



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










القنوات اللاسلكية للإتصالات

www.wifi-wimax.com.sa

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

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

مرحباً بك في شبكة القنوات اللاسلكية للإتصالات لتقديم خدمة الإنترنت

EnGenius ECP600

الآن وصل حديثاً

يتميز بشحن مزدوج - مثقف جداً بت
سرعة نقل عالية - متفاحة لأمر

- Dual Band
- 2.4Ghz + 5Ghz
- 300+300Mbps
- Gigabit Port
- POE 802.3at
- E2 Controller
- up to 2* 0dbm
- 5GHz
- VLAN
- Multi SSID

MUM SAUDI ARABIA

RIYADH, OCTOBER 22, 2017

UniFi-AC

الآن وصل حديثاً

أول أكسس بوينت يعمل بنظام AC

- 802.11ac Technology
- Dual Band 2.4Ghz and 5Ghz
- 460Mbps in 2.4Ghz
- 1300Mbps in 5Ghz
- 2600m in 2.4Ghz and 5Ghz
- 3x3 MIMO
- 2 Gigabit Ethernet Port
- POE 802.3at
- Zero Hand-off Technology
- Management Software
- VLAN
- Multi SSID

للتواصل معنا :

0590076820

	اسم المستخدم (username)\$
	كلمة المرور
OK	

www.wifi-wimax.com.sa

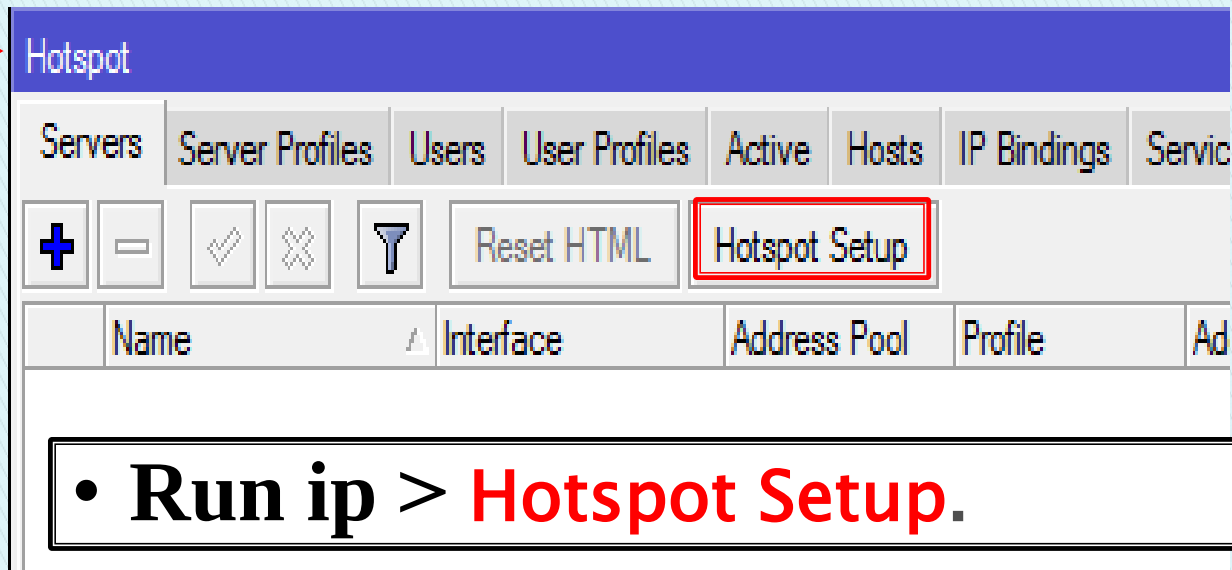
القنوات اللاسلكية للإتصالات

Hotspot Requirements

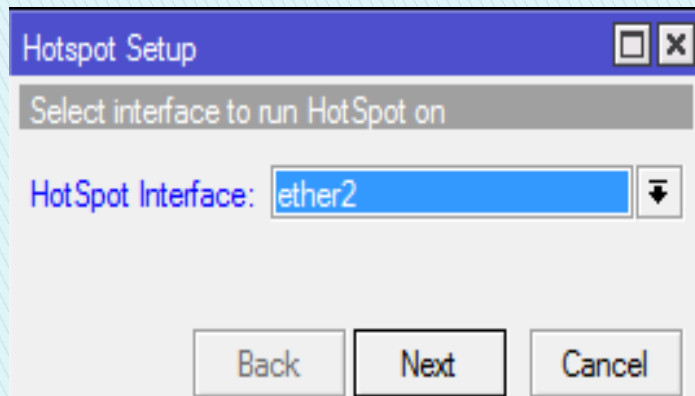
- **Valid IP addresses on Internet and Local Interfaces.**
- **DNS servers addresses added to ip dns.**
- **At least one HotSpot user.**

Hotspot Wizard

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



Hotspot Setup



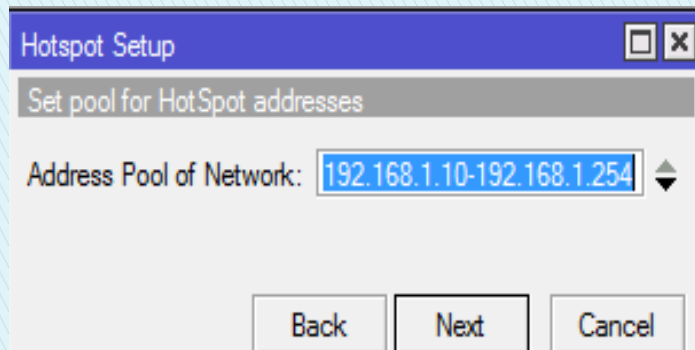
Hotspot Setup

Select interface to run HotSpot on

HotSpot Interface: ether2

Back Next Cancel

1. Select Interface to run HotSpot on.



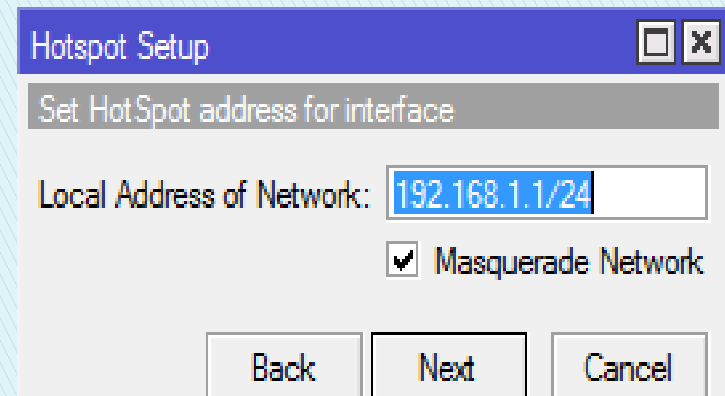
Hotspot Setup

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

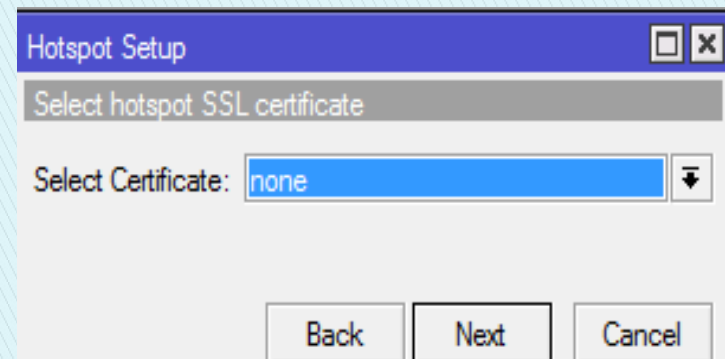
Set HotSpot address for interface

Local Address of Network: 192.168.1.1/24

☒ Masquerade Network

Back Next Cancel

2. HotSpot address will be selected automatically.



Hotspot Setup

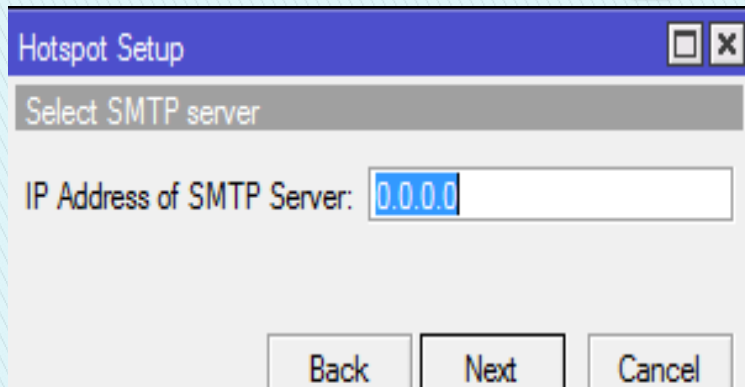
Select hotspot SSL certificate

Select Certificate: none

Back Next Cancel

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

Hotspot Setup



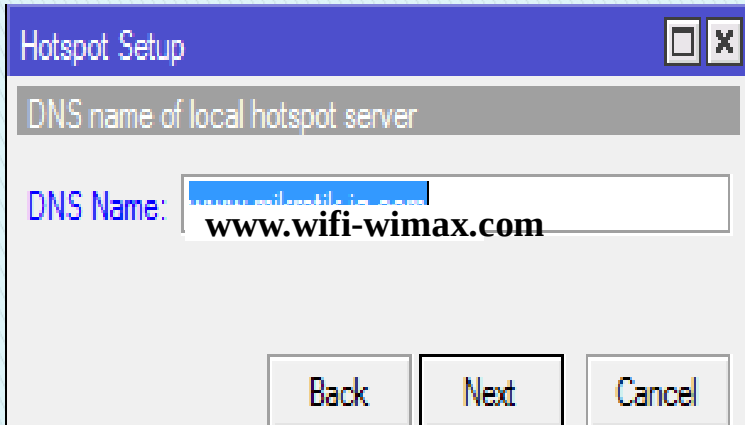
Hotspot Setup

Select SMTP server

IP Address of SMTP Server:

