



Hotspot with Active Directory

Eng. Ahmed AlBakri
Wireless Communications Channels

Mikrotik User Meeting
Saudi Arabia – Riyadh
22 October 2017

Eng. Ahmed AlBakri

- ❖ **Bachelor in Computer Science and Engineering**
- ❖ **Working with wireless since 2007**
- ❖ **Mikrotik Master Distributor with WCC**
- ❖ **MikroTik Certified Network Associates – MTCNA**
- ❖ **MikroTik Certified Routing Engineer - MTCRE**
- ❖ **MikroTik Certified Wireless Engineer - MTCWE**

Topics

- ❖ **What is hotspot?**
- ❖ **Where installed?**
- ❖ **Hotspot Wizard**
- ❖ **Hotspot Advance features**
- ❖ **Integration with Active Directory**

Hotspot

- **It is RouterOs Tool for Instant Plug-and-Play Internet access**
- **HotSpot is a way to authorize users to access some network resources, but does not provide traffic encryption.**
- **It also provides Flexible User Accounting.**
- **Different ways of authorization.**

Where?

- Open Access Points, Internet Cafes, Airports, universities campuses
- Hotel, restaurant, café
- Shopping Mall,
- Public Park and areas,
- Camping, Beach
- Marinas
- Hospital
- Municipal Hotspot

... where you want



Example of Hotspot page



WCC
القنوات اللاسلكية للإتصالات
Wireless Communication Channels

القنوات اللاسلكية للإتصالات

www.wifi-wimax.com.sa

تسجيل الدخول + أسعار الخدمة + شروط الخدمة + الحسابات البنكية + إتصل بنا

(if trial == 'yes') يمكن تجربة الإنترنت 5 دقائق مجاناً، بالضغط هنا.\$(endif)

مرحباً بك في شبكة القنوات اللاسلكية للإتصالات لتقديم خدمة الإنترنت.

الآن وصل حديثاً

EnGenius ECP600

يتميز عن النماذج - ممتد جداً بت
سرعة نقل عالية - متفاحة لاجر

- Dual Band
- 2.4Ghz + 5Ghz
- 300-300Mbps
- Gigabit Port
- POE 802.3at
- 22 Connector
- up to 24 dBm
- S/BI
- VLAN
- Multi SSID

WCC

الآن وصل حديثاً

UniFi-AC

أول أكسس بوينت يعمل بنظام AC

- 802.11ac Technology
- Dual Band 2.4Ghz and 5Ghz
- 450Mbps in 2.4Ghz
- 1300Mbps in 5Ghz
- 2000m in 2.4Ghz and 5Ghz
- 3x3 MIMO
- 2 Gigabit Ethernet Port
- POE 802.3at
- Zero Hand-off Technology
- Management Software
- VLAN
- Multi SSID

WCC

MUM SAUDI ARABIA

RIYADH, OCTOBER 22, 2017

للتواصل معنا :
0590076820

<input type="text" value="(username)"/>	اسم المستخدم
<input type="text"/>	كلمة المرور
<input type="button" value="OK"/>	

www.wifi-wimax.com.sa

القنوات اللاسلكية للإتصالات

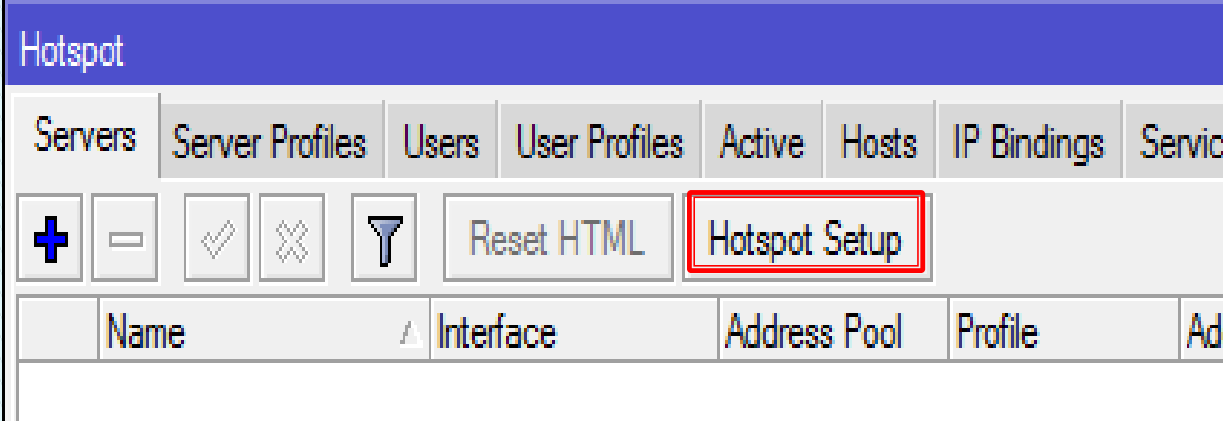
WCC
القنوات اللاسلكية للإتصالات
Wireless Communication Channels

Hotspot Requirements

- **Valid IP addresses on Internet and Local Interfaces.**
- **DNS servers addresses added to ip dns.**
- **At least one HotSpot user.**

Hotspot Wizard

- HotSpot setup is easy.
- Setup is similar to DHCP Server setup.



Hotspot

Servers Server Profiles Users User Profiles Active Hosts IP Bindings Service

+ - ✓ ✗ ⏏ Reset HTML **Hotspot Setup**

Name	Interface	Address Pool	Profile	Ad
------	-----------	--------------	---------	----

• **Run ip > Hotspot Setup.**

Hotspot Setup

Hotspot Setup

Select interface to run HotSpot on

HotSpot Interface: ether2

Back Next Cancel

1. Select Interface to run HotSpot on.

Hotspot Setup

Set pool for HotSpot addresses

Address Pool of Network: 192.168.1.10-192.168.1.254

Back Next Cancel

3. Select hotspot addresses.

Hotspot Setup

Set HotSpot address for interface

Local Address of Network: 192.168.1.1/24

Masquerade Network

Back Next Cancel

2. HotSpot address will be selected automatically.

Hotspot Setup

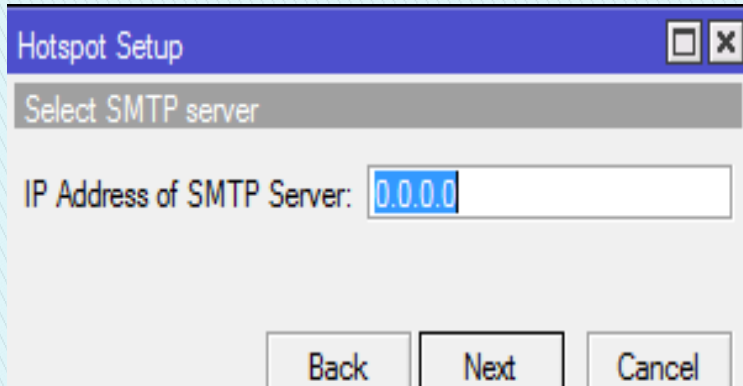
Select hotspot SSL certificate

Select Certificate: none

Back Next Cancel

4. Whether to use certificate together with HotSpot or not.

Hotspot Setup



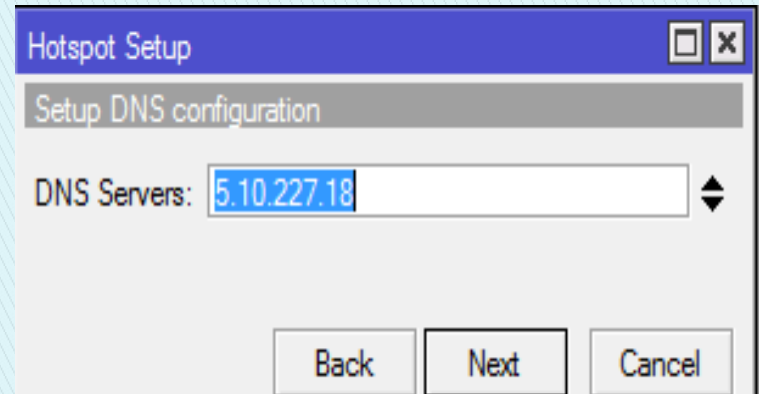
Hotspot Setup

Select SMTP server

IP Address of SMTP Server:

Back Next Cancel

5. IP address to redirect SMTP (e-mails) to your SMTP server.



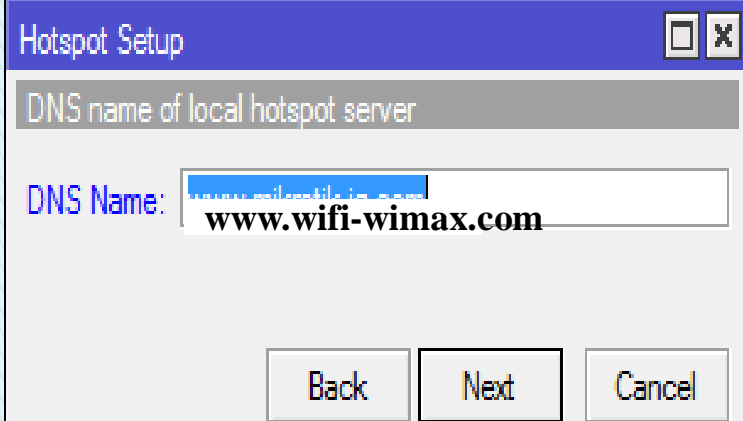
Hotspot Setup

Setup DNS configuration

DNS Servers:

