Manual:Interface/PPTP

From MikroTik Wiki

< Manual:Interface

Contents

Summary

Standards: RFC 2637

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 the sending of 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 128bit RC4 encryption is 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.

PPTP Client

Sub-menu: `/interface pptp-client`

Properties

Property	Description
`add-default-route` (*yes | no*; Default: **no**)	Whether to add PPTP remote address as a default route.
`allow` (*mschap2 | mschap1 | chap | pap*; Default: **mschap2, mschap1, chap, pap**)	Allowed authentication methods.
`connect-to` (*IP*; Default:)	Remote address

	of PPTP server
default-route-distance (*byte [0..255]*; Default: **1**)	sets distance value applied to auto created default route, if `add-default-route` is also selected
dial-on-demand (*yes / no*; Default: **no**)	connects to PPTP server only when outbound traffic is generated. If selected, then route with

	gateway address from 10.112.112.0/24 network will be added while connection is not established.
disabled (*yes* | *no*; Default: **yes**)	Whether interface is disabled or not. By default it is disabled
keepalive-timeout (*integer*; Default: **60**)	Sets keepalive timeout in

	seconds.
max-mru (*integer*; Default: **1460**)	Maximum Receive Unit. Max packet size that PPTP interface will be able to receive without packet fragmentation.
max-mtu (*integer*; Default: **1460**)	Maximum Transmission Unit. Max packet size that PPTP interface will be

	able to send without packet fragmentation.
mrru (*disabled | integer*; 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. `Read more >>`
name (*string*; Default:)	Descriptive name of the interface.
password (*string*; Default: "")	Password used for authentication.
profile (*name*; Default: **default-encryption**)	Used PPP profile.
user (*string*; Default:)	User name used for authentication.

Quick example

This example demonstrates how to set up PPTP client with username "pptp-hm", password "123" and server 10.1.101.100

```
/interface pptp-client add name=pptp-hm user=pptp-hm password=123 connect-to=10.1.101.100 disabled=no
```

```
/interface pptp-client print detail
```

```
Flags: X - disabled, R - running
 0   name="pptp-hm" max-mtu=1460 max-mru=1460 mrru=disabled
     connect-to=10.1.101.100 user="pptp-hm" password="123"
     profile=default-encryption add-default-route=no dial-on-demand=no
     allow=pap,chap,mschap1,mschap2
```

PPTP Server

Sub-menu: `/interface pptp-server`

This sub-menu shows interfaces for each connected PPTP clients.

An interface is created for each tunnel established to the given server. There are two types of interfaces in PPTP server's configuration

- 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 persistent rules for that user, create a static entry for him/her. Otherwise it is safe to use dynamic configuration.

> **Note:** in both cases PPP users must be configured properly - static entries do not replace PPP configuration.

Server configuration

Sub-menu: `/interface pptp-server server`

Properties

Property	Description
authentication (*pap* | *chap* | *mschap1* | *mschap2*; Default: **mschap1,mschap2**)	Authentication methods that server will accept.
default-profile (*name*; Default: **default-encryption**)	Default PPP Profile to use
enabled (*yes* | *no*; Default: **no**)	Defines whether PPTP server is enabled or not.
keepalive-timeout (*time*; Default: **30**)	

If server during keepalive period does not receive any packet, it will send keepalive packets every second five times. If the server does not receives response from

	the client, then disconnect after 5 seconds. Logs will show 5x "LCP missed echo reply" messages and then disconnect.
`max-mru` (*integer*; Default: **1460**)	Maximum Receive Unit. Max packet

	size that PPTP interface will be able to receive without packet fragmentation.
`max-mtu` (*integer*; Default: **1460**)	Maximum Transmission Unit. Max packet size that PPTP interface will be able to

	send without packet fragmentation.
mrru (*disabled | integer*; 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. Read more >>

To enable PPTP server:

```
/interface pptp-server server set enabled=yes
```

```
/interface pptp-server server print
          enabled: yes
          max-mtu: 1460
          max-mru: 1460
             mrru: disabled
   authentication: mschap2,mschap1
 keepalive-timeout: 30
   default-profile: default
```

Monitoring

Monitor command can be used to monitor status of the tunnel on both client and server.

```
/interface pptp-client monitor 0
     status: "connected"
     uptime: 7h24m18s
  idle-time: 6h21m4s
   encoding: "MPPE128 stateless"
        mtu: 1460
        mru: 1460
```

Read-only properties

Property	Description
status ()	Current PPTP status. Value other than "connected" indicates that there are some problems establishing tunnel.
uptime (*time*)	

|	Elapsed time since tunnel was established.
`idle-time` (*time*)	Elapsed time since last activity on the tunnel.
`encoding` ()	Used encryption method
`mtu` (*integer*)	Negotiated and used MTU
`mru` (*integer*)	