Back Next Cancel

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



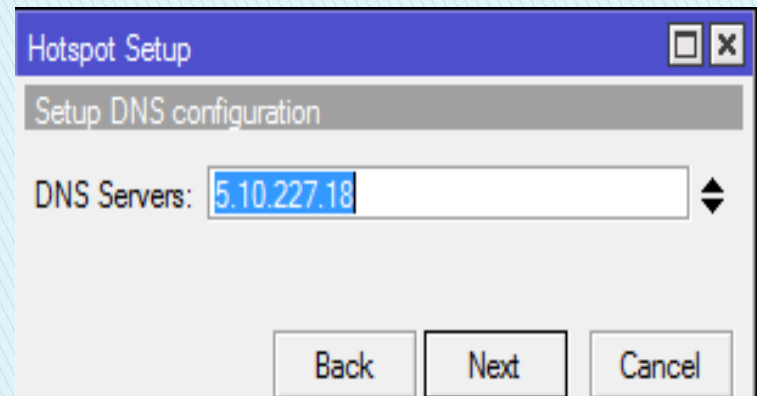
Hotspot Setup

DNS name of local hotspot server

DNS Name:

Back Next Cancel

7. DNS name for HotSpot server



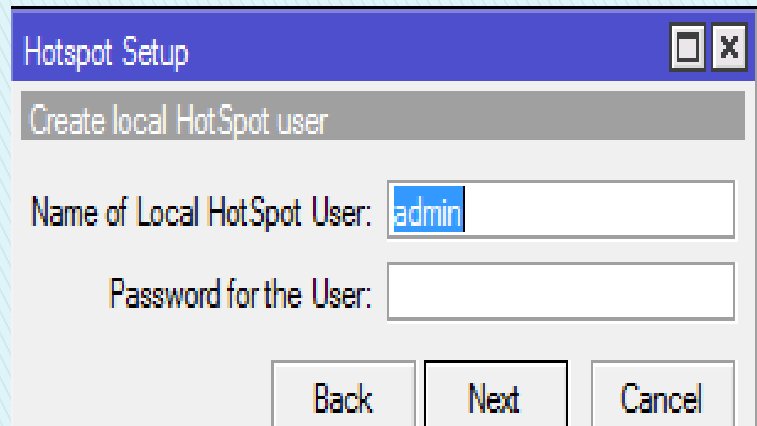
Hotspot Setup

Setup DNS configuration

DNS Servers:

Back Next Cancel

6. Insert DNS ip address or use router DNS.



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

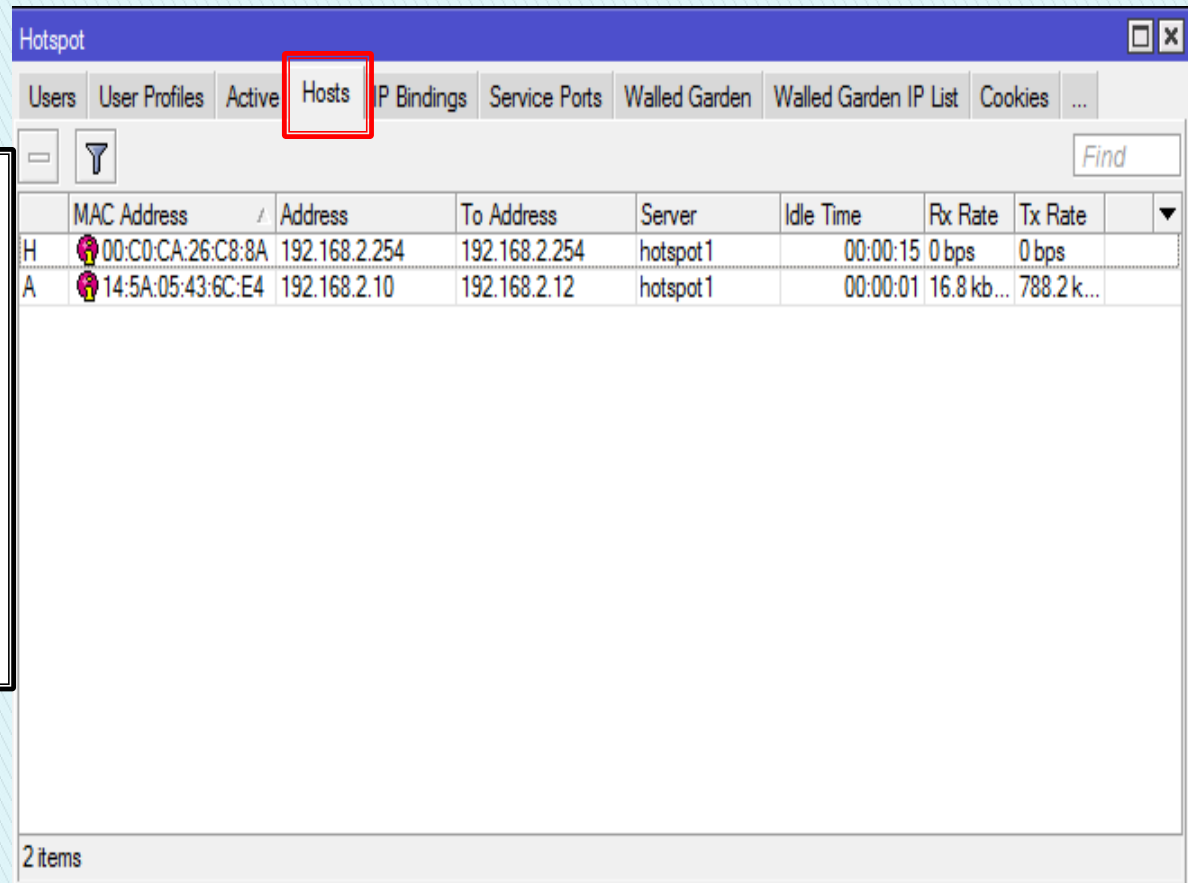
- Users connected to HotSpot interface will be disconnected from the Internet.
- Client will have to authorize in HotSpot to get access to Internet.
- Remember you cant search or enter to router by using WinBox or CLI through interface configured as Hotspot server.
- HotSpot default setup creates additional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



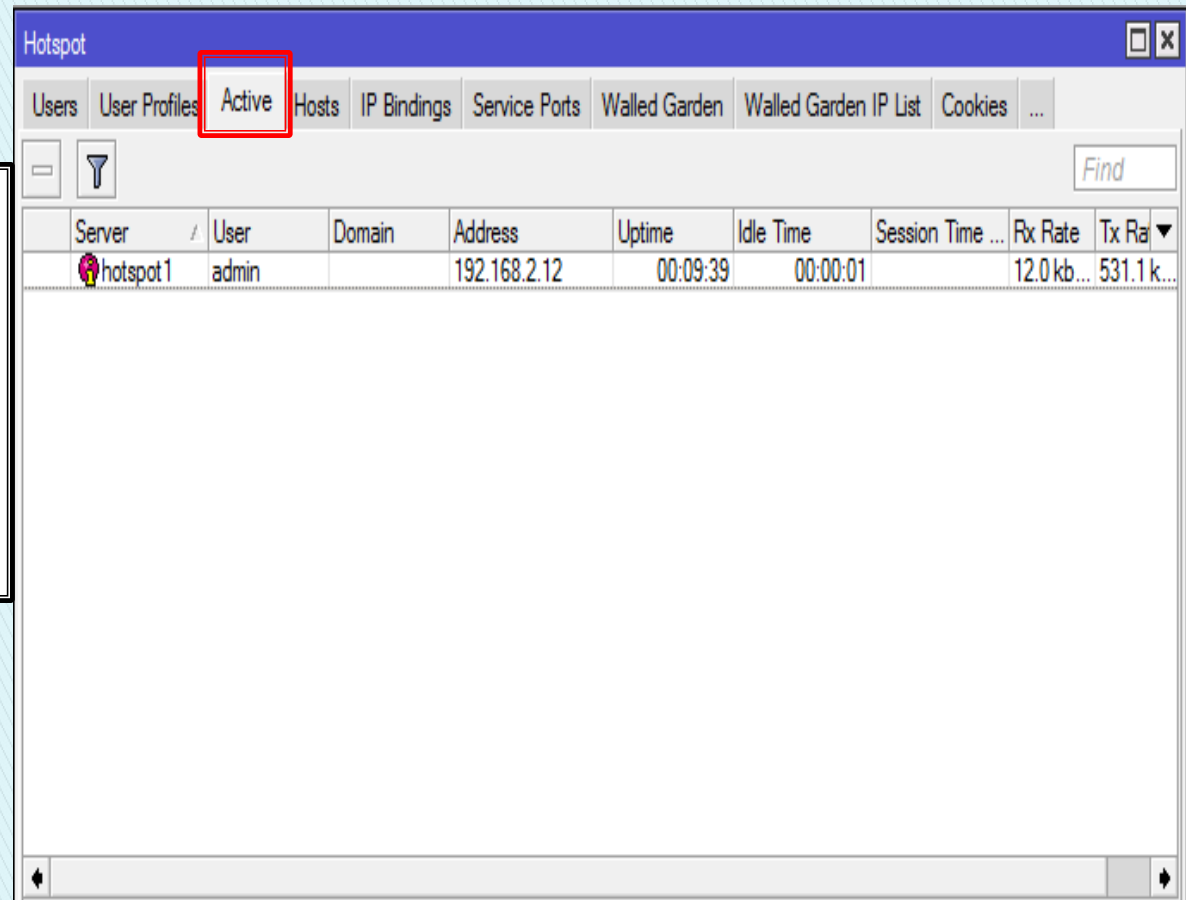
	MAC Address	Address	To Address	Server	Idle Time	Rx Rate	Tx Rate
H	00:C0:CA:26:C8:8A	192.168.2.254	192.168.2.254	hotspot1	00:00:15	0 bps	0 bps
A	14:5A:05:43:6C:E4	192.168.2.10	192.168.2.12	hotspot1	00:00:01	16.8 kb...	788.2 k...

2 items

- Information about clients connected to HotSpot router.