Back Next Cancel

6. Insert DNS ip address or use router DNS.



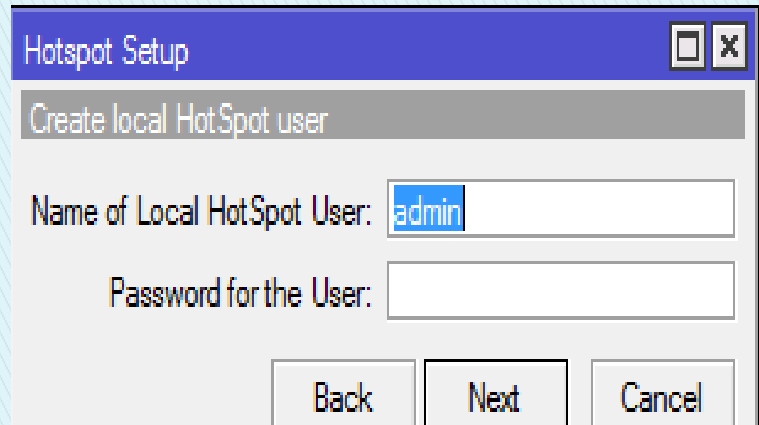
Hotspot Setup

DNS name of local hotspot server

DNS Name:

Back Next Cancel

7. DNS name for HotSpot server



Hotspot Setup

Create local HotSpot user

Name of Local HotSpot User:

Password for the User:

Back Next Cancel

8. Add first HotSpot user that use to login in hotspot server.

Important Notes

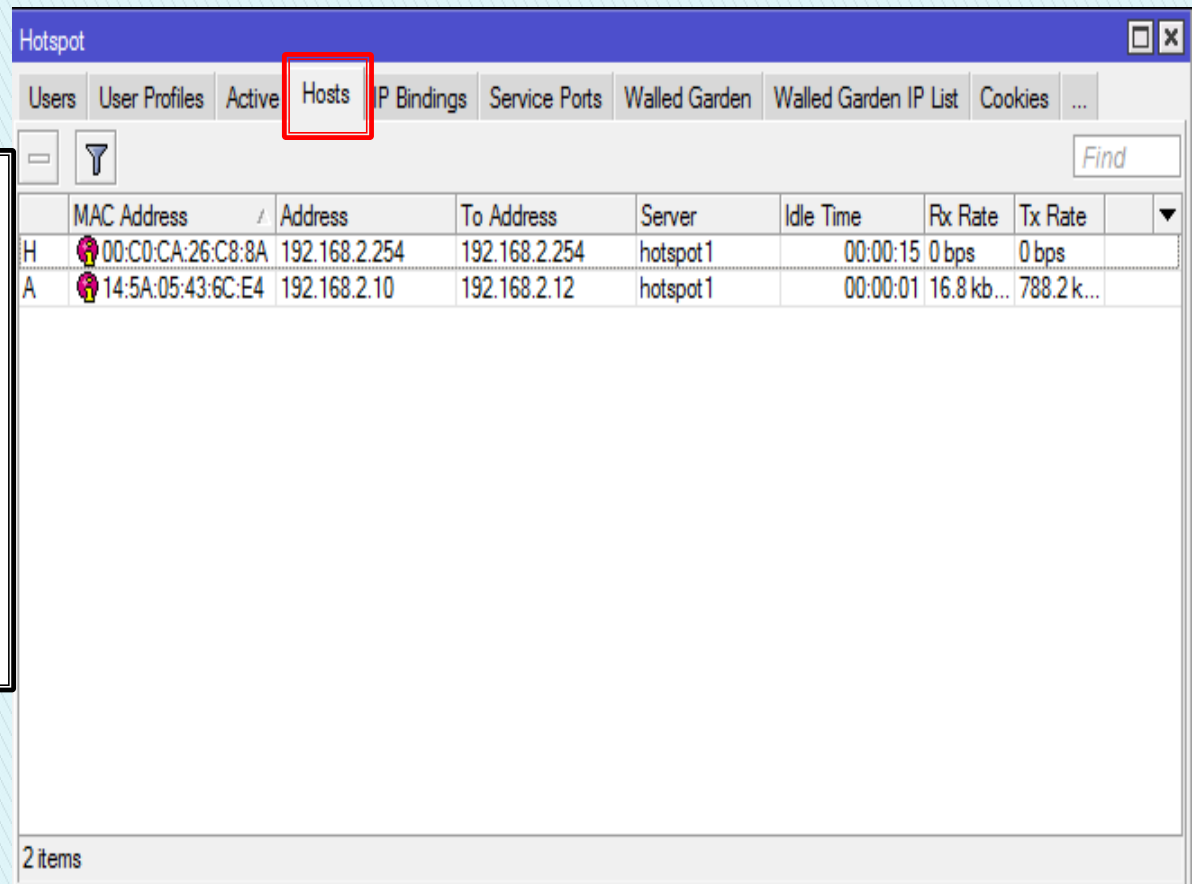
- **Users connected to HotSpot interface will be disconnected from the Internet.**
- **Client will have to authorize in HotSpot to get access to Internet.**
- **Remember you cant search or enter to router by using WinBox or CLI through interface configured as Hotspot server.**
- **HotSpot default setup creates additional configuration:**
 - **Dynamic Firewall rules (Filter and NAT).**

HotSpot Help

- HotSpot login page is provided when user tries to access any web-page.
- To logout from HotSpot you need to go to **<http://router-IP>** or **<http://HotSpot-DNS>**

HotSpot Network Hosts

**Information
about connected
clients (PC)
appear at Hosts
sub menu**



The screenshot shows the 'Hotspot' management interface. The 'Hosts' tab is selected and highlighted with a red box. Below the tabs, there is a search bar and a table of connected clients. The table has columns for MAC Address, Address, To Address, Server, Idle Time, Rx Rate, and Tx Rate. Two items are listed in the table.

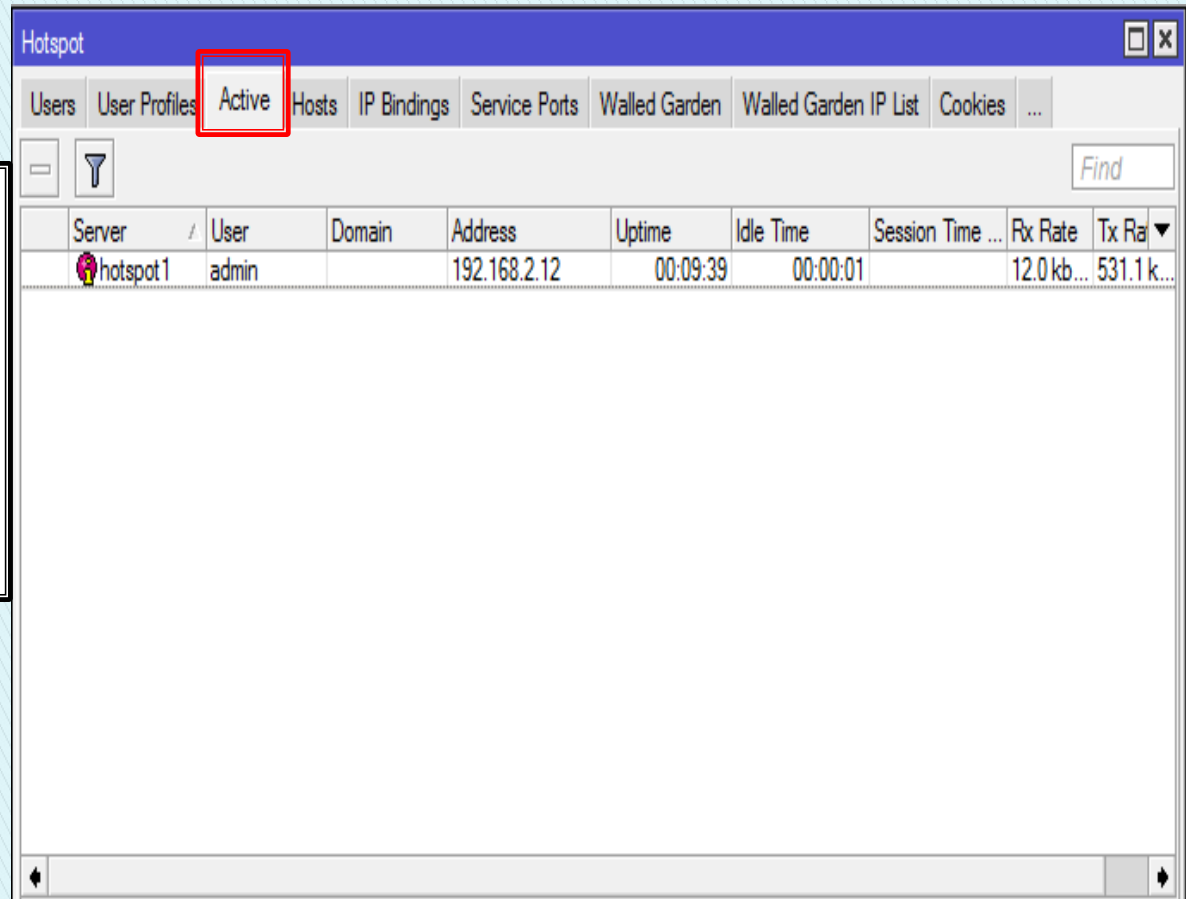
	MAC Address	Address	To Address	Server	Idle Time	Rx Rate	Tx Rate	
H	00:C0:CA:26:C8:8A	192.168.2.254	192.168.2.254	hotspot1	00:00:15	0 bps	0 bps	
A	14:5A:05:43:6C:E4	192.168.2.10	192.168.2.12	hotspot1	00:00:01	16.8 kb...	788.2 k...	

