AAA

Document revision 2.1 (Fri Dec 17 18:28:01 GMT 2004)
This document applies to MikroTik RouterOS V2.8

Table of Contents

General Information

Summary

Authentication, Authorization and Accounting feature provides a possibility of local and/or remote (on RADIUS server) Point-to-Point and HotSpot user management and traffic accounting (all IP traffic passing the router is accounted).

Specifications

Packages required: ***system***
License required: ***level1***
Home menu level: ***/user, /ppp, /ip accounting, /radius***
Standards and Technologies: ***RADIUS***
Hardware usage: *Local traffic accounting requires additional memory*

Related Documents

- ***Package Management***
- ***IP Addresses and ARP***
- ***HotSpot Gateway***
- ***PPP and Asynchronous Interfaces***
- ***PPPoE***
- ***PPTP***

- ***L2TP***
- ***ISDN***

Description

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

Local authentication is performed consulting User Database and Profile Database. The configuration is collected from the respective item in User Database (determined by the username), from the item in Profile Database, that is associated with this item and from the item in Profile Database, that is set as default for the service the user is authenticating to. Settings received from the default profile for the service is overriden by the respective settings from the user's profile, and the resulting settings are overriden by the respective settings taken from the User Database (the only exception is that particular IP addresses take precedence over IP pools in the **local-address** and **remote-address** settings, as described later on).

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 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.

Traffic is accounted locally with Cisco **IP pairs** and snapshot image can be gathered using Syslog utilities. If RADIUS accounting is enabled, accounting information is also sent to the RADIUS server default for that service.

Router User Groups

Home menu level: ***/user group***

Property Description

name (*name*) - the name of the user group

policy (*multiple choice: local | telnet | ssh | ftp | reboot | read | write | policy | test | web*; default: **!local,!telnet,!ssh,!ftp,!reboot,!read,!write,!policy,!test,!web**) - group rights set

- **local** - user can log on locally via console
- **telnet** - user can log on remotely via telnet
- **ssh** - user can log on remotely via secure shell
- **ftp** - user can log on remotely via ftp and send and retrieve files from the router
- **reboot** - user can reboot the router
- **read** - user can retrieve the configuration
- **write** - user can retrieve and change the configuration
- **policy** - user can manage user policies and add and remove users
- **test** - user can run ping, traceroute, bandwidth test
- **web** - user can log on remotely via winbox

Notes

There are three system groups which cannot be deleted:

```
[admin@MikroTik] user group> print
  0 ;;; users with read only permission
    name="read"
    policy=local,telnet,ssh,!ftp,reboot,read,!write,!policy,test,web

  1 ;;; users with write permission
    name="write"
    policy=local,telnet,ssh,!ftp,reboot,read,write,!policy,test,web

  2 ;;; users with complete access
    name="full" policy=local,telnet,ssh,ftp,reboot,read,write,policy,test,web

[admin@MikroTik] user group>
```

Exclamation sign '**!**' just before policy name means **NOT**.

Example

To add **reboot** group that is allowed to reboot the router locally or using telnet, as well as read the router's configuration:

```
[admin@MikroTik] user group> add name=reboot policy=telnet,reboot,read
[admin@MikroTik] user group> print
  0 ;;; users with read only permission
    name="read"
    policy=local,telnet,ssh,!ftp,reboot,read,!write,!policy,test,web

  1 ;;; users with write permission
    name="write"
    policy=local,telnet,ssh,!ftp,reboot,read,write,!policy,test,web

  2 ;;; users with complete access
    name="full" policy=local,telnet,ssh,ftp,reboot,read,write,policy,test,web

  3 name="reboot"
    policy=!local,telnet,!ssh,!ftp,reboot,read,!write,!policy,!test,!web

[admin@MikroTik] user group>
```

