Service Announcements for Hot-Spots: Enabling Automated Access and Provider Selection for (WLAN-based) Voice

2005-05-11 Upperside WiFi Voice 2005

Jörg Ott jo@netlab.hut.fi
Dirk Kutscher dku@tzi.org

Overview

- Brief Introduction to SIP
- SIP Telephony in WLANs
- WLAN Hot-spot Setups
- Autoconfiguration
- Hot-Spot Authentication
- Simple Heuristics for Hot-spot Access
- WiFi Alliance Smart Client Authentication Procedure
- Service Announcements using Internet Media Guides (IMGs)
- Conclusion

Session Initiation Protocol (SIP, RFC 3261)

- Initiate, terminate, and modify sessions
  - Multimedia(!) sessions (*not just voice!*)
  - Point-to-point and multiparty
- Support for
  - Caller and callee authentication / call authorization
  - Privacy for call signaling and media streams
  - Media path with ensured QoS
  - Policy-based control mechanisms
- Flexible service creation
  - End-to-end principle (“dumb network”)
  - Support through SIP servers (located anywhere)
- Extensible protocol to cover new communication aspects
  - Such as presence and instant messaging

Terminology

- SIP User Agent
  - User Agent Server (UAS)
  - User Agent Client (UAC)

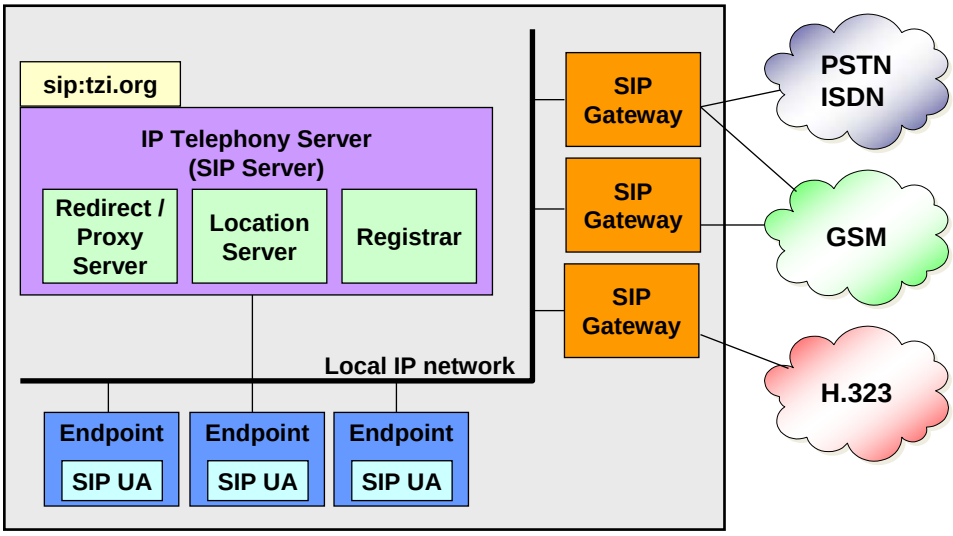
} **User Agent = Endpoint, Gateway**

- SIP Registrar
- SIP Location Server
- SIP Redirect Server
- SIP Proxy Server
- SIP Back-to-Back (B2B) User Agent

