PPPoE

Document revision 1.4 (Fri Apr 30 06:43:11 GMT 2004)
This document applies to V2.8

Table of Contents

Table of Contents
General Information
  Summary
  Quick Setup Guide
  Specifications
  Related Documents
  Additional Documents
PPPoE Client Setup
  Description
  Property Description
  Notes
  Example
Monitoring PPPoE Client
  Property Description
  Example
PPPoE Server Setup (Access Concentrator)
  Description
  Property Description
  Notes
  Example
PPPoE Server Users
  Property Description
  Example
Troubleshooting
  Description
Application Examples
  PPPoE in a multipoint wireless 802.11 network

General Information

Summary

The PPPoE (Point to Point Protocol over Ethernet) protocol provides extensive user management, network management and accounting benefits to ISPs and network administrators. Currently PPPoE is used mainly by ISPs to control client connections for xDSL and cable modems as well as plain Ethernet networks. PPPoE is an extension of the standard Point to Point Protocol (PPP). The difference between them is expressed in transport method: PPPoE employs Ethernet instead of modem connection.

Generally speaking, PPPoE is used to hand out IP addresses to clients based on the user (and workstation, if desired) authentication as opposed to workstation only authentication, when static IP addresses or DHCP are used. It is advised not to use static IP addresses or DHCP on the same interfaces as PPPoE for security
reasons.

MikroTik RouterOS can act as a RADIUS client - you can use a RADIUS server to authenticate PPPoE clients and use accounting for them.

A PPPoE connection is composed of a client and an access concentrator (server). The client may be a Windows computer that has the PPPoE client protocol installed. The MikroTik RouterOS supports both - client and access concentrator implementations of PPPoE. The PPPoE client and server work over any Ethernet level interface on the router - wireless 802.11 (Aironet, Cisco, WaveLan, Prism, Atheros), 10/100/1000 Mbit/s Ethernet, RadioLan and EoIP (Ethernet over IP tunnel). No encryption, MPPE 40bit RSA and MPPE 128bit RSA encryption is supported.

**Note** that when RADIUS server is authenticating a user with CHAP, MS-CHAPv1, MS-CHAPv2, it does not use shared secret, it is used only in authentication reply. So if you have a wrong shared secret, RADIUS server will accept the request. You can use `/radius monitor` command to see **bad-replies** parameter. This value should increase whenever a client tries to connect.

**Supported connections**

- MikroTik RouterOS PPPoE client to any PPPoE server (access concentrator)
- MikroTik RouterOS server (access concentrator) to multiple PPPoE clients (clients are available for almost all operating systems and some routers)

**Quick Setup Guide**

- To configure MikroTik RouterOS to be a PPPoE client
  1. Just add a pppoe-client:

```
interface pppoe-client add name=pppoe-user-mike user=mike password=123 interface=wlan1
... service-name=internet disabled=no
```

- To configure MikroTik RouterOS to be an Access Concentrator (PPPoE Server)
  1. Add an address pool for the clients from **10.1.1.62** to **10.1.1.72**, called pppoe-pool:

```
ip pool add name="pppoe-pool" ranges=10.1.1.62-10.1.1.72
```

  2. Add PPP profile, called **pppoe-profile** where **local-address** will be the router's address and clients will have an address from **pppoe-pool**:

```
/ppp profile add name="pppoe-profile" local-address=10.1.1.1 remote-address=pppoe-pool
```

  3. Add a user with username **mike** and password **123**:

```
/ppp secret add name=mike password=123 service=pppoe profile=pppoe-profile
```

  4. Now add a pppoe server:

```
interface pppoe-server server add service-name=internet interface=wlan1
... default-profile=pppoe-profile
```

**Specifications**
Packages required: **ppp**
License required: **level1 (limited to 1 interface), level3 (limited to 200 interfaces), level4 (limited to 200 interfaces), level5 (limited to 500 interfaces), level6 (unlimited)**
Home menu level: */interface pppoe-server, /interface pppoe-client*
Standards and Technologies: **PPPoE (RFC 2516)**
Hardware usage: **PPPoE server may require additional RAM (uses approx. 50kB for each connection) and CPU power. Supports maximum of 10000 connections**

**Related Documents**
- **Package Management**
- **IP Addresses and ARP**
- **Log Management**

**Additional Documents**

Links for PPPoE documentation:

PPPoE Clients:
- RASPPPoE for Windows 95, 98, 98SE, ME, NT4, 2000, XP, .NET
  [http://user.cs.tu-berlin.de/~normanb](http://user.cs.tu-berlin.de/~normanb)

**PPPoE Client Setup**

Home menu level: */interface pppoe-client*

**Description**

The PPPoE client supports high-speed connections. It is fully compatible with the MikroTik PPPoE server (access concentrator).

