STUDY MIKROTIK ROUTER AND HOTSPOT GATEWAY BUILDING SYSTEM FOR AUTHENTICATION OF SERVICES INTERNET-WIFI LAN

TÌM HIỂU MIKROTIK ROUTER VÀ XÂY DỰNG DEMO HỆ THỐNG HOTSPOT GATEWAY CHO DỊCH VỤ INTERNET LAN-WIFI CÓ CHỨNG THỰC

Thạc sĩ. Nguyễn Hữu Trung
Khoa CNTT - Trường Đại Học Sư Phạm Kỹ Thuật TP.HCM

ABSTRACTS

Topics presented an overview of the Wireless LAN technology, the RADIUS authentication protocol.

Topics presented concepts, architectures, features, applications, and how to build Wi-Fi hotspot authentication system using MikroTik Router gateway.

The topic has successfully built 01 wireless authentication system allows the user to have access to the internet to run programs and access to information

TÓM TẮT

Đề tài trình bày các khái quát về công nghệ Wireless LAN, Giao thức chứng thực RADIUS.

Đề tài trình bày khái niệm, kiến trúc, đặc điểm, ứng dụng và cách thức xây dựng hệ thống chứng thực Wifi hotspot gateway sử dụng Mikrotik Router .

Đề tài đã xây dựng thành công 01 hệ thống Wifi chứng thực cho phép user có thể truy cập internet để chạy chương trình và truy cập thông tin.

NỘI DUNG

I. Wireless LAN

Wireless LAN (*WLAN)* là một loại mạng máy tính mà việc kết nối giữa các thành phần trong mạng không sử dụng các loại cáp như một mạng thông thường, môi trường truyền thông của các thành phần trong mạng là không khí và các thành phần trong mạng sử dụng sóng điện từ để truyền thông với nhau.

1. Ưu - nhược điểm của mạng Wireless LAN

Ưu điểm	**Nhược điểm**
• *Sự tiện lợi* • *Khả năng di động* • *Hiệu quả* • *Triển khai* • *Khả năng mở rộng*	• *Bảo mật* • *Phạm vi* • *Độ tin cậy* • *Tốc độ*

2. Các chuẩn phổ biến của WLAN

Tên chuẩn	Ý nghĩa
Chuẩn 802.11b	Ra đời năm 1999, hoạt động ở dải tần 2.4GHz, tốc độ truyền dữ liệu tối đa là 11 Mbps
Chuẩn 802.11a	Dùng kĩ thuật điều chế OFDM *(Orthogonal frequency-division multiplexing)*, Tốc độ truyền dữ liệu từ 20 Mbps đến 54 Mbps, Hoạt động ở băng tần 5Ghz
Chuẩn 802.11g	Hoạt động ở dải tần 2.4GHz, Tốc độ truyền dữ liệu tối đa có thể lên tới 54Mbps, Tương thích hoàn toàn với chuẩn 802.11b và 802.11g
Chuẩn 802.11n	Hỗ trợ tốc độ dữ liệu từ 54 đến 600 Mbps, Hoạt động trên cả hai băng tần 2.4GHz lẫn 5GHz, tương thích với các thiết bị 802.11g
Chuẩn 802.11ac	Tốc độ tối đa hiện là 1730Mbps, chỉ chạy ở băng tần 5GHz, *Băng thông kênh truyền rộng hơn, Nhiều luồng dữ liệu hơn, Hỗ trợ Multi user-MIMO, Tầm phủ sóng rộng hơn*

II. Giao thức RADIUS

RADIUS (Remote Authentication Dial In User Service) là một giao thức có khả ngăn cung cấp xác thực tập trung, cấp phép và kiểm toán (Authentication, Authorization và Accounting-AAA)

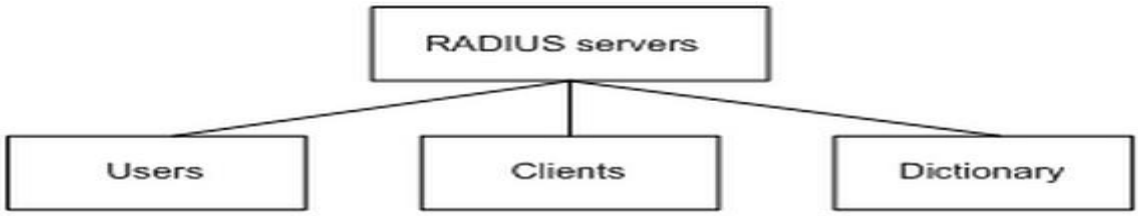
1. Hoạt động

RADIUS hoạt động theo mô hình client/ server.

