Univerzita Karlova v Praze

Matematicko-fyzikální fakulta

BAKALÁŘSKÁ PRÁCE

Daniel Winter

Vliv zabezpečení VPN sítí na výkonnost systému

Katedra softwarového inženýrství

Vedoucí bakalářské práce: RNDr. Ing. Jiří Peterka

Studijní program: Informatika

Studijní obor: správa počítačových systémů

Praha 2014

V úvodu bych chtěl poděkovat RNDr. Ing. Jiřímu Peterkovi za obětavou pomoc a vedení práce.

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona.

V Praze dne 22. května 2014 Daniel Winter

Název práce: Vliv zabezpečení VPN sítí na výkonnost systému

Autor: Daniel Winter

Katedra / Ústav: Katedra softwarového inženýrství

Vedoucí bakalářské práce: RNDr. Ing. Jiří Peterka, Katedra softwarového inženýrství

Abstrakt: Spolu s rozvojem informačních technologií v posledních desetiletích dochází i k rozvoji počítačových sítí, často spojujících geograficky velmi vzdálená místa. To s sebou nese nemalé náklady na vybudování a provoz síťové infrastruktury. Tento problém můžeme vyřešit pronájmem datových linek, nebo využitím již existující síťové infrastruktury, Internetu, a pomocí technologie zvané Virtuální privátní síť (VPN) vytvořit s minimálními finančními náklady počítačovou síť nad sdílenou infrastrukturou. Tato práce se zabývá principem fungování těchto virtuálních privátních sítí, různými možnostmi jejich realizace s následným dopadem na výkonnost systémového prostředí a rychlost komunikace. Vše je nejprve zkoumáno v teoretické rovině a následně ověřeno na konkrétních sestavách na platformě MS Windows.

Klíčová slova: VPN, nastavení, výkonnost, bezpečnost

Title: VPN security settings influence on system peformance

Author: Daniel Winter

Department: Katedra softwarového inženýrství

Supervisor: RNDr. Ing. Jiří Peterka, Katedra softwarového inženýrství

Abstract: Development of computer networks along with the growth of information technology connects geographically remote places. Considerable cost of building and operating the network infrastructure is entailed. This issue can be solved by leasing of data lines, or using Internet as an existing network infrastructure. Not to forget to mention a technology called Virtual Private Network (VPN) to create a minimal financial cost computer network over a shared infrastructure. This paper deals with the principle of operation of virtual private networks, various possibilities of their implementation with consequent impact on the performance of the system environment and the communication speed. First of all everything is first examined in theory and then subsequently validated on specific reports on MS Windows platform.

Keywords: VPN, settings, performance, security

Obsah

Úvod

Žijeme v éře informačních technologií, kdy je celý svět doslova protkán pavučinami telekomunikačních a počítačových sítí, bez jejichž služeb si už neumíme život snad ani představit, neboť jsme se na nich stali zcela závislými.

Zkusme se obejít jen jeden jediný den bez mobilního telefonu a možnosti komukoliv zavolat, nebo být naopak kdykoliv k zastižení. Nebo bez Internetu a on-line informací všeho druhu. Nebo v poslední době stále populárnějších chytrých telefonů kombinujících obojí.

Ne vše lze ale vyřešit pomocí chytrého mobilu a Internetu. Mohu odeslat email, zjistit si program kin, ale co když najednou potřebuji důležitý soubor uložený na podnikovém serveru a nejsem zrovna v práci? Nebo co dělat v případě, že firma otevřela novou pobočku v úplně jiném městě a pochopitelně by ráda využívala i zde podnikovou databázi a spoustu skvělých aplikací běžících na její centrále?

Budovat vlastní sítě přes rozsáhlá území je finančně velice nákladné a navíc to neřeší problém mobilních uživatelů, putujících z místa na místo a majících touhu přístupu k podnikovým datům a aplikacím odkudkoliv, kde se zrovna nachází. Pronájem datových linek je také poměrně nákladná záležitost a opět to nevyřeší problém mobility.

Nejsnazším a stále populárnějším řešením je využití celosvětové sítě Internet, jejíž infrastrukturu lze použít k vytvoření tzv. virtuální privátní sítě, která se tváří z pohledu uživatele jako síť skutečná. Stačí vlastně jen přístup k Internetu a problém vzdálených poboček a mobilních uživatelů je tím elegantně vyřešen.

Cílem práce je objasnit fungování virtuálních privátních sítí, jejich různá nastavení s následným dopadem na výkon. Toto vše bude nejprve zkoumáno v teoretické rovině a následně ověřeno na skutečném serveru a stanicích fungujících na platformě MS Windows.

V kapitole 1 je představena vrstvová architektura počítačových sítí, v následující kapitole 2 pak nejpoužívanější architektura TCP/IP, na níž je postavena celosvětová síť Internet. Kapitola 3 slouží jako úvod do principů fungování virtuálních privátních sítí. V kapitole je 4 probráno šifrování, nezbytná technika

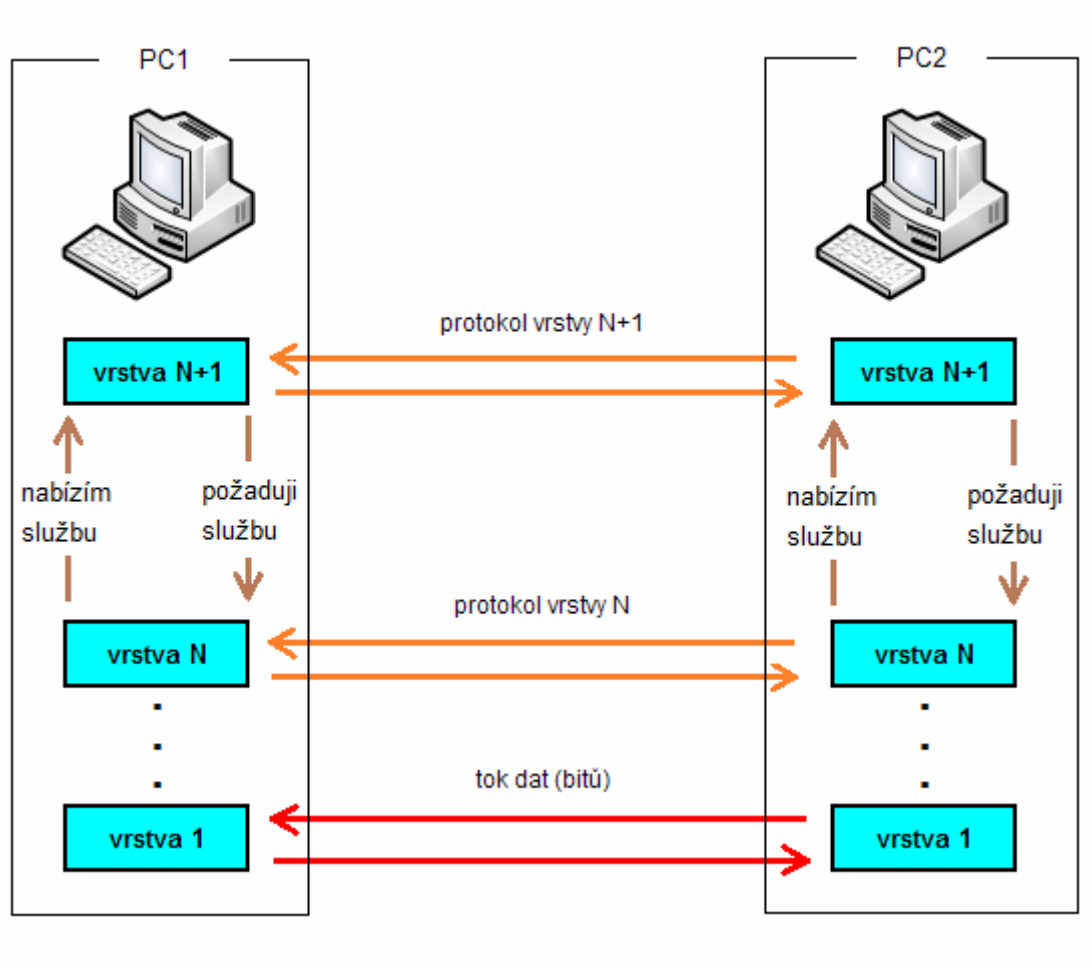
ochrany dat, která jsou přenášena přes sdílenou infrastrukturu. Kapitola 5 popisuje bezpečnostní rozšíření architektury TCP/IP, IP Security, umožňující šifrování a autentizaci dat. Kapitola 6 představuje virtuální privátní sítě na platformě Windows. Kapitola 7 popisuje metodiku testování výkonnosti jak přímého zapojení, tak jednotlivých VPN řešení. V poslední kapitole 8 jsou zveřejněny a vyhodnoceny výsledky testů přímého zapojení i jednotlivých VPN řešení.

1 Architektura počítačových sítí

1.1 Vrstvové modely počítačových sítí

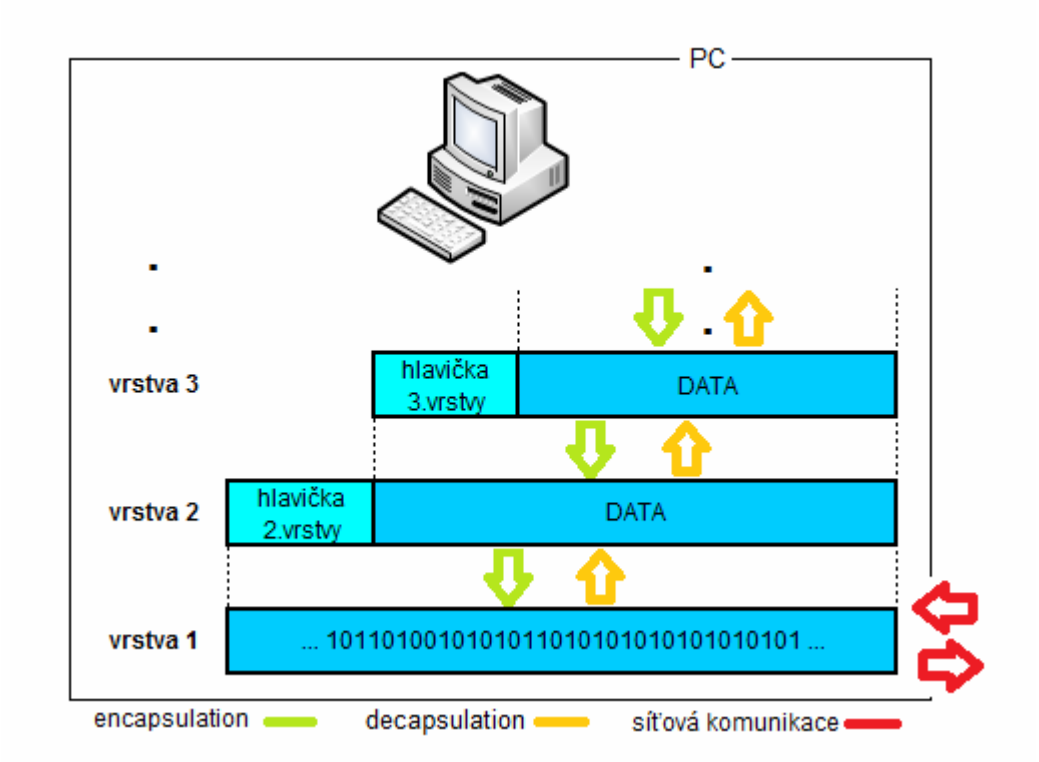
Síťová komunikace mezi počítačovými systémy se skládá z mnoha úkolů (kam a jak doručit požadovaná data, v jaké podobě doručit požadovaná data,...) a hrozí při ní mnoho problémů (zahlcení sítě, hardwarové poruchy, ztráta / poškození dat, neúnosné zpoždění dat, multiplicita dat,...). Principem vrstvových modelů počítačových systémů je oddělit vzájemně jednotlivé dílčí úkoly síťové komunikace do tzv. vrstev tak, aby každá vrstva řešila jen určitou část komunikace.

Tyto vrstvy jsou hierarchicky uspořádané, každá vrstva (kromě té nejvyšší) poskytuje sousední vyšší vrstvě službu, má danou funkci a je schopna komunikovat se stejnolehlou vrstvou jiné entity pomocí nějakého konkrétního protokolu (obr. 1).



obr. 1: Obecný vrstvový model

Aby mohla být data na straně příjemce jednotlivými vrstvami korektně zpracována, je třeba v každé vrstvě připojit k samotným datům tzv. hlavičku obsahující pokyny pro příslušný protokol, jak s daty naložit. Tento proces se nazývá zapouzdření (angl. encapsulation), na straně příjemce pak dochází k vybalování (angl. decapsulation). Každá vrstva, krom té nejnižší, která většinou jen přenáší data, tedy znamená v síťové komunikaci nějakou režii navíc (obr. 2).

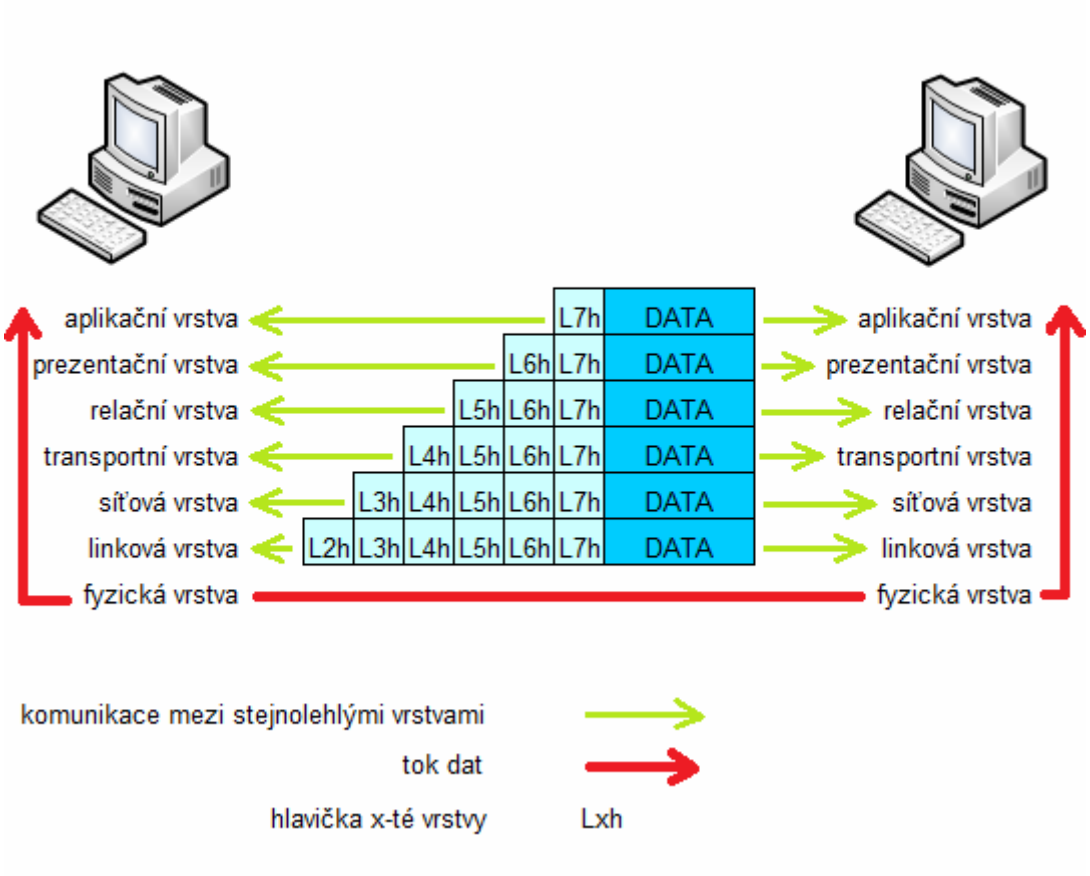


obr. 2: Encapsulation, decapsulation

Výčet všech vrstev modelu včetně popisu jejich činností definuje konkrétní síťový model počítačové sítě. Pokud k jednotlivým vrstvám navíc přiřadíme protokoly řešící úkoly dané vrstvy, nejedná se již o síťový model, tedy pouze jakési abstraktní schéma, ale o síťovou architekturu.

1.2 Referenční model ISO/OSI

Mezi aktuálně používanými síťovými modely je nejznámější a nejdůležitější síťový model OSI (Open System Interconnection). Byl vypracován organizací ISO (International Organization for Standardization) a v roce 1984 toutéž organizací přijat jako mezinárodní norma ISO 7498. Definuje 7 vrstev, angl. „layers“, většinou zkráceně označovaných jako L1 až L7 (obr. 3).



obr. 3: Schéma modelu ISO/OSI

Jednotlivé vrstvy tohoto modelu plní následující funkce:

L7 Aplikační – poskytuje aplikačním procesům přístup ke komunikačnímu systému.
L6 Prezentační – reprezentuje přenášená data tak, aby byla pro obě komunikující aplikační entity srozumitelná. Je to jediná vrstva modelu, ve které může docházet k modifikaci dat předaných vyšší vrstvou.
L5 Relační – řídí a synchronizuje dialog mezi komunikujícími prezentačními entitami.
L4 Transportní – propojuje síťovou a relační vrstvu. Data náležející určité relaci předává v požadované podobě síťové vrstvě a naopak. Odděluje horní, většinou softwarově založené vrstvy, od dolních, převážně hardwarových.
L3 Síťová – poskutuje síťové spojení komunikujících entit. Data přenáší v blocích, tzv. paketech. Zajišťuje směrování pro určení trasy těchto paketů mezi komunikujícími entitami.
L2 Linková – zajišťuje spojení mezi sousedními síťovými entitami. Data přenáší v blocích, tzv. datových rámcích.
L1 Fyzická – přenáší jednotlivé bity z jednoho místa na druhé, pomocí elektrických, nebo jiných signálů.

Model OSI se v praxi příliš nerozšířil. I v sítích, které z něj původně vycházely, je většinou modifikován. Běžně jsou např. vypuštěny vrstvy relační a prezentační, jejichž služby jsou jen velmi málo využívané, a proto často jen zbytečně zvyšují zátěž a objem přenášených dat.

Hlavní přínos tohoto modelu spočívá především v teoretickém popisu počítačových sítí a jejich přenosových mechanismů. Jednotlivé vrsty tohoto modelu a jejich funkce jsou v počítačové branži natolik vžité, že jsou používány i v obecné terminologii počítačových sítí, nejen v souvislosti s tímto modelem.

1.3 Referenční model TCP/IP

V roce 1969 došlo v USA ke spuštění sítě ARPANET (Advanced Research Projects Agency Network), původně jen experimentální počítačové sítě, ke které bylo připojeno několik univerzit a jejímž úkolem bylo ověřit fungování systému přepojování paketů v síti, která nemá žádnou centrální složku. Takováto síť je totiž velmi robustní, funguje i po zničení některé své části, např. při vojenském útoku.

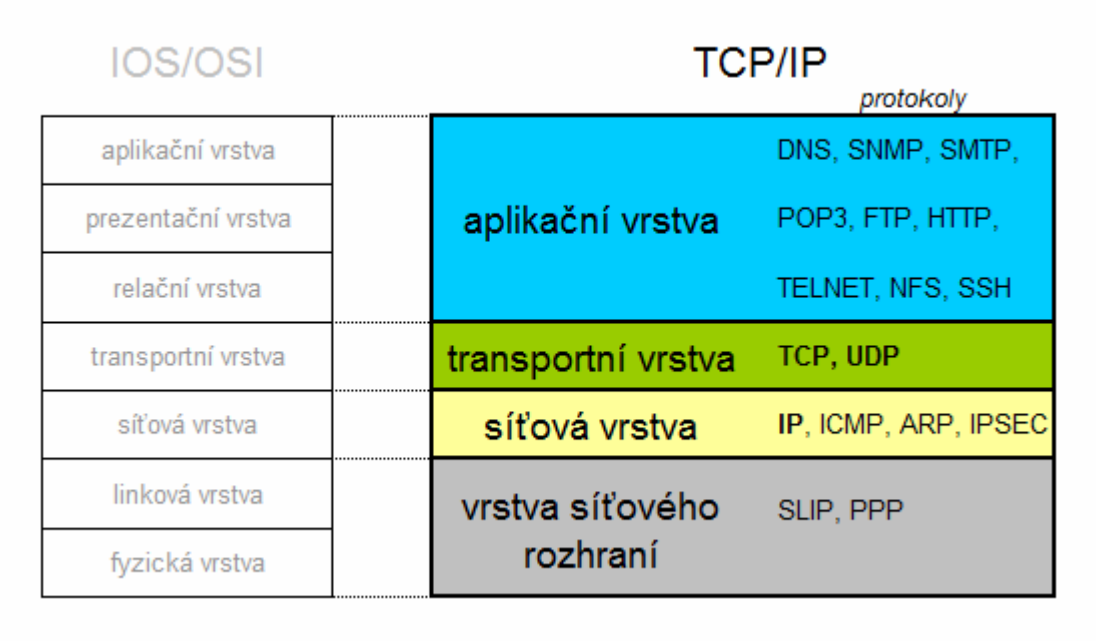
Experiment byl velmi úspěšný, paketový přenos a decentralizované řízení sítě se osvědčily, což mělo za následek postupné zvětšování této sítě, jak se k ní připojovaly další a další univerzity, později i sítě mimo akademickou sféru, až nakonec vznikla globální celosvětová sít, nazývaná Internet.

Nejprve bylo ovšem nutné vyřešit problém vzájemné komunikace nově připojovaných sítí fungujících na různých architekturách a protokolech. S tím bylo spojeno několik klíčových otázek: Kolik vrstev síťového modelu a s jakými funkcemi má mít nově vznikající globální síť? Lze použít některé již existující protokoly různých počítačových architektur, nebo je nutné vymyslet nové?

Snahou bylo vytvořit takový model sítě, který bude na vrstvách majících na starosti směrování a přenos dat (dle OSI jsou to vrstvy síťová, linková a fyzická) co možná nejjednodušší a poskytující jen nezbytné minimum, aby zůstala zachována hlavní vlastnost původního Arpanetu, robustnost, a samozřejmě také nízké náklady na budování a údržbu přenosové infrastruktury. Případné požadavky některých aplikací na spojovaný přenos, spolehlivý přenos, apod. by byly řešeny až ve vyšších vrstvách, které nejsou obsaženy přímo v přenosové infrastuktuře sítě, ale jen v komunikujících koncových uzlech.

Dále se ujala myšlenka, že není nutné vymýšlet něco, co již v nějaké podobě existuje, v tomto případě protokoly linkové a fyzické vrstvy, kterými komunikují počítače uvnitř jednotlivých sítí. Stačí jen definovat takový protokol síťové vrstvy, který bude fungovat nad všemi běžně se vyskytujícími protokoly linkovými.

V rámci snahy o vytvoření jednoduchého modelu sítě a vzhledem k tomu, že služby prezentační a relační vrstvy využívají jen některé aplikace, nebyly tyto vrstvy do nově vznikajícího modelu vůbec zahrnuty. Těm aplikacím, které vyžadují jejich služby, jsou tyto služby poskytovány až v rámci nejvyšší, aplikační vrstvy. Tak vznikl čtyřvrstvý model, resp. síťová architektura TCP/IP (obr. 4).

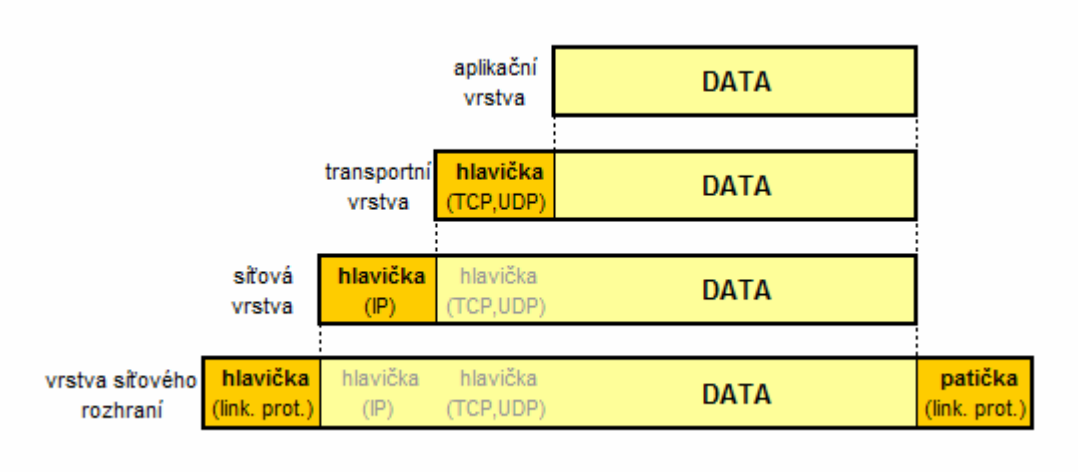


obr. 4: Architektura TCP/IP včetně některých protokolů

2 Síťová architektura TCP/IP

Jádrem čtyřvrstvé síťové architektury TCP/IP jsou síťové protokoly IP, jeho bezpečnostní rozšíření IPSec (IP security), služební protokol ICMP a transportní protokoly TCP a UDP. IPsec je probrán v samostatné kapitole, která následuje až po kapitole o šifrování, jenž je k pochopení principů fungování IPSec nezbytná.

V souladu s obecnou vrstevnatou filozofií dochází i v této architektuře při přenosu dat v síti k jejich zapouzdření u odesílatele a následnému vybalení u příjemce (obr. 5).



obr. 5: Zapouzdření v TCP/IP

2.1 Vrstva síťového rozhraní

Pro směrování na této vrstvě se používá linková adresa (též HW adresa, MAC adresa, nebo fyzická adresa). Její podoba závisí na použitém linkovém protokolu. Tato adresa identifikuje síťové rozhraní. Data jsou na této vrstvě balena do bloků, nazývaných rámce (angl. frame).

Směrování zajišťuje zařízení zvané přepínač (angl. switch), které přijme rámec z jednoho svého rozhraní, přečte z jeho hlavičky linkovou adresu a odešle jej na příslušné rozhraní. K tomuto účelu si uchovává ve své paměti tabulku linkových adres a k nim příslušných portů svých rozhraní.

