SLOVENSKÁ TECHNICKÁ UNIVERZITA
Fakulta elektrotechniky a informatiky
Katedra Telekomunikácií

Point to point tunneling protocol

Školský rok: 2007/2008

Martin Figura
Marek Solčanský
3.roč.

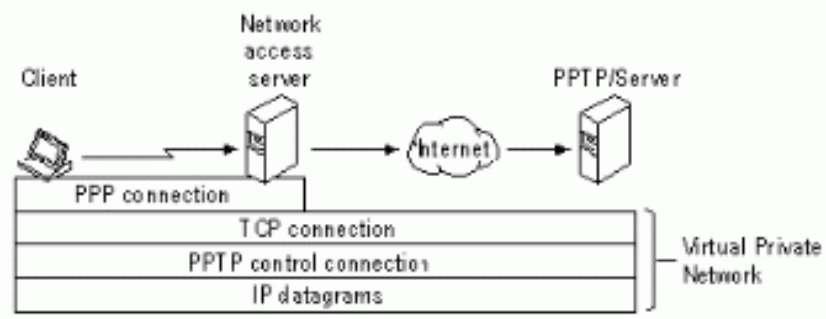
PPTP - je sieťový protokol ktorý zaisťuje prenos dát od vzdialeného účastníka k privátnemu serveru napríklad podniku pomocou vytvorenia virtuálnej siete (VPN) cez protokol TCP/IP. PPTP podporuje multiprotokol, virtuálne siete, cez verejné siete ako je internet. Sieťová technológia PPTP je rozsah vzdialeného prístupu PPP, definovaná v dokumente od IETF (Internet Engineering Task Force) pod názvom „Poit to Point Protocol fot the Transmissions of Multiprotocol Datagrams over Point to Point Links“ dokumentovaná ako RFC 2637. Tento protokol zapuzdruje PPP pakety do IP datagramov a prenáša ich cez internet, alebo inú verejnú sieť TCP/IP sieti. PPTP môže byť použitý aj v privátnych sieťach LAN to LAN. PPTP je rozšírením PPP. Tento dokument je pre administrátorov, vývojárov, ktorí potrebujú rozumieť ako PPTP môže byť poskytovaný pre lacné riešenia pripojení, alebo prístupov.

1. Základné pojmy PPTP

analógový kanál- spojený okruh s komunikačnými cestami ktoré dokážu prenášať 3,1 Khz audio v každom smere.
digitálny kanál - spojený okruh s komunikačnými cestami, ktoré dokážu prnášať digitálnu informáciu v každom smere.
Call – spojenie alebo skúšobné spojenie medzi dvoma koncovými zariadeniami na PSTN alebo ISDN (telefónny hovor medzi dvoma modemami).
Control Connection – Control connection je vytvorené pre každý pár PAC, PNS a funguje nad protokolom TCP. Spravuje tunel a spojenia pridelené tunelu.
Network Access Server (NAS)
Zariadenie poskytujúce užívateľom prístup do siete na požiadanie, tento prístup je typu point-to-point cez linky PSTN alebo ISDN.
PPTP Access Concentrator (PAC) - zariadenie pripojené k jednej alebo viacerým PSTN alebo ISDN linkám, schopné používať protokol PPP a riadiť protokol PPTP. PAC potrebuje iba implementovať TCP/IP na prepúšťanie prevádzky do viacerých PNS, môže tiež tunelovať non-IP protokoly.
PPTP Network Server (PNS) - PNS funguje na univerzálnych počítačových/serverových platformách. PNS spravuje server-side protokolu PPTP. Pretože je protokol PPTP kompletne nad protokolmi TCP/IP a je nezávislý od hardvérového rozhrania, PNS môže používať rôzne kombinácie IP hardvérového rozhrania vrátane LAN a WAN zariadení.
Session – PPTP je spojovo orientovaný protokol, PNS a PAC udržiavajú stav každého užívateľa, ktorý je pripojený k PAC. Session je vytvorená po pokuse o vytvorenie koncového PPP spojenia medzi "dial" užívateľom a PNS. Datagramy spojené so session sú posielané cez tunel medzi PAC a PNS.
Tunnel – tunel je definovaný párom PNS-PAC, tunelový protokol je definovaný modifikovanou verziou Internet Generic Routing Encapsulation (GRE) protocol. Tunel prenáša datagramy PPP medzi PAC a PNS. Viaceré session sú multiplexované v jednom tuneli. Kontrolné spojenie riadi vznik, uvoľnenie, udržiavanie session a samotného tunelu.