- *Client:* được chạy trên NAS (network access server) nằm trên toàn mạng. Nó chuyển các thông tin người dùng lên server bằng các phương thức được định nghĩa sẵn.

- *Server:* chạy trên máy tính hoặc máy trạm tại trung tâm mạng và duy trì các thông tin liên quan đến việc xác thực người dùng và các dịch vụ truy cập mạng. Nó xác thực một người dùng sau khi nhận được một yêu cầu kết nối và xử lý sau đó trả về

kết quả (ví dụ như từ chối truy cập, chấp nhận yêu cầu của người dùng) cho client. Nói chung RADIUS server duy trì ba cơ sở dữ liệu gồm người dùng (Users), khách (Clients), từ điển (Dictionary) như hình bên dưới.

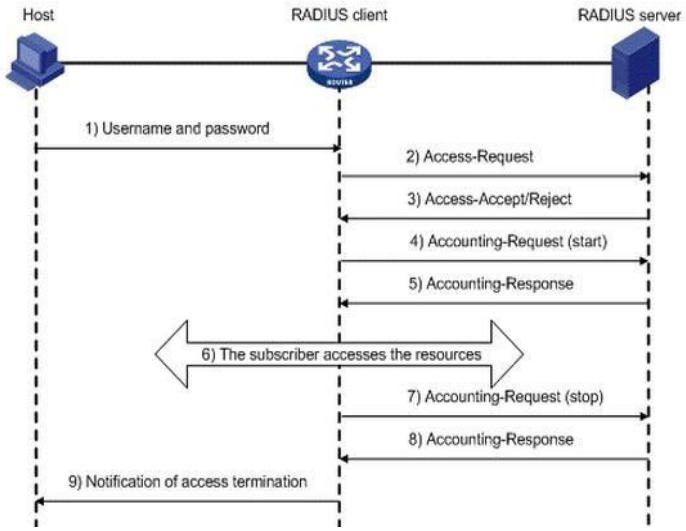


Hình 2-4: Radius server hoạt động theo mô hình Client/server

- *Users*: lưu trữ thông tin về người dùng như tài khoản, mật khẩu, các giao thức ứng dụng và địa chỉ IP.
- *Clients*:lưu trữ các thông tin về RADIUS client như khóa chia sẻ, địa chỉ IP.
- *Dictionary*: lưu trữ các thông tin mô tả các thuộc tính và giá trị của giao thức RADIUS.

2. ***Cách radius hoạt động:*** Hình bên dưới thể hiện sự tương tác giữa host, client và radius server.

   - *Bước 1:* Các host khởi tạo và gửi các yêu cầu kết nối đến radius client (chứa tài khoản và mật khẩu người dùng).
   - *Bước 2:* Sau khi nhận được tên người dùng và mật khẩu, RADIUS client sẽ gửi một yêu cầu chứng thực (Access-Request) đến máy chủ RADIUS, mật khẩu người dùng được mã hóa bởi các Message-Digest 5 (MD5) thuật toán với khóa chia sẻ trước khi được gửi đi.

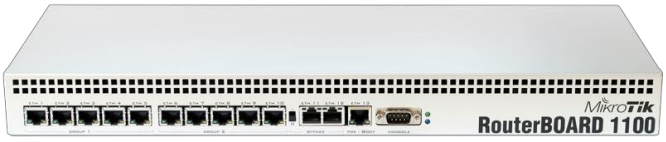


   - *Bước 3:* Các máy chủ RADIUS xác nhận tên người dùng và mật khẩu. Nếu xác thực thành công, nó sẽ gửi lại một thông báo Access-Accept có chứa các thông tin về quyền của người sử dụng. Nếu xác thực thất bại, nó sẽ trả về một thông báo Access-Reject .

