VPN (1) - historie, definice a důvody budování

Termín "VPN" nebo "Virtual Private Network" se používá k popisu širokého spektra řešení, i když přitom není sám předmět přesně specifikován. Tato volnost v terminologii vede ke stavu, kdy termín "VPN" je používán pro označení i dosti různých technologií. V tomto seriálu jsou teoreticky rozebrány různé typy virtuálních privátních sítí z hlediska vhodnosti použití pro specifické účely, jejich přednosti a nedostatky.

Termín "VPN" nebo "Virtual Private Network" se používá k popisu širokého spektra řešení, i když přitom není sám předmět přesně specifikován. Tato volnost v terminologii vede ke stavu, kdy termín "VPN" je používán pro označení i dosti různých technologií. Existence spousty definicí virtuálních sítí umožňuje pak mnoha výrobcům komunikačních produktů směle tvrdit, že jejich produkt je právě VPN.

V tomto seriálu jsou teoreticky rozebrány různé typy virtuálních privátních sítí z hlediska vhodnosti použití pro specifické účely, jejich přednosti a nedostatky.

Historický úvod

Na začátek bych chtěl zmínit několik historických souvislostí. Pojem virtuální sítě se ve větším měřítku začal používat u přepínačů, kde umožňoval na jediné fyzické infrastruktuře (kabeláži) vytvořit několik vzájemně oddělených sítí. Ačkoliv dnešní využití těchto virtuálních sítí je trošku odlišné od původních představ, kdy se předpokládalo, že každé oddělení bude mít svou vlastní virtuální síť napříč celým podnikem, ve své podstatě představují myšlenkového předchůdce virtuálních privátních sítí, kde kabeláž je nahrazena veřejným poskytovatelem datových služeb.

Hlavním impulsem rozvoje VPN pak byl mohutný rozvoj Internetu. Dokud byly firemní pobočky propojeny pevnými linkami nebo frame-relay spoji od zpravidla státního telekomu (tzv. plně privátní sítě), nikdo necítil zvláštní potřebu chránit svá data. Situace se ale výrazně změnila, když vznikla možnost a nabídka levného propojení poboček (nebo připojení uživatele k centrále) přes internet.

Ve své podstatě pak velice podobný problém představuje bezpečné připojení uživatelů na WWW server. Používají se zde podobné techniky virtualizace s tím rozdílem, že zde zpravidla není dopředu jasné, kteří uživatelé se budou připojovat. V případě extranetu se pak volí jeden z těchto dvou přístupů.

Definice

Úplně obecná definice virtuální privátní sítě by mohla znít:

VPN je privátní síť, kde privátnost je vytvořena nějakou metodou virtualizace. VPN může být vytvořena v mnoha variantách - mezi dvěma koncovými systémy, mezi dvěma organizacemi, mezi několika koncovými systémy v rámci jedné organizace nebo mezi více organizacemi pomocí např. globální sítě Internet. Může být vytvořena také přímo mezi aplikacemi a samozřejmě také libovolnou kombinací všech uvedených možností.

Poněkud formální, ale jasná a asi nejpřesnější definice VPN zní:

VPN je komunikační prostředí, ve kterém je řízen přístup ke komunikaci mezi jednotlivými entitami z definovaného souboru, je vytvořeno nějakou formou rozdělení společného komunikačního média, a kde tato nižší vrstva komunikačního média poskytuje síťové služby na ne-exkluzivní bázi.

Jednodušší, tedy jen přibližná, ale zato mnohem méně formální definice by mohla znít:

VPN je privátní síť, vybudovaná v rámci veřejné síťové infrastruktury, jakou je např. globální Internet.

Důvody budování VPN

Pro budování VPN existuje několik důvodů, jejich společným jmenovatelem je požadavek "virtualizace" jisté části komunikace v dané organizaci. Řečeno jinými slovy, požadavek "skrýt" jistou část komunikace (možná i celou) před "ostatním světem" a přitom využít efektivity společné komunikační infrastruktury.

Základní motivace pro budování virtuálních privátních sítí leží v ekonomice. Dnešní komunikační systémy se vyznačují vysokými fixními náklady a relativně nízkými variabilními náklady, závislými na přenosové kapacitě či šířce pásma. V takovémto ekonomickém prostředí je pak finančně výhodné spojit větší počet diskrétních komunikačních služeb do společné výkonné platformy a "rozpustit" tak vysoké pevné náklady mezi velký počet klientů. V duchu této myšlenky je pak vybudování i provoz celé sady virtuálních sítí na společné fyzické komunikační základně levnější než vybudování a provoz fyzicky samostatných diskrétních sítí.

Spojování jednotlivých komunikačních služeb do jedné společné a veřejné platformy má ale své limity, a těmi jsou právě výše zmíněné požadavky na "privátnost" komunikace - požadavky na vzájemné "odstínění" komunikace mezi jednotlivými uživateli či skupinami uživatelů. Náročnost řešení tohoto vzájemného odstínění je pak úměrná výši požadavků na bezpečnost a integritu dat jednotlivých komunikujících klientů či skupin.

VPN (2) – Internet versus plně privátní sítě

Současný globální Internet je pro budování VPN velkou výzvou. Se svojí prakticky celosvětovou dostupností umožňuje snadnou výměnu dat mezi libovolnými připojenými uzly na světě. Tento model všude přítomného Internetu ale nemusí vyhovovat všem potenciálním požadavkům (zajištění kvalitativních parametrů přenosů, dostupnost a spolehlivost, bezpečnost a integrita dat).

VPN a Internet

Současný globální Internet je pro budování virtuálních sítí velkou výzvou. Se svojí prakticky celosvětovou dostupností umožňuje snadnou výměnu dat mezi libovolnými připojenými uzly na světě. Internet je vybudován na jednotném adresovém schématu a směrovací hierarchii, všechny připojené entity sdílejí společnou síťovou infrastrukturu.

Tento model všude přítomného Internetu ale nevyhovuje všem potenciálním požadavkům, speciálně pak požadavkům na bezpečnost privátních dat. Nemusí být z mnoha důvodů přijatelným řešením pro organizaci, která chce využít tuto veřejnou síť pro privátní propojení svých geograficky vzdálených poboček. Těmito důvody mohou být problémy se zajištěním QoS (quality of service - obecně kvalitativní parametry přenosů), dostupnost a spolehlivost, použití veřejných adresových schémat a protokolů, bezpečnost a integrita dat (možnost odposlechu dat).

