

Hradec Králové, 2014

Univerzita Hradec Králové

Filozofická fakulta

Zadání diplomové práce

Autor:	**Bc. René Šmída**
Studijní program:	N7105 Historické vědy
Studijní obor:	Archivnictví
Název závěrečné práce:	**Připojení vzdálených poboček přes širokopásmový internet a technologii šifrovaných tunelů Astaro/Shopos**
Název závěrečné práce AJ:	Connecting Remote Branches Through Broadband Internet and Astaro/Shopos Secure Tunnels

Cíl, metody, literatura, předpoklady:

Stručný obsah: Teorie, popis připojení negarantovaného internetu prostřednictvím technologie ASTARO, vyhodnocení testů - datových přenosů a výpadků, porovnání cenové nabídky LLnet od O2 a xDSL, závěry. Metody zpracování: Porovnání a testování připojení typu negarantovaný Internet s využitím šifrovaných tunelů typu IPsec (AES256) prostřednictvím technologie Astaro. Literatura nebo archivní fondy: Zabezpečení sítí Cisco – Autorizovaný výukový průvodce od Michael Wenstrom, Širokopásmový internet – Přístupové a domácí sítě od Rita Pužmanová, Velký průvodce protokoly TCP/IP a systémem DNS od Libor Dostálek, Alena Kabelová

Garantující pracoviště:	Katedra pomocných věd historických a archivnictví
Vedoucí práce:	**Ing. Monika Borkovcová**
Konzultant:	
Oponent:	Mgr. Radek Pokorný
Datum zadání práce:	1. 2. 2013
Datum odevzdání práce:	

Prohlášení:

Prohlašuji, že jsem tuto diplomovou práci pod vedením vedoucí práce vypracoval samostatně a uvedl jsem všechny použité prameny a literaturu.

V Hradci Králové dne 17. prosince 2014

……..…….....

(podpis)

Poděkování

Rád bych tímto poděkoval vedoucí diplomové práce Ing. Monice Borkovcové za čas, který mi věnovala, inspiraci a za odborné vedení při vytváření této závěrečné diplomové práce.

Dále bych rád poděkoval své rodině za zázemí a podporu při studiu.

Děkuji i všem pedagogům Univerzity Hradec Králové, kteří mne motivovali a umožnili mi rozšířit přehled natolik potřebný s oborem moderních systémů v archivnictví.

Zvláštní poděkování patří firmě Annex NET, s.r.o., která poskytla nejen zapůjčení zařízení, ale i za její odbornou pomoc zejména v praktické části a má velký podíl na vzniku této práce.

Anotace

Šmída, René. *Připojení vzdálených poboček přes širokopásmový internet a technologii šifrovaných tunelů Astaro/Shopos*:diplomová práce. Hradec Králové: Univerzita Hradec Králové, Filozofická fakulta, Katedra pomocných věd historických a archivnictví. 2014, 82s.

Diplomová práce pojednává o problematice propojení vzdálené stanice do vnitropodnikové sítě se zachováním stávajících služeb.
Práce zahrnuje odborný popis informačních technologií a zároveň představuje výsledné řešení specifického úkolu, jež se opírá o výsledky praktického zkoumání a testování.
Na základě provedených testů se podařilo navrhnout funkční a bezpečné připojení, které představuje vhodné řešení pro malé a střední organizace.

Klíčová slova

širokopásmový; šifrované tunely; vzdálená pobočka; síť; internet; zabezpečení

Annotation

Šmída, René. *Connecting Remote Branches Through Broadband Internet and Astaro/Shopos Secure Tunnels*: master´s thesis. Hradec Králové: University of Hradec Králové, FacultyofArts, Department ofAuxiliaryHistoricalSciences and Archival Science. 2014, 82s

The thesis deals with different aspects of the connection of a remote station to aninternal network of a company while maintaining existing services.
The paper includes professional description of information technologies and also presents a solution to a specific task, which is based on results of practical research and testing.
Based on the tests which were carried out, it was possible to design functional and secure connection, which should serve as a suitable solution for small and medium-sized organizations.

Keywords

broadband; secure tunnels; remote branch; network; internet; security

Obsah

1 Úvod

Propojování uživatelů vnitropodnikovými počítačovými sítěmi je v dnešní době stále větší samozřejmostí. Rozvoj informačních technologií a nárůst připojených uživatelů klade stále větší nároky na zabezpečení informací při přenosech dat během datových připojení. Zajištění bezpečnosti podnikových počítačových sítí bývá v dnešní době na vysoké úrovni, přesto bezpečné používání informačních technologií mimo pracoviště má svoje zákonitosti.

Již v průběhu roku 2012 byl zadán firemní požadavek k nalezení efektivního řešení a vytvoření levnějšího způsobu připojení vzdálené pobočky k resortní telekomunikační síti při zachování stávající úrovně služeb tak, aby bylo možno zachovat stávající technologii, která v sobě již zahrnuje konvergenci hlasové a datové sítě.

Cílem výše uvedeného požadavku je najít vhodné a optimální řešení, splňující veškeré podmínky koncového uživatele. Práce je zaměřena na odborný popis jednotlivých pojmů z pohledu informačních technologií a zároveň představuje výsledné řešení specifického úkolu, jež se opírá o praktickou část. Předmětem ověřování bylo připojení typu negarantovaný internet s využitím šifrovaných tunelů typu IPsec (AES256) prostřednictvím technologie Astaro. Ověřování probíhalo nejprve v podmínkách testovacího zapojení mimo reálný provoz, následně byl proveden a ověřen přenos v reálném datovém a hlasovém provozu.

Tato práce představuje vhodné řešení pro malé a střední organizace, jejichž důležitou potřebou je spojení vzdálené pobočky s centrálou, zabezpečení rychlého přístupu k internetu a zároveň představuje cenově přijatelný a dostupný způsob zabezpečení všech stanic.

2 Vysvětlení pojmů

Pro správné pochopení funkčnosti připojení vzdálené pobočky je třeba nejprve objasnit některé aspekty komunikace mezi počítači. Celá problematika je velmi složitá a technicky obsáhlá, a proto je teoretická část zaměřena zejména na vysvětlení a objasnění pojmů a důležitých souvislostí, které se týkají technického řešení a jsou neoddělitelnou součástí praktické části této práce.

2.1 Počítačové sítě

Počítačová síť je soustava vzájemně propojených počítačů tak, aby byla zajištěna vzájemná komunikace libovolných uživatelů mezi sebou. Samostatným výrazem *síť* by se dalo vyjádřit cokoli od lokální sítě **LAN** až po rozlehlou síť **WAN** a proto v zásadě rozlišujeme dva typy počítačových sítí.[1]
Výraz *internetová síť* vyjadřuje soubor jednotlivých sítí, které jsou propojené mezilehlými zařízeními a společně fungují jako jediná obrovská síť.[2]
Komunikace mezi počítači je souborem pravidel síťového provozu a takovémuto souboru komunikačních pravidel se říká *protokol*. Není možné, aby dva počítače ke vzájemné komunikaci mezi sebou používaly rozdílný protokol.[3]

LAN (Local Area Network) můžeme charakterizovat těmito vlastnostmi:

- propojuje jednotlivá zařízení na krátké vzdálenosti
- je rychlá
- bývá v soukromé správě
- je k dispozici nepřetržitě.

[1] DOSTÁLEK, Libor, KABELOVÁ, Alena. *Velký průvodce protokoly TCP/IP a systémem DNS*. 2. aktualizované vyd. Praha: Computer Press, 2000, 423 s. ISBN 80-7226-323-4.
[2] SPORTAK, Mark A. *Směrování v sítích IP*. 1.vyd. Brno: Computer Press, 2004, 368 s. ISBN 80-251-0127-4.
[3] TEARE, Diane. Návrh a realizace sítí Cisco. 1.vyd. Brno: Computer Press, 2003, 784 s. ISBN 80-251-0022-7.

Pro potřeby propojování počítačů v lokální síti existuje celá řada technologií, z nichž nejznámější je **Ethernet/IEEE 802.3**, který pracuje s rychlostí od 10 Mb/s až po Gb/s. Protokoly sítí LAN zajišťují funkce dvou nejnižších vrstev modelu OSI a to fyzické vrstvy a vrstvy datových spojů.[4]

V síti **Ethernet** jsou data přenášena po společném přenosovém kanálu. Po připojení na tento kanál používá tzv. přístupu s kolizí CSMA/CD (Carrier Sense Multiple Acces with Collision Detection). Každá stanice, která vysílá data, se snaží připojit na společný přenosový kanál. Pokud se pokoušejí připojit současně dvě stanice, dochází ke kolizi. Systém CSMA/CD tyto kolize odhalí a příslušné stanice ukončí přenos. Stanice, které chtějí vysílat, počkají náhodně dlouhou dobu a potom zkusí vysílat znovu.[5]

Síťové technologie se používají na obou koncích celého spektra sítí:

- přístupové sítě LAN, které tvoří rozbočovače (hub) nebo přístupové přepínače, umožňují svým uživatelům a zařízením připojit se na úrovni místní sítě
- páteřní sítě LAN, které tvoří směrovače nebo přepínače LAN, umožňují propojení zařízení v síti LAN s jinou sítí LAN.

K propojení sítě LAN s rozsáhlou sítí WAN se využívají směrovače.[6]

WAN (Wide Area Network) je rozlehlá síť, která umožňuje komunikaci mezi koncovými uzly, stanicemi a to zpravidla na velké vzdálenosti. Rozlehlé sítě mohou tvořit přenosovou páteř podnikové sítě všude tam, kde je zapotřebí připojit vzdálené pobočky či kanceláře, ale i lidé pracující na dálku s potřebou propojit se do podnikové sítě. Pro koncového uživatele má největší význam rozhraní přístupu k síti, jeho vlastnost, funkce a možnosti.[7]

---

[4] TEARE, Diane. *Návrh a realizace sítí Cisco*. 1.vyd. Brno: Computer Press, 2003, 784 s. ISBN 80-251-0022-7.

[5] PUŽMANOVÁ, Rita. *Širokopásmový Internet Přístupové a domácí sítě*. 1.vyd. Brno: Computer Press, 2004, 377 s. ISBN 80-251-0139-8.

[6] VELTE, Toby J, VELTE, Anthony T. *Síťové technologie Cisco*. 1.vyd. Brno: Computer Press, 2003, 800 s. ISBN 80-7226-857-0.

[7] PUŽMANOVÁ, Rita. *Moderní komunikační sítě od A do Z*. 1.vyd. Praha: Computer Press, 1998, 432 s. ISBN 80-7226-098-7.

Má-li rozlehlá síť WAN poskytovat skutečně spolehlivé služby pro koncového uživatele a přitom si zachovat nákladově efektivní způsob, musíme pro síť WAN zvolit správnou technologii.[8]

Přenosové prostředky určené pro konstrukci rozlehlých sítí WAN a jejich způsob zajišťování spojení se liší a proto je můžeme rozdělit do těchto kategorií:

- **vyhrazené neboli pronajaté linky** – se používají ve dvoubodových sítích. Tato komunikační cesta je propojena od zařízení zákazníka přes síť a zařízení operátora[9]
- **přepínání okruhů** – je komunikační metoda, pří které se mezi koncovými stanicemi vytvoří přepínaná, vyhrazená cesta a toto spojení je fyzickým okruhem a po dobu trvání relace je vyhrazeno. Typickým příkladem této technologie jsou linky ISDN (Integrated Services Digital Network) [10]
- **přepínání paketů** – je metoda, při které se balík dat rozdělí do paketů a každý paket se označí cílovou adresou, díky čemuž je možné posílat pakety po síti odděleně. V takovéto síti se pakety předávají mezi stanicemi v počítačové síti po právě nejlepší dostupné trase, a to mezi zdrojem a místem určení. Klasickým příkladem paketové sítě je X.25 a Frame Relay[11]
- **přepínání buněk** – síť buňkové komunikace má na rozdíl od paketu nebo rámce pevnou délku. Nejznámější technologií s přepínáním buněk je asynchronní síť ATM. Vlastní síť se skládá z komunikačních cest mezi jednotlivými přepínači ATM a definuje jak rozhraní mezi uživatelem a sítí, tak mezi jednotlivými přepínači v síti.[12]

Virtuální okruhy v sítích WAN slouží pro zajištění spolehlivé komunikace mezi dvěma síťovými zařízeními.

[8] TEARE, Diane. *Návrh a realizace sítí Cisco*. 1.vyd. Brno: Computer Press, 2003, 784 s. ISBN 80-251-0022-7.
[9] SPORTAK, Mark A. *Směrování v sítích IP*. 1.vyd. Brno: Computer Press, 2004, 368 s. ISBN 80-251-0127-4.
[10] Totéž
[11] PUŽMANOVÁ, Rita. *Moderní komunikační sítě od A do Z*. 1.vyd. Praha: Computer Press, 1998, 432 s. ISBN 80-7226-098-7.
[12] Totéž

Virtuální okruhy můžeme rozdělit na dva typy:

- **přepínané virtuální okruhy** (switched virtual circuits, SVC) – se zavádějí dynamicky na vyžádání a ukončují se po dokončení přenosu dat. SVC se vytváří pomocí signalizačních protokolů, jejichž pomocí spolu mohou komunikovat uživatel a samotná síť[13]
- **trvalé virtuální okruhy** (pernament virtual circuits, PVC) – jsou pevně sestavené administrátorem sítě.[14]

Rozlehlé sítě WAN jsou velmi složité struktury a provoz takovéto sítě, která má splňovat všechny požadavky uživatele, nebývá snadným úkolem.

2.1.1 Síťová architektura

Síťová architektura nepředstavuje žádnou jednotlivou síť, nýbrž komunikaci mezi systémy, které se skládají s poměrně rozsáhlých množství různých operací. Tyto různé operace byly rozděleny do tzv. **vrstev**, které odpovídají hierarchii činností při vykonávání komunikace mezi koncovými systémy.[15] Hierarchie uspořádaných vrstev je řešena tak, aby na nejnižších vrstvách byly řešeny věci, jakými jsou například přenosy jednotlivých bitů na vyšších vrstvách, pak přenosy celých bloků dat a na nejvyšších vrstvách už budou tyto přenosy využívány například k přenosu celých souborů.[16]

Spolupráce mezi vrstvami a služeb probíhá na základě zásad, kde každá vrstva komunikuje v rámci daného uzlu vždy jen se svými bezprostředně sousedními vrstvami a to bezprostředně nižší nebo bezprostředně vyšší. Jednotlivé vrstvy se mezi sebou nepřeskakují, jelikož funkce vrstvy využívá služeb nejbližší nižší, jak znázorňuje obrázek č. 1.

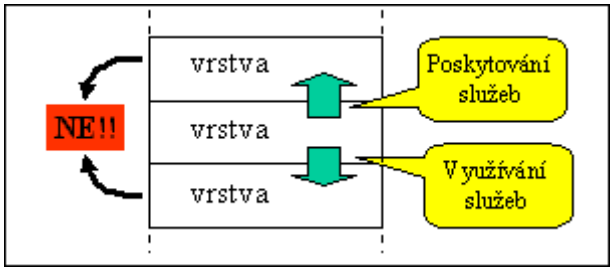
---

[13] TEARE, Diane. *Návrh a realizace sítí Cisco*. 1.vyd. Brno: Computer Press, 2003, 784 s. ISBN 80-251-0022-7.

[14] Totéž

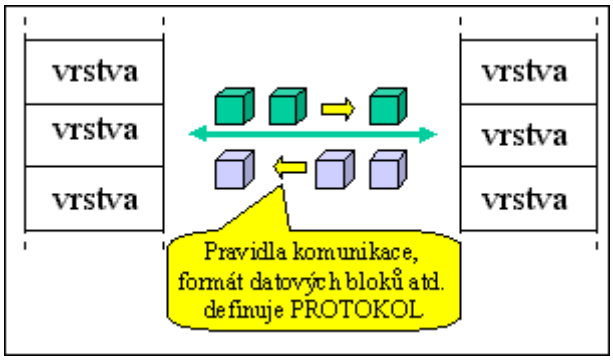
[15] PUŽMANOVÁ, Rita. *Moderní komunikační sítě od A do Z*. 1.vyd. Praha: Computer Press, 1998, 432 s. ISBN 80-7226-098-7.

[16] PETERKA, Jiří. *Síťová architektura*[online]. eArhiv.cz [citováno 03. 10. 2013]. Dostupné z: http://www.earchiv.cz/anovinky/ai1483.php3



Obr. 1 – Spolupráce vrstev[17]

U komunikace stejnolehlých vrstev mezi jednotlivými uzly jsou stanovena pravidla tak, že při výměně dat musí rozumět danému formátu a adresám, které jsou v dané vrstvě využity. Tato spolupráce mezi dvěma systémy je řízena **komunikačním protokolem**, který znázorňuje obrázek 2.



Obr. 2 – Komunikace stejnolehlých vrstev mezi uzly[18]

V rámci jedné vrstvy může být využito různých protokolů, které plní či pomáhají realizovat příslušné úkoly.

Síťová architektura je deklarována systémem vrstev, služeb, funkcí a protokolů. Představitel univerzálního modelu s otevřenou síťovou architekturou je **referenční model OSI** (Open Systems Interconnection) a architektura **TCP/IP** (Transmission Control Protocol/Internet Protocol), na kterém je vybudován dnešní internet.[19]

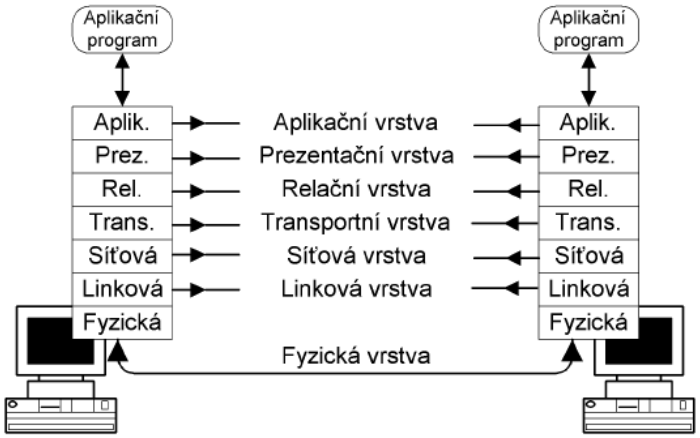
[17] Obrázek převzat ze *Síťová architektura*[online]. eArhiv.cz [citováno 05. 10. 2013]. Dostupné z: http://www.earchiv.cz/anovinky/ai1483.php3

[18] Totéž

[19] PETERKA, Jiří. *Síťová architektura*[online]. eArhiv.cz [citováno 05. 10. 2013]. Dostupné z: http://www.earchiv.cz/anovinky/ai1483.php3

2.1.1.1 Referenční model OSI

RF model OSI je sedmivrstvý model, který přesně definuje jednotlivé funkční vrstvy pro zajištění komunikační relace. Obrázek 3 představuje jednotlivé vrstvy RF modelu OSI. Při koncipování referenčního modelu OSI měli hlavní slovo zástupci spojových organizací. Cílem bylo vzájemné propojení či spolupráce různých a nekompatibilních systému k plnění společných úkolů.



Obr. 3 – RF model OSI[20]

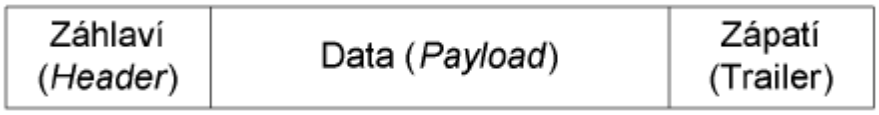
Vrstva 1: fyzická vrstva

Úkolem této vrstvy je zajistit přenos jednotlivých bitů mezi příjemcem a odesílatelem prostřednictvím fyzické přenosové cesty, kterou tato vrstva bezprostředně ovládá. K tomu je třeba vyřešit mnoho otázek převážně technického charakteru, jelikož fyzická vrstva pracuje pouze s nulami a jedničkami a neobsahuje žádný mechanismus ke zjištění významu přijatých či odeslaných bitů. Pouze ji zajímají charakteristiky elektrických či optických technik k přenosu signálu po využívaném přenosové médiu např. (koaxiální kabel, měděný kabel - UTP nebo optický kabel ze skleněných vláken).[21]

[20] DOSTÁLEK, Libor, KABELOVÁ, Alena. *Velký průvodce protokoly TCP/IP a systémem DNS*. 2. aktualizované vyd. Praha: Computer Press, 2000, 423 s. ISBN 80-7226-323-4.
[21] SPORTAK, Mark A. *Směrování v sítích IP*. 1.vyd. Brno: Computer Press, 2004, 368 s. ISBN 80-251-0127-4.

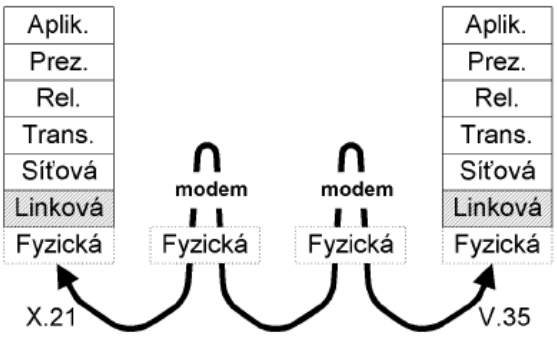
Vrstva 2: linková vrstva neboli vrstva datových spojů

Jestliže fyzická vrstva poskytuje své služby pro přenos jednotlivých bitů, tak vyšší linková vrstva má za úkol zajistit pomocí těchto služeb bezchybný přenos celých bloků dat, označovaných jako **rámce**. Datový rámec se skládá ze záhlaví, přenášených dat a zápatí, jak je znázorněno na obrázku 4.



Obr. 4 – Datový rámec[22]

V záhlaví se nese linková adresa příjemce a odesílatele, v zápatí je kontrolní součet z přenášených dat, jelikož na linkové vrstvě je, aby správně rozpoznala začátek a konec rámce. Na přenosové cestě může docházet k nejrůznějším poruchám a rušení, v jejichž důsledku mohou být přijaty jiné hodnoty bitů, než jaké byly původně vyslány a právě tento druh chyb rozpozná až linková vrstva, která kontroluje celé rámce. Odesílateli potvrzuje přijetí přenesených rámců, zatímco v případě poškozených rámců si vyžádá jejich opětovné vyslání.[23] Komunikaci na linkové vrstvě vidíme na obrázku 5.