2 items

- Information about clients connected to HotSpot router.

HotSpot Active Table

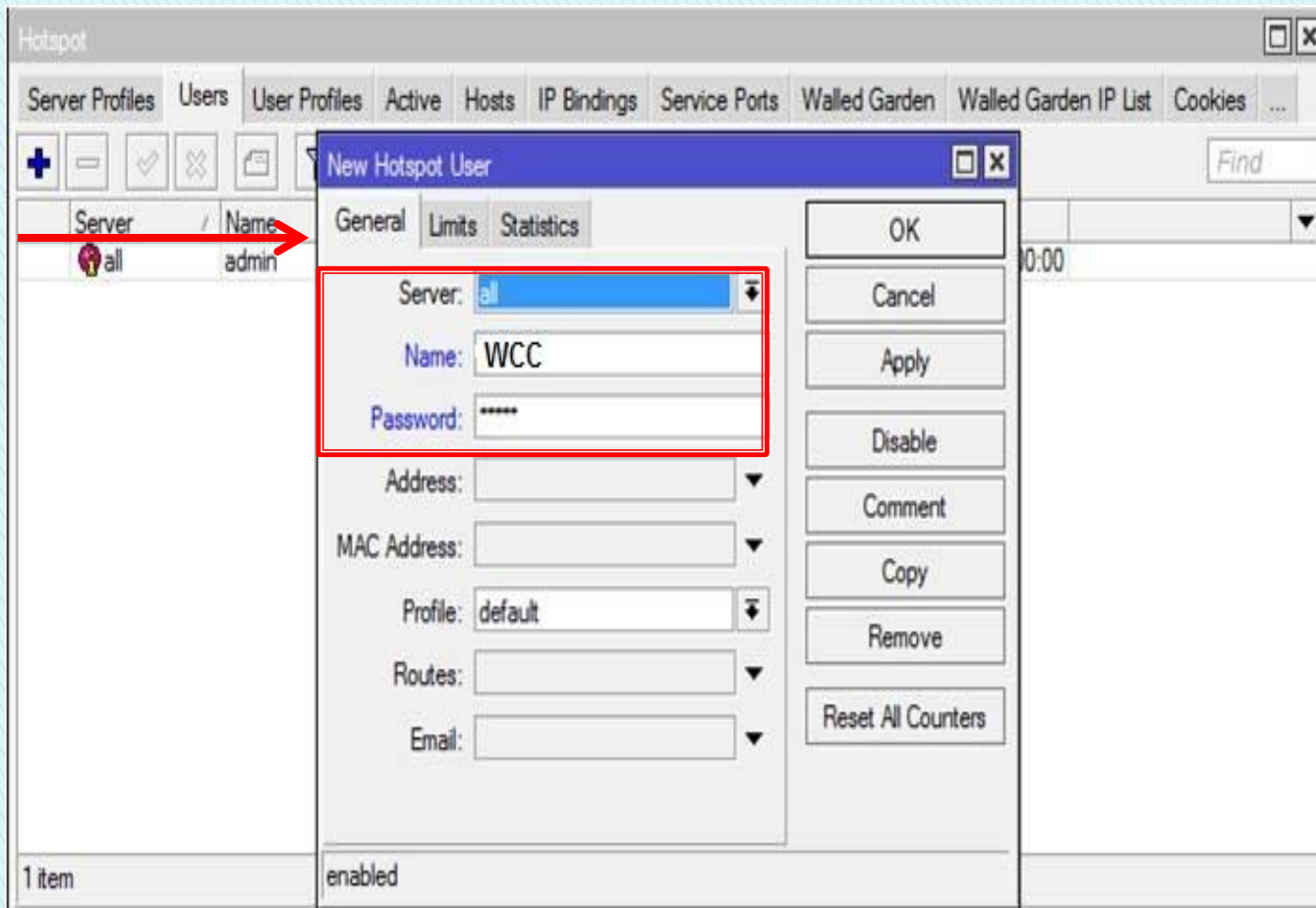
Information about connected person appear at active sub menu.



Server	User	Domain	Address	Uptime	Idle Time	Session Time ...	Rx Rate	Tx Rate
hotspot1	admin		192.168.2.12	00:09:39	00:00:01		12.0 kb...	531.1 k...

- Information about authorized HotSpot clients.

User Management



- Add/Edit/Remove HotSpot users.

Advance Features

HotSpot Walled-Garden

- Tool to get access to specific resources without HotSpot authorization.
- Specific resources could be local web server or external web page like (www.mikrotik.com).
- Walled-Garden for HTTP and HTTPS.
- Walled-Garden IP for other resources (Telnet, SSH, Winbox, etc).

HotSpot Walled-Garden

Hotspot

Server Profiles Users User Profiles Active Hosts IP Bindings Service Ports **Walled Garden** Walled Garden IP List Cookies ...

+ - ✓ ✕ 📄 🔍 Find

Action	Server	Method
--------	--------	--------

0 items

New Walled Garden Entry

Action: allow deny

Server: [Dropdown]

Src. Address: 192.168.X.0/24 ▲

Dst. Address: [Text]

Method: [Dropdown]

Dst. Host: www.google.com ▲

Dst. Port: [Dropdown]

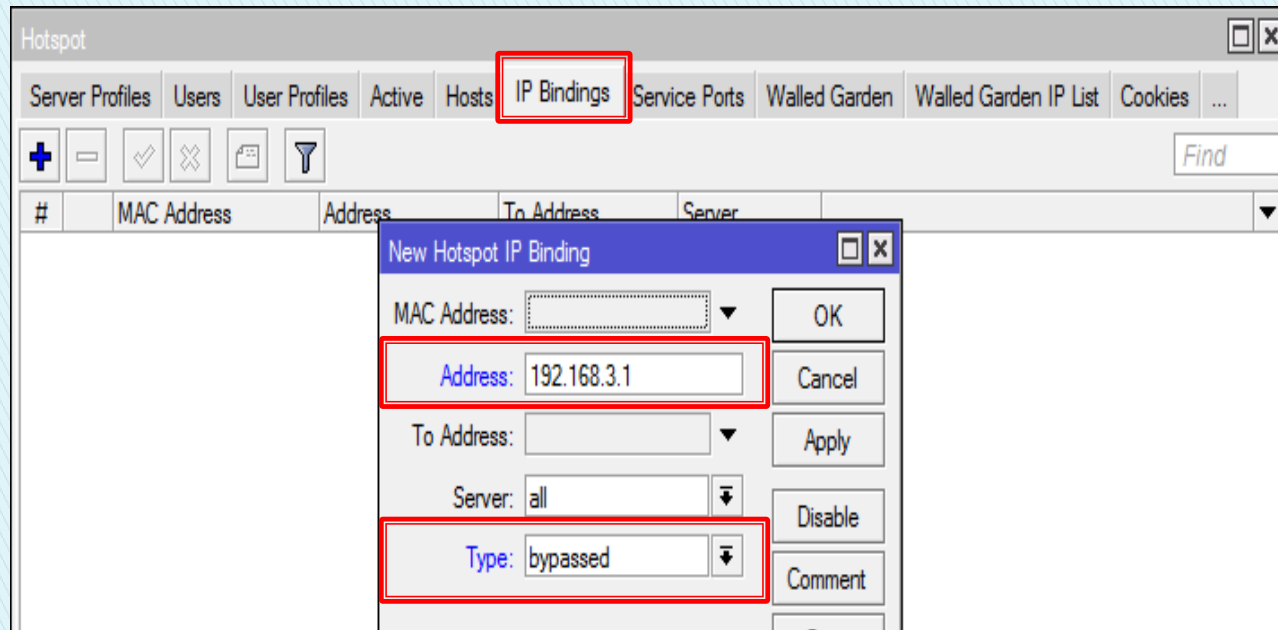
Path: [Dropdown]