Plně privátní sítě

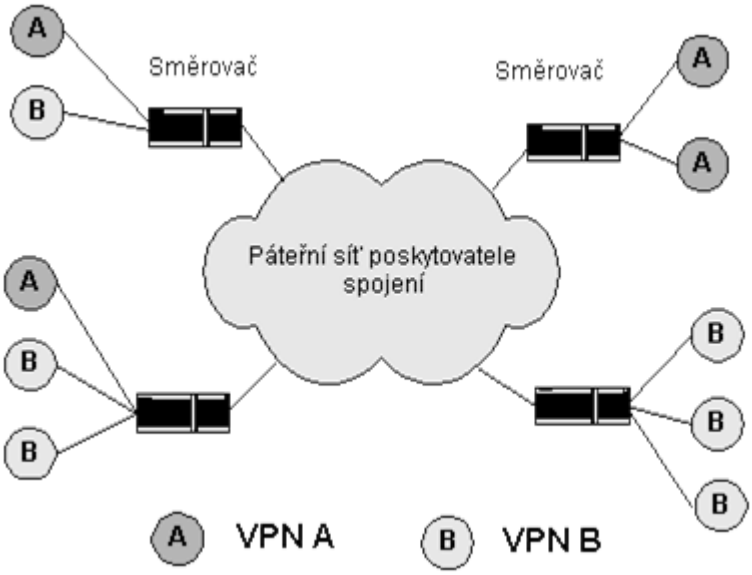
Alternativou k Internetu s všeobecným veřejným přístupem jako základní infrastruktuře pro vybudování VPN je zatím nejběžnější model privátní počítačové sítě - uzavřené síťové prostředí, kde celá infrastruktura, adresové schéma, směrovací hierarchie a správa sítě je dedikována uzavřené skupině uživatelů. Tento model kopíruje vlastní strukturu organizace a fyzicky sestává z lokálních sítí v jednotlivých budovách a pronajatých dedikovaných komunikačních okruhů od poskytovatelů spojových služeb (Frame Relay, ATM) pro propojení geograficky odlehlých lokalit. Vytvořenou síť můžeme pak v terminologii VPN nazvat "plně privátní virtuální sítí", protože tyto dedikované komunikační služby (nižší vrstvy protokolového zásobníku) jsou opět součástí společného přenosového systému.

Vytvoření a hlavně provoz plně privátní sítě nese s sebou ale vysoké finanční náklady na investice do síťové infrastruktury, vyškoleného personálu atd. a předpokládá tedy nést plnou zodpovědnost za provoz síťových služeb. U menších a středních firem nemusí být tato cena odpovídající přínosu plně privátní sítě. Vzniká tak silná potřeba redukce nutné ceny na vytvoření a provoz privátní sítě využitím sdílením přenosových služeb, zařízení i správy sítě.

Nejběžnější VPN

Na obr. 1 je znázorněn příklad nejběžnějšího typu virtuální privátní sítě. Síť A i síť B jsou vytvořeny propojením geograficky odlehlých jednotlivých entit (subsítí) páteřní sítí veřejného poskytovatele spojení nebo Internetem, přičemž obě sítě "nevědí" vzájemně o své existenci. Základní motivace pro vybudování takovéto sítě již byla zmíněna - požadavek na zabezpečení přenášených dat na straně jedné a příliš vysoké náklady na řešení pomocí dedikovaného privátního komunikačního systému.

Nejběžnější typy VPN ale nemusí znamenat jen propojení celých subsítí. VPN lze dále rozdělit či redukovat až na základní spojení typu uzel - uzel. Příkladem tohoto typu VPN je dial-up spojení uživatele se zabezpečenou aplikací, např. on-line bankovní službou, nebo zabezpečené kódované spojení mezi uživatelem a serverem při WWW obchodní transakci. Tento typ dynamických VPN typu uzel - uzel se dnes stává nejpoužívanějším v souvislosti s rozvojem elektronického obchodování.

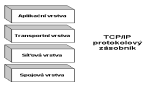


Obr. 1 - nejběžnější typ virtuální sítě

VPN (3) – typologie virtuálních privátních sítí

Existuje několik různých typů virtuálních privátních sítí. V závislosti na požadavcích na funkcí sítě pak můžeme přistoupit k vybudování sítě daného typu několika způsoby. Který způsob zvolíme, závisí na druhu problému, jež má daná VPN řešit, požadavcích na míru bezpečnosti, škálovatelnost řešení a náročnosti na implementaci, správu a údržbu.

Existuje několik různých typů virtuálních privátních sítí. V závislosti na požadavcích na funkcí sítě pak můžeme přistoupit k vybudování sítě daného typu několika způsoby. Rozhodnutí, který způsob zvolit, závisí na druhu problému, který má daná VPN řešit, požadavcích na míru bezpečnosti sítě, požadavcích na škálovatelnost řešení a náročnosti na implementaci, správu a údržbu.



Obr. 2 - Protokolový zásobník TCP/IP

Nejnázornější rozdělení typů VPN se dá provést podle pohledu na funkčnost sítě v relaci s jednotlivými vrstvami protokolového zásobníku TCP/IP, viz obr. 2. Rozeznáváme tak:

- **VPN na síťové vrstvě**. Síťová vrstva obsahuje informace, podle kterých probíhá směrování IP protokolu a práce se směrovacími informacemi je základem pro vytvoření VPN na síťové vrstvě. Některé metody na vybudování těchto sítí budou dále popsány podrobněji:
  - filtrování směrovacích informací;
  - tunelování;
  - šifrování na síťové vrstvě.
- **VPN na spojové vrstvě**. Přenosový síťový systém je použit pro spojení na fyzické a spojové vrstvě, tato síť je funkční analogií konvenční privátní datové síti. Budeme se v dalším věnovat těmto typům VPN na spojové vrstvě:
  - VPN v sítích LANE;

- VPN v sítích MPOA;
- VPN v sítích MPLS.
- **VPN se šifrováním na spojové vrstvě**
- **VPN na transportní a aplikační vrstvě**. Tento typ sítí není příliš běžný, příkladem mohou být e-mailové systémy s kódovaným přenosem zpráv.

VPN na síťové vrstvě

Základem pro vytvoření VPN na síťové vrstvě je práce se směrovacími informacemi. Tyto informace, podle kterých probíhá směrování IP protokolu, obsahuje síťová vrstva. Před podrobnějším pohledem na tento typ VPN objasněme si ve stručnosti rozdíl mezi tzv. "peer" a "overlay" modelem virtuální privátní sítě.

Peer model VPN je takový, ve kterém jsou směrovací výpočty prováděny vždy v každém uzlu na dráze paketu k cíli ("hop-by-hop"), jednotlivé uzly jsou si tak významově rovny ("peer"). Příkladem tohoto peer modelu jsou tradiční sítě, založené na směrovačích. Alternativní "overlay" model je takový, kde směrování na síťové vrstvě není založeno na směrování v každém mezilehlém uzlu na dráze paketu, ale na využití techniky vytváření přímých spojení ("cut-through") na úrovni spojové vrstvy mezi dvěma body sítě. Příkladem tohoto modelu jsou sítě založené na technologii ATM, Frame Relay nebo technice tunelování.

Vedle tohoto základního rozdílu mezi oběma modely zde existuje rozdíl ve škálovatelnosti obou modelů. Na rozdíl od peer modelu mohou u overlay modelu nastat problémy u rozlehlých sítí z důvodů vysoké výpočetní náročnosti.

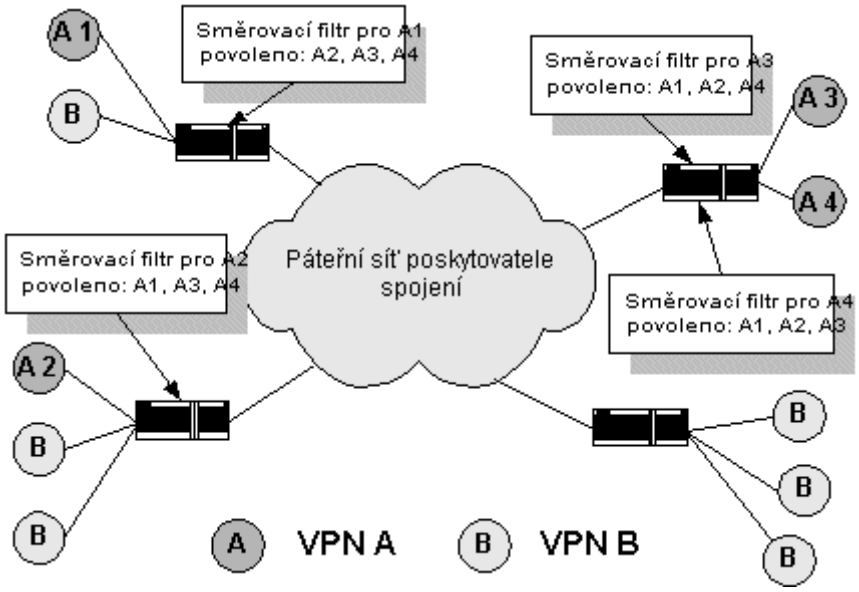
Příště se podíváme na první typ VPN na síťové vrstvě, a to na VPN s filtrováním směrovacích informací.