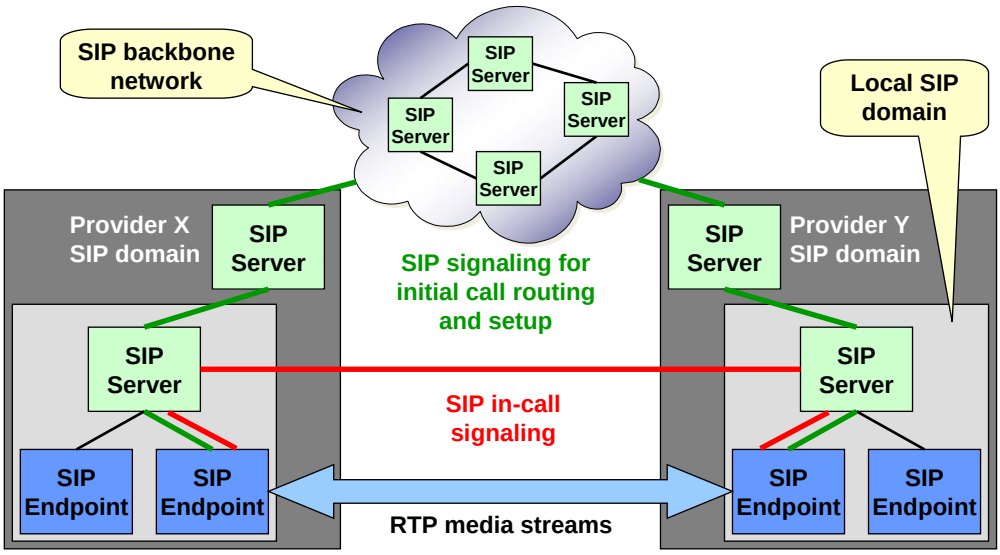
} **IP Telephony Server**

- SIP Application Servers

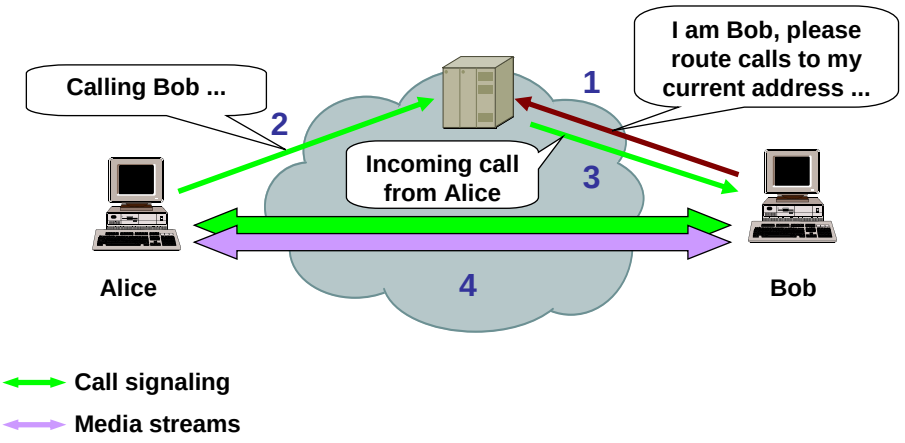
Local SIP Architecture



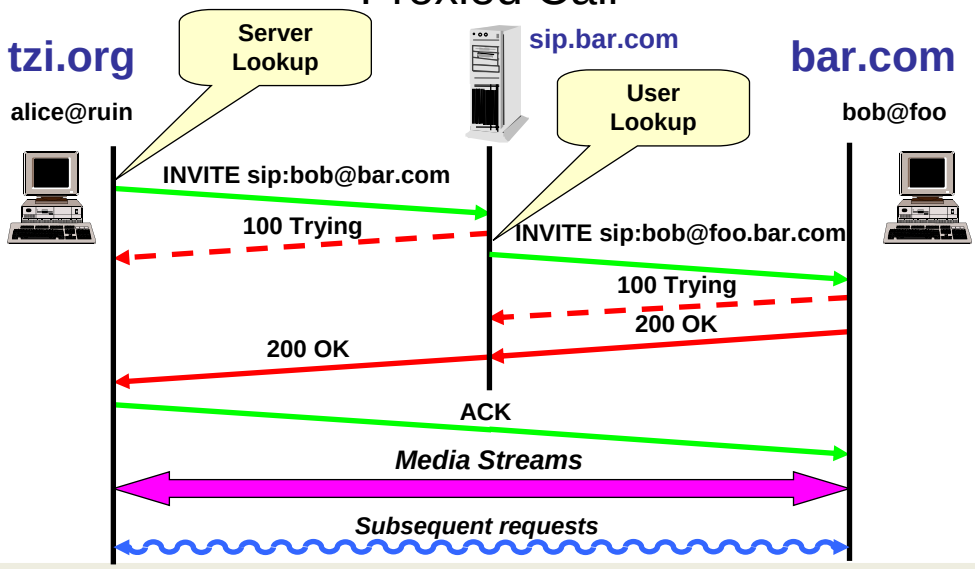
Global SIP Architecture



Simple Scenario of a SIP Call



Proxied Call



Relevant SIP Characteristics

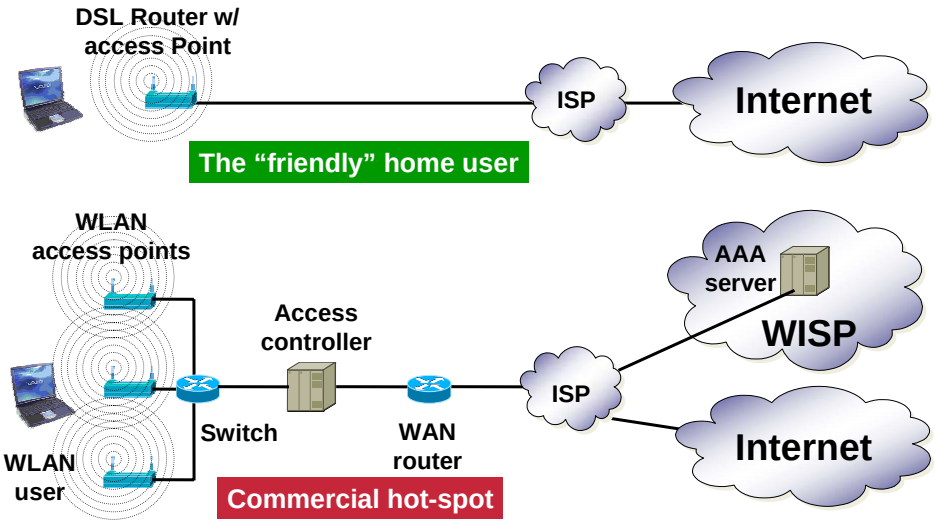
- SIP registrations are essential for reachability
  - Require periodic refresh and persistent addresses between refreshs
- Other SIP messages
  - Call control carries information about RTP media streams, possibly keys
  - Other messages may also carry data (e.g. MESSAGE)
- SIP may use TLS for hop-by-hop security
  - SIP phone to trusted server
- SIP messages may be encrypted end-to-end
  - SIP servers cannot see the contents
- SIP messages may be authenticated end-to-end
  - SIP servers cannot modify the contents

SIP Phones

- Support autoconfiguration
