The Use of Mikrotik Router Boards With Radius Server for ISPs.

By Zaza Zviadadze, Irakli Nozadze.

Intellcom Group, Georgia.

RouterOS features for ISP's

RouterOS reach features gives possibilities to ISP's, for managing

Their users, including:

- User authorization
- Traffic shaping
- Internet access restriction

RouterOS as radius client

Configuring multiple RouterOS based devices as
radius clients and setting up radius server, gives
possibility to ISP's for centralizing user
management.

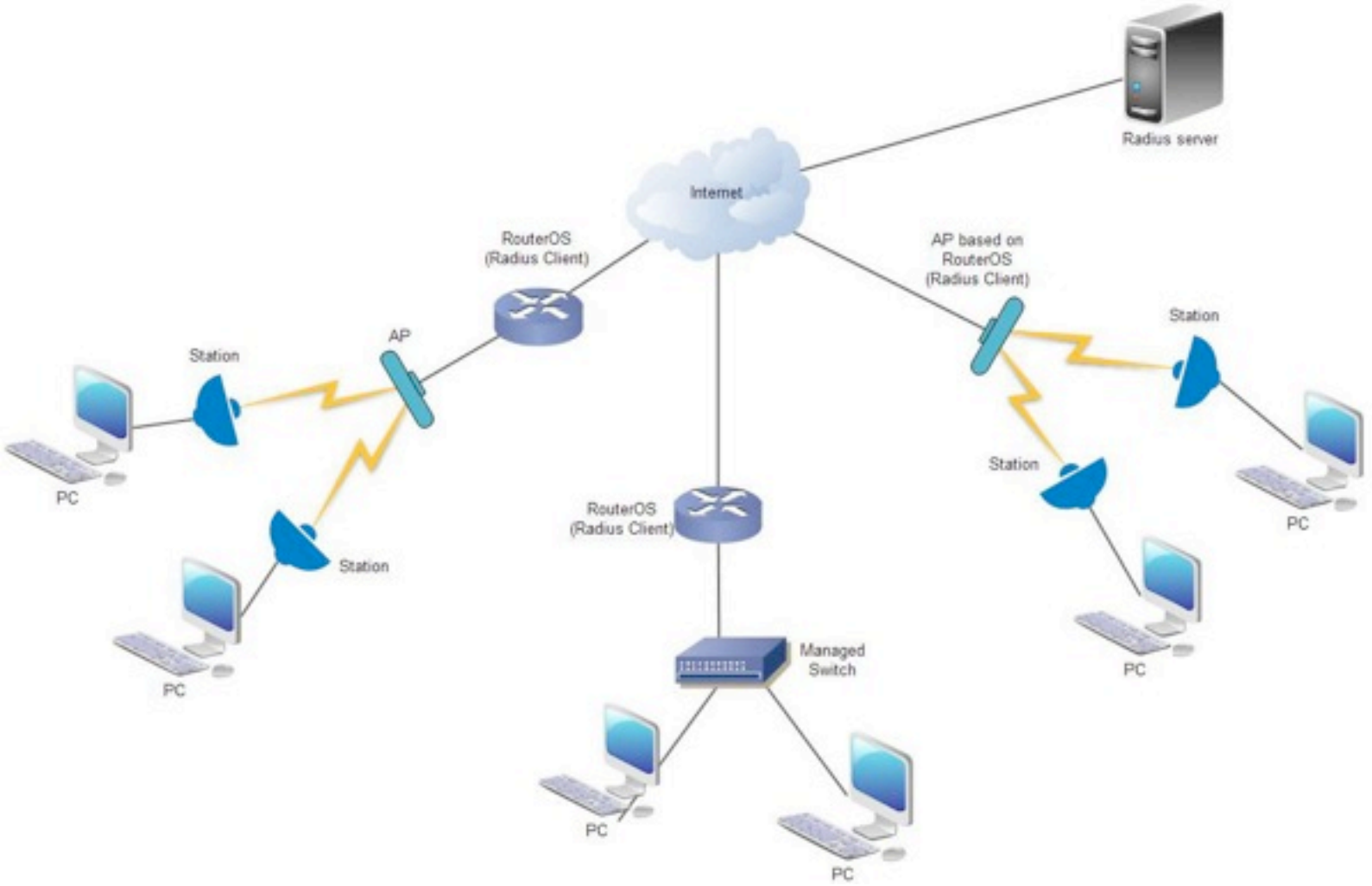
Network components

The network consists of at least three basic components:

1. Remote Stations (WiFi Stations, PC's, SoHo routers, etc)
2. RouterOS's
3. Radius Server

Remote stations connect to the RouterOS via LAN or WLAN, and

Network Diagram



1. Remote Stations should be configured as DHCP clients.

2. RouterOS's should be configured as DHCP servers and as Radius clients.

3. Radius Server stores Remote Stations data (IP Addresses, MAC Addresses, Rate Limits, etc.) in their database.

Remote Stations as DHCP

Station/PC is configured as DHCP client. After DHCP client is powered on, it's

requesting following parameters from DHCP Server:

- IP Address
- Default Gateway
- Subnet Mask
- DNS

RouterOS as DHCP server and as Radius client

RouterOS is configured as DHCP Server + Radius Client.

After getting DHCP request from user, RouterOS sends MAC

address as username to Radius Server.

First, Radius server checks whether user exists, in their database.

If user exists, Radius server sends “Access-Accept”

Radius Server

Remote Authentication Dial In User Service (**RADIUS**) is a networking
protocol that provides centralized Authentication, Authorization and
Accounting (AAA) management for computers to connect and use a
network service.

RADIUS is a client/server protocol that runs in the application layer,
using UDP as transport

RADIUS protocol often used by ISPs and enterprises to