Application Examples

Connecting Remote Client

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

Consider following setup:
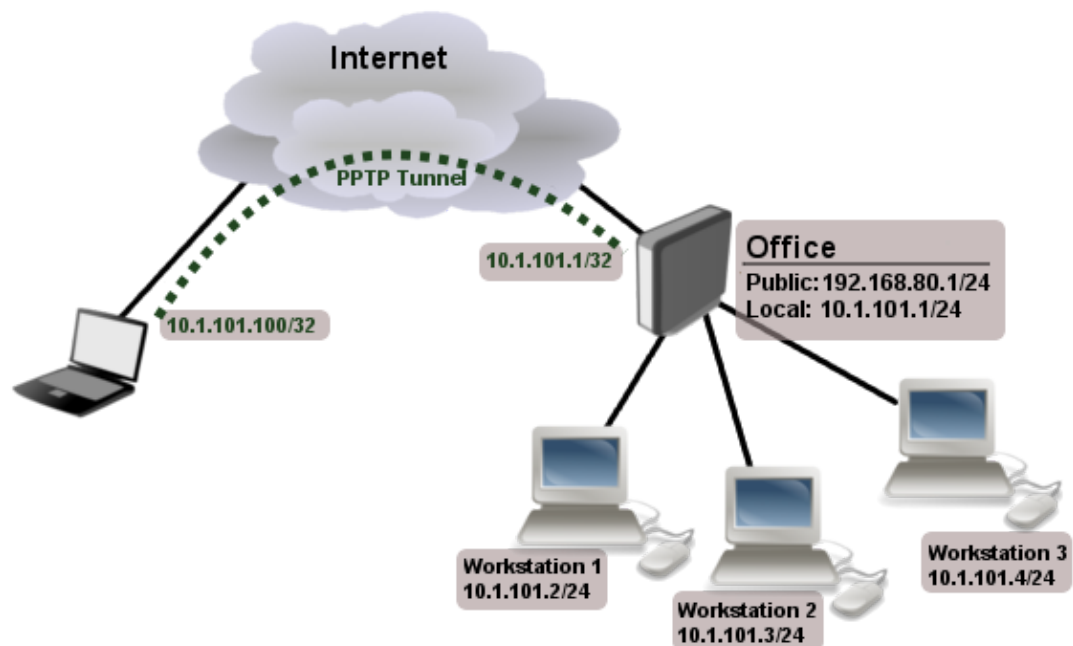
Office router is connected to internet through **ether1**. Workstations are connected to **ether2**. Laptop is connected to the internet and can reach Office router's public IP (in our example it is 192.168.80.1).

First step is to create a user

```
/ppp secret add name=Laptop service=pptp password=123 local-address=10.1.101.1 \
    remote-address=10.1.101.100
```

```
/ppp secret print detail
Flags: X - disabled
  0   name="Laptop" service=pptp caller-id="" password="123" profile=default
      local-address=10.1.101.1 remote-address=10.1.101.100 routes==""
```

Notice that the PPTP local address is the same as the router's address on the local interface and the remote address is from the same range as the local network (10.1.101.0/24).

Next step is to enable the PPTP server and the PPTP client on the laptop.

```
/interface pptp-server server set enabled=yes
```

```
/interface pptp-server server print
          enabled: yes
          max-mtu: 1460
          max-mru: 1460
             mrru: disabled
   authentication: mschap2
 keepalive-timeout: 30
   default-profile: default
```

PPTP client from the laptop should connect to routers public IP which in our example is 192.168.80.1.
(Consult the respective manual on how to set up a PPTP client with the operating system software you are using).