Router Users

Home menu level: ***/user***

Property Description

address (*IP address/mask*; default: **0.0.0.0/0**) - IP address from which the user is allowed to log in

group (*name*) - name of the group the user belongs to

name (*name*) - user name. Although it must start with an alphanumeric character, it may "*", "_", ".", "@" symbols

password (*text*; default: "") - user password. If not specified, it is left blank (hit [Enter] when logging in). It conforms to standard Unix characteristics of passwords and can contain letters, digits, "*" and "_" symbols

Notes

There is one predefined user that cannot be deleted:

```
[admin@MikroTik] user> print
Flags: X - disabled
  #   NAME                                            GROUP ADDRESS
  0   ;;; system default user
      admin                                           full  0.0.0.0/0

[admin@MikroTik] user>
```

When the user has logged in he can change his password using the **/password** command. The user is required to enter his/her current password before entering the new password. When the user logs out and logs in for the next time, the new password must be entered.

Example

To add user **joe** with password **j1o2e3** belonging to **write** group:

```
[admin@MikroTik] user> add name=joe password=j1o2e3 group=write
[admin@MikroTik] user> print
Flags: X - disabled
  0   ;;; system default user
      name="admin" group=full address=0.0.0.0/0

  1   name="joe" group=write address=0.0.0.0/0


[admin@MikroTik] user>
```

Monitoring Active Router Users

Home menu level: ***/user active print***

Property Description

address (*read-only: IP address*) - IP address from which the user is accessing the router

- **0.0.0.0** - the user is logged in locally

name (*read-only: name*) - user name

via (*read-only: console* | *telnet* | *ssh* | *web*) - user's access method

when (*read-only: date*) - log-in time

Example

```
[admin@MikroTik] user> active print
Flags: R - radius
  #   WHEN                 NAME                            ADDRESS         VIA
  0   feb/21/2003 17:48:21 admin                           0.0.0.0         console
  1   feb/24/2003 22:14:48 admin                           10.0.0.144      ssh
  2   mar/02/2003 23:36:34 admin                           10.0.0.144      web

[admin@MikroTik] user>
```

Router User Remote AAA

Home menu level: ***/user aaa***

Property Description

accounting (yes | no; default: **yes**) - specifies whether to use RADIUS accounting

default-group (*name*; default: **read**) - user group used by default for users authenticated via RADIUS server

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

use-radius (yes | no; default: **no**) - specifies whether a user database on a RADIUS server should be consulted

Notes

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

Example

To enable RADIUS AAA:

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

Local Point-to-Point AAA

Local PPP User Profiles

Home menu level: ***/ppp profile***

Description

PPP profiles are used to define default values to users managed in **/ppp secret** submenu. Settings in **/ppp secret** override corresponding **/ppp profile** settings except in the case when **local-address** or **remote-address** are configured in both **/ppp secret** and **/ppp profile**, but in one of them ip pool is referred, concrete IP addresses always take precedence.

Property Description

idle-timeout (*time*; default: **0s**) - specifies the amount of time after which the link will be terminated if there was no activity present

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

incoming-filter (*name*; default: **""**) - firewall chain name for incoming packets. If set, then for

each packet coming from the client, this firewall chain will get control. You have to manually add chain ppp and jumps to this chain from other chains in order this feature to work

local-address (*IP address* | *name*; default: **0.0.0.0**) - either address or pool name of the PPP server

name (*name*) - profile name

only-one (yes | no; default: **no**) - if enabled, allows the user only one connection at a time

outgoing-filter (*name*; default: **""**) - firewall chain name for outgoing packets. If set, then for each packet coming to the client, this firewall chain will get control. You have to manually add chain ppp and jumps to this chain from other chains in order this feature to work

remote-address (*IP address* | *name*; default: **0.0.0.0**) - either address or pool name of the PPP client

require-encryption (yes | no; default: **no**) - defines whether to require encryption from the client or simply prefer it

rx-bit-rate (*integer*; default: **0**) - receive bitrate in bits/s

session-timeout (*time*; default: **0s**) - maximum time the connection can stay up

- **0s** - no connection timeout

tx-bit-rate (*integer*; default: **0**) - transmit bitrate in bits/s

use-compression (yes | no; default: **no**) - defines whether to compress traffic or not

use-encryption (yes | no; default: **no**) - defines whether to encrypt traffic or not