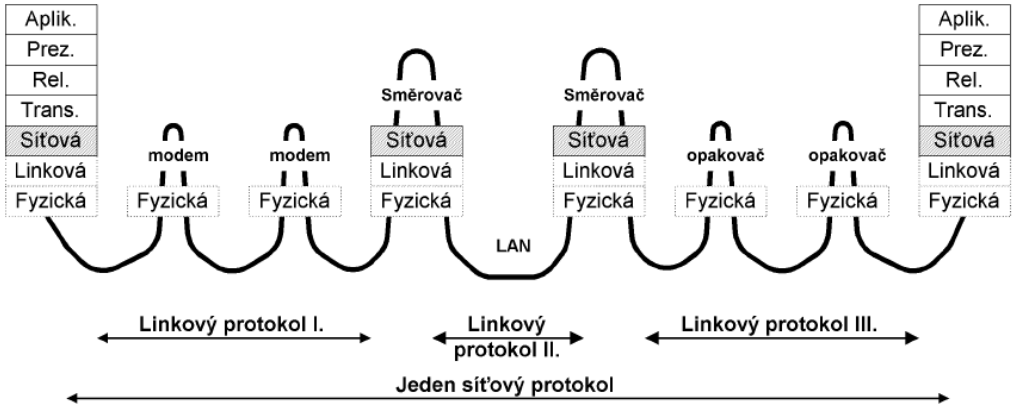


Obr. 5 – Komunikace na linkové vrstvě[24]

[22] DOSTÁLEK, Libor, KABELOVÁ, Alena. *Velký průvodce protokoly TCP/IP a systémem DNS*. 2. aktualizované vyd. Praha: Computer Press, 2000, 423 s. ISBN 80-7226-323-4.
[23] Totéž
[24] DOSTÁLEK, Libor, KABELOVÁ, Alena. *Velký průvodce protokoly TCP/IP a systémem DNS*. 2. aktualizované vyd. Praha: Computer Press, 2000, 423 s. ISBN 80-7226-323-4

Vrstva 3: síťová vrstva

Úkolem síťové vrstvy je zajistit potřebné **směrování (routing)** přenášených rámců, označovaných jako **pakety**. Síťový paket se skládá ze záhlaví a datového pole, jen zřídka je možno se setkat se zápatím. Síťová vrstva zajišťuje volbu vhodné trasy (route) přes mezilehlé uzly a postupné předávání jednotlivých paketů po trase od odesílatele až ke konečnému příjemci.[25] K přeposlání dat v paketech a výpočet cest za hranice místní sítě vysílajícího počítače je již zapotřebí směrovače. V rozsáhlých sítích mezi počítači leží jeden či více směrovačů se znalostí topologie sítě a způsobu vzájemného přímého propojení jednotlivých uzlů. Ke směrování se využívají směrovatelné protokoly a převládajícím protokolem se postupně stal IP.[26] Komunikace na síťové vrstvě ilustruje obrázek 6.



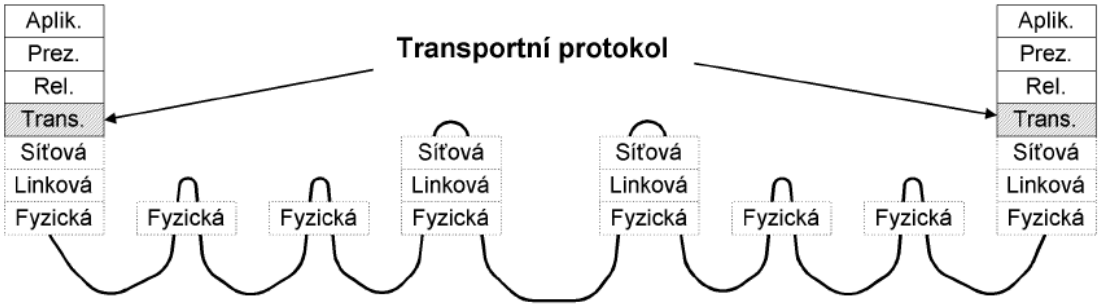
Obr. 6 – Komunikace na síťové vrstvě[27]

[25] DOSTÁLEK, Libor, KABELOVÁ, Alena. *Velký průvodce protokoly TCP/IP a systémem DNS*. 2. aktualizované vyd. Praha: Computer Press, 2000, 423 s. ISBN 80-7226-323-4.
[26] SPORTAK, Mark A. Směrování v sítích IP. 1.vyd. Brno: Computer Press, 2004, 368 s. ISBN 80-251-0127-4.
[27] DOSTÁLEK, Libor, KABELOVÁ, Alena. *Velký průvodce protokoly TCP/IP a systémem DNS*. 2. aktualizované vyd. Praha: Computer Press, 2000, 423 s. ISBN 80-7226-323-4.

Vrstva 4: transportní vrstva

Síťová vrstva poskytuje bezprostředně vyšší vrstvě služby, zajišťující přenos paketů mezi libovolnými dvěma uzly sítě. Transportní vrstvu tak zcela odstiňuje od skutečné topologie sítě a vytváří jí tak dojem, že každý uzel sítě má přímé spojení s kterýmkoliv jiným uzlem sítě bez modemů, opakovačů či směrovačů.

Transportní vrstva je tak zcela odkázána na služby nižších vrstev, které zajišťují spojení mezi počítači, a její pozornost je věnována na spojení mezi aplikacemi na vzdálených počítačích.[28] Důležitou funkcí této vrstvy je sestavování správného pořadí paketů, neboť mohou dorazit v nesprávném pořadí. Jelikož pakety mohou v síti využívat různých cest, nebo z důvodu ztráty či poškození dochází k novému vysílání a tím ke zpoždění oněch paketů, proto tato vrstva seřadí všechny pakety do správného pořadí a předá do relační vrstvy.[29] Na obrázku 7 vidíme spojení na transportní vrstvě, kterých může být mezi dvěma počítači několik.



Obr. 7 – Spojení na transportní vrstvě[30]

[28] DOSTÁLEK, Libor, KABELOVÁ, Alena. *Velký průvodce protokoly TCP/IP a systémem DNS*. 2. aktualizované vyd. Praha: Computer Press, 2000, 423 s. ISBN 80-7226-323-4.
[29] SPORTAK, Mark A. *Směrování v sítích IP*. 1.vyd. Brno: Computer Press, 2004, 368 s. ISBN 80-251-0127-4.
[30] DOSTÁLEK, Libor, KABELOVÁ, Alena. *Velký průvodce protokoly TCP/IP a systémem DNS*. 2. aktualizované vyd. Praha: Computer Press, 2000, 423 s. ISBN 80-7226-323-4.

Vrstva 5: relační vrstva

Úkolem této vrstvy je navazování, udržování a rušení **relací** (sessions) mezi koncovými účastníky. V rámci navazování relace si tato vrstva vyžádá na transportní vrstvě vytvoření spojení, prostřednictvím kterého probíhá komunikace mezi účastníky relace. Příkladem služby relační vrstvy je například RPC (Remote Procedure Call).[31]

Vrstva 6: prezenční vrstva

Prostřednictvím sítě se přenášejí data, která mohou mít povahu čísel, textů či obecných datových struktur. Jednotlivé stanice však mohou pracovat s odlišnou vnitřní reprezentací těchto dat. Cílem této vrstvy je, aby přenášené zprávy byly prezentovány jednotným způsobem a její povinností je, zabývat se pouze strukturou zpráv a nikoliv jejich významem, jejich význam je znám pouze aplikační vrstvě.[32]

„*Prezentační vrstvu podporuje celá řada norem, jako kódování textu (ASCII nebo EBCDIC), kódování grafických informací (PICT, TIFF, JPEG, GIFF), přenos obrazových, zvukových nebo multimediálních informací (MIDI, MPEG, QuickTime, HTML) apod.*“[33]

Vrstva 7: aplikační vrstva

Tato vrstva neobsahuje vlastní uživatelské aplikace, ale tvoří rozhraní mezi koncovými aplikacemi a síťovými službami, ve kterých jsou využity tzv. aplikační protokoly pro vzájemnou spolupráci.[34]

„Mezi nejznámější síťové aplikace patří např. elektronická pošta (např. aplikační protokol SMTP v architektuře TCP/IP nebo MHS v architektuře OSI), přenos souborů (např. protokoly FTP nebo TFTP v architektuře TCP/IP), vzdálený přístup (např. protokol TELNET u TCP/IP nebo VT u OSI).“[35]

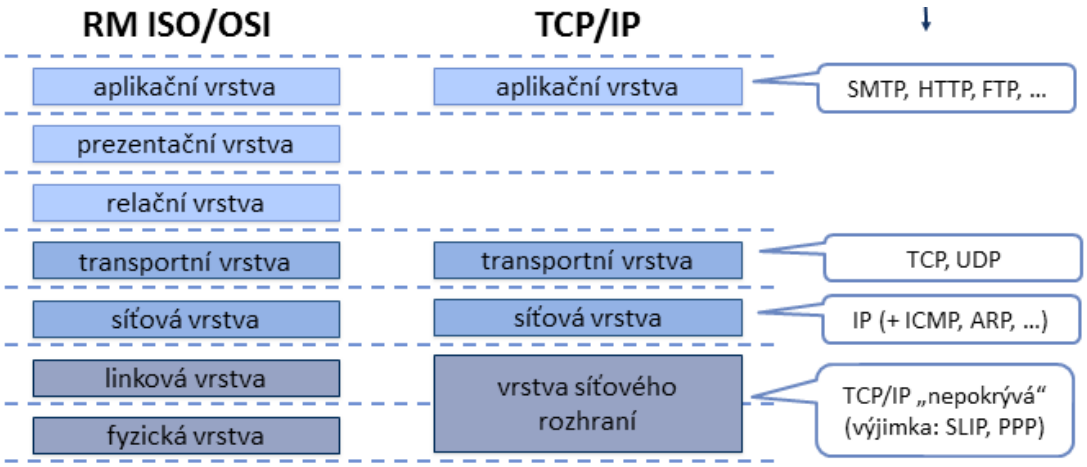
---

[31] SPORTAK, Mark A. *Směrování v sítích IP*. 1.vyd. Brno: Computer Press, 2004, 368 s. ISBN 80-251-0127-4.
[32] PUŽMANOVÁ, Rita. *Moderní komunikační sítě od A do Z*. 1.vyd. Praha: Computer Press, 1998, 432 s. ISBN 80-7226-098-7.
[33] Totéž
[34] SPORTAK, Mark A. *Směrování v sítích IP*. 1.vyd. Brno: Computer Press, 2004, 368 s. ISBN 80-251-0127-4.
[35] PUŽMANOVÁ, Rita. *Moderní komunikační sítě od A do Z*. 1.vyd. Praha: Computer Press, 1998, 432 s. ISBN 80-7226-098-7.

Referenční model OSI nenašel uplatnění v takové míře jako TCP/IP, přesto mnoho termínu vychází právě odtud.

2.1.1.2 TCP/IP

TCP/IP je síťová architektura, která vychází z předpokladu, že zajištění spolehlivosti je problémem koncových uživatelů komunikace a mělo by být řešeno až na úrovni transportní vrstvy. Protokoly fyzické a linkové vrstvy v praxi většinou vyhovují normám ISO OSI modelu, přesto každá skupina má vlastní definici svých vrstev. Z technologického pohledu se zdá, že balík TCP/IP právě zapadá do referenčního modelu OSI. Na obrázku 8 jsou znázorněny rozdíly obou těchto síťových architektur.[36]



Obr. 8 – Rozdíl mezi OSI a TCP/IP[37]

Model TCP/IP s protokoly je rozdělen do čtyř vrstev:

- Aplikační (HTTP, SMTP, POP3, FTP).
- Transportní (TCP, UDP).
- Síťová neboli Internetová (IP).

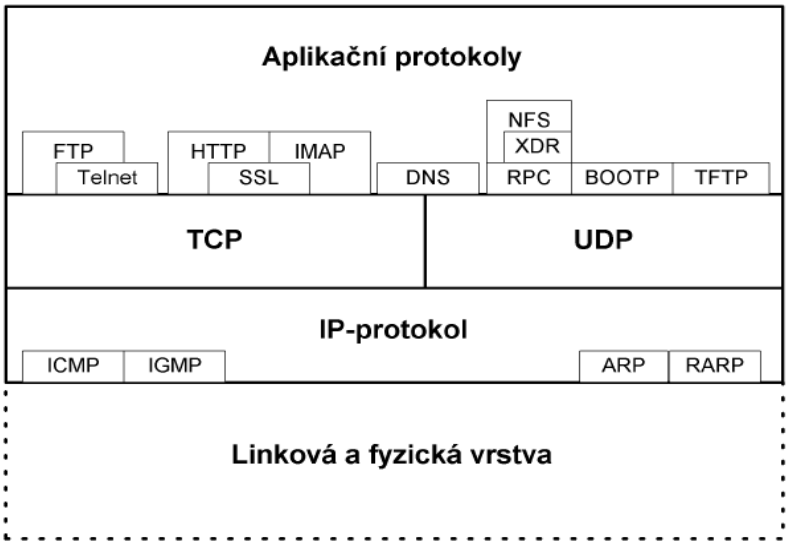
[36] VELTE, Toby J, VELTE, Anthony T. *Síťové technologie Cisco*. 1.vyd. Brno: Computer Press, 2003, 800 s. ISBN 80-7226-857-0.
[37] Obrázek převzat z *TCP/IP je síťovou architekturou*[online]. eArhiv.cz [citováno 26. 10. 2013]. Dostupné z: http://www.earchiv.cz/l225/slide.php3?l=3&me=2

- Vrstva síťového rozhraní (Ethernet, Frame Relay).

Aplikační vrstva

V této vrstvě poskytují aplikační protokoly rozhraní mezi sítí a aplikacemi ve formě služeb, které aplikace potřebují např. k přenosu souborů. V této jedné vrstvě jsou zredukovány vrstvy RM ISO/OSI modelu a to aplikační, prezentační a relační vrstvy. Výhodou je, že jednotlivé aplikační programy komunikují přímo s transportní vrstvou. Velké množství aplikačních protokolů můžeme rozdělit na:

- Uživatelské protokoly - využívají je převážně uživatelské aplikace k vyhledávání informací na internetu (HTTP, SMTP, Telnet, FTP, POP3 atd.).[38]
- Služební protokoly – využívají se převážně ke správné funkci internetu, jejichž funkci používají například směrovače (směrovací protokoly), nebo ke správě sítí (SNMP).[39]



Obr. 9 – Protokoly TCP/IP[40]

[38] DOSTÁLEK, Libor, KABELOVÁ, Alena. *Velký průvodce protokoly TCP/IP a systémem DNS*. 2. aktualizované vyd. Praha: Computer Press, 2000, 423 s. ISBN 80-7226-323-4.
[39] Totéž
[40] DOSTÁLEK, Libor, KABELOVÁ, Alena. *Velký průvodce protokoly TCP/IP a systémem DNS*. 2. aktualizované vyd. Praha: Computer Press, 2000, 423 s. ISBN 80-7226-323-4.

Transportní vrstva

Hlavním úkolem této vrstvy je zajistit spojení mezi běžícími aplikacemi na vzdálených počítačích. V transportní vrstvě se používají dva protokoly:

- TCP (Transmission Control Protocol) je spojovou službou, jelikož příjemce potvrzuje přijímaná data, která se v případě ztráty zopakují, a tím je zaručena spolehlivost přenosu dat. Protokoly TCP dopravují data pomocí TCP segmentů, které se adresují jednotlivým aplikacím.
- UDP (User Datagram Protocol) je nespojovaná služba, jelikož odesílatel odešle datagram příjemci a již se nestará o to, jestli byl doručen. Nezajišťuje tedy spolehlivost přenosu.[41]
-

„*Podstatné je vědět, že přenos zprávy může vždy řídit pouze jeden přenosový neboli transportní protokol. Při stahování webové stránky obsluhuje například veškeré pakety protokol TCP, zatímco protokol UDP se práce nijak neúčastní. Stahování nebo umisťování souborů v jednoduchém protokolu TFTP (Trivial File Transfer Protocol) zajišťuje naopak výhradně protokol UDP.*“[42]

Aplikace je v Internetu adresována IP adresou, číslem portu a použitým TCP nebo UDP protokolem. Operační systém v cílovém počítači pozná, které aplikaci se má doručit například TCP segment a to podle čísla cílového portu.[43]

Protokoly TCP/IP jsou v podstatě standardem, který sjednocuje Internet.

Síťová neboli Internetová vrstva

Úkolem této vrstvy je, aby se jednotlivé pakety dostaly od odesílatele až ke svému skutečnému příjemci, přes případné směrovače. Tento úkol je realizován pomocí IP (Internet Protocol) a přenáší tzv. IP datagramy (*datagram je základní jednotkou dat v paketech IP*) mezi vzdálenými počítači. IP datagram nese ve svém záhlaví adresu příjemce, která slouží pro dopravu IP datagramu k adresátovi. K jednoznačné identifikaci v síti Internet, který je tvořen jednotlivými sítěmi, musí být splněna

[41] DOSTÁLEK, Libor, KABELOVÁ, Alena. *Velký průvodce protokoly TCP/IP a systémem DNS*. 2. aktualizované vyd. Praha: Computer Press, 2000, 423 s. ISBN 80-7226-323-4.
[42] VELTE, Toby J, VELTE, Anthony T. *Síťové technologie Cisco*. 1.vyd. Brno: Computer Press, 2003, 800 s. ISBN 80-7226-857-0.
[43] DOSTÁLEK, Libor, KABELOVÁ, Alena. *Velký průvodce protokoly TCP/IP a systémem DNS*. 2. aktualizované vyd. Praha: Computer Press, 2000, 423 s. ISBN 80-7226-323-4.

podmínka a to taková, že každé síťové rozhraní v sítí má svou jednoznačnou IP adresu. Z toho vyplývá, že jedno síťové rozhraní může mít více IP adres, ale v žádném případě nesmí mít jednu IP adresu více síťových rozhraní.[44]

Vrstva síťového rozhraní

Úkolem této vrstvy je vše, co je spojeno s ovládáním konkrétní přenosové cesty a s přímým vysíláním a příjmem datových paketů. Jde o vlastní komunikaci protokolů TCP/IP se všemi síťovými technologiemi, které odpovídají modelu OSI. V rámci soustavy TCP/IP není tato vrstva blíže specifikována, neboť je závislá na použité přenosové technologii.[45]

2.1.1.3 IP protokol (Internet Protocol)

IP protokolem je umožněno spojení lokálních sítí LAN do celosvětového internetu. Tento protokol spojující jednotlivé sítě umožňuje dopravovat data od odesílatele k příjemci přes směrovače (router). Směrování v TCP/IP je založeno na jednotlivých adresách sítí nikoli na adresách jednotlivých počítačů v rámci sítě. Každý hostitelský počítač, který chce odeslat IP datagram jinému hostitelskému počítači, dokáže z IP adresy příjemce rozpoznat, zda se stanice příjemce nachází ve stejné síti či nikoli. Pokud se nachází ve stejné síti, pošle mu odesílatel svůj datagram přímo, jestliže se příjemce nachází v jiné síti, pošle odesílatel svůj datagram nejbližšímu směrovači (brány) ve své síti. Každý směrovač pak řeší samostatně směrování k následujícímu směrovači a data jsou tímto předávána od směrovače ke směrovači.[46]

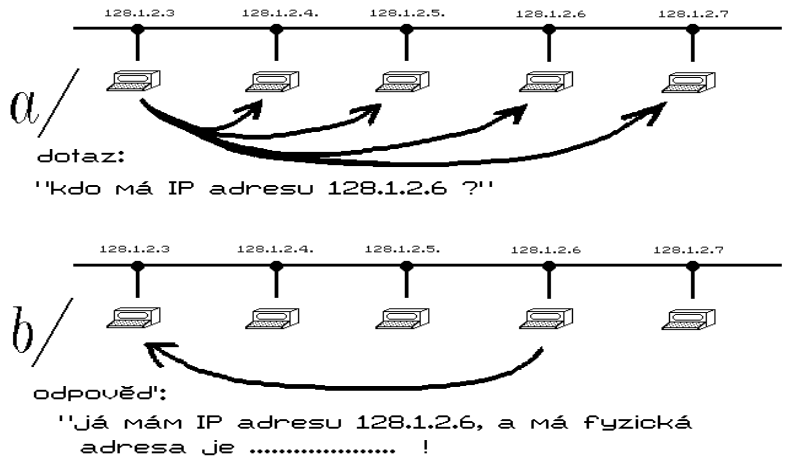
IP-protokol je tvořen několika dílčími protokoly:

- Vlastním protokolem IP.
- Služebním protokolem ICMP (Internet Control Message Protocol), sloužící k signalizaci chyb a jiných významných událostí v síti, který podává chybové zprávy výhradně původnímu odesílateli. Protokol ICMP je umístěn v datové

[44] DOSTÁLEK, Libor, KABELOVÁ, Alena. *Velký průvodce protokoly TCP/IP a systémem DNS*. 2. aktualizované vyd. Praha: Computer Press, 2000, 423 s. ISBN 80-7226-323-4.
[45] VELTE, Toby J, VELTE, Anthony T. *Síťové technologie Cisco*. 1.vyd. Brno: Computer Press, 2003, 800 s. ISBN 80-7226-857-0.
[46] *Protokol IP*[online]. [citováno 23. 11. 2013]. Dostupné z: http://pc-site.owebu.cz/?page=PIP

části IP diagramu. ICMP zprávy informují o nedoručitelnosti IP datagramu, nesou jeho celé záhlaví a prvních 64 bitů dat a odesílatel podle toho dokáže lépe identifikovat původní datagram, ke kterému se ICMP zpráva váže. Tento protokol je popsán v RFC 792.

- Služebním protokolem IGMP (Internet Group Management Protocol), sloužící pro dopravu adresných oběžníků ve skupině (*multicasts)*. Komunikace ve skupině musí být podporována protokolem síťové vrstvy, který umožňuje přihlášení a odhlášení ze skupiny.
- Služební protokoly ARP (Address Resolution Protocol) a RARP (Reverse Address Resolution Protocol), které jsou často vyčleňovány jako samostatné na IP nezávislé protokoly, jelikož pracují na hranici mezi spojovou a síťovou vrstvou, kde budují a udržují převodní tabulky mezi IP adresami a fyzickými adresami (MAC) a jejich rámce nejsou předcházeny IP-záhlavím.[47]



Obr. 10 – Způsob zjištění fyzické adresy[48]

[47] *IP Protokol*[online]. Velký průvodce protokoly [citováno 24. 11. 2013]. Dostupné z: http://zam.opf.slu.cz/botlik/CD-0x/5.html

[48] Obrázek převzat z *Adresování v TCP/IP v sítích II*[online]. eArhiv.cz [citováno 24. 11. 2013]. Dostupné z: http://www.earchiv.cz/a92/a235c110.php3

„Představme si situaci, kdy jeden uzlový počítač chce zaslat nějaká data jinému počítači v téže dílčí síti. Zná však pouze jeho IP adresu, nikoli jeho fyzickou adresu. Protokol ARP prvního počítače proto využije možnosti všesměrového vysílání, a všem uzlům dané dílčí sítě pošle zvláštní rámec resp. paket s dotazem: "Kdo má IP adresu....?". Tento rámec přijmou všechny uzly, a všechny také vyhodnotí paket, který je v něm obsažen. Pouze uzel B však rozpozná, že obsahuje jemu určený dotaz, a tak na něj odpoví zasláním své fyzické adresy (opět prostřednictvím speciálního paketu, jehož formát definuje protokol ARP). Ostatní uzly přitom na původní dotaz neodpovídají.“[49]

Princip dotazu a odpovědi protokolem ARP demonstruje obrázek č. 10.

