Fakulta Elektrotechniky a Informatiky Slovenskej Technickej Univerzity

Katedra Telekomunikácií

Point – to – Point Tunneling Protocol (PPTP)

Martin Kovács, Vladimír Hangáč
23.11.2007

3. Ročník
TLK 2

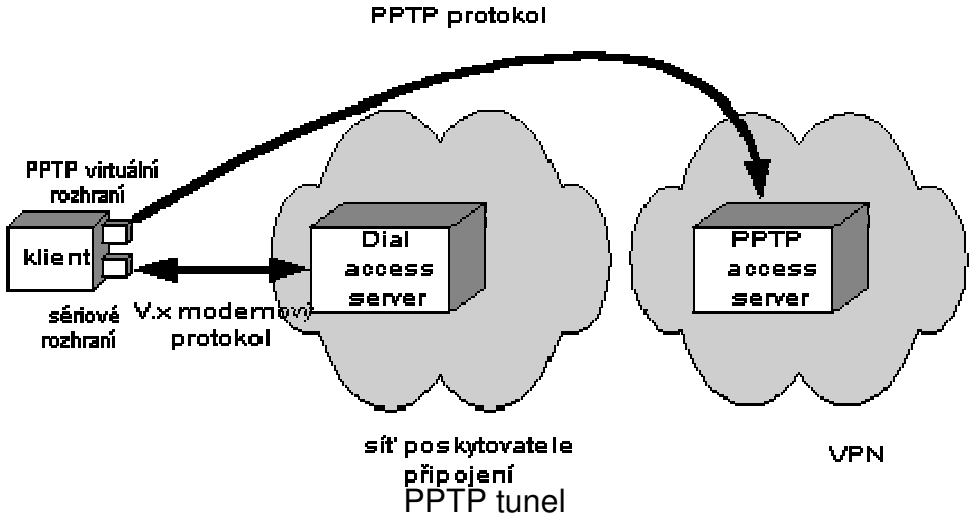
Úvod

Najskôr na úvod pár slov o VPN pripojení. VPN server chráni komunikáciu medzi klientami chránenej siete a autorizovanými klientami inych sietí pomocou šifrovania. V závislosti na celkovom objeme prenášaných dát môže byť táto služba samostatná, alebo može byť jeho funkcia vykonávaná na vnútornom smerovači alebo firewalle. V praxi u velkých objemoch dát sú tieto zariadenia nahradzované špeciálnymi aktívnymi prvkami, tzv. koncentrátormi. Bezpečnosť tohoto serveru závisí na striktnej autentifikácii a autorizácii.

Na trhu sú v súčasnosti tri hlavné štandardy pre VPN. Standart Point-to-Point tunneling protocol (PPTP) podporovaný firmou Microsoft a Ascend. Microsoft spojil sily s firmou CISCO a vznikol hybridný protokol označený ako L2TP, obidva fungujú na druhej vrstve referenčného modelu OSI, tzv. spojovej vrstve . Treťou variantou je štandart IPSec integrovaný do IP protokolu. Každá z týchto technológii má svoje výhody a nevýhody. PPTP a L2TP sú vhodnejšie do viacprotokolového prostredia, napríklad kombinácia IP prevádzky s IPX NetWare a NetBEUI. IPSec je vhodnejší pre čisté IP prostredie, pretože pracuje na tretej vrstve. Konkrétne implementácie jednotlivých protokolov boli podrobené rôznej kritike, vždy si treba overiť, či je daný protokol vhodný na riešenie ktoré chceme nasadiť a neboli preň zistené vážne chyby.

PPTP pripojenie klientovej IP adresy využíva dynamicky pridelený TCP port , na strane serverovej IP adresy využíva rezervovaný port pre PPTP číslo 1723. PPTP control connection , prenáša PPTP call control , spravuje prenos dát a udržiava PPTP tunel. Toto obsahuje pravidelné vysielanie PPTP Echo-Requestu a PPTP Echo-Replay pre zistenie chyby spojenia medzi PPTP klientom a serverom.

Využíva sa TCP pripojenie zname ako PPTP control connection na vytvorenie, udržiavanie a ukončenie tunelu a modifikovanú verziu Generic Routing Encapsulation (GRE) uzatvára PPP rámce ako tunelové dáta. Obsah PPP rámcov môže byť zakódované, komprimované alebo oboje.



PPTP tunel

PPTP umožnuje koncovému systému vytvorenie a konfiguráciu individuálneho tunelu bod-bod s lubovoľne umiestneným PPTP serverom, bez toho, aby sa prístupový server účastnil na vytvorení tohoto tunelu. V tomto prípade sa užívateľ pripojí k prístupovému serveru, kde je ale PPP spojenie ukončené tak, ako v klasickom modely PPP spojenia. Následne klient vytvorí PPTP spojenie so žiadaným PPTP serverom, ktorý je dosiahnuteľný v rámci štandartných smerovacích informácii a ku ktorému má klient patričné prístupové práva.

