# 18. VPN, PPP, PPTP, Direct tunel, RIP

## Teoretická část

**Vysvětlete a popište metody tunelování v síti, tzv. protokoly PPP, PPTP, VPN** či metody přímého přístupu. **Popište a vysvětlete funkci protokolu RIP.**

## Praktická část

1. **Předveďte protokol VPN v rámci Teamviewer.**
2. **V CMD předveďte příkaz tracert a popište, jak pracuje RIP.**
3. **Předveďte přímé propojení například pomocí SMB či http spojení.**

## Doplňující otázky

1. **Pomocí Wireshark vyhledejte pakety SMB či http komunikace a izolujte je**
2. **Popište, jak pracuje VPN v rámci použití pro 2PC a jak pro propojení celých sítí.**
3. **Jaké formy ověřování zabezpečení VPN, PPP a PPTP využívá?**

# Definice VPN

VPN je možné definovat jako soukromé logické spojení vyhrazené autorizovaným osobám pro připojení ke vzdáleným zdrojům. Toto spojení je realizováno prostřednictvím veřejného internetu či WAN sítí lokálních ISP. Na obou koncích tohoto logického spoje se nachází patřičně nakonfigurovaný hardware a/nebo software, který zajištuje celý proces zapouzdření, šifrováni a tunelování.

# Proč volit VPN?

Stěžejní okamžik pro zavedení VPN do rozrůstající se společnosti nastane většinou ve chvíli, kdy dojde k havárii serveru, či jen pouhé nedostupnosti nějaké služby, a správce IT v této společnosti se nachází na dovolené, či je jiným způsobem nedostupný. Nastávají pak situace, kdy se v IT nejzběhlejší zaměstnanec v sídle společnosti snaží (patřičně instruován po telefonu) například obnovit data z RAIDového pole, restartovat služby na serveru atp. Ovšem, důvodů pro zavedení VPN do jakékoliv společnosti je mnoho a nemusí být nutně předcházeny katastrofou.

 Dostupnost - zaručený přístup ke všem zdrojům ve vzdálené lokalitě

 Vzdálený přístup - zaměstnanci společnosti mohou přistupovat odkudkoliv

 Kontrola - možnost monitorování přístupů vzdálených klientů

Jak je patrné z těchto bodů, veškeré výhody vycházejí ze základní myšlenky umožnit ověřenému uživateli pracovat odkudkoliv prostřednictvím stávajících připojení lokálních ISP či veřejného internetu. Pro lepší představu o případném využití VPN si představme síť společnosti s centrálou v Praze a pobočkou v Brně. Tato síť má několik desítek pevných uživatelů a několik zaměstnanců, kteří pravidelně cestují po Čechách. Nastává otázka, jak umožnit těmto cestujícím zaměstnancům přistup do systémů společnosti při zachování patřičného zabezpečení a zároveň nízkých nákladů. Pakliže zároveň vezmeme v potaz nutnost propojit síť obou poboček do jednoho segmentu, jeví se VPN jako ideální volba.

Co lze očekávat od VPN sítě

Každý manažer, majitel společnosti či zákazník má jistá specifika, která se promítnou v očekávání do nově nasazované technologie. Pokusím se seřadit několik klíčových vlastností těchto sítí, abychom se vyhnuli případným nenaplněným očkováním a nejasnostem. Většina VPN je ideálním řešením pro vzdálený přístup, pomoc uživatelům či zvýšené zabezpečení pro přístup k firemní síti a informačním systémům. Je ovšem důležité dopředu plánovat jaké programy budeme vzdáleně obsluhovat, neboť lze obecně říci, že až na výjimky jsou VPN:

 Pomalejší než LAN

 Méně spolehlivé než LAN

 Hůře monitorovatelné pro firewally

Z uvedených bodů tedy vyplývá, že očekávat možnost zálohování jednoho serveru skrze VPN na pobočku v jiné lokalitě by bylo velmi nerozumné. Naopak vzdálená plocha na terminálový server, klient aplikace využívající SQL, či intranetová aplikace postavená na HTTP jsou ideální kandidát pro využití této technologie.

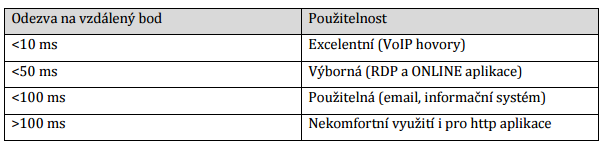
# Tunelování

[Virtuální privátní síť](https://cs.wikipedia.org/wiki/Virtuální_privátní_síť) využívá tunely pro vytvoření [zabezpečeného](https://cs.wikipedia.org/wiki/Kryptografie) spojení počítačů (nebo počítačových sítí) pomocí nedůvěryhodné sítě (například [Internet](https://cs.wikipedia.org/wiki/Internet)).