2. PPTP a VPN

Počítače bežiace v tomto procese môžu používať PPTP na bezpečné pripojenie do privátnej siete ,ako vzdialený účastník, cez verejnú sieť ako je internet. PPTP môže tiež byť používaný počítačmi pripojenými v privátnej sieti na vytvorenie VPN. Dôležitý znak v používaní PPTP je podpora VPN použitím verejnej telekomunikačnej siete (PSTNs). PPTP zjednodušuje a znižuje cenu pre rozvoj podnikových sieti, pre vzdialený prístup, pre vzdialených alebo mobilných užívateľov, pretože to poskytuje cez verejne telefónne linky a internet. Eliminuje taktiež potrebu drahých komunikačných serverov lebo ju možno použiť v PSTN linkách. Zvyčajne sú tam 3 počítače spojené pomocou PPTP:
PPTP klient
NAS (Network Access Server)
PPTP server
Typické využitie PPTP je, keď vzdialený užívateľ potrebuje prístup do privátnej siete použitím Internet Service Provider (ISP). Užívateľ sa pripája na NAS cez ISP. Jedinečné spojenie, kde klient môže prenášať pakety cez internet. NAS používa TCP/IP protokol pre všetky spojenia do internetu.



obr. 1: spojenie klienta s PPTP servom

3. Network Access Server

PPTP umožňuje oddeliť funkcie Network Access Serveru (NAS) použitím architektúry klient-server. Obvykle sú NAS serverom implementované tieto funkcie:
1. Fyzické pripojenie do PSTN alebo ISDN a riadenie externými modemami alebo koncovými adaptérmi.
2. Logické ukončenie spojenia Point-to-Point protokolu (PPP) a Logical Control protokolu (LCP).
3. Zapojenie sa do overovacích protokolov PPP.
4. Agregácia kanálov a riadenie zväzkov pre PPP Multilink protokol.
5. Logické ukončenie rôznych PPP Network Control protokolov (NCP).
6. Multiprotokolové smerovanie(routing) a premosťovanie(bridging) medzi rozhraniami(interfaces) NAS.

PPTP rozdeľuje tieto funkcie medzi PAC(PPTP Access Concentrator) a PNS(PPTP Network Server). PAC zodpovedá za funkcie 1, 2 a môže obsahovať aj funkciu 3. PNS môže obsahovať funkciu 3 a zodpovedá za funkcie 4, 5, 6. Protokol na prenos protokolových dátových jednotiek(PDUs) PPP medzi PAC a PNS rovnako aj kontrola a riadenie spojenia je určené protokolom PPTP. ***Výhody oddelenia funkcií NAS:***

- Flexibilita IP address management
- Riešenie problému „multilint hunt-group splitting".
- Podpora non-IP protokolov pre "dial" siete za IP sieťami. Toto umožňuje protokolom Appletalk a IPX, aby boli tunelované cez IP-only provajdera. PAC nemusí vedieť spracovávať tieto protokoly.

4. Control Connection Protocol - špecifikácia

Správy kontrolného spojenia sú použité pri vytváraní a skončení session. Prvá skupina správ kontrolného spojenia sa používa na udržiavanie samotného kontrolného spojenia. Kontrolné spojenie je iniciované PNS alebo PAC po vytvorení TCP spojenia. Všetky nasledujúce správy kontrolného spojenia sú posielané cez vytvorené TCP spojenie medzi daným párom PNS-PAC. Každá správa kontrolného spojenia PPTP začína pevnou 8-bajtovou hlavičkou, ktorá obsahuje tieto časti: celková dĺžka správy, typ PPTP správy a "Magic Cookie".

