

# AZOTEL S08-02 v104 (2016-12)

# S08 - RADIUS Mikrotik: Customer PPPoE Authentication



Phone (EMEA): +353-21-234-8100 Phone (North America): +1-312-239-0680 / +1-902-539-2665 Phone (Poland): +48-71-710-1530 Phone (UK): +44-20-719-3417 Phone (South Africa): +27-11-083-6900 Fax: +353-21-467-1699 <u>info@azotel.com</u>

# Contents

| Conte                                              | nts                                                                                                                                                                                                                        | 2                                              |
|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|
| 1                                                  | Scope                                                                                                                                                                                                                      | 3                                              |
| 2                                                  | Prerequisites                                                                                                                                                                                                              | 4                                              |
| 3<br>3.1<br>3.2<br>3.3<br>3.4                      | SIMPLer server configuration<br>Adding a new Network Access Server to the system<br>Setting up RADIUS Groups for Bandwidth Limiting<br>Customer settings – manual configuration<br>Customer settings – automated provision | 5<br>5<br>7<br>9<br>10                         |
| 4<br>4.1<br>4.2<br>4.3<br>4.4<br>4.5<br>4.6<br>4.7 | Mikrotik NAS configuration<br>RADIUS configuration<br>Address List<br>IP Pools<br>PPPoE Setup<br>Web Proxy Setup<br>Firewall Setup<br>Redirection Page                                                                     | . 14<br>14<br>16<br>16<br>17<br>19<br>19<br>22 |
| 5<br>5.1                                           | Debugging<br>Expected throughputs are not achieved                                                                                                                                                                         | . 23                                           |
| 6<br>6.1<br>6.2                                    | IPv6 Notes<br>Getting dynamic IPv6 prefix from IP pool<br>Getting a static IPv6 prefix from RADIUS / SIMPLer                                                                                                               | . 24<br>24<br>25                               |
| Annez<br>A.1<br>A.2                                | x A: References<br>Document References<br>Link References                                                                                                                                                                  | . 26<br>26<br>26                               |
| Annez<br>B.1<br>B.2                                | x B: Definitions & Abbreviations<br>Definitions<br>Abbreviations                                                                                                                                                           | . 27<br>27<br>27                               |
| Anne                                               | x C: Typical index.html file                                                                                                                                                                                               | . 28                                           |
| Anne                                               | x D: Change history                                                                                                                                                                                                        | .30                                            |

# 1 Scope

The purpose of this guide is to explain the integration of an Operator's Network with Azotel's SIMPLer platform, using a Mikrotik device with PPPoE authentication and a RADIUS server.

Note that the operator's network must be integrated with the SIMPLer platform, in order to have the ability to:

- control customer access to the network based on the customer's status,
- authorise an appropriate level of service to the customer's connection accordingly to the products provisioned to their account, and
- logging of the usage data to their account, which can then be used for Usage Based Billing.

There are two main branches to integrating the SIMPLer platform:

- using WIB-C controllers in-line to control the traffic in the operator network
- using **RADIUS** to integrate SIMPLer with Network Access Server (NAS'es) deployed in the operator network

This manual explains the second scenario: "using RADIUS to integrate SIMPLer with NAS'es" where a Mikrotik device is used as a NAS. There are number of options a Mikrotik controller can utilise to provide RADIUS authenticated customer traffic control:

- **PPPoE** a PPPoE server can be run on Mikrotik. This approach provides a full Authentication / Authorization / Accounting integration with SIMPLer platform. It requires switching the network to use the PPPoE protocol. *This is the precise scenario, described in this guide.*
- *Hotspot* a standard hotspot controller can be run on Mikrotik this approach provides a full Authentication / Authorization / Accounting integration with the SIMPLer platform. The Operator can use hotspot services for both 'recurring' and 'hotspot' type customers. Customers are required to log in via a splash page.
- *Hotspot with Mac Authentication* using this mode allows the Operator to deploy a *login-less* authentication mechanism for recurring customers. This approach provides a full Authentication / Authorization / Accounting integration with SIMPLer platform. If the MAC address for a customer already exists in RADIUS, that customer will be authenticated without the need to go through the Customer Portal. It requires a Layer 2 connection between the Mikrotik and the customer.
- *WiFi* Mikrotik can authenticate a wireless CPE access and register only units with MAC addresses that are defined under customer accounts. This approach provides only the Authentication / Authorization integration with SIMPLer platform. There will be no Accounting data sent from Mikrotik to SIMPLer. This can be used as an additional security measure, by the Operator.
- **DHCP** Mikrotik can run a standalone DHCP server that will assign IP addresses based on what is defined under the customer account in SIMPLer. This approach provides only the Authentication / Authorization integration with SIMPLer platform. There will be no Accounting data sent from Mikrotik to SIMPLer. This should be treated as an additional service that can be provided from RADIUS integration.

To conclude, this document will discuss in detail the first scenario i.e. PPPoE option.

## 2 Prerequisites

In order to have this setup completed Operator's network must cover following components / requirements:

- 1) **RADIUS server** Azotel recommend using a local to operator RADIUS servers
- 2) Mikrotik Router
- 3) Flat (switched or VLAN) network run between Mikrotik and CPE.



Fig. 2.1. Mikrotik: customer PPPoE Authentication integrated with SIMPLer using RADIUS server

# 3 SIMPLer server configuration

#### 3.1 Adding a new Network Access Server to the system

Note: Local RADIUS server (if local RADIUS server is used) must be integrated with the SIMPLer platform prior to starting the configuration procedure. Contact Azotel at: *support@azotel.com* to get details on that procedure

Note: It is possible to use a RADIUS server embedded into SIMPLer platform. Each SIMPLer server runs a RADIUS server at standard ports (1812 for Authentication and Authorization and 1813 for Accounting) under its public IP address. Though it is not recommended to use the embedded server for production environment – a local to operator's network RADIUs server should be deployed

Note: For the purpose of this guide following assumptions have been made on the RADIUS server:

- RADIUS IP address: 192.168.1.125
- The RADIUS server is local to operator's network
- RADIUS server has already been integrated with SIMPLer platform

Note: The SIMPLer platform management actions described here may not cover all details/options available for RADIUS integration under SIMPLer. For further details please refer to *RADIUS Integration User's Guide* that can be found under: *http://www.azotel.com/azotel-operator-manuals-doc/* 

For security reasons each RADIUS server runs it's ACL (Access Lists) that covers the NAS'es allowed to communicate with the server. This list can be managed from SIMPLer platform. Follow the steps below to add a new NAS position to your local RADIUS server using SIMPLer platform:

- 1. Login to SIMPLer platform using your credentials
- 2. Click on "RADIUS" button than choose "Network Access Servers" (Fig. 3.1.1)

| azot                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | tside WISP:<br>login:<br>Radius                | Testss<br>maciej<br>Server Manage | ement    |         | Recently Viewe | ed Customers |        |       | 🛥 Inbox (1) | SIN    | APLer       | ~ |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|-----------------------------------|----------|---------|----------------|--------------|--------|-------|-------------|--------|-------------|---|
| Dashboard Map                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Customers                                      | Invoices                          | Products | Network | Hotspots       | Voip         | Radius | Tools | Settings    | Logout | QuickSearch |   |
| Radius Databa<br>127.0.0.1-radius<br>Settinos:<br>Network Access<br>IP Pool<br>Individual Checi<br>Individual | se:<br>v<br>s Servers<br>on<br>nns<br>ignement |                                   |          |         |                |              |        |       |             |        |             |   |

Fig. 3.1.1. RADIUS -> Network Access Server page

3. Click "Add Blank Row" button to add a new NAS entry to the table (Fig. 3.1.2)

| Network Access Servers |           |         |         |      |           |                         |
|------------------------|-----------|---------|---------|------|-----------|-------------------------|
| IP Address / Hostname* | Name*     | Туре*   | Secret* | Port | Community | Description             |
| 192.168.1.135          | test_main | other 🗘 | secret  | 3799 | read      | Test Description Delete |
| Add Blank Row          |           |         |         |      |           |                         |

Fig. 3.1.2. Add a new Network Access Server entry

Below find description of each field you can define for new Network Access Server entries:

• Mikrotik IP address: (example) 192.168.1.135

NOTE: IP address defined under this field must represent the effective IP address used to communicate with the RADIUS server. If a Mikrotik IP address is NAT'ed on the path to RADIUS server the IP address of the NATing router should be used.