Technicky se tunelování provádí [zabalením (zapouzdřením)](https://cs.wikipedia.org/wiki/Zapouzdření_(počítačové_sítě)) datových prvků (PDU - Protocol Data Unit) přenášeného (tunelovaného) protokolu do PDU jiného protokolu. Přitom je obvykle narušeno normální pořadí vrstev, protože se PDU jedné vrstvy [referenčního modelu ISO/OSI](https://cs.wikipedia.org/wiki/Referenční_model_ISO/OSI) [balí (zapouzdřuje)](https://cs.wikipedia.org/wiki/Zapouzdření_(počítačové_sítě)) do PDU vyšší nebo stejné vrstvy.

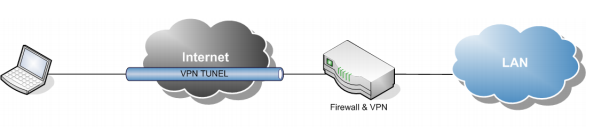
# Rozdělení VPN dle struktury

Sítě VPN lze rozdělit do tří typů dle logického členění: klient - síť, síť - síť, klient - server. Obecně lze říci, že pro všechny varianty VPN sítě platí následující tabulka.



*Vliv časové prodlevy na použitelnost spojení*

# Klient - Síť



*Klient – síť*

Jak design na obrázku napovídá, jedná se o časté řešení. Umožňuje využití většiny firemních prostředků, jako je interní informační systém, CRM, správa dokumentů, tisk a jiné. Všechny počítače, včetně vzdálených stanic připojených do VPN se chovají tak, jakoby byly součástí jednoho síťového segmentu. Výhodou pro tyto společnosti je fakt, že outsourcingové organizace si často za vzdálenou pomoc přes VPN účtují jinou – řádově nižší sazbu než za výjezd technika.

# Klient – Server



*Klient – Server*

Klient – server je asi nejvíce zastoupené řešení. Benefit spočívá ve využití bezpečnosti VPN k realizaci citlivých operací. Prostředky, použitelné pro klienta, jsou ovšem omezeny pouze na jediný server. Tato varianta je často používána v bankovním sektoru, kdy zákazník pomocí clientless SSL - VPN ovládá svůj účet přes běžný internetový prohlížeč. Bohužel využití služeb je vzhledem k omezení dnešních prohlížečů dosti omezeno. Nicméně, například společnost Microsoft Inc. nabízí velmi silné řešení na bázi SSL - VPN - Microsoft Web Access, kdy je Internet Explorer schopen zobrazit i plochu vzdáleného serveru.

# Síť – Síť



*Síť - Síť*

Nejmohutnější a nejkomplexnější možná varianta. Jedná se v podstatě o privátní síť, která je ovšem – s ohledem na náklady- realizována po síti partnera. Toto řešení je ideální volbou všude tam, kde je potřeba spolupracovat a komunikovat v jednotném celku bez ohledu na geografickou pozici zaměstnanců. Tato varianta je tedy vhodná například pro vysoké školy s několika fakultami, ale hlavně pro společnosti s obchodním zastoupením na několika kontinentech. Dnes již je běžnou praxí, že se ICT oddělení velké korporace nachází například v Indii (Dell, Microsoft), kde je dostatek kvalifikovaných odborníků a zároveň nižší mzdové požadavky.

# Protokoly využívané pro VPN

Protokolů určených pro VPN je velké množství.

PPP protokol

Protokol linkové vrstvy, používaný pro přímé spojení mezi dvěma síťovými uzly. Umožňuje autentizaci, šifrování a kompresi přenášených dat.

# PPTP Protokol

Point-to-Point Tunneling Protocol (PPTP) je způsob realizace Virtuální privátní sítě ([VPN](https://cs.wikipedia.org/wiki/Virtuální_privátní_síť)). Obvyklými náhradami za PPTP jsou Layer 2 Tunneling Protocol ([L2TP](https://cs.wikipedia.org/w/index.php?title=L2TP&action=edit&redlink=1)) nebo [IPsec](https://cs.wikipedia.org/wiki/IPsec). Na konci července 2012 byl prolomen šifrovací protokol MS-CHAPv2 a od té doby nelze použití PPTP VPN považovat za bezpečné

Protokol PPTP umožňuje, aby byla data více protokolů zašifrována a následně zapouzdřena do hlavičky protokolu IP, která je následně odeslána přes síť protokolu IP nebo veřejnou síť protokolu IP, jako je Internet. Protokol PPTP lze použít pro vzdálený přístup a propojení VPN mezi lokalitami. Je-li jako veřejná síť pro síť VPN využíván Internet, serverem PPTP je server sítě VPN s povoleným protokolem PPTP, který má jedno rozhraní v Internetu a druhé rozhraní v síti intranet.

