Layer 2 Tunneling Protocol (L2TP)

Teorie a praktické použití ve Windows a Linuxu

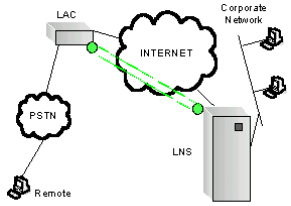
Richard Biječek, BIJ006
Lubomír Moric, MOR135

19.1.2007

Úvod

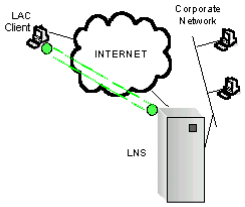
L2TP (Layer 2 Tunneling Protocol) je protokol tunelového propojení sítí, vyvinutý v roce 1998 spoluprací členů PPTP fóra, firmy Cisco a organizace IETF. Jeho funkcí je tunelování protokolu PPP po sítích různého typu (např. FrameRelay, ATM, Internet…). Je definován ve standardu RFC2661.

Protokol L2TP nabízí dva základní způsoby přístupu. První z nich spočívá v připojení typicky vytáčených klientů prostřednictvím LAC (L2TP Access Concentrator) do domovské sítě, viz obrázek 1. Vzdálený klient (Remote) zde naváže standardní PPP spojení přes telefonní síť na LAC, které toto PPP spojení dále tuneluje (zde přes internet) na LNS (L2TP Network Server). LNS je již součástí tzv. Home LAN, což na obrázku reprezentuje síť firmy (Corporate network)



obr. 1

Druhý způsob (viz obrázek 2) slouží pro přímé připojení klienta do Home LAN. V tomto případě musí samozřejmě klient L2TP protokol podporovat sám, a klient musí mít přímý přístup k síti, přes kterou je navázán tunel (zde internet).

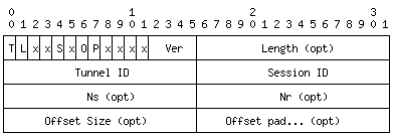


obr. 2

Protokol

L2TP pracuje se dvěma typy zpráv, řídícími a datovými. Řídící zprávy se přenášejí na spolehlivém kanále (je garantováno jejich doručení), zatímco datové zprávy, sloužící k přenosu uživatelských PPP rámců, jsou přenášeny bez záruky. V případě ztráty se tedy L2TP nestará o jejich opětovný přenos.

Řídící i datové L2TP zprávy sdílí stejnou hlavičku, viz obrázek 3.



obr. 3

Na jejím začátku se nacházejí následující vlajky:
T – (Type) – indikuje typ zprávy (0 pro datové a 1 pro řídící)
L, S, O – (Length, Sequence, Offset) – indikují přítomnost volitelných polí v hlavičce

P – (Priority) – Určuje, zda-li má být datový rámec zpracován přednostně. Využívá se například pro LCP echo request aby se zajistilo udržení navázaného spojení.

Pole verze v L2TP hlavičce má hodnotu 2, verze 1 je rezervována pro rozpoznání protokolu L2F, jakožto předchůdce L2TP. Více informací o L2F je například na *http://www.cisco.com/warp/public/732/L2F/* nebo v RFC 2341.

Hodnota Tunnel ID reprezentuje identifikátor řídícího spojení, tedy tunelu, avšak pouze jednostranně. Obě strany tunelu mají vlastní Tunnel ID a hodnota v rámci neslouží k identifikaci odesílatele, nýbrž příjemce. Obě hodnoty se přidělí při vytváření tunelu. Session ID slouží k identifikaci relace v rámci vytvořeného tunelu. Principy jsou obdobné jako u předchozí Tunnel ID. V rámci jednoho tunelu může být více relací (=sessions), proto je identifikace dvouúrovňová.