enabled

OK Cancel Apply Disable Comment Copy Remove

- Allow access to google.com

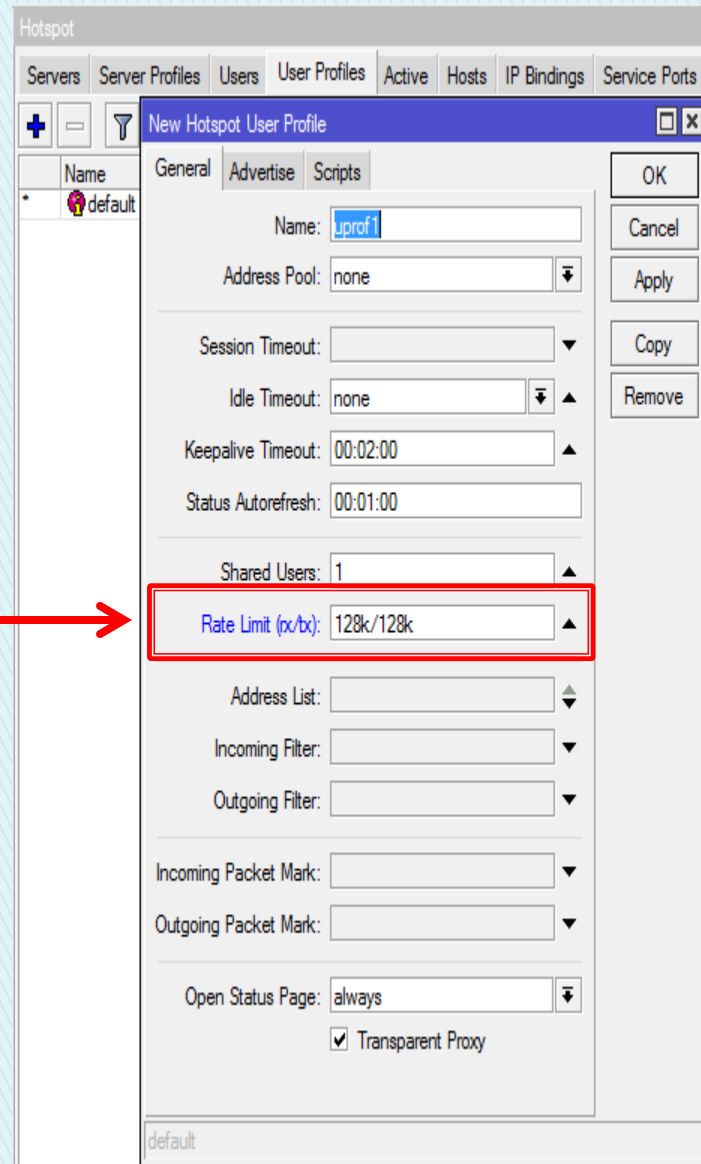
Bypass HotSpot



- Bypass specific clients over HotSpot.
- VoIP phones, printers, super users.
- IP-binding is used for that.
- IP bindings not like walled-garden it's open all public network resources

HotSpot Speed limitation

- To give each client 128k upload and 128k download, set **Rate Limit**.



Hotspot

Servers Server Profiles Users User Profiles Active Hosts IP Bindings Service Ports

New Hotspot User Profile

Name:

Address Pool:

Session Timeout:

Idle Timeout:

Keepalive Timeout:

Status Autorefresh:

Shared Users:

Rate Limit (rx/tx):

Address List:

Incoming Filter:

Outgoing Filter:

Incoming Packet Mark:

Outgoing Packet Mark:

Open Status Page:

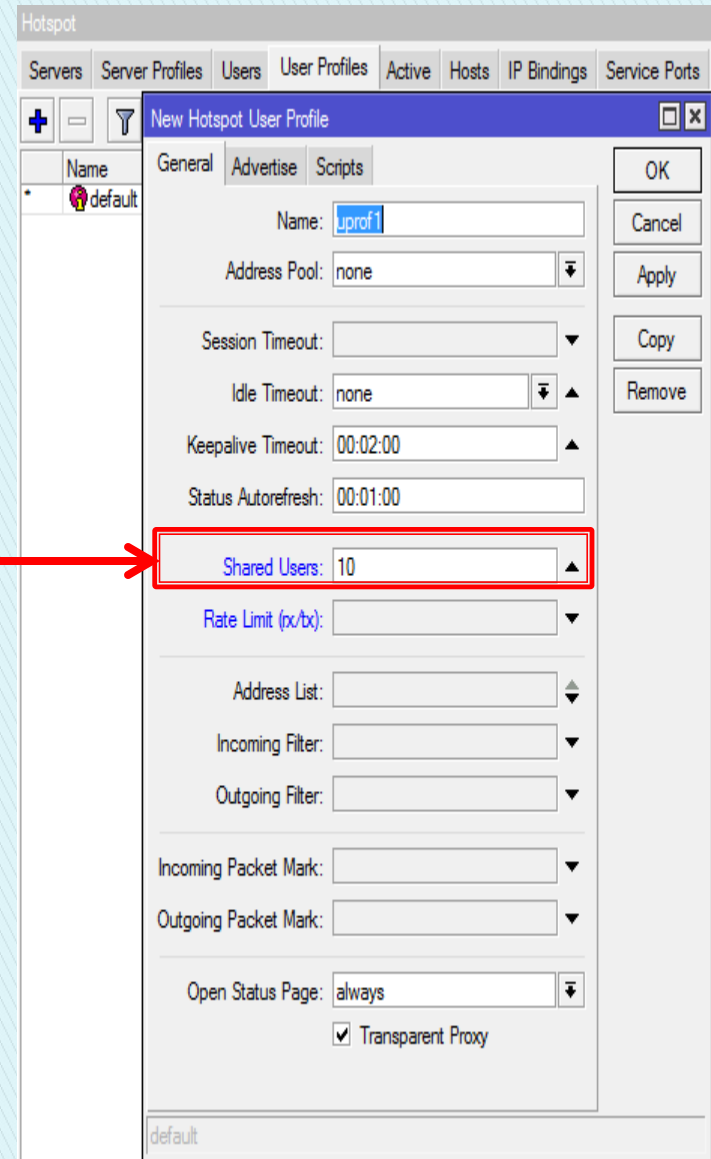
Transparent Proxy

OK Cancel Apply Copy Remove

default

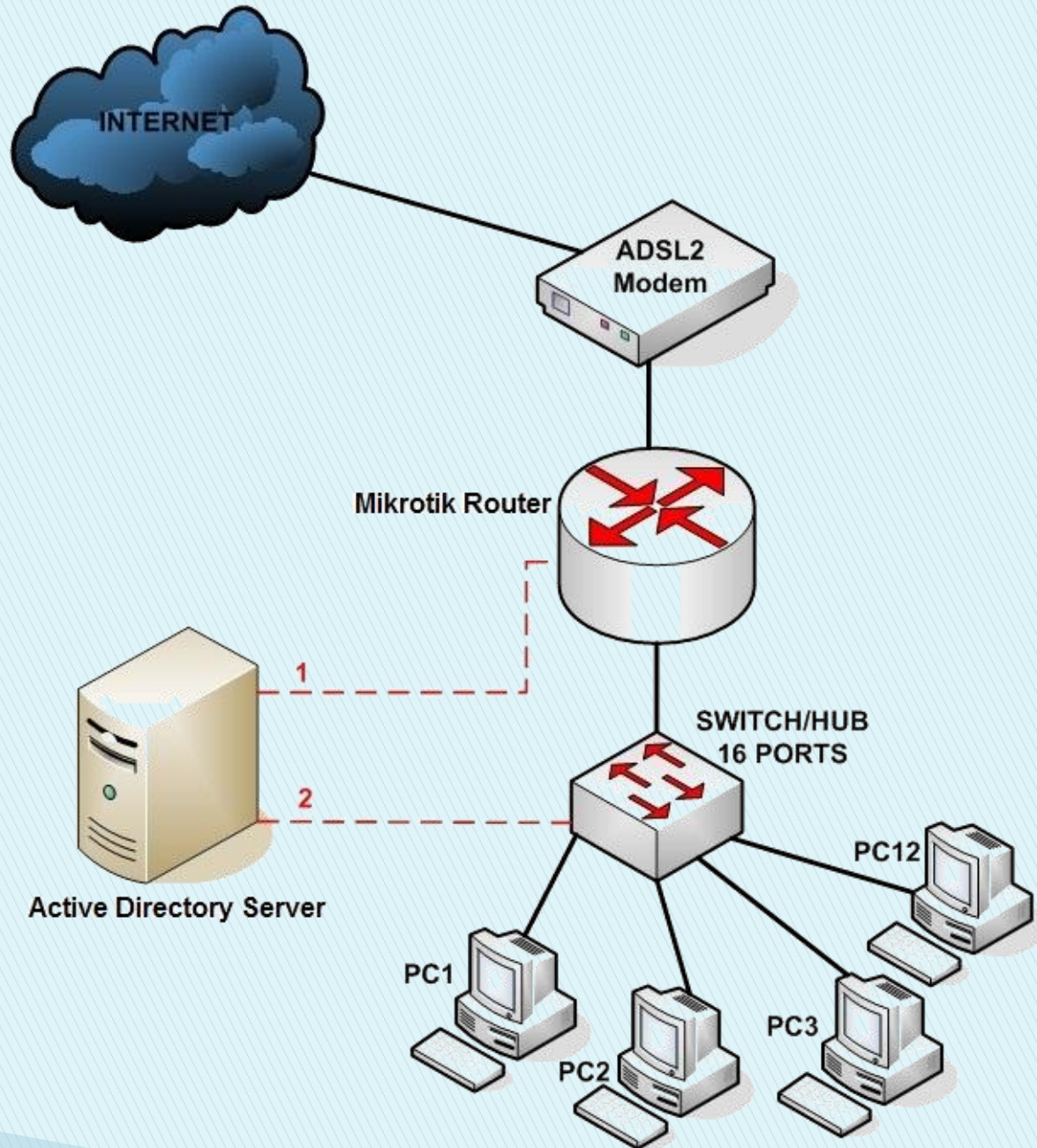
HotSpot Shared users

- To let 10 or more users use the same hotspot account(username and password).