V TCP/IP není tato vrstva definována, s výjimkou protokolů SLIP (Serial Line Internet Protocol) a PPP (Point-to-Point Protocol). Oba jsou určeny pro

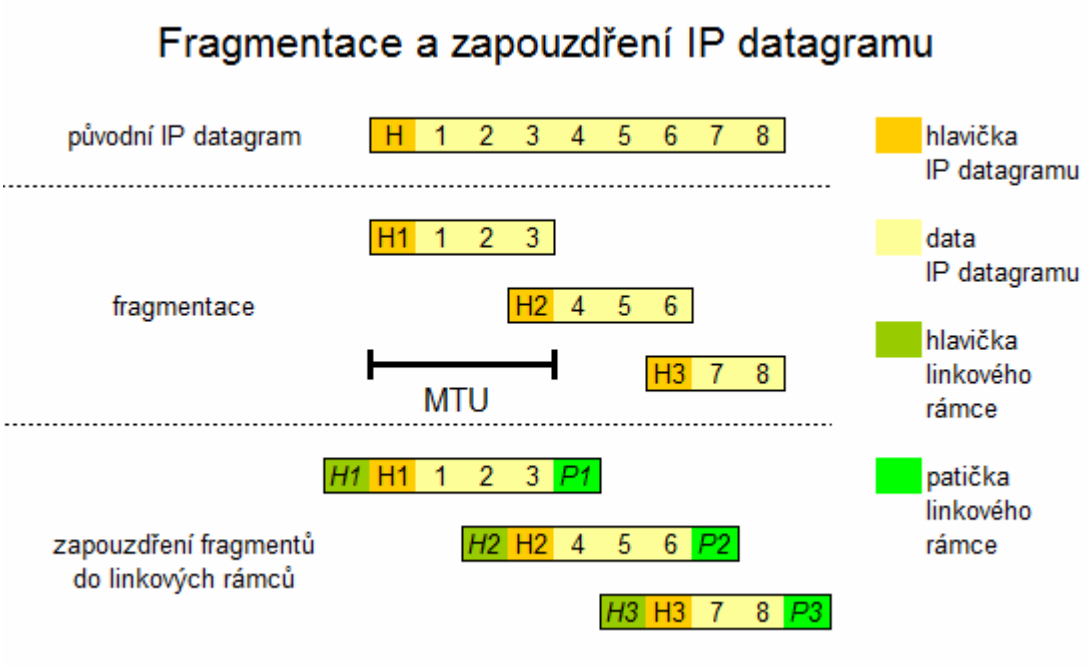
dvoubodové spoje, kde by znamenalo použití jiných linkových protokolů zbytečnou zátěž navíc, neboť tyto protokoly řeší přístupovou metodu na sdílené médium, kolize a další problémy, které se dvoubodových spojů netýkají.

Jednotlivé linkové protokoly mají různé maximální velikosti svých rámců. Parametr MTU (Maximum transmission unit) udává maximální velikost PDU (Protocol Data Unit, Protokolová datová jednotka) v B (angl. byte, jednotka množství dat v informatice znamenající 8 bitů), který lze vložit do příslušného linkového rámce.

2.2 Síťová vrstva

Ke směrování na síťové vrstvě slouží tzv. IP adresy. V IPv4 (Internet Protocol verze 4) se jedná o 32-bitové číslo. Většinou se zapisuje, kvůli lepší čitelnosti, v decimální podobě, po jednotlivých oktetech oddělených tečkami. Má dvě části: adresu sítě, sloužící ke směrování a adresu síťového rozhraní, identifikující toto rozhraní v rámci dané sítě. Adresu sítě lze určit z IP adresy pomocí prefixu (počet cifer zleva určujících adresu sítě z IP adresy v jejím binárním zápisu), nebo síťové masky (32-bitové číslo, zleva souvislá řada jedniček, zbytek nuly; konjunkcí po jednotlivých bitech IP adresy a její síťové masky dostaneme adresu sítě). V rámci celosvětové sítě Internet je IP adresa každého rozhraní jedinečná.

Data jsou na této vrstvě balena do bloků, označovaných jako IP datagramy (též pakety), které jsou následně vkládány do linkových rámců. Pokud je velikost IP datagramu větší, než MTU příslušného linkového protokolu, dochází k tzv. fragmentaci (obr. 6), kdy je IP datagram rozdělen na několik menších, které se již vejdou do linkového rámce. Fragmentace zvyšuje režii přenosu, neboť každý fragment musí být opatřen vlastní hlavičkou, u které musí být mj. vypočítán její kontrolní součet. Je proto dobré fragmentaci předcházet a nevytvářet větší IP datagramy, než je MTU použitého linkového protokolu.



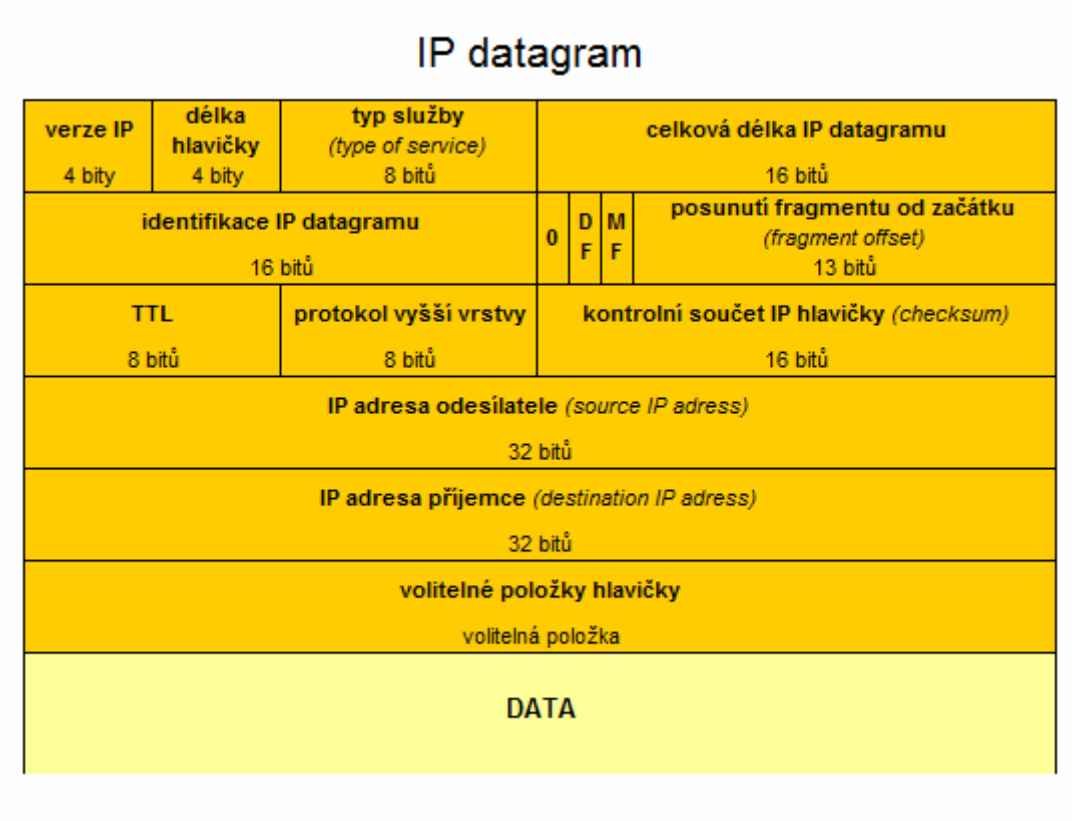
obr. 6: Fragmentace a zapouzdření IP datagramu

O směrování IP datagramů se stará směrovač (angl. router). Směrovač přijme některým svým rozhraním linkový rámec, vybalí z něj IP datagram, sníží položku TTL (většinou o 1), přepočítá kontrolní součet IP hlavičky a dle IP adresy příjemce odešle IP datagram příslušným rozhraním dál (tzn. opět ho zabalí do linkového rámce, ve kterém bude adresa odesílatele linkovou adresou daného směrovače a adresa příjemce linková adresa nejbližšího dalšího směrovače na cestě k příjemci). Zpracování IP datagramů směrovači je tedy mnohem náročnější a tím i pomalejší, než zpracování linkových rámců přepínači.

Převod z IP adresy na linkové adresy a naopak zajišťují protokoly ARP (Address Resolution Protocol) a RARP (Reverse Address Resolution Protocol).

2.2.1 Protokol IPv4

Nejdůležitějším protokolem síťové vrstvy je Internet Protocol, zkráceně IP. PDU tohoto protokolu je IP datagram s hlavičkou o velikosti 20 až 60 B (obr. 7). Úkolem IP protokolu je přenos IP datagramů v TCP/IP sítích. Funguje bez záruky, tzn. negarantuje doručení jednotlivých IP datagramů, pořadí doručení podle odeslání, ani zamezení duplicitního doručení.



obr. 7: IP datagram

verze IP – číslo verze IP protokolu

délka hlavičky – délka hlavičky v násobcích 4 B (pokud velikost hlavičky není násobkem 4 B, doplní se nevýznamnými daty)

typ služby – nepoužíváno; původně mělo sloužit k zajištění šířky přenosového pásma

celková délka IP datagramu – délka celého IP datagramu (hlavička + data) v B

identifikace IP datagramu – využíváno při fragmentaci pro identifikaci souvisejících fragmentů

0 – nevyužívaný příznak, napevno nastavená nula

DF – příznak *Don´t Fragment* (0 = povolení / 1 = zákaz fragmentace)

MF – příznak *More Fragments* (0 = je / 1 = není posledním fragmentem)

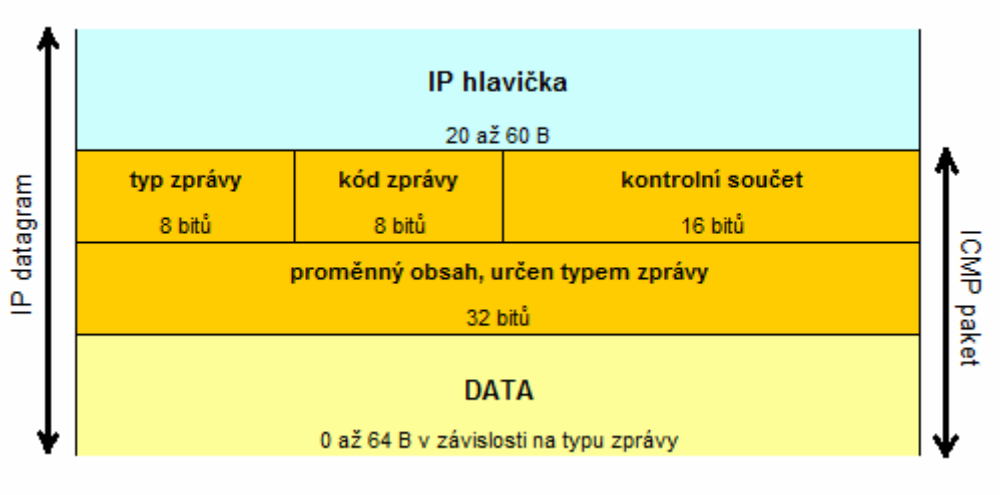
posunutí fragmentu od začátku – pozice v původním datagramu, na které začíná tento fragment (myšleno v datové části IP datagramu); uvádí se v násobcích 8 B

TTL – *time to live*, maximální počet průchodů směrovači; každým směrovačem je tato hodnota dekrementována, po dosažení nuly je datagram zahozen

protokol vyšší vrstvy – číselné označení protokolu, který je v IP datagramu přenášen (např. 6 – TCP, 17 - UDP)
kontrolní součet IP hlavičky – kontrolní součet počítaný z hlavičky IP datagramu
IP adresa odesílatele – IP adresa síťového rozhraní odesílatele
IP adresa příjemce - IP adresa síťového rozhraní příjemce
volitelné položky hlavičky – umožňují záznam průchodů směrovači, záznam času, explicitní směrování; max. velikost 40 B; z bezpečnostních důvodů jsou IP datagramy s volitelnými položkami většinou směrovačů zahazovány

2.2.2 Protokol ICMP

Zatímco o přenos datagramů se na síťové vrstvě stará protokol IP, řešení mimořádných událostí má na starosti služební protokol ICMP (Internet Control Message Protocol). Přestože se jedná o protokol síťové vrstvy, jeho pakety jsou baleny do IP protokolu (obr. 8), přičemž ale IP pracuje také na síťové vrstvě. Tato výjimka z pravidla o balení PDU vyšší vrstvy do PDU nižší vrstvy je způsobena potřebou dopravovat ICMP pakety i mimo lokální sítě.



obr. 8: ICMP paket

typ zprávy – hodnota v tomto poli určuje typ ICMP zprávy:
0 = odpověď na žádost o echo
3 = nedoručitelný IP datagram (neznámá/nedosažitelná cílová síť/uzel)
4 = snížit rychlost odesílání
5 = změnit směrování

8 = žádost o echo
9 = odpověď na žádost o směrování
10 = žádost o směrování
11 = vypršel čas (hodnota TTL byla směrovačem snížena na nulu, nebo se nepodařilo v daném čase adresátovi složit IP datagram z jeho jednotlivých fragmentů)
12 = neplatný parametr (v IP záhlaví)
13 = požadavek na časovou synchronizaci
14 = odpověď na časovou synchronizaci
17 = žádost o masku subsítě
18 = odpověď na žádost o masku subsítě
kód zprávy – jemnější dělení typů zpráv
kontrolní součet – kontrolní součet celého ICMP paketu
proměnný obsah – obsah tohoto pole závisí na typu zprávy

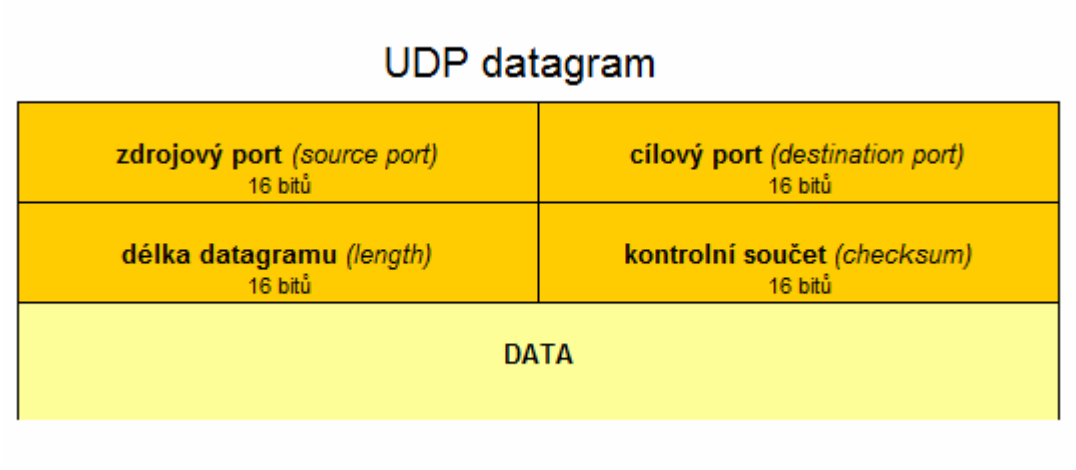
ICMP je využíván např. programem ping, kdy je nejprve odeslána na cílový uzel žádost o echo (typ zprávy = 8, kód zprávy = 0), cílový uzel pak odpovídá na echo (typ zprávy = 0, kód zprávy = 0).

2.3 Transportní vrsta

Adresou na transportní vrstvě je tzv. port, což je 16-ti bitové číslo identifikující protokol aplikační vrsty v rámci daného uzlu. Na serverech jsou vetšinou používány „dobře známé porty“ 0 až 1023 (např. 80 – HTTP, 25 - SMTP), na klientských stanicích dochází k náhodnému přidělení portu v rozsahu 1024 až 65565. Některé aplikační protokoly používají jiný „dobře známý port“ v případě transportního protokolu TCP a jiný v případě UDP, obecně je tedy aplikace v rámci daného uzlu jednoznačně identifikována dvojicí: transportní protokol + port.

2.3.1 Protokol UDP

Pro přenosy nepožadující spolehlivost doručování je určen protokol UDP (User Datagram Protocol). Data přenáší v UDP datagramech (obr. 9) obsahujících hlavičku pevné velikosti 8 B jen s těmi nejnutnějšími údaji.



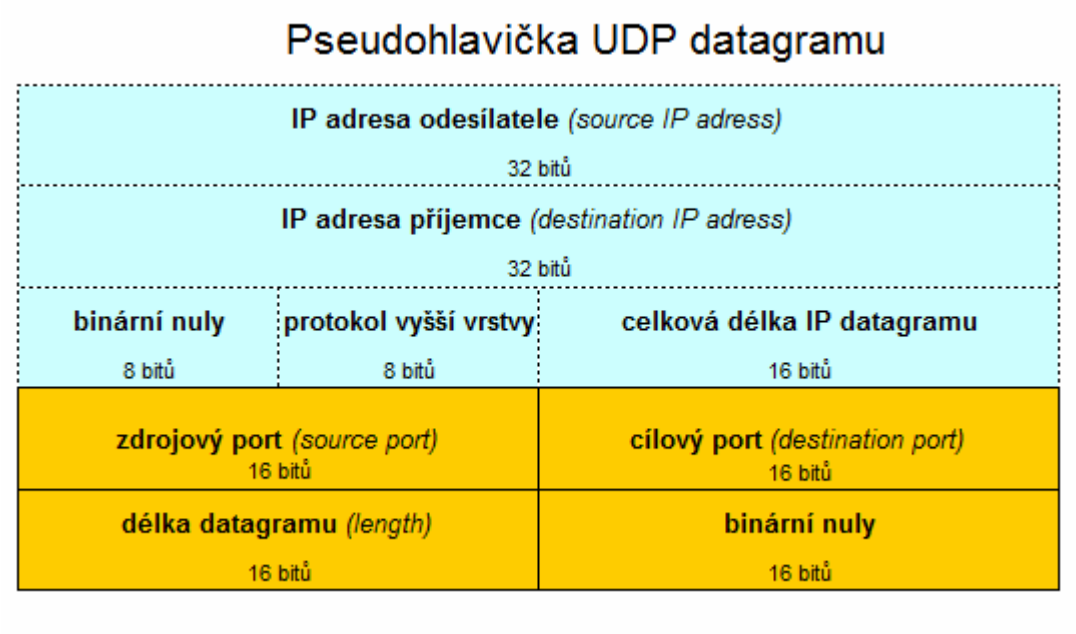
obr. 9: UDP datagram

zdrojový port – číslo portu odesílatele UDP datagramu

cílový port – číslo portu adresáta UDP datagramu

délka datagramu – celková délka datagramu (hlavička + data) v B

kontrolní součet – nepovinná položka; počítá se z tzv. pseudohlavičky, tj. hlavička UDP datagramu doplněná o některé položky z hlavičky IP datagramu (obr. 10)



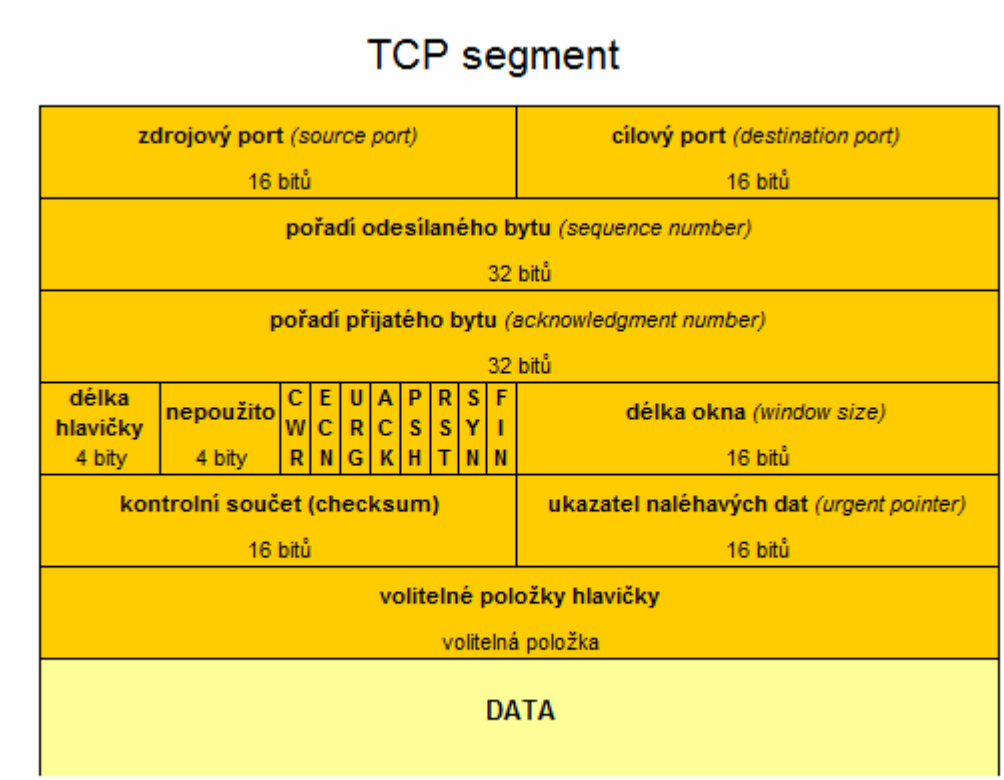
obr. 10: Pseudohlavička UDP datagramu pro kontrolní součet

2.3.2 Protokol TCP

Pro spolehlivé přenosy je určen protokol TCP (Transmission Control Protocol). Funguje stavově, data přenáší jako proud (angl. stream), s číslováním pořadí jednotlivých B, garantuje doručování svých PDU, což je vykoupeno vyšší režií na přenos, než v případě nespolehlivého UDP:

1. Nejprve je nutné navázat spojení. K tomu slouží trojcestný handshaking (angl. three-way handshake). Klient (ten, kdo žádá o navázání spojení) odešle TCP segment serveru s příznakem SYN a náhodně vygenerovaným číslem v poli „pořadí odesílaného B“ (x). Server odpoví TCP segmentem s příznaky ACK, SYN, polem „pořadí přijatého B“ (x+1) a svým náhodně vygenerovaným číslem v poli „pořadí odesílaného B“ (y). Následně klient odpoví TCP segmentem s příznakem ACK, a polem „pořadí přijatého B“ (y+1).
2. Poté je možné přenášet data.
3. Nakonec musí být spojení řádně ukončeno. Klient odešle segment s příznakem FIN, server odpoví segmentem s příznakem ACK. Komunikace klient → server je tím ukončena, opačným směrem ale stále lze dále přenášet data. Server odešle segment s příznakem FIN, klient odpoví segmentem s příznakem ACK. Komunikace klient ← server je tím ukončena.

Proud dat je balen do PDU zvaného TCP segment s velikostí hlavičky 20 až 60 B (obr. 11).



obr. 11: TCP segment

zdrojový port – číslo portu odesílatele TCP segmentu

cílový port – číslo portu adresáta TCP segmentu

pořadí odesílaného B – pořadové číslo prvního B toku dat od odesílatele k příjemci; číslování začíná od náhodně zvoleného čísla mezi 0 až 2^{32}-1

pořadí přijatého B – pořadové číslo posledního B toku dat, který příjemce přijal, navýšené o 1; číslování začíná od náhodně zvoleného čísla mezi 0 až 2^{32}-1

délka hlavičky – délka hlavičky v násobcích 4 B (pokud velikost hlavičky není násobkem 4 B, doplní se nevýznamnými daty)

CWR – příznak potvrzení přijetí TCP segmentu s nastaveným příznakem ECN

ECN – příznak nastaven, dokud není přijat segment s nastaveným příznakem CWR

URG – příznak „TCP segment obsahuje naléhavá data“

ACK – příznak „pole pořadí přijatého B je platné“

PSH – příznak „TCP segment obsahuje aplikační data“

RST – příznak „odmítnutí TCP spojení“

SYN – příznak „odesílatel nově nastavil pořadové číslo prvního odesílaného B“

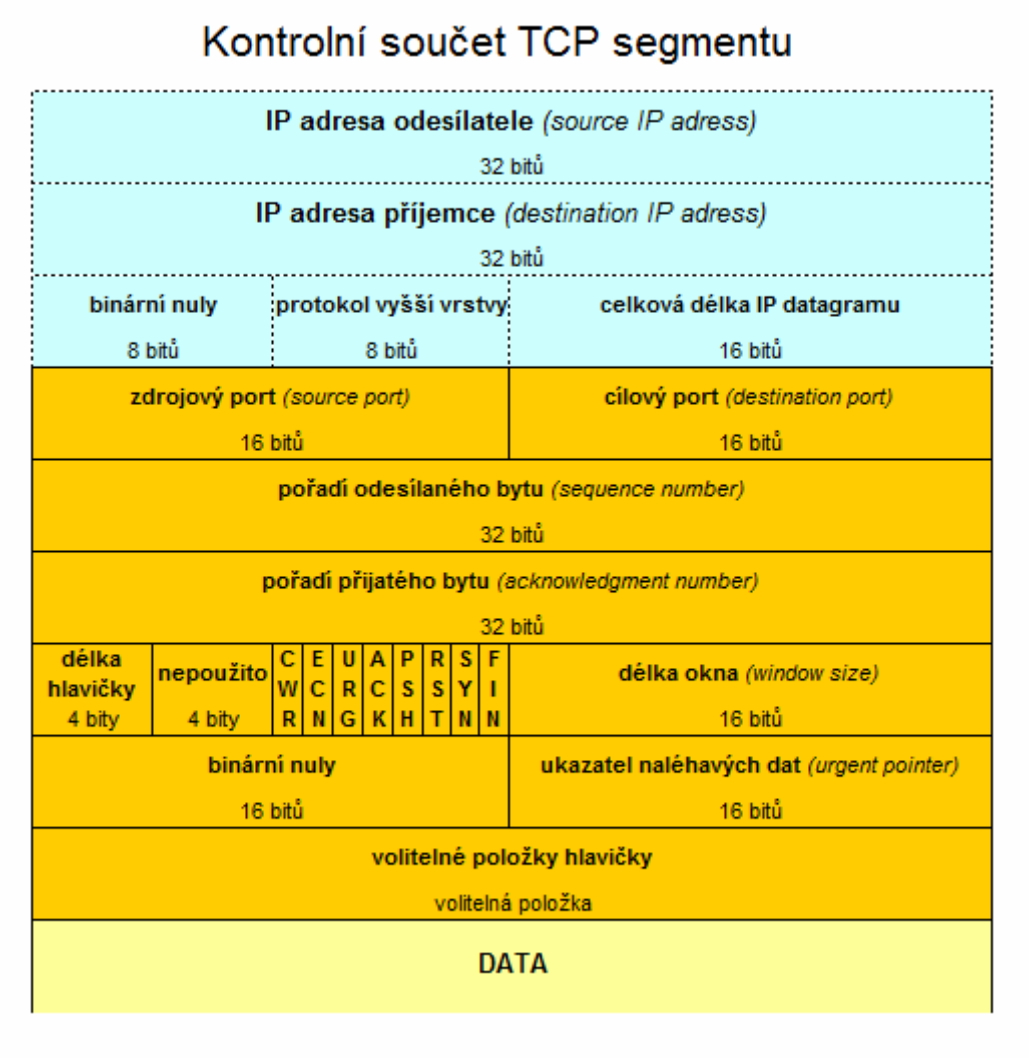
FIN – příznak „odesílatel ukončil odesílání dat“; nadále však může data přijímat

délka okna – příjemce určuje odesílateli, kolik aktuálně může poslat dat v B; velikost odeslaných a ještě nepotvrzených dat plus velikost právě odesílaných dat nesmí překročit hodnotu „délka okna“

kontrolní součet – počítá se z celého TCP segmentu (datová část je případně doplněna binárními nulami na sudou velikost v B) doplněného o některé položky z hlavičky IP datagramu (obr. 12)

ukazatel naléhavých dat – pokud je nastaven příznak URG, součet tohoto pole s polem „pořadí odesílaného B“ ukazuje na konec úseku naléhavých dat

volitelné položky hlavičky – max. velikost 40 B; lze použít např. pro časové razítko, maximální délku segmentu (MSS), zvětšení okna nad 16-bitů



obr. 12: Kontrolní součet TCP segmentu

2.4 Aplikační vrstva

Aplikace, přesněji řečeno aplikační protokoly, využívají pro svoji vzájemnou komunikaci protokoly transportní vrstvy. Pro spolehlivý přenos protokol TCP, pro nespolehlivý UDP. Hlavními úkoly aplikačních protokolů jsou definovat pravidla vzájemné komunikace aplikací běžících na různých uzlech a definovat formát předávaných dat, aby byl srozumitelný oběma komunikujícím stranám.