Navazování spojení

Navazování tunelového spojení se skládá ze dvou kroků; navázání řídícího spojení a navázání relace. Řídící spojení musí být vytvořeno jako první a navazuje se mezi LAC resp. klientem a LNS a zajišťuje mimo jiné identifikaci verze nebo parametry přenosové linky;. Za účelem navázání řídícího kanálu si zúčastněné strany vymění následující zprávy (zasílány přes hostující síť):

Strana 1 vyšle: **SCCRQ →** (Start-Control-Connection-Request)
Strana 2 odpoví: **← SCCRP** (Start-Control-Connection-Reply)
Strana 1 odpoví: **SCCCN →** (Start-Control-Connection-Connected)
Pozn.: Obě strany mohou být jak LAC resp. Klient, tak LNS.

Při zakládání tunelu je volitelně možno kteroukoli stranou vyžádat autentizaci, založenou na mechanismu CHAP. Tento požadavek je pak součástí zprávy SCCRQ nebo SCCRP a odpověď (Challenge response) musí druhá strana zaslat v bezprostředně následné zprávě – SCCRP resp. SCCCN. Není-li druhá strana schopna na požadavek první provést tuto autentizaci, spojení se neuskuteční.

V existujícím tunelu se za účelem přenosu dat musí vytvořit minimálně jedna relace (relace = PPP spojení). Při vytváření relace je popsáno jako „volání“ a rozlišuje se příchozí resp. odchozí. Příchozí volání je typický případ, kdy relaci chce založit LAC (klient) směrem k LNS resp. odchozí je opačné (od LNS k LAC). Následují příkazy, zasílané v řídícím kanále L2TP, pro obě situace:

Příchozí volání:
<požadavek na volání na LAC>
LAC vyšle: **ICRQ →**
LNS odpoví: **← ICRP**
LAC odpoví: **ICCN →**

Odchozí volání:
LNS vyšle: **← OCRQ**
LAC odpoví: **OCRP →**
<LAC provede vyžádané volání>
LAC odpoví: **OCCN →**

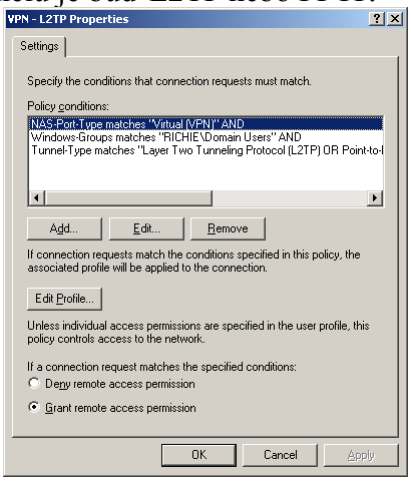
Konfigurace ve Windows

Popis konfigurace a chování je platný pro Windows Server 2003 jako LNS a Windows XP jako klienta v anglické resp. české verzi.

Implementace protokolu L2TP ve Windows je součástí protokolového stacku TCP/IP. Z hlediska konfigurace serveru existuje jediné využití - vytvoření portů pro VPN v režimu L2TP/IPSec. Portem se zde rozumí „slot“ pro jedno tunelové spojení.

Serverová část (LNS) se konfiguruje v konzoli „Routing and Remote Access“ v sekci „Ports“. Přes vlastnosti máme možnost konfigurovat maximální počty portů příchozích

připojení nejen pro protokol L2TP. Limitní počet L2TP portů je 1000, což je zároveň celkový počet připojených klientů přes všechny WAN porty. Dále je nutno na serveru v konzoli „Routing and remote access“ povolit přístup, ať už po stránce seznamu uživatelů, či přístupových protokolů, neboť ve výchozím nastavení není přístup povolen. Nastavení se provádí vytvářením nebo editací politik v sekci „Remote Access Policies“. Konfigurace politiky použité při testování je na obrázku č. 4. Jednotlivé položky v pořadí určují, že politika se týká připojení VPN klientů, kteří musí být zároveň ověřeni jako uživatelé testovací domény (skupina Domain Users) a typ tunelu je buď L2TP nebo PPTP.