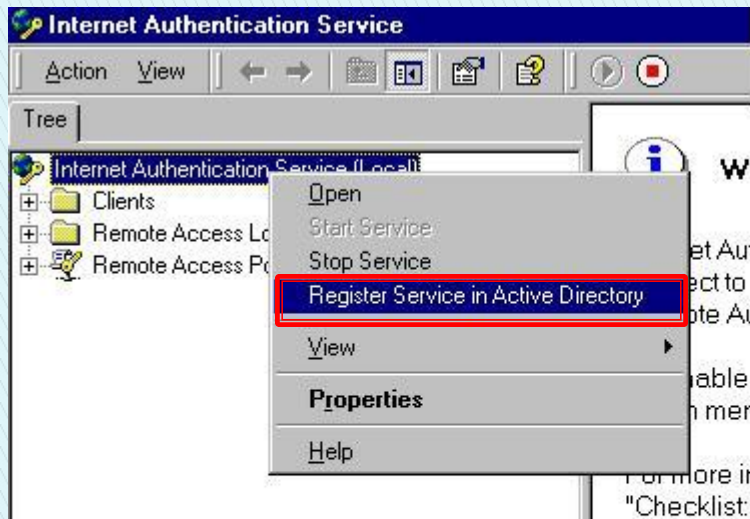


The screenshot shows the Mikrotik Hotspot configuration interface. The 'New Hotspot User Profile' dialog is open, showing the 'General' tab. The 'Shared Users' field is highlighted with a red box and a red arrow pointing to it, indicating that it is set to 10. Other fields include Name (lprof1), Address Pool (none), Session Timeout, Idle Timeout (none), Keepalive Timeout (00:02:00), Status Autorefresh (00:01:00), Rate Limit (px/bx), Address List, Incoming Filter, Outgoing Filter, Incoming Packet Mark, Outgoing Packet Mark, Open Status Page (always), and a checked 'Transparent Proxy' checkbox.

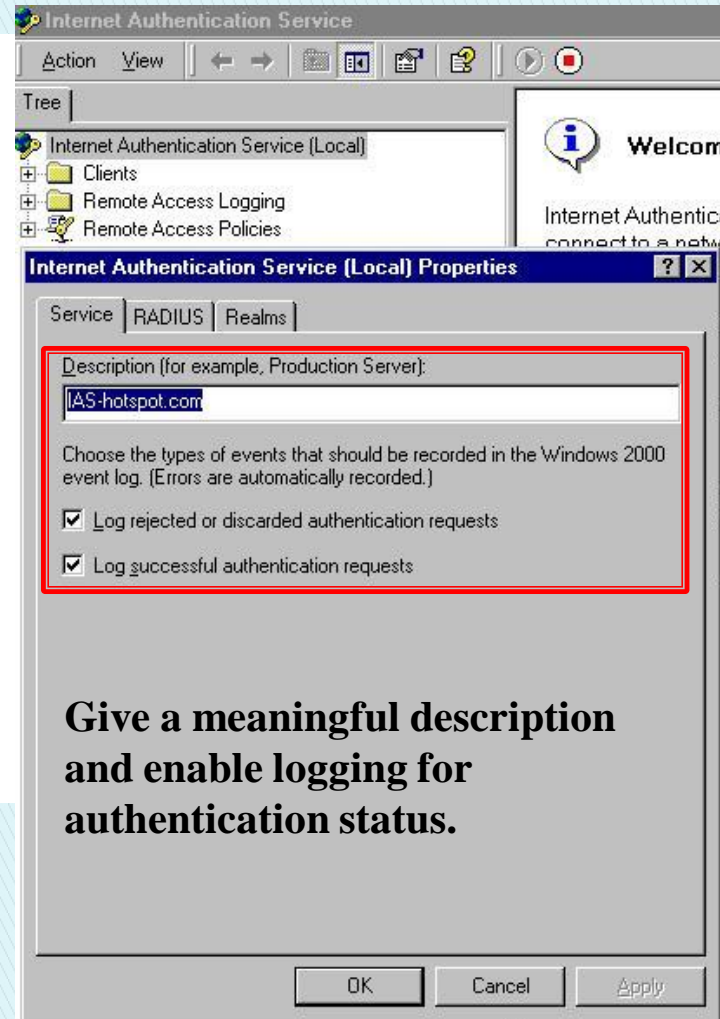
Hotspot Integration with Active Directory



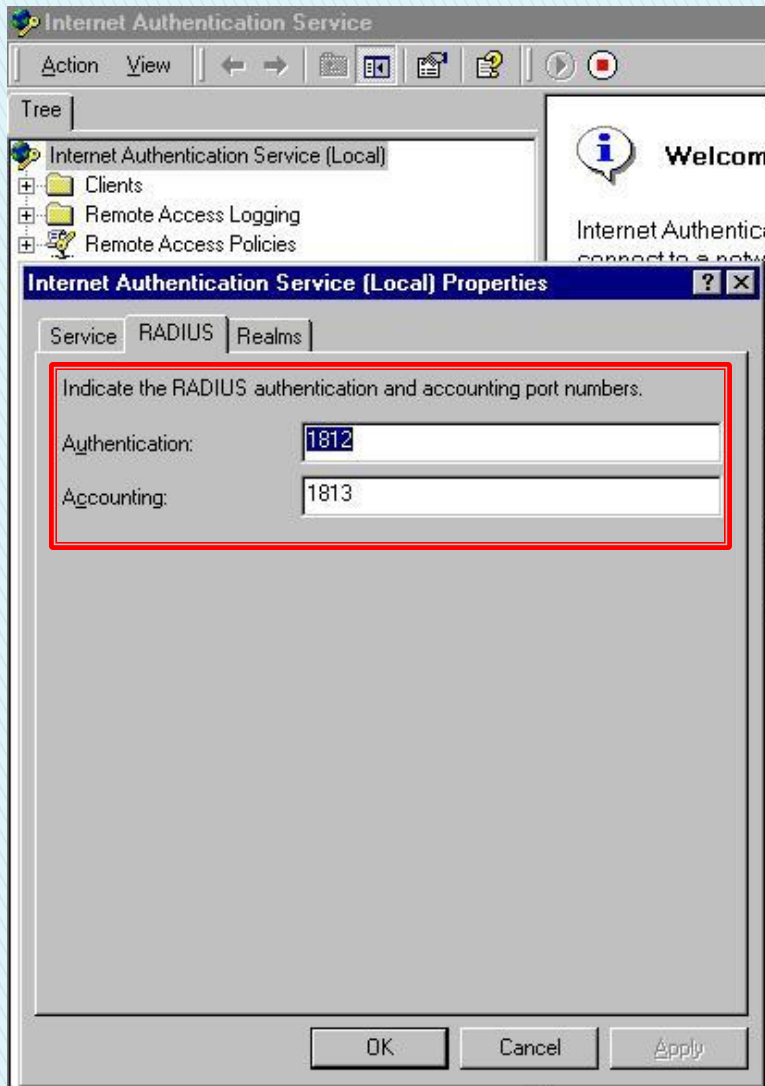
Configuration in Microsoft windows server



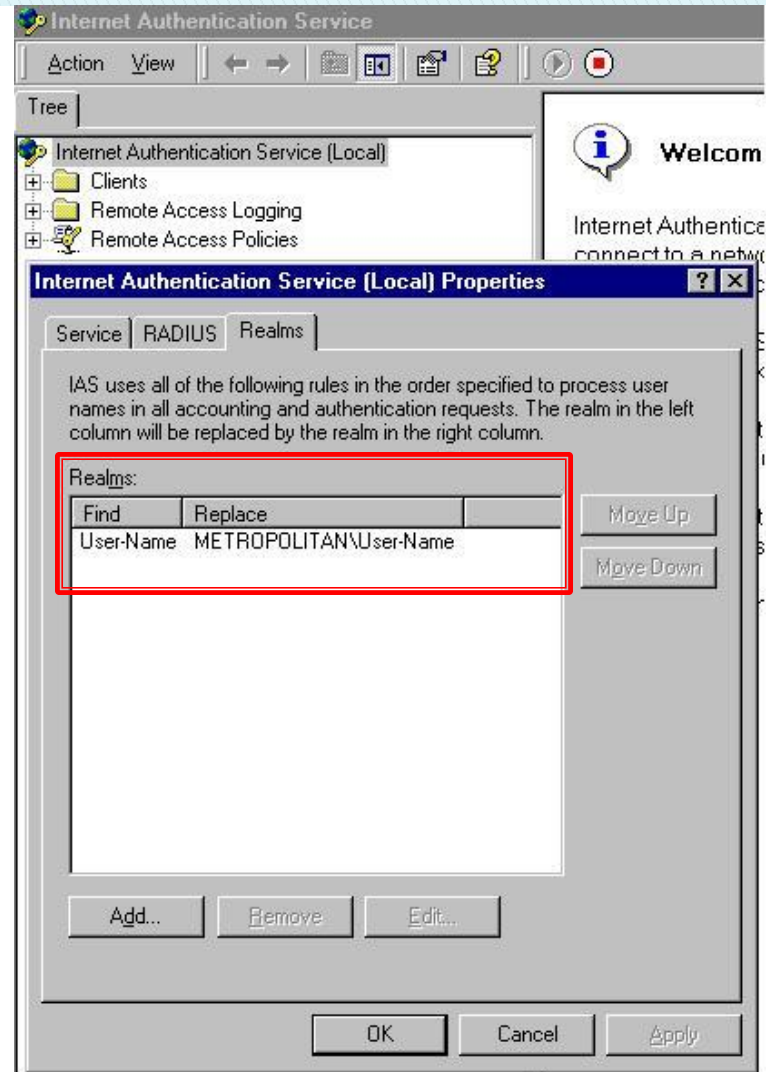
Setup IAS on a server acting as Active Directory Services Domain Controller and register it's services.



