КОНФИГУРИРАНЕ НА PPTP VPN КЛИЕНТ LINUX

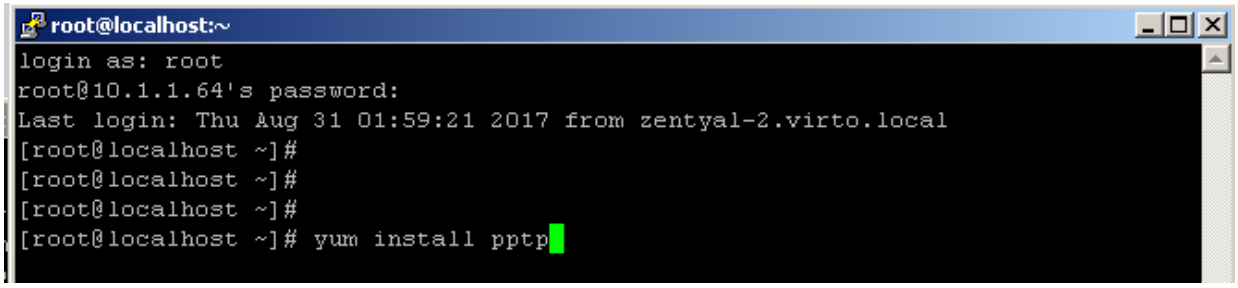
Инсталирането на PPTP клиент под Linux операционни системи включва следните стъпки:

- Инсталиране на PPTP клиент
- Създаване на конфигурационни файлове
- Коригиране на мрежовите настройки
- Стартиране на VPN връзката
- Създаване на статичен път (static route)
- Тестване

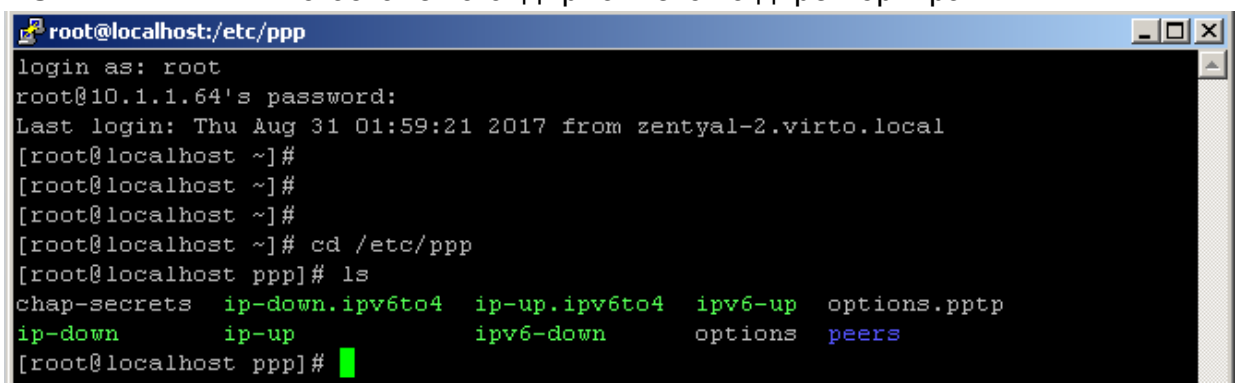
1. Инсталиране на PPTP клиент

1.1. За операционни системи Fedora/Red Hat/CentOS изпълнете командата
yum install pptp или **sudo yum install pptp**

1.2. За операционни системи Debian/Ubuntu изпълнете командата
apt-get install pptp-linux или **sudo apt-get install pptp-linux**



2. Създаване на конфигурационни файлове
При успешна инсталация в виректория **/etc/ppp,** като използвате текстов редактор по ваш избот (vi, nano или друг) редактирайте файл **chap-secrets**
Команди:
#cd /etc/ppp - преминаване в директория /etc/pp
#ls - показване на съдържанието на директорияра



Като използвате текстов редактор (в случая nano), заредете файл **chap-secrets.** Ако nano не е инсталиран можете да го направите с комади **#yum install nano** или **#apt-get install nano** в зависимост от операционната система

Команда:

#nano chap-secrets

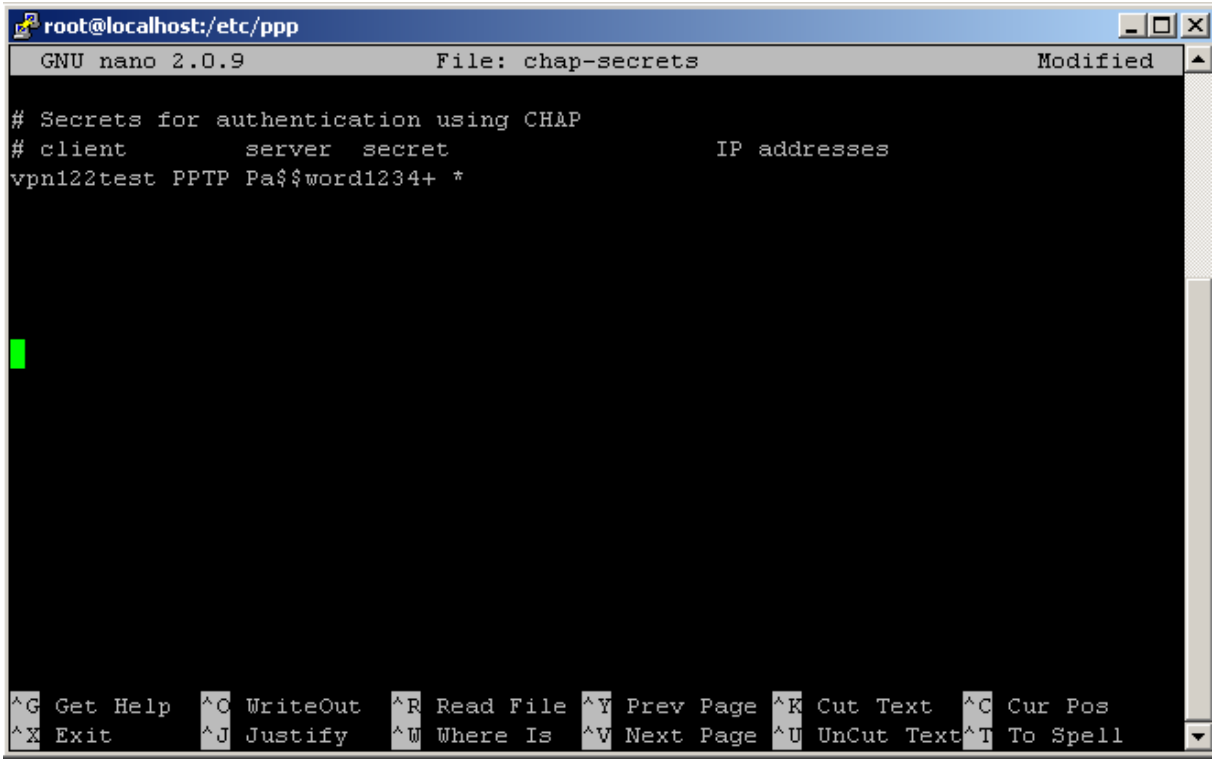
```
[root@localhost ppp]# ls
chap-secrets  ip-down.ipv6to4  ip-up.ipv6to4  ipv6-up  options.pptp
ip-down       ip-up            ipv6-down      options  peers
[root@localhost ppp]# nano chap-secrets
```

Като съдържание на файла въведете потребителско си име, сървър, вашата парола и символ ***** за IP адрес, като разделяте стойностите с интервал (шпация)

Формат:

[Потребителско име] [име на сървър] [парола] *

Пример: За потребителско име vpn123test с парола Pa$$word1234+ следва да се въведе: **vpn123test PPTP Pa$$word1234+ ***



Запишете файла като задържите **Ctrl** и натиснете **O (Ctrl+O)**. Излезте от редактора като задържите **Ctrl** и натиснете **X (Ctrl+X)**

Преминете в директория **/etc/ppp/peers**

Команда: **#cd /etc/ppp/peers**

```
[root@localhost /]#
[root@localhost /]#
[root@localhost /]# cd /etc/ppp/peers/
```

