Deploying VoIP over Public Wireless Networks

Challenges and Perspectives

2005-07-05 IQPC VoWLAN Conference, Berlin

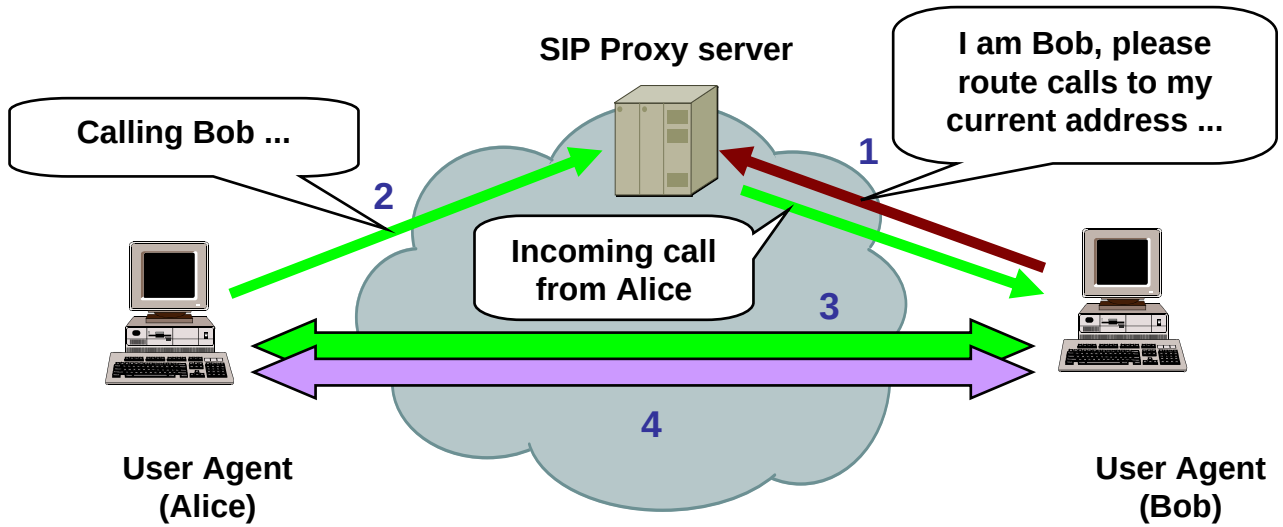
Dirk Kutscher dku@tzi.org
Jörg Ott jo@netlab.hut.fi

Overview

- SIP and WLAN Phones
- Typical Hot-Spot Setups
- Autoconfiguration
- Hot-Spot Authentication (Mechanism + Policy)
- SIP Services in Hot-Spots
- Some Thoughts on Solutions
- Conclusion

Session Initiation Protocol (SIP, RFC 3261)

- Initiate, terminate, and modify sessions (voice, multimedia)
  - Extensible and flexible end-to-end protocol
  - User and service-provider-based service creation
  - Multimedia calls, conferencing, presence, instant messaging, chat, …
  - Inherent support for mobility
- Using IP telephony service providers (ITSPs) or peer-to-peer
  - Operator-based approach essential part of UMTS Release 5 IMS
- User registration
  - At multiple locations
- Call routing
  - Based upon registrations
  - User & provider policy
  - Possibly presence
- Media stream configuration



Relevant SIP Characteristics

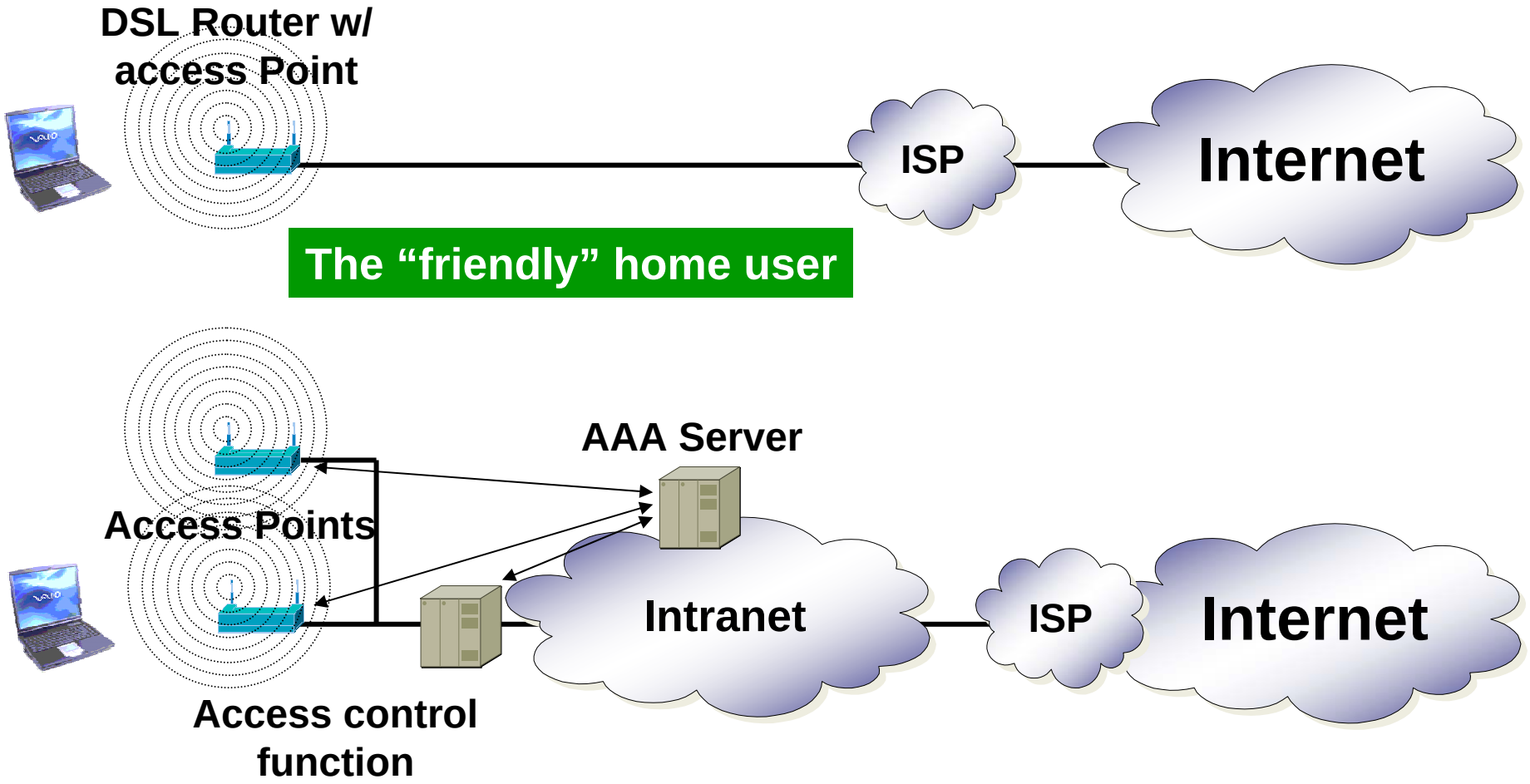
- SIP registrations are essential for reachability
  - Require periodic refreshing and persistent addresses between refreshes
- Other SIP messages
  - Call control carries information about RTP media streams, possibly keys
  - Other messages may also carry data (e.g. MESSAGE)
- SIP may use TLS for hop-by-hop 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 (except for a few headers)