IP datagram

IP-datagram se skládá:

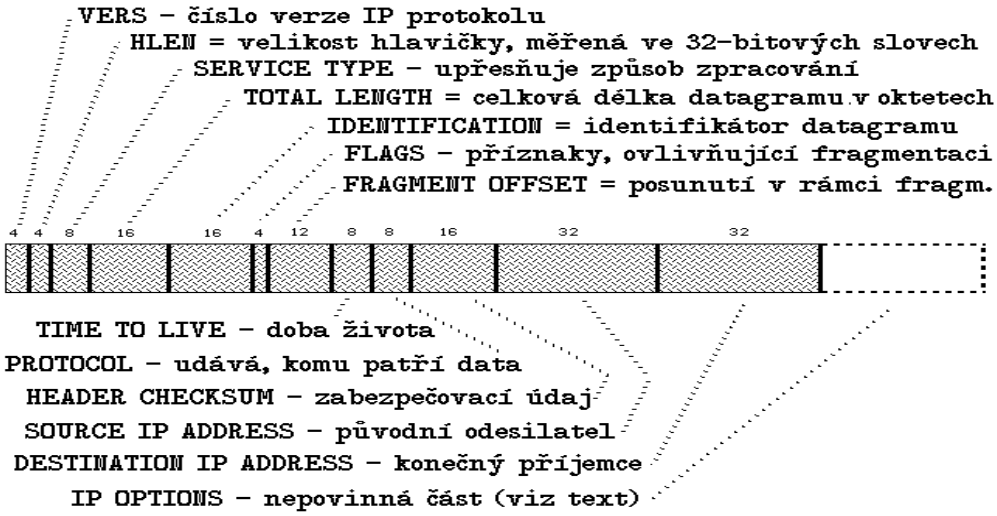
- Ze **záhlaví** - obsahují různé informace, které jsou potřebné pro řízení a správu komunikace. Tyto informace využívají směrovače a počítače ke zpracování paketu po cestě a po doručení do cíle dojde k sestavení zprávy ve správném pořadí ze všech paketů.
- **Přenášených dat** – obsahuje samotnou datovou zátěž, která je odeslána po síti až do cíle.

Každý datagram je samostatná jednotka, která musí obsahovat veškeré informace o adresátovi i odesilatelovi. Datagramy se po síti posílají nezávisle na sobě a mohou být doručeny v různém pořadí.[50]

Údaje neboli formát hlavičky IP datagramu se skládá z několika položek, jakými jsou např. *maximální délka IP datagramu* – (hlavičky i datové části, měřenou v oktetech), *doba života* - (údaj, který je měřen v sekundách a určuje, jak dlouho se daný IP datagram může nacházet v soustavě vzájemně propojených sítí), *fragmentace*

[49] *IP adresy*[online]. [citováno 07. 12. 2013]. Dostupné z: http://pc-site.owebu.cz/?page=PTCPIP3
[50] VELTE, Toby J, VELTE, Anthony T. *Síťové technologie Cisco*. 1.vyd. Brno: Computer Press, 2003, 800 s. ISBN 80-7226-857-0.

datagramů – (dochází k rozdělení původního datagramu na několik dílčích fragmentů a to z důvodu, aby se celé vešly do rámců, které je příslušná síť schopna skutečně přenést), celý formát hlavičky IP datagramu znázorňuje obrázek 11.[51]



Obr. 11 – Formát hlavičky IP datagramu[52]

Adresování v protokolu IP

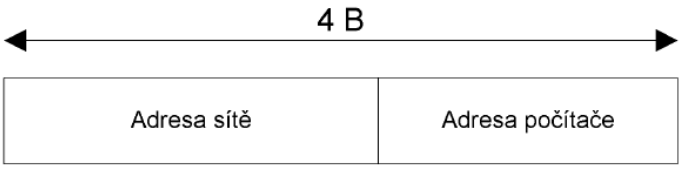
Každý počítač v síti TCP/IP má přidělenou jednoznačnou 32 bitovou (4byte) IP adresu, která se používá při komunikaci s tímto PC. Každá IP adresa je tvořena dvojící *netid* což je adresa sítě, ke které PC patří a *hostid* což je adresa PC v dané síti. Tato dvojitá adresace slouží k úspoře objemu směrových tabulek, protože směrování v TCP/IP sítích je založeno pouze na adresách dílčích sítí a nikoli na adresách hostitelských počítačů. Celou podstata spočívá v tom, že hostitelský počítač, který odesílá IP datagram jinému hostitelskému počítači, již podle IP adresy pozná, jestli patří do stejné sítě. Jestliže cílový hostitelský počítač patří do jiné sítě, pak odesílatel pošle IP datagram do směrovače a ten již rozhodne, kudy datagram pošle. V celé škále směrovačů (brán) v rozlehlé síti, tak až poslední brána v řetězci určí podle

[51] PETERKA, Jiří. *Protokol IP*[online]. eArhiv.cz [citováno 15. 02. 2014]. Dostupné z: http://www.earchiv.cz/a92/a248c110.php3

[52] Obrázek převzat z *Adresování v TCP/IP v sítích II*[online]. eArhiv.cz [citováno 15. 02. 2014]. Dostupné z: http://www.earchiv.cz/a92/a235c110.php3

zbývající části IP adresy příjemce, která vyjadřuje adresu hostitelského počítače v rámci cílové sítě, odešle datagram přímo konečnému adresátovi.[53]

Formát IP adresy tvoří 32 bitů a je rozdělena do čtyř skupin po osmi bitech (4oktety = 4B), které se zapisují v dekadickém formátu a navzájem jsou oddělené tečkami. Tento zápis je mnohem srozumitelnější pro člověka, ale je možné celou 32 bitovou IP adresu vyjádřit jako celá dvojková čísla. Například v dekadickém čísle máme IP adresu – 128.10.2.30 tak ve dvojkovém formátu dostaneme - 1000000 00001010 00000010 00011110.[54]
IP adresy jsou rozděleny do tříd podle toho, kolik bitů je vyhrazeno pro síťovou a pro hostitelskou část adresy, jak můžeme vidět na obrázku 12.



Obr. 12 – Složení IP adresy[55]

Celkem rozlišujeme tří základní třídy a dvě specializované třídy, které označujeme jedním velkým písmenem a to **A, B, C, D a E**.
Třída A je rozdělena tak, že první oktet je využit pro identifikaci adresy sítě a zbývající tři oktety pro identifikaci adresy počítače. Interval adres v této třídě je 0.0.0.0 až 127.0.0.0 a tím je její rozsah omezen na 126 platných adres sítě a to z důvodu, že adresa 127.0.0.0 je vyhrazena pro adresu lokální smyčky (loop-back).
Třída B je rozdělena tak, že první dva oktety jsou využity pro identifikaci adresy sítě a zbývající dva oktety pro identifikaci adresy počítače. Interval adres je 128.0.0.0 až 191.255.0.0 a z toho je umožněno 16384 různých sítí a 65534 možných adres v každé síti.

[53] PETERKA, Jiří. *Adresování v TCP/IP sítích-I*[online]. eArhiv.cz [citováno 16. 02. 2014]. Dostupné z: http://www.earchiv.cz/a92/a233c110.php3
[54] totéž
[55] DOSTÁLEK, Libor, KABELOVÁ, Alena. *Velký průvodce protokoly TCP/IP a systémem DNS*. 2. aktualizované vyd. Praha: Computer Press, 2000, 423 s. ISBN 80-7226-323-4.

Třída C je rozdělena tak, že první tři oktety jsou využity pro identifikaci sítě a poslední oktet je využit pro identifikaci adresy počítače. Interval adres je 192.0.0.0 až 223.255.255.0 a z toho je umožněno 2 097 152 různých sítí a 254 možných adres v každé síti. [56]

Třída D je určena pro potřeby skupinového vysílání v sítích IP, ale s omezenou možností uplatnění, protože je tato adresa jedinečná a směruje cílové pakety do předem definované skupiny jednotlivých IP adres. Interval adres je 224.0.0.0 až 239.255.255.254. [57]

Třída E je vyhrazena pro výzkumné účely.

Třídy IP adres

Třída	začátek (bin)	1. bajt	standardní maska	bitů sítě	bitů stanice	sítí	stanic v každé síti
A	0	0–127	255.0.0.0	7	24	$2^7 = 128$	$2^{24}-2 = 16\,777\,214$
B	10	128–191	255.255.0.0	14	16	$2^{14} = 16384$	$2^{16}-2 = 65\,534$
C	110	192–223	255.255.255.0	21	8	$2^{21} = 2\,097\,152$	$2^8-2 = 254$
D	1110	224–239	*multicast*				
E	1111	240–255	*vyhrazeno jako rezerva*				

Obr. 13 – Třídy IP adres[58]

Síťová maska

Síťová maska určuje adresu sítě a je jakousi hranicí mezi adresou sítě a počítače. Formát síťové masky tvoří čtyřbajtové číslo (32bitů) a v bitovém tvaru obsahuje jedničky na místech, kde se nachází adresa sítě, a nuly jsou na místech, kde se nachází adresa počítače. Jednotlivé třídy A, B a C mají standardní síťové masky, jak jsou uvedeny v následující tabulce.

[56] *IPv4*[online].[citováno 20. 02. 2014]. Dostupné z: http://home.zcu.cz/~hliboka/ipv4/ipv4.html
[57] SPORTAK, Mark A. *Směrování v sítích IP*. 1.vyd. Brno: Computer Press, 2004, 368 s. ISBN 80-251-0127-4.
[58] Obrázek převzat z *IP adresa*[online]. wikipedie [citováno 20. 02. 2014]. Dostupné z: http:// http://cs.wikipedia.org/wiki/IP_adresa

A	255.0.0.0	11111111.00000000.00000000.00000000
B	255.255.0.0	11111111.11111111.00000000.00000000
C	255.255.255.0	11111111.11111111.11111111.00000000

Tab. 1 – Síťová maska ve třídách A, B, C

Určit adresu sítě, na které leží počítač o IP adrese, si můžeme předvést v následujícím příkladu. Máme-li počítač o IP adrese v desítkové soustavě 170.85.255.248 (dvojkově 10101010.01010101.11111111.11111000) a podle tabulky tříd zjistíme, že patří do třídy B, jehož standardní maska v desítkové soustavě je 255.255.0.0 (dvojkově 11111111.11111111.00000000.00000000).
Vynásobením IP adresy a masky, dostaneme adresu sítě, jak je vidět na příkladu v následující tabulce.

IP počítače	10101010.01010101.11111111.11111000	170.85.255.248
x IP maska	11111111.11111111.00000000.00000000	255.255.0.0
IP sítě	10101010.01010101.00000000.00000000	170.85.0.0

Tab. 2 – Příklad získání adresy sítě

S ohledem na dnešní složení internetových sítí, se přestalo nahlížet na třídy adres, ale výhradně přes síťové masky, protože z pohledu masky je síť a subsíť (subnet) jeden celek. Metoda subsítí spočívá v tom, že adresování může být logicky rozděleno do několika dalších hostitelských bitů uvozujících subsíť, jejichž základem je využití masek podsítí. Tato technika umožňuje rozdělit jednu síťovou adresu na více menších adres. Toto řešení je efektivním prostředkem pro vytvoření více sítí z jedné a tímto je umožněno většině firem rozšířit svůj adresní prostor na konfiguraci lokálních sítí. Vše je způsobeno z nedostatku IP adres přidělených poskytovatelem internetových služeb.[59]

[59] DOSTÁLEK, Libor, KABELOVÁ, Alena. *Velký průvodce protokoly TCP/IP a systémem DNS*. 2. aktualizované vyd. Praha: Computer Press, 2000, 423 s. ISBN 80-7226-323-4.

Subsíť (subnetting) je metoda rozdělování sítě a znamená, že maska podsítě rozdělí IP adresu na adresu sítě a adresu hostitele. Ve výsledku máme IP adresu a masku podsítě, které jsou efektivněji zpracovatelné, jelikož znalost sítí a subsítí je důležitá pro směrování v Internetu a to právě z důvodu, že směrovače nepotřebují znát jednotlivé adresy hostitelských stanic, ale jejich rozhodnutí je na základě první částí adresy sítě nebo subsítě.

<table>
<tr><td colspan="3">IP-adresa (4B)</td></tr>
<tr><td>Adresa sítě</td><td>Adresa subsítě</td><td>Adresa počítače</td></tr>
<tr><td colspan="3">Síťová maska (4B)</td></tr>
<tr><td colspan="2">jedničky</td><td>nuly</td></tr>
</table>

Obr. 14 Subnetting

Příkladem rozdělení sítě například třídy C je standardní maska 255.255.255.0 (dvojkově 11111111.11111111.11111111.00000000) a ta určuje, že prvních 24 bitů je vyhrazeno pro adresování sítě a posledních 8 bitů zbývá pro adresy subsítě a hostitelských stanic. Možnosti o počtu subsítí a hostitelských stanic ve třídě C znázorňuje následující tabulka.[60]

Počet bitů ve 4 oktetu	Maska subsítě binárně čtvrtý oktet	Maska subsítě dekadicky	Počet použitelných adres subsítí	Počet použitelných host. adres v jedné subsíti
2	11000000	255.255.255.192	2	62
3	11100000	255.255.255.224	6	30
4	11110000	255.255.255.240	14	14
5	11111000	255.255.255.248	30	6
6	11111100	255.255.255.252	62	2

Tab. 3 – Subsítě a hostitelské stanice

[60] SPORTAK, Mark A. *Směrování v sítích IP*. 1.vyd. Brno: Computer Press, 2004, 368 s. ISBN 80-251-0127-4.

CIDR (Classles Inter-Domain Routing) je směrování na základě prefixu adres a vyjadřuje se počtem bitů prefixu za adresou IP s lomítkem, kde oznamuje konkrétní bitovou masku a tím nahrazuje pevné kategorie původní architektury tříd adres. Tato metoda umí rozdělit adresový prostor přesně podle velikosti konkrétní sítě a v podstatě se IP adresy přidělují po tzv. CIDR blocích s příslušnou maskou.
Příklad zápisu beztřídního směrování CIDR je například *200.100.50.64/28,* kde hodnota za lomítkem *28* udává počet jedničkových bitů v masce sítě v binární formě a v dekadickém zápisu by ona maska měla hodnotu *255.255.255.240*.[61]

VLSM (Variable Length Subnet Masks) umožňuje používat v rámci jedné adresy sítě několika podsíťových masek různé délky podle konkrétních potřeb a tím využívají efektivněji adresový prostor IP dané organizace.[62]

2.1.2 Topologie sítí

Topologie sítě popisuje fyzické propojení komunikačních stanic a uspořádání jejích uzlů se způsobem toku signálu a obvykle je vyjádřena jako logická mapa, která graficky znázorňuje každý jednotlivý uzel a linky, které uzly propojují. Pro správu sítě s pomocí softwárových nástrojů, ve kterých fungují topologické mapy sítě i s uživatelským grafickým rozhraním.
Topologie lokálních sítí (LAN) se liší od rozlehlých sítí (WAN), jelikož řešení sítí WAN je poněkud volnější a opírají se o postupné předávání zpráv mezi uzly po dvoubodových spojích polygonálně či hvězdicově.[63]
Topologie sítí LAN má zásadní význam na řadu vlastností lokální sítě:

- Snadná rozšiřitelnost sítě. Při nutnosti rozšíření je možné k síti přidávat další prvky s minimálním dopadem na stávající síť.
- Spolehlivost. Chyby jsou většinou izolovány do segmentů, kde vznikají.

[61] PUŽMANOVÁ, Rita. *Moderní komunikační sítě od A do Z*. 1.vyd. Praha: Computer Press, 1998, 432 s. ISBN 80-7226-098-7.
[62] SPORTAK, Mark A. *Směrování v sítích IP*. 1.vyd. Brno: Computer Press, 2004, 368 s. ISBN 80-251-0127-4.
[63] PUŽMANOVÁ, Rita. *Moderní komunikační sítě od A do Z*. 1.vyd. Praha: Computer Press, 1998, 432 s. ISBN 80-7226-098-7.

- Srozumitelnost sítě díky její jednoduchosti, která přináší další úspory nákladů za správu sítě a školení personálu.
- Bezpečnost. Přístup k síti je přesně definován.

Rozeznáváme následující typy topologií:

- sběrnice
- hvězda
- strom
- kruh
- propojená síť.

Sběrnice

Základním prvkem sběrnicové sítě je spojovací vedení – (koaxiální kabel nebo symetrické vedení), ke kterému jsou připojeny jednotlivé stanice sítě a to bez centrální či hlavní stanice. Datová zpráva, která je šířena po vedení je k dispozici pro všechny stanice v této síti. Vlastnosti sběrnicové sítě jsou:

- použití jednoho vedení
- snadné připojování a odpojování stanic
- odolnost proti výpadkům stanic.

Hvězda

Jednotlivé stanice jsou připojeny k centrálnímu uzlu sítě, kterému se říká *rozbočovač* (hub). Rozbočovač můžeme rozlišit na:

- **pasivní**, ve kterém je signál pouze dělen odporovým děličem a pouze distribuuje vyslaný signál
- **aktivní**, ve kterém má přijatý signál na výstupních linkách požadovanou úroveň.

Vlastnosti této sítě jsou:

- síť je méně náchylná k poruchám v rámci jednotlivých propojení stanic
- jednoduché monitorování
- snadno ralizovatelné dvoubodové spojení[64]

[64] PUŽMANOVÁ, Rita. *Moderní komunikační sítě od A do Z*. 1.vyd. Praha: Computer Press, 1998, 432 s. ISBN 80-7226-098-7.

Strom

Stromová topologie je seskupení uzlů s vícenásobnými větvemi s kombinací několika propojení topologie typu hvězda a právě tuto kombinaci *strom* a *hvězda* využívají složitější topologie sítí.

Vlastnosti této topologie jsou podobné s topologií typu hvězda.

Kruh

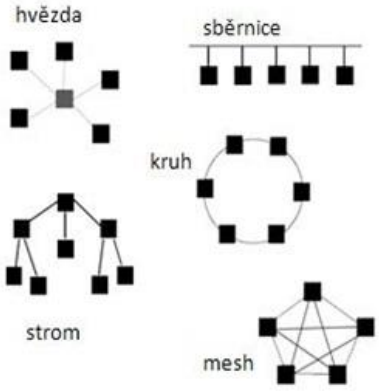
Jednotlivé stanice jsou propojeny spoji, které jsou využívány jednosměrně a datové zprávy se předávají postupně mezi stanicemi ve tvaru kruhu.

Vlastnosti této sítě jsou:

- v síti můžeme kombinovat různé spojovací vedení (symetrické nebo světlovodné na dlouhé vzdálenosti), protože se jedná o jednosměrné a dvoubodové spojení
- síť je náchylná na chod sítě, jelikož při výpadku jednotlivé stanice dojde k přerušení činnosti sítě.[65]

Propojená síť

Propojená síť (mesh) je propojení všech nebo částečných spojů rovnocenných uzlů.[66]



Obr. 15 – Topologie sítí[67]

[65] PUŽMANOVÁ, Rita. *Moderní komunikační sítě od A do Z*. 1.vyd. Praha: Computer Press, 1998, 432 s. ISBN 80-7226-098-7.
[66] PUŽMANOVÁ, Rita. *Širokopásmový Internet Přístupové a domácí sítě*. 1.vyd. Brno: Computer Press, 2004, 377 s. ISBN 80-251-0139-8.
[67] Totéž

2.2 Konvergence sítí

Vývoj telefonních a datových sítí byly v nedávné minulosti tvořeny dvěma samostatnými typy sítí, jelikož každá z nich byla určena k odlišnému účelu. Budování dvou odlišných sítí bylo z jisté části dáno historickými a převážně technickými možnostmi, protože přenos hlasu a přenos dat mají odlišné požadavky na přenosovou síť. Tato dvojkolejnost dvou odlišných sítí byla dosti neekonomická a to z důvodu provozu a rozvoje. S rozvojem technologických možností dochází k integraci telefonních a datových sítí do jedné společné sítě. Díky vzájemnému propojení neboli konvergenci technologií se Internet stává jediným společným potrubím pro veškeré služby a potřebnou komunikaci.[68]

Integrací těchto dvou sítí dochází k dynamickému rozvoji služeb a ke konvergenci na vyšší úrovni. Rychlost přístupu s různorodostí nabízených technologií připojení se k integrované síti, na které poskytovatelé nabízejí služby obsahující tzv. trojici služeb (data+obraz+hlas).

Přístup k těmto službám by měl být:

- rychlý,
- neustále dostupný,
- snadno ovladatelný,
- spolehlivý,
- bezpečný,
- nezávislý na technologii nebo koncovém zařízení.

Výhoda jednotné sítě je vytváření nových služeb a jejich implementace, tím se stávají atraktivnější pro zákazníky a provozovatelům to umožní snížit náklady na provoz a údržbu sítě.[69]

[68] RUDINSKÝ, J. *Sítě nové generace - NGN*[online]. Access server 4.5.2006 [citováno 15. 03. 2014]. Dostupné z: http://access.feld.cvut.cz/view.php?cisloclanku=2006050401

[69] PUŽMANOVÁ, Rita. *Širokopásmový Internet Přístupové a domácí sítě*. 1.vyd. Brno: Computer Press, 2004, 377 s. ISBN 80-251-0139-8.

2.2.1 Vývoj telefonních a datových sítí

Ke správnému pochopení a smyslu konvergence sítí je nutné objasnit základní technické odlišnosti požadavků hlasových a datových služeb na přenosovou infrastrukturu.