Като използвате текстов редактор създайте файл с име **obmen**

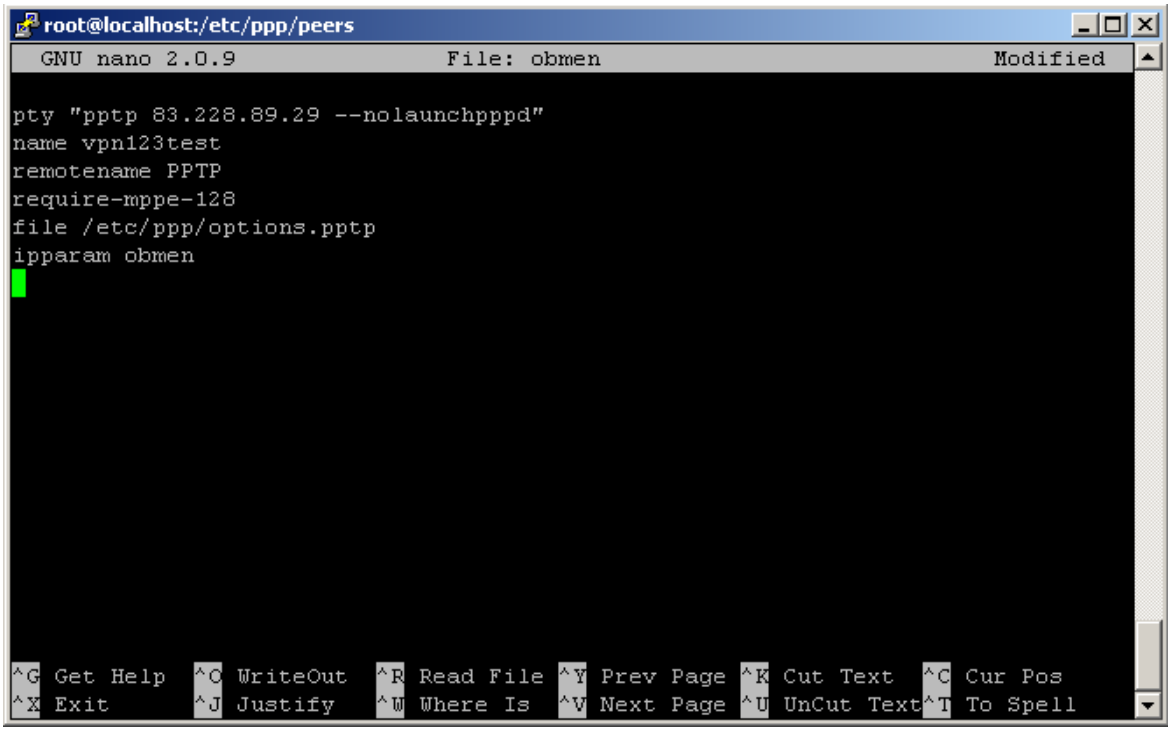
Команда: **#nano obmen**

```
[root@localhost /]#
[root@localhost /]# cd /etc/ppp/peers/
[root@localhost peers]# nano obmen
```

Като съдържание на файла въведете:

При свързаност през Интернет	**При свързаност през ЕЕСМДАНС**
pty "pptp 83.228.89.29 --nolaunchpppd" name vpn123test remotename PPTP require-mppe-128 file /etc/ppp/options.pptp ipparam obmen	pty "pptp 10.89.23.3 --nolaunchpppd" name vpn123test remotename PPTP require-mppe-128 file /etc/ppp/options.pptp ipparam obmen