• Name: (example) main

NOTE: Name should match name defined under "System->Identity" on Mikrotik Router (Fig. 3.1.3). Setting up Mikrotik will be covered in chapter 4.

| 101 2.5 |   | Diam                                     |          |        |
|---------|---|------------------------------------------|----------|--------|
| Routing |   | Drivers                                  | Identity |        |
| System  | 1 | Health                                   |          |        |
| Queues  |   | History                                  |          | UK     |
| Files   |   | Identity                                 |          | Cancel |
| Log     |   | LEDs                                     |          | Apply  |
| Radius  |   | License                                  |          |        |
|         |   | 1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1. |          |        |

Fig. 3.1.3. Winbox: Mikrotik NAS "System->Identity"

- *Type:* other
- Secret: (example) secret

NOTE: Secret must match secret defined under "RADIUS server" general details on Mikrotik (Fig. 3.1.4). Setting up Mikrotik will be covered in chapter 4.

| Radius Server <192.1 | 68.1.125>           |           |              |
|----------------------|---------------------|-----------|--------------|
| General Status       |                     |           | ОК           |
| - Service            |                     | _         | Cancel       |
| ✓ hotspot            | i login<br>wireless |           | Apply        |
| dhcp                 |                     |           | Disable      |
| Called ID:           |                     | •         | Comment      |
| Domain:              |                     | -         | Сору         |
| Address              | 102.100.1.120       |           | Remove       |
| Secret:              | secret              | $\supset$ | Reset Status |
| Authentication Port: | 1812                |           |              |
| Accounting Port:     | 1813                |           |              |
| Timeout:             | 300                 | ms        |              |
|                      | Accounting Backup   |           |              |
| Realm:               |                     | •         |              |
| Src. Address:        | 0.0.0.0             | •         |              |
| enabled              |                     |           |              |

Fig 3.1.4. Winbox: Mikrotik NAS "RADIUS Secret" field

• Port: (example) 3799

NOTE: Port number must match port number under "RADIUS -> Incoming" section on Mikrotik (Fig. 3.1.5). Setting up Mikrotik will be covered in chapter 4.

|     |         |                      |                                                            | 1       | _       |                                      |        |      |
|-----|---------|----------------------|------------------------------------------------------------|---------|---------|--------------------------------------|--------|------|
| + - | × ×     |                      | Reset Sta                                                  | atus Ir | ncoming |                                      |        | Find |
| #   | Service |                      | Called ID                                                  | Dom     | nin     | Lauress                              | Secret | -    |
| 0   | hotspot |                      |                                                            |         |         | 192.168.1.125                        | secret |      |
|     |         | Radius<br>R<br>Bad R | Port: 37<br>equests: 3<br>equests: 0<br>Acks: 3<br>Naks: 0 | 99      | Re      | OK<br>Cancel<br>Apply<br>eset Status |        |      |

Fig. 3.1.5. Winbox: Mikrotik NAS "Incoming port" number

- Community: (example) read
- Description: (example) Test Description
- 4. Click "Update Table" to submit adding a new entry

Note: It may take up to 60 seconds for a new NAS entry to become active on the local RADIUS server.

#### 3.2 Setting up RADIUS Groups for Bandwidth Limiting

Note: The SIMPLer platform management actions described here may not cover all details/options available for RADIUS integration under SIMPLer. For further details please refer to *RADIUS Integration User's Guide* that can be found under: *http://www.azotel.com/azotel-operator-manuals-doc/* 

All authenticated customers will get service they are authorized for. Most typical setup will cover the upload/download speed rates definition. This can be done under *"RADIUS->Group Reply"* section of the SIMPLer platform (Fig. 3.2.1). RADIUS Group Replies can be used to define common attributes (effectively services). Customers assigned to a group will inherit the group services. To add a new "RADIUS Group Reply" with Uplink / Downlink rate limits on a Mikrotik follow below steps:

|        | Outside Radius Server Management |           |           |          |          |         |          | .,100) out of s | ync! Update V | VIB files |
|--------|----------------------------------|-----------|-----------|----------|----------|---------|----------|-----------------|---------------|-----------|
| Dashbo | oard                             | Мар       | Customers | Invoices | Products | Network | Hotspots | Voip            | Radius        | Tocls     |
|        |                                  |           |           |          |          |         |          |                 |               |           |
| R      | adius D                          | atabase   | :         |          |          |         |          |                 |               |           |
|        |                                  |           |           |          |          |         |          |                 |               |           |
|        | 127.0.0.1                        | -radius   | <u> </u>  |          |          |         |          |                 |               |           |
| Se     | ettings:                         |           |           |          |          |         |          |                 |               |           |
| Ν      | Vetwork A                        | Access Se | ervers    |          |          |         |          |                 |               |           |
| I      | P Pool                           |           |           |          |          |         |          |                 |               |           |
| li     | ndividual                        | Check     |           |          |          |         |          |                 |               |           |
| li     | ndividual                        | Reply     |           |          |          |         |          |                 |               |           |
| F      | Post Auth                        | orization |           |          |          |         |          |                 |               |           |
| V      | WiMAX E                          | xtensions |           |          |          |         |          |                 |               |           |
| L L    | Jser/Gro                         | up Assign | ement     |          |          |         |          |                 |               |           |
| -      | Croup Ci                         | icut:     |           |          |          |         |          |                 |               |           |
|        | Group Re                         | ply       |           |          |          |         |          |                 |               |           |
| A      | ceeunti                          | ngi       |           |          |          |         |          |                 |               |           |
| L      | Jsage De                         | etails    |           |          |          |         |          |                 |               |           |

1. Navigate to "Radius" -> "Group Reply" page (Fig. 3.2.1)



2. On "RADIUS Group Reply" page click "Add" to add a new group or add a new attribute to an existing group.

| Back Radius Management |           |    |       |                                              |
|------------------------|-----------|----|-------|----------------------------------------------|
| Radius Database:       |           |    |       |                                              |
| 127.0.0.1-radius 💌     |           |    |       |                                              |
| Browse Group Reply     |           |    |       |                                              |
| Attribute              |           |    |       |                                              |
| Value                  |           |    |       |                                              |
| Search                 |           |    |       |                                              |
|                        |           |    |       |                                              |
|                        |           |    |       |                                              |
| Group Reply            |           |    |       |                                              |
| Results 0 - 0 of 0     |           |    |       | Number of results to display per page : 50 💌 |
| ID Groupname           | Attribute | Ор | Value |                                              |
|                        |           |    |       |                                              |
| Add                    |           |    |       |                                              |

Fig. 3.2.2. "RADIUS -> Group Reply" page

- 3. If you add a new group do check radio button "Define new group" and enter following information:
  - Fill in the "Groupname": (example) fast speed.
  - From "*Dictionary*" dropdown select "*Mikrotik*" that will limit "*Attribute*" dropdown menu to list only Mikrotik attributes.
  - From "Attribute" dropdown menu select "Mikrotik-Rate-Limit".
  - Leave "*Operator*" to "=". Enter the desired speed for a customer connection in the following format: xxxk/yyyk (*example 512k/1024k*) where:
    - $\circ$  *xxx* numeric upload speed in kbits/sec
    - $\circ$  *yyy* numeric download speed in kbits/sec

See figure 3.2.3 for reference.

| Add Group Ra | aius Reply                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |  |  |  |  |  |
|--------------|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|--|--|--|
| Groupname*   | Choose from existing Groups<br>test_70 ♀ | In the second |  |  |  |  |  |
| Attribute*   | Mikrotik-Rate-Limit                      | Dictionary<br>Mikrotik                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |  |  |  |  |  |
| Op*          |                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |  |  |  |  |  |
| Value*       | /alue* 1024k/512k                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |  |  |  |  |  |
| Back         | eset Add                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |  |  |  |  |  |

Fig. 3.2.3. "RADIUS -> Group Reply -> Add Group Radius Reply" page

- 4. Click "Add" button to finish adding new group.
- 5. *Repeat steps 2-4* to define further groups with other speed definitions accordingly to the planned product / services.