obr. 4

V tuto chvíli je na serveru nakonfigurováno vše potřebné co se týká připojení, nicméně je důležité nastavit autentizaci. Ta je skrz svázanost s protokolem IPSec ve výchozím stavu nastavena pouze na ověření pomocí certifikátů počítačů (jak stanic, tak serveru). Chceme-li využívat ověření pomocí certifikátů, musíme mít k dispozici certifikáty. V rámci Windows Serveru je lze vygenerovat přes vestavěnou certifikační autoritu. Pokud je navíc budoucí VPN klient členem domény, ve které máme nainstalován certifikační server, je možno nechat certifikáty automaticky nainstalovat. Na straně klienta se certifikát vybírá přes vlastnosti VPN připojení na záložce „Zabezpečení“ v sekci „Upřesnit nastavení“.

Druhá metoda je ověřování pomocí předsdílených klíčů. Konfigurace na straně klienta je snadná, neboť na zmíněné záložce VPN připojení je možno zadat předsdílený klíč. Na serveru ovšem musíme provést zásah do registru systému, aby byly předsdílené klíče umožněny. Je potřeba přidat do klíče
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters
hodnotu **ProhibitIpSec** typu **REG_DWORD** a do datové části zapsat **1**. Po této změně je možno přes konzolu „IP Security Policie“ vytvořit politiku, která umožňuje zadání předsdíleného klíče. Politika byla v našem testovacím zapojení editována přes konzoli „Domain Controller security policy“, neboť testování probíhalo na doménovém řadiči. Zde je potřeba v sekci „IP Security policy on Active Direktory (…)“ aktivovat volbu „Server (Request Security)“ pomocí kontextového menu a volby „Assign“. V samotném nastavení této šablony pak editujeme pravidlo pro IP provoz a na záložce „Authentication Methods“ zadáme předsdílený klíč.

Konfigurace klientského systému Windows XP je snadná. V okně „Síťová připojení“ zvolíme „Vytvořit nové připojení“ a v průvodci postupujeme podle následujících kroků: „Připojení k firemní síti“ → „Připojení k virtuální privátní síti“ → zadáme název připojení → a nakonec zadáme IP adresu nebo doménový název serveru (LNS). Tímto se nám vytvoří nové připojení k VPN serveru, vhodné jak pro PPTP tak pro L2TP. Protokol volíme ve vlastnostech na záložce „Sítě“ a pokud nastavujeme předsdílený klíč, je potřeba vyvolat dialog pro zadání přes tlačítko „Nastavení protokolu IPSec“ na záložce „Zabezpečení“.

Závěr, Windows: Nastavení serveru i klienta bylo ověřeno přesně podle předchozího popisu a spojení proběhlo bezproblémově. Architektura testovacího zapojení byla odzkoušena mezi dvěma počítači spojenými směrovačem. Klientský počítač s adresou z rozsahu 10.0.0.0/24 se připojoval na server s adresou v rozsahu 192.168.1.0/24. Na serveru běžela také služba dynamického přidělování adres (z jeho rozsahu 192.168.1.0/24) od níž klient po úspěšném připojení získal adresu. Náčrtek sítě je shodný se zapojením pro platformu Linuxu, viz obrázek 5. S tímto typem VPN přístupu máme pozitivní zkušenosti také přes internet (Vzdálená správa firemní sítě).

Konfigurace v Linuxu

Implementací protokolu L2TP v Linuxu se zabývá projekt nacházející se na http://www.l2tpd.org. Poslední verze programu nese označení 0.69 a je z roku 2002. Od té doby projekt stagnuje a nepokračuje se ve vývoji nových verzí nebo modulů pro začlenění do jádra operačního systému (l2tpd tak v současné implementaci pracuje pouze v user-space prostoru).

Možnou alternativou L2TP v linuxu je také implementace společnosti Katalix Systems s názvem OpenL2TP. Pracuje s kernely verzí 2.4 a 2.6. OpenL2TP je určen pro klient/server VPN propojení za pomocí L2TP a linuxového démona pppd.

