
PPPoE kiszolgáló telepítése Linux-ra

Bálint Zoltán – Kincses Levente
Szabadkai Műszaki Főiskola
Szabadka
2007. II. 5.

Tartalomjegyzék

TARTALOMJEGYZÉK	3
BEVEZETŐ	4
JOGI ÉS FELELŐSSÉG NYILATKOZAT	4
HARDVER	4
KÖVETELMÉNYEK	5
RENDSZER KAPACITÁS FELMÉRÉSE	5
SZOFTVER	5
RP-PPPoE	6
PPPD	6
BEÁLLÍTÁSOK	6
PPPD BEÁLLÍTÁSOK	6
AZ /ETC/PPP/OPTIONS MEGVÁLTOZTATÁSA:	6
AZ /ETC/PPP/PAP-SECRETS MEGVÁLTOZTATÁSA:	7
RP-PPPoE BEÁLLÍTÁSOK	7
ETHERNET CSATOLÓK	8
IP TOVÁBBÍTÁS	11
HIBAELOHÁRÍTÁS – HIBAKERESÉS	11

Bevezető

PPPoE rövidítés az angol Point to Point over Ethernet szavakból jött létre, jelentése Pont-Pont Protokoll Etherneten keresztül. Ez egy másodszintű OSI protokoll, amely PPP (Pont-Pont) protokollt használ egy kliens-rendszer szerver-rendszerre való kapcsolódáshoz egy hálózati kapcsolaton. Egy PPPoE kapcsolatú kliens összes adatforgalma a PPPoE kiszolgálón keresztül érkezik meg a klienshez. Így egy PPPoE kiszolgáló használható: útválasztás, NAT, tűzfal és QOS forgalom formálás. Az újabb PPP kiszolgáló megjelenésével RADIUS attribútumok támogatást nyertek, lehetővé téve a kliensek azonosítását illetve a konfiguráció intézhető távolról, RADIUS kiszolgálóról. A Linux egy kiváló, nagy teljesítményű operációs rendszer, amely könnyedén kezel nagyobb számú PPPoE klienst szerény hardver platformon is.

E dokumentum leginkább az internet szolgáltatók, informatikusok és más hálózat menedzserek részére lehet hasznos.

Jogi és felelősség nyilatkozat

A dokumentum tartalmáért semmilyen felelősség nem vállalható. Saját felelősségre használhatók az elvek, példák és más tartalom. Mivel e dokumentum igen friss megjelenésű, ezért lehetnek benne hibák és pontatlanság, amelyek természetesen kárt tehetnek rendszerében. Elővigyázatos eljárással, habár ez roppant hihetetlen, de a szerzők semmi felelősséget nem vállalnak érte.

Minden szerzői jog az őt megillető tulajdonosé, kivéve ha külön másképp van feljegyezve. A dokumentumban használt kifejezések nem értelmezhetik a védjegyek érvényességét.

Termékrészek vagy márkanév megnevezése nem értelmezhető hozzájárulásként.

Nyomatékosan javasolt egy biztonsági mentés készítése a rendszerről, jelentősebb telepítés előtt és biztonsági mentések rendszeres időközönként.

Hardver

A Linux egy nagy teljesítményű operációs rendszer. Ennek bizonyítéka a mai trend, mégpedig a SOHO útválasztók és vezeték nélküli eszközök Linux firmware-el érkeznek. A PPPoE egy CPU-t alaposan igénybevevő alkalmazás és több példányban futtatva egy kiszolgálón elkerülhetetlenül "felenné" a memóriát. Megállapításunk szerint egy lineáris összefüggés létezik az egyidejűleg kapcsolódott kliensek és a CPU valamint memória szükségletek közt.

Biztonsággal állíthatjuk, hogy egy kapcsolódott kliens 2 MHz CPU-t illetve 2 Mbyte rendszer memóriát igényel. Ezek az értékek a gyakorlati alkalmazások során mutatkoztak.

Követelmények

A rendszer két ethernet NIC-t (Network Interface Card) igényel. Ez azért van, mert a PPPoE-nek egy olyan csatolón kell működnie, amelynek nincs IP cím kiosztva. Azonban a másik csatoló eszköznek van egy IP címe, hogy hozzáférése legyen a hálózathoz (internet). Több PPPoE kapcsolat lebonyolítása a cím nélküli NIC-en történik, és át lesznek irányítva a címmel rendelkező NIC-en keresztül. Bármely Pentium III rendszer elegendő RAM-al könnyedén kezel 100 egyidejű kapcsolatot. Ajánlott 100 Mbit vagy Gigabit teljesítményű NIC-ek használata.