Základní rozdělení telefonních a datových sítí:

- **Telefonní síť PSTN** (Public Switch Telephone Network) – komunikace v této síti probíhá v reálném čase a funguje tak, že mezi dvěma komunikujícími stanicemi je vytvořeno trvalé spojení, které je udržováno po celou dobu. K rozpadu spojení dochází tehdy, kdy jedna z komunikujících stran ukončí spojení. V PSTN hovoříme o tzv. **přepojování okruhů** (circuit switching) - garantuje přenosovou kapacitu (nedá se dynamicky měnit) - šířka pásma 64 kbit/s pro jeden telefonní hovor.
- **Datová síť –** komunikace v této síti neprobíhá v reálném čase. Data mezi dvěma stanicemi jsou přenášena v blocích, kterým se říká pakety. Paket v sobě obsahuje adresu příjemce a odesílatele. V síti je paket přepojován a vysílán tak, aby se dostal až do určeného cíle a to tak, že není podstatné, jakou cestou se k příjemci dostane. V datové síti hovoříme o tzv. **přepojování paketů** (packet switching) – sdílení přenosové kapacity. Nepříjemným jevem paketových přenosů jsou nepravidelnosti anebo v doručování jednotlivých částí dat. Tyto nepravidelnosti vznikají v důsledku různě velkého zpoždění při přenosu jednotlivých paketů v síti.[70]

Výkonostní paramtery reálných sítí:

- **Šířka pásma - propustnost** (bandwidth, throughput) – důležitým parametrem sítě je přenosová rychlost a právě šířka pásma, jenž nám udává maximální možnou přenosovou rychlost pro dané typy technologií, jakými mohou být např.: Modem / Dialup(56 Kbit/s), ADSL Lite (1.5 Mbit/s), Ethernet (10 Mbit/s).

[70] PUŽMANOVÁ, Rita. Širokopásmový Internet Přístupové a domácí sítě. 1.vyd. Brno: Computer Press, 2004, 377 s. ISBN 80-251-0139-8.

- **Latence – zpoždění** (latency/delay) – je parametr, který nám udává, jak dlouho trvá cesta paketu od odesílatele k příjemci. Odezva signálu v datové síti se uvádí v milisekundách – např. *ping*.[71]
- **Ztrátovost paketů** (packet loss) – je parametr, který popisuje spolehlivost a stabilitu sítě. Jde o poměr poslaných paketů, které nebyly přijaty v cíli nebo byly přijaty s chybou. Síť by měla mít nulovou nebo minimální ztrátovost.
- **Dostupnost** (availability) – tento parametr je důležitý, protože nám udává dobu spolehlivosti, po kterou je danná služba poskytována. Nejčastěji je uváděn v procentech a to za určité časové období.
- **Rozptyl zpoždění** (jitter) – je prarametr, který nám udává rozdíl mezi minimální a maximální přenosovou rychlostí za určitý čas.
- **Kvalita služby QoS** (Quality of Service) – tento parametr je velmi důležitý pro provoz konkrétní služby, která vyžaduje určitou prioritu v síti.

[71] KOVÁŘ, Jiří. *SLA – kvalita služeb*[online]. Ing. Jiří Kovář – znalec v oboru elektronika a kybernetika[citováno 23. 03. 2014]. Dostupné z: http://jirikovar.cz/index.php/13-internet-a-datove-site/datova-sit/10-sla-kvalita-sluzeb

3 Zabezpečení počítačové sítě

Moderní počítačové sítě se stávají stále složitějšími a bez odpovídajícího zabezpečení sítě se nemůžeme připravit na obranu útoků ze strany *hackerů*. Zabezpečení sítě je sice nepřetržitý a nekončící proces, přesto by systém zabezpečení měl být jednotný, jednoduchý, výkonný a osvědčený. Kompletní zabezpečení neznamená jenom útoky detekovat, ale nekompromisně likvidovat veškeré hrozby.
Bezpečnostní problémy v síti mohou nastat, pokud máme:

- **Slabá místa v technologiích** – mohou být v protokolech TCP/IP (sledování paketů, telnet, atd.), operačních systémech a síťových vybavení (nedostatečná hesla, špatně nastavený firewall, atd.)
- **Slabá místa v konfiguraci** – která mohou nastat nesprávnou konfigurací počítače nebo síťového zařízení, jakými například mohou být nezabezpečené uživatelské účty či nesprávně nastavené internetové služby.
- **Slabá místa v bezpečnostních zásadách** – hovoříme zde o bezpečnostní politice, kterou představují popisy pravidel a jejich dodržování v dané organizaci.

Zabezpečení sítě není tedy jednotným standardem či uceleným systémem, ale skládá se z různých komponent a nástrojů, které slouží před útoky *zvenčí* a *zevnitř* a proto je zapotřebí věnovat pozornost otázce bezpečnosti, jelikož ochrana počítačové sítě je poměrně rozsáhlá problematika.[72]

[72] WENSTROM, Michael. *Zabezpečení sítí Cisco*. 1.vyd. Brno: Computer Press, 2003, 784 s. ISBN 80-7226-952-6.

3.1 Bezpečnostní služby v počítačových sítích

Počítačová síť by měla nabízet bezpečnostní služby takové, které se mohou v praxi implementovat na různých vrstvách komunikačního protokolu. Bezpečnostní služby dělíme do následujících kategorií:

- **Autentizace** (authentication) – jedná se o ověření identity komunikujících subjektů. Ověření totožnosti se tedy provádí na jedné, nebo na obou stranách probíhající komunikace.
- **Řízení přístupu** (access kontrol) – jedná se o autorizaci, která poskytuje ochranu na základě identifikace uživatele a jeho přístupových práv. Tato služba je spíše využívána až v operačním systému nebo v aplikaci.
- **Utajení a zabezpečení dat** (confidentiality a privacy) – jde o ochranu přenášených dat proti odposlechu v rámci navázaného spojení.
- **Integrita dat** (integrity) – jedná se o ochranu přenášených dat před neautorizovanou změnou tak, aby zpráva přijatá byla identická se zprávou vyslanou.
- **Ochrana proti odmítnutí původu zprávy** (nonrepudiation) – princip spočívá v tom, že zabrání odesílateli nebo příjemci odmítnout potvrzení o vyslání nebo přijetí zprávy.[73]

K zajištění bezpečnosti těchto služeb se uplatňují kryptografické mechanismy – (*šifrování*). To znamená, že data byla zašifrována pomocí určitého algoritmu, jehož účelem je převádět data do nečitelné podoby a zpět. Kryptografické algoritmy můžeme rozdělit do dvou základních metod. Jedná se o šifrování *symetrické* (tajný klíč) a *asymetrické* (tajný a veřejný klíč).

Symetrické šifrování využívá pouze jeden klíč, který slouží pro šifrování i dešifrování zprávy. Tento šifrovací klíč zná pouze odesílatel a příjemce. Hlavní výhodou symetrických algoritmu je jejich rychlost. Nevýhodou symetrických šifer je nutnost odesílatele i příjemce se domluvit na jednom tajném klíči. Mezi symetrické

[73] HANÁČEK, Petr. *Bezpečnostní funkce v počítačových sítích*[online]. Ústav výpočetní techniky Masarykova univerzita 14.11.2011 [citováno 26. 03. 2014]. Dostupné z: http://www.ics.muni.cz/bulletin/articles/171.html

šifry patří DES (Data Encryption Standard), AES (Advanced Encryption Standard), Blowfish, CAST, IDEA, MARS, RC4, RC5, RC6, Skipjack, Twofish.

Asymetrické šifrování využívá dvou klíčů pro každého uživatele, které jsou složeny z veřejného a soukromého klíče. Princip spočívá v tom, že k zašifrování zprávy se použije veřejný klíč a naopak k dešifrování zprávy je použit soukromý klíč. Veřejný klíč není tedy nutné tajit a v podstatě bude znám širokému okolí, aniž by byla ohrožena bezpečnost zprávy. Naopak soukromý klíč klade důraz na své zabezpečení a je udržován v lokálním systému. Hlavní výhodou asymetrické kryptografie je jednoduší distribuce veřejného klíče. Při použití asymetrických klíčů může být komunikace veřejných klíčů zachycena třetí osobou, kde dochází k podvrhu veřejného klíče. Třetí osoba zachytává šifrované zprávy a odpovědi, vše je dešifrováno a znovu zašifrováno, aby se zamezilo podezření. Takovému útoku se dá předejít, pokud veřejný klíč využívá certifikační autority a v podstatě se jedná o poskytnutí digitálního certifikátu uživatelům. Mezi asymetrické šifry patří RSA (iniciály autorů Rivest, Shamir, Adleman), ElGamal, Diffie-Hellman, DSA (Digital Signature Algorithm).[74]

3.2 Typy bezpečnostních útoků

K prolomení a nalezení zranitelných míst v počítačovém systému či podnikové sítě slouží různé techniky a metody, jejichž záměrem je zneužití systému ke shromažďování a získávání důležitých informací, které jsou k útoku potřebné. Narušení bezpečnosti sítě můžeme rozdělit na hrozby, které mohou přicházet od nezkušených jednotlivců provádějících své útoky pomocí různých nástrojů a to většinou z důvodu vyzkoušení si svých schopností. Dále tu jsou zkušení hackeři, kteří své útoky provádějí cíleně s jistým úmyslem, anebo mohou být najímány např. organizovaným zločinem či různými konkurenčními firmami atd. Tyto hrozby mohou být *externí*, kdy se zpravidla dostávají do vnitřní sítě z internetu, nebo

[74] *Asymetrická kryptografie*[online]. Wikipedie[citováno 10. 05. 2014]. Dostupné z: http://cs.wikipedia.org/wiki/Asymetrick%C3%A1_kryptografie

z vytáčených přístupových serverů bez přístupových práv a *interní*, kdy k nabourání sítě dochází zpravidla od jednotlivců, majících přístupová práva do vnitřní sítě.

Mezi nejčastější metody k prolomení bezpečnosti patří:

- **Odposlech sítě** – jedná se o odposlouchávání provozu sítě a pomocí vhodného softwaru například (Packet Sniffer, IP Sniffer) může útočník sledovat veškeré pakety procházející odposlouchávané sítě. Cílem takovéhoto útoku je zjištění síťového vzorku za účelem analýzy, nebo odcizení informací. Příkladem může být zachycení paketů TCP/IP, jelikož většina provozu není šifrována a útočník z něj může vyčíst uživatelská jména a hesla.
- **Útoky na přístupová hesla** – heslo je základním prvkem autentizace a tak dodržování bezpečnostních zásad by mělo být samozřejmostí. Heslo lze odhalit několika způsoby a to například uhodnutím či odkoukáním hesla, anebo využitím softwarových utilit, které mohou být nainstalovány např. pomocí trojského koně. Spuštěním takového programu, dochází k monitorování klávesnice uživatele.[75]
- **Zranitelná místa v programech** – jde o princip využívání programových chyb v různých aplikacích. Proto je velmi důležité aktualizovat nejnovější záplaty k jednotlivým programům a operačním systémům.
- **Útoky odmítnutím služby** – tento způsob útoku není určen k nabourání se do počítačové sítě, ale má způsobit nedostupnost jedné či více nabízených služeb. Nejčastějším příkladem jsou útoky typu zahlcení, kdy běžící server s danou službou je zahlcen požadavky tak, že není schopen reagovat. Tento útok může být uplatněn jak na vnitřního uživatele, nebo na zahlcení přístupu do podnikové intranetové sítě.
- **Manipulace s daty** – jedná se o princip zachytávání dat v komunikačním kanálu, která se mohou pozměnit, nebo znovu poslat. Útočník se takto může dostat doprostřed běžící relace mezi dvěma stanicemi TCP/IP. Tento způsob je využíván k prolomení šifrované komunikace.
- **Falšování adresy IP** – jde o metodu, kdy útočník podvrhne IP adresu a tím napodobí totožnost určitého hostitele. Může tak získat přístupová oprávnění.

[75] PUŽMANOVÁ, Rita. Širokopásmový Internet Přístupové a domácí sítě. 1.vyd. Brno: Computer Press, 2004, 377 s. ISBN 80-251-0139-8.

Tímto způsobem lze i za určitých okolností obejít autentizační mechanismy.[76]

- **Útoky pomocí malware** – *vir* je zlomyslný softwarový kód, který se připojí k jiným programům a dochází k nekontrolovanému šíření bez vědomí uživatele.

  Trojský kůň je program, který po svém spuštění může vykonávat i destrukční činnost ve formě smazaných souborů, či nainstaluje jiný program, ale sám o sobě se nešíří.

  Backdoor v systému vytváří zadní vchod do systému, kterého může využít případný útočník.

  Spyware je v podstatě program, který shromažďuje různé informace o uživatelích.

  Adware jsou v podstatě reklamní okna.

  Hoaxem jde o poplašné zprávy a většinou se nejedná o škodlivé programy.

  Phishing je metoda, která se využívá ke krádeži identity, hesel, atd., doručena je většinou pomocí nevyžádané pošty.

3.3 Internet a bezpečnost podnikové sítě

Internetová síť je složena z mnoha různorodých propojených sítí a proto je správné zabezpečení naprosto základním prvkem každé podnikové sítě, která chce svoji privátní síť propojit s veřejnou sítí. Aby bylo možné zachovat bezpečnost privátní sítě, je nutné vytvořit zabezpečenou oblast. Hlavním prostředkem k oddělení sítě je **firewall**.

„*Podle slovníku pojmů Dictionary of Internetworking Terms and Acronyms od vydavatelství Cisco Press je firewall definován jako směrovač nebo přístupový server, případně několik směrovačů nebo přístupových serverů, které jsou určeny*

[76] WENSTROM, Michael. *Zabezpečení sítí Cisco*. 1.vyd. Brno: Computer Press, 2003, 784 s. ISBN 80-7226-952-6.

jako nárazníkové zařízení mezi veřejnou sítí a privátní sítí. Firewallový směrovač zajišťuje bezpečnost privátní sítě pomocí přístupových seznamů a jiných metod.“[77]

3.3.1 Firewall

Firewall je ochranný systém sloužící k oddělení dvou nebo více sítí a chrání tak před útoky z vnější sítě. Jedná se o to, že síťová komunikace prochází přes jakýsi kontrolní bod mezi vnější a vnitřní sítí, kde monitoruje a filtruje probíhající procesy podle přísných pravidel komunikace.

Firewally můžeme rozdělit na *softwarový* a *hardwarový*, přesto splňují základní vlastnosti a to takové, že veškerý síťový provoz z vnitřní sítě do venkovní a naopak musí projít kontrolním bodem. Dále zabezpečí, že průchod firewallem má povolený jen oprávněný provoz a samotný firewall je zabezpečen proti proniknutí a vše se chová tak, že vnitřní síť je skrytá před vnějším světem.[78]

Správné využití služeb a funkce firewallů můžeme rozdělit do následujících kategorií:

- paketový filtr,
- aplikační brána,
- brána na úrovni okruhu,
- proxy server,

Paketový filtr patří mezi nejjednodušší typy firewallu pracující na úrovni síťové nebo transportní vrstvy. Princip spočívá v tom, že má nadefinovaný seznam pravidel (*Access listy*), kde uvádějí, která IP adresa smí komunikovat s jinou IP adresou a na jakém portu. Na základě vyhodnocení údajů z IP hlavičky povolí nebo zakáže komunikaci. Výhodou tohoto firewallu je jeho rychlost zpracování a nenáročnost hardwarového výkonu.[79]

---

[77] CHAPMAN JR., David W., FOX, Andy. *Zabezpečení sítí pomocí Cisco PIX Firewall*. 1.vyd. Brno: Computer Press, 2004, 368 s. ISBN 80-722-6963-1.
[78] WENSTROM, Michael. *Zabezpečení sítí Cisco*. 1.vyd. Brno: Computer Press, 2003, 784 s. ISBN 80-7226-952-6.
[79] CHAPMAN JR., David W., FOX, Andy. *Zabezpečení sítí pomocí Cisco PIX Firewall*. 1.vyd. Brno: Computer Press, 2004, 368 s. ISBN 80-722-6963-1.

Aplikační brána kontroluje všechny procházející pakety pro dané aplikace a tato kontrola probíhá na aplikační vrstvě. Princip spočívá v tom, že uživatelské aplikace nekomunikují přímo se skutečným cílovým počítačem, ale komunikace nejprve probíhá s aplikačním firewallem. Teprve tento firewall předává komunikaci dále cílovým počítačům. Aplikační firewall tedy řídí a kontroluje spojení, ve kterém zabraňuje přenosu nepovolených dat.[80]

Brána na úrovni okruhu povoluje průchod jen platným paketům a před otevřením okruhu přes tento firewall se kontrolují relace TCP a UDP. Tento firewall si udržuje tabulku platných relačních spojení, na kterých je povolen přenos dat. Pokud souhlasí s danou tabulkou a to až do ukončení dané relace, daná položka se v tabulce odstraní a okruh se uzavře.

Proxy server - jejich funkci dnes obsahuje většina aplikačních bran. Proxy filtr zkoumá pakety ve vyšších vrstvách a princip spočívá v tom, že vnitřní sítě se k vnějším službám připojují přes aplikační proxy programy, které jsou spuštěny na daném firewallu.[81]

Všeobecné výhody firewallu:

- Oddělením vnitřní sítě od vnější se stává firewall viditelným pro vnější síť a úplně skryje síť lokální.
- Komunikace mezi vnější a vnitřní sítí je povolena pouze oprávněným uživatelům se správnou identifikací a autentizací.
- Překlad adres NAT (Network Address Translation).
- Kontroluje data, která přes něj procházejí.

Všeobecné nevýhody firewallu:

- Firewall je ochranou proti útokům z vnější sítě, pokud uživatel nevytvoří alternativní cestu mimo firewall.
- Nezabrání zničení dat při přenosu po síti.
- Nechrání před útoky prostřednictvím pošty, www atd.

[80] WENSTROM, Michael. *Zabezpečení sítí Cisco*. 1.vyd. Brno: Computer Press, 2003, 784 s. ISBN 80-7226-952-6.
[81] WENSTROM, Michael. *Zabezpečení sítí Cisco*. 1.vyd. Brno: Computer Press, 2003, 784 s. ISBN 80-7226-952-6.

3.3.2 Demilitarizovaná zóna – DMZ

Demilitarizována zóna je izolovaná vnitřní LAN síť, která je dostupná i pro uživatele z vnější sítě. Pro vytvoření demilitarizované zóny se využívají firewally, které musí obsahovat konfiguraci pro přístup do DMZ. Vytvořením oddělené zóny se mohou zpřístupnit určité služby vnějším uživatelům, které jsou ve vymezené oblasti zabezpečené a kontrolované. Princip spočívá v tom, že v DMZ zóně můžeme definovat pravidla tak, abychom určili, které počítače z vnitřní sítě mohou komunikovat s počítači v DMZ zóně a dokonce i na kterých portech. Dále určujeme pravidla, na kterých portech se může komunikovat z vnější sítě do DMZ.[82]

3.3.3 VPN (Virtual Private Network)

Virtuální privátní síť lze popsat jako zašifrovaný tunel mezi dvěma důvěryhodnými uzly přes nezabezpečenou síť. Prostřednictvím VPN lze zajistit vzájemný přístup firemních vzdálených pracovišť, která může provozovat po běžném veřejném internetu nebo prostřednictvím jakéhokoliv poskytovatele internetových služeb. Při navazování spojení VPN zajišťuje Autentizaci pro ověření identity komunikujících stran s využitím šifrovaného zabezpečeného spojení tak, aby přenášená informace zůstala důvěrná a privátní, při zachování integrity dat. Můžeme říci, že se jedná o rozšířené zabezpečení podnikové sítě tak, aby mohla poskytovat vnitropodnikové služby i vzdáleným oprávněným uživatelům, kterými mohou být například zaměstnanci pracující jako home office, vzdálené pobočky anebo zaměstnanci na služebních cestách.[83]

V síťové architektuře existují různé typy VPN technologií, které pracují na různých vrstvách síťového modelu. Typy protokolů v síťovém modelu jsou:

[82] CHAPMAN JR., David W., FOX, Andy. *Zabezpečení sítí pomocí Cisco PIX Firewall*. 1.vyd. Brno: Computer Press, 2004, 368 s. ISBN 80-722-6963-1.
[83] VELTE, Toby J, VELTE, Anthony T. *Síťové technologie Cisco*. 1.vyd. Brno: Computer Press, 2003, 800 s. ISBN 80-7226-857-0.

- **PPTP** (Point-to-Point Tunneling Protocol) a **L2TP** (Layer Two Tunneling Protocol) – jsou protokoly tunelového propojení, které pracují na druhé vrstvě síťového modelu.
- **IPsec** - je protokol, který pracuje na třetí vrstvě síťového modelu. Jde o doplněk zabezpečení protokolu IP, kde se pouze šifrují data protokolu IP.
- **VPN SSL** – je protokol, který pracuje na čtvrté vrstvě síťového modelu, jehož funkcí je umožnit zabezpečený přístup přes konkrétní port pomocí webového prohlížeče.[84]

[84] KRSIČKA, Daniel. *Technologie SSL VPN jejich řešení firmou Cisco Systems* [online]. 15.1.2006[citováno 16. 05. 2014]. Dostupné z: http://www.cs.vsb.cz/grygarek/TPS/projekty/0506Z/krs008_TPS_projekt.pdf

4 Teorie

V předchozích kapitolách jsem v kostce vysvětlil důležité části počítačové sítě jako takové a základní pojmy týkající se zabezpečení počítačové sítě. Jelikož součástí této práce je propojení vzdálené stanice přes negarantovaný Internet a technologie šifrovaných tunelů, budu se v této části kapitoly zabývat teoretickým popisem, zabývajícím se technickým řešením a připojením vzdálené pobočky přes širokopásmový Internet typu ADSL.

4.1 Širokopásmový Internet

Technologie digitálních účastnických linek xDSL (Digital Subscriber, Line) jsou určeny pro poskytování širokopásmových služeb a obecně můžeme říci, že slouží pro přenos velkých objemů dat s vysokou rychlostí, podporující více digitálních služeb najednou. U takovéhoto připojení pak požadujeme obousměrnou komunikaci a rychlost v Mbps ve směru k uživateli (downstream) a ve směru od uživatele (upstream) se rychlost pohybuje již od kbps. Přenos dat je uskutečněn prostřednictvím modemů mezi uživatelem a telefonní ústřednou s využitím účastnického vedení, které bylo původně určeno pro přenos telefonní stanice v kmitočtovém pásmu v rozsahu 300 až 3400 Hz. Technologie xDSL využívají mnohem širší kmitočtové pásmo v účastnickém vedení a tím je umožněno poskytování širokého spektra digitálních služeb.[85]

Technologie xDSL můžeme rozdělit do těchto základních skupin:

- **ADSL** (Asymmetric DSL) – asymetrická digitální přípojka, která bude podrobněji vysvětlena v následující kapitole.
- **HDSL** (High-bit-rate DSL) – vysokorychlostní digitální přípojka, která využívá vyrovnanou kapacitu v obou směrech. Jedná se o symetrické využití přenosového pásma s rychlostí do 2048 Mbit/s s označením E1.

[85] PUŽMANOVÁ, Rita. *Širokopásmový Internet Přístupové a domácí sítě*. 1.vyd. Brno: Computer Press, 2004, 377 s. ISBN 80-251-0139-8.

- **SDSL** (Symmetric DSL) – jedná se o symetrickou digitální přípojku.
- **VDSL** (Very-high-bit-rate DSL) – jedná se o velmi vysokou přenosovou rychlost nabízející asymetrickou variantu přenosového pásma a to až do rychlosti 52Mbit/s ve směru k uživateli a do 2,3Mbit/s ve směru od uživatele. Tato digitální přípojka umí i symetrickou variantu přenosového pásma a to až do rychlosti 36Mbit/s v obou směrech.

