Vzdálená správa počítačů

Remote Administration of Computers

Lukáš Mlýnek

Bakalářská práce
2013

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2012/2013

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

Jméno a příjmení:	**Lukáš MLÝNEK**
Osobní číslo:	**A10046**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Informační a řídicí technologie**
Forma studia:	**prezenční**
Téma práce:	**Vzdálená správa počítačů**

Zásady pro vypracování:

1. **Vypracujte rešerši v oblasti vzdálené správy počítače přes Internet.**
2. **Popište možnosti pro vzdálenou správu počítače pro různé OS.**
3. **Navrhněte vhodné programy pro vzdálenou správu počítače.**
4. **V praktické části vytvořte návody na instalaci a popište problémy instalace a nastavení programů.**
5. **Otestujte hardwarovou a síťovou náročnost vybraného software.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **ŠTEIDL, Přemysl. Srovnání VPN realizací. [online]. 2007 [cit. 2012-11-25]. Diplomová práce. Masarykova univerzita, Fakulta informatiky. Vedoucí práce Radek Ošlejšek. Dostupné z: http://is.muni.cz/th/60463/fi_m/**
2. **TULLOCH, M., NORTHRUP, T. and HONEYCUTT J. Windows 7 resource kit. 1 Pap/Cdr. Redmond, Washington: Microsoft Press, 2009. ISBN 07-356-2700-2.**
3. **RUSSEL, Charlie a Sharon CRAWFORD. THE MICROSOFT WINDOWS TEAM. Microsoft Windows XP Professional: Resource Kit. 3. vyd. Redmond, Washington: Microsoft Press, 2005. ISBN 0-7356-1485-7.**
4. **LAMMLE, Todd. CCNA: Cisco Certified Network Associate Study Guide. Indianaposlis, Indiana: Wiley Publishing, 2007. ISBN 978-0-470-11008-9.**
5. **ODOM, Wendell. Počítačové sítě bez předchozích znalostí. Vyd. 1. Brno: CP Books, 2005, 383 s. ISBN 80-251-0538-5.**

Vedoucí bakalářské práce:	**Ing. Jiří Vojtěšek, Ph.D.** Ústav řízení procesů
Datum zadání bakalářské práce:	**24. února 2013**
Termín odevzdání bakalářské práce:	**14. června 2013**

Ve Zlíně dne 24. února 2013

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

prof. Ing. Vladimír Vašek, CSc.
ředitel ústavu

ABSTRAKT

Tato bakalářská práce je věnována vzdálené správě a ovládání počítače. Jsou zde rozebrány základní teoretické oblasti týkající se daného tématu s mírným ohledem na bezpečnost. V praktické části je vybráno několik možných řešení, která jsou následně aplikována. Po prostudování tohoto materiálu by měl být člověk schopen vysvětlit, jak vzdálený přístup obecně funguje a dále by měl být schopen vybrat vhodnou metodu vzdáleného přístupu a aplikovat ji v praxi.

Klíčová slova: VNC, VPN, RDP, RFB, RD, Vzdálená správa, Vzdálená podpora, Vzdálený přístup, Vzdáleně ovládaný počítač

ABSTRACT

This thesis is devoted to remote administration and remote computer control. Basic theoretical areas relevant to the topic are analysed, with a slight emphasis put on security problems. In the practical part several possible solutions are chosen and applied. Having studied the thesis, one should be able to explain how remote access generally works and to choose a suitable remote access method and apply it in practice.

Keywords: VNC, VPN, RDP, RFB, RD, Remote Administration, Remote Support, Remote Access, Remote Computer Control

Poděkování:

Rád bych touto cestou poděkoval především panu Ing. Jiřímu Vojtěškovi, Ph.D. za ochotu, trpělivost a věcné rady, které velmi pomohly vzniku této práce.

Poděkování patří také mé rodině a přítelkyni za podporu a vytvoření kvalitního zázemí pro studium na vysoké škole.

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….…….

podpis diplomanta

OBSAH

ÚVOD

Tématem mé bakalářské práce je vzdálené ovládání počítače. Dané téma jsem si zvolil, protože tuto činnost považuji za velmi užitečnou a aktuální. Vzdálené ovládání počítače by mělo patřit k základním dovednostem každého administrátora či zkušenějšího uživatele.

V dnešní „uspěchané“ době může vzdálené ovládání počítače ušetřit mnoho času a také finančních nákladů. Není již nutné být fyzicky přítomen u spravované stanice a toto konání nemusí být praktikováno pouze k pomoci méně zkušeným uživatelům nebo pro správu serverových či síťových zařízení. Vzdálená správa napomáhá i v případě, kdy člověk vlastní více počítačů a inteligentních zařízení jako je smartphone (chytrý telefon) nebo tablet. S rozšířením Internetu a užíváním této činnosti může mít člověk vždy všechna svá data přístupná.

K tomuto tématu jsem nenalezl příliš mnoho vhodné literatury, a proto bych rád čtenáře seznámil se základními principy, protokoly a některými aplikacemi určenými ke vzdálenému přístupu k počítači. V teoretické části jsou proto popsány důležité pojmy z oblasti sítí a operačních systémů, na kterých vzdálené ovládání počítače staví. Je zde zmíněn protokol RFB, RDP, komunikace typu klient-server aj.

Praktická část se věnuje několika programům, které umožňují vzdálené ovládání počítače. Je zde zmíněn postup jejich instalace, nastavení a samotného zprovoznění přístupu. Spolu s těmito činnostmi jsou provedena i měření síťové zátěže a vytíženosti hardwaru. V neposlední řadě se zde nachází také popis řešení obvyklých problémů spojených s navázáním spojení.

I. TEORETICKÁ ČÁST

1 VYMEZENÍ ZÁKLADNÍCH POJMŮ

Pro správné pochopení principů spjatých se vzdáleným připojením k počítači jsou v první kapitole uvedeny základní pojmy z oblasti operačních systémů a počítačových sítí. Nejprve tedy pojem Internet.

1.1 Internet

Skupinu počítačů navzájem propojených a schopných komunikace můžeme nazvat počítačovou sítí. Těchto sítí může být několik, mohou být propojeny mezi sebou a mohou využívat pro svou komunikaci různých protokolů. Takovéto uskupení se někdy nazývá internet (s malým „i“). Naproti tomu Internet (s velkým „I“) je celosvětová počítačová komunikační a informační síť, postavená na rodině protokolů TCP/IP. Vychází z mnoha sítí, které jsou navzájem propojeny napříč vyspělými civilizacemi.

1.2 IP (Internet Protocol)

Internet využívá pro řadu služeb mnoha různých protokolů. Důležitým protokolem pro vzdálenou plochu a nejen pro ni je protokol IP. Je základním protokolem dnešního Internetu a počítačových sítí. Způsobem komunikace jej řadíme mezi nespolehlivé, nespojované protokoly. Definuje logické adresování a směrování. Pracuje na úrovni vrstvy síťového rozhraní (network layer) modelu OSI[1] a využívá 32 bitové[2] abstraktní adresy (nejsou spjaty s hardware a výrobcem).

Z hlediska vzdáleného připojení k počítači je nutné poznamenat, že každý počítač, uzel (obecně zařízení pracující minimálně s třetí vrstvou modelu OSI) připojený k Internetu, by měl mít jednoznačnou (unikátní) IP adresu. Pokud počítač takovou adresu má, je možné se na něj při správné konfiguraci vzdáleně připojit. Existují také výjimky např. privátní IP adresy, které využívá velké množství zařízení vyskytujících se převážně v lokálních sítích za směrovačem (routerem) využívajícím NAT (Network Address

[1] Sedmivrstvý abstraktní model, který popisuje komunikaci mezi počítači.

[2] 32bitů pro protokol IPv4, který je nejpoužívanější (k r. 2013), IPv6 používá adresu složenou z 128bitů

Translation). Nejznámější rozsah privátních adres je typu C: 192.168.0.0 - 192.168.255.255.

1.2.1 Statická, dynamická IP adresa

Jak již z názvu vyplývá, statická IP adresa je staticky přidělena „nějakému“ interface[3] a pokud to není nutné, tak se nemění. Tato adresa je vhodná pro realizaci vzdáleného připojení, či VPN (viz *1.9 VPN)*. Naopak dynamická IP adresa je obvykle během trvání připojení stejná (pokud nevyprší doba exspirace), ale při každém novém připojení nebo restartování zařízení (interface) se zpravidla změní. Tato adresa je dynamicky přidělená z daného rozsahu IP adres. Dynamické přidělované IP adresy nejsou vhodné pro remote desktop (vzdálená plocha, dále jen RD).

Statické i dynamické adresy mohou být adresami veřejnými nebo neveřejnými.

1.2.2 Veřejná, neveřejná IP adresa

Zjednodušeně se dá veřejná IP adresa charakterizovat tak, že je „viditelná“ z Internetu. Naopak neveřejná IP adresa je zpravidla z Internetu nepřístupná. Ačkoli není dnes naprosto nevyhnutelné mít veřejnou IP adresu, z pohledu RD je to nadmíru vhodné. Pokud veřejná IP adresa není k dispozici, je možné využít pro RD „pomocných“ prostředků jako je VPN, specifická čísla portů či speciální programy (popsáno dále v teoretické i praktické části).

1.3 Port

Za pomoci IP adresy je možné adresovat počítač, či obecně uzel v síti. Za pomoci portu se pak upřesňuje, ke které službě resp. procesu (úloze, vláknu dále jen proces) se data vztahují v rámci daného koncového zařízení.

Lze říci, že mezi procesem a portem existuje vztah *jedna k n*. Jeden proces může být sdružen s více porty, ale s jedním portem může být sdružen pouze jeden proces.

---

[3] Interface, česky rozhraní. V tomto případě myšleno jako síťová karta nebo zařízení komunikující za pomoci počítačové sítě.

Port je obecně dvoubajtové číslo, tedy o rozsahu 0 až 65535. Přidělováním portů se zabývá organizace IANA, která dělí tento rozsah do tří částí. Prvních 1024 portů resp. 0 až 1023 jsou tzv. *dobře známé porty* (z angl.. well-known ports). Mezi nejznámější porty patří např. port 80 (HTTP), 110 (POP3) apod. Druhou skupinou jsou tzv. *registrované porty* v rozsahu 1024 až 49152. Třetí skupinou jsou porty *dynamické a privátní* (někdy také překládané jako dynamické a soukromé). Mají rozsah 49152 až 65535 a nemohou být registrovány u organizace IANA. Tato řada se používá pro vlastní nebo dočasné účely a pro automatické přidělování dočasných portů.

Tabulka 1 uvádí obvyklá čísla portů aplikací a protokolů týkajících se RD a jemu příbuzných činností. Jedná se především o protokoly spojované služby TCP (na rozdíl od nespojované služby UDP).

Aplikace nebo protokol	**Porty (defaultní)**
ARD (Apple Remote Desktop)	3283
LogMeIn (Hamachi)	80, 443 nebo 2002, 12975 (initiator port), 32976 (session port)
OpenSSH	911
Radmin (Remote Administrator)	4899
RD (Windows)	3389
RDP	3389
Real VNC	5900 až 5906 (číslo 0,1, atd. značí číslo obrazovky)
RFB	5900 nebo 5800 pro klienta, 5500 tzv. naslouchací mód - pozorovatel
RSH (Remote Shell)	514
Secured Telnet	992
SSH	22
TeamViever	80 (HTTP) nebo 443(HTTPS)
TeamViewer - Remote Desktop Protocol	5938
Telnet	23, 107 Remote TELNET Service
VNC	5900 až 5906 nebo 5800 až 5806 (číslo 0,1, atd. značí číslo obrazovky)

Tabulka 1 Obvyklé porty RD aplikací a protokolů

Některé aplikace používají standardní porty jako je 80 (HTTP) nebo 443 (HTTPS). Je tomu tak hlavně z důvodu, že tyto porty jsou obvykle povoleny na všech směrovačích (routerech) kvůli standartním službám Internetu.

1.4 Komunikace typu klient-server

Při používání vzdáleného přístupu a nejen u něj rozlišujeme dva typy komunikujících koncových zařízení. Jedná se o klienta a server. Hlavním účelem modelu klient/server je snaha minimalizovat objem dat, přenášených po síti mezi klientem a serverem.

Klient (client, někdy také viewer) je zařízení, u kterého jsme obvykle fyzicky přítomni. Z hlediska hardwaru, klient zpravidla obsahuje zobrazovací zařízení (monitor) a vstupní zařízení, jako je klávesnice, myš apod. Klientem může být např. i aplikace jakou je webový prohlížeč, který se připojuje k webovým serverům.

Na opačném konci počítačové sítě je pak server. Od serveru žádá klient obvykle nějakou službu. Je snaha, aby se většina náročných operací vykonávala na straně serveru. V praxi to pak znamená, že klient není zatěžován zpracováním, ale pouze dostává výsledné informace.

Z hlediska RD lze chápat klienta a server následovně.

Server je program na počítači, který sdílí svou obrazovku a prostředky. Server pasivně umožňuje klientovi, aby nad ním měl kontrolu. Klient je program, který sleduje, kontroluje a interaguje se serverem. Jednoduše řečeno klient ovládá server. Pokud se klient odpojí nebo se spojení přeruší a následně se znovu naváže, server a všechny běžící aplikace v něm zůstanou ve stavu, ve kterém jste jej opustili. Model klient/server využívají aplikace pro vzdálené ovládání počítače typu VNC (viz *Obrázek 1).*

Obrázek 1 Komunikace klient – server v RD

Jiným typem komunikace je např. Peer-to-Peer, někdy také zkracována na P2P. Zde jsou obě dvě koncová zařízení rovna. Zjednodušeně řečeno, obě dvě zařízení mohou pracovat zároveň jako server či klient. Tento způsob využívá např. aplikace MingleView, která je založena na protokolu RFB.

1.5 Tenký a tlustý klient

Tenkým klientem je většinou software, který přijímaná data nikterak složitě nezpracovává, ale rovnou je předává uživateli. Často není nutné jej ani instalovat. Reprezentantem tenkého klienta je např. klient používaný v aplikaci „Připojení ke vzdálené ploše“ od společnosti Microsoft. Dále může být tenkým klientem i počítač s minimální instalací operačního systému. Takovýmto operačním systém je obvykle speciální distribuce Linuxu a všechno kromě výstupu a vstupu za něj provádí server. Tato varianta je náročná především na server.

Tlustý klient integruje obvykle více funkcí a je na jeho straně vykonávána část logiky. Tlustý klient by měl být na stanici nainstalovaný nebo by se měl automaticky spouštět. Tato varianta je již náročná i na klientskou část, protože data jsou zpracovávána na straně klienta. Server pak slouží jako zdroj dat, ale může je také zpracovávat. Výhodou tohoto řešení je větší flexibilita klienta.

1.6 Telnet

Telnet je jedním z nejstarších protokolů (a aplikací) sloužících ke vzdálenému připojení k počítači. Samotná komunikace mezi klientem a serverem je nezabezpečená, resp. přenášená data nejsou šifrována. Proto se nedoporučuje tento způsob připojení používat a byl nahrazen pokročilejšími protokoly jako je např. SSH (Secure Shell). I přesto je však Telnet součástí dnešních Microsoft Windows i Unixových systémů.

Služba Telnet je založena na specifikaci RFC (Request for Comments) 854. Tato specifikace určuje, jakým způsobem se přenášejí nešifrované znaky sady ASCII (myšlen prostý text) za pomoci počítačové sítě.

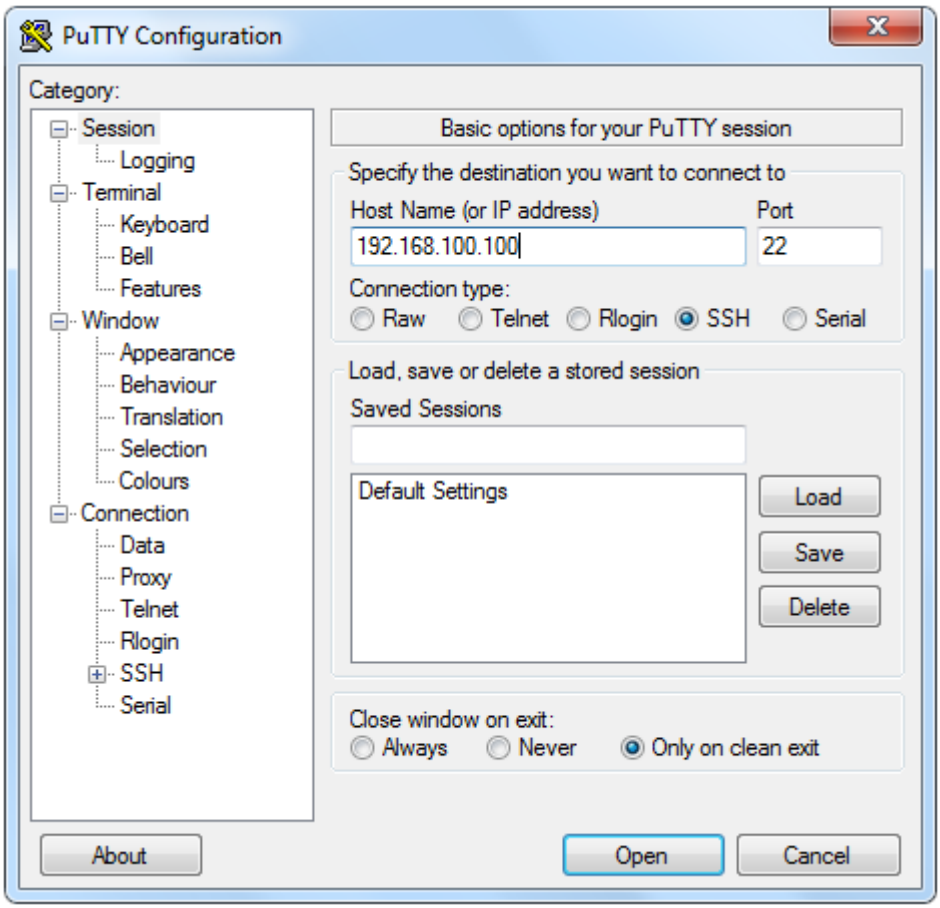
Telnet pracuje v textovém režimu a nepodporuje žádné grafické funkce. Lze tedy pracovat pouze programy využívající textový režim. Toto se může zdát poněkud nevýhodné, avšak Telnet má jednu nespornou výhodou – lze jej použít napříč různými operačními systémy. V dnešní době se ještě stále používá a to zejména pro výukové účely nebo např. pro komunikaci s emailovými servery, simulacemi SMTP a konfigurací síťových zařízení.

1.7 SSH

Jak již bylo zmíněno výše, SSH byl vyvinut jako náhrada za (nebezpečný) protokol/aplikaci Telnet. Rozšířený je především v Linuxu, kde se používá pro textovou vzdálenou správu počítače nebo pro přenos souborů. Na rozdíl od Telnetu však veškerou komunikaci (včetně autentizace) šifruje. Sám o sobě neposkytuje vzdálené ovládání (to je záležitostí OS), ale vytváří šifrovaný komunikační kanál. Od prvopočátku SSH vzniklo několik změn protokolu. Nyní patří mezi běžně nasazované verze SSH 2.