VPN (4) – filtrování směrovacích informací

Vytváření VPN s filtrováním směrovacích informací je založeno na jednoduchém principu omezení propagace směrovacích informací o dosažitelnosti jiných sítí. Tento model můžeme považovat za typ "peer ", protože jeden směrovač zastupující skupinu uzlů, patřících do VPN, navazuje spojení spředáváním směrovacích informací pouze se vstupním směrovačem sítě poskytovatele spojení a ne se všemi okolními sítěmi.

Vytváření VPN s filtrováním směrovacích informací je založeno na jednoduchém principu omezení propagace směrovacích informací o dosažitelnosti jiných sítí. Tento model můžeme považovat za typ "peer ", protože jeden směrovač zastupující skupinu uzlů, patřících do VPN, navazuje spojení s předáváním směrovacích informací pouze se vstupním směrovačem sítě poskytovatele spojení a ne se všemi okolními sítěmi. Informace o dosažitelnosti vybrané sady sítí, tvořících VPN, tak není propagována okolním sítím, do dané VPN nenáležejícím. To samé platí i v obráceném směru.

Podívejme se znovu na situaci, znázorněnou na obr. 1. Bude-li směrovač poskytovatele spojení filtrovat informace, které získá z jedné sítě, patřící do VPN A tak, že je bude poskytovat pouze ostatním sítím VPN A, ostatní sítě (tzn. sítě VPN B) nebudou mít žádnou explicitní informaci o dosažitelnosti, či vůbec existenci VPN A. Situace je z0jednodušeně znázorněna na obr. 3. Tím, že omezíme znalosti o dosažitelnosti jiných sítí než těch, patřících do stejné VPN, zabráníme kterémukoliv uzlu z dané VPN odpovídat na pakety, jejichž zdroj leží mimo danou VPN. Toto je základní prvek implementace privátních služeb do virtuálních sítí s filtrováním směrovacích informací.



Obr. 3 - VPN s filtrováním směrovacích informací

Tento způsob vytváření VPN má ale své nedostatky. Jedním z potenciálních problémů je obtížné zabránění přístupu z jednotlivých částí VPN na nejbližší implicitní směrovač, sloužící k externí komunikaci se sítěmi mimo danou vlastní VPN - implicitní směrovač dané sítě pro vnější komunikaci s ostatními částmi dané VPN musí být přístupný. Na tomto směrovači je nutná řádná implementace komunikačních filtrů k zablokování veškeré komunikace, směřující mimo danou VPN.

Protože popisované řešení používá společnou páteřní síť se směrovači, jejím jiným omezením je nutnost používání jedinečných adres v rámci celé VPN. Privátní adresy nejde použít bez implementace nějakého způsobu technologie překladu adres (NAT - network address translation). Připojení VPN k vnějšímu světu (např. k Internetu) se pak řeší pomocí specializovaných brán (firewalls), umožňujících zavedení dokonalých bezpečnostních pravidel pro veškerou vnější komunikaci.

VPN (5) – tradiční model tunelování

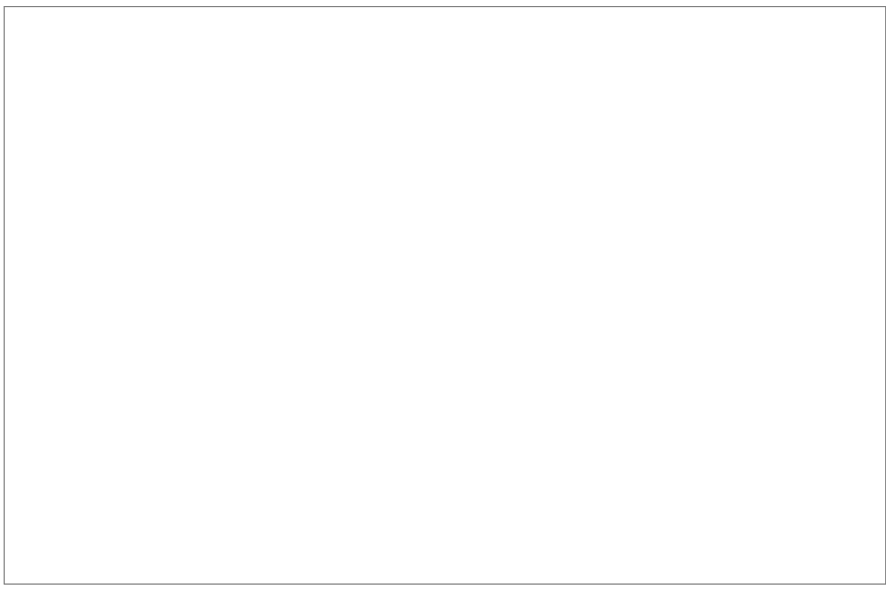
Tunelování je další metodou využívanou při budování virtuálních sítí. Jde o efektivní metodu, při které je specifická část síťové komunikace přenášena po síti speciálně vytvořeným "tunelem". Nejběžněji používaným typem tunelování pro spojení mezi zdrojovým a cílovým směrovačem.je GRE (Generic Routing Encapsulation).

Tunelování je další metodou využívanou při budování virtuálních sítí. Jde o efektivní metodu, při které je specifická část síťové komunikace přenášena po síti speciálně vytvořeným "tunelem". Nejběžněji používaným typem tunelování pro spojení mezi zdrojovým a cílovým směrovačem.je GRE (Generic Routing Encapsulation).

Mechanismus tunelování můžeme považovat za překryvný (overlay) model VPN. Jak jsme již uvedli, u tohoto modelu mohou nastat vážnější problémy se škálovatelností. A to je právě i případ tunelování, obzvláště spojení typu bod - více bodů. Spojení typu bod - bod nejsou natolik problematické, vyjma případu, kdy jeden uzel má vybudovat více spojů typu bod - bod s více koncovými uzly. Zde jde jen o lineární problém škálovatelnosti, zatímco u tunelů typu bod - více bodů, speciálně těch, co využívají vytváření přímých spojení mezi koncovými body, je problém škálovatelnosti podstatně vážnější.

Tunely GRE (Generic Routing Encapsulation)

Tunely GRE jsou budovány směrovači páteřní sítě, které slouží jako vstupní a výstupní body do této páteřní sítě pro jednotlivé části VPN. Pakety, určené pro přenos tunelem, jsou vybaveny zvláštní přídavnou hlavičkou (GRE header) a cílovou adresou, odpovídající směrovači na konci tunelu. Toto zabalení (encapsulation) paketu je v cílovém bodu tunelu odstraněno a paket pak pokračuje ke svému cíli podle informací ve své původní IP hlavičce (viz obr. 4).