Rendszer kapacitás felmérése

Ahogy az előzőekben említve lett, minden aktív kapcsolat 2 MHz CPU és 2 Mbyte memóriát igényel. Ráadásul ez független attól milyen memóriát és CPU-t igényel a Linux és a szerveren futó többi szoftver. Biztonsággal állítható, hogy egy 500 MHz-es Pentium 512 Mbyte RAM-al nagyjából 250 párhuzamos kapcsolatot kiszolgál. Ha kétség merülne fel, legyünk biztosak, a CPU és a memória nem költséges. Multi-processzoros rendszerek kívánatosabbak ebben a szolgáltatásban, a kisebb rendszer késések miatt. Azonban több PPPoE kiszolgáló előnyösebb egyetlen erős kiszolgálótól, mivel amikor egy kiszolgáló elromlik a hálózaton lévő többi kiszolgáló viszi a terhelést, redundancia jó.

A PPP vagy a PPPoE kiszolgáló egy hibát rejt magában, amely gondot okoz a PPP254-es virtuális eszköz létesítésénél. Ez egy elkerülhetetlen gond, hacsak nem szándékozik a PPP vagy PPPoE forrás kódot módosítani, kijavítani. Azért az nem várható, hogy egy otthoni PPPoE kiszolgáló több mint 255 PPPoE kapcsolatot létesítsen. Remélhetőleg ezt a problémát a fejlesztők ki fogják javítani. Több kiszolgáló futása párhuzamosan egy LAN gerincen mindenképp megbízhatóbb megoldás. Ezzel lehet kiiktatni ezt a kis korlátozást.

Szoftver

Bármely újabb Linux disztribúció használható PPPoE kiszolgáló építésére, 2.6-os vagy későbbi kernel verzióval. Az későbbi kiadású Linuxok újabb verziójú PPPd-t használja.

Legtöbb Linux disztribúció rendelkezik a szükséges csomagokkal a telepítő adathordozón. Esetünkben Open SuSE 10.2 -t használunk és minden szükséges csomag megtalálható a telepítő DVD-n. Az Open SuSE jó választás, mivel a kernel módú PPPoE támogatás van beépítve a disztribúcióba. Praktikusan ezért nem szükséges újrafordítani a kernelt a kernel mód használatához. Lehetséges azonban a csomagok letöltése és telepítése, ha kellőképp hozzáértő a saját kedvenc Linux-ához és azon telepítené.

RP-PPPoE

A Roaring Penguin PPPoE kiszolgáló szoftver szükséges. A 3.5 vagy későbbi verziójú használatos. Ahogy már fentebb említve volt, ez a kiszolgáló verzió támogatja a kernel módú PPPoE-t, amikor ez és a kernel erre a módra fordítva. Az RP-PPPoE szerzői állítják, hogy az általuk megvalósított kiszolgáló nem igazán nagybani felhasználásra termett.

PPPd

A 2.4 verzió számmal rendelkező PPPd is telepítve kell legyen a rendszeren.

Beállítások

A beállítások megkezdése előtt meg kell győződni arról, hogy rendszergazdaként (root) vagyunk bejelentkezve. Tűzfal kikapcsolása javasolt a beállítások idejére.

PPPd beállítások

PPP egy hatalmas és összetett protokoll a “point to point” kapcsolatok kiépítésére akármilyen elképzelhető közegen keresztül. PPPoE egy “csomag alapú protokoll” a PPPd szoftver körül, ami létrehozza és megszakítja a PPP kapcsolatokat ethernet keresztül. PPPoE meghívja PPPd-t egyszer, ami tartalmazza a szükséges információt a PPPd igényéről, hogy fenntartsa egy kapcsolatot.

A PPPd konfigurációs fájlok az **/etc/ppp**-ben vannak jelen. Itt két fájl van ami érdekes számunkra. Ezek az **/etc/ppp/options** és az **/etc/ppp/pap-secrets**. Mi csak a minimális nélkülözhetetlen beállításokat hajtjuk végre a PPP daemon-on ahhoz, hogy támogassa a PPPoE kapcsolatokat.