# L2TP Protokol

L2TP je protokolem společnosti Cisco a využívá některých vlastností PPTP. Ačkoli je tento protokol ideální pro přenos libovolných dat na síťové vrstvě, tak v základu není schopen šifrovat přenášená data, a proto se samotného protokolu L2TP v podstatě nevyužívá. Využívanější variantou této technologie je kombinace L2TP a IPSec, kdy první protokol slouží k sestavení tunelu a šifrování je dosaženo pomocí IPSec. Výsledná technologie je označována jako L2TP/IPsec. Microsoft považuje L2TP za ideální mechanismus pro autentizaci uživatelů, pokud se požaduje silné zabezpečení uživatelů se vzdáleným přístupem. Protože protokol L2TP poskytuje bezpečnou autentizaci uživatelů a pak pro autentizaci zařízení používá IPSec, mohou se vzdálení uživatelé připojovat bez mezery v autentizaci.

# IPsec Protokol

IPsec (IP security) je v [informatice](https://cs.wikipedia.org/wiki/Informatika) název [bezpečnostního](https://cs.wikipedia.org/wiki/Počítačová_bezpečnost) rozšíření [IP protokolu](https://cs.wikipedia.org/wiki/Internet_Protocol) založené na [autentizaci](https://cs.wikipedia.org/wiki/Autentizace) a [šifrování](https://cs.wikipedia.org/wiki/Kryptografie) každého [IP datagramu](https://cs.wikipedia.org/wiki/IP_datagram).

Vytváří logické kanály – Security Associations (SA), které jsou vždy jednosměrné, pro duplex se používají dvě SA.

Bezpečnostní rozšíření vypadá následovně:

* Ověřování – při přijetí paketu může dojít k ověření, zda vyslaný paket odpovídá odesilateli či zda vůbec existuje.
* Šifrování – obě strany se předem dohodnou na formě šifrování paketu. Poté dojde k zašifrování celého paketu krom IP hlavičky, případně celého paketu a bude přidána nová IP hlavička.

# Kryptování

Kryptografie neboli šifrování je nauka o metodách utajování smyslu zpráv převodem do podoby, která je čitelná jen se speciální znalostí. Jedná se tedy o klíčový požadavek na VPN. Od těchto sítí očekáváme, že i když jsou realizovány skrz veřejný internet, zaručí nám velmi rozumné zabezpečení přenášených dat. Některé protokoly, jako jsou PPTP či IPSec, poskytují šifrování přenášených dat již nativně, ostatní jako například L2TP tuto možnost v základu nenabízejí. Běžné metody kryptování jsou například MPPE (používané pro PPTP), DES či AES. Některé algoritmy, jako MPPE společnosti Microsoft, bývají často označovány jako slabé, či nedůvěryhodné. Domnívám se ovšem, že než slabé šifrování je častějším původcem bezpečnostního incidentu slabé uživatelské heslo, které lze jednoduše napadnout slovníkovým útokem. Před volbou šifrovací metody a slepou vírou v její sílu a bezpečnost se hodí podotknout, že většina těchto algoritmů pochází se Spojených států, a tyto se vcelku odmítavě staví k vývozu tzv. Silných šifer, nebo lépe řečeno k vývozu šifer, které nejsou vládní organizace USA schopny v krátké době dekryptovat. Princip šifrování lze zjednodušeně shrnout do jednoduchého diagramu.

**DATA + KLÍČ + ALGORITMUS = ZAŠIFROVÁNO**

# Routing Information Protocol

Routing Information Protocol (RIP) je v informatice směrovací protokol umožňující směrovačům (routerům) komunikovat mezi sebou a reagovat na změny topologie počítačové sítě. Ačkoliv tento protokol patří mezi nejstarší doposud používané směrovací protokoly v sítích IP, má stále své uplatnění v menších sítích a to především pro svoji nenáročnou konfiguraci a jednoduchost.