HotSpot Active Table

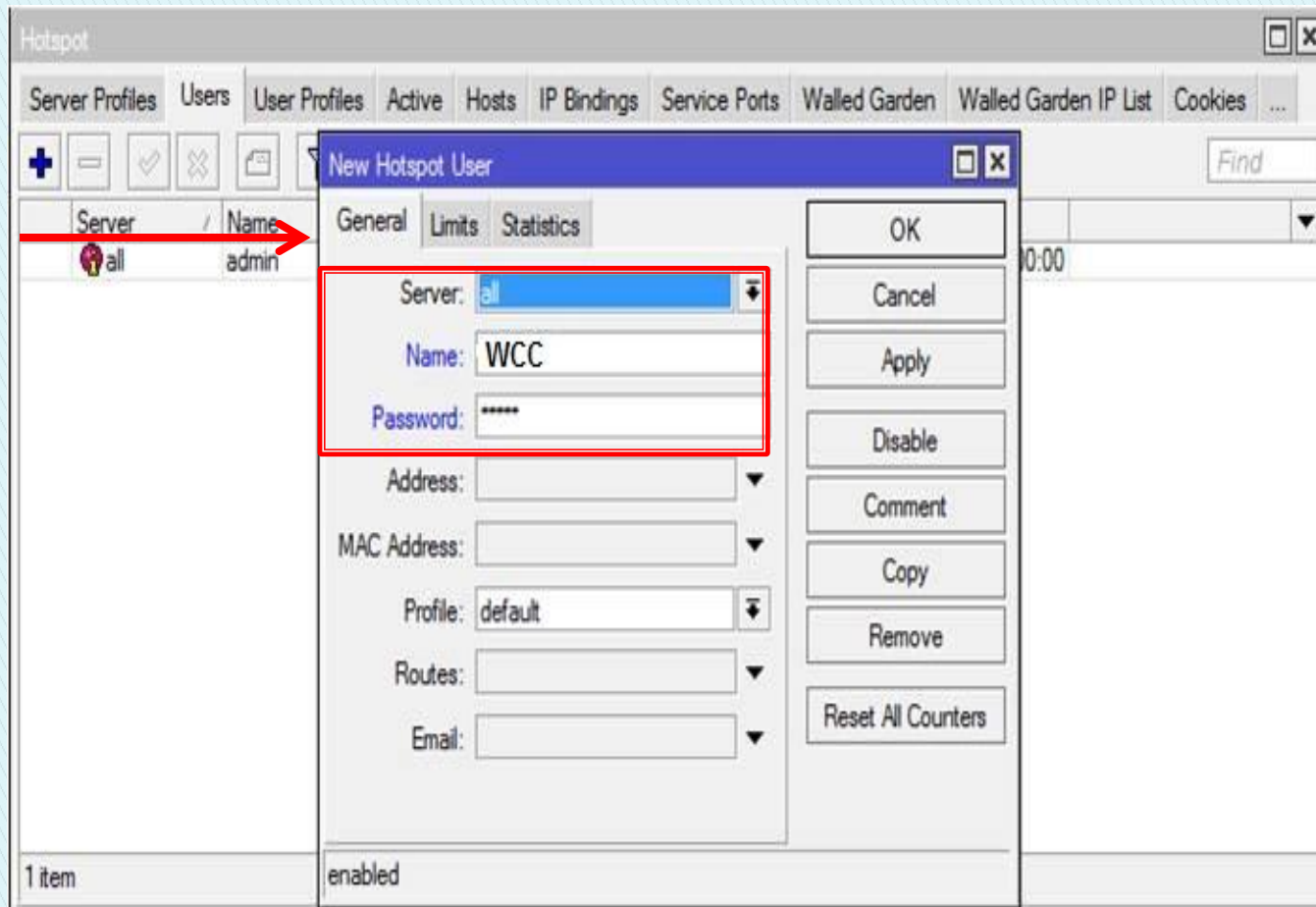
**Information
about connected
person appear at
active sub menu.**



Server	User	Domain	Address	Uptime	Idle Time	Session Time ...	Rx Rate	Tx Ra
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



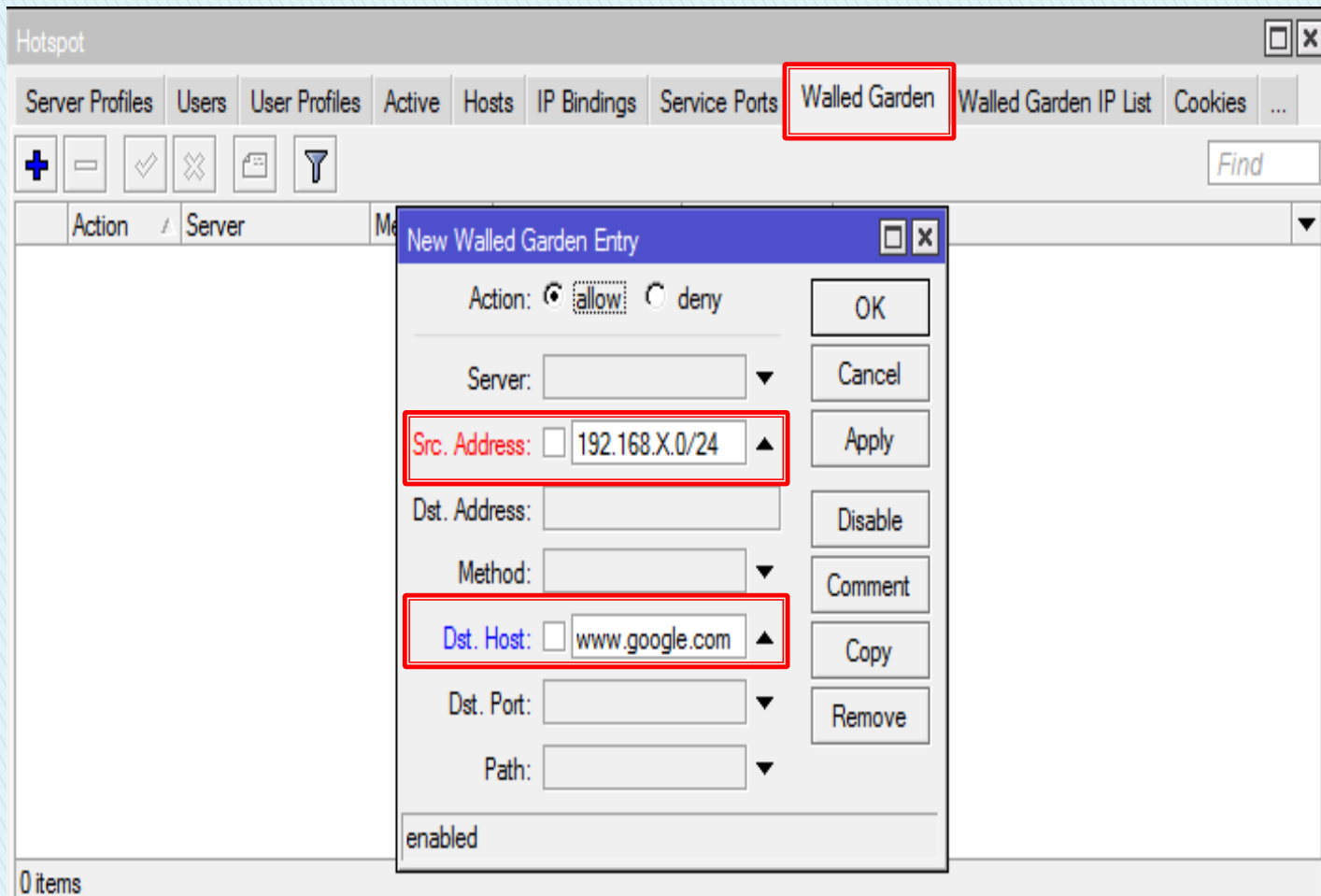
- Add/Edit/Remove HotSpot users.

Advance Features

HotSpot Walled-Garden

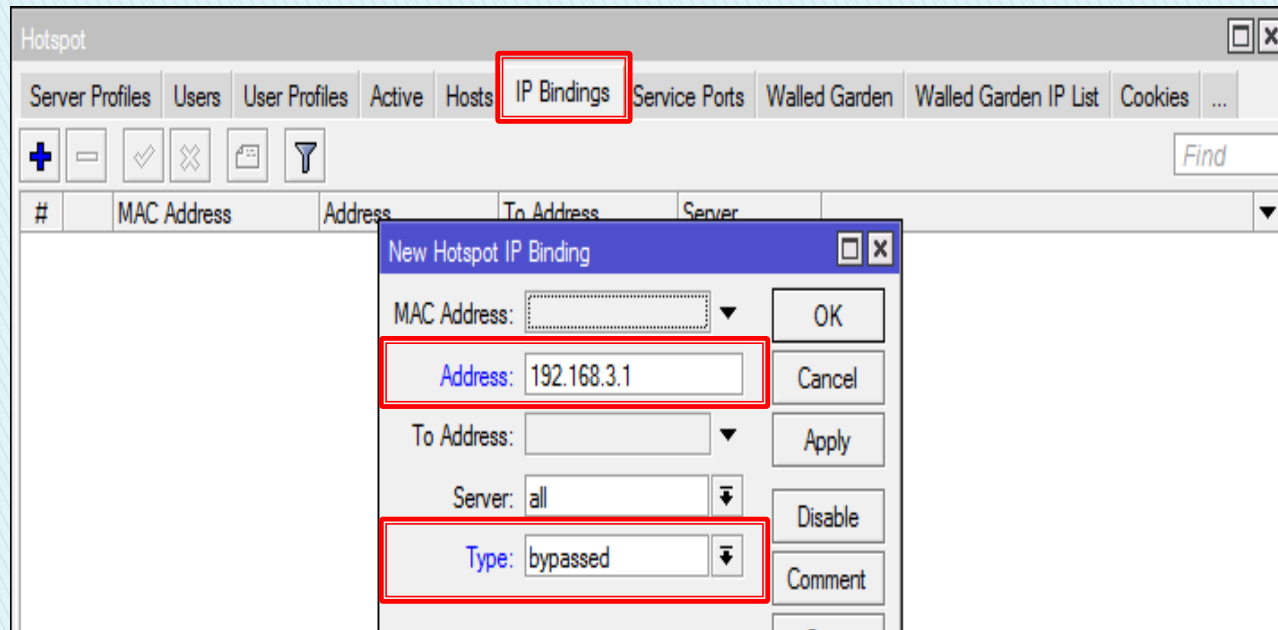
- **Tool to get access to specific resources without HotSpot authorization.**
- **Specific resources could be local web server or external web page like (www.mikrotik.com).**
- **Walled-Garden for HTTP and HTTPS.**
- **Walled-Garden IP for other resources (Telnet, SSH, Winbox, etc).**