Another important attribute used in most PPPoE applications is Framed Pool (fig. 3.2.4). As a value of Framed Pool attribute one enters the name of one of the pools defined on the Mikrotik router (fig. 3.2.5).

| Group Details<br>Groupname<br>Assigned to | test_fast_speed<br>1. customer(s) |            |
|-------------------------------------------|-----------------------------------|------------|
| Modify Group R                            | adius Reply                       |            |
| Groupname*                                | test_fast_speed                   | Distignary |
| Attribute*                                | Framed-Pool                       | ¢          |
| Op*                                       | = =                               |            |
| Value*                                    | PublicPool                        |            |
| Back Rese                                 | t Delete Update                   |            |
|                                           |                                   |            |

Fig. 3.2.4. "RADIUS -> Group Reply -> Add Group Radius Reply" page - "Framed Pool" example

| IP Pool              |                             |             |
|----------------------|-----------------------------|-------------|
| Pools Used Addresses |                             |             |
| + - 7                |                             | Find        |
| Name 🛆               | Addresses                   | Next Pool 🔹 |
| 🕆 PublicPool         | 172.16.191.2-172.16.191.250 | none        |
| 🕆 disconnected       | 172.16.190.2-172.16.190.254 | none        |
|                      |                             |             |
|                      |                             |             |
|                      |                             |             |
|                      |                             |             |
|                      |                             |             |
|                      |                             |             |

Fig. 3.2.5. Winbox: Mikrotik NAS "IP Pools"

Note: You can also define other group attributes here. Please refer to "Supported RADIUS Attributes" section of the following web page:

• http://www.mikrotik.com/testdocs/ros/2.9/guide/aaa radius.php

#### 3.3 Customer settings – manual configuration

Note: A customer account must be active (in *'current'* state) and assigned to a network gateway that has RADIUS option enabled prior to adding any RADIUS related details to a customer account. A network gateway setup is typically performed as a part of "integrating with a local RADIUS gateway" process, when an appropriate network gateway is created.

Note: The SIMPLer platform management actions described here may not cover all details/options available for RADIUS integration under SIMPLer. For further details please refer to *RADIUS Integration User's Guide* that can be found under: *http://www.azotel.com/azotel-operator-manuals-doc/* 

Following steps describe manual provision of a RADIUS details to a customer account.

• In SIMPLer platform on *customer account details* page scroll down to the "*Customer Network Details*" section. From "RADIUS details" subsection select "*modify*" (Fig. 3.4.1)

| Radius Details (modify) (his ory) |                                      |  |  |  |  |  |  |
|-----------------------------------|--------------------------------------|--|--|--|--|--|--|
| Gateway                           | WIB100 - RADIUS (wib-100)<br>0.0.0.0 |  |  |  |  |  |  |
| <b>Radius Authentication</b>      | Yes                                  |  |  |  |  |  |  |
| Radius Authorization              | Yes                                  |  |  |  |  |  |  |
| Radius Accounting                 | Yes                                  |  |  |  |  |  |  |
|                                   |                                      |  |  |  |  |  |  |

Fig. 3.3.1 Customer details page: "RADIUS Details" section

• On "*Customer RADIUS details*" page click on "*Customer RADIUS usernames*" button in order to add new customer username(s) (Fig. 3.3.2)

| Customer 711 (7                                | /11 )                     |                            |                           |  |
|------------------------------------------------|---------------------------|----------------------------|---------------------------|--|
| ID                                             | 711                       |                            |                           |  |
| Name                                           | John Doe "Office"         |                            |                           |  |
| Nickname                                       | 711                       |                            |                           |  |
| Invoicing ID                                   | 711                       |                            |                           |  |
| Customer Radius Det                            | ails                      |                            |                           |  |
| RADIUS Credentials                             |                           | Username                   | Password                  |  |
| Individual Radius Che<br>Individual Radius Reg | ecks                      | Not Defined<br>Not Defined |                           |  |
| Customer Details                               | Customer Radius Usernames | ndividual Radius Checks    | Individual Radius Replies |  |

Fig. 3.3.2. Customer RADIUS details page

• The usernames defined under "*RADIUS usernames*" page are used to authenticate the PPPoE account that is being pushed via Mikrotik controller (Fig. 3.3.3).

| Radius Usernames    |          |      |           |        |  |
|---------------------|----------|------|-----------|--------|--|
| Username* Password* |          | Prio | Priority* |        |  |
| jdoe                | password | 5    | •         | Delete |  |
| Add Blank Row       |          |      |           |        |  |

Fig. 3.3.3. Customer RADIUS Usernames

• Radius Groups contain information about services that customer can be authorized to. Once the usernames are added – it is best to add a customer to a RADIUS group in order to assign speed definitions to a customer connection. Click "*Add*" at the bottom of "Customer RADIUS details" page. From username list select the effective customer PPPoE account (*example: jdoe*). Check radio button "Choose from existing group" and select pre-defined group (*example: test fast speed*). Click "*Add*" to add new assignment (Fig. 3.3.4)

| Add Customer G          | iroup                                              |
|-------------------------|----------------------------------------------------|
| Username*               | jdoe 🗢                                             |
| Groupname*<br>Priority* | Ochoose from existing Groups   test_fast_speed   5 |
| Back Rese               | t Add                                              |

Fig. 3.3.4. Customer Group Assignment

Customers can also get static IP addresses assigned. To do that go back to the customer account page and click on "modify" near the customer IP table (fig. 3.3.5)



Fig. 3.3.5. "Customer Account"->"modify" IP table link

On "Customer IP table" page specify IP address that should be assigned to the customer account and assign RADIUS username to this specific IP address. This configuration will push "Framed IP address" attribute to the Mikrotik for customer authentication (fig. 3.3.6).

#### **Customer IP table**

| IP Address     | Туре    | MAC address | MAC to IP<br>Restiction | Hostname / Label | RADIUS<br>Username | рнср |
|----------------|---------|-------------|-------------------------|------------------|--------------------|------|
| 172.16.191.252 | Private | <b>.</b>    |                         |                  | jdoe               | Ðſ   |
| Add Blank Row  |         |             |                         |                  | $\sim$             |      |

Fig. 3.3.6. "Customer Account"->"modify" IP table link

This concludes a basic, manual customer setup. At this stage operator should have an active user account ready to be authenticated on a Mikrotik device.

#### 3.4 Customer settings – automated provision

There is a quick way to provision a customer while these are still in *'waiting for install'* status – a 'Provision w/o CPE' option is available for such account. This tool - that is designed to help bringing a customer 'current' without active provisioning process happening with a CPE - can be used to provision an account in a quick and efficient manner. It can be found on a customer details page.