Az **/etc/ppp/options** megváltoztatása:

Meg kell nyitnunk az **/etc/ppp/options**-öt egy szövegszerkesztőben. A legtöbb Linux konfigurációs fájlban a **#** jelzi a sor elején, hogy az a sor egy megjegyzés. Keressük meg azt a sort ami tartalmazza a **login** és változtassuk meg **#login**-ra. Keressük meg azt a sort amiben a **#mru 1492** olvasható és töröljük ki a **#**-t. Keressük meg azt a sort amiben a **#mtu 1492** olvasható és töröljük ki a **#**-t. Keressük meg azt a sort amiben a **#noplacedefaultroute** olvasható és töröljük ki a **#**-t.

Keressük meg azt a sort amiben a **#proxyarp** olvasható és töröljük ki a **#**-t. Ez csak akkor szükséges ha nyilvános IP-t akarunk kiosztani néhány kliensnek. Ha az összes kliens NAT-olva lesz, akkor nem kell a proxyarp-ot engedélyezni. A biztonságos választás ha a proxyarp-ot engedélyezzük, mert a legrosszabb esetben is létrehoz egy hibaüzenetet a log-ban.

Keressük meg azokat a sorokat amik **#ms-dns 192.168.** -cal kezdődnek. Ez az ahol beállíthatjuk a DNS szerveret a kliensek számára. A kliensek hozzá lesznek rendelve a DNS

szerverhez. Kitörölhetjük a #-t ezek a sorok közül ahhoz, hogy szerkeszteni tudjuk és a szerver figyelembe vegye.

Az /etc/ppp/pap-secrets megváltoztatása:

Nyissuk meg az **/etc/ppp/pap-secrets** fájlt egy szövegszerkesztőben. Keressük meg azt a részt, ami a következőképpen néz ki:

```
# INBOUND CONNECTIONS
```

```
#client hostname <password> 192.168.1.1
```

Egy csillag jelet kell tenni a “**client**”, “**host name**”, és az “**IP address**” alá. Ez megadja, hogy bármely kliens, akármilyen host névvel, hozzá lesz rendelve valamilyen IP címhez, ha a kliens rendelkezik megfelelő bejelentkezési információval. Változtassunk meg egy részt a pap-secrets fájlban, hogy így nézzen ki:

```
# INBOUND CONNECTIONS
```

```
#client hostname <password> 192.168.1.1
```

```
* * " " *
```

Ezzel készen van az alapbeállítás az **/etc/ppp**-ben. Ezek az minimális beállítások amik szükségesek a PPPoE szervernek.

RP-PPPoE beállítások

RP-PPPoE-nek van egy konfigurációs fájlja ami szintén az **/etc/ppp**-ban található. Ez az **/etc/ppp/pppoe-server-options**. Ezt nem szükséges változtatni. A PPPoE szerver daemon egy folyamat aminek futnia kell hogy figyelje a kísérleteket a csatlakozásra. Ez a rendszer induláskor futtatva lesz. Használtunk egy script-et hogy futtassuk a PPPoE szerver folyamatot és hogy konfiguráljuk a NAT-ot (Network Address Translation) a “non-routeable” címeknek a PPPoE kiszolgáló mögött. A script a következő:

```
#!/bin/bash
```

```
# -----
```

```
# Starts the PPPoE server and turns on NAT
```

```
# -----
```

```
# MAX is the maximum number of addresses your server
```

```
# is allowed to hand out.
```

```
MAX=250
```

```
# BASE is the lowest IP address your server is allowed
```

```
# to hand out.
```

```
BASE=10.67.7.1
```

```
# NAT is the set of addresses which your server will
```

```
# NAT behind it. Other addresses behind your server
```

```
# WILL NOT be NATed.
```

```
NAT=10.67.7.0/24
```

```
# MYIP is the public IP address of this server.
MYIP=65.122.24.7

#####
# Here is where the script actually starts executing.
#####
# Disable IP spoofing on the external interface.
/usr/sbin/iptables -A INPUT -i eth0 -s $NAT
#
# Enable NAT for the private addresses we hand out.
/usr/sbin/iptables -t nat -A POSTROUTING -s $NAT -j SNAT --to-source $MYIP
#
# Launch the server.
/usr/sbin/pppoe-server -T 60 -I eth1 -N $MAX -C PPPoE7 -S PPPoE7 -R $BASE
```

Ennek a scriptnek a neve **pppoe-up**. Ezt mentsük el az **/etc/rc.d/pppoe-up** helyre. Készítsünk egy másolatot erről a script-ről és utána módosítsuk. Állítsuk a **MAX=** értékét a maximális egyidejű kapcsolatok számára, amit a PPPoE szerver elfogadjon. Állítsuk a **BASE=** értékét az alap IP címre ahonnan a PPPoE szerver használja a kezdeti IP cím kiosztást. Ezek a címek lehetnek 192.168.0.1 vagy másmilyen IP címek, route-olható vagy nem. Állítsuk a **NAT=** értéket egy olyan értékre, amely lefedi a hálózat címzési területét. Állítsuk a **MYIP=** értékét arra az IP címre, amit szeretnénk választani a PPPoE szervernek. Ez az a cím amin a PPPoE szerver kommunikálni fog a világgal. Minden felhasználó, aki csatlakozva van a PPPoE szerverhez ezt a címet fogja használni.