HotSpot Walled-Garden



- Allow access to google.com

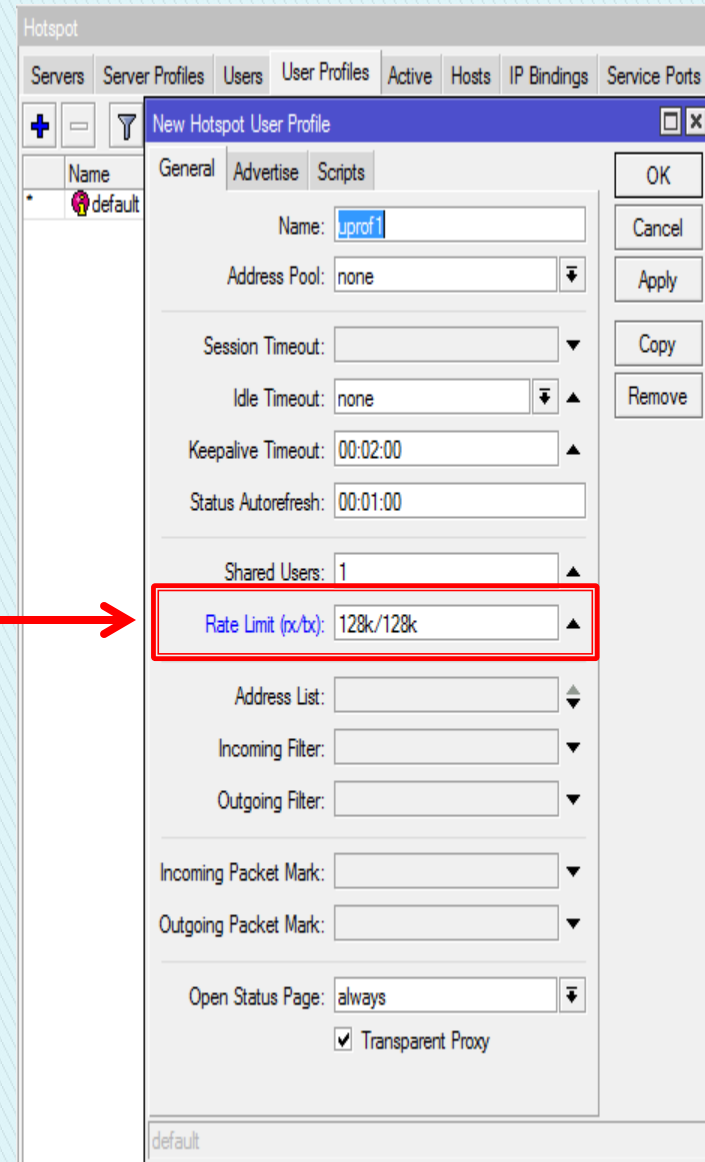
Bypass HotSpot



- 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

+ - Filter

New Hotspot User Profile

General Advertise Scripts

Name: uprof1

Address Pool: none

Session Timeout: [dropdown]

Idle Timeout: none

Keepalive Timeout: 00:02:00

Status Autorefresh: 00:01:00

Shared Users: 1

Rate Limit (x/bx): 128k/128k

Address List: [dropdown]

Incoming Filter: [dropdown]

Outgoing Filter: [dropdown]

Incoming Packet Mark: [dropdown]

Outgoing Packet Mark: [dropdown]

Open Status Page: always

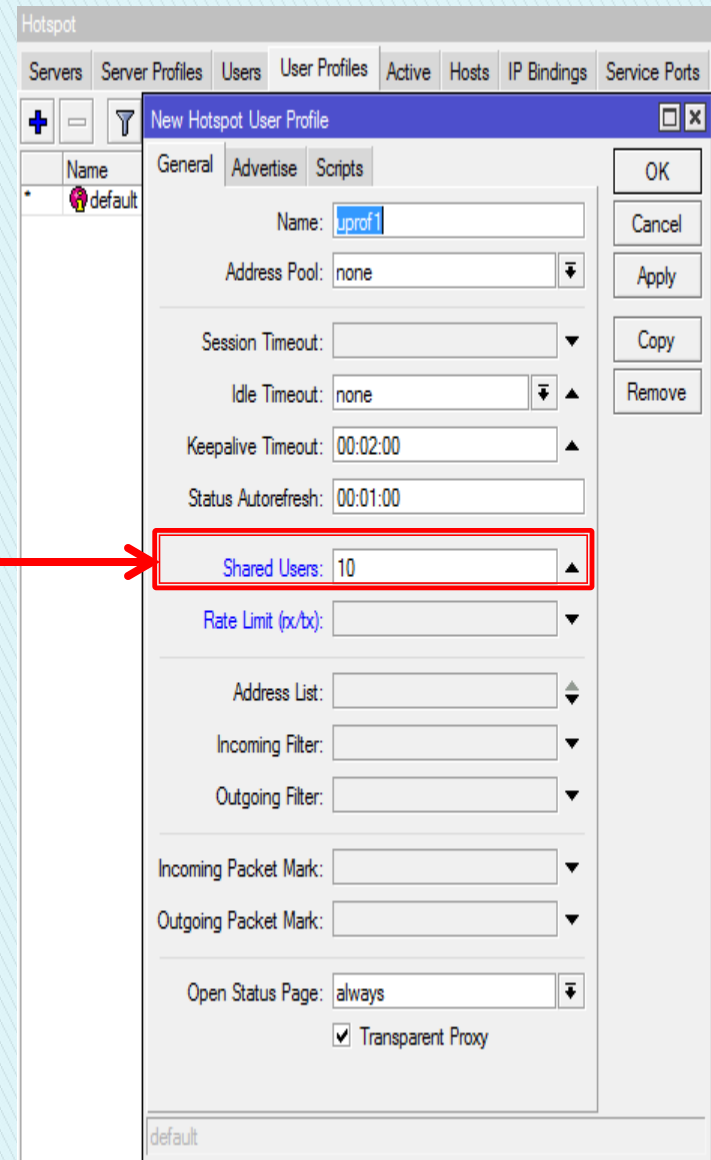
☒ Transparent Proxy

OK Cancel Apply Copy Remove

default

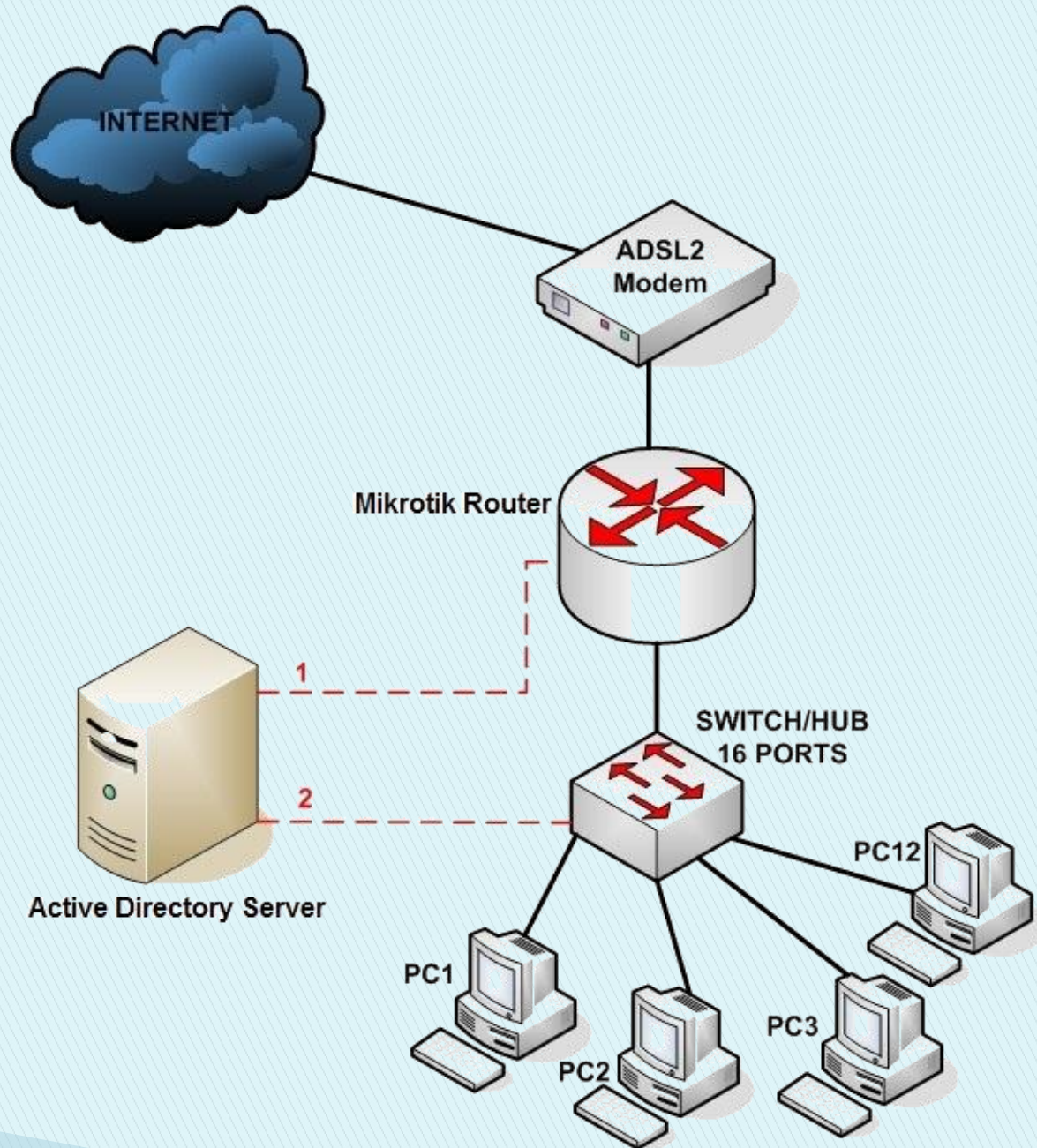
HotSpot Shared users

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

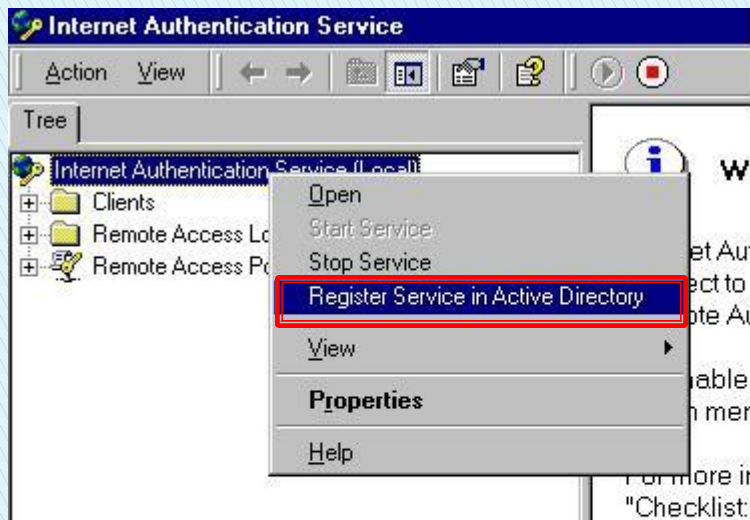


The screenshot shows the 'New Hotspot User Profile' dialog box in Mikrotik WinBox. The 'General' tab is selected. The 'Name' field is 'uprof1'. The 'Address Pool' is 'none'. The 'Session Timeout' is empty. The 'Idle Timeout' is 'none'. The 'Keepalive Timeout' is '00:02:00'. The 'Status Autorefresh' is '00:01:00'. The 'Shared Users' field is highlighted with a red box and a red arrow pointing to it from the text box on the left. The 'Shared Users' field is set to '10'. Below it, the 'Rate Limit (px/bx)' is empty. The 'Address List' is empty. The 'Incoming Filter' is empty. The 'Outgoing Filter' is empty. The 'Incoming Packet Mark' is empty. The 'Outgoing Packet Mark' is empty. The 'Open Status Page' is 'always'. The 'Transparent Proxy' checkbox is checked. The 'OK', 'Cancel', 'Apply', 'Copy', and 'Remove' buttons are on the right.