PPTP rozoznáva 2 typy správ Control connection:
a) kontrolné správy (Control Messages)
b) riadiace správy (Management Messages)

a) Kontrolné správy

1 Start-Control-Connection-Request – sa používa na zriadenie riadiaceho spojenia.
2 Start-Control-Connection-Reply – posiela sa ako odpoveď na predošlú správu
3 Stop-Control-Connection-Request – hovorí o tom, že riadiace spojenie bude ukončené
4 Stop-Control-Connection-Reply – potvrdzuje prijatie Stop-Control-Connection-Request
5 Echo-Request – slúži na udržiavanie riadiaceho spojenia. Je to tzv. "keep-alive" správa
6 Echo-Reply – posielaná ako odpoveď po prijatí Echo-Request
7 Outgoing-Call-Request – ja posielaná z PNS do PAC. Oznamuje, že sa zostavuje odchodzie spojenie(volanie). PAC dostane všetky potrebné informácie na zostavenie spojenia a na následnú reguláciu prenosu dát.
8 Outgoing-Call-Reply – potvrdzuje prijatie predch. správy. Zároveň informuje o výsledku zostavenia spojenia a tiež obsahuje informácie slúžiace na reguláciu prenosu dát
9 Incoming-Call-Request – je posielaná z PAC do PNS. Oznamuje, že sa zostavuje príchodzie spojenie(volanie) z daného PAC. PAC podrží hovor dokým nedostane od PNS odpoveď
10 Incoming-Call-Reply – touto správou PNS potvrdzuje prijatie Requestu od PAC. Obsahuje informáciu či má PAC odpovedať na hovor(že môže byť obslúžený, zastavený or not).
11Incoming-Call-Connected – je posielaná z PAC do PNS po prijatí Reply. Obsahuje dodatočné informácie o hovore, ktoré nemohli byť poslané v Requeste

12 Call-Clear-Request – správa je posielaná z PNS do PAC. Informuje o tom, že volanie bude ukončené
13 Call-Disconnect-Notify – je posielaná z PAC do PNS buď ako odpoveď na Request alebo má informovať, že hovor bol ukončený. Správa obsahuje aj dôvod ukončenia hovoru
14 WAN-Error-Notify – je posielaná z PAC do PNS. Informuje o chybe, ktorá nastala na WAN rozhraní, teda na rozhraní podporujúcom PPP. Táto správa je posielaná len keď vznikne chyba a nie častejšie ako raz za 60 sekúnd.
15 Set-Link-Info – posielaná z PNS do PAC. Obsahuje nastavenia PPP relácie. Pretože nastavenia sa môžu počas hovoru meniť, PAC musí byť schopné meniť nastavenia pre konkrétny hovor dynamicky.

Pomocou správ Start-Control-Connection-Request a Start-Control-Connection-Reply sa určí, ktorá verzia protokolu kontrolného spojenia sa použije. Maximálna dĺžka paketov enkapsulovaných v GRE je 1532 bajtov bez zahrnutia hlavičiek IP a GRE.

b) Riadiace správy

Používajú sa na zriadenie a zrušenie relácií (spojení) medzi užívateľmi. Prvá sada správ sa používa na správu riadiaceho spojenia. Riadiace spojenie sa vytvára ako TCP spojenie medzi PAC a PNS. Môže byť iniciované ktoroukoľvek stranou. Tento protokol neurčuje aké parametre sa majú použiť pri zriaďovaní TCP spojenia. Riadiace správy sa posielajú cez toto spojenie ako dáta.

Start Control Connection Request

Správa používaná na vytvorenie spojenia medzi PNS a PAC. každé spojenie PNS-PAC potrebuje priradenie kontrolného spojenia pred začatím. kontrolné spojenie musí byť začaté predtým ako budú vyslané ostatné PPTP správy.