Examples for (S)IP WLAN phones

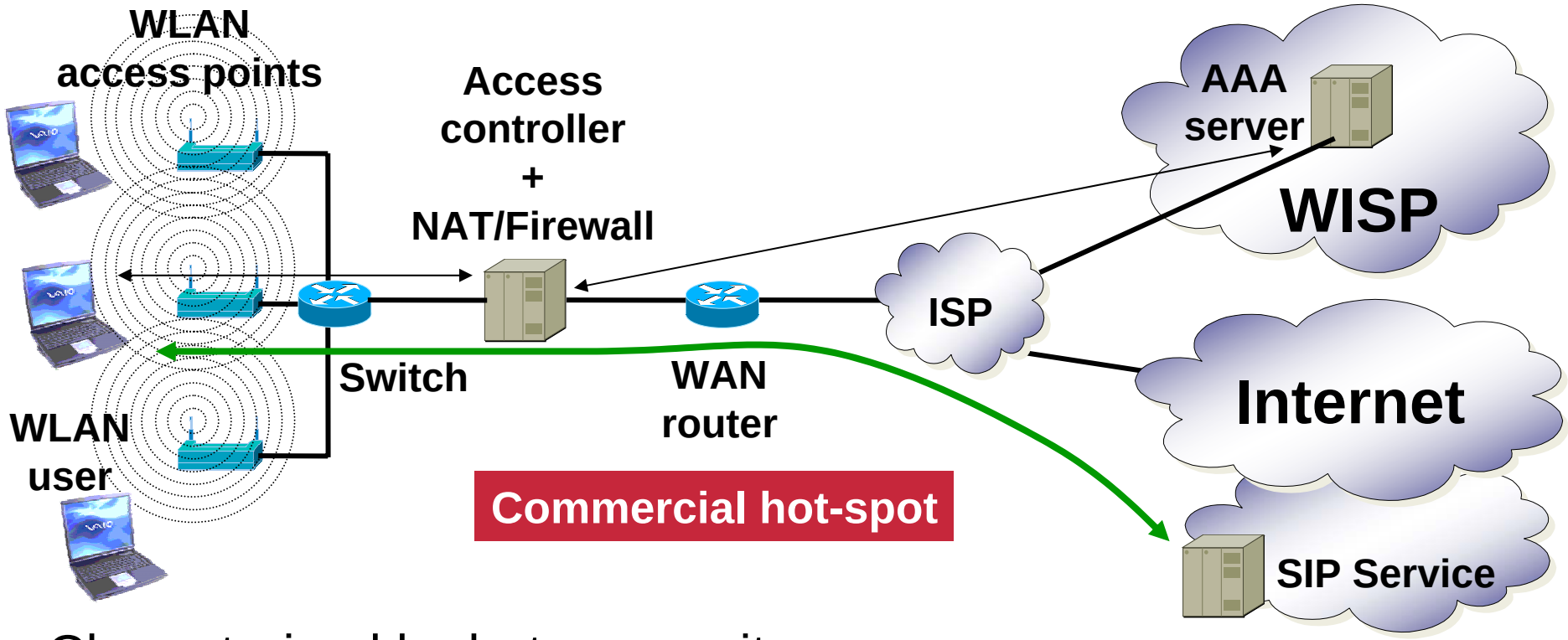
Typical (WLAN) SIP Phones Today

- Support autoconfiguration
  - For IP stack parameters, time, SIP servers
  - User preferences
- Support NAT/firewall traversal (using STUN/TURN/ICE)
- Communicate directly with their trusted server (using TLS)
  - For outbound and inbound calls
- Configuration usually easy only via a web browser
  - Limited user interface due to form factor
  - Done once and then preferences are stored
  - No need to touch during regular operation
  - (enterprise and operator phones use centralized provisioning)

Typical Hot-Spot Setups (1)