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

wins-server (*text*) - the Windows DHCP client will use this as the default WINS server. Two comma-separated WINS servers can be specified to be used by PPP user as primary and secondary WINS servers

Notes

One default profile is created:

```
[admin@MikroTik] ppp profile> print
Flags: * - default
  0 * name="default" local-address=0.0.0.0 remote-address=0.0.0.0
      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="" wins-server=""

[admin@MikroTik] ppp profile>
```

Use VJ 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

Example

To add the profile **ex** that will assign the router itself the **10.0.0.1** address, and the addresses from the **ex** pool to the clients:

```
[admin@MikroTik] ppp profile> add name=ex local-address=10.0.0.1 remote-address=ex
[admin@MikroTik] ppp profile> print
Flags: * - default
  0 * name="default" local-address=0.0.0.0 remote-address=0.0.0.0
      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="" wins-server=""

  1   name="ex" local-address=10.0.0.1 remote-address=ex session-timeout=0s
      idle-timeout=0s use-compression=no use-vj-compression=no
      use-encryption=no require-encryption=no only-one=no tx-bit-rate=0
      rx-bit-rate=0 incoming-filter="" outgoing-filter="" wins-server=""


[admin@MikroTik] ppp profile>
```

Local PPP User Database

Home menu level: ***/ppp secret***

Description

PPP User Database stores PPP users and defines owner and profile for each of them.

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 volume of client upload, in bytes, for a session

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

local-address (*IP address* | *name*; default: **0.0.0.0**) - either address or pool name of the PPP server

name (*name*) - user name

password (*text*; default: **""**) - user's password

profile (*name*; default: **default**) - profile name for the user

remote-address (*IP address* | *name*; default: **0.0.0.0**) - either address or pool name of the PPP client

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

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

Example

To add the user **ex** with **lkjrht** password for PPTP service only and with **ex** profile:

```
[admin@MikroTik] ppp secret> add name=ex password=lkjrht service=pptp profile=ex
[admin@MikroTik] ppp secret> print
Flags: X - disabled
  #   NAME              SERVICE CALLER-ID       PASSWORD        PROFILE
  0   ex                pptp                    lkjrht          ex
[admin@MikroTik] ppp secret> print detail
Flags: X - disabled
  0   name="ex" service=pptp caller-id="" password="lkjrht" profile=ex
      local-address=0.0.0.0 remote-address=0.0.0.0 routes=""


[admin@MikroTik] ppp secret>
```

Monitoring Active PPP Users

Home menu level: ***/ppp active print***

Property Description

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

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

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

name (*read-only: name*) - user name

service (*read-only: async* | *isdn* | *l2tp* | *pppoe* | *pptp*) - shows the kind of service the user is using

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

Example

```
[admin@MikroTik] ppp profile> .. active print
Flags: R - radius
  #   NAME         SERVICE CALLER-ID         ADDRESS         UPTIME   ENCODING
  0   ex           pptp    10.0.0.148        10.1.0.148      1d15h... MPPE12...

[admin@MikroTik] ppp profile> .. active print detail
Flags: R - radius
  0   name="ex" service=pptp caller-id="10.0.0.148" address=10.1.0.148
      uptime=1d15h4m41s encoding="MPPE128 stateless"

[admin@MikroTik] ppp profile>
```

PPP User Remote AAA

Home menu level: ***/ppp aaa***

Property Description

accounting (yes | no; default: **yes**) - specifies whether to use RADIUS accounting

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

use-radius (yes | no; default: **no**) - specifies whether to consult user database on a RADIUS server