Následující popis se bude zabývat démonem l2tpd verze 0.69-13mdk (http://www.l2tpd.org). RPM balíček lze získat např. na *http://www.rpmseek.com*. L2TP klient (LAC) i server (LNS) používají shodného démona l2tpd, ten se nachází v adresáři `/usr/sbin`. Dokumentace a manuálové stránky jsou v `/usr/share/doc` a `/usr/share/man`. V adresáři `/etc` se nacházejí konfigurační soubory. Jejich umístění i názvy jsou taktéž shodné jak pro klienta, tak server (zda se spustí l2tpd v režimu LAC nebo LNS určí až obsah konfiguračních souborů).

Hlavní konfigurační soubor `/etc/l2tpd/l2tpd.conf` obsahuje tyto položky (pokud položka není uvedena, je použita její výchozí hodnota):

Sekce '**`global`**' obsahuje základní nastavení služby:

`[global]`

`auth file = /etc/l2tp-secrets`

Specifikace umístění souborů s hesly.
(Výchozí hodnota pro toto pole je `/etc/l2tp-secrets`)

`Port = 1701`

Použít jiný UDP port.
(Výchozí hodnota pro toto pole je **`1701`**.)

`access control = no`

V případě **`'yes'`** bude navázáno spojení pouze s protistranami explicitně uvedenými v dalších sekcích.
(Výchozí hodnota **`'no'`**.)

`listen-addr = 10.153.18.35`

IP adresa rozhraní, na kterém bude démon naslouchat.
(Výchozí hodnota: **`INADDR_ANY`** (0.0.0.0) - naslouchání na všech rozhraních.)

`debug avp = yes`
`debug network = yes`
`debug packet = yes`
`debug state = yes`

debug tunnel = yes

Povolí vytváření ladících záznamů o běhu L2TP AVP (Attribute-Value Pair[1]), síti, přenesených paketech (tyto záznamy se vypisují pouze do aktuálního terminálu, tudíž služba musí být spuštěna s parametrem -D (viz. níže)), stavu FSM (Finite State Machine[2]) a vytvořených tunelech.
(Výchozí hodnoty jsou **'no'.**)

Pod hlavičkou LNS se nalézá konfigurace pro L2TP Network Server:

[lns default]

ip range = 192.168.1.100-192.168.1.200

Rozsah adres, které se budou přidělovat připojeným klientům. V případě použití parametru ve tvaru '**no ip range**' se toto přidělování zakáže.
(Výchozí hodnota: '**no ip range**'.)

local ip = 192.168.1.99

IP adresa LNS serveru. Nemusí se shodovat s IP adresou síťového rozhraní.
V takovém případě se vytvoří rozhraní virtuální s touto IP adresou.

lac = 192.168.50.1-192.168.50.100

IP adresy LAC stanic, které mají povolení připojit se k LNS serveru.

require chap = yes

Bude požadováno ověření hesla metodou CHAP.
(Výchozí hodnota: **'yes'.**)

refuse pap = yes

Bude odmítnuto ověření hesla metodou PAP.
(Výchozí hodnota: **'yes'.**)

require authentication = yes

Požadujeme ověřování.
(Výchozí hodnota: **'yes'.**)

unix authentification = no

V případě povolení této položky se pro ověřování vzdálených ppp klientů použijí záznamy z `/etc/passwd`.
(Výchozí hodnota: **'no'.**)

name = Linuxserver

Jméno (pro vazbu v chap-secrets).
(Výchozí hodnota: **hostname.**)

ppp debug = yes

Povolí výpis ladících informací pro pppd.
(Výchozí hodnota: **'no'.**)

pppoptfile = /etc/ppp/options.l2tpd

Soubor s konfiguračními parametry pro pppd.
(Výchozí hodnota: **'/etc/ppp/options.l2tpd'.**)

V jednom konfiguračním souboru se může nalézat konfigurace pro více LNS. Ta se pak uvádí pod hlavičkou **[lns server_name]**. Vždy se použije konfigurace se jménem odpovídající hostname stanice. Pokud není nalezena, použije se konfigurace **default**.