3 Virtuální privátní sítě (VPN)

V souvislosti s rozvojem informačních technologií v dnešní době dochází ke stále vzrůstající potřebě přesunu dat z místa na místo, nebo k nutnosti přístupu dat uložených na vzdálených místech. Jak již bylo naznačeno v úvodu této práce, budovat vlastní sítě, nebo pronajímat datové linky je zbytečně nákladné, když zde máme k dispozici celosvětovou síťovou infrastrukturu, Internet, kterou můžeme využít k propojení libovolných míst na celém světě.

S použitím sdílené infrastruktury podstupujeme samozřejmě bezpečnostní riziko, kdy přesouváme data po sdílené síti, kde mohou být útočníkem odchycena a následně zneužita. K zajištění zabezpečení datové komunikace přes sdílenou infrastrukturu byla vyvinuta technologie zvaná Virtuální privátní síť (VPN).

Jak již vyplývá ze samotného názvu VPN, jedná se o privátní síť, jejíž privátnost je pouze virtuální. Na logické úrovni se tedy tváří jako samostatní síť, ačkoliv na fyzické úrovni je pouze částí nějaké větší sítě.

3.1 Typy sítí VPN

Jelikož VPN funguje nad sdílenou infrastrukturou, její komunikace musí být pro zajištění privátnosti před zbytkem této infrastruktury nějakým způsobem skryta pomocí šifrování. Šifrovat komunikaci můžeme na různých vrstvách:

- aplikační

Na této úrovni může být šifrování řešeno programově, např. šifrovací metodou Pretty Good Privacy (PGP), používající algoritmus RSA asymetrického šifrování (viz kapitola 4.6 RSA). Šifrovány jsou však pakety pouze na aplikační vrstvě, údaje z hlaviček nižších vrstev nijak chráněny nejsou (výjimkou je např. program Secure Shell, který je schopen v režimu port-forwarding vytvořit zabezpečený komunikační tunel).

- transportní

I na této úrovni je chráněn pouze užitečný obsah komunikace, IP datagramy však šifrovány nejsou.

- síťová

Na síťové úrovni jsou již skryty informace z TCP záhlaví, navíc v případě použití tunelovacího režimu (což je zapouzdření jednoho paketu do jiného) lze skrýt i IP adresy a další pole z původní hlavičky IP datagramu. Pro VPN na této vrstvě se využívá převážně protokol IPSec, kterému je věnována samostatná kapitola č. 5.

- vrstva síťového rozhraní

Na této vrstvě jsou VPN nejčastěji realizovány protokoly Point-to-Point Tunneling Protocol (PPTP) a Layer 2 Tunneling Protocol (L2TP).

Jiný způsob, jak dělit VPN sítě, je podle typu připojení jednotlivých uzlů:
hostitel-hostitel: VPN spojení je vytvořeno mezi dvěma uzly
***hostitel-vstupní brána*:** VPN spojení je vytvořeno mezi uzlem a vstupní bránou do zbytku VPN sítě
vstupní brána-vstupní brána: VPN spojení je vytvořeno mezi dvěma, nebo více vstupními bránami

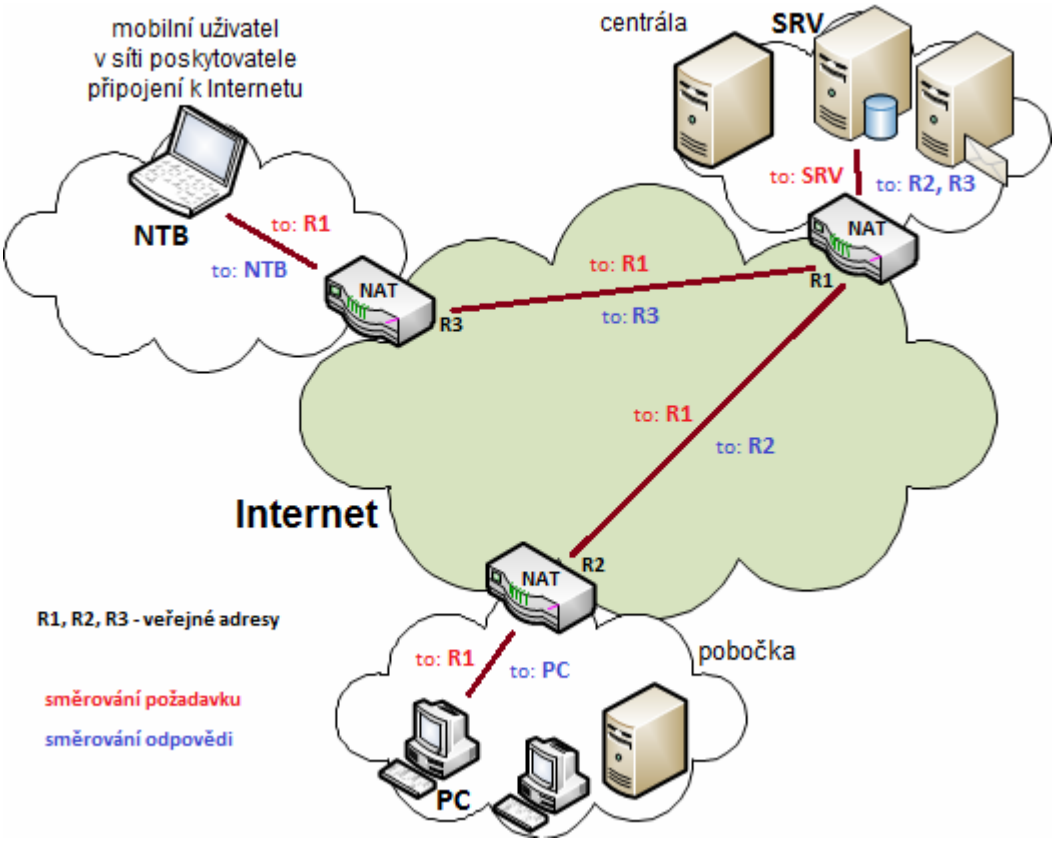
Vstupní brána je zařízení starající se o připojování vzdálených klientů a ostatních vstupních bran do části VPN umístěné z pohledu Internetu „za“ touto vstupní branou v místní síti. Může se jednat např. o směrovač, firewall, nebo VPN koncentrátor.

3.2 Překlad IPv4 adres (NAT/PAT), tunelování

Jak již bylo uvedeno v kapitole 2, IPv4 adresa každého uzlu v Internetu je jedinečná. To ale neplatí o místních sítích, kde se používají v drtivé většině tzv. privátní IP adresy. Jedná se o vyhrazené rozsahy, které nejsou v Internetu použity a tudíž v něm ani nemohou být směrovány:

10.0.0.0 až 10.255.255.255
172.16.0.0 až 172.31.255.255
192.168.0.0 až 192.168.255.255

Vzniká tedy problém, jak směrovat komunikaci používající privátní IP adresy přes Internet, kde jsou používány veřejné IP adresy. Řešením je překlad IP adres na rozhraní Internetu a místní sítě (obr. 13).



obr. 13: Překlad IPv4 adres (NAT)

Odesílatelem je směrováno vždy vnější rozhraní cílové místní sítě (R1, R2), nebo poskytovatele připojení k Internetu (R3), až v rámci cílové místní sítě směrujeme uzel přímo (SRV, PC, NTB). Překládat můžeme vnější IP adresu na vnitřní a naopak, tzv. Network Address Translation (NAT), nebo vnější adresu a port na vnitřní adresu a port, tzv. Port Address Translation (PAT). Druhá varianta se používá v případě, že nemáme k dispozici dostatek veřejných IP adres. Jednu veřejnou adresu lze tak využít pro více vnitřních uzlů, při překladu adres je rozliší číslo portu.

Díky NAT/PAT mohou používat pro vzájemnou komunikaci všechny subjekty připojené do stejné VPN (obr. 13 - pobočka, centrála, mobilní uživatel) IP adresy této sítě, i když ve skutečnosti spolu komunikují přes Internet, který používá

veřejné IP adresy z jiného rozsahu a privátní ani není schopen směrovat. Routery na rozhraní Internetu a místních sítí se tak stávají vstupními branami, kdy komunikaci směřující ven zapouzdřují - celý IP datagram je zašifrován a zabalen do jiného IP datagramu, kde je jako IP odesílatele uvedeno vnější rozhraní (myšleno rozhraní s veřejnou IP adresou) odesílající vstupní brány a jako cílová IP vnější rozhraní vstupní brány do cílové místní sítě. Tam dojde k vybalení paketu a jeho odeslání do cílového uzlu. Na tomto principu založené VPN spojení se nazývá **tunelovaná VPN linka**.

Tunely nemusejí vznikat jen mezi vstupními branami, mohou sahat „hlouběji“ do místních sítí, neboť vnější rozhraní cílové vstupní brány může být směrováno odkudkoliv. Tak můžeme vytvořit tunel typu uzel – vstupní brána, nebo uzel – uzel.

Tunelování zajišťuje kromě možnosti směrování dat přes Internet i jejich zabezpečení pomocí šifrování, což s sebou nese dodatečnou zátěž použitých šifrovacích algoritmů a zvýšený objem přenášených dat. Za výhodu zvýšené bezpečnosti platíme tedy snížením využitelné šířky pásma a vyšší výpočetní zátěží síťových prvků.

Pokud zašifrujeme jen datovou část IP datagramu, jedná se o tzv. **transportní VPN linku**, která sice nepřidává tolik výpočetní a přenosové zátěže navíc, ale zase poskytuje méně zabezpečení, neboť hlavička IP datagramu není zašifrována, jako v případě tunelované VPN linky.

3.3 Požadavky na bezpečnost

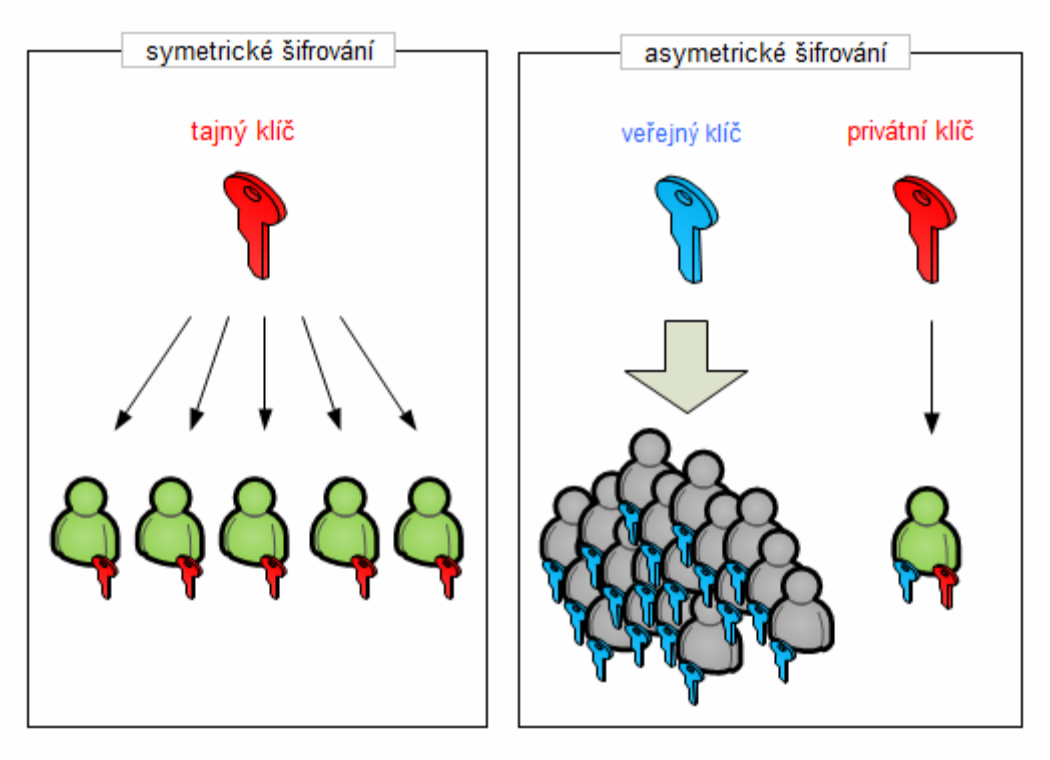
Jelikož pomocí VPN přenášíme soukromá data přes sdílenou infrastrukturu, musíme zajistit jejich integritu, tj. aby při přenosu nedošlo k úmyslné, či neúmyslné změně obsahu a jejich důvěrnost, tj. aby nebyla někým neoprávněným odchycena a následně zneužita. Obojí nám zajistí v této kapitole již zmíněné **šifrování**.

Dále je třeba ověřit původce dat, provést jeho **autentizaci**. Zda je skutečný odesílatel opravdu tím, za koho se vydává. Na základě úspěšného ověření může poté dojít k jeho autorizaci, tj. jaké činnosti jsou pro daného uživatele v systému povoleny a účtování, což je záznam jeho aktivit v systému. Celá tato architektura se nazývá Authentication, Authorization, Accounting (AAA).

4 Šifrování

Existují dva základní způsoby šifrování dat (obr. 14):

- **symetrické**, kdy používáme k šifrování i dešifrování stejný, tajný, klíč
- **asymetrické**, kdy používáme dvojici klíčů, veřejný a privátní, jeden pro šifrování, druhý pro dešifrování



obr. 14: Symetrické & asymetrické šifrování – distribuce klíčů

4.1 Symetrické šifrování

Máme pouze jeden klíč, tajný, který je sdílen oprávněnými uživateli. Tímto klíčem jeden uživatel zašifruje data a jiný je může stejným klíčem dešifrovat (obr. 15).

obr. 15: Symetrické šifrování

Většina symetrických šifer používá tzv. blokové šifrování, kdy jsou vstupní data rozdělena na úseky pevné délky. Na každý takovýto úsek je následně aplikován šifrovací algoritmus. Existují tři módy blokového šifrování:

ECB (Electronic Code Book)

Každý blok šifrujeme nezávisle na ostatních stejným klíčem. Jeho výhodou je, že jednotlivé bloky můžeme změnit a opětovně zašifrovat, aniž bychom museli zašifrovat znovu všechna data. Nevýhodou je, že bloky se shodným obsahem budou zašifrovány stejně, což poněkud snižuje bezpečnost šifry.

CFB (Cipher FeedBack):

Náhodně vybereme jeden blok dat, tzv. nultý (B0). Ten zašifrujeme (sifrB0), ale neukládáme. Se zašifrovaným nultým blokem provedeme opreraci XOR s prvním blokem ještě nezašifrovaných dat (sifrB0 XOR B1). Výsledkem je první zašifrovaný blok (sifrB1), který již uložíme. V dalších krocích vždy šifrujeme poslední uložený blok již zašifrovaných dat, s výsledkem provádíme operaci XOR s následujícím ještě nezašifrovaným blokem a výsledek ukládáme.

Výhodou CFB je, že bloky se shodným obsahem nebudou (většinou) zašifrovány stejně. Nevýhodou CFB je, že po změně jednoho bloku musíme opětovně zašifrovat všechna data. Poslední blok je totiž zašifrován jen pomocí operace XOR s předposledním blokem, můžeme tedy změnit jeho původní obsah, pokud změníme i příslušné bity zašifrovaných dat!

CBC (CipherBlockChaining):
Funguje stejně, jako CFB, jen se nejprve v každém kroku provádí operace XOR posledního zašifrovaného bloku a prvního ještě nezašifrovaného a až její výsledek se šifruje, čímž odpadá problém možnosti editace posledního bloku dat.

RC4 (též ARC4)
Kromě blokového šifrování existuje ještě šifrování proudové, kdy se šifruje po jednotlivých znacích, jeho možné využití je tedy při znakově orientovaných přenosech dat. Příkladem takové šifry je RC4. Tato šifra generuje pseudonáhodný proud, k šifrování pak používá operaci XOR na tento proud a šifrovaný text.

Výhodou symetrického šifrování je nižší algoritmická náročnost, než v případě asymetrického šifrování. Nevýhodou je problém distribuce klíčů (Jak bezpečně dopravit tajný klíč oprávněným uživatelům, aby nebyl cestou zachycen a následně zneužit?). Symetrické šifrování lze využít pro ochranu dat (dešifrovat data může jen některý z oprávněných uživatelů vlastnících tajný klíč).

4.1.1 DES

DES (Data Encryption Standard) je bloková šifra používající mód ECB a klíč délky 64 bitů, ve kterém je ale jen 56 bitů využito, zbylých 8 jsou paritní bity. Šifrovány jsou úseky dat o délce 64 bitů. Existuje jen 2^{56} variant tohoto klíče, což ho nečiní bezpečným vůči útokům hrubou silou. V letech 1977 až 2005 platila za standard pro šifrování dat v civilních státních organizacích v USA, již od roku 1999 ale nebylo doporučováno její používání v nových systémech.

4.1.2 TDES

Vylepšení předchozího algoritmu založené na jeho trojnásobné aplikaci se nazývá TDES (Triple DES). Spočívá v postupném šifrování dat klíči K1, K2 a K3. Pokud jsou všechny tři klíče na sobě nezávislé, efektivní délka klíče je 168 (3x56) bitů, v případě nezávislých K1, K2 a shodných K1, K3 je efektivní délka klíče 112 bitů. Pokud je aplikován stejný klíč třikrát po sobě, což znamená efektivní délku

klíče 56 bitů, jedná se o ekvivalent klasického DES (první aplikace klíče data zašifruje, druhá je dešifruje, třetí opět zašifruje), což umožňuje zpětnou kompatibilitu TDES s DES.

4.1.3 AES

AES (Advanced Encryption Standard) je bloková šifra používající mód ECB, šifrující úseky dat délky 128 bitů klíčem o délce 128, 192, nebo 256 bitů. Je algoritmicky méně náročná, než DES a zároveň odolná vůči útokům hrubou silou, neboť existuje 2^{128}, 2^{192}, nebo 2^{256} různých variant klíče v závislosti na jeho délce. Od roku 2002 je používána jako federální standard v USA.

4.1.4 Diffie-Hellman

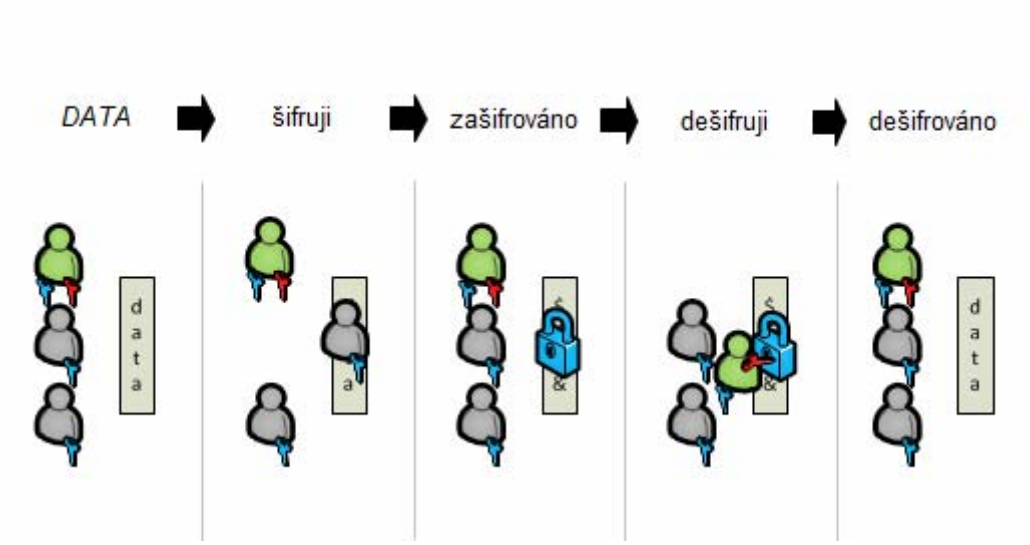
Pokud chtějí spolu dva subjekty (A a B) zabezpečeně komunikovat a nemají žádné klíče, řešením je kryptografický protokol, vynalezený v roce 1976 Whitfieldem Diffiem a Martinem Hellmanem, který umožňuje vytvořit zabezpečené spojení bez původní existence klíče. Jeho princip je následující:

1. A a B se dohodnou na prvočíslu p a přirozeném číslu n
2. A si zvolí „velké“ přirozené číslo a, B si zvolí „velké“ přirozené číslo b
3. A spočítá $n^a \bmod p$, B spočítá $n^b \bmod p$ a výsledky si zašlou
4. A spočítá $(n^b \bmod p)^a \bmod p$, B spočítá $(n^a \bmod p)^b \bmod p$
5. $(n^b \bmod p)^a \bmod p = (n^a \bmod p)^b \bmod p = n^{ab} \bmod p$ je nově vygenerovaný tajný klíč, kterým může být následující komunikace mezi A a B již šifrována

Protokol samotný neumožňuje autentizaci komunikujících stran, je zde tedy nebezpečí vstupu útočníka do komunikace. Klíč je ovšem vytvářen postupně a nikdy není zasílán ve své kompletní podobě. Útočník je pouze schopen zachytit čísla p, n, $n^a \bmod p$, $n^b \bmod p$. Bez znalosti čísel a a b ale není schopen spočítat hodnotu klíče.

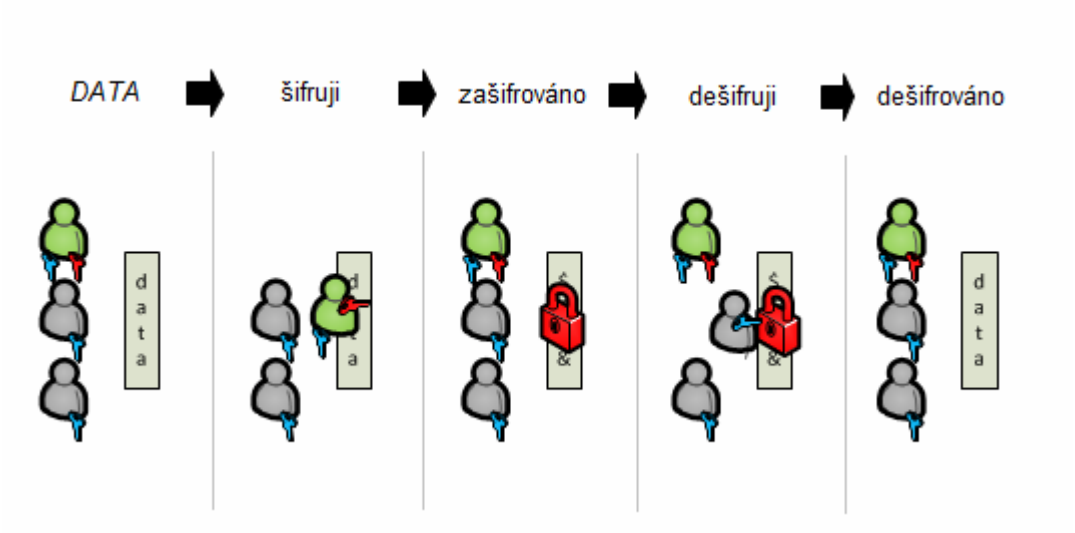
4.2 Asymetrické šifrování

V asymetrickém šifrování máme k dispozici dvojici vzájemně korespondujících klíčů. Pokud zprávu zašifrujeme jedním z nich, k dešifrování musíme použít ten druhý. Pro praktické použití je jeden klíč prohlášen za privátní, zůstává u majitele, druhý, veřejný, je dán k dispozici ostatním. Kdokoliv pak může zprávu zašifrovat veřejným klíčem adresáta, přičemž pouze adresát, majitel privátního klíče, je schopen zprávu dešifrovat (obr. 16). Tohoto postupu lze využít pro ochranu dat (poslat data může kdokoliv, dešifrovat data může jen majitel privátního klíče).



obr. 16: Asymetrické šifrování veřejným klíčem

Možné je i opačné použití, kdy je zpráva zašifrována privátním klíčem odesílatele, kterou poté může kdokoliv dešifrovat jeho veřejným klíčem (obr. 17). V tomto případě je ověřen odesílatel zprávy.



obr. 17: Asymetrické šifrování privátním klíčem

Výhodou asymetrického způsobu šifrování je snadná distribuce klíčů, kdy privátní klíč zůstává u majitele a veřejný je dán k dispozici ostatním. Nevýhodou je vyšší algoritmická náročnost šifrování, než v případě symetrického.

V praxi se často kombinuje symetrické i asymetrické šifrování: Nejprve subjekt A vygeneruje náhodný tajný klíč K určený pro symetrické šifrování, který zašifruje veřejným klíčem subjektu B a takto zašifrovanou zprávu mu zašle. Subjekt B zprávu dešifruje svým privátním klíčem, díky čemuž má i on k dispozici tajný klíč K. Nyní již spolu oba subjekty mohou zabezpečeně komunikovat rychlejším symetrickým šifrováním pomocí klíče K.