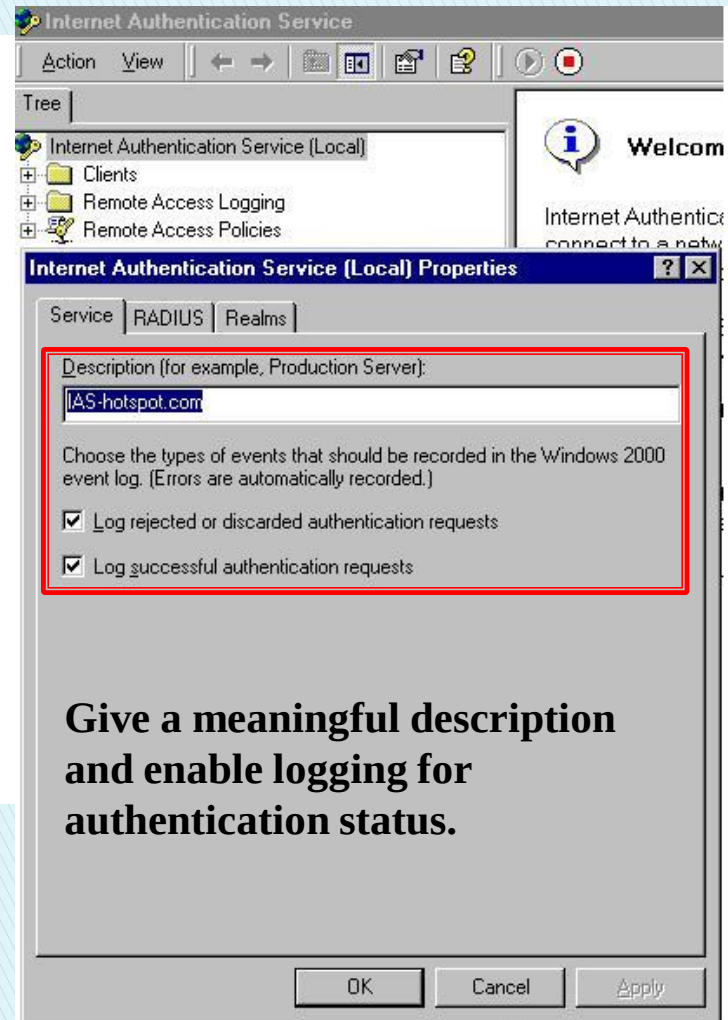
Hotspot Integration with Active Directory



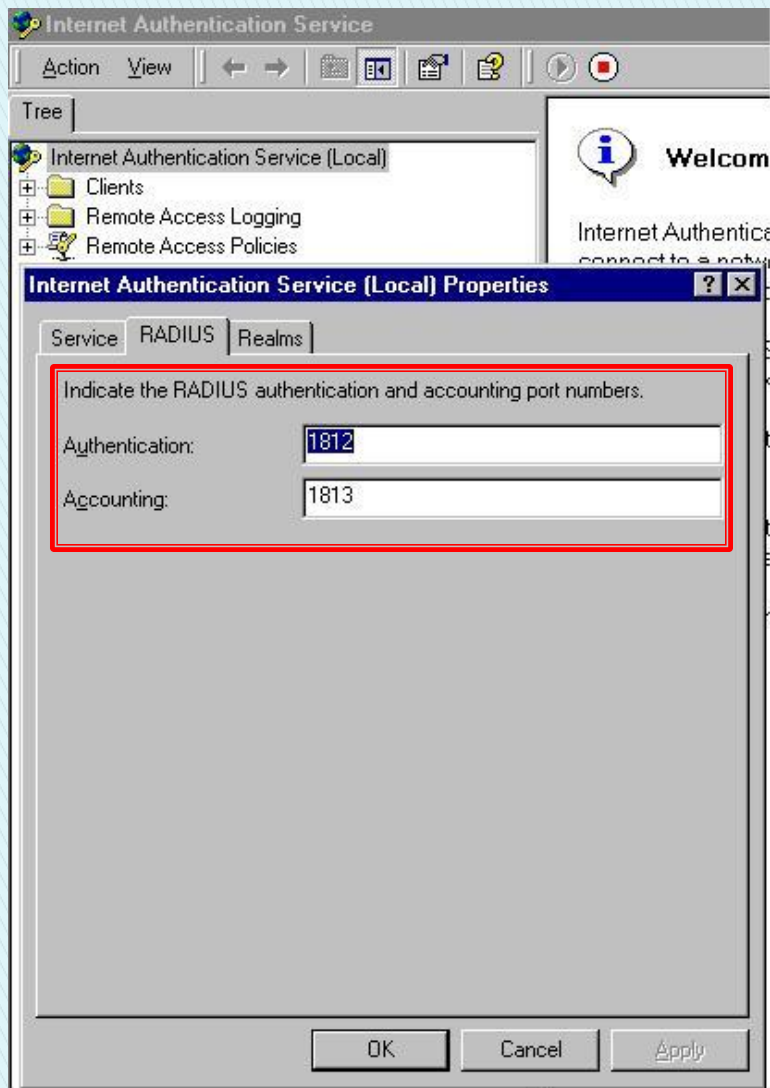
Configuration in Microsoft windows server



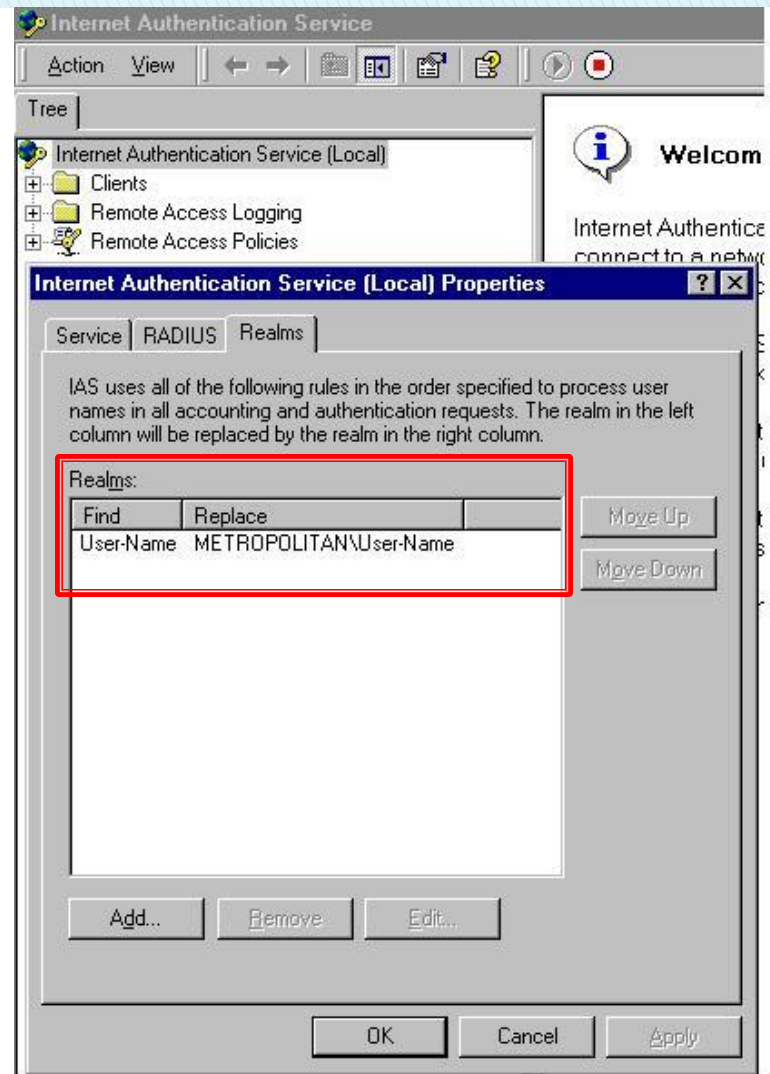
Setup IAS on a server acting as Active Directory Services Domain Controller and register it's services.