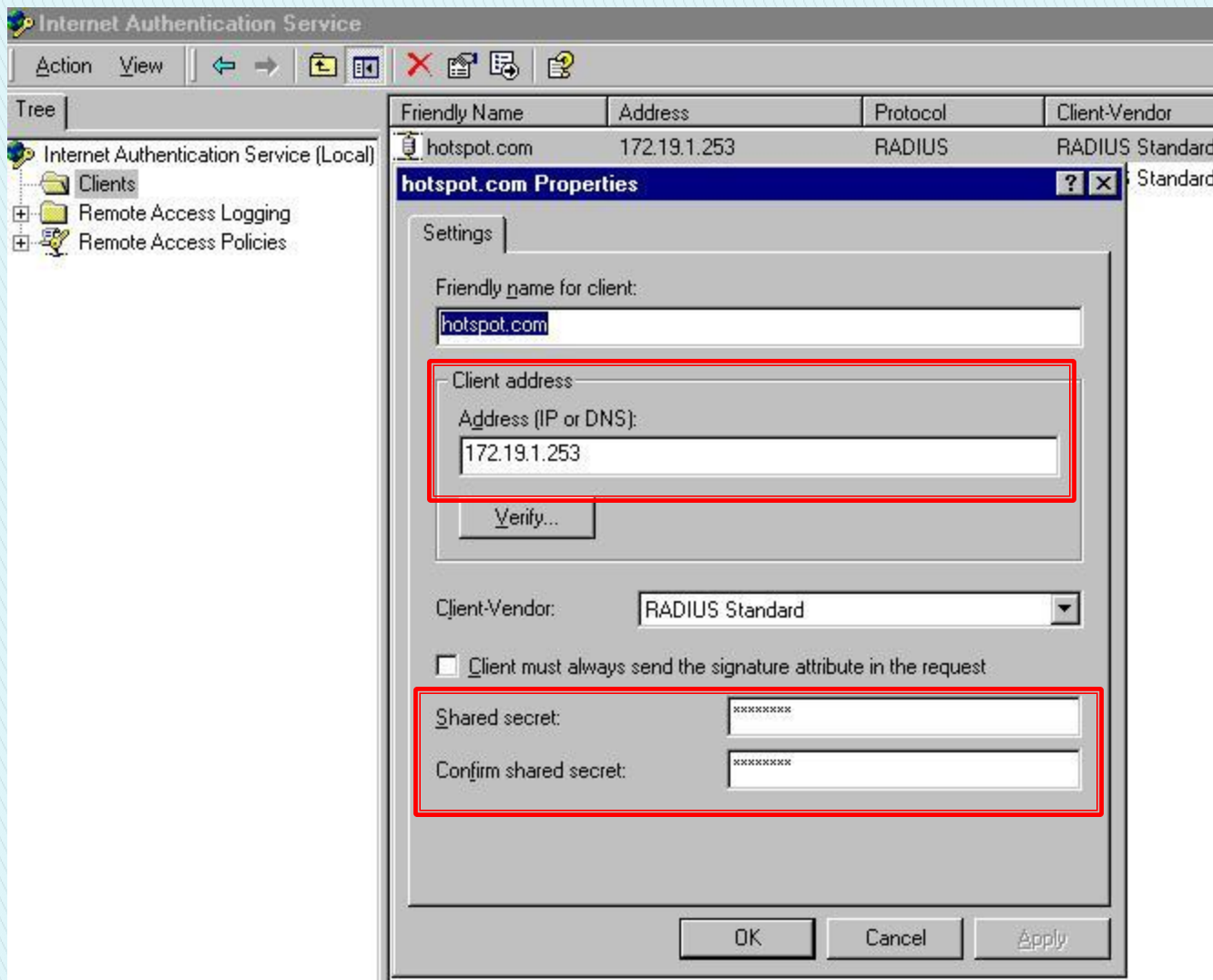
Give a meaningful description and enable logging for authentication status.



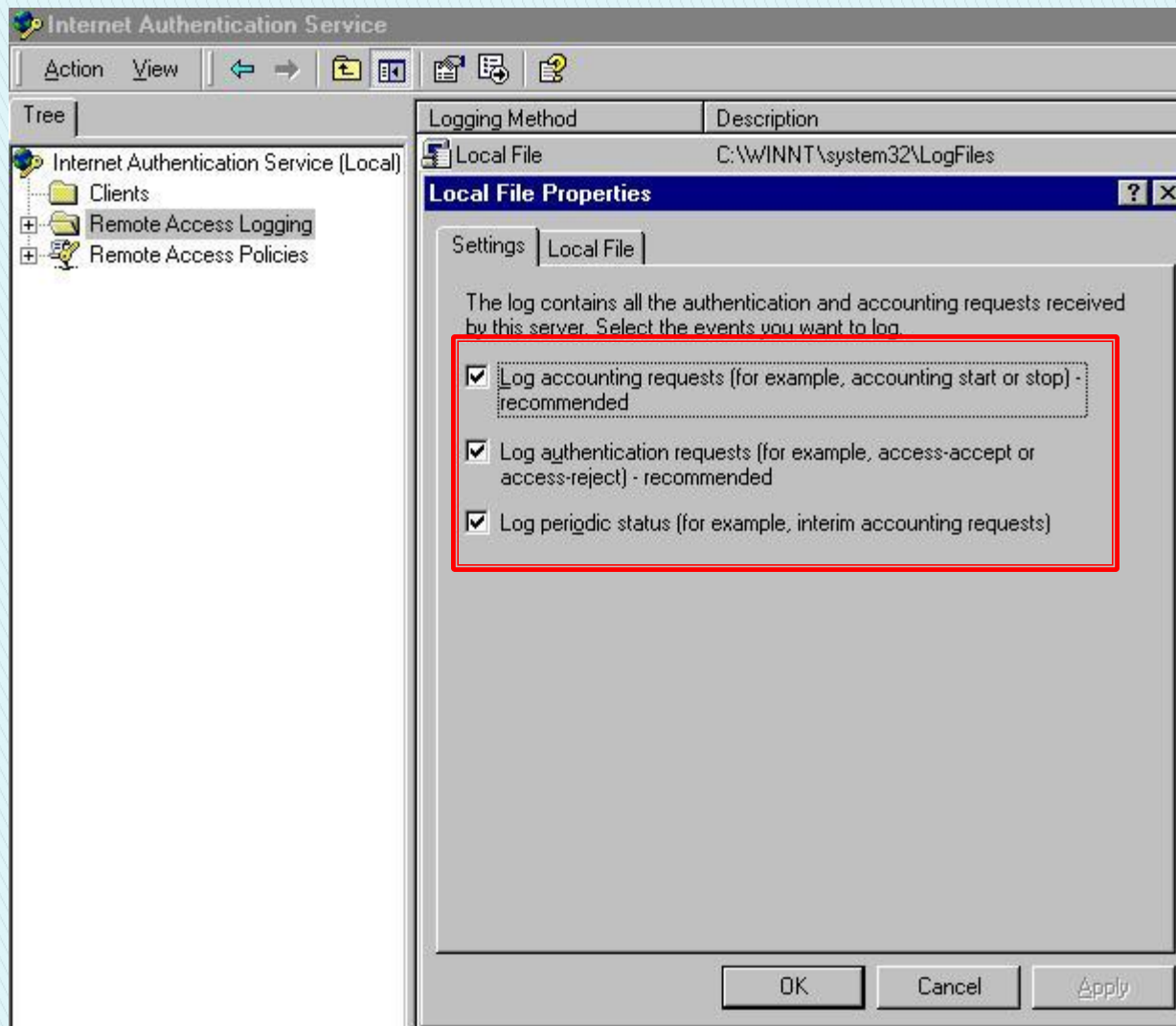
User respective 1812 for Authentication and 1813 for Accounting port only.