4.3 Hash

Funkci, převádějící libovolně dlouhý úsek dat na číslo pevně dané délky, zvané otisk zprávy, a splňující následující požadavky, nazýváme hash:

- i sebemenší změna vstupních dat se projeví velkou změnou výstupní hodnoty
- z výsledné hodnoty nelze odvodit podobu původních dat
- v případě dvou rozdílných vstupů je i vysoká pravděpodobnost rozdílného výstupu

V praxi se nejčastěji setkáme s hashovací funkcí SHA (Secure Hash Algorithm), což je celá sada hashovacích algoritmů s otisky zpráv délky 160 až 512 bitů.

4.4 Elektronický podpis

Mějme situaci, kdy chce odesílatel zprávy zajistit, aby tato zpráva dorazila v nezměněné podobě adresátovi. Toho může docílit následovně: Nejprve pomocí vybrané hashovací funkce získá otisk této zprávy, který následně zašifruje svým privátním klíčem. Poté zprávu odešle a přiloží k ní i její zašifrovaný otisk. Adresát spočítá z došlé zprávy (pomocí stejné hashovací funkce jako odesílatel) její otisk a zároveň dešifruje pomocí veřejného klíče odesílatele otisk došlý se zprávou. Pokud se oba otisky, spočítaný i dešifrovaný, shodují, zpráva nebyla cestou změněna. Navíc je potvrzené, že jejím autorem je skutečně odesílatel, neboť příjemce použil k dešifrování otisku zprávy jeho veřejný klíč. Otisk (též hash) zprávy zašifrovaný privátním klíčem odesílatele se nazývá „elektronický podpis“.

4.5 Certifikační autorita, PKI a digitální certifikát

S používáním veřejných klíčů je spojeno i jedno riziko: Jak ověřit, že je veřejný klíč skutečně spojen se subjektem, za který se vydává? Možným řešením je princip přenosu důvěry, kdy někdo, komu sami důvěřujeme, tzv. certifikační autorita, ověří totožnost majitele veřejného klíče a následně tento klíč elektronicky podepíše, čímž nám garantuje, že je majitel tohoto klíče opravu tím, za koho se vydává. Takto pojatý systém správy veřejných klíčů se nazývá PKI (Public Key Infrastructure). Řídí se standardem X.509, který specifikuje formát a parametry certifikátů, způsoby ověřování jejich platnosti a seznamy odvolaných certifikátů. Elektronicky podepsaný veřejný klíč se nazývá digitální certifikát.

4.6 RSA

Prvním algoritmem, určeným k šifrování i podepisování zpráv, je RSA z roku 1977, pojmenovaný dle iniciálů jeho autorů (Rivest, Shamir, Adleman). Funguje na předpokladu, že rozložit „velké“ číslo na součit prvočísel, tzv. faktorizace, je výpočetně velice náročná úloha, narozdíl od opačné operace, násobení.

Nejprve si musí komunikující strany vytvořit klíče, které následně mohou používat k zašifrování, dešifrování a elektronickému podepisování zpráv:

Vytvoření klíčů: Jedna komunikující strana, označme ji A, si zvolí dvě „velká“ různá prvočísla p, q. Spočítá jejich součin n = p * q a hodnotu Eulerovy funkce $\varphi(n) = (p-1)(q-1)$. Zvolí si číslo x, které je menší, než $\varphi(n)$ a je s ním nesoudělné a spočítá jeho multiplikativní inverzi $y = x^{-1}$, tzn. musí platit $y * x \equiv 1 \pmod{\varphi(n)}$. Veřejným klíčem je pak dvojice (n, x), privátním klíčem dvojice (n, y). Veřejný klíč dá A k dispozici druhé straně B, privátní si ponechá. Obdobně postupuje i B při tvorbě klíčů.

Šifrování: B chce zaslat zprávu A. Zprávu převede dohodnutým způsobem na číslo z, $z < n$. Spočítá $c = z^x \bmod n$ a zašle c nezabezpečeným kanálem A.

Dešifrování: A z čísla c spočítá $z = c^y \bmod n$. Následně převede číslo z dohodnutým způsobem na původní zprávu.

Elektronický podpis: Jak již bylo vysvětleno v kapitole o elektronickém podpisu, odesílatel zašifruje hash zprávy svým privátním klíčem, příjemce dešifruje veřejným klíčem odesílatele.

5 IP security (IPSec)

Největším nedostatkem protokolu IPv4 je nemožnost zabezpečit přenášená data, což bylo, vzhledem k jeho používání nad sdílenou infrastrukturou, Internetem, jeho největší slabinou. Z tohoto důvodu vzniklo jeho bezpečnostní rozšíření, umožňující autentizaci a šifrování obsahu IP datagramu, zvané IP security, zkáceně IPSec (RFC 2401).
Protokol IPSec může pracovat ve dvou režimech, transportním a tunelovacím.

V **transportním režimu** probíhá komunikace typu hostitel-hostitel, nelze jej použít v režimu vstupní brána-vstupní brána. Šifruje se pouze datová část IP datagramu, nelze tedy skrýt informace o IP adresách komunikujících uzlů. Tento režim se používá převážně při komunikaci počítačů ve stejné síti. Při jeho použití ve veřejné síti, jako je Internet, je vhodné použít ještě jiné bezpečnostní prostředky.

V **tunelovacím režimu** dochází k zapouzdření celého původního datagramu, tudíž jsou šifrovány i informace v jeho hlavičce. Může se používat při všech typech komunikace: hostitel-hostitel, hostitel-vstupní brána a vstupní brána-vstupní brána.

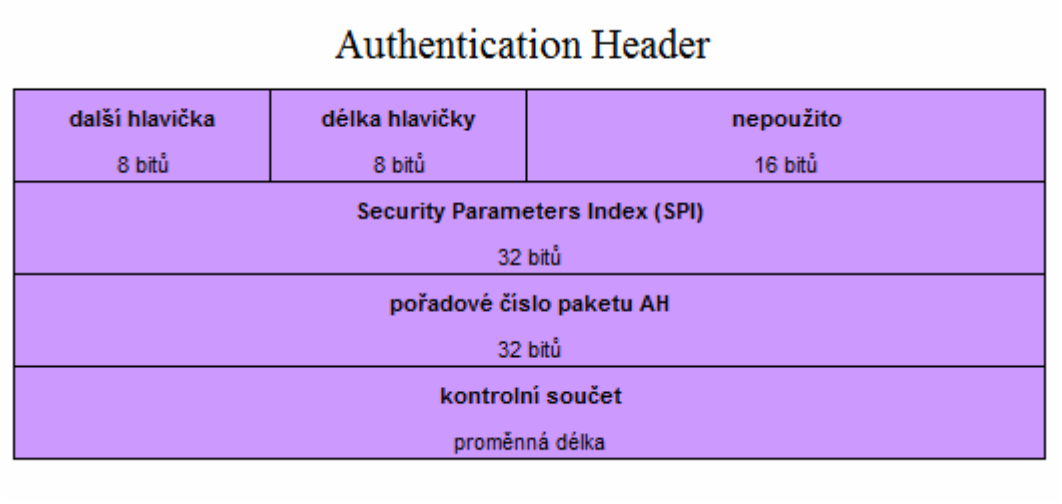
Právě komunikace vstupní brána-vstupní brána je poslední dobou v praxi nepopulárnější, neboť stačí provést konfiguraci těchto bran a klientské počítače v různých sítích spolu přes ně mohou komunikovat, aniž by je bylo nutné nějak speciálně nastavovat. O zapouzdření a vybalení datagramů se starají vstupní brány na koncích tunelů a komunikující strany o jejich existenci ani nemusejí vědět.

I když je v tunelovacím režimu zašifrován celý původní IP datagram a útočník tedy nemůže zjistit IP adresy komunikujících stran, přesto může zjistit IP adresy vstupních bran a tedy určit sítě, které spolu komunikují.

IPSec je tvořen mechanismy: Authentication Header (AH), Encapsulating Security Payload (ESP), IP Security Association Key Management Protocol (ISAKMP) a Internet Key Exchange (IKE). V novější verzi protokolu IP, IPv6, je již IPSec integrován.

5.1 AH

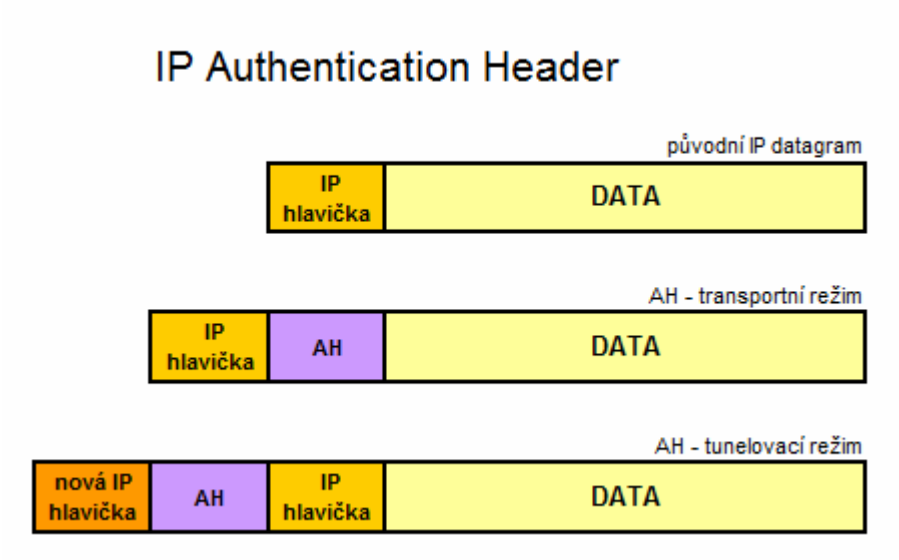
Authentication Header (AH, obr. 18) zajišťuje autentizaci komunikujících stran, integritu dat a ochranu proti útoku, kdy jsou opětovně posílána již odeslaná data.



obr. 18: Authentication Header

další hlavička – číslo vnořeného protokolu (obdoba pole „protokol vyšší vrstvy“ v IP datagramu)
délka hlavičky – délka hlavičky v násobcích 4 B, snížená o hodnotu 2
Security Parameters Index (SPI) – číslo spojení odchozích IP datagramů, identifikované podle IP adres a portů komunikujících stran a použitého protokolu vyšší vrstvy
pořadové číslo paketu AH – pořadové číslo odesílaného paketu zamezující případnému útoku opakováním již odeslaného paketu
kontrolní součet – počítá se z celého IP Authentication Header, u IP hlavičky (v tunelovacím režimu u nové IP hlavičky) jsou vynechána pole, která se mohou při přenosu měnit (např. TTL)

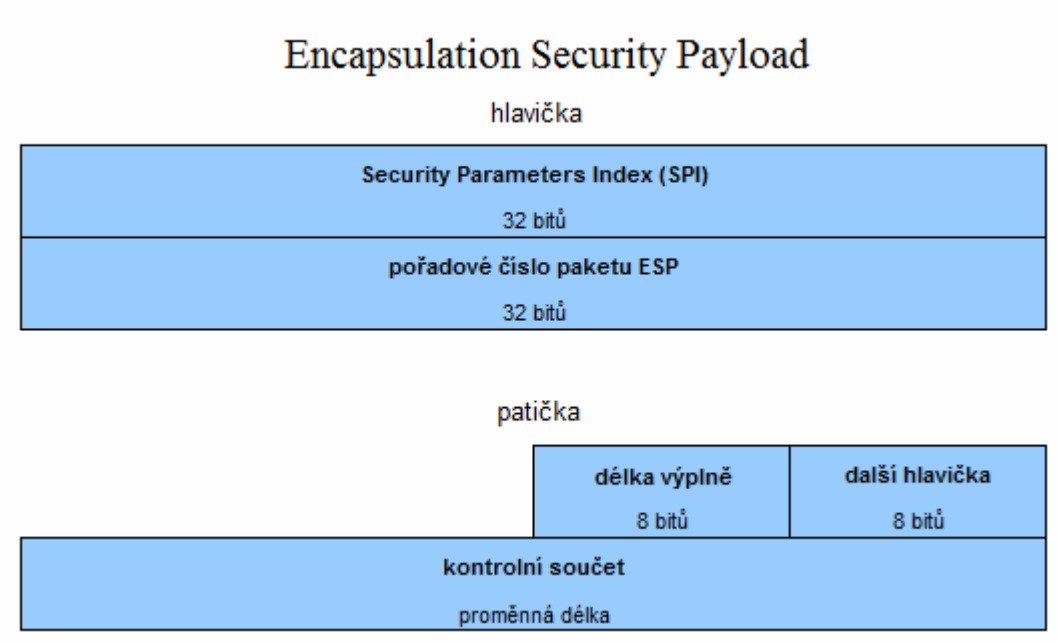
V transportním režimu se AH vkládá do IP datagramu mezi jeho hlavičku a data. V tunelovacím režimu se vkládá před původní IP datagram a za nově vytvořenou hlavičku IP datagramu (obr. 19).



obr. 19: IP Authentication Header

5.2 ESP

Encapsulation Security Payload (ESP, obr. 20) ovládá stejné bezpečnostní mechanismy, jako AH, navíc přidává možnost šifrování dat.



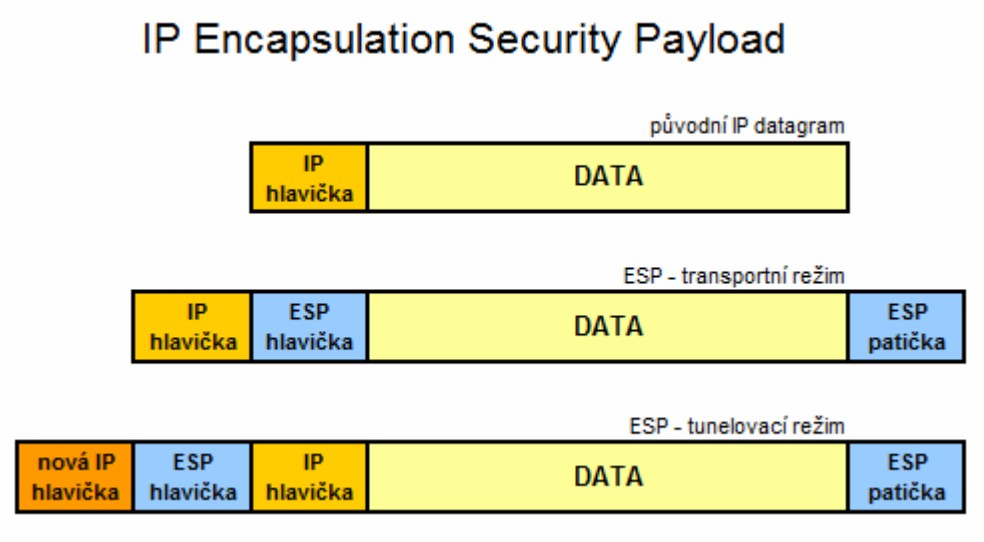
obr. 20: Encapsulation Security Payload

Security Parameters Index (SPI) – stejný význam jako u AH

pořadové číslo paketu ESP – stejný význam jako u AH

délka výplně – šifruje se blokovou šifrou, data tedy musí být zarovnána výplní na násobek bloku (0 znamená žádná výplň)
další hlavička – stejný význam jako u AH
kontrolní součet – počítá se obdobně, jako u AH

Použití kontrolního součtu je volitelné, záleží na dohodě obou komunikujících stran. Totéž platí o šifrování. Stejně jako u AH, máme dva režimy přenosu, transportní a tunelovací (obr. 21).



obr. 21: IP Encapsulation Security Payload

5.3 ISAKMP

Položka SPI v AH i ESP identifikuje odchozí spojení IP datagramů. Každý takovýto datagram musí být nejprve na straně odesílatele zachycen, podle hodnoty SPI určeno spojení a na datagram aplikovány příslušné Security Policy (SP), což jsou oběma komunikujícími stranami předem domluvená pravidla zabezpečení (autentizace, kontrolní součet, šifrování). Tato pravidla jsou uložena v databázi Security Policy Database (SPD) o jejíž dynamické plnění se stará protokol Internet Security Association Key Management Protocol (ISAKMP). Jednotlivá SP jsou v SPD identifikována hodnotou SPI, cílovou IP adresou a použitým protokolem (AH, nebo ESP) – tato trojice se nazývá Security Association (SA). SA je ukazatelem na jednotlivá SP v databázi SPD.

Než tedy může začít probíhat mezi dvěma stranami komunikace protokolem IPSec, musí dojít pomocí protokolu ISAKMP k dohodě na SP a vytvoření SA záznamu v databázi SPD. SP se mohou v obou směrech komunikace lišit, nebo mohou být shodná.

5.4 IKE

Vlastní dialog dvou stran o nastavení SA zajišťuje protokol Internet Key Exchange (IKE). Celý proces navázání komunikace protokolem IPSec má dvě fáze:

Fáze 1 (nastavení ISAKMP SA)
Můžeme zvolit ze dvou módů, pomalejšího „main“, nebo rychlejšího „aggressive“.

„main“ mód (6 zpráv):
1. A → B návrh IKE SA
2. A ← B akceptuji návrh IKE SA
3. A → B info o klíči (pozměněný Diffie-Hellman algoritmus)
4. A ← B info o klíči (pozměněný Diffie-Hellman algoritmus)
5. A → B autentizace (elektronický podpis, šifrování veřejným klíčem, apod.)
6. A ← B autentizace (elektronický podpis, šifrování veřejným klíčem, apod.)

„aggressive“ mód (3 zprávy):
1. A → B návrh IKE SA, info o klíči
2. A ← B akceptuji návrh IKE SA, info o klíči, autentizace
3. A → B autentizace

Fáze 2 (nastavení IPSec SA)
Ve fázi 2 je jen jeden mód, komunikace je již šifrovaná.

„quick mód“
1. A → B hash 1, návrh IPSec SA
2. A ← B hash 2, akceptuji návrh IPSec SA
3. A → B hash 3

Na konci jsou celkem tři SA. Dvě IPSec SA pro příchozí a odchozí spojení a jedna ISAKMP SA pro „quick mód“ fáze 2 (po vyčerpání časového limitu, nebo limitu přenosu dat je nutné znovu nastavit IPSec SA).

6 VPN na platformě Windows

Informace uvedené v této kapitole platí pro kombinaci VPN serveru Windows Server 2008 a klienta Windows 7, na kterých budou následně probíhat testy.

6.1 Ověřování vzdáleného přístupu ve Windows

Existuje několik způsobů autentizace vzdáleného přístupu v Microsoft Windows Server 2008:

6.1.1 Protokol PAP

Password Authentication Protocol (PAP) používá heslo ve formátu prostého textu. Jedná se o nejméně zabezpečený protokol, který se obvykle používá v případě, že se vzdáleně přistupující klient a server nemohou dohodnout na bezpečnějším autentizačním protokolu.

6.1.2 Protokol CHAP

Challenge Handshake Authentication Protocol (CHAP) funguje na principu výzva-odpověď. K zašifování odpovědi používá hashovací funkci MD5. Server, kde běží služba Směrování a vzdálený přístup, podporuje CHAP pro ověření klientů, kteří ho vyžadují. Protokol CHAP požaduje zpětně šifrované heslo, z tohoto důvodu se doporučuje použití jiného protokolu pro autentizaci.

6.1.3 Protokol MS-CHAP v2

Microsoft Challenge Handshake Authentication Protocol (MS-CHAP v2) poskytuje oboustrannou autentizaci. Obě komunikující strany, server i klient, prokazují znalost hesla klienta. Nejprve server vyzve klienta, ten odpoví a požádá o následné potvrzení server. Jestliže server neprokáže znalost hesla klienta správnou odpovědí na výzvu, komunikace je ze strany klienta ukončena.

Protokol MS-CHAP v2 jako jediný ověřovací protokol Windows 2008 podporuje změnu hesla uživatele během jeho přihlašování.

6.1.4 Protokol EAP

Extensible Authentication Protocol (EAP) zprostředkovává komunikaci klienta a ověřovatele (server vzdáleného přístupu, nebo server RADIUS). Nestará se přímo o proces autentizace.

EAP-Transport Level Security (EAP-TLS) je typ ověřování pracující s certifikáty. Zajišťuje ověření, volbu šifrování a určení klíčů.

EAP-RADIUS předává zprávy od ověřovatele na server RADIUS, který provádí vlastní ověřování.

6.1.5 Protokol MPPE

Microsoft Point-to-Point Encryption (MPPE) se používá k šifrování dat u telefonických připojení protokolem PPP a VPN připojení protokolem PPTP. Šifrovací klíče jsou generované v rámci ověřovacího procesu pomocí MS-CHAP, MS-CHAP v2, nebo EAP-TLS. Používá 40, 56, nebo 128-bitové klíče.

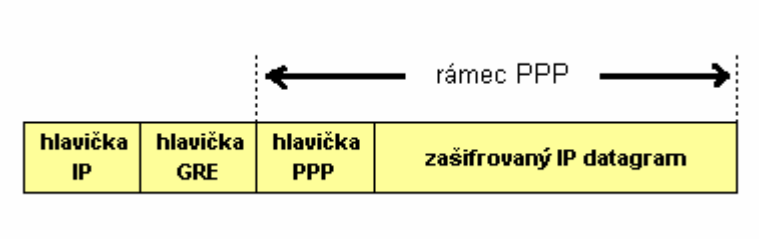
6.2 Popis jednotlivých VPN řešení

6.2.1 PPTP

Point-to-Point Tunneling Protocol (RFC 2637) používá k zapouzdření komunikace hlavičky protokolů PPP a GRE (Generic Encapsulation Protocol), viz. obr. 22.

PPP je protokol pro dvoubodové spoje. Ve skutečnosti se jedná o protokoly dva. LCP (Link Control Protocol) navazuje spojení a testuje konfiguraci, NCP (Network Control Protocol) slouží vyšším vrstvám pro přenos samotných dat.

Protokol GRE se používá k zapouzdření paketů přenášených VPN tunelem. Hraniční směrovač odesílatele přidá hlavičku GRE k paketu, hraniční směrovač v přijímající síti přečte informace ze záhlaví GRE, vyjme paket a pošle jej dál k cíli. Je to čistě směrovací protokol, neumí šifrovat přenášená data.



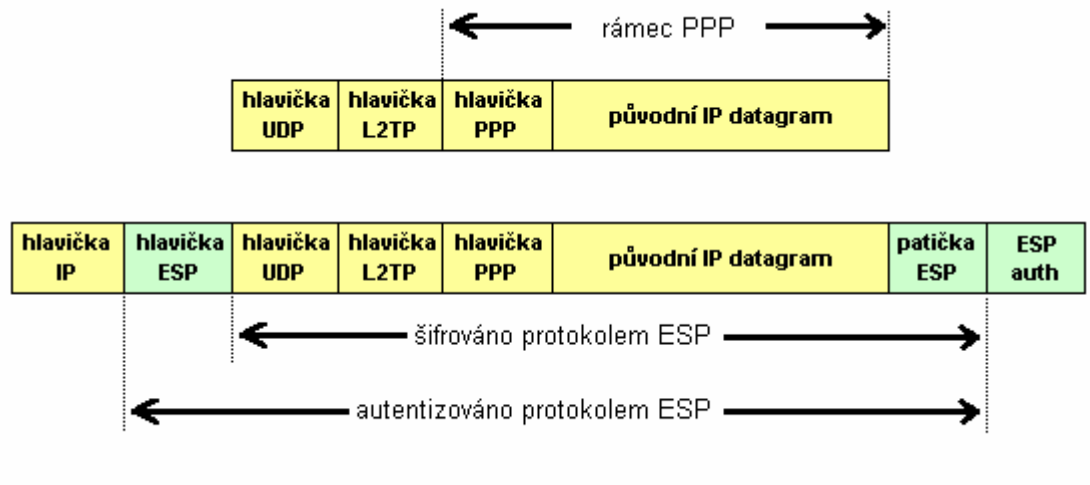
obr. 22: PPTP zapouzdření

K šifrování dat na OS Windows se využívá protokolu MPPE (Microsoft Point-to-Point Encryption), který vytváří klíče pro relace na základě hesel a to pomocí MS-CHAP v2, nebo EAP-TLS. K samotnému šifrování používá 128-bitový klíč a algoritmus RC4. Bezpečnost zašifrovaných dat je tedy mj. závislá na kvalitě hesla. Volitelně lze data komprimovat protokolem MPPC (Microsoft Point-To-Point Compression). Šifrování i případná komprese se týká jen původního IP datagramu, tedy datové části PPP rámce.

Spojení se navazuje též pomocí protokolů MS-CHAP v2, nebo EAP-TLS. PPTP používá dvě relace, jedna je klasická PPP s GRE zapouzdřením a slouží pro přenos dat, druhá na TCP portu 1723 slouží k navázání a řízení té první.

6.2.2 L2TP/IPSEC

VPN řešení kombinující linkový protokol L2TP se zabezpečením IPSec (popsán v kapitole 5) se nazývá L2TP/IPSec (RFC 3193).



obr. 23: L2TP/IPSec zapouzdření

Zapouzdření má dvě fáze (obr. 23):

1. Nejprve se před rámec PPP přidá hlavička L2TP, obsahující mj. ID tunelu a ID spojení a dále se připojí UDP hlavička. To je L2TP zapouzdření.

2. Tato L2TP zpráva je následně zašifrována a zapouzdřena ESP, vypočítán kontrolní součet pro její integritu a autentizaci (v položce auth ESP) a obalena IP hlavičkou.

O šifrování, integritu i autentizaci zpráv se stará ESP sám. Šifrovacím algoritmem je TDES, o integritu a ověření zpráv se stará algoritmus SHA1.

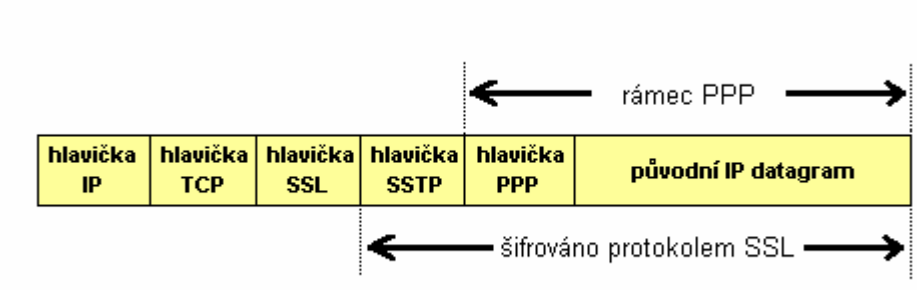
Navázání spojení se provádí pomocí IKE. Z parametrů SA se poté naváže šifrovaná komunikace pomocí ESP v tunelovacím režimu. Následně se vytvoří L2TP tunel mezi koncovými body.

