PPTP Tunnel

Document revision 1.7 (January 16, 2008, 9:10 GMT)
This document applies to V3.0

Table of Contents

General Information

Summary

PPTP (Point to Point Tunnel Protocol) supports encrypted tunnels over IP. The MikroTik RouterOS implementation includes support for both PPTP client and server.

General applications of PPTP tunnels:

- secure router-to-router tunnels over the Internet

- linking (bridging) local Intranets or LANs
- accessing an Intranet/LAN of a company for remote (mobile) clients (employees)

Each PPTP connection is composed of a server and a client. The MikroTik RouterOS may function as a server or client or, for various configurations, it may be the server for some connections and client for other connections. For example, the client created below could connect to a Windows 2000 server, another MikroTik Router, or another router which supports a PPTP server.

Quick Setup Guide

To make a PPTP tunnel between 2 MikroTik routers with IP addresses **10.5.8.104** (PPTP server) and **10.1.0.172** (PPTP client), follow the next steps.

- Configuration on PPTP server router:
  1. Add a user:

```
[admin@PPTP-Server] ppp secret> add name=user password=passwd \
\... local-address=10.0.0.1 remote-address=10.0.0.2
```

  2. Enable the PPTP server:

```
[admin@PPTP-Server] interface pptp-server server> set enabled=yes
```

- Configuration on PPTP client router:
  1. Add the PPTP client:

```
[admin@PPTP-Client] interface pptp-client> add user=user password=passwd \
\... connect-to=10.5.8.104 disabled=no
```

Specifications

Packages required: ***ppp***
License required: ***level1 (limited to 1 tunnel), level3 (limited to 200 tunnels), level5***
Home menu level: ***/interface pptp-server, /interface pptp-client***
Standards and Technologies: ***PPTP (RFC 2637)***
Hardware usage: ***Not significant***

Description

PPTP is a secure tunnel for transporting IP traffic using PPP. PPTP encapsulates PPP in virtual lines that run over IP. PPTP incorporates PPP and MPPE (Microsoft Point to Point Encryption) to make encrypted links. The purpose of this protocol is to make well-managed secure connections between routers as well as between routers and PPTP clients (clients are available for and/or included in almost all OSs including Windows).

Multilink PPP (MP) is supported in order to provide MRRU (the ability to transmit full-sized 1500 and larger packets) and bridging over PPP links (using Bridge Control Protocol (BCP) that allows to send raw Ethernet frames over PPP links). This way it is possible to setup bridging without EoIP. The bridge should either have an administratively set MAC address or an Ethernet-like interface in it, as PPP links do not have MAC addresses.

PPTP includes PPP authentication and accounting for each PPTP connection. Full authentication and accounting of each connection may be done through a RADIUS client or locally.

MPPE 40bit RC4 and MPPE 128bit RC4 encryption are supported.

PPTP traffic uses TCP port 1723 and IP protocol GRE (Generic Routing Encapsulation, IP protocol ID 47), as assigned by the Internet Assigned Numbers Authority (IANA). PPTP can be used with most firewalls and routers by enabling traffic destined for TCP port 1723 and protocol 47 traffic to be routed through the firewall or router.

PPTP connections may be limited or impossible to setup though a masqueraded/NAT IP connection. Please see the Microsoft and RFC links listed below for more information.

Additional Documents

- http://msdn.microsoft.com/library/backgrnd/html/understanding_pptp.htm
- http://support.microsoft.com/support/kb/articles/q162/8/47.asp
- http://www.ietf.org/rfc/rfc2637.txt?number=2637
- http://www.ietf.org/rfc/rfc3078.txt?number=3078
- http://www.ietf.org/rfc/rfc3079.txt?number=3079

