

PPP User AAA

Document revision 2.6 (February 6, 2008, 1:40 GMT)

This document applies to V3.0

Table of Contents

[Table of Contents](#)

[Summary](#)

[Specifications](#)

[Description](#)

[Local PPP User Profiles](#)

[Description](#)

[Property Description](#)

[Notes](#)

[Example](#)

[Local PPP User Database](#)

[Description](#)

[Property Description](#)

[Example](#)

[Monitoring Active PPP Users](#)

[Property Description](#)

[Example](#)

[PPP User Remote AAA](#)

[Property Description](#)

[Notes](#)

[Example](#)

General Information

Summary

This document provides summary, configuration reference and examples on PPP user management. This includes asynchronous PPP, PPTP, L2TP, OpenVPN, PPPoE and ISDN users.

Specifications

Packages required: *system*

License required: *level1*

Home menu level: */ppp*

Description

The MikroTik RouterOS provides scalable Authentication, Authorization and Accounting (AAA) functionality.

Local authentication is performed using the User Database and the Profile Database. The actual configuration for the given user is composed using respective user record from the User Database, associated item from the Profile Database and the item in the Profile database which is set as default for a

given service the user is authenticating to. Default profile settings from the Profile database have lowest priority while the user access record settings from the User Database have highest priority with the only exception being particular IP addresses take precedence over IP pools in the **local-address** and **remote-address** settings, which described later on.

Support for RADIUS authentication gives the ISP or network administrator the ability to manage PPP user access and accounting from one server throughout a large network. The MikroTik RouterOS has a RADIUS client which can authenticate for PPP, PPPoE, PPTP, L2TP, OpenVPN and ISDN connections. The attributes received from RADIUS server override the ones set in the default profile, but if some parameters are not received they are taken from the respective default profile.

Local PPP User Profiles

Home menu level: */ppp profile*

Description

PPP profiles are used to define default values for user access records stored under **/ppp secret** submenu. Settings in **/ppp secret** User Database override corresponding **/ppp profile** settings except that single IP addresses always take precedence over IP pools when specified as **local-address** or **remote-address** parameters.

Property Description

bridge (*name*) - bridge interface name, which the PPP tunnel will automatically be added in case BCP negotiation will be successful (i.e., in case both peers support BCP and have this parameter configured)

change-tcp-mss (*yes | no | default*; default: **default**) - modifies TCP connection MSS settings

- **yes** - adjust connection MSS value
- **no** - do not adjust connection MSS value
- **default** - derive this value from the interface default profile; same as no if this is the interface default profile

dns-server (*IP address*) - IP address of the DNS server to supply to clients

idle-timeout (*time*) - specifies the amount of time after which the link will be terminated if there was no activity present. There is no timeout set by default

- **0s** - no link timeout is set

incoming-filter (*name*) - firewall chain name for incoming packets. Specified chain gets control for each packet coming from the client. The ppp chain should be manually added and rules with action=jump jump-target=ppp should be added to other relevant chains in order for this feature to work. For more information look at the Examples section

local-address (*IP addressname*) - IP address or IP address pool name for PPP server

name (*name*) - PPP profile name

only-one (*yes | no | default*; default: **default**) - defines whether a user is allowed to have more than one connection at a time

- **yes** - a user is not allowed to have more than one connection at a time

- **no** - the user is allowed to have more than one connection at a time
- **default** - derive this value from the interface default profile; same as no if this is the interface default profile

outgoing-filter (*name*) - firewall chain name for outgoing packets. Specified chain gets control for each packet going to the client. The ppp chain should be manually added and rules with action=jump jump-target=ppp should be added to other relevant chains in order for this feature to work. For more information look at the Examples section

rate-limit (*text*; default: "") - rate limitation in form of rx-rate[/tx-rate] [rx-burst-rate[/tx-burst-rate] [rx-burst-threshold[/tx-burst-threshold] [rx-burst-time[/tx-burst-time] [priority] [rx-rate-min[/tx-rate-min]]]] from the point of view of the router (so "rx" is client upload, and "tx" is client download). All rates are measured in bits per second, unless followed by optional 'k' suffix (kilobits per second) or 'M' suffix (megabits per second). If tx-rate is not specified, rx-rate serves as tx-rate too. The same applies for tx-burst-rate, tx-burst-threshold and tx-burst-time. If both rx-burst-threshold and tx-burst-threshold are not specified (but burst-rate is specified), rx-rate and tx-rate are used as burst thresholds. If both rx-burst-time and tx-burst-time are not specified, 1s is used as default. Priority takes values 1..8, where 1 implies the highest priority, but 8 - the lowest. If rx-rate-min and tx-rate-min are not specified rx-rate and tx-rate values are used. The rx-rate-min and tx-rate-min values can not exceed rx-rate and tx-rate values.