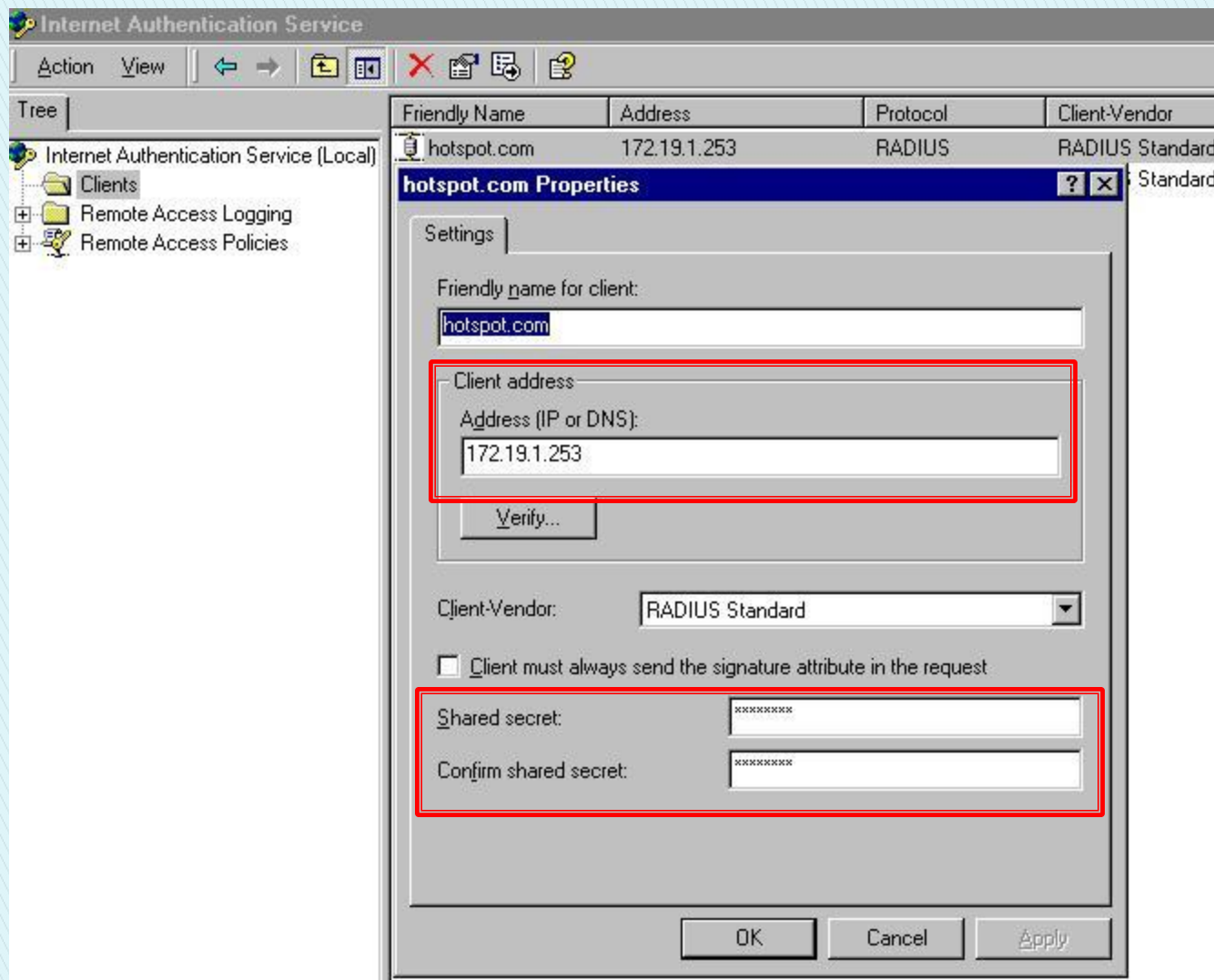
Give a meaningful description and enable logging for authentication status.



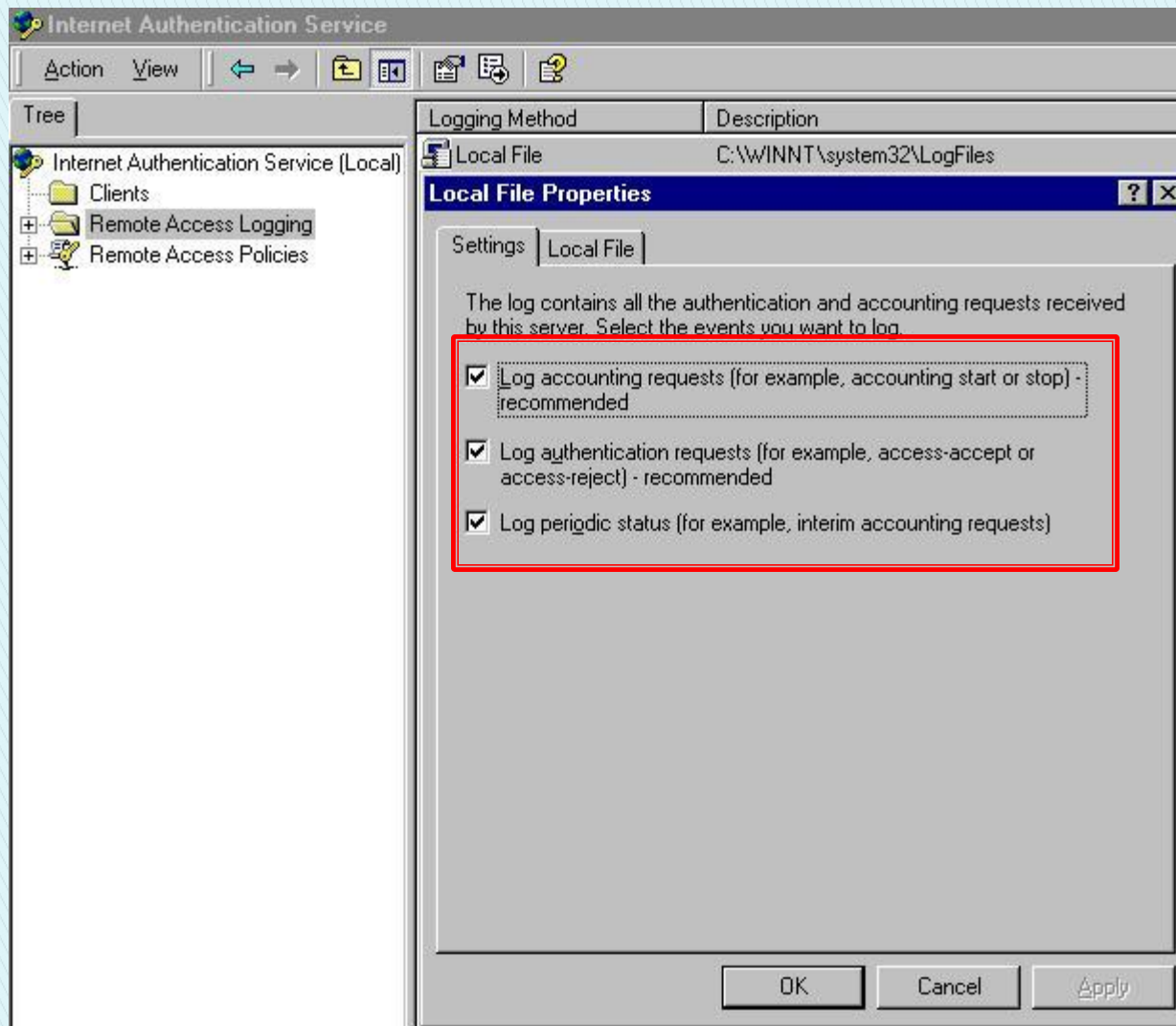
User respective 1812 for Authentication and 1813 for Accounting port only.



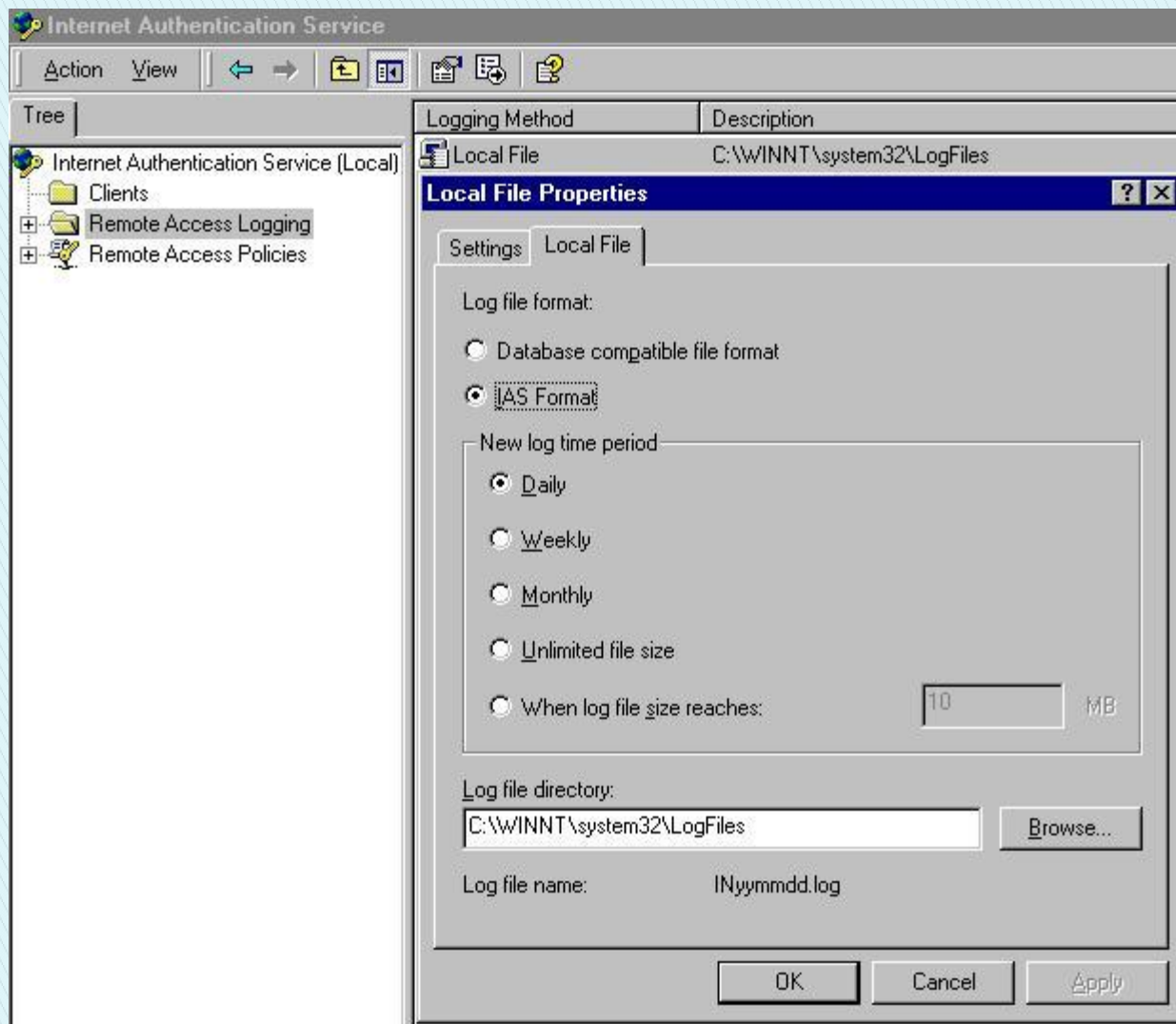
Create a Realms profile, find “User-Name” replace it with “DOMAIN\User-Name” variables into IAS.