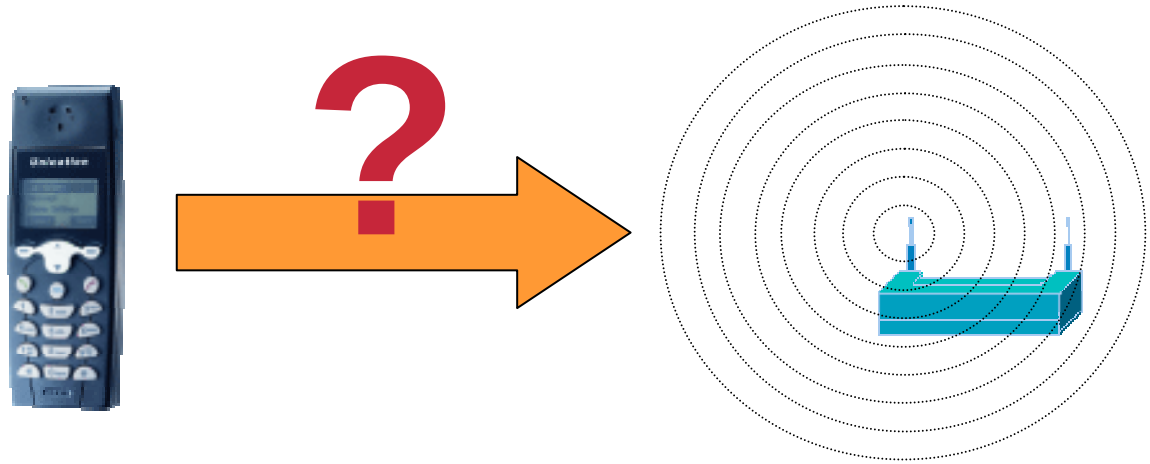


Typical Hot-Spot Setups (2)



- Characterized by heterogeneity
  - Different WISPs use different authentication mechanisms
  - Service / access portals for multiple WISPs
  - (Local communication among devices may be possible)

So, how to access a Hot-Spot?