Radius Server Data

Radius server has abilities to store and retrieve data

from SQL databases. In our case radius server is

used to retrieve following data:

1) Framed-IP-Address.

2) MT-Rate-Limit.

Framed-IP-Address

Framed-IP-Address is user IP address.

In our case they statically are assigned to remote station's MAC Addresses.

This data is stored in Radius Server Database.

MT-Rate-Limit

MT-Rate-Limit defines RX/TX bit rate limits for
remote stations, including:

- Max Limit
- Burst Limit
- Burst Threshold
- Burst Time
- Priority
- Min Limit

MT-Address-List

- MT-Address-List is string used for identifying user groups. In our case, “nopayment “ used to identify suspended users.
- After service period expiration, a application changes user status, assigns address-list “nopayment” and stores this data in Radius Server Database.
- When Remote Station sends DHCP request to DHCP server, address-list among other data are being retrieved from Radius Server.
- Then some rules configured in RouterOS are used to make appropriate action.

Session-Timeout

- Session-Timeout attribute sets the maximum number of seconds of service to be provided to the user before this session is expired.
- This attribute is configured at Radius Server, to be sent by the server to the client in an Access-Accept.
- Attribute configured in RouterOS, will be overridden by value sent from Radius Server.
- Changes made in user status (suspension/ unsuspension) or rate limits at Radius Server side, will be effective after current session expiration and new session establishment.

RouterOS Configuration Steps

- IP Addresses, Gateway, DNS
- Radius client
- DHCP server
- Interface
- Firewall
- Web proxy
- Additional configuration

IP Addresses, Gateway, DNS

- **Assigning IP addresses to the interfaces.**

/ip address
add address=192.168.1.1/24 Interface=ether1 comment="LAN"
add address=10.0.0.2/24 interface=ether2 comment="WAN"