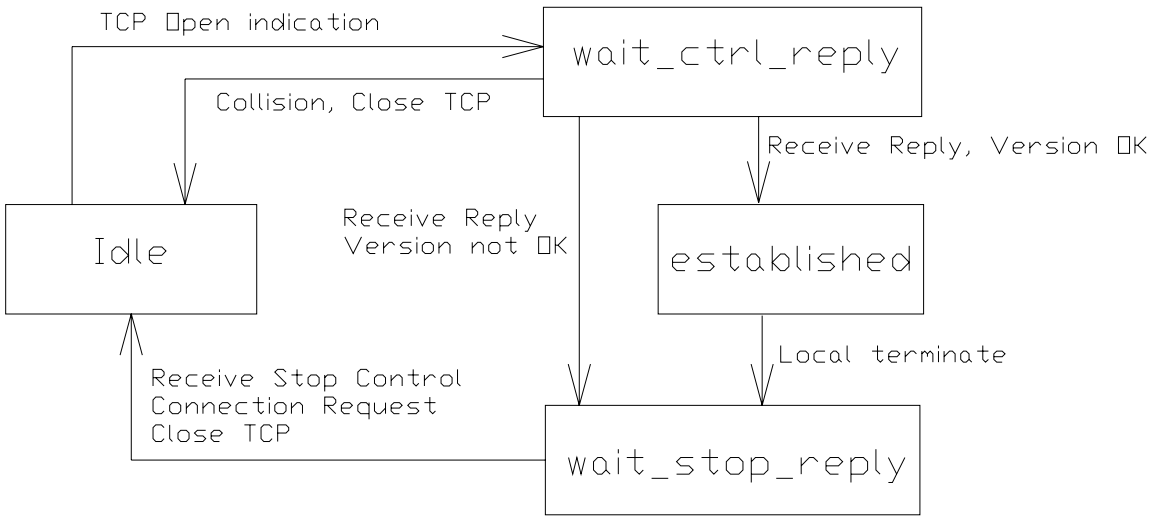
16	32
Length	PPTP message type
Magic cookie	
Control message type	Reserved 0
Protocol Version	Reserved 1
Framing capability	
Bearing capability	
Maximum channels	Firmware revision
Host name (64 bajtov)	
Vendor string (64 bajtov)	

obr.2: Start Control Connection Request pole

length - úplná dĺžka tejto správy, vrátane celej PPTP hlavičky
PPTP massage type – 1 pre control massage
Magic Cookie - je vždy nastavený na hodnotu 0x1A2B3C4D. Jeho hlavnou úlohou je umožniť prijímaču zistiť, či je správne zosynchronizovaný s dátovým tokom TCP. Nemôže sa použiť na znovu-zosynchronizovanie dátového toku TCP, ale strata synchronizácie musí viesť k okamžitému ukončeniu TCP session kontrolného spojenia.
Control massage type – 1 pre Start control Connection Request
Reserved0 – totot políčo musí byť 0
Protocol Version – Verzia PPTP protokolu ktorú si užívateľ praje používať
reserved1 – toto políčko musí byť 0
framing Capabilities – 1 – podporovaný asynchrónny vstup
2 – podporovaný synchrónny vstup
Bearer Capabilities – 1 – podporovaný analógový vstup
2 podporovaný digitálny vstup
Maximum Channels – konečné číslo individuálnych PPP sekcií ktoré PAC podporuje. tato hodnota má byť nastavená na 0. musí to byť ignorované PAC
Firmware Revision – číslo používania PAC, vydaný PAC, albo verziou PNS PPTP.
Host name – 64 bajtové políčko obsahujúce DNS meno používaného PAC albo PNS. ak menej ako 64, zvyšok má byť plnený hodnotou 0.
Vendor name – 64 bajtové políčko obsahujúce vendor špecifikácie opisujúci typ prebiehajúceho použiatia PAC.

Control Connection – nadviazanie spojenia
Keďže PPTP funguje na TCP prenose, z hľadiska inicializácie na zostavenie spojenia nerozlišujeme či sa jedná o PAC alebo PNS. Obe zariadenia môžu inicializovať vytvorenie spojenia. No medzi PAC a PNS môže byť len jedno kontrolné spojenie. Rozlišujeme teda len medzi tvorcom a príjemcom spojenia.