PPTP Client Setup

Home menu level: ***/interface pptp-client***

Property Description

add-default-route (*yes* | *no*; default: **no**) - whether to use the server which this client is connected to as its default router (gateway)

allow (*multiple choice: mschap2, mschap1, chap, pap*; default: **mschap2, mschap1, chap, pap**) - the protocol to allow the client to use for authentication

connect-to (*IP address*) - The IP address of the PPTP server to connect to

max-mru (*integer*; default: **1460**) - Maximum Receive Unit. The optimal value is the MRU of the interface the tunnel is working over decreased by 40 (so, for 1500-byte Ethernet link, set the MRU to 1460 to avoid fragmentation of packets)

max-mtu (*integer*; default: **1460**) - Maximum Transmission Unit. The optimal value is the MTU of the interface the tunnel is working over decreased by 40 (so, for 1500-byte Ethernet link, set the MTU to 1460 to avoid fragmentation of packets)

mrru (*integer*: 512..65535; default: **disabled**) - maximum packet size that can be received on the link. If a packet is bigger than tunnel MTU, it will be split into multiple packets, allowing full size IP or Ethernet packets to be sent over the tunnel

- **disabled** - disable MRRU on this link

name (*name*; default: **pptp-outN**) - interface name for reference

password (*text*; default: **""**) - user password to use when logging to the remote server

profile (*name*; default: **default**) - profile to use when connecting to the remote server

user (*text*) - user name to use when logging on to the remote server

Notes

Specifying MRRU means enabling MP (Multilink PPP) over single link. This protocol is used to split big packets into smaller ones. Under Windows it can be enabled in Networking tag, Settings button, "Negotiate multi-link for single link connections". Their MRRU is hardcoded to 1614. This setting is usefull to overcome PathMTU discovery failures. The MP should be enabled on both peers.

Example

To set up PPTP client named **test2** using unsername **john** with password **john** to connect to the **10.1.1.12** PPTP server and use it as the default gateway:

```
[admin@MikroTik] interface pptp-client> add name=test2 connect-to=10.1.1.12 \
\... user=john add-default-route=yes password=john
[admin@MikroTik] interface pptp-client> print
Flags: X - disabled, R - running
  0 X  name="test2" max-mtu=1460 max-mru=1460 mrru=disabled connect-to=10.1.1.12
       user="john" password="john" profile=default add-default-route=yes
       allow=pap,chap,mschap1,mschap2
[admin@MikroTik] interface pptp-client> enable 0
```

Monitoring PPTP Client

Command name: ***/interface pptp-client monitor***

Property Description

encoding (*text*) - encryption and encoding (if asymmetric, separated with '/') being used in this connection

idle-time (*read-only: time*) - time since the last packet has been transmitted over this link

mru (*read-only: integer*) - effective MRU of the link

mtu (*read-only: integer*) - effective MTU of the link

status (*text*) - status of the client

- **dialing** - attempting to make a connection
- **verifying password...** - connection has been established to the server, password verification in progress
- **connected** - self-explanatory
- **terminated** - interface is not enabled or the other side will not establish a connection

uptime (*time*) - connection time displayed in days, hours, minutes and seconds

Example

Example of an established connection:

```
[admin@MikroTik] interface pptp-client> monitor test2
     status: "connected"
     uptime: 6h44m9s
  idle-time: 6h44m9s
   encoding: "MPPE128 stateless"
```

```
        mtu: 1460
        mru: 1460
[admin@MikroTik] interface pptp-client>
```

PPTP Server Setup

Home menu level: ***/interface pptp-server server***

Description

The PPTP server creates a dynamic interface for each connected PPTP client. The PPTP connection count from clients depends on the license level you have. Level1 license allows 1 PPTP client, Level3 or Level4 licenses up to 200 clients, and Level5 or Level6 licenses do not have PPTP client limitations.