**Note for Windows.** Some connection instructions may use the form where the "phone number" us "MikroTik_AC\mt1" to indicate that "MikroTik_AC" is the access concentrator name and "mt1" is the service name.

**Property Description**

**name** (*name*; default: **pppoe-out1**) - name of the PPPoE interface

**interface** (*name*) - interface the PPPoE server can be connected through

**mtu** (*integer*; default: **1480**) - Maximum Transmission Unit. The optimal value is the MTU of the interface the tunnel is working over decreased by 20 (so, for 1500-byte ethernet link, set the MTU to 1480 to avoid fragmentation of packets)

**mru** (*integer*; default: **1480**) - Maximum Receive Unit. The optimal value is the MTU of the interface the tunnel is working over decreased by 20 (so, for 1500-byte ethernet link, set the MTU
to 1480 to avoid fragmentation of packets)

user (text; default: "") - a user name that is present on the PPPoE server

password (text; default: "") - a user password used to connect the PPPoE server

profile (name) - default profile for the connection

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

service-name (text; default: "") - specifies the service name set on the access concentrator. Leave it blank unless you have many services and need to specify the one you need to connect to

ac-name (text; default: "") - this may be left blank and the client will connect to any access concentrator that offers the "service" name selected

add-default-route (yes | no; default: no) - whether to add a default route automatically

dial-on-demand (yes | no; default: no) - connects to AC only when outbound traffic is generated and disconnects when there is no traffic for the period set in the idle-timeout value

use-peer-dns (yes | no; default: no) - whether to set the router's default DNS to the PPP peer DNS (i.e. whether to get DNS settings from the peer)

Notes

If there is a default route, add-default-route will not create a new one.

Example

To add and enable PPPoE client on the gig interface connecting to the AC that provides testSN service using user name john with the password password:

```bash
[admin@RemoteOffice] interface pppoe-client> add interface=gig \
... service-name=testSN user=john password=password disabled=no
[admin@RemoteOffice] interface pppoe-client> print
Flags: X - disabled, R - running
0 R name="pppoe-out1" mtu=1480 mru=1480 interface=gig user="john"
password="password" profile=default service-name="testSN" ac-name=""
add-default-route=no dial-on-demand=no use-peer-dns=no
```

Monitoring PPPoE Client

Command name: /interface pppoe-client monitor

Property Description

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

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

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

**service-name** *(text)* - name of the service the client is connected to

**ac-name** *(text)* - name of the AC the client is connected to

**ac-mac** *(MAC address)* - MAC address of the access concentrator (AC) the client is connected to

**Example**

To monitor the **pppoe-out1** connection:

```
[admin@MikroTik] interface pppoe-client> monitor pppoe-out1
    status: "connected"
    uptime: 10s
    encoding: "none"
    service-name: "testSN"
    ac-name: "10.0.0.1"
    ac-mac: 00:C0:DF:07:5E:E6
[admin@MikroTik] interface pppoe-client>
```

**PPPoE Server Setup (Access Concentrator)**

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

**Description**

The PPPoE server (access concentrator) supports multiple servers for each interface - with differing service names. Currently the throughput of the PPPoE server has been tested to 160 Mb/s on a Celeron 600 CPU. Using higher speed CPUs, throughput should increase proportionately.

The **access concentrator name** and PPPoE **service name** are used by clients to identity the access concentrator to register with. The **access concentrator name** is the same as the **identity** of the router displayed before the command prompt. The identity may be set within the /system identity submenu.

PPPoE users are created in /ppp secret menu, see the AAA manual for further information.

**Note** that if no service name is specified in WindowsXP, it will use only service with no name. So if you want to serve WindowsXP clients, leave your service name empty.

**Property Description**

**service-name** *(text)* - the PPPoE service name

**mtu** *(integer; default: 1480)* - Maximum Transmission Unit. The optimal value is the MTU of the interface the tunnel is working over decreased by 20 (so, for 1500-byte Ethernet link, set the MTU to 1480 to avoid fragmentation of packets)

**mru** *(integer; default: 1480)* - Maximum Receive Unit. The optimal value is the MTU of the interface the tunnel is working over decreased by 20 (so, for 1500-byte Ethernet link, set the MTU to 1480 to avoid fragmentation of packets)

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

**keepalive-timeout** - 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.

**one-session-per-host** (yes | no; default: no) - allow only one session per host (determined by MAC
address). If a host will try to establish a new session, the old one will be closed

**default-profile** (name; default: default) - default profile to use

**Notes**

The default *keepalive-timeout* value of 10 is OK in most cases. If you set it to 0, the router will not
disconnect clients until they log out or router is restarted. To resolve this problem, the
**one-session-per-host** property can be used.