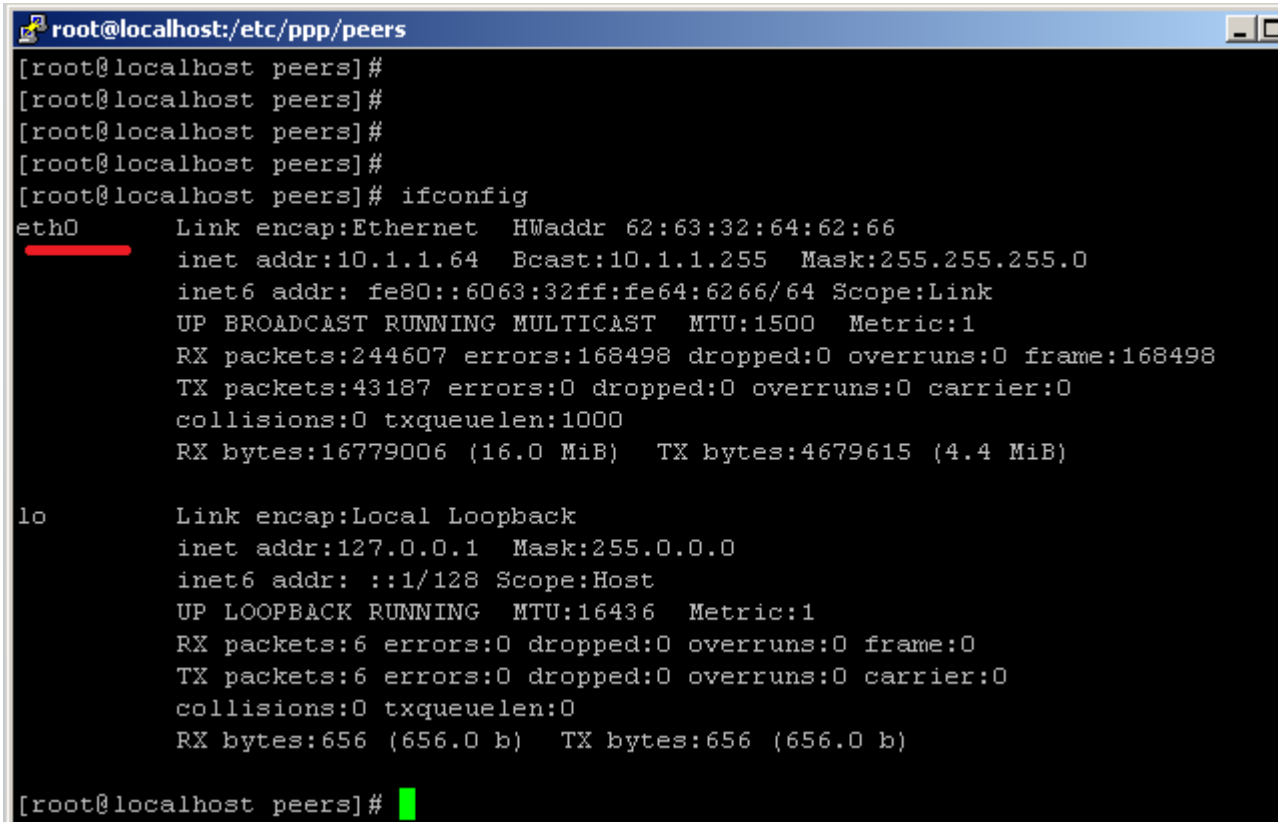
Където срещу **name** поставете вашето потребителско име, а срещу ipparam запишете името на самия файл (в случая obmen)



Запишете файла (Ctrl+O) и излезте от редактора (Ctrl+X)

3. Коригиране на мрежовите настройки
   Примерът е за Fedora/Red Hat/CentOS.

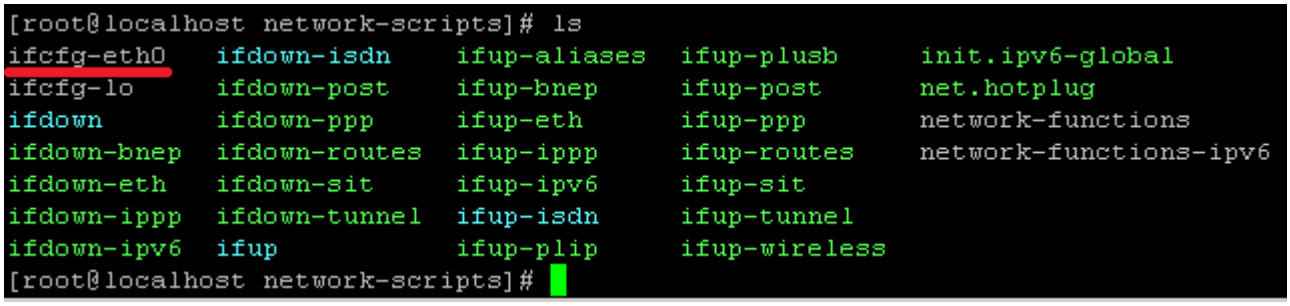
   Команди:
   #ifconfig - показва мрежовите адаптери на компюъра