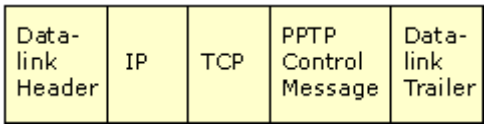
Nám zadaný protokol umožnuje užívateľovi výber cielového uzlu tunela až po zostavení PPP spojenia. To je doležitá vlastnosť v prípade, že sa cielový uzol často mení. Inou prednosťou je transparentnosť tunelu pre poskytovateľa pripojenia – PPTP komunikacia je prenášaná sieťou rovnako ako ostatne IP pakety a tunel tak môže presahovať i viac sietí. Typickým príkladom tejto konfigurácie je užívateľ , pripojený k internetu pomocou lokálneho ISP(Internet Service Provider) a naväzujúci prekrýcajúce tunelové spojenie zo svojho počítača až ku vzdialenému cieľovému uzlu.

Štruktúra paketu:

16	32 bits
Length	PTPP message type
Magic cookie	
Control message type	Reserved 0
PPTP header structure	

Autentifikácia pri vytváraní PPTP – VPN pripojenia využíva ten istý autentifikačný mechanizmus ako PPP pripojenie ako Extensible Autenthification Protocol (EAP), Microsoft Challenge-Handshake Authentification Protocol (MS-CHAP), CHAP, Shiva Password Authentification Protocol (SPAP) a Password Authentification Protocol (PAP). PPTP zdedí kódovanie alebo kompresiu, poprípade oboje od PPP rámcov z PPP pripojenia.

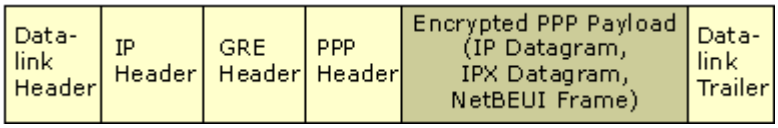
Štruktura PPTP control connection packet:



Typy správ PPTP Call Control a Connection Management

Start-Control –Connection-Request	Posiel a ju PPTP klient k naviazaniu pripojenia.
Start-Control-Connection-Reply	Posiela ho PPTP server ako odpoved na Start-Control-Connection-Request
Outgoing-Call-Request	Posiela ho PPTP klient na vytvorenie PPTP tunela. V Outgoing –Call-Request je obsiahnuté Call ID, ktoré je použité v GRE hlavičke na identifikáciu tunelovej premávky, alebo špecifického tunelu.
Outgoing-Call-Reply	Posielaná PPTP serverom ako odpoveď na Outgoing-Call-Request
Echo-Request	Odoslaná PPTP klientom alebo PPTP serverom ako komunikáciu udržiavajúci mechanizmus. Pokiaľ nedostane odpoveď, tak PPTP tunel je pravdepodobne ukončený.
Echo-Reply	Odpoved na Echo-Request
WAN-Error-Notify	Posielaná PPTP serverom k všetkým VPN klientom pre indikáciu na rozhraní PPP PPTP servera
Set-Link-Info	Posielané PPTP klientom alebo serverom pre zrealizovanie PPP možností.
Call-Clear-Request	Žiadost posielaná PPTP klientom o ukončení tunela
Call-Disconnet-Notify	Posielaná PPTP serverom ako odpoveď na Call-Clear-Request že tunel bude ukončený, aj keď sa ukončí na podnet PPTP servera
Stop-Control-Connection-Request	Posielaná PPTP klientom, alebo serverom s informáciou, že Control Connection bude ukončené
Stop-Control-Connection-Reply	Odpoveď na Stop-Control-Connection-Request

Konštrukcia PPP rámcov



Inicializačný balíček PPP je zakódovaný a spojený s PPP hlavičkou na vytvorení PPP rámca. Rámec je potom spojený s modifikovanou GRE hlavičkou . GRE je zdokumentovaný v RFC 1701 a RFC 1702 a bol vytvorený aby zabezpečoval jednoduchý, lahký a univerzálne použitelný mechanizmus balenia dát pre posielanie cez IP internetové siete. GRE je klientom IP protokolu, využíva port 47.

Pre PPTP je GRE hlavička modifikovaná v týchto bodoch:

- Overovací bit indikuje že je pritomné 32 bitové pole
- Kľúčové pole je nahradené 16-bit dĺžkou rámca a 16-bit Call ID field. Call ID je vytvorené PPTP klientom pri vzniku PPTP tunela.
- Je pridané 32-bitové overovacie pole

Za GRE hlavičkou, typ protokolu je zadaný ako 0x880B, the EtherType hodnota pre PPP rámec.

V IP header je obsiahnutá príslušná IP adresa PPTP servera a klienta.