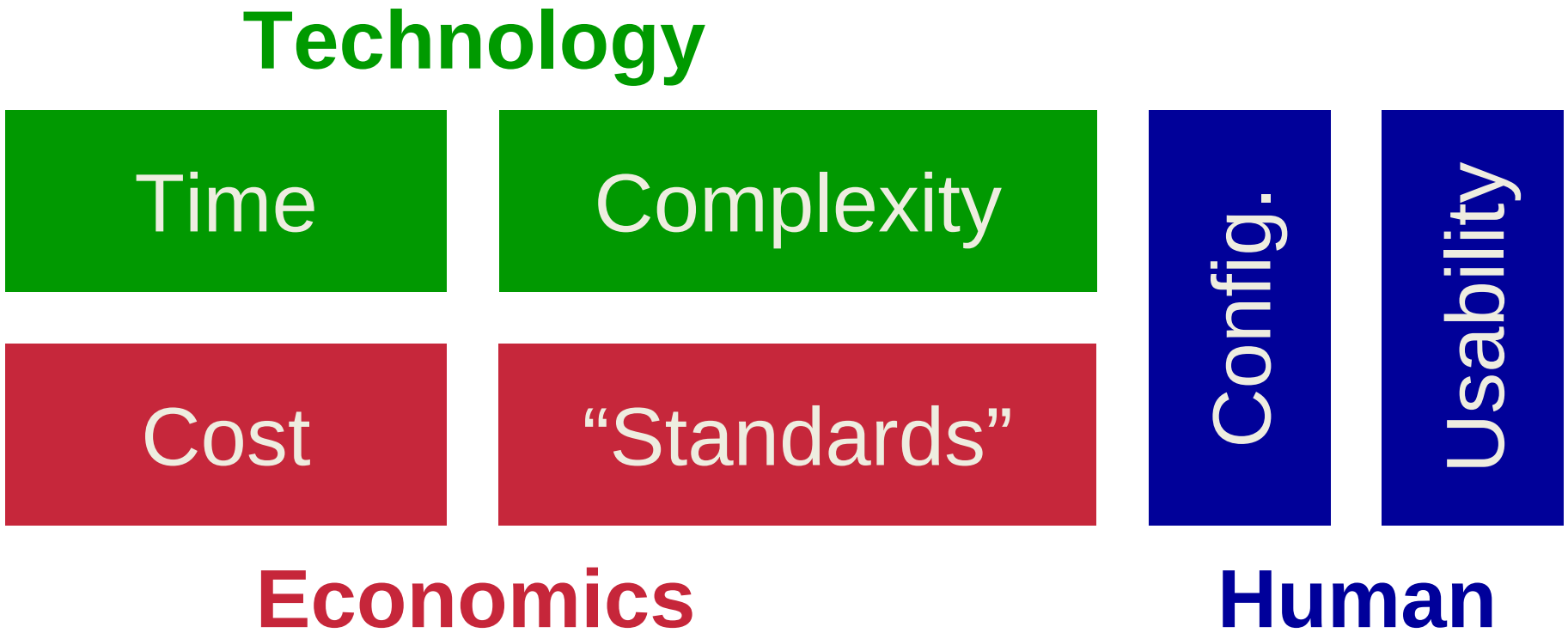


1. Autoconfiguration
2. Authentication

Accounting & Billing

3. Placing SIP Calls
4. Receiving SIP Calls
5. Further SIP Services

Access Issues: Overview



Technical Issues

1. Hot-Spot Autoconfiguration

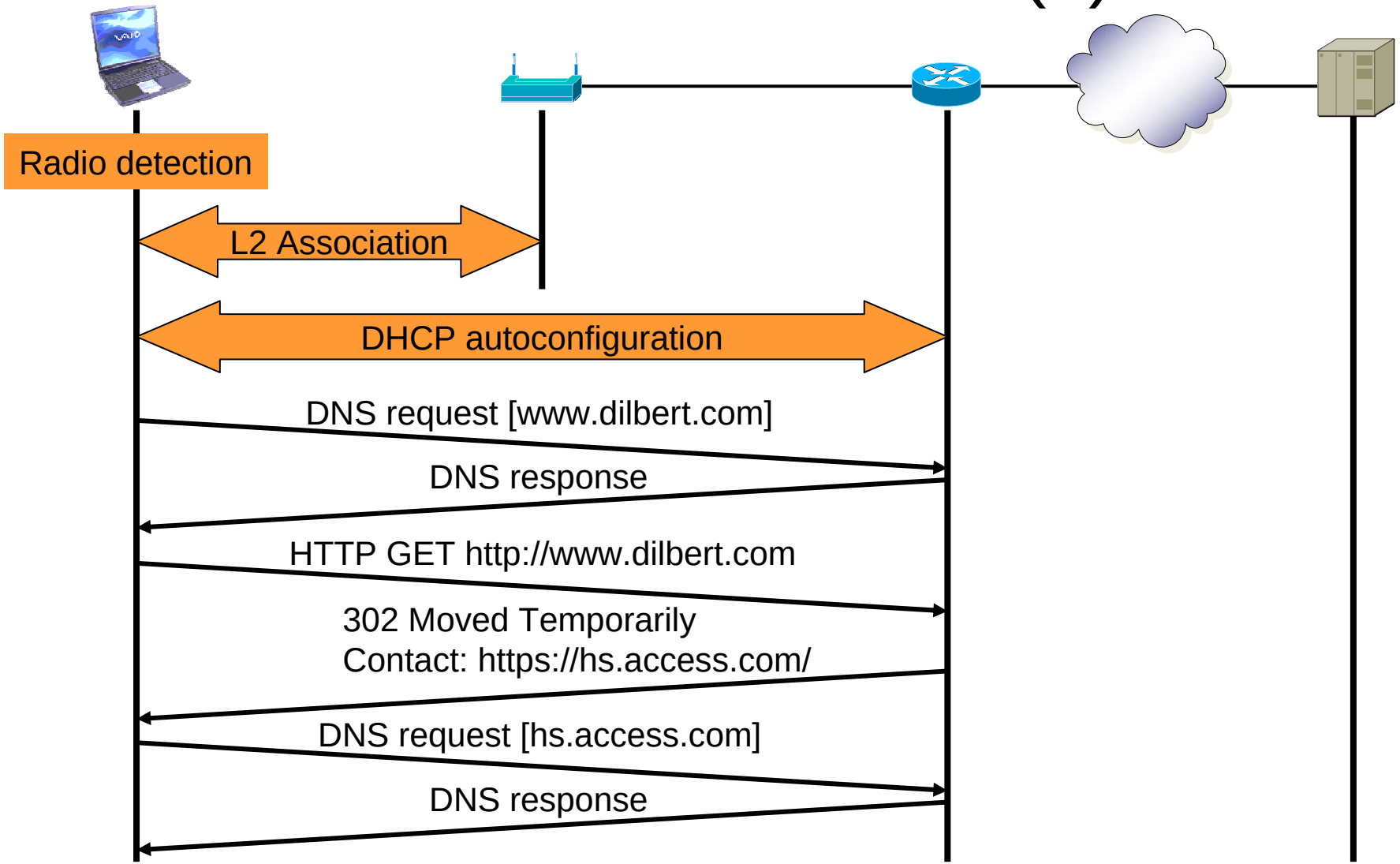
- L1/2: Scan 802.11 radio channels for access points
  - Determine SSIDs and modes of operation
- L3: Device needs to obtain IP stack configuration
  - IP address + netmask
  - Default router (usually access point)
  - Domain name suffix
- L4-7: Perform SIP-specific functions
  - Determine the presence of NATs
    - Obtain publicly usable addresses (STUN, TURN, ICE) for RTP media
  - Update SIP registration with new contact information
    - Authenticate with telephony service provider

Return to this later!