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>
```

Local IP Traffic Accounting

Home menu level: ***/ip accounting***

Description

As each packet passes through the router, the packet source and destination addresses are matched against an IP pair in the accounting table and the traffic for that pair is increased. The traffic of PPP, PPTP, PPPoE, ISDN and HotSpot clients can be accounted on per-user basis too. Both the number of packets and the number of bytes are accounted.

If no matching IP or user pair exists, a new entry will be added to the table

Only the packets that enter and leave the router are accounted. Packets that are dropped in the router are not counted as well as ones that are sent from the router itself. Packets that are NATted on the router will be accounted for with the actual IP addresses on each side. Packets that are going through bridged interfaces (i.e. inside the bridge interface) are also accounted correctly.

Property Description

enabled (yes | no; default: **no**) - whether local IP traffic accounting is enabled

threshold (*integer*; default: **256**) - maximum number of IP pairs in the accounting table (maximal value is 8192)

Notes

For bidirectional connections two entries will be created.

Each IP pair uses approximately 100 bytes

When the threshold limit is reached, no new IP pairs will be added to the accounting table. Each packet that is not accounted in the accounting table will then be added to the **uncounted** counter!

Example

Enable IP accounting:

```
[admin@MikroTik] ip accounting> set enabled=yes
[admin@MikroTik] ip accounting> print
```

```
      enabled: yes
    threshold: 256
[admin@MikroTik] ip accounting>
```

Example

See the uncounted packets:

```
[admin@MikroTik] ip accounting uncounted> print
    packets: 0
      bytes: 0
[admin@MikroTik] ip accounting uncounted>
```

Local IP Traffic Accounting Table

Home menu level: ***/ip accounting snapshot***

Description

When a snapshot is made for data collection, the accounting table is cleared and new IP pairs and traffic data are added. The more frequently traffic data is collected, the less likelihood that the IP pairs thereshold limit will be reached.

Property Description

bytes (*read-only: integer*) - total number of bytes, matched by this entry

dst-address (*read-only: IP address*) - destination IP address

dst-user (*read-only: text*) - recipient's name (if aplicable)

packets (*read-only: integer*) - total number of packets, matched by this entry

src-address (*read-only: IP address*) - source IP address

src-user (*read-only: text*) - sender's name (if aplicable)

Notes

Usernames are shown only if the users are connected to the router via a PPP tunnel or are authenticated by HotSpot.

Before the first snapshot is taken, the table is empty.

Example

To take a new snapshot:

```
[admin@MikroTik] ip accounting snapshot> take
[admin@MikroTik] ip accounting snapshot> print
 # SRC-ADDRESS     DST-ADDRESS     PACKETS    BYTES      SRC-USER    DST-USER
 0 192.168.0.2     159.148.172.197 474        19130
 1 192.168.0.2     10.0.0.4        3          120
 2 192.168.0.2     192.150.20.254  32         3142
 3 192.150.20.254  192.168.0.2     26         2857
 4 10.0.0.4        192.168.0.2     2          117
 5 159.148.147.196 192.168.0.2     2          136
 6 192.168.0.2     159.148.147.196 1          40
```

```
 7 159.148.172.197 192.168.0.2     835        1192962
[admin@MikroTik] ip accounting snapshot>
```

Web Access to the Local IP Traffic Accounting Table

Home menu level: ***/ip accounting web-access***

Description

The web page report make it possible to use the standard Unix/Linux tool wget to collect the traffic data and save it to a file or to use MikroTik shareware Traffic Counter to display the table. If the web report is enabled and the web page is viewed, the **snapshot** will be made when connection is initiated to the web page. The **snapshot** will be displayed on the web page. TCP protocol, used by http connections with the wget tool guarantees that none of the traffic data will be lost. The **snapshot** image will be made when the connection from wget is initiated. Web browsers or wget should connect to URL: **http://routerIP/accounting/ip.cgi**

Property Description

accessible-via-web (yes | no; default: **no**) - wheather the snapshot is available via web

address (*IP address/mask*; default: **0.0.0.0**) - IP address range that is allowed to access the snapshot

Example

To enable web access from **10.0.0.1** server only:

```
[admin@MikroTik] ip accounting web-access> set accessible-via-web=yes \
\... address=10.0.0.1/32
[admin@MikroTik] ip accounting web-access> print
    accessible-via-web: yes
               address: 10.0.0.1/32
[admin@MikroTik] ip accounting web-access>
```

RADIUS Client Setup

Home menu level: ***/radius***

Description

This facility allows you to set RADIUS servers the router will use to authenticate users.

Property Description

accounting-backup (yes | no; default: **no**) - specifies whether this entry should serve as RADIUS accounting backup

accounting-port (*integer*; default: **1813**) - specifies the server's port used for accounting

address (*IP address*; default: **0.0.0.0**) - IP address of the RADIUS server

authentication-port (*integer*; default: **1812**) - specifies the server's port used for authentication

called-id (*text*; default: **""**) - this setting depends on Point-to-Point protocol:

- **ISDN** - phone number dialled (MSN)

- **PPPoE** - service name
- **PPTP** - server's IP address
- **L2TP** - server's IP address

domain (*text*; default: "") - Microsoft Windows domain of client

realm (*text*) - explicitly stated realm (user domain), so the users do not have to provide proper ISP domain name in user name

secret (*text*; default: "") - shared secret used to access the server

service (*multiple choice: hotspot | login | ppp | telephony | wireless*; default: "") - specifies services that will use this RADIUS server

- **hotspot** - HotSpot authentication service
- **login** - router's local user authentication
- **ppp** - Point-to-Point clients authentication
- **telephony** - IP telephony accounting
- **wireless** - wireless client authentication(client's MAC address is sent as User-Name)

timeout (*time*; default: **100ms**) - specifies timeout after which the request should be resend

Notes

The order of the items in this list is significant.

Microsoft Windows clients send their usernames in form **domain\username**

When RADIUS server is authenticating user with CHAP, MS-CHAPv1, MS-CHAPv2, it is not using shared secret, secret is used only in authentication reply, and router is verifying it. So if you have wrong shared secret, RADIUS server will accept request, but router won't accept reply. You can see that with **/radius monitor** command, "bad-replies" number should increase whenever somebody tries to connect.

Example

To set a RADIUS server for **HotSpot** and **PPP** services that has **10.0.0.3** IP address and **ex** shared secret, you need to do the following:

```
[admin@MikroTik] radius> add service=hotspot,ppp address=10.0.0.3 secret=ex
[admin@MikroTik] radius> print
Flags: X - disabled
  #   SERVICE         CALLED-ID     DOMAIN        ADDRESS         SECRET
  0   ppp,hotspot                                 10.0.0.3        ex

[admin@MikroTik] radius>

AAA for the respective services should be enabled too:

[admin@MikroTik] radius> /ppp aaa set use-radius=yes
[admin@MikroTik] radius> /ip hotspot aaa set use-radius=yes

To view some statistics for a client:

[admin@MikroTik] radius> monitor 0
             pending: 0
            requests: 10
             accepts: 4
             rejects: 1
             resends: 15
```

