PPPoE

Document revision 1.7 (January 16, 2008, 9:13 GMT)
This document applies to V3.0

Table of Contents

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 serial modem connection.

Generally speaking, PPPoE is used to hand out IP addresses to clients based on the username (and workstation, if desired) authentication as opposed to workstation only authentication, when static IP addresses or DHCP are used. It is adviced not to use static IP addresses or DHCP on the same interfaces as PPPoE for obvious 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 any computer that has the PPPoE client protocol support installed. MikroTik RouterOS supports both - client and access concentrator sides 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). MPPE 40bit RSA and MPPE 128bit RSA encryption is supported.

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.

Note that when RADIUS server is authenticating a user with CHAP, MS-CHAPv1 or MS-CHAPv2, the RADIUS protocol 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 avaliable for almost all operating systems and most 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=user password=passwd \
\... 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=user password=passwd 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. 9KiB (plus extra 10KiB for packet queue, if data rate limitation is used) for each connection) and CPU power. Maximum of 65535 connections is supported.*

Additional Documents

Links for PPPoE documentation:

- http://www.faqs.org/rfcs/rfc2516.html

PPPoE Clients:

- RASPPPoE for Windows 95, 98, 98SE, ME, NT4, 2000, XP, .NET
  http://www.raspppoe.com/

PPPoE Client Setup

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

Property Description

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

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

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

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

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: **pppoe-out1**) - name of the PPPoE interface

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

profile (*name*) - default profile for the connection

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

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)

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

Notes

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

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 add and enable PPPoE client on the **ether1** interface connecting to the AC that provides **testSN** service using user name **user** with the password **passwd**:

```
[admin@RemoteOffice] interface pppoe-client> add interface=ether1 \
\... service-name=testSN user=user password=passwd disabled=no
[admin@RemoteOffice] interface pppoe-client> print
Flags: X - disabled, R - running
 0  R name="pppoe-out1" max-mtu=1480 max-mru=1480 mrru=disabled interface=ether1
      user="user" password="passwd" profile=default service-name="testSN"
      ac-name="" add-default-route=no dial-on-demand=no use-peer-dns=no
      allow=pap,chap,mschap1,mschap2
[admin@RemoteOffice] interface pppoe-client>
```

Monitoring PPPoE Client

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

Property Description

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

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

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

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

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

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

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

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

```
[admin@MikroTik] interface pppoe-client> monitor pppoe-out1
        status: "connected"
        uptime: 6s
     idle-time: 6s
      encoding: "MPPE128 stateless"
  service-name: "testSN"
       ac-name: "MikroTik"
        ac-mac: 00:0C:42:04:00:73
           mtu: 1480
           mru: 1480

[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.

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

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

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

interface (*name*) - interface, which the clients are connected to

keepalive-timeout (*time*; default: **10**) - 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: **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)

max-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)

max-sessions (*integer*; default: **0**) - maximum number of clients that the AC can serve

- **0** - unlimited

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

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

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

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 explicitly log out or the 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.

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

```
[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 mrru=disabled
      authentication=mschap2,mschap,chap,pap keepalive-timeout=10
      one-session-per-host=yes max-sessions=0 default-profile=default
[admin@MikroTik] interface pppoe-server server>
```

PPPoE Tunnel Interfaces

Home menu level: ***/interface pppoe-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

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

remote-address (*read-only: MAC address*) - MAC address of the connected client

service (*name*) - name of the service the user is connected to

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

user (*name*) - the name of the connected user (must be present in the user darabase anyway)

Example

To view the currently connected users:

```
[admin@MikroTik] interface pppoe-server> print
Flags: X - disabled, D - dynamic, R - running
 #     NAME       USER      SERVICE   REMOTE... ENCODING  UPTIME
 0  DR <pppoe-ex> user      ex        00:0C:... MPPE12... 40m45s
[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>
```

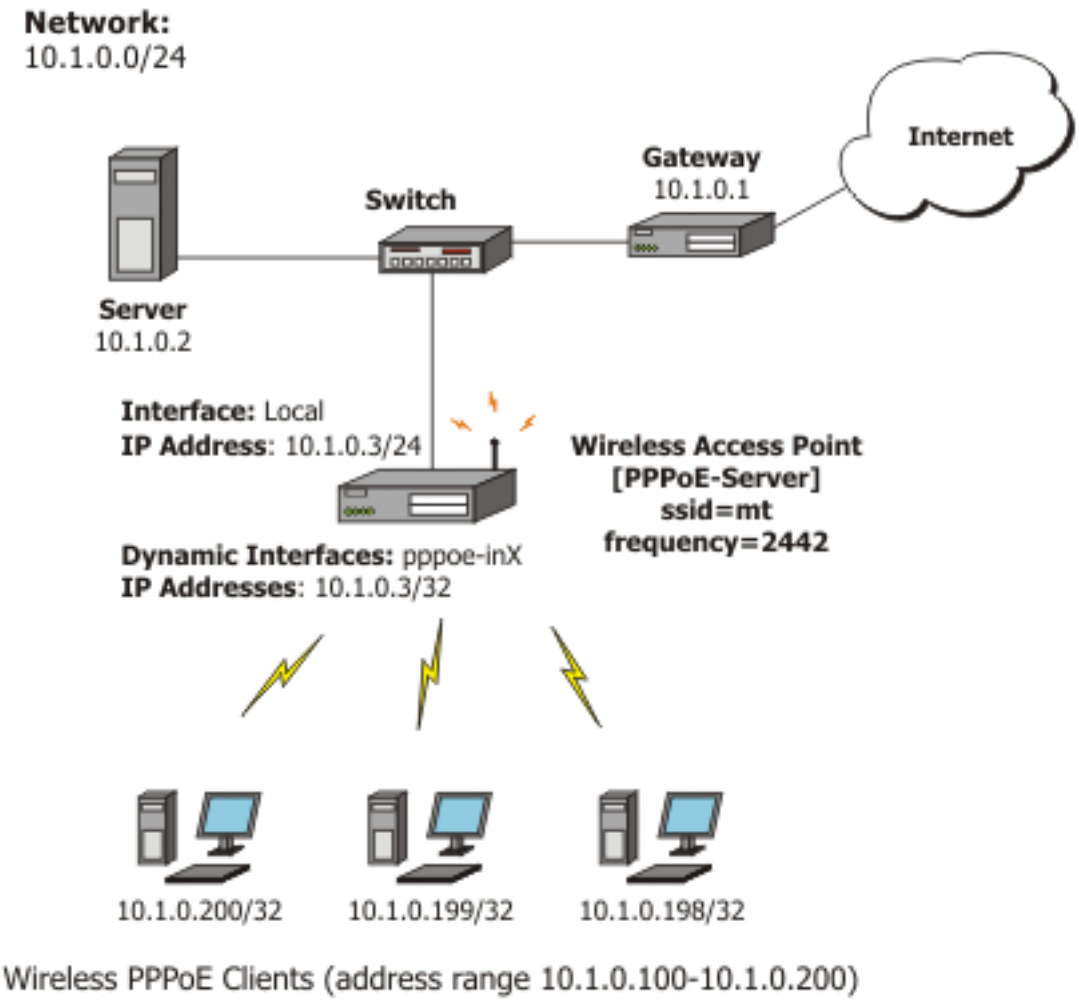
Application Examples

PPPoE in a multipoint wireless 802.11g 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:



First of all, the wireless interface should be configured:

```
[admin@PPPoE-Server] interface wireless> set 0 mode=ap-bridge \
   frequency=2442 band=2.4ghz-b/g ssid=mt disabled=no
[admin@PPPoE-Server] interface wireless> print
Flags: X - disabled, R - running
 0 X  name="wlan1" mtu=1500 mac-address=00:0C:42:18:5C:3D arp=enabled
      interface-type=Atheros AR5413 mode=ap-bridge ssid="mt" frequency=2442
      band=2.4ghz-b/g scan-list=default antenna-mode=ant-a wds-mode=disabled
      wds-default-bridge=none wds-ignore-ssid=no default-authentication=yes
      default-forwarding=yes default-ap-tx-limit=0 default-client-tx-limit=0
      hide-ssid=no security-profile=default compression=no
[admin@PPPoE-Server] interface wireless>
```

Now, configure the Ethernet interface, add the IP address and set the default route:

```
[admin@PPPoE-Server] ip address> add address=10.1.0.3/24 interface=Local
[admin@PPPoE-Server] ip address> print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         BROADCAST       INTERFACE
 0   10.1.0.3/24        10.1.0.0        10.1.0.255      Local
[admin@PPPoE-Server] ip address> /ip route
```

```
[admin@PPPoE-Server] ip route> add gateway=10.1.0.1
[admin@PPPoE-Server] ip route> print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        G GATEWAY         DISTANCE INTER...
 0 ADC  10.1.0.0/24        10.1.0.3                          0        Local
 1 A S  0.0.0.0/0                          r 10.1.0.1        1        Local
[admin@PPPoE-Server] ip route> /interface ethernet
[admin@PPPoE-Server] interface ethernet> set Local arp=proxy-arp
[admin@PPPoE-Server] interface ethernet> print
Flags: X - disabled, R - running
 #    NAME                                MTU   MAC-ADDRESS       ARP
 0  R Local                               1500  00:0C:42:03:25:53 proxy-arp
[admin@PPPoE-Server] interface ethernet>
```

We should add PPPoE server to the wireless interface:

```
[admin@PPPoE-Server] interface pppoe-server server> add interface=wlan1 \
   service-name=mt one-session-per-host=yes disabled=no
[admin@PPPoE-Server] interface pppoe-server server> print
Flags: X - disabled
 0   service-name="mt" interface=wlan1 max-mtu=1480 max-mru=1480 mrru=disabled
     authentication=pap,chap,mschap1,mschap2 keepalive-timeout=10
     one-session-per-host=yes max-sessions=0 default-profile=default
[admin@PPPoE-Server] interface pppoe-server server>
```

Finally, we can set up PPPoE clients:

```
[admin@PPPoE-Server] ip pool> add name=pppoe ranges=10.1.0.100-10.1.0.200
[admin@PPPoE-Server] ip pool> print
 # NAME                                      RANGES
 0 pppoe                                     10.1.0.100-10.1.0.200
[admin@PPPoE-Server] ip pool> /ppp profile
[admin@PPPoE-Server] ppp profile> set default use-encryption=yes \
   local-address=10.1.0.3 remote-address=pppoe
[admin@PPPoE-Server] ppp profile> print
Flags: * - default
 0 * name="default" local-address=10.1.0.3 remote-address=pppoe
     use-compression=no use-vj-compression=no use-encryption=yes only-one=no
     change-tcp-mss=yes

 1 * name="default-encryption" use-compression=default
     use-vj-compression=default use-encryption=yes only-one=default
     change-tcp-mss=default
[admin@PPPoE-Server] ppp profile> .. secret
[admin@PPPoE-Server] ppp secret> add name=w password=wkst service=pppoe
[admin@PPPoE-Server] ppp secret> add name=l password=ltp service=pppoe
[admin@PPPoE-Server] ppp secret> print
Flags: X - disabled
 #   NAME        SERVICE CALLER-ID PASSWORD  PROFILE           REMOTE-ADDRESS
 0   w           pppoe             wkst      default           0.0.0.0
 1   l           pppoe             ltp       default           0.0.0.0
[admin@PPPoE-Server] ppp secret>
```

Thus we have completed the configuration and added two users: **w** and **l** who are able to connect to Internet, 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 not to require encryption. In other case, the server will accept clients that do not encrypt data.

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**
- **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