# 12. Remote služby a wol

## Teoretická část

Vysvětlete a předveďte protokoly a aplikace remote složeb (vzdálená procha, VNC, Teamviewer).

## Praktická část

1. V úloze WIN7 předveďte připojení pomocí dvou dodaných programů.
2. Funkční remote připojení změřte a upravte pomocí programu Wireshark.

## Doplňující otázky

1. Předveďte úpravy měřeného logu na vyhledání specifické IP adresy či portu (služby).

# Remote služby a wol

# RDP

Remote Desktop Protocol (zkratka RDP) je v informatice [proprietární](https://cs.wikipedia.org/wiki/Proprietární_software) [síťový](https://cs.wikipedia.org/wiki/Počítačová_síť) [protokol](https://cs.wikipedia.org/wiki/Protokol_(informatika)), který umožňuje uživateli ovládat vzdálený počítač prostřednictvím připojení k jeho [desktopovému prostředí](https://cs.wikipedia.org/wiki/Desktopové_prostředí). Připojení pracuje na principu [klient-server](https://cs.wikipedia.org/wiki/Klient-server), kdy uživatel na svém počítači využívá jednoduchého [klienta](https://cs.wikipedia.org/wiki/Klient_(počítače)) pro zobrazení [grafického uživatelského prostředí](https://cs.wikipedia.org/wiki/Grafické_uživatelské_rozhraní), které je spuštěno na vzdáleném počítači.

Protokol RDP byl poprvé představen ve [Windows NT 4.0](https://cs.wikipedia.org/wiki/Windows_NT_4.0) Terminal Server Edition. Klienti pro připojení pomocí RDP protokolu existují pro většinu verzí [Windows](https://cs.wikipedia.org/wiki/Microsoft_Windows), [Mac OS X](https://cs.wikipedia.org/wiki/OS_X) a další [operační systémy](https://cs.wikipedia.org/wiki/Operační_systém). Server implicitně naslouchá na [TCP](https://cs.wikipedia.org/wiki/TCP) [portu](https://cs.wikipedia.org/wiki/Síťový_port) 3389. Firma Microsoft nabízí klientský software [Remote Desktop Connection](https://cs.wikipedia.org/w/index.php?title=Remote_Desktop_Connection&action=edit&redlink=1) (RDC) nebo Terminal Services Client (TSC). V operačním systému Mac OS X se klient nazývá Remote Desktop.

Remote Desktop Services

MSTSC

# VNC – Virtual Network Computing

**Virtual Network Computing (VNC)** je grafický [program](https://cs.wikipedia.org/wiki/Počítačový_program), který umožňuje vzdálené připojení ke [grafickému uživatelskému rozhraní](https://cs.wikipedia.org/wiki/Grafické_uživatelské_rozhraní) pomocí [počítačové sítě](https://cs.wikipedia.org/wiki/Počítačová_síť). VNC pracuje jako [klient-server](https://cs.wikipedia.org/wiki/Klient-server), kde [server](https://cs.wikipedia.org/wiki/Server) vytváří grafickou plochu v [operační paměti](https://cs.wikipedia.org/wiki/Operační_paměť) počítače a komunikuje přes síť s [klientem](https://cs.wikipedia.org/wiki/Klient_(počítače)), který plochu zobrazuje [uživateli](https://cs.wikipedia.org/wiki/Uživatel_(počítačový)) (většinou na jiném počítači). Pro komunikaci se používá protokol **RFB** ([anglicky](https://cs.wikipedia.org/wiki/Angličtina) remote framebuffer), jehož cílem je minimalizovat objem přenášených [dat](https://cs.wikipedia.org/wiki/Data) mezi klientem a serverem a umožnit tak komunikaci i přes pomalejší datové linky (např. přes [Internet](https://cs.wikipedia.org/wiki/Internet)).

## Systém VNC

Kompletní VNC systém se skládá z klienta, serveru a komunikačního protokolu. VNC [server](https://cs.wikipedia.org/wiki/Server) je program, který sdílí svoji obrazovku. VNC [klient](https://cs.wikipedia.org/wiki/Klient) (viewer) je program, který zobrazuje sdílenou plochu a ovládá server. VNC protokol ([RFB](https://cs.wikipedia.org/wiki/RFB)) používá bitmapové řešení, kde každý pixel má své souřadnice, kde plocha se bere jako jeden obrázek, na který se malují objekty a jako celek se to pošle klientovi. Přenášejí se pouze změny (například pohyb myši, psaní textu, zobrazování videa). V praxi pohneme kurzorem, server si přebere souřadnice, a na hostitelském počítači se provede pohyb kurzoru, který se pak zpětně promítne do klienta.