6.2.3 SSTP

Secure Socket Tunneling Protocol využívá pro vytváření VPN sítí standardní webový port 443 protokolu Secure Socket Layer version 3 (SSL). SSL je protokol vložený mezi transportní a aplikační vrstvu, který poskytuje zabezpečení komunikace šifrováním a autentizací komunikujících stran. Komunikace přes port 443 je obrovskou výhodou, neboť tento port nebývá na většině směrovačů blokován.

K navázání spojení se využívá certifikátu ověření serveru a asymetrického šifrování, k přenosu dat se již poté používá rychlejší šifrování symetrické (viz kapitola 4).

Šifrovacím algoritmem je AES s 256-bitovým klíčem, o integritu a ověření zpráv se stará SHA a 256-bitový klíč.



obr. 24: SSTP zapouzdření

Postup navázání spojení je následující:

1. **K** (Klient) naváže pomocí TCP protokolu spojení se **S** (Serverem) na portu 443
2. **K → S** SSL protokolem pošle zprávu „chci SSL relaci“
3. **S → K** certifikát ověření serveru
4. **K→ S** potvrdí certifikát, nabídne šifrování, vygeneruje symetrický klíč relace SSL a zašifruje jej veřejným klíčem certifikátu serveru
5. **S → K** dešifruje SSL klíč svým privátním klíčem; K i S tedy mají klíč relace SSL, od této chvíle je komunikace šifrována tímto klíčem
6. **K→ S** vyjedná se SSL tunel a spojení PPP

6.3 Srovnání PPTP, L2TP/IPSEC, SSTP

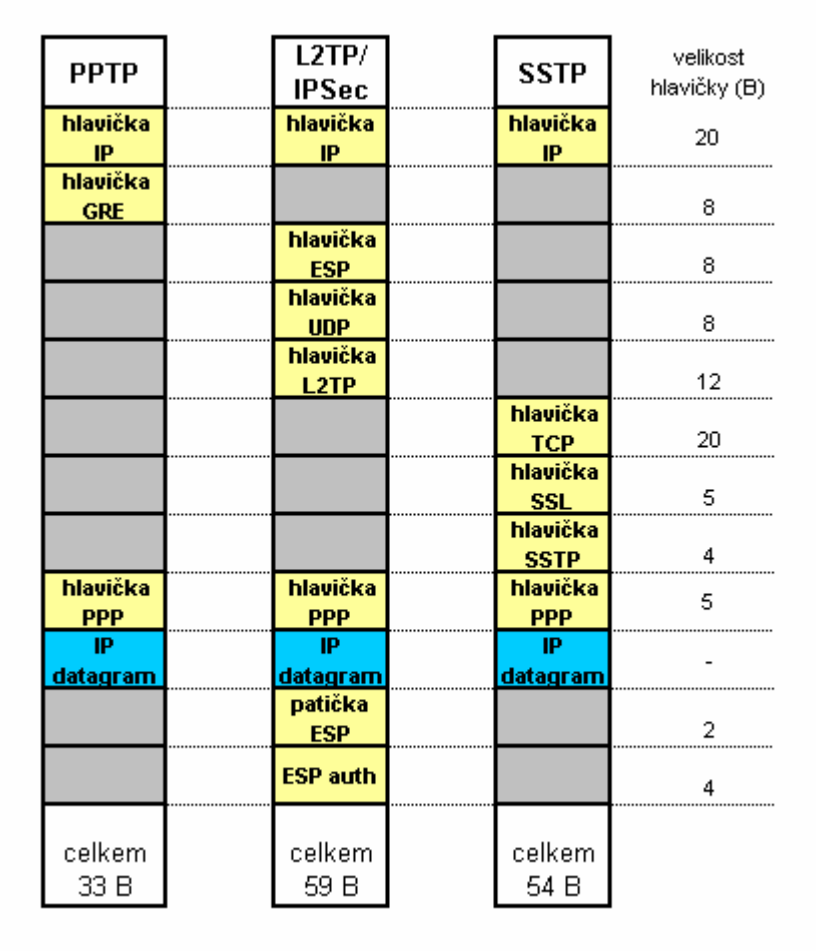
Abychom mohli odhadnout výkon jednotlivých VPN řešení, musíme nejprve vědět, kolik činí objem navíc přenášených dat a jak náročné zabezpečovací techniky šifrování dat se používají.

6.3.1 Nárůst objemu přenášených dat

Na obr. 25 vidíme, o kolik B se zvýší s každým IP datagramem vstupujícím do VPN tunelu objem přenášených dat. Nejméně je to u PPTP, následuje SSTP a L2TP/IPSec. Skutečné hodnoty mohou být vyšší, neboť některé hlavičky obsahují volitelné položky, případně se datová část dorovnává na daný násobek B.

Uvedená čísla rozhodně nejsou nízká. Když použijeme Wireshark a sledujeme síťový provoz, vidíme např. IP datagramy nesoucí ICMP dotaz (velikost 60 B), nebo DNS dotaz (velikost 63 B), tedy spoustu „malých“ IP datagramů putujících v síti, jejichž velikost se může při použití VPN řádově zdvojnásobit.

U „velkých“ IP datagramů, např. u TCP spojení přenášejících soubory, zase může dojít k tomu, že nebude možné zapouzdřený IP datagram vložit do linkového rámce, neboť jeho velikost bude přesahovat parametr MTU a tudíž bude muset být fragmentován.

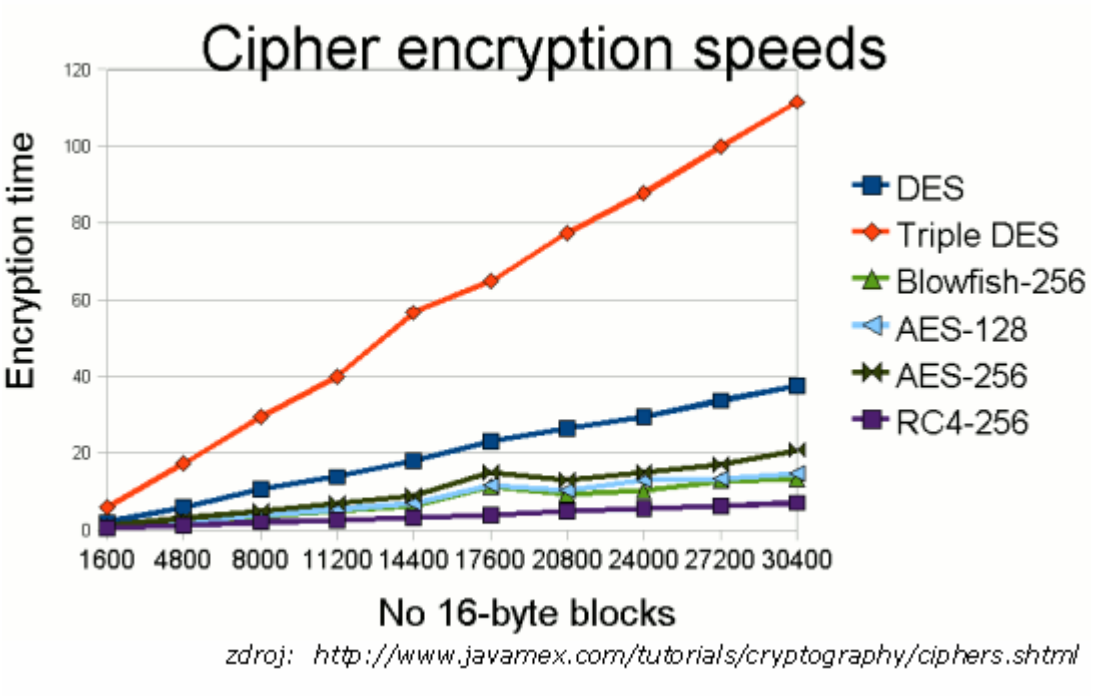


obr. 25: Nárůst objemu přenášených dat v B

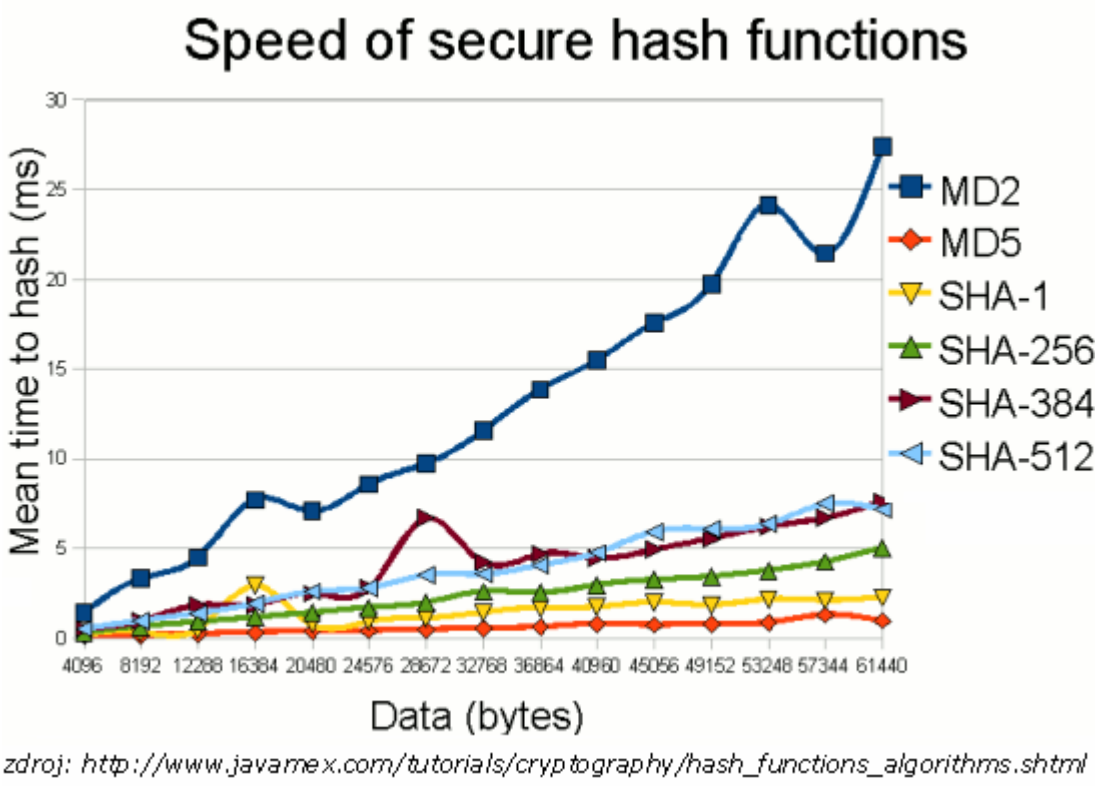
6.3.2 Šifrování dat

Srovnání rychlosti šifrovacích algoritmů použitých pro utajení přenášených dat ukazuje obr. 26, čerpající ze zdroje [13]. Nejrychlejší algoritmus RC4 používá PPTP, pomalejší AES-256 používá SSTP a nejpomalejší TDES používá L2TP/IPSec.

Srovnání rychlosti hashovacích funkcí zajišťujících integritu a autentizaci dat ukazuje obr. 27, čerpající ze zdroje [13]. Rychlejší algoritmus SHA1 používá L2TP/IPSec, pomalejší SHA256 používá SSTP, PPTP hashovací funkci nepoužívá.



obr. 26: Srovnání algoritmů RC4, TDES, AES-256



obr. 27: Srovnání algoritmů SHA-1, SHA-256

6.3.3 Odhad výkonnosti

PPTP má nejmenší režii přenosu dat ze všech tří VPN řešení, data šifruje nejrychlejší algoritmem a o jejich integritu se nestará. **PPTP by tedy měla vykazovat nejvyšší výkonnost**. L2TP/IPSec přidává o něco více dat k přenosu, než SSTP, ale především šifruje data několikanásobně pomalejším algoritmem, než SSTP. SSTP sice používá zhruba dvojnásobně pomalejší hashovaní algoritmus, ale zde je nutné si uvědomit, že hashovací algoritmy jsou jednosměrné funkce a jejich složitost je tedy v porovnání se šiframi obecně nižší. Pomalejší hashovací funkce u SSTP tedy neeliminuje vliv jeho rychlejšího šifrovacího algoritmu a o něco nižší přidané datové zátěže. **L2TP/IPSec by tedy měla vykazovat nejnižší výkonnost a SSTP by měla být se svojí výkonností mezi oběma zbylými**.

7 Metodika testování

Testování proběhne na platformě Microsoft Windows. Nejprve popíšeme testovací sestavu: server Windows Server 2008, stanici Windows 7 a síťové prvky včetně jednotlivých schémat zapojení. Poté popíšeme konfiguraci VPN na serveru i stanici. Nakonec budou popsány jednotlivé testy, jejichž výsledky budou následně srovnány s našimi odhady z předchozí kapitoly.

7.1 Testovací síť

7.1.1 Server

Model: IBM eServer xSeries 346 (Type 8840)
CPU: dual-core Intel Xeon 3.0GHz, 2x 2MB L2 cache
RAM: 4GB DDR2 400MHz ECC SDRAM RDIMM
HDD: 2x 150GB Ultra320 SCSI, RAID 0
Network: BroadCom NetXtreme 10/100/1000 Ethernet

OS: Microsoft Windows 2008 Enterprise 32-bit EN (Service Pack 1)
Computer name: SERVER
Domain: TEST-FIRMA

Server je nainstalován jako řadič domény „TEST-FIRMA“. Obsahuje role Active Directory Domain Services, DNS Server a DHCP Server. Na serveru jsou nainstalovány programy Wireshark 1.8.8, hrPING 5.04 a iperf 2.0.5.

Pro účely testování byl na serveru vytvořen doménový uživatel „UZIV“, pod kterým bodou testy ze stanice spouštěny.

7.1.2 Stanice

Model: Notebook ASUS K54C
CPU: dual-core Intel Pentium CPU B950 2.1GHz
RAM: 2GB DDR3 1333MHz SO-DIMM
HDD: Seagate ST9320325AS 320GB SATA300, 5400 rpm, 8MB Cache
Network: Atheros AR8151 10/100/1000 Ethernet
Wireless: Atheros AR9485WB-EG 802.11n

OS: Microsoft Windows 7 Ultimate 32-bit EN (Service Pack 1)
Computer name: PC
Domain: TEST-FIRMA

Na stanici jsou, stejně jako na serveru, nainstalovány programy Wireshark 1.8.8, hrPING hrPING 5.04 a iperf 2.0.5.

7.1.3 Router

Model: TP-LINK TL-WR1043ND
Network: 4x 10/100/1000 Mbit/s LAN, 1x 10/100/1000 Mbit/s WAN
Wireless: 802.11b/g/n

Router obsahuje 4 LAN porty pro místní síť, kde se chová jako přepínač na L2 vrstvě. Dále obsahuje jeden WAN port pro připojení k Internetu. Lze jej využít i jako Wi-Fi přístupový bod standardů 802.11b/g/n.

7.1.4 Kabely

Pro datovou komunikaci jsou použity standardní UTP (Unshielded twisted pair) kabely kategorie 5E podporující rychlosti až 1000Mbit/s. Délka kabelů je 3 metry.

7.1.5 SW Wireshark

Zřejmě nejpopulárnějším open-source síťovým analyzátorem je software Wireshark. Umožňuje zachytávat data přímo ze sítě a to jak v promiskuitním módu, kdy zachytí všechny pakety putující sítí, tak v nepromiskuitním, kdy zachytává jen ty pakety, u kterých je adresátem. Zachycená data může ukládat v různých formátech pro pozdější znovunačtení a analýzu. Podporuje přibližně 800 protokolů všech vrstev. V testech je použita verze Wireshark 1.8.8.

S pomocí Wiresharku můžeme např. změřit s větší přesností dobu odezvy, než příkazem ping:

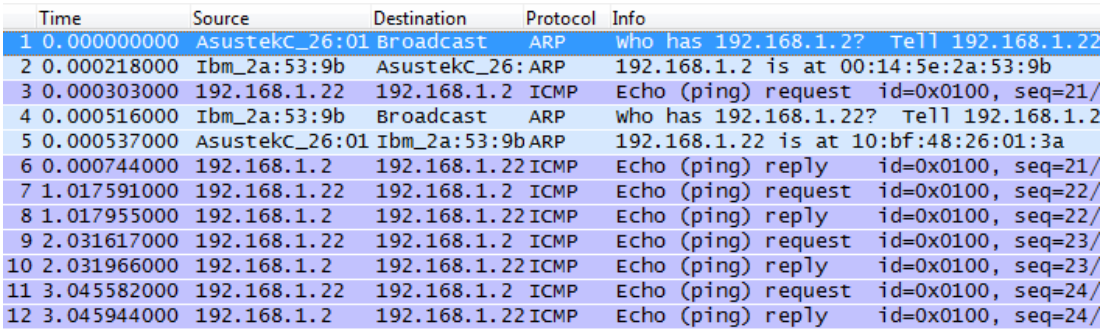
1. spustíme Wireshark
2. vybereme síťové rozhraní, na kterém chceme zachytávat komunikaci a klikneme na Start (Choose one or more interfaces to capture from, then Start)
3. menu Capture / volba Start → Wireshark začne zachytávat na vybraném rozhraní pakety
4. ping na cílovou stanici
5. ve Wiresharku uvidíme výslednou komunikaci, viz obr. 28.

	Time	Source	Destination	Protocol	Info
1	0.000000000	AsustekC_26:01	Broadcast	ARP	Who has 192.168.1.2? Tell 192.168.1.22
2	0.000218000	Ibm_2a:53:9b	AsustekC_26:	ARP	192.168.1.2 is at 00:14:5e:2a:53:9b
3	0.000303000	192.168.1.22	192.168.1.2	ICMP	Echo (ping) request id=0x0100, seq=21/
4	0.000516000	Ibm_2a:53:9b	Broadcast	ARP	Who has 192.168.1.22? Tell 192.168.1.2
5	0.000537000	AsustekC_26:01	Ibm_2a:53:9b	ARP	192.168.1.22 is at 10:bf:48:26:01:3a
6	0.000744000	192.168.1.2	192.168.1.22	ICMP	Echo (ping) reply id=0x0100, seq=21/
7	1.017591000	192.168.1.22	192.168.1.2	ICMP	Echo (ping) request id=0x0100, seq=22/
8	1.017955000	192.168.1.2	192.168.1.22	ICMP	Echo (ping) reply id=0x0100, seq=22/
9	2.031617000	192.168.1.22	192.168.1.2	ICMP	Echo (ping) request id=0x0100, seq=23/
10	2.031966000	192.168.1.2	192.168.1.22	ICMP	Echo (ping) reply id=0x0100, seq=23/
11	3.045582000	192.168.1.22	192.168.1.2	ICMP	Echo (ping) request id=0x0100, seq=24/
12	3.045944000	192.168.1.2	192.168.1.22	ICMP	Echo (ping) reply id=0x0100, seq=24/

obr. 28: Wireshark – příkaz PING, zdrojová stanice

Zajímavé jsou řádky 1,2,4,5, zbytek je již vždy žádost o echo a odpověď na žádost o echo. Stanice, na které jsme zadali příkaz ping, nezná linkovou adresu k IP adrese uvedené v příkazu ping, tak musí vyslat broadcast, aby ji zjistila (řádek 1). Cílová stanice tento broadcast přijme a odpoví na něj (řádek 2). Nyní již tedy může putovat žádost o echo ke svému cíli (řádek 3). Na řádku 4 zase zjišťuje stanice vysílající odpověď na žádost o echo linkovou adresu původce příkazu ping a na řádku 5 ji dostane. Důležitý závěr z tohoto výstupu komunikace tedy je, že čas první odezvy na žádost o echo byl prodloužen o dvojí zjišťování linkové adresy

protokolem ARP, což výrazně ovlivnilo jeho hodnotu. Dále je třeba si uvědomit, že čas odezvy se skládá z času putování ICMP paketu k cíli, doby zpracování v cíli a následné cesty ICMP paketu zpět. Na stanici přijímající žádosti o echo můžeme vidět ve Wiresharku toto (obr. 29):



	Time	Source	Destination	Protocol	Info
1	0.000000000	AsustekC_26:01	Broadcast	ARP	Who has 192.168.1.2? Tell 192.168.1.22
2	0.000218000	Ibm_2a:53:9b	AsustekC_26:	ARP	192.168.1.2 is at 00:14:5e:2a:53:9b
3	0.000303000	192.168.1.22	192.168.1.2	ICMP	Echo (ping) request id=0x0100, seq=21/
4	0.000516000	Ibm_2a:53:9b	Broadcast	ARP	Who has 192.168.1.22? Tell 192.168.1.2
5	0.000537000	AsustekC_26:01	Ibm_2a:53:9b	ARP	192.168.1.22 is at 10:bf:48:26:01:3a
6	0.000744000	192.168.1.2	192.168.1.22	ICMP	Echo (ping) reply id=0x0100, seq=21/
7	1.017591000	192.168.1.22	192.168.1.2	ICMP	Echo (ping) request id=0x0100, seq=22/
8	1.017955000	192.168.1.2	192.168.1.22	ICMP	Echo (ping) reply id=0x0100, seq=22/
9	2.031617000	192.168.1.22	192.168.1.2	ICMP	Echo (ping) request id=0x0100, seq=23/
10	2.031966000	192.168.1.2	192.168.1.22	ICMP	Echo (ping) reply id=0x0100, seq=23/
11	3.045582000	192.168.1.22	192.168.1.2	ICMP	Echo (ping) request id=0x0100, seq=24/
12	3.045944000	192.168.1.2	192.168.1.22	ICMP	Echo (ping) reply id=0x0100, seq=24/

obr. 29: Wireshark – příkaz PING, cílová stanice

Doba odezvy tedy činila, vyjma prvního pingu, v průměru 0.358 ms, z toho průměrně 0.092 ms byla tato žádost zpracovávána v oslovené stanici.

7.1.6 SW hrPING

Utilita podobná klasickému příkazu ping. Její největší výhodou oproti pingu je vyšší přesnost měření. Zatímco ping měří dobu odezvy v milisekundách, hrPING ji měří v mikrosekundách.

7.1.7 SW iperf

Iperf je jednoduchá utilita typu klient-server, která umožňuje testovat propustnost počítačové sítě. Nejprve je nutné spustit na některém počítači iperf v serverovém módu (iperf -s), kde bude naslouchat na určeném portu (defaultně 5001), poté je nutné spustit na jiném počítači klienta iperf s parametrem konkrétní IP adresy serveru (iperf –c IP). Klient poté začne vysílat na určený server a port data dle zvolených parametrů, následně bude datový provoz vyhodnocen.