Property Description

authentication (*multiple choice: pap | chap | mschap1 | mschap2*; default: **mschap2**) - authentication algorithm

default-profile - default profile to use

enabled (*yes | no*; default: **no**) - defines whether PPTP server is enabled or not

keepalive-timeout (*time*; default: **30**) - defines the time period (in seconds) after which the router is starting to send keepalive packets every second. If no traffic and no keepalive responses has came for that period of time (i.e. 2 * keepalive-timeout), not responding client is proclaimed disconnected

max-mru (*integer*; default: **1460**) - Maximum Receive Unit. The optimal value is the MRU of the interface the tunnel is working over decreased by 40 (so, for 1500-byte ethernet link, set the MRU to 1460 to avoid fragmentation of packets)

max-mtu (*integer*; default: **1460**) - Maximum Transmission Unit. The optimal value is the MTU of the interface the tunnel is working over decreased by 40 (so, for 1500-byte ethernet link, set the MTU to 1460 to avoid fragmentation of packets)

mrru (*integer*: 512..65535; default: **disabled**) - maximum packet size that can be received on the link. If a packet is bigger than tunnel MTU, it will be split into multiple packets, allowing full size IP or Ethernet packets to be sent over the tunnel

- **disabled** - disable MRRU on this link

Notes

Specifying MRRU means enabling MP (Multilink PPP) over single link. This protocol is used to split big packets into smaller ones. Under Windows it can be enabled in Networking tag, Settings button, "Negotiate multi-link for single link connections". Their MRRU is hardcoded to 1614. This setting is usefull to overcome PathMTU discovery failures. The MP should be enabled on both peers.

Example

To enable PPTP server:

```
[admin@MikroTik] interface pptp-server server> set enabled=yes
[admin@MikroTik] interface pptp-server server> print
            enabled: yes
```

```
            max-mtu: 1460
            max-mru: 1460
               mrru: disabled
     authentication: mschap2,mschap1
  keepalive-timeout: 30
    default-profile: default
[admin@MikroTik] interface pptp-server server>
```

PPTP Tunnel Interfaces

Home menu level: ***/interface pptp-server***

Description

There are two types of interface (tunnel) items in PPTP server configuration - static users and dynamic connections. An interface is created for each tunnel established to the given server. Static interfaces are added administratively if there is a need to reference the particular interface name (in firewall rules or elsewhere) created for the particular user. Dynamic interfaces are added to this list automatically whenever a user is connected and its username does not match any existing static entry (or in case the entry is active already, as there can not be two separate tunnel interfaces referenced by the same name). Dynamic interfaces appear when a user connects and disappear once the user disconnects, so it is impossible to reference the tunnel created for that use in router configuration (for example, in firewall), so if you need a persistent rules for that user, create a static entry for him/her. Otherwise it is safe to use dynamic configuration. **Note** that in both cases PPP users must be configured properly - static entries do not replace PPP configuration.

Property Description

client-address (*read-only: IP address*) - shows the IP address of the connected client

encoding (*read-only: text*) - encryption and encoding (if asymmetric, separated with '/') being used in this connection

mru (*read-only: integer*) - client's MRU

mtu (*read-only: integer*) - client's MTU

name (*name*) - interface name

uptime (*read-only: time*) - shows how long the client is connected

user (*name*) - the name of the user that is configured statically or added dynamically

Example

To add a static entry for **ex1** user:

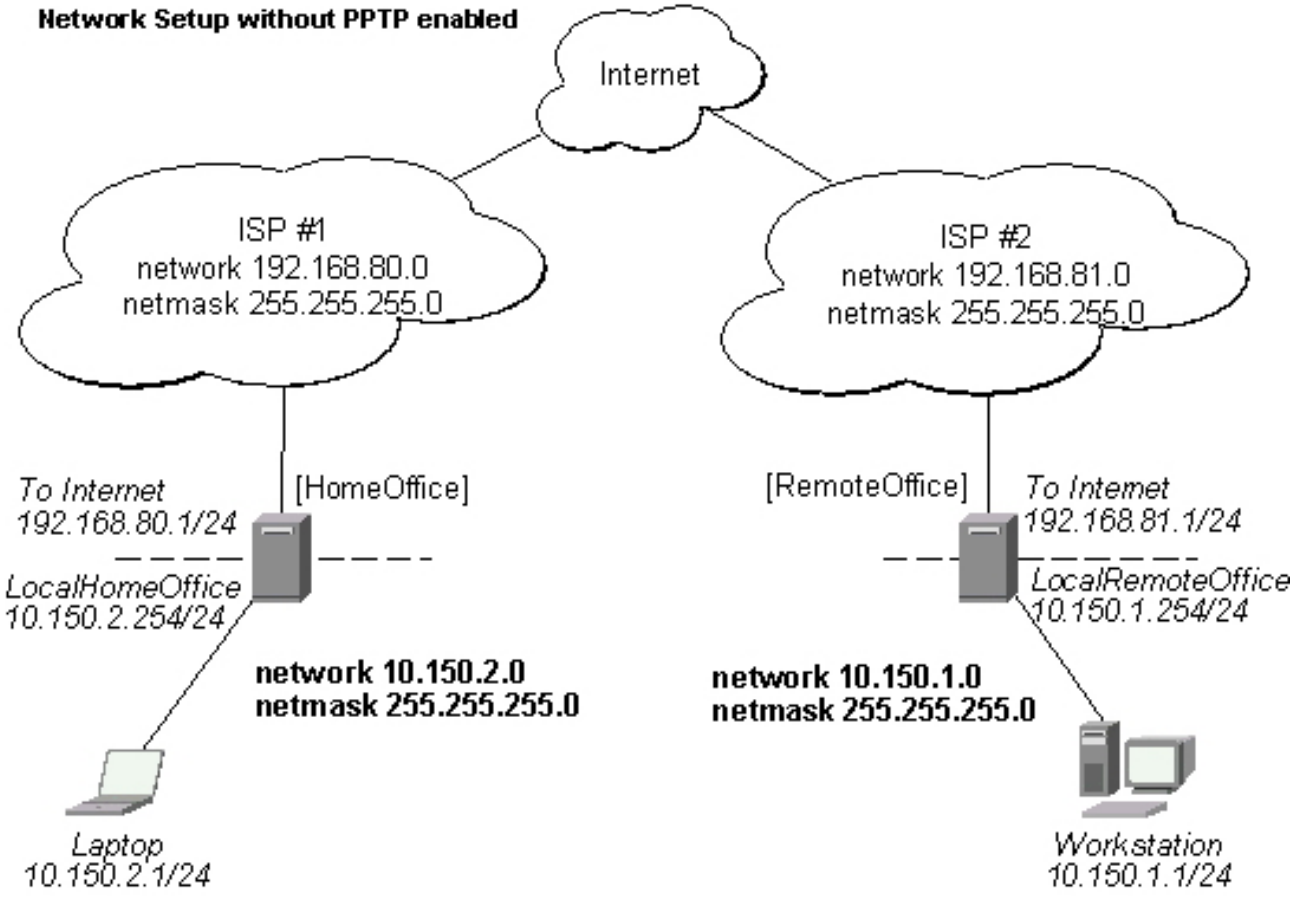
```
[admin@MikroTik] interface pptp-server> add user=ex1
[admin@MikroTik] interface pptp-server> print
Flags: X - disabled, D - dynamic, R - running
  #     NAME                USER         MTU   CLIENT-ADDRESS  UPTIME    ENC...
  0  DR <pptp-ex>           ex           1460  10.0.0.202      6m32s     none
  1     pptp-in1            ex1
[admin@MikroTik] interface pptp-server>
```

In this example an already connected user **ex** is shown besides the one we just added. Now the interface named **pptp-in1** can be referenced from anywhere in RouterOS configuration like a regular interface.

PPTP Application Examples

Router-to-Router Secure Tunnel Example

The following is an example of connecting two Intranets using an encrypted PPTP tunnel over the Internet.



There are two routers in this example:

- [HomeOffice]
  Interface LocalHomeOffice 10.150.2.254/24
  Interface ToInternet 192.168.80.1/24
- [RemoteOffice]
  Interface ToInternet 192.168.81.1/24
  Interface LocalRemoteOffice 10.150.1.254/24

Each router is connected to a different ISP. One router can access another router through the Internet.