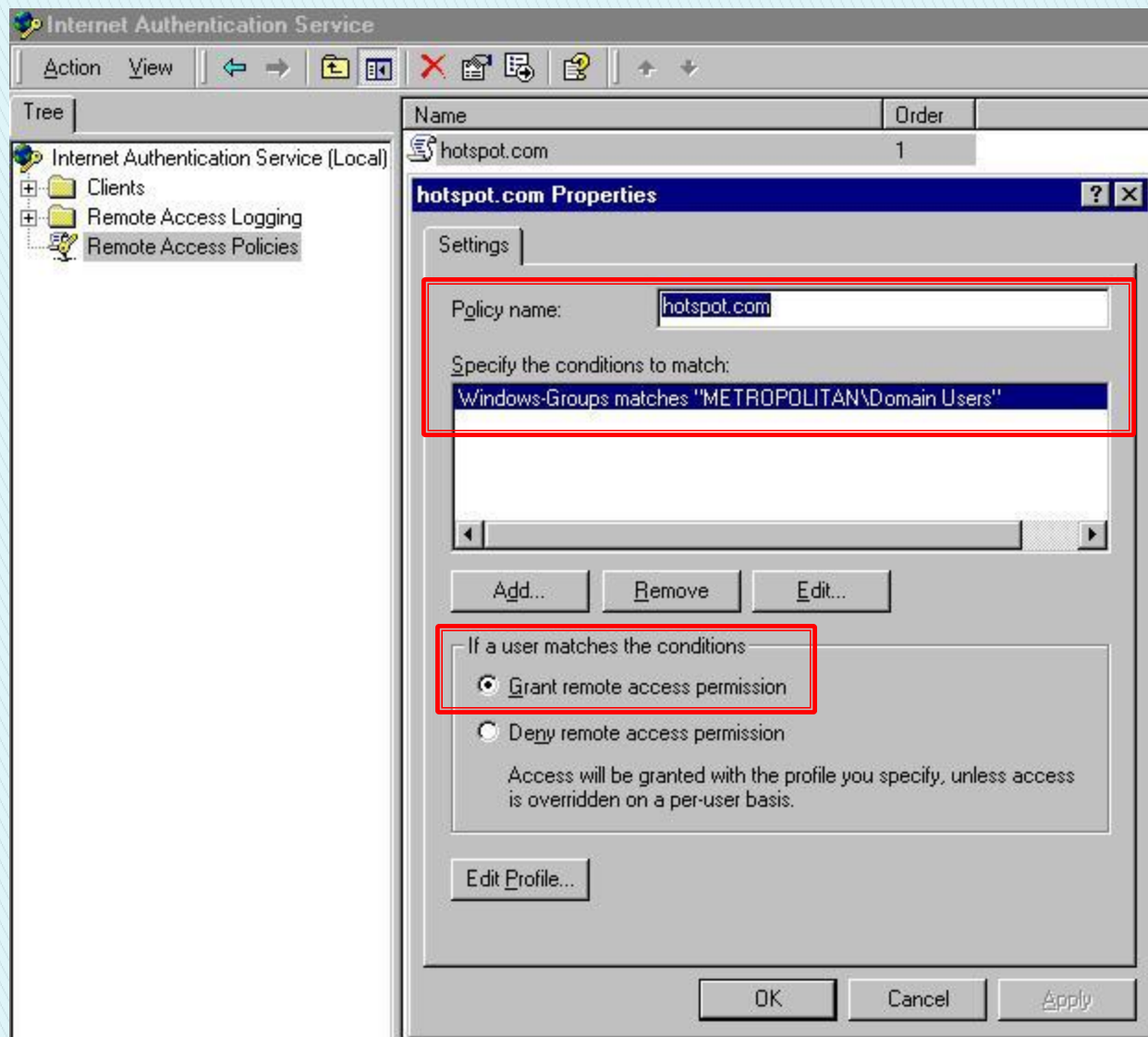
Create a “hotspot.com” client profile and set IP address pointing to MikroTik hotspot server 172.19.1.253 Set Client Vendor to RADIUS Standard and enter a unique password for IAS. Do not enable Attributes Signature check box.



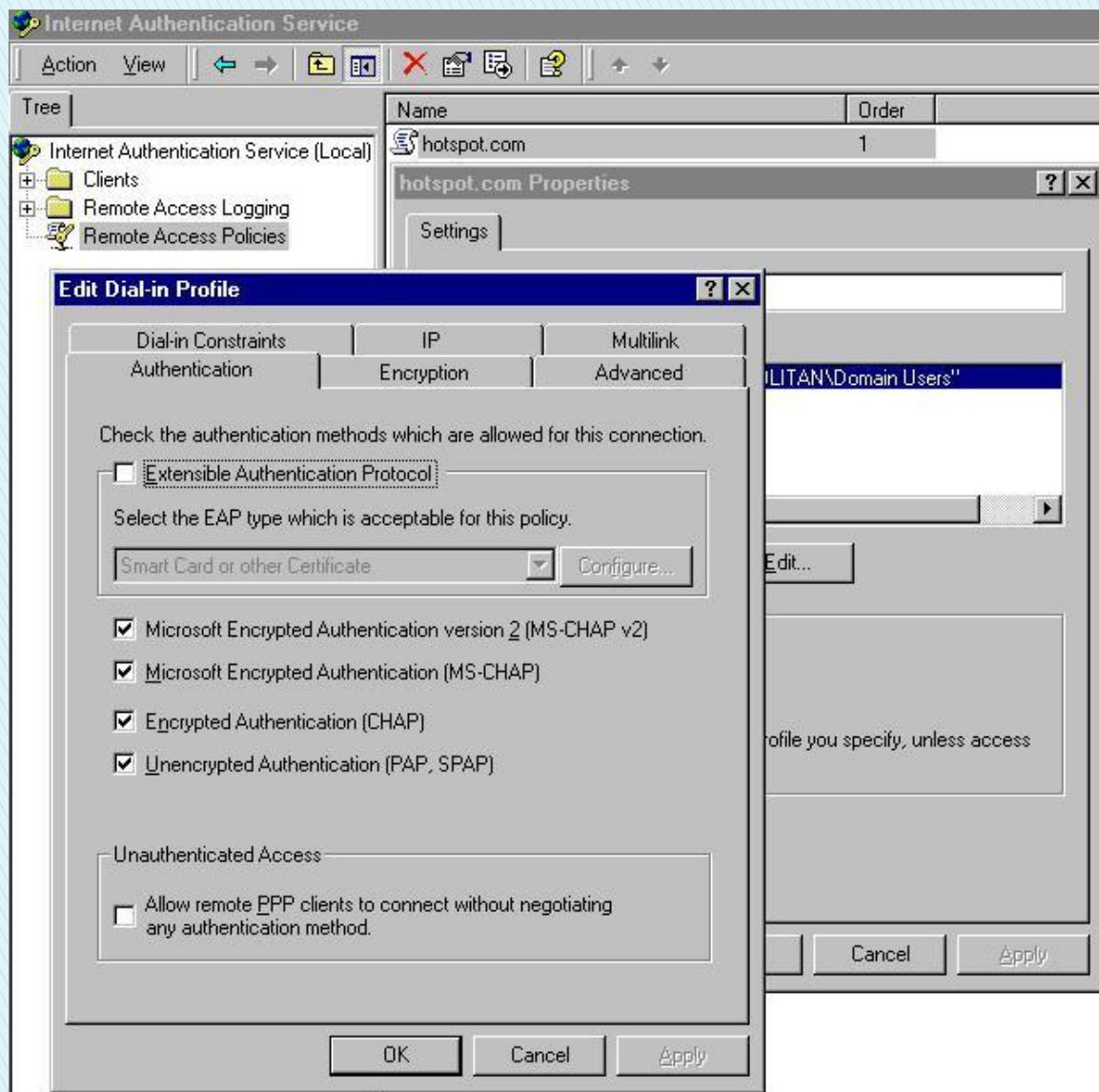
Enable Remote Access Logging check box for all properties.



Select IAS Format and set Log Time Period to Daily.

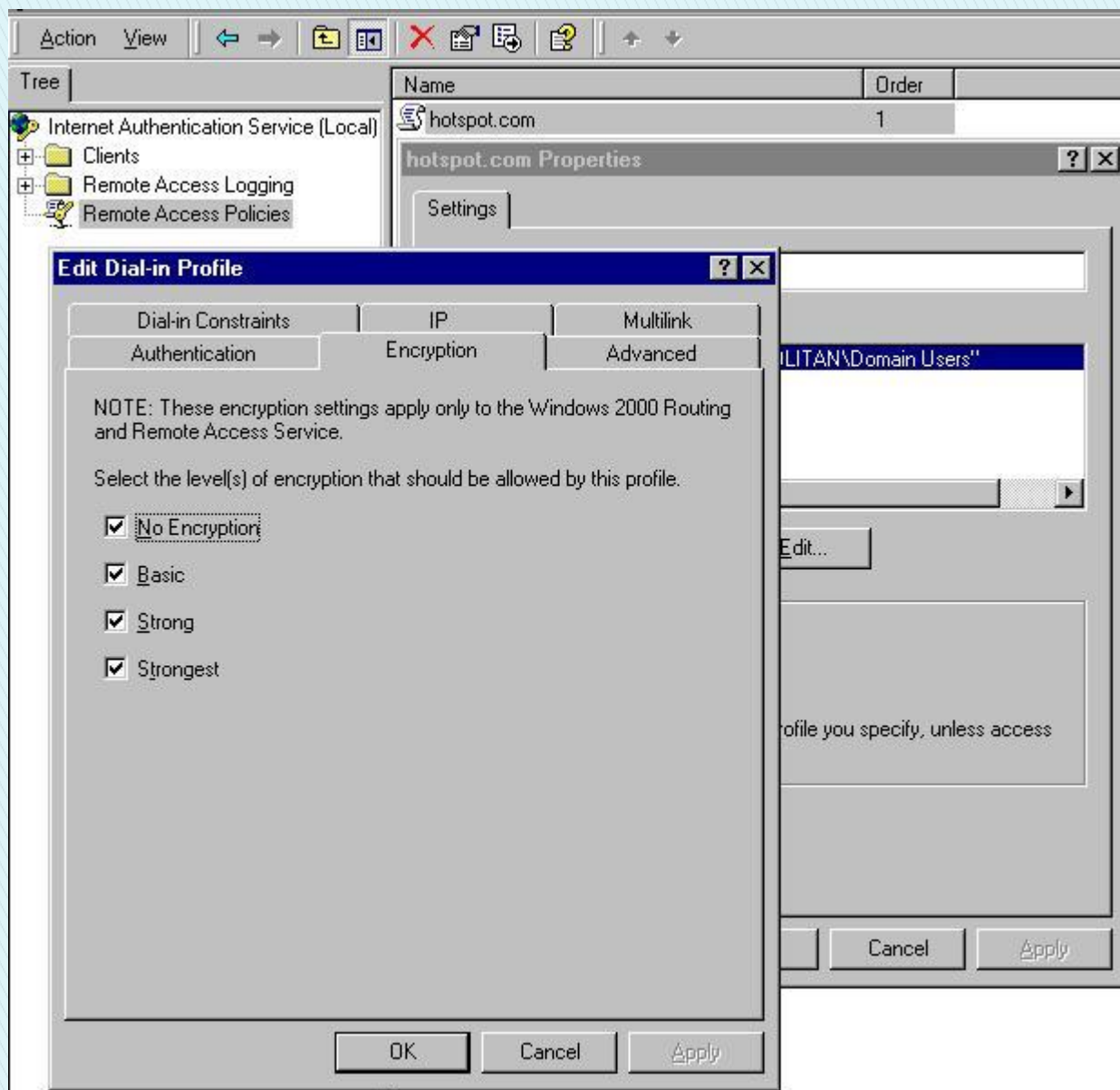


**Create Remote Access Policies profile to “hotspot.com”.
Add “Windows-Groups” matches “DOMAIN\Username”
profile. Enable Grant remote access permission.**



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.