Kódovanie Data-Link header a trailer

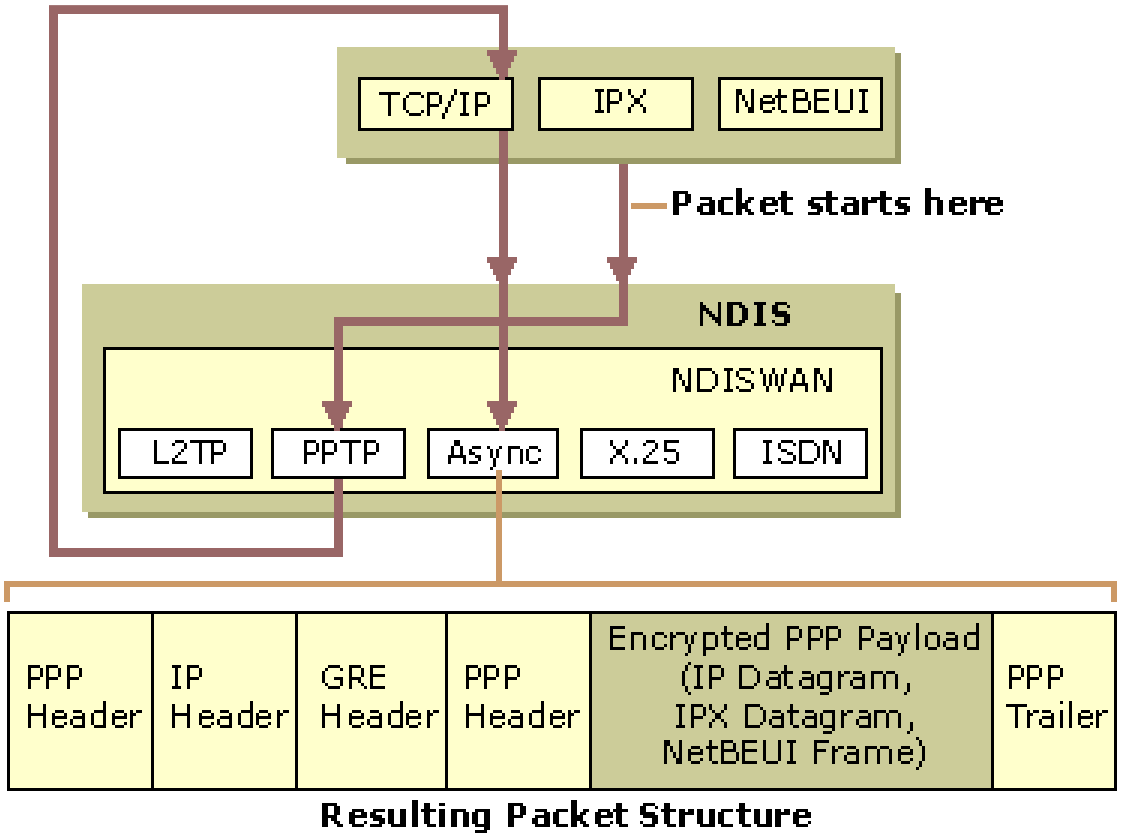
Pre posielanie cez LAN alebo WAN linku, IP rámec musí mať začiatok i koniec. Využíva Data-Link vrstvou na strane odchádzajúceho fyzického rozhrania. Napríklad, ked IP datagramy sú poslané cez ethernetové rozhranie, IP datagram je spojený s ethernetovou hlavičkou a koncom. Ked IP datagramy sú posielané cez point- to-point WAN linku, ako analogová, alebo ISDN, IP datagram je spojený s PPP hlavičkou a koncom.

Spracovanie PPTP dát

- Spracuje a odoberie data-link header and trailer
- Spracuje a odoberie IP hlavičku
- Spracuje a odoberie GRE a PPP hlavičky
- Dekóduje a odkomprimuje PPP obsah
- Spracuje obsah na prijatie, či preposlanie ďalej

PPTP Pakety a Windows XP

Obrázok nám ilustruje cestu tunelových dát v systéme Windows XP cez analógový modem od VPN klienta po VPN server. Postupnosť krokov je nasledovná:



1. IP diagram, IPX datagram, alebo rámec NetBEUI je priradený k príslušnému protokolu k virtuálnemu rozhraniu, ktoré reprezentuje VPN pripojenie používajúce Network Driver Interface Specification (NDIS)
2. NDIS priradí paket k NDISWAN, ktorý zakóduje, resp. skomprimuje dáta a poskytne PPP hlavičku pozostávajúcu len z ID pola PPP Protokolu.Nie sú pridávané žiadne značky alebo rámcové kontrolné sekvencie (FCS). To zabezpečí že kompresiu pola adresy a kontroly sa vykoná Link Control Protocol (LCP) v nasledujúcej fáze.

3. NDISWAN postúpi dáta k PPTP protocol driver-u, ktorý uzavrie PPP rámec s GRE hlavičkou. V GRE hlavičke je jednoznačne identifikované Call ID k identifikácii tunela.
4. PPTP protokol driver potom posunie packet k TCP/IP protocol driver
5. TCP/IP protocol driver uzavrie PPTP dáta s IP hlavičkou a pošle daný paket na interface reprezentovaný dial-up pripojením k lokálnemu ISP pomocou NDIS
6. NDIS posunie paket k NDISWAN, ktorý zabezpečuje PPP hlavičky a konce
7. NDISWAN posunie výsledný PPP rámec do prislúchajúcemu WAN miniport driver reprezentujúcemu dial-up-ový hardware.