SSH již není nativně obsažen v Microsoft Windows ani jako klient, ani jako server. Je spíše výhradou Linuxových operačních systémů. Lze jej, respektive jeho serverovou část snadno doinstalovat v Linuxových distribucích. Mezi nejznámější serverové části patří SSH Tectia (navržen firmou SSH Communication Security a jedná se o komerční produkt), OpenSSH, který je šířen pod licencí BSD, FreeSSH taktéž šířen pod BSD licencí.

Známým klientem SSH pro Windows je program s názvem Putty (viz *Obrázek 2)*. Program není nutno instalovat.



Obrázek 2 Konfigurační okno programu Putty

SSH neslouží pouze pro vzdálenou správu, ale je možné jej využít pro přenos souborů nebo jako šifrovací tunel pro různé aplikace.

1.8 VNC

VNC je systém sloužící k vzdálenému ovládání počítače s grafickým uživatelským prostředím. Celý systém se pak skládá z klienta, serveru a komunikačního protokolu. Komunikace probíhá přes počítačovou síť za pomoci protokolu RFB (popsán níže).

První zmínka o VNC se objevuje v laboratoři Olivetti & Oracle Research Lab, kde vzniknul i program RealVNC, který existoval i s licencí open source. Proto je dnes možné setkat se s VNC od mnoha různých výrobců. VNC software lze nalézt na mnoha platformách a to i mobilních. Často jsou samotné programy vybaveny nadstandartními funkcemi, které protokol RFB neposkytuje.

Nevýhodou původní implementace je, že komunikace není šifrována. Proto lze u většiny nových programů VNC (konkrétně u nastavení serverové části) zvolit jednu

z možností šifrování komunikace. Jedním z možných způsobů je využití zabezpečeného síťového tunelu pomocí SSH.

1.9 VPN

VPN (Virtual Private Networks) jsou virtuální sítě umožňující propojení zařízení (servery, počítače, telefony apod.), nebo celých sítí skrze počítačovou síť – nejčastěji skrze veřejný Internet. Toho je dosaženo za pomoci speciálních protokolů založených na rodině protokolů TCP/IP nazývaných tunelovací protokoly, nebo za pomoci správně nastaveného hardwaru resp. směrovačů (routerů). Jedním z protokolů k zapouzdřování paketů protokolu IP při přenosu prostřednictvím veřejné sítě je protokol PPTP (Point-to-Point Tunneling Protocol). Mezi další protokoly např. patří L2TP (Layer Two Tunneling Protocol) nebo SSTP (Secure Socket Tunneling Protocol).

Komunikace je samozřejmě šifrována. Protokol PPTP využívá např. MPPE (Microsoft Point-to-Point Encryption) a jsou využívány šifrovací klíče (MS-CHAP verze 2 nebo EAP-TLS). U L2TP se pak používá algoritmu DES (Data Encryption Standard) nebo složitější varianty 3DES (Triple DES).

VPN sítě lze rozdělit do tří základních forem:

1. Propojení Uzel – Uzel. Lze si představit jako připojení klienta banky skrze Internet k zabezpečené bankovní aplikaci.
2. Propojení Uzel – Síť někdy také známé pod názvem „Road Warrior“. Příkladem je např. zaměstnanec firmy, který se připojuje mimo své pracoviště do podnikové sítě.
3. Propojení Síť – Síť. Zde je možné si představit lokální síť vytvořenou propojením dvou vzdálených pracovišť resp. lokálních sítí dvou pracovišť skrze Internet.

VPN lze tedy využít pro vzdálené ovládání stanice, pokud stanice není přímo viditelná z Internetu, tedy nemá veřejnou IP adresu nebo je spojení zabráněno firewallem.

2 PROTOKOLY VZDÁLENÉ PLOCHY

V této kapitole jsou popsány základní principy dvou protokolů vzdáleného připojení k počítači a to RFB a RDP. Konec této kapitoly se věnuje protokolům „neveřejným“ principům či protokolům používaných programy TeamViewer a LogMeIn.

2.1 RFB

RFB (Remote FrameBuffer) je jednoduchý protokol určený ke vzdálenému přístupu s grafickým uživatelským prostředím. Do češtiny bychom jeho název volně přeložili jako *vzdálená snímková vyrovnávací paměť*. Tento protokol je široce aplikován v mnoha VNC aplikacích.

2.1.1 Architektura protokolu

Jak již z názvu vyplývá právě framebuffer je podstatnou částí protokolu. Díky němu je možné RFB protokol využít v nejrůznějších systémech např. Microsoft Windows, Mac OS aj., které využívají grafický režim správce oken.

Framebuffer se skládá z více částí (bufferů). Uchovává informace o barevných hodnotách pro každý pixel (bod, který může být zobrazen na obrazovce). Tyto hodnoty jsou dle počtu barev 1bitové tzv. monochromatický, 4 bitové s paletou, 8 bitové s barevnou paletou, 16 bitové tzv. HighColor nebo dnes nejčastěji 24 bitové tzv. TrueColor. Často se také uchovává informace alfa kanálu. Alfa kanál se používá ve spojitosti s transparentností, jinými slovy průhledností daného pixelu. Dále se skládá např. z Stencil buffer (paměť šablony) či Accumulation buffer (akumulační buffer).

Celkové množství paměti potřebné pro práci framebufferu závisí na rozlišení výstupního signálu, na barevné hloubce a velikosti palety. Minimální velikost snímkové paměti pak získáme, když při daném rozlišení monitoru vynásobíme počet obrazových bodů barevnou hloubkou.

RFB stejně jako RDP používá pro komunikaci rodiny protokolů TCP/IP. Samotné navazování komunikace mezi serverem a klientem probíhá ve třech fázích.

První fáze (někdy nazývána Handshaking) je zaměřena na dohodnutí o používané verzi protokolu RFB a následně je zvolen typ zabezpečení. Server oznámí klientovi, kterou

nejvyšší verzi protokolu může použít a klient následně odpoví zvolenou verzí. Zabezpečení může být buď s autentizací, nebo bez ní. K autentizaci se používá šifrování DES.

Pokud první fáze proběhne úspěšně, následuje druhá - inicializační fáze, ve které se server s klientem dohodnou na formě přístupu a parametrech obrazovky serveru. Forma přístupu může být *výlučný přístup* nebo *sdílený přístup* k serveru s jinými klienty.

Třetí fází je již běžná komunikace, kde se na server posílají vstupní data klienta a ze serveru se posílají obrazová data. Komunikace je samozřejmě kódována, aby se zmenšila vytíženost linky. Mezi metody kódování patří RAW, ZRLE, REE, Hextile apod.

2.1.2 Vlastnosti protokolu

- Použitelný pro všechny „okenní“ systémy
- Efektivní pro pomalé připojení
- Přenosy souborů
- Použití schránky pouze pro text
- Vylepšená komprese
- Dalších mnoho rozšíření v samotných implementacích VNC
- tenký klient
- Možnost výlučného nebo sdíleného přístupu

2.2 RDP

RDP (Remote Desktop Protocol) je protokol vytvořený firmou Microsoft, který poskytuje uživateli grafické připojení k jinému počítači. Je založen na standartu T.120, který se týká doporučení pro základní technologie přenosu multimediálních dat a především pak pro konference obsahující datové přenosy.

Ačkoli jde o produkt Microsoftu, klienti pro připojení k serverům existují na mnoha platformách včetně telefonních, jako jsou Android a iOS. Serverové části se pak pochopitelně nacházejí u OS Microsoftu a existují řešení i pro OS Linux.

2.2.1 Architektura protokolu

Architektura protokolu je velice obsáhlá a Microsoft ji veřejně popisuje v dokumentu s označením „MS-RDPBCGR“.

Protokol je navržen tak, aby jej bylo možné snadno rozšiřovat a modifikovat, k tomu slouží např. virtuální kanály. Při navázaném spojení klienta a serveru klávesnice, myš a obrazová data zabírají jeden kanál a ostatní kanály jsou volné pro jiné služby. Návrh RDP podporoval různé protokoly a topologie počítačových sítí jako jsou IPX, NetBios, TCP/IP atd. V současné době s velkým rozšířením protokolu TCP/IP je v posledních verzích protokolu RDP umožněna činnost jen v souvislosti s tímto protokolem, ač v návrhu zůstala podpora i ostatních.

V zjednodušené podobě protokol RDP zajišťuje čtyři akce: požadavek na připojení, potvrzení připojení, požadavek na odpojení a přenos dat. Požadavek na připojení a požadavek na odpojení vzniká na straně klienta. Všechny tyto akce jsou definované a protokol je zajišťuje, může však nastat např. ukončení ze strany serveru, které již protokol nedefinuje a je nutné jej ošetřit softwarově na klientské straně.

Při navazování komunikace server neví, který typ tenkého klienta jej kontaktuje. Proto veškeré parametry, které charakterizují klienta, se předávají při navazování připojení. Mezi tyto parametry patří: obecné schopnosti klienta (používaný OS, verze protokolu, typ komprese dat), video (velikost rozlišení desktopu, barevná hloubka, bitmapové komprese), bitmapová cache, podpora znakových sad atd.

Bezpečnostní vrstva protokolu zajišťuje veškeré šifrování a podpisy. K šifrování využívá algoritmus RC4, který se vyskytuje i u jiných protokolů jako je např. HTTPS. Podpis se skládá z kombinace metod MD5 a SHA-1. Bezpečnostní vrstva sama řídí přenos ověřování uživatele. Těmito metodami zabraňuje protokol RDP neoprávněným uživatelům naslouchat komunikaci nebo modifikovat přenášená data.

Relevantní vrstva protokolu se stará o přenos dat klávesnice, myši a samotného obrazu. Tato komunikace využívá metody komprimace dat za účelem snížení síťové zátěže. Mimo kompresní činnost využívá také bufferů, které pomáhají snížit zátěž. Buffer je paměť (česky známá jako dočasná paměť), která slouží pro dočasné uchování dat určených k přesunu. Do těchto pamětí se ukládají např. bitmapové obrázky (plocha, často

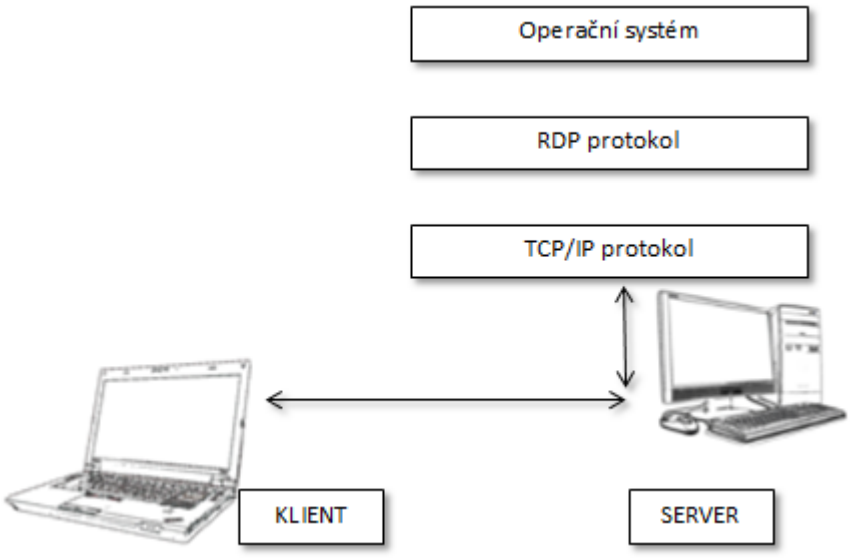
používané programy aj.), znaky apod. Z hlediska bezpečnosti RDP jsou právě buffery někdy útočníky napadány a přehlceny nekorektními daty.

K přenosu obrazu se využívá rastrové grafiky, tedy bitmap, které určují přesnou polohu pixelu a jeho barvu. V současné verzi protokolu je podpora 24 bitových barev.

S protokolem souvisí také speciální pojem Virtuální kanál. Klient RDP nebo aplikace může použít virtuální kanál a předat tak konkrétní informace. Virtuální kanály tím pomáhají přidat funkce, které ještě nejsou definovány v samotném protokolu RDP. Např. ve verzi RDP 5.2 se používaly virtuální kanály (v OS Windows) pro společnou schránku klienta a serveru nebo např. pro přesměrování tiskové úlohy.

Další schopností protokolu je tzv. zrcadlení, které se používá především u terminálových stanic komunikujících se serverovou verzí OS Windows. Zrcadlení se využívá pro odesílání dat více připojeným klientům.

Obrázek 3 zjednodušeně ukazuje způsob komunikace při spojení za pomoci RDP.



Obrázek 3 Integrace protokolu v systému OS Microsoft

2.2.2 Vlastnosti protokolu

- Podpora 32bitových barev

- 56bitové nebo 128bitové šifrování
- Podpora schránky
    - Uživatelé mohou mazat, kopírovat, vkládat text a grafiku mezi aplikací běžící na lokálním počítači a aplikací běžící v relaci vzdálené plochy.
- Přesměrování zvuku
    - Je možnost konfigurovat šířku pásma.
- Přesměrování portů COM
- Přesměrování tiskových úloh

2.3 Proprietární protokoly

V praktické části této práce jsou zmíněné aplikace, které nemají veřejně popsán princip či protokol, který používají pro vzdálené ovládání počítače. Dostupné informace způsobu jejich práce jsou shrnuty v této kapitole.

2.3.1 TeamViewer

TeamViewer nevyužívá výše zmíněných protokolů RFB nebo RDP určených pro vzdálenou správu a používá vlastní, veřejně nepopsaný protokol.

Komunikace v rámci TeamVieweru je plně šifrována s 1024bitovou veřejnou a neveřejnou výměnou klíčů založenou na RSA s 256bitovým šifrováním AES (podobně jako technologie HTTPS/SLL). K připojení je obvykle využito přímo TCP či UDP. Pokud nastane problém, je komunikace automaticky vedena za pomoci TCP nebo HTTP tunelování. Ke správné činnosti není nutná veřejná IP adresa i z důvodu, že spojení není přímo mezi dvěma počítači, ale probíhá za pomoci serverů TeamVieweru (dále jen TV).

Po spuštění programu je vygenerováno na základě HW stanice jedinečné ID. Poté je započato navazování komunikace se servery TV. Pokud navazování proběhlo úspěšně, jsou ze strany klienta na servery TV poslány přihlašovací údaje (jsou-li zadány), ID a nastavení

programu. Na základě těchto údajů jsou pak ze strany TV serverů poslány konfigurace jako VPN IP a další.

2.3.2 LogMeIn

Principiálně je komunikace LogMeIn podobná jako u TeamVieweru - server i klient komunikují mezi sebou za pomoci serverů společnosti.

Tato komunikace je provozována za pomoci protokolu SSL (celým názvem Secure Sockets Layer) nebo jeho následovníkem TLS (Transport Layer Security). Tyto protokoly mohou používat vícero druhů šifrování s metodami jako je RC4, 3DES či AES. Tím, které šifrování je zvoleno se tyto protokoly nezabývají, proto LogMeIn vybírá vždy tu nejlepší možnou metodu, kterou klient (myšleno software) nabízí. S těmito protokoly je možné se setkat napříč Internetem a využívají se často u webových aplikací bankovní sféry aj. Tyto protokoly zajišťují bezpečnou komunikaci pomocí šifrování a autentizace (dokonce lze využít i RSA Secur ID).

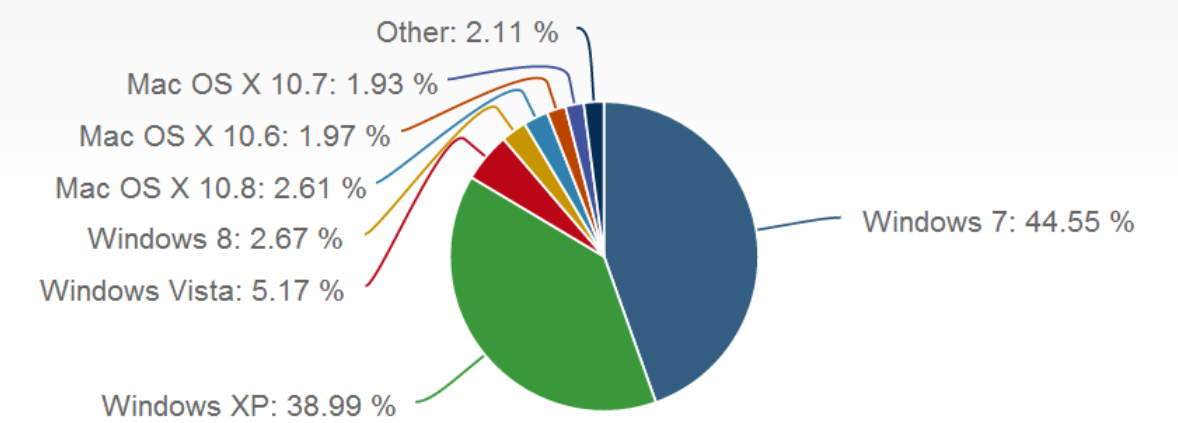
Při využívání SSL komunikace často není potřeba žádné speciální nastavení firewallu. I z tohoto důvodu je možné využívat LogMeIn s neveřejnou IP adresou.

3 VZDÁLENÁ PLOCHA POD OS MS WINDOWS

Microsoft se RD zabývá již dlouhou dobu. V serverových edicích se s RD objevuje již s příchodem Windows NT 4.0. V běžných edicích Windows se pak poprvé pod názvem Terminal Services nativně objevila tato možnost ve Windows 2000, pod názvem Vzdálená plocha se pak objevuje v první verzi Windows XP Professional a dále.

3.1 Edice MS Windows

Ke konci roku 2012 se v České republice dle dat z portálu Gemius Rankings stal MS Windows 7 nejpoužívanějším operačním systémem. Z celosvětového hlediska je dle serveru Netmarketshare.com ve vedení také MS Windows 7. Druhým nejpoužívanějším systémem je Windows XP. Následující koláčový graf (Obrázek 4) ze serveru Netmarketshare.com zobrazuje údaje k datu 30. 3. 2013 o četnosti desktopových operačních systémů.



Obrázek 4 Tržní podíl operačních systémů [3]

V praktické části se z hlediska operačních systémů společnosti Microsoft nalézá popis jak zprovoznit RD v edicích Windows XP a Windows 7. Popis, který je uveden u Windows 7 lze také aplikovat ve Windows Vista.

Vzdálená plocha je k dispozici ve všech edicích systému Windows 7, ale serverem může být pouze počítač s edicí Professional, Ultimate nebo Enterprise. Výjimku však tvoří RD při použití aplikace Vzdálená pomoc, kde může být serverem i stanice s nižšími edicemi Windows např. edice Home. Podobné to je u OS s Windows XP, kde serverem může být pouze edice Professional.

3.2 Jednouživatelský systém

Microsoft Windows je „jednouživatelským“ systémem. To v praxi znamená, že na jedné stanici nemůže pracovat více uživatelů zároveň. Výjimku tvoří serverové verze Windows, kde při vzdáleném připojení více uživatelů k jednomu serveru mohou uživatelé tento server používat zároveň. Toto je hlavní rozdíl mezi RD na serverových verzích Windows a osobních verzích Windows.

