# 14. Telnet, SSH, SNMP, VNC, Teamviewer

## Teoretická část

Vysvětlete, co mají protokoly nebo programy v tématu společné a čím se liší. Vysvětlete a popište jednotlivě jejich použití, výhody a nevýhody.

## Praktická část

1. Na úloze WIN7 předveďte použití VNC a Teamviewer.

## Doplňující otázky

1. Popište a vysvětlete, kde najdete a využijete SNMP a jak byste jej použili.

# Telnet

Telnet (zkratka z Telecommunication Network) je v informatice označení protokolu používaného v počítačových sítích, který pomocí stejnojmenné aplikace umožňuje uživateli připojení ke vzdálenému počítači.

Protokol telnet pracuje na aplikační vrstvě používaný TCP/IP. Používá se v Internetu pro realizaci spojení typu klient-server protokolem TCP, přičemž přenáší osmibitové znaky oběma směry (duplexní spojení). Serverová část standardně naslouchá na portu číslo 23. Součástí protokolu je vyjednání nastavení určitých voleb důležitých pro vzájemnou komunikaci.

## Program telnet

Telnet je též označení pro program, který realizoval komunikaci mezi dvěma počítači pomocí telnet protokolu. Program je dodnes součástí Microsoft Windows a unixových systémů. Dříve se používal (spolu s protokolem telnet) pro připojení ke vzdálenému počítači prostřednictvím počítačové sítě jako emulace terminálu, která poskytovala možnost práce uživatele na vzdáleném počítači v příkazovém řádku. Telnet tak byl nástupcem terminálů, ze kterých se uživatelé připojovali ke vzdálenému počítači pomocí sériové linky. Hlavní nevýhodou telnetu je absence šifrování přenášených dat, a proto dnes uživatelé místo telnetu používají protokol SSH.

V současné době se program telnet používá pro ruční komunikaci mezi počítačovými programy (například simulace připojení webového prohlížeče k webovému serveru, při simulaci SMTPprotokolu pro přepravu elektronické pošty a podobně).

# SSH

SSH (Secure Shell) je v informatice označení pro program a zároveň pro zabezpečený komunikační protokol v počítačových sítích, které používají TCP/IP. SSH byl navržen jako náhrada za telnet a další nezabezpečené vzdálené shelly (rlogin, rsh apod.), které posílají heslo v nezabezpečené formě a umožňují tak jeho odposlechnutí při přenosu pomocí počítačové sítě. Šifrování přenášených dat, které SSH poskytuje, slouží k zabezpečení dat při přenosu přes nedůvěryhodnou síť, jako je například Internet.

## Charakteristika

SSH umožňuje bezpečnou komunikaci mezi dvěma počítači, která se využívá pro zprostředkování přístupu k příkazovému řádku, kopírování souborů a též jakýkoliv obecný přenos dat (s využitím síťového tunelování). Zabezpečuje autentizaci obou účastníků komunikace, transparentní šifrování přenášených dat, zajištění jejich integrity a volitelnou bezeztrátovou kompresi. Server standardně naslouchá na portu TCP/22.

Označení „Secure Shell“ je mírně zavádějící, protože nejde ve skutečnosti o náhradu shellu ve smyslu interpret příkazů. Název byl odvozen z existujícího programu rsh, který má podobné funkce, ale není zabezpečený.

# Simple Network Management Protocol

Simple Network Management Protocol (SNMP) je součástí sady internetových protokolů. Slouží potřebám správy sítí. Umožňuje průběžný sběr nejrůznějších dat pro potřeby správy sítě, a jejich následné vyhodnocování. Na tomto protokolu  je dnes založena většina prostředků a nástrojů pro správu sítě.

## Charakteristika

Protokol SNMP se vyvíjel postupně ve třech verzích: první verze (SNMPv1) zajišťuje základní funkcionalitu SNMP, druhá (SNMPv2) obsahuje navíc autentizaci a třetí (SNMPv3) šifrování (zabezpečení). Nejvíce zařízení podporuje druhou verzi.