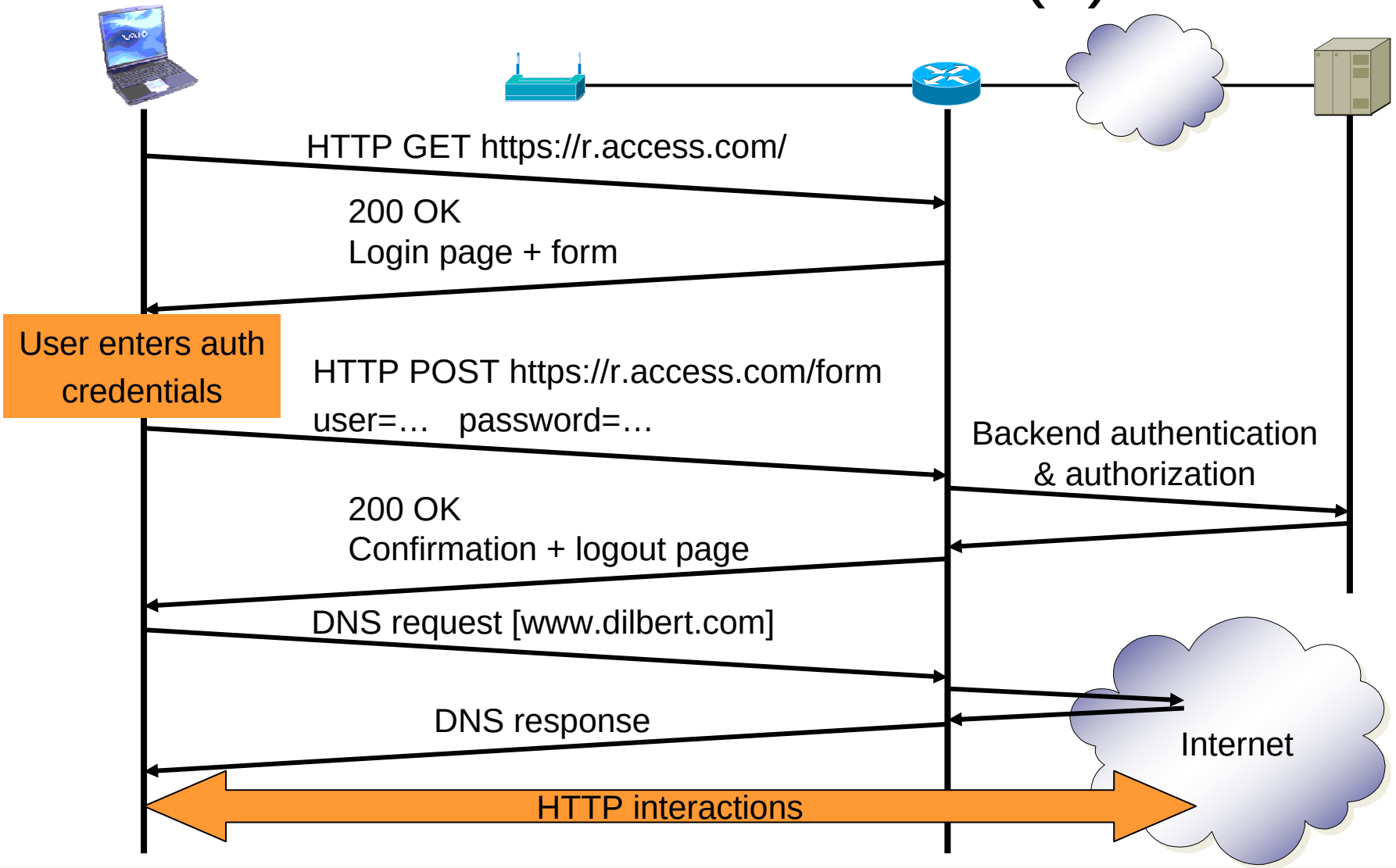
2. Authentication & Hot-Spot Access

- 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 shared key from SSID)
  - Wi-Fi Alliance Universal Access Method (UAM) – commonly used (and most problematic…)
  - 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)



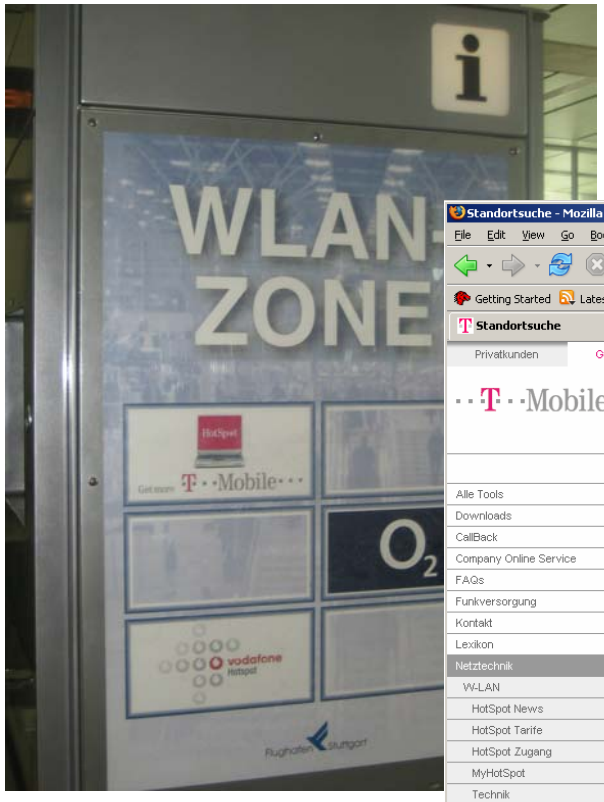
UAM Overview (2)