Follow below steps to provision an account:

• On the "customer details" page click on "Provision w/o CPE" link (Fig 3.4.1)



11

Fig. 3.4.1. Customer Details Page

• Choose an appropriate gateway, than deselect the "*Create CPE entry*" and "*Generate IP address*" checkboxes unless we actually want to create a new CPE entry / assign a static IP to a customer account (Fig 3.4.2). Click "*Next*" button.

| Console           |                                                                                                                          |         |
|-------------------|--------------------------------------------------------------------------------------------------------------------------|---------|
| Provisio          | n w/o CPE                                                                                                                |         |
| Customer ID       | 27744                                                                                                                    |         |
| Invoicing ID      | AUTOP1                                                                                                                   |         |
| Nickname          | AUTOP1                                                                                                                   |         |
| Name              | Auto-Prov Customer                                                                                                       |         |
| Status            | waiting for install<br>Changed: Jan 12, 2013<br>Priority: 3<br>Waiting Since: Jan 21, 2013<br>Installer: nobody assigned |         |
| Step #1           |                                                                                                                          |         |
| Select Gateway    | RadiusWIB - wib 121 [1                                                                                                   | 18 ac 🔻 |
| Generate IP addre | sses                                                                                                                     |         |
| Create CPE entry  |                                                                                                                          |         |
| Next              |                                                                                                                          |         |
|                   |                                                                                                                          |         |
|                   |                                                                                                                          |         |
|                   |                                                                                                                          |         |

Fig. 3.4.2. "Provision w/o CPE" Step #1

• From a dropdown manu pick an appropriate "Bucket" for a customer and make sure the "Create RADIUS accounts" checkbox is selected (Fig. 3.4.3). Click "Next" button.

| Console            |                                                                                                                          | X |
|--------------------|--------------------------------------------------------------------------------------------------------------------------|---|
| Provision          | w/o CPE                                                                                                                  |   |
| Customer ID        | 27744                                                                                                                    |   |
| Invoicing ID       | AUTOP1                                                                                                                   |   |
| Nickname           | AUTOP1                                                                                                                   |   |
| Name               | Auto-Prov Customer                                                                                                       |   |
| Status             | waiting for install<br>Changed: Jan 12, 2013<br>Priority: 3<br>Waiting Since: Jan 21, 2013<br>Installer: nobody assigned |   |
| Step #2            |                                                                                                                          |   |
| Select Bucket      | Radius Group #1, 512, 512 💌                                                                                              |   |
| Create RADIUS acco | punts 🔽                                                                                                                  |   |
| Back Next          |                                                                                                                          |   |
|                    |                                                                                                                          |   |

Fig. 3.4.3. "Provision w/o CPE" Step #2

• Select the *"RADIUS group"* that defines best level of service for a customer, make sure to set the *"Number of RADIUS Accounts"* to 1. Set the *"RADIUS Username"* with an PPPoE username of customer and "RADIUS password" (Fig. 3.4.4)

#### Console

## **Provision w/o CPE**

| Customer ID  | 10911                                                                                                                  |
|--------------|------------------------------------------------------------------------------------------------------------------------|
| Invoicing ID | 10006                                                                                                                  |
| Nickname     | jimsmith                                                                                                               |
| Name         | Jim Smith                                                                                                              |
| Status       | waiting for install<br>Changed: 25 Jul 2012<br>Priority: 3<br>Waiting Since: 25 Jul 2012<br>Installer: nobody assigned |

#### Step #3

| Number of RADIUS<br>Accounts<br>RADIUS group | 1        |
|----------------------------------------------|----------|
| KADIOS group                                 | test_70  |
| RADIUS Username                              | jdoe     |
| RADIUS Password                              | password |
| Back Next                                    |          |

Fig. 3.4.4. "Provision w/o CPE" Step #3

Azotel Confidential Proprietary © Azotel Technologies Ltd 2024 X

• Verify the details on the provision process summary page. Go back and correct if anything is wrong, otherwise proceed clicking "Provision" button (Fig 3.4.5).

| Customer ID                                                                                                                                               | 27744                                        |                                                                                                                                                       |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| nvoicing ID                                                                                                                                               | AUTOP1                                       | 1                                                                                                                                                     |
| lickname                                                                                                                                                  | AUTOP1                                       |                                                                                                                                                       |
| lame                                                                                                                                                      | Auto-Pro                                     | ov Customer                                                                                                                                           |
|                                                                                                                                                           | Change<br>Priority:<br>Waiting<br>Installer: | d: Jan 12, 2013<br>3<br>Since: Jan 21, 2013<br>: nobody assigned                                                                                      |
|                                                                                                                                                           |                                              |                                                                                                                                                       |
| rovision<br>Gateway                                                                                                                                       |                                              | Radius/WIB - wib 121 [18 active sub(s)]                                                                                                               |
| Gateway<br>Bucket                                                                                                                                         |                                              | RadiusWIB - wib 121 [18 active sub(s)]<br>Radius Group #1, 512, 512 (25 in use)                                                                       |
| Gateway<br>Bucket<br>Generate IP Addresses                                                                                                                |                                              | RadiusWIB - wib 121 [18 active sub(s)]<br>Radius Group #1, 512, 512 (25 in use)<br>No                                                                 |
| Covision<br>Gateway<br>Bucket<br>Generate IP Addresses<br>Create RADIUS account                                                                           | ts                                           | RadiusWIB - wib 121 [18 active sub(s)]<br>Radius Group #1, 512, 512 (25 in use)<br>No<br>Yes                                                          |
| Covision<br>Gateway<br>Buoket<br>Generate IP Addresses<br>Create RADIUS accoun<br>Radius Group                                                            | ts                                           | RadiusWIB - wib 121 [18 active sub(s)]<br>Radius Group #1, 512, 512 (25 in use)<br>No<br>Yes<br>testss_87                                             |
| Covision<br>Gateway<br>Bucket<br>Generate IP Addresses<br>Create RADIUS accoun<br>Radius Group<br>Number of RADIUS                                        | ts<br>6 Accounts                             | RadiusWIB - wib 121 [18 active sub(s)]<br>Radius Group #1, 512, 512 (25 in use)<br>No<br>Yes<br>testss_87<br>1                                        |
| Covision<br>Gateway<br>Bucket<br>Generate IP Addresses<br>Create RADIUS accoun<br>Radius Group<br>Number of RADIUS<br>RADIUS Username                     | ts<br>6 Accounts                             | RadiusWIB - wib 121 [18 active sub(s)]<br>Radius Group #1, 512, 512 (25 in use)<br>No<br>Yes<br>testss_87<br>1<br>00:15:58:C2:95:F2                   |
| Crovision<br>Gateway<br>Bucket<br>Generate IP Addresses<br>Create RADIUS accoun<br>Radius Group<br>Number of RADIUS<br>RADIUS Username<br>RADIUS Password | ts<br>6 Accounts                             | RadiusWIB - wib 121 [18 active sub(s)]<br>Radius Group #1, 512, 512 (25 in use)<br>No<br>Yes<br>testss_87<br>1<br>00:15:58:C2:95:F2<br>password       |
| Create CPE entry<br>RADIUS Service<br>Radius Group<br>Number of RADIUS<br>RADIUS Username<br>RADIUS Password<br>Create CPE entry                          | ts<br>6 Accounts                             | RadiusWIB - wib 121 [18 active sub(s)]<br>Radius Group #1, 512, 512 (25 in use)<br>No<br>Yes<br>testss_87<br>1<br>00:15:58:C2:95:F2<br>password<br>No |

Fig. 3.4.5. "Provision w/o CPE" Step #4

• Wait for the SIMPLer platform to configure the customer account. Once that is finished a report page listing all steps undertaken by the system will be displayed (Fig. 3.4.6). This concludes the setup



Fig. 3.4.6. "Provision w/o CPE" Step #5

# 4 Mikrotik NAS configuration

Note: It is highly recommended to use Winbox to configure Mikrotik devices. The Winbox software can be downloaded from Mikrotik site:

• http://www.mikrotik.com/download

Note: Mikrotik NAS should be added to the SIMPLer RADIUS server NAS list in order to communicate properly with RADIUS server (see fig. 3.1.2). This has been covered in the chapter 3 of this guide.