On the PPTP server a user must be set up for the client:

```
[admin@HomeOffice] ppp secret> add name=ex service=pptp password=lkjrht \
\... local-address=10.0.103.1 remote-address=10.0.103.2
[admin@HomeOffice] ppp secret> print detail
Flags: X - disabled
  0   name="ex" service=pptp caller-id="" password="lkjrht" profile=default
      local-address=10.0.103.1 remote-address=10.0.103.2 routes==""
```

```
[admin@HomeOffice] ppp secret>
```

Then the user should be added in the PPTP server list:

```
[admin@HomeOffice] interface pptp-server> add user=ex
[admin@HomeOffice] interface pptp-server> print
Flags: X - disabled, D - dynamic, R - running
  #     NAME                USER         MTU   CLIENT-ADDRESS  UPTIME   ENC...
  0     pptp-in1            ex
[admin@HomeOffice] interface pptp-server>
```

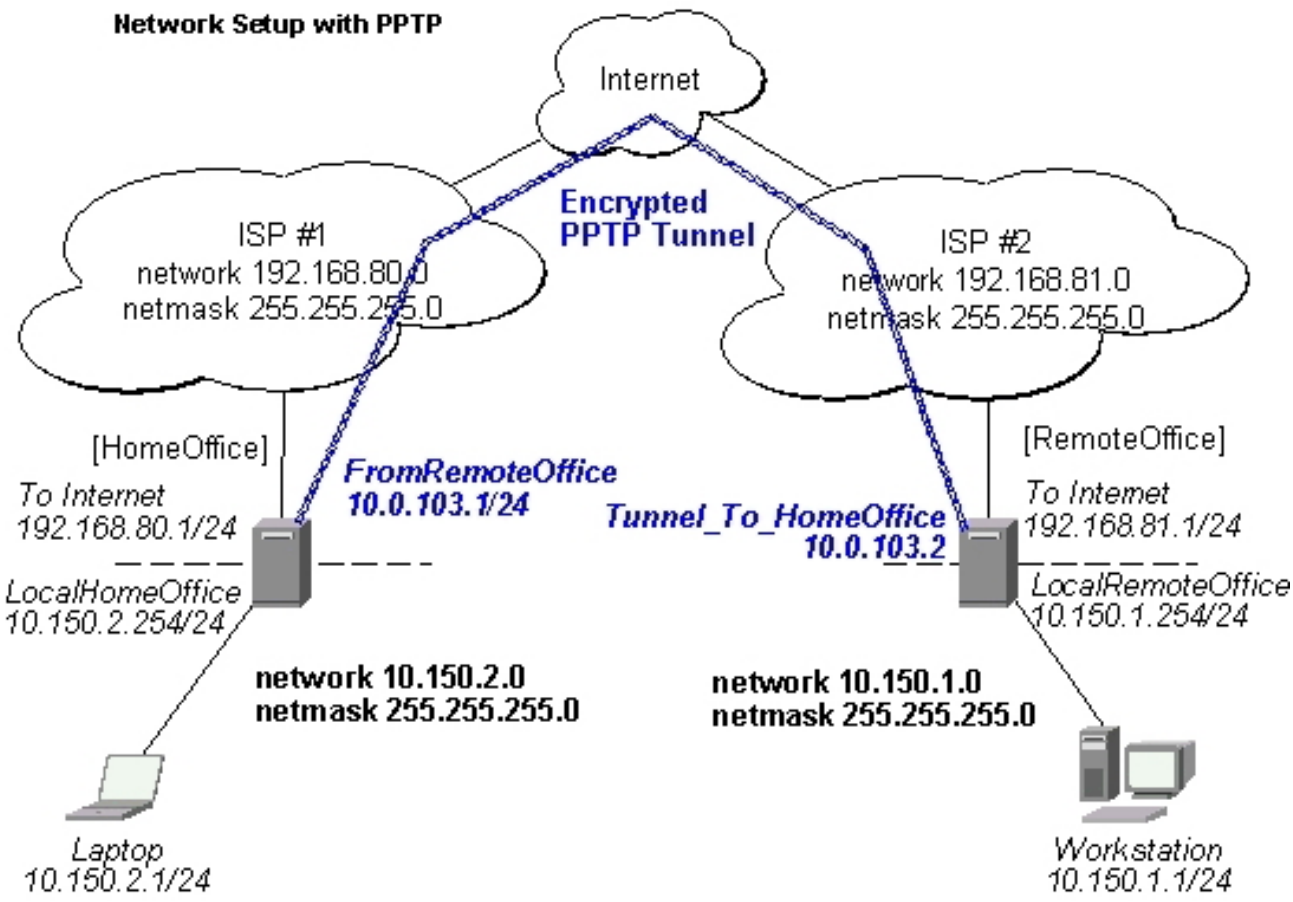
And finally, the server must be enabled:

```
[admin@HomeOffice] interface pptp-server server> set enabled=yes
[admin@HomeOffice] interface pptp-server server> print
            enabled: yes
            max-mtu: 1460
            max-mru: 1460
               mrru: disabled
     authentication: mschap2
  keepalive-timeout: 30
    default-profile: default
[admin@HomeOffice] interface pptp-server server>
```

