RADIUS client

Document revision 1.6 (February 14, 2007, 12:00 GMT)
This document applies to V2.9

Table of Contents

General Information

Summary

This document provides information about RouterOS built-in RADIUS client configuration, supported RADIUS attributes and recommendations on RADIUS server selection.

Specifications

Packages required: ***system***
License required: ***level1***
Home menu level: ***/radius***
Standards and Technologies: ***RADIUS***

Related Documents

- HotSpot User AAA
- Router User AAA

- PPP User AAA
- Software Package Management
- IP Addresses and ARP

Description

RADIUS, short for Remote Authentication Dial-In User Service, is a remote server that provides authentication and accounting facilities to various network apliances. RADIUS authentication and accounting gives the ISP or network administrator 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 HotSpot, 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.

The RADIUS server database is consulted only if no matching user acces record is found in router's local database.

Traffic is accounted locally with MikroTik Traffic Flow and 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.

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**) - this entry is a backup RADIUS accounting server

accounting-port (*integer*; default: **1813**) - RADIUS server port used for accounting

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

authentication-port (*integer*; default: **1812**) - RADIUS server port used for authentication

called-id (*text*; default: "") - value 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 passed to RADIUS servers that require domain validation

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 RADIUS server

service (*multiple choice: hotspot | login | ppp | telephony | wireless | dhcp*; default: **""**) - router 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)
- **dhcp** - DHCP protocol client authentication (client's MAC address is sent as User-Name)