Note: Mikrotik NAS System -> Identity (see fig. 4.1) should match NAS name defined under SIMPLer RADIUS NAS details table (fig. 3.1.3)

## 4.1 RADIUS configuration

1. On the left side menu in winbox click on the "RADIUS" button to get to the radius servers window (Fig. 4.1.1)

| 0            | admin@D4:CA:6D:52 | :5F:E3 (MikroTik) - WinBox v5.16 on RB751G-2HnD (mipsbe) |   |
|--------------|-------------------|----------------------------------------------------------|---|
| 5            | Cafe Mode         | 🗹 Hide Passwords 📕 🖻                                     | ð |
|              | Quick Set         |                                                          |   |
|              | Interfaces        |                                                          |   |
|              | Wireless          |                                                          |   |
|              | Bridge            | Radius 🗆 🗙                                               |   |
|              | PPP               | (+)→ ◇ ☆ ☎ ▼ Reset Status Incoming Find                  |   |
|              | Switch            | # Service Called ID Domain Address Secret 💌              |   |
|              | Mesh              |                                                          |   |
|              | IP 🗅              |                                                          |   |
|              | MPLS D            |                                                          |   |
|              | Routing           |                                                          |   |
|              | System N          |                                                          |   |
|              | Queues            |                                                          |   |
| ×            | Files             |                                                          |   |
| <sup>8</sup> | Loa               |                                                          |   |
| 3            | Radius            |                                                          |   |
| $\geq$       | Tools             |                                                          |   |
| SO           | New Terminal      |                                                          |   |
| er(          | MetaROUTER        | 0 items                                                  |   |
| ut           | Make Supout.rif   |                                                          |   |
| R            | Manual            |                                                          |   |

Fig. 4.1.1. Radius servers window

- 2. Click on red "+" (plus) button to add a new entry
- 3. Fill the new RADIUS server window with the following details (fig. 4.1.2):
  - Service: make sure that at least 'ppp' service is ticked (other services might be added if needed)
  - Address: fill in with the IP address of local RADIUS server (example: 192.168.1.125)
  - Secret: (example: secret) must match secret defined in SIMPLer RADIUS NAS table (refer to fig. 3.1.2)
  - *Authentication Port:* port 1812 is a default setting for a RADIUS Authentication use '1812' unless the local RADIUS server has been set otherwise
  - Accounting Port: port 1813 is a default setting for a RADIUS Accounting use '1813' unless the local RADIUS server has been set otherwise
  - *Timeout:* 300 ms (default). It depends on connection between Mikrotik and RADIUS. In some cases it might be required to increase its value. For local servers Azotel would recommend using the Timeout values up to a 1000ms, for remote server this value can be defined to anything up to 3000ms.

| Radius Server <192.1                     | 168.1.125>         |    |              |
|------------------------------------------|--------------------|----|--------------|
| General Status                           |                    |    | ОК           |
| - Service                                |                    |    | Cancel       |
| <ul> <li>ppp</li> <li>hotspot</li> </ul> | i login i wireless |    | Apply        |
| dhcp                                     |                    |    | Disable      |
| Called ID:                               |                    | -  | Comment      |
| Domain:                                  |                    | •  | Сору         |
| Address:                                 | 192.168.1.125      |    | Remove       |
| Secret:                                  | secret             |    | Reset Status |
| Authentication Port:                     | 1812               |    |              |
| Accounting Port:                         | 1813               |    |              |
| Timeout:                                 | 300                | ms |              |
|                                          | Accounting Backup  |    |              |
| Realm:                                   |                    | •  |              |
| Src. Address:                            | 0.0.0.0            | •  |              |
|                                          |                    |    |              |
| enabled                                  |                    |    |              |

Fig. 4.1.2. RADIUS server details

4. Click "OK" button to submit new entry

NOTE: If a RADIUS server that is not hosted on SIMPLer server (i.e. local RADIUS server) is used it is required to add second RADIUS server entry to the radius servers table on Mikrotik that will point at the SIMPLer server IP address. It should have all services disabled and the secret field should match the secret defined under the local RADIUS server defined in the previous step (Fig. 4.1.2). This is required for incoming CoA packets to be allowed and accepted. In example: 84.203.220.3 IP address (public IP of the wib.azotel.com server) has been used as an example on figure 4.1.3

| General Status       |                   |    | OK           |
|----------------------|-------------------|----|--------------|
| - Service            |                   |    | Cancel       |
| ppp<br>hotspot       | login<br>wireless |    | Apply        |
| dhcp                 |                   |    | Disable      |
| Called ID:           |                   | •  | Comment      |
| Domain:              |                   | -  | Сору         |
| Address:             | 84.203.220.3      |    | Remove       |
| Secret:              | *****             |    | Reset Status |
| Authentication Port: | 1812              |    |              |
| Accounting Port:     | 1813              |    |              |
| Timeout:             | 300               | ms |              |
|                      | Accounting Backup |    |              |
| Realm:               |                   | •  |              |
| Src. Address:        |                   | •  |              |

Fig. 4.1.3. additional RADIUS server details

Azotel Confidential Proprietary

© Azotel Technologies Ltd 2024

 Under Radius window click on "Incoming" button to bring up the "RADIUS Incoming" section (fig. 4.1.4). Tick "Accept" box and enter port number (example: 3799) that will match port number defined under SIMPLer RADIUS NAS table (fig. 3.1.2)

| Rad   |   |         |        |           |                                    |        |       |               |        |      |
|-------|---|---------|--------|-----------|------------------------------------|--------|-------|---------------|--------|------|
| ÷     |   |         | 7      | Rese      | t Status                           | Inco   | oming |               |        | Find |
| #     |   | Service |        | Called II | D                                  | Domain | 1     | Address       | Secret | •    |
| 0     |   | hotspot |        |           |                                    |        |       | 192.168.1.125 | secret |      |
|       |   |         | Radius | Incoming  | )                                  |        |       |               |        |      |
|       |   |         |        | Port:     | <ul><li>Acc</li><li>3799</li></ul> | ept    |       | OK<br>Cancel  |        |      |
|       |   |         | Re     | equests:  | 3                                  |        |       | Apply         |        |      |
|       |   |         | Bad Re | equests:  | 0                                  |        | Re    | set Status    |        |      |
|       |   |         |        | Acks:     | 3                                  |        |       |               |        |      |
|       |   |         |        | Naks:     | 0                                  |        |       |               |        |      |
|       |   | L       |        |           |                                    |        |       |               |        |      |
| 1 ite | m |         |        |           |                                    |        |       |               |        |      |

Fig. 4.1.4. RADIUS Incoming section

At this stage the Mikrotik is set to send the RADIUS requests to SIMPLer (to do the Authentication, Authorisation and Accounting) and receive the incoming CoA packet from the SIMPLer server (to reprovision a customer).

#### 4.2 Address List

Setup IP subnets on a given interfaces. In the example shown on fig. 4.2.1 *Public4* is an Internet interface and IP address *192.168.1.136* should be considered as public IP address of Mikrotik. *172.16.191.0/24* and *172.16.190.0/24* are subnets attached to the *Public2* interface – in this case Operator's Network Interface.

|   | Address List     |              |              |           |  |
|---|------------------|--------------|--------------|-----------|--|
|   | + - 🖉 🗶 🖆 🍸      |              |              |           |  |
|   | Address          | $\mathbb{Z}$ | Network      | Interface |  |
| I | 172.16.190.1/24  |              | 172.16.190.0 | Public2   |  |
| I | 172.16.191.1/24  |              | 172.16.191.0 | Public2   |  |
| ł | 192.168.1.136/24 |              | 192.168.1.0  | Public4   |  |

Fig. 4.2.1. Winbox: "Address List" window

#### 4.3 IP Pools

Define IP Pools. We will use group of addresses from the previously defined address list – see fig. 4.2.1 for reference. Name of given IP Pool is important as it must match Framed Pools defined on the RADIUS server. If we define Framed Pool on SIMPLer-RADIUS server (see fig. 3.2.4) then customer assigned to the defined Framed Pool will get an IP address from that pool. In the example shown on fig 4.2.2 "PublicPool" is name of the pool that will be used by authenticated customers. "disconnected" pool will match pool that will be defined in the backend configuration file on RADIUS server. All customers who are disconnected should get IP address from the "disconnected" pool.

| IP Pool              |                             |           |      |
|----------------------|-----------------------------|-----------|------|
| Pools Used Addresses |                             |           |      |
| + - 7                |                             |           | Find |
| Name 🗸               | Addresses                   | Next Pool | -    |
| 🕆 Public Pool        | 172.16.191.2-172.16.191.250 | none      |      |
| 🕆 disconnected       | 172.16.190.2-172.16.190.254 | none      |      |
|                      |                             |           |      |
|                      |                             |           |      |
| 2 items              |                             |           |      |

Fig. 4.2.2. Winbox: "IP Pool" window

#### 4.4 PPPoE Setup

1. On "*PPP*" window open "Secrets tab" and click "*PPP Authentication & Accounting*" button. On the window that shows up check the boxes "Use Radius" and "Accounting" and set "Interim Update" to 5 minutes (fig. 4.4.1).