Obr. 4 - Schéma GRE (Generic Routing Encapsulation) tunelu

GRE tunely jsou obecně typu bod-bod, tzn., že pro tunel existuje jen jedna zdrojová a obvykle jen jedna cílová adresa. Některé firemní implementace však umožňují konfiguraci bod - více bodů, tedy existenci více cílových adres.

Základním konceptem při tvorbě VPN pomocí tunelování je tedy vytvoření sady tunelů přes společnou sdílenou síť (ať už privátní síť, veřejnou síť poskytovatele spojení nebo Internet). Tato architektura má mnoho přitažlivých vlastností. Jedna z těchto výhodných vlastností se týká adresace. Všechny přístupové body do páteřní sítě, které jsou i koncovými body vytvořených tunelů, používají adresaci a směrování této společné sítě. Technika tunelování používá adresaci cílových bodů tunelů z tohoto adresového prostoru, zatímco pakety přenášené tímto tunelem používají adresy z adresového prostoru VPN. Výsledkem je tedy vzájemné "odstínění" obou adresových prostorů, směrování v obou sítích jsou od sebe izolována, což je jeden ze základních principů použitého overlay modelu. Praktická výhoda, kterou tento přístup nabízí je nabíledni - můžeme použít v rámci VPN privátní adresový prostor a to dokonce vícenásobně v několika VPN, existujících na společné sdílené síti. Zde je významný rozdíl proti VPN s filtrováním směrovacích informací, kde není možné použít privátní adresy, celá VPN musí využívat přidělený jedinečný adresový prostor.

Další významnou předností tunelování je schopnost přenosu tunelem v principu libovolného síťového protokolu. Použitý protokol v rámci dané VPN je tak přenášen přes sdílenou páteř beze změn a je tak v podstatě pro VPN simulována privátní dedikovaná síť se zachováním funkčnosti použitého protokolu i s jeho směrováním. Dochází zde tedy opět ke vzájemnému odstínění obou sítí (společné přenosové sítě a VPN) i z hlediska směrování.

Mohlo by se tedy zdát, že tunelování je ideální metoda pro vytváření VPN. Avšak i zde existují jisté slabší stránky, týkající se zejména administrativní náročnosti a škálovatelnosti při větším počtu tunelů, kvality poskytovaných služeb a výkonnosti. Protože všechny GRE tunely musí být manuálně zkonfigurovány, existuje zde přímá úměra mezi jejich počtem a administrativní náročností při jejich vytváření a údržbě. Stejná úměra platí pro velikost sítě (a množství komunikace na ní) a potřebným výkonem na zpracování paketů v koncových bodech tunelů.

VPN (6) – komutovaný přístup

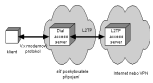
Jiným typem virtuálních sítí, využívajících tunelování, jsou sítě s komutovaným přístupem (VPDN - Virtual Private Dial Networks). Přestože existují různé firemní implementace této technologie, v poslední době je pozornost věnována dvěma základním metodám: tunelům L2TP a PPTP.

Jiným typem virtuálních sítí, využívajících tunelování, jsou sítě s komutovaným přístupem (VPDN - Virtual Private Dial Networks). Přestože existují různé firemní implementace této technologie, v poslední době je pozornost věnována dvěma základním metodám: tunelům L2TP a PPTP. Novější model L2TP vychází ze staršího standardu L2F a ze specifikace PPTP,

předpokládá se však větší rozšíření standardu PPTP, protože je zahrnut ve většině operačních systémů osobních počítačů.

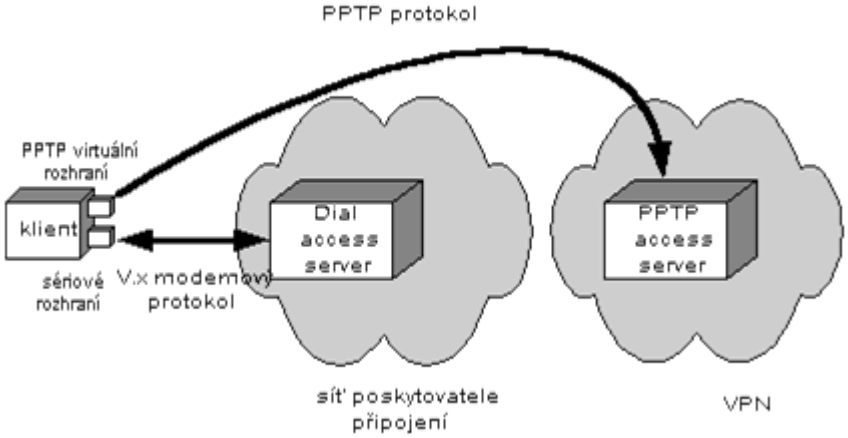
U tohoto typu tunelování se používají dva způsoby inicializace komunikace. První typ je inicializován klientem a jde vlastně o "dobrovolné" tunelování na základě požadavku klienta, vyvolaného specifickými důvody (většinou požadavek na zabezpečení dat). Druhý typ tunelování je iniciován přístupovým serverem, takže je pro klienta "povinný" a nemůže být jím nijak ovlivněn.

Standard L2TP je druhým typem tunelování ("povinným"), vytvoření tunelu probíhá následujícím způsobem. Uživatel se připojí k přístupovému serveru (dial-up server, network access server) a na základě svého konfiguračního profilu (případně zjištěného ze speciálního zabezpečovacího serveru, tzv. policy serveru) proběhne autentizace. Je-li ověření úspěšné, je dynamicky vytvořen L2TP tunel (obr. 5).



Obr. 5 - L2TP tunel

Na druhé straně tunel PPTP (jako "dobrovolný" model) umožňuje koncovému systému vytvoření a konfiguraci individuálního tunelu bod-bod s libovolně umístěným PPTP serverem bez toho, že by se přístupový server účastnil vytvoření tohoto tunelu. V tomto případě se uživatel připojí k přístupovému serveru, zde je ale PPP spojení ukončeno tak, jako v tradičním modelu PPP spojení. Následně klient vytvoří PPTP spojení se žádaným PPTP serverem, jenž je dosažitelný v rámci standardních směrovacích informací a ke kterému má klient patřičná přístupová práva (obr.6).



Obr. 6 - PPTP tunel

Na první pohled jsou oba výše uvedené modely tunelování sice velmi podobné, použití jednoho nebo druhého modelu spočívá v typu problému, který mají řešit, zejména z hlediska řízení přístupových oprávnění.

Srovnání obou modelů

Model PPTP umožňuje uživateli výběr cílového uzlu tunelu až po sestavení PPP spojení. To je důležitá vlastnost v případě, že se cílový uzel často mění. Jinou předností je transparentnost tunelu pro poskytovatele připojení - PPTP komunikace je přenášena sítí stejně jako jakákoliv jiné IP pakety a tunel tak může přesahovat i více sítí. Typickým příkladem této konfigurace je uživatel, připojený k Internetu pomocí lokálního ISP (Internet Service Provider) a navazující překryvné tunelové spojení ze svého počítače až ke vzdálenému cílovému uzlu.

V případě modelu L2TP je PPP spojení ukončeno v síti poskytovatele komutovaného připojení. Tento poskytovatel pak musí spojení předat dále do sítě poskytovatele obsahu, ve které leží cílový uzel. Z pohledu uživatele musí být toto přesměrování transparentní. L2TP model je používán v případech, kdy velcí poskytovatelé obsahu přenechávají přístupové sítě (např. modemové centrály pro komutovaný přístup) jiným firmám. Všechna navázaná spojení se sítí poskytovatele obsahu mohou být z dané lokality soustředěna a přenášena společně po výkonných páteřních spojích. Motivaci pro vytvoření tohoto modelu je možno hledat v

hierarchické architektuře veřejné telefonní sítě.