Protokol SNMP rozlišuje se mezi stranou monitorovanou (hlídaný systém) a monitorovací (sběrna dat). Tyto strany mohou běžet buď odděleně na různých fyzických strojích, nebo v rámci jednoho stroje. Na monitorované straně je spuštěn agent a na straně monitorovací manager. Na straně monitorované jsou operativně shromažďovány informace o stavu systému (zařízení). Manager vznáší požadavky agentovi, zpravidla na zaslání požadovaných informací (zpráv). Agent zajišťuje realizaci reakcí na požadavky managera. Získaný obsah zpráv se na straně monitorovací může dále různým způsobem zpracovávat (tabulky, grafy, …). Komunikace mezi agentem a managerem se označuje jako SNMP operace.

# 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).

# Praktická část

## Na úloze WIN7 předveďte použití VNC a Teamviewer.

Teamviewer viz. Remote služby

Použití VNC:

Na obou počítačích nainstalován program Real VNC. Ten se po standardní instalaci usadí v liště vedle hodin a spouští se při startu windows. Přesněji řečeno jeho serverová část, která je nutná,aby se k vám mohl váš zdatnější pomocník nebo kolega připojit ze svého PC. Pokud na tuto ikonku VNC Server (Service) poklepnete (anebo čerstvě po instalaci), zobrazí se vám okno VNC Server Properties ( Service-Mode ), kde je možno pro větší bezpečnost nastavit heslo ( VNC Password Autentication ) kliknutím na tlačítko Configure. Zadáte nové heslo (new password), které potvrdíte (confirm password) a kliknete na OK. Tímto heslem se bude váš kolega přihlašovat do vašeho PC.

Dalším krokem je povolení programu VNC ve vašem Firewalu (musí být povolen v obou směrech příchozí i odchozí).

Takže PC je zapnutý a běží vám VNC (i přes váš firewal), můžete tedy požádat kolegu o pomoc a jeho připojení na váš PC.

Pokud má VNC nainstalováno jako vy. Bude potřebovat vaši IP adresu (pokud najedete šipkou na ikonu VNC Serveru vedle hodin zobrazí se tam číslo vaší IP adresy) a heslo, které jste si nastavil v úvodu. Je-li vše v pořádku za chvíli se vám ikona VNC serveru začerní což indikuje připojení na váš PC a po vaší ploše bude běhat kurzor myši ovládaný vaším kamarádem, který se bude kochat kontrolou nad vaším PC.

# Doplňující otázky

## Popište a vysvětlete, kde najdete a využijete SNMP a jak byste jej použili.

**Simple Network Management Protocol (SNMP)** je součástí sady internetových protokolů. Slouží potřebám správy sítí. Umožňuje průběžný sběr nejrůznějších [dat](https://cs.wikipedia.org/wiki/Data) pro potřeby správy sítě, a jejich následné vyhodnocování. Na tomto protokolu je dnes založena většina prostředků a nástrojů pro správu sítě.

SNMP je typicky využíváno na jednom či více správcovských počítačích (manažeři), které mají za úkol sledovat nebo řídit skupinu počítačů či jiných zařízení v síti. Na straně sledovaných zařízení je spuštěn agent, který následně poskytuje pomocí SNMP informace manažerovi.

Spravovaná data agentů jsou evidována jako proměnné. Protokol umožňuje jejich aktivní správu, kdy lze vzdáleně modifikovat tyto proměnné a změnit tak konfiguraci. Proměnné přístupné přes SNMP jsou uspořádány hierarchicky. Tato hierarchie a další metadata (jako například typ a popis proměnné), jsou popsány pomocí [MIBs](https://cs.wikipedia.org/w/index.php?title=Management_Information_Base&action=edit&redlink=1) (Management Information Bases).

Síť řízená pomocí SNMP se skládá ze tří hlavních částí:

1. Spravované zařízení
2. Agent – software, který běží na spravovaných zařízeních
3. NMS (Network management station) – software, který běží na správcovských počítačích