explain me about mikrotik ip → hotspot menu

what is any tab uses, logic behind it

The MikroTik **IP > Hotspot** menu is a comprehensive interface in RouterOS for configuring and managing captive portal (Hotspot) services. This system is widely used to control, authenticate, and monitor network access, often in public or guest Wi-Fi environments. Below is a detailed explanation of each main tab/menu, their uses, and the logic behind them.

Main Tabs and Their Functions

1. Servers

- **Purpose:** Lists and manages Hotspot servers running on router interfaces.
- **Logic:** Each interface (Ethernet, wireless, VLAN, or bridge) can have one Hotspot server. This is where you add, remove, or configure which interface runs a Hotspot instance. You usually run the setup wizard here to initialize all necessary settings for a new Hotspot[1] [2] [3].

2. Server Profiles

- **Purpose:** Stores configuration profiles for Hotspot servers.
- **Logic:** A profile defines common settings like authentication methods (HTTP PAP, HTTPS, MAC cookie), RADIUS integration, HTML customization, and proxy settings. Multiple servers can share the same profile for consistency[4] [3].

3. Users

- **Purpose:** Manages local Hotspot user accounts.
- **Logic:** Here you create, edit, or remove users, set passwords, assign profiles, and define time or bandwidth limits. These are the credentials users will use to log in via the captive portal[4] [3].

4. User Profiles

- **Purpose:** Defines user group settings and limitations.
- **Logic:** Profiles allow you to group users with similar restrictions (e.g., bandwidth, session time, data cap). Assigning a profile to a user enforces these policies automatically[4].

5. Active

- **Purpose:** Real-time list of authenticated (logged-in) users.
- **Logic:** Shows currently connected users, their IP/MAC, session duration, and usage. Useful for monitoring and troubleshooting connected clients[4] [3].

6. Hosts

- **Purpose:** Lists all detected devices on the Hotspot-enabled interfaces, regardless of authentication status.
- **Logic:** Displays both authenticated and unauthenticated devices, their IP/MAC, and status flags (like D, AD, DH, etc.). This helps you see who is connected and their current state in the Hotspot process[5] [4].

7. IP Binding

- **Purpose:** Sets static rules for specific clients.
- **Logic:** You can bypass Hotspot authentication for certain devices (type=bypassed), block them (type=blocked), or apply 1:1 NAT translations. This is useful for exceptions like printers or admin devices[1] [2].

8. Walled Garden

- **Purpose:** Allows unauthenticated access to specific web resources.
- **Logic:** You can whitelist certain domains or URLs (HTTP-level) so users can access them without logging in. Useful for free access to company websites, payment portals, etc.[4] [3].

9. Walled Garden IP

- **Purpose:** Similar to Walled Garden, but at the IP/protocol level.
- **Logic:** Allows unauthenticated access to specific IP addresses or protocols, bypassing the captive portal for those destinations[4].

10. Service Ports

- **Purpose:** Manages NAT helpers for specific protocols.
- **Logic:** Ensures proper translation and handling of protocols like FTP, PPTP, etc., for Hotspot clients[4].

11. Cookie

- **Purpose:** Lists valid HTTP cookies for Hotspot authentication.
- **Logic:** Used for MAC cookie or HTTP cookie-based login, allowing devices to re-authenticate automatically within a set timeout[4].

Logic Behind the Hotspot System

- **Captive Portal Workflow:** When a device connects, it is redirected to a login page (unless bypassed or walled gardened). After successful authentication, access is granted according to user profile limits.
- **DHCP Integration:** Hotspot often works with DHCP to assign IPs to clients, but can also change client IPs to fit the Hotspot subnet if needed[1] [2].
- **Authentication:** Supports local users, RADIUS, HTTP/HTTPS, MAC-based login, and cookies for seamless re-login[6] [4].
- **Accounting:** Tracks session time, data usage, and can send this info to a RADIUS server for external management[4].

- **Customization:** Landing/login pages can be customized for branding or additional logic[6] [3].

Summary Table

Tab/Menu	Main Use	Key Logic/Features
Servers	Manage Hotspot instances per interface	One per interface; setup wizard recommended
Server Profiles	Store server settings	Auth methods, RADIUS, HTML, proxy, shared across servers
Users	Manage user accounts	Add/edit/delete users, set limits
User Profiles	Group user settings	Bandwidth, session/data limits, group policies
Active	Show logged-in users	Real-time monitoring
Hosts	Show all detected devices	Authenticated/unauthenticated, status flags
IP Binding	Static rules for devices	Bypass/block/NAT certain clients
Walled Garden	Whitelist domains/URLs	Allow unauthenticated access to specific web resources
Walled Garden IP	Whitelist IPs/protocols	Allow unauthenticated access at IP/protocol level
Service Ports	Protocol helpers	NAT helpers for FTP, PPTP, etc.
Cookie	Manage auth cookies	For seamless re-login (MAC/HTTP cookie)

This modular design allows fine-grained control over network access, user experience, and security in a wide range of deployment scenarios[1] [4] [2] [3].

⁂

1. https://help.mikrotik.com/docs/spaces/ROS/pages/56459266/HotSpot+-+Captive+portal
2. https://wiki.mikrotik.com/Manual:IP/Hotspot
3. https://nds.id/en/interesting-features-and-mikrotik-hotspot-settings/
4. https://wiki.mikrotik.com/Manual:Hotspot_Introduction
5. https://forum.mikrotik.com/viewtopic.php?t=21687
6. https://mum.mikrotik.com/presentations/MY19/presentation_6985_1560751904.pdf