- *Bước 4:* Các RADIUS Client chấp nhận hoặc từ chối người sử dụng theo kết quả xác thực nhận được từ server . Nếu nó chấp nhận người sử dụng, nó sẽ gửi một yêu cầu bắt đầu – kiểm toán (Accounting-Request) đến máy chủ RADIUS .
- *Bước 5:* Các RADIUS Server trả về một thông điệp khởi động kế toán (Accounting-Response) và bắt đầu kế toán (start-Accounting).
- *Bước 6:* Các host có thể truy cập các tài nguyên trong mạng theo quyền đã được quy định sẵn.
- *Bước 7:* Để kết thúc phiên làm việc host gửi một yêu cầu ngắt kết nối tới RADIUS client và RADIUS client gửi một yêu cầu ngắt kết nối đến RADIUS server.
- *Bước 8:* RADIUS server trả về thông điệp ngắt kết nối (stop-accounting) và dừng kiểm toán.
- *Bước 9:* Host ngừng truy cập tài nguyên mạng.

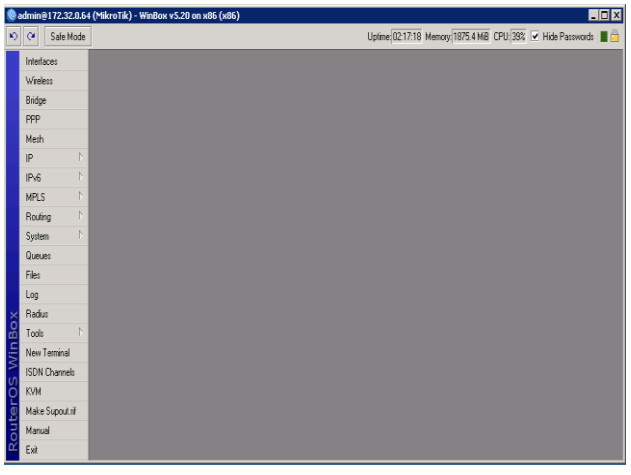
III. Mikrotik Router

Mikrotik là tên của một nhà sản xuất thiết bị mạng máy tính ở Latvian (một nước thuộc vùng Baltic – bắc Âu). Công ty thành lập năm 1995.Sản phẩm chính của Mikrotik là một hệ điều hành dựa trên Linux có tên là *Mikrotik RouterOS*. Được cài đặt trên phần cứng độc quyền của công ty (RouterBOARD) hoặc trên máy tính bình thường, biến máy tính đó thành router và thực hiện các tính năng như Router (DHCP, NAT, Routing...), firewall, bandwidth management, wireless access point, virtual private network (VPN), hotspot gateway và một số tính năng khác rất thích hợp để ứng dụng làm gateway cho cơ quan, doanh nghiệp và nhất là các dịch vụ internet công cộng.

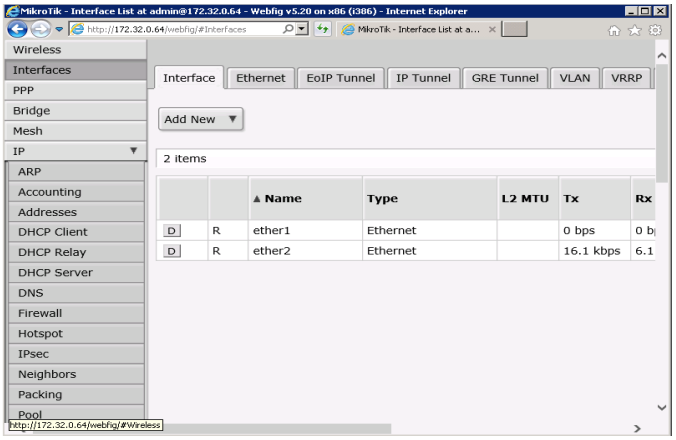


1. *Những bước cơ bản*

Sau khi cài đặt xong *hệ điều hành RouterOS* lên máy tính hoặc mở nguồn *Bộ định tuyến* (router) lần đầu tiên, chúng ta có nhiều cách để kết nối với nó:



- ***Winbox***

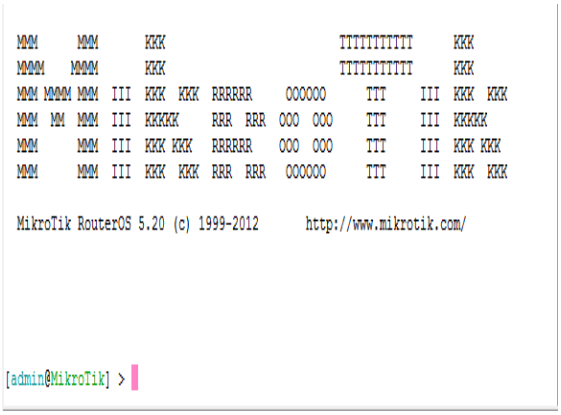


Winbox là tiện ích dùng để cấu hình, có thể kết nối với router thông qua địa chỉ MAC hoặc địa chỉ IP.