**Security issue:** do not assign an IP address to the interface you will be receiving the PPPoE requests on.

**Example**

To add PPPoE server on ether1 interface providing ex service and allowing only one connection per host:

```bash
[admin@MikroTik] interface pppoe-server server> add interface=ether1 \
... service-name=ex one-session-per-host=yes
[admin@MikroTik] interface pppoe-server server> print
Flags: X - disabled
  0 X service-name="ex" interface=ether1 mtu=1480 mru=1480
  authentication=mschap2,mschap,chap,pap keepalive-timeout=10
  one-session-per-host=yes default-profile=default
[admin@MikroTik] interface pppoe-server server>
```

**PPPoE Server Users**

Home menu level: /interface pppoe-server

**Property Description**

- **name** (name) - interface name
- **service-name** (name) - name of the service the user is connected to
- **remote-address** (MAC address) - MAC address of the connected client
- **user** (name) - the name of the connected user
- **encoding** (text) - encryption and encoding (if asymmetric, separated with '/') being used in this
  connection
- **uptime** - shows how long the client is connected

**Example**

To view the currently connected users:

```bash
[admin@MikroTik] interface pppoe-server> print
Flags: R - running
  # NAME SERVICE REMOTE-ADDRESS USER ENCO... UPTIME
  0 R <pppoe-ex> ex 00:C0:CA:16:16:A5 ex pap 12s
[admin@MikroTik] interface pppoe-server>
```
To disconnect the user **ex**:

```
[admin@MikroTik] interface pppoe-server> remove [find user=ex]
[admin@MikroTik] interface pppoe-server> print
[admin@MikroTik] interface pppoe-server>
```

## Troubleshooting

### Description

- **I can connect to my PPPoE server. The ping goes even through it, but I still cannot open web pages**
  
  Make sure that you have specified a valid DNS server in the router (in `/ip dns` or in `/ppp profile` the `dns-server` parameter).

- **The PPPoE server shows more than one active user entry for one client, when the clients disconnect, they are still shown and active**
  
  Set the `keepalive-timeout` parameter (in the PPPoE server configuration) to **10** if You want clients to be considered logged off if they do not respond for 10 seconds. **Note** that if the `keepalive-timeout` parameter is set to **0** and the `only-one` parameter (in PPP profile settings) is set to **yes** then the clients might be able to connect only once. To resolve this problem `one-session-per-host` parameter in PPPoE server configuration should be set to **yes**

- **I can get through the PPPoE link only small packets (eg. pings)**
  
  You need to change `mss` of all the packets passing through the PPPoE link to the value of PPPoE link's MTU-40 at least on one of the peers. So for PPPoE link with MTU of 1480:

  ```
  [admin@MT] interface pppoe-server server> set 0 max-mtu=1440 max-mru=1440
  [admin@MT] interface pppoe-server server> print
  Flags: X - disabled
  0 service-name="mt" interface=wlan1 max-mtu=1440 max-mru=1440
  authentication=pap,chap,mschap1,mschap2 keepalive-timeout=10
  one-session-per-host=yes max-sessions=0 default-profile=default
  [admin@MT] interface pppoe-server server>
  ```

- **My windows PPPoE client obtains IP address and default gateway from the MikroTik PPPoE server, but it cannot ping beyond the PPPoE server and use the Internet**
  
  PPPoE server is not bridging the clients. Configure masquerading for the PPPoE client addresses, or make sure you have proper routing for the address space used by the clients, or you enable Proxy-ARP on the Ethernet interface (See the IP Addresses and Address Resolution Protocol (ARP) Manual)

- **My Windows XP client cannot connect to the PPPoE server**
  
  You have to specify the "Service Name" in the properties of the XP PPPoE client. If the service name is not set, or it does not match the service name of the MikroTik PPPoE server, you get the "line is busy" errors, or the system shows "verifying password - unknown error"

- **I want to have logs for PPPoE connection establishment**
  
  Configure the logging feature under the `/system logging facility` and enable the PPP type logs

## Application Examples
PPPoE in a multipoint wireless 802.11 network

In a wireless network, the PPPoE server may be attached to an Access Point (as well as to a regular station of wireless infrastructure). Either our RouterOS client or Windows PPPoE clients may connect to the Access Point for PPPoE authentication. Further, for RouterOS clients, the radio interface may be set to MTU 1600 so that the PPPoE interface may be set to MTU 1500. This optimizes the transmission of 1500 byte packets and avoids any problems associated with MTUs lower than 1500. It has not been determined how to change the MTU of the Windows wireless interface at this moment.