Služba přes širokopásmovou přípojku může zahrnovat tyto atributy:

- Různé možnosti způsobu přenosu dané služby. Možným způsobem přenosu je například – (okruhový, asynchronní a paketový přenosový mód).
- Typ přenášených informaci charakterizuje, o jaké přenášené informace se jedná, a můžeme rozlišovat různé typy těchto informací – (hovorové, obrazové, zvukové, textové a datové informace).
- Sestavení spojení popisuje, jakým způsobem je sestaveno spojení, zdali se jedná o *pevné* či o spojení vystavené *na požádání*.
- Symetrie charakterizuje způsob toku informací mezi uživatelem a sítí Internet. Informace přenášena v obou směrech se stejnou rychlostí znamená, že se jedná o *symetrický* přenos. Informace přenášena v obou směrech, ale s rozdílnou rychlostí znamená, že se jedná o *asymetrický* přenos.
- Přenosová rychlost udává hodnotu, kterou má uživatel k dispozici pro přenos informací.
- Agregace je koeficient, který nám udává hodnotu, kolik účastníků sdílí společný datový tok.
- Typ IP adresy popisuje způsob přidělení. Rozlišujeme *dynamickou* a *statickou* IP adresu.
- Objem přenesených dat v obou směrech může být neomezený, nebo omezený na určitý datový limit tzv. FUP (Fair User Polici). Po překročení datového limitu obvykle dochází ke snížení přenosové rychlosti.[86]

[86] HRSTKA, Jaroslav. *Vysokorychlostní přístup ke službám elektronických komunikací* [online]. Testcom 2006[citováno 17. 05. 2014]. Dostupné z: http://www.testcom.cz/pdf/vyzkum/Vysokorychlostni_pristup_ke_sluzbam.pdf

Závěrem můžeme říci, že pro tradiční poskytovatele telefonních služeb jsou technologie xDSL zajímavým řešením pro zřízení širokopásmového přístupu k Internetu a s využitím modulačních technik tak mohou nabídnout velké přenosové kapacity potenciálním uživatelům. Nevýhodou nasazení xDSL je závislost na délce a kvalitě účastnického vedení od veřejné telefonní ústředny ke koncovému zákazníkovi.

*„**Normalizací xDSL** se zabývá ITU-T, ANSI a ETSI. Nezanedbatelnou roli v podpoře rozvoje xDSL ve světě hraje průmyslové sdružení **DSL Forum** (založené v roce 1994, tehdy ještě jako **ADSL Forum**).“*[87]

4.1.1 ADSL (Asymmetric Digital Subscriber Line)

Technologii přenosového prostředí ADSL jsem využil k provedení testů a ověření technologie zabezpečených tunelů vzdáleného pracoviště. Od ověření technologií s využitím kvalitnějšího připojení například VDSL či Internet s garantovanou šířkou pásma a dostupností bylo s ohledem na organizační, finanční i časové nároky testů upuštěno.

ADSL - jedná se o vysokorychlostní připojení k Internetu po telefonní lince neboli účastnickém vedení a může být provozována společně s telefonní přípojkou nebo ISDN linkou. Pro datový přenos ADSL využívá jinou šířku pásma a to nad 4000Hz. K oddělení signálu od hovorové části pásma se využívá tzv. rozbočovače – (splitter) na straně účastníka i na straně místní ústředny. Přenosová rychlost směrem k uživateli (downstream) může být až 8448 Mbit/s a rychlost směrem od uživatele (upstream) do 1,5 Mbit/s. Koncová část uživatele je složena z *rozbočovače* a *ADSL modemu*.

Rozbočovač je zapotřebí na obou koncích vedení, jelikož odděluje data od hlasu. Na straně uživatele jsou použity dva filtry a to pro oddělení telefonních hovorů – *Filtr s dolní propustí pod 3,4kHz* a datového přenosu – *Filtr s horní propustí,* který je

[87] PUŽMANOVÁ, Rita. *Širokopásmový Internet Přístupové a domácí sítě*. 1.vyd. Brno: Computer Press, 2004, 377 s. ISBN 80-251-0139-8.

přiveden do ADSL modemu a modulovaný signál je převeden na datový pro rozhraní LAN.

ADSL modem v sobě sdružuje datovou síť a provádí převod dat na speciální analogový signál, který je možno přenášet v nepoužívaném pásmu – (25kHz až 1,1MHz). Modemy ADSL v sobě mohou zahrnovat funkce směrovače na úrovní třetí vrstvy pro datový provoz, ale i pro hlasové služby. Modemy v sobě mohou obsahovat i funkce WiFi pro rádiový přenos koncových zařízení.

Hlavním nedostatkem ADSL je omezující vzdálenost od telefonní ústředny k zákazníkovi, jelikož vzdálenost má vliv i na poskytovanou šířku pásma. Také míra agregace na páteřní části celého okruhu má vliv na kapacitu ADSL. Jedná se o asymetrický způsob přenosu.

Naopak výhodou technologie ADSL je vyhrazené připojení každého uživatele s trvalým připojením k Internetu s bezpečnou komunikací. Využití může být výhodné pro domácnosti, domácí kanceláře drobných a středních firem.[88]

4.2 Šifrovaný tunel typu - IPsec (AES256)

Předmětem ověřování bylo připojení typu negarantovaný Internet s využitím šifrovaných tunelů typu IPsec (AES256) prostřednictvím technologie Astaro. Šifrovaný tunel umožní bezpečnou komunikaci mezi vzdálenou stanicí a centrální firemní sítí přes širokopásmovou přípojku ADSL. V našem případě je tato zabezpečená síť mezi stanicemi tvořena soustavou IPSec tunelů.

Protokol IPSec je systém otevřených standardů popisujících způsob bezpečného přenosu IP paketů. Standardy slouží k zabezpečení dat na síťové třetí vrstvě a umožňují podporu autentizačních a šifrovacích služeb mezi koncovými body. Specifikace protokolu jsou v dokumentech RFC (Request for Comments) a jsou vyhlašovány ze strany organizace IETF (Internet Engineering Task Force).[89]

IPSec umožňuje pracovat ve dvou režimech a to v *transportním* a *tunelovém* režimu.

---

[88] PUŽMANOVÁ, Rita. *Širokopásmový Internet Přístupové a domácí sítě*. 1.vyd. Brno: Computer Press, 2004, 377 s. ISBN 80-251-0139-8.

[89] WENSTROM, Michael. *Zabezpečení sítí Cisco*. 1.vyd. Brno: Computer Press, 2003, 784 s. ISBN 80-7226-952-6.

Transportní režim je jednodušší varianta protokolu IPSec, jelikož zabezpečuje/šifruje datovou část paketu a vlastní IP hlavička zůstává nezabezpečena/nezašifrována.
Tunelový režim nachází mnohem širší uplatnění, jelikož nejen zabezpečuje/šifruje datovou část paketu, ale i původní IP hlavičku. Z toho vyplývá, že v tomto režimu je zapouzdřen celý paket a před něj je přiřazena nová bezpečnostní hlavička.

4.2.1 Protokoly IPSec

K zajištění služeb bezpečného přenosu v sítích IP slouží soubory protokolů, které zabezpečují autentizaci, šifrování přenášených dat a ochranu informací v hlavičce a to od jednoho koncového zařízení ke druhému. Pro tuto komunikaci je zapotřebí vytvořit jednosměrnou komunikaci, kde toto řešení specifikuje organizace IETF takzvané bezpečnostní asociace. SA (Security Associations) je souhrn dohodnutých parametrů mezi partnery IPSec. Jedná se o to, jakým způsobem dojde k autentizaci, v jakém režimu má IPSec pracovat, jaký bude použit algoritmus a jakým způsobem dojde k obměně klíčů.
IPSec používá tři hlavní protokoly:

- AH (Authentication Header) je protokol, který poskytuje služby autentizace celého paketu. Přenášená data nejsou šifrována, ale nelze je pozměnit. Autentizace slouží k zajištění pravosti komunikace a je ověřena klíčem, který je znám pouze oběma komunikujícím stranám.
- ESP (Encapsulating Security Payload) je protokol, který poskytuje služby šifrování, autentizace jako protokol AH, integrity dat a obsahuje ochranu před opakováním. Šifrování je sjednáno předem dle domluveného algoritmu a je zašifrováno vše kromě IP hlavičky. Používá se v transportním i tunelovém režimu.
- IKE (Internet Key Exchange) je hybridní protokol, který se stará o vlastní výměnu vygenerovaných šifrovacích klíčů mezi komunikujícími stranami. Pro protokol IKE poskytuje strukturu protokol ISAKMP (Internet Security Association and Key Management Protocol), Oakley a SKEME (Secure Key

Exchange Mechanism). Výměna šifrovacích klíčů a bezpečnostní informace mezi stranami si v IKE pomocí ISKMP v první fázi domluví způsob, jak si budou zabezpečené informace vyměňovat. Výsledkem této komunikace je vytvoření ISKMP SA, které je využito ve druhé fázi. V první fázi dochází k dohodě, jaký bude použit šifrovací algoritmus – (DES, AES, 3DES), jaká hešovací funkce – (MD5, SHA) a metoda ověřování – (autentizace). Ve druhé fázi se nastavují již samotné parametry bezpečných kanálů SA protokolu AH, ESP nebo AH+ESP.[90]

DES (Data Encryption Data) je šifrovací algoritmus, kterého je využito pro šifrování a dešifrování dat v paketu. Jedná se o symetrickou šifru s délkou klíče 64 bitů, z toho je 56 bitů efektivních a 8 bitů kontrolních.

3DES (Triple DES) je rozšířenou trojnásobnou variantou šifrovacího algoritmu DES o délce klíče 168 bitů.

MD5 (Message Digest 5) je hašovací algoritmus, který autentizuje data přenášená v paketu. Jedná se o jednosměrný šifrovací algoritmus, který při zpracování dat provede otisk s délkou 128 bitů.

SHA (Secure Hash Algorithm) je hašovací algoritmus, který autentizuje a podepisuje data v paketech. Používá stejné principy jako MD5 a nejpoužívanější verzí je SHA-1, která provádí otisk s délkou 160 bitů.[91]

AES (Advanced Encryption Standard)

AES je nejpoužívanějším příkladem symetrické šifry uznávaný NSA jako šifra vhodná pro utajovaná data USA a je standardem organizace NATO. Americký Národní institut standardů a technologie (NITS) schválil tuto šifru v roce 2001 a vychází z Rijndaelova algoritmu od autorů Joada Daemena a Vincenta Rijmena. Jedná se o blokovou šifru, která k šifrování a dešifrování používá tři velikosti délek

[90] WENSTROM, Michael. *Zabezpečení sítí Cisco*. 1.vyd. Brno: Computer Press, 2003, 784 s. ISBN 80-7226-952-6.

[91] CHAPMAN JR., David W., FOX, Andy. *Zabezpečení sítí pomocí Cisco PIX Firewall*. 1.vyd. Brno: Computer Press, 2004, 368 s. ISBN 80-722-6963-1.

klíčů – (AES-128, AES-192 a AES-256 bitů) a právě délka šifrovacího klíče je důležitým parametrem pro bezpečnost šifrovacího algoritmu.[92]

Závěrem bych dodal, že protokol IPSec poskytuje velmi vysokou úroveň zabezpečení na síťové vrstvě.

4.3 Popis připojení negarantovaného internetu prostřednictvím technologie ASTARO/SOPHOS

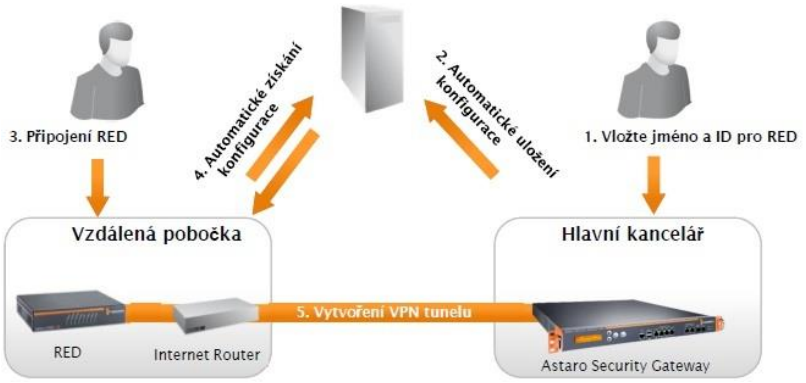
K nalezení levnějšího způsobu připojení vzdálené lokality k centrále při zachování stávající úrovně služeb bylo k ověřování využito technologie Astaro SG+RED zajišťující šifrované tunely typu IPsec (AES256). Technologie Astaro a technická podpora při testování připojení byla poskytnuta společností Annex NET, s.r.o..
Historie společnosti Annex Net, s.r.o. se datuje již od roku 1995 a s rozvojem informačních technologií se začala specializovat na oblast datové komunikační techniky.

*„**Annex NET**, s.r.o. je ryze česká společnost zabývající se dodávkou komplexních služeb v oblasti informačních technologií, zejména pak návrhem a dodávkou systémů pro řešení bezpečných komunikačních sítí, IP telefonie a síťového managementu.“*[93]

Astaro SG+RED představuje jednoduchý a zároveň cenově dostupný způsob zabezpečení vzdálené pobočky a to během několika minut a bez nutnosti jakýchkoli technických znalostí na pobočce. Produkt integruje funkcionalitu VPN a komplexní bezpečnostní řešení. **Astaro RED** 1O funguje jako vzdálená jednotka systému Astaro Security Gateway (ASG) a nevyžaduje žádnou konfiguraci v místě instalace.

[92] STANEK, Martin. *Kryptológia Pragmatický pohľad*[online]. Katedra informatiky Fakulta matematiky, fyziky a informatiky Univerzity Komenského, Bratislava, Slovensko 02.2014 [citováno 30. 05. 2014]. Dostupné z: http://www.dcs.fmph.uniba.sk/~stanek/Kryptologia%20v1c.pdf
[93] *O NÁS*[online]. ANNEX NET [citováno 31. 05. 2014]. Dostupné z: http://annexnet.cz/o-nas-zakladni-informace

Po připojení k internetu se jednotka sama zaregistruje k centrální bráně ASG a propojí pobočku s centrálou pomocí VPN tunelu. Jak funguje Astaro RED demonstruje následující obrázek.



Obr. 16 - Vytvoření VPN tunelu.

Technický popis Astaro RED 10:

- Pevný metalický korpus,
- 1 WAN port,
- 4 x LAN port switch,
- >30 Mbit/s VPN propustnost,
- <7Watt příkon,
- neomezený počet uživatelů.

Obr. 17 - Astaro RED 10

Centrální zařízení **Astaro SG** zajišťuje centrální konfiguraci pro všechny RED zařízení a centrální DNS a DHCP. Určuje jednotnou bezpečnostní politiku pro všechny vzdálené pobočky včetně detailních reportů jednotlivých vzdálených poboček a to bez nutnosti dalšího zvláštního reportovacího zařízení.

„Společnost Astaro, v současné době Sophos company, byla založena roku 2000 a má své centrály ve městě Wilmington, stát Massachusetts, USA a také německém Karlsruhe.“[94]

V závěrečném popisu produktu Astaro nyní SOPHOS můžeme říci, že toto zařízení nabízí nový standard v zabezpečení vzdálených poboček. Podstatně eliminuje investici do drahého hardwaru a tím významně snižuje náklady na připojení a údržbu vzdálených lokalit.

4.3.1 Popis testovaného spojení

Připojení vzdálené lokality do centrály prostřednictvím negarantovaného přenosového prostředí bylo řešeno pomocí asymetrického připojení službou veřejného Internetu přes xDSL s přenosovou rychlostí směrem k uživateli (downstream) 8Mbps a směrem od uživatele (upstream) 512kbps.

Specifikace typu ověřovaného připojení Astaro SG+RED:

- **Security Gateway** (SG) se instaluje v centrálním komunikačním uzlu a zajišťuje kompletní sadu bezpečnostních aplikací, mezi něž patří firewall, VPN, IPS a antivirus.
- Koncové zařízení **Remote Ethernet Device** (RED) se umisťuje na straně vzdálené lokality a zajišťuje aplikaci centrálně nastavených parametrů a bezpečnostních politik.
- Z hlediska bezpečnosti jsou technologie komunikace pomocí šifrovaných tunelů IPsec algoritmem AES256 standardem organizace NATO. V prostředí ČR je technologie Astaro několik let rutinně využívána finančními institucemi, což lze doložit ze strany dodavatele referencemi.
- Z bezpečnostního hlediska nepracuje S-GW jako router, který směruje datový tok do všech směrů, které nejsou explicitně zakázány. S-GW se chová jako

[94] *SOPHOS | SOPHOS komplexní zabezpečení Vaší sítě*[online]. ANNEX NET [citováno 06. 06. 2014]. Dostupné z: http://annexnet.cz/sophos-zakladni-informace/

firewall, který propouští datové toky s patřičnými parametry jen, pokud jsou tyto explicitně povoleny a ostatní provoz S-GW nepropustí. To je další aspekt, který zlepšuje bezpečnostní parametry komunikace přes veřejné komunikační prostředí.

- Technologie Astaro umožňuje prioritizaci datových toků uvnitř vytvořeného tunelu. Jelikož máme dodržet stávající služby, bude této prioritizace využito při testech pro upřednostnění hlasového provozu. Původní připojení vzdálené pobočky do centra je umožněno za pomocí technologie Vanguard /Frame Relay zajišťující datové a hlasové služby.

5 Praktické testování připojení typu negarantovaný internet s využitím šifrovaných tunelů typu IPsec (AES256) prostřednictvím technologie Astaro/Sophos.

V praktické části diplomové práce probíhalo ověření připojení vzdálené stanice s centrálním uzlem. K zachování stávajících služeb a v maximální míře využití stávající technologií bylo testováno několik variant připojení jak z datového tak z hlasového hlediska provozu. Aby bylo možno otestovat několik variant, byly navíc firmou Annexnet zapůjčeny dvě IP ústředny - Innovaphone (IP305+IP24) a IP telefon (IP110).

5.1 Typy ověřovaných zapojení z hlediska datového provozu

Varianta - L2–RED + router

Vzdálená stanice je navázána z hlediska datové i hlasové sítě po L2 vrstvě a to formou příslušných VLAN pro data a hlas. Koncový router je navázán do podnikové sítě pomocí *multivrf* nebo *plného MPLS (Multiprotocol Label Switching)*[95].

V režimu *multivrf* jde o sadu datových VLAN, které jsou určeny neboli příslušející dané vzdálené pobočce.

V případě režimu *plného MPLS* jde o jednu datovou VLAN, která přísluší dané vzdálené stanici.

Brána pro koncová PC je poskytována místně a Astaro je v tzv. „bridgovaném módu“[96]. Při větším množství připojených vzdálených poboček je potřeba, aby každá vzdálená stanice byla připojena svou vlastní sadou datových VLAN.

[95] Je standardizovaná technologie určená ke zrychlování toku síťového provozu.
[96] Na základě cílové MAC adresy dokáže vybrat odchozí rozhranní, přes které data přepošle.

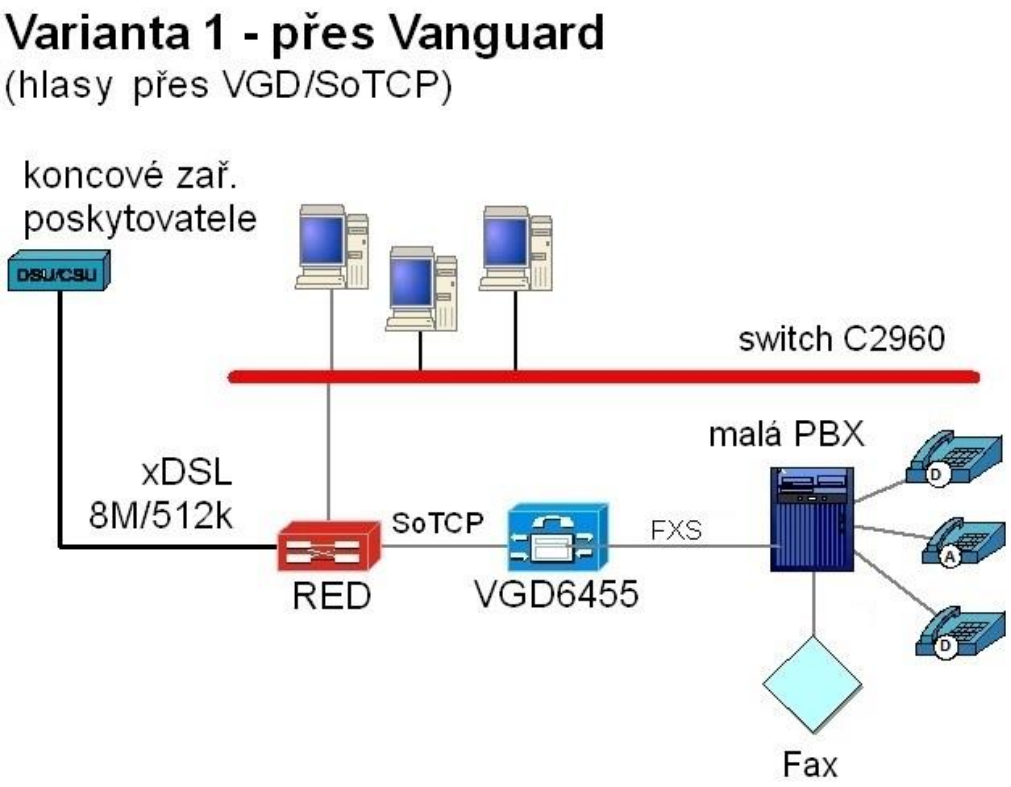
Varianta - L3–RED gateway

Vzdálená stanice je navázána z hlediska datové i hlasové sítě po L3 vrstvě. RED zajišťuje bránu pro místní LAN segment a pro hlasový provoz. Astaro je v tzv. „routovaném módu“. Poskytované sítě formou VLAN se šíří jen do příslušné vzdálené stanice. Tato varianta je vhodnější pro připojení malých vzdálených stanic a byla ověřena v reálném provozu.