Add a PPTP client to the RemoteOffice router:

```
[admin@RemoteOffice] interface pptp-client> add connect-to=192.168.80.1 user=ex \
\... password=lkjrht disabled=no
[admin@RemoteOffice] interface pptp-client> print
Flags: X - disabled, R - running
  0  R name="pptp-out1" mtu=1460 mru=1460 mrru=disabled connect-to=192.168.80.1
       user="ex" password="lkjrht" profile=default add-default-route=no
       allow=pap,chap,mschap1,mschap2
[admin@RemoteOffice] interface pptp-client>
```

Thus, a PPTP tunnel is created between the routers. This tunnel is like an Ethernet point-to-point connection between the routers with IP addresses 10.0.103.1 and 10.0.103.2 at each router. It enables 'direct' communication between the routers over third party networks.



To route the local Intranets over the PPTP tunnel you need to add these routes:

```
[admin@HomeOffice] > ip route add dst-address 10.150.1.0/24 gateway 10.0.103.2
[admin@RemoteOffice] > ip route add dst-address 10.150.2.0/24 gateway 10.0.103.1
```

On the PPTP server it can alternatively be done using **routes** parameter of the user configuration:

```
[admin@HomeOffice] ppp secret> print detail
Flags: X - disabled
  0   name="ex" service=pptp caller-id="" password="lkjrht" profile=default
      local-address=10.0.103.1 remote-address=10.0.103.2 routes==""

[admin@HomeOffice] ppp secret> set 0 routes="10.150.1.0/24 10.0.103.2 1"
[admin@HomeOffice] ppp secret> print detail
Flags: X - disabled
  0   name="ex" service=pptp caller-id="" password="lkjrht" profile=default
      local-address=10.0.103.1 remote-address=10.0.103.2
      routes="10.150.1.0/24 10.0.103.2 1"

[admin@HomeOffice] ppp secret>
```

Test the PPTP tunnel connection:

```
[admin@RemoteOffice]> /ping 10.0.103.1
10.0.103.1 pong: ttl=255 time=3 ms
10.0.103.1 pong: ttl=255 time=3 ms
10.0.103.1 pong: ttl=255 time=3 ms
ping interrupted
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 3/3.0/3 ms
```

Test the connection through the PPTP tunnel to the LocalHomeOffice interface:

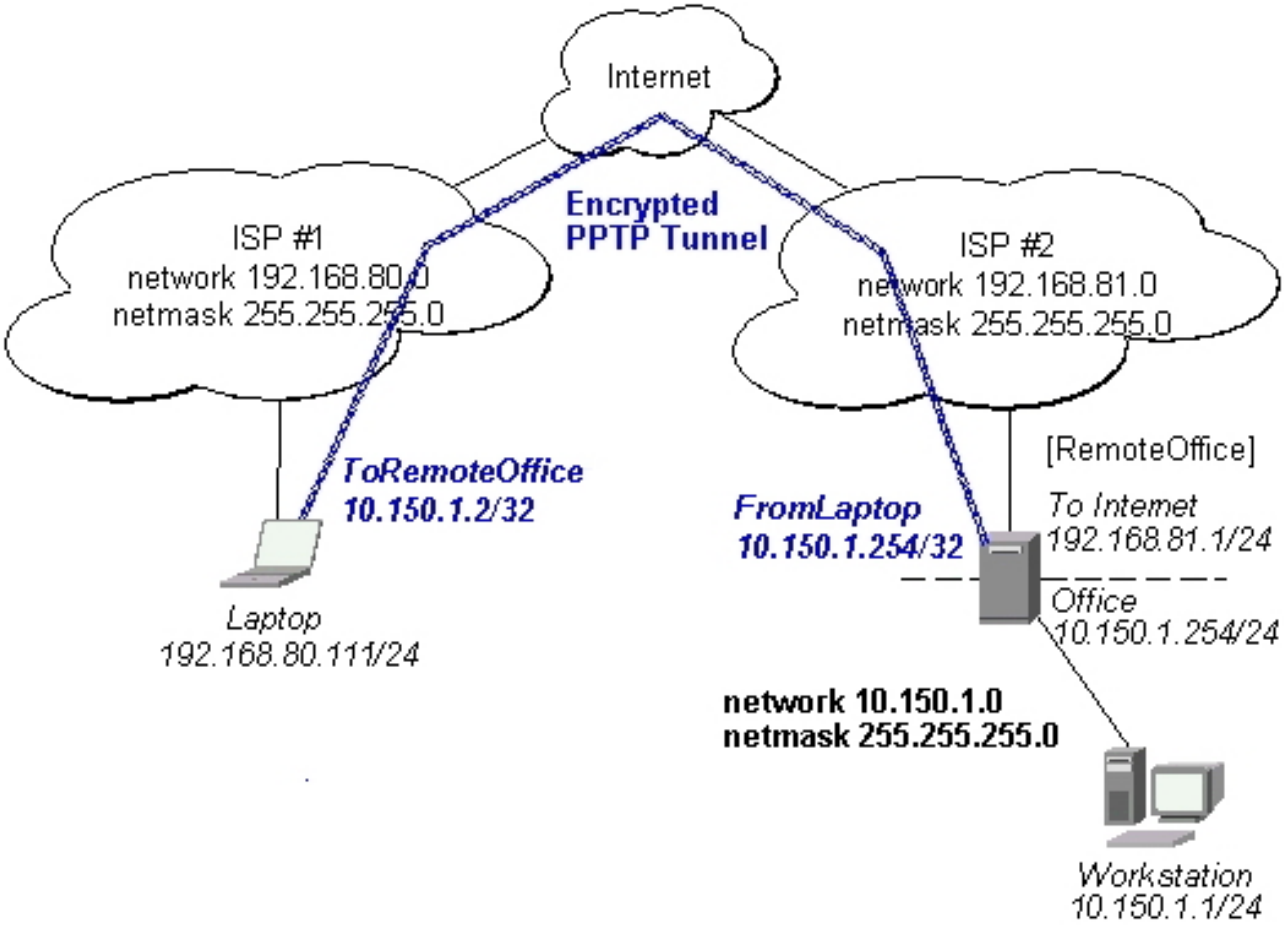
```
[admin@RemoteOffice]> /ping 10.150.2.254
10.150.2.254 pong: ttl=255 time=3 ms
10.150.2.254 pong: ttl=255 time=3 ms
10.150.2.254 pong: ttl=255 time=3 ms
ping interrupted
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 3/3.0/3 ms
```

To bridge a LAN over this secure tunnel, please see the example in the 'EoIP' section of the manual. To set the maximum speed for traffic over this tunnel, please consult the 'Queues' section.