```
            timeouts: 5
         bad-replies: 0
     last-request-rtt: 0s

 [admin@MikroTik] radius>
```

Suggested RADIUS Servers

Description

MikroTik RouterOS RADIUS Client should work well with all RFC compliant servers. It has been tested with:

- ***FreeRADIUS***
- ***XTRadius*** (does not currently support MS-CHAP)
- ***Steel-Belted Radius***

Supported RADIUS Attributes

Description

MikroTik RADIUS Dictionaries

Here you can download ***MikroTik reference dictionary***, which incorporates all the needed RADIUS attributes. This dictionary is the minimal dictionary, which is enough to support all features of MikroTik RouterOS. It is designed for FreeRADIUS, but may also be used with many other UNIX RADIUS servers (eg. XTRadius).

Note that it may conflict with the default configuration files of RADIUS server, which have references to the Attributes, absent in this dictionary. Please correct the configuration files, not the dictionary, as no other Attributes are supported by MikroTik RouterOS.

There is also ***dictionary.mikrotik*** that can be included in an existing dictionary to support MikroTik vendor-specific Attributes.

Definitions

- **PPPs** - PPP, PPTP, PPPoE and ISDN
- **default configuration** - settings in default profile (for PPPs) or HotSpot server settings (for HotSpot)

Access-Request

- **Service-Type** - always is "Framed" (only for PPPs)
- **Framed-Protocol** - always is "PPP" (only for PPPs)
- **NAS-Identifier** - router identity
- **NAS-IP-Address** - IP address of the router itself

- **NAS-Port** - unique session ID
- **NAS-Port-Type** - async PPP - "Async"; PPTP and L2TP - "Virtual"; PPPoE and HotSpot - "Ethernet"; ISDN - "ISDN Sync"
- **Calling-Station-Id** - PPPoE - client MAC address with capital letters; PPTP and L2TP - client public IP address; HotSpot - MAC address of the client if it is known, or IP address of the client if MAC address is unknown; ISDN - client MSN
- **Called-Station-Id** - PPPoE - service name; PPTP and L2TP - server IP address; ISDN - interface MSN; HotSpot - MAC of the hotspot interface (if known), else IP of hotspot interface specified in hotspot menu (if set), else attribute not present
- **NAS-Port-Id** - async PPP - serial port name; PPPoE - ethernet interface name on which server is running; HotSpot - name of the hotspot interface (if known), otherwise - not present; not present for ISDN, PPTP and L2TP
- **Framed-IP-Address** - IP address of HotSpot client (for HotSpot enabled-address login method only)
- **User-Name** - client login name
- **MS-CHAP-Domain** - User domain, if present
- **Realm** - If it is set in /radius menu, it is included in every RADIUS request as Mikrotik-Realm attribute. If it is not set, the same value is sent as in MS-CHAP-Domain attribute (if MS-CHAP-Domain is missing, Realm is not included neither)
- **User-Password** - encrypted password (used with PAP authentication)
- **CHAP-Password, CHAP-Challenge** - encrypted password and challenge (used with CHAP authentication)
- **MS-CHAP-Response, MS-CHAP-Challenge** - encrypted password and challenge (used with MS-CHAPv1 authentication)
- **MS-CHAP2-Response, MS-CHAP-Challenge** - encrypted password and challenge (used with MS-CHAPv2 authentication)

Depending on authentication methods (NOTE: HotSpot uses CHAP by default and may use also PAP if unencrypted passwords are enabled, it can not use MSCHAP):

Access-Accept

- **Framed-IP-Address** - IP address given to client. PPPs - if address belongs to 127.0.0.0/8 or 224.0.0.0/3 networks, IP pool is used from the default profile to allocate client IP address. HotSpot - used only for dhcp-pool login method (ignored for enabled-address method), if address is 255.255.255.254, IP pool is used from HotSpot settings; if Framed-IP-Address is specified, Framed-Pool is ignored
- **Framed-IP-Netmask** - client netmask. PPPs - if specified, a route will be created to the network Framed-IP-Address belongs to via the Framed-IP-Address gateway; HotSpot - ignored by HotSpot