Rozhodnutí o tom, který model je pro vybudování VPDN vhodnější, je tedy závislé na způsobu řízení vytvoření tunelu - je-li řízeno klientem nebo poskytovatelem spojení. L2TP model poskytuje klientovy VPN komplexní službu, zatímco PPTP model je více distribuovaný.

VPN (7) - šifrování na síťové vrstvě

Šifrovací technologie jsou pro vytváření virtuálních sítí velice efektivní a mohou být využity prakticky na libovolné vrstvě protokolového zásobníku. Nejpoužívanější architektura IPSec (IP Security) využívá síťovou vrstvu a představují v současnosti jedno z nejlepších a nejrozšířenějších řešení pro budování VPN.

Šifrovací technologie jsou pro vytváření virtuálních sítí velice efektivní a mohou být využity prakticky na libovolné vrstvě protokolového zásobníku. Nejpoužívanější architektura IPSec (IP Security) využívá síťovou vrstvu a představují v současnosti jedno z nejlepších a nejrozšířenějších řešení pro budování VPN.

Původně byla tato architektura popsána v RFC 1825-1829. Tyto dokumenty jsou už nyní ale překonané a v širším slova smyslu IPsec v současnosti představuje jakýsi rámec pro souhrn mnoha protokolů, definovaných sdružením IETF. V užším slova smyslu pak IPsec představuje definovanou sadu hlaviček, které jsou přidány za IP hlavičku před hlavičky 4. vrstvy (typicky TCP nebo UDP). Tyto hlavičky pak nesou informace pro zabezpečení obsahu paketu.

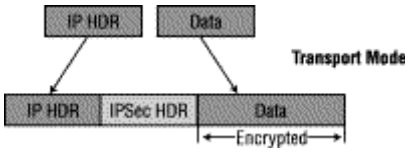
IPsec je založen na vytvoření šifrovaného tunelu mezi dvěma koncovými zařízeními, které mohou představovat např. směrovač, firewall nebo koncovou stanici. Tento standard definuje nejen samotné šifrování, ale i standardní metody pro výměnu a správu klíčů.

Šifrované spojení zajišťuje následující vlastnosti:

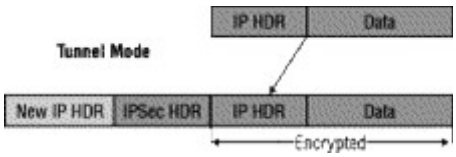
1. utajení (data jsou šifrována);
2. integritu (přijímací strana ověřuje, zda nedošlo během přenosu k manipulaci s daty);
3. ověření pravosti zdroje;
4. anti-replay (přijímací strana rozpozná a odmítne opakované zasílání paketu – jedná se o případnou obranu proti replay útokům).

Největší výhodou IPsec proti jiným šifrovacím systémům je především to, že byl navržen nezávislou organizací (IETF) a jedná se o snadno škálovatelné řešení. Zabezpečení komunikace tak není vázáno na konkrétní aplikaci, ale je přímo součástí síťové infrastruktury. Díky platformní nezávislosti je také dostupné pro různá řešení od směrovačů nebo firewallů až po klientské stanice nebo přístupové servery.

Pro IPsec tunel jsou definovány dva přenosové módy. Z obrázků je zřejmý rozdíl mezi oběma módy. Výhodou transportního módu jsou nižší nároky na přenosové pásmo. Tím, že jsou k dispozici informace o cílovém zařízení, lze rovněž během přenosu paketu sítí aplikovat některé nadstandardní mechanismy (např. QoS). V tunelovacím módu je celý IP datagram šifrován a je vytvořena nová hlavička. Tento mód zase umožňuje, že některá zařízení mohou fungovat jako IPsec proxy. Tyto zařízení pak pošlou rozšifrovaný paket cílovému zařízení. Tímto způsobem lze používat IPsec bez nutnosti implementovat jej na všechna koncová zařízení. V současnosti je nejčastěji používán tunelovací mód.



Obr. 7 - Transportní mód



Obr. 8 - Tunelovací mód

Před vytvořením šifrovaného tunelu je potřeba dohodnout parametry spojení:

1. šifrovací algoritmus (DES, 3DES);
2. hašovací funkci (MD5, SHA);
3. metodu autentikace;
4. dobu životnosti.

Pro konfigurace koncových zařízení se používají dvě metody. Buď lze v obou koncových bodech použít předem definovaný klíč nebo lze využít pro sdílení klíčů certifikační autority. První metoda má výhodu v jednoduchosti konfigurace a přitom neklade žádné nároky na další infrastrukturu, druhá metoda umožňuje poměrně jednoduše vytvářet rozlehlé a komplikované virtuální sítě.

Při definování IPsec tunelu se zároveň vytváří filtry, které určují jaká komunikace bude šifrována a jaká proběhne standardní cestou. Díky tomu, že IPsec je skrytý pro aplikace nad síťovou vrstvou, lze jej použít i v kombinaci s jiným VPN řešením, např. s L2TP nebo GRE tunelem.

VPN (8) - sítě na spojové vrstvě

Použití vlastního přenosového systému a síťové infrastruktury pro vytvoření virtuální privátní sítě patří mezi nejpřímější metody budování VPN, umožňuje přitom budovat na tomto základě nezávislé VPN na vyšší přenosové vrstvě -diskrétní virtuální sítě na síťové vrstvě. Ty pak můžeme považovat za blízkou (či přesnou) funkční analogii konvenčních privátních datových sítí.

Použití vlastního přenosového systému a síťové infrastruktury pro vytvoření virtuální privátní sítě patří mezi nejpřímější metody budování VPN, a umožňuje přitom budovat na tomto základě nezávislé VPN na vyšší přenosové vrstvě - diskrétní virtuální sítě na síťové vrstvě. VPN na síťové vrstvě můžeme považovat za blízkou (či přesnou) funkční analogii konvenčních privátních datových sítí.

Virtuální spojení v sítích ATM a Frame Relay

Konvenční privátní datové sítě používají kombinaci dedikovaných linek (obvodů), pronajatých od veřejného poskytovatele spojových služeb, a privátní komunikační infrastruktury. Tímto způsobem je vytvořena kompletní soběstačná síťová infrastruktura. VPN může být vytvořena v rámci jen této plně privátní infrastruktury, nebo ji může přesahovat. V případě, že přesahuje plně privátní strukturu, VPN se rozprostírá i po pronajatých, dedikovaných linkách (obvodech). Základní charakteristikou pronajatých dedikovaných linek (obvodů) od poskytovatele spojových služeb je nějaký způsob využívání časového nebo frekvenčního multiplexingu a synchronizace vysílání a příjmu dat (synchronní přenosy).

VPN vytvořené na spojové vrstvě volí naproti výše uvedenému jiný přístup. Koncepce VPN na síťové vrstvě předpokládá dosažení plné funkční soběstačnosti a vysoké ekonomičnosti využitím sdílené veřejné přepínané infrastruktury. Sada VPN tak může využívat společnou spojovou infrastrukturu a přepínací prvky, přitom musí být explicitně zajištěna vzájemná "neviditelnost" těchto sítí, a to jak přímá tak nepřímá. Obecně tyto sítě operují na třetí a vyšší vrstvě (dle OSI modelu), zatímco použitá "infrastruktura" je tvořena sítěmi ATM a Frame Relay.