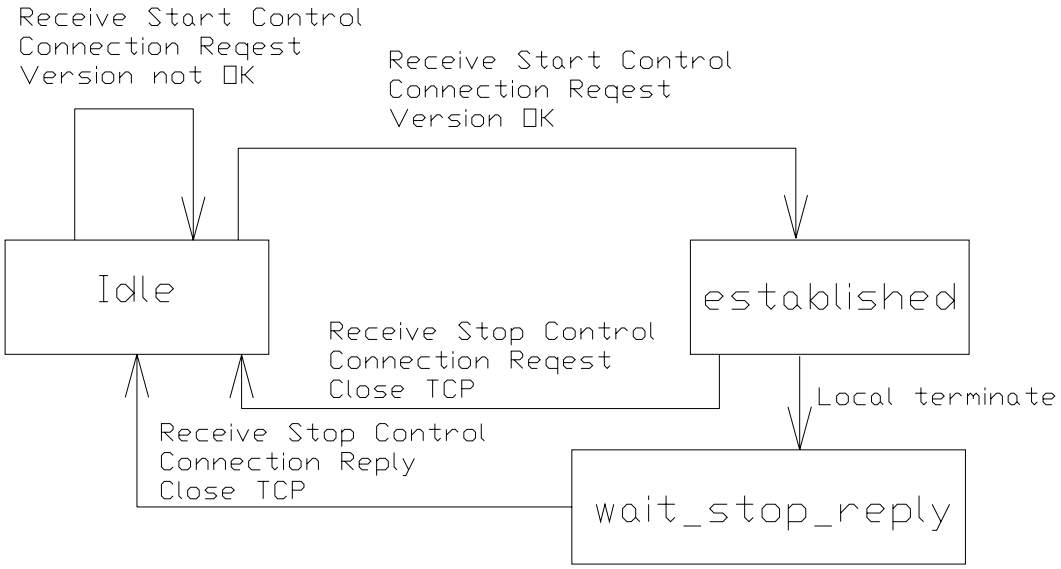
Tvorca:



obr.3: vytvorenie kontrolného spojenia od tvorcu spojenia

Idle (nečinnosť, nečinný) – tvorca spojenia sa pokúša vytvoriť TCP spojenie. Ak sa mu to podarí, pošle správu Start-Control-Connection-Request a prejde do stavu wait_ctl_reply
wait_ctl_reply (čakanie na odpoveď) – tvorca spojenia pozerá, či sa ten uzol, na ktorý sa pripájal, nepokúšal spojiť s ním. Ak áno, vznikne kolízia. Vlastne oba uzly dostanú Requesty. Vyhrá ten uzol, ktorý má vyššiu IP adresu. Ak je všetko v poriadku a tvorca prijme Start-Control-Connection-Reply, skontroluje akú verziu protokolu používa príjemca spojenia. Ak je to podporovaná verzia (tvorca ju pozná), tak tvorca prejde do stavu established. Ak verzia nie je podporovaná (je príliš stará) pošle sa správa Stop-Control-Connection-Request a tvorca prejde do stavu wait_stop_reply
established (zostavené spojenie) – vytvorené spojenie môže byť zrušené lokálne alebo prijatím správy Stop-Control-Connection-Request. Ak je spojenie lokálne ukončené, tak tvorca musí poslať Stop-Control-Connection-Request a prejsť do stavu wait_stop_reply. Ak tvorca prijme správu Stop-Control-Connection-Request, tak odpovie poslaním správy Stop-Control-Connection-Reply a ukončí TCP spojenie.
wait_stop_reply (čakanie na potvrdenie ukončenia) – ak je prijatá správa Stop-Control-Connection-Reply, TCP spojenie sa môže ukončiť a riadiace spojenie je nečinné