- **Framed-Pool** - IP pool name (on the router) from which to get IP address for the client. If specified, overrides Framed-IP-Address

NOTE: if Framed-IP-Address or Framed-Pool is specified it overrides remote-address in default configuration

- **Idle-Timeout** - overrides idle-timeout in the default configuration

- **Session-Timeout** - overrides session-timeout in the default configuration
- **Class** - cookie, will be included in Accounting-Request unchanged
- **Framed-Route** - routes to add on the server. Format is specified in RFC2865 (Ch. 5.22), can be specified as many times as needed
- **Filter-Id** - firewall filter chain name. It is used to make a dynamic firewall rule. Firewall chain name can have suffix .in or .out, that will install rule only for incoming or outgoing traffic. Multiple Filter-id can be provided, but only last ones for incoming and outgoing is used. For PPPs - filter rules in ppp chain that will jump to the specified chain, if a packet has come to/from the client (that means that you should first create a ppp chain and make jump rules that would put actual traffic to this chain). The same applies for HotSpot, but the rules will be created in hotspot chain
- **Acct-Interim-Interval** - interim-update for RADIUS client, if 0 uses the one specified in RADIUS client
- **MS-MPPE-Encryption-Policy** - require-encryption property (PPPs only)
- **MS-MPPE-Encryption-Types** - use-encryption property, non-zero value means to use encryption (PPPs only)
- **Ascend-Data-Rate** - tx/rx data rate limitation if multiple attributes are provided, first limits tx data rate, second - rx data rate. If used together with Ascend-Xmit-Rate, specifies rx rate. 0 if unlimited
- **Ascend-Xmit-Rate** - tx data rate limitation. It may be used to specify tx limit only instead of sending two sequental Ascend-Data-Rate attributes (in that case Ascend-Data-Rate will specify the receive rate). 0 if unlimited
- **MS-CHAP2-Success** - auth. response if MS-CHAPv2 was used (for PPPs only)
- **MS-MPPE-Send-Key, MS-MPPE-Recv-Key** - encryption keys for encrypted PPPs provided by RADIUS server only is MS-CHAPv2 was used as authentication (for PPPs only)
- **Ascend-Client-Gateway** - client gateway for DHCP-pool HotSpot login method (HotSpot only)
- **Recv-Limit** - total receive limit in bytes for the client
- **Xmit-Limit** - total transmit limit in bytes for the client
- **Wireless-Forward** - not forward the client's frames back to the wireless infrastructure if this attribute is set to "0" (Wireless only)
- **Wireless-Skip-Dot1x** - disable 802.1x authentication for the particulat wireless client if set to non-zero value (Wireless only)
- **Wireless-Enc-Algo** - WEP encryption algorithm: 0 - no encryption, 1 - 40-bit WEP, 2 - 104-bit WEP (Wireless only)
- **Wireless-Enc-Key** - WEP encruption key for the client (Wireless only)
- **Rate-Limit** - Datarate limitation for clients (PPPs only). Format is: rx-rate[/tx-rate] [rx-burst-rate[/tx-burst-rate] [rx-burst-threshold[/tx-burst-threshold] [rx-burst-time[/tx-burst-time]]]]. All rates should be numbers with optional 'k' (1,000s) or 'M' (1,000,000s). If tx-rate is not specified, rx-rate is as tx-rate too. Same goes for tx-burst-rate and 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 is used as burst thresholds. If both rx-burst-time and tx-burst-time are not specified, 1s is used as default.
- **Group** - Router local user group name (defimes in /user group; only for local users)

Note that the received attributes override the default ones (set in the default profile), but if an attribute is not received from RADIUS server, the default one is to be used.

Here are some Rate-Limit examples:

- **128k** - rx-rate=128000, tx-rate=128000 (no bursts)
- **64k/128M** - rx-rate=64000, tx-rate=128000000
- **64k 256k** - rx/tx-rate=64000, rx/tx-burst-rate=256000, rx/tx-burst-threshold=64000, rx/tx-burst-time=1s