A script beolvassa ezeket az értékeket és csak a **MYIP=** érték alatti három sor hajtódik verge mint igazi parancs. Az első sor blokkolja a bejövő csomagokat amelyek címéről a szerver azt hiszi hogy mögé tartoznak. A második sor engedélyezi a NAT-ot minden “non-routeable” címnek, amelyet a PPPoE kiszolgálón használni fogunk. A harmadik sor valójában futtatja a PPPoE szervert.

A script létrehozása és az **usr/sbin/pppoe-up** helyre való mentése után a következő parancsokat kell végrehajtani a shell parancssorban:

```
# Change to the directory
cd /etc/rc.d
# Make the file executable.
chmod 755 ./pppoe-up
# Set up the script to run in run levels three and five.
chkconfig pppoe-up 35
```

Ethernet csatolók

A PPPoE szerver össze kell legyen kötve egy számozatlan ethernet csatolóval, ami “promiscuous” módban fut. Akármilyen Linux kínálta eszközzel mindkét Ethernet csatolót üzemeljük be és adjunk mindkettőnek címet. Adjunk a világ felőli csatolónak (eth0) egy valós IP címet. A kliens oldali csatolónak (eth1) 192.168.1.1 címet adjuk. Mentsük a beállításokat. Most váltsunk az **/etc/sysconfig/network** könyvtárra és listázzuk a fájlokat (**ls -l**). A listázásnak így kell kinéznie:


```
PPPoE7:/etc/sysconfig/network # ls -l
total 54
drwxr-xr-x 6 root root 440 2006-01-03 12:11 .
drwxr-xr-x 7 root root 1424 2006-01-03 11:58 ..
-rw-r--r-- 1 root root 6979 2005-09-09 12:15 config
-rw-r--r-- 1 root root 6705 2006-01-02 15:58 dhcp
-rw-r--r-- 1 root root 181 2006-01-03 12:10 ifcfg-eth-id-00:50:bf:43:51:47
-rw-r--r-- 1 root root 250 2006-01-03 12:11 ifcfg-eth-id-00:50:bf:43:66:05
-rw-r--r-- 1 root root 141 2005-09-09 12:15 ifcfg-lo
-rw-r--r-- 1 root root 5779 2005-09-09 12:15 ifcfg.template
drwxr-xr-x 2 root root 48 2005-09-09 12:27 if-down.d
-rw-r--r-- 1 root root 239 2005-09-09 12:15 ifroute-lo
drwxr-xr-x 2 root root 88 2005-12-30 11:59 if-up.d
drwx----- 2 root root 48 2005-09-09 12:27 providers
-rw-r--r-- 1 root root 25 2006-01-02 15:58 routes
drwxr-xr-x 2 root root 1336 2005-12-30 11:59 scripts
-rw-r--r-- 1 root root 5469 2005-12-30 11:57 wireless
PPPoE7:/etc/sysconfig/network #
```

A két **ifcfg-eth-id-<csatoló mac címe>** nevű állományt használja a rendszer a bootoláskor a csatolók beállítására. Az **ifconfig eth1** végrehajtása a parancssorban egy hasonló eredményhez vezet mint itt:

```
PPPoE7:/etc/sysconfig/network # ifconfig eth1
eth0 Link encap:Ethernet HWaddr 00:50:BF:43:66:05
inet addr:192.168.1.1 Bcast:192.168.1.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:1562715 errors:0 dropped:0 overruns:0 frame:0
TX packets:58595 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:127223033 (121.3 Mb) TX bytes:9415968 (8.9 Mb)
Interrupt:10 Base address:0xc000
```

```
PPPoE7:/etc/sysconfig/network #
```