Základní rozdíl v architektuře mezi virtuálními a dedikovanými obvody spočívá v neexistenci časové synchronizace přenosů, navíc zde ani nemusí existovat dedikovaná přenosová cesta. Vysílající uzel také nemá apriori žádnou znalost dostupné přenosové kapacity virtuálního obvodu, protože ta je závislá na celkových požadavcích ostatních simultánních přenosů. Proto může na rozdíl od dedikovaných obvodů docházet k přetížení sítě tvořené virtuálními obvody.

Významnou výhodou veřejných přepínaných sítí (sítí poskytovatelů přenosových služeb) je jejich velká flexibilita. Většina uživatelů si pronajímá virtuální obvody z ekonomických důvodů a součástí smlouvy je samozřejmě i dohoda o kvalitě poskytovaných služeb, která umožňuje specifikovat konkrétní technické parametry sítě podle požadavků zákazníka.

V sítích Frame Relay se např. používá pojem CIR (Committed Information Rate), sloužící jako referenční hodnota pro kontrolu velikosti přenosové rychlosti ve vstupním bodu sítě. Překročí-li rychlost dohodnutou hodnotu CIR, vstupní rámce jsou sice dále sítí akceptovány, jsou ale označeny jako DE (Discard Eligible). Takto označené rámce pak mohou být jako první zahozeny, dojde-li na jejich cestě sítí k přetížení (je překročena max. vstupní rychlost na přepínači a dojte k přetečení vyrovnávacích pamětí).

Výše uvedené charakteristiky sítí s virtuálními obvody platí i pro sítě ATM (Asynchronous Transfer Mode). Stejně jako u sítí Frame Relay, i u sítí ATM není používána synchronizace datových přenosů mezi vysílačem, sítí a přijímačem. Obdobně se i používá vstupní funkce na kontrolu rychlosti vstupního proudu buněk, které mohou být označeny v případě překročení dohodnuté rychlosti indikátorem CLP (Cell Loss Prority) a při přetížení sítě jsou tyto buňky jako první zahozeny.

Architektura sítí s virtuálními obvody na spojové vrstvě nabízí vysoce kvalitní alternativu k sítím pevných dedikovaných obvodů. Různé technologie pak umožňují využití těchto sítí různými způsoby, třeba až po přímou emulaci pevných linek při nutnosti konstantní přenosové rychlosti a garantovaného max. zpoždění.

VPN (9) - sítě pomocí LAN Emulace

Za zvláštní typ VPN můžeme považovat i virtuální sítě, vytvořené technologií LAN Emulace. Ačkoliv technologie virtuálních sítí vznikla původně v prostředí Ethernetových přepínačů, nic nebrání jejímu použití i v sítích ATM. V heterogenních sítích, tvořených jak segmenty sdíleného či přepínaného Ethernetu, tak technologií ATM, lze aplikovat VLAN dvěma způsoby.

Za zvláštní typ VPN můžeme považovat i virtuální sítě, vytvořené technologií LAN Emulace. Ačkoliv technologie virtuálních sítí vznikla původně v prostředí Ethernetových přepínačů, nic nebrání jejímu použití i v sítích ATM. V heterogenních sítích, tvořených jak segmenty sdíleného či přepínaného Ethernetu (to nejčastěji, plus FDDI a Token Ring), tak technologií ATM, lze aplikovat VLAN (Virtual LAN) dvěma způsoby:

- Je-li technologie ATM použita pouze na páteřní přepínače, tzn., že v síti nejsou žádné koncové uzly ATM, je toto prostředí páteře ATM pro virtuální sítě naprosto transparentní. Připojené LAN přepínače komunikují mezi sebou (pakety označenými členstvím v dané VLAN) bez toho, že by si "uvědomovaly" existenci ATM sítě mezi sebou. Tento jednoduchý případ ale není v reálných sítích častý.
- Častějším případem je stav, kdy i sdílené servery jsou připojeny k páteři přímým ATM připojením. Abychom zajistili členství v některé VLAN i těmto uzlům, musíme použít technologii emulovaných LAN (LANE - LAN Emulation).

Jak je již zřejmé z názvu, základní funkcí LANE je emulace LAN nad ATM sítí. LANE protokol definuje rozhraní pro stávající protokoly vyšší, tzn. síťové vrstvy. Pakety těchto síťových protokolů jsou pak posílány přes ATM síť zapouzdřeny v jednom ze dvou možných LANE MAC rámcích. Řečeno jinými slovy, LANE protokol způsobuje, že ATM síť vypadá jako síť typu Ethernet nebo Token Ring - je jen podstatně rychlejší.

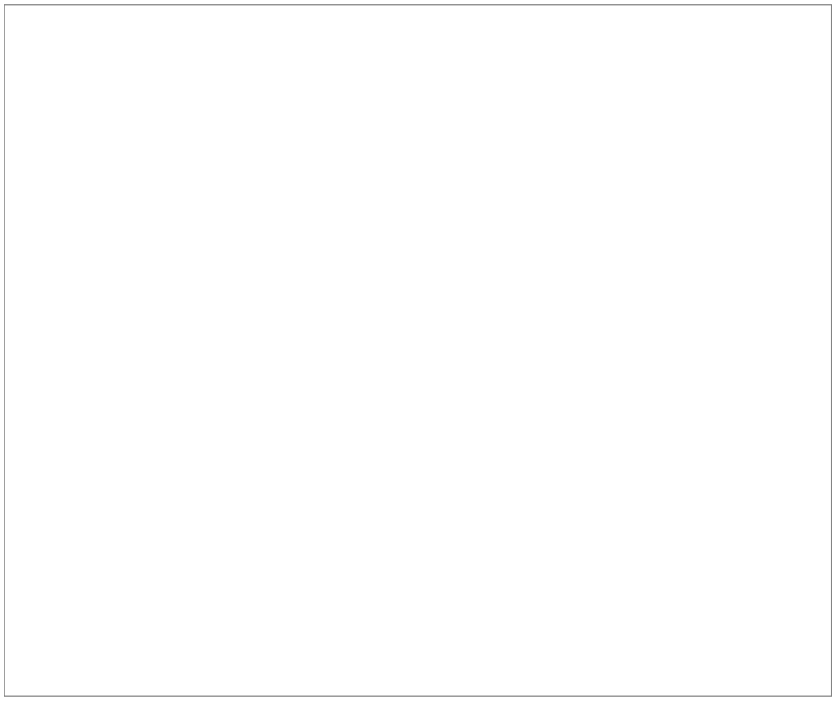
Základními prvky LANE jsou LES (LAN emulation server), poskytující mapování mezi MAC a ATM adresami, a LEC (LAN emulation client), rozhraní, které musí obsahovat každý člen ELAN (emulované LAN) - okrajové přepínače ATM a koncové uzly ATM. Jednotlivé LEC v okrajových přepínačích mohou jako proxy zastupovat standardní uzly, k těmto přepínačům připojené.

LES poskytuje dle požadavků jednotlivých LEC překlad mezi MAC a ATM adresami, takže LEC mohou komunikovat mezi sebou přímo po ATM síti a zprostředkovat tak přímou komunikaci přes páteř ATM jednotlivým klasickým uzlům, připojeným k okrajovým přepínačům.

Protože LEC může být členem více ELAN, standard LANE umožňuje vytvoření více

překrývajících se virtuálních sítí. Tak mohou uzly z různých ELAN přistupovat ke společným síťovým zdrojům bez nutnosti průchodu přes směrovač.