- **64k/64k 256k/256k 128k/128k 10/10** - rx/tx-rate=64000, rx/tx-burst-rate=256000, rx/tx-burst-threshold=128000, rx/tx-burst-time=10s

Accounting-Request

- **Acct-Status-Type** - Start, Stop, or Interim-Update
- **Acct-Session-Id** - accounting session ID
- **Service-Type** - same as in request (PPPs only)
- **Framed-Protocol** - same as in request (PPPs only)
- **NAS-Identifier** - same as in request
- **NAS-IP-Address** - same as in request
- **User-Name** - same as in request
- **MS-CHAP-Domain** - same as in request (only for PPPs)
- **NAS-Port-Type** - same as in request
- **NAS-Port** - same as in request
- **NAS-Port-Id** - same as in request
- **Calling-Station-Id** - same as in request
- **Called-Station-Id** - same as in request
- **Acct-Authentic** - either authenticated by the RADIUS or Local authority (PPPs only)
- **Framed-IP-Address** - IP address given to the user
- **Framed-IP-Netmask** - same as in RADIUS reply
- **Class** - RADIUS server cookie (PPPs only)
- **Acct-Delay-Time** - how long does the router try to send this Accounting-Request packet

Stop and Interim-Update Accounting-Request

- **Acct-Session-Time** - connection uptime in seconds
- **Acct-Input-Octets** - bytes received from the client
- **Acct-Input-Gigawords** - 4G (2^32) bytes received from the client (bits 32..63, when bits 0..31 are delivered in Acct-Input-Octets) (HotSpot only)
- **Acct-Input-Packets** - nubmer of packets received from the client
- **Acct-Output-Octets** - bytes sent to the client
- **Acct-Output-Gigawords** - 4G (2^32) bytes sent to the client (bits 32..63, when bits 0..31 are delivered in Acct-Output-Octets) (HotSpot only)

- **Acct-Output-Packets** - number of packets sent to the client

Stop Accounting-Request

These packets can additionally have:

- **Acct-Terminate-Cause** - session termination cause (see RFC2866 ch. 5.10)

Attribute Numeric Values

Name	VendorID	Value	RFC where it is defined
Acct-Authentic		45	RFC2866
Acct-Delay-Time		41	RFC2866
Acct-Input-Gigawords		52	RFC2869
Acct-Input-Octets		42	RFC2866
Acct-Input-Packets		47	RFC2866
Acct-Interim-Interval		85	RFC2869
Acct-Output-Gigawords		53	RFC2869
Acct-Output-Octets		43	RFC2866
Acct-Output-Packets		48	RFC2866
Acct-Session-Id		44	RFC2866
Acct-Session-Time		46	RFC2866
Acct-Status-Type		40	RFC2866
Acct-Terminate-Cause		49	RFC2866
Ascend-Client-Gateway	529	132	
Ascend-Data-Rate	529	197	
Ascend-Xmit-Rate	529	255	
Called-Station-Id		30	RFC2865
Calling-Station-Id		31	RFC2865
CHAP-Challenge		60	RFC2866
CHAP-Password		3	RFC2865
Class		25	RFC2865
Filter-Id		11	RFC2865
Framed-IP-Address		8	RFC2865
Framed-IP-Netmask		9	RFC2865
Framed-Pool		88	RFC2869
Framed-Protocol		7	RFC2865

Framed-Route		22	RFC2865
Group	14988	3	
Idle-Timeout		28	RFC2865
MS-CHAP-Challenge	311	11	RFC2548
MS-CHAP-Domain	311	10	RFC2548
MS-CHAP-Response	311	1	RFC2548
MS-CHAP2-Response	311	25	RFC2548
MS-CHAP2-Success	311	26	RFC2548
MS-MPPE-Encryption-Policy	311	7	RFC2548
MS-MPPE-Encryption-Types	311	8	RFC2548
MS-MPPE-Recv-Key	311	17	RFC2548
MS-MPPE-Send-Key	311	16	RFC2548
NAS-Identifier		32	RFC2865
NAS-Port		5	RFC2865
NAS-Port-Id		87	RFC2869
NAS-Port-Type		61	RFC2865
Rate-Limit	14988	8	
Realm	14988	9	
Recv-Limit	14988	1	
Service-Type		6	RFC2865
Session-Timeout		27	RFC2865
User-Name		1	RFC2865
User-Password		2	RFC2865
Wireless-Enc-Algo	14988	6	
Wireless-Enc-Key	14988	7	
Wireless-Forward	14988	4	
Wireless-Skip-Dot1x	14988	5	
Xmit-Limit	14988	2	

Troubleshooting

Description

- **My radius server accepts authentication request from the client with "Auth: Login OK:...", but the user cannot log on. The bad replies counter is incrementing under radius monitor**

This situation can occur, if the radius client and server have high delay link between them. Try to increase the radius client's timeout to 600ms or more instead of the default 300ms! Also, double check, if the secrets match on client and server!