3.3 Připojení ke vzdálené ploše, Vzdálená pomoc

Často je možné ve spojitosti s Windows 7 zaměňovat nebo ztotožňovat pojmy *Připojení ke vzdálené ploše* a *Vzdálená pomoc*. Ač je možné se ke vzdálenému počítači připojit pomocí obou aplikací, tak se jejich účel použití mírně liší.

Připojení ke vzdálené ploše (někdy také Vzdálená plocha) respektuje Windows jako jednouživatelský systém (vyjímá serverových řešení a terminálových licencí). To v praxi znamená, že pokud se uživatel připojí na vzdálenou stanici, tak s ní nemůže nikdo jiný pracovat. Přímo na stanici se totiž zobrazí tzv. Logon Screen (obrazovka, na které se uživatelé běžně přihlašují). To umožňuje klientovi pracovat se vzdálenou stanicí stejně jako by u ní byl přímo přítomen. Pokud by se však chtěl někdo na vzdálené stanici přihlásit, je mu to umožněno. V tomto případě je spojení připojenému klientovi přerušeno se zprávou o přihlášení jiného uživatele.

Naopak u Vzdálené pomoci sdílí klient i server stejnou obrazovku. Pokud to uživatel na serveru umožní, může klient také ovládat server (zároveň se serverem). Zde už je mírně zavádějící pojem klient a server. Proto se zde často hovoří o uživateli, který pomoc nabízí a naopak o uživateli který pomoc vyžaduje. V systému XP se pak účastníci nazývají *Poradce* a *Začínající uživatel*. Při použití Vzdálené pomoci tedy mohou pracovat dva uživatelé zároveň, avšak s tím omezením, že si navzájem imponují s pohyby myší a psaním textu. Vzdálená pomoc nabízí také vestavěný chatovací nástroj.

Obě dvě řešení se liší ještě ve způsobech připojení a v několika nastaveních. Vzdálená pomoc například vyžaduje tzv. Pozvání. To znamená, že server (Začínající uživatel) musí poslat pozvání klientovi (Poradci). Obvyklým postupem je pozvání uložit do souboru a následně jej poslat pomocí emailu. Blíže jsou jednotlivé rozdíly patrné v praktické části při konfiguraci a použití těchto aplikací.

3.4 Připojení k aplikacím RemoteApp a vzdálené ploše

Připojení k aplikacím RemoteApp a vzdálené ploše je nástroj pro přístup především k programům na vzdálených nebo virtuálních počítačích. Tento nástroj může být nastaven pouze na serverových edicích Windows. Následně je možné na klientské straně pracovat s programy téměř, jako by byly instalované na dané stanici. Při korektním nastavení jsou na klientské straně ikony stejné jako na serveru a je možné aplikace spustit běžným dvojklikem a pracovat s nimi.

3.5 Windows Intune

Jedná se o službu nabízenou firmou Microsoft, která je kombinací cloudové[4] služby pro správu a dohled klientských počítačů. Je vhodná především pro větší firmy s mnoha stanicemi.

Windows Intune obsahuje mnoho funkcí, mezi nejvýznamnější pak kromě samotného RD patří antivirus a antimalware, distribuce software, reporting (informace o software a hardware klientských stanic), monitoring (sledování výskytu chyb). Všechny tyto služby pak lze spravovat pro jednotlivce i pro skupinu stanic.

Windows Intune je paušálně placená služba a je možné ji zdarma vyzkoušet na 30 dní na 25 stanicích. V současné době (květen 2013) stojí Windows Intune od 4,90 Eura na stanici měsíčně.

Službu je možné provozovat na Windows u edicí Windows XP Professional ServicePack 3, Windows Vista Business a vyšší či Windows 7 Professional a vyšší, Windows 8 Professional a Enterprise edice.

[4] Cloud nebo také Cloud Computing je sdílení softwarových a hardwarových prostředků za pomoci počítačové sítě.

4 VZDÁLENÁ PLOCHA POD OS LINUX

Linux již od svých začátků podporuje vzdálenou práci se systémem, na rozdíl od MS Windows. [4, s. 209] Velkou výhodu potom je, že Linux je více uživatelským systémem. To v praxi znamená možnost existence a práce více uživatelů na jedné stanici zároveň. V tomto případě může každý z uživatelů pracovat s vlastní „plochou“ a otevřenými aplikacemi (na rozdíl od běžných MS Windows). Tohoto faktu lze elegantně využít při vzdáleném ovládání počítače.

Ačkoli dnes již uživatelé Linuxových distribucí využívají zejména grafické prostředí, některé úkony je efektnější vykovávat v textovém režimu. Administrátoři tento režim často používají pro konfigurování serverů apod. Z dob, kdy ještě neexistovalo GUI (Graphical User Interface - Grafické uživatelské rozhraní) zůstala podpora textového vzdáleného ovládání běžné stanice dodnes. Výhodou této metody je i nízká síťová náročnost. Setkat se lze s aplikacemi jako Telnet, Kerberizovaný[5] Telnet, rlogin, rsb a oblíbeným SSH.

Ke grafickému vzdálenému připojení Linux využívá několik různých protokolů. V dnešní době je obvykle implementována aplikace typu VNC používající protokol RFB. Dále je možné se setkat s dnes již starším protokolem X (někdy nazýván X11), který byl optimalizován firmou NoMachine a pojmenován NX. Aplikace NX spojuje do hromady protokol X, SSH a přidává podporu zvuků, sdílení apod. přičemž si zachovává výhodu protokolu X, který je vhodný pro pomalé připojení.

V praktické části této bakalářské práce je popsáno a aplikováno spojení za pomoci SSH a VNC.

[5] Kerberos je síťový protokol sloužící k bezpečné autentizaci. Je specifikován v IETF RFC 1510 (později RFC 4120)

II. PRAKTICKÁ ČÁST

ÚVOD K PRAKTICKÉ ČÁSTI

Praktická část práce se zaměřuje na konkrétní programy a aplikace využívané pro vzdálené připojení či správu počítačů s ohledem na jejich použití pod různými operačními systémy. Jsou zde aplikovány programy nativně obsažené v MS Windows a Linux, které využívají protokol RDP resp. VNC, dále se zde nacházejí externí aplikace typu VNC, které využívají protokolu RFB, a je zde také kapitola věnující se použití speciálních programů, které používají své proprietární protokoly. Základní vlastnosti těchto řešení jsou shrnuty v *Tabulce 2*.

Další část se zaobírá měřením síťové a hardwarové zátěže. Závěr praktické části se věnuje řešení nejčastějších problémů spojených s RD. Je zde řešeno povolování portů, forwardování portů, a pro případy neveřejných IP adres je zde uvedena aplikace pro vytvoření virtuální privátní sítě.

5 MS WINDOWS

První tři možnosti se týkají nativních aplikací MS Windows. Jde konkrétně o Telnet, Připojení ke vzdálené ploše a Vzdálená pomoc.

5.1 Telnet

Telnet je stále ještě součástí Microsoft Windows a patří k prvním možnostem vzdáleného přístupu k počítači. V této kapitole je zmíněn postup, jak jej zprovoznit pod OS Microsoft Windows 7. Tento postup lze aplikovat také pod Microsoft Windows Vista.

5.1.1 Nastavení serveru

Nejprve je nutné povolit službu Telnet Server, která je standardně zakázána.

1. Klikněte na tlačítko „Start“, nebo stiskněte klávesu Windows.
2. Klikněte na položku „Ovládací panely“.
3. Klikněte na položku „Programy“.
4. Klikněte na položku „Zapnout nebo vypnout funkce systému Windows“. Systém Vás může vyzvat k zadání nebo potvrzení hesla správce, tudíž zadejte heslo nebo proveďte potvrzení.
5. V dialogovém okně „Funkce systému Windows“ zaškrtněte políčko „Server Telnet“.
6. Potvrďte tlačítkem „OK“.

Nastavení upřesňující spouštění Telnet Serveru může být nakonfigurováno jako *automatické, ruční* nebo *zakázáno*. Ve výchozím stavu je *zakázáno*, proto je nutné jej povolit a spustit dle následujícího postupu.

1. Stiskněte klávesy Windows + R, nebo klidněte na „Start“ a následně na „Spustit“.
2. Do textového pole zadejte *„services.msc*“ (bez uvozovek) a potvrďte kliknutím na tlačítko „OK“.
3. Nyní se nacházíte v okně Řízení uživatelských účtů. Pokud se zobrazí hláška, zda chcete provést zobrazovanou akci, tak ji potvrďte.
4. Pravým tlačítkem myši klikněte na položku „Telnet“ a levým klikněte na „Vlastnosti“.

5. V seznamu „Typ spouštění“ vyberte jednu z následujících položek:
   a. „Automatické“ – služba Server Telnet bude automaticky spuštěna při startu systému Windows.
   b. „Ruční“ – umožní spuštění a zastavení služby Server Telnet ručně dle potřeby.
   c. „Zakázáno“ – v tomto případě nelze službu Server Telnet spustit.
6. „Stav služby“, tedy „zapnuto“, „zastaveno“, „pozastaveno“ můžete měnit v tomtéž okně. Nyní tedy službu spusťte kliknutím na tlačítko „Spustit“.

Posledním nutným krokem nastavení serveru je povolení určité skupině uživatelů nebo jednotlivým uživatelům použití služby Telnet. V tomto případě nestačí znát pouze uživatele, kteří se přihlašují na stanici, ale je nutné je přiřadit této službě, resp. povolit jim vzdálené přihlašování. Tento krok se skládá ze dvou částí. Samotného vytvoření místní skupiny *TelnetClients* a přiřazením uživatelů do této skupiny.

1. Stiskněte klávesy Windows + R, nebo klidněte na Start a následně na „Spustit“.
2. Do textového pole zadejte *„mmc lusrmgr.msc*“ (bez uvozovek včetně mezery) a potvrďte kliknutím na tlačítko „OK“.
3. V navigačním podokně klikněte na položku „Skupiny“
4. Zkontrolujte, zda skupina „TelnetClients“ v podokně podrobností již existuje. Pokud ano, pokračujte krokem číslo 6.
5. Klikněte pravým tlačítkem myši na položku „Skupiny“ a následně klikněte na příkaz „Nová skupina“.
6. V dialogovém okně Nová skupina je nutné zadat název „TelnetClients“ a je možné přidat i popis.
7. Klikněte na položku „Přidat“ (vlevo dole) a přihlašovací jména uživatelů, které chcete použít, zadejte do dialogového okna. Můžete zde také zvolit ručně uživatele počítače nebo skupiny.

Nyní je služba Telnet Server spuštěna a připravena k použití.

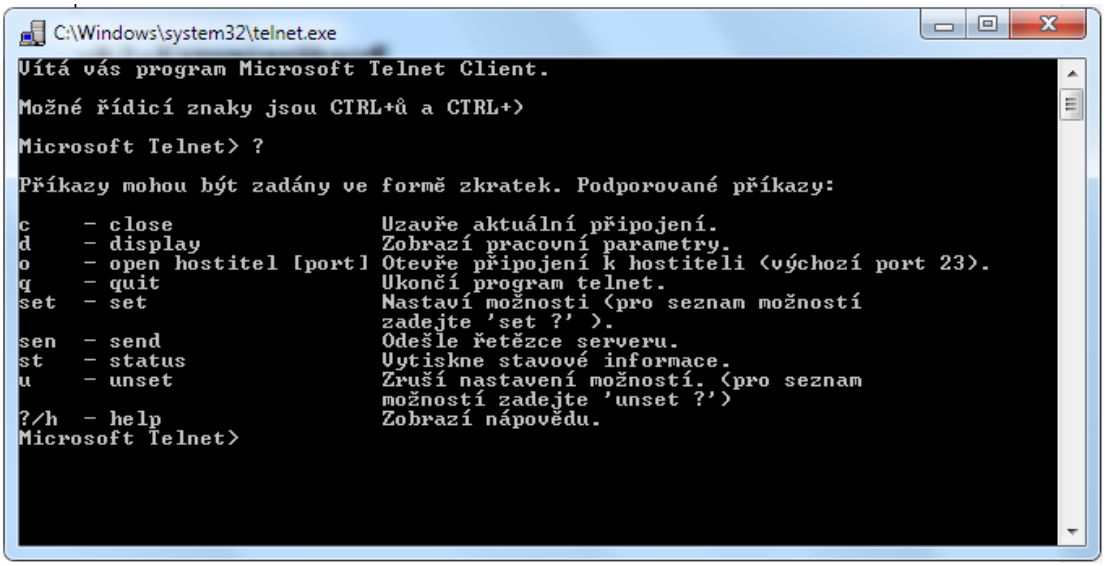
5.1.2 Klient

Zpravidla je klient Telnetu *vypnutý* a *zakázaný* stejně jako v případě serveru Telnetu, proto je nutné jej nejprve povolit. Postup je analogický k výše uvedené serverové části.

1. Klikněte na tlačítko „Start“, nebo stlačte klávesu Windows, klikněte na položku „Ovládací panely“, následně na „Programy“ a potom na „Zapnout nebo vypnout funkce systému Windows“. Systém Vás může vyzvat k zadání nebo potvrzení hesla správce, proto zadejte heslo nebo proveďte potvrzení.
2. V dialogovém okně „Funkce systému Windows“ zaškrtněte políčko „Klient služby Telnet“.
3. Potvrďte tlačítkem „OK“.

Následuje postup, jak spustit klienta a připojit se.

1. Stiskněte klávesy Windows + R, nebo klikněte na „Start“ a následně na „Spustit“
2. Do textového pole zadejte *„telnet*“ (bez uvozovek) a potvrďte kliknutím na tlačítko „OK“.
3. Objeví se okno s textovým režimem, ve kterém si můžete zobrazit nápovědu vepsáním otazníku a následným stiskem klávesy Enter. Poté by se vám mělo zobrazit okno jako na *Obrázku 5*.



Obrázek 5 Okno klienta Telnet s vypsanou nápovědou

4. Pro připojení k hostiteli (serveru) zadejte písmeno „*o*“, následně mezeru a za ní IP adresu serveru (např. o 192.168.1.100).
5. Pokud navázání spojení proběhlo úspěšně, tak se obvykle objeví hláška s upozorněním, že odesílání hesla přes Internet nemusí být bezpečné. Stiskněte klávesu Y a potvrďte klávesou Enter (je vhodné mít přepnutu klávesnici na anglickou; učiníte tak stiskem kombinace kláves *alt* + *shift*).
6. Posledním krokem je zadání uživatelského jména (login) a hesla. Pozor, z bezpečnostních důvodů se heslo při psaní nezobrazuje.

5.2 Vzdálená plocha Windows 7

Na Internetu je možné se dočíst, že *Připojení ke vzdálené ploše* v produktech od společnosti Microsoft slouží pouze pro připojení v místní sítí (LAN), ale není tomu tak. Avšak pro připojení k počítači z jiné sítě (myšleno ne LAN sítě) skrze Internet je nutná veřejná IP adresa, případně správně nastavené (naforwardováné) porty směrovače (routeru).

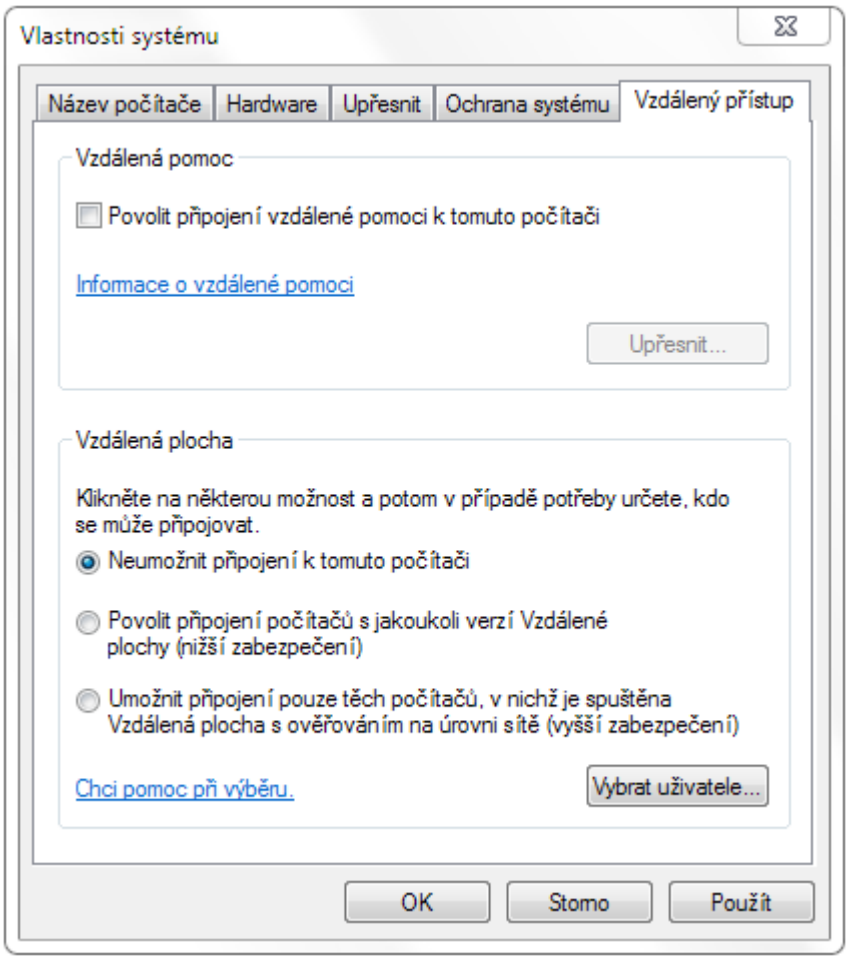
5.2.1 Nastavení serveru

Zpravidla je *Vzdálená plocha* i *Vzdálena pomoc* na počítači vypnuta (viz *Obrázek 6).* Spustit ji lze dle následujícího postupu. Nejdříve je však nutné zkontrolovat, zda používaný systém Windows 7 je z edic Professional, Enterprise nebo Ultimate. Jak již bylo uvedeno v teoretické části, pouze tyto edice umožní býti serverem pro Vzdálenou plochu. Pokud chcete zjistit, kterou edici systému Windows 7 používáte, klikněte na tlačítko „Start“, následně klikněte pravým tlačítkem na možnost „Počítač“ a poté klikněte na příkaz „Vlastnosti“. Nyní samotné spuštění Vzdálené plochy:

1. Klikněte na tlačítko „Start“.
2. Klikněte pravým tlačítkem myši na položku „Počítač“ a pokračujte kliknutím na tlačítko „Vlastnosti“.
3. V nově otevřeném okně „Systém“ pokračujte kliknutím v levém panelu na „Upřesnit nastavení systému“.
4. V okně Vlastnosti systému klikněte na záložku „Vzdálený přístup“ (viz *Obrázek 6).*

5. Zde zvolte jednu z možností dle toho, z jakého systému budete přistupovat na tuto stanici. Pokud se jedná o edice Windows Vista, 7 či 8, vyberte poslední možnost s vyšším zabezpečením. V opačném případě pak zvolte možnost druhou, tedy s nižším zabezpečením.

Nyní již zbývá nastavit uživatele, kteří mají oprávnění tuto stanici (server) využívat. Administrátor má toto oprávnění defaultně. Pro přidání dalších uživatelů klepněte na tlačítko „Vybrat uživatele“.

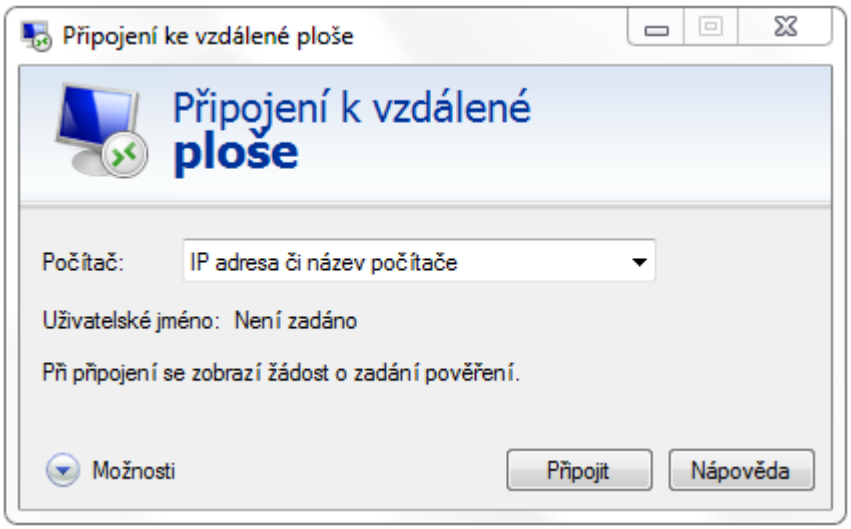


Obrázek 6 Povolení Vzdálené pomoci a Vzdálené plochy

5.2.2 Klient

1. Stiskněte klávesy Windows + R nebo klidněte na Start a následně na „*Spustit*“.
2. Vepište „*mstsc*“ (bez uvozovek) a potvrďte stisknutím enteru nebo kliknutím na tlačítko OK.

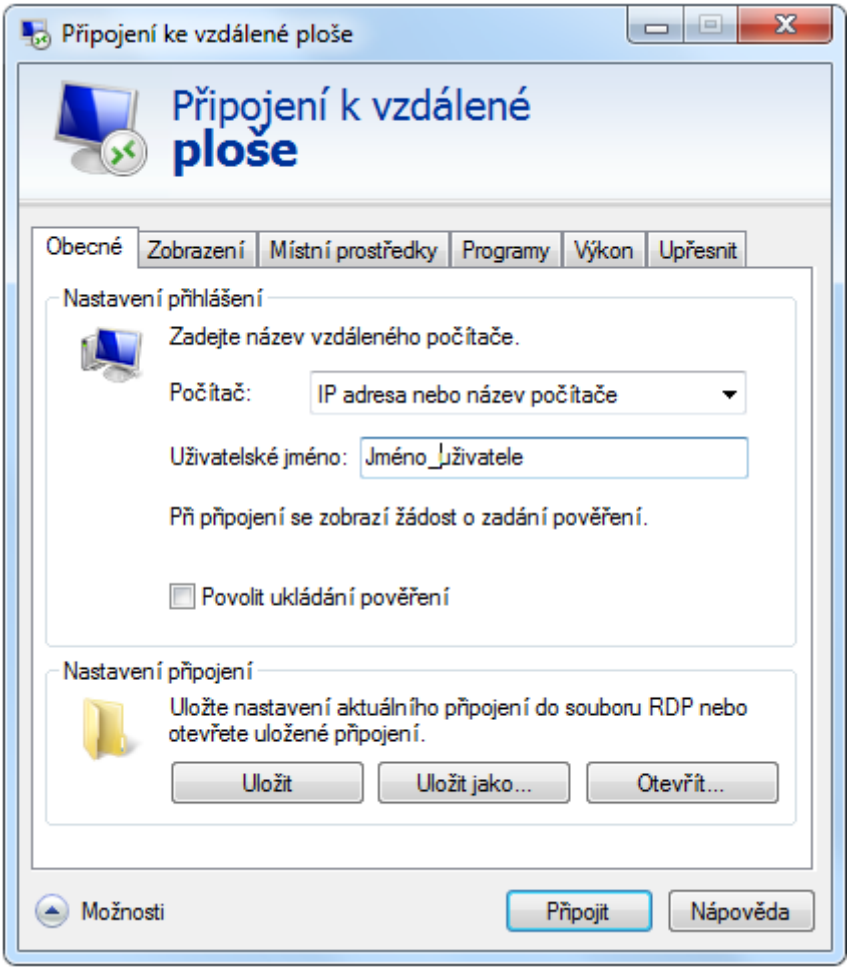
Objeví se okno (viz Obrázek 7), ve kterém zadáte do položky Počítač IP adresu či název počítače. Poté stačí kliknout pouze na tlačítko Připojit.



Obrázek 7 Připojení ke vzdálené ploše – klient

Je možné rozbalit nabídku Možnosti umístěnou vlevo dole (viz *Obrázek 7*) a získat tak rozšířené nastavení (viz *Obrázek 8*). Mezi nejpodstatnější volby zde patří volba uživatelského jména, ke kterému se na vzdálené stanici tento klient připojuje. Lze takto nastavit uživatele i s heslem – poté se klient automaticky na vzdálené stanici přihlásí. Toto nastavení lze také uložit do souboru a připojovat se pouze spuštěním daného souboru. Další možnosti se týkají hlavně kvality přenosu, resp. velikosti okna, zobrazování vizuálních prvků apod. Tato nastavení pak ovlivňují využívanou šířku pásma a je možné s jejich pomocí zajistit lepší běh aplikace při pomalejším připojení.

Jedním z významných nastavení je služba *Brána vzdálené plochy*. Ta umožňuje se připojit do lokální sítě (např. firemní), aniž by bylo nutné využití VPN. Bohužel je nutný alespoň jeden běžící server a to s edicí Windows Server 2008 a novější. Pokud tento server v lokální síti není, obvykle se pak k stanicím nelze připojit.



Obrázek 8 Rozšířené nastavení u klienta Připojení ke vzdálené ploše

5.3 Vzdálená pomoc Windows 7

Nespornou výhodou této aplikace oproti Vzdálené ploše je, že serverem může být počítač s jakoukoli edicí Windows 7. Bohužel stejně jako Připojení ke vzdálené ploše ani Vzdálená pomoc nelze bez VPN nebo příslušného nastavení směrovačů (routerů) použít v lokálních sítích (LAN) při přistupování z Internetu.

Vzdálenou pomoc lze využít také pro prezentaci či kooperativní ovládání počítače. Obsahuje také vestavěný chatovací nástroj. To vše hlavně proto, aby se usnadnilo zkušenějšímu uživateli pomoci méně zkušenému uživateli.

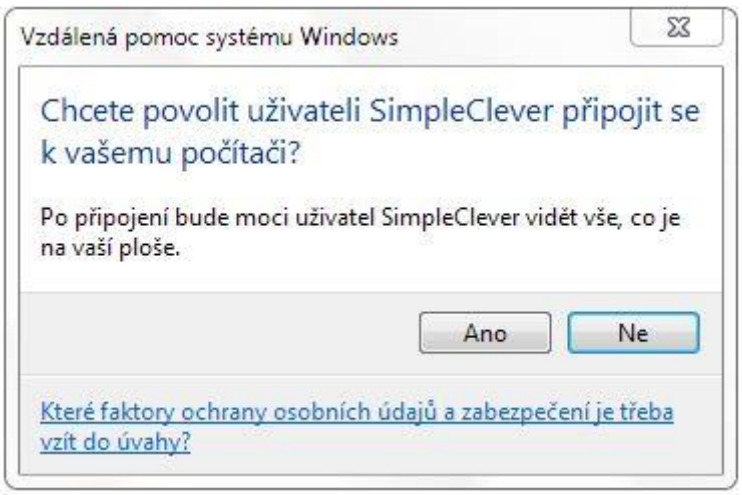
5.3.1 Nastavení serveru

Zde je třeba aplikovat stejný postup, jako v případě Připojení ke vzdálené ploše (viz *5.2.1 Nastavení serveru)*. Samozřejmě pak v okně, (viz *Obrázek 6)* je nutno zaškrtnout příslušné políčko s názvem „Povolit připojení vzdálené pomoci k tomuto počítači."

Nyní zbývá vytvořit tzv. pozvání pro klienta (zkušenějšího uživatele – dále jen klient).

1. Klikněte na tlačítko „Start".
2. Napište „*Vzdálená pomoc*" a následně klikněte na „Vzdálená pomoc systémů Windows".
3. Zde vyberete první možnost, tedy „Požádat jiného uživatele o pomoc".
4. Nyní lze zvolit jednu z možností jak pozvat klienta. Praktické je poslat pozvánku emailem (tedy druhá možnost), případně zvolit první možnost, kde je možné uložit pozvánku a předat ji libovolným způsobem. Poslední možností je tzv. Snadné připojení, které lze také vybrat pro systémy Windows 7 a vyšší.
5. Spolu s předanou pozvánkou je nutné klientovi sdělit i heslo, které se automaticky vygeneruje.

Až se bude chtít klient připojit, objeví se na serverové straně potvrzení (viz *Obrázek 9 Potvrzení přístupu při užití Vzdálené pomoci)*.



Obrázek 9 Potvrzení přístupu při užití Vzdálené pomoci

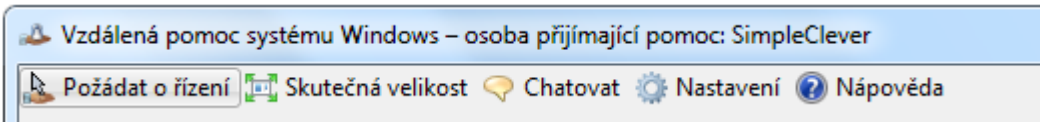
V případě jiných verzí Windows je nastavení obdobné. Menší rozdíl je u verze XP, kde cesta k průvodci vytvoření pozvání, resp. pozvánky, je následující.

1. Klikněte na tlačítko „Start“.
2. Klikněte na „Všechny programy“.
3. Poté klikněte na „Vzdálená pomoc“.

Ještě je třeba mít na paměti, že v případě Windows XP nelze připojení pozastavit. Mohou s tím být spojené problémy, pokud se připojujete na tento operační systém z novějších edicí Windows (Vista atd.).

5.3.2 Klient

Klient pro připojení musí otevřít pozvánku získanou od serveru a zadat heslo. Pokud server potvrdí připojení, tak je spojení navázáno. V tuto chvíli může klient pouze sledovat server a radit mu pomocí vestavěného chatovacího nástroje. V případě, že chce server i ovládat, musí o to požádat, a to položkou v levém horním rohu okna s názvem *Požádat o řízení* (viz *Obrázek 10*).



Obrázek 10 Vzdálená pomoc – pohled zkušenějšího uživatele (klienta)

V případě, že server odsouhlasí požadavek na řízení, může klient ovládat danou stanici.

6 LINUX

Jako zástupce linuxových distribucí byla zvolena distribuce Ubuntu 13.04, která byla vydána v dubnu roku 2013. Ubuntu je založeno na Debian GNU/Linux a využívá desktopové prostředí Gnome.

Od verze 12.10 nabízí Ubuntu také možnost vzdáleného přihlášení přímo z přihlašovací obrazovky. Jedná se o užitečnou novinku. Nejprve je nutné se zaregistrovat na webových stránkách a poté asociovat s účtem stanice. Následně se lze ke svému účtu přihlásit na přihlašovací obrazovce (tzv. LogonScreen). Připojit se je možné napříč platformami Unixových, Windows i Mac operačních systémů.

V praktické části této kapitoly bude zmíněno nastavení SSH spojení pro textový přístup ke stanici a sofistikovaná aplikace Remmina, která je nativně obsažena v distribuci.

6.1 SSH

V této kapitole je uvedeno, jak se lze za pomocí šifrovaného kanálu vytvořeného pomocí SSH připojit ke stanici.

6.1.1 Nastavení serveru (OpenSSH)

Nejprve je nutné doinstalovat OpenSSH – server. To lze udělat např. pomocí terminálu a příkazu *sudo apt-get install ssh* nebo v dnešní době již pomocí grafické distribuce balíčků.

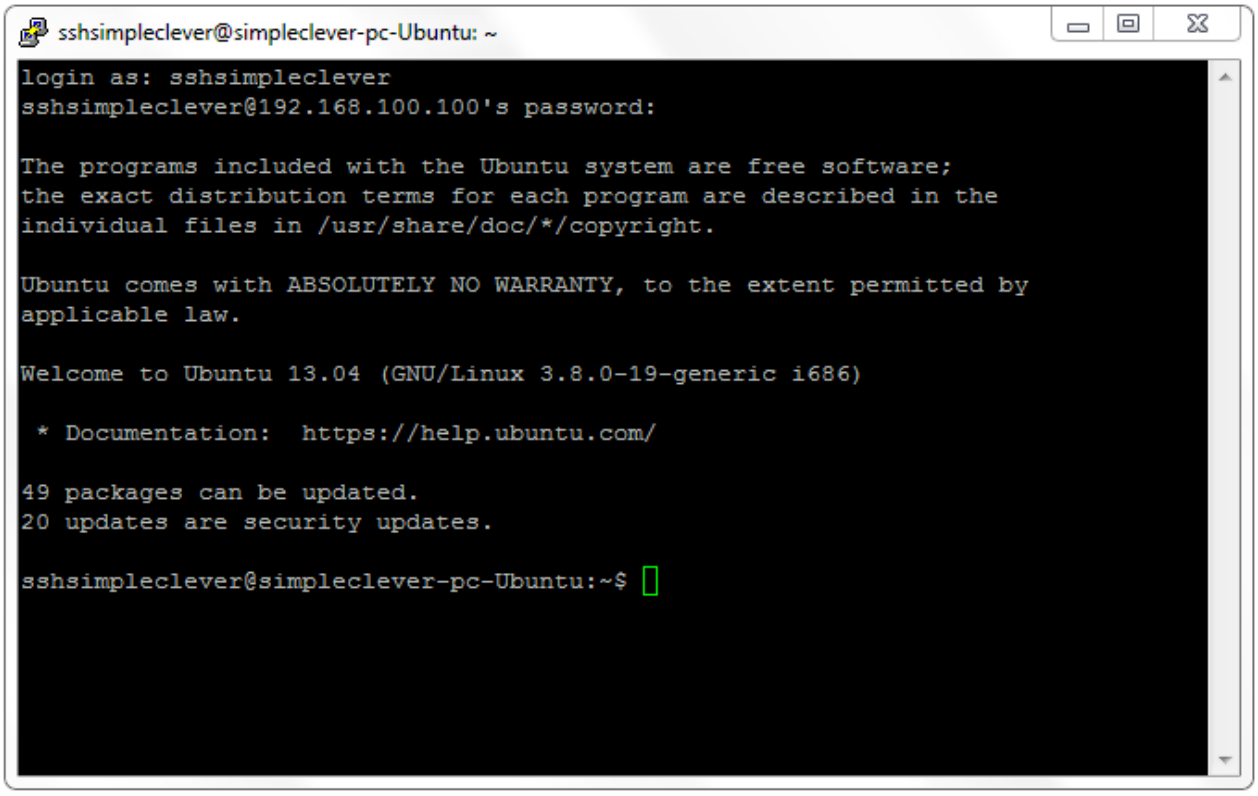
1. Otevřete „Centrum softwaru pro Ubuntu“.
2. Do vyhledávání zadejte: „*openss-server*“.
3. Poté otevřete nalezenou položku a nechte ji nainstalovat.

Nyní je již možné se za pomocí šifrovaného kanálu připojit k této stanici.

6.1.2 Připojení

K připojení je možné využít terminálu nebo v teoretické části zmíněného programu Putty, který se nemusí instalovat. K připojení stačí Putty pouze spustit a zadat IP adresu nebo jméno počítače (ve výchozím nastavení je připraven na spojení za pomoci ssh verze 2) stejně jako je zobrazeno na *Obrázku 2*. Následně je nutné kliknout na „Open“.

V případě úspěšného spojení je nyní nutné zadat jméno uživatele. Na *Obrázku 11* je uvedeno jméno *sshsimpleclever*. Následně je vznesen dotaz na heslo. Při zadávání hesla se nezobrazují hvězdičky ani jiné znaky – vypadá to jako by se nevpisoval text, ale opak je pravdou. Po stisknutí klávesy Enter při správně zadaných přihlašovacích údajích je možné vzdálenou stanici ovládat.



Obrázek 11 Připojení přes SSH z Windows do distribuce Ubuntu

6.2 Nastavení vzdáleného přístupu

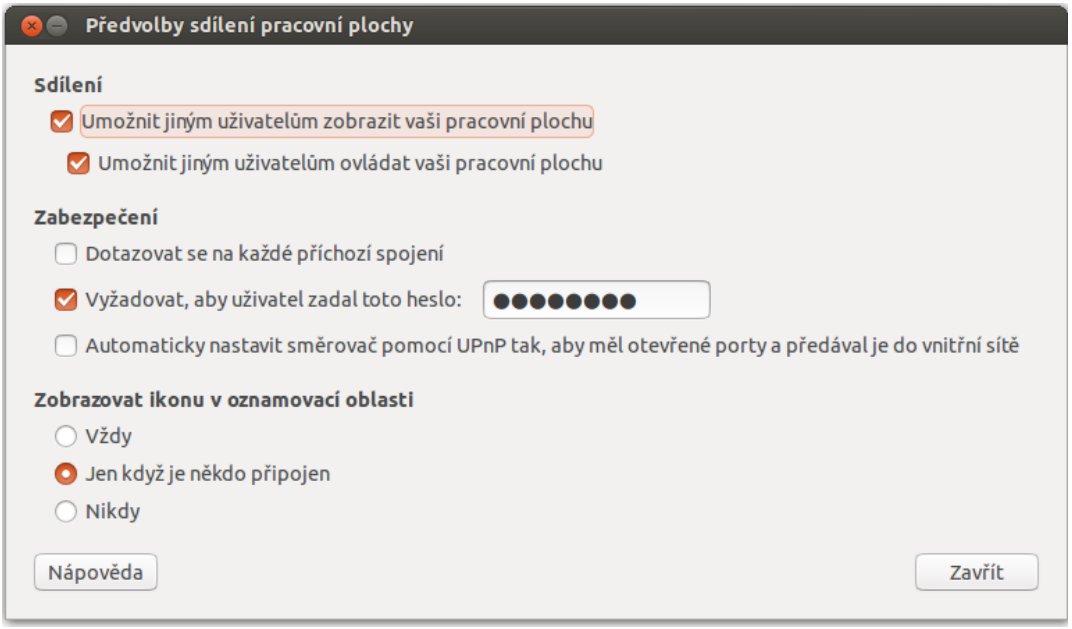
Ubuntu obsahuje nástroj *Sdílení pracovní plochy*, který lze vyvolat následujícím postupem.

1. Klikněte na „Systém“.
2. Poté na „Volby“.
3. Následně na „Vzdálená pracovní plocha“.

Případně vyvolejte hlavní nabídku a do ní vepište „*Vzdálená pracovní plocha*“.

Objeví se okno (viz *Obrázek 12*), ve kterém je možné povolit sledování, případně řízení této stanice. Ubuntu v tomto případě nastavuje VNC server, proto se lze připojit pomocí

VNC klientů z různých OS a to i mobilních. Pozornost je nutné věnovat komunikaci, která je v tom případě nešifrovaná. Zabezpečit lze pouze vstup neboli autentizaci a to pomocí maximálně osmi znaků. Pokud se chce uživatel k této stanici připojovat bez potvrzení, je nutné odznačit položku „Dotazovat se na každé příchozí spojení“, tak jako je to vyobrazeno na *Obrázku 12*. Pro lepší konfiguraci směrovače (routeru) v rámci připojení v místní síti je vhodné zvolit možnost Atomického nastavení směrovače pomocí UPnP.



Obrázek 12 Nastavení přístupu k Ubuntu (Sdílení pracovní plochy)

6.3 Remmina

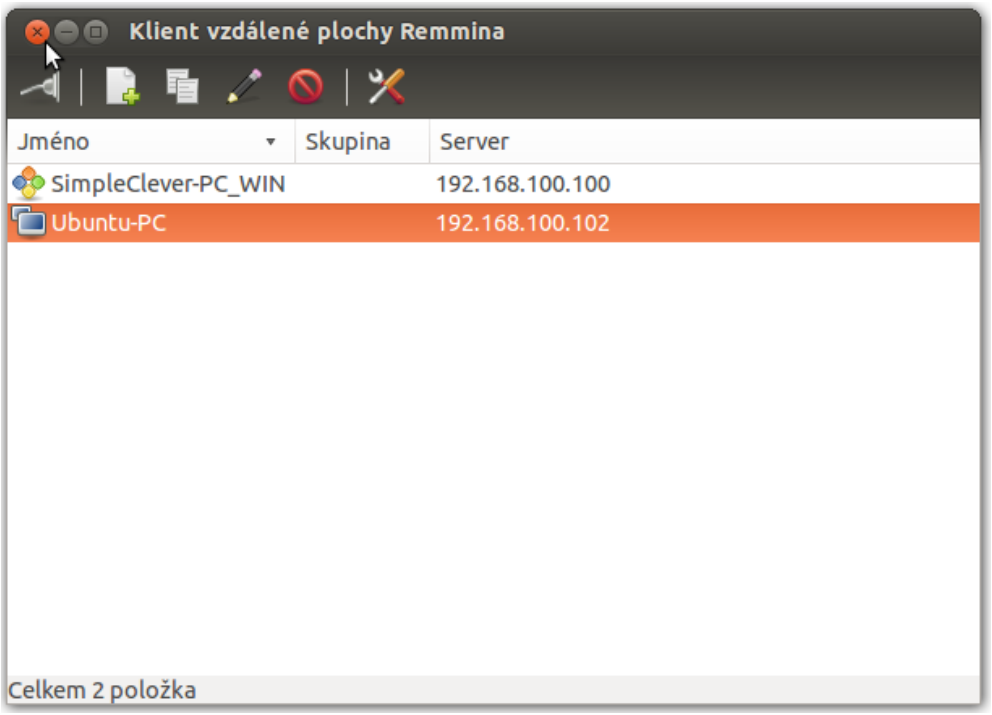
Remmina je aplikace sloužící pro vzdálený přístup, která nahrazuje Vinagre a rdesktop a je obsažená v Ubuntu. Zvládá nejen přihlášení k jiné distribuci Linuxu nebo jinému „okennímu“ systému za pomoci VNC, ale také celou řadu protokolů včetně RDP pro připojení k Windows a dále pak SSH, NX, XDMCP a SFTP.

6.3.1 Nastavení serveru

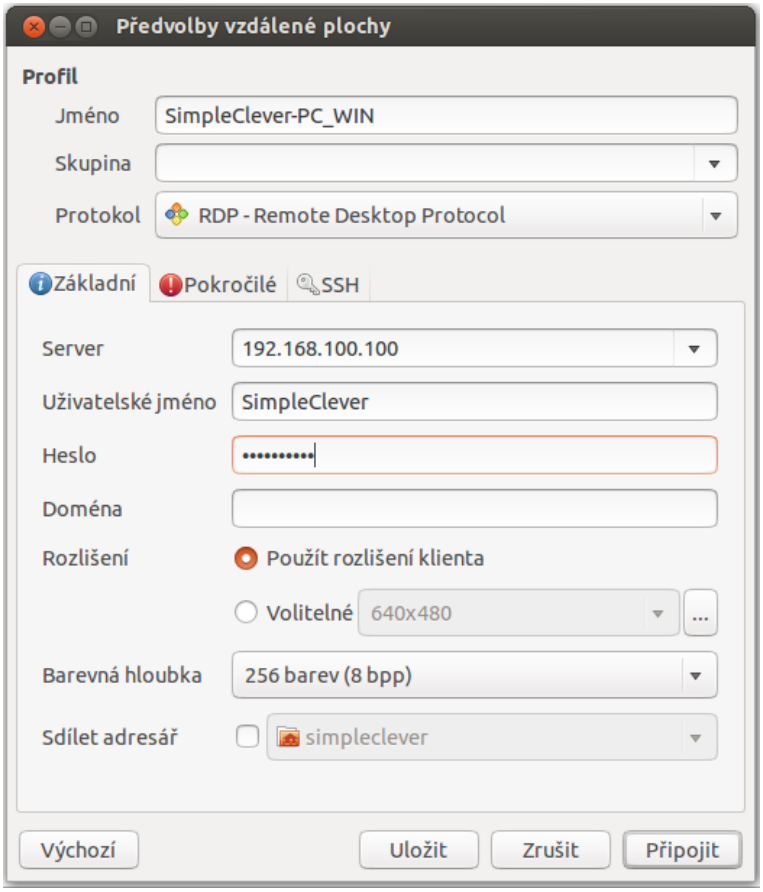
Aplikaci je možné nastavit také pro příchozí spojení a to i pro šifrovaná spojení, avšak hlavním účelem je připojení k jiným aplikacím na vzdálených stanicích.

6.3.2 Klient

Po spuštění aplikace se objeví okno (viz *Obrázek 13*), které zobrazuje uložené konfigurace pro připojení ke vzdáleným počítačům. Po kliknutí na druhou ikonu zleva s názvem „Vytvořit nový RD soubor“ se objeví další okno s názvem „Předvolby vzdálené plochy“ jako na *Obrázku 14*. Zde je možné nakonfigurovat nové připojení k vzdálené stanici. Podstatnou položkou je třetí vysouvací nabídka, kde se volí používaný protokol (RDP, VNC apod.). V záložce obecné je potom nejdůležitější položkou adresa spolu s případnými přihlašovacími údaji (pro RDP). V ostatních záložkách lze nastavit např. kvalitu (záložka Pokročilé), případně SSH tunel v záložce SSH. Kvalitu je možné upravovat i v hlavním okně po kliknutí na poslední ikonu (překřížený šroubovák s šestihranným klíčem).



Obrázek 13 Seznam nastavených připojení Remmina



Obrázek 14 Konfigurace nového připojení Remmina

7 MULTIPLATFORMNÍ ŘEŠENÍ

7.1 TEAMVIEWER 8

TeamViewer je dnes jedním z mnoha programů pro vzdálený přístup. Od svých konkurentů se odlišuje v nabízených službách. Mimo RD nabízí také tzv. prezentační mód, ve kterém umožňuje více uživatelům vidět obrazovku jednoho PC, dále nabízí vestavěný software pro přenos souboru, možnost VPN, vzdálený tisk, vzdálené audio, video a mnoho dalšího. Nejvýznamnější předností však je, že program pro svou práci nevyžaduje veřejnou IP adresu.

Program je pro nekomerční (domácí) použití zdarma. Pokud je používán v komerční sféře, platí se za něj jednorázový poplatek s ohledem na množství spravovaných stanic. Cena nejlevnějšího balíčku je 11739,- Kč (květen 2013).

TeamViewer pracuje na platformách Microsoft Windows, Mac OS X, Linux, iOS a Android. V linuxových distribucích pro svůj běh používá software Wine. Ten umožňuje běh aplikací určených pro Microsoft Windows pod Linuxem. Na stránkách http://appdb.winehq.org/ lze potom nalézt hodnocení kompatibility daného softwaru. TeamViewer je od verze 8.0x hodnocený zlatou medailí – tedy plně stabilní.

7.1.1 Instalace

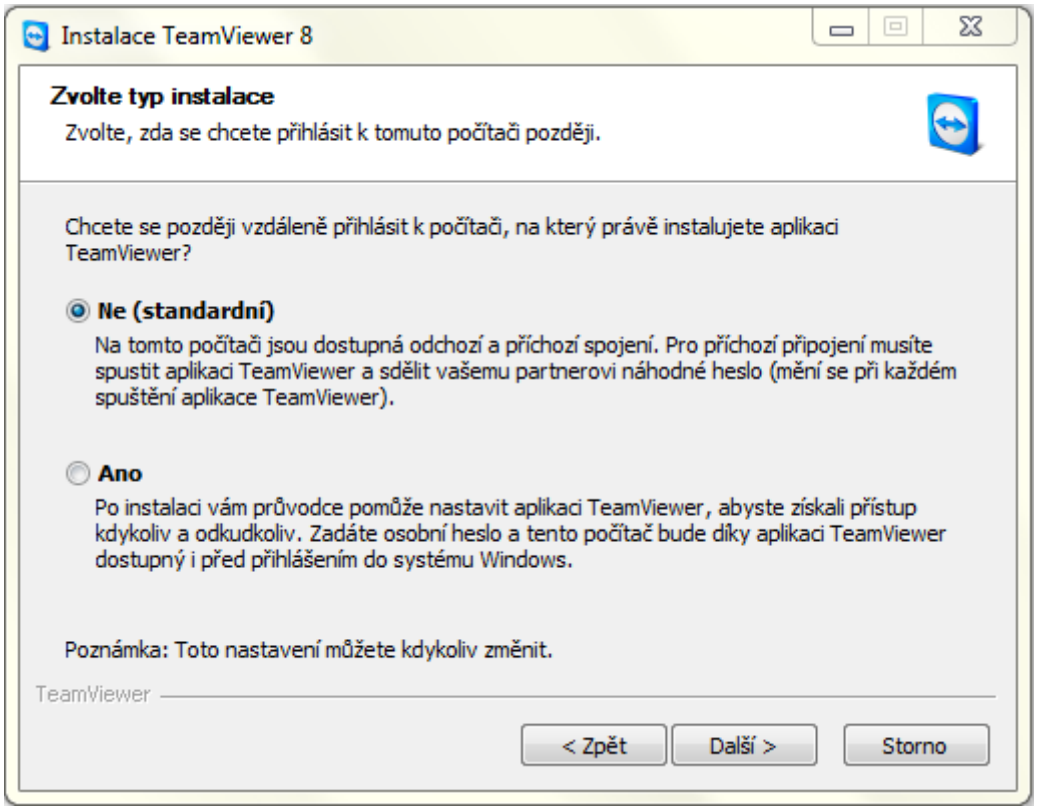
TeamViewer existuje v několika možných variantách a to dokonce i bez nutnosti instalace na stráně zákazníka (serveru). Lze nalézt i verzi *portable* nebo tzv. verzi *QuickSupport* (tedy Rychlá podpora).

QuickSupport slouží pro rychlou pomoc uživateli na vzdálené stanici (viz *Obrázek 15). Okno aplikace QuickSupport programu TeamViewer* Po stažení aplikace (http://download.teamviewer.com/download/TeamViewerQS_cs.exe) stačí soubor jen spustit a sdělit straně, která nabízí pomoc ID a heslo. QuickSupport nemá téměř žádné nastavení, slouží pouze jako aplikace umožňující přístup ke stanici, na které je spuštěna.

Obrázek 15 Okno aplikace QuickSupport programu TeamViewer

Naopak u verze *Portable*, která se také neinstaluje, lze nalézt veškeré možnosti aplikace (myšleno těch pro nekomerční využití). Hlavní okno aplikace ve verzi *Portable* je shodné jako okno v plnohodnotné verzi nazývané *Vše v jednom*.

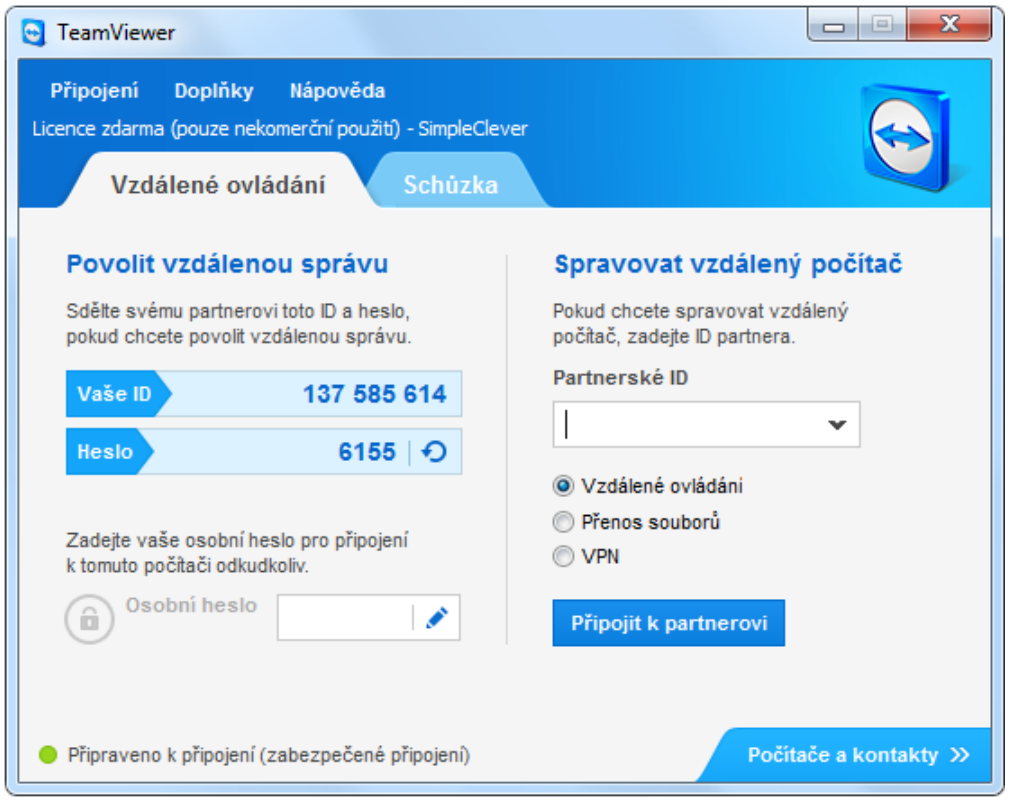
Při instalaci verze *Vše v jednom* lze nastavit, zda se má TeamViewer pouštět automaticky jako služba, nebo zda se má nainstalovat „normální“ verze (viz *Obrázek 16)*. Volba automatického spuštění je vhodná, pokud uživatel chce se ke stanici přihlásit, aniž by někdo musel na stanici spustit program TeamViewer – pouze stačí, aby stanice byla zapnutá. V tomto případě nemusí být uživatel v rámci MS Windows ani přihlášen a lze se (např. po restartu) přihlásit ke stanici přímo do obrazovky LogonScreen.



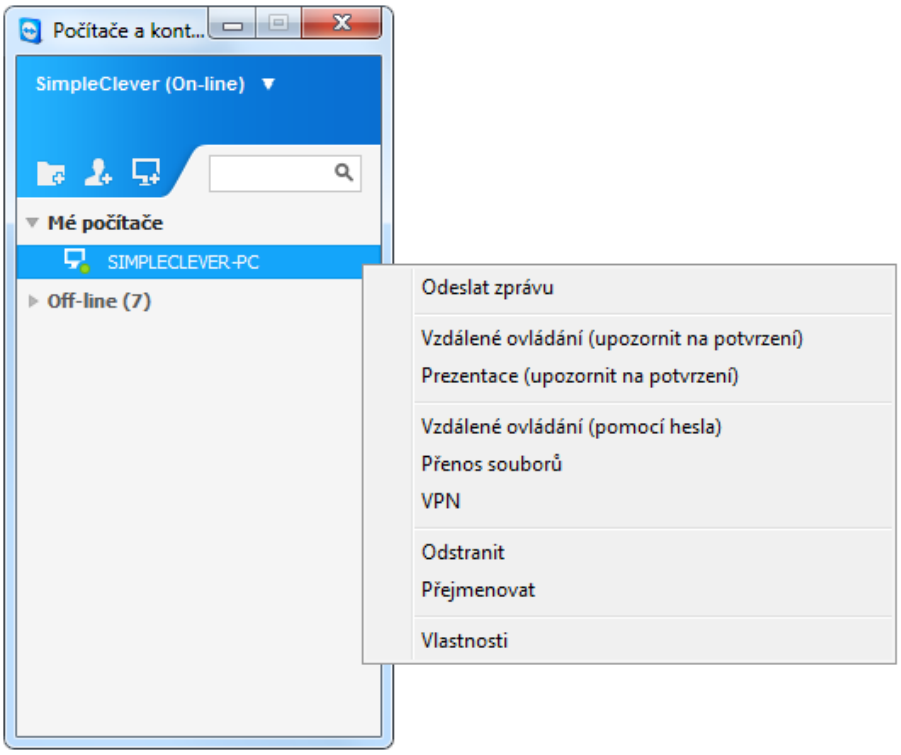
Obrázek 16 Instalace TeamViewer – volba dostupnosti serveru

7.1.2 Připojení

Jak již bylo zmíněno v teoretické části, TeamViewer generuje ID a Heslo. To je nutné předat klientské straně. Hlavní okno programu, kde je možné zjistit tyto údaje nebo kde je možné zadat tyto údaje pro připojení k partnerovi, je na *Obrázku 17*. Na levé straně se zobrazují údaje dané stanice a na pravé straně je možné vložit ID vzdálené stanice. Dále je zde volba, zda danou stanici chce klient ovládat nebo s ní přenášet soubory. Také je zde možné vytvořit VPN.

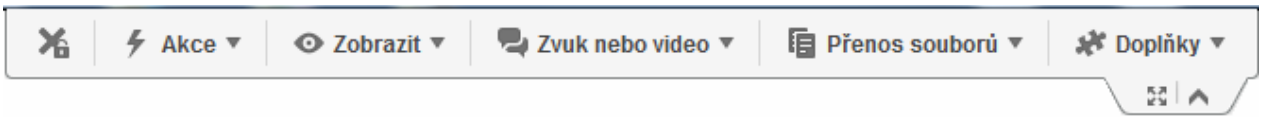


Obrázek 17 Okno aplikace TeamViewer



Obrázek 18 Možnosti nabízející TeamViewer

Pokud si uživatel vytvoří účet, může mít uložené vzdálené stanice i s hesly. Vždy lze vidět, zda je daná stanice zapnutá a připojená k internetu (viz *Obrázek 18)*. Pokud ano, může s touto stanicí navázat spojení. Na vzdálených stanicích je zpravidla TeamViewer nainstalován tak, aby se spouštěl sám po startu počítače.



Obrázek 19 TeamViewer panel možností při vzdáleném ovládání

Pomocí panelů možností při vzdáleném ovládání (*Obrázek 19*) lze vzdálenou stanici restartovat, restartovat do nouzového režimu, spustit chat, hovor, přenos souborů apod.

7.1.3 Shrnutí a další možnosti

Ve výchozím stavu je kvalita obrazu automaticky upravována. Přenos zvuku je také zapnutý. Upravovat tyto parametry lze před připojením v nabídce „Doplňky“ -> „Možnosti“ -> „Vzdálené ovládání“ nebo přímo za běhu v nabídce zobrazené na zobrazené na *Obrázku 19*. Lze zvolit nastavení automatické, pro rychlost, pro kvalitu nebo vlastní. U přenosu zvuků pak lze pouze tuto funkci zapnout nebo vypnout.

Jak již bylo zmíněno výše, TeamViewer je velmi sofistikovaný program, který nabízí více možností než jen vzdálené ovládání počítače. Může být použít pro konference, vytvoření VPN, přenášení souborů, komunikaci a mnoho dalších činností.

Mezi základní vlastnosti pak patří podpora zvuku, podpora schránky, šifrovaný přenos, přenos souborů, sdílení desktopu (prezentace), vzdálený tisk, vestavěný chatovací nástroj a další. Velkou výhodou je, že program nepotřebuje veřejnou IP adresu.

TeamViewer využívá vlastní (proprietární) protokol, šifrování AES a je možné jej nainstalovat na MS Windows, Mac nebo Linux, kde poběží za pomoci aplikace Wine. Z mobilních platforem je možné využít Andorid a iOS.

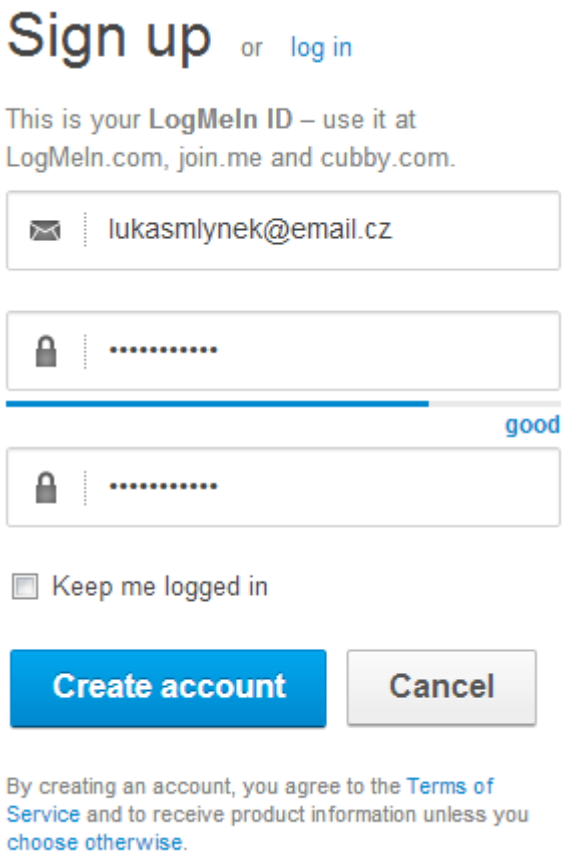
TeamViewer je zdarma pro nekomerční využití, pro komerční účely pak cena začíná na 11.739,-Kč za licenci na neomezenou dobu. (květnu 2013)

7.2 LogMeIn aneb vzdálená plocha přes webové rozhraní

Aplikace LogMeIn je známá především z pohledu své klientské části. Klientská část není program, který lze stáhnout, ale rozsáhlá webová aplikace. Pomocí ní lze přehledně spravovat velké množství stanic a jejich nastavení.

7.2.1 Instalace

Aby bylo možné program stáhnout (z oficiálních webových stránek), je nutné se nejprve zaregistrovat a vytvořit si tak ID. Tento úkon je velmi jednoduchý, stačí pouze vyplnit email a heslo jako na *Obrázku 20*.



Obrázek 20 Vytvoření účtu ID u LogMeIn

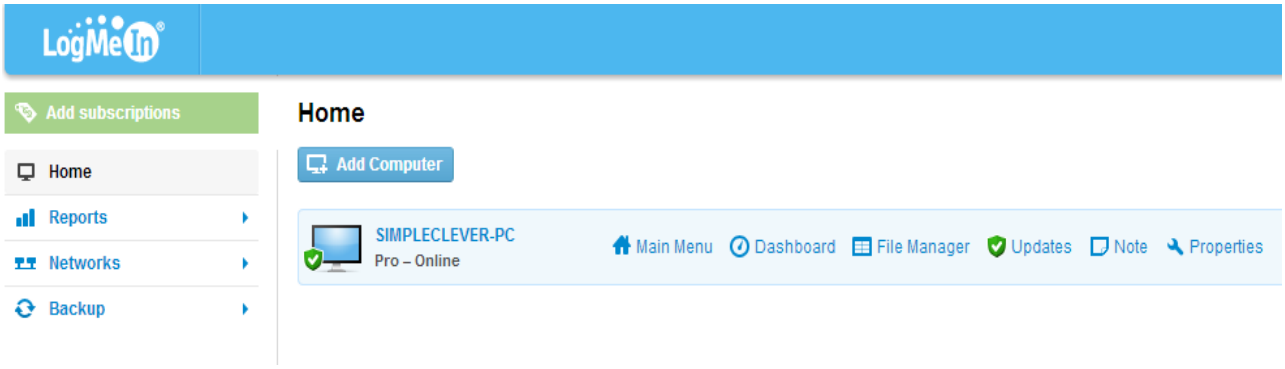
Pro ověření vytvořeného účtu je zapotřebí kliknout na odkaz, který je po registraci zaslán na registrační adresu (v tomto případě na lukasmlynek@email.cz).

Po přihlášení na stránky je možné svůj profil doplnit zbývajícími údaji. Podstatnější částí je však stažení instalátoru. Ten je svázaný s vytvořeným účtem a je nutné jej na

vzdálenou stanici nainstalovat. Po instalaci jen stačí nastavit, z jakého zařízení se budete k tomuto počítači připojovat, a je vše nachystáno.

7.2.2 Připojení

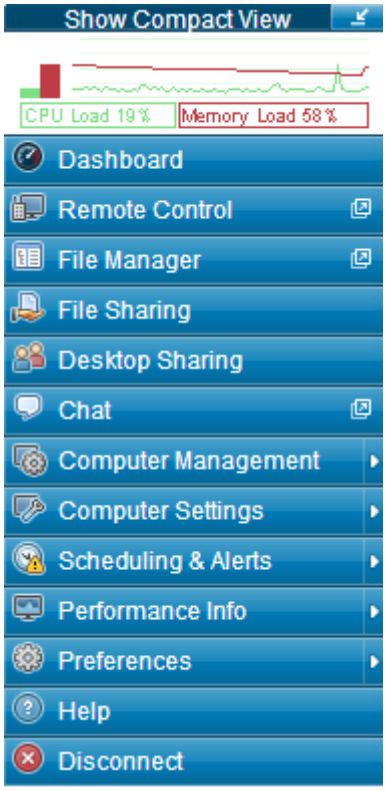
Pokud byla instalace a základní nastavení provedeno korektně, tak po přihlášení na stránky je možné vidět počítač a připojit se k němu (viz *Obrázek 21)*.



Obrázek 21 Seznam stanic spjatých s účtem na LogMeIn

Připojení je možné uskutečnit po kliknutí na položku „Main Menu“. Pravděpodobně budete vyzváni k instalaci doplňku pro váš prohlížeč, ale to není nutné. Následuje přihlašovací obrazovka, kde je nutné vyplnit uživatelské jméno a heslo uživatele na vzdálené stanici.

Po přihlášení se v pravé části webového prohlížeče objeví tzv. Dashboard, který shrnuje informace o vzdálené stanici (používaný systém, volné místo na disku, události, procesy apod.). V levé části je menu (viz *Obrázek 22)*, pomocí něhož lze po kliknutí na položku „Remote Control“ ovládat daný počítač. Jsou zde uvedeny i další možnosti jako je např. „File Manager“, který je určený pro přenášení dat mezi počítači, dále chatovací okno, nastavení počítače apod. K mnoha funkcím je potřeba mít nainstalovanou a povolenou Javu v prohlížeči.



Obrázek 22 LogMeIn hlavní menu při navázaném spojení se stanicí

7.2.3 Shrnutí a další možnosti

Stejně jako TeamViewer je LogMeIn velmi propracovaná aplikace, která nabízí více možností než jen vzdálené ovládání počítače. Může být použít pro konference, vytvoření VPN (za pomocí softwaru LogMeIn VPN), přenášení souborů, komunikaci a mnoho dalších činnosti.

Na rozdíl od TeamVieweru je však LogMeIn vhodnější pro administrátory, kteří hned po přihlášení mohou sledovat přehlednou zprávu o stanici a mohou jednoduše pomocí několika vestavěných nástrojů např. přidávat uživatele, ukončovat procesy, nastavovat velikost virtuální paměti, pracovat s ovladači a mnoho dalšího. Samozřejmě tyto možnosti lze konfigurovat přímo v systému, ale výhodou tohoto vestavěného řešení je, že administrátor má vždy na stejném místě danou možnost a nemusí ji pod různými operačními systémy hledat.

Mezi základní vlastnosti pak patří podpora zvuku, podpora schránky, šifrovaný přenos, přenos souborů, sdílení desktopu (prezentace), funkce Wake-On-Lan (vzdálené

zapnutí počítače), vestavěný chatovací nástroj a další. Velkou výhodou je, že program nepotřebuje veřejnou IP adresu.

LogMeIn využívá vlastní (proprietární) protokol, šifrování SSL a je možné jej provozovat jak v MS Windows, tak v Mac. Z mobilních platforem je možné využít Android, iOS, Windows Mobile.

LogMeIn je zdarma pro nekomerční využití, pro komerční účely pak cena začíná na 1.800,-Kč/rok. Cena pro mobilní platformy pak cca 610,- Kč. (ceny ke květnu 2013)

Obrázek 23 LogMeIn nastavení kvality obrazu

Nastavit kvalitu obrazu lze přímo při připojení v nabídce „Options“ -> „Color Quality“ dle *Obrázku 23*. Kvalita je zde rozdělena do čtyř úrovní, kde zleva je kvalita optimalizovaná pro rychlost a směrem doprava potom na lepší obraz.

7.3 VNC

Existuje mnoho implementací VNC. Jak již bylo uvedeno v teorii, prvním programem tohoto typu byl RealVNC. Ve shrnutí této kapitoly budou uvedeny rozdíly mezi implementacemi UltraVNC, RealVNC a TightVnc. Nastavení serverových i klientských částí je velmi obdobné, proto se následující text věnuje konfiguraci pouze UltraVNC, které nabízí s pomocí pluginu i šifrovaný přenos. V části instalace je zmíněn postup pro všechny výše uvedené typy VNC aplikace.

7.3.1 Instalace

V defaultním nastavení instalátoru je zvolena instalace jak vieweru, tak i serveru. Při instalaci nebo před ukončením instalátoru je vznesen dotaz, zda má daný program zanést výjimku do firewallu.

Ke spuštění serverové části RealVNC je nutné se zaregistrovat na stránkách a získat tak licenci. Jsou tři možnosti. První z nich je získat licenci na 30 dní zdarma a vyzkoušet verzi Enterprise, nebo je možné zdarma na 30 dni vyzkoušet verzi Personal, případně poslední možností je licence zdarma. Právě licence zdarma není vhodná, protože nešifruje komunikaci (šifruje pouze autentizaci). Při vložení jejího licenčního klíče je uživatel na nezabezpečenou komunikaci upozorněn. Rozdíly mezi licencemi jsou v podporovaných funkcích, viz shrnutí této kapitoly. Instalace UltraVNC i TightVNC je obdobná s tím rozdílem, že u druhého zmíněného je možné rovnou na konci instalace zadat heslo pro vzdálený přístup a administrátorské heslo (nemusí být zadáno). U UltraVNC a TightVNC není nutné se registrovat.

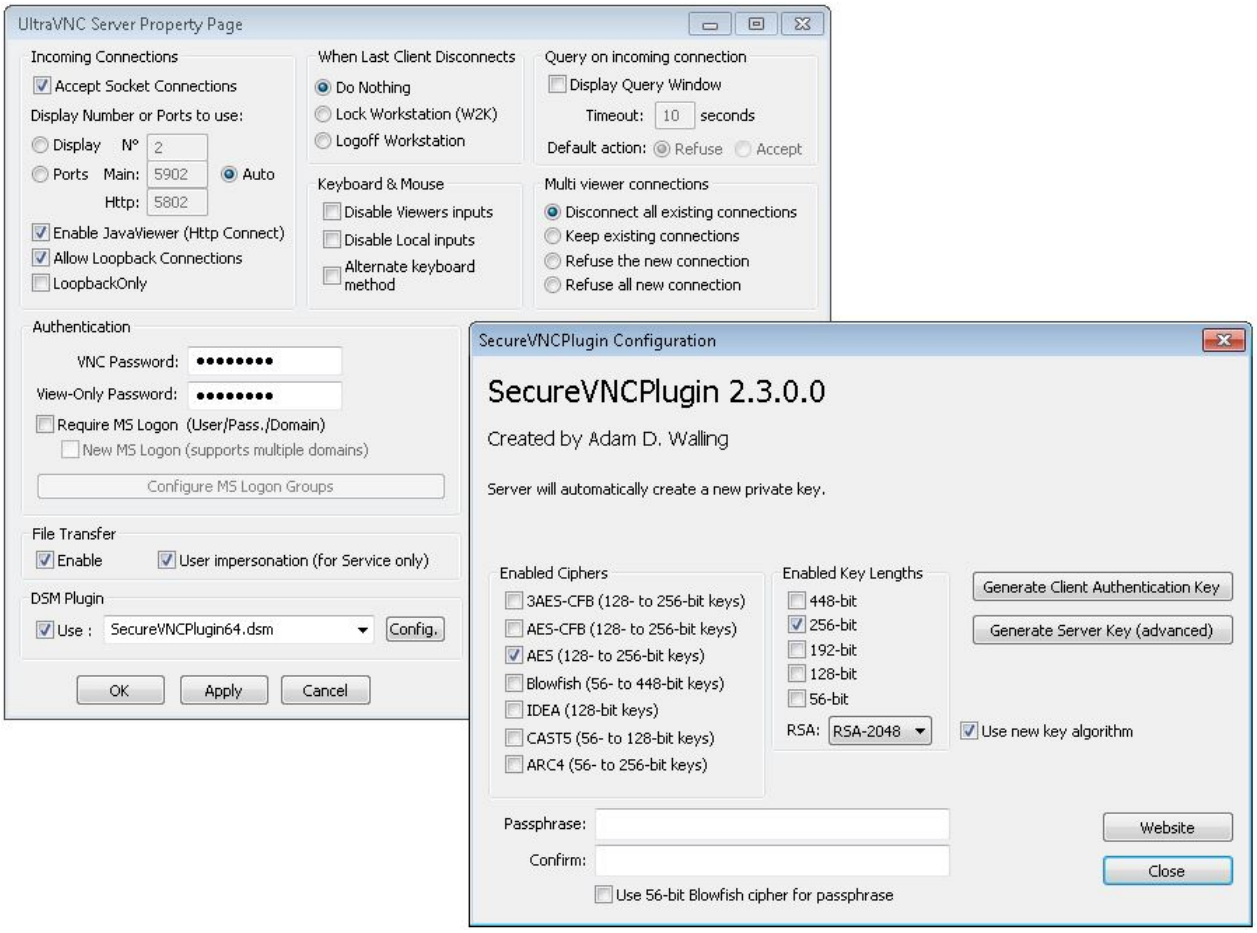
Pro zabezpečení přenosu u UltraVNC lze použít například plugin ze stránek http://adamwalling.com/SecureVNC/ od Adama D. Wallinga. Je nutné jej stáhnout a přesunout do složky s nainstalovaným programem (obvykle C:\Program Files\UltraVNC) a to jak u klientské, tak i u serverové časti. Existují varianty pro 32bitový a pro 64bitový systém s názvy „SecureVNCPlugin“ a „SecureVNCPlugin64“ s příponou *.dms. Nastavit lze šifrování AES (ve výchozím stavu), Blowfish, IDEA, CAST5, ARC4, RSA.

7.3.2 Připojení

Ve výchozím nastavení je server připravený k navázání spojení. Na Klientské straně stačí jen zadat IP adresu serveru a spojení je možné ihned navázat. Obvykle lze navázat spojení napříč různými implementacemi VNC. Proto se lze připojit např. pomocí klienta UltraVNC na server vytvořený pomocí RealVNC. Problém může nastat v situaci, kdy je spojení šifrováno např. za pomoci pluginu použitém v programu UltraVNC. Jak spojení zašifrovat, je uvedeno v následujícím odstavci.

Pokud je správně umístěn plugin (viz *7.3.1 Instalace)*, tak je nutné jej použít jak na straně klienta, tak na straně serveru. *Obrázek 24* ukazuje nabídku *Property* s konfiguračním

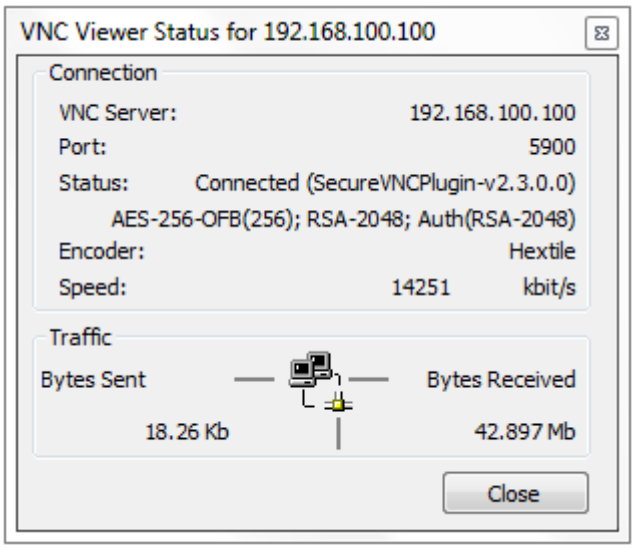
oknem *SecureVNC Plugin*. Plugin je nejprve nutné použít, a k tomu slouží zaškrtávací políčko „Use“ vpravo dole v nastavení UltraVNC serveru (stejně i u klienta).



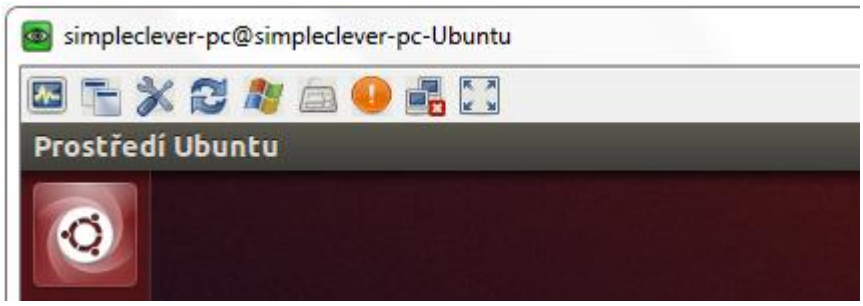
Obrázek 24 SecureVNC Plugin konfigurace

Zvolená šifra a délka klíčů je na uvážení uživatele. Obecně platí: čím delší klíč, tím lepší zabezpečení. Na straně serveru je třeba vygenerovat klíč pro klientskou a pro serverovou stranu (privátní a veřejný). Tyto klíče je pak nutné umístit do složky, kde je program nainstalován (stejně jako plugin v části instalace). Privátní klíč se umístí na straně klienta a veřejný na straně serveru.

V UltraVNC je možné si zobrazit status připojení (jako je na *Obrázku 25*), kde je možné vidět počet přenesených dat a použité šifrování. Pokud by byl přenos příliš pomalý, lze upravit nastavení kvality kliknutím na nářadí (třetí ikona zleva, viz *Obrázek 26)*, nebo např. u TightVNC lze upravovat kvalitu po kliknutí na třetí ikonu zleva (*Obrázek 27*). U RealVNC je to pak čtvrtá ikona zleva (*Obrázek 28*).



Obrázek 25 UltraVNC status připojení (šifrováno za pomoci SecureVNC Plugin)



Obrázek 26 Panel UltraVNC při vzdáleném ovládání

Obrázek 27 Panel TightVNC při vzdáleném ovládání

Obrázek 28 Panel RealVNC při vzdáleném ovládání

7.3.3 Shrnutí a další možnosti

Možnosti zde zmíněných VNC řešení se liší dle výrobce. Lepší implementace obsahují obvykle nástroj pro přenos souborů, vestavěný chat, šifrování apod. Nevýhodou veškerých VNC je absence přenosu zvuku – protokol RFB není k tomuto účelu konstruován. VNC servery zpravidla umožňují připojení přes webový prohlížeč, lze tedy

na klientské straně za pomoci webového prohlížeče s Javou vzdáleně ovládat stanice. Všechny testované VNC umožňují nastavení kvality přenosu.

Ultra VNC umožnuje přenos souborů, použití autentizačního hesla, rozšíření pomocí pluginů (včetně šifrovacího), komunikovat za pomoci chatovacího nástroje, automaticky přizpůsobit kvalitu, a dokáže se také automaticky přihlásit v rámci OS. Mimo klienta na bázi Javy lze Ultra VNC provozovat pouze na OS MS Windows XP a novějších verzích. UltraVNC je šířen zdarma pod licencí GNU GPL.

Tight VNC umožnuje přenos souborů, použití autentizačního, administrátorského a pozorovatelského hesla, automaticky přizpůsobit kvalitu a jiné. Mimo klienta na bázi Javy lze TightVNC provozovat na OS WMS Windows a Linux a mobilními platformami Android, Windows Mobile, iOS. TightVNC je šířen zdarma pod licencí GNU GPL.

Real VNC umožnuje v základní verzi pouze použití autentizačního hesla a obvyklé funkce jako je nastavení kvality, změna portu apod. Ostatní funkce jsou již placené, kde se cena jedné licence začíná na 30 dolarech (květen 2013). Vyšší (placené) verze potom dovolují přenos souborů, šifrování (128b AES - Personal edice, 256b AES - Enterprise edice), vzdálený tisk atd. RealVNC je ze zmiňovanějších VNC implementací nejstabilnější a je možné server provozovat na mnoha OS (Windows, Mac, Linux, Solaris, HP-UX, AIX, speciální verze pro Google Chrome). Klienti se pak nacházejí na mobilních platformách Android, Windows Mobile, iOS.

Aplikace / vlastnost	Nativně zabezpečený přenos	Podpora OS	Mobilní platformy	Přenos souborů	Vestavěný chatovací nástroj	Vzdálený tisk	Přenos audia
Vzdálená plocha (Připojení ke vzdálené ploše)	Ano	Windows, Linux (klient), iOS(klinet)	Android, iOS	Ne	ne	Ano	Ano
Vzdálená pomoc	Ano	Windows	ne	Ano	Ano	ne	
TeamViewer	Ano	MS Windows, Mac, Linux (Wine)	Android, iOS	Ano	Ano	Ano	Ano
LogMeIn	Ano	MS Windows, Mac	Android, iOS, Windows Mobile	Ano	Ano	ne	ne
UltraVNC	ne / plugin	Windows / + Java klient	ne	Ano	Ano	ne	ne
TightVNC	ne	Windows, Linux / + Java klient	Android, Windows Mobile, iOS	Ano	ne	ne	ne
RealVNC (free)	ne	Windows, Mac, Linux, Solaris, HP-UX, AIX, speciální verze pro Google Chrome	Android, Windows Mobile, iOS	ne	ne	ne	ne

Tabulka 2 Srovnání základních funkcí použitých grafických aplikací

8 MĚŘENÍ VYTÍŽENÍ SÍŤOVÉHO PROVOZU

Měření vytíženosti síťového provozu je jednou z podstatných částí této práce. Rychlost připojení k Internetu neustále stoupá, ale u většiny mobilních připojení ještě stálé není dostatečná. Proto je nutné mít správně nakonfigurovaný vzdálený přístup k počítači.

8.1 Volba vhodného softwaru

Vybrat vhodný software není snadné. Existuje řada aplikací, které měří síťový provoz. Především jsou ale určeny k měření celkového počtu stažených a odeslaných dat. Takovouto aplikaci není nutné stahovat, ale lze využít tzv. netstat.

Netstat je nativně obsažen pod operačními systémy MS Windows, Linux, Mac a jiných. Netstat pracuje v textovém režimu. Statistiku lze vyvolat např. v terminálu příkazem *netstat –e*. Nevýhodou tohoto programu jsou odlišnosti pod různými systémy, např. pod systémem Windows nelze vynulovat statistika a je nutný restart systému.

Pro většinu měření byl použit program NetLimiter 3 Pro ve verzi trial. NetLimiter dokáže přehledně rozdělit komunikaci k daným aplikacím a jejich procesům komunikujících se sítí. Zobrazuje jak aktuální provoz, tak i statistiky přenesených dat. Přenosy lze zobrazovat formou grafů, číselně nebo kombinací obou. Netlimiter má mnoho dalších využití mezi které patří např. omezení rychlosti zvoleným procesům, exportování dat apod.

8.2 Způsob měření

Pro měření bylo využito tří základních nastavení každé měřené aplikace. Důraz byl kladen na co nejjednodušší korekci kvality obrazu tak, jak by se ji pravděpodobně běžný uživatel pokusil nastavit. Korekce probíhala vždy na klientské straně, kde bylo postupně provedeno měření pro minimální, maximální, střední nebo automatickou kvalitu obrazu. Někteří klienti dovolovali vypnutí pozadí plochy, vypnutí AERO efektů apod. Toto nastavení bylo ponecháno v původním stavu (případně jej ovlivňovaly tři výše zmíněné režimy kvality). Obraz byl za pomoci tzv. scale obrazu upraven tak, aby umožňoval rozlišení obrazu serverové stanice (1920 na 1080 pixelů) redukovat na velikost okna na klientské straně. Serverové nastavení aplikací zůstalo v defaultním nastavení.

Po navázání spojení bylo na vzdálené stanici spuštěno video s názvem Divočina. Toto video je obsaženo v běžné distribuci Windows 7 a je možné jej nalézt v umístění *C:\Users\Public\Videos\Sample Videos*. Parametry videa jsou:

- Velikost: 25MB
- Rozlišení: 1280 na 720 pixelů
- Frekvence snímků: 29 snímků/s
- Délka: 30 s

Video bylo přehráváno ve fullscreen módu (celoobrazovkový mód). Spolu s měřením videa bylo vždy otevřeno a uzavřeno 5 složek.

Měření probíhalo v nouzovém režimu, který umožňuje práci se sítí. Tento režim byl zvolen, protože nespouští žádné externí aplikace, které by mohly zatěžovat provoz (např. aktualizace programů apod.). Měření probíhalo v rámci sítě LAN, vytvořené směrovačem značky TP-LINK modelem TL-WR543G s verzí firmwaru 3.6.1 Build 071010 Rel.33028n. Směrovač byl připojen k Internetu. Internetový provider byl Sychrovnet, použitý tarif Individual, který běžně dosahuje (dle www.rychlost.cz) v testu rychlosti připojení k Internetu parametrů 30000 kbit/s download a 8000 kbit/s upload.

8.3 Výsledky měření

Výsledky měření jsou zaznamenány v *Tabulce 3*. Subjektivní hodnocení kvality a plynulosti obrazu je v rozmezí 0-10, kde vyšší číslo znamená lepší. V pravé části tabulky se nachází způsob vykreslování přehrávaného videa z pohledu uživatele (principiální způsob vykreslování obrazu je popsán v teorii). Stažená a odeslaná data jsou uvedena v MB (megabyte), kde číslo před lomítkem jsou stažená data a číslo za ním jsou odeslaná data. Textové režimy vzdáleného ovládání počítače byly vynechány.

Program	**Nastavení kvality (download/upload) [MB]**			**Hodnocení obrazu (kvalita/plynulost)**			**Způsob vykreslování videa**
	Malá	**Vysoká**	**Střední nebo automatická**	**Malá**	**Vysoká**	**Střední nebo automatická**	
TeamViewer	21,3/0,3	27,4/0,3	20,0/0,3	8/7	8/5	7/7	Po celých snímcích
LogMeIn	2,3/0,2	10,0/0,4	3,3/0,2	1/1	7/0	2/1	Po obdélnících
Vzdálená plocha	29,0/1,0	29,2/0,8	29,3/1,0	9/10	10/10	10/10	Po celých snímcích
Vzdálená pomoc	280,8/7,8			3/1			Po řádcích
RealVNC	7,7/0,3	272,8/7,7	272,5/7,5	2/6	8/5	9/4	Po celých snímcích
UltraVNC	12,1/0,3	39,9/1,1	269,1/7,0	2/8	5/8	9/5	Po celých snímcích
TightVNC	17,7/0,5	41,5/1,1	27,5/0,75	5/7	8/6	7/7	Po celých snímcích

Tabulka 3 Měření zatížení sítě.

9 POŽADAVKY NA HARDWARE A MĚŘENÍ ZÁTĚŽE

Tato kapitola se věnuje hardwarovým požadavkům a hardwarovému vytížení některých výše popsaných aplikací. Výsledky jsou shrnuty v části *9.4 Výsledky měření*.

9.1 Požadavky

Hardwarové (dále jen HW) požadavky pro výše zmíněné aplikace nejsou vysoké. Nejdůležitější podmínkou je připojení k počítačové síti obou (nebo více) stanic, které budou ovládat, nebo budou ovládány. Připojení k Internetu je nutné pro aplikaci TeamViewer a LogMeIn, protože jak již bylo zmíněno v teorii – komunikace probíhá přes servery těchto firem. Aplikace využívající protokol RDP (Vzdálená plocha) a VNC řešení nemusí být pro správnou funkci připojeny k Internetu.

Microsoft nezveřejňuje žádné HW požadavky na Vzdálenou plochu mimo jediného – na daném hardwaru musí běžet MS Windows. Pokud je tato podmínka splněna, Vzdálená plocha by měla fungovat. Podobně je tomu i u všech výše zmíněných aplikací typu VNC, TeamViewer a LogMeIn, které neudávají žádné HW požadavky.

Jedinými požadavky jsou nainstalované operační systémy na stanice s kompatibilními grafickými kartami a síťovými kartami. U některých řešení je nutná také podpora Javy (LogMeIn, případně VNC aplikace).

9.2 Volba vhodného software

Operační systém MS Windows obsahuje software pro sledování vytížení jednotlivými procesy s názvem Sledování prostředků. Lze v něm sledovat především aktuální údaje využití procesoru a využití paměti.

Spolu s touto aplikací bylo využito i aplikací Process Explorer v15.3 a System Explorer v4.2.2. Tyto dvě aplikace přehledně graficky i číselně poskytují údaje o běžících procesech.

9.3 Způsob měření

Měření probíhalo ve třech fázích. Bylo měřeno zatížení při spuštěné aplikaci, ale nepřipojené, dále pak po připojení (bez činnosti) a poslední fází bylo měření při přehrávání

videa. Video bylo použito stejné jako v předchozím případě, ale z důvodu měření nebylo přehráváno ve fullscreen módu (přes celou obrazovku).

Měření probíhalo zvlášť pro klientskou a zvlášť pro serverovou část. Klientská část byla testována na stanici Lenovo Thinkpad SL410 s konfigurací:

- Intel GM45 čipová sada
- Intel Core 2 Duo T6670, 2200 MHz
- 4 GB paměti RAM DDR3
- Mobile Intel(R) 4 Series Express Chipset Family
- WDC WD3200BEVT-08A23T1

Běžné vytížení počítače se spuštěným a plně nastartovaným operačním systémem Microsoft Windows 7 Professional 32b je 8% CPU a 39% RAM.

Serverová část byla testována na sestavě s operačním systémem Microsoft Windows 7 Professional 64b. Běžné vytížení sestavy se spuštěným a plně nastartovaným operačním systémem je 2% CPU a 35% RAM. Konfigurace sestavy:

- Gigabyte GA-MA69G-SH3 (AMD 690G, AMD Hammer čipová sada)
- DualCore AMD Athlon 64 X2, 3200 MHz 6400+ BlackBox
- 3 GB paměti RAM DDR2
- ATI Radeon HD 3870, 512MB
- Segate Barracuda 7200.11 500320

9.4 Výsledky měření

Aplikace	Stav	Server			Klient		
		Využití CPU	Využití RAM	Virtuální paměť	Využití CPU	Využití RAM	Virtuální paměť
TeamViewer	spuštěno	0%	11324	5312	0%	26568	16904
	navázané spojení	2%	15276	10196	11%	130660	132876
	přehrávání videa	7%	16004	10669	22%	153742	155772
LogMeIn	spuštěno	0%	36356	28608	-	-	-
	navázané spojení	1%	59908	49064	5%	304572	314464
	přehrávání videa	1%	59908	49064	35%	364196	357440
Vzdálená plocha	spuštěno	-	-	-	-	-	-
	navázané spojení	-	-	-	2%	113688	166932
	přehrávání videa	-	-	-	19%	113688	166932
VNC (Tight)	spuštěno	0%	10428	3514	0%	5960	1280
	navázané spojení	4%	59764	43476	7%	35548	26784
	přehrávání videa	5%	59846	44236	8%	32628	26784

Tabulka 4 Měření HW náročnosti

Z naměřených výsledků (viz *Tabulka 4)* vyplývá, že nejvíce je zatěžována klientská část. Měření není zcela objektivní, protože probíhalo na dvou různých, výše zmíněných sestavách. Tyto sestavy mají jiný výpočetní výkon.

Nejvíce byla zatěžována klientská část při použití aplikace LogMeIn. Zde se objevil velký problém s měřením, protože LogMeIn jako klienta používá webový prohlížeč s

Javou. Při měření byl použit prohlížeč Google Chrome verze 27.0.1453.94 m, který při jednom otevřeném okně a panelu s aplikací LogMeIn měl spuštěných více než 40 podprocesů. V měření je započteno i zatížení zmíněnou Javou ve verzi 7 Update 21. S použitím jiného prohlížeče by bylo jiné využití procesoru a paměti.

Z hlediska vytížení paměti nejlépe dopadlo VNC řešení, které po navázání spojení již téměř nezvyšovalo potřebu paměti ani při přehrávání videa. Podobně je na tom i Vzdálená plocha, která využívala neustále stejné množství paměti na klientské straně.

V tabulce se nacházejí pomlčky na místech, kde se nepodařilo změřit zatížení (část Vzdálená plocha na straně serveru) nebo kde je měření irelevantní (klientská strana LogMeIn při zapnutí aplikace resp. webového prohlížeče).

10 ŘEŠENÍ OBVYKLÝCH PROBLÉMŮ

Tato kapitola je zde uvedena, protože s konfigurací vzdáleného připojení se na Internetu objevuje mnoho dotazů, které souvisí obvykle se špatně nastaveným firewallem nebo porty na směrovači. Vyhnout se těmto problémům lze při použití výše uvedeného programu TeamViewer nebo LogMeIn, avšak při konfiguraci Vzdálené plochy nebo VNC je obvykle nutné povolit porty, které tyto aplikaci využívají (viz *Tabulka 1 Obvyklé porty RD aplikací a protokolů).*

10.1 Porty

Pokud se vyskytnou problémy s připojením, je velice pravděpodobné, že na vině budou uzavřené porty, špatně nastavený firewall či směrovač (router). Otevření či forwardování portů může problém s nenavázaným připojením v tomto případě vyřešit.

Které porty náleží kterým aplikacím, je možné nalézt na stránkách výrobce softwaru nebo v *Tabulce Obvyklé porty RD aplikací a protokolů* uvedené v části teorie.

10.1.1 Otevření portů MS Windows XP

1. Klikněte na tlačítko „Start“ na hlavním panelu Windows.

2. Klikněte na „Síťová připojení“.

3. V záložce „Síťové úlohy“ klikněte na „Zobrazit síťová připojení“.

4. Nyní byste měli vidět seznam dostupných síťových připojení vašeho PC. U síťového připojení, které právě používáte, by měl být nápis „Připojeno“. Všechna ostatní připojení by měla hlásit „Odpojeno“.

5. Pravým tlačítkem klikněte na stávající síťové připojení a z nabídky zvolte „Vlastnosti“.

6. Klikněte na záložku „Upřesnit“.

7. Klikněte na tlačítko „Nastavení“.

8. Klikněte na záložku „Výjimky“.

9. Klikněte na tlačítko „Přidat port“.

10. Nyní by se mělo objevit vyskakovací okno.

11. Pojmenujte svůj port (název by měl být stručný a měl by se vztahovat k aplikaci).

12. Zadejte číslo portu do textového políčka „Číslo portu“.

13. Zvolte buď „TCP“ nebo „UDP“ (dle dané aplikace).

14. Klikněte na „OK“.

Nyní by měly být Windows XP nastaveny korektně a aplikace by měla na příslušných portech komunikovat.

10.1.2 Otevření portů MS Windows 7

1. Klikněte na tlačítko „Start“ na hlavním panelu Windows.

2. Klikněte na položku „Ovládací panely“.

3. Do políčka pro vyhledávání napište „firewall“.

4. Klikněte na položku „Brána Windows Firewall“.

5. Na panelu vlevo klikněte na položku „Upřesnit nastavení“.

6. Jestliže vás systém zažádá o zadání administrátorského hesla či o potvrzení, napište heslo a příkaz potvrďte. Pokud ne, přejděte k dalšímu kroku.

7. V levém panelu okna „Brána Windows Firewall s pokročilým zabezpečením“ klikněte na položku „Příchozí pravidla“.

8. V pravém panelu klikněte na možnost „Nové pravidlo“.

9. Spustí se průvodce vytvářením nového příchozího pravidla, ve kterém budete moci zadat příslušné číslo portu a zvolit možnost TCP nebo UDP.

10.1.3 Otevření portů Linux Ubuntu

Nastavení portů není zpočátku pro běžné služby nutné. Porty jsou sic standardně uzavřeny (Closed), avšak při instalaci služby, např. SSH serveru, se daný port sám otevře (v tomto případě port č. 22). Je doporučováno instalovat z repozitářů.

Jádro Ubuntu obsahuje nástroj Iptables. Iptables je využíván mnoha grafickými „firewally“ a umožňuje nastavit veškerá pravidla síťové komunikace.

Výchozím firewallem je však od verze Ubuntu 8.04 firewall UFW (Uncomplicated Firewall). UFW se spravuje pomocí terminálu, proto se často mimo serverové prostředí používá jeho grafická nástavba GUFW neboli GUI for Uncomplicated Firewall (pro použití je nutné nainstalovat balík *gufw*). Při používání UFW firewallu je nutné jej nejprve aktivovat a to příkazem *sudo ufw enable*. Více používaní syntaxi příkazu v [16].

10.1.4 Forwardování portů

Jak je již známo z předešlých řádků, pro správnou činnost RD je nutná veřejná IP adresa. Často se však stane, že požadavek na spojení RD „narazí“ na místní (domácí) router ač máme veřejnou IP adresu. V tomto případě je možné si pomoci a to správnou konfigurací routeru resp. tzv. forwardováním portů.

Forwardování portů není snadná záležitost. Každý výrobce routeru používá jiné uživatelské rozhraní a může mít také jinak sestavenou strukturu jednotlivého nastavení. Velice vhodným pomocníkem pro takové nastavení je návod k danému zařízení nebo webová stránka HTTP://PORTFORWARD.COM/ . Na této webové stránce je možné dohledat návody k nastavení velkého množství routerů od většiny výrobců. Nutno podotknout, že webová stránka je v angličtině.

10.2 Neveřejná IP adresa

Jak již bylo zmíněno v teoretické části, pokud server má neveřejnou IP adresu, lze se k počítači připojit také. Jedním z možných řešení je použití nějakého z programů, které jsou zmíněny (TeamViewer, LogMeIn) nebo zřízení vlastní VPN či tunelového spoje.

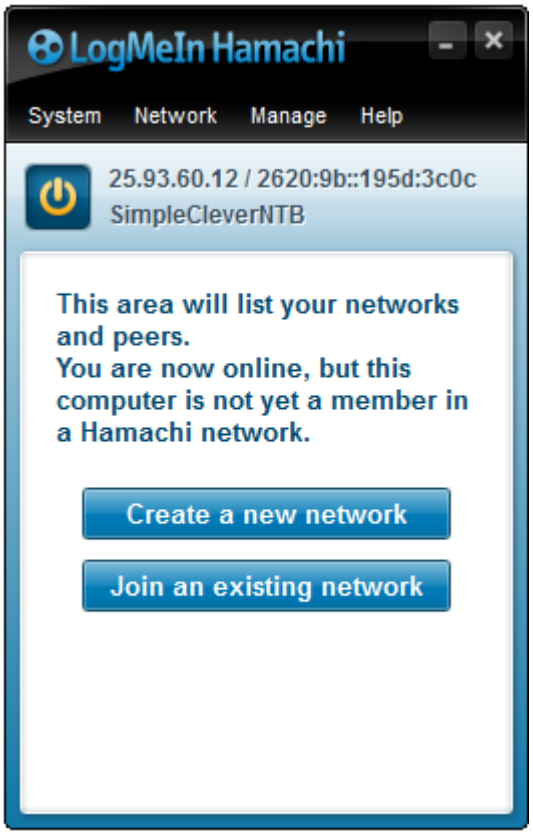
Zřídit vlastní VPN lze mnoha způsoby, které jsou obvykle určené pro zkušenější uživatele, administrátory nebo správce sítě. Běžný uživatel má potom možnost zřídit si vlastní VPN např. pomoci programu LogMeIn Hamachi (dříve jen Hamachi).

Po instalaci LogMeIn Hamachi je v počítači vytvořena „virtuální síťová karta“ přes kterou probíhá virtuální komunikace jako by v místní síti. Praxe je však taková, že je využito tunelování přes reálnou kartu připojenou k Internetu.

Po následném spuštění programu LogMeIn Hamachi je počítači přidělena jedinečná IP adresa ve tvaru 25. xxx. xxx. xxx (např. 25.93.60.12 tak jako je na *Obrázku 29*), dříve 5.

xxx. xxx. xxx. Uživatel má na výběr buď připojení k již exitující síti *Join an existing network* nebo vytvoření nové sítě *Create a new network.*

Aplikace není výrobcem lokalizována do českého jazyka, ale lze stáhnout alternativní překlad (např. ze stránek http://ricrdsson.ic.cz/hcz.html). Podporované operační systémy jsou Microsoft Windows XP (a novější), Mac OS X a Linux.



Obrázek 29 Hlavní okno programu LogMeIn Hamachi

ZÁVĚR

V závěru bych rád shrnul stěžejní poznatky práce. Vzdálené připojení k počítači resp. jeho ovládání lze aplikovat téměř vždy. Někdy je tato cesta snazší, jindy však méně. Náročnost na realizaci záleží na zvoleném programu či protokolu a také na typu IP adresy, kterou má přiřazen server. Z hlediska IP adresy mohou nastat tyto situace.

Počítač, na který se uživatel připojuje (server) má veřejnou IP adresu. Tím je myšleno, že není veřejná IP adresa na směrovači (routeru) umístěném v Internetu před tímto počítačem. Případně se nacházejí obě stanice v místní síti sic připojené k Internetu, ale připojení bude probíhat pouze v rámci této sítě. Tento případ je na realizaci nejsnadnější a lze využít všech výše zmíněných metod s důrazem na zabezpečení aplikací typu VNC.

Druhou možností je, že počítač má jednu z privátních IP adres, ale směrovač předřazený před ním k Internetu má veřejnou IP adresu. V tomto případě je nutné naforwardovat (nasměrovat) porty, nebo využít DMZ (v rámci připojení z Internetu). V případě, že uživatel nechce nebo nemůže konfigurovat směrovač, lze použít např. výše zmíněných programů TeamViewer, LogMeIn nebo použít VPN či tunelový spoj.

Ve výše uvedené situaci je zmíněno, že veřejná IP adresa je statická. Pokud není, existuje řešení např. v DDNS (Dynamické DNS), které lze nastavit i na levnějších „domácích“ směrovačích.

Poslední možností je, že serverová stanice nemá veřejnou IP adresu (stejně jako směrem k Internetu nadřazený směrovač). V tomto případě již nezbývá nic jiného než použití VPN či tunelového spoje, nejsnáze pak pomocí programů LogMeIn – Hamachi či TeamViweru, které toto umožňují. Případně je možné použití vzdáleného ovládání za pomoci TeamViewer nebo LogMeIn.

Další otázkou je bezpečnost. Ta se dá rozdělit na bezpečnou autentizaci a zabezpečený přenos dat. Nejbezpečnější je kombinace obou. Zvýšenou pozornost je nutné věnovat především použití VNC, kde není přenos běžně šifrován. Naopak přenos za použití např. TeamVieweru nebo LogMeIn je šifrován, ale veškerá komunikace probíhá přes servery zmíněných společností. Jejich reference jsou velmi přesvědčivé, avšak stále tu existuje někdo třetí, přes koho zabezpečená komunikace probíhá.

V neposlední řádě se práce zabývá síťovou náročností popsaných řešení. U všech grafických možností lze korigovat kvalitu přenášeného obrazu, případně i metodu komprimace dat. Z naměřených výsledků vyplývá, že nejmenší nároky na síťové připojení má aplikace LogMeIn. Nevýhodou LogMeIn je kvalita obrazu. Z hlediska podpory nezkušených uživatelů bych dle naměřených výsledků a získaných zkušeností volil TeamViewer jako nejlepší řešení. Kvalita obrazu je ve výchozím stavu automaticky upravována během přenosu a program si dobře poradí i se změnami odezvy během spojení. TeamViewer však není vhodný pro připojení v rámci sítě LAN, protože zbytečně komunikuje přes Internet a své servery. Zde je výhodnější použít např. protokol RDP, tedy Vzdálené plochy, který v rámci MS Windows dobře interaguje se systémem.

Rád bych se ještě zmínil o programu TeamViewer. Jeho přednosti zde již byly poznamenány, ale tato aplikace má i svou špatnou vlastnost a to zejména pro administrátory. Protokol RDP lze zablokovat, stejně tak lze nepovolit uživatelům instalaci cizího software (VNC a jiné aplikace), je možné také zakázat stránky LogMeIn na směrovačích, ale ubránit se TeamVieweru je téměř nemožné. Stačí totiž spuštění verze QuickSupport, kterou si záškodník může donést na nějakém médiu (nemusí jej ani stahovat ani instalovat) a poté je již možné se ke stanici připojit a to i přes různé nastavení firewallů – postačuje pouze, aby stanice měla přístup k Internetu a povolené standardní porty pro prohlížení webových stránek.

CONCLUSION

In the conclusion, I would like to summarize the main findings of the thesis. Remote connection to a computer, respectively its remote control, can be applied in almost all cases. Sometimes it is easier this way, sometimes not. Difficulty of the implementation depends on the selected program or protocol and also on the type of IP address that is assigned to the server. From the perspective of the IP address, these situations can occur.

Computer, to which user is connected (server) has a public IP address, i.e. that there is no public IP address of the router located on the Internet in front of the computer. Alternatively, there may be two stations in the local network connect to the Internet, but the connection only takes place within the network. This case is the easiest for the implementation and all the above mentioned methods can be used with an emphasis on security of applications such as VNC.

The second possibility is that the computer has one of the private IP addresses, but the router in front of the computer is connected to the Internet and router has public IP address. In this case forwarding ports or use of DMZ (within the connection from the Internet) is necessary. Should the use not want to or be unable to configure the router, above mentioned programmes such as TeamViewer, LogMeIn can be used, as well as VPN or tunnel connection.

In this situation, we assume that the public IP address is static. If this is not the case, there are solutions such as DDNS (Dynamic DNS), that can be set also to cheap, "home" routers.

The last possibility is that the server station does not have a public IP address (nor towards Internet superior router). In such a case, there is no other option than using VPN or tunnel connections. The easiest way to do this is through programmes like LogMeIn – Hamachi or TeamViewer. Use of remote control via TeamViewer or LogMeIn is also an option.

Security is another issue. It can be divided into secure authentication and secure data transfer. The safest is a combination of both. Increased attention should be paid to using VNC, if the transmission is not standardly encrypted. On the contrary, the transmission of applications such as TeamViewer or LogMeIn is encrypted, but all communications go through the servers of the mentioned companies. Their references are quite convincing, but there always is someone, through whom the encrypted communication is transferred.

Last but not least, the thesis deals with network demands of the described solutions. All grapchicall options allow correction of video transmission quality, some even of the method of data compression. The measured results show, that application LogMeIn has the lowest network connection demands. A disadvantage of LogMeIn is image quality. Bearing in mind importance of supporting less experienced users, I believe that the measured results suggest that using TeamViewer is the best option. The image quality is automatically adjusted during transmission and the programme is able to work out response changes during connection effectively. On the other hand, TeamViewer is not suitable for connection to LAN, because it unnecessarily communicates via the Internet and its servers. For this purpose, using Remote Desktop is more suitable, as it interacts very well with the system in MS Windows environmet.

There is one more thing I would like to add about TeamViewer.

Its advantages have already been mentioned, but this application has problematic attributes, especially for administrators. RDP Protocol can be blocked, or users may be forbidden to install unknown software (VNC and other applications) and forbidding LogMeIn websites on routers can be done too, but defending against TeamViewer is practically impossible. Mere start-up of QuickSupport version (brought by a saboteur on a medium with no need of downloading or installing) is sufficient for connection to a station, in spite of various firewall settings. It suffices that the station is connected to the Internet and standard ports for web browsing are allowed.

SEZNAM POUŽITÉ LITERATURY

[1] HLAVENKA, Jiří. A KOL. *Výkladový slovník výpočetní techniky a komunikací*. 3. vyd. Praha: Computer Press, 1997, 452 s. ISBN 80-722-6023-5.

[2] SMITH, Roderick W. *Linux ve světě Windows: průvodce administrátora heterogenních sítí*. 1. vyd. Tomáš ZNAMENÁČEK. Praha: Grada, 2006, 460 s. ISBN 80-247-1470-1.

[3] AUTHORS NETAPPLICATIONS.COM. Desktop Operating System Market Share [online]. *Net Applications.com*, 2013, Únor 2013 [cit. 2013-03-30]. Dostupné z: http://netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0

[4] RFC: 854. *Telnet Protocol Specification*. IETF: IETF, 1983 [cit. 2013-04-02]. Dostupný z WWW: http://tools.ietf.org/html/rfc854

[5] Protokoly tunelového propojení VPN. In: MICROSOFT. *Technet Microsoft* [online]. 2013 [cit. 2013-03-23]. Dostupné z: http://technet.microsoft.com/cs-cz/library/cc771298(v=ws.10).aspx

[6] MICROSOFT CORPORATION. *Remote Desktop Protocol: Basic Connectivity and Graphics Remoting* [online]. v20130118. 2013 [cit. 2013-03-25]. ISBN MS-RDPBCGR. Dostupné z: http://download.microsoft.com/download/9/5/E/95EF66AF-9026-4BB0-A41D-A4F81802D92C/[MS-RDPBCGR].pdf

[7] RICHARDSON, Tristan. *The RFB Protocol: Version 3.8* [online]. RealVNC Ltd, 2010, 26.11.2010 [cit. 2013-03-26]. Dostupné z: http://www.realvnc.com/docs/rfbproto.pdf

[8] TIŠNOVSKÝ, Pavel. Grafická knihovna OpenGL (12): Vlastnosti framebufferu. *Root.cz (www.root.cz), informace nejen ze světa Linuxu* [online]. 2003, [cit. 2013-04-11]. ISSN 1212-8309. Dostupné z: http://www.root.cz/clanky/opengl-12-vlastnosti-framebufferu/

[9] THOMAS, Braden. TeamViewer authentication protocol. In: *Accuvant Labs: RawTech blog* [online]. 2013 [cit. 2013-04-14]. Dostupné z:

http://blog.accuvantlabs.com/blog/bthomas/teamviewer-authentication-protocol-part-1-3

[10] WALTER, Björn a Vladislav JANEČEK. *Telefonujeme přes Internet: Sada programů a názorný průvodce*. Vyd. 1. Překlad David Čepička. Brno: Computer Press, 2007, 237 s. ISBN 978-80-251-1631-9.

[11] VAŠEK, Jiří. VNC a Vzdálená plocha - kouzlo vzdáleného přístupu. *PCTuning.cz* [online]. 2009 [cit. 2013-04-14]. ISSN 1214-0201. Dostupné z: http://pctuning.tyden.cz/software/jak-zkrotit-internet/12639-vnc_a_vzdalena_plocha-kouzlo_vzdaleneho_pristupu

[12] PŘISPĚVATELÉ DO DOKUMENTACE NA ČESKÉ UBUNTU WIKI. Firewall. In: *Ubuntu.cz* [online]. 2012, 20. 7. 2012 [cit. 2013-05-06]. Dostupné z: http://wiki.ubuntu.cz/Bezpe%C4%8Dnost/Firewall?redirect=1

[13] PŘISPĚVATELÉ DO DOKUMENTACE NA ČESKÉ UBUNTU WIKI. ufw. In: *Ubuntu.cz* [online]. 2012, 20. 7. 2012 [cit. 2013-05-06]. Dostupné z: http://wiki.ubuntu.cz/bezpe%C4%8Dnost/firewall/ufw

[14] PŘISPĚVATELÉ DO DOKUMENTACE NA ČESKÉ UBUNTU WIKI. Iptables. In: *Ubuntu.cz* [online]. 2012, 1.8.2012 [cit. 2013-05-06]. Dostupné z: http://wiki.ubuntu.cz/bezpe%C4%8Dnost/firewall/iptableshttps://tools.ietf.org/html/rfc6143

[15] DEVELOPMENT TEAM REMMINA. *Remmina: The GTK+ Remote Desktop Client* [online]. 2013 [cit. 2013-05-08]. Dostupné z: http://remmina.sourceforge.net/index.shtml

[16] VNC a Linux: vzdálená plocha. *Root.cz: informace nejen ze světa Linuxu* [online]. 2009 [cit. 2013-05-15]. DOI: 1212-8309. Dostupné z: http://www.root.cz/clanky/vnc-a-linux-vzdalena-plocha/

[17] BARAN, René. LogMeIn aneb Vzdálená plocha přes web. *LinuxEXPRES* [online]. 2008 [cit. 2013-05-20]. ISSN 1801-3996. Dostupné z: http://www.linuxexpres.cz/blog/logmein-aneb-vzdalena-plocha-pres-web

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

3DES	Triple DES
AES	Advanced Encryption Standard
AMD	Advanced Micro Devices
ARD	Apple Remote Desktop
ASCII	American Standard Code for Information Interchange
BSD	Berkeley Software Distribution
CPU	Central Processing Unit
DDNS	Dynamic Domain Name Server
DES	Data Encryption Standard
DMZ	Demilitarized Zone
DNS	Domain Name Systém
EAP-TLS	Extensible Authentication Protocol - Transport Layer Security
GNU GPL	GNU General Public License
GUFW	GUI Uncomplicated Firewall
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol.
HTTPS	Hypertext Transfer Protocol Secure
HW	Hardware
IANA	Internet Assigned Numbers Authority
ID	Identification
IP	Internet Protocol
IPX	Internetwork Packet Exchange
L2TP	Layer Two Tunneling Protocol
MAC	Media Access Control

MB	Megabyte
MS	Microsoft
MS-CHAP	Microsoft - Challenge-Handshake Authentication Protocol
NAT	Network Address Translation
NT	New Technology
OS	Operační systém
OSI	Open Systems Interconnection
P2P	Peer-to-Peer
PC	Personal Computer.Význam
PPTP	Point-to-Point Tunneling Protocol
RD	Remote Deskop
RDP	Remote Desktop ProtocolVýznam
REE	Rise-and-Run length Encoding
RFB	Remote FramebufferVýznam
RFC	Request for Comments
RMA	Random Access Memory
RSA	Rivest, Shamir, Adleman (iniciály autorů)
RSH	Remote Shell
SFTP	SSH File Transfer Protocol
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
SSTP	Secure Socket Tunneling Protocol
TCP	Transmission Control Protocol

UDP	User Datagram Protocol
UFW	Uncomplicated Firewall
UPnP	Universal Plug and Play
VNC	Virtual Network Computing
VPN	Virtual Private Network
XDMCP	X Display Manager Control Protocol
ZRLE	Zlib Run-Length Encoding

SEZNAM OBRÁZKŮ

SEZNAM TABULEK