   В случая мрежовата карта е с име **eth0**

   # cd /etc/sysconfig/network-scripts/ - преминаване в директория cd /etc/sysconfig/network-scripts/

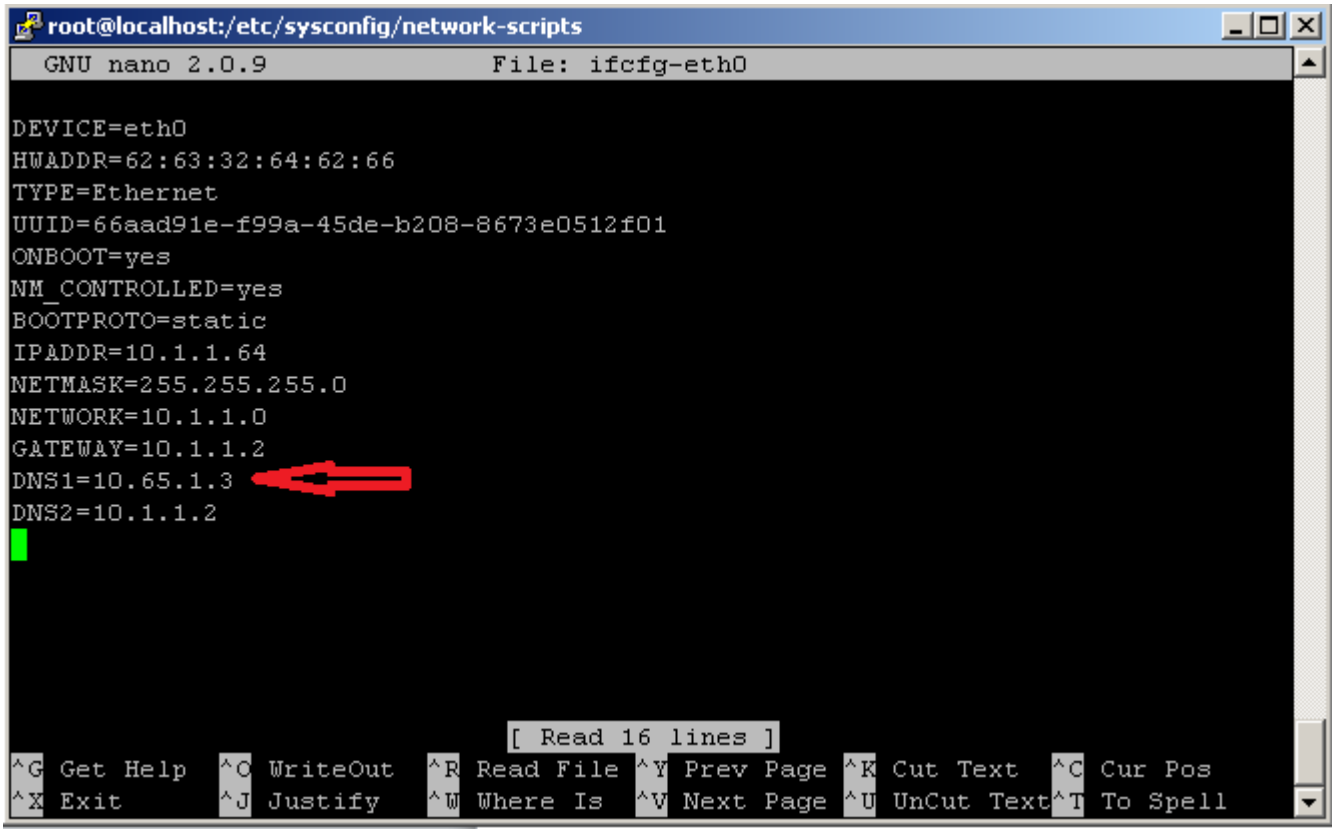
   #ls - показване на съдържанието на директорияра



   В директория /etc/sysconfig/network-scripts/ като използвате текстов редактор заредете файл **ifcfg-име на мрежовата карта**. В случая **ifcfg-et0**

   Команда: **nano ifcfg-eth0**

Променете записите за DNS, като за първи DNS запишете **10.65.1.3**, а за втори и следващ DNS, тези които сте ползвали до момента.