5.2 Typy ověřovaných zapojení z hlediska hlasového provozu

Varianta 1 - Hlasy přes Vanguard/SoTCP

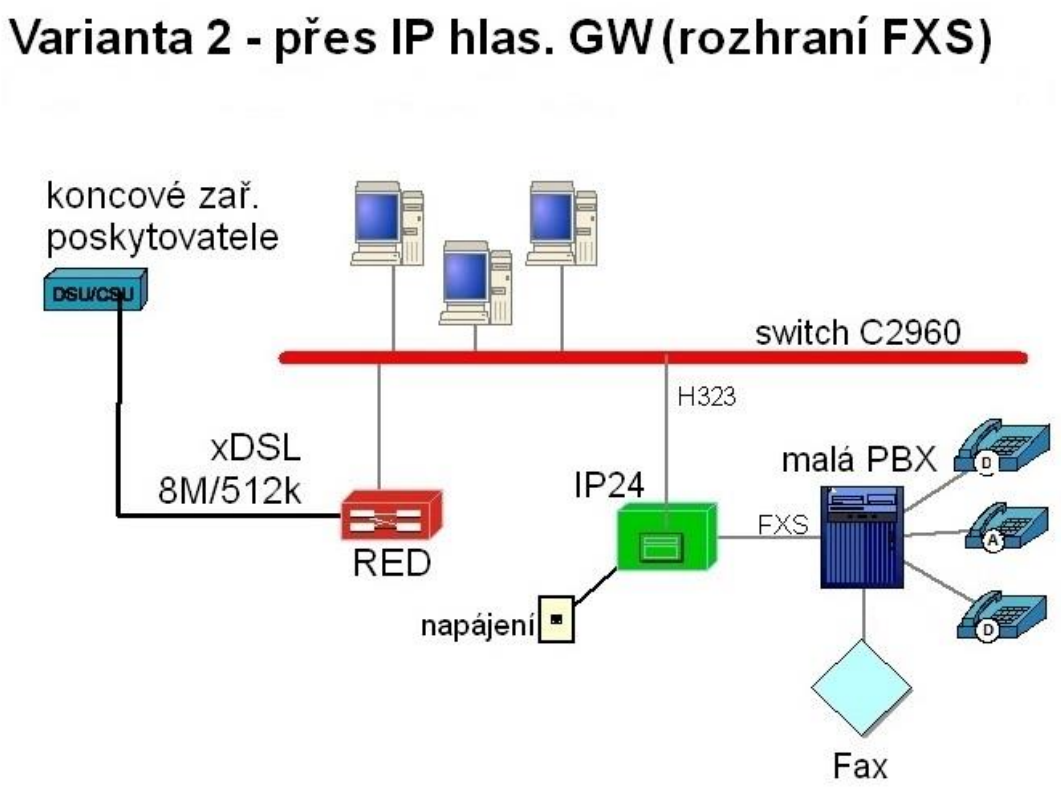
Zapojení hlasového provozu využívá stávající zařízení Vanguard6455 navázané protokolem SoTCP a prostředím Ethernet na Vanguard7310 v centrální lokalitě. Vanguard7310 je napojena trunkem E1 do krajské PBX Alcatel typu 4400. Vanguard6455 ve vzdálené lokalitě poskytuje funkci hlasové brány pro malou pobočkovou ústřednu typu Panasonic KXT6/16 s připojenými telefony a faxem. Hlasové propojení mezi zařízením Vanguard a pobočkovou ústřednou zůstalo v původním zapojení a je realizováno přes analogové porty typu FXS a vstupními porty CO ve stávající pobočkové ústředně. Z obrázku č. 17 je patrné, že hlasová technologie zůstala v původním zapojení, což by v budoucnu vedlo k migraci zapojení sítě do prostředí Ethernet a to by minimalizovalo náklady na obnovu technologie nebo alespoň oddálilo kompletní obměnu celé technologie. Vzhledem ke změně typu prostředí z Frame Relay na prostředí Ethernet bylo nutné provést pouze změnu v konfiguraci zařízení Vanguard 6455.



Obr. 18 – HlaspřesVanguard SoTCP

Varianta 2 - Hlasy přes IP a H.323

Zapojení je založeno na hlasové IP technologii Innovaphone s využitím zařízení IP24, které obsahuje 4 porty FXS a podobně jako Vanguard poskytuje funkci hlasové brány pro malou místní pobočkovou ústřednu s připojenými telefony a faxem, jak je patrné z obrázku č. 18. V zapojení je využita i IP305, na kterou je zaregistrován testovací IP telefon IP110. V testované konfiguraci je IP24 i IP305 navázána pomocí protokolu H.323 na centrální IP6000, která je napojena trunkem E1 do krajské PBX Alcatel typu 4400. Pro návaznost do rezortní hlasové sítě je možné i v tomto případě využít stávající centrální zařízení Vanguard a protokol H.323. Tento způsob připojení se neosvědčil z důvodu nefunkčního přenosu faxového provozu.



Obr. 19 – Hlas přes IP PBX

IP technologie Innovaphone – (IP24, IP305 a IP110) byla poskytnuta spolu s technickou podporou společností Annex NET, s.r.o..

Produkty Innovaphone slouží k implementaci IP telefonie a k sestavení IP telefonního systému.

IP telefony se podobají klasickým telefonům. Umožňují uživateli spojit se s ostatními uživateli. Vezmou hlas, přemění ho na IP datový tok a odešlou ho k cíli, kde je opět datový tok přeměněn zpět na hlas.

Úkolem **brány** je převést IP datový tok, který přenáší hlas a signalizační data na fyzické médium určitého typu a naopak. Jako příklad pro použití brány je připojení k PSTN. Brána může nabízet i služby pobočkové ústředny (PBX). Oproti tomu adaptér slouží k připojení analogových zařízení, ale nemůže sloužit jako PBX.

Pokud se IP telefon pokouší sestavit hovor, je třeba určit, kde se nachází cíl. Jestliže volaný účastník je IP telefon, který je součástí stejného systému, je nutné znát jeho IP adresu. Pokud se volaný účastník nachází v externí síti (např. PSTN) musí být identifikována správná brána, které se předá hovor. Aby ústředna mohla řídit

jednotlivé hovory, musí znát všechny telefony a brány. Proto musí být telefony a brány zaregistrovány.

PBX – ústředna není zařízení, ale je to software, který je přítomný na většině bran a je aktivován správnou licencí. Všechna Innovaphone zařízení podporují H.323 a SIP protokoly.

Popis použitých produktů Innovaphone:

- **IP6000** - je jednou z VoIP bran v produktové řadě innovaphone s rozhraním ISDN PRI. IP6000 Gateway funguje jako prostředník mezi tradiční telefonní sítí a světem IP telefonie (SIP/H.323). Na straně telefonní sítě ji lze připojit až dvěma PRI porty. Licenční model Innovaphone umožňuje použití pouze nezbytného počtu portu a hovorových kanálů tak, aby bylo dosaženo maximální úspory pořizovacích nákladu i efektivního využití ISDN připojení. Jednotka samotná je optimalizována pro stabilní, bezpečný, dlouhodobý a bezporuchový provoz i v náročných provozních podmínkách. Z tohoto důvodu neobsahuje žádné pohyblivé součásti a její operační systém je primárně navržen a optimalizován pro telefonní provoz. Operační systém je kompletně vyvíjen společností Innovaphone a neobsahuje žádné standardní komponenty systému.
- **IP305 –** pomocí této VoIP gateway brány s rozhraním ISDN BRI můžeme propojit klasickou telefonní sít (PSTN) se světem IP telefonie, ale zároveň může být použita i jako Innovaphone VoIP PBX s kapacitou do 50 registrovaných uživatelů. Rozhraní IP305 se skládá ze dvou ISDN BRI portů a dvou Ethernet portů, které můžeme připojit do dvou oddělených sítí. Gateway může mezi sítěmi směrovat datový provoz anebo do oddělených sítí směrovat telefonní volání a to k různým VoIP poskytovatelům. Nevyužitý Ethernet port může sloužit i k pouze k administraci systému.[97]
- **IP24 –** tento VoIP adaptér v sobě skrývá čtyři analogové porty typu FXS, které slouží k připojení jakýchkoliv standardních analogových zařízení. Pomocí tohoto adaptéru propojíme standardní analogové zařízení s prostředím VoIP včetně innovaphone PBX. Všechny analogové porty

[97] *IP305*[online]. ANNEX NET [citováno 20. 06. 2014]. Dostupné z: http://www.annexnet.cz/innovaphone-voip-brany-ip305/

podporují protokol T.38, což je standard ITU pro spolehlivý přenos faxu v IP síti. Adaptér IP24 můžeme napájet pomocí externího zdroje nebo prostřednictvím Ethernet portu, který splňuje standard PoE.[98]

- **IP110 -** Tento IP přístroj je základní řadou společností Innovaphone a podporuje protokoly SIP i H323. Přístroj je vybaven sedmiřádkovým displejem, na kterém můžeme vidět veškeré stavy telefonu a zároveň umožňuje snadnou a rychlou orientaci při jeho obsluze. V této základní řadě se nacházejí čtyři programovatelná funkční tlačítka se světelnou signalizací, které můžeme použít pro rychlou volbu nebo pro přímý vstup k některým funkcím Innovaphone PBX. Přístroj patří k oblíbeným modelům a to převážně díky své spolehlivosti.[99]

H.323 (Packet-based multimedia communications systems) zastřešuje celou skupinu protokolů určených pro přenos nejen hlasu, ale také multimediálních dat v celé jejich šíři a je definovaný Mezinárodní telekomunikační unií (ITU). Protokol H.323 rozlišuje tyto komponenty:

- **Terminál** – obvykle HW nebo SW telefon, za speciální případ terminálu lze považovat i např. systém hlasové pošty
- **Brána** (Gateway) – zařízení, které umožňuje obousměrnou komunikaci se zařízeními v jiné komunikační síti (např. ISDN, analogová tlf. síť, jiná H.323 síť). Brána formálně sestává z "Media Gateway Controller" (MGC, obsluha hovorové signalizace) a "Media Gateway" (MG, směrování audio/video proudů). MGC a MG tvoří obvykle jedno fyzické zařízení, v opačném případě se hovoří o tzv. dekomponované bráně.
- **Konferenční jednotka** (MCU) – opět se formálně dělí na Multipoint Controller (MC, obsluha hovorové signalizace během konference) a Multipoint Processor (MP, obsluha multimediálních kanálů, mixování audia, atd.)

[98] *IP24*[online]. ANNEX NET [citováno 21. 06. 2014]. Dostupné z: http://www.annexnet.cz/innovaphone-produkty-ip24/
[99] *IP110*[online]. ANNEX NET [citováno 21. 06. 2014]. Dostupné z: http://www.annexnet.cz/innovaphone-voip-telefony-ip110/

- **Gatekeeper** – volitelná entita, která poskytuje služby překladu adres a řízení provozu v H.323 síti.

Standard H.323 je často kritizován za svou nedokonalost, složitost a velikost. I když H.323 není zcela optimální, přesto se hodí pro komunikaci mezi VoIP branami.[100]

5.3 Ověření v podmínkách testovacího zapojení mimo reálný provoz

Ověřování probíhalo nejprve v podmínkách testovacího zapojení mimo reálný provoz. Bylo zapotřebí vyzkoušet veškeré varianty zapojení a tím eliminovat případnou chybovost při zapojování technologie. Tím se vyloučily možné nežádoucí výpadky reálného provozu.
Specifikace připojení je následující:

- Astaro RED je připojen do Internetu přes xDSL linku 8Mbps/512kbps.
- Ověřeny jsou všechny varianty dle bodu 5.1.
- Všechny varianty jsou funkční, nicméně byl patrný vliv negarantovaného připojení, které vykazovalo během času kolísající ztrátovost paketů v jednotkách procent.
- Ověření funkčnosti faxů bylo provedeno dvěma způsoby a to tak, že faxový přístroj byl nejprve zapojený do koncového zařízení Vanguard6455 přes analogovou kartu FXS. Vanguard6455 komunikoval s centrálním zařízenímVanguard7310 pomocí protokolu SoTCP. Druhým způsobem zapojení se testoval faxový provoz přes zapůjčené zařízení Innovaphone IP24. Fax byl zapojený na koncovou VoIP bránu IP ústředny Innovaphone IP24 přes čtyřportovou analogovou kartu FXS, komunikující s IP ústřednou Innovaphone IP6000 v centru pomocí protokolu H.323. Obě ověření funkčnosti faxového provozu proběhla bez závad.

[100] PETERKA, Jiří. *Architektura H.323 verze 1*[online]. eArhiv.cz [citováno 06. 09. 2014]. Dostupné z: http://www.earchiv.cz/a912s200/a912s237.php3

5.4 Ověření v reálném provozu vzdálené stanice

Ověření v reálném provozu proběhlo přepojením vzdálené lokality ze stávajícího připojení, kde bylo využito pronajatého okruhu typu LLnet 512Mbps za pomocí technologie Vanguard /Frame Relay. Nové připojení bylo realizováno pomocí služby veřejného Internetu ADSL linka 8Mbps/512kbps, bez garantované šířky pásma a dostupnosti stupně agregace s technologií Astaro - nakonfigurovaného dle bodu 5.1.

První dva dny probíhalo testování dle varianty *L2-RED + router*. Následujících osm dní se testovalo dle varianty *L3-RED gateway*, která má menší nároky na hardwarové vybavení vzdálené stanice, přesto umožňuje funkci lokální gateway pro koncové počítače.

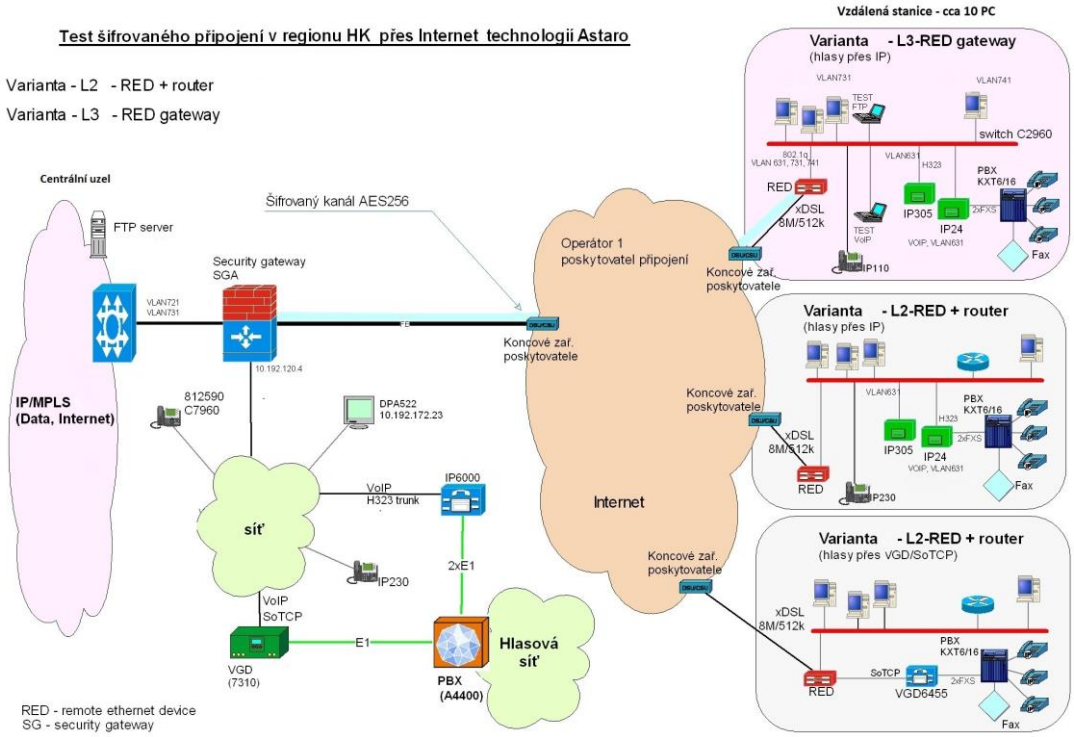
V zapojení hlasové části na vzdálené pobočce byl první dva dny ověřován provoz přes zařízení Vanguard6455 a protokol SoTCP. Stávající malá pobočková ústředna Panasonic KXT6/16 se zapojenými pobočkami a faxem byla propojena přes analogovou kartu FXS se zařízení Vanguard6455.

Následujících osm dní probíhalo ověřováním IP telefonie s využitím hlasové gateway formou IP ústředny Innovaphone IP24 s výstupem čtyřportové analogové karty typu FXS, která sloužila pro navázání stávající malé pobočkové ústředny Panasonic KXT6/16 a faxového přístroje. Dále byla osazena malá IP ústředna Innovaphone IP305, na kterou byl registrován testovací IP telefon typu IP110, pro komunikaci testovacích techniků.

Specifikace testovacího prostředí byla zvolena tak, aby byla dobře srovnatelná s provozními parametry (úrovní služeb) stávajícího připojení typu LLnet a odpovídala předpokládané konfiguraci technologie Astaro z hlediska řešení koncové lokality.

Během testovaného období byl datový, hlasový i faxový provoz ze strany koncového uživatele vyhodnocen bez jakýchkoliv připomínek.

Vzhledem k nepravidelnému využití připojení ze strany koncového uživatele bylo nutno ověřit kvalitu celkového připojení a služeb kvantitativně neboli generovaným provozem.



Obr. 20 - Typy ověřovaných zapojení

5.5 Popis původního zapojení přes Frame Relay

Zařízení **Vanguard** tvoří ucelenou produktovou řadu datových multifunkčních zařízení, určených k vytvoření paketové sítě sdružující hlasové a datové signály a k vzájemnému propojení sítí na úrovni LAN, WAN a telefonní sítě. Hardwarová i softwarová modularita jednotlivých zařízení a množství podporovaných protokolů dovoluje vytvářet takové sítě, které zaručují možnost dalšího současného rozvoje podle rostoucích potřeb.

Zařízení Vanguard 6455 je stávající technologie, která je plně funkční na vzdálené stanici a prostředím Frame Relay je propojen s centrálním Vanguardem 7310. Variability této technologie bylo možno využít a propojit jí s prostředím Ethernet přes zabezpečené tunely Astaro za pomocí protokolu SoTCP.

Základní popis Vanguard 6455.

Tento směrovač je převážně určen pro nasazení v regionálních bodech dané sítě. Zařízení nabízí nákladově efektivní podporu pro hlasové, faxové a smíšené protokoly přenosu dat po IP, Frame Relay, X.25, ISDN, ATM nebo Nx64 T1 / E1 služby. Vanguard můžeme rozšířit o různé daughter karty.

Podporované porty pro rozšíření daughter karty:

- 6 FXS portů
- 3 FXO porty
- 3 ISDN S0 porty
- 6 E&M portů
- 2 E1 port (G.703) s 30 kanály

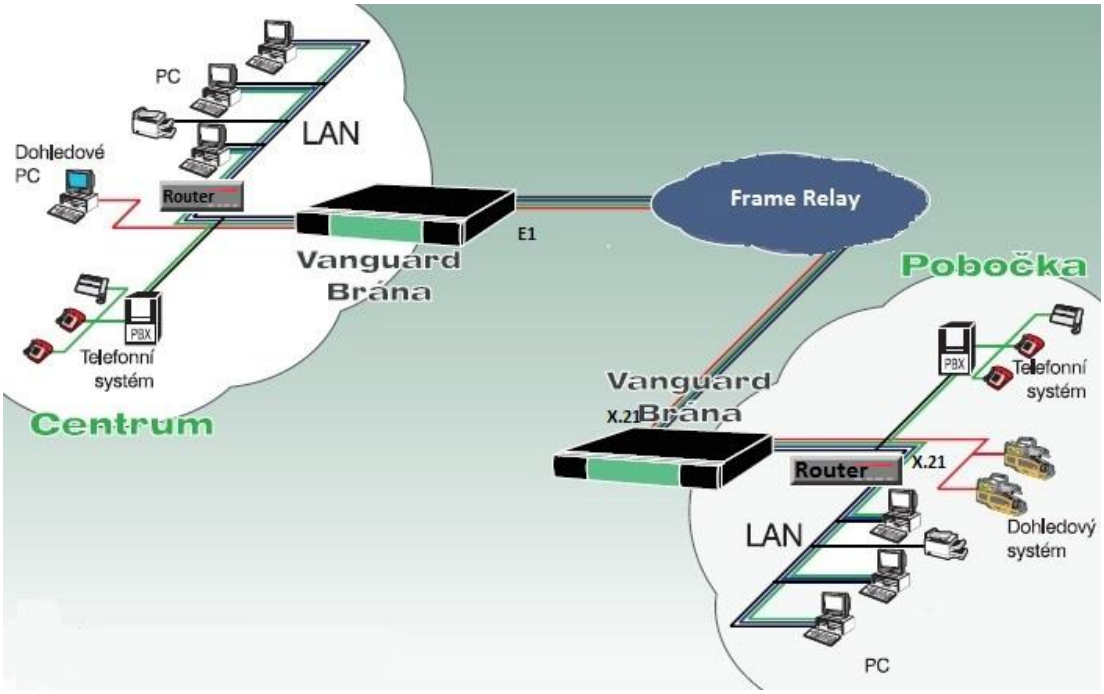
Testovaná pobočka je v původním zapojení připojena X.21 rozhraním k modemu daného poskytovatele a přes Frame Relay k centrálnímu bodu Vangurad 7310 přes rozhraní E1. Vanguard 6455 v koncovém bodě oddělí datové spojení od hlasového a druhým rozhraním X.21 v zařízení je propojen s routerem, který směruje data do switche, na která jsou propojená koncová uživatelská PC. Koncový Vanguard je vybaven dvouportovou FXS kartou, která je propojena s místní pobočkovou ústřednou Panasonic KX-T612.

Základní popis Vanguard 7310.

Tento směrovač je určen pro nasazení v centrálních bodech spojení, který umožňuje připojení podřízených uzlů ke stávajícím sítím LAN, WAN a telefonních technologií, které umožňují jejich vzájemné propojení.

Vanguard 7310 – základní jednotka (5 slotů pro karty, 128MB SDRAM, 2X 16MB Flask) doplněná o následující karty:

- 8 port Seriál Card
- 8 port T1/E1 Card
- CPU Central Processor Unit



Obr. 21 – Původní spojení přes FrameRelay

6 Vyhodnocení a analýza provedených testů - datových přenosů a výpadků

V této části diplomové práce probíhalo testování datových přenosů a výpadků. Ověření a testování bylo provedeno nejen v reálném provozu, ale jak bylo uvedeno v předchozí kapitole, bylo zapotřebí vytvořit generovaný provoz mezi vzdálenou pobočkou a centrálním spojením. Zda byla veškerá data bezpečně doručena, a jaká byla případná ztrátovost reálného i generovaného provozu bylo zjištěno na základě odezev ICMP protokolu. Tento protokol slouží k odesílání různých chybových hlášení při přenosu protokolem IP a neprovádí žádné opravy paketu, pouze informuje zdroj o vzniklé chybě. ICMP Echo Request a Replay je dvojice ICMP Echo zpráv, kterých využívá nástroj ping pro testování dostupnosti stanic a síťových uzlů. Odesílá se požadavek Echo Request na ověření dostupnosti stanice a odpovědí je zpráva Echo Replay.