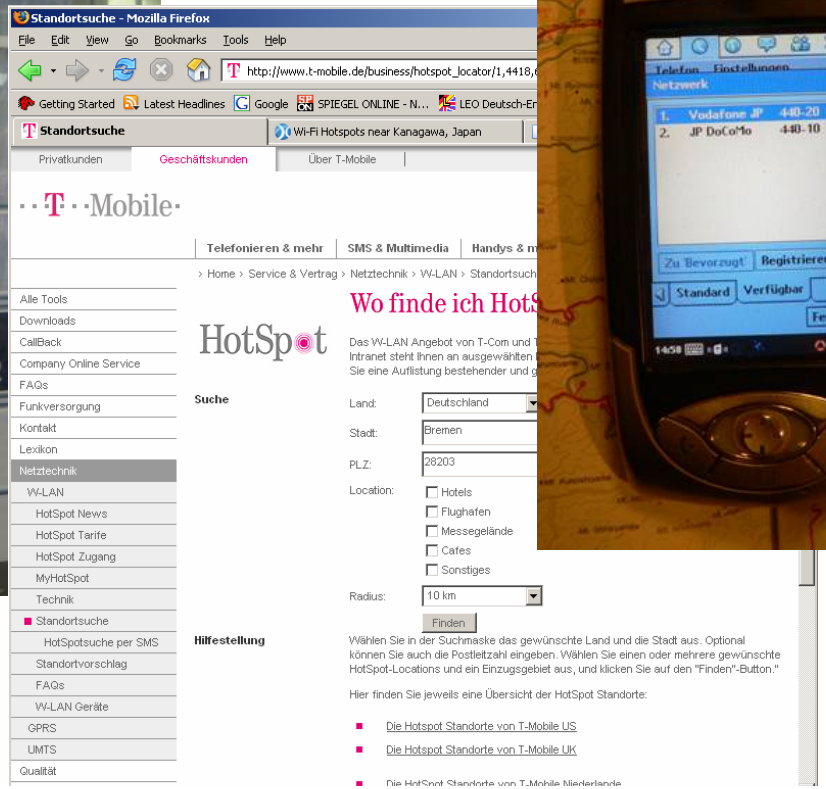


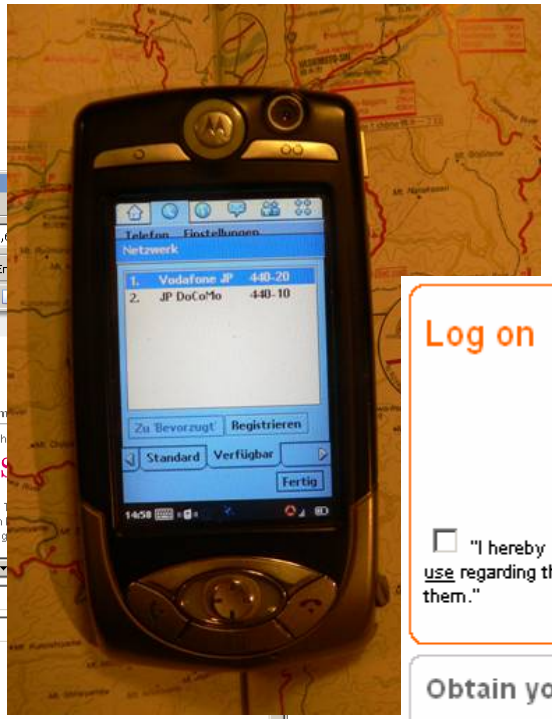
UAM Issue: Real-World Hot-Spots

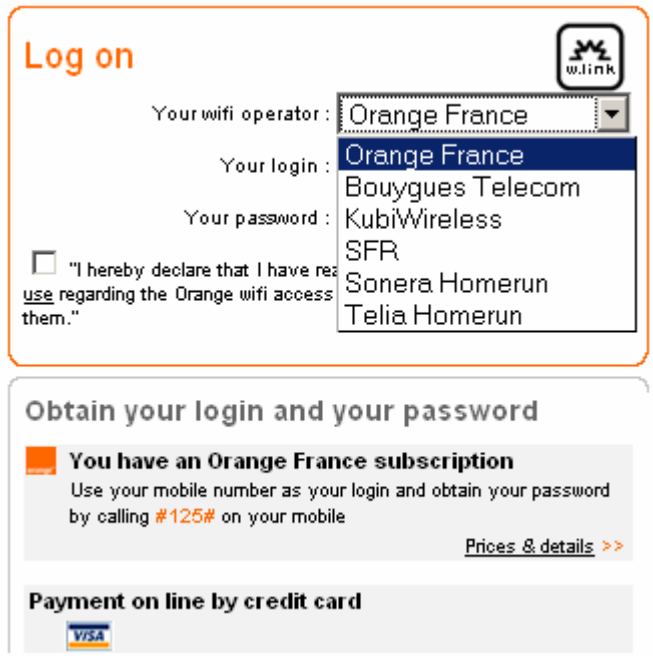
- If it works: authentication usually done in less than 10s
  - Once you have chosen a particular service provider
- But: Hot-spots are often “a little but not entirely unlike” UAM
- Deviation from UAM web page structure
  - Initial overview pages with a link to a login page
  - Need to find and follow 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

Issue: Usability



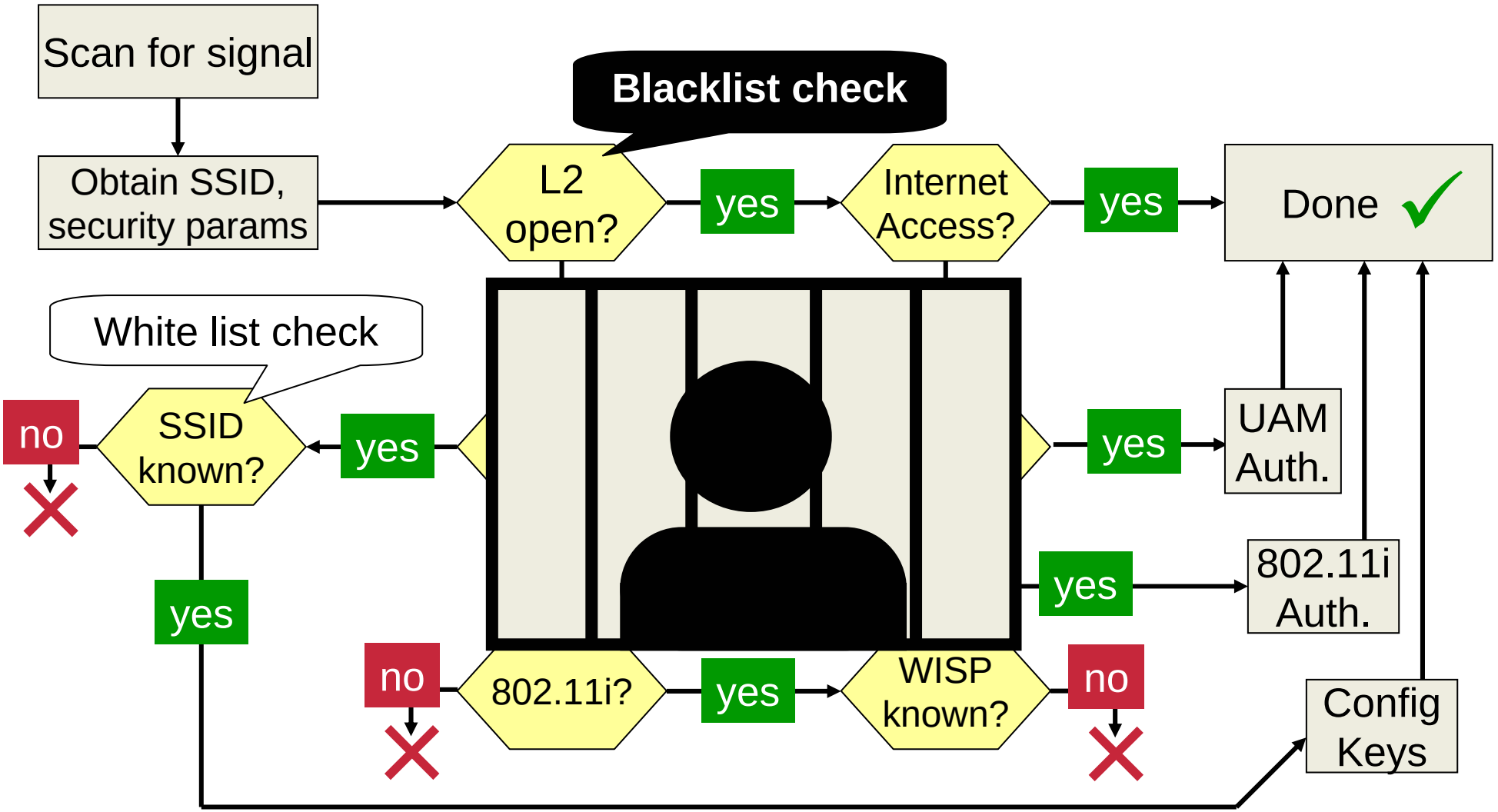






Can clearly benefit from some optimizations… :-)