Запишете файла (Ctrl+O) и излезте от редактора (Ctrl+X)

Рестартирайте мрежовата услуга

Команда: **#service network restart**

За всички операционни системи:

Изпълнете команда

#modprobe nf_conntrack_pptp

4. Стартиране на VPN връзката

   Команда: #pppd call [име на файл]
   В случая: **#pppd call obmen**

```
[root@localhost /]#
[root@localhost /]# pppd call obmen
[root@localhost /]#
```

Изпълнете команда **#ifconfig**

```
[root@localhost /]# ifconfig
eth0      Link encap:Ethernet  HWaddr 62:63:32:64:62:66
          inet addr:10.1.1.64  Bcast:10.1.1.255  Mask:255.255.255.0
          inet6 addr: fe80::6063:32ff:fe64:6266/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:247610 errors:171208 dropped:0 overruns:0 frame:171208
          TX packets:43406 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:16968674 (16.1 MiB)  TX bytes:4704580 (4.4 MiB)

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:6 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:656 (656.0 b)  TX bytes:656 (656.0 b)

ppp0      Link encap:Point-to-Point Protocol
          inet addr:10.65.3.200  P-t-P:10.65.1.20  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1396  Metric:1
          RX packets:21 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:3
          RX bytes:1022 (1022.0 b)  TX bytes:80 (80.0 b)

[root@localhost /]#
```

При успешно изградена VPN връзка в списъка с мрежовите адаптери следва да се появи VPN адаптер с присвоен от отдалечения VPN сървър IP адрес (в случая **ppp0** с присвоен адрес 10.65.3.200)

Изпълнете команда #**netstat -tn**

```
[root@localhost /]# netstat -tn
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             Stat
e
tcp        0      0 10.1.1.64:45784             83.228.89.29:1723           ESTA
BLISHED
tcp        0     52 10.1.1.64:22                10.1.1.2:28301              ESTA
BLISHED
tcp        0      0 10.1.1.64:22                10.1.1.2:22331              ESTA
BLISHED
[root@localhost /]#
```

В колона Foreign Address трябва да е наличен IP адреса на отдалечения VPN сървър:1723 в състояние ESTA (established) в колона Stat

5. Създаване на статичен път (static route).

Изпълнете следната команда

#ip route add 10.65.0.0/16 dev ppp0

като замените името на VPN адаптер (в случая **ppp0**) с името, при изпълнение на команда **ifconfig**

6. Тестване на връзката.

Изпълнете команди **ping 10.65.1.15** и **ping register.obmen.local** Сравнете с показания резултат

```
[root@localhost /]# ping 10.65.1.15
PING 10.65.1.15 (10.65.1.15) 56(84) bytes of data.
64 bytes from 10.65.1.15: icmp_seq=1 ttl=63 time=9.81 ms
64 bytes from 10.65.1.15: icmp_seq=2 ttl=63 time=6.72 ms
64 bytes from 10.65.1.15: icmp_seq=3 ttl=63 time=6.90 ms
64 bytes from 10.65.1.15: icmp_seq=4 ttl=63 time=7.88 ms
64 bytes from 10.65.1.15: icmp_seq=5 ttl=63 time=7.90 ms
^C
--- 10.65.1.15 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4193ms
rtt min/avg/max/mdev = 6.729/7.847/9.819/1.104 ms
[root@localhost /]# ping register.obmen.local
PING register.obmen.local (10.65.1.15) 56(84) bytes of data.
64 bytes from 10.65.1.15: icmp_seq=1 ttl=63 time=7.40 ms
64 bytes from 10.65.1.15: icmp_seq=2 ttl=63 time=7.85 ms
64 bytes from 10.65.1.15: icmp_seq=3 ttl=63 time=6.89 ms
64 bytes from 10.65.1.15: icmp_seq=4 ttl=63 time=7.90 ms
^C
--- register.obmen.local ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3291ms
rtt min/avg/max/mdev = 6.899/7.516/7.904/0.406 ms
[root@localhost /]#
```

Ако вашият компютър има инсталиран графичен интерфейс стартирайте браузър и полето за URL адрес въведете **http://test.obmen.local**





6. Спиране на връзката
   За спиране на VPN връзката изпълнете команда

   #killall pppd

7. **Стартиране на връзката**
   ВНИМАНИЕ:

Статичния път, зададен чрез команда ip route add 10.65.0.0/16 dev ppp0 ще е активен докато има активна VPN свързаност. При пропадане на комуникационна свързаност или спиране на връзката чрез killall pppd, този статичен път ще се загуби.

За коректно повторно изграждане на VPN свързаност изпълнете последователно командите:

#killall pppd
#pppd call obmen
#ifconfig
#ip route add 10.65.0.0/16 dev ppp0

В зависимост от използваната операционна система, може да се извършат допълнителни настройки за автоматизиране на някои от процесите.