timeout (*time*; default: **100ms**) - 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 profile set default 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>
```

Connection Terminating from RADIUS

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

Description

This facility supports unsolicited messages sent from RADIUS server. Unsolicited messages extend RADIUS

protocol commands, that allow to terminate a session which has already been connected from RADIUS server. For this purpose DM (Disconnect-Messages) are used. Disconnect messages cause a user session to be terminated immediately

Property Description

accept (yes | no; default: **no**) - Whether to accept the unsolicited messages

port (*integer*; default: **1700**) - The port number to listen for the requests on

Notes

RouterOS doesn't support POD (Packet of Disconnect) the other RADIUS access request packet that performs a similar function as Disconnect Messages

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
- **Acct-Session-Id** - unique session ID
- **NAS-Port-Type** - async PPP - "Async"; PPTP and L2TP - "Virtual"; PPPoE - "Ethernet"; ISDN - "ISDN Sync"; HotSpot - "Ethernet | Cable | Wireless-802.11" (according to the value of nas-port-type parameter in /ip hotspot profile
- **Calling-Station-Id** - PPPoE and HotSpot- client MAC address in capital letters; PPTP and L2TP - client public IP address; ISDN - client MSN
- **Called-Station-Id** - PPPoE - service name; PPTP and L2TP - server IP address; ISDN - interface MSN; HotSpot - name of the HotSpot server
- **NAS-Port-Id** - async PPP - serial port name; PPPoE - ethernet interface name on which server is running; HotSpot - name of the physical HotSpot interface (if bridged, the bridge port name is showed here); not present for ISDN, PPTP and L2TP
- **Framed-IP-Address** - IP address of HotSpot client after Universal Client translation
- **Mikrotik-Host-IP** - IP address of HotSpot client before Universal Client translation (the original IP address of the client)
- **User-Name** - client login name
- **MS-CHAP-Domain** - User domain, if present
- **Mikrotik-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)
- **WISPr-Location-ID** - text string specified in radius-location-id property of the HotSpot server
- **WISPr-Location-Name** - text string specified in radius-location-name property of the HotSpot server
- **WISPr-Logoff-URL** - full link to the login page (for example, http://10.48.0.1/lv/logout)
- **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. 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. 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 Framed-IP-Address is specified, this attribute is ignored

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
- **Port-Limit** - maximal number of simultaneous connections using the same username (overrides te shared-users property of the HotSpot user profile)
- **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
- **Mikrotik-Mark-Id** - firewall mangle chain name (HotSpot only). The MikroTik RADIUS client upon receiving this attribute creates a dynamic firewall mangle rule with action=jump chain=hotspot and jump-target equal to the atribute value. Mangle chain name can have suffixes .in or .out, that will install rule only for incoming or outgoing traffic. Multiple Mark-id attributes can be provided, but only last ones for incoming and outgoing is used.
- **Acct-Interim-Interval** - interim-update for RADIUS client. PPP - if 0 uses the one specified in RADIUS client; HotSpot - only respected if radius-interim-update=received in HotSpot server profile
- **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. Ignored if Rate-Limit attribute is present
- **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. Ignored if Rate-Limit attribute is present
- **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)

- **Mikrotik-Recv-Limit** - total receive limit in bytes for the client
- **Mikrotik-Recv-Limit-Gigawords** - 4G (2^32) bytes of total receive limit (bits 32..63, when bits 0..31 are delivered in Mikrotik-Recv-Limit)
- **Mikrotik-Xmit-Limit** - total transmit limit in bytes for the client
- **Mikrotik-Xmit-Limit-Gigawords** - 4G (2^32) bytes of total transmit limit (bits 32..63, when bits 0..31 are delivered in Mikrotik-Recv-Limit)
- **Mikrotik-Wireless-Forward** - not forward the client's frames back to the wireless infrastructure if this attribute is set to "0" (Wireless only)
- **Mikrotik-Wireless-Skip-Dot1x** - disable 802.1x authentication for the particulat wireless client if set to non-zero value (Wireless only)
- **Mikrotik-Wireless-Enc-Algo** - WEP encryption algorithm: 0 - no encryption, 1 - 40-bit WEP, 2 - 104-bit WEP (Wireless only)
- **Mikrotik-Wireless-Enc-Key** - WEP encruption key for the client (Wireless only)
- **Mikrotik-Rate-Limit** - Datarate limitation for clients. Format is: 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 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. 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.
- **Mikrotik-Group** - Router local user group name (defines in /user group) for local users. HotSpot default profile for HotSpot users.
- **Mikrotik-Advertise-URL** - URL of the page with advertisements that should be displayed to clients. If this attribute is specified, advertisements are enabled automatically, including transparent proxy, even if they were explicitly disabled in the corresponding user profile. Multiple attribute instances may be send by RADIUS server to specify additional URLs which are choosen in round robin fashion.
- **Mikrotik-Advertise-Interval** - Time interval between two adjacent advertisements. Multiple attribute instances may be send by RADIUS server to specify additional intervals. All interval values are threated as a list and are taken one-by-one for each successful advertisement. If end of list is reached, the last value is continued to be used.
- **WISPr-Redirection-URL** - URL, which the clients will be redirected to after successfull login
- **WISPr-Bandwidth-Min-Up** - minimal datarate (CIR) provided for the client upload
- **WISPr-Bandwidth-Min-Down** - minimal datarate (CIR) provided for the client download
- **WISPr-Bandwidth-Max-Up** - maxmal datarate (MIR) provided for the client upload
- **WISPr-Bandwidth-Max-Down** - maxmal datarate (MIR) provided for the client download
- **WISPr-Session-Terminate-Time** - time, when the user should be disconnected; in "YYYY-MM-DDThh:mm:ssTZD" form, where Y - year; M - month; D - day; T - separator symbol (must be written between date and time); h - hour (in 24 hour format); m - minute; s - second; TZD - time zone in one of these forms: "+hh:mm", "+hhmm", "-hh:mm", "-hhmm"

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.

Rate-Limit takes precedence over all other ways to specify data rate for the client. Ascend data rate attributes are considered second; and WISPr attributes takes the last precedence.

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

The accounting request carries the same attributes as Access Request, plus these ones:

- **Acct-Status-Type** - Start, Stop, or Interim-Update
- **Acct-Authentic** - either authenticated by the RADIUS or Local authority (PPPs only)
- **Class** - RADIUS server cookie, as received in Access-Accept
- **Acct-Delay-Time** - how long does the router try to send this Accounting-Request packet

Stop and Interim-Update Accounting-Request

Additionally to the accounting start request, the following messages will contain the following attributes:

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

Stop Accounting-Request

These packets will, additionally to the Interim Update packets, have:

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

Change of Authorization

RADIUS disconnect and Change of Authorization (according to RFC3576) are supported as well. These attributes may be changed by a CoA request from the RADIUS server:

- Mikrotik-Group
- Mikrotik-Recv-Limit
- Mikrotik-Xmit-Limit
- Mikrotik-Rate-Limit
- Ascend-Data-Rate (only if **Mikrotik-Rate-Limit** is not present)
- Ascend-XMit-Rate (only if **Mikrotik-Rate-Limit** is not present)
- Mikrotik-Mark-Id
- Filter-Id
- Mikrotik-Advertise-Url
- Mikrotik-Advertise-Interval
- Session-Timeout
- Idle-Timeout
- Port-Limit

Note that it is not possible to change IP address, pool or routes that way - for such changes a user must be disconnected first.

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
Idle-Timeout		28	RFC2865
Mikrotik-Advertise-Interval	14988	13	
Mikrotik-Advertise-URL	14988	12	
Mikrotik-Group	14988	3	
Mikrotik-Host-IP	14988	10	
Mikrotik-Mark-Id	14988	11	
Mikrotik-Rate-Limit	14988	8	
Mikrotik-Realm	14988	9	
Mikrotik-Recv-Limit	14988	1	
Mikrotik-Recv-Limit-Gigawords	14988	14	
Mikrotik-Wireless-Enc-Algo	14988	6	
Mikrotik-Wireless-Enc-Key	14988	7	
Mikrotik-Wireless-Forward	14988	4	
Mikrotik-Wireless-Skip-Dot1x	14988	5	
Mikrotik-Xmit-Limit	14988	2	
Mikrotik-Xmit-Limit-Gigawords	14988	15	
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-IP-Address		4	RFC2865
NAS-Port-Id		87	RFC2869
NAS-Port-Type		61	RFC2865
Port-Limit		62	RFC2865
Service-Type		6	RFC2865
Session-Timeout		27	RFC2865
User-Name		1	RFC2865
User-Password		2	RFC2865
WISPr-Bandwidth-Max-Down	14122	8	wi-fi.org
WISPr-Bandwidth-Max-Up	14122	7	wi-fi.org
WISPr-Bandwidth-Min-Down	14122	6	wi-fi.org
WISPr-Bandwidth-Min-Up	14122	5	wi-fi.org
WISPr-Location-Id	14122	1	wi-fi.org
WISPr-Location-Name	14122	2	wi-fi.org
WISPr-Logoff-URL	14122	3	wi-fi.org
WISPr-Redirection-URL	14122	4	wi-fi.org
WISPr-Session-Terminate-Time	14122	9	wi-fi.org

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!