Členy ELAN mohou být jen uzly ATM, zatímco členy VLAN mohou být jak uzly ATM, tak i uzly na standardních segmentech. Na členy ELAN tak můžeme pohlížet jako na podmnožinu VLAN. Vzájemný vztah obou sítí názorně zobrazuje obrázek č. 7.



Obr. 9 - Vzájemný vztah virtuálních a emulovaných LAN v sítích ATM

Propojování ELAN

Vytváření vícenásobných ELAN na jedné ATM síti vyvolává i potřebu jejich propojování - jak mezi sebou, tak se stávajícími LAN a WAN sítěmi. Tak jako mezi všemi virtuálními sítěmi, i mezi ELAN je jediná možná komunikace pomocí směrovače. Nejběžnější způsob je přímo pomocí ATM směrovačů - tj. směrovačů s výkonnými ATM rozhraními. Často se používá tzv. one-armed router, směrovač jen s jedním ATM rozhraním. Na tomto jednom fyzickém rozhraní je implementován vícenásobný LEC, každý pro jednu ELAN.

Směrování datových paketů pak probíhá stejným způsobem jako u standardních sítí. Jednotlivým ELAN jsou totiž přiřazeny různá čísla sítě (např. IP Subnet Number). Podle adresy cíle LEC pak pozná, že paket není lokální (cíl není na stejné ELAN) a pošle jej na svůj default router, který samozřejmě musí být členem stejné ELAN.

Tento směrovač po obdržení paketu určí ze svých směrovacích tabulek cílovou ELAN. Je-li směrovač jejím členem, přesměruje do ní daný paket, v případě one-armed routeru po tom stejném fyzickém rozhraní, jakým byl paket přijat (ale jiným LEC do jiné ELAN). V případě více ELAN na jednom rozhraní je ale nevýhodou možnost vzniku úzkého místa sítě z hlediska propustnosti, stejně tak existence nebezpečného místa z hlediska poruchovosti.

VPN (10) - sítě s protokolem MPOA

Do standardu MPOA (Multiprotocol over ATM) se koncem minulého desetiletí vkládaly velké naděje. Měl jako první přinést onu požadovanou integraci směrování s ATM technologií, neboli umožnit lepší spoluprácí ATM sítí se sítěmi jiného typu. Ačkoliv dnes již rozvoj sítí MPOA již není zdaleka tak aktuální, nemůžeme je v našem teoretickém přehledu vynechat.

Do standardu MPOA (Multiprotocol over ATM) se koncem minulého desetiletí vkládaly velké naděje. Standardu, který měl jako první přinést onu požadovanou integraci směrování s ATM technologií, neboli umožnit lepší spoluprácí ATM sítí se sítěmi jiného typu. Ačkoliv dnes již rozvoj sítí MPOA již není zdaleka tak aktuální, nemůžeme je v našem teoretickém přehledu

vynechat.

Na rozdíl od LAN Emulace je v sítích MPOA (Multiprotocol over ATM) použit úplně jiný přístup ke směrování paketů. Zavedení pojmu virtuální směrovač umožňuje velkou škálovatelnost a flexibilitu řešení, které přinesl MPOA standard. Co se tedy za tímto pojmem skrývá? "Virtuální směrovač" emuluje funkci tradiční sítě se směrovači, přitom ale eliminuje výkonnostní omezení této sítě, dané principem směrování. Toto omezení vyplývá z nutnosti výpočetně zpracovávat každý paket v každém směrovači na cestě mezi koncovými uzly (hop-by-hop routing).

Naproti tomu je mezi uzly s MPOA schopností ustanoveno přímé spojení přes ATM síť, a to i když náleží do různých logických podsítí (a v případě LAN emulace nebo IP over ATM bychom museli použít směrovač). Zjednodušeně řečeno, MPOA identifikuje datové toky a mapuje je přímo do virtuálních spojení VC. Tato technika je také nazývána "cut-through" nebo "zero-hop" routing.

Pakety tak již nejsou na své cestě zpracovávány směrovači a vedle podstatného zvýšení výkonnosti dochází ke zmenšení transportního zpoždění, které je navíc více deterministické.

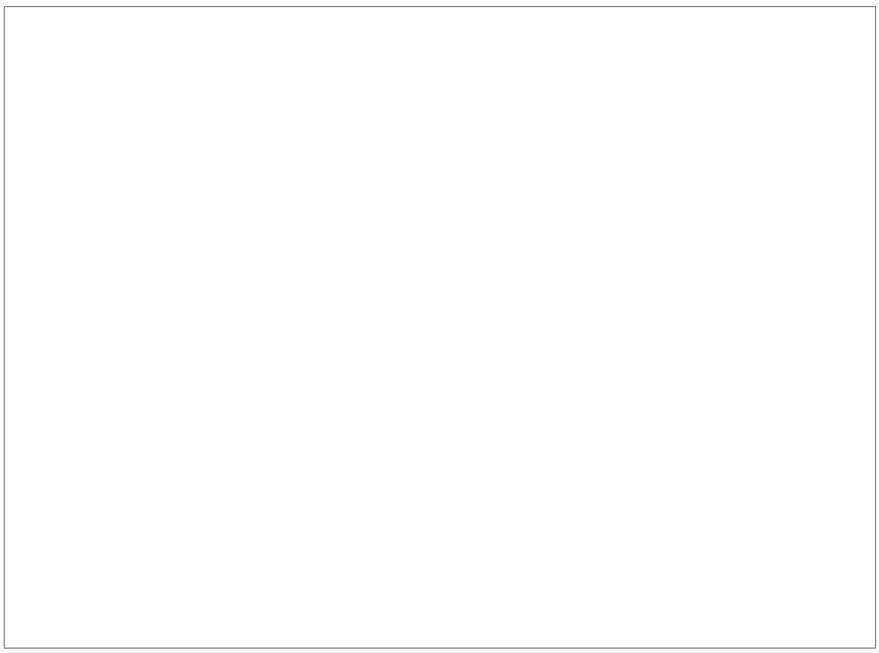
Základní principy MPOA

Obecný koncept MPOA standardu vychází z rozdělení funkcí tradičního multiprotokolového směrovače, tzn. oddělení výpočetního zpracování směrování od vlastního fyzického směrování (přenosu) paketů mezi jednotlivými subsítěmi. Výpočetní zpracování (správa adres, topologické informace atd.) je prováděno tzv. MPOA serverem (MPS), zatímco vlastní fyzické směrování paketů provádí tzv. MPOA Clients (MPC). Této architektura bývá také nazývána distribuované směrování.

MPS pracuje jako samostatný směrovací server s ATM připojením nebo je tato funkce implementována do ATM přepínače. Funkce MPC je zabudována do okrajových ATM přepínačů a do připojených ATM stanic. Tím je provedena fyzická separace mezi zařízeními, která provádí směrovací výpočty a zařízeními, která provádí vlastní fyzické přenosy.

Zapojení vlastně celé ATM infrastruktury do fyzického procesu směrování datových toků představuje z výkonnostního hlediska obrovskou výhodou v porovnání s omezenou propustností sběrnic jednotlivých směrovačů. Navíc přenos standardních protokolů jako je IP po ATM síti umožňuje využití služeb pro řízení kvality přenosu (QoS) pomocí řídících protokolů jako je např. RSPV.