Zajímavé parametry pro server jsou:

-u server je spuštěn v UDP módu (defaultně je spouštěn v TCP módu)

-p port nastavení portu místo defaultního 5001

-B adresa nastavení IP adresy, na které naslouchá; defaultně naslouchá na všech svých IP adresách

-D je spuštěn jako démon (v Unixu)

Zajímavé parametry pro klienta jsou:

-b rychlost nastav maximální rychlost vysílání dat (např. 10M je 10Mbits/s)

-d obousměrný test najednou

-r obousměrný test, zvlášť pro každý směr

-t doba doba běhu testu (v sekundách)

-i interval zobrazuje výsledky průběžně (vždy po uplynutí intervalu v sekundách)

-n velikost kolik dat se bude odesílat (např. 10M je 10MB)

-w window nastavení velikosti okna pro TCP komunikaci

-F soubor data pro odeslání budou načtena z uvedeného souboru

-I data pro odeslání budou načtena ze standardního vstupu

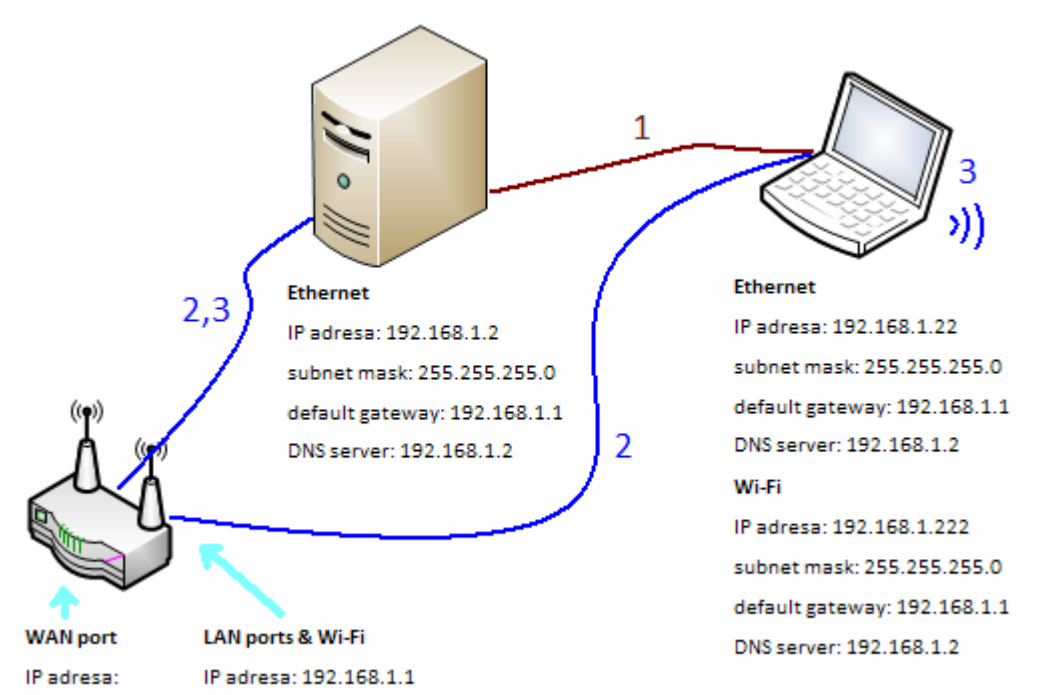
-P počet simulace spuštění více klientů naráz

-M velikost umožňuje nastavit velikost TCP segmentu

Nápovědu k programu zobrazíme příkazem **iperf --help.**

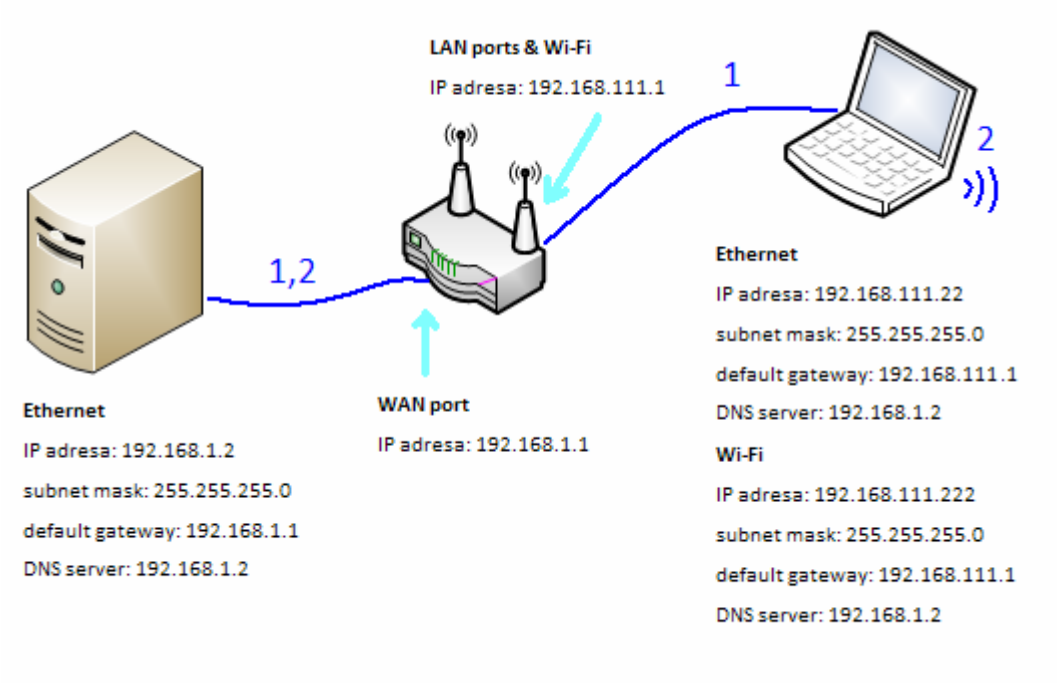
7.2 Schéma zapojení

Testování bude probíhat jednak v rámci jedné lokální sítě (obr. 30), kdy budou stanice a server zapojeny přímo kříženým kabelem – 1, nebo propojeny přes LAN porty routeru – 2, nebo bude server zapojen do LAN portu a stanice připojena přes Wi-Fi – 3.



obr. 30: Schéma zapojení testovací sestavy v jedné lokální síti (LAN)

V další fázi testování budou stanice a server zapojeny do dvou různých podsítí (obr. 31), server bude připojen do WAN portu a stanice do LAN portu – 1, nebo bude server připojen do WAN portu a stanice přes Wi-Fi – 2.



obr. 31: Schéma zapojení testovací sestavy ve dvou podsítích (WAN)

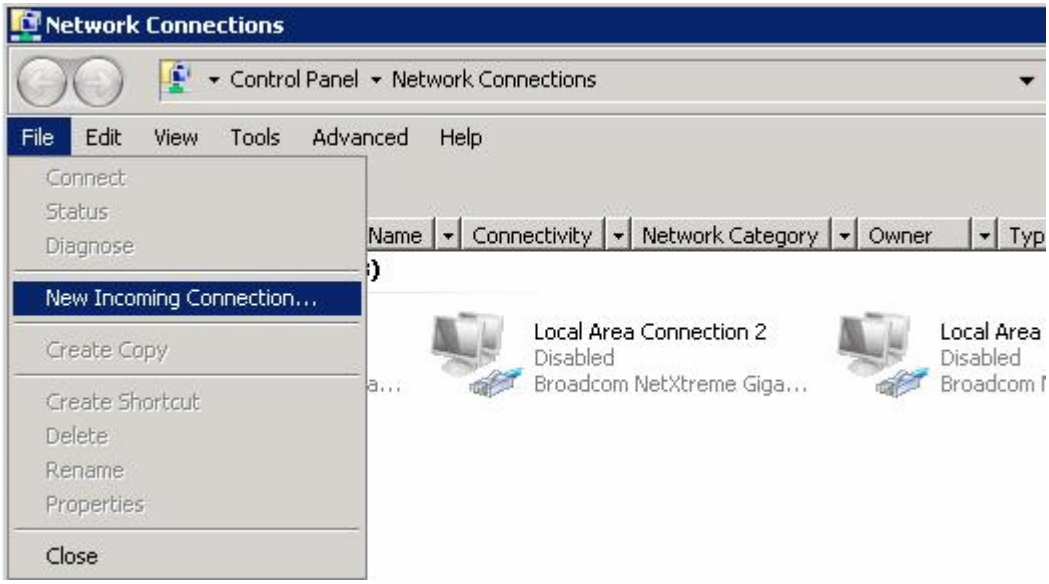
Celkem tedy budeme testovat 5 různých fyzických připojení serveru a stanice.

Pokud je stanice se serverem připojena kabelem přímo, default gateway není vyplněna. V případě připojení stanice přes Wi-Fi použijeme zabezpečení WPA2 (Wi-Fi Protected Access II), které používá k autentizaci sdílený klíč a jehož šifrování je založeno na AES.

7.3 Konfigurace Windows Serveru 2008

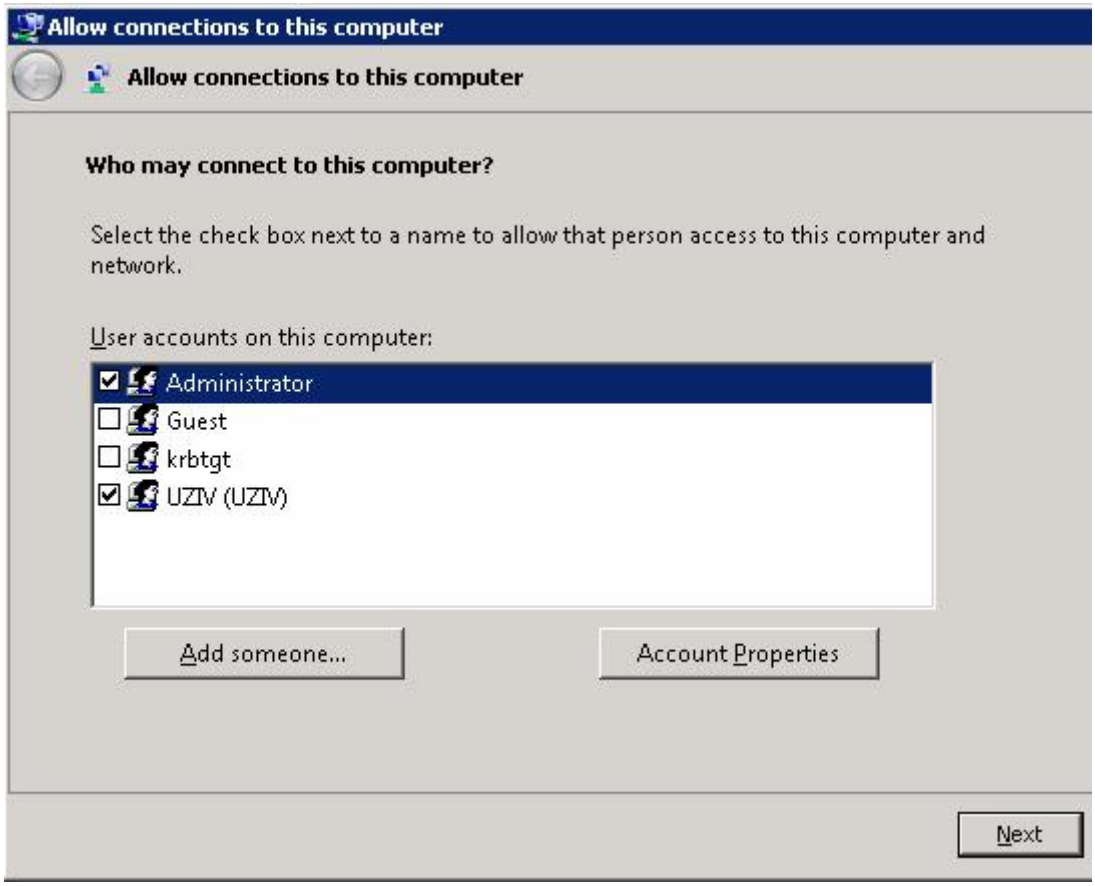
Nejsnažší je nakonfigurovat server pro používání PPTP. Stačí povolit příchozí VPN spojení:

Control Panel / Network Connection, menu File, volba New Incoming Connection... (obr. 32).



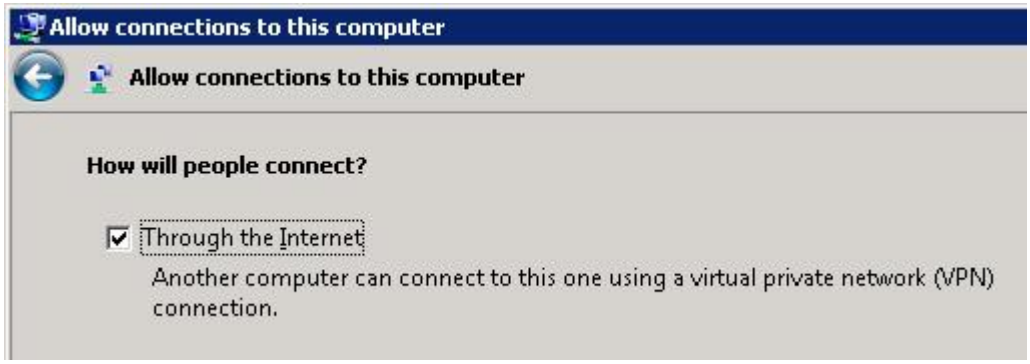
obr. 32: Windows Server 2008 – povolení příchozích spojení 1

V dialogu Who may connect to this computer? Vybereme uživatelské účty, které mají mít oprávnění vzdáleně se připojovat pomocí VPN k serveru a klikneme na Next (obr. 33).



obr. 33: Windows Server 2008 – povolení příchozích spojení 2

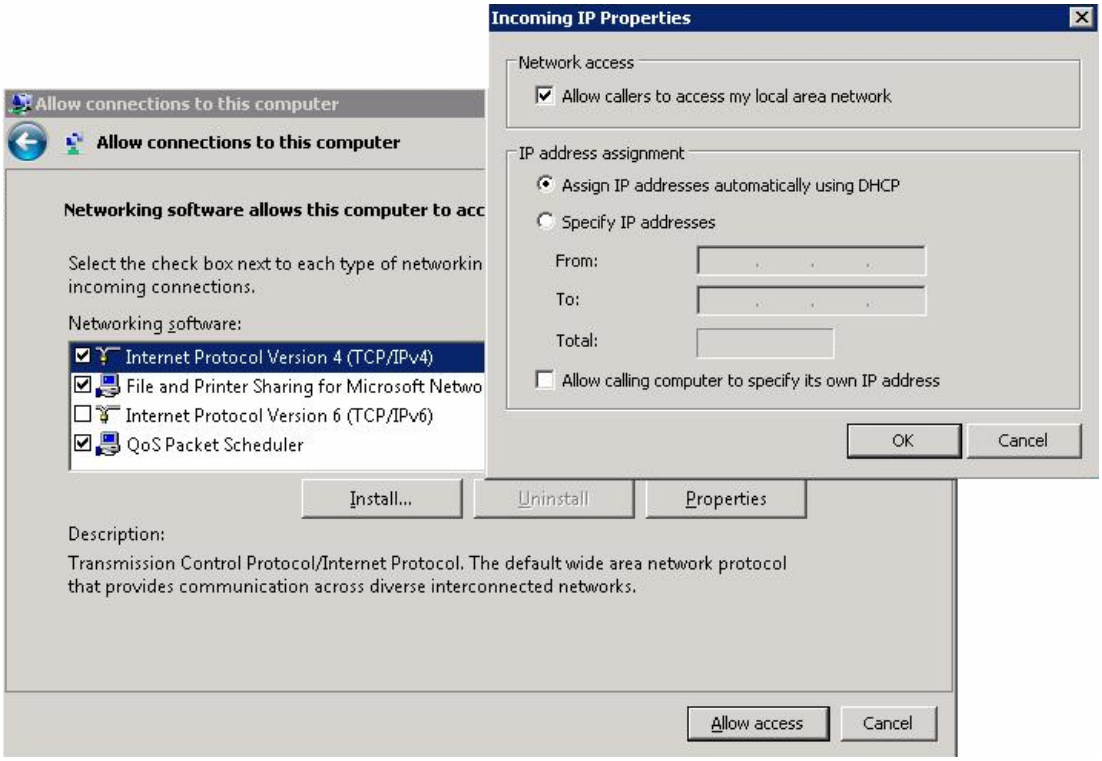
V dalším kroku (How will people connect?) volíme druh vzdáleného připojení. Pokud se uživatelé připojují jen z místní sítě, volba se nezaškrtává (obr. 34).



obr. 34: Windows Server 2008 – povolení příchozích spojení 3

Dále vybíráme síťové součásti, které mají být použity pro příchozí spojení (obr. 35). V Properties protokolu IPv4 můžeme zvolit, zda bude připojovaným klientům adresa přidělena automaticky protokolem DHCP, vybrána z určitého

rozsahu, příp. zda si ji klient může určit sám. My pro naše testování zvolíme rozsah 192.168.15.106 – 192.168.15.107. Server pak dostane v případě navázání VPN spojení nižší adresu tohoto rozsahu, stanice tu vyšší.



obr. 35: Windows Server 2008 – povolení příchozích spojení 4

Po kliknutí na Allow access jsou příchozí spojení na serveru povolena a PPTP VPN by již byla funkční. Jelikož ale chceme používat i jiné typy VPN, musíme zvolit jinou konfiguraci.

Nejprve smažeme v Control Panel / Network Connection v předchozích krocích povolené příchozí spojení a poté přidáme službu Routing and Remote Access Services, která je součástí role Network Policy and Access Services. Tato služba umožňuje vzdáleným uživatelům připojení k síti prostřednictvím VPN. Vyžaduje dva síťové adaptéry, kdy jeden je zapojen do Internetu a druhý do vnitřní sítě (kterou my v našich testech nemáme). Nakonfigurujeme proto na serveru druhý síťový adaptér např. na IP 10.0.0.5 a pokračujeme přidáním služby:

- Spustíme Server Manager
- Pravým tlačítkem myši na Roles, volba Add Roles

- Zvolíme Network Policy and Access Services, Next, Next
- Zaškrtneme Routing and Remote Access Services a jeho obě podvolby, tj. Remote Access Service a Routing a klikneme na Install

Dále musíme přidanou roli zkonfigurovat:
- V Server Manageru klikneme pravým tlačítkem myši na Routing and Remote Access a zvolíme Configure and Enable Routing and Remote Access
- Volba Remote Access, Next, Volba VPN, Next
- Jako interface připojený do Internetu zvolíme 192.168.1.2, Next
- Jako interface připojený do vnitřní sítě zvolíme 10.0.0.5, Next
- Přidělování IP adres vybereme volbu From a specified range of addresses zvolíme opět rozsah 192.168.15.106 – 192.168.15.107
- Klik na Finish, Start service

V Server Manageru / Routing and Remote Access / Ports můžeme nyní vidět a konfigurovat WAN Miniporty čekající na SSTP, L2TP a PPTP spojení.

Kdybychom nyní nastavili pro L2TP/IPSec spojení na stanici i serveru sdílený klíč (Stanice: klik pravým tlačítkem v Network Connections na VPN Connection / záložka Security / Type of VPN L2TP/IPSec / Advanced settings / Use preshared key for authentication vyplníme „SdilenyKlic“ / OK / OK. Server: Klik pravým tlačítkem myši na Routing and Remote Access / Properties / záložka Security – zaškrtneme volbu Allow custom IPSec policy for L2TP connection a do Preshared Key vyplníme „SdilenyKlic“ / OK) bylo by již možné L2TP/IPSec využívat.

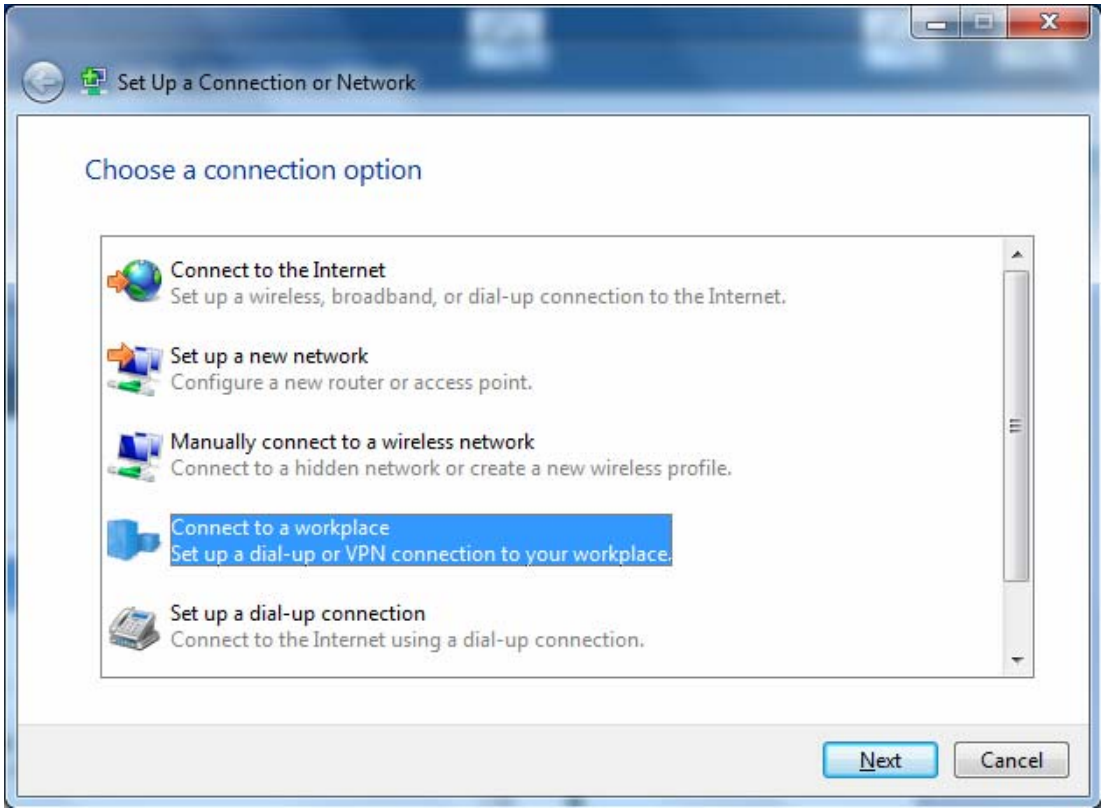
Jelikož ale použití sdíleného klíče není kvůli nižšímu zabezpečení doporučováno a navíc kvůli SSTP stejně budeme potřebovat certifikáty, pokračujeme dále přidáním role Active Directory Certificate Services. Ta umožňuje na serveru vytvořit a spravovat certifikační autority a certifikáty. Dále potřebujeme roli Application Server, která povolí přidání role Web Server (IIS) . Posledně jmenovaná role nám umožní webový zápis certifikátu pro počítač. Celý poměrně zdlouhavý postup je detailně popsán v *Microsoft Windows Server 2008 Velký průvodce administrátora, kapitola 26* [5]. Ve stručnosti jde o vytvoření certifikační autority na serveru, dále vytvoření certifikátu ověření serveru, který je následně naimportován

na server i stanici mezi důvěryhodné kořenové certifikační autority (Trusted Root Certification Authorities). Tím je konfigurace serveru hotova.

Nyní se můžeme na server připojit pomocí SSTP, L2TP i PPTP a tedy provést všechny testy.

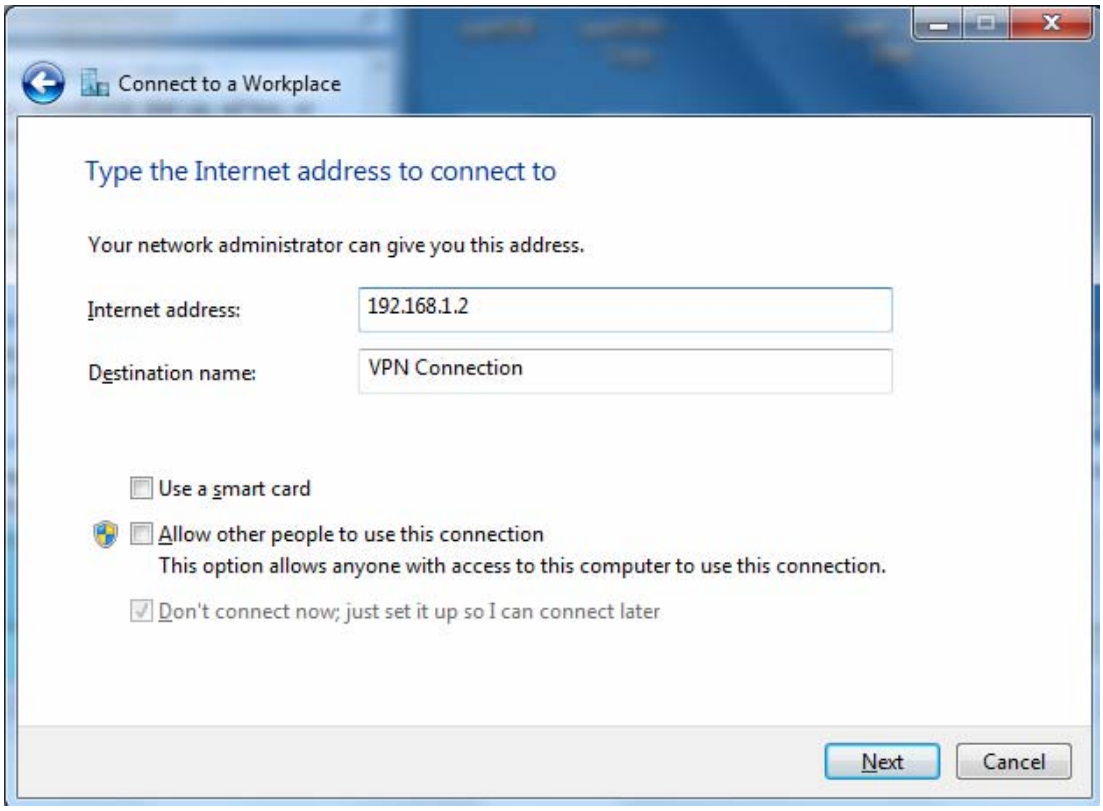
7.4 Konfigurace stanice

Control Panel / Network and Internet / Network and Sharing Center /
Set up a new connection or network.
Zvolíme Connect to a workplace (obr. 36).



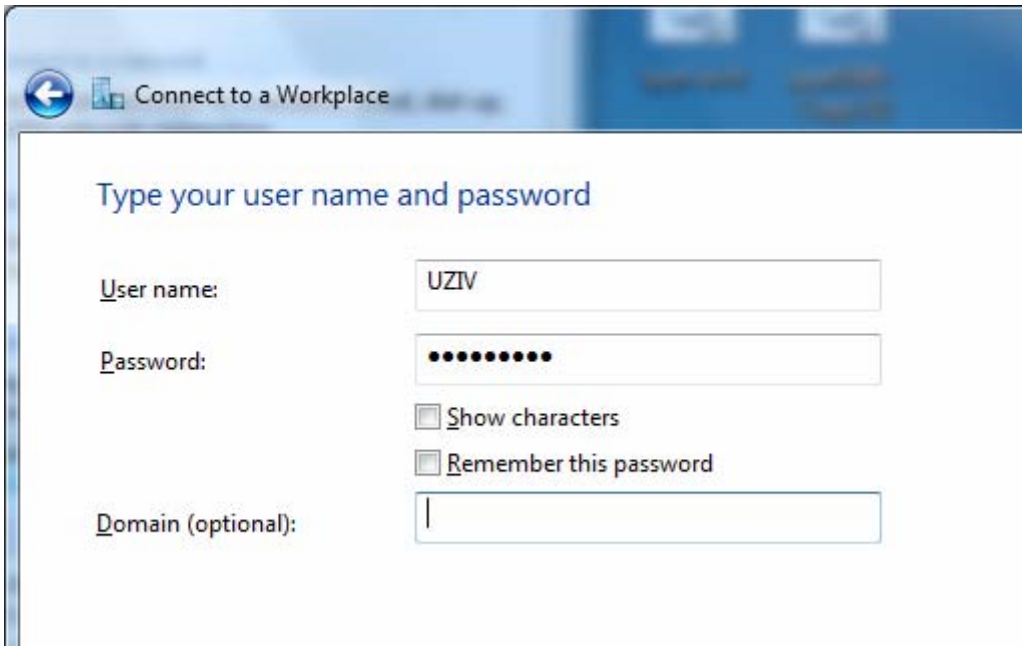
obr. 36: Windows 7 – konfigurace VPN klienta 1

Dále klikneme na Use my Internet connection (VPN), v dalším kroku vyplníme IP adresu serveru, název připojení a volitelně používání smart card a povolení ostatním uživatelům využívat toto připojení na (obr. 37).



obr. 37: Windows 7 – konfigurace VPN klienta 2

Nyní již stačí jen v dalším okně vyplnit jméno a heslo (volitelně doménu), kliknout na Create a VPN spojení je vytvořeno (obr. 38).



obr. 38: Windows 7 – konfigurace VPN klienta 3

Ve vlastnostech VPN připojení poté můžeme nastavit typ VPN : Klik pravým tlačítkem myši na VPN Connection / Properties / Security / Type of VPN.

7.5 Testy

Testy jednotlivých fyzických připojení a VPN řešení budou zaměřeny na zjišťování doby odezvy a propustnosti sítě.

Nejprve otestujeme výkonnost sítě jako takové, bez VPN připojení. Na základě takto získaných výsledků a znalosti principů fungování jednotlivých VPN řešení bude možné odhadnout chování sítě při použití VPN.

Následně otestujeme jednotlivé VPN a výsledky testů porovnáme s našimi odhady.

V každém testu bude provedeno 10 měření, výsledná hodnota daného testu pak bude vypočítána jako jejich průměr.

7.5.1 Test 1: měření odezvy

Pro změření doby odezvy použijeme program Wireshark a postup uvedený v kapitole 7.1.5, kdy zadáme ze stanice příkaz ping na server a následně z Wiresharku odečteme dobu odezvy. První vrácená hodnota bude z důvodu možného zpoždění kvůli vyhledávání linkové adresy protokolem ARP ignorována. Dobu odezvy též změříme programem hrPING. Je třeba si uvědomit, že Wireshark zachytává pakety přímo na síťové kartě, ale hrPING je aplikace, tudíž k ní odezva doputuje později. Jelikož nás zajímá odezva na aplikační úrovni, bude u VPN testů použit již jen program hrPING.