Heuristics-based Authentication Automation



Some Technical Solutions

First Step: WiFi Alliance Smart Clients

- Use machine-readable format for authentication procedure
  - Rudimentary 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, no tariff information, …

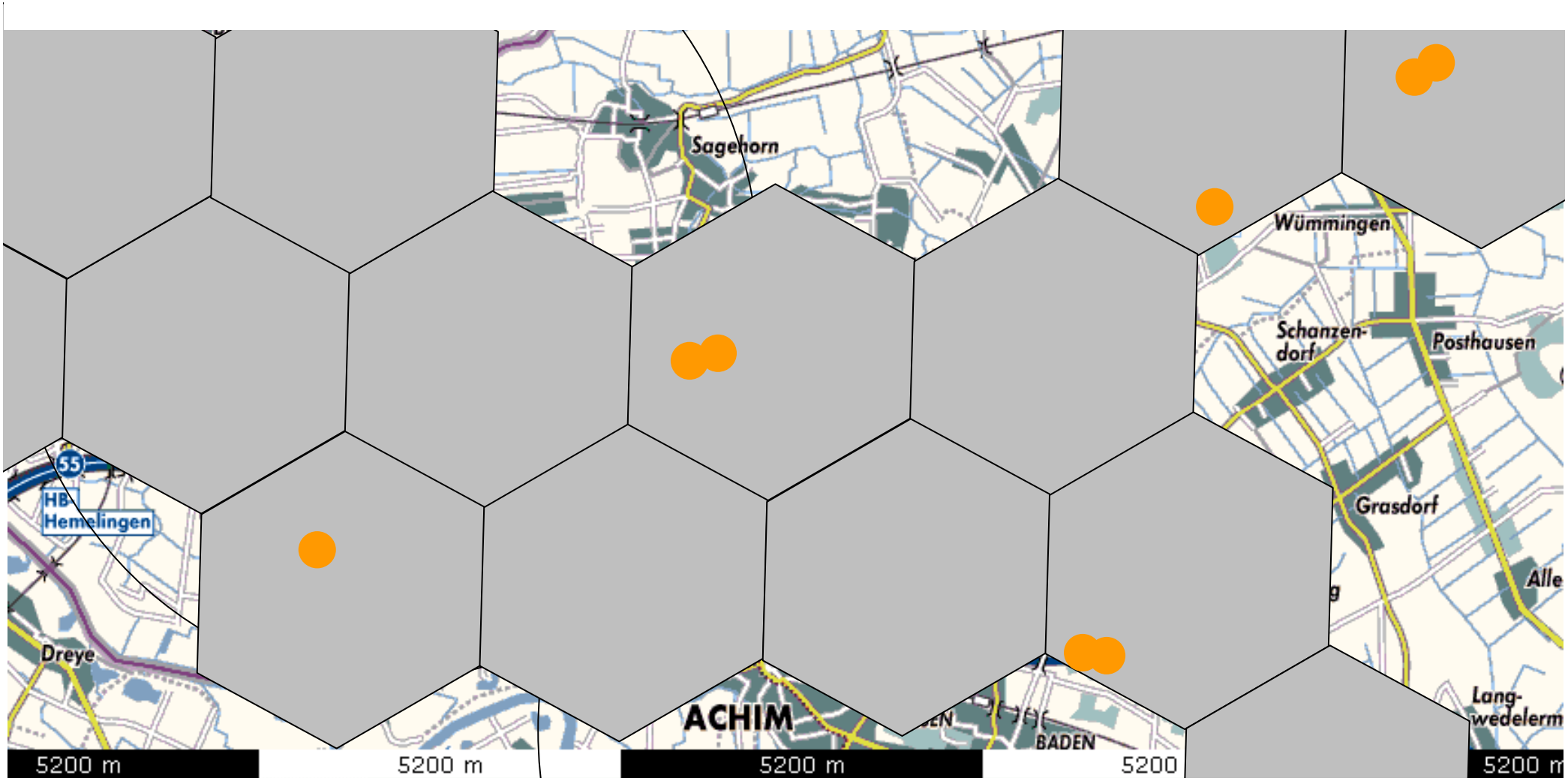
Sample WISP “Service Offer”

```
<?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>
```

One Step Further: IEEE 802.21

- IEEE 802.21: Network Information Service as one component
  - For supporting media-independent handover
- Objective: acquire global view in a heterogeneous network
  - Facilitate seamless handover
  - Allow network selection according to MN's requirements
  - Information about lower layers (neighbor maps) but also higher layers (Internet access, VPN services, VoIP services etc.)
- MIIS allows looking for network service in a geographic region
  - e.g., look for available 802.11 networks using the current 3G link
- IEEE 802.21 still a moving target
  - Might provide transport and data models for describing higher services
  - Primarily targeted at handover optimization

All the way: Network Service Maps



IEEE 802.16 coverage zone

3G cell

802.11 WLAN hotspot

Economic / Cost Issues

Accounting / Billing and Access Policy

- Hot-spot tariff models mostly time-based
  - Very coarse granularity
  - Users pay per half hour or hour
    - Getting better recently, but even per minute charges are of little use
  - Flat rates still uncommon
    - Even where they exist: lack for global roaming
- Regardless of the rate types: user needs to choose
  - Present: typically requires web research beforehand or studying tariff models as described in the hot-spot's web pages
  - Often, true cost cannot be determined ad-hoc
  - Network service maps help to address this part

Getting more tricky with SIP

- Unlike with (closed) cellular networks:
  - IP networks allow arbitrary information to be exchanged
  - Infrastructure provider (WISP, ISP) and application service provider (ITSP) are typically **not** identical
- Consequence: from a WISP's perspective, the SIP control messages are data traffic
  - This is a feature! (and should stay this way)
  - Yet, the WISP may want them to be billed for
  - Exceptions: flat rates or community efforts

  (not assuming this ideal for the next few slides)
- WISP tolerance threshold may be low
  - See prior DNS abuse for tunneling packets (want to avoid "IP-over-SIP")