Na obr. 10 je základní schéma MPOA sítě. Server MPOA musí pracovat s celým protokolovým zásobníkem běžných směrovacích protokolů. Okrajové ATM přepínače jsou optimalizovány na přesměrování síťové komunikace na 2. i 3. vrstvě a to spolu se standardními, relativně levnými ATM přepínači, tvořícími vlastní ATM přenosovou infrastrukturu, umožňuje vytvořit efektivní výkonné virtuální sítě se směrováním "bez přeskoků". Centralizace směrování (jeho výpočetní a administrativní složky) do jednoho místa samozřejmě také velmi zjednodušuje jeho správu, což je významný aspekt tohoto řešení.



Obr. 10 - Základní princip MPOA sítě

Základním nedostatkem MPOA sítě z pohledu VPN je její výhradní omezení na ATM jako přenosové technologie na spojové vrstvě. Ze širšího pohledu velkých hybridních VPN sítí je toto omezení pro použití MPOA značně limitující. Jiným možným problémem je omezení škálovatelnosti MPOA sítí. Důvodem je možnost vzniku suboptimálních směrování na síťové vrstvě.

Velká přednost MPOA technologie spočívá v dynamickém vytváření virtuálních obvodů mezi koncovými uzly. Na rozdíl od těžkopádného statického přístupu, obnášejícího velký podíl manuální konfigurace a údržby jednotlivých přepínacích elementů, použití MPOA přináší významné snížení provozních nákladů - jak již bylo ale výše uvedeno, vyžaduje jednotné ATM prostředí, což není případ velkých hybridních VPN.

VPN (11) - virtuální sítě MPLS

MPLS (Multiprotocol Label Swapping) je hybridní technologii, která integruje dva základní přístupy k tvorbě VPN - použití směrování na síťové vrstvě a přepínání paket po paketu na straně jedné a virtuální obvody na spojové vrstvě a přepínání podle datových toků na straně druhé.

MPLS (Multiprotocol Label Switching) je hybridní technologii, která integruje dva základní přístupy k tvorbě VPN - použití směrování na síťové vrstvě a přepínání paket po paketu na straně jedné a virtuální obvody na spojové vrstvě a přepínání podle datových toků na straně druhé.

Cílem tohoto článku není podrobný rozbor technologie MPLS (Multiprotocol Label Switching), ale popis možnost tvorby MPLS/VPN, proto se omezíme jen na její stručný popis a zařazení do kontextu našeho teoretického přehledu VPN sítí.

MPLS je hybridní technologii, která integruje směrování na síťové vrstvě s tzv. přepínáním podle návěští (značek), v anglické terminologii label switching/swapping. Toto přepínání podle návěští je definováno jako nový princip pro přenos dat, který umožňuje jejich plynulý přenos mezi koncovými uzly (a jednotlivými vstupně/výstupními porty přepínačů). Pro identifikaci dat (datových toků), která se mají přenést, se používají speciální návěští.

Jsou tak integrovány dva základní přístupy k tvorbě VPN - použití směrování na síťové vrstvě a přepínání paket po paketu na straně jedné a virtuální obvody na spojové vrstvě a přepínání podle datových toků na straně druhé.

MPLS není svázána s žádnou specifickou technologií spojové vrstvy (2. vrstva OSI modelu), může pracovat s libovolným médiem, po kterém se dají přenášet síťové pakety mezi uzly, definovanými svými síťovými adresami (síťový - rozuměj definovaný na 3. vrstvě OSI). MPLS

poskytuje jen základní mechanismy, které mohou být implementovány různými způsoby. Tyto mechanismy mj. zahrnují:

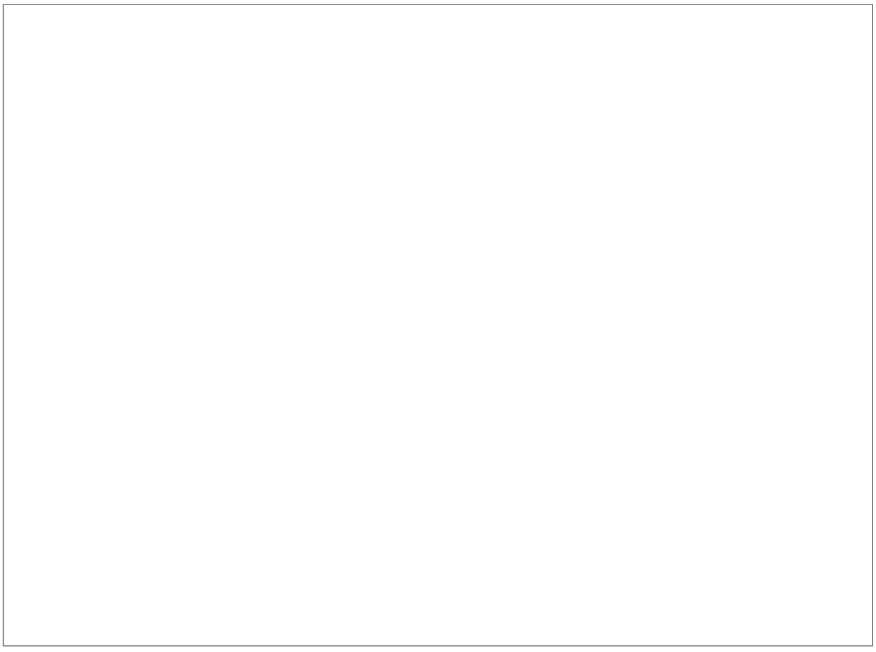
- přidělení krátkých návěští pevné délky specifikovaným datovým tokům;
- zjednodušení přenosu paketů pomocí identifikace těchto návěští;
- možnost přímého využití přenosových mechanismů 2. vrstvy, které poskytují spojově orientované technologie jako ATM a Frame Relay;
- procedury a protokoly pro přidělování návěští jednotlivým datovým tokům a distribuci těchto informací mezi jednotlivými zúčastněnými uzly.

Z hlediska VPN má pak vytvořená MPLS virtuální privátní síť tři základní složky:

1. řízenou distribuci směrovacích informací jako způsob vytvoření VPN a řízení vzájemného propojení mezi nimi;
2. použití identifikátorů pro jednotlivé virtuální sítě (VPN ID) a obzvláště jejich provázanost s IP adresami k jejich (potenciální) změně na unikátní adresy;
3. použití přepínání podle značek (MPLS) na směrování paketů cestami, vytvořenými pomocí bodů (1) a (2).

Pro konkrétní implementaci VPN v prostředí MPLS je možné zvolit různé přístupy. Základní architektura MPLS je tedy založena na aplikaci návěští na paket, vstupující do sítě MPLS. Tím je pro daný paket určena sekvence přepínačů, kterými musí projít na své cestě mezi okrajovými uzly sítě, a výstupní směrovač. Rozšířením této architektury z hlediska VPN je zavedení pojmu per-VPN global identifier (nebo též Closed User Group identifier). Tento globální identifikátor může být přiřazen paketu při vstupu do MPLS sítě a pak použit jako index ve směrovací tabulce pro VPN k určení počátečního návěští. Na výstupu ze sítě MPLS je pak identifikátor CUG znovu použit jako index v globální tabulce VPN k určení výstupního směrovače. Konkrétní způsob práce směrovacích protokolů s identifikátorem CUG je stále ještě předmětem vývoje.

Příklad MPLS VPN sítí je na obr. 11, kde tabulka ukazuje vyváření virtuálních MPLS obvodů.



Obr. 11 - VPN s přepínáním podle značek (MPLS)