V sekci LAC se nalézá konfigurace klienta (L2TP Access Concentrator):

[1] AVP představuje elementární datový pár Atribut, Hodnota. Jeho použití umožňuje vytvoření strukturálně otevřeného protokolu s možností budoucího rozšíření o nové atributy.

[2] FSM neboli Konečný Automat. L2TP démon se během svého běhu nachází v různých stavech (např. čekání na klienta, vyhledávání serveru, vyjednávání parametrů o spojení ...).

[lac default]
lns = 192.168.1.99
IP adresa přístupového LNS serveru.
(Výchozí hodnota: **'DEFAULT_GW'.)**
redial = yes
Znovunavázat spojení se serverem, v případě výpadku spojení?
(Výchozí hodnota: **'no'.**)
redial timeout = 10
Počet sekund mezi pokusy o navázání spojení se serverem (volba redial musí být povolena).
(Výchozí hodnota: **'10'.**)
max redial = 3
Počet pokusů o navázání spojení se serverem.
(Výchozí hodnota: **'3'.**)

Stejně jako u LNS i LAC konfigurací může být uvedeno více.

Soubor `/etc/l2tpd/l2tp-secrets` obsahuje seznam hesel pro ověřování mezi klientem a serverem. Každý řádek se skládá ze tří záznamů. První záznam obsahuje hostname stanice. Lze taktéž použít '*' jako zástupný řetězec. Druhá položka obsahuje jméno serveru. Třetí položkou je heslo, které se použije pro autentifikaci v případě, že jméno stanice a serveru odpovídají prvnímu a druhému záznamu.

Příklad:

```
#LAC_name      LNS_name       password
john           lenon          beatles
*              bob            sting
alice          *              ed
*              *              some_password
```

Záznamy se procházejí shora dolů. Klient použije pro autentizaci řádek(záznam) se jménem uvedeným v konfiguraci protokolu vytvářejícího tunelové spojení mezi LAC a LNS (viz. ppp níže).

Démon l2tpd lze pak spouštět s těmito parametry:
-D
Zabrání aplikaci v démonizaci, ta tak zůstane běžet na popředí a do aktuálního terminálu bude vypisovat informace o svém běhu.
-c <konfigurační soubor>
Použije alternativní konfigurační soubor místo `/etc/l2tpd/l2tpd.conf`.
-s <soubor s hesly>
Použije alternativní soubor s hesly místo `/etc/l2tpd/l2tp-secrets`.
-p <pid soubor>
Jiné umístění pro soubor s PID. Standardně `/var/run/l2tpd.pid`.

Démon L2TP podle své konfigurace vyjedná spojení mezi stanicemi a následně spustí protokol ppp (v Linuxu se většinou jedná o službu pppd). Pro spojení a nastavení protokolů L2TP a ppp slouží konfigurační soubor `/etc/ppp/options.l2tpd`. Nejpodstatnější položkou v tomto souboru je '**name**', kde se uvede jméno stanice, které bude použito pro

autentizaci na LNS. Musíme mít tedy vytvořen záznam s tímto jménem v `l2tp-secrets`. Všechny položky odpovídají standardnímu nastavení ppp v prostředí linux.
Příklad souboru `options.l2tpd`:

auth

Pokud server požaduje autentizaci, uvede se klíčové slovo '**auth**'.

name my_hostname

Jméno klienta uvedené v `l2tp-secrets`. Řádek s tímto záznamem se poté použije pro autentizaci.

crtscts

Povolí HW kontrolu dat během přenosu (výhodné uvést v případě všech linek rychlejších než 9,6kb/s)

mtu 1400

Maximum transmission unit: určuje maximální velikost přenášeného paketu v bajtech. V případě překročení této hodnoty dojde k fragmentaci (rozdělení dat do více paketů).

mru 1400

Maximum reception unit: pokusit se vyjednat s protistranou, aby velikost příchozích paketů nebyla větší než uvedená hodnota. Větší pakety se budou fragmentovat.