| PPP                                     |                                                |
|-----------------------------------------|------------------------------------------------|
| Interface PPPoE Servers Secrets Profile | Active Connections                             |
| 🕂 — 🖉 💥 🖽 🧃 🗗 PPP A                     | Authentication & Accounting                    |
| Name A Password Service                 | Caller ID Profile Local Address Remote Address |
|                                         |                                                |
|                                         |                                                |
|                                         | PPP Authentication & Accounting                |
|                                         | Use Radius OK                                  |
|                                         | Accounting Cancel                              |
|                                         | Interim Update: 00:05:00                       |
|                                         |                                                |
|                                         |                                                |
|                                         |                                                |

Fig. 4.4.1. Winbox: "PPP Authentication & Accounting" window

- 2. On "PPP" window open "Profiles" tab and add new profile. On "General" tab enter the following (fig. 4.4.2):
  - *a.* Name: *(example) PPPoE-profile*

b. Local Address: (example) 172.16.191.1

| PPP Profile <pppoe-profile></pppoe-profile> |         |
|---------------------------------------------|---------|
| General Protocols Limits                    | OK      |
| Name: PPPoE-profile                         | Cancel  |
| Local Address: 172.16.191.1 🔻 🔺             | Apply   |
| Remote Address:                             | Comment |
| Bridge:                                     | Сору    |
|                                             | Remove  |
|                                             |         |
| Outgoing Filter:                            |         |
| Address List:                               |         |
| DNS Server:                                 |         |
| WINS Server:                                |         |
| - Change TCP MSS                            |         |
|                                             |         |
| ,                                           |         |
|                                             |         |
|                                             |         |
|                                             |         |
|                                             |         |

Fig. 4.4.2. Winbox: "Profiles" tab -> "Add PPP Profile" window -> "General" tab

- 3. On "PPP" window open "PPPoE Servers" tab and add new PPPoE service with following details (fig. 4.4.4)
  - a) Service Name: (example) PPPoE
  - b) Interface: (example) Public2 interface which PPPoE service will run on
  - c) Max MTU: 1480 by default
  - d) Max MRU: 1480 by default
  - e) Keepalive Timout: 10 by default
  - f) Default Profile: *(example) PPPoE-profile* previously created profile (see fig. 4.4.2. and 4.4.3)
  - g) Authentication: chap

| PPPoE Service <ppi< th=""><th>PoE&gt;</th><th></th></ppi<> | PoE>                 |         |
|------------------------------------------------------------|----------------------|---------|
| Service Name:                                              | PPPoE                | OK      |
| Interface:                                                 | Public2              | Cancel  |
| Max MTU:                                                   | 1480                 | Apply   |
| Max MRU:                                                   | 1480                 | Disable |
| MRRU:                                                      | •                    | Сору    |
| Keepalive Timeout:                                         | 10                   | Remove  |
| Default Profile:                                           | PPPoE-profile ₹      |         |
|                                                            | One Session Per Host |         |
| Max Sessions:                                              | ▼                    |         |
| - Authentication                                           |                      |         |
| 🗌 pap                                                      | ✓ chap               |         |
| mschap 1                                                   | mschap2              |         |
| enabled                                                    |                      |         |

Fig. 4.4.4. Winbox: "PPPoE Service" tab -> "Add PPPoE Service" window

#### 4.5 Web Proxy Setup

Traffic for disconnected users will be redirected to the web proxy on Mikrotik device. Enable web proxy on port 8080 and under Access Tab define 3 entries (fig. 4.5.1):

- allow destination address (example) 192.168.1.125 which is IP address of SIMPLer server
- allow destination host (example) demo.azotel.com which is domain name of SIMPLer server
- deny any other traffic and redirect to (example) demo.azotel.com/redirect/<operator instance>/

| Web Praxy Settings                |                    |                    |      |        |        |                                 |      |    |
|-----------------------------------|--------------------|--------------------|------|--------|--------|---------------------------------|------|----|
| General Status Lookups Inserts Re | freshes            | ОК                 |      |        |        |                                 |      |    |
| Enabled                           |                    | Cancel             |      |        |        |                                 |      |    |
| Src. Address:                     | •                  | Apply              |      |        |        |                                 |      |    |
| Port: 8080                        | ÷                  | Clear Cache        |      |        |        |                                 |      |    |
| Parent Proxy:                     |                    | Root UTM           |      |        |        |                                 |      |    |
| Parent Proxy Port:                |                    | Access             | >    |        |        |                                 |      |    |
| Cache Administrator: webmaster    | ^                  | Cache              |      |        |        |                                 |      |    |
| Web Proxy Access                  | ( <u>-</u> )       | Direct             |      |        |        |                                 |      |    |
| +- / = 6 7 =:                     | Reset Counters 🛛 😂 | Reset All Counters |      |        |        |                                 | Find | d  |
| # Src. Address Dst. Address       | ss Dst. Port       | Dst. Host          | Path | Method | Action | Redirect To                     | Hits | -  |
| 0 • 192.168.1.                    | 125                |                    |      |        | allow  |                                 |      | 0  |
| 2 0                               |                    | demo.azotel.com    |      |        | denv   | demo azotel com/redirect/w3pet/ |      | -0 |
|                                   |                    |                    |      |        | derly  | demo.deorer.com/16dil6c//w316t/ |      | •  |

Fig. 4.5.1. Winbox: "Web Proxy Settings" & "Web Proxy Access"

#### 4.6 Firewall Setup

1. On "*IP*" -> "*Firewall*" window go to the "*Address Lists*" tab and enter any addresses that should be inspected by firewall. In our case it will be pool 172.16.190.0/24 of disconnected customers (fig. 4.6.1).

| Azotel Confidential Proprietary |
|---------------------------------|
| © Azotel Technologies Ltd 2024  |

| Firewall                         |                             |                                                            |                                                                   |                                               |
|----------------------------------|-----------------------------|------------------------------------------------------------|-------------------------------------------------------------------|-----------------------------------------------|
| Filter Rules NAT Mangle          | Service Ports               | Connections                                                | Address Lists                                                     | Layer7 Protocols                              |
| + - × × 🗅                        | T                           |                                                            |                                                                   |                                               |
| Name /                           | Address                     |                                                            |                                                                   |                                               |
| <ul> <li>disconnected</li> </ul> | 172.16.190.0/               | /24                                                        |                                                                   |                                               |
| 1 item (1 colorited)             | Firewall<br>Name<br>Address | Address List <o<br>e: Hisconnecte<br/>s: 172.16.190</o<br> | disconnected><br>d ∓<br>.0/24 Ca<br>Di<br>Con<br>Con<br>Con<br>Re | OK<br>ancel<br>pply<br>sable<br>mment<br>Copy |
|                                  | enabled                     |                                                            |                                                                   |                                               |

Fig. 4.6.1. Winbox: "IP" -> "Firewall" – "Address Lists" tab

2. On "*IP*" -> "*Firewall*" window go to the "*NAT*" window and make sure that *srcnat* entry exists on correct public interface. Also add *dstnat* entry to redirect any customer traffic to the local web proxy on port 8080. (fig. 4.6.2).