At this point (when PPTP client is successfully connected) if you try to ping any workstation form the laptop, the ping will time out because the Laptop is unable to get ARPs from workstations. The solution is to set up `proxy-arp` on the local interface.

```
/interface ethernet set Office arp=proxy-arp
```

```
/interface ethernet print
Flags: X - disabled, R - running
  #    NAME                     MTU    MAC-ADDRESS            ARP
```
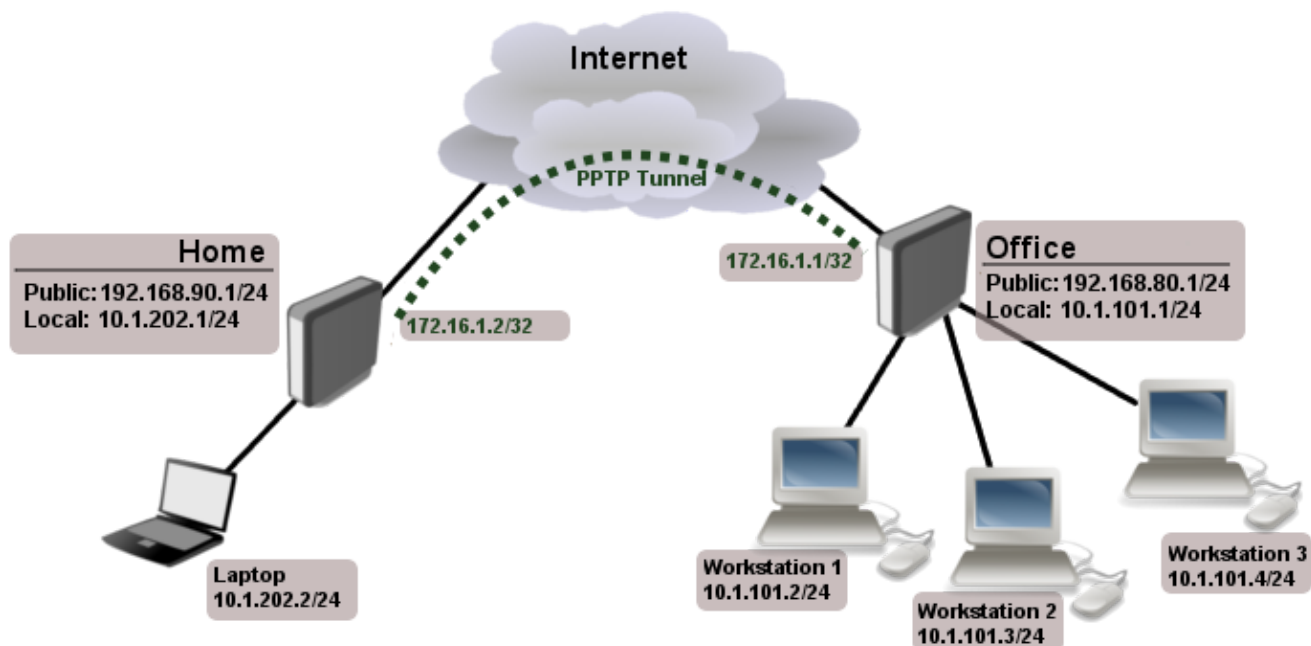
```
 0   R ether1               1500  00:30:4F:0B:7B:C1 enabled
 1   R ether2               1500  00:30:4F:06:62:12 proxy-arp
```

After `proxy-arp` is enabled, the remote client can successfully reach all workstations in the local network behind the router.

Site-to-Site PPTP

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

Consider following setup:

Office and Home routers are connected to the internet through **ether1**, workstations and laptops are connected to **ether2**. Both local networks are routed through a PPTP client, thus they are not in the same broadcast domain. If both networks should be in the same broadcast domain then you need to use BCP and bridge the PPTP tunnel with the local interface.

First step is to create a user

```
/ppp secret add name=Home service=pptp password=123 local-address=172.16.1.1 \
  remote-address=172.16.1.2 routes="10.1.202.0/24 172.16.1.2 1"
```

```
/ppp secret print detail
Flags: X - disabled
  0   name="Home" service=pptp caller-id="" password="123" profile=default
      local-address=172.16.1.1 remote-address=172.16.1.2 routes=="10.1.202.0/24 172.16.1.2 1"
```

Notice that we set up PPTP server's PPP secret where a route is added automatically whenever the client connects. If this option is not set, then you will need to add static routing on the server to route traffic between the two sites through the PPTP tunnel. (See PPP User Database for more info on `routes` variable).

Next step is to enable the PPTP server on the office router and configure the PPTP client on the Home router.

```
/interface pptp-server server set enabled=yes
```

```
/interface pptp-server server> print
          enabled: yes
          max-mtu: 1460
          max-mru: 1460
             mrru: disabled
   authentication: mschap2
 keepalive-timeout: 30
   default-profile: default
```

```
/interface pptp-client add user=Home password=123 connect-to=192.168.80.1 disabled=no
```

```
/interface pptp-client print
Flags: X - disabled, R - running
 0    name="pptp-out1" max-mtu=1460 max-mru=1460 mrru=disabled connect-to=192.168.80.1 user="Home"
      password="123" profile=default-encryption add-default-route=no dial-on-demand=no
      allow=pap,chap,mschap1,mschap2
```

Now we need to add the route to reach the local network behind the Home router

```
/ip route add dst-address=10.1.101.0/24 gateway=pptp-out1
```

Now after the tunnel is established and routes are set, you should be able to ping remote network.

Read More

- BCP (Bridge Control Protocol)
- http://technet.microsoft.com/en-us/library/cc768084.aspx
- 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

[Top | Back to Content]

- This page was last edited on 4 January 2017, at 16:46.