7.5.2 Test 2: měření propustnosti kopírováním souboru

V rámci tohoto testu bude zkopírován 500 MB soubor ze serveru na stanici. Použitím příkazu echo %TIME% před a po kopírování bude zjištěn čas kopírování s přesností setiny sekundy. Cílová složka bude v kopírujícím bat-souboru uvedena v

podobě \\IP_stanice\sdilena_slozka. IP_stanice je buď jedna z IP adres 192.168.1.22, 192.168.1.222, 192.168.111.22, 192.168.111.222 v případě připojení přímo, nebo 192.168.15.107 (což je IP adresu VPN tunelu na straně stanice) v případě připojení VPN.

Výstupem testu bude doba přenosu 500 MB souboru, z níž se vypočítá rychlost přenosu.

7.5.3 Test 3: syntetický test propustnosti TCP

Na serveru bude spuštěn: iperf.exe –s –w 64M
Na stanici bude spuštěn: iperf.exe -c IP_serveru -n 500M –w 64M

Celkem bude odesláno 500 MB dat. Velikost TCP Window size (pole délka okna v TCP segmentu) nastavena na 64 MB. Defaultní velikost TCP Window size programu iperf je totiž pouhých 16384 B, což by mohlo mít negativní vliv na testy v případě delší odezvy sítě. Stanice by mohla být schopna odesílat další TCP segmenty, ale jelikož by ještě neměla potvrzené odeslání posledních 16384 B dat, neučinila by tak.

Výstupem testu bude doba přenosu 500 MB dat, zjištěná utilitou iperf na stanici, z níž se vypočítá rychlost přenosu.

7.5.4 Test 4: syntetický test propustnosti UDP

Na serveru bude spuštěn: iperf.exe -s -u
Na stanici bude spuštěn: iperf.exe -c IP_serveru -u -t 30

Po dobu 30 vteřin bude stanice vysílat maximální možnou rychlostí UDP datagramy o velikosti 1478 B (tzn. 1470 B data).

Výstupem testu bude celkový počet vyslaných datagramů a kolik z nich bylo ztraceno a jitter - rozdíl ve zpoždění „nejrychlejšího“ a „nejpomalejšího“ datagramu.

Z počtu datagramů doručených na server a z jejich známé velikosti se vypočítá propustnost sítě.

7.5.5 Dodatečné informace

V detailních výsledcích testů v příloze této práce bude vždy uveden způsob připojení stanice:

LAN (Lokální síť):
KABEL = stanice je připojena kabelem přímo k serveru
SWITCH = stanice je připojena do LAN portu routeru
Wi-Fi = stanice je připojena přes Wi-Fi

WAN (Dvě podsítě):
ROUTER = stanice je připojena do LAN portu routeru
Wi-Fi = stanice je připojena přes Wi-Fi

Ve všech testech propustnosti (test 2, 3, 4) je počítána velikost užitečného obsahu, tzn. velikost datové části TCP segmentu, resp. UDP datagramu. Výsledná propustnost tedy určuje, kolik jsme schopni v daném čase přenést užitečných (aplikačních) dat.

Na závěr ještě jedna poznámka k předponě M = Mega. Dle převažujících zvyklostí znamená MB v případě velikosti souboru 2^{20} B, v případě přenosové rychlosti Mb (též Mbits) znamená 10^6 b. V tomto duchu je tako předpona používána i zde.

8 Vyhodnocení testů

8.1 Přímé připojení

Abychom mohli vyhodnotit výkonnost sítě pro jednotlivé VPN, je nutné nejprve zjistit její výkonnost při přímém připojení. Detailní výsledky testů přímého připojení jsou v přílohách A, B, souhrnné v tabulkách 1 a 2, kde jsou uvedeny průměrné naměřené hodnoty jednotlivých testů a relativní hodnoty jednotlivých testů vzhledem k přímému připojení kříženým kabelem.

průměrné hodnoty		doba odezvy		kopírování 500 MB		iperf TCP 500 MB		iperf UDP 30 sekund	
		Wrs (ms)	hrPING (ms)	čas (s)	rychlost (Mbits/s)	čas (s)	rychlost (Mbits/s)	rychlost (Mbits/s)	jitter (ms)
LAN	KABEL	0,326	0,580	21,03	199,85	4,49	934,12	451,85	0,474
	SWITCH	0,332	0,604	22,61	185,88	4,53	925,92	447,92	0,695
	Wi-Fi	1,613	1,909	58,19	72,14	63,04	66,66	107,66	1,077
WAN	ROUTER	0,680	0,950	32,04	131,11	28,08	149,41	212,93	3,170
	Wi-fi	2,188	2,430	49,59	84,64	60,05	70,28	103,89	27,605

tab. 1: Přímé připojení – průměrné hodnoty

relativní hodnoty		doba odezvy		kopírování 500 MB		iperf TCP 500 MB		iperf UDP 30 sekund	
		Wrs (%)	hrPING (%)	čas (%)	rychlost (%)	čas (%)	rychlost (%)	rychlost (%)	jitter (%)
LAN	KABEL	100,00	100,00	100,00	100,00	100,00	100,00	100,00	100,00
	SWITCH	101,62	104,12	107,50	93,01	100,89	99,12	99,13	146,62
	Wi-Fi	494,36	329,35	276,70	36,10	1404,01	7,14	23,83	227,29
WAN	ROUTER	208,40	163,96	152,36	65,60	625,39	15,99	47,12	669,07
	Wi-fi	670,67	419,24	235,83	42,35	1337,42	7,52	22,99	5826,19

tab. 2: Přímé připojení – relativní hodnoty

Z naměřených výsledků můžeme vyčíst několik očekávaných faktů, co se týká chování sítě samotné. Je dobré je zde zmínit, neboť mají vliv na hodnocení následných VPN testů:

Zapojení přes switch jen nepatrně zvýší odezvu a sníží propustnost v porovnání se zapojením křiženým kabelem. To komunikace přes router má na odezvu a propustnost sítě mnohem vyšší dopad. Kopírování souboru vykazuje výrazně nižší propustnost, než syntetické testy iperf – důvodem je pomalejší zápis dat na pevný disk stanice v porovnání s propustností sítě.

Wi-Fi spojení je navazováno rychlostí 150 Mbits/s, je tak úzkým místem celé sítě. Dále je nutné si uvědomit, že se nejedná o duplexní (vysílat i přijímat data lze zároveň) spojení, jako v případě zapojení kabelem, které je v případě našich testovacích komponent vždy 1000 Mbits/s duplexní. Data přenášená přes Wi-Fi spojení jsou navíc šifrována, což dále snižuje rychlost přenosu. Wi-Fi spojení dokonce vykazuje u testů kopírování souboru a iperf TCP nižší propustnost u zapojení LAN, než zapojení WAN, jeho propustnost je tedy značně kolísavá.

8.2 VPN připojení

Detailní výsledky testů VPN připojení jsou v přílohách C až H, souhrnné v tabulkách 3 a 4, kde jsou uvedeny relativní hodnoty výsledků jednotlivých testů vzhledem k přímému připojení.

LAN		doba odezvy	kopírování 500 MB		iperf TCP 500 MB		iperf UDP 30 sekund	
		hrPING	čas	rychlost	čas	rychlost	propustnost	jitter
		(%)	(%)	(%)	(%)	(%)	(%)	(%)
KABEL	prime	100,00	100,00	100,00	100,00	100,00	100,00	100,00
	PPTP	181,40	119,54	83,49	489,98	20,42	28,64	89145,25
	L2TP	206,18	134,66	70,68	569,49	17,57	25,19	3147,36
	SSTP	356,38	125,79	75,66	524,94	19,05	27,04	2665,39
SWITCH	prime	100,00	100,00	100,00	100,00	100,00	100,00	100,00
	PPTP	180,68	112,12	89,04	492,27	20,34	28,38	24598,22
	L2TP	197,40	125,64	75,76	567,33	17,63	24,37	6192,93
	SSTP	355,14	119,66	79,55	515,45	19,41	26,94	226,01
Wi-Fi	prime	100,00	100,00	100,00	100,00	100,00	100,00	100,00
	PPTP	146,29	108,92	92,24	102,05	98,07	56,49	39022,56
	L2TP	155,14	111,30	85,62	115,61	86,41	55,69	2862,48
	SSTP	171,94	101,14	94,22	99,83	100,03	84,94	1714,34

tab. 3: VPN připojení – LAN

WAN		doba odezvy	kopírování 500 MB		iperf TCP 500 MB		iperf UDP 30 sekund	
		hrPING	čas	rychlost	čas	rychlost	propustnost	jitter
		(%)	(%)	(%)	(%)	(%)	(%)	(%)
ROUTER	prime	100,00	100,00	100,00	100,00	100,00	100,00	100,00
	PPTP	117,53	112,54	88,74	102,74	97,31	60,92	265,64
	L2TP	150,41	119,64	79,59	114,17	87,61	50,35	5166,81
	SSTP	250,55	104,23	91,36	102,39	97,67	53,98	175,74
Wi-Fi	prime	100,00	100,00	100,00	100,00	100,00	100,00	100,00
	PPTP	105,19	118,55	84,36	111,96	88,89	61,00	1829,11
	L2TP	194,37	157,12	60,65	123,85	80,31	52,43	1734,89
	SSTP	172,46	120,70	78,95	117,14	84,90	55,55	160,98

tab. 4: VPN připojení – WAN

Pokud chceme stručné srovnání výkonnosti jednotlivých VPN, potřebujeme jedno číslo, charakterizující danou VPN. Zkusme tedy spočítat průměrnou relativní propustnost (tab. 5) a průměrnou relativní odezvu (tab. 6) vzhledem k přímému připojení pro každou VPN.

PROPUSTNOST (%)	celá síť	bez Wi-Fi	jen LAN bez Wi-Fi
prime	100,00	100,00	100,00
PPTP	66,56	57,48	45,05
L2TP/IPSEC	57,99	49,86	38,53
SSTP	65,95	54,52	41,27

tab. 5: Průměrná relativní propustnost VPN

Pokud zprůměrujeme všechny testy propustnosti za celou síť, vyjde nám jako nejvýkonnější PPTP, jen těsně následovaná SSTP a s velkým odstupem končí L2TP/IPSec. Jelikož nám ale Wi-Fi spojení ukázalo už při přímém připojení velkou kolísavost propustnosti, zkusíme spočítat průměrnou hodnotu propustnosti bez něj. V tomto případě SSTP vykazuje o 2,96% nižší propustnost, než PPTP (za základ 100% se vždy považuje propustnost připojení přímo, ne propustnost PPTP) a o 4,66 % vyšší propustnost, než L2TP/IPSec. Pokud zprůměrujeme testy v lokální síti, bez Wi-Fi a routeru, SSTP má o 3,78% nižší propustnost, než PPTP a o 2,74% vyšší propustnost, než L2TP/IPSec.

V případě propustnosti lze tedy naše odhady výkonu jednotlivých VPN považovat za správné, největší propustnost má PPTP, nejmenší L2TP/IPSec a SSTP je zhruba uprostřed.

ODEZVA (%)	celá síť	bez Wi-Fi	jen LAN bez Wi-Fi
prime	100,00	100,00	100,00
PPTP	146,22	159,87	181,04
L2TP/IPSEC	180,70	184,66	201,79
SSTP	261,30	320,69	355,76

tab. 6: Průměrná relativní odezva VPN

V případě odezvy vykazuje ve všech případech nejlepší hodnotu PPTP, následovaná L2TP/IPSec. Výrazně nejpomalejší odezvu má SSTP. Hodnota odezvy je u SSTP relativně nejvyšší u zapojení v rámci LAN bez použití Wi-Fi, což jasně ukazuje na příčinu v samotném SSTP. Důvodem může být to, že protokol SSL patří mezi transportní a aplikační vrstvu, k zapouzdření a šifrování dat proto dochází na vyšší vrstvě, než v případě zbylých dvou VPN. Jelikož obecně platí, že čím nižší vrstva, tím více je orientována na přenos dat a čím vyšší vrstva, tím více je orientována na uživatelské aplikace, není „pomalá“ odezva SSTP tak překvapivá.

V případě odezvy se naše odhady výkonu jednotlivých VPN nepotvrdily. Nejrychlejší odezvu má sice PPTP, ale za ní následuje L2TP/IPSec a SSTP je s velkým odstupem s nejpomalejší odezvou poslední. Jako pravděpodobné vysvětlení se nabízí to, že SSTP funguje na vyšší vrstvě, než zbylé dvě VPN řešení.

Závěr

Teoretická část práce nejprve detailně popisuje fungování počítačových sítí na architektuře TCP/IP, dále principy fungování virtuálních privátních sítí (VPN) a způsoby ochrany dat přenášených pomocí VPN po sdílené infrastruktuře. Poté jsou zde představeny různé varianty VPN na platformě Microsoft Windows včetně popisu, jak konkrétní způsob realizace VPN řeší ochranu přenášených dat po sdílené infrastruktuře a odhadu, jaký to bude mít dopad na výkon systémového prostředí a rychlost komunikace.

V praktické části jsou provedeny testy výkonnosti systémového prostředí a rychlosti komunikace na konkrétních počítačových sestavách na platformě Microsoft Windows a to jak při přímém připojení, tak při připojení přes různě realizované VPN. Tyto testy jsou poté vyhodnoceny a porovnány s našimi původními odhady. Většina testů dopadla podle našich předpokladů, jen v jednom případě byl výsledek jiný, než jsme čekali. Podařilo se nám ovšem najít pravděpodobné vysvětlení.

Hlavní přínos práce vidím v tom, že je zde popsáno vše v souvislostech a to od samotných základů, jak fungují počítačové sítě, až po detailní popis principů fungování VPN jak z obecného pohledu, tak na platformě Microsoft Windows. Bez předchozích teoretických základů v oblasti počítačových sítí tak lze proniknout do způsobu fungování technologie zvané VPN. Vše je navíc ověřeno na konkrétních počítačových sestavách v prostředí Microsoft Windows a následně zanalyzováno.

Tato práce mi umožnila proniknout hlouběji jak do světa počítačových sítí a jejich zabezpečení, tak i do platformy Microsoft Windows. Díky tomu jsem si výrazně rozšířil v těchto oblastech své znalosti a hodlám se v obou těchto směrech dále intenzivně vzdělávat.

Seznam použité literatury

[1] SOSINSKY, Barrie. *Mistrovství - počítačové sítě*. 1. vydání. Brno: Computer Press, 2011. ISBN 978-80-251-3363-7.

[2] DOSTÁLEK, Libor, KABELOVÁ Alena. *Velký průvodce protokoly TCP/IP a systémem DNS*. 5. vydání. Brno: Computer Press, 2008. ISBN 978-80-251-2236-5.

[3] DOSTÁLEK, Libor a kolektiv. *Velký průvodce protokoly TCP/IP: Bezpečnost*. 2. vydání. Praha: Computer Press, 2003. ISBN 80-7226-849-X.

[4] PUŽMANOVÁ, Rita. *Moderní komunikační sítě od A do Z*. 2. vydání. Brno: Computer Press, 2006. ISBN 80-251-1278-0.

[5] RUSSEL, Charlie, CRAWFORD, Sharon. *Microsoft Windows Server 2008 Velký průvodce administrátora*. 1. vydání. Brno: Computer Press, 2009. ISBN 978-80-251-2115-3.

[6] BOTT, Ed, SIECHERT, Carl, STINSON, Craig. *Mistrovství v Microsoft Windows 7*. 1. vydání. Brno: Computer Press, 2010. ISBN 978-80-251-2817-6.

[7] PUŽMANOVÁ, Rita. *Bezpečnost bezdrátové komunikace*. 1. vydání. Brno: CP Books, 2005. ISBN 80-251-0791-4.

[8] THOMAS, M. Thomas. *Zabezpečení počítačových sítí bez předchozích znalostí*. 1. vydání. Brno: CP Books, 2005. ISBN 80-251-0417-6.

[9] MLÝNEK, Jaroslav. *Zabezpečení obchodních informací*. 1. vydání. Brno: Computer Press, 2007. ISBN 978-80-251-1511-4.

[10] NORTHCUTT, Stephen, ZELSTER, Lenny, FREDERICK, Karen, Kent, RITCHEY, Ronald, WINTERS, Scott. *Bezpečnost počítačových sítí*. 1. vydání. Brno: CP Books, 2005. ISBN 80-251-0697-7.

[11] OREBAUGH, Angela, RAMIREZ, Gilbert, BURKE, Josh, MORRIS, Greg, PESCE, Larry, WRIGHT, Joshua. *Wireshark a Ethereal*. 1. vydání. Brno: Computer Press, 2008. ISBN 978-80-251-2048-4.

[12] SANDERS, Chris. *Analýza sítí a řešení problémů v programu Wireshark*. 1. vydání. Brno: Computer Press, 2012. ISBN 978-80-251-3718-5.

[13] Javamex, http://www.javamex.com/tutorials/cryptography

[14] RFC 4301 : Security Architecture for the Internet Protocol

[15] Microsoft TechNet, htp://technet.microsoft.com/

Seznam obrázků

Seznam tabulek

Seznam použitých zkratek

AAA *Authentication, Authorization, Accounting*. Autentizace, autorizace a záznam všech činností uživatele v systému.

ACK Příznak v hlavičce TCP segmentu „pole pořadí přijatého B je platné“.

AES *Advanced Encryption Standard.* Symetrická šifra.

AH *Authentication Header*. Jeden z protokolů IPSec.

ARP *Address Resolution Protocol.* Protokol síťové vrstvy. Používá se k získání ethernetové adresy z IP adresy.

ARPA *Advanced Research Projects Agency*. Agentura amerického ministerstva obrany, pod kterou spadá vývoj vojenských technologií. Založena byla roku 1958, v roce 1972 se přejmenovala na DARPA.

ARPANET *Advanced Research Projects Agency Network*. Počítačová síť spuštěná v roce 1969 původně jen jako experimentální síť, fungující bez centrální složky. Byla zárodkem dnešního Internetu.

b *Bit*. *Binary digit*. Nejmenší jednotka množství dat v informatice, jednociferné binární číslo.

B *Byte*. Jednotka množství dat v informatice. Označuje 8 bitů.

CBC *CipherBlockChaining*. Mód symetrické blokové šifry.

CFB *Cipher FeedBack*. Mód symetrické blokové šifry.

CWR Příznak v hlavičce TCP segmentu znamenající potvrzení přijetí TCP segmentu s nastaveným příznakem ECN.

DARPA *Defense Advanced Research Projects Agency*. Agentura amerického ministerstva obrany, pod kterou spadá vývoj vojenských technologií. Do roku 1972 se jmenovala ARPA.

DES *Data Encryption Standard*. Symetrická šifra.

DF *Don´t Fragment.* Příznak v hlavičce IP datagramu (0 = povolení / 1 = zákaz fragmentace).

DNS *Domain Name System.* Aplikační protokol. Převádí doménová jména na IP adresy a naopak.

EAP *Extensible Authentication Protocol*. Protokol pro ověření vzdáleného přístupu.

ECB	*Electronic Code Book*. Mód symetrické blokové šifry.
ECN	Příznak v hlavičče TCP segmentu. Je nastaven, dokud není přijat segment s nastaveným příznakem CWR.
ESP	*Encapsulating Security Payload*. Jeden z protokolů IPSec.
FIN	Příznak v hlavičče TCP segmentu „odesílatel ukončil odesílání dat“. Nadále však může data přijímat.
FTP	*File Transfer Protocol*. Aplikační protokol. Slouží k přenosu souborů v počítačové síti.
GRE	*Generic Encapsulation Protocol*.
HTTP	*Hypertext Transfer Protocol*. Aplikační protokol. Umožňuje přenos hypertextových dokumentů na internetu.
HTTPS	*Hypertext Transfer Protocol Secure*. Nadstavba protokolu HTTP umožňující šifrování a autentizaci.
CHAP	*Challenge Handshake Authentication Protocol*. Protokol pro ověření vzdáleného přístupu.
ICMP	*Internet Control Message Protocol.* Protokol síťové vrstvy. Odesílá chybové zprávy a oznámení.
IKE	*Internet Key Exchange*. Jeden z protokolů IPSec.
IP	*Internet Protocol.* Protokol síťové vrstvy. Zodpovídá za směrování a doručování paketů v sítích.
IPSec	*IP security*. Bezpečnostní rozšíření protokolu IPv4.
IPv4	*Internet Protocol version 4*. IP ve své čtvrté verzi.
IPv6	*Internet Protocol version 6*. IP ve své nejnovější verzi.
IPSEC	*IP security.* Protokol síťové vrstvy. Bezpečnostní rozšíření protokolu IP.
ISAKMP	*Internet Security Association Key Management Protocol*. Jeden z protokolů IPSec.
ISO	*International Organization for Standardization.* Mezinárodní organizace pro normalizaci.
LCP	*Link Control Protocol*. Součást protokolu PPP.
L2TP	*Layer 2 Tunneling Protocol*. Tunelovací protokol pro VPN.

MD5 *Message-Digest algorithm*. Hashovací funkce s otiskem zprávy dlouhým 128 bitů.

MF *More Fragments*. Příznak v hlavičče IP datagramu (0 = je / 1 = není posledním fragmentem).

MPPC *Microsoft Point-To-Point Compression Protocol*.

MPPE *Microsoft Point-to-Point Encryption Protocol*. Šifrovací protokol OS Windows.

MS-CHAP *Microsoft Challenge Handshake Authentication Protocol*. Protokol pro ověření vzdáleného přístupu.

MSS *Maximum segment size*. Volitelná položka TCP segmentu určující maximální velikost datové části TCP segmentu.

MTU *Maximum transmission unit*. Udává maximální velikost IP datagramu v B, který lze vložit do příslušného linkového rámce bez fragmentace.

NAT *Network Address Translation*. Překlad IP adres.

NCP *Network Control Protocol*. Součást protokolu PPP.

NFS *Network File System.* Aplikační protokol. Umožňuje vzdálený přístup k souborům přes počítačovou síť.

OSI *Open System Interconnection.* Referenční síťový model od organizace ISO.

PAP *Password Authentication Protocol*. Protokol pro ověření vzdáleného přístupu.

PAT *Port Address Translation*. Překlad IP adres a portů.

PDU *Protocol Data Unit*. Protokolová datová jednotka.

PGP *Pretty Good Privacy*. Program umožňující šifrování a podepisování zpráv. Je založen na algoritmu RSA pro asymetrické šifrování.

PKI *Public Key Infrastructure*. Infrastruktura pro správu a distribuci veřejných klíčů asymetrického šifrování.

POP3 *Post Office Protocol*. Aplikační protokol. Používá se ke stahování emailových zpráv z poštovního serveru na počítač klienta.

PPP *Point-to-Point Protocol*. Linkový protokol pro přímé spojení mezi dvěma uzly v síti sériovou linkou.

PPTP *Point-to-Point Tunneling Protocol*. Tunelovací protokol pro VPN.

PSH Příznak v hlavičče TCP segmentu - „segment obsahuje aplikační data“.

RADIUS *Remote Authentication Dial In User Service.* AAA protokol.

RARP *Reverse Address Resolution Protocol.* Protokol síťové vrstvy. Používá se k získání IP adresy z ethernetové adresy.

RC4 Proudová šifra.

RFC *Request for comments.* Označení řady standardů a dalších dokumentů popisujících Internetové protokoly. Každé RFC má při svém zveřejnění přiděleno číslo.

RSA *Rivest, Shamir, Adleman*. Kryptografický systém používající asymetrické šifrování. Pojmenován podle svých autorů.

RST Příznak v hlavičce TCP segmentu znamenající odmítnutí TCP spojení.

SA *Security Association*. Ukazatel do databáze SPD.

SHA *Secure Hash Algorithm*. Sada hashovacích algoritmů s otisky zpráv délky 160 až 512 bitů.

SLIP *Serial Line Internet Protocol*. Linkový protokol pro přímé spojení mezi dvěma uzly v síti sériovou linkou.

SMB2 *Server Message Block 2*. Aplikační protokol sloužící ke sdílenému přístupu k souborům, tiskárnám a sériovým portům.

SMTP *Simple Mail Transfer Protocol*. Aplikační protokol. Používá se k přenosu emailových zpráv mezi poštovními servery, příp. od klienta k serveru.

SNMP *Simple Network Management Protocol*. Aplikační protokol sloužící ke správě sítě.

SP *Security Policy*. Pravidla zabezpečení aplikovaná v protokolech AH a ESP.

SPD *Security Policy Database*. Databáze obsahující jednotlivá SP.

SPI *Security Parameters Index*. Pole hlavičky protokolu AH.

SSH *Secure Shell*. Aplikační protokol pro zabezpečenou komunikaci po síti. Náhrada za nezabezpečený Telnet.

SSL *Secure Sockets Layer.* Protokol převážně používaný pro bezpečnou komunikaci s webovými servery pomocí HTTPS.

SSTP	*Secure Socket Tunneling Protocol*. Tunelovaní protokol pro VPN.
SYN	Příznak v hlavičče TCP segmentu „odesílatel nově nastavil pořadové číslo prvního odesílaného B“.
TDES	*Triple DES*. Symetrická šifra.
TCP	*Transmission Control Protocol*. Transportní, spojově orientovaný protoko, zajišťující spolehlivý přenost datl.
TCP/IP	*Transmission Control Protocol*/ *Internet Protocol*. Síťová architektura definující 4 vrstvy a sadu příslušných protokolů. Stejnou zkratkou jsou označovány i samotné protokoly.
TELNET	*Telecommunication Network.* Aplikační protokol sloužící k připojení se uživatele ke vzdálenému počítači.
TTL	*Time to live*. Pole v hlavičče IP datagramu, určující maximální počet průchodů datagramu směrovači. Každým směrovačem je tato hodnota dekrementována, po dosažení nuly je datagram zahozen.
UDP	*User Datagram Protocol.* Transportní, nespojově orientovaný protokol.
URG	Příznak v hlavičce TCP segmentu - „segment obsahuje naléhavá data“.
UTP	*Unshielded twisted pair*. Typ datového kabelu “kroucená dvojlinka”.
VPN	*Virtual private network.* Počítačová síť vytvořená nad sdílenou síťovou infrastrukturou.
Wi-Fi	Standardy IEEE 802.11 popisující bezdrátovou komunikaci.
WPA2	*Wi-Fi Protected Access II*.
X.509	Standard pro PKI systémy.