  - For IP stack parameters, time, SIP servers
  - User preferences
- Support STUN/TURN/ICE for NAT/firewall traversal
- Communicate directly with their trusted server (using TLS)
  - For outbound and inbound calls
- Configuration usually easy only via browser
  - Done once and then preferences are stored
  - No need to touch during regular operation

Examples for (S)IP WLAN phones

Typical Hot-Spot Setup



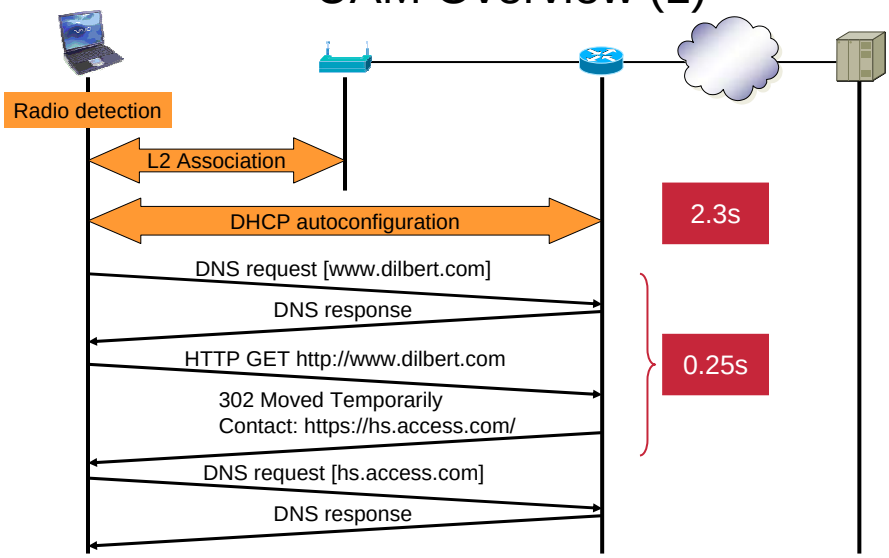
Autoconfiguration

- Scan 802.11 radio channels for access points
  - Determine SSIDs and modes of operation
- Device needs to obtain IP stack configuration
  - IP address + netmask
  - Default router (usually access point)
  - Domain name suffix
- Perform functions specific to IP telephony
  - Determine the presence of NATs
    - Obtain publicly usable addresses (STUN, TURN, ICE) for RTP media
  - Update registration with new contact information
    - Authenticate with telephony service provider