- ***WebFig***

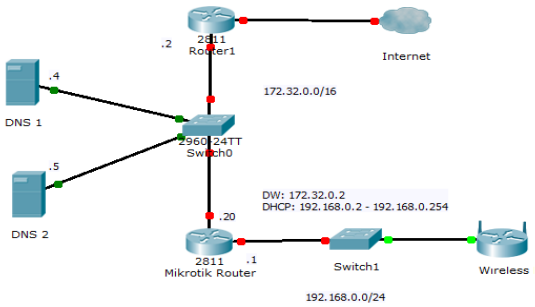
Nếu bạn có một router với cấu hình mặc định, khi đó chúng ta có thể kết nối với router bằng giao diện web thông qua địa chỉ IP của router. WebFig gần như có các chức năng cấu hình giống như Winbox.

- ***CLI***



Giao diện dòng lệnh (CLI) cho phép cấu hình router sử dụng dòng lệnh. Có rất nhiều lệnh có sẵn, vì thế họ chia chúng thành những nhóm tổ chức bằng cách phân cấp đơn cấp. Sau khi giao diện dòng lệnh hiện lên, bạn sẽ thấy phần đăng nhập. Điền tên đăng nhập là **admin** và mật khẩu đăng nhập để rỗng.

2. Mô hình thực nghiệm



3. Cấu hình mikrotik thông qua dòng lệnh

a. Cấu hình địa chỉ IP

- Cấu hình IP cho Interface Ethernet sẽ kết nối với Internet. Ở đây IP của Interface này là *172.32.0.64/16* và IP này sẽ được gán cho interface *ether2*.

[Admin@Mikrotik]> ip address add address=172.32.0.64/16 interface=ether2

- Cấu hình IP cho Interface Ethernet kết nối với các Access Point hay mạng Lan. Ở đây IP sẽ là 192.168.0.1/24 , Interface này sẽ được gán cho *ether1*.

[Admin@Mikrotik]> ip address add address=192.168.0.1/24 interface=ether1

- Cấu hình IP default gateway ví dụ ở đây là *172.32.0.1*.

[Admin@Mikrotik]> ip route add gateway 172.32.0.1

b. Cấu hình DHCP Server

Thêm các thông tin DNS cho máy chủ. Nếu trong mạng có máy chủ DNS thì ta thêm địa chỉ máy chủ này vào.

[admin@MikroTik] /ip dns set servers=172.32.0.4,8.8.8.8

Gõ lệnh sau để hiển thị các dòng yêu cầu nhập thông tin dhcp-server:

[admin@MikroTik] > ip dhcp-server setup dhcp server interface: ether1

dhcp address space: 192.168.0.0/24 gateway for dhcp network: 192.168.0.1

addresses to give out: 192.168.0.3-192.168.0.254 (Đây là dải IP mà dịch vụ dhcp sẽ cấp cho các máy con khi kết nối)

dns servers: 172.32.0.4,8.8.8.8

lease time: 3d (Thời gian cho thuê mặc định là 03 ngày)

c. ***Cấu hình Hotspot***

Việc cấu hình Hotspot sẽ bao gồm cấu hình dịch vụ DHCP server, các thông tin DNS… Gõ lệnh sau:

[Admin@Mikrotik] ip hotspot setup (sau ghi gõ lệnh này sẽ xuất hiện các hàng yêu cầu nhập thông tin như sau)

Hotspot interface: **ether1**

Local address of network: **192.168.0.1/24**

Masquerade network: yes

Address pool of network: **192.168.0.2-192.168.0.254**

Select certificate: **none** (chú ý: mặc định xuất hiện dòng import-other-certificate, chúng ta xóa dòng đó và nhập vào none).

Ip address of smtp server: **0.0.0.0** (nếu trong mạng có máy chủ smtp thì gõ địa chỉ ip vào, còn không thì để mặc định 0.0.0.0).

Dns server: **172.32.0.4, 8.8.8.8**.

Dns name: điền vào tên của máy Hotspot này được khai báo trên DNS server của mạng, nếu không có thì để trống chứ không khai tùy ý.

Name of local hotspot user: **Admin** (tạo một account cho hệ thống để test đăng nhập hotspot).