Connecting a Remote Client via PPTP Tunnel

The following example shows how to connect a computer to a remote office network over PPTP encrypted tunnel giving that computer an IP address from the same network as the remote office has (without need of bridging over EoIP tunnels)

Please, consult the respective manual on how to set up a PPTP client with the software You are using.



The router in this example:

- [RemoteOffice]
  Interface ToInternet 192.168.81.1/24
  Interface Office 10.150.1.254/24

The client computer can access the router through the Internet.

On the PPTP server a user must be set up for the client:

```
[admin@RemoteOffice] ppp secret> add name=ex service=pptp password=lkjrht
local-address=10.150.1.254 remote-address=10.150.1.2
[admin@RemoteOffice] ppp secret> print detail
Flags: X - disabled
  0   name="ex" service=pptp caller-id="" password="lkjrht" profile=default
      local-address=10.150.1.254 remote-address=10.150.1.2 routes==""

[admin@RemoteOffice] ppp secret>
```

Then the user should be added in the PPTP server list:

```
[admin@RemoteOffice] interface pptp-server> add name=FromLaptop user=ex
[admin@RemoteOffice] interface pptp-server> print
Flags: X - disabled, D - dynamic, R - running
  #     NAME                USER         MTU   CLIENT-ADDRESS  UPTIME   ENC...
  0     FromLaptop          ex
[admin@RemoteOffice] interface pptp-server>
```

And the server must be enabled:

```
[admin@RemoteOffice] interface pptp-server server> set enabled=yes
[admin@RemoteOffice] interface pptp-server server> print
            enabled: yes
            max-mtu: 1460
            max-mru: 1460
               mrru: disabled
     authentication: mschap2
  keepalive-timeout: 30
    default-profile: default
[admin@RemoteOffice] interface pptp-server server>
```

Finally, the proxy APR must be enabled on the 'Office' interface:

```
[admin@RemoteOffice] interface ethernet> set Office arp=proxy-arp
[admin@RemoteOffice] interface ethernet> print
Flags: X - disabled, R - running
  #    NAME                MTU   MAC-ADDRESS       ARP
  0  R ToInternet          1500  00:30:4F:0B:7B:C1 enabled
  1  R Office              1500  00:30:4F:06:62:12 proxy-arp
[admin@RemoteOffice] interface ethernet>
```

PPTP Setup for Windows

Microsoft provides PPTP client support for Windows NT, 2000, ME, 98SE, and 98. Windows 98SE, 2000, and ME include support in the Windows setup or automatically install PPTP. For 95, NT, and 98, installation requires a download from Microsoft. Many ISPs have made help pages to assist clients with Windows PPTP installation.

- http://www.real-time.com/Customer_Support/PPTP_Config/pptp_config.html
- http://www.microsoft.com/windows95/downloads/contents/WUAdminTools/S_WUNetworkingTools/W95WinsockU

Sample instructions for PPTP (VPN) installation and client setup - Windows 98SE

If the VPN (PPTP) support is installed, select 'Dial-up Networking' and 'Create a new connection'. The option to create a 'VPN' should be selected. If there is no 'VPN' options, then follow the installation instructions below. When asked for the 'Host name or IP address of the VPN server', type the IP address of the router. Double-click on the 'new' icon and type the correct user name and password (must also be in the user

database on the router or RADIUS server used for authentication).

The setup of the connections takes nine seconds after selection the 'connect' button. It is suggested that the connection properties be edited so that 'NetBEUI', 'IPX/SPX compatible', and 'Log on to network' are unselected. The setup time for the connection will then be two seconds after the 'connect' button is selected.

To install the 'Virtual Private Networking' support for Windows 98SE, go to the 'Setting' menu from the main 'Start' menu. Select 'Control Panel', select 'Add/Remove Program', select the 'Windows setup' tab, select the 'Communications' software for installation and 'Details'. Go to the bottom of the list of software and select 'Virtual Private Networking' to be installed.

Troubleshooting

Description

- **I use firewall and I cannot establish PPTP connection**
  Make sure the TCP connections to port 1723 can pass through both directions between your sites. Also, IP protocol 47 should be passed through