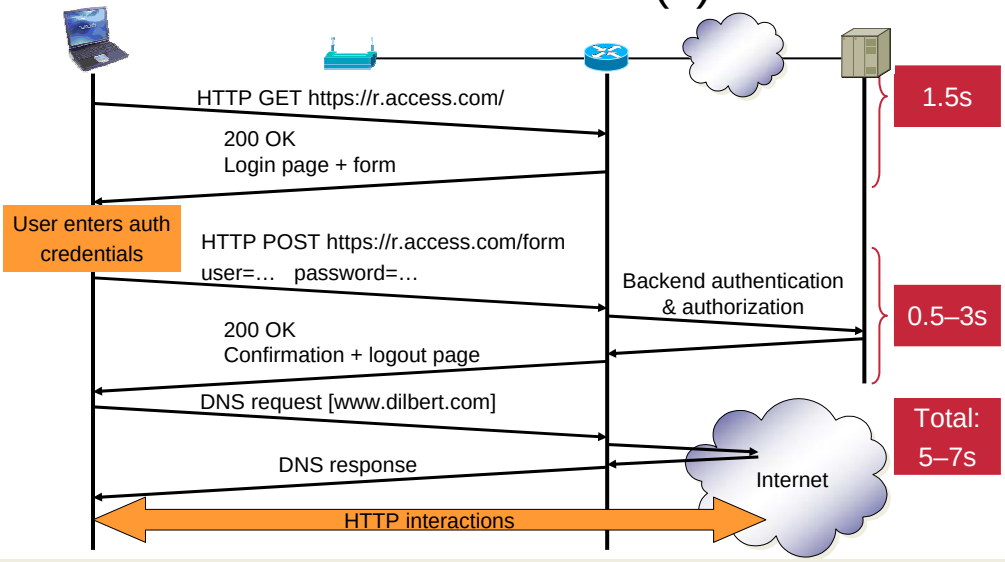
Hot-Spot Access

- Protecting WLAN hot-spots against unauthorized access
  - For privacy protection
  - For billing purposes
  - For legal reasons (accountability)
- Hot-spot access control
  - Open (just works – but IP autoconfiguration needed)
  - WEP-based (well, … – need to determine key from SSID)
  - Wi-Fi Alliance Universal Access Method (UAM) – commonly used
  - 802.1X & .11i (coming up)
  - IPsec and PPTP (sometimes; needs to be known in advance)
- Issue: manual process not suitable for WLAN IP phones
  - Determine what is used, who is the service provider, …

UAM Overview (1)



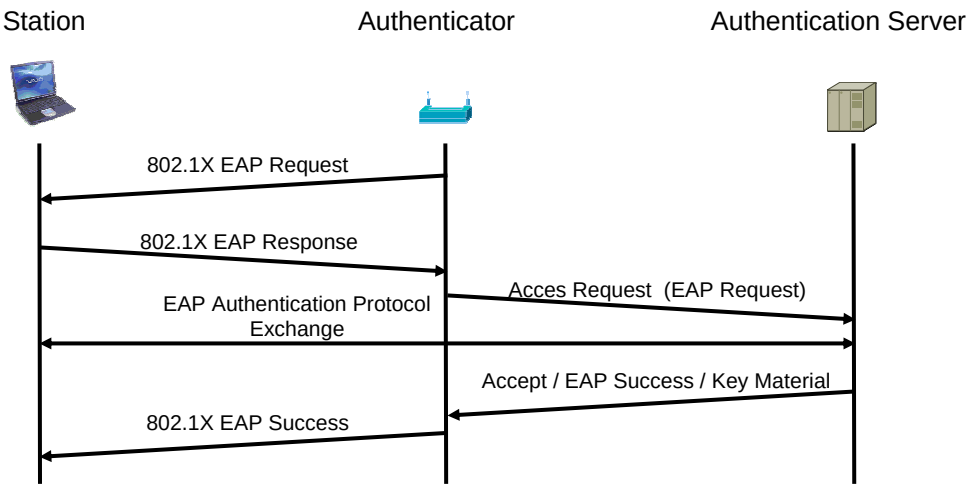
UAM Overview (2)