## Tracert

**Traceroute** zvyšuje hodnotu „time to live“ ([TTL](https://cs.wikipedia.org/wiki/Time_to_live)) po každém úspěšném odeslání balíčku paketů. První tři pakety mají jednotnou hodnotu TTL nastavenou na 1 (odesílají se současně), další tři pakety mají hodnotu TTL 2 atd. Při cestě k cíli paket prochází jednotlivými směrovači (uzly). Při průchodu směrovač sníží hodnotu TTL o 1 a pošle ho dál. Je-li hodnota TTL paketu nula a není v cílové [IP](https://cs.wikipedia.org/wiki/Internet_Protocol) síti, pak je paket zahozen a směrovač pošle chybovou [ICMP](https://cs.wikipedia.org/wiki/ICMP) zprávu odesílateli. traceroute využívá právě těchto chybových hlášení, aby sestavil tabulku cesty paketu od odesílatele k cíli. Ve výpisu jsou tak zobrazeny všechny uzly, které položku TTL snižují (tj. směrovače).

# TeamViewer

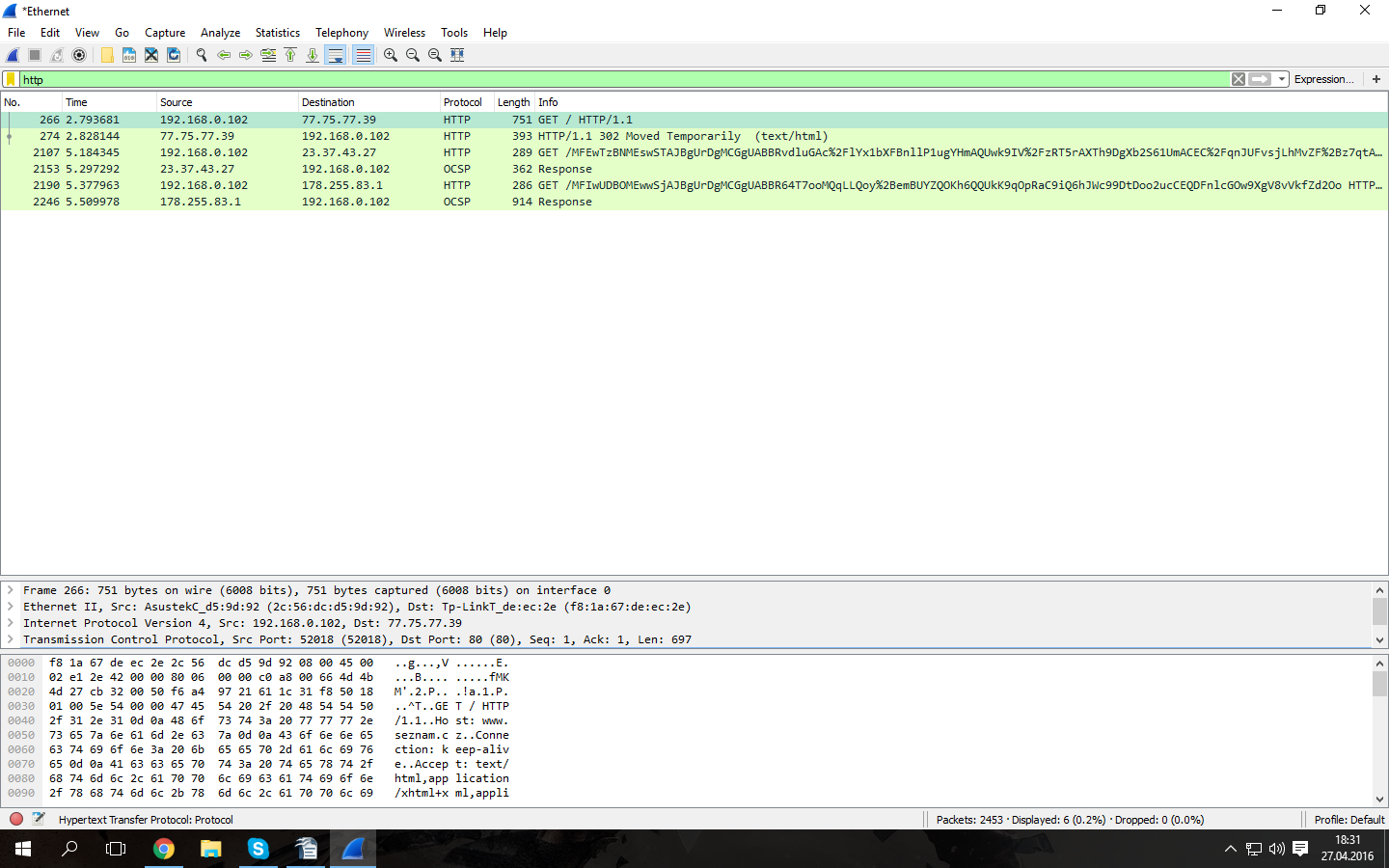
TeamViewer je program pro vzdálený přístup a podporu přes počítačové sítě. Umožňuje vzdálené ovládání počítače vašeho partnera, sdílení pracovní plochy, on-line schůzky, webové konference a přenos souborů mezi počítači. TeamViewer umožňuje připojení k jakémukoli počítači nebo serveru na světě v několika sekundách. Program je kompatibilní s platformami Microsoft Windows, Mac OS X, Linux, iOS a 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, která byla založena v roce 2005 v Uhingen v Německu.