Príjemca:



obr.4: vytvorenie kontrolného spojenia od príjemcu

Idle (nečinnosť, nečinný) – Príjemca spojenia čaká že na porte 1723 na otvorenie TCP spojenia. Po vytvorení TCP spojenia a prijatí správy Start-Control-Connection-Request sa otestuje verzia protokolu tvorcu spojenia. Ak je podporovaná, tak sa vyšle správa Start-Control-Connection-Reply a príjemca prejde do stavu established. Ak verzia nie je podporovaná, príjemca pošle Stop-Control-Connection-Reply, zavrie TCP spojenie a zostane v stave idle.
established (zostavené spojenie) - vytvorené spojenie môže byť zrušené lokálne alebo prijatím správy Stop-Control-Connection-Request. Ak je spojenie lokálne ukončené, tak stanica musí

poslať Stop-Control-Connection-Request a prejsť do stavu wait_stop_reply. Ak stanica prijme správu Stop-Control-Connection-Request, tak odpovie poslaním správy Stop-Control-Connection-Reply a ukončí TCP spojenie.
wait_stop_reply (čakanie na potvrdenie ukončenia) - ak je prijatá správa Stop-Control-Connection-Reply, TCP spojenie sa môže ukončiť a riadiace spojenie je nečinné.

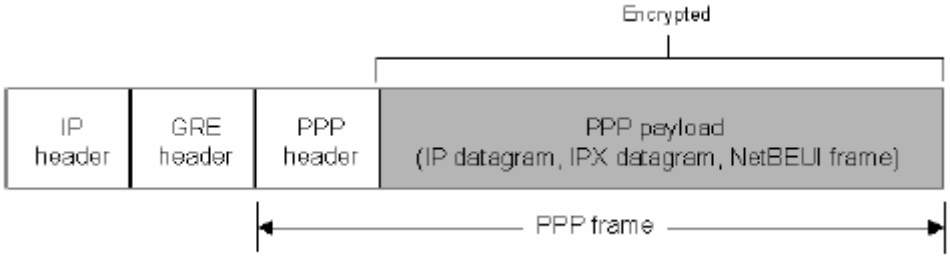
Control Connection - ukončenie spojenia
Kontrolné spojenie by malo ukončiť TCP spojenie pod sebou pri týchto okolnostiach:
- Keď sa nepodarilo nadviazať kontrolné spojenie, bude po 60 sekundách čakania na správu Start-Control-Connection-Request alebo Start-Control-Connection-Reply ukončené.
- Keď je kontrolné spojenie nadviazané a peer 60 sekúnd nedostal kontrolnú správu, mal by poslať správu Echo-Request. Ak po ďalších 60 sekundách nepríde Echo-Reply, bude kontrolné spojenie ukončené.

5. Tunelový protokol

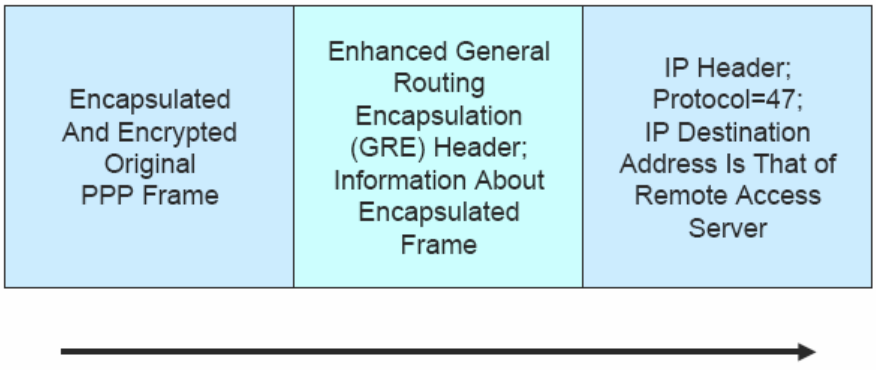
PPTP vyžaduje vytvorenie tunelu pre každý komunikujúci PNS-PAC pár. Tento tunel slúži na prenos PPP paketov užívateľskej session zahŕňajúcej daný PNS-PAC pár. To, ku ktorej session patrí konkrétny PPP paket je určené kľúčom, ktorý je prítomný v hlavičke GRE.
Týmto spôsobom potom môžu byť PPP pakety multiplexované a demultiplexované cez tunel medzi daným párom PNS-PAC. Hodnota kľúča je určená cez kontrolné spojenie pri procedúre vytvorenia spojenia.