## Bezpečnost

Komunikace mezi klientem a serverem standardně zabezpečena není. Samotná [autentizace](https://cs.wikipedia.org/wiki/Autentizace) je poměrně bezpečná, protože se pro ověření hesla používá systém [challenge-response](https://cs.wikipedia.org/wiki/Challenge-response) (náhodná výzva a kontrolovaná odpověď), takže heslo neputuje po síti v nezašifrované podobě (je omezen útok [Replay attack](https://cs.wikipedia.org/wiki/Replay_attack)). Po autentizaci už však síťový provoz mezi klientem a serverem [zašifrován](https://cs.wikipedia.org/wiki/Kryptografie) není, a tak může být veškerá komunikace odposlouchávána.

# Teamviewer

**TeamViewer** je program pro vzdálený přístup a podporu přes počítačové sítě. Umožňuje vzdálené ovládání počítače vašeho partnera, sdílení pracovní plochy, on-line schůzky, webové konference a přenos souborů mezi počítači. TeamViewer umožňuje připojení k jakémukoli počítači nebo serveru na světě v několika sekundách. Program je kompatibilní s platformami [Microsoft Windows](https://cs.wikipedia.org/wiki/Microsoft_Windows), [Mac OS X](https://cs.wikipedia.org/wiki/OS_X), [Linux](https://cs.wikipedia.org/wiki/Linux), [iOS](https://cs.wikipedia.org/wiki/IOS) a [Android](https://cs.wikipedia.org/wiki/Android). TeamViewer využívá více než 100 000 000 uživatelů po celém světě. Je to jedno z nejrychleji rostoucích řešení pro vzdálené ovládání a dálkové prezentace na světě. TeamViewer je vyvinut firmou [TeamViewer GmbH](https://cs.wikipedia.org/w/index.php?title=TeamViewer_GmbH&action=edit&redlink=1), která byla založena v roce 2005 v Uhingen v Německu.

## Nastavení spojení

TeamViewer musí být nainstalován pomocí instalačního manuálu, ačkoliv Quick support verze je funkční bez instalace. Pro připojení k jinému počítači pomocí TeamViewer musí být program nainstalován na obou zařízeních. Na jednom zařízení musí být aktivní práva administrátora, na ostatních zařízeních jsou dostačující práva standardního uživatele.

Jakmile je TeamViewer v počítači nainstalován, vygeneruje si partnerské ID číslo a heslo (heslo definované uživatelem je také přípustné). Pro navázání spojení mezi oběma zařízeními (administrátorem a ovládaným klientem) musí administrátor a klient použít výše uvedené ID číslo a heslo a zadat je do svého lokálního TeamVieweru.

Pro zahájení online konference pošle moderátor jednání ID číslo jednotlivým účastníkům. Za pomocí plné verze TeamViewer nebo přihlášením na http://go.teamviewer.com/ a zadáním ID se účastníci přihlásí do konference.

## Zabezpečení

TeamViewer využívá RSA kódový klíč (1024 bitů) a AES klíč (256-bitů) kódovací relaci.

V základním nastavení TeamViewer využívá jeden ze serverů TeamViewer.com pro navázání a směrování spojení mezi administrátorem a ovládaným klientem. Nicméně v 70% případů je spojení navázáno přes [UDP](https://cs.wikipedia.org/wiki/UDP) nebo [TCP](https://cs.wikipedia.org/wiki/TCP).

# WOL

**Wake on LAN** (WOL) je v [informatice](https://cs.wikipedia.org/wiki/Informatika) technologie umožňující zapnutí vypnutého [počítače](https://cs.wikipedia.org/wiki/Počítač) přes [počítačovou síť](https://cs.wikipedia.org/wiki/Počítačová_síť).