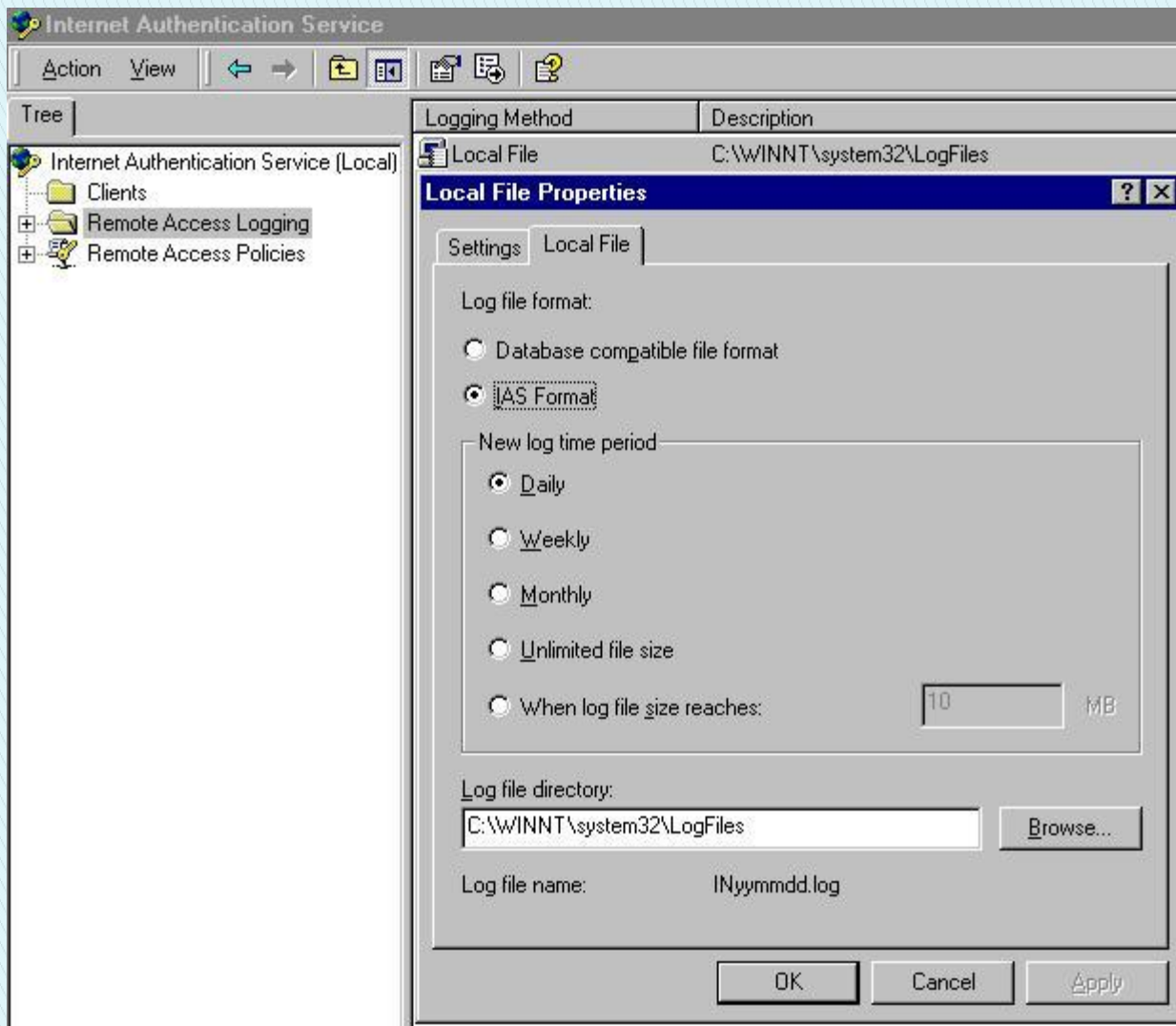
Create a Realms profile, find “User-Name” replace it with “DOMAIN\User-Name” variables into IAS.



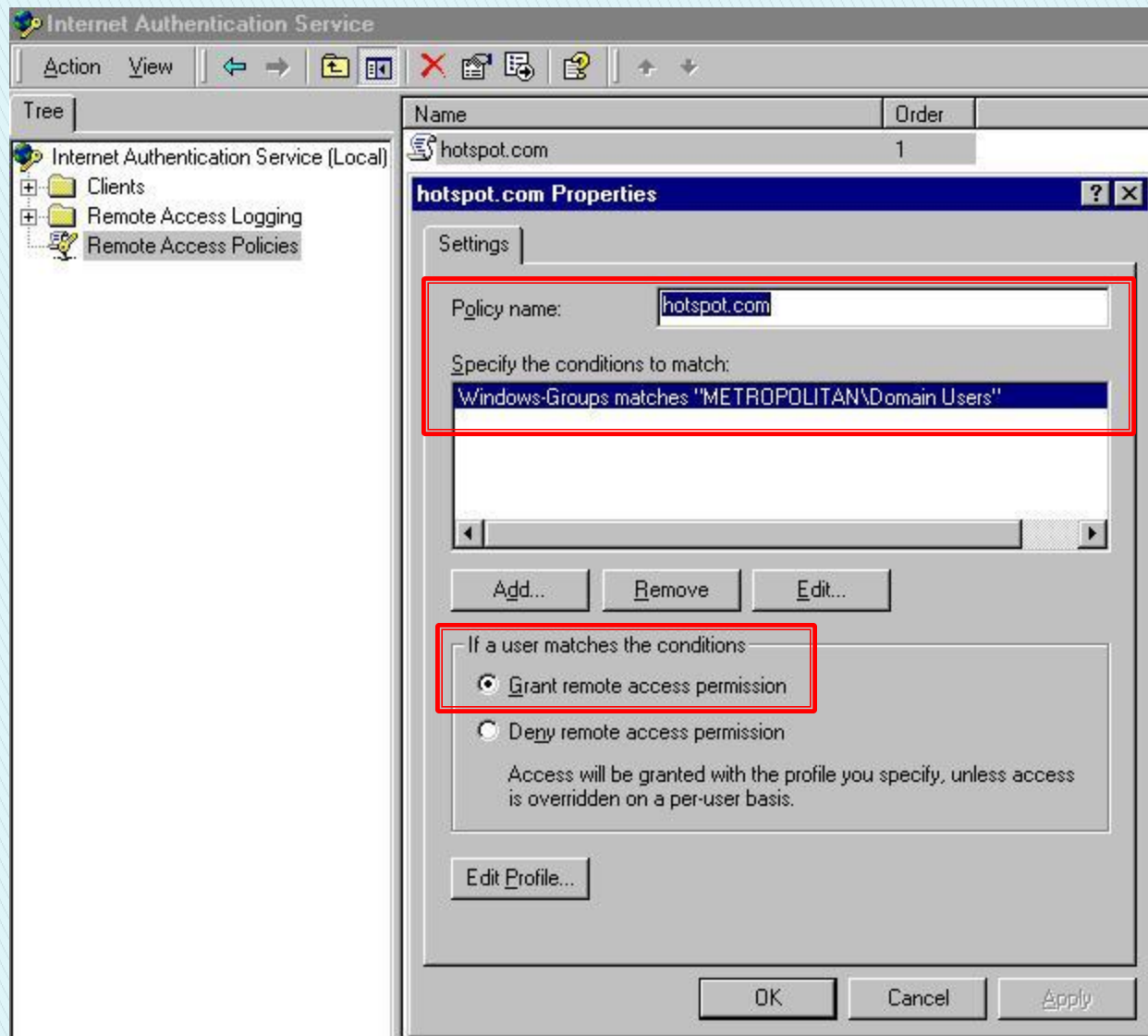
Create a “hotspot.com” client profile and set IP address pointing to MikroTik hotspot server 172.19.1.253 Set Client Vendor to RADIUS Standard and enter a unique password for IAS. Do not enable Attributes Signature check box.