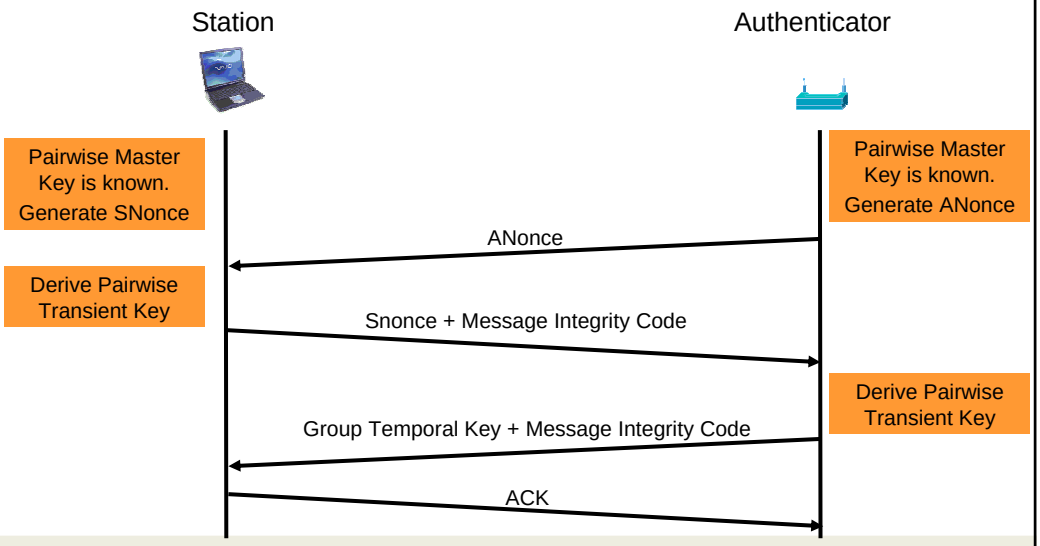
IEEE 802.11i

- IEEE 802.11i
  - IEEE 802.1X-based authentication with EAP
  - Supersedes IEEE 802.11 WEP-based security
- Extensible Authentication Protocol (EAP)
  - Media-independent framework for network access authentication
  - RFC 3748: EAP over PPP
  - IEEE 802.1X: EAP over wired IEEE 802 networks
  - IEEE 802.11i: EAP over IEEE 802.11
- IEEE 802.11i – 3 phases:
  1. IEEE 802.11 association
  2. IEEE 802.1X EAP authentication
  3. 4-Way Handshake and Group Key Handshake

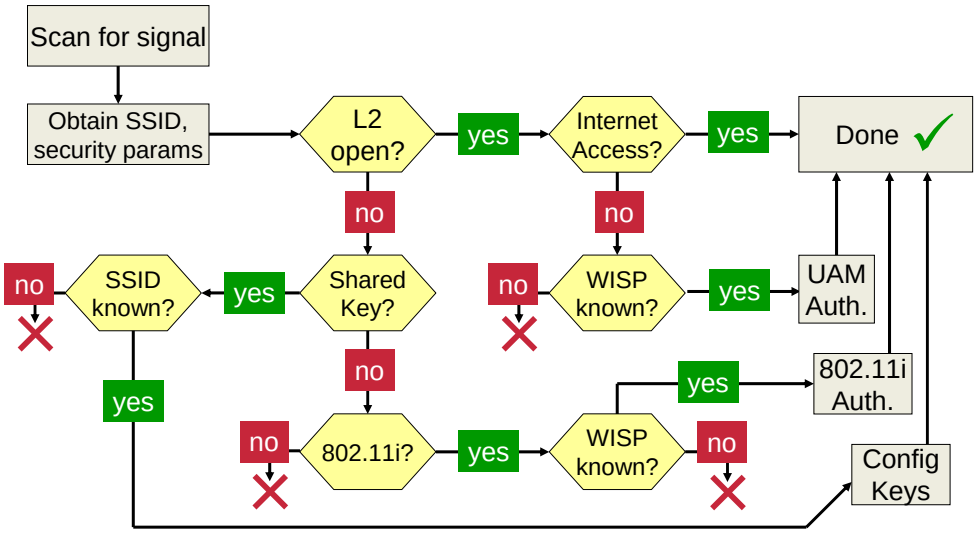
802.1X EAP Authentication



IEEE 802.11i 4-Way Handshake

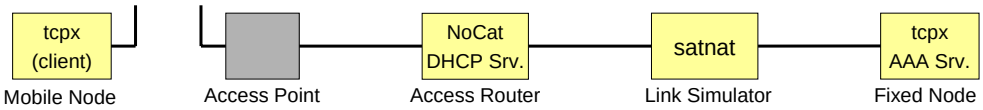


Authentication Heuristics



Evaluating Autoconfiguration and Authentication

- Prototype Implementation
  - ConnectivityDetector: monitors WLAN link, sends triggers
  - Enhanced DHCP client: receives triggers and timely initiates DHCP
  - AutoAuthenticator: when triggered performs UAM authentication
  - tcpx test tool: data transfer as soon as connectivity established
- Controlled tests with experimental setup on the road