# Pomocí Wireshark vyhledejte pakety http komunikace a izolujte je.

Nejjednoduší způsob:

1.) Zapneme Wireshark a začneme zachýtávat komunikaci.

Otevřeme například http://www.seznam.cz vrátíme se do wiresharku a do Filteru napíšeme: „http“



Další možnost je ve filteru odchýtavat veškerou komunikaci na portu 80, to lze udělat následujícími příkazy:

tcp.port == 80 || udp.port == 80

tcp.port == 80

udp.port == 80

# Jaké formy ověřování a zabezpečení používá VPN, PPP, PPTP a L2TP?

**PPP** - Rámec protokolu PPP je šifrován pomocí šifrování MPPE (Microsoft Point-to-Point Encryption) a jsou využívány šifrovací klíče generované procesem ověření protokolem MS-CHAP verze 2 nebo EAP-TLS. Klienti sítě VPN musí používat ověřovací protokol MS-CHAP verze 2 nebo EAP-TLS, jinak nebude možné datové části rámců protokolu PPP šifrovat. Protokol PPTP využívá podkladové šifrování protokolu PPP a zapouzdřuje již zašifrovaný rámec protokolu PPP.

**PPTP** - Protože PPTP vyžaduje dvě síťové relace, je pro něj nesnadné proniknout síťovým [firewallem](https://cs.wikipedia.org/wiki/Firewall). Spojení PPTP jsou ověřována pomocí autentizačních metod [Microsoft](https://cs.wikipedia.org/wiki/Microsoft) [MSCHAP-v2](https://cs.wikipedia.org/w/index.php?title=MSCHAP-v2&action=edit&redlink=1) nebo [EAP-TLS](https://cs.wikipedia.org/w/index.php?title=EAP-TLS&action=edit&redlink=1). Přenos VPN je nepovinně chráněn [MPPE](https://cs.wikipedia.org/w/index.php?title=MPPE&action=edit&redlink=1) šifrováním (Microsoft Point-to-Point Encryption), které je popsáno pomocí standardu [RFC 3078](https://tools.ietf.org/html/rfc3078). Microsoft [MSCHAP-v2](https://cs.wikipedia.org/w/index.php?title=MSCHAP-v2&action=edit&redlink=1) může být narušeno, pokud uživatelé zvolí slabá hesla. Kvalitnější bezpečnostní volbu pro PPTP představuje certifikované [EAP-TLS](https://cs.wikipedia.org/w/index.php?title=EAP-TLS&action=edit&redlink=1).

**L2TP** - Zpráva protokolu L2TP je šifrována pomocí standardu DES (Data Encryption Standard) nebo trojnásobného algoritmu DES (3DES) pomocí šifrovacích klíčů generovaných v procesu vyjednávání protokolu IKE (Internet Key Exchange).

# [Připojení VPN mezi sítěmi](javascript:void(0))

Připojení VPN mezi sítěmi (označované také jako připojení VPN mezi směrovači) umožňuje organizacím směrovat připojení mezi odloučenými pracovišti nebo jinými organizacemi přes veřejnou síť při zachování zabezpečené komunikace. Připojení VPN směrované přes Internet funguje logicky jako vyhrazená linka rozlehlé sítě WAN. Při propojení sítí přes Internet, jak znázorňuje následující obrázek, předává směrovač pakety dalšímu směrovači přes připojení VPN. Připojení VPN funguje vzhledem ke směrovačům jako linka ve spojové vrstvě.

Připojení VPN mezi sítěmi propojuje dvě části privátní sítě. Server VPN poskytuje směrované připojení k síti, ve které se tento server VPN nachází. Volající směrovač (klient VPN) se ověří vůči odpovídajícímu směrovači (serveru VPN) a z důvodu vzájemného ověření se odpovídající směrovač ověří vůči volajícímu směrovači. Pakety, které jsou odesílány z obou směrovačů přes připojení VPN, u připojení VPN mezi sítěmi obvykle nepocházejí z těchto směrovačů.

**Dvě vzdálená místa propojená sítí VPN přes Internet**