defaultroute

Parametr říká, zda se má změnit výchozí cesta na zařízení ppp0.

debug

Zapne zapisování ladících informací do souboru.

noipdefault

Po vytvoření spojení žádáme o přidělení IP adresy.

lock

Zamkne zařízení ppp0 výhradně pro obsluhu démonem pppd.

proxyarp

Umožní viditelnost klienta v síti, do které se připojuje. Server na opačné straně přidá konkrétní ARP záznam a Proxy server použije jako výhradní router pro veškerý provoz směřující k ppp klientovi.

usepeerdns

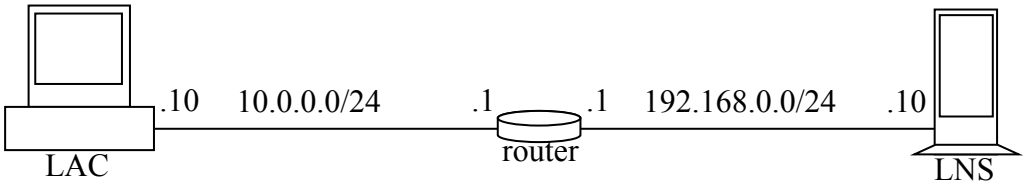
Po připojení vznikne soubor `/etc/ppp/resolv.conf` s adresami DNS serverů providera.

Služba l2tpd se spouští na portu 1701. Chceme-li vytvořit šifrovaný kanál, např. za pomocí protokolu IPSec, po kterém následně proběhne autentizace na úrovni L2TP, můžeme tak učinit pomocí nástroje '**setkey**' pro nastavení síťové politiky(viz. manuálové stránky k tomuto nástroji)[3]:

```
#!/bin/sh
/sbin/setkey -FP
/sbin/setkey -F
/sbin/setkey -c << EOF
spdadd 0.0.0.0/0 ip.serveru [1701] any -P out ipsec \
esp/transport//require ;
spdadd ip.serveru [1701] 0.0.0.0/0 any -P in ipsec \
esp/transport//require ;
EOF
```

[3] Daný protokol třetí strany použitý pro vytvoření zabezpečeného spojení musí být na systému samozřejmě přítomen.

Praktická implementace proběhla na následujícím zapojení:



obr. 5

`/etc/l2tpd/l2tpd.conf` na LAC:

```
[lac default]
lns = 192.168.1.10
```

LAC klient se bude připojovat k LNS serveru s IP adresou **`192.168.1.10`**.

`/etc/l2tpd/l2tpd.conf` na LNS:

```
[lns default]
ip range = 192.168.0.10-192.168.0.20
lac = 10.0.0.10-10.0.0.20
require chap = yes
refuse pap = yes
require authentication = yes
unix authentification = no
name = my_LNS
```

LNS server se jménem **`my_LNS`** bude přidělovat LAC klientům IP adresy uvedeného rozsahu (**`ip range`**). Připojení bude povoleno pouze klientům s IP adresami z rozsahu **`10.0.0.10-10.0.0.20`**, kteří se autentizují metodou CHAP.

`/etc/l2tpd/l2tp-secrets` na LAC i LNS jsou totožné:

```
*               my_LNS                  heslo
```

Pro LNS tato konfigurace umožní připojení všem klientům připojujícím se na server jménem **`my_LNS`** a znajícím tajné heslo.
Pro LAC klienty to znamená, že při autentizaci použijí svůj **`hostname`**, uvedené jméno LNS serveru a tajné heslo.

Po připojení klienta k serveru, klient obdrží IP adresu patřící do sítě 192.168.0.0/24 z poolu **`ip range`**. Tak je vytvořen tunel do oné sítě.

Závěr, Linux: Samotné nastavení a zprovoznění L2TP v Linuxu nepůsobilo žádné větší problémy. Vzhledem k stagnujícímu vývoji protokolu pro systémy Linux a faktu, že běží zatím pouze v user-space prostoru, na většině systémů se volí raději alternativa pptp (taktéž společně s IPSec) pro Linux.