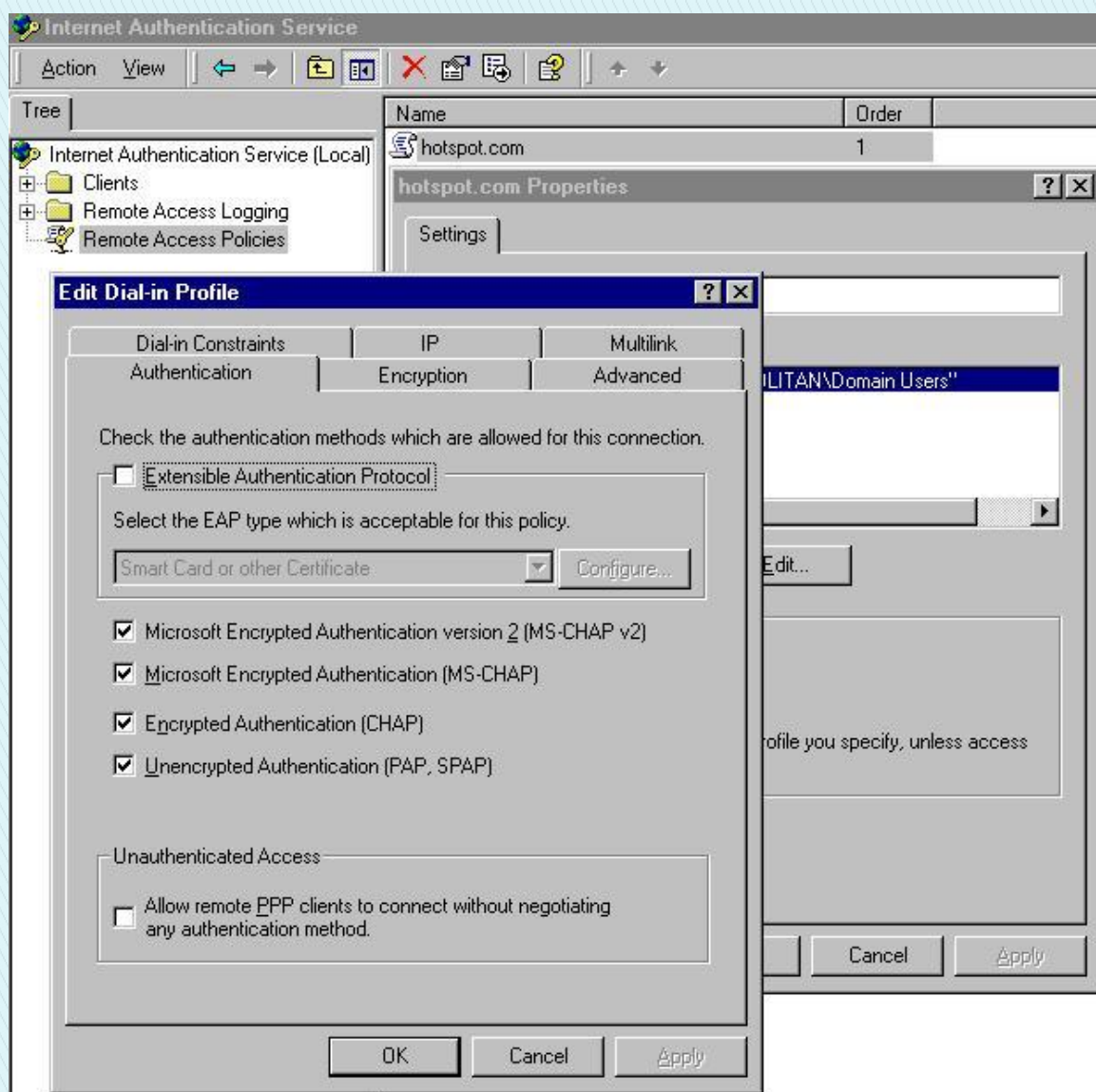
Enable Remote Access Logging check box for all properties.



Select IAS Format and set Log Time Period to Daily.

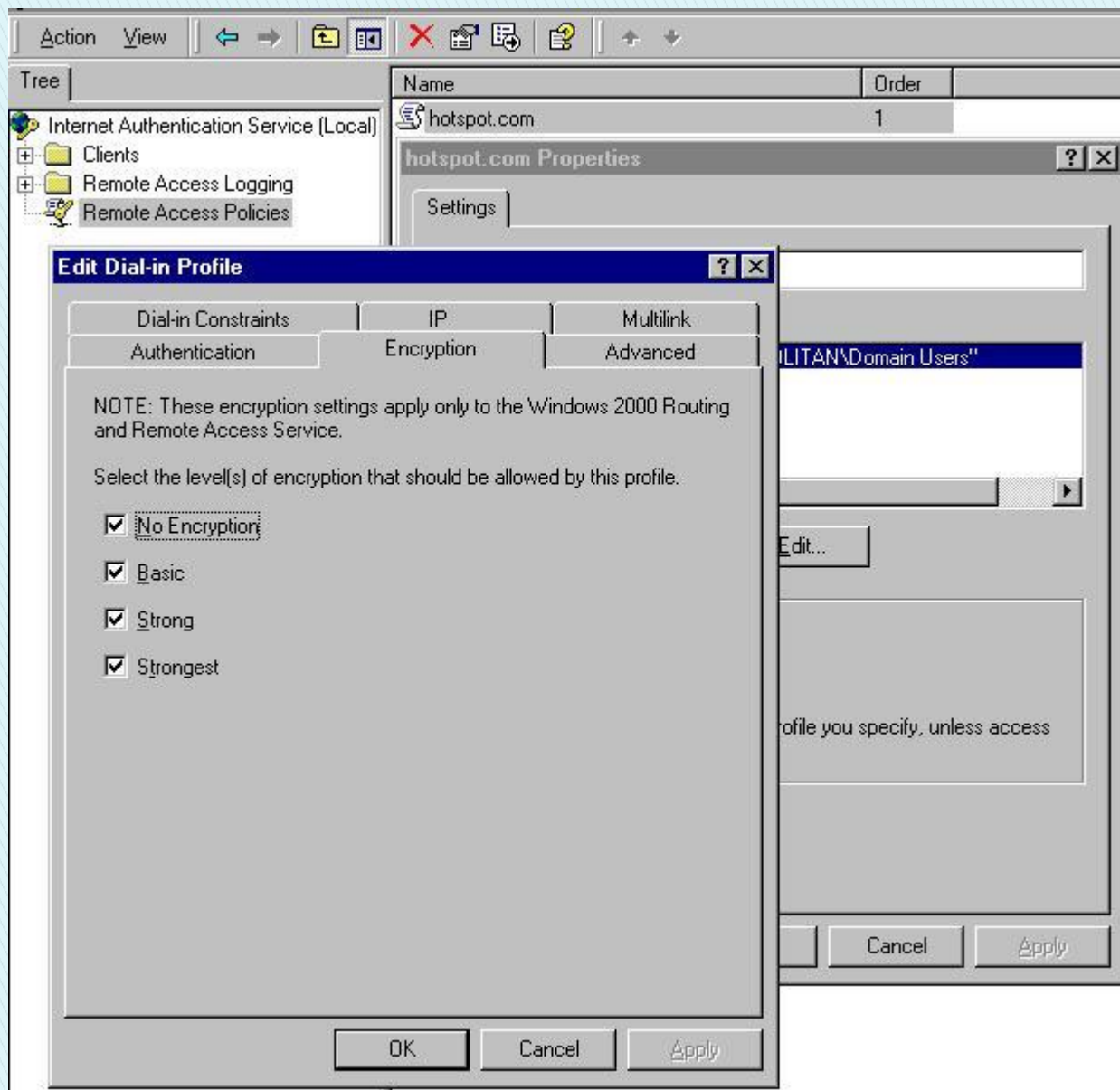


**Create Remote Access Policies profile to “hotspot.com”.
Add “Windows-Groups” matches “DOMAIN\Username”
profile. Enable Grant remote access permission.**



At Authentication tab Enable check box for “MS-CHAP v2, MS-CHAP, CHAP and PAP” method.

Note: HotSpot only uses PAP method.



At Encryption tab Enable all the check box allowed by this profile.

Configuration in Mikrotik

The image shows two windows from the Mikrotik WinBox interface. The left window, titled "Radius", displays a table of RADIUS server profiles. The right window, titled "Radius Server <172.17.8.200>", shows the configuration for a specific server.

#	Service	Called ID	Domain	Address	Secret
1	ADserver IAS RADIUS				
2	hotspot			172.17.8.200	MetroHotSpotDotCom01102006
3	CMSserver IAS RADIUS				
4	hotspot			172.16.8.206	MetroHotSpotDotCom01102006

The right window shows the configuration for the selected server. The "hotspot" service is checked. The "Address" field is set to 172.17.8.200, and the "Secret" field is set to MetroHotSpotDotCom01102006. The "Authentication Port" is set to 1812, and the "Accounting Port" is set to 1813. The "Timeout" is set to 300 ms. The "Accounting Backup" checkbox is unchecked. The "Realm" field is empty. The status of the server is "disabled".

Add a RADIUS server profile and enable service for “hotspot”. Enter IP Address of IAS RADIUS server. Enter the same password created earlier for RADIUS secret. Use port 1812 for Authentication and 1813 for Accounting with Timeout at 300ms.

Name	DNS Name	HTML Directory	Rate Limit
* default	metrohotspot.com	hotspot	
hsprof1	metrohotspot.com	hotspot	

Hotspot Server Profile <hsprof1>

General Login RADIUS

- Login By -

MAC Cookie

HTTP CHAP HTTPS

HTTP PAP Trial

HTTP Cookie Lifetime: 3d 00:00:00

SSL Certificate: none

Split User Domain

Trial Uptime Limit: 00:30:00

Trial Uptime Reset: 1d 00:00:00

Trial User Profile: default

OK
Cancel
Apply
Copy
Remove

At “Hotspot Server Profiles” Login By check “HTTP PAP” only.

Name	DNS Name	HTML Directory	Rate Limit
* default	metrohotspot.com	hotspot	
hsprof1	metrohotspot.com	hotspot	

Hotspot Server Profile <hsprof1>

General Login RADIUS

Use RADIUS

Default Domain: _____

Location ID: _____

Location Name: _____

Accounting

Interim Update: _____

NAS Port Type: 19 (wireless-802.11)

OK
Cancel
Apply
Copy
Remove

At “Hotspot Server Profiles” check Use RADIUS and Accounting. NAS Port Type leave it as (19 wireless-802.11) or change to 15 (Ethernet) mode

MikroTik



Thanks for your attention !

Any Question ?