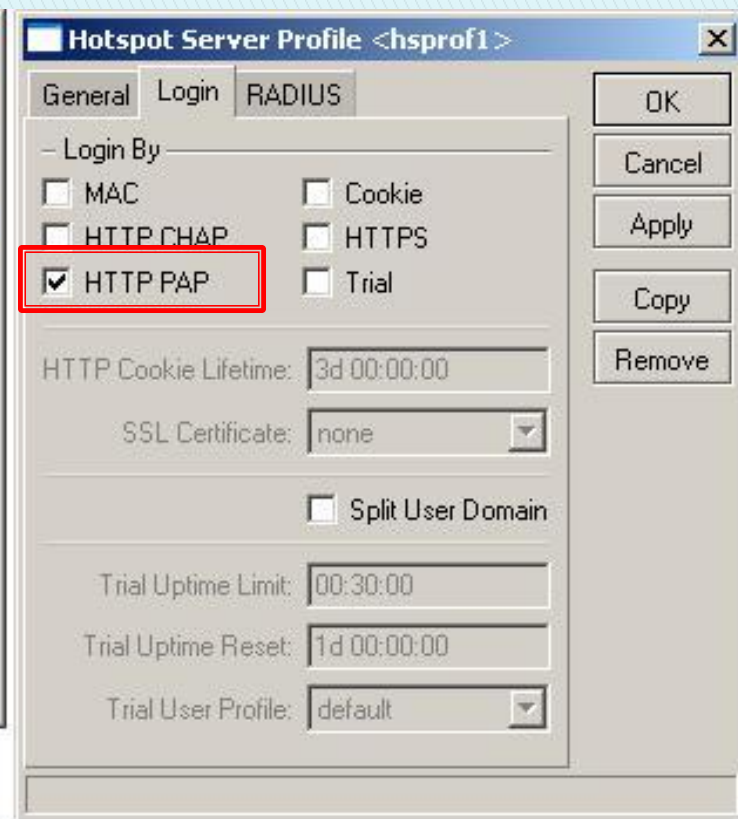
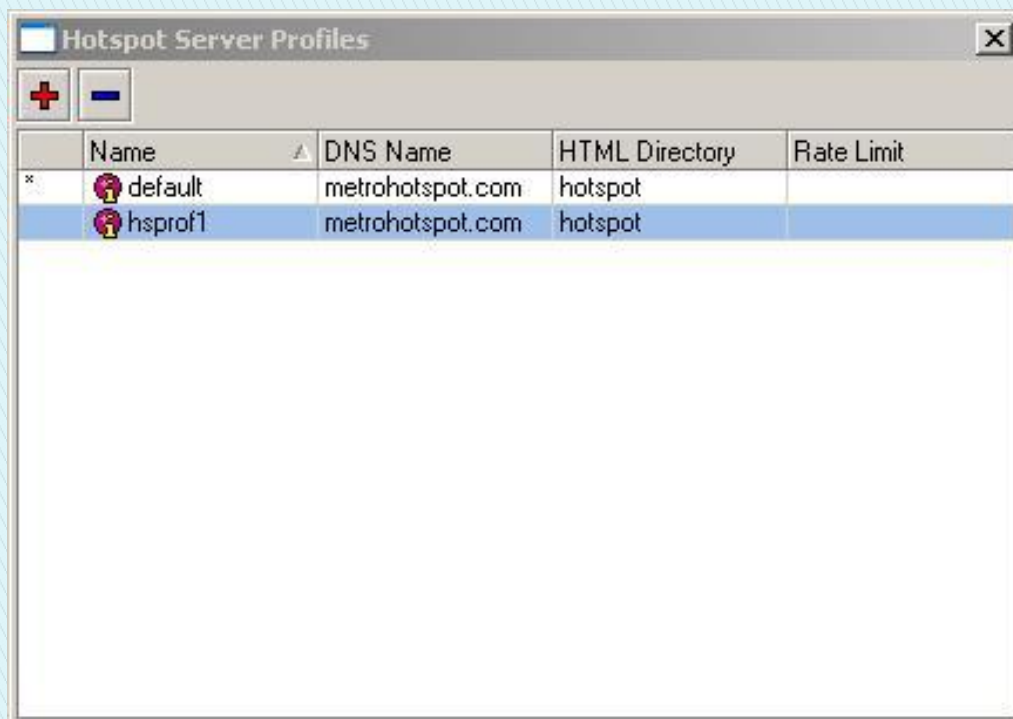
Configuration in Mikrotik

The screenshot displays two windows from the Mikrotik WinBox interface. The left window, titled 'Radius', shows a table of configured Radius servers. The right window, titled 'Radius Server <172.17.8.200>', shows the configuration details for a specific server.

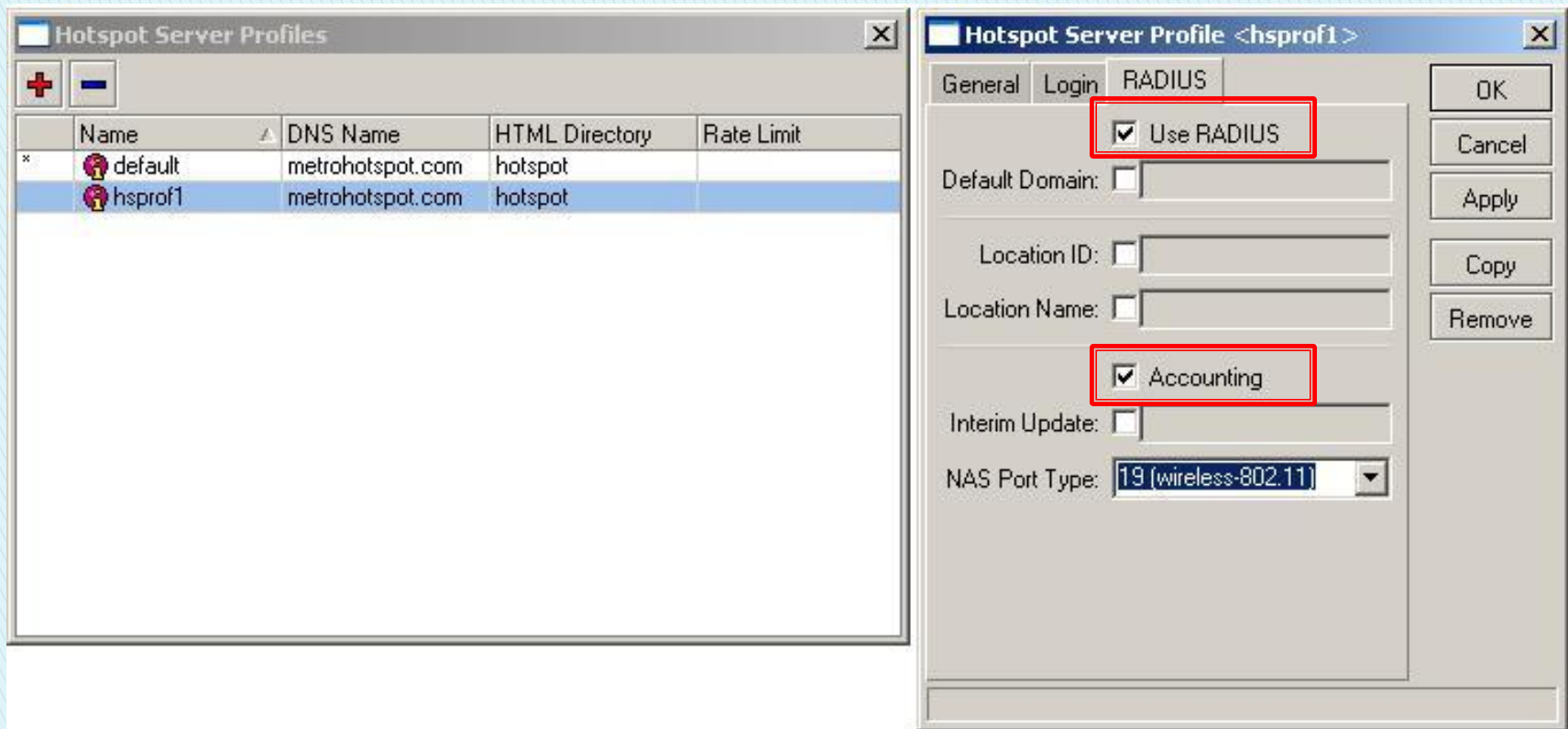
#	Service	Called ID	Domain	Address	Secret
1	ADserver IAS RADIUS				
2	hotspot			172.17.8.200	MetroHotSpotDotCom01102006
3	CMSserver IAS RADIUS				
4	hotspot			172.16.8.206	MetroHotSpotDotCom01102006

The right window shows the configuration for the Radius server at 172.17.8.200. The 'General' tab is selected. The 'Service' section has 'hotspot' checked. The 'Called ID' and 'Domain' fields are empty. The 'Address' field is 172.17.8.200. The 'Secret' field is MetroHotSpotDotCom01102006. The 'Authentication Port' is 1812. The 'Accounting Port' is 1813. The 'Timeout' is 300 ms. The 'Accounting Backup' checkbox is unchecked. The 'Realm' field is empty. The status 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.



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



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



Thanks for your attention !

Any Question ?