6.1 Ověření reálným a generovaným provozem s vyhodnocením odezev ICMP protokolu

Specifikace ověření:

- **Generovaný provoz** byl vytvořen obousměrným přenosem velkého souboru 1GB a to ve směru *vzdálená stanice – centrála* i *centrála – vzdálená stanice,* za pomocí serverů a klientů ftp a tftp.
- **Test pro dostupnost služby přenosu dat** v síti Intranet (podniková síť) ICMP mezi *centrálou* (PC FTP server centrála) – *vzdálenou stanicí* (servisní notebook v datové síti) a opačně. Počet testovaných paketů v každé sérii: 300 (velikost paketů 100B, 1000B, 1600B - odpovídá mailové aplikaci).
- **Test pro dostupnost služby přenosu hlasů** - ICMP mezi PC (DPA522 viz obrázek č. 19) v centrále - servisní notebook v hlasové síti vzdálené stanice a opačně. Velikost paketů 100B odpovídá typickému hlasovému provozu. Zároveň byla vyhodnocována subjektivní kvalita hovoru během měření.

- Provoz byl zjišťován na rozhraní **Astaro Security Gateway** směrem do interní hlasové sítě v datové i hlasové VLAN.
- **Subjektivní hodnocení kvality přenosu hlasu** bylo prováděno souběžně s hlasovou komunikací s pracovníky na vzdálené pobočce během ověřování ICMP odezev. Hodnocení kvality vychází ze zavedené stupnice kvality přenosu hlasu parametrem MOS (Mean Opinion Score) – odhad kvality a srozumitelnosti řeči pro posluchače. Hodnota MOS na základě hodnocení subjektivního vzorku na stupnici kvality se pohybuje v rozmezí 5 – 1, jak je vidět v následující tabulce č. 4.

Stupeň MOS	Kvalita	Hodnocení kvality
5	Vynikající (Excelent)	Bez znatelného rušení
4	Dobrá (Good)	Rušení lze rozpoznat, ale není obtěžující
3	Průměrná (Fair)	Rušení lze rozpoznat a mírně obtěžuje
2	Špatná (Poor)	Rušení obtěžuje a porozumění řeči je obtížné
1	Velmi špatná (Bad)	Rušení velmi obtěžuje a řeč je nesrozumitelná

Tab. 4 – Hodnoty stupnice MOS

Subjektivní hodnocení je založeno na hodnocení živých posluchačů a na základě jejich vnímaní a spokojenosti daného hovoru.

- **Vyhodnocení faxového provozu**: Fax v koncové lokalitě je standardně zapojen na analogové pobočce místní pobočkové ústředny typu - Panasonic KXT616, která byla navázána z analogového trunkového portu CO do IP ústředny Innovaphone IP305/IP24 přes její analogový port FXS a odtud protokolem H.323 na IP ústřednu Innovaphone IP6000, která je zapojena v centrále, a odtud trunkem E1 do interní podnikové hlasové sítě ITS. V ITS je zapojeno několik faxových přístrojů, na které byly provedeny testy ze vzdálené lokality a opačně.

6.1.1 Odezvy ICMP

Výsledky z odezev ICMP byly převedeny do tabulek dle odchozí specifikace ověření. Rozdělená měření byla provedena pro reálný a generovaný provoz, jak z datového zatížení, tak hlasového provozu na vzdálené pobočce a Security Gateway (SG) v centrálním komunikačním uzlu.

Následující výsledky měření zobrazují **pouze reálný provoz** mezi pobočkou (P) a centrálou (C).
Zatížení bylo vytvořeno obousměrným přenosem velkého souboru 1GB (ve směru P-C i C-P) za pomocí serverů a klientů ftp a tftp.

Data								
směr testu	**čas**	**paket**	**počet**	**odezva min.**	**max.**	**průměr**	**ztrátovost**	**ztracené**
		[B]	[-]	[ms]	[ms]	[ms]	[%]	[-]
C - P	9:45	100	300	18	63	19	0	0
P - C	9:45	100	300	20	65	20	0	0
C - P	9:52	1000	300	38	109	41	0	0
P - C	9:52	1000	300	43	68	45	0	0
C - P	10:01	1600	300	54	102	55	1	3
P - C	10:01	1600	300	61	95	62	0	2

Tab. 5 – Bez zátěžového provozu

Security GW - statistika rozhraní data			
rozhraní \ čas	9:45	9:52	10:01
IN (rychlost [kbps])	7,4	23,4	42,1
OUT (rychlost [kbps])	7,4	78,4	91,9

Tab. 6 – Security Gateway, měřená rychlost v centrále

Test pro dostupnost služby přenosu hlasů: ping mezi PC522 v centrále (C) a notebooku v hlasové síti pobočky (P) a opačně - velikost paketů 100B odpovídá typickému hlasovému provozu.
Syntaxe pro ping [délka paketu, počet paketů], #ping 10.192.xxx.yyy -l 100 -n 300

hlas (VoIP/H.323)									
směr testu	**Čas**	**paket**	**počet**	**odezva min.**	**max.**	**průměr**	**ztrátovost**	**ztracené**	**hlas**
		[B]	[-]	[ms]	[ms]	[ms]	[%]	[-]	subjektivně
C - P	9:45	100	300	18,7	64,4	21,2	0	0	4
P - C	9:45	100	300	18	71	19	0	0	

Tab. 7 – Test hlasového ověření

Security GW - statistika rozhraní hlas (VoIP/H.323)	
rozhraní \ čas	9:45
IN (rychlost [kbps])	1,8
OUT (rychlost [kbps])	1,5

Tab. 8 - Security Gateway, měřená rychlost v centrále

Následující výsledky měření zobrazují **reálný a generovaný provoz** mezi pobočkou (P) a centrálou (C).

Test pro dostupnost služby přenosu dat (síť Intranet): ping mezi PC FTP server v centrále a notebook v datové síti vzdálené pobočky a opačně - (velikost paketů 100B, 1000B, 1600B/ odpovídá mailové aplikaci).

data								
směr testu	**čas**	**paket**	**počet**	**odezva min.**	**max.**	**průměr**	**ztrátovost**	**ztracené**
		[B]	[-]	[ms]	[ms]	[ms]	[%]	[-]
C - P	10:15	100	300	18	259	68	2	6
P - C	10:15	100	300	19	222	75	0	1
C - P	10:29	1000	300	38	322	93	1	5
P - C	10:29	1000	300	43	238	92	0	0
C - P	10:42	1600	300	54	244	107	6	20
P - C	10:42	1600	300	61	237	107	3	9

Tab. 9 – Generovaný provoz

Security GW - statistika rozhraní data			
rozhraní \ čas	10:15	10:29	10:42
IN (rychlost [kbps])	235,5	271	230,2
OUT (rychlost [kbps])	171,2	165	82

Tab. 10 - Security Gateway, měřená rychlost v centrále

Testování hlasového provozu bylo provedeno stejným způsobem jako v předchozím testu. Rozdílnost testu spočívala v tom, že se navíc k reálnému provozu přidal generovaný.

hlas (VoIP/H.323)									
směr testu	**Čas**	**paket**	**počet**	**odezva min.**	**max.**	**průměr**	**ztrátovost**	**ztracené**	**hlas**
		[B]	[-]	[ms]	[ms]	[ms]	[%]	[-]	subjektivně
C - ZU	10:15	100	300	18,8	189	65	0	0	4
ZU - C	10:15	100	300	18	228	84	1	4	

Tab. 11 - Test hlasového ověření

Security GW - statistika rozhraní hlas (VoIP/H.323)	
rozhraní \ čas	10:15
IN (rychlost [kbps])	1,5
OUT (rychlost [kbps])	1,4

Tab. 12 - Security Gateway, měřená rychlost v centrále

6.1.2 Odezvy ICMP původního zapojení

Pro porovnání zapojení vzdálené stanice přes LLnet bylo následně provedeno měření, a to v nezbytném rozsahu.

Pro srovnání reálného provozu přes Frame Relay bylo zapotřebí přepojit stávající rozhraní typu LLnet 512 kbps přes Vanguard/Frame Relay, jak bylo popsáno v kapitole 5.5.

Výsledky měření zobrazují **pouze reálný provoz** mezi pobočkou (P) a centrálou (C).

Zatížení datového provozu bylo vytvořeno obousměrným přenosem velkého souboru 1GB (ve směru P-C i C-P) za pomocí serverů a klientů ftp a tftp

data - přes Frame Relay							
směr testu	**paket**	**počet**	**odezva min.**	**max.**	**průměr**	**ztrátovost**	**ztracené**
	[B]	[-]	[ms]	[ms]	[ms]	[%]	[-]
C - P	100	300	---	---	---	---	---
P - C	100	300	---	---	---	---	---
C - P	1000	300	---	---	---	---	---
P - C	1000	300	---	---	---	---	---
C - P	1600	300	94	663	103	0	0
P - C	1600	300	100	404	108	0	1

Tab. 13 – Bez zátěžového provozu přes FR

Test pro dostupnost služby přenosu hlasů byl proveden pouze ve směru - Centrála (C) a Pobočka (P): ping mezi PC522 v centrále a Vanguard 6455, který je umístěn na vzdálené pobočce - velikost paketů 100B odpovídá typickému hlasovému provozu.

hlas - přes Frame Relay								
směr testu	**paket**	**počet**	**odezva min.**	**max.**	**průměr**	**ztrátovost**	**ztracené**	**hlas**
	[B]	[-]	[ms]	[ms]	[ms]	[%]	[-]	subjektivně
C - P	100	300	24	251	32	0	0	4
P - C	100	300	---	---	---	---	---	

Tab. 14 – Test hlasového provozu přes FR

Následující výsledky měření zobrazují **reálný a generovaný provoz přes Frame Relay** mezi pobočkou (P) a centrálou (C).

Test pro dostupnost služby přenosu dat (síť Intranet): ping mezi PC FTP server v centrále a notebook v datové síti vzdálené pobočky a opačně - (velikost paketů 100B, 1000B, 1600B/ odpovídá mailové aplikaci).

data - přes Frame Relay							
směr testu	**paket**	**počet**	**odezva min.**	**max.**	**průměr**	**ztrátovost**	**ztracené**
	[B]	[-]	[ms]	[ms]	[ms]	[%]	[-]
C - P	100	300	27	330	134	0	0
P - C	100	300	38	308	144	0	0
C - P	1000	300	79	234	156	0	0
P - C	1000	300	79	275	186	0	1
C - P	1600	300	129	198	157	0	0
P - C	1600	300	153	237	199	0	0

Tab. 15 – Generovaný provoz přes FR

Zkouška funkce dostupnosti hlasového provozu byla provedena stejným způsobem, jako v předchozím testu bez zátěžového provozu přes FR. Rozdílnost testu spočívala v tom, že se navíc k reálnému provozu přidal generovaný.

hlas - přes Frame Relay								
směr testu	**paket**	**počet**	**odezva min.**	**max.**	**průměr**	**ztrátovost**	**ztracené**	**hlas**
	[B]	[-]	[ms]	[ms]	[ms]	[%]	[-]	subjektivně
C - P	100	300	28,2	274,2	67,2	0	0	4 - 3
P - C	100	300	---	---	---	---	---	

Tab. 16 – Test hlasového provozu přes FR

Vyhodnocení odezev pro stávající připojení přes Frame Relay bylo provedeno ve vybraném rozsahu, pro srovnání - viz tabulka č. 13, kde jsou zaneseny hodnoty jen pro velké pakety 1600B, v tabulkách č. 14 a 16 jsou uvedeny hodnoty jen ve směru C - P.

Ze získaných hodnot testů se zátěží i bez zátěže je patrné, že provoz probíhá přes garantované a symetrické připojení, kdy i při generovaném provozu je ztrátovost 0% a nejsou výraznější rozdíly v odezvách v obou směrech.

6.2 Zhodnocení provedených testů

V rozsahu reálného provozu nebyly ze strany koncového uživatele po dobu testovaného období deseti dnů zjištěny nedostatky. Prověření provozem zde bylo ovlivněno nepravidelným využitím připojení ze strany koncového uživatele a to v závislosti na plnění pracovních úkolů vzdálené stanice, kdy typický reálný provoz byl vytvářen pouze na jednom až dvou stolních počítačích.

Z technického hlediska výsledky testů odezev ICMP splnily očekávané předpoklady, kdy kolísající kvalita negarantovaného připojení ovlivňuje ztrátovost paketů. Nicméně z hlediska přenášeného hlasového provozu nebyl díky nastavené prioritizaci datových toků uvnitř vytvořeného IPsec tunelu zaznamenán pokles kvality hlasu.

Faxový provoz byl při výše uvedené konfiguraci pomocí protokolu H.323 proti IP 6000 po testovacího provozu vyhodnocen „bez závad“. Pro zajištění faxové Gateway na centrální lokalitě není nezbytně nutné použít IP ústřednu Innovaphone IP6000, stačí využít finančně dostupnější řešení a to například ústředny Innovaphone - IP302/IP305.

Porovnání odezev ICMP negarantovaného připojení se stávajícím řešením přes LLnet vykázalo obdobné parametry, až na akceptovatelnou ztrátovost paketů, která je pro datový provoz ošetřena z úrovně nejvyšší aplikační vrstvy.

Z výsledku měření vyplývá, že pro připojení vzdálených stanic, které generují větší provoz připojením více aktivních PC pracovišť a s větším objemem hlasového provozu doporučuji volit kvalitnější připojení do Internetu, a to s garantovanou šířkou pásma a dostupností, popř. se symetrickým pásmem.

Testy vzhledem k technickým podmínkám prokázaly předpokládanou výhodnost tohoto řešení datových a hlasových služeb.

6.3 Porovnání cenové nabídky LLnet od O2 a xDSL

Nejjednodušším testem a přitom zásadním při řešení efektivního a levnějšího způsobu připojení vzdálené pobočky se jeví porovnání cenové nabídky pronajatého dosavadního LLnet okruhu s novým typem standardního ADSL připojení a to od stejného poskytovatele.

připojení	**měsíčně (bez DPH)**	**ročně (bez DPH)**
stávající LLnet H. Králové - Třebechovice p. O. (512 kbps, pásmo B)	24 769 Kč	297 228 Kč
O2 Internet Optimal (až 16Mbps /1Mbps)	417 Kč	5 004 Kč
O2 Internet Aktiv (až 25Mbps /2Mbps)	500 Kč	6 000 Kč

Tab. 17 – Srovnání provozních nákladů

Finanční náklady ušetřené na pronajatém připojení xDSL se mohou velmi brzo vrátit v podobě investice do základní obměny potřebné IT technologie, kterou je možno v budoucnu rozšířit a zcela nahradit za stávající. V příloze této diplomové práce je navrženo několik variant připojení technologie Astaro.

7 Závěr

Cílem diplomové práce bylo najít vhodné a optimální řešení, které vzešlo z požadavku nalezení levnějšího způsobu připojení vzdálené pobočky k resortní telekomunikační síti při zachování stávající úrovně služeb tak, aby bylo možno zachovat stávající technologii, která již zahrnovala danou konvergenci hlasu a dat. Na základě tohoto požadavku bylo nalezeno vhodné a bezpečné řešení pro připojení vzdálené stanice přes negarantovaný internet v technologii Astaro(SOPHOS).

V první části předložené práce je uveden odborný popis jednotlivých pojmů z pohledu informačních technologií, které souvisejí s danou problematikou tak, aby bylo možno pochopit celé úskalí a řetězce souvisejících činností při připojení vzdálené stanice. Součástí práce je závěrečné řešení specifického úkolu, jež se opírá o výsledky praktického zkoumání a testování.

Z výsledků testování je zřejmé, že tato cesta vede ke značným firemním úsporám, jak bylo potvrzeno ze srovnání provozních nákladů za připojení a zároveň se jeví jako ekonomická implementace technologie Astaro formou virtualizované Security Gateway.

Může vzniknout jistá obava o zajištění bezpečnosti přenášených dat při přenosu, a to zejména ve státní správě či v různých bezpečnostních složkách. Nelze však vyloučit, že dojde k prolomení kódů šifrovaných tunelů a ke ztrátě cenných informací. Práce nebyla testována a podrobena fyzickému testu ve snaze prolomit dané zabezpečení. Přesto se lze domnívat, že není důvod k obavám a to vzhledem k vytvoření šifrovaných tunelů typu IPsec (AES256) mezi centrem a vzdálenou stanicí, které splňují standard NATO. Nabízí se tak otázka: „*kdo dnes dokáže říci, že tento přenos je zcela bezpečný*“? Zde lze dospět k závěru, že bezpečnostní riziko můžeme nalézt všude a to zejména v lidském faktoru.

Na základě analýzy a provedených testů se podařilo navrhnout funkční a bezpečné připojení, které představuje vhodné řešení pro malé a střední organizace, jejichž důležitou potřebou je spojení vzdálené pobočky s centrálou, zabezpečení rychlého přístupu k internetu a zároveň představuje cenově přijatelný a dostupný způsob zabezpečení všech stanic s tím, že je zapotřebí zvážit kvalitnější připojení do Internetu, zejména s garantovanou šířkou pásma a dostupností.

Použitá literatura a prameny

DOSTÁLEK, Libor, KABELOVÁ, Alena. *Velký průvodce protokoly TCP/IP a systémem DNS*. 2. aktualizované vyd. Praha: Computer Press, 2000, 423 s. ISBN 80-7226-323-4.

CHAPMAN JR., David W., FOX, Andy. *Zabezpečení sítí pomocí Cisco PIX Firewall*. 1.vyd. Brno: Computer Press, 2004, 368 s. ISBN 80-722-6963-1.

PUŽMANOVÁ, Rita. *Moderní komunikační sítě od A do Z*. 1.vyd. Praha: Computer Press, 1998, 432 s. ISBN 80-7226-098-7.

PUŽMANOVÁ, Rita. *Širokopásmový Internet Přístupové a domácí sítě*. 1.vyd. Brno: Computer Press, 2004, 377 s. ISBN 80-251-0139-8.

SPORTAK, Mark A. *Směrování v sítích IP*. 1.vyd. Brno: Computer Press, 2004, 368 s. ISBN 80-251-0127-4.

TEARE, Diane. *Návrh a realizace sítí Cisco*. 1.vyd. Brno: Computer Press, 2003, 784 s. ISBN 80-251-0022-7.

VELTE, Toby J, VELTE, Anthony T. *Síťové technologie Cisco*. 1.vyd. Brno: Computer Press, 2003, 800 s. ISBN 80-7226-857-0.

WENSTROM, Michael. *Zabezpečení sítí Cisco*. 1.vyd. Brno: Computer Press, 2003, 784 s. ISBN 80-7226-952-6.

Adresování v TCP/IP v sítích II[online]. eArhiv.cz [citováno 24. 11. 2013]. Dostupné z: http://www.earchiv.cz/a92/a235c110.php3

Adresování v TCP/IP v sítích II[online]. eArhiv.cz [citováno 15. 02. 2014]. Dostupné z: http://www.earchiv.cz/a92/a235c110.php3

Asymetrická kryptografie[online]. Wikipedie[citováno 10. 05. 2014]. Dostupné z: http://cs.wikipedia.org/wiki/Asymetrick%C3%A1_kryptografie

HANÁČEK, Petr. *Bezpečnostní funkce v počítačových sítích*[online]. Ústav výpočetní techniky Masarykova univerzita 14.11.2011 [citováno 26. 03. 2014]. Dostupné z: http://www.ics.muni.cz/bulletin/articles/171.html

HRSTKA, Jaroslav. *Vysokorychlostní přístup ke službám elektronických komunikací* [online]. Testcom 2006[citováno 17. 05. 2014]. Dostupné z: http://www.testcom.cz/pdf/vyzkum/Vysokorychlostni_pristup_ke_sluzbam.pdf

IP adresa[online]. wikipedie [citováno 20. 02. 2014]. Dostupné z: http://cs.wikipedia.org/wiki/IP_adresa

IP adresy[online]. [citováno 07. 12. 2013]. Dostupné z: http://pc-site.owebu.cz/?page=PTCPIP3

IP Protokol[online]. Velký průvodce protokoly [citováno 24. 11. 2013]. Dostupné z: http://zam.opf.slu.cz/botlik/CD-0x/5.html

IP110[online]. ANNEX NET [citováno 21. 06. 2014]. Dostupné z: http://www.annexnet.cz/innovaphone-voip-telefony-ip110/

IPv4[online]. [citováno 20. 02. 2014]. Dostupnéz: http://home.zcu.cz/~hliboka/ipv4/ipv4.html

IP24[online]. ANNEX NET [citováno 21. 06. 2014]. Dostupné z: http://www.annexnet.cz/innovaphone-produkty-ip24/

IP305[online]. ANNEX NET [citováno 20. 06. 2014]. Dostupné z: http://www.annexnet.cz/innovaphone-voip-brany-ip305/

KOVÁŘ, Jiří. *SLA – kvalita služeb*[online]. Ing. Jiří Kovář – znalec v oboru elektronika a kybernetika[citováno 23. 03. 2014]. Dostupné z: http://jirikovar.cz/index.php/13-internet-a-datove-site/datova-sit/10-sla-kvalita-sluzeb

KRSIČKA, Daniel. *Technologie SSL VPN jejich řešení firmou Cisco Systems* [online]. 15.1.2006[citováno 16. 05. 2014]. Dostupné z: http://www.cs.vsb.cz/grygarek/TPS/projekty/0506Z/krs008_TPS_projekt.pdf

O NÁS[online]. ANNEX NET [citováno 31. 05. 2014]. Dostupné z: http://annexnet.cz/o-nas-zakladni-informace

PETERKA, Jiří. *Adresování v TCP/IP sítích-I*[online]. eArhiv.cz [citováno 16. 02. 2014]. Dostupné z: http://www.earchiv.cz/a92/a233c110.php3

PETERKA, Jiří. *Architektura H.323 verze 1*[online]. eArhiv.cz [citováno 06. 09. 2014]. Dostupné z: http://www.earchiv.cz/a912s200/a912s237.php3

PETERKA, Jiří. *Protokol IP*[online]. eArhiv.cz [citováno 15. 02. 2014]. Dostupné z: http://www.earchiv.cz/a92/a248c110.php3

PETERKA, Jiří. *Síťová architektura*[online]. eArhiv.cz [citováno 03. 10. 2013]. Dostupné z: http://www.earchiv.cz/anovinky/ai1483.php3

Protokol IP[online]. [citováno 23. 11. 2013]. Dostupné z: http://pc-site.owebu.cz/?page=PIP

RUDINSKÝ, J. *Sítě nové generace – NGN*[online]. Access server 4.5.2006. [citováno 15.03.2014]. Dostupné z: http://access.feld.cvut.cz/view.php?cisloclanku=2006050401

Síťová architektura[online]. eArhiv.cz [citováno 05. 10. 2013]. Dostupné z: http://www.earchiv.cz/anovinky/ai1483.php3