NOTE: HTTPS protocol cannot be proxied thus any HTTPS traffic should not be redirected to port 8080. It will be blocked by firewall filter.

| NAT Rule 443                             |
|------------------------------------------|
| General Advanced Extra Action Statistics |
| Chain: dstnat                            |
| Src. Address:                            |
| Dst. Address:                            |
| Protocol: 6 (tcp)                        |
| Src. Port:                               |
| Dst. Port: 1 443                         |
| Any. Port:                               |
| NAT Rule 443                             |
| General Advanced Extra Action Statistics |
| Src. Address List: 🗌 disconnected 🛛 🔻 🔺  |
| Dst. Address List:                       |
|                                          |
| NAT Rule 443                             |
| General Advanced Extra Action Statistics |
| Action: redirect                         |
| To Ports: 8080                           |
|                                          |

Fig. 4.6.2. Winbox: "IP" -> "Firewall" -- "NAT" tab

- 3. On *"IP" -> "Firewall"* window go to the *"Filter Rules"* tab and define 3 entries for disconnected address list (fig. 4.6.3):
  - a. accept forward rule to SIMPLer server address *(example)* 192.168.1.125 to allow any HTTPS traffic to the SIMPLer server which hosts End User Portal and redirection page
  - b. accept forward rule to any DNS servers if required
  - c. drop forward rule for any other type of traffic

| Firewall     |                                        |               |                  |               |                 |           |           |          |          |         |   |
|--------------|----------------------------------------|---------------|------------------|---------------|-----------------|-----------|-----------|----------|----------|---------|---|
| Filter Rules | NAT Mangle Service Ports Connections # | Address Lists | Layer7 Protocols | 3             |                 |           |           |          |          |         |   |
| + - [        | 🖉 🖾 🍸 🔚 Reset Counters 🕻               | DO Reset AI ( | Counters         |               |                 |           |           |          |          |         |   |
| #            | Action                                 | Chain         | Src. Address     | Dst. Address  | Proto Src. Port | Dst. Port | In. Inter | Out. Int | Bytes    | Packets |   |
| ;;; default  | configuration                          |               |                  |               |                 |           |           |          |          |         |   |
| 0            | accept                                 | input         |                  |               | 1 (c            |           |           |          | 13.5 KB  | 172     |   |
| default      | configuration                          |               |                  |               |                 |           |           |          |          |         |   |
| 1            | accept                                 | input         |                  |               |                 |           |           |          | 21.1 MB  | 184 403 |   |
| ;;; default  | configuration                          |               |                  |               |                 |           |           |          |          |         |   |
| 2            | accept                                 | input         |                  |               |                 |           |           |          | 0 B      | 0       |   |
| ::: default  | configuration                          |               |                  |               |                 |           |           |          |          |         |   |
|              |                                        |               | -                |               | _               | -         | 0.00.1    | _        |          | 0       | _ |
| 4            | accept                                 | forward       |                  | 192.168.1.125 |                 |           |           |          | 22.2 KIB | 178     |   |
| 5            | ✓ accept                               | forward       |                  | 8.8.8.8       |                 |           |           |          | 532.1 KB | 8 651   |   |
| 6            | × drop                                 | forward       |                  |               |                 |           |           |          | 31.3 KB  | 469     |   |
|              |                                        |               |                  |               |                 |           |           |          |          |         |   |

Fig. 4.6.3. Winbox: "IP" -> "Firewall" – "Filter Rules" tab

21

### 4.7 Redirection Page

The last step is to create redirection page file index.html and send it to <u>support@azotel.com</u> to upload it to the web server. index.html should contain link to EUP where disconnected customer can pay their outstanding bills or buy additional bandwidth. Link to EUP is https://<server\_name>/CustomerPortal/login.pl?operator=<operator\_instance> or <u>https://<server\_name>/CP/login.pl?operator=<operator\_instance></u>. Annex C contains typical index.html file.

# 5 Debugging

This section of the guide should help with resolving typical issues operator can run on with the running PPPoE on a Mikrotik integrated with SIMPLer system. This part of a manual is meant to be kept up-to-date with resolutions of support cases Azotel finds generic and useful for other operators.

#### 5.1 Expected throughputs are not achieved

When a customer connects and has a MikroTik Rate Limit RADIUS attribute, the MikroTik creates a simple queue for the customer to limit their bandwidth. By default a queue type of "default-small" is used, and this queue type is defined in Queues -> Queue Types to be of type "pfifo" and size 10:

| Que |             |                                                                                      |            |            |     |           |   |
|-----|-------------|--------------------------------------------------------------------------------------|------------|------------|-----|-----------|---|
| Sir | mple Queues | Interface                                                                            | e Queues   | Queue Tree | Que | eue Types |   |
| ÷   | - 7         |                                                                                      |            |            |     |           |   |
|     | Type Name   | •                                                                                    | A          | Kind       |     |           |   |
| •   | default     |                                                                                      |            | pfifo      |     |           |   |
| •   | default-sma | dl -                                                                                 |            | pfifo      |     |           |   |
| +   | 11 1        | C 10                                                                                 |            | 107        |     |           | _ |
| -   | Queue Type  | <default-< th=""><th>small&gt;</th><th></th><th></th><th></th><th>×</th></default-<> | small>     |            |     |           | × |
| •   | -           |                                                                                      |            |            |     |           | 7 |
| •   | lyp         | e Name:                                                                              | default-sn | nall       |     | ОК        |   |
| •   |             | Kind:                                                                                | ofifo      | :          | Ŧ   | Cancel    | ٦ |
| •   |             |                                                                                      |            |            |     | Cancer    |   |
| •   | 0           | ~                                                                                    | 10         |            |     | Apply     |   |
| •   | Que         | eue Size:                                                                            | 10         | packe      | ts  |           |   |
|     |             |                                                                                      |            |            |     |           |   |

Fig. 5.5.1. Default Queue Types

Unfortunately this type of queue can cause problems with certain types of radio networks - e.g. WiMax, where the packet scheduler on the AP can delay the delivery of packets. Symptoms of this happening are that throughput is limited to about 1.5Mb/s. If this appears to be happening, then the queue type should be changed.

Unfortunately it is not possible to configure the MikroTik to use a different queue-type – it always defaults to "default-small" for RADIUS authenticated customers. Therefore it is necessary to re-define "default-small" to use one of the other queue types. This can be done on the Queue Type tab as in Fig 6.5.1 above. It may be necessary to try different queue types to find the one which works best. For a Purewave WiMax AP changing the Queue Size to 50 worked well, as did changing the Queue Kind to "sfq" with default parameters of perturb=5, allot=1514.

## 6 IPv6 Notes

In the case of IPv6 usage there are two suggested ways of getting IPv6 prefixes out to the customers:

- Dynamic IPv6 prefix from IP pool
- Static IPv6 prefix from RADIUS / SIMPLer

This is very similar to the way IPv4 addresses are being given out. From the RADIUS perspective the difference is in the attributes being used. The attribute for IP pool is called: Framed-IPv6-Pool (instead of Framed-Pool) and the attribute for the static IP prefix is called: Framed-IPv6-Prefix (instead of Framed-IP-Address)

NOTE: If the PPPoE client works in the dual stack mode (ie. they request both IPv4/IPv6 addresses) it is important to define "Local Address" under the PPPoE profile and make sure that client gets IPv4 address as well (either from regular Framed-Pool or as a Framed-IP-Address). If the client requests IPv6 only then "Local Address" is not required (see fig. 6.0.1)

| PPP Profile <ipv6profile></ipv6profile> |                                |         |
|-----------------------------------------|--------------------------------|---------|
| General Protocols Lin                   | nits                           | ОК      |
| Name:                                   | ipv6profile                    | Cancel  |
| Local Address:                          | ★                              | Apply   |
| Remote Address:                         | ▼                              | Comment |
| Remote IPv6 Prefix Pool:                | ▼                              | Сору    |
| DHCPv6 PD Pool:                         | ▼                              | Remove  |
| Bridge:                                 | ▼                              |         |
|                                         |                                |         |
| PPP Profile <ipv6profile></ipv6profile> |                                |         |
| General Protocols Lin                   | nits                           | OK      |
| - Use IPv6                              |                                | Cancel  |
| - Use MPLS                              | O no 🗢 <u>yes</u> : O required | Apply   |
| <ul> <li>default</li> </ul>             | C no C yes C required          | Comment |
| - Use Compression                       | C C                            | Сору    |
| ve uerault                              | C no C yes                     | Demous  |