remote-address (*IP addressname*) - IP address or IP address pool name for PPP clients

session-timeout (*time*) - maximum time the connection can stay up. By default no time limit is set

- **0s** - no connection timeout

use-compression (*yes | no | default*; default: **default**) - specifies whether to use data compression or not

- **yes** - enable data compression
- **no** - disable data compression
- **default** - derive this value from the interface default profile; same as no if this is the interface default profile

use-encryption (*yes | no | required | default*; default: **default**) - specifies whether to use data encryption or not

- **yes** - enable data encryption
- **no** - disable data encryption
- **required** - enable and require encryption
- **default** - derive this value from the interface default profile; same as no if this is the interface default profile

use-vj-compression (*yes | no | default*; default: **default**) - specifies whether to use Van Jacobson header compression algorithm

- **yes** - enable Van Jacobson header compression
- **no** - disable Van Jacobson header compression
- **default** - derive this value from the interface default profile; same as no if this is the interface default profile

wins-server (*IP address*) - IP address of the WINS server to supply to Windows clients

Notes

There are two default profiles that cannot be removed:

```
[admin@rb13] ppp profile> print
Flags: * - default
0 * name="default" use-compression=default use-vj-compression=default
  use-encryption=default only-one=default change-tcp-mss=yes

1 * name="default-encryption" use-compression=default
  use-vj-compression=default use-encryption=yes only-one=default
  change-tcp-mss=yes
[admin@rb13] ppp profile>
```

Use Van Jacobson compression only if you have to because it may slow down the communications on bad or congested channels.

incoming-filter and **outgoing-filter** arguments add dynamic **jump** rules to chain **ppp**, where the **jump-target** argument will be equal to **incoming-filter** or **outgoing-filter** argument in **/ppp profile**. Therefore, chain **ppp** should be manually added before changing these arguments.

only-one parameter is ignored if RADIUS authentication is used.

If there are more than 10 simultaneous PPP connections planned, it is recommended to turn the **change-mss** property off, and use one general MSS changing rule in mangle table instead, to reduce CPU utilization.

By configuring **bridge** property you enable the BCP protocol on the link. It is useful to enable MRRU as well in order for the link to be capable of transmitting full-size Ethernet frames. If the BCP negotiation is successful, the link will automatically be added to the specified bridge. Note that the bridge must have either a valid administrative MAC address, or another Ethernet-like port with a valid MAC address, as the PPP link do not have any MAC address.

Client will use a fake IP address (10.112.112.x) as a remote end address if no remote address is known. It won't be possible to ping this address, and it should be used as a gateway for routes (like default route) only. This helps GSM/GPRS setups where dial-in servers for some reason does not advertise their ip address.

Example

To add the profile **ex** that assigns the router itself the **10.0.0.1** address, and the addresses from the **ex** pool to the clients, filtering traffic coming from clients through **mypppclients** chain:

```
[admin@rb13] ppp profile> add name=ex local-address=10.0.0.1 remote-address=ex
incoming-filter=mypppclients
[admin@rb13] ppp profile> print
Flags: * - default
0 * name="default" use-compression=default use-vj-compression=default
  use-encryption=default only-one=default change-tcp-mss=yes

1 * name="default-encryption" use-compression=default
  use-vj-compression=default use-encryption=yes only-one=default
  change-tcp-mss=yes
2  name="ex" local-address=10.0.0.1 remote-address=ex use-compression=default
  use-vj-compression=default use-encryption=default only-one=default
  change-tcp-mss=default incoming-filter=mypppclients
[admin@rb13] ppp profile>
```

Local PPP User Database

Home menu level: */ppp secret*

Description

PPP User Database stores PPP user access records with PPP user profile assigned to each user.