SOPHOS | SOPHOS komplexní zabezpečení Vaší sítě[online]. ANNEX NET [citováno 06. 06. 2014]. Dostupné z: http://annexnet.cz/sophos-zakladni-informace/

STANEK, Martin. *Kryptológia Pragmatický pohľad*[online]. Katedra informatiky Fakulta matematiky, fyziky a informatiky Univerzity Komenského, Bratislava, Slovensko 02.2014 [citováno 30. 05. 2014]. Dostupné z: http://www.dcs.fmph.uniba.sk/~stanek/Kryptologia%20v1c.pdf

TCP/IP je síťovou architekturou[online]. eArhiv.cz [citováno 26. 10. 2013]. Dostupné z: http://www.earchiv.cz/l225/slide.php3?l=3&me=2

Seznam obrázků:

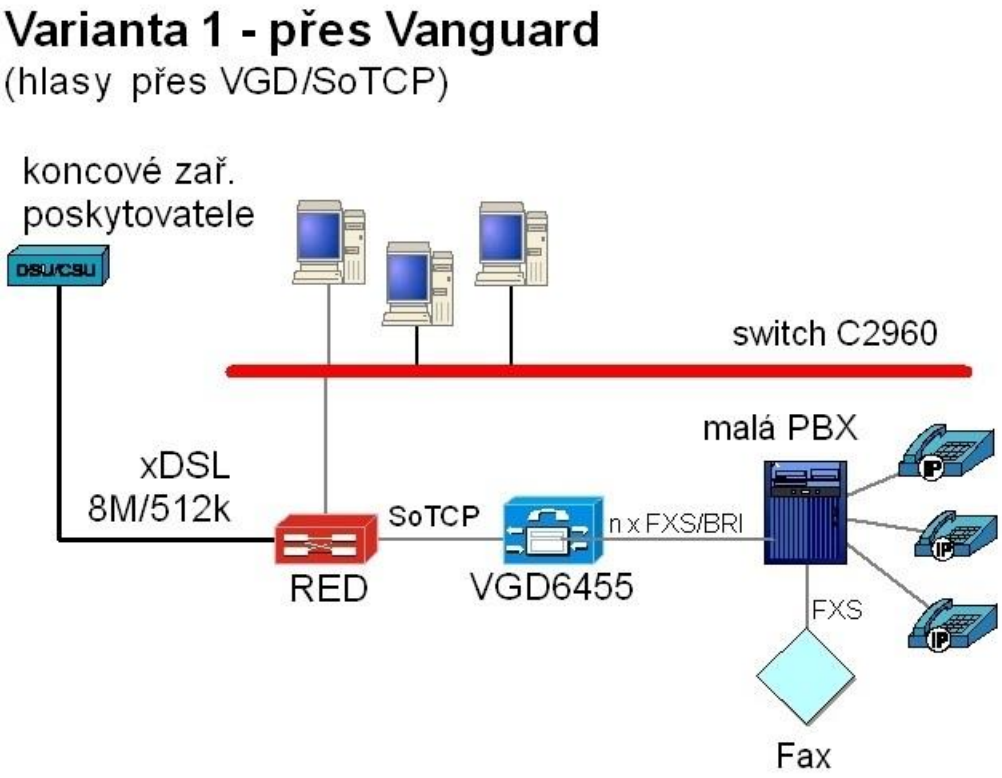
Seznam tabulek:

Přílohy

Přiloha 1 - Varianty zapojení vzdálené stanice

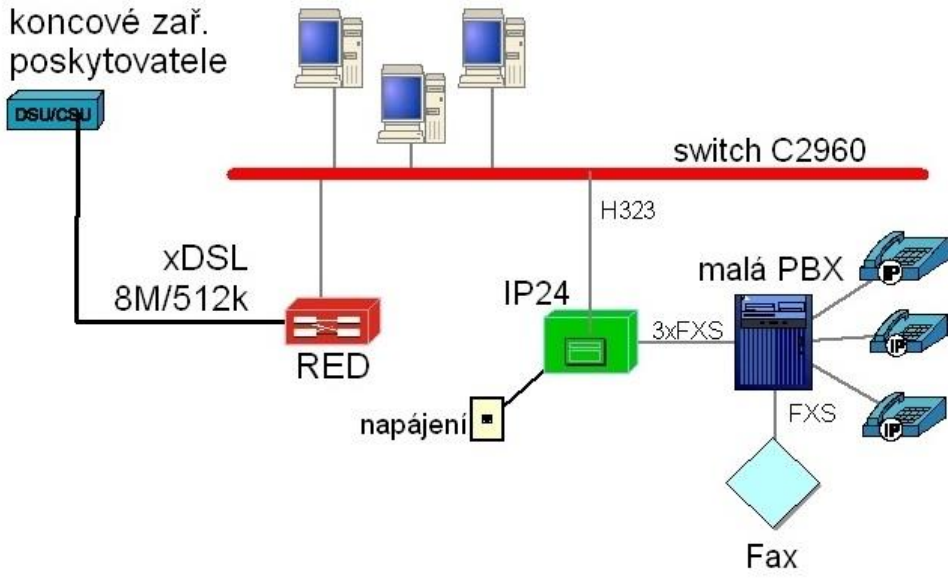
Přiloha 2 - Varianty Astaro SG zapojení v centru

Přiloha 1 - Varianty zapojení vzdálené stanice



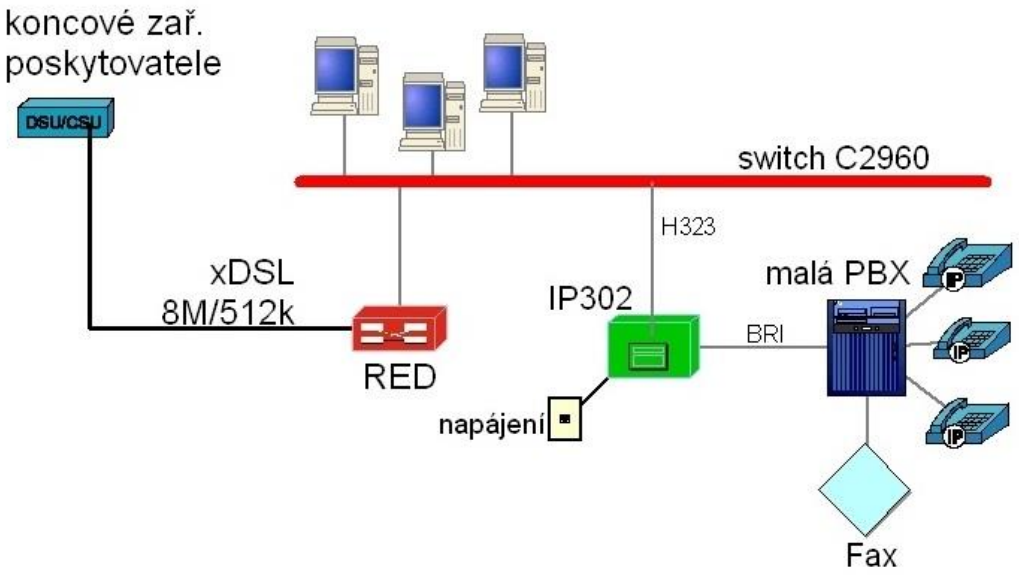
Varianta 2 - přes IP hlas. GW (rozhraní FXS)

(hlasy přes H.323 zakončené na centrálním VGD či IP PBX)



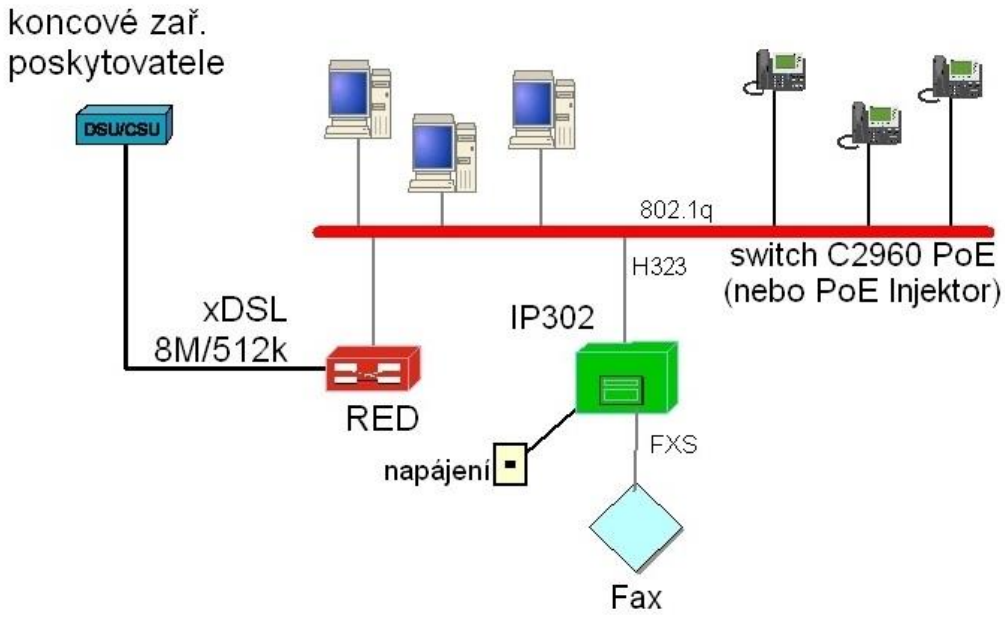
Varianta 3 - přes IP hlas. GW (rozhraní BRI)

(hlasy přes H.323 zakončené na centrálním VGD či IP PBX)



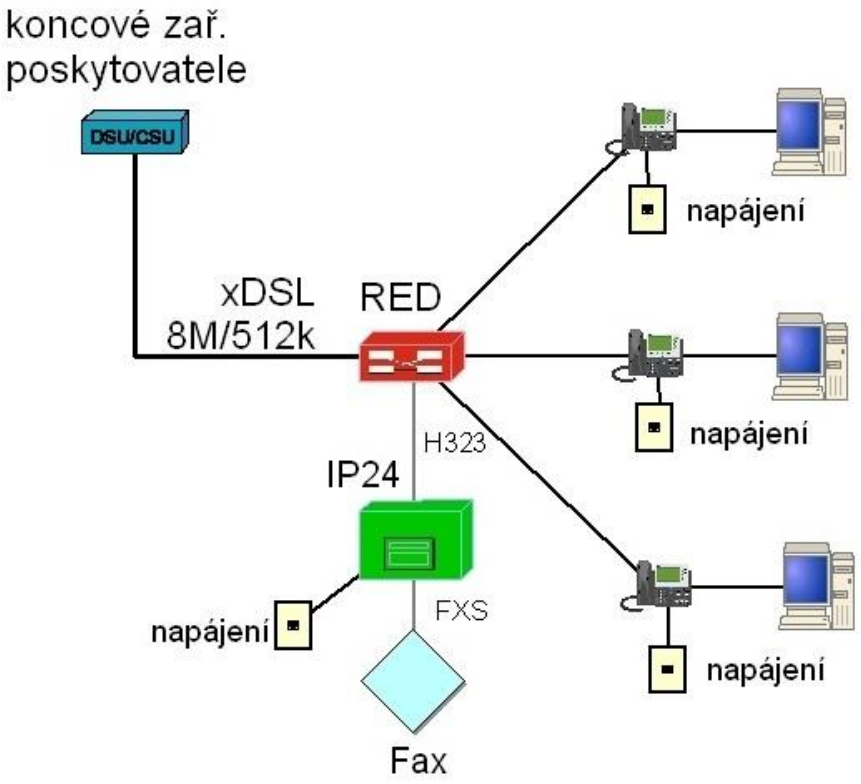
Varianta 4 - IP PBX (lokální CS)

(hlasy přes H.323 zakončené na centrálním VGD či IP PBX)



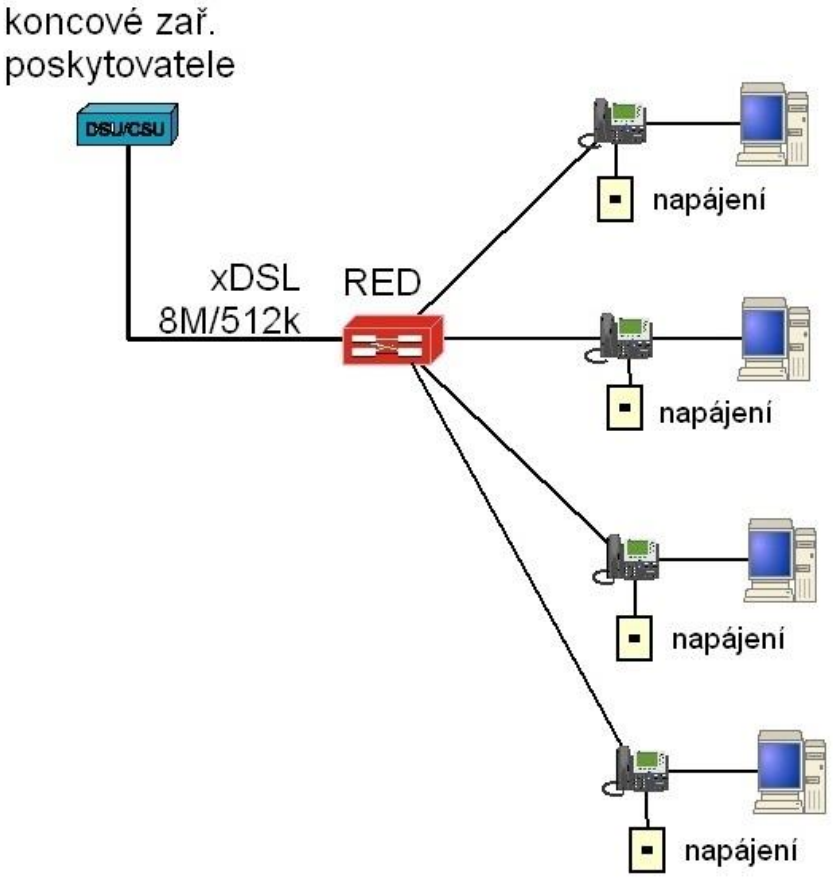
Varianta 5 - IP PBX v centru (vzdálený CS)

(hlasy přes H.323 zakončené na centrálním VGD či IP PBX)



Varianta 6 - IP PBX v centru (vzdálený CS)

(hlasy přes H.323 zakončené na centrálním VGD či IP PBX, fax nahrazen pomocí centrálního faxserveru - "Emailem")



Níže je provedeno finanční porovnání variant dle Přílohy 1.

Vychází ze zjištěných cen a pomocí nich se kalkulují náklady na jednotlivé varianty:

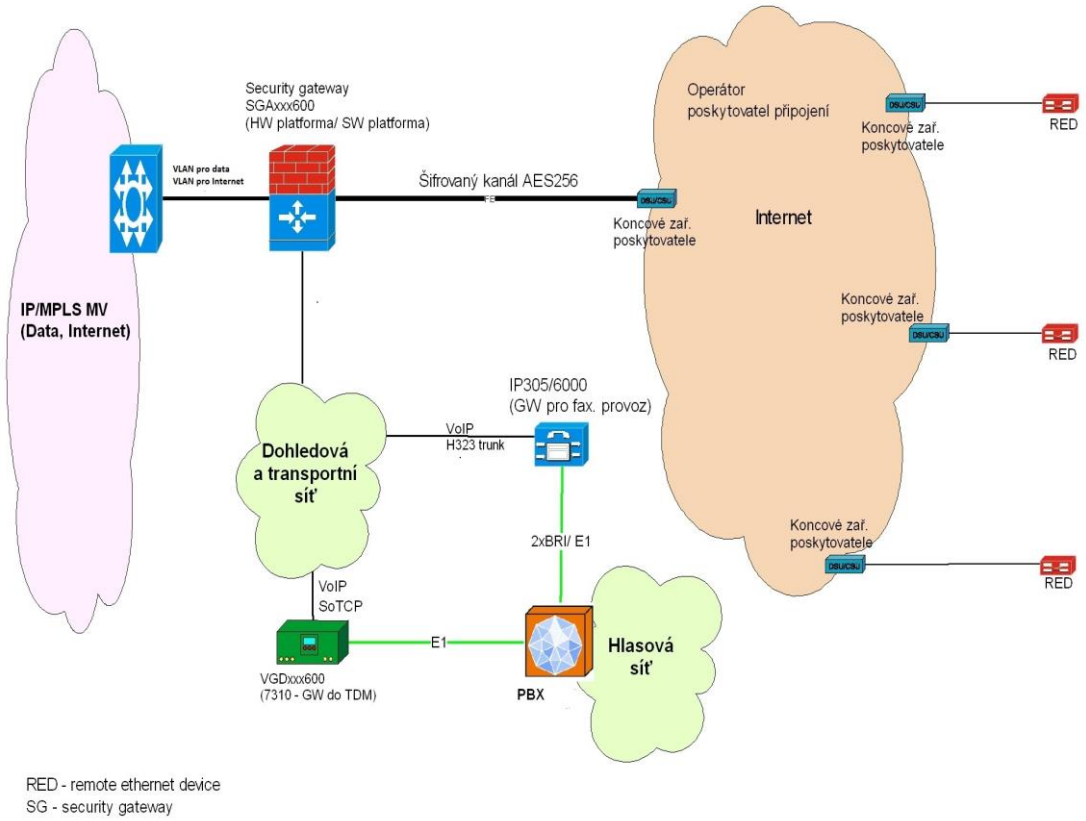
- varianty 1. až 4. počítají s 10 uživateli,
- varianta 5. se 3 uživateli,
- varianta 6. se 4 uživateli.

zařízení	cena Kč	cena s DPH
RED + rozšíř. záruka	9250	11100
switch C2960-24-TC-L	16950	20340
switch C2960-24-LTL (8xPoE)	19500	23400
Injektor PoE-1port	420	504
router C1841 (2x FE, v.12.4)	41000	49200
IP24 (media GW)	12800	15360
IP302 (media GW)	14800	17760
IP302-PBX (lic. PBX+ 15úč,..)	49960	59952
tel. IP110	2340	2808
tel. IP230	4420	5304
licence IP tel. na PBX (centrum]	130	156
napájení IP PBX	1000	1200
napájení IP tel.	800	960
rack 18U s výstrojí	19500	23400

Varianta/ počet zařízení	RED	switch	switch PoE	Inj PoE	C1841	IP24	IP302	IP302-PBX	IP 110	IP 232	lic. centrum	nap. IP PBX	nap. IP tel.	rack	CELKEM
Var.1 - Vanguard (stávající)	1	1	0	0	1	0	0	0	0	0	0	0	0	0	80640
Var.2 - IP GW-FXS (10 úč.)	1	1	0	0	0	1	0	0	0	0	0	1	0	1	71400
Var.3 - IP GW-BRI (10 úč.)	1	1	0	0	0	0	1	0	0	0	0	1	0	1	73800
Var.4 - IP PBX (10 úč.)	1	0	1	2	0	0	0	1	8	2	0	1	0	1	153132
Var.5 - IP tel. +FXS (3 úč.)	1	0	0	0	0	1	0	0	3	0	3	1	3	0	39432
Var.6 - IP tel. (4 úč.)	1	0	0	0	0	0	0	0	4	0	4	0	4	0	26796

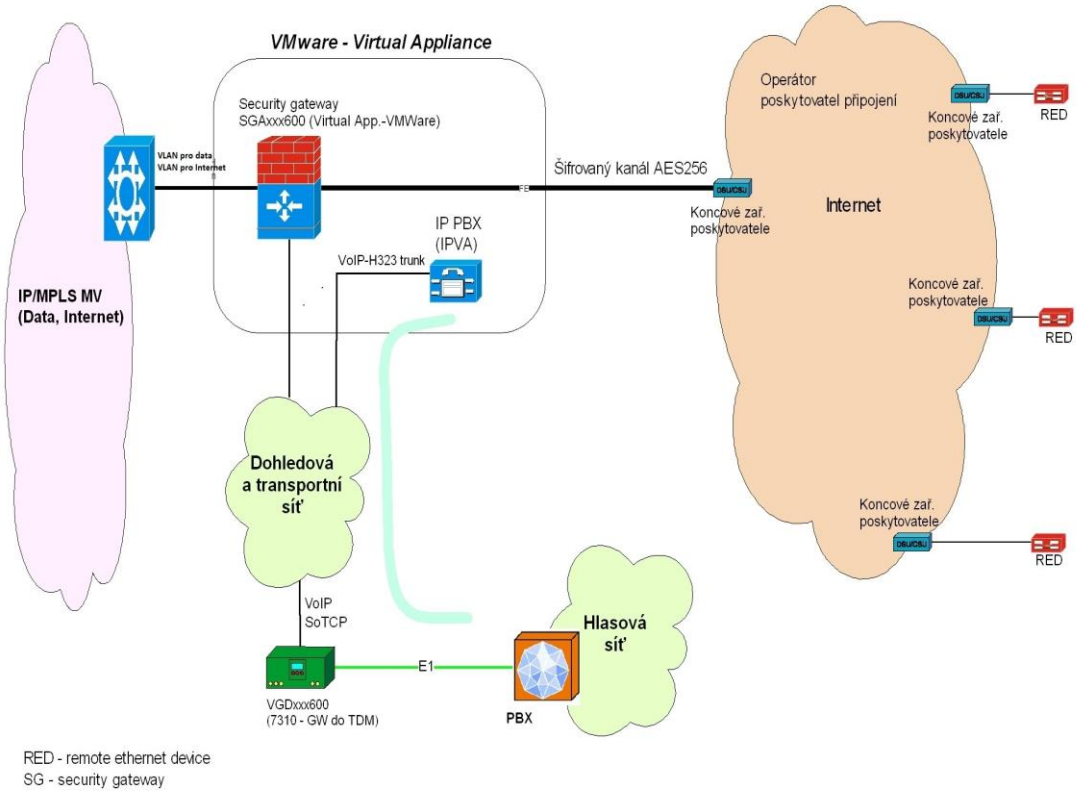
Příloha 2 - Varianty Astaro SG zapojení v centru

Varianta 1 – HW řešení



RED - remote ethernet device
SG - security gateway

Varianta 2 – virtuální platforma



Pro finančně méně náročnou počáteční implementaci lze využít virtualizovanou aplikaci Astaro Security Gateway (virtual appliance) i virtuální PBX Innovaphone (IPVA), je-li k dispozici na straně datového centra volná kapacita virtualizovaných serverů na platformě VMware.

Licence Astaro SG jsou časově specifikované dle počtu připojených koncových zařízení (počtu PC popř. počtu VoIP telefonů/PBX v příslušných vzdálených lokalitách). Výsledná cena je tvořena počtem licencí koncových zařízení a podpory, počtem boxů RED a nákladů za implementaci – dle konkrétní cenové nabídky.

Licencování IPVA se skládá z licence za funkcionalitu IP PBX (s degresí na početní rozsah registrovaných zařízení od počtu 500) a za počet registrovaných zařízení.