Přílohy – Detailní výsledky testů

A. Přímé připojení – LAN

	doba odezvy		kopírování 500 MB		iperf TCP 500 MB		iperf UDP 30 sekund				
	Wrs	hrPING	čas	rychlost	čas	rychlost	ztraceno	posláno	ztrátovost	rychlost	jitter
	(ms)	(ms)	(s)	(Mbits/s)	(s)	(Mbits/s)	datagramů	datagramů	(%)	(Mbits/s)	(ms)
KABEL	0,362	0,572	21,22	197,64	4,5	932,00	0	1168374	0,000	454,50	0,936
	0,398	0,611	19,95	210,23	4,5	932,00	0	1159066	0,000	450,88	0,054
	0,311	0,590	20,16	208,04	4,5	932,00	0	1158694	0,000	450,73	0,540
	0,248	0,512	20,55	204,09	4,4	953,18	11	1168219	0,001	454,43	0,250
	0,361	0,582	22,30	188,07	4,5	932,00	0	1152619	0,000	448,37	0,023
	0,326	0,611	20,11	208,55	4,5	932,00	0	1165374	0,000	453,33	0,914
	0,331	0,660	23,00	182,35	4,5	932,00	0	1155266	0,000	449,40	0,954
	0,399	0,631	21,73	193,01	4,5	932,00	15	1159694	0,001	451,12	0,110
	0,303	0,559	20,34	206,19	4,5	932,00	0	1166622	0,000	453,82	0,889
	0,224	0,468	20,93	200,38	4,5	932,00	0	1161725	0,000	451,91	0,068
	0,326	**0,580**	**21,03**	**199,85**	**4,49**	**934,12**	**2,6**	**1161565**	**0,000**	**451,85**	**0,474**
SWITCH	0,413	0,778	23,25	180,39	4,5	932,00	0	1150048	0,000	447,37	0,914
	0,356	0,547	21,94	191,13	4,5	932,00	0	1151279	0,000	447,85	0,024
	0,257	0,511	21,77	192,65	4,6	911,74	0	1150503	0,000	447,55	0,035
	0,398	0,649	25,16	166,69	4,5	932,00	5	1150678	0,000	447,61	1,113
	0,301	0,571	22,07	190,03	4,6	911,74	0	1152784	0,000	448,43	1,686
	0,257	0,523	21,95	191,07	4,5	932,00	0	1149526	0,000	447,17	0,914
	0,320	0,577	22,27	188,33	4,5	932,00	15	1152578	0,001	448,35	0,914
	0,317	0,590	22,55	186,00	4,5	932,00	0	1152451	0,000	448,30	0,879
	0,439	0,778	21,65	193,74	4,6	911,74	2	1150268	0,000	447,45	0,121
	0,258	0,511	23,46	178,80	4,5	932,00	0	1154582	0,000	449,13	0,347
	0,332	**0,604**	**22,61**	**185,88**	**4,53**	**925,92**	**2,2**	**1151470**	**0,000**	**447,92**	**0,695**
Wi-Fi	1,524	1,799	55,51	75,55	60,1	69,78	55478	320475	17,311	103,08	1,175
	1,628	1,874	58,12	72,16	65,2	64,33	42185	311141	13,558	104,62	0,921
	1,824	2,140	60,47	69,36	63,3	66,26	77369	342002	22,622	102,94	1,221
	1,547	1,854	57,04	73,53	60,2	69,67	47533	322014	14,761	106,77	1,294
	1,547	1,890	61,40	68,31	62,0	67,65	66581	350921	18,973	110,61	1,026
	1,957	2,200	56,07	74,80	67,1	62,50	59358	353387	16,797	114,38	0,958
	1,550	1,912	58,18	72,09	59,7	70,25	50470	331870	15,208	109,46	1,068
	1,581	1,902	57,69	72,70	60,2	69,67	25	291378	0,009	113,34	0,959
	1,426	1,722	59,04	71,04	67,0	62,60	66409	333166	19,933	103,77	0,977
	1,547	1,796	58,36	71,86	65,6	63,93	59929	336671	17,800	107,65	1,170
	1,613	**1,909**	**58,19**	**72,14**	**63,04**	**66,66**	**52533,7**	**329302,5**	**15,697**	**107,66**	**1,077**

tab. 7: Přímé připojení – LAN detailní výsledky

B. Přímé připojení – WAN

	doba odezvy		kopírování 500 MB		iperf TCP 500 MB		iperf UDP 30 sekund				
	Wrs (ms)	hrPING (ms)	čas (s)	rychlost (Mbits/s)	čas (s)	rychlost (Mbits/s)	ztraceno datagramů	posláno datagramů	ztrátovost (%)	rychlost (Mbits/s)	jitter (ms)
ROUTER	0,595	0,875	33,65	124,65	27,5	152,51	549348	1092944	50,263	211,46	0,938
	0,546	0,799	30,56	137,23	27,1	154,76	601939	1150581	52,316	213,42	1,195
	0,845	1,220	32,47	129,17	28,3	148,20	564214	1120547	50,352	216,41	15,025
	0,679	0,980	31,07	134,99	28,5	147,16	577481	1132417	50,995	215,87	5,241
	0,790	1,061	32,89	127,52	28,1	149,25	566478	1100574	51,471	207,76	0,874
	0,664	0,936	32,12	130,57	27,8	150,86	584274	1142574	51,137	217,18	3,574
	0,660	0,947	33,01	127,05	28,2	148,72	590478	1123800	52,543	207,46	2,010
	0,697	0,839	33,49	125,24	28,6	146,64	592040	1140442	51,913	213,33	0,938
	0,724	0,999	31,58	132,81	28,8	145,63	590448	1138367	51,868	213,14	0,968
	0,600	0,847	29,57	141,81	27,9	150,32	589096	1137361	51,795	213,28	0,938
	0,680	**0,950**	**32,04**	**131,11**	**28,08**	**149,41**	**580579,6**	**1127961**	**51,465**	**212,93**	**3,170**
Wi-Fi	1,667	1,932	49,57	84,61	61,2	68,53	52168	309963	16,830	100,28	1,137
	1,947	2,147	50,07	83,76	58,7	71,45	52002	304805	17,061	98,34	5,248
	1,899	2,145	47,98	87,41	60,9	68,87	65828	332168	19,818	103,61	3,247
	1,654	1,854	48,05	87,28	63,7	65,84	49707	329679	15,077	108,91	1,047
	2,604	2,874	48,24	86,94	59,9	70,02	53478	303458	17,623	97,24	155,247
	3,009	3,214	51,47	81,48	52,0	80,65	49005	325741	15,044	107,65	5,320
	2,877	3,102	49,62	84,52	65,7	63,84	51047	330057	15,466	108,53	0,938
	1,707	1,967	50,77	82,61	58,4	71,82	42685	305150	13,988	102,10	99,154
	2,564	2,834	48,09	87,21	52,9	79,28	51087	323240	15,805	105,87	3,245
	1,956	2,230	52,07	80,55	67,1	62,50	55060	328558	16,758	106,39	1,462
	2,188	**2,430**	**49,59**	**84,64**	**60,05**	**70,28**	**52206,7**	**319281,9**	**16,347**	**103,89**	**27,605**

tab. 8: Přímé připojení – WAN detailní výsledky

C. PPTP – LAN

	doba odezvy	kopírování 500 MB		iperf TCP 500 MB		iperf UDP 30 sekund				
	hrPING	čas	rychlost	čas	rychlost	ztraceno	posláno	ztrátovost	rychlost	jitter
	(ms)	(s)	(Mbits/s)	(s)	(Mbits/s)	datagramů	datagramů	(%)	(Mbits/s)	(ms)
KABEL	1,235	25,16	166,69	21,6	194,17	92713	429242	21,599	130,91	574,848
	0,994	24,97	167,96	21,6	194,17	103299	422148	24,470	124,03	537,297
	1,057	25,30	165,77	21,5	195,07	60666	411432	14,745	136,45	0,914
	0,964	25,17	166,63	22,1	189,77	72522	423961	17,106	136,71	459,053
	0,999	25,57	164,02	21,7	193,27	151231	438417	34,495	111,72	808,629
	1,155	25,89	161,99	23,5	178,47	99393	422656	23,516	125,75	361,912
	0,908	24,90	168,43	21,8	192,39	58670	413130	14,201	137,88	0,932
	1,185	25,08	167,22	22,1	189,77	110506	433954	25,465	125,82	1114,284
	0,954	24,57	170,70	22,0	190,64	82940	431142	19,237	135,45	6,393
	1,063	24,78	169,25	21,8	192,39	90532	423159	21,394	129,39	359,440
	1,051	**25,14**	**166,87**	**21,97**	**191,01**	**92247,2**	**424924,1**	**21,623**	**129,41**	**422,370**
SWITCH	1,007	25,55	164,15	21,3	196,90	100541	444983	22,594	133,99	3,975
	1,070	25,84	162,31	21,5	195,07	97735	440248	22,200	133,24	0,914
	1,383	24,85	168,77	23,3	180,00	134580	447328	30,085	121,66	279,893
	1,084	26,05	161,00	22,8	183,95	76304	417775	18,264	132,83	1,257
	1,045	25,45	164,79	21,9	191,51	117011	450423	25,978	129,70	600,590
	0,846	24,96	168,03	23,6	177,71	171236	487878	35,098	123,17	789,358
	1,120	25,47	164,66	21,6	194,17	117994	430112	27,433	121,41	1,091
	1,028	25,36	165,38	21,9	191,51	107146	434403	24,665	127,30	5,678
	1,140	24,77	169,32	23,3	180,00	136103	449990	30,246	122,10	0,937
	1,181	25,17	166,63	21,8	192,39	131193	454769	28,848	125,87	25,145
	1,090	**25,35**	**165,50**	**22,30**	**188,32**	**118984,3**	**445790,9**	**26,541**	**127,13**	**170,884**
Wi-Fi	2,125	61,15	68,59	60,2	69,67	230635	382820	60,246	59,20	759,547
	2,845	67,60	62,04	67,8	61,86	230269	382220	60,245	59,11	237,177
	2,325	59,77	70,17	61,8	67,86	228452	377842	60,462	58,11	653,536
	2,431	67,05	62,55	60,6	69,21	221059	382419	57,805	62,77	513,542
	2,974	71,65	58,53	61,4	68,31	227813	382817	59,510	60,30	247,024
	4,075	58,30	71,94	65,0	64,52	216177	379829	56,914	63,66	105,079
	2,698	69,79	60,09	69,0	60,78	223111	381222	58,525	61,51	585,124
	3,365	59,69	70,26	62,1	67,54	228543	382475	59,754	59,88	340,045
	2,547	60,14	69,74	65,5	64,03	217548	378540	57,470	62,63	189,900
	2,541	58,67	71,48	69,9	60,00	225805	382578	59,022	60,98	571,365
	2,793	**63,38**	**66,54**	**64,33**	**65,38**	**224941,2**	**381276,2**	**58,995**	**60,81**	**420,234**

tab. 9: PPTP – LAN detailní výsledky

D. PPTP – WAN

	doba odezvy	kopírování 500 MB		iperf TCP 500 MB		iperf UDP 30 sekund				
	hrPING	čas	rychlost	čas	rychlost	ztraceno	posláno	ztrátovost	rychlost	jitter
	(ms)	(s)	(Mbits/s)	(s)	(Mbits/s)	datagramů	datagramů	(%)	(Mbits/s)	(ms)
ROUTER	1,125	36,61	114,56	29,4	142,65	187688	513338	36,562	126,68	24,221
	1,095	36,51	114,87	28,5	147,16	173663	499817	34,745	126,87	0,938
	1,247	35,06	119,62	28,8	145,63	165496	490518	33,739	126,43	1,014
	1,116	36,56	114,72	28,4	147,68	181810	515649	35,258	129,86	14,645
	1,099	36,11	116,15	29,1	144,12	192236	529413	36,311	131,16	1,762
	1,324	36,31	115,51	28,7	146,13	175899	510506	34,456	130,16	0,938
	1,062	36,06	116,31	29,0	144,62	135408	475965	28,449	132,48	15,626
	0,964	35,41	118,44	28,6	146,64	159853	496516	32,195	130,96	1,262
	1,009	35,95	116,66	29,1	144,12	166541	501415	33,214	130,27	18,561
	1,128	35,99	116,53	28,9	145,12	145214	485232	29,927	132,27	5,241
	1,117	**36,06**	**116,34**	**28,85**	**145,39**	**168380,8**	**501836,9**	**33,486**	**129,71**	**8,421**
Wi-Fi	2,524	59,10	70,96	63,8	65,74	237319	393649	60,287	60,81	162,600
	2,934	57,90	72,44	71,1	58,99	185852	347643	53,461	62,94	1109,700
	1,930	58,60	71,57	65,9	63,64	218590	380005	57,523	62,79	301,640
	3,587	56,34	74,44	68,9	60,87	218288	383416	56,932	64,23	808,880
	2,258	58,24	72,01	64,0	65,53	205137	378839	54,149	67,57	569,010
	2,368	63,37	66,18	69,7	60,17	219192	382421	57,317	63,50	337,890
	2,157	58,01	72,30	64,8	64,72	211039	382421	55,185	66,67	671,440
	2,011	59,07	71,00	66,0	63,55	221834	382222	58,038	62,39	896,070
	3,254	60,30	69,55	70,3	59,66	243106	398646	60,983	60,51	52,670
	2,537	57,01	73,57	67,8	61,86	235485	395805	59,495	62,36	139,254
	2,556	**58,79**	**71,40**	**67,23**	**62,47**	**219584,2**	**382506,7**	**57,337**	**63,38**	**504,915**

tab. 10: PPTP – WAN detailní výsledky

E. L2TP/IPSEC - LAN

	doba odezvy	kopírování 500 MB		iperf TCP 500 MB		iperf UDP 30 sekund				
	hrPING	čas	rychlost	čas	rychlost	ztraceno	posláno	ztrátovost	rychlost	jitter
	(ms)	(s)	(Mbits/s)	(s)	(Mbits/s)	datagramů	datagramů	(%)	(Mbits/s)	(ms)
KABEL	1,254	28,10	149,25	25,1	167,09	135475	415247	32,625	108,83	5,527
	1,214	27,97	149,95	24,9	168,43	130547	425685	30,668	114,81	15,247
	1,096	28,50	147,16	25,9	161,93	122547	421457	29,077	116,28	35,685
	1,345	28,34	147,99	24,5	171,18	121698	426895	28,508	118,72	3,647
	1,142	28,14	149,04	26,1	160,69	115478	405874	28,452	112,96	1,028
	1,234	28,96	144,82	26,2	160,08	114574	406985	28,152	113,75	3,247
	1,301	27,86	150,54	25,7	163,19	125478	411257	30,511	111,17	15,247
	1,009	28,64	146,44	25,0	167,76	125405	415698	30,167	112,92	56,875
	1,121	28,06	149,47	26,6	157,67	126850	421574	30,090	114,65	9,365
	1,234	28,60	146,64	25,7	163,19	122306	415879	29,409	114,20	3,254
	1,195	**28,32**	**141,26**	**25,57**	**164,12**	**124035,8**	**416655,1**	**29,766**	**113,83**	**14,912**
SWITCH	1,057	28,15	148,99	25,0	167,76	124567	400547	31,099	107,36	3,254
	1,196	29,63	141,55	25,4	165,12	130574	411245	31,751	109,18	0,978
	1,205	28,54	146,95	26,0	161,31	128475	421478	30,482	113,98	15,247
	1,147	28,06	149,47	25,7	163,19	140214	405124	34,610	103,05	105,502
	1,006	28,15	148,99	25,5	164,47	145210	435124	33,372	112,78	3,698
	1,167	28,43	147,52	26,0	161,31	148574	421025	35,289	105,98	3,574
	1,507	27,94	150,11	25,4	165,12	157480	436360	36,089	108,48	11,104
	1,224	28,06	149,47	26,1	160,69	140254	418574	33,508	108,27	145,254
	1,209	28,60	146,64	26,0	161,31	141249	425425	33,202	110,54	136,365
	1,195	28,47	147,31	25,9	161,93	142574	430280	33,135	111,92	5,247
	1,191	**28,40**	**140,83**	**25,7**	**163,22**	**139917,1**	**420518,2**	**33,254**	**109,15**	**43,022**
Wi-Fi	2,293	61,07	68,68	73,8	56,83	200547	356854	56,199	60,80	16,600
	5,109	63,99	65,54	71,3	58,82	198745	355127	55,964	60,83	3,600
	3,175	65,08	64,44	76,3	54,97	208560	359647	57,990	58,77	1,254
	2,907	64,38	65,14	75,1	55,85	223475	374578	59,660	58,78	15,550
	2,874	67,50	62,13	69,9	60,00	222456	370574	60,030	57,62	1,670
	3,095	64,35	65,17	74,2	56,52	224870	386439	58,190	62,85	26,142
	2,741	63,86	65,67	70,0	59,91	218561	354020	61,737	52,69	65,187
	2,654	62,57	67,03	75,9	55,26	231156	399723	57,829	65,57	5,057
	2,593	69,67	60,20	71,8	58,41	218749	374585	58,398	60,62	11,100
	2,173	65,16	64,36	70,5	59,49	221475	378457	58,521	61,07	162,100
	2,961	**64,76**	**61,76**	**72,88**	**57,61**	**216859,4**	**371000,4**	**58,452**	**59,96**	**30,826**

tab. 11: L2TP/IPSEC – LAN detailní výsledky

F. L2TP/IPSEC - WAN

	doba odezvy	kopírování 500 MB		iperf TCP 500 MB		iperf UDP 30 sekund				
	hrPING	čas	rychlost	čas	rychlost	ztraceno	posláno	ztrátovost	rychlost	jitter
	(ms)	(s)	(Mbits/s)	(s)	(Mbits/s)	datagramů	datagramů	(%)	(Mbits/s)	(ms)
ROUTER	1,257	37,99	110,40	32,1	130,65	229407	514050	44,627	110,73	68,991
	1,503	38,61	108,62	33,2	126,33	200475	478257	41,918	108,06	93,435
	1,335	38,11	110,05	31,6	132,72	232140	522417	44,436	112,92	84,316
	1,647	37,98	110,43	30,9	135,73	231022	511407	45,174	109,07	60,639
	1,364	38,51	108,91	31,0	135,29	220548	498541	44,239	108,14	192,219
	1,420	38,05	110,22	32,9	127,48	215899	487522	44,285	105,66	353,001
	1,358	38,66	108,48	32,1	130,65	189472	456008	41,550	103,68	291,532
	1,254	39,11	107,24	31,9	131,47	221578	505445	43,838	110,42	282,891
	1,608	37,69	111,28	31,8	131,89	202405	462544	43,759	101,19	41,714
	1,547	38,61	108,62	33,1	126,71	198685	461405	43,061	102,20	169,168
	1,429	**38,33**	**104,35**	**32,06**	**130,89**	**214163,1**	**489759,6**	**43,689**	**107,21**	**163,791**
Wi-Fi	3,015	77,65	54,01	71,3	58,82	224750	357946	62,789	51,81	358,567
	2,969	76,95	54,50	73,7	56,91	234507	376047	62,361	55,06	632,909
	5,096	78,11	53,69	75,5	55,55	211457	354890	59,584	55,80	845,124
	4,512	78,15	53,67	78,9	53,16	223059	360508	61,874	53,47	677,110
	5,505	77,88	53,85	72,2	58,09	235470	380463	61,890	56,40	659,202
	4,993	78,12	53,69	73,6	56,98	232401	377401	61,579	56,41	221,020
	5,044	78,22	53,62	77,0	54,47	204105	340505	59,942	53,06	344,005
	5,014	78,01	53,76	73,2	57,30	221570	356986	62,067	52,68	178,227
	4,534	77,50	54,12	74,7	56,14	205006	342578	59,842	53,52	526,976
	6,547	78,64	53,33	73,6	56,98	200417	345789	57,959	56,55	345,934
	4,723	**77,92**	**51,33**	**74,37**	**56,44**	**219274,2**	**359311,3**	**60,989**	**54,47**	**478,907**

tab. 12: L2TP/IPSEC – WAN detailní výsledky

G. SSTP – LAN

	doba odezvy	kopírování 500 MB		iperf TCP 500 MB		iperf UDP 30 sekund				
	hrPING	čas	rychlost	čas	rychlost	ztraceno	posláno	ztrátovost	rychlost	jitter
	(ms)	(s)	(Mbits/s)	(s)	(Mbits/s)	datagramů	datagramů	(%)	(Mbits/s)	(ms)
KABEL	2,024	26,44	158,62	23,5	178,47	121524	435471	27,906	122,13	1,085
	1,964	25,68	163,32	23,8	176,22	104580	419874	24,907	122,65	3,254
	2,347	27,74	151,19	23,9	175,48	112470	430457	26,128	123,70	74,254
	2,147	27,25	153,91	23,2	180,78	105628	428451	24,653	125,58	2,369
	2,067	28,07	149,41	24,1	174,02	107407	435060	24,688	127,46	2,478
	2,397	25,78	162,68	23,7	176,96	101547	420412	24,154	124,04	0,987
	1,978	24,99	167,83	23,5	178,47	121478	418745	29,010	115,64	35,254
	2,338	25,36	165,38	24,0	174,75	106356	434521	24,477	127,66	0,998
	2,147	26,17	160,26	23,1	181,56	121478	424512	28,616	117,88	2,360
	1,247	27,05	155,05	22,9	183,14	124478	419874	29,647	114,91	3,247
	2,066	**26,45**	**151,21**	**23,57**	**177,99**	**112694,6**	**426737,7**	**26,419**	**122,16**	**12,6286**
SWITCH	1,945	26,55	157,97	23,6	177,71	168190	488489	34,431	124,60	1,096
	1,893	28,22	148,62	23,8	176,22	104016	405420	25,656	117,25	1,322
	1,832	28,11	149,20	23,8	176,22	102783	408904	25,136	119,08	0,946
	3,070	25,56	164,08	22,4	187,23	103924	440787	23,577	131,04	0,939
	2,170	27,07	154,93	23,2	180,78	100740	389814	25,843	112,45	0,915
	2,067	27,10	154,76	22,9	183,14	101166	413192	24,484	121,38	0,034
	2,194	26,45	158,56	23,5	178,47	102975	412909	24,939	120,56	5,235
	1,993	25,98	161,43	24,0	174,75	115214	408749	28,187	114,19	1,025
	2,175	26,96	155,56	22,8	183,95	131450	438904	29,950	119,60	0,935
	2,094	28,50	147,16	23,5	178,47	105407	430479	24,486	126,45	3,254
	2,143	**27,05**	**147,87**	**23,35**	**179,69**	**113586,5**	**423764,7**	**26,669**	**120,66**	**1,5701**
Wi-Fi	2,969	55,97	74,93	63,7	65,84	2233	242706	0,920	93,54	0,907
	3,437	61,60	68,08	60,2	69,67	2585	243362	1,062	93,66	11,247
	3,033	58,94	71,16	64,3	65,23	1556	213350	0,729	82,39	0,731
	4,267	57,80	72,56	62,6	67,00	2801	270694	1,035	104,21	3,354
	3,318	60,06	69,83	64,9	64,62	1610	227284	0,708	87,79	1,250
	3,825	61,21	68,52	61,3	68,42	5478	257480	2,128	98,03	12,254
	3,048	55,84	75,11	62,8	66,78	38720	287476	13,469	96,77	28,547
	2,913	59,47	70,52	63,0	66,57	11230	224706	4,998	83,04	118,745
	3,118	57,98	72,34	64,6	64,92	1874	254786	0,736	98,38	1,257
	2,894	59,64	70,32	61,9	67,75	5603	202678	2,764	76,66	6,325
	3,282	**58,85**	**67,97**	**62,93**	**66,68**	**7369**	**242452,2**	**2,855**	**91,45**	**18,4617**

tab. 13: SSTP – LAN detailní výsledky

H. SSTP - WAN

	doba odezvy	kopírování 500 MB		iperf TCP 500 MB		iperf UDP 30 sekund				
	hrPING	čas	rychlost	čas	rychlost	ztraceno	posláno	ztrátovost	rychlost	jitter
	(ms)	(s)	(Mbits/s)	(s)	(Mbits/s)	datagramů	datagramů	(%)	(Mbits/s)	(ms)
ROUTER	2,431	31,80	131,89	28,8	145,63	102354	434361	23,564	129,15	0,914
	2,397	34,90	120,17	28,5	147,16	101813	404304	25,182	117,67	24,125
	2,427	32,60	128,65	28,6	146,64	101387	357331	28,373	99,56	1,207
	2,484	33,05	126,90	28,3	148,20	131577	444493	29,602	121,72	0,980
	2,395	33,98	123,43	30,1	139,34	105717	413425	25,571	119,70	1,013
	2,404	32,54	128,89	29,1	144,12	121478	405088	29,988	110,32	3,254
	2,308	32,78	127,94	28,9	145,12	136587	415478	32,875	108,49	11,236
	2,395	35,78	117,22	28,3	148,20	125740	420475	29,904	114,65	3,254
	2,258	33,47	125,31	28,8	145,63	121470	418956	28,993	115,72	2,140
	2,311	33,07	126,82	28,1	149,25	136589	425408	32,108	112,35	7,587
	2,381	**33,40**	**119,77**	**28,75**	**145,93**	**118471,2**	**413931,9**	**28,616**	**114,93**	**5,571**
Wi-Fi	3,620	56,20	74,63	69,5	60,35	80788	246750	32,741	64,56	5,247
	3,123	63,71	65,83	71,1	58,99	83210	236394	35,200	59,59	0,917
	3,230	58,90	71,21	68,3	61,41	83444	251915	33,124	65,54	27,875
	3,176	61,25	68,47	70,1	59,83	89144	189767	46,976	39,14	1,028
	3,553	59,69	70,26	69,2	60,61	82964	243064	34,133	62,28	155,207
	4,985	65,70	63,84	70,0	59,91	91240	254124	35,904	63,36	145,024
	3,225	58,68	71,47	72,6	57,77	83421	236580	35,261	59,58	3,024
	5,658	59,30	70,73	67,2	62,41	81511	222145	36,693	54,71	68,547
	6,915	57,48	72,96	73,1	57,37	95360	258024	36,958	63,28	36,257
	4,422	57,70	72,69	72,3	58,01	107485	223406	48,112	45,09	1,245
	4,191	**59,86**	**66,82**	**70,34**	**59,66**	**87856,7**	**236216,9**	**37,510**	**57,71**	**44,4371**

tab. 14: SSTP – WAN detailní výsledky