3., 4., 5. Regular SIP Operation

- Placing a call
  - User-initiated activity: seems to provide a natural mapping to login/logout
    - Pre- or Post-dial delay
    - Unsuccessful call would still incur WLAN billing
    - WLAN billing granularity may not match call duration
    - What to infer from teardown?
      - Will another call be placed shortly? How long to keep the WLAN access open?
- Receiving a call
  - Registration required + continuous soft state updates
    - When shall a WLAN phone register?
    - Which of the potentially suitable hotspots shall be used?
    - How shall a phone know how long a user will remain in a hot-spot?
    - Configuration nightmare OR manual interaction OR potentially expensive OR rather limited provider selection O turn off your phone when you don't need it
- Further services
  - Presence incurs regular traffic (state updates), receiving messages prior registration
- General issue: background SIP traffic required

Meta-Issue: Security

- Hotspots cannot and should not (need to) be trusted
  - Different hotspots variants from private access points to commercial service
  - All kinds of attacks are conceivable: eavesdropping, impersonation etc.
    - Public WLANs are typically broadcast networks, after all
- Need strong security for all aspects of communication
  - SIP signaling
  - Real-time media transport
  - Demand will grow anyway, e.g., to prevent IP telephony spam (SPIT)
- Excludes involvement of independent WISP in SIP signaling
  - And thus limits the solution space

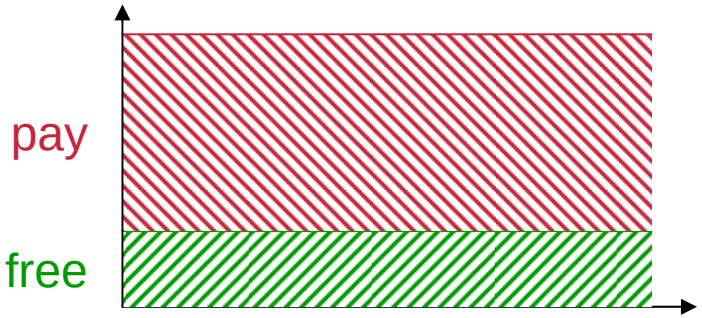
Economics: “Solutions”

The Non-Solution: 3GPP-style Control

- WISP assumption: letting SIP messages just pass is too risky
  - Proxy for registration messages only ➔ risk of misuse (IP-over-SIP?)
  - As soon as TLS is used, impossible to inspect messages
- Provide a local SIP proxy in the Hot-spot to support SIP phones?
  - Announced as part of service announcement
  - Require local connection to proxy (which then forwards SIP messages)
- Security aspect ➔ no TLS to trusted server, user becomes visible
  - Remedy: use end-to-end encryption (S/MIME)
  - WISP can no longer inspect message contents and may block traffic
- Any kind of screening will prevent true end-to-end SIP operation
  - Inhibit innovation (in the “best” case)
  - Prevent proper functioning (in the worst case)
- Would ultimately require WISP to become or explicitly host ITSP

A Half-baked Solution

- WISP to allow a minimum traffic flow ("bytes per hour")
  - Free of charge or at minimal cost
  - Accept (marginal) misuse



- Example: ~1 hour period (65.5 minutes)
  - SIP UDP registration and STUN traffic: 41 packets, Ø 1.8 bytes/s, 6.4 KB/h
    - 2 registrations (incl. digest authentication)
  - Comparison: Skype traffic: 1274 packets, Ø 36.5 bytes/s, 130 KB/h
- Issues:
  - How much background traffic is tolerable?
    - Depends on client implementations and settings and SIP service providers
    - Cannot necessarily be influenced by the user (and she should not need to worry)

A Workable Solution

- Don’t try to invent new metering and tariffing mechanisms that mimic POTS
  - Treat signaling and media transport as what they are: IP traffic
  - Apply the same tariffing schemes as for any other data traffic
  - Keep access service separate from telephony service
- Need universal WLAN hotspot flat rates
  - Allow for roaming
  - Don’t try to count bytes
  - Don’t consider hotspot users cash cows
- Business models for ITSPs
  - Bundle telephony service to hotspot flat rate?
  - Promote roaming possibilities, provide users with information about usable hotspots?
- In summary: Make life easier for users and service providers

Some Recent Influencing Trends

- Increased capabilities in WLAN phones
  - Sufficient screen resolution + web browser
  - Linksys WLAN phone, Nokia 770 Internet tablet, PDAs, recent cellphones
- Unlicensed Mobile Access (UMA)
  - Mobile operators leveraging WLAN as access to their core networks
  - Governed by basic mobile operator model
  - (also IMS may be expanded to wireless networks such as WiFi and WiMAX)
- Handset manufacturer and WISPs
  - Example: Boingo Wireless licensing
    - Software suite for (automated) operation of embedded devices (Boingo hotspots)
  - Example: Toshiba ConfigFree wireless device driver (for laptops)
- Community and other free hot-spot efforts grow steadily
  - www.free-hotspot.com, www.freifunk.de, en.fon.com, SFO Bay area, Freiburg, …

Relevant IETF Activities

- Connection establishment in challenged networks
  - STUN, TURN, ICE
- General SIP security
  - SIP over TLS, S/MIME in SIP (all specified in RFC 3261)
- Secure media transport and session setup
  - SRTP (RFC 3711)
  - Key management: establish session keys for SRTP with SDP/SIP
    - MIKEY-based key-management and other approaches
  - Recent proposals: ZRTP (key management in RTP stream)
- Emergency Context Resolution with Internet Technologies (ECRIT)
  - Emergency call routing, work in progress
- Session PEERing for Multimedia INTerconnect (SPEERMINT)
  - VoIP peering, work in progress

Conclusions

- WLANs are widely deployed today
- Public hot-spots usable with laptops — but users must care
- Barely usable for embedded devices
- Automated authentication approach solves part of the problem

- Support for SIP-based communications limited by tariff models
- Proper security mechanisms inhibit independent WISP support

Two extreme options

1. Cellular network style with present mobile operators
2. Flat-rate operation, common authentication schemes, and service discovery mechanisms key to making SIP just work in hot-spots