GRE hlavička - obsahuje aj potvrdzovacie informácie a informácie o poradí, ktoré zabezpečujú istú úroveň kontroly zahltenia a detekcie chýb cez tunel. Oproti kontrolnému spojeniu je použitá na určenie parametrov rýchlosti a buffera, ktoré sa používajú na riadenie toku PPP paketov pre danú session cez tunel. PPTP nešpecifikuje algoritmy, ktoré sa majú použiť pre kontrolu zahltenia a kontrolu toku.

Formát dátovej správy - dáta prepravované protokolom PPTP sú dátové pakety protokolu PPP. PPP pakety sú prepravované medzi PAC a PNS, potom sú enkapsulované do paketov GRE, ktoré sú potom prepravované cez IP. Enkapsulované PPP pakety sú v podstate dátové pakety PPP bez elementov špecifických pre médium. Neobsahujú žiadne HDLC flagy, vkladanie bitov, kontrolné znaky. Cez tunel sa neposielajú žiadne CRC.



obr.5: Všeobecná štruktúra IP paketov posielaných cez tunel medzi PAC a PNS



obr.8: Postup enkapsulácie PPP paketu

6. Flow control

Riadenie toku dát v tuneli pomocou metódy **sliding window** vykonáva prostredníctvom obsahu **Enhanced GRE header** (rozšírená hlavička GRE), konkrétne políčok **Acknowledgement** a **Sequence number**.

Acknowledgement je potvrdením, že GRE paket s určitým poradovým číslom v poriadku dorazil do cieľa. Políčko definujúce protokol je nastavené na hodnotu 880B a hlavička ďalej obsahuje aj info ktorému spojeniu daný PPP paket prislúcha, dĺžku paketu, call ID a poradové číslo.

Sequence number je na začiatku každej session nastavené na nulu a každému paketu (danej session), ktorý obsahuje dáta, je pridelené nasledujúce poradové číslo. Protokol umožňuje, aby boli potvrdenia prepravované spolu s dátami a tým je celý protokol účinnejší, čo vedie k potrebe menších bufferov pre pakety.

Sliding Window metóda zabezpečí efektívny prenos dát, čo má za následok menší potrebný buffering paketov. Jej dôležitým parametrom je Time out - dáva priestor na vyprázdnenie buffra, zotavenie v prípade straty dát alebo ich potvrdení. Vykonáva teda tieto funkcie:
- inicializovanie veľkosti okna. Hoci každá zo strán oznamuje maximálnu hodnotu veľkosti svojho okna, na začiatku sa veľkosť okna nastavuje na polovičnú od tej, ktorú žiadal príjemca výzvy na komunikáciu (minimálne veľkosť 1paketu).
- zmenšovanie okna
- zväčšovanie okna
- pretečenie okna - ak príjemcovo okno pretečie s množstvom prichádzajúcich paketov, tie ktoré sú navyše sa vyhodia. Toto sa však nestane ak sú sliding window procedúry vykonávané súbežne na vysielači aj prijímači.
- potvrdenie viacerých paketov

Môže sa stať, že paket sa po ceste od PNS do PAC stratí, prípadne príde až za nasledujúcim paketom. Potom ak sa už vyšle potvrdenie toho nasledujúceho a príde ten stratený, nesmie sa už

potvrdzovať. Takýto paket by mal byť potom odstránený, pretože PPP sa vie vysporiadať so stratou paketu ale nevie pakety preusporiadať.

Rozšírená hlavička GR - Oproti hlavičke GRE je rozšírená o nové pole - číslo potvrdenia(Acknowledgement Number), ktoré slúži na určenie, či konkrétny GRE paket alebo skupina paketov dorazila na opačný koniec tunela. Táto potvrdzovania schopnosť sa nepoužíva pri retransmisii paketov, ale na určenie rýchlosti posielania paketov cez tunel pre danú session.