Property Description

caller-id (*text*; default: `""`) - for PPTP and L2TP it is the IP address a client must connect from. For PPPoE it is the MAC address (written in CAPITAL letters) a client must connect from. For ISDN it is the caller's number (that may or may not be provided by the operator) the client may dial-in from

- `""` - no restrictions on where clients may connect from

limit-bytes-in (*integer*; default: `0`) - maximal amount a client can upload, in bytes, for a session

limit-bytes-out (*integer*; default: `0`) - maximal amount a client can download, in bytes, for a session

local-address (*IP addressname*) - IP address or IP address pool name for PPP server

name (*name*) - user's name used for authentication

password (*text*; default: `""`) - user's password used for authentication

profile (*name*; default: **default**) - profile name to use together with this access record for user authentication

remote-address (*IP addressname*) - IP address or IP address pool name for PPP clients

routes (*text*) - routes that appear on the server when the client is connected. The route format is: `dst-address [[gateway] [metric]]` (for example, `10.1.0.0/24 10.0.0.1 1`). Several routes may be specified separated with commas. If gateway is not specified, the remote address is used. If metric is not specified, the metric of 1 is used

service (*any | async | l2tp | ovpn | pppoe | pptp*; default: **any**) - specifies the services available to a particular user

Example

To add the user **ex** with password **lkjrht** and profile **ex** available for PPTP service only, enter the following command:

```
[admin@rb13] ppp secret> add name=ex password=lkjrht service=pptp profile=ex
[admin@rb13] ppp secret> print
Flags: X - disabled
#   NAME                SERVICE CALLER-ID PASSWORD PROFILE REMOTE-ADDRESS
0   ex                  pptp          lkjrht   ex       0.0.0.0
[admin@rb13] ppp secret>
```

Monitoring Active PPP Users

Command name: `/ppp active print`

Property Description

address (*read-only: IP address*) - IP address the client got from the server

bytes (*read-only: integerinteger*) - amount of bytes transferred through this connection. First figure represents amount of transmitted traffic from the router's point of view, while the second one shows amount of received traffic

caller-id (*read-only: text*) - for PPTP and L2TP it is the IP address the client connected from. For PPPoE it is the MAC address the client connected from. For ISDN it is the caller's number the client dialed-in from

- "" - no restrictions on where clients may connect from

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

limit-bytes-in (*read-only: integer*) - maximal amount of bytes the user is allowed to send to the router

limit-bytes-out (*read-only: integer*) - maximal amount of bytes the router is allowed to send to the client

name (*read-only: name*) - user name supplied at authentication stage

packets (*read-only: integerinteger*) - amount of packets transferred through this connection. First figure represents amount of transmitted traffic from the router's point of view, while the second one shows amount of received traffic

service (*read-only: async | l2tp | ovpn | pppoe | pptp*) - the type of service the user is using

session-id (*read-only: text*) - shows unique client identifier

uptime (*read-only: time*) - user's uptime

Example

```
[admin@rb13] > /ppp active print
Flags: R - radius
#  NAME      SERVICE CALLER-ID      ADDRESS      UPTIME      ENCODING
0  ex        pptp    10.0.11.12      10.0.0.254  1m16s      MPPE128...
[admin@rb13] > /ppp active print detail
Flags: R - radius
0  name="ex" service=pptp caller-id="10.0.11.12" address=10.0.0.254
    uptime=1m22s encoding="MPPE128 stateless" session-id=0x8180002B
    limit-bytes-in=200000000 limit-bytes-out=0
[admin@rb13] > /ppp active print stats
Flags: R - radius
#  NAME      BYTES      PACKETS
0  ex        10510/159690614  187/210257
[admin@rb13] >
```

PPP User Remote AAA

Home menu level: */ppp aaa*

Property Description

accounting (yes | no; default: **yes**) - enable RADIUS accounting

interim-update (*time*; default: **0s**) - Interim-Update time interval

use-radius (yes | no; default: **no**) - enable user authentication via RADIUS

Notes

RADIUS user database is consulted only if the required username is not found in local user database.

Example

To enable RADIUS AAA:

```
[admin@MikroTik] ppp aaa> set use-radius=yes  
[admin@MikroTik] ppp aaa> print  
    use-radius: yes  
    accounting: yes  
    interim-update: 0s  
[admin@MikroTik] ppp aaa>
```