Password for the user: mật khẩu của account này.

d. ***Cấu hình NAT***

[Admin@Mikrotik] ip firewall nat add chain=srcnat action=masquerade out-interface=ether2

Như vậy cơ bản cấu hình song hệ thống Hotspot với Mikrotik. Lúc này dùng một máy con đăng nhập web sẽ thấy màn hình đăng nhập của Mikrotik xuất hiện, nhập vào account tạo sẵn ở bước cấu hình hotspot trên là có thể truy xuất web…

e. Cấu hình Radius

Sau khi hotspot đã hoạt động tốt, chúng ta tiến hành cấu hình user-manager. Mở winbox, chọn **Radius** – sau đó chọn dấu cộng (+) để thêm. Cửa sổ mới xuất hiện. Điền địa chỉ IP của Radius User Manager, mã bí mật. Ví dụ, ithcmute.local. *Chú ý*: Địa chỉ IP của Radius server phải là IP WAN của router mikrotik hoặc localhost (127.0.0.1). Chọn OK. Sau đó chọn **Incoming**. Chọn **Accept**, điền port mình cần vd: 3799. Sau đó **OK**.

Sau đó mở cửa sổ Hotspot (**IP – Hotspot**), chọn thẻ **Server profiles**. Chọn Chọn Profiles cần cấu hình **Default**. Sau đó cửa số mới xuất hiện. Chọn thẻ **RADIUS**. Đánh dấu vào **Use radius**, và **Accounting**. Sau đó chọn **OK**.

f. ***Cấu hình router***

Kết thúc cấu hình ở winbox, mở trình duyệt, và đi đến trang web *http://<ip-address-mikrotik>/userman*. Vidụ: ***http://172.32.0.64/userman*** . Đăng nhập với tên là **admin** và mật khẩu.

Chọn **routers – add – New**. Mô tả của router mới hiện lên, điền name, IP address, secret, và coa port.

g. Cấu hình Firewall ngăn chặn website

Trong màn hình config chọn IP > Firewall. Chọn dấu + để thiết lặp firewall. Ví dụ: Thiết lập ngăn web vnexpress.net, Game, Facebook, bảo vệ Router… như sau:

/ip firewall filter
add chain=forward action=reject reject-with=tcp-reset protocol=tcp content="Host: www.facebook.com"

KẾT LUẬN

Khi nghiên cứu đề tài " Tìm hiểu về Mikrotik router và xây dựng demo hệ thống hotspot gateway cho dịch vụ internet LAN Wifi có chứng thực", người nghiên cứu đã cơ bản đạt được những mục tiêu:

- Cung cấp những kiến thức cơ bản và hoàn chỉnh về WLAN cũng như cung cấp cho người đọc những thông tin tổng quan về sự phát triển của WLAN và những lợi ích mà WLAN mang lại.

- Tìm hiểu và đưa ra những thông tin quan trọng giúp người đọc nắm rõ nguyên tắc hoạt động cũng như cấu trúc của giao thức chứng thực RADIUS.

- Xây dựng demo hệ thống hotspot gateway cho dịch vụ Iintenet-WLAN sử dụng giao thức xác thực RADIUS trên Mikrotik router.

TÀI LIỆU THAM KHẢO

[1]. Cấu hình Mikrotik từ A-Z : *http://www.mikrotik.com/testdocs/ros/2.9/*

[2]. Cấu hình chặn web đen với Mikrotik mô hình proxy: *http://wiki.mikrotik.com/wiki/How_to_Block_Websites_%26_Stop_Downloading_Using_Proxy*

[3]. Cấu hình giới hạn băng thông: *http://wiki.mikrotik.com/wiki/PCQ_Examples*

[4]. Cấu hình webproxy:*http://www.mikrotik.com/testdocs/ros/2.9/ip/webproxy.php* *http://www.mikrotik.com/testdocs/ros/2.9/ip/webproxy_content.php#7.53.7*

[5]. Cấu hình Mikrotik làm Firewall cho mạng lan có kết nối internet: *http://wiki.mikrotik.com/wiki/How_to_Connect_your_Home_Network_to_xDSL_Li ne*

[6]. Diễn đàn trao đổi, thảo luận về Mikrotik *www.forum.mikrotik.com*

Họ tên: **ThS. Nguyễn Hữu Trung**
Đơn vị: Khoa Công Nghệ Thông Tin
Điện thoại: 0908617108
Email:trungnh@hcmute.edu.vn