Fig. 6.0.1. PPP profile for IPv6 addresses

#### 6.1 Getting dynamic IPv6 prefix from IP pool

In order to get an IPv6 prefix from the IP pool that pool must be defined. It can be done from IPv6 -> Pool section:

| IPv6    | $\triangleright$ | Addresses   |
|---------|------------------|-------------|
| MPLS    | $\square$        | DHCP Client |
| Routing | $\square$        | DHCP Server |
| System  | $\square$        | Firewall    |
| Queues  |                  | ND          |
| Files   |                  | Neighbors   |
| Log     |                  | Pool        |
| Radius  |                  | Routes      |

| IPv6 Pool           |                 |                 |              |
|---------------------|-----------------|-----------------|--------------|
| Pools Used Prefixes |                 |                 |              |
| + - 7               |                 |                 | Find         |
| Name 🛆 Pref         | xí              | Prefix Length E | xpire Time 🔻 |
| ipv6pool 200        | 1:470:62fa::/48 | 64              |              |
|                     |                 |                 |              |
|                     | IPv6 D          | Addresses       |              |
|                     | MPLS D          | DHCP Client     |              |
|                     | Routing D       | DHCP Server     |              |
|                     | System D        | Firewall        |              |
|                     | Queues          | ND              |              |
|                     | Files           | Neighbors       |              |
|                     | Log             | Pool            |              |
|                     | Radius          | Routes          |              |

Fig. 6.1.1 IPv6 -> Pool

If the attribute "Framed-IPv6-Pool" = "ipv6pool" is defined on the RADIUS server and belongs to the RADIUS group that the customer username is assigned to, then upon PPPoE session establishment the customer will get an IPv6 prefix from the "ipv6pool"

#### 6.2 Getting a static IPv6 prefix from RADIUS / SIMPLer

If the attribute "Framed-IPv6-Prefix" is defined on the RADIUS server and its value is a correct IPv6 prefix and it is defined as Individual RADIUS reply that is assigned to a customer username, then upon PPPoE session establishment the customer will get that IPv6 prefix.

Note that defining an IPv6 Prefix under the customer IP table and assigning it to the RADIUS username will take an exactly the same effect.

Note that in case the customer is assigned both to the pool and prefix attributes, prefix takes precedence.

25

# Annex A: References

#### A.1 Document References

10017 SIMPLer RADIUS Server Integration

#### A.2 Link References

http://www.azotel.com - Azotel Website

http://wiki.mikrotik.com/wiki/Main\_Page - Mikrotik WIKI

http://forum.ubnt.com/ - Ubiquity Forum

# Annex B: Definitions & Abbreviations

# B.1 Definitions

#### **B.2** Abbreviations

SIMPLer Subscriber Information Management Platform from Azotel

- NAS Network Access Server
- EUP End User Portal
- AP Access Point
- CPE Customer Premises Equipment

RADIUS Remote Authentication Dial In User Service

# Annex C: Typical index.html file

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd"> <html><head> <meta http-eguiv="Content-Type" content="text/html; charset=iso-8859-1"><title>Azotel</title> k href="http://wib.azotel.com/PortalImages/styles.css" rel="stylesheet" type="text/css"> <style media="all" type="text/css">@import "http://wib.azotel.com/PortalImages/menu/menu\_style.css";</style> <!--[if lt IE 7]> <style type="text/css"> <!body { background-color: #F3F3F3; margin-top: 18px; \_ \ </style></head><body> style="padding-right: 50px;" align="left" valign="bottom"> <div align="right">
<a href="http://wib.azotel.com/CP/login.pl?operator=template" class="top\_but">Login</a> </div> 

 style="border: 1px solid rgb(153, 153, 153);" align="left" bgcolor="#ffffff" height="326" valign="top"> style="padding-top: 28px; padding-left: 78px;" align="left" valign="top" width="498"> Operator Name <div class="payment\_info" align="left">Customer Portal </div> style="padding-top: 45px; padding-bottom: 29px; padding-right: src="/PortalImages/logo.gif"></div> 78px;" width="279"><div align="right"><img <di style="padding-top: 0px; padding-bottom: 30px;">
<div align="center"> <dt valign=top><img src="inc/spacer.gif" width=15 height=1 border=0 alt=''><br><img src="inc/spacer.gif" width=1 height=37 border=0
alt=''><br>&nbsp;<br> 24px; color: red;">Your Internet Access Is Temporarily Unavailable!</span></center> <center> <br> <h2>Your IP: \$(ip)</h2> <h2>Your MAC: \$(mac)</h2> </center> <h2>You are seeing this message for one of the following reasons:</h2> style="font-size:15px">You are not an authorized customer of Operator Name. style="font-size:15px">Your Computer and/or Router is not configured properly.style="font-size:15px">Your Computer and/or Router is not configured properly.style="font-size:15px">A virus has become delinquent.</or> <br> <h2>In order to clear this message you will need to either:</h2> <111> <ur>style="font-size:15px">Reboot your Computer and/or Router.style="font-size:15px">Run a virus scanning/removal tool. <!--<li style="font-size:15px">Call Customer Support at PHONENUMBER. style="font-weight: font-size: 16px; font-style: italic;">You may also pay your bill online by <a <span bold; href="https://wib.azotel.com/CP/login.pl? operator=template/">Clicking Here</a>.</span> <br><br>> </div>  $</t_r>$ cscript type="text/javascript"><!--google\_ad\_client = "pub-5535280914415875"; google\_ad\_width = 120; google\_ad\_height = 240; google\_ad\_format = "120x240\_as\_rimg"; google\_cpa\_choice = "CAAQhfCXhAIaCJM442ipyzWdKFG193M"; google\_ad\_channel = "9130903211";//--></script> 

<img src="inc/spacer.gif" width=30 height=1 border=0 alt=''><br><img src="inc/spacer.gif" width=1 height=37 border=0
alt=''><br><indsp;<br><//div>
<//div> 

</body></html>

|                                                                                                                                                 | Login                                                                                                       |  |  |  |
|-------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|--|--|--|
| Operator Name                                                                                                                                   |                                                                                                             |  |  |  |
| Customer Portal                                                                                                                                 |                                                                                                             |  |  |  |
| Your Internet Access Is Temporarily Unavailable!                                                                                                |                                                                                                             |  |  |  |
|                                                                                                                                                 | Your IP: \$(ip)                                                                                             |  |  |  |
|                                                                                                                                                 | Your MAC: \$(mac)                                                                                           |  |  |  |
| You are seeing this me                                                                                                                          | ssage for one of the following reasons:                                                                     |  |  |  |
| <ul> <li>You are not an authorize</li> <li>Your Computer and/or R</li> <li>Your account has becon</li> <li>A virus has been detected</li> </ul> | ed customer of Operator Name.<br>Louter is not configured properly.<br>ne delinquent.<br>ed on your system. |  |  |  |
| In order to clear this m                                                                                                                        | essage you will need to either:                                                                             |  |  |  |
| <ul> <li>Reboot your Computer a</li> <li>Run a virus scanning/rel</li> </ul>                                                                    | and/or Router.<br>moval tool.                                                                               |  |  |  |
| You may also pay your bil                                                                                                                       | Il online by <u>Clicking Here</u> .                                                                         |  |  |  |
| ght ©2013 Operator Name, All rights reserved                                                                                                    | Powered by AZOTE                                                                                            |  |  |  |

Fig. A.C.1. "You are not authenticated" page

# Annex D: Change history

| Change history |           |                                                                                                                                                    |     |     |  |  |
|----------------|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----|-----|--|--|
| Date           | Author(s) | Subject/Comment                                                                                                                                    | Old | New |  |  |
| 10-01-13       | Pawel     | Initial Draft                                                                                                                                      | n/a | 001 |  |  |
| 26-03-13       | Pawel     | Put the initial draft into the Azotel template format, reviewed the text, added common introduction, expanded descriptions, added network drawings | 001 | 002 |  |  |
| 04-04-13       | Stephen   | Added MikroTik Queue info                                                                                                                          | 002 | 003 |  |  |
| 17-06-13       | paul      | Changed doc's title, copyright and correct year, doc num on all pages                                                                              | 003 | 100 |  |  |
| 15-01-15       | Stephen   | Corrected MikroTik-Rate-Limit information                                                                                                          | 100 | 101 |  |  |
| 15-04-16       | Pawel     | Added IPv6 Notes                                                                                                                                   | 101 | 102 |  |  |
| 15-04-16       | emma      | Reviewed Section 6                                                                                                                                 | 102 | 103 |  |  |
| 23-12-16       | pawel     | Remove session limit                                                                                                                               | 103 | 104 |  |  |