<table>
<tr><td colspan="10">0</td><td colspan="10">1</td><td colspan="10">2</td><td colspan="2">3</td></tr>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td></tr>
<tr><td>C</td><td>R</td><td>K</td><td>S</td><td>s</td><td colspan="3">Recur</td><td>A</td><td colspan="3">Flags</td><td colspan="3">Ver</td><td colspan="20">Protocol Type</td></tr>
<tr><td colspan="16">Key (HW) Payload Length</td><td colspan="16">Key (LW) Call ID</td></tr>
<tr><td colspan="32">Sequence Number (Optional)</td></tr>
<tr><td colspan="32">Acknowledgment Number (Optional)</td></tr>
</table>

obr.9: rozšírená hlavička GRE

7. Zabezpečenie protokolu

Autentifikácia – je to overenie oprávnenosti prístupu užívateľa.Vykonávaná je pomocou už existujúcich Win NT Remote Access Service (RAS) protokolov, a to sú Challenge Handshake Authentication Protocol (CHAP), Microsoft Challenge Handshake Authentication Protocol (MS-CHAP), a Password Authentication Protocol (PAP). Môže prebiehať aj na strane prístupu k providerovi ak je to potrebné.
Kódovanie dát – je vykonávané pomocou RAS "shared-secret" to znamená že obe strany poznajú klúč ktorý slúži ako základ pre šifrovaciu metódou RC4 pomocou 40, 56 alebo 128 bitového pseudonáhodne generovaného kľúča, ktorý je výsledkom samotnej autentifikácie(treba poznať prihlasovacie heslo z ktorého sa vypočíta kľuč). Kódovanie prebieha uplatnením logickej funkcie XOR medzi sekciami dát a kľúčom.

Najnovšie výsledky však ukazujú, že PPTP je dokázateľne veľmi citlivá na útoky. A to napríklad pomocou ultra-vysoko rýchlostnej pasword cracking tool aplikácie nazvanej ASLEAP, ktorá nabúrava autentifikáciu PPTP klienta. Bola vyvinutá na dôkaz, že zabezpečenie VPN komunikácii nie je až také dobré ako hlásal Microsoft a Cisco, 3Com. Bezpečnosť sa dá zvýšiť použitím zložitejích hesiel, ktoré však používa málokto, preto sa PPTP dostalo do situácie keď už bezpečnosť dát jeho používateľov nie je zaručená. Na ukážku,bežný dnešný počítač s aplikáciou ASLEAP dokáže za sekundu preveriť 45miliónov variácii hesla. Po zverejnení tejto aplikácie Microsoft odporučil buď použitie iného typu autentifikácie - napr. TLS alebo uprednostnenie úplne inej technológie, napr. IPsec, čo v podstate zastavilo ďalší vývoj PPTP.Napriek tomu množstvo ľudí PPTP aj kvôli širokej softwarovej podpore a jednoduchosti naďalej používa.

Zabezpečenie dát posielaných cez tunelované PPP spojenie je určené protokolom PPP ako autentifikácia PPP. Je možné zmocniť sa TCP spojenia pod kontrolným kanálom, pretože správy

kontrolného kanála nie sú autentifikované ani chránené. Tiež je možné vytvárať falošné kontrolné správy a meniť pravé správy bez možnosti odhalenia. Pakety GRE tvoriace samotný tunel nie sú šifrované a pretože začiatočné dohadovania PPP sú prepravované cez tunel, je možné ich odpočúvať alebo meniť. Pokiaľ nie sú PPP dáta šifrované, tak ich môže niekto zachytávať, čítať alebo meniť.

Používanie PPTP z Firewallom - činnosť firewallov a PPTP sa vzájomne neovplyvňuje. Ak je na PNS serveri nejaký firewall, spojenie bude nadviazané medzi ním a PAC klientom a to na možných portoch:
TCP/na porte 1723, UDP/ NetBios-NS, UDP/ NetBios-DGM, IP/ protokol používa ID 47
Tieto porty boli vyhradené organizaciov Internet Assigned Numbers Authority (IANA).

Použitá literatúra a zdroje

[1] http://tools.ietf.org/html/rfc2637
[2] http://www.microsoft.com/technet/archive/winntas/plan/pptpudst.mspx?mfr=true
[3] http://www.javvin.com/protocolPPTP.htmlwww.wikipedia.com
[4] http://www.wikipedia.com