Feljegyezni az eth 1 csatoló Hwaddr-t. Mostmár világos, hogy melyik **ifcfg-eth-id-xx:xx:xx:xx:xx:xx** állomány tartozik az eth1-hez. Nyisd meg a fájlt egy szövegszerkesztőben. A következőképpen kell kinéznie:

```
BOOTPROTO='static'
BROADCAST='192.168.1.255'
IPADDR='192.168.1.1'
MTU=''
NAME='Realtek RT8139'
NETMASK='255.255.255.0'
NETWORK='192.168.1.0'
REMOTE_IPADDR=''
STARTMODE='auto'
UNIQUE='rBUF.IQxIdIhhuH7'
USERCONTROL='no'
```

```
_nm_name='bus-pci-0000:00:09.0'
```

BROADCAST címet üresen hagyni, hagyjuk el az aposztrófot, ha vannak. Töröljük az **IPADDR** sort teljesen. **NETWORK** címet üresen hagyni, hagyjuk el az aposztrófot, ha vannak Törölni a **NETMASK** sort teljesen. A módosított fájl így néz ki:

```
BOOTPROTO='static'  
BROADCAST=""  
MTU=""  
NAME='Realtek RT8139'  
NETWORK=""  
REMOTE_IPADDR=""  
STARTMODE='auto'  
UNIQUE='JNkJ.IQxIdIhhuH7'  
USERCONTROL='no'  
_nm_name='bus-pci-0000:00:0a.0'
```

Beállítottuk a rendszert, hogy működésbe hozza mindkét csatolót (eth0, eth1). Futtatni a következő parancsot: **/etc/rc.d/network restart**. Ez leállítja majd újraindítja a hálózatot. Utána gépeljük be: **ifconfig** és valami hasonlóan kell hogy kinézzen:

```
PPPoE7:/etc/sysconfig/network # ifconfig  
eth0 Link encap:Ethernet HWaddr 00:50:BF:43:66:05  
inet addr:65.122.24.7 Bcast:65.122.24.255 Mask:255.255.255.0  
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
RX packets:1570208 errors:0 dropped:0 overruns:0 frame:0  
TX packets:58630 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:127738167 (121.8 Mb) TX bytes:9425522 (8.9 Mb)  
Interrupt:10 Base address:0xc000
```

```
eth1 Link encap:Ethernet HWaddr 00:50:BF:43:51:47  
UP BROADCAST MULTICAST MTU:1500 Metric:1  
RX packets:69 errors:0 dropped:0 overruns:0 frame:0  
TX packets:3 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:6348 (6.1 Kb) TX bytes:258 (258.0 b)  
Interrupt:11 Base address:0xc000
```

```
lo Link encap:Local Loopback  
inet addr:127.0.0.1 Mask:255.0.0.0  
inet6 addr: ::1/128 Scope:Host  
UP LOOPBACK RUNNING MTU:16436 Metric:1  
RX packets:646 errors:0 dropped:0 overruns:0 frame:0  
TX packets:646 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:0  
RX bytes:46470 (45.3 Kb) TX bytes:46470 (45.3 Kb)
```

```
PPPoE7:/etc/sysconfig/network #
```

IP Továbbítás

Most az Ipv4 továbbítást fogjuk bekapcsolni az **/etc/sysconfig** könyvtárban, ahol egy **sysctl** nevű állomány található. Nyissuk meg ezt egy szövegszkesztővel. Itt található egy hivatkozás, az **IP_FORWARD**. Az alapértelmezett értéke “no”, cseréljük ezt le “yes”-re és mentjük le az állományt.

Gratulálunk! Sikeresen telepítette és beállította a PPPoE kiszolgálót!

Hibaelhárítás – hibakeresés

A rendszer újraindítása után kíséreljen meg egy PPPoE klienssel kapcsolódni. A PPPoE kiszolgáló és a PPPd egy lényeges részt hoznak létre a napló információkban, alapbeállításuk alkalmával is. Ez az információ a **/var/log/messages**-ben található. Lehetőség van növelni a naplózás mértékét az **/etc/ppp/options** állományban. Erről részletesebben az options állományban a „debug” részleg alatt található.

Ha a PPPoE kapcsolat létrejön, de mégsem elérhető a külső hálózat, akkor ellenőrizni kell a **/proc/sys/net/ipv4/ip_forward**-ban tárolt értéket. Ha ez 1, akkor van Ipv4 forgalom továbbítás. Ha ez 0, akkor pedig nincs Ipv4 forgalom továbbítás. Ellenőrizni kell, hogy a tűzfal nincs-e kihatással erre az értékre. Javasolt a tűzfal kikapcsolása amíg minden nem működik megfelelően. Az **IP_FORWARD** értékét a SuSE tűzfala felülírja az **/etc/sysconfig/sysctl** állományban.