- Real-world tests with real-world hot-spots: mixed success

Observations with Real-World Hot-Spots

- If it works: authentication usually done in less than 10s
- But: Hot-spots are often “a little but not entirely unlike” UAM
- Deviation from UAM web page structure
  - Initial overview pages with a link to a login page
  - Need to find and follow the link requires further second-guessing
- Deviation from UAM field structure and names
  - Slightly or totally different names
  - Additional fields to fill in (e.g., checkbox for terms and conditions)
- Multiple service providers to choose from
- JavaScript code, etc. in web pages
  - Requires more effort to parse and evaluate

First Step: WiFi Alliance Smart Clients

- Use machine-readable format for authentication procedure
  - XML-based data structures (“hidden” in HTML page!)
  - Otherwise, follow the same approach as UAM as above
- Use TLS
- Redirect message provides details about hot-spot and operator
  - Login and logoff URIs, location
- Subsequent authentication exchange
  - User name, password, …
- Abort and logoff messages
- Still no well-defined multi-provider support

Sample WISP “Service Offer”

```
<?xml version="1.0" encoding="UTF-8"?>
<WISPAccessGatewayParam
       xmlns:xsi=”http://www.w3.org/2001/XMLSchema-instance”
       xsi:noNamespaceSchemaLocation=
           "http://www.acmewisp.com/WISPAccessGatewayParam.xsd">
  <Redirect>
    <AccessProcedure>1.0</AccessProcedure>
    <AccessLocation>12</AccessLocation>
    <LocationName>
      ACMEWISP,Gate_14_Terminal_C_of_Newark_Airport
    </LocationName>
    <LoginURL>http://www.acmewisp.com/login/</LoginURL>
    <AbortLoginURL>
      http://www.acmewisp.com/abortlogin/
    </AbortLoginURL>
    <MessageType>100</MessageType>
    <ResponseCode>0</ResponseCode>
  </Redirect>
</WISPAccessGatewayParam>
```

Issue: User Policy for Access

- Hot-spot tariff models mostly time-based
  - Very coarse granularity
  - Users pay per half hour or hour
    - But even per minute charges are of little use
  - Flat rates still uncommon
- User to pay for her phone automatically registering?
- User policy
  - Which provider to accept, which ones to prefer
    - e.g., flat-rate only automatically, others inquired
- Hot-spot support for (S)IP phones?
  - Proxy for registration messages only ➔ risk of misuse (IP-over-SIP?)
  - Security aspect ➔ no TLS to trusted server, SIP user becomes visible

Internet Media (and Service) Guides

- Delivery framework
  - Multicast announcements
    - FLUTE: Reliable multicast
    - Workable in broadcast networks(!)
  - Individual retrieval and asynchronous notifications
    - SIP + HTTP
  - Full descriptions (arbitrary size, not limited to MTU) or deltas
- Description
  - Envelope format for content identification, versioning, security
  - Intended for media descriptions (e.g., electronic program guides)
  - May carry arbitrary data (to be defined elsewhere)
  - Allows embedding WiFi Alliance **`<WISPAccessGatewayParam>`**

Adding Services to IMGs

- Expand on a general hot-spot definition
  - Allow for multiple service providers
  - Embed WiFi alliance “redirection” reply as part of the announcement
  - Add explicit information about WISP, tariff, etc.
    - Include information about roaming charges
  - Add hot-spot-specific services (e.g., telephony proxying without charge)
  - Add regional services
    - e.g., ITSPs with local terminations
  - Add geo information (e.g., GPS)
- Enable drawing up a map of a region, city, quarter, …
  - Gained from combining local + global announcements
  - Allow for advance retrieval and caching

Conclusions

- Only few hot-spots are really UAM compliant
  - Variable naming of username and password fields, etc.
  - Sites with multiple Wireless Internet Service Providers
- Determining wireless services difficult
  - WISP identities, tariff models, etc.
  - User policies important for reasonable access models
- Enhanced service announcements
  - More detailed information about the current hotspot
  - Enable smart decisions for smart clients
- Explicit service support for IP telephony in hot-spots desirable