Let us consider the following setup where the MikroTik Wireless AP offers wireless clients transparent access to the local network with authentication:

Note that you should have Basic + Wireless + Wireless AP licenses for this setup.

First of all, the Prism interface should be configured:

```bash
[admin@MT_Prism_AP] interface prism> set 0 mode=ap-bridge frequency=2442MHz \
... ssid=mt disabled=no
[admin@MT_Prism_AP] interface prism> print
Flags: X - disabled, R - running
 0 R name="prism1" mtu=1500 mac-address=00:90:4B:02:17:E2 arp=enabled
    mode=ap-bridge root-ap=00:00:00:00:00:00 frequency=2442MHz ssid="mt"
    default-authentication=yes default-forwarding=yes max-clients=2007
    card-type=generic tx-power=auto supported-rates=1-11 basic-rates=1
    hide-ssid=no
[admin@MT_Prism_AP] interface prism> /ip address
```

Now, the Ethernet interface and IP address are to be set:

```bash
[admin@MT_Prism_AP] ip address> add address=10.0.0.217/24 interface=Local
[admin@MT_Prism_AP] ip address> print
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS NETWORK BROADCAST INTERFACE
0 10.0.0.217/24 10.0.0.0 10.0.0.255 Local
[admin@MT_Prism_AP] ip address> /ip route
[admin@MT_Prism_AP] ip route> add gateway=10.0.0.1
[admin@MT_Prism_AP] ip route> print
Flags: X - disabled, I - invalid, D - dynamic, J - rejected, C - connect, R - rip, O - ospf, B - bgp
# DST-ADDRESS G GATEWAY DISTANCE INTERFACE
0 S 0.0.0.0/0 r 10.0.0.1 1 Local
1 DC 10.0.0.0/24 r 0.0.0.0 0 Local
[admin@MT_Prism_AP] ip route> /interface ethernet
[admin@MT_Prism_AP] interface ethernet> set Local arp=proxy-arp
[admin@MT_Prism_AP] interface ethernet> print
# NAME MTU MAC-ADDRESS ARP
0 R Local 1500 00:50:08:00:00:F5 proxy-arp
```

We should add PPPoE server to the Prism interface:

```bash
[admin@MT_Prism_AP] interface pppoe-server server> add interface=prism1 \
... service-name=mt one-session-per-host=yes disabled=no
[admin@MT_Prism_AP] interface pppoe-server server> print
Flags: X - disabled
0 service-name="mt" interface=prism1 mtu=1480 mr=1480
    authentication=mschap2,mschap,chap,pap keepalive-timeout=10
    one-session-per-host=yes default-profile=default
[admin@MT_Prism_AP] interface pppoe-server server>
```
MSS should be changed for the packets flowing through the PPPoE link:

```
[admin@MT_Prism_AP] ip firewall mangle> add protocol=tcp tcp-options=syn-only \ 
 action=passthrough tcp-mss=1440
[admin@MT_Prism_AP] ip firewall mangle> print
Flags: X - disabled, I - invalid
  0 src-address=0.0.0.0:0-65535 in-interface=all
dst-address=0.0.0.0:0-65535 protocol=tcp tcp-options=syn-only
icmp-options=any-any flow="" src-mac-address=00:00:00:00:00:00
limit-count=0 limit-burst=0 limit-time=0s action=passthrough
mark-flow="" tcp-mss=1440
```

And finally, we can set up PPPoE clients:

```
[admin@MT_Prism_AP] ip pool> add name=pppoe ranges=10.0.0.230-10.0.0.240
[admin@MT_Prism_AP] ip pool> print
  # NAME          RANGES
  0 pppoe          10.0.0.230-10.0.0.240

[admin@MT_Prism_AP] ip pool> /ppp profile
[admin@MT_Prism_AP] ppp profile> set default use-encryption=yes \ 
local-address=10.0.0.217 remote-address=pppoe
[admin@MT_Prism_AP] ppp profile> print
Flags: * - default
  0 * name="default" local-address=10.0.0.217 remote-address=pppoe
  session-timeout=0s idle-timeout=0s use-compression=no
  use-vj-compression=no use-encryption=yes require-encryption=no
  only-one=no tx-bit-rate=0 rx-bit-rate=0 incoming-filter=""
  outgoing-filter=""
```

Thus we have completed the configuration and added two users: w and l who are able to connect using PPPoE client software.

**Note** that Windows XP built-in client supports encryption, but RASPPPOE does not. So, if it is planned not to support Windows clients older than Windows XP, it is recommended to switch `require-encryption` to `yes` value in the `default` profile configuration. In other case, the server will accept clients that do not encrypt data.