- **Adding Default Gateway**

/ip route
add dst-address=0.0.0.0/0 gateway=10.0.0.1

- **Configuring DNS client.**

/ip dns
set servers=213.157.196.131, 213.157.196.132

Radius client

- **Configuring Radius client and adding DHCP service.**

/radius

add service=dhcp address=80.200.100.200

- **Adding backup radius servers is also possible.**

DHCP server

- **During DHCP server configuration we are selecting ether1 interface and enabling following options: add ARP for leases, use RADIUS.**

```
/ip dhcp-server
add add-arp=yes address-pool=static-only interface=ether1 use-
    radius=yes disabled=no
```

- **Adding network parameters for DHCP server.**

```
/ip dhcp-server network
add address=192.168.1.0/24  gateway=192.168.1.1
    comment="LAN"
```

Interface

After DHCP server setup we are configuring Ethernet interface (ether1) and

selecting option: arp=reply-only. So, only DHCP server will be able to add

Data to the ARP.

/interface ethernet

set arp=reply-only ether1

If user enters network configuration manually it will not work. This

provides additional security to the network.

Web-proxy

- **Next we are enabling Web-proxy server and setting port to 8080.**

/ip proxy

set enabled=yes port=8080

- **Now we are enabling some URLs in order to make certain web sites available for suspended users. For example, web site of ISP and/or online payments.**

/ip proxy access

add dst-host=isp.com action=allow

- **Finally we are restricting access to all other URLs and redirecting users to suspend page.**

add dst-host=* action=deny redirect-to="isp.com/suspend"

Firewall

- **Identification of suspended users is being performed via address-list. For example: address-list=nopayment.**

- **In the firewall -> nat a rule should be added which will redirect all http traffic of suspended users to Web proxy.**

```
/ip firewall nat
add chain=dstnat action=redirect to-ports=8080 protocol=tcp src-address-
    list=nopayment dst-port=80
```

- **Next, should be opened HTTP and DNS ports in Firewall - > Filter. Finally, access to all other protocols are to be restricted.**

```
/ip firewall filter
add chain=forward action=accept protocol=tcp dst-port=80
add chain=forward action=accept protocol=udp dst-port=53
add chain=forward action=reject reject-with=icmp-host-prohibited src-address-
    list=nopayment
```

Additional Configuration

RouterOS also acts as AP

For additional security, Radius MAC authentication in wireless security
policies should be enabled . In this case, AP accepts only the stations with
MAC addresses registered in Radius Server database.

/ interface wireless security-profiles
set [find default=yes] radius-mac-authentication=yes

/radius
Add address=80.200.100.200 service=wireless,dhcp

In addition it's also possible to use other security mechanisms

Additional Configuration

When AP is placed between RouterOS and Remote Stations, AP must be
configured in bridge Mode in order to make possible MAC authentication via
RouterOS.

For security purposes it's also preferable to use other wi-fi security
Mechanisms like WPA/WPA2 authentication , EAP TLS, etc.

Additional Configuration

When managed switch is placed between RouterOS and Remote

Stations (PC's), for security purposes port isolation should be

enabled in the switch configuration.

Otherwise users can discover and connect to each other, which may

cause serious security issue.

Address List (additional usage)

Optionally, Address-List can be used to apply additional policies for different

user groups. For example, for the following tasks:

- Bandwidth limitations for Local and global traffic
- Bandwidth limitations based on certain time periods
- Traffic prioritization
- Access restriction by protocols

Securing Radius Server

To secure connections betweens Radius Server and Radius Clients, it is possible to use the following mechanisms:

- VPN Tunnels between Server and Clients.
- Firewall configuration on Radius Server side, to allow connections only from certain IP addresses.
- Use Secret to authorize radius requests from Clients.

Integration with billing system

Using RouterOS based devices as Radius clients and Radius Server with

custom applications gives possibilities to fully Centralize and Automate

all processes :

- Suspension / unsuspension of users
- Integration with payment gateways
- SMS notifications
- Sending Invoices via email
- Integration with Web Services
- etc.

Thank you!