Podpora Wake on LAN musí být zabudována do [základní desky](https://cs.wikipedia.org/wiki/Motherboard), často bývá v deskách [ATX](https://cs.wikipedia.org/wiki/ATX). Základní deska musí být vybavena konektorem WAKEUP-LINK, kterým je propojena pomocí 3pinového kabelu se [síťovou kartou](https://cs.wikipedia.org/wiki/Síťová_karta). Síťové karty a základní desky podporující WOL a standard [PCI 2.2](https://cs.wikipedia.org/w/index.php?title=PCI_2.2&action=edit&redlink=1) už takový kabel nepotřebují, neboť oživovací signál i nezbytné napájení se šíří přímo po sběrnici [PCI](https://cs.wikipedia.org/wiki/PCI). Většina moderních základních desek s integrovanou síťovou kartou standard WOL podporuje.

Funkce Wake on LAN musí být povolena v [BIOSu](https://cs.wikipedia.org/wiki/BIOS), kde musí být zvoleno neustálé napájení síťové karty i po vypnutí počítače. Většinou v nastavení[Power Management](https://cs.wikipedia.org/w/index.php?title=Power_Management&action=edit&redlink=1).

Buzení počítače probíhá přes síť [LAN](https://cs.wikipedia.org/wiki/Local_Area_Network). Vypnutý počítač má v BIOSu nastaveno napájení síťové karty při vypnutí (viz výše). Síťová karta naslouchá a čeká na speciální posloupnost bajtů (paket), která se nazývá Magický packet. Tento paket je odeslán do konkrétní LAN, která je určena [broadcastovou](https://cs.wikipedia.org/wiki/Broadcast) IP adresou sítě. Pokud síťová karta tento paket přijme a zjistí, že se jedná o Magický paket s odpovídající MAC adresou, spustí počítač.

## Magický packet

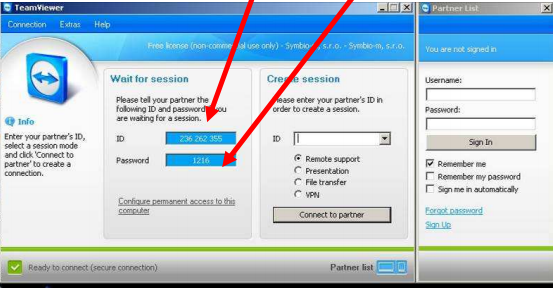
Magický paket, na který reaguje síťová karta, je v podstatě speciální rámec odeslaný protokolem UDP na port 7 nebo 9, dříve také protokolem IPX. Paket obsahuje šest konstantních bajtů hexadecimálně zapsaných jako **FF:FF:FF:FF:FF:FF** následovaných šestnáctkrát se opakující MAC adresou.

# Praktická část

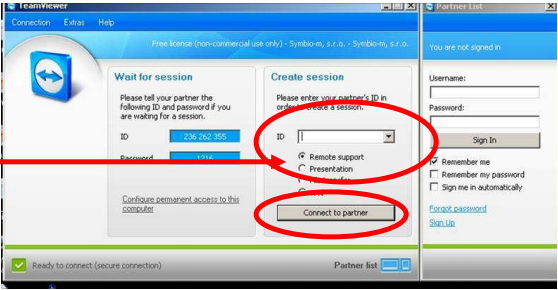
## 1. V úloze WIN7 předveďte připojení pomocí dvou dodaných programů.

Teamviewer:

Aktivní program Po spuštění programu je pro počítač vygenerovaný kód (ID) a heslo („Password“)



Pokud chce, aby někdo ovládal Váš počítač, je potřeba mu sdělit pouze tyto 2 údaje. Tj. ID (jenž představuje 9 čísel) a heslo (jenž představuje 4 čísla). Pokud naopak chcete Vy ovládat jiný počítač, je potřeba zadat ID (9 čísel) do kolonky v pravo; mít vybranou položku Remote support a kliknou níže na „Connect to partner“



Poté se objeví okno pro vyplnění hesla (4 čísla); vyplnímě heslo a klikneme na „Log On“

## Funkční remote připojení změřte a upravte pomocí programu Wireshark.

Potřebné příkazy:

ip.addr == 77.75.79.53 – Vyhledá komunikaci s ip adresou 77.75.79.53

tcp.port == 80 – Vyhledá veškerou komunikaci na portu 80 (Pouze TCP)

udp.port == 80 - Vyhledá veškerou komunikaci na portu 80 (Pouze UDP)

tcp.port == 80 || udp.port == 80 - Vyhledá veškerou komunikaci na portu 80 (TCP i UDP)

Teamviewer pracuje na portech: